EnCase® Legal Journal

Over the last decade, the field of computer investigations and forensics has expanded greatly, mirroring the explosion of digital data in society at large. What began as a practice of a select few technical experts has become a field in which thousands are involved. Computer evidence is now a mainstay not only in criminal matters, but also in civil discovery, internal corporate investigations, and computer security incident response. In each of these situations, the authentication and presentation of electronic evidence at trial is either a primary goal or, at a minimum, a consideration that the computer investigator must take into account.

This EnCase® Legal Journal is provided with three goals in mind. First, it reports on court decisions involving EnCase® software, as well as notable court decisions involving computer evidence in general. Second, it addresses how the EnCase process facilitates the authentication and admission of electronic evidence in light of past industry practices and the current status of the law, providing investigators and their counsel with an added resource when addressing questions involving computer forensics and the use of EnCase software. Third, it focuses on the collection and preservation of electronic evidence in civil matters and internal investigations, as well as certain legal issues (such as workplace privacy) that arise in that context.

The EnCase Legal Journal is provided for informational purposes and is not intended as legal advice, nor should it be construed or relied upon as such. Each set of circumstances may be different and all cited legal authorities should be confirmed and updated.

Just as Guidance Software is committed to ongoing product research and development, so must we also be on top of the latest legal developments impacting this field. As such, this journal should be considered as a work perpetually in progress. If you have any questions, comments or suggestions for future revisions, please feel free to contact either of us at John.Patzakis@EnCase.com or Victor@EnCase.com

John Patzakis
Victor Limongelli
Guidance Software, Inc.

Table of Contents

6. Challenges to EnCase Software and Cases Involving EnCase Software.......... 60

New in November 2005 Revision

The following sections have been added or revised for this edition:

<u>Section 1.5:</u> Expanded discussion and added detail regarding *Zubulake* and *Greathouse* cases.

<u>Section 2.3:</u> Added discussion of *Logan v. State*, as well as a cross-reference to *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*

<u>Section 3.1:</u> Added discussion of *Galaxy Computer Services, Inc. v. Baker*

<u>Section 4.1:</u> Added very brief discussion of *United States v. Crume*

<u>Chapter 6:</u> Added discussions of *State (South Dakota) v. McKinney, United States v. Bass, United States v. Davis, United States v. Long, Foust v. McFarland,* and *State (N.C.T. of Delhi) v. Sandhu*, as well as cross-references to *Logan v. State, United States v. Riccardi,* and *United States v. Calimlim*

<u>Section 7.3:</u> Added discussions of *United States v. Riccardi, United States v. Brooks,* and *United States v. Calimlim*

<u>Section 7.5:</u> Added very brief discussion of *United States v. Triumph Capital Group*

<u>Chapter 9:</u> Added further discussion of *Zubulake v. UBS Warburg LLC*

<u>Section 9.1:</u> Added discussions of *Tantivy Communications, Inc. v. Lucent Technologies, Inc.* and *Broccoli v. Echostar Communications Corp.*

<u>Section 9.3:</u> New section that addresses metadata in civil discovery

<u>Section 10.4:</u> Added discussion of *United States v. Long*

Authentication of Computer Evidence

§ 1.0 Overview

Documents and writings must be authenticated before they may be introduced into evidence. The United States Federal Rules of Evidence, as well as the laws of many other jurisdictions, define computer data as documents.[1] Electronic evidence presents particular challenges for authentication as such data can be easily altered without proper handling. The proponent of evidence normally carries the burden of offering sufficient support to authenticate documents or writings, and electronic evidence is no exception.

What testimony is required to authenticate computer data? How does a witness establish that the data he or she recovered from a hard drive is not only genuine but completely accurate? Are there guidelines or checklists that should be followed? How familiar with the software used in the investigation must the examiner be in order to establish a proper foundation for the recovered data? These are some of the questions that face computer investigators and counsel when seeking to introduce electronic evidence. This chapter will address these questions.

§ 1.1 Authentication of Computer Data

Oftentimes, the admission of computer evidence, typically in the form of active ("non-deleted") text or graphical image files, is accomplished without the use of specialized computer forensic software. Federal Rule of Evidence 901(a) provides that the authentication of a document is "satisfied by evidence sufficient to support a finding that the matter in question is what the proponent claims." The Canada Evidence Act specifically addresses the authentication of computer evidence, providing that an electronic document can be authenticated "by evidence capable of supporting a finding that the electronic document is that which it is purported to be."[2] Under these statutes, a printout of an e-mail message can often be authenticated simply through direct testimony from the recipient or the author.[3]

The US Federal Courts have thus far addressed the authentication of computer-generated evidence based upon Rule 901(a) in much the same manner as other types of evidence that existed before computer usage became widespread.[4] *United States v. Tank,*[5] which involves evidence of Internet chat room conversation logs, is an important illustration.

In *Tank*, the Defendant appealed from his convictions for conspiring to engage in the receipt and distribution of sexually explicit images of children and other offenses. Among the issues addressed on appeal was whether the government made an adequate foundational showing of the relevance and the authenticity of a co-

conspirator's Internet chat room log printouts. A search of a computer belonging to one of Defendant Tank's co-conspirators, Riva, revealed computer text files containing "recorded" online chat room discussions that took place among members of the Orchard Club, an Internet chat room group to which Tank and Riva belonged.[6] Riva's computer was programmed to save all of the conversations among Orchid Club members as text files whenever he was online.

At an evidentiary hearing, Tank argued that the district court should not admit the chat room logs into evidence because the government failed to establish a sufficient foundation. Tank contended that the chat room log printouts should not be entered into evidence because: (1) they were not complete documents, and (2) undetectable "material alterations," such as changes in either the substance or the names appearing in the chat room logs, could have been made by Riva prior to the government's seizure of his computer.[7] The district court ruled that Tank's objection went to the evidentiary weight of the logs rather than to their admissibility, and allowed the logs into evidence. Tank appealed, and the appellate court addressed the issue of whether the government established a sufficient foundation for the chat room logs.

The appellate court considered the issue in the context of Federal Rule of Evidence 901(a), noting that "[t]he rule requires only that the court admit evidence if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification . . . The government must also establish a connection between the proffered evidence and the defendant."[8]

In authenticating the chat room text files, the prosecution presented testimony from Tank's co-conspirator Riva, who explained how he created the logs with his computer and stated that the printouts appeared to be an accurate representation of the chat room conversations among members of the Orchid Club. The government also established a connection between Tank and the chat room log printouts. Tank admitted that he used the screen name "Cessna" when he participated in one of the conversations recorded in the chat room log printouts. Additionally, several co-conspirators testified that Tank used the chat room screen name "Cessna" that appeared throughout the printouts. They further testified that when they arranged a meeting with the person who used the screen name "Cessna," it was Tank who showed up.[9]

Based upon these facts, the court found that the government made an adequate foundational showing of the authenticity of the chat room log printouts under Rule 901(a). Specifically, the government "presented evidence sufficient to allow a reasonable juror to find that the chat room log printouts were authenticated."[10]

The *Tank* decision is consistent with other cases that have addressed the issue of the authenticity of computer evidence in the general context of Fed.R.Evid. 901(a).[11] *Tank* illustrates that there are no specific requirements or set procedures for the authentication of chat room conversation logs, but that the facts and circumstances of the creation and recovery of the evidence as applied to Rule 901(a) is the approach generally favored by the courts. (See also *United States v. Scott-Emuakpor,* [12] [Government properly authenticated documents recovered from a computer forensic

examination under Rule 901(a)]).

In *State (Ohio) v. Cook,* an Ohio Appellate Court upheld the validity of EnCase software under Ohio Rule of Evidence 901(a), which is nearly identical to the corresponding federal rule.

NOTE: Please See Chapter 6 for a Detailed Analysis of *State v. Cook.*

---

§ 1.2   Authentication of the Recovery Process

Where direct testimony is not available, a document may be authenticated through circumstantial evidence. A computer forensic examination is often an effective means to authenticate electronic evidence through circumstantial evidence. The examiner must be able to provide competent and sufficient testimony to connect the recovered data to the matter in question.

Courts have recognized the importance of computer forensic investigations to authenticate computer evidence. *Gates Rubber Co. v. Bando Chemical Indus., Ltd.,*[13] is a particularly important published decision involving competing computer forensics expert testimony, where the court essentially defines a mandatory legal duty on the part of litigants or potential litigants to perform proper computer forensic investigations. There, one party's examiner failed to make a mirror image copy of the target hard drive and instead performed a "file-by-file" copy in an invasive manner, resulting in lost information.[14] The opposing expert noted that the technology needed for a mirror image backup was available at the time (February 1992), even though not widely used. In its ruling issuing harsh evidentiary sanctions, the court criticized the errant examiner for failing to make an image copy of the target drive, finding that when processing evidence for judicial purposes a party has "a duty to utilize the method which would yield the most complete and accurate results."[15]

Some courts have required only minimal testimony concerning the recovery process, particularly where the defense fails to raise significant or adequate objections to the admission of the computer evidence. In *United Sates v. Whitaker,*[16] an FBI agent obtained a printout of business records from a suspect's computer by simply operating the computer, installing Microsoft Money and printing the records.[17] The court affirmed the admission of the printouts, finding that testimony of the agent with personal knowledge of the process used to retrieve and print the data provided sufficient authentication of the records.[18] However, in an apparent admonition to the defense bar, the court noted that the defense conspicuously failed to question the FBI agent "about how the disks were formatted, what type of computer was used, or any other questions of a technical nature."[19]

In a similar decision, *Bone v. State,*[20] the defendant contended that the trial court erred when it admitted pictorial images recovered from a hard drive without proper authentication. The appellate court noted that the computer investigator testified about

the process he used to recover the data — that he "remove[d] the hard drive" from Bone's computers and "made an image of it"; he "right [sic] protected" the various floppy diskettes before viewing them, and testified about the software program he used to recover deleted files.[21] The detective further testified as to how he exported images found on the image of Bone's computer media. He testified that he printed copies of images in Bone's computer files "exactly" as he found them, and further stated that the images "fairly and accurately" showed the images that he had seen "on the computer that [he was] using to examine Mr. Bone's computer."[22] In reviewing Indiana Evidence Rule 901(a), which is identical to the federal rule, and citing *Whitaker*, the appellate court determined that the trial court testimony was sufficient to establish the authenticity of the images contained in Bone's computer.[23]

People v. Lugashi[24] is another particularly notable case involving a detailed analysis by the court on this subject. Although not involving a computer forensic investigation per se, the Court addressed issues concerning the authentication of computer-based evidence challenged by the defense in a criminal prosecution. *Lugashi* involved a credit card fraud investigation, where a bank's internal computer system recorded and stored relevant data relating to a series of transactions in question. Each night, the bank's computer systems ran a program known as a "data dump," which retrieved and organized the daily credit card transactions reported to the bank. Shortly thereafter, a backup tape was made of the "dump" from which a microfiche record was prepared and maintained.[25]

The prosecution sought to introduce the computer-generated evidence generated by this process largely through the testimony of one of the bank's systems administrators, who conceded that she was not a computer expert. She did, however, work with those who ran the "data dumps," maintained the microfiche records, and was familiar with the system. She personally produced the data in question from the microfiche records and knew how to interpret it.[26] The defense contended that as the systems administrator was not a computer expert she was incompetent to authenticate the data in question and that, essentially, only the computer programmers involved in the design and operation of the bank's computer systems could adequately establish that the systems and programs in question were reliable and free from error. The defense also asserted that because the systems administrator's understanding of how the system worked came from her discussions with the bank's programmers and other technical staff, her testimony constituted hearsay and thus should not be allowed.[27]

The court rejected the defense's argument, noting that the defense's position incorrectly assumed that only a computer expert "who could personally perform the programming, inspect and maintain the software and hardware, and compare competing products, could supply the required testimony."[28] Instead the court ruled that "a person who generally understands the system's operation and possesses sufficient knowledge and skill to properly use the system and explain the resultant data, even if unable to perform every task from initial design and programming to final printout, is a 'qualified witness'" for purposes of establishing a foundation for the computer evidence.[29] The court noted that if the defense's proposed test were applied to conventional hand-entered accounting records, for example, the proposal "would require not only the testimony of the bookkeeper records custodian, but that of an

expert in accounting theory that the particular system employed, if properly applied, would yield accurate and relevant information."[30] Further, if the defense's position were correct, "only the original hardware and software designers could testify since everyone else necessarily could understand the system only through hearsay." The *Lugashi* court also commented that the Defense's proposed test would require production of "hordes" of technical witnesses that would unduly burden both the already crowded trial courts and the business employing such technical witnesses "to no real benefit."[31]

It should be noted that there are some factors and aspects of the *Lugashi* decision that may not be completely applicable to computer forensics. For instance, *Lugashi* deals with records created in the normal course of business, which courts in the United States generally presume to be authentic, subject to the presentation of any direct evidence to the contrary. Further, a disinterested third party to the litigation generated the computer records in *Lugashi*, while courts would likely apply increased scrutiny to records generated by a law enforcement investigator or retained party expert. Nevertheless, certain aspects of the *Lugashi* decision are applicable to questions regarding what is required to establish a proper foundation for evidence obtained from a computer forensic examination. (See also *Federal Deposit Insurance Corporation v. Carabetta*[32] [similar facts and holding to *Lugashi*]; *Hahnemann University Hosp. v. Dudnick*[33]; *Garden State Bank v. Graef*[34]).

In addition to the citations provided throughout this text relating to the admission of recovered computer data, other court rulings concerning various forms of electronic evidence provide additional and important insight regarding what many courts require for establishing a proper foundation for such data. Many of these cases frame the same issues as to what extent the investigator must be familiar with the process used to obtain or generate the electronic evidence.

Bray v. Bi-State Development Corp.[35] addressed whether an expert's testimony provided a sufficient foundation to establish the validity of computer software that produced a chart depicting light intensity levels to determine adequate lighting for commercial areas. The software program utilized photometric data to accurately calculate light intensity based on general parameters and inputted data. The expert testified that he was familiar with the software and its general functionality and that the program was known to produce accurate results and was generally used by lighting manufacturer representatives and lighting engineers. He also testified that while he had personal knowledge of the data that was inputted into the program, he generally relied on the manufacturer's representative to actually operate the computer.[36] The objecting party contended that the expert failed to establish a sufficient foundation because the expert did not program the computer software, did not actually operate the program in question, and offered no specific evidence that the software was accurate or reliable.

The court in its opinion determined that the "[r]elevant technical or scientific community's use of or reliance on particular computer software is sufficient to establish accuracy of that software for purposes of admissibility of computer-generated evidence."[37] The court also noted *Federal Rule of Evidence* 901(b)(9) and ultimately relied on both concepts in its ruling, finding testimony that the "software was a program which produced accurate results and was used generally by the lighting manufacturer's

representative and relied on by engineers to design light and make lighting decisions was sufficient under these circumstances."[38]

In *State of Arizona v. Rivers,*[39] the defendant's terms of parole subjected him to electronic monitoring to verify compliance with his house arrest. The monitoring equipment included an ankle-bracelet transmitter and a receiver connected to the defendant's telephone. The receiver was programmed with the defendant's schedule and was designed to automatically notify a parole office computer if the defendant left his home or failed to return to his home during curfew hours.[40] After the monitoring equipment detected multiple curfew violations, the defendant was apprehended and charged with various parole violations. At trial, the defendant argued that because the parole officers were not qualified to testify "from a scientific standpoint" about how the subject monitoring equipment functioned, the state was unable to demonstrate that the equipment was in proper working condition when it registered his failure to return home. The parole officer acknowledged that he did not consider himself to be an "expert" on how the monitoring equipment worked, but did testify that he had worked with approximately 200 to 300 parolees on home arrest and that he did not recall ever having received incorrect information from the equipment. He told the jury that, to the best of his knowledge, the equipment was working properly when it registered the defendant's failure to return on the day in question.[41] Based upon this testimony, the trial court ruled that the state established a sufficient foundation for the electronic evidence of curfew violations.

On appeal, the appellate court found no error in the trial court's conclusion that the state provided sufficient foundation and evidence from which the jurors could reasonably conclude that the monitoring equipment was functioning properly when it registered the defendant's curfew violation. The court cited key testimony provided by the parole officers concerning the equipment's general accuracy and reliability. Additionally, the court noted that the officers testified that the equipment was correctly installed and in proper working condition on the date in question.[42] The court relied on the case of *Ly v. State of Texas,*[43] which involved a nearly identical fact scenario, and where that court similarly rejected a defendant's contention that because the government witness was not familiar with the scientific principles behind the electronic-monitoring equipment, the state could not demonstrate that the equipment was reliable and that it had worked properly in his case.

In *United States v. Sanchez,*[44] the defendants contended that the government failed to establish that a forward-looking infrared device ("FLIR") attached to a surveillance aircraft was functioning properly when a United States Customs agent observed an aircraft engage in a night-time delivery of narcotics on a remote airstrip. Specifically, the defendants argued that because the agent admitted that he was not an expert in how the FLIR worked, the government had failed to demonstrate that the device functioned properly, and thus the testimony was insufficient to lay a proper foundation for introduction of the evidence obtained through the use of the FLIR. Rejecting the defendants' argument, the court concluded that the agent's "significant experience as a pilot in a FLIR-equipped plane" was sufficient to enable him to testify that the device "appeared to be functioning properly" at the time.[45] The court also noted that the agent was able to describe the basic principles upon which the FLIR operated.

Thus, the trial court did not abuse its discretion in admitting the agent's testimony concerning the events viewed through the FLIR.

These cases demonstrate that when addressing proper foundation for electronic evidence generated by complex devices or software, the courts generally apply the same analysis of "sufficient familiarity" by the user, general acceptance, and whether the process involved is standard and commercially available. The general acceptance standard, which is more fully addressed in the next chapter, is clearly a predominant consideration. Additionally, whether the expert is experienced and/or trained in the software and process involved is also important consideration.

However, while experience and proper training are clearly important, it is also clear that the courts do not mandate that the expert be intimately familiar with the scientific principles or detailed inner workings of the technical processes that generate electronic evidence.

§ 1.3 Authentication of the EnCase Recovery Process

Under the standard articulated under *Lugashi* and several other similar cases, the examiner need not be able to intricately explain how each and every function of EnCase software works in order to provide sufficient testimony regarding the EnCase process. There are no known authorities requiring otherwise for software that is both commercially available and generally accepted. A skilled and trained examiner with a strong familiarity with the EnCase process should be able to competently present EnCase-based evidence obtained through a forensic examination.[46]

NOTE: See Chapter 6 for a Detailed Analysis of Reported Cases Involving EnCase Software.

An examiner should have a strong working familiarity of how the program is used and what the EnCase process involves when seeking to introduce evidence recovered by the program. This means that the examiner should ideally have received training on EnCase software, although such training should not be strictly required, especially where the witness is an experienced computer forensic investigator and has received computer forensic training on computer systems in the past. Examiners should also conduct their own testing and validation of the software to confirm that the program functions as advertised. However, a "strong working familiarity" does not mean that an examiner must obtain and be able to decipher all 600,000+ lines of the program source code or be able to essentially reverse engineer the program on the witness stand.

§ 1.4 Challenges to Foundation Must Have Foundation

In the event the initial evidentiary foundation established by the computer forensic examiner's testimony is sufficiently rebutted, so as to challenge the admissibility or the weight of the evidence, expert testimony to, in turn, rebut such

contentions may be required. However, courts will normally disallow challenges to the authenticity of computer-based evidence absent a specific showing that the computer data in question may not be accurate or genuine—mere speculation and unsupported theories generally will not suffice. [47] There is ample precedent reflecting that unsupported claims of possible tampering or overlooked exculpatory data are both relatively common and met with considerable skepticism by the courts. One federal court refused to consider allegations of tampering that was "almost wild-eyed speculation . . . [without] evidence to support such a scenario."[48] Another court noted that the mere possibility that computer data could have been altered is "plainly insufficient to establish untrustworthiness."[49]

One court suggests that the defense should perform its own credible computer forensic examination to support any allegation of overlooked exculpatory evidence or tampering.[50] Another court noted that while some unidentified data may have been inadvertently altered during the course of an exam, the defendant failed to establish how such alteration, even if true, affected the data actually relevant to the case.[51] As such, in order for a court to even allow a challenge based upon alleged tampering or alteration of the computer data, the defense should be required to establish both specific evidence of alteration or tampering and that such alteration affected data actually relevant to the case. Further, even if some basis to allegations that relevant computer records have been altered, such evidence would go to the weight of the evidence, not its admissibility. [52]

§ 1.5 Evidentiary Authentication Within the EnCase Enterprise Process

Computer data retrieved in a network environment in the regular course of business has been successfully admitted into evidence in many reported cases.[53] In the corporate enterprise environment, effective computer incident response examinations must occur in real time and over the network, either because the targeted workstations or servers are in a remote location or because the drives cannot be powered down without causing significant harm to the business. In order to evaluate issues concerning chain of custody and data integrity through the EnCase Enterprise process, the disadvantages of other more limited procedures often utilized for remote analysis and file recovery over a network must first be understood. For example, utilizing virus-checking utilities or system administrator tools to conduct remote analysis of active files presents several problems from an evidentiary standpoint. First, such applications will materially alter the files being accessed or examined. In addition to changing critical file date stamps, including last accessed, and last modified times, remotely opening files through Windows NT and other system administration processes will likely result in a temporary file and other shadow data being generated on the target drive being examined.

EnCase Enterprise software is designed to address these challenges presented by real-time enterprise investigations. Importantly, EnCase Enterprise software operates at the disk level, allowing EnCase software to analyze the subject media in a read-only manner, without querying the resident operating system. This means that when the native files are read by EnCase software, the various metadata related to those files, such as time stamps, date stamps, and other information, are not altered. This also

means that no backup files or shadow data are generated during this process.

Courts recognize the importance of employing best practices in the collection of computer evidence. Best practices, or, in the words of the *Gates Rubber* Court, "the method which would yield the most complete and accurate results," is a shifting standard based upon both the circumstances of the investigation and the evolution of new technology. In incident response investigations, the analysis must be as rapid as possible to mitigate the loss and increase the likelihood of identifying the culprit. As the European Convention on Cybercrime has noted, "effective collection of evidence in electronic form requires very rapid response."[54]

For these reasons, many law enforcement agencies in the United States and throughout the world are employing EnCase Enterprise software in criminal investigations in situations in which (i) the circumstances do not allow for systems to be taken off-line, (ii) the necessity of a rapid response requires utilization of a wide area network (WAN) to access the target media, or (iii) there is a need to investigate numerous volumes of computer media attached to a WAN. Under these situations, best practices require the use of EnCase Enterprise software.

Of course, because EnCase Enterprise software operates in a live environment, a "static" imaging process is simply not possible. Whenever a computer drive remains operating in its native environment, there will be changes made to that drive by virtue of its continued operation, such as writes to the swap file or other automatic functions of the resident operating system. However, despite operating in a live environment, EnCase Enterprise software does not itself write to the target drive during the exam, nor are files altered in any way when viewed or copied by EnCase software.

It is often more advantageous from both an evidentiary and a cost standpoint to remotely image or forensically search a live computer system, rather than to shut down a system for standalone analysis, for reasons including the following:

- Critical systems often cannot be brought down without causing substantial damage to an enterprise's business operations. With the advent of EnCase Enterprise software, it is no longer absolutely necessary to shut down mission critical servers in order to conduct a proper computer investigation.

- Critical evidence will often be lost between the time an investigation is deemed necessary, and when the investigator can gain physical access to a computer. It is thus often more advantageous to conduct an immediate remote investigation, rather than waiting several hours or even days to either travel to a site or conduct a clandestine standalone computer investigation. With the advent of the EnCase Enterprise technology, such a delay is no longer reasonable.

- When operating on a live system, a substantial amount of volatile data can be accessed that would otherwise disappear or not be available if a system were shut down. Running processes, open ports, data in

RAM, connected devices, and current open documents are a just a few examples of forensically important live data that is only available when a computer is running in its native environment.

Factors such as these are considered by the courts in determining the appropriateness of methodology to search computer systems for purposes of recovering evidence.[55]

Another question sometimes raised whenever a live system is remotely previewed or recovered over a network is whether the recovered data is genuine and can be connected to the specific computer in question. EnCase Enterprise software addresses this equation on three fronts. First, EnCase Enterprise software, unlike typical system administrative tools, cannot write to the subject media at any time during the examination. This means that any relevant data found on the Subject drive could not have been placed there through the use of EnCase Enterprise software, even if the investigator had wanted to do so. Secondly, the elaborate, role-based security apparatus of EnCase Enterprise software disallows unauthorized access and securely logs and identifies all users and activity throughout the course of the examination through a secure server, thus documenting important chain of custody and creating a detailed and secure record of the examination. Finally, all transported data in the EnCase Enterprise software environment and the resulting Evidence Files are encrypted with 128-bit AES encryption. In addition, when creating Evidence Files, EnCase Enterprise software calculates CRC and MD5 checksums in the same manner as the standalone forensic version.

Cases Involving the Use of EnCase Enterprise and Other Relevant Authority

EnCase Enterprise software is based upon the same code and foundation as the EnCase stand-alone software (known as EnCase Forensic software). EnCase Enterprise software is essentially the core EnCase stand-alone product, but network-enabled in a highly scalable manner, with the addition of internal role-based security and database support for increased functionality. As such, the above case law set forth below in Chapter 6 is highly relevant to EnCase Enterprise software and serves as an important foundation of credibility that is simply not present with any other tool used in corporate computer investigations.

In terms of cases involving the EnCase Enterprise software, while EnCase Enterprise software has been used in thousands of investigations to date, the following are some key decisions:

Positive Software v. New Century Mortgage

Positive Software Solutions Inc. v. New Century Mortgage,[56] is a U.S. federal court case in which EnCase Enterprise software was used by the defendant's expert to image 11 of the defendant's 250+ servers. The plaintiff raised objections and sought direct access to the defendant's network to conduct their own imaging. In denying the plaintiff's motion to conduct their own imaging of defendant's servers, the Court ordered the defendant "to preserve all extant backups or images of all servers or personal computers that now or

previously contained any [relevant evidence] . . . and to preserve all extant backups or images of all e-mail servers, pending further order of the Court or directive of the arbitrator." The Court did not fault the use of EnCase Enterprise software or otherwise find that the forensic imaging that was conducted using EnCase Enterprise software was in any way deficient or unacceptable, despite the fact that the plaintiff's motion raised unspecified allegations questioning "the quality and accuracy of the imaging."

United States v. Greathouse[57]

The *Greathouse* case is a published decision that is highly relevant to EnCase Enterprise and Field Intelligence Model (EnCase Enterprise for Law Enforcement) because the Court approvingly addresses the network preview function of EnCase, which is the engine of EnCase Enterprise, as well as key functionality found in EnCase Enterprise, such as its data triage and "port scan" capabilities.

In Greathouse, Federal agents executed a search warrant at a residence and discovered that five people lived in the house, and that six computers networked together (five of which were in the den, and one of which was in defendant's bedroom).[58] Two other computers were located in the den but not connected to the network. The execution of the warrant and the interviewing of the residents took place over a three-to-four hour time period.[59] According to the Court:

> [The investigating agent] explained that he decided to seize all of the computers and shut down the network because he could not tell which of the computers had the suspected child pornography and it would take several days to review and make this determination. [The investigating agent] further testified that he could see that the defendant's computer was hooked up to the network because of the presence of a network cable and a network card installed on the computer.
>
> At the hearing, defendant proffered testimony from . . . a computer forensic consultant . . . [who] explained that there is a computer preview program known as ENCASE that has been available for many years that makes it possible to quickly scan computers for certain information. [The expert] testified that, with ENCASE, a computer could be scanned for the presence of child pornography within just a few minutes. [The expert] also testified that there is a "port scan" that can be used to learn more about the nature of computer equipment. [The investigating agent] testified that he was aware of the ENCASE program, that he has this program available, but that he did not bring the program with him for this particular search.[60]

The Court ultimately granted the defendant's motion to suppress the evidence based on other grounds, but did address what constitutes best practices in conducting searches in locations where multiple computers may well be present:

> "Defendant also claims that the seizure of all eight computers was

overly broad and he challenges, under *Franks,* [the investigating agent's] statement in the search warrant affidavit that the computers would need to be searched off-site by a forensics expert. Defendant relies upon [his expert's] testimony regarding the ENCASE preview program.

Numerous cases have upheld the wholesale seizure of computers and computer disks and records for later review for particular evidence as the only reasonable means of conducting a search. *See Hay,* 231 F.3d at 637 (agents justified in taking entire computer system off-site for proper analysis); *Lacy,* 119 F.3d at 746; *United States v. Upham,* 168 F.3d 532, 534 (1st Cir.1999).

However, I recognize that this may not always be true due to technological developments. In this case, I find that [the investigating agent] acted in reasonable reliance upon well-settled and clear Ninth Circuit authority upholding the right of investigating authorities to seize computers for later forensic analysis given that he had no way of knowing, prior to entry, that he would encounter eight computers instead of one. **Had there been any evidence that a number of suspect computers would be found on site, there may well be an obligation to use a program like ENCASE to more narrowly tailor the search and seizure.**[61]

Thus, the *Greathouse* case, although decided on other grounds, puts investigators on notice that best practices require up-to-date tools, and that when sophisticated programs like EnCase software and its network analysis (EnCase Enterprise) are available for an investigation involving networked computers, investigators will be expected to use them.

This decision is very important as companies that use EnCase Enterprise can point to the important guidance from the *Greathouse* court that essentially endorses the functionality of EnCase Enterprise as best practices for investigations involving networked computers. Additionally, this guidance is in the law enforcement context, which generally involves a higher degree of scrutiny than corporate investigations.

Zubulake v. UBS Warburg, LLC[62]

The landmark *Zubulake* line of cases are very important in the electronic evidence discovery (eDiscovery) field as they serve as seminal cases that establish a procedural framework involving processes, policies and general technology. In *Zubulake V*, the court laid out an important recommended technological procedure when a company seeks to preserve and collect computer evidence in a larger scale investigation:

To the extent that it may not be feasible for counsel to speak with every key player, given the size of a company or the scope of the lawsuit, counsel must be more creative. It may be possible to run a system-wide keyword search; counsel could then preserve a copy of each "hit." Although this sounds burdensome, it

need not be. Counsel does not have to review these documents; only see that they are retained. For example, counsel could create a broad list of search terms, run a search for a limited time frame, and then segregate responsive documents.[63]

Whether the Court intended it or not, this is a very important validation of the EnCase Enterprise technology, which, at its core, uniquely provides the ability to perform a "system-wide keyword search" and "then preserve a copy of each 'hit.'" Like *Greathouse*, *Zubulake V* is very important, as companies that use EnCase Enterprise can point to this important guidance from the *Zubulake* court that essentially endorses the functionality of EnCase Enterprise software as best practices when preserving and collecting computer evidence for corporate investigations.

Keesoondoyal case

In this criminal case in Wales,[64] EnCase Enterprise software was used to gather the relevant electronic evidence. As described in the local press:

> Dheej Keesoondoyal, 34, was employed by the BP/Safeway partnership as an accountant at their head office.
>
> But he set a fictional company to create a series of false invoices for building work which had never been carried out - and planned to start a jet-set life abroad with the proceeds.
>
> The money was paid into an account set up by brother-in-law Eric James under the made-up Global Construction and Electrical Contractors.
>
> Prosecutor Martyn Kelly said, "The company had never traded. It was not real.
>
> "The scheme was hatched and 12 false invoices were created authorising payment for more than £1.5m from the BP/Safeway Partnership." [65]

Keesoondoyal received a sentence of four years imprisonment.

State (Ohio) v. Morris

Also see the discussion of the *State v. Morris* case in Chapter 6, below. Although the case does not directly involve EnCase Enterprise software, the Court considers EnCase disk images to be exact copies and admissible when the "original" is no longer available, which is important for cases involving the collection of computer evidence using network-enabled computer forensic software, such as EnCase Enterprise software.

NOTE: Please See Chapter 7 for a discussion of *United States v. Maali,* another case in which the forensic images comprised the only computer evidence in existence, as the original drives had been returned to the defendants.

Validation of Computer Forensic Tools

§ 2.0 Overview

Chapter 1 addressed authenticating computer evidence through direct or circumstantial evidence in order to establish that the recovered data is genuine and accurate. Another form of an objection to authenticity may involve questioning the reliability of the computer program that generated or processed the computer evidence in question. In such cases, the proponent of the evidence must testify to the validity of the program or programs utilized in the process. This chapter discusses what standards the courts are actually applying in such challenges, and what testimony the examiner may need to provide to validate computer forensic tools.

§ 2.1 *Frye/Daubert* Standard

Daubert v. Merrell Dow Pharmaceuticals, Inc,[66] is a landmark U.S. Supreme Court decision that sets forth a legal test to determine the validity of scientific evidence and its relevance to the case at issue. Many state court jurisdictions in the US follow the *Frye*[67] test, which is very similar, but not identical to *Daubert*. The introduction of DNA evidence is a typical scenario where a court may require a *Daubert/Frye* analysis, although many courts now take judicial notice of the accuracy of DNA typing procedures as the science is no longer considered "novel."[68]

Most concerted challenges to EnCase software involve the *Daubert* or *Frye* standards. However, a corporate defendant advocating the EnCase-based evidence in *Mathew Dickey v. Steris Corporation*[69] (further discussed at §6.01) successfully asserted that EnCase constituted an automated process that produces accurate results, and thus evidence obtained from that process would be subject to a presumption of authenticity under Rule 901(b)(9). Rule 901(b)(9) provides that evidence produced by an automated process, including computer-generated evidence, may be authenticated if such an automated process is shown to produce accurate results. However, the court also addressed the *Daubert* factors. Although it is clear that EnCase software meets the standards under both Rule 901 and *Daubert*,[70] the trend of the courts is to include "non-scientific" technical evidence within the purview of *Daubert/Frye*, in addition to the purely scientific forms of evidence, such as DNA analysis, that are more traditionally subject to *Daubert*. The judicial analysis applied in notable challenges to EnCase software is clearly consistent with this trend. As such, a computer forensic examiner should be very familiar with the basic elements of the *Daubert* analysis, which are as follows:

1) Whether a "theory or technique … can be (and has been) tested;"

2) Whether it "has been subjected to peer review and publication;"
3) Whether, in respect to a particular technique, there is a high "known or potential rate of error;" and
4) Whether the theory or technique enjoys "general acceptance" within the "relevant scientific community."[71]

Under the first prong of the test, courts have expressly noted that EnCase software is a commercially available program that can be easily tested and validated. This is in contrast to tools that are not commercially available to the general public or are custom tools with arcane command line functionality that are not easily tested by third parties unfamiliar with those processes. The law is clear that in the context of computer-generated evidence, the courts favor commercially available and standard software.[72] Further, many agencies have tested EnCase software in their labs before standardizing their agents with the software. Importantly, the widespread adoption of EnCase software by the computer forensics community serves as a crucial factor for authentication, as the community generally knows the capabilities and accuracy of the program through such extensive usage. Additionally, many publications have featured EnCase software as the highest-rated tool in testing and comparisons among other commercially available software tools.[73]

These reviews are among several industry publications featuring EnCase software, and are relevant to the second prong of the *Daubert* test. Peer review and publication in the relevant industry is an important factor looked to by the Courts in considering the validity of a technical process under *Daubert/Frye*. Various published articles in the information security and high-tech crime investigation industries favorably review or mention EnCase software favorably.[74] It is important for computer forensic examiners to keep abreast of peer review of computer forensic tools in industry publications. Examiners should also be cognizant of whether developers decline invitations from respected industry publications to participate in testing and peer review opportunities, as such refusals could raise questions regarding the validity of such tools.

An important peer review article that appeared in *The Computer Paper*, Canada's leading IT Publication, illustrates how peer review is also an important source to establish general acceptance and industry trends:

Because courts around the world have accepted EnCase as a standard, commercially available forensic software application, defense attorneys have switched from attacking the accuracy of the software to attacking the methodology of the operator, or forensic technician. This makes training important--and is also the reason why Guidance Software has an extensive and busy training facility in California.[75]

It is not uncommon for investigators to be asked to testify to specific examples of peer review and publication of technical or scientific processes. For instance, in *People*

v. Rodriguez,[76] a case in Sonoma County, California where EnCase software was subjected to a *Frye* analysis, the District Attorney investigator referenced in his testimony the above-mentioned IEEE Computer Society article, as well as other published articles. Often, testifying experts will bring copies of relevant articles from industry publications to court for admission into evidence as part of the validation process.

The prosecution in *Rodriguez* also provided testimony that there were no known reports of a high known or potential rate of error regarding EnCase software. While all software programs contain bugs to varying degrees, the various tests and extensive usage of EnCase software reveal that the program does not have a high error rate, especially in contrast to other available tools. Additionally, it is important for an investigator to be able to point to either his/her own testing of EnCase software or that performed by his/her agency. In a detailed and documented published testing of computer forensic software, *SC Magazine* noted in 2001 that EnCase Forensic Edition "outperformed all the other tools" that were tested by the magazine, and in a report on its group test of data forensics in 2003, noted that EnCase software "sets the standard for other forensic products" and is "[d]efinitely the best option for professional forensics investigations."[77]

Courts have referred to the need for a body of data from "meaningful testing" efforts to guide them in their *Daubert* analysis. There is no requirement for a regimented and universal standard for such testing agreed on by all the experts in the field. However, any testing should be meaningful and objective, subject to the same peer review as the tools and processes being analyzed. Further, professional testing ideally culminates in the preparation of a detailed report or white paper, allowing for proper analysis and comment. In *United States v. Saelee*[78], the court noted that peer review should be conducted by "disinterested parties, such as academics."). Needless to say, the more thoroughly a tool has been tested, and the wider its acceptance within the relevant community, the more likely it is to withstand a *Daubert* challenge.

At one time, there was only a limited amount of published testing concerning computer forensics tools. Although many large agencies had conducted successful tests with EnCase software, often they had not published their results. Additionally, tests that had been conducted were often problematic, because it is difficult to determine whether a particular tool has a high rate of error unless the testing process and methodologies are disclosed and documented in full, and it is also difficult to define a "high rate of error" when many developers of popular forensic tools declined to allow testing on their tools, depriving the analysis of a wider field of comparison. In 2003, however, the published testing landscape changed considerably when the National Institute of Standards and Technology ("NIST") published the results of its extensive testing of computer forensics tools under its Computer Forensics Tools Testing Project. The rigorous and comprehensive testing revealed no flaws in the EnCase imaging engine, as reflected in the NIST report "Test Results for Disk Imaging Tools: EnCase 3.20."[79] (Note that there have been no substantial changes made to the imaging engine portion of the EnCase code since Version 3.20). The NIST testing process for EnCase software was remarkably comprehensive, involving over fifty separate test scenarios of

IDE and SCSI hard drives, including using the FastBloc® hardware write-blocking device. All performed NIST testing was disclosed in the report. In addition:

- EnCase software flawlessly imaged all sectors and achieved expected results on tests utilizing direct disk access mode. EnCase flawlessly imaged all sectors and achieved expected results on tests utilizing BIOS disk access with one exception. There was one reported anomaly when accessing IDE drives on an older computer using a legacy BIOS. This anomaly reflects a flaw in the legacy BIOS technology. As noted by the NIST Report, GSI has previously addressed this limitation of legacy BIOS technology by easily enabling direct disk access through the ATAPI interface.

- EnCase software properly verified the imaged media in all such test scenarios.

- EnCase software properly reported and logged I/0 errors during the imaging process in all such test scenarios.

- EnCase software properly detected and reported verification errors when the image files were intentionally altered by a disk editor.

- Two items were noted regarding the restore function, which is not related to the imaging process and were solely reflective of the limitations of the Windows Operating systems.

- The three identified anomalies in the report reflected limitations of third party technology, with proper workarounds documented. The results of this report establish that no changes or modifications to the code of the EnCase imaging engine is warranted.

In short, the NIST testing is an example of the sort of scientific, independent, thorough and fully disclosed testing that had been lacking in the computer forensics industry. It should further aid the already widespread court acceptance of EnCase software under the *Daubert* standard.

The final prong — whether a process enjoys "general acceptance" within the "relevant scientific community" — is a particularly important factor strongly considered by the courts in validating scientific tools and processes. "`[A] known technique that has been able to attract only minimal support within the community,' ... may properly be viewed with skepticism."[80] EnCase software is without question the most widely used computer forensic process in the field. Thousands of law enforcement agencies and companies worldwide employ EnCase software for their computer investigations. In addition, EnCase software has over fourteen thousand users and Guidance Software trains over three thousand five hundred individuals annually in the use of EnCase software. The widespread general acceptance of a process is often considered to be the most important prong in a *Daubert/Frye* analysis. In addition, even outside the litigation context, there are practical considerations: if it should become necessary to

replace an expert, his or her use of standard software will make the transition to a replacement expert much easier.

In the case of many other technical processes, counsel will often struggle to establish that all the *Daubert* factors are sufficiently met. However, it is difficult to imagine any other computer forensic process that could better qualify under the *Daubert/Frye* analysis. In fact, at least one trial court has taken official judicial notice that EnCase software is a commercially available tool with widespread general acceptance.[81] Counsel should consider seeking judicial notice from the court of several of the *Daubert* factors as applied to EnCase software, including its general acceptance, the fact that is commercially available and subject to widespread peer review.[82]

§ 2.2   Computer Forensics as an Automated Process

Federal Rule of Evidence 901(b)(9) provides a presumption of authenticity to evidence generated by or resulting from a largely automated process or system that is shown to produce an accurate result. This rule is often cited in the context of computer-processed evidence.[83] There is some debate as to whether testimony from computer forensic examiners should be considered expert scientific testimony, and thus subject to an analysis under *Daubert*, or non-scientific technical testimony regarding the recovery of data through a technical investigation process, and thus subject to Federal Rule of Evidence 901(a), 901(b)(9). The United States Supreme Court blurred this distinction between scientific vs. non-scientific expert testimony in its *Kumho Tire Company, Ltd. v. Carmichael*,[84] which extended the *Daubert* test to cover technical processes as well as scientific opinion evidence. However, many courts still draw a general distinction between scientific and non-scientific expert testimony.[85]

At least one federal appeals case has referred to this issue in *dicta*, hypothesizing that in light of Rule 901(b)(9), computer or x-ray evidence resulting from a process or system would not fall under a *Frye* analysis as "[t]he underlying principles behind x-ray and computers are well understood; as to these technologies, serious questions of accuracy and reliability arise, if at all, only in connection with their application in a particular instance."[86] The court in *United States v. Whitaker*,[87] held that, without addressing *Daubert,* a foundation for forensically recovered computer evidence could be established by the investigating agent with personal knowledge of the process used to retrieve and print the data.[88]

In *United States v. Quinn*, [89] the prosecution sought to introduce "photogrammetry" evidence through expert testimony to determine the height of a suspect from surveillance photographs. The trial court allowed the testimony after a simple proffer from the government as to the basis of a photogrammetry process, which the court found to be "nothing more than a series of computer-assisted calculations that did not involve any novel or questionable scientific technique."[90] The court of appeal rejected the defendant's contention that the photogrammetric evidence required an evidentiary hearing under *Daubert*, finding that the trial court acted within its discretion.[91] In *Burleson v. State,*[92] the court held that expert testimony resulting from a complicated computer-generated display showing deleted records was admissible, as the software and computer systems creating the output relied upon by the expert were

shown to be standard, accurate and reliable. The court noted that it was unnecessary for the computer system technology to be authenticated under a *Frye* test, finding that the showing of an accurate and reliable system producing the display was sufficient.[93]

In *State (Ohio) v. Cook,* an Ohio Appellate Court upheld the validity of the EnCase software, citing, in part, Ohio Rule of Evidence 901(b)(9), and which is nearly identical to the corresponding federal rule.

NOTE: Please See Chapter 6 for a Detailed Analysis of *State v. Cook* and other Cases Addressing the Validity of the EnCase Process.

EnCase software is proven to provide a more accurate, objective and complete search and recovery process through a substantially automated process. In more complex computer forensic cases, evidence concerning the search and recovery function with its resulting visual outputs and printed reports is often as important as the recovered data itself. Some tools exclusively employed by a minority of computer forensics examiners are little more than basic single-function DOS disk utilities that, when combined as a non-integrated suite, are manipulated to perform computer forensic applications. This formerly common practice presents three fundamental problems: 1) results from the examiner's search and recovery process are often subjective, incomplete and variant; 2) the data restoration process can either improperly alter the evidence on the evidentiary image copy or provide a visual output that is not a complete and accurate reflection of the data contained on the target media; and 3) the lack of integration of all essential forensic functions within a single software application presents potential challenges to the authenticity of the processed computer evidence.

Applying Rule 901(b)(9) to the context of electronic data discovery, computer forensic software should ideally provide an objective and automated search and data restoration process that facilitate consistency and accuracy. To provide a hypothetical illustration, a group of ten qualified and independently operating forensic examiners analyzing the same evidentiary image should achieve virtually the same search results when entering identical text search keywords or seeking to recover all specified file types on the image, such as all graphical images or all spreadsheet files. If not, the process employed cannot be considered to be either automated or accurate and thus would not be considered a process qualifying for a presumption of authenticity under Rule 901(b)(9). Further, it is often necessary to duplicate search processing results during or before trial, and thus if a colleague or, even worse, an opposing expert obtains significantly differing search results from the same media, the impact or even the very foundation of the evidence may be substantially weakened. While the court in *Gates Rubber* did not expressly cite Rule 901(b)(9), its holding that a computer examiner has "a duty to utilize the method which would yield the most complete and accurate results" is clearly consistent with the statute.

Results from search and recovery procedures utilizing DOS utilities will significantly vary depending upon the type and sequence of non-integrated utilities

employed, the amount of media to be searched, and the skill, biases and time availability of the examiner. Further, each piece of acquired media must be searched separately, using the same tedious and time consuming protocol for each hard drive, floppy disk, CD or other media involved in the case. In sum, the likelihood of different independently operating examiners duplicating the search and restoration process on the same evidentiary image is extremely remote, if not impossible.

Due to the inordinate burden of searching a Windows image with DOS utilities, some investigators resort to operating Windows Explorer on the evidentiary image disk. In addition to not being able to view file slack, swap files and all other types of unallocated data, Explorer will corrupt the data in such a situation by altering file date stamps, temporary files and other transient information. Better practice requires specially designed Windows-based computer forensic software that employs a completely non-invasive and largely automated search process. A more objective search process facilitates results that are dramatically more accurate and consistent, thereby enabling duplication of the process at trial and by independently operating examiners. For example, when utilizing EnCase software, simply clicking a request to display all graphical image files contained on an evidentiary image disk will instantaneously list all such files in a graphical interface, including files "re-named" or hidden in obscure directories by a suspect in order to conceal them, and even, in most cases, previously deleted files. EnCase software duplicates the Windows Explorer interface and viewing functions, with the critical added benefits of viewing deleted files and all other unallocated data in a completely non-invasive manner. An EnCase search process often reduces an examiner's lab analysis time by several weeks. Most importantly, an examiner can present the discovered evidence in court with confidence that the search and recovery process provided more complete, consistent and objective results.

It should be noted that the line of cases that applied rule 901(a)(b) discussed above preceded *Kumho Tire*, which, as also noted above, extended the *Daubert* test to technical processes as well as scientific opinion evidence. EnCase software has been authenticated at trial under both *Daubert/Frye* and Rule 901(b)(9), and it is advisable that both approaches be considered in authenticating the software.

§ 2.3 Commercial vs. Custom Forensic Software and Authentication Issues

Some computer forensic investigations utilize custom software tools developed by the investigating agency or a private company that are not commercially available to the general public. Courts have addressed issues concerning the type of software involved where computer-generated evidence is at issue. Such cases provide a presumption of authenticity for evidence resulting from or processed by commercially available computer systems and software over customized systems and software. As noted by one respected treatise on the subject:

> "Evidence generated through the use of standard, generally available software is easier to admit than evidence generated with custom software. The reason lies in the fact that the capabilities of commercially marketed software packages are well known and cannot

normally be manipulated to produce aberrant results. Custom software, on the other hand, must be carefully analyzed by an expert programmer to ensure that the evidence being generated by the computer is in reality what it appears to be. Nonstandard or custom software can be made to do a host of things that would be undetectable to anyone except the most highly trained programmer who can break down the program using source codes and verify that the program operates as represented."[94]

In fact, courts in many jurisdictions actually require that any computer-generated evidence be a product of a "standard" computer program or system in order to admit such evidence.[95] This body of authority would seem especially relevant to software used by law enforcement for computer forensic purposes, given the sensitive function of such software. A law enforcement agency that utilized customized proprietary software for computer forensic investigations could face various complications when seeking to introduce evidence processed with such software. Such actual or potential pitfalls could include the following:

1. The defense could seek to exclude the results of any computer investigation that utilized tools that were inaccessible to non-law enforcement. Federal courts are unanimous in holding that computer evidence generated by or resulting from a process is only admissible if the defense has access to such software in order to independently duplicate the results of that process and thus "is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence."[96]

2. If the defense is provided with a copy of the proprietary software and all evidentiary images, an expert retained by the defense will require substantial time to learn the software and recreate the process, resulting in substantial cost to the government in cases involving indigent defendants. The government will incur even further costs if the purchase of supporting operating systems and file servers is required to support the custom software.

3. While, as noted above, the source code for commercially available software is not required to be introduced into evidence in order to establish the authenticity of computer processed evidence, it is apparent that such presumptions of authenticity would not be afforded to customized software. Thus, the defense would seek to exclude the results of any computer investigation utilizing custom software tools, unless the source code was made available to the defense for testing and analysis. This would be especially true for computer forensic software, given the sensitive nature of presenting evidence of deleted files and other transient electronic information.

Conversely, when questioned in court regarding the reliability of a commercially available software application such as EnCase, the proponent of the evidence would be able to testify that EnCase software is a widely used and commercially available software program and thus any member of the public can purchase, use and test the program. The defense could not claim prejudice by the use of EnCase software as any

reasonably skilled computer examiner would be able to examine the discovery copy of the evidence, nor would the government be subject to questions regarding its access to the source code of the program. The prosecution in the case of *Logan v. State*[97] dealt with these types of issues directly, described by the Court of Appeals of Indiana as follows:

> On August 14, 2003, Logan filed a motion for discovery requesting production of the computer program the State used to discover evidence on the computer. The State failed to produce the computer program, known as iLook, even after the trial court entered an order compelling production
>
> On January 20, 2004, Logan moved to dismiss the charges based upon First Amendment grounds. On February 20, 2004, the State dismissed the charges and refiled charges using a different forensic computer program, called EnCase. On April 6, 2004, approximately sixty days prior to trial, the State provided Logan with a copy of the EnCase program, thereby complying with the court's discovery order.[98]

As the *Logan* case illustrates, using software that is not commercially available can result in discovery conflicts. Resulting delays can even put the prosecution's case at risk by impacting the right to a speedy trial.

Even in the civil litigation arena, using custom software can prove problematic. For instance, in the high-profile case of *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, which resulted in a jury verdict of $1.4 billion, Morgan Stanley was lambasted by the court because software it had written to collect electronic information has missed thousands of relevant emails.

NOTE: Please See Chapter 9 for a Detailed Discussion of *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*

3

Expert Witness Testimony

§ 3.0 Overview

Are computer forensic investigators considered experts? Many courts outside of the United States, such as in Great Britain, employ a higher (perhaps wiser) threshold as to who is qualified to provide expert testimony on a technical subject. This chapter will discuss the threshold for qualifying a computer investigator as an expert and brief some cases where the court addressed this very issue. Also presented in this chapter are two fictional transcripts of sample direct examinations. The first example is a transcript from a mock pre-trial evidentiary hearing under either Federal Rules of Evidence 104, 702 and/or *Daubert v. Merrell Dow Pharmaceuticals*. A court may schedule such an evidentiary hearing to consider any foundational questions regarding the EnCase process. The second example is a direct examination in the context of a jury trial presenting evidence obtained from a computer forensic examination.

Although these examples are fictional, they are based upon actual investigation procedures and techniques taught in Guidance Software's training program and employed daily in the field by hundreds of agencies and organizations. These examples are by no means mandatory scripts to be strictly followed, but should provide a general reference for prosecutors in preparing direct examinations of their computer examiners in the context of either an evidentiary hearing or a jury trial.

§ 3.1 Threshold Under Rule 702

In the United States, *Federal Rule of Evidence* 702 provides that in order for a witness to be qualified as an expert, the expert must simply be shown to have "knowledge, skill, experience, training, or education" regarding the subject matter involved. Under this threshold, trained computer forensic experts have qualified as experts in the US courts. However, oftentimes prosecutors opt not to offer the examiner as an expert, especially where the records in question can be authenticated under *Federal Rule of Evidence* 901(b)(9) or a corresponding state statute, or where the examiner can be offered as a percipient witness presenting more objective and empirical findings of their investigation. This approach tends to be more common in many state courts.

This question was directly addressed in *United States v. Scott-Emuakpor,*[99] where the court considered whether the United States Secret Service agents who conducted the computer forensic examination needed to be a qualified expert in computer science to present their findings. The defendant in *Scott-Emuakpor* brought a motion *in limine* contending that the USSS agents should be precluded from providing

testimony regarding the results of their computer examinations, particularly as one of the agents admitted that he was not an expert in the area of computer science. Nevertheless, the court opined that:

> "[T]here is no reason why either witness may not testify about what they did in examining the computer equipment and the results of their examinations. The question before the Court at this time is not whether these witnesses have the expertise, for example, to develop sophisticated software programs. The question is whether they have the skill to find out what is on a hard drive or a zip drive. Apparently, they have this skill because they determined what was on the drives. By analogy, a person need not be an expert on English literature in order to know how to read. . . .The fact that (the USSS agent) admitted that he is not an expert in the area of computer science is not binding on the Court."

The court in *Galaxy Computer Services, Inc. v. Baker*[100] reached a similar result. In that case, the defendants had filed a motion *in limine* seeking to bar the expert opinion testimony of Paul Taylor. Taylor, who had worked in the field of computer forensics for five years, had analyzed nine hard drives and had prepared an expert report detailing the defendants' deletion of certain files. Plaintiff offered Taylor's testimony both to authenticate the recovered documents and to permit jury instructions on spoliation of evidence and consciousness of wrongdoing.[101] As described by the court:

> Defendants argue that Taylor is not qualified to testify as a computer expert because: (1) none of his degrees are in computer science; (2) he is not fluent in any computer language; (3) he is not a computer programmer; (4) he holds no certificates in computer science; and (5) he possesses no training or special education for Microsoft certification. . . .
>
> The Court finds that Taylor qualifies as an expert based on his knowledge, skill, experience, training and education. **The field of computer forensics does not require a background in computer programming or reading and writing code.** Taylor has been working in the field of computer forensics for five years. During this period, he has been completed between 1,600 and 1,700 forensic reports based on his findings, some of which have been accepted by various courts.[102]

It is not uncommon for an examiner to be asked to interpret the recovered data. The case of *United States v. Hilton*[103] provides a very good example of a computer forensic examiner offering expert witness testimony to interpret the data gleaned from his examination. Among the issues in Hilton was whether the Defendant had utilized interstate commerce (i.e. the Internet) in the process of distributing child pornography, thereby satisfying a key element and requirement of the statute. The computer investigator from the United States Customs Service testified that the images in

question were located in a subdirectory named "MIRC," which contained software and files related to "IRC" (Internet Relay Chat). The Special Agent testified that, in his expert opinion, because the contraband was located in the MIRC subdirectory that contained Internet chat-related files, the images were likely associated with the Internet.

The special agent also testified that the file time and date stamps reflecting the creation time of each of the subject images were indicative that the Defendant downloaded the images from the Internet via a modem. The special agent based this conclusion on the fact that the images were created on Defendant's computer at intervals of time consistent with downloading the images via a modem. The special agent's expert testimony, among other factors, convinced the court the subject images were transmitted to the Defendant's computer via the Internet, thereby satisfying the interstate commerce requirement of section 18 U.S.C. § 2252A(a)(5)(B).

§ 3.2 Illustrations of Testimony

DIRECT EXAMINATION -- PRE-TRIAL EVIDENTIARY HEARING

A. <u>PREFACE</u>

If any challenge is raised to the qualifications of the computer examiner or the foundation of the evidence concerning the tools or methodologies used in the course of a computer forensic investigation, many prosecutors prefer to address such objections outside the presence of the jury through a hearing under either Federal Rule of Evidence 702, Rule 104 or *Daubert*. Judges are typically more receptive toward technical evidence and it is obviously desirable to avoid presenting complex testimony on contested technical issues before a jury by resolving such foundational issues in a separate hearing beforehand. The following fictional "mock trial" direct examination is designed to illustrate how a proper foundation may (but certainly not must) be established for the EnCase process under both Rule 901(b)(9) and *Daubert*. For illustration purposes, the below example contains more detail than what would normally be presented on direct examination, even in the context of a court trial or hearing. However, much of the information may be useful for re-direct examination.

B. <u>BACKGROUND</u>

[After stating name for the record]
Q: Sir, are you a Senior Special Agent for the United States Customs Service?
A: Yes I am.
Q: And do you have any specialized duties as a Customs agent?
A: I am a computer evidence examiner certified as a Seized Computer Evidence Recovery Specialist by the United States Department of the Treasury.
Q: Please tell us how long you have been a computer evidence examiner.
A: I have been a Seized Computer Evidence Recovery Specialist with Customs for eight years.
Q: Tell us about your educational background.
A: I received a Bachelor of Science degree in electrical engineering from University of _____ in 19__.
Q: And could you briefly describe your training for the handling and examination of computer evidence?
A: In 19__ I received three-weeks of intensive training, known as Seized Computer Evidence Recovery Specialist training at the Federal Law Enforcement Training Center. In 19__ I obtained Computer Forensic Examiner Certification from the International Association of Computer Specialists, known as IACIS, after receiving two weeks of their intensive training. The next year I received Advanced Course Certification from IACIS after taking their two-week advanced training course. I have also received computer forensic training from The National Consortium for Justice Information and Statistics, known as SEARCH and have received training from Guidance Software on their EnCase computer forensic application.
Q: Are you a member of any professional organizations?

A: Yes I am.

Q: Which ones?

A: I am a member of the International Association of Computer Specialists, and the High Tech Crime Investigation Association.

C. OVERVIEW OF COMPUTER FORENSICS

Q: You mentioned the subject of computer forensics. Can you provide an overview of what computer forensics is?

A: Computer Forensics is the acquisition, authentication and reconstruction of electronic information stored on computer media, such as hard drives, floppy disks or zip drives. A computer forensics technician is needed whenever there is evidence stored in a computer.

Q: Can you briefly tell us how a computer forensic specialist such as yourself conducts a typical investigation?

A: First, the electronic information contained on computer storage media must be acquired by making a complete physical copy of every bit of data located on computer media in a manner that does not alter that information in any way. Then the information must be authenticated in a special process that establishes that the acquired electronic information remained completely unaltered from the time the examiner acquired it. Finally, the examiner must use special software and processes to recover and reconstruct the information in its forensic state, even if such information is found in files that have been deleted by the user.

D. THE ACQUISITION PROCESS

Q: You described three basic steps, and I want to discuss them one at a time beginning with the acquisition process. How is digital information copied from computer media in a proper forensic manner?

A: Specialized computer forensic software, such as EnCase, utilizes a special boot process that ensures the data on the subject computer is not changed. After the boot procedure is initiated, the examiner utilizes the forensic software to create a complete forensic image copy or "exact snapshot" of a targeted piece of computer media, such as a hard drive, or external media, such as floppy or zip disks. This forensic image is a complete sector-by-sector copy of all data contained on the target media and thus all information, including available information from deleted files, is included in the forensic image created by the examiner.

E. THE AUTHENTICATION PROCESS

Q: The second step you mentioned was the authentication process; please briefly describe how the acquired electronic information is authenticated and verified.

A: Computer forensic examiners rely upon software that generates a mathematical value based upon the exact content of the information contained in the forensic image copy of the seized computer media. This value is known as an MD5 hash value and is often referred to as a special type of digital

signature. The same software also verifies that this value remains the same from the time it is generated. If one bit of data on the forensic image copy is subsequently altered in any way, meaning that even if a single character is changed or one space of text is added, this value changes. So if the hash value of the information contained on seized media remains the same, then it is established that the electronic data has not been altered in any way.

Q: What are the odds of two forensic images with different contents having the same hash value?

A: The odds of two computer files, including a forensic image file, with different contents having the same hash value is roughly ten raised to the 38th power. If you wrote out that number, it would be a one followed by 38 zeros. By contrast, the number one trillion written out is one followed by only twelve zeros.

F. THE RECOVERY PROCESS

Q: Because the third step of data recovery is complex, I am going to first ask you a few basic questions about how a computer works. First, and without being too technical, could you give us a description of how information on a hard drive is stored by the computer?

A: Yes. Basically, computer disks are storage media that are divided into concentric circles or tracks. This can be thought of as a small version of the old 78 rpm records people used to play on phonographs. The tracks are divided into sectors. Each sector has its own address, a number that is unique to that part of the disk. The operating system assigns and stores the address, so that it may retrieve all information constituting a computer file stored in a specific sector when requested by the user.

Q: How is the information recorded on the hard disk?

A: The disk is covered with a thin coat of magnetic material. When information is written to the disk, the data is recorded by magnetizing specific parts of the disk coating. The information resides there until it is overwritten.

Q: Thank you. I think we have the basic idea. I am very interested in how a computer technician can recover electronic information that has been deleted or automatically purged. Please tell us what is involved in this process.

A: When the computer user deletes electronic information, it is often assumed that the information is removed from the computer forever. That is not necessarily true. The information is still in the computer; only it is now marked by the computer to allow it to be overwritten. A general analogy would be a library card catalogue system, where the books represents files and the card catalogue represents the file directory with information as to where the files are located on the disk. When a file is deleted, its location information is removed from the card catalogue index, but the book remains on the shelf until another book randomly replaces it.

Q: To what extent can this deleted information be retrieved?

A: If the information has not yet been overwritten by other data, it is still there and can be retrieved using specialized software.

G. <u>AUTHENTICATING THE ENCASE PROCESS UNDER RULE 901</u>

Q: And what specialized software did you use for this investigation?
A: I used the computer forensic software known as EnCase.
Q: Tell us a little about the EnCase software.
A: EnCase is a standard, commercially available software program that is specifically designed as a tool for computer forensic investigations. It is a fully integrated tool, meaning it performs all essential functions of a computer forensic investigation, including the imaging of a target drive, the generation of an MD5 hash of the evidentiary forensic image, and the analysis of the subject evidence. The software allows for a completely non-invasive investigation in order to view all information on a computer drive, whether it is in the form of a deleted file, a non-deleted file, file fragments and even temporary or buffer files.
Q: How does the investigator use the EnCase software to recover deleted files?
A: First, EnCase creates a complete forensic image copy or "exact snapshot" of a targeted computer drive. EnCase will be able to read all existing information on that forensic image, regardless of whether the information is in the form of a deleted file that is marked by the operating system to be overwritten. Any information that has not been actually overwritten will be recovered for analysis. EnCase will organize all the files, deleted files and blocks of physical data, also known as unallocated clusters, in a convenient graphical user interface to allow the evidence to be viewed and sorted by the examiner.
Q: Does the same software perform these functions?
A: Yes. EnCase is a software process that is much more automated than other computer forensic investigation processes, as it is a fully integrated program where all the required computer forensic investigation functions are integrated into a single application in a Windows-based graphical user interface.
Q: How is the EnCase process more automated than other tools?
A: To a large extent EnCase duplicates the Windows Explorer interface and file viewing functions, with the critical added benefits of viewing deleted files and all other information on the disk that the user normally cannot see or detect without specialized software. Just as Windows Explorer presents the entire file directory and folder structure on a computer to the user in a very organized manner, EnCase will also present that information, in addition other data on the target drive in a similar manner. Other forensic software tools require a great deal of more manual steps utilizing a series of arcane DOS commands and separate tools to recreate file structures and perform separate searches on different areas of a drive.

H. <u>ADDRESSING *DAUBERT* FACTORS</u>

Q: To your knowledge, is the EnCase software generally accepted in the computer forensic investigation community?
A: More than just generally accepted, EnCase is widely used in the computer forensics industry, and in my experience it is the tool of choice of the majority of computer forensic investigators in law enforcement. It is the primary computer forensic tool used by US Customs, which is my agency, and I am aware that it is the primary tool of other federal agencies, including United States Secret

Service, as well as hundreds of state and local agencies. EnCase is a major part of the Seized Computer Evidence Recovery Specialist training curriculum for federal agents, and is part of the curriculum in many computer forensic training courses offered by professional organizations — most notably the annual IACIS training conference.

Q: How would one go about testing computer forensic software?

A: There are three main steps in testing computer forensic software. The first step is to generate an MD5 hash value for an image of a targeted computer drive using the forensic tool being tested and then using another standard tool to repeat the process for the same drive. The MD5 hash values generated by both tools for the same drive should be exactly the same. The second step is to verify that whatever evidence is recovered from an evidentiary forensic image can be independently confirmed by a standard disk utility. With EnCase for instance, the program will identify the precise location on the original drive for each bit of data recovered by the examiner. With that information, the examiner can then use a disk utility such as Norton DiskEdit to independently confirm the existence and precise location of that data. The third step is to confirm that throughout the examination process, the content on the forensic image has not been altered in any way by repeating the MD5 hash analysis of the forensic image to verify that the MD5 hash is has not changed since the time of acquisition. These tests should be performed several times with different pieces of computer media.

Q: To what extent can EnCase be tested by a third party?

A: EnCase is commercially available and thus any examiner can purchase, use and test the program on their own. One of the advantages of the program is that all the required forensic functions are integrated into a single program with a Windows-based graphical user interface. Thus, compared to other computer forensic software, the program is easy to use.

Q: Has your agency tested the software?

A: Yes.

Q: How was it tested?

A: Before we purchased the software on a large scale, there were two computer investigation agents in my agency who conducted an extensive evaluation of the software employing the three steps I just described. I am aware that the Secret Service conducted a similar testing procedure as well. Also, since our agencies' adoption of the software we have had nearly 100 computer examination agents using the program on a daily basis in the field.

Q: What were the results of those tests?

A: By all accounts the software has met the three standards I described above.

Q: Has EnCase been tested by any independent third parties?

A: Yes. The U.S. Government conducted extensive testing of computer forensics tools and published its results in June 2003.[104] The testing was conducted as part of the Computer Forensics Tool Testing ("CFTT") project, which was a joint effort of the National Institute of Justice, the National Institute of Standards and Technology ("NIST"), the U.S. Department of Defense, the Technical Support Working Group, and other related agencies. The CFTT testing process for EnCase was remarkably comprehensive, involving over 50 separate test scenarios of IDE and SCSI hard drives, including using the FastBloc hardware write blocking device. All performed NIST testing was

disclosed in the Report.

Q: What were the results of the CFTT project testing of EnCase?

A: The results were impressive. First, EnCase flawlessly imaged all sectors and achieved expected results on tests utilizing direct disk access mode. EnCase also flawlessly imaged all sectors and achieved expected results on tests utilizing BIOS disk access, with one exception. There was one reported anomaly when accessing IDE drives on an older computer using a legacy BIOS. This anomaly reflects a flaw in the legacy BIOS technology. As noted by the CFTT report, Guidance Software has previously addressed this limitation of legacy BIOS technology by easily enabling direct disk access through the ATAPI interface. Second, EnCase properly verified the imaged media in all test scenarios. Third, EnCase properly reported and logged I/0 errors during the imaging process in all test scenarios. Fourth, EnCase properly detected and reported verification errors when the image files were intentionally altered by a disk editor.

Q: You mentioned one anomaly. Were there any others?

A: Two items were noted regarding the restore function, which is not related to the imaging process and were solely reflective of the limitations of the Windows Operating systems. All told, the three identified anomalies in the report reflected limitations of third party technology, with proper workarounds documented. The results of the CFTT report establish that no changes or modifications to the code of the EnCase imaging engine is warranted.

Q: Has EnCase been subjected to any publication in the industry that you are aware of?

A: Yes, I have read various published articles in the information security and high-tech crime investigation industries that either favorably review the product or mention the product favorably. An article in the April 2001 issue of SC Magazine featured the most detailed and documented published testing results to date. The magazine gave EnCase its highest rating and noted that in its testing EnCase "outperformed all the other tools" that were tested by the magazine.

Q: At this time Your Honor, I'd like to submit as the Government's exhibit __, which are copies of published articles in the industry discussing the EnCase software.[105]

THE COURT: So received.

Q: Thank you, Your Honor, nothing further.

DIRECT EXAMINATION FOR THE PRESENTATION OF COMPUTER EVIDENCE BEFORE A JURY

A. PREFACE

Many prosecutors maintain that when presenting computer evidence before a jury, the testimony should be as simple and straightforward as possible. Burdening the jury with overly technical information could prove counter-productive and may actually open the door to areas of cross-examination that the court would normally have

disallowed. As such, the following direct examination is more detailed than is likely needed, but again, should provide a general resource in preparing direct examinations or for responding on re-direct. Further, there are many other foundational areas that are normally outside the scope of the EnCase process, such as establishing how an Internet chat room works, what the Windows operating system is, or establishing that the computer belonged to the defendant, which are not addressed here. (For a good discussion of establishing a foundation for a printout of a chat room conversation, see *United States v. Tank.*[106])

When presenting EnCase-based evidence, it is recommended that the proponent take full advantage of the EnCase process and graphical user interface by presenting screen shots of the EnCase "All Files" and other views, in order to show the full context of the electronic evidence. This technique may also be required to comply with Best Evidence Rule considerations in computer evidence. Federal Rule of Evidence 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" When presenting evidence contained within a computer file, a screen shot of the EnCase File View may be the best means to present a visual output which is "shown to reflect the data accurately," and thus constitute an "original" under Rule 1001(3). (See Chapter 4 for a more detailed discussion of the Best Evidence Rule.)

When seeking to establish a defendant's state of mind by presenting an electronic audit trail or connecting file date stamps, the ability to display a visual output showing various file attributes and other metadata provides a tremendous advantage to the advocate of such evidence. EnCase software provides the best method to visually display all physical and logical data contained on the target drive, while showing the context of such files by displaying file metadata and other means. When providing testimony, many examiners present evidence through screenshots in a PowerPoint presentations format, or take EnCase software with them into Court for a live demonstration. In *United States v. Dean*, (discussed further in § 4.2) the opinion reflects that the prosecution presented results of its computer forensic examination through PowerPoint.[107]

Please note that for sake of brevity, many of the foundational portions of the direct exam are incorporated by reference from the above section.

[After stating name for the record]
A. <u>BACKGROUND</u>
Q: Sir, what is your current occupation?
A: I am a Senior Special Agent for the United States Customs Service.
Q: And do you have any specialized duties as a Customs agent?
A: I am a computer evidence examiner certified as a Seized Computer Evidence Recovery Specialist by the United States Department of the Treasury.
Q: What was your involvement in the investigation of this case?
A: I conducted a computer forensic investigation of the Defendant's computer to recover relevant evidence.
Q: OK, before we discuss the results of your investigation, please tell us

how long you been a computer evidence examiner.

[Please Refer To Previous Section, which is incorporated herein by reference, for foundation testimony]

*   *   *   *

Q: Turning to the computer forensic investigation you conducted in this case, please tell us when you first came into contact with the Defendant's computer and computer disks.

A: Pursuant to a search warrant, on May 18, 2000 I seized the Defendants computer at his home, along with seven CD-ROMs and sixteen floppy disks that were in his desk or otherwise in the vicinity of his computer.

Q: What did you do with the Defendants' computer equipment and disks after you seized them?

A: After leaving receipts for the computer and disks, I transported the items back to our lab, where I immediately proceeded to make forensic image copies of the hard drive found in the Defendant's computer. I also made forensic images of each of the CD-ROM and floppy disks. Using the EnCase software, I also generated MD5 hash values for the hard drive and for each floppy and CD-ROM disk at the same time the forensic images were made. I then logged the Defendant's computer and the floppy and CD-ROM disks as evidence and secured them into our evidence storage room.

Q: Did you then analyze the forensic images you made?

A: Yes I did.

Q: Please describe your analysis on the forensic image of the Defendants' hard drive.

B. RECOVERY OF HIDDEN FILES WITH RENAMED FILE EXTENSIONS

A: In my analysis of the forensic image of the hard drive, I first employed an automated function of the EnCase forensic software that analyzes all the computer files on an image of a computer drive and identifies any file signature mismatches.

Q: What are file signature mismatches?

A: A file signature mismatch is a situation where the file name extension that normally identifies the file type has been renamed, usually in order to hide the true contents of a file.

Q: What is a file name extension?

A: A file name extension is an optional addition to the file name that allows a file's format to be described as part of its name so that users can quickly understand the type of file it is without having to open files on a trial and error basis. For instance, a text file will usually have a ".txt" extension and the most common type of picture file has a ".jpg" extension.

Q: How does EnCase identify file signature mismatches?

A: Most computer files containing text or graphical images have a well-defined signature of electronic data unique to that file type. This allows file

viewers to recognize the type of file, regardless of the file extension. EnCase utilizes the same process as file viewers in order to identify files that have renamed file extensions.

A: What was the result of the file mismatch analysis that you conducted in this case?

Q: The file signature mismatch analysis revealed 16 files that were renamed as text files with a "txt" extension, but were actually graphical image files that originally had a "jpg" extension until they were renamed manually. I viewed those files and upon determining that those images appeared to be child pornography, I printed out those images.

Q: Showing to you what have been pre-marked as United States exhibits 1 through 16, can you identify these exhibits?

A: Yes. These are the printouts I made of the 16 images in question that I recovered from the Defendant's hard drive.

[Exhibits are introduced into evidence.]

C. RECOVERY OF DELETED FILES

Q: Did you examine the images you made of the Defendant's floppy disks?

A: Yes I did.

Q: What did you find?

A: I found that one of the floppy disks had five files with a "jpg" extension that had been deleted, meaning that that the computer had marked the data of those files to be overwritten. However, we were able to still recover those deleted graphical image files as the data had not actually been overwritten by the computer.

Q: How did you identify those deleted files?

Q: The EnCase software will automatically identify any files that are marked by the computer to be overwritten. I located and viewed those five graphical image files and upon determining that those images appeared to be child pornography, I printed out those images.

Q: Showing to you what have been pre-marked as United States exhibits 17 through 22, can you identify these exhibits?

A: Yes. These are the printouts I made of the five images that I recovered from the Defendant's reformatted floppy drive.

[Exhibits are introduced into evidence.]

D. RECOVERY OF FILES "DELETED" FROM MULITPLE CD-ROM SESSIONS

Q: Special Agent _____, did you examine the images you made of the Defendant's CD-ROM disks?

A: Yes I did.

Q: And what did you find?

A: I found that the CD-ROM disks were actually writeable, meaning that data can be written to this type of compact disk to store computer files. A special CD writing software program, such as CD Creator, is needed to

write data to a writeable compact disk. One of the writeable CDs we seized from Defendant's home had multiple sessions on it. A CD session is created when the user writes any number of files to the CD. When this is done, the CD writing software will create a table of contents for that session that points the operating system to the location of the files on the CD within the session.

Q: Can files on a writeable CD be deleted?

A: Not really. Unlike a hard drive or floppy disk, data written to a CD is actually burned to the media by a small optical laser instead of being magnetized. Once data is burned to a CD, it cannot be overwritten. However, if a new session is created on the CD, the user can omit existing files from the new table of contents created for the new session. A computer operating system will only read the table of contents from the latest created session on a CD. Thus, by omitting existing files from the table of contents of a new session, those files will normally be hidden from the view of a user. Specialized software, such an EnCase, will see all the sessions on a writeable compact disk and will allow the user to compare any differences in the file contents of each session.

Q: You mentioned that one of the CDs you examined had multiple sessions. What did your analysis of the multiple session CD reveal?

A: The CD actually had two sessions on it. Using EnCase, we discovered that the second session contained seven files with jpg extensions that were not included in the table of contents of the first session. I then examined those seven files, which turned out to be graphical images appearing to be child pornography, and printed out those images.

Q: Showing to you what have been pre-marked as United States exhibits 23 through 30, can you identify these exhibits?

A: Yes. These are the printouts I made of the seven images that I recovered from the first session of Defendant's writeable compact disk. [Exhibits are introduced into evidence.]

E. <u>EVIDENCE FROM SWAP FILES</u>

Q: What else did you find in your examination of the Defendant's computer?

A: I conducted a text string search of the forensic image of the Defendants hard drive. In the course of our investigation, we received information that the defendant had contacted a minor over the Internet who had an America Online account under the screen name Jenny86. I ran a text search by entering the keyword Jenny86, again using the EnCase software. The search registered several hits in an area of unallocated clusters identified by EnCase as a swap file.

Q: What is a swap file?

A: A swap file is a random area on a hard disk used by the computer's operating system to temporarily store data as a means to manage the available operating memory of a computer. The operating system will swap information as needed between the memory chips and the hard disk in order to process that information. As a result, temporary data is placed

on the computer that cannot be viewed without special software designed for that purpose.

Q: What type of data is typically written to the swap file?

A: Any data that appears on the computer screen, even in the form of an unsaved word processing document or a Web page being viewed by the user, is often written to the swap file by the operating system.

Q: What did you do after you identified search hits for the keyword Jenny86 in the swap file area?

A: I retrieved the full text of the information contained in the swap file and printed it out.

Q: I'm now handing you what has been previously marked as exhibit 31, and ask if you can identify it?

A: Yes. This is the print-out I made of the data contained in the swap file where my keyword search registered hits for the keyword Jenny86.

Q: If you would, please read the text as it appears on this printout.

A: The text appears in transcript form and reads, "Welcome to Yahoo Young Teen Chat …. [full text is read]"

 [Exhibit is introduced into evidence.]

F. <u>EVIDENCE FOUND IN FILE SLACK</u>

Q: What else did you find in your examination of the Defendant's computer?

A: I conducted a separate text string search of the forensic image of the Defendant's hard drive. In our investigation, we received additional information that the Defendant had corresponded approximately one to two years ago to another individual on more than one occasion. That person has since been convicted of possession of child pornography and sexual assault on a minor. This person's name is John Doe, and he commonly went by the nickname Lolita's Man. We conducted a text string search with the keyword Lolita's Man and registered a hit in an area of data known as file slack, which contained remnants of a deleted file.

Q: What is file slack?

A: Data storage areas on a hard disk are segmented into clusters. All the data constituting a file may occupy an entire cluster, or the file data may not take up all of the space in the physical cluster. The space between the end of a file and the physical end of a cluster is called the file slack. After the point in the cluster where the file ends, there may be pre-existing bytes in a cluster that are remnants of previous files or folders. *[NOTE: A projected PowerPoint slide or other form of demonstrative graphic illustrating this issue would be effective at this part of the examination.]*

Cluster Boundary ⎯⎯⎯ | | ⎯⎯ End of Logical File
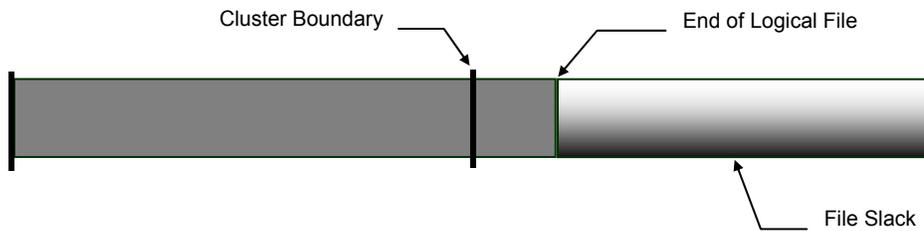
File Slack

Example of A Demonstrative Trial Graphic

Q: What did you do after you identified search hits for the keyword John Doe in the area of file slack?

A: I retrieved the full text of the remainder of the document contained in the file slack, and printed it out.

Q: Could you determine what kind of document the remnant text in file slack was a part of?

A: Based upon my observation of the format of the two remaining paragraphs in the document and the signature block at the end of the document, it appears that the text recovered from file slack was the remnants of a correspondence of some type.

Q: I'm now handing you what has been previously marked as exhibit 32, and ask if you can identify it?

A: Yes. This is the print-out I made of the data contained in the file slack area where my text search registered a hit for the text string search Lolita's Man.

Q: If you would, please read the text as it appears on this print-out.

A: [The text is read into the record]

[NOTE: Because oral testimony of the recovery of file slack may seem too abstract to the jury and the court and because of best evidence rule considerations, it is recommended that a full screen shot of EnCase in from the "File View" with the highlighted text hit in file slack be projected in order to show the full context of the relevant text].

Q: Showing what has been pre-marked as exhibit 33 on the projection screen, does this look familiar to you?

A: Yes, that is a screen shot of the File View of EnCase I created, showing the search hit for "Lolita's Man" in file slack.

Q: Part of the text on the screen is in red, while the text before it is in normal black font. Does the text coloring have any significance?

A: The black text is the active, or non-deleted file that occupies the point from the beginning of the cluster to the end of that file. The red text represents the file slack in the area from the end of the non-deleted file to the end of the cluster.

[Exhibits 32 and 33 are introduced into evidence.]

G. <u>EVIDENCE OF WINDOWS METAFILES RECOVERED FROM UNALLOCATED CLUSTERS</u>

Q: What else did you find in your examination of the Defendant's

computer?

A: As part of my routine practice, I recovered all Windows metafiles that were located on the hard drive.

Q: What are Windows metafiles?

A: When a user sends a command to print a file, the Windows operating system makes a copy of that file and sends the copy to the printer. After the file is sent to the printer, Windows deletes that file. Windows does not inform the user that the copy, or metafile, has been made, nor can the user usually detect the existence of the metafiles without special software.

Q: How did you recover the metafiles in this case?

A: The EnCase software has an automated function that locates all the metafiles residing in normally unseen areas on a hard drive, decodes them, and outputs them to a separate folder allowing them to be viewed.

Q: What did you do after you utilized this software function that located the metafiles and outputted them to a folder?

A: I opened the folder and viewed each of the recovered metafiles.

Q: What did you find?

A: I found a text document in an e-mail format addressed to the Defendant's e-mail account. According to the e-mail header information, the message was sent from the account of Jenny86@hotmail.com.

Q: What does the fact that this e-mail document existed in the form of a metafile mean to you?

A: This recovered metafile means that this e-mail message was printed out from the Defendant's computer.

Q: I'm now handing you what has been previously marked as exhibit 34, and ask if you can identify it?

A: Yes. This is the printout I made of the metafile of the e-mail document from Jenny86@hotmail.com to the e-mail account of the Defendant.

Q: If you would, please read the text as it appears on this printout.

4

The Best Evidence Rule

§ 4.0 Overview

Probably the most misunderstood rule of evidence among many computer forensic investigators is the Best Evidence Rule. The Best Evidence Rule is a doctrine of evidentiary law in the United States, Canada, and certain other countries that essentially requires that, absent some exceptions, the original of a writing must be admitted into evidence in order to prove its contents. As one might imagine, significant questions arise when applying this evidentiary doctrine to computer data. Among the issues raised by this rule are how to present computer evidence at trial, what constitutes a valid image of a computer drive, and data compression. This chapter will provide the law and address some myths as well.

§ 4.1 "Original" Electronic Evidence

The Best Evidence Rule under the US Federal Rules of Evidence provides that "[t]o prove the content of a writing, recording or photograph, the original writing, recording or photograph is required…"[108] Notably, electronic evidence falls under the Federal Rules definition of "documents." [109] However, with electronic evidence, the concept of an "original" is difficult to define. For example, when seeking to reproduce an original photographic image, a negative of that photograph, while containing all the "data" of the original, must be processed in order to provide an accurate visual replication of the original photograph. Fortunately, the Federal Rules of Evidence have expressly addressed this concern. Rule 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Under this rule and similar rules in state jurisdictions, multiple or even an infinite number of copies of electronic files may each constitute an "original."[110] Note that the law in the UK regarding civil matters is even broader:

> (1) Where a statement contained in a document is admissible as
>   evidence in civil proceedings, it may be proved—
>   (a) by the production of that document, or
>   (b) whether or not that document is still in existence, by the
>   production of a copy of that document or of the material
>   part of it, authenticated in such manner as the court may
>   approve.
>
> (2) It is immaterial for this purpose how many removes there are
>   between a copy and the original.[111]

Thus, the UK rule in civil matters makes no distinction between copies and originals.

The operative language in Rule 1001(3) is "accurate reflection." It is a mistake to analogize computer files to hard copy documents for purposes of the Best Evidence Rule. A mere bit-stream copy of a graphical image file does not provide a completely accurate "printout or other output readable by sight" unless Windows-supported forensic tools or other viewers are used to non-invasively create an accurate visual output of the recovered data, without changing any of the data. Conversely, if a computer file is compressed, encrypted, transmitted as an e-mail attachment (thus sending a copy of that decrypted, compressed file in a different file format and even divided into many packets), and then received, decompressed, decrypted and opened, the file now in possession of the recipient would be another 'original' of that file under the Federal Rules. Printing that file also converts it to another file format. However, as long as the printout is an accurate reflection of the original data, it is irrelevant what the operating system or the network does to that file during the printing process.

The important concept here is the accuracy of the visual output once the image is mounted. If an examiner were to simply extract key data from slack space and export that data to a text file, will a printout of that text file always constitute an accurate reflection of the original data? Many prosecutors do not think so, because the context of computer data is often as important as the data itself. Congress, by enacting Rule 1001(3), placed the emphasis on the accuracy of the visual output of computer data (printout or otherwise) once the image or file is mounted, not on the stored state of that file or image. Obviously, if the original data is actually compromised, the visual output will not be accurate. It is mandatory that the original data remain unchanged, but whether that data is compressed, encrypted or converted to a different file format in its stored state is immaterial as long as the data itself is not compromised. This is one of the reasons the MD5 hash and verification processes are so important. Even though the file format of the data in question may change, the integrity of that data must remain intact.

The Best Evidence Rule has been raised in the context of an entire drive image as well as an individual file. The Eight Circuit Court of Appeals described one such situation as follows: ". . . the district court permitted [defendant's] probation officer to describe briefly one image of child pornography found on a computer disk in his apartment. Although the court initially overruled [defendant's] objection that the admission of testimony describing the contents of the computer disk violated the best evidence rule, *see* Fed.R.Evid. 1002, it later reversed course and instructed the jury to disregard that portion of the officer's testimony."[112] A Texas Appellate Court ruled that an image copy of a hard drive qualifies as an "original" for the purposes of the Best Evidence Rule.[113] The issue of whether an EnCase Evidence File suffices as an "original" under the Best Evidence Rule was litigated successfully in US Federal District Court, New Hampshire (see § 4.4 for a full discussion).

In situations where computer evidence is collected from a business, a drive image copy is often the only "original" available to the examiner, as the company often requires immediate return of the original drives in order to remain in business, or the

company does not allow its mission-critical servers to be shut down, thereby necessitating a live acquisition of the forensic image. See Section 1.5, above, for a discussion of the authentication issues concerning live acquisition.

§ 4.2 Presenting Electronic Evidence at Trial

The United States DOJ Guidelines on Searching and Seizing Computers states "an accurate printout of computer data always satisfies the best evidence rule."[114] This certainly is true in general. However, in *Armstrong v. Executive Office of The President,*[115] the court correctly ruled that a "hard copy" paper printout of an electronic document would not "necessarily include all the information held in the computer memory as part of the electronic document."[116] The court further noted that without the retention of a complete digital copy of an electronic document such as an e-mail message, "essential transmittal relevant to a fuller understanding of the **context and import** of an electronic communication will simply vanish."[117]

As illustrated by the *Armstrong* case, the presentation of electronic evidence often requires the visual display of the logical data structure of a file, its context, and its associated metadata, in addition to the physical data of that file. When seeking to establish a defendant's state of mind by presenting an electronic audit trail, the ability to display a visual output showing various file attributes and other metadata and demonstrating the logical connection to various data files—instead of relying upon dry and technical expert testimony—provides a tremendous advantage to the advocate of such evidence. EnCase software provides the best method to visually display all physical and logical data contained on the target drive, while showing the context of such files by displaying file metadata and other means. When providing testimony, many examiners present evidence through screenshots in a PowerPoint presentations format, or take EnCase software with them into Court for a live demonstration. In *United States v. Dean*, the opinion reflects that the prosecution presented results of its computer forensic examination through PowerPoint slides.[118] Such a presentation, fast becoming common if not mandatory in modern trial practice, is virtually impossible using the available command-line utilities.

In *Dean*, the prosecution sought to establish that the Defendant accessed and viewed files on a series of floppy disks. While the Defendant denied ever accessing and viewing those files, his computer operating system created temporary link files when he accessed the files on the floppy disk. A forensic investigator from the US Customs Service recovered those temporary link files from the Defendant's hard drive. In order to show the context and metadata associated with the link files, including file created dates, full path location and other information, the prosecution successfully presented EnCase screen shots as evidentiary exhibits. These screen capture exhibits provided the most accurate visual display of the data, as it existed on the Defendant's computer at the time of seizure. The court allowed the screenshots into evidence and Dean was convicted on all counts.

Lnk. Files Deleted from \Windows\Recent Directory

Preview		File Name	File Created	Full Path
:\ ▮▮▮ jpg....A:\.N<y..M..	⊘	▮▮dy.lnk	08/26/99 10:13:08PM	DeanHD\C\WINDOWS\Recent▮▮y.lnk
.A: ▮▮ jpg....A:\.........	⊘	▮▮s.lnk	08/19/99 11:19:56AM	DeanHD\C\WINDOWS\Recent▮▮lnk
..A:\10_x7 jpg....A:\.....h...	⊘	10_x7.lnk	08/19/99 11:20:34AM	DeanHD\C\WINDOWS\Recent\10_x7.lnk
:\ !04spr~1 jpg....A:\..l...(..	⊘	!04spr~1.lnk	08/26/99 10:14:28PM	DeanHD\C\WINDOWS\Recent\!04spr~1.lnk
:\ygs-00~3 jpg....A:\F="%s"><B	⊘	·GS-00~3.LNK	07/17/99 10:56:34PM	DeanHD\C\WINDOWS\Recent\·GS-00~3.LNK
.A:\07f1ac jpg....A:\.........	⊘	·7FJAC.LNK	08/26/99 10:11:48PM	DeanHD\C\WINDOWS\Recent\·7FJAC.LNK
.A: ▮▮ .jpg....A:\\.Z.o.l.~	⊘	▮▮3.lnk	07/17/99 10:57:50PM	DeanHD\C\WINDOWS\Recent▮▮lnk

Exhibit 12h

Figure 3: A screenshot exhibit offered by the prosecution and entered into evidence in *United States v. Dean*. The Court ordered the redaction of certain filenames on the grounds that their probative value was outweighed by their prejudicial nature.

Dean is an important illustration that the context of computer evidence is often just as important as the data itself. If portions of relevant data are recovered in unallocated or slack space areas of a drive, how is that evidence presented? For example, if that data recovered from slack space is simply exported to a text file and then printed out, a proponent will likely face significant difficulty in admitting that evidence without establishing its context. What file partially overwrote the first section of the cluster where the slack data still resides? When was the file currently occupying that cluster created and last modified? What is the precise address (physical cluster, sector offset, etc.) of the data recovered from slack space? Figure 4 illustrates how such data should be presented both for demonstrative purposes and to comply with the Best Evidence rule.
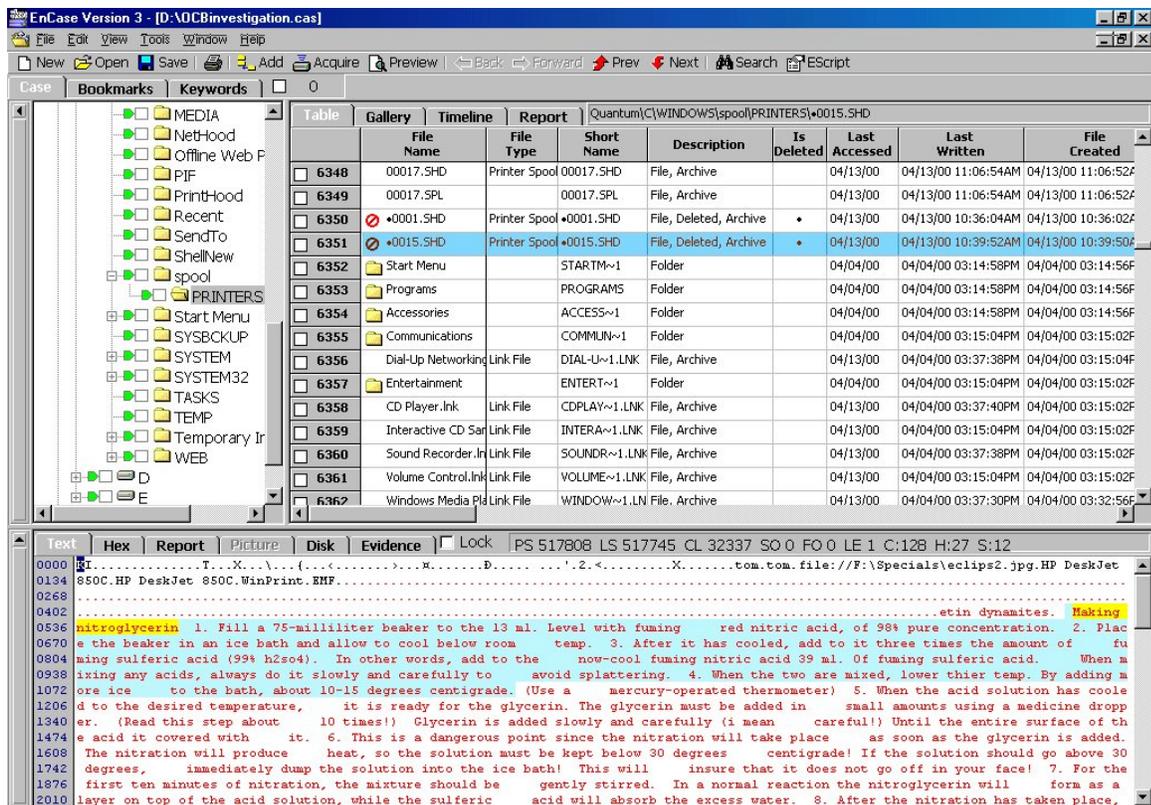
Figure 4: Key evidence of bomb making instructions found in the slack area of a cluster also occupied (at the beginning) by a deleted printer spool file. Screen shot presentation enables full contextual presentation of the data.

In a 2005 case that did not involve computer forensics, there was an interesting best evidence discussion involving a digitally enhanced videotape. In *United States v. Seifert*,[119] a defendant charged with arson challenged whether a digitally enhanced videotape recovered from the fire was "best evidence." The defendant asserted that the technician's modification of brightness and contrast and enlargement of the image rendered the tape untrustworthy as an original. The court did not agree, holding the enhanced tape to be a duplicate "which accurately reproduces the original." While the process used by the technician was satisfactory, the court suggested in dicta, "that technology which provides a digital trail could provide an even stronger forensic basis for admission of enhanced electronic evidence."[120]

§ 4.3   Compression And the Best Evidence Rule

The issue of compression in the context of computer evidence is one that has never been addressed by the courts in any known published decisions. However, there is some appreciable authority where US courts have discussed data compression in the context of intellectual property disputes. These rulings do provide a degree of guidance on how the courts would address compressed computer files as evidence.

In *Storer v. Hayes Microcomputer Products*, the court defined computer data compression as follows: "Data compression is the process of reducing the size of the representation of a string of electronic data in order to permit it to be transmitted or

stored more efficiently and later to be reconstructed without error."[121] While the *Storer* case addressed whether a company's compression technology infringed upon a patent held by a competitor for similar technology, the case provides a clear and concise definition of data compression as articulated by a court. In *Universal City Studios v. Reimerdes,*[122] a Napster-genre copyright infringement case, the court determined that a software application that compresses and then decompresses DVD recordings using "lossy" compression infringes upon the copyright of the publisher. This is so even though "lossy" compression involves inexact replication of the original file. Thus, the compressed and then decompressed end product infringes upon the copyright of the original material.

Compression technology allows EnCase software to store a large disk image in a relatively small file. An Evidence File can be compressed upon acquisition or at a later point in the investigation. Compressed Evidence Files can be searched and examined by EnCase software in the same manner as uncompressed Evidence Files. EnCase software uses an industry standard "lossless" compression algorithm to achieve an average of 50% size reduction. Lossless data compression, where the compressed-then-decompressed data is an exact replication of the original data, is a very basic and standard aspect of computer science. It is also important to note that whenever a computer file is transmitted over the Internet or it is sent to the printer, it undergoes compression. Some excellent resources on lossless data compression and data compression in general can be found at http://www.data-compression.com.

As noted above, Federal Rule of Evidence 1001(3) provides "[if] data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.'" Compression does not have any effect on the actual content of the Evidence Files or the integrity of the evidence. Importantly, a compressed Evidence File will register the same CRC and MD5 hash values as an uncompressed Evidence File of the same drive, as the file content is identical. Further, in the post-acquisition verification process, EnCase software verifies the compressed blocks as well as the MD5 hash for the entire image in the same manner as with uncompressed Evidence Files.

As a compressed Evidence File will contain the exact same contents and the same CRC and MD5 hash values as an uncompressed Evidence File of the same disk image, both will constitute an "original" under Fed.R.Evid. 1001(3). For the same reason, an Evidence File that is acquired uncompressed and is subsequently copied in a compressed format also constitutes an "original" under Rule 1001(3).

§ 4.4 *United States v. Naparst* – The EnCase Evidence File Validated As Best Evidence

The issue of whether EnCase Evidence Files constituted the best evidence of the computer data contained therein was litigated in a federal criminal prosecution in New Hampshire. The prosecution offered to allow the Defense access to a copy of the EnCase Evidence File for discovery purposes. However, the Defense contended that it required access to the original computer systems in question so that they could operate those computers and examine them in their native environment, and filed a formal

written request for a Court order allowing such unfettered access to the "original" computer evidence. The Government filed a successful objection to the request, asserting that the "mirror image" created by the Special Agent is the proper way to preserve the original evidence, as turning on the computer, as the Defense requested, will change the state of the evidence by altering critical date stamps and potentially overwriting existing files and information.

The Court ruled that the EnCase Evidence File qualified as the Best Evidence and that a discovery copy of the Evidence File would be sufficient discovery disclosure. Alternatively, the court ruled that the defense could have access to the original computer systems only if its expert created another proper forensic image under the supervision of the Special Agent. The defense was barred from booting the original computer systems to their native operating systems. A copy of the three-page brief filed by the Government in support of its successful objection is reprinted here with permission.

UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

(United States of America
(
(v.   Cr.: 00-11-1-M
(
(Harold Naparst

<u>GOVERNMENT'S OBJECTION TO DEFENDANT'S</u>
<u>MOTION FOR ACCESS TO COMPUTER EVIDENCE</u>

NOW COMES the United States of America, by Paul M. Gagnon, United States Attorney for the District of New Hampshire and states the following:

1. On August 16 & 17, 2000, an expert retained by the defense in this matter was permitted access to the government's expert witness, all of his reports, and an exact mirror image of the defendant's computer hard drives.

2. The defense has now moved this Court to grant them access to the defendant's actual computer equipment which was seized from his home on January14, 2000.

3. The defense argues that this is necessary for preparation of their defense; however, the government submits that if the defense has truly consulted with an expert,

then they are aware that the mere act of turning on or "booting up" the defendant's computer will alter that evidence forever.

4. Turning on the computer will change the state of the evidence by altering critical date stamps, and will potentially write over and erase existing files. See affidavit of Shawn McCreight attached as Exhibit 1.

5. The "mirror image" created by Supervisory Special Agent Marx is the proper way to preserve the original evidence and the government will demonstrate that this evidence is the original evidence of the defendant's hard drives. See affidavits of Shawn McCreight and SSA Stephen Marx attached as exhibits 1 and 2.

6. The importance of conducting reviews of computer evidence on mirror image backups is so universally understood that in one civil action, the plaintiffs were sanctioned for failing to create a mirror image of the defendant's hard drive before their review. See Gates Rubber Company v. Bando Chemical Industries, Limited, 167 F.R.D. 90, (D. Colorado, 1996). Instead, they ran a program on the original hard drive which "obliterated, at random, 7 to 8 percent of the information which would otherwise have been available." 167 F.R.D. 90, 112. The Court, therefore ruled that sanctions were appropriate because the plaintiff "had a duty to utilize the method which would yield the most complete and accurate results" and "should have done an 'image backup' of the hard drive which would have collected every piece of information on the hard drive…" Id.

7. Defendant has not demonstrated that he has been deprived of access to any of the evidence of this matter [1] or prejudiced in any way.

---

[1] Presumably, the defense has made allegations about the quality or handling of the evidence in their Asecret@ affidavit; the government is obviously in no position to respond to any such allegation(s).

8.   In fact, prior to the defendant's expert retention, on July 7, 2000, defense counsel was notified by correspondence that any expert retained should be familiar with EnCase software to facilitate their review of the computer evidence. No objection was raised at that time, nor did the defense ever ask for or suggest different imaging software.

WHEREFORE for the above stated reasons, the government respectfully requests that this honorable Court deny the defendant's motion for access to the defendant's computer.

Respectfully submitted

PAUL M. GAGNON
United States Attorney

By:
Helen White Fitzgibbon
Assistant United States Attorney

5

Legal Analysis of the EnCase Evidence File

§ 5.0 Overview

The central component of the EnCase methodology is the Evidence File, which contains the forensic bit-stream image backup made from a seized piece of computer media. The Evidence File consists of three basic parts -- the file header, the checksums and the data blocks -- which work together to provide a secure and self-checking "exact snapshot" of the computer disk at the time of analysis. The EnCase Evidence File is unique in that it is a secure, self-verifying and fully integrated forensic image specifically designed as read-only random access data in the context of a computer forensic investigation. Many other imaging tools are backup utilities modified for forensic purposes, and as a result do not contain integrated authentication and verification processes.

This section discusses in detail the major components and functions of the EnCase Evidence File that may be relevant for purposes of authenticating the Evidence File in a court of law.

§ 5.1 Evidence File Format

The EnCase process begins with the creation of a complete physical bit-stream forensic image of a target drive in a completely non-invasive manner. With the exception of floppy and CD-ROM disks, all evidence is acquired by EnCase software in either a DOS environment, or in a Windows environment, where a specially designed hardware write-blocking device is utilized. The ability of EnCase software to image in Windows in conjunction with a write-blocking device presents several advantages to the examiner, including dramatically increased speed, more flexibility, and superior drive recognition.

The acquired bit-stream forensic image is mounted as a read-only "virtual drive" from which EnCase software proceeds to reconstruct the file structure by reading the logical data in the bit-stream image. This allows the examiner to search and examine the contents of the drive in a Windows GUI, all in a completely non-invasive manner. Additionally, the integrated process enables EnCase software to identify the exact original location of all evidence recovered from a targeted drive without the use of invasive disk utilities.

Every byte of the Evidence File is verified using a 32-bit Cyclical Redundancy Check (CRC), which is generated concurrent to acquisition. Rather than compute a

CRC value for the entire disk image, EnCase software computes a CRC for every block of 64 sectors (32KB) that it writes to the Evidence File. A typical disk image contains many tens of thousands of CRC checks. This means that an investigator can determine the location of any error in the forensic image and disregard that group of sectors, if necessary. The Cyclical Redundancy Check is a variation of the checksum, and works in much the same way. The advantage of the CRC is that it is order sensitive. That is, the string "1234" and "4321" will produce the same checksum, but not the same CRC. In fact, the odds that two sectors containing different data produce the same CRC is roughly one in a billion. The CRC function allows the investigators and legal team to confidently stand by the evidence in court.

In addition to the CRC blocks, EnCase software calculates an MD5 hash for all the data contained in the evidentiary bit-stream forensic image. As with the CRC blocks, the MD5 hash of the bit-stream image is generated and recorded concurrent to the acquisition of a physical drive or logical volume. The MD5 hash is calculated through a publicly available algorithm developed by RSA Security. The odds of two computer files with different contents having the same MD5 hash value is roughly ten raised to the 38th power. If one were to write out that number, it would be a one followed by thirty-eight zeros. By contrast, the number one trillion written out is one followed by only twelve zeros. The MD5 hash value generated by EnCase software is stored in a footer to the Evidence File and becomes part of the documentation of the evidence.

Throughout the examination process, EnCase software verifies the integrity of the evidence by recalculating the CRC and MD5 hash values and comparing them with the values recorded at the time of acquisition. This verification process is documented within the EnCase-generated report. It is impossible for EnCase software to write to the Evidence File once it is created. As with any file, it is possible to alter an EnCase Evidence File with a disk utility such as Norton Disk Edit. However, if one bit of data on the acquired evidentiary bit-stream image is altered after acquisition, even by adding a single space of text or changing the case of a single character, EnCase software will report a verification error in the report and identify the location where the error registers.

§ 5.2 CRC and MD5 Hash Value Storage and Case Information Header
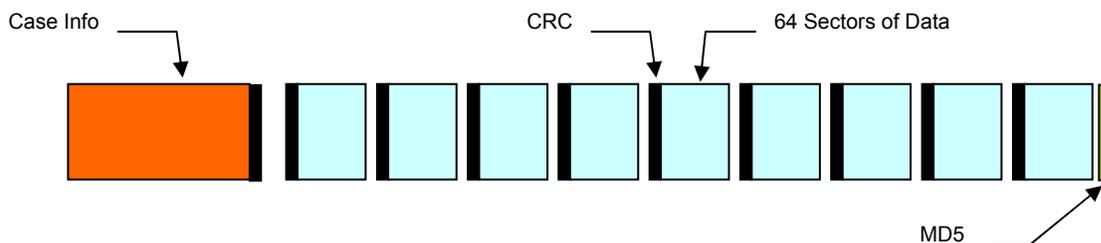
Figure 1: A Graphical Representation of the EnCase Evidence File

The CRC and MD5 hash values are stored in separate blocks in the EnCase Evidence File, which are external to the evidentiary forensic image itself. Those blocks containing the CRC and MD5 hash values are separately authenticated with separate CRC blocks, thereby verifying that the recordings themselves have not been corrupted.

If any information is tampered with, EnCase software will report a verification error. Conversely, merely generating an MD5 hash with another tool and recording it manually or in an unsecured file where it may be altered without detection may not fully insulate the examiner from questions of evidence tampering. For this reason, the CRC and MD5 hash value calculations generated with EnCase software are secured and tamper-proof.

The Case Info header contains important information about the case created at the time of the acquisition. This information includes system time and actual date and time of acquisition, the examiner name, notes regarding the acquisition, including case or search warrant identification numbers, and any password entered by the examiner prior to the acquisition of the computer evidence. There is no "backdoor" to the password protection. All the information contained in the Case Info file header, with the exception of the examiner password, is documented in the integrated written reporting feature of EnCase software. The Case Info file header is also authenticated with a separate CRC, making it impossible to alter without registering a verification error.

§ 5.3 Chain of Custody Documentation

A distinct advantage of the EnCase process is the documented chain of custody information that is automatically generated at the time of acquisition, and continually self-verified thereafter. The time and date of acquisition, the system clock readings of the examiner's computer, the acquisition MD5 hash value, the examiner's name and other information are stored in the header to the EnCase Evidence File. This important chain of custody information cannot be modified or altered within EnCase software, and EnCase software will automatically report a verification error if the Case Info File is tampered with or altered in any way.

EnCase Report

Case: **CIN Investigation**

Evidence Number "2000-11-2"   Alias "Quantum"

File "C:\EnCase\Quantum.E01" was acquired by Sheldon at 05/22/00 05:50:44PM.
The computer system clock read: 05/22/00 05:50:46PM.

Acquisition Notes:
  Copyright 2000 Guidance Software, Inc..

File Integrity:
  Completely Verified, 0 Errors.
  Acquisition Hash: 7E76AB52735960245330533EAA246A6A
  Verification Hash: 7E76AB52735960245330533EAA246A6A

Figure 2: Chain of custody information is documented in an automatically generated report

§ 5.4 The Purpose of Sterile Media and The EnCase Process

Computer forensic investigation procedures developed before the EnCase process require that sterile computer media be used to restore an image backup for analysis by separate search utilities that conduct a physical or "end-to-end" analysis of a single drive. Sterile media is required under such a procedure because the non-integrated disk utilities cannot identify the boundaries of the restored forensic image file. Thus, if an image file of an eight gigabyte drive is restored to a ten gigabyte non-sterile drive filled with data, the two gigabytes of "slack" will be improperly read and analyzed by non-integrated DOS tools. In the past, examiners have experienced problems when utilizing media they believed to be brand new and thus sterile, only to eventually learn that that the storage media was actually only recycled and reformatted. For these reasons, a manually created sterile environment must exist when utilizing search tools that cannot differentiate data residing outside of the original boundaries of the disk image.

The EnCase process does not require the use of sterile media for the same reasons that a word processing program does not require that its text files be stored on sterile media in order to be accurately read. As described above, the EnCase Evidence File is a logical file with logical file boundaries that EnCase software recognizes in the same way that MS Word for Windows recognizes a MS Word document. There is no concern that when reading one file, data from another file on the disk will inadvertently bleed onto your screen. As such, the requirement that "sterile media" be used for a computer forensic investigation actually reflects the limitations of the software employed as opposed to being an absolutely necessary item of protocol. EnCase software is specifically designed to only read data contained within the Evidence File. As such, there is no possibility that data residing outside of an EnCase Evidence File will be inadvertently searched or analyzed by EnCase software.

§ 5.5 Analyzing The Evidence File Outside of the EnCase Process

The EnCase Evidence File is designed not only to contain a forensic image, but a forensic image of a targeted drive that is secured and verified through an integrated process. If an investigator wishes to conduct an analysis of the forensic image contained in the EnCase Evidence File with a tool other than EnCase software, the best practice is to restore the physical drive to a separate and dedicated partition before proceeding with the analysis. Otherwise, an investigator may face problems authenticating evidence extracted from an EnCase Evidence File with third party software for several reasons.

First, the CRC and MD5 hash values that EnCase software generates and records concurrent to acquisition can only be read and reported by EnCase software. The continual verification by EnCase software of the integrity of the Evidence File throughout the course of the examination is a key component of the EnCase process. While an MD5 hash of the targeted drive can be independently taken with a separate utility for verification purposes, software operating outside of the EnCase environment cannot confirm the Evidence File data integrity based upon the information recorded by EnCase software upon acquisition and stored within the Evidence File. For security

reasons, the MD5 hash, CRC values and other case information is secured within the Evidence File and is not designed to be read by third party software that Guidance Software cannot verify and thus cannot provide testimony regarding its functionality. Further, allowing the EnCase Evidence File to be reverse engineered or "cracked" by third party software is inconsistent with the fundamental principles of computer forensic investigations.   The EnCase process has been designed specifically for computer forensic investigations and has been widely shown to produce consistent and accurate results. When third party software outside of the design and intent of the EnCase process is utilized, any presumption of authenticity, such as that afforded under Fed.R.Evid. 901(b)(9), may be lost.

Secondly, various acquisition data (investigator's name, dates, passwords, etc), jump tables, file pointers, CRC data and the MD5 hash block are stored either in the Evidence File header or at intervals between blocks of acquired data to allow integrated verification of data integrity and to enhance error detection and speed. While EnCase software recognizes this "external" data as outside of the evidentiary forensic image, third party search tools cannot so differentiate and thus will scan this data when running a search directly on an EnCase Evidence File. In other words, these programs may "find" something that was not placed there by the suspect or user. Further, if any such "non-evidentiary" data happens to fall in between blocks of acquired data that make up a picture or document, the evidence will likely not be recovered at all, leading to incomplete results. At best, the investigator will have to repeat the whole exercise in a forensically proper manner.

Another critical factor involves the important EnCase function of identifying the precise location of each byte of data on the original drive. This is an important feature of the EnCase process, as any evidence recovered by EnCase software can be independently verified by disk utilities such as the Norton tools when utilizing the precise disk location information automatically provided by EnCase software. However, even if data is successfully extracted from an EnCase Evidence file by a third party utility, that tool cannot identify the precise location where that data resided on the suspect's media at the time of acquisition. While it is possible to attempt to manually approximate the location under such a methodology, such a practice is forensically unsound for obvious reasons.

Finally, in the same way that a Zip file's contents are not readable until "unzipped," raw information on a hard drive or in a forensic image file is not "evidence." It only becomes evidence when it is "mounted" as a file system in the same way that the suspect used it. EnCase software reads file system partition tables and fragmentation blocks by analyzing the file system structure (MBR, FAT tables, etc). Only by knowing the "cluster chain" of all the files (and the unallocated areas) can a complete recovery process be possible. By simply conducting a physical "end-to-end" search of the Evidence File, third party utilities ignore this crucial information and therefore cannot attain the complete recovery of data. At worst, the process could result in "splicing" together pieces of unrelated documents and pictures, and thus "creating" evidence in the process. For the same reasons, EnCase software is not designed to mount images created by other proprietary imaging tools, such as a Safeback or Ghost image. In addition to the verification and rule 901(b)(9) issues, there are significant questions

whether reverse engineering a proprietary file format constitutes copyright infringement. [123] Further, the concerns regarding infringement raise symmetrical questions about the accuracy of a process that involves reverse engineering a proprietary image file format without the consent of the developer. Because of such questions, EnCase software is not designed to mount or "crack" other proprietary file images.

6

Challenges to EnCase Software and Cases Involving EnCase Software

Computer forensic investigators throughout the world utilize EnCase software for the seizure, analysis and court presentation of computer evidence. With over 18,000 licensed users, computer evidence processed with EnCase software has been successfully admitted into evidence in thousands of criminal and civil court cases. To date, there are no known instances of sustained objections to EnCase-based computer evidence on authentication grounds relating to the use of EnCase software. Courts have on occasion entertained, and subsequently overruled, objections to the authenticity or foundation of EnCase-based evidence, and we have documented several such favorable rulings at the trial court level, with transcripts provided on the resources section of our website. In a few instances, a U.S. appellate court has addressed the validity of the EnCase process in a published decision. Appellate court rulings are important as they stand as binding law in their subject jurisdiction, while providing compelling "persuasive authority" everywhere else. In addition, courts in Canada, Australia, and Singapore have published decisions accepting evidence gathered using EnCase software.

The following are summaries of notable appellate and trial court decisions that address EnCase software.

State (Ohio) v. Cook

State v. Cook, 777 N.E.2d 882 (Ohio App. 2002) represents the first appellate decision that both validates and specifically addresses the EnCase software. In *Cook,* the defendant appealed his conviction on 20 separate counts of possessing child pornography and designation as a sexual predator, challenging what he claimed to be "the lack of reliability of processes used to create two mirror images of the hard drive."[124] The Ohio appellate court addressed this argument by first describing in detail the process of how the law enforcement investigator in that case utilized EnCase software to make a forensic "mirror image" of the target drive. The court then noted that "[u]sing EnCase with the mirror image hard drive, [the investigator] generated a report hundreds of pages long, containing a complete history of everything on the computer's hard drive. Among the contents were over 14,000 pornographic pictures, covering a wide range of dates."[125] The court also specifically noted that the investigator was trained in the use of the EnCase software. In upholding the validity of the EnCase software, the Court stated:

"In the present case, there is no doubt that the mirror image was an authentic copy of what was present on the computer's hard drive."[126]

The court cited Ohio Rule of Evidence 901(A) and 901(B), which are nearly identical to the corresponding federal rules, (and are discussed in length in Sections 1.1 and 2.1, respectively, of this text). The court found that Rule 901(A), which provides that authentication "as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims," governed the issue of authentication of the computer evidence. The court further noted that Rule 901(B)(9), which provides that "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result" is one example of authentication being established under 901(A). The court concluded that the EnCase software was such a process or system that produced an accurate result, thus satisfying authentication under Rule 901(A).

Williford v. State of Texas[127]

The Court of Appeals of Texas, in a case called *Williford v. State*, explicitly validated the reliability of EnCase software and a police investigator's status as an expert witness. The *Williford* case involved a defendant who had taken his home computer to a repair shop, which found child pornography on the computer and notified the police. The defendant then consented to a search of the hard drive. The police computer forensics investigator used EnCase software to image the drive and analyze its contents. When the investigator testified at trial, the defendant objected on the grounds that the investigator "was not qualified as an expert to testify about the theory or technique in developing the EnCase software or its reliability."[128] The defendant further contended that the investigator "was not qualified to testify as an expert witness regarding the scientific technique that he used to reproduce pictures . . . from appellant's computer."[129] In rejecting the defendant's claims, the Court held that:

> We find that Detective Owings's testimony satisfied the *Kelly* criteria for reliability. Detective Owings provided testimony on each of the seven factors identified in *Kelly*. Detective Owings is the computer expert for the Brownwood Police Department and is knowledgeable about EnCase. He testified that EnCase is generally accepted in the computer forensic investigation community, that EnCase is used worldwide, that he knew how to use EnCase, that he knew how EnCase worked, that he had successfully used EnCase in the past, that EnCase can be tested by anyone because it was commercially available and anyone could purchase it, that EnCase has been tested, that there have been several articles written about EnCase and other computer forensic software programs, that SC Magazine gave EnCase an overall five-star rating out of five stars, that EnCase has a low potential rate of error, that he successfully copied appellant's hard drive by using EnCase, and that EnCase verified that he had successfully copied appellant's hard drive. Detective Owings described in detail for the trial court how EnCase worked. Detective Owings's testimony established EnCase's reliability.[130]

The *Williford* case is important because it re-emphasizes (and from an appellate court, no less) two key points: 1) a computer forensics investigator need not have developed EnCase software himself to serve as an expert witness at trial regarding the forensic examination conducted; and 2) EnCase software is a reliable, widely available, thoroughly tested, and court-approved computer forensics tool.

State (Ohio) v. Morris

In this appellate case from Ohio, the original hard drive, which "belonged to a non-party . . . who used the computer in his business," was overwritten by the forensic investigator.[131] All that was available at trial was the forensic image of the drive, created using EnCase software. The Court noted:

> [T]he evidence in question was actually presented at trial in the form of a copy of the hard drive... In this case, [the forensic investigator] testified that the software utilized, Encase Version 3, takes the contents of the hard drive through a complex math equation and creates a 128 bit number known as a fingerprint. . . . [The forensic investigator] went on to note that in the instant matter, the copy created by Encase was an exact copy of the original hard drive. Appellant has seemingly argued on appeal that, absent a software engineer verifying that Encase software does what it purports to do, this hard drive should not have been admitted. **This Court disagrees**.[132]

The Court's decision: (i) validates the MD-5 hash process, and (ii) considers forensic disk images to be exact copies and admissible when the "original" is no longer available. This is important not merely in cases in which the forensic investigator has overwritten a hard drive, but for matters involving the collection of computer evidence using network-enabled computer forensic software, such as EnCase Enterprise software.

Taylor v. State

Taylor v. State, 93 S.W.3d 487 (Tex. App. 2002) is another appellate decision that addresses the EnCase software, although not to the same degree as *Cook* or *Williford*. Taylor involved several different issues on appeal, most of which did not involve EnCase software. The issue that did address EnCase software centered on whether the acquisition and verification MD5 hash readings documented in the EnCase Report for authentication purposes constituted hearsay. The court determined that because the acquisition and verification hash readings are generated by a computer analysis independent of any data inputted by a human, the information is not hearsay.[133] As a result, the court rejected the defendant's contention that the drive image was not authentic.

This ruling is significant as it provides that EnCase Evidence Files can potentially be authenticated at trial, even if the examiner who created the image is unavailable to testify. EnCase software generates a MD5 hash value of an acquired drive concurrent

with acquisition in a secure, integrated and automated manner, meaning that this critical authentication data is computer-generated and automatically documented. Other processes to generate and record an MD5 hash are not integrated or secure, thus requiring the manual recording and documentation of the readings, which, under Taylor, would be inadmissible hearsay if the examiner who acquired the drive was unavailable at trial, and, even if available, subject the examiner to additional scrutiny.

Matthew Dickey v. Steris Corporation

One of the first known instances of a "serious" challenge to the use of EnCase software occurred in a civil litigation matter before the United States Federal District Court, Kansas, where at an April 14, 2000 pre-trial hearing, the court ruled that the testimony of an Ernst & Young expert regarding his computer forensic investigation based upon EnCase software would be allowed, overruling objections from the Plaintiff. In *Matthew Dickey v. Steris Corporation*, the trial court overruled evidentiary objections to the introduction of EnCase-based evidence at an April 14, 2000 pre-trial hearing. Plaintiff Dickey brought a motion *in limine* seeking to exclude the testimony of an Ernst & Young expert, regarding the results of his computer forensic investigation based upon the use of EnCase software. The Plaintiff's motion was based upon the report of his own expert, which consisted of a critique of the Ernst & Young report.

Steris Corporation ("Steris") successfully opposed Dickey's motion, clearing the way for the expert testimony based upon EnCase software. Steris brought its own motion to exclude the testimony of the Plaintiff's expert. Among Steris's arguments was the contention that the Plaintiff's expert was unqualified to provide an expert opinion about computer forensics as, among other reasons, she was admittedly unfamiliar with the EnCase software. The court denied both motions, finding that 1) the challenge to the EnCase process employed by the Ernst & Young expert was without merit, and 2) the testimony of the Plaintiff's expert would not be excluded, although she could be questioned at trial regarding her unfamiliarity with EnCase software, which would be relevant to her credibility as a computer forensics expert.

State of Washington v. Leavell

On October 20, 2000 in a Washington State Superior Court, a contested hearing took place in the matter of *State of Washington v. Leavell*[134] where the defense brought an unsuccessful suppression motion to exclude from trial all computer evidence obtained through a forensic investigation utilizing EnCase software. A copy of the complete hearing transcript is included as an attachment to this issue.

The defense brought its challenge on two grounds: 1) That the government's examiner could not establish a proper foundation for the evidence, asserting that EnCase software was essentially providing "expert testimony" and that the defense was unable to cross-examine the government witness in detail regarding how EnCase software works and how it was developed; and 2) That EnCase software should be subject to a *Frye*[135] analysis, which is a legal test employed by many courts in the United States to determine whether a scientific technique for obtaining, enhancing or

analyzing evidence is generally accepted within the relevant scientific community as a valid process.

The Court ruled that the government's trained computer examiner could provide a sufficient foundation for the evidence recovered by EnCase software, and that EnCase software met the *Frye* test as a process with general acceptance and widespread use in the industry. On the issue of evidentiary foundational requirements, the Court relied on the case of *State v. Hayden,*[136] which upheld the validity of enhanced digital imaging technology and the admissibility of evidence obtained through this process. The Court noted that like enhanced digital imaging technology, EnCase software is merely a tool utilized by the State's examiner and is not providing expert "testimony." The Court determined that the investigating officer who was trained in computer forensics could testify regarding the EnCase process.

On the related argument of the *Frye* analysis, the Court similarly upheld the introduction of evidence obtained with EnCase software. The Court determined that EnCase software was a widely used and commercially available software tool for recovering computer evidence, including deleted files, and that the investigating officer had conducted his own testing and successfully recovered deleted files on many other occasions. The defense based its *Frye* challenge in part on the theory that only Microsoft could completely and accurately recover deleted files, as the inner workings of the Windows operating system were proprietary. The government countered by producing an affidavit from an internal computer forensic investigator at Microsoft who testified that his department utilized commercially available software for the forensic recovery of deleted files, and that EnCase software was one of their primary tools for this purpose. The Court expressly took judicial notice of Microsoft's use of EnCase software, which served as one of the considerations in the Court's ruling.

Finally, the Court relied upon the case of *United States v. Scott-Emuakpor.*[137] The court in *Scott-Emuakpor* determined that the United States Secret Service agents who conducted the computer forensic examination did not need to be a qualified experts in computer science to present their findings and that the USSS agents could provide testimony to authenticate and introduce documents purportedly found on the Defendant's computers.

People v. Rodriguez

On January 11 and 12, 2001 in Sonoma County, California Superior Court, a contested hearing took place in the matter of *People v. Rodriguez*[138] where the court subjected EnCase software to a lengthy pretrial evidentiary hearing to establish its foundation as a valid and accepted process to recover computer evidence for admission into court. (A copy of the complete hearing transcript is included as an attachment to this issue.) The Rodriguez case involved recovered e-mail messages from defendant Rodriguez's seized computer. Many of the e-mails sent by Rodriguez included his boasts of committing several armed burglaries and robberies. The e-mails were highly relevant to Rodriguez's intent and state of mind.

The defense brought its challenge on two grounds: 1) That EnCase software should be subject to a *Frye*[139] analysis, which is a legal test employed by many courts in the United States to determine whether a process for obtaining, enhancing or analyzing scientific or technical evidence is generally accepted within the relevant scientific community as a valid process; and 2) That the EnCase Report itself should not be admitted into evidence. The *Frye* test is employed in many state courts, while *Daubert*,[140] is the standard in US Federal court. Many other countries with a common law system also utilize standards with many similarities to a *Daubert* analysis for scientific evidence.

Upon the conclusion of the hearing, the defense conceded that EnCase software was an "appropriate and accepted" methodology under the *Frye* test for recovering computer evidence.[141] After finally admitting that EnCase software represented a valid and accepted process, the defense then focused its attention on whether the EnCase Report itself should be admitted into evidence, under the grounds that the prosecution could not properly authenticate the document. The court overruled the defense's objection and allowed the EnCase Report generated by the examiner into evidence. After the court's ruling, the trial proceeded and the jury ultimately returned a verdict convicting Rodriguez of robbery, burglary and assault with a deadly weapon.

The transcript features an extensive direct examination and a cross-examination of the computer forensic examiner, addressing in detail the factors related to authenticating the EnCase process under a *Frye* analysis. The prosecution testimony in the *Rodriguez* case is very similar to that of the mock trial transcript provided in Vol. 1, issue 4 of this journal. Among the findings presented in the hearing were that EnCase software was a widely used and commercially available software tool for recovering computer evidence, including deleted files, and that the investigating officer had conducted his own testing and successfully recovered deleted files on many other occasions. The extensive peer review and publication of the EnCase software was also emphasized. These points and the widespread acceptance of EnCase software in the industry were important factors that successfully authenticated the EnCase process under the *Frye* test.

The *Rodriguez* case represents another example of the Courts subjecting EnCase software to a *Daubert/Frye*-type hearing, which is normally applied to determine the validity of scientific evidence. For this reason, the next section reviews the *Daubert/Frye* analysis in the context of authenticating EnCase software as a valid and accepted process.

United States v. Habershaw

In *United States v. Habershaw,* 2001 WL 1867803 (D.Mass. May, 13, 2001), the court upheld the legality of a computer search by a computer forensic expert, David Papargiris, over the defendant's objections. While not reflected in the court's published opinion, EnCase software was used by the experts for both the prosecution and the defense. The expert report submitted to the court by David Papargiris is included in full at the end of this chapter.

Habershaw involved a prosecution for possession of child pornography, where the defendant orally agreed to have his computer searched. The first responder agents briefly (and, as contended by the defense, improperly) reviewed the defendant's computer, finding child pornography. The defendant subsequently signed a written consent form providing the police consent to search his computer and take "from the premises any property which they desired as evidence for criminal prosecution." The police then took the defendant's computer and some floppy disks into police custody. A few days later, the police obtained a search warrant to search the computer in its custody for material and information related to child pornography stored in the computer. Papargiris then conducted a computer forensics analysis of the hard drive, finding a great deal of incriminating evidence.

There are several compelling rulings and lessons in Habershaw, including the following:

1) The Court rejected the defense's claims that a "sector-by-sector" search with computer forensic software exceeded the scope of the warrant. The court relied on the *United States v. Upham*[142] decision, which upheld a search where the government retrieved "deleted" computer files, and thus determining that the government could use any means to retrieve information from a computer so long as the information was within the scope of the warrant.

2) The EnCase Timeline feature proved to be important in this case. The opinion reflects intensive testimony regarding file time and date stamps, such as what files were accessed by the case agent and what files were accessed by the suspect before the case agent arrived, and when the computer was shut down for imaging when Mr. Papargiris arrived on the scene and saved the day. The expert report submitted to the court by Papargiris (Provided in full at the end of this chapter) reflects that screen captures from the Timeline view were instrumental in providing important context to the sequence of events described at length in the opinion. Papargiris's report also features effective use of EnCase screen captures.

3) The actions of the case agent, who operated the target computer and accessed files in a live environment, were called into question by the defense's computer forensic expert, who claimed that evidence may have been planted by the case agent. Mr. Papargiris was able to show that while files were accessed during the time when the case agent was on the scene, but before Mr. Papargiris arrived, no files on the computer were created or modified during that time. Further, the Timeline showed no additional activity from the point when the computer was ultimately shut down for imaging by Papargiris. The Evidence File's integrated chain of custody feature was helpful in correlating the imaging of the computer to the cessation in activity on the Timeline.

4) This case reflects a growing trend of increased sophistication amongst defense experts. It is apparent that defense experts are not challenging accepted computer forensics software, but instead using computer forensic software to put on their case. In this case, the defense expert managed to establish that the computer was searched by the case agent before a written consent form was signed. However, the court

determined that the suspect had previously given oral consent and Mr. Papargiris was able to demonstrate that the files in question were accessed during this "oral consent" period. While the end result was favorable, this is an important example of how defense experts can impeach case agents who mishandle computer evidence.

People v. Merken

An earlier prosecution featuring the EnCase process, *People v. Merken*, case no. 1815448 (Cal. Sup. Ct., San Francisco, May 1999, involved issues regarding the defense's access to the EnCase evidence files and software for discovery purposes. In Merken, the defendant was charged with possession of child pornography images found on his hard drive. Initially, the defense was told by the prosecution that it could not obtain a copy of EnCase, as the software was only available to law enforcement. On that basis, the defense objected to the admission of the evidence obtained with EnCase software on fairness grounds, asserting prejudice from being unable to independently duplicate the processing of the computer evidence. As a compromise apparently invited by the court, the defense moved for and obtained an order for "permission" to purchase EnCase software and obtain a discovery copy of the evidentiary bit-stream image. The defense subsequently did not challenge the admission of the computer forensic evidence introduced by the prosecution, and in fact relied upon the testimony of their own computer forensics expert, who presented findings from his independent analysis of the discovery image evidence using EnCase software.

This development is potentially significant in light of the legal requirements for the admission of electronic evidence and the Best Evidence Rule. The *Merken* case is significant as it serves as an illustration where the defense relied upon the EnCase process instead of opposing it. As EnCase software allows for a more objective and automated search process that facilitates accuracy and independent duplication, courts should be less inclined to bar electronic evidence on the grounds that its admission would be unfair to the defense.[143]

State of Nebraska v. Nhouthakith

In 2001, EnCase software was used to recover evidence in a child exploitation case in Nebraska state court called *State v. Nhouthakith*.[144] The case involved a computer forensics examination by the Nebraska State Patrol that was conducted with EnCase software and that revealed computer graphic image files, whose contents included child pornography. EnCase software was subjected to an extensive *Daubert* hearing, in which the Court weighed whether to accept the evidence recovered by EnCase software. The Court held:

> That the technique of Acquisition, Authentication and Recovery of Computer Data specifically used in the Encase Software Forensic Tool is relevant in that it will assist the trier of fact to understand the evidence and to help determine a fact in issue and that it is reliable and valid because its methodology has been tested, has been subjected to peer review and publication, has a known or potential rate of error and has been generally accepted within the computer forensic

community.[145]

Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.

In this civil case, the issue was not the acceptability of evidence gathered with EnCase software. Rather, the magistrate judge addressed the use of a wiping program, Evidence Eliminator, by the plaintiff.[146] This case highlights the disastrous results that can befall a litigant that uses a wiping program such as Evidence Eliminator. In this patent infringement case in federal court in Illinois, the district court, in response to a discovery request by the defendant, had ordered the inspection of a computer used by the plaintiff. The defendant then hired an experienced forensic investigator to use EnCase software to create a forensic image and analyze the plaintiff's computer.

On February 28, 2003 the investigator imaged the subject computer. His analysis revealed that the plaintiff had employed Evidence Eliminator on his computer between midnight and 4 AM on February 28th to delete and overwrite over 12,000 files, and that an additional 3,000 files had been deleted and overwritten three days earlier. In addressing the proprietary of the plaintiff's use of Evidence Eliminator, the Magistrate Judge stated "Any reasonable person can deduce, if not from the name of the product itself, then by reading the website, that **Evidence Eliminator is a product used to circumvent discovery**. Especially telling is that the product claims to be able to defeat EnCase." (emphasis added).

The Court described the plaintiff's actions as "egregious conduct" that was wholly unreasonable, and found the plaintiff at fault for not preserving evidence that it had a duty to maintain. As a result, the Magistrate Judge recommended to the district court that the plaintiff's case be dismissed with prejudice, and that the plaintiff be ordered to pay the defendant's attorney fees and costs incurred with respect to the issue of sanctions. Although the district court did not immediately dismiss the entirety of plaintiff's case, it did dismiss plaintiff's declaratory judgment claims, and left open the possibility of monetary sanctions.[147] In short, the *Kucala* case is an excellent example of the proposition that one of the surest ways to lose a case is to attempt to destroy relevant electronic evidence.

United States v. Greathouse[148]

The *Greathouse* case presents a new twist in computer forensic caselaw: rather than the typical situation in which the defense challenges the prosecution's use of a particular piece of software, in *Greathouse* the defense argued instead that the prosecution should have used EnCase software!

The *Greathouse* case involved information relayed from the German Nation Police to law enforcement authorities in the U.S. in September 2000 regarding child pornography allegedly made available on the Internet by a computer user that went by the name "cyotee."[149] After tracking the user name through the ISP, the investigating agent determined that cyotee was located at specific residence in Oregon. According to the ISP, the subscriber associated with the name cyotee was David Ihnen, the owner of the residence in question. After further investigation over a period of months, including

surveillance over a three-day period in September 2001, the investigating agent sought and obtained a search warrant on October 16, 2001.[150] Upon execution of the warrant the following day, law enforcement officers discovered that there were five people living in the house, including Ihnen and defendant, and six computers networked together (five of which were in the den, and one of which was in defendant's bedroom).[151] Two other computers were located in the den but not connected to the network. The execution of the warrant and the interviewing of the residents took place over a three-to-four hour time period.[152] According to the Court:

> [The investigating agent] explained that he decided to seize all of the computers and shut down the network because he could not tell which of the computers had the suspected child pornography and it would take several days to review and make this determination. [The investigating agent] further testified that he could see that the defendant's computer was hooked up to the network because of the presence of a network cable and a network card installed on the computer.
>
> At the hearing, defendant proffered testimony from . . . a computer forensic consultant . . . [who] explained that there is a computer preview program known as ENCASE that has been available for many years that makes it possible to quickly scan computers for certain information. [The expert] testified that, with ENCASE, a computer could be scanned for the presence of child pornography within just a few minutes. [The expert] also testified that there is a "port scan" that can be used to learn more about the nature of computer equipment. [The investigating agent] testified that he was aware of the ENCASE program, that he has this program available, but that he did not bring the program with him for this particular search.[153]

Later forensic analysis revealed 166 suspect image files on defendant's computer, but none on the other computers in the residence.[154]

The Court found that, when the German national police contacted law enforcement authorities in the U.S., there was probable cause to believe that a computer located within the residence contained child pornography, and that "it was entirely reasonable for the agents to assume, based upon the evidence available, that they were investigating a single computer located in a single family residence."[155] However, the Court granted the defendant's motion to suppress the evidence based on staleness, noting that "the thirteen month delay in this case is simply too long."[156]

Although the basis of the Court's decision was the staleness of the information supporting the warrant, the Court went on to address what constitutes best practices in conducting searches in locations where multiple computers may well be present:

> Defendant also claims that the seizure of all eight computers was overly broad and he challenges, under *Franks,* [the investigating agent's] statement in the search warrant affidavit that the computers

would need to be searched off-site by a forensics expert. Defendant relies upon [his expert's] testimony regarding the ENCASE preview program.

Numerous cases have upheld the wholesale seizure of computers and computer disks and records for later review for particular evidence as the only reasonable means of conducting a search. *See Hay,* 231 F.3d at 637 (agents justified in taking entire computer system off-site for proper analysis); *Lacy,* 119 F.3d at 746; *United States v. Upham,* 168 F.3d 532, 534 (1st Cir.1999).

However, I recognize that this may not always be true due to technological developments. In this case, I find that [the investigating agent] acted in reasonable reliance upon well-settled and clear Ninth Circuit authority upholding the right of investigating authorities to seize computers for later forensic analysis given that he had no way of knowing, prior to entry, that he would encounter eight computers instead of one. **Had there been any evidence that a number of suspect computers would be found on site, there may well be an obligation to use a program like ENCASE to more narrowly tailor the search and seizure.**[157]

Thus, the *Greathouse* case, although decided on other grounds, puts investigators on notice that best practices require up-to-date tools, and that when sophisticated programs like EnCase software are available, investigators will be expected to use them.

State (Ohio) v. Anderson[158]

The *Anderson* case began with a law enforcement investigation into the activities of Eugene Anderson, who lived in West Virginia but worked in Ohio for Marietta College.[159] The investigation ultimately led to search warrants for Anderson's residence and work place where officers seized items that included computers and computer media.[160] As described by the Court of Appeals:

Trained forensic officers and analysts examined the computers and used a EnCase program to look at deleted files. Anderson's work computer had recently accessed a computer identified as "Caleb." Officers discovered that Caleb was a special computer server that only Anderson and a Robert Sandford could access. . . . Officers eventually located Caleb at Marietta College and disable and seized it.

. . . [T]he forensic officers continued to use EnCase and other methods to image or copy the computer hard drives, storage devices, and Caleb to recover deleted data. They found images of child pornography and evidence that Andersen used and maintained Caleb as a hidden server to store pictures, which included images of child pornography. These images depicted juveniles that were nude or engaged in sexual

activity.

The computer examiners also found close to 8,000 internet relay chat transcripts. One officer identified chats that Anderson had with young men that he had transported from West Virginia to Marietta College so that they could engage in sexual activity. . . . The chat logs further showed that Anderson used Caleb and helped Sandford set up and maintain it at Marietta College. In the chat logs, Anderson repeatedly identified himself, his position, his e-mail address and telephone numbers.[161]

Based largely on the computer forensics evidence, in the trial court the jury found Anderson guilty of 108 criminal offenses; Anderson appealed, arguing that the evidence produced at trial was insufficient to support the verdicts.[162] The Court of Appeals found that the convictions were supported by sufficient evidence, and were not against the manifest weight of evidence.[163]

NOTE: Please See Chapter 7 for a discussion of *United States v. Maali,* another case in which the forensic images comprised the only computer evidence in existence, as the original drives had been returned to the defendants.

People v. Donath

In this Illinois case, EnCase software played a critical role in the conviction of, and the sentencing of Howard Donath to 100 years imprisonment, for child pornography and predatory criminal sexual assaults.[164] In a forensic investigation using EnCase software, Senior Special Agent Jarrod L. Winkle of the United States Customs Service found 224,376 images and video of child pornography on five computers, seven hard drives, 402 floppy disks, and 376 computer compact disks and other media seized from the defendant's home. According to the appellate Court, "SSA Winkle had been involved with 150 forensic examination for child pornography but had never seen a case involving such an enormous amount of images."[165]

People v. Donath represents the longest sentence for child pornography in Illinois to date. According to Agent Winkle, "I exclusively use EnCase in all of my investigations. In this particular case, I was able to locate images files in which Donath was found to be molesting young girls. In another unrelated case, I found one of those files of a girl that Donath victimized that Donath had sent over the Internet. Donath is now serving a 100 year prison sentence, based on my investigation and on the items found during the forensic analysis."[166] The appellate court found that the trial court's imposition of a sentence of "30 years' imprisonment for each of three counts of predatory criminal sexual assault . . . and 10 years' imprisonment for child pornography . . . all sentences to run consecutively" was not an abuse of discretion, and upheld the sentence imposed.[167]

State (Minnesota) v. Levie

In another appellate case, this time in Minnesota, the Court addressed the defendant's argument that evidence of his Internet usage and the existence of an encryption program on his computer should have been excluded.[168] The Court explained that, prior to the start of the trial:

> [The defendant had] objected to the admission of a forensic report on the contents of his computer known as an EnCase Report . . . But the district determined that sections of the report were admissible, and stated, "[I]t is important for the State to be able to follow-up with that evidence to show . . . what the Defendant allegedly did, how he allegedly did it, and what [the author of the report] may have found."[169]

The appellate Court affirmed the trial court's evidentiary rulings.

State (Washington) v. Luther

In this case, computer forensic examiner Thomas Giboney used EnCase software to conduct an examination of the defendant's two computers and data on defendant's floppy disks.[170] The appellate Court explained that Giboney testified at trial "that the various images introduced into evidence had not been deleted, as [the defendant] had told detectives] but had been intentionally saved and accessed at later dates."[171] The defendant was convicted, and his conviction was upheld on appeal.

Liebert Corp. v. Mazur

In *Liebert Corp. v. Mazur*[172] a manufacturer of computer network protection equipment and its exclusive reseller brought an action seeking to enjoin the reseller's former employees from using alleged trade secrets in a new competing business. The trial court denied the plaintiffs' motion for a preliminary injunction, and the plaintiffs appealed. A computer forensics investigation using EnCase software played a prominent role. The appellate Court held that Defendant misappropriated trade secrets by improper means. "We can infer from [Defendant's] spoliation of the evidence on the laptop that he destroyed evidence of misappropriation, leading us to believe [Defendant] acquired the [trade secrets] through improper means."[173] The court also granted Plaintiffs' a preliminary injunction based on the "real threat" that Defendant copied the trade secrets onto at least one CD and therefore has the ability to continue to use the trade secrets.

The evidence regarding defendant's spoliation of computer files and CD-burning activity was presented to the court through plaintiffs' expert witness, Lee Neubecker. Using EnCase software, "Neubecker made an exact copy of [defendant John] Mazur's hard drive and then performed extensive searches of the hard drive for any information related to [plaintiffs]."[174] According to the court, the results of Neubecker's investigation "made it more likely than not that Mazur successfully burned the CD."[175] Additionally, the computer forensics investigation revealed that Mazur implemented a "mass wave of deletion," including files containing trade secrets.[176] Moreover, "Neubecker discovered

Mazur also purged his computer's application log sometime on February 9."[177]

One aspect of this case that stands out is the deference that the Appellate Court gave Neubecker's conclusions:

> Plaintiff's expert witness testified the information on the laptop indicated [defendant John] Mazur attempted and probably succeeded in copying the price books to a CD. Neubecker also described several scenarios in which information would remain in the "CD burning" folder after a successful burn. Mazur's questionable testimony was the only evidence disputing the expert's findings. Had plaintiffs been able to show Mazur successfully burned the CD, the trial court well may have reached a different outcome, which leads us to Mazur's destruction of the evidence on his laptop's hard drive. Although Mazur's deletion of all the [plaintiffs'] files was problematic, we find his decision to purge the application log particularly suspicious."

> Where a party has deliberately destroyed evidence, a trial court will indulge all reasonable presumptions against the party. Whether Mazur successfully made CD copies of the price books is a key issue in this case, and, for some unexplained reason, he deleted the application log which would have decisively answered the question. Because Mazur destroyed this crucial piece of evidence, we presume it would have showed he successfully copied the price books onto a CD.

> *   *   *   *   *

> Based on all the evidence presented at the hearing, we reject the trial court's finding on inevitable use.[178]

Porath v. State (Texas)

In this appellate case from Texas,[179] the defendant had been charged with felony child possession of child pornography. The Court described the forensics investigation: "Nickie Drehel, a computer forensics officer, retrieved evidence from the two computers, diskettes, and compact disks. On the diskettes, Drehel found a large number of photographs, some of which appeared to be child pornography."[180] At a pre-trial hearing, Drehel, who used EnCase software in the investigation, "testified to the method utilized to retrieve the images from appellant's computer."[181] The Court affirmed the trial court, and the defendant's sentence of seven years' imprisonment.

People v. Zavala

In this unpublished appellate decision from California,[182] San Jose police officer Kevin Fagalde conducted an investigation using EnCase software of defendant's personal computer hard drive. Sergeant Fagalde found thousands of images of child pornography including at least one that had been "deliberately downloaded and saved onto the computer" and he "determined that defendant was the only person using the

computer in 2001."[183] The image in question had been deleted from the desktop, but Fagalde was able to recover the image because the defendant saved a link to the image on his computer.

People v. Upton

In another unpublished appellate decision from California involving the testimony of Sergeant Fagalde, [184] the Court upheld the admission of evidence of child pornography recovered from defendant's computer through the use of EnCase software. According to the Court:

> Sergeant Kevin Fagalde of the San Jose Police Department was qualified as an expert in computer forensics and replication of data. Sergeant Fagalde testified about images he found on three computers and a digital camera seized from defendant's home.[185]

The Court affirmed the defendant's conviction.

State (North Carolina) v. Howell

In this case, the Court of Appeals of North Carolina upheld the defendant's conviction on forty-three counts of third-degree sexual exploitation of a minor, based on forty-three pictures recovered from defendant's computer by State Bureau of Investigation Agent Mike Smith, who used EnCase software in the investigation.[186]

Fridell v. State (Texas)

In this appellate case from Texas, the defendant appealed his conviction for possession of child pornography, arguing that the evidence was insufficient to support the conviction.[187]   As in the *Kucala Enterprises* case discussed above, this case illustrates how the use of wiping utilities can backfire.   The Court described the situation as follows:

> [Detective] Almond testified . . . that he used "Encase," a computer program that acquires data from a suspect's hard drive and analyzes the data without writing anything to the images obtained. Using this program on appellant's computer, the investigators recovered certain photographs, identified as State's exhibits 1-54.   Almond also explained that a "wash" program had been used on the computer's hard drive during the early morning hours of June 19, 2003, and the images of State's exhibits 1-54 had been deleted from the computer but had been recovered during the investigation.
>
> *   *   *   *   *
>
> The numerous photographs recovered, the extensive use of appellant's computer in searching for child pornography, and the appellant's attempts to erase material from the computer all show that

appellant's possession of child pornography was knowing or intentional. We find that the evidence is legally sufficient to support appellant's conviction.[188]

State (South Dakota) v. McKinney

In a case that reached the Supreme Court of South Dakota, evidence collected using EnCase software helped corroborate the testimony of the victim, a young girl.[189] The victim testified that McKinney showed her a pornographic movie. Her "testimony concerning the movie on the computer was corroborated by the testimony of Kevin Atkins, a criminalist/forensic computer analyst. Atkins testified that he found movies of child pornography on the hard drive of the computer and that they were associated with the security ID for McKinney. . . . Considering the partial corroboration and our standard of review, we conclude that there was sufficient evidence for the jury to convict McKinney."[190]

United Stated v. Bass

In this Tenth Circuit case,[191] the FBI had learned that the defendant was a member of the "Candyman" internet group. When the FBI, accompanied by a detective of the Enid, Oklahoma police department, interviewed him, the defendant admitted that he had viewed child pornography on the internet, and he stated that his computer, at some point in the past, had had a virus that saved such images.[192] The agents received consent to take the computer and conduct a forensic search. As described by the Court: "[t]he Enid Police Department conducted the computer forensic search using two programs, "ENCASE" and " SNAGIT." ENCASE recovered over 2000 images of child pornography, and SNAGIT recovered 39 images . . ." In addition, wiping utilities were found. One of the main issues on appeal was whether the defendant had knowingly possessed child pornography. The presence – and admitted use by the defendant – of wiping utilities persuaded the Court that "the jury here reasonably could have inferred that Bass knew child pornography was automatically saved to [the] computer based on evidence that Bass attempted to remove the images."[193]

United States v. Davis

This appellate case is of particular note to Guidance Software because the testifying expert, Jon Bair, has been an employee of Guidance Software since 2002. Prior to joining Guidance Software, he was a Special Agent with the U.S. Army Criminal Investigation Command. In this case heard by the U.S. Army Court of Appeals, the defendant had appealed his conviction on the basis that certain privileged testimony was admitted into evidence in error.[194] While the Court ruled that the privileged testimony was indeed admitted in error, it nonetheless upheld the conviction because the computer forensic evidence, gathered using EnCase software, was so strong as to make the error harmless:

> Special Agent (SA) Jonathan Bair, U.S. Army Criminal Investigation Command (CID), examined the hard-drives and disks that he seized from appellant's home, and discovered deleted files containing

thousands of images depicting what appeared to be children engaging in sexual activity. Special Agent Bair also discovered seven undeleted images of a similar nature on a floppy disk seized from the vicinity of appellant's home computer.

*   *   *   *   *

The government's case was very strong. The computer hard-drives and floppy disks seized with appellant's consent from his home contained thousands of images of child pornography, thus supporting the government's theory that appellant wrongfully possessed child pornography . . . The defense case was, by contrast, very weak. The crux of the defense was that these images had been unknowingly downloaded to appellant's computer and deleted upon discovery. The possibility of such innocent possession was severely undercut by the fact that images were found in a number of different drives and folders, including seven images that were found on a floppy disk that had to have been manually saved to that location.[195]

United States v. Long

In this Seventh Circuit case, the Court described the search of the defendant's digital media as follows:

[The detectives' laptop] was equipped with EnCase diagnostic software. (The "EnCase Cybercrime Arsenal" package is sold by a company called Guidance Software to the law enforcement community;[196] it is described as a powerful search and diagnostic program. See http://www.guidancesoftware.com.) Using the EnCase software, the detectives searched the CDs and found movies and photos of child pornography on them. When Long's laptop was searched at a later date, the detectives found tens of thousands of images and over a hundred movies of child pornography on it as well.[197]

The Court of Appeals affirmed the district court's denial of Long's motion (made on the basis that the search exceed his conset) to suppress the evidence.

Foust v. McFarland

In this case, EnCase software played a crucial role in the imposition of an adverse inference instruction against the *plaintiff* for spoliation.[198] The defendants' forensic expert, Mark Lanterman, used EnCase software to examine the plaintiff's computer. According to Lanterman, his analysis showed that a wiping program was run from 9:05 a.m. to 11:05 a.m. on the day that the computer was delivered to Lanterman for analysis.[199] According to the Court:

Lanterman had found that portions of unallocated space on the laptop

computer had been "scrubbed" using a "WipeInfo" program. The WipeInfo program is a computer program that permanently deletes data from the hard drive of a computer. On the same day, the district court made a determination that [plaintiffs] were responsible for spoliation of computer data. As a result, the court granted [defendants'] request for sanctions and concluded that an adverse inference instruction would be read to the jury.[200]

The Appellate Court found the adverse inference instruction proper; defendants' appeal arguing that the failure to impose harsher sanctions constituted reversible error was denied.

NOTE: Please See Chapter 2 for a Discussion of *Logan v. State*, a Court of Appeals of Indiana Decision involving EnCase Software, and Chapter 7 for a Discussion of both *United States v. Riccardi*, a Tenth Circuit Decision that involved EnCase Software, and *United States v. Calimlim*, a federal case from Wisconsin involving EnCase software.

Other Jurisdictions

Regina v. Cox

In addition to the wealth of case law in the United States, the use of EnCase software has been widely accepted by courts in other common-law jurisdictions. For example, in 2003 a Canadian court addressed EnCase software in *Regina v. Cox*.[201] In that child pornography case, the Royal Canadian Mounted Police had used EnCase software to image and analyze three hard drives. On application by the defendant to compel the prosecution to turn over a copy of the EnCase software, the Court discussed how EnCase software is used, and ruled that the images and the forensic report produced by EnCase software were relevant evidence, but that the software itself was a tool used by experts, and not evidence.

Regina v. D.E.W.B.

In another Canadian case in Alberta Provincial Court called *R. v. D.E.W.B.*[202], police computer forensics investigators used EnCase software to preview and recover crucial evidence. The Court explicitly accepted the reliability of EnCase software and its use in uncovering admissible evidence for a criminal trial.

The defendant in the case shared a home computer with his wife. His wife had inadvertently discovered child pornography on the computer, which she mentioned to certain Child Welfare authorities. The Child Welfare officials notified the Calgary Police, who obtained a search warrant. Detectives from the Technological Crimes Unit of the Calgary Police Service used EnCase software to examine the subject computer. There was conflicting testimony about whether the defendant actually informed the police investigators of the location of the child pornography, but in any event the evidence was recovered and the defendant was charged with possession of child

pornography.

The Court noted that "the 'Encase' program allows the police to view what is on a computer without altering any of the date on the computer." The Court further elaborated regarding EnCase software: "[o]ne of the things that the police were able to determine through the 'EnCase' programme were the dates that the child pornography was placed in the computer's files . . . Those images were found in files created between August, 2001 and January, 2002."

Ultimately, the defendant was convicted of possession of child pornography. The *R. v. D.E.W.B.* case is important because it re-emphasizes that EnCase software is a reliable, widely available, and court-approved computer forensics tool.

Regina v. J.M.H.[203]

In this case, the Ontario Superior Court of Justice addressed the admissibility of a computer forensics report that had been prepared by a detective in the Ottawa Police Service using EnCase software. The defendant was alleged to have detained a child inside of his residence and to have shown the child adult pornography on his computer.[204] Pursuant to a warrant, two computers were seized at the defendant's home, and a forensic analysis was undertaken to determine if the computers had been used during the time the offense was allegedly committed.[205]

The Court reviewed the qualifications of the computer forensics investigator, which included training described by the Court as "Intermediate Encase Computer Forensic course."[206] The Crown asserted, and the Court accepted, that scrutiny of expert evidence is based on four factors: (1) relevance, (2) necessity, (3) the absence of an exclusionary rule; and (4) a properly qualified expert.[207] The Court held that the investigator was qualified to present digital evidence located on the defendant's computer.[208] The investigator's testimony established that one of the defendant's computers was in use during the time in question, and that the computer was used exclusively to surf pornographic sites.[209] The Court held that "the evidence is material, relevant, compelling and reliable."[210]

Sony Music Entertainment (Australia) Ltd. v. Univ. of Tasmania, et al.

The Federal Court of Australia addressed EnCase software in *Sony Music Entertainment (Australia) Ltd. v. Univ. of Tasmania, et al.*,[211] The *Sony* case involved the use of file-sharing networks by university students for alleged copyright piracy, and a discovery dispute between the parties regarding the scope of information that should be supplied by three universities. The Federal Court of Australia allowed the computer forensics investigator hired by Sony to employ EnCase software to search the available digital evidence. The court noted that if the computer forensics investigator agreed to certain confidentiality provisions, "then access could be given to all of the preserved records to search using the EnCase program." The Court specifically found the use of EnCase software preferable to the discovery methods proposed by the universities, stating that "if the narrow search tools and methods proposed by the Universities . . . are used, then it is likely that there will be insufficient discovery."

Grant v. Marshall[212]

The *Grant* case involved a discovery matter in which the applicant, Grant, sought information concerning the identity of the author of emails that made allegations of corruption by Grant.[213] The Federal Court of Australia noted "that it may be possible, by examination of the hard drive of the computer in question, to obtain information that could assist in identifying the author of the emails.[214] The Court specifically addressed the forensic imaging process, as follows:

> Proper acquisition of computer evidence requires the use of non-task. Such software recovers, searches, authenticates and documents relevant electronic evidence without compromising the integrity of the original evidence. PricewaterhouseCoopers currently use "EnCase" software, **which is the industry standard**.
>
> *   *   *   *   *
>
> **The EnCase forensic image has an in-built audit trail with a sophisticated integrity validation process**.[215]

The Court ordered the Council of the Municipality of Mosman to "refrain from deleting, moving, erasing, altering, concealing or tampering with any document, whether electronic or otherwise" that is relevant to the issue in question.[216] In addition, the Court ordered the Council of the Municipality of Mosman to provide Peter Chapman, a computer forensics investigator with PricewaterhouseCoopers, "with access to the hard drive . . . of the computer which is associated with IP address 203.111.117.212 for the purpose of enabling" a forensic investigation.[217]

Ler Wee Teang Anthony v. Public Prosecutor

In 2002 an appellate court in Singapore, in upholding a murder conviction, relied on evidence recovered through the use of EnCase software.[218] The Techno Forensic Branch of the Technology Crime Division of the Criminal Investigation Department of the Singapore Police had used EnCase software to retrieve a deleted file from one of the defendant's computers. The recovered file was quoted in detail by the court as evidence of the defendant's guilt.

State (N.C.T. of Delhi) v. Sandhu[219]

This extremely high profile case centered on the December 13, 2001 terrorist attack on the Parliament of India in which 8 policemen, 1 civilian, and 5 terrorists were killed.[220] Mohammed Afzal's death sentence was upheld in the Supreme Court of India based in part on evidence, acquired using EnCase software, obtained from a laptop computer that had been seized from Afzal, who was charged with coordinating the attack. Using EnCase software, police recovered evidence showing that the laptop had been used to make forged identity cards found on the bodies of the terrorists who were killed in the attack.[221]

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA   Criminal No. 01-10195-PBS

KEVIN HABERSHAW

REPORT OF GOVERNMENT EXPERT WITNESS
DETECTIVE DAVID C. PAPARGIRIS

I, David C. Papargiris do hereby state:

I am a detective with the Norwood Police Department in Norwood Massachusetts. I have been employed with the Norwood Police for 17 Years and have been assigned to the Bureau of Criminal Investigations for 4 years. I conduct all investigations into computer crime, Internet investigations as well as being a computer forensics examiner.

I have been working with personal computers for (8) years. I am a member of the United States Secret Service Electronic Crimes Task Force Boston Region, the High Technology Crime Investigation Association (HTCIA) and the Regional Electronic and Computer Crime Task Force located in Raynham, Massachusetts. I have received formal training on the processing of computer evidence and the science of computer forensics from HTCIA, United States Attorney Generals Office and the Internet Crimes Inc. I have also successfully completed the National White Collar Crime Centers Basic Data Recovery four and a half day school in Portland, Maine. I have completed the four day training course on Guidance Software Corporation's computer forensics software program," Encase". I have attended the Boston University's weeklong training on Windows NT titled Network Essentials. I have safely recovered evidentiary data from personal computers, during investigations involving fraud, identity fraud, hacking cases and crimes against children. I have testified in district court, grand juries and federal court on computer issues, along with the proper means of securing and processing computer evidence.

In preparing this brief, I conferred with court certified computer forensic expert, William C. Siebert, the Director of Technical Services for Guidance Software, maker of the computer forensic software, EnCase. A copy of his CV is attached at the end of this report.

I.   Newsgroups:

USENET is a world-wide distributed discussion system. It consists of a set of "newsgroups" with names that are classified hierarchically by subject. "Articles" or "messages" are "posted" to these newsgroups by people on computers with the appropriate software -- these articles are then broadcast to other interconnected

computer systems via a wide variety of networks. Usenet is available on a wide variety of computer systems and networks, but the bulk of modern Usenet traffic is transported over either the Internet or UUCP.

USENET newsgroups consist of some 15,000+ topical entities which constitute an immense worldwide forum for discussion and discourse. These newsgroups actually pre-date the existence of the World Wide Web and are now an integral part of the "Internet experience". These forums for discussion range in subject from Ancient Art to Zen Buddhism, and within the "threaded" structure of each group emerges the true spirit of debate and a poignant example of freedom of speech. Though a few newsgroups are moderated (having a designated member of the group with oversight powers to keep the discussion on track,) most newsgroups are free forums, and may seem at times like free-for-alls, but taken as a whole, they provide a noble service in giving each and every user an equal voice.

Newsgroups can be compared to a bulletin board that you might see at a grocery store or on the wall at any college campus, except that imagine if after pinning a postcard to the bulletin board a duplicate postcard appeared on every bulletin board in every grocery store or college campus in the world within one hour.

It is true that Usenet originated in the United States, and the fastest growth in Usenet sites has been there. Nowadays, however, Usenet extends worldwide. The heaviest concentrations of Usenet sites outside the U.S. seem to be in Canada, Europe, Australia and Japan.

No person or group has authority over Usenet as a whole. No one controls who gets a news feed, which articles are propagated where, who can post articles, or anything else. There is no "Usenet Incorporated," nor is there a "Usenet User's Group." You're on your own.

Despite its most noble intent, the darkest side of the Internet will be found within a number of newsgroups. These are the pedophile newsgroups. Perhaps at one time, these forums functioned as discussion groups for people of similar, though no less frightening interests, that being the exploitation of children for the sexual gratification of the adults who control them. These newsgroups, as most pornographic newsgroups, are not moderated.

Granted, there are various activities organized by means of Usenet newsgroups. The newsgroup creation process is one such activity. But it would be a mistake to equate Usenet with the organized activities it makes possible. If they were to stop tomorrow, Usenet would go on without them.

Newsgroups are an area of the Internet that are accessed through a mail program such as Outlook Express. You have to set up your news account using information supplied to you by an Internet Service Provider (ISP); i.e. Mediaone.net, AT&T Roadrunner, Earthlink.net, etc. Your newsgroup section is different from your mail program that is also managed by your ISP. Your ISP has numerous servers one is a mail server and one is a news server, many customers never set up there news server

and never go onto newsgroups at all.

This technology allows for the instantaneous electronic transmission of pictures over the Internet. These pictures are converted or encoded to a binary format and sent in a similar manner as a text message. The process is as simple as sending an email. Once uploaded, the encoded binary message appears within the newsgroup where it can be downloaded by any user and decoded back into its original form, and when this decoded format is accessed through an image viewer, it becomes a photograph. I have witnessed for myself some of the images that have emerged from the pedophilia newsgroups. The computer picture format most often found on the newsgroup is jpegs.

II.   What is a JPEG?

JPEG (pronounced "jay-peg") is a standardized image compression mechanism. JPEG stands for Joint Photographic Experts Group, the original name of the committee that wrote the standard.

JPEG is designed for compressing full-color or gray-scale images of natural, real-world scenes. It works well on photographs, naturalistic artwork, and similar material; not so well on lettering, simple cartoons, or line drawings. JPEG handles only still images, but there is a related standard called MPEG for motion pictures.

JPEG is "lossy," meaning that the decompressed image isn't quite the same as the one you started with. (There are lossless image compression algorithms, but JPEG achieves much greater compression than is possible with lossless methods.) JPEG is designed to exploit known limitations of the human eye, notably the fact that small color changes are perceived less accurately than small changes in brightness. Thus, JPEG is intended for compressing images that will be looked at by humans. If you plan to machine-analyze your images, the small errors introduced by JPEG may be a problem for you, even if they are invisible to the eye.

III.   Continued Review of Kevin Habershaw's Computer

On February 15, 2002, as part of my research, I signed on to a news server on a computer which never had one assigned to it before. After setting up the account the first thing you are told is that the news server is going to get a list of newsgroups that are available on your ISP's news server. I received a list of 67,019 newsgroups. There are newsgroups available for just about any subject, as described above. After the list comes down into the window, you can scroll through the list or type in a keyword of what type of newsgroup you are looking for.

There are two ways to go to a newsgroup one way is to highlight the newsgroup and select GOTO and the other way is to select SUBSCRIBE. If you select GOTO, you are brought to that newsgroup and as much as three hundred messages could appear in the news window. If you double click on a message it could bring you to text or to a hyperlink to go to a web page or show you a graphic (photo) file. Once you exit the newsgroup it will ask you if you would like to SUBSCRIBE to the newsgroup.

If you select GOTO, or SUBSCRIBE to, in the newsgroup box a reference to that newsgroup is placed in your outlook express folder.
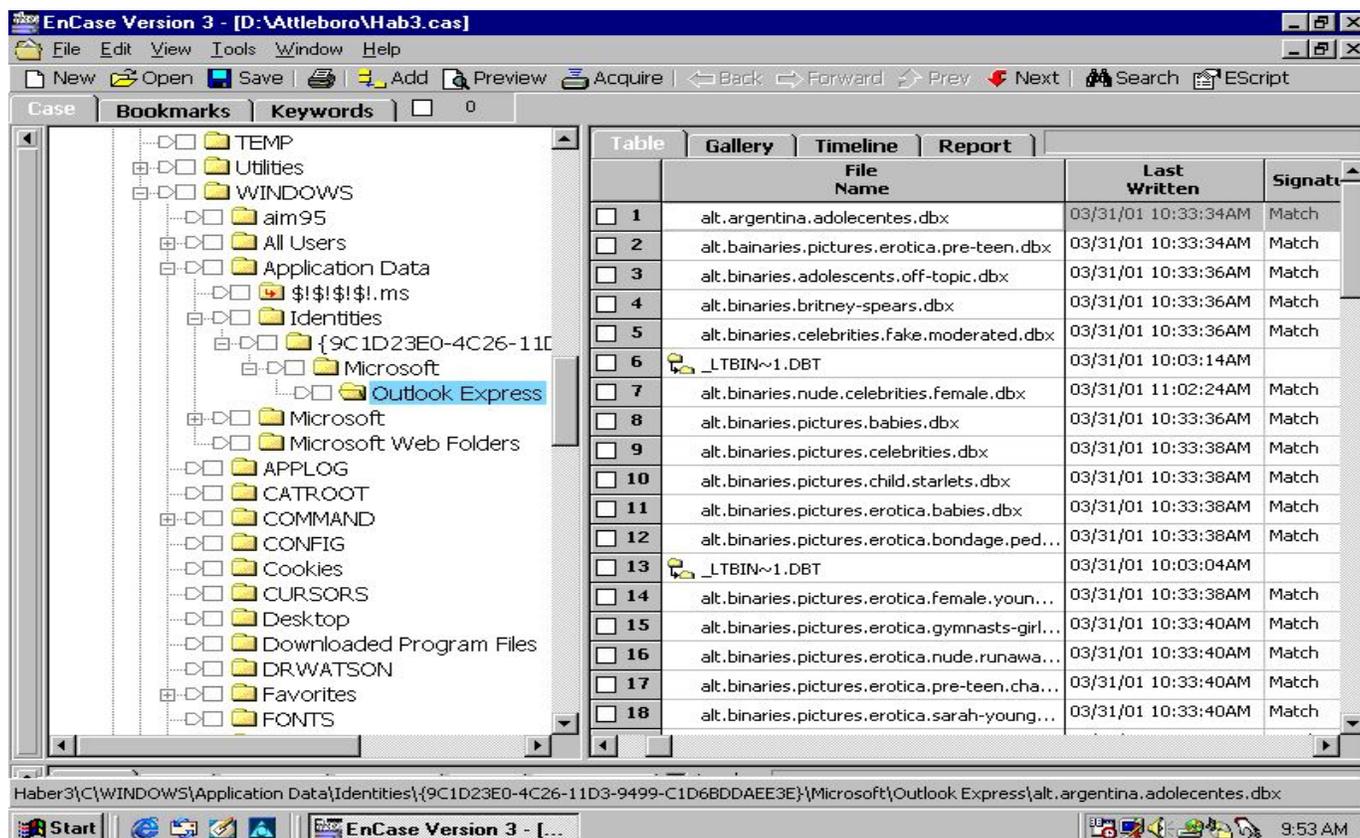
As you can see from this graphic, the left side of the windows indicates that I am in the Outlook Express folder. The right side of the window shows the items in that folder. The right side lists the newsgroups that were visited.

When an individual configures up their newsreader and either selects GOTO or SUBSCRIBE to a newsgroup, that information is stored on their hard drive. The computer forensic software, Encase, allows an examiner to review the contents of a hard drive under investigation.

IV: Newsgroups on Kevin Habershaw's Computer

A review of the contents of Kevin Habershaw's Outlook Express folder shows those newgroups of interest to him. The newsgroups included:

Alt.argentina.adolescents   Alt.bainaries.pictures.erotica.pre-teen
Alt.binaries.adolescents.off-topic   Alt.binaries.britney-spears
Alt.binaries.celebrities.fake.moderated   Alt.binaries.nude.celebrities.female
Alt.binaries.pictures.babies   Alt.binaries.pictures.celebrities
Alt.binaries.pictures.child.starlets   Alt.binaries.pictures.erotica.babies
Alt.binaries.pictures.erotica.bondage.ped   Alt.binaries.pictures.erotica.female.young
Alt.binaries.pictures.erotica.gymnasts-girl Alt.binaries.pictures.erotica.nude.runaway

Alt.binaries.pictures.erotica.pre-teen.chatter Alt.binaries.pictures.erotica.sara-young
Alt.binaries.pictures.girls   Alt.binaries.pictures.humor.babies
Alt.binaries.pictures.kids   Alt.binaries.pictures.olsen.twins
Alt.binaries.pictures.spice-girls   Alt.binaries.stories.sex
Alt.disgusting.stories.my-imagination   Alt.fan.britney-spears
Alt.fan.emma-bunton   Alt.fan.Melissa.j-hart
Alt.fan.olsen.twins   Alt.hipclone.kids.sexual-abstinence
Alt.idiot.pedophile.reb-ruster   Alt.idiot.pedophile.snoopy
Alt.no.advertising.files.images.sex.preteens Alt.no.advertising.files.images.nude.preteens
Alt.Pedophiles   Alt.sex.children
Alt.sex.girls   Alt.sex.incest
Alt.sex.pedo.moderated   Alt.sex.pedophilia
Alt.sex.pedophilia.girls   Alt.sex.pedophilia.glen.webb
Alt.sex.pedophilia.Linda-and-kuibob   Alt.sex.pedophilia.pictures
Alt.sex.preteens   Alt.sex.stories.babies
Alt.sex.stories   Alt.sex.stories.incest
Alt.sex.stories.moderated   Alt.sex.stories.tg
Alt.sex.young   Alt.stories.erotic
Alt.stories.incest   Alt.Transformation.stories
Alt.transgendered   Alt.transgendered.Jeffrey-boyd
Alt.binaries.nude.celebrities.female   Pedo.binaries.pictures.erotica.children

Once you click on a newsgroup name, you can see the database of messages for the newsgroup, alt.sex.pre-teens for March 31st at 10:33:58 AM. These titles could lead you to text or a graphic file or a hyperlink (text that once clicked brings you to a web page) that had shown up in the newsgroup box. These references are left on a person's hard drive only if they have selected GOTO or SUBSCRIBE in their newsreader. Habershaw's Outlook Express folder showed that there were 61 references to newsgroups that he had visited. Alt.Sex.Pre-Teens, showed references to the terms like lolita, alt.sex and preteen, as did other newsgroups that had been accessed at 10:34 AM on the 31st of March. It was said that the term "preteen" did not come up during the keyword search under EnCase. The reason for this was because of the spelling in the newsgroup showed it as P=R=E=T=E=E=N.
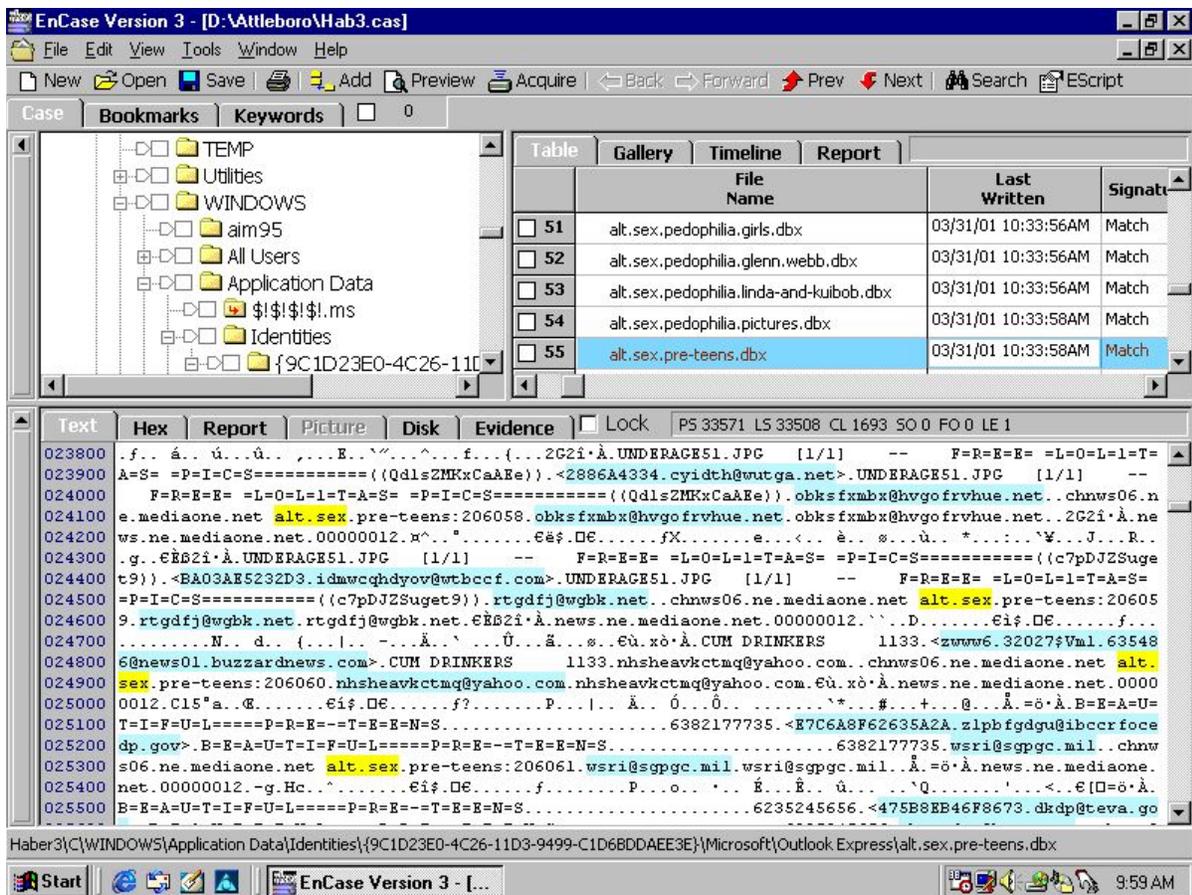
Looking with in the lower box in EnCase it shows references to the newsgroup alt.sex.pre-teens. On the first line you can see a reference to underage51.jpg, which is an attached computer picture file available for downloading.

I also checked the timeline to see if in fact that the newsgroups were being updated every 30 minutes.

After checking the timeline, I could see that at 0930 hours on the 31st of March, two newsgroups were accessed. At 1002 Hours, four newsgroups were accessed, and starting at 1033 hours forty-five different newsgroups were accessed. At 1101 hours 1 newsgroup was accessed. If the newsgroup were being checked automatically every thirty minutes, there would be the same amount of newsgroups accessed every thirty minutes, and this would show up in the timeline within Encase. Because different numbers of the newsgroups appear at different time intervals on the timeline, I do not believe that Habershaw's computer was automatically updating newsgroups every thirty minutes.

-- END OF REPORT --

7

Search and Seizure Issues and EnCase Software

§ 7.0 Overview

Issues related to the search and seizure of computer data is an area that has seen some excellent research and writing by prosecutors and government attorneys. The Federal Guidelines on Searching and Seizing Computers, found at www.cybercrime.gov, is a must read for every computer investigator. This Journal focuses on the more narrow search and seizure processes that are potentially impacted by the use of EnCase software. The plain view doctrine, for example, is an area that becomes more complex as EnCase software allows forensic examiners to view, sort and manage many more files than previously possible with command line utilities.

The remote preview function of EnCase software also plays an important role in search and seizure issues. Many users report successful employment of the non-invasive EnCase remote preview feature in consent search situations. Obviously, one is more likely to allow the search of one's computer if the preliminary exam can be done quickly and without "impounding" a favorite laptop. The feature is also very useful in increasingly common scenarios where the examiner is faced with numerous items of media and/or severe time constraints and can triage the media on the scene, or where a "blind" examination of media potentially containing other privileged documentation is required.

This chapter will focus on the areas of search and seizure law where EnCase software impacts many of the procedures and considerations addressed by current case law.

§ 7.1 Computer Files and the Plain View Doctrine

The Plain View Doctrine allows for seizure of evidence without a warrant where (1) the officer is in a lawful position to observe the evidence; (2) the object's incriminating nature is immediately apparent; and (3) the officer has a lawful right to access the object itself.[222] In the context of computer investigations, a "plain view" seizure of a computer file would likely only arise where officers lawfully observed a monitor attached to an operating computer displaying material evidencing criminal activity. However, absent exigent circumstances, clear consent to search the computers themselves, routine border searches[223] or more rare instances of a plain view display of criminal activity on a running monitor, courts have routinely excluded evidence obtained from warrantless searches of computer files.[224] The gray areas typically arise in more common situations where an officer lawfully searching computer files pursuant to a

warrant comes upon evidence of criminal activity unrelated to that specified in the warrant. Recent judicial trends indicate that courts are affording special protection to electronic data stored on computers by narrowly construing the articulated terms of the warrant. In order to understand the Plain View Doctrine in the context of computer files, the related issue of warrant particularity requirements should be understood.

The Fourth Amendment to the United States Constitution requires that all warrants particularly describe the place to be searched and the items to be seized. In order to pass constitutional muster, a warrant (1) must provide sufficiently specific information to guide the officer's judgment in selecting what to seize, and (2) the warrant's breadth must be sufficiently narrow to avoid seizure of purely unrelated items.[225] While courts readily tailor warrants authorizing searches of more traditional items of physical evidence, "computers create a 'virtual' world where data exists 'in effect or essence though not in actual fact or form.'"[226] Ultimately, whether or not computer files containing information not included within the scope of the warrant can be searched often depends upon the specific language of the warrant. Thus, magistrates should ideally strike a careful balance between a warrant that is too overbroad and one that is so narrow as to prevent the search of all items relevant to the investigation. However, due to a computer's ability to store vast amounts of information, the potential difficulty in accessing particular files in a computer, and the fact that the titles of many files do not satisfactorily indicate the substance of that file, it is often difficult to meet the constraints of the Fourth Amendment.[227]

Courts have generally upheld the search of all files contained within a computer where the warrant authorizes a broad search of computer equipment. In *United States v. Simpson*[228] the court found that where a warrant authorized the broad search of a suspect's computer, an additional warrant was not required for the individual computer files. The court noted that, at the time, there was no known authority providing that computer disks and files were closed containers separate from the computers themselves.[229] In *United States v. Upham,*[230] the court held that the recovery of deleted files pursuant to a search warrant authorizing the seizure of "any and all computer software and hardware, … computer disks, disk drives … visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]" was valid and did not exceed the scope of the warrant.[231] The court noted that from a legal standpoint, the recovery of deleted files is "no different than decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note."[232]

In cases involving the investigation of child pornography, many courts have ruled that a warrant allowing seizure of a computer and all its associated printing, storage, and viewing devices is constitutional as the computer, applications, and various storage devices not only may contain evidence of distribution of child pornography, but are also the instrumentalities of the crime.[233] In *United States v. Lacy,*[234] the court allowed seizure of the suspect's entire computer system, hardware and software, because "the affidavit in this case established probable cause to believe Lacy's entire computer system was likely to evidence criminal activity."

However, other courts have invalidated warrants found to lack sufficient particularity. In *United States v. Kow,*[235] the court held a warrant to be overbroad as it

allowed seizure of computers, computer files and storage devices without any real limitations in scope such as the criminal conduct being investigated or a time frame within which the alleged criminal activity took place. As such, the court found that the warrant impermissibly permitted the seizure of essentially every computer-generated document relating to the defendant's business.[236] In response to the concerns raised in *United States v. Kow*, most magistrates are now drafting warrants authorizing the search and seizure of computer media with more narrow definitions of the items to be seized. In turn, the latitude of a search is sharply curtailed where the magistrate provides very specific delineations as what is to be seized pursuant to the warrant and what is to be ignored.[237]

§ 7.2 United States v. Carey

The case of *United States v. Carey*[238] is a clear example of where narrowly drafted search warrants prevent any expansion of the search of computer media beyond the scope of that prescribed by the warrant. In *Carey*, officers investigating evidence of drug transactions obtained a warrant to search the defendant's computers. The subject warrant limited the search to the specific purpose of only searching defendant's computer files for "names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[239] The scope of the search was thus confined to evidence pertaining to drug trafficking. After conducting a series of unsuccessful text string searches for files related to illegal drug activity, the investigating officer noticed other directories with files that he "was not familiar with," which turned out to be .jpg files.[240] Apparently unable to view the .jpg files with the forensic software utility he was using, the officer exported the files to floppy disks and then viewed them on another computer.[241] Upon opening the first file, the officer determined that it contained an image of child pornography. He then, by his own admission, abandoned the original search for evidence of narcotic transactions and instead searched for and seized evidence related to child pornography.[242] The Court ruled the officer's actions exceeded the articulated scope of the warrant and thus violated the Fourth Amendment.

The government unsuccessfully argued that the Plain View Doctrine authorized the search of the child pornography files. The government asserted that "a computer search such as the one undertaken in this case is tantamount to looking for documents in a file cabinet, pursuant to a valid search warrant, and instead finding child pornography." The government further contended that "[j]ust as if officers had seized pornographic photographs from a file cabinet, seizure of the pornographic computer images was permissible because officers had a valid warrant, the pornographic images were in plain view, and the incriminating nature was readily apparent as the photographs depicted children under the age of twelve engaged in sexual acts."[243] The warrant authorized the officer to search any file, according to the government, because "any file might well have contained information relating to drug crimes and the fact that some files might have appeared to have been graphics files would not necessarily preclude them from containing such information."[244] At oral argument, the government expounded on the filing cabinet theory, arguing that the situation "is similar to an officer having a warrant to search a file cabinet containing many drawers. Although each drawer is labeled, he had to open a drawer to find out whether the label was misleading

and the drawer contained the objects of the search."[245]

The Court rejected the government's argument that the files were in plain view, finding that "it (was) the contents of the files and not the files themselves which were seized." The Court also noted that the pornographic images "were in closed files and thus not in plain view."[246] By this language, the *Carey* Court seems to imply that file folders evidencing criminal conduct outside the scope of the search warrant may be seized, but the actual file contents may not be searched absent a supplemental warrant. The Court also rejected the file cabinet analogy noting that "[t]his is not a case in which ambiguously labeled files were contained in the hard drive directory. It is not a case in which the officers had to open each file drawer before discovering its contents. Even if we employ the file cabinet theory, the testimony of (the officer) makes the analogy inapposite because he stated he knew, or at least had probable cause to know, each drawer was properly labeled and its contents were clearly described in the label."[247] The Court further noted that "because this case involves images stored in a computer, the file cabinet analogy may be inadequate. 'Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information.' Relying on analogies to closed containers or file cabinets may lead courts to oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage."[248]

The *Carey* Court, seizing the opportunity for pontification in an unsettled area of the law, then proposed in *dicta* that courts addressing this issue in future "acknowledge computers often contain 'intermingled documents.' Under this approach, law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant which type of files are sought."[249] In support of its proposal, the Court invokes a Harvard Law Review notation, which theorizes that where a warrant "seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain the financial records sought. Where relying on the type of computer files fails to narrow the scope of the search sufficiently, the magistrate should review the search methods proposed by the investigating officers."[250] The Court further opines that with "the computers and data in their custody, law enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory. In this case, (the officers) did list files on the directory and also performed a key word search, but they did not use the information gained to limit their search to items specified in the warrant, nor did they obtain a new warrant authorizing a search for child pornography."

However, notwithstanding its extensive comments on the topic and its rejection of the filing cabinet analogy advocated by the government, the Court ultimately states that

it did not reach its decision on the applicability of the Plain View Doctrine.[251] Instead, the Court expressly bases its ruling upon the testimony of the investigating officer who conceded that he intentionally abandoned his search for evidence of drug trafficking and began opening the .jpg files with the intent to search for files containing erotic depictions of minors. Under such circumstances, the Court notes, "we cannot say the contents of each of those files were inadvertently discovered."[252] The Court indicates throughout the opinion that had the investigating officer obtained a supplemental warrant after viewing the first file containing child pornography, such a supplemental warrant and authorized search would have been proper. The Court also implies that had the officer come across the various items of child pornography inadvertently while continuing his search for drug-related information, the Plain View Doctrine would have been applicable. Unlike the majority opinion, concurring opinion is less than subtle on this point, noting that "if the record showed that (the officer) had merely continued his search for drug-related evidence and, in doing so, continued to come across evidence of child pornography, I think a different result would have been required."[253]

§ 7.3 Post-*Carey* Case Law

Several courts have issued published decisions involving the search and seizure of computer media that feature a discussion of *Carey*, while others courts have addressed the Plain View Doctrine in the context of forensic searches of computer files, but without a discussion of *Carey*. These decisions provide some indications as to the impact of the *Carey* decision.

In *United States v. Gray,*[254] FBI agents executed a search warrant at the home of a suspected computer hacker and seized four computers belonging to defendant, which were taken back to the FBI's offices. The warrant authorized the FBI to search the defendant's computer files for evidence of computer hacking activity, including stolen computer files and utilities enabling unauthorized access to protected computer systems. After imaging the four computer drives onto magneto-optical disks, the FBI Computer Analysis Response Team (CART) agent created a series of CD-ROMs from the disk images to allow the case agents to view the information in readable form. While the information was being copied onto the CD-ROMs, the agent, pursuant to routine CART practice, opened and looked briefly at each of the files contained in the directories and subdirectories being copied to look for the materials listed in the search warrant in the hope that they might facilitate the case agent's search.[255] To accomplish this, the CART agent utilized the CompuPic program to display thumbnail views of the text and graphical image files contained in each directory. In the course of this action, the CART agent came across and opened a subdirectory entitled "Teen" that contained numerous files with ".jpg" extensions.[256] While the agent noted that the files in that subdirectory appeared to contain images of child pornography, he continued his original search pursuant to the warrant.

Thereafter, the agent saw another subdirectory entitled "Tiny Teen," causing the agent to wonder if child pornography resided in that subdirectory.[257] The CART agent testified that he then opened the "Tiny Teen" subdirectory not because he believed it might contain child pornography, which it did, but rather "because it was the next subdirectory listed and he was opening all of the subdirectories as part of his routine

search for the items listed in the warrant."[258] Upon determining that the "Tiny Teen" subdirectory did apparently contain child pornography, the CART agent ceased his search and obtained a second warrant authorizing a search of defendant's computer files for child pornography. The search pursuant to the supplemental warrant revealed additional images of child pornography, which, along with the images that triggered the application for the warrant, the defendant moved to suppress.[259]

In upholding the original search and supplemental warrant as lawful, the court noted that:

> "Although care must be taken to ensure a computer search is not overbroad, searches of computer records 'are no less constitutional than searches of physical records, where innocuous documents may be scanned to ascertain their relevancy.' It follows, then, that (the agent's) search of the 'Teen' and 'Tiny Teen' subdirectories was not beyond the scope of the search warrant. In searching for the items listed in the warrant, (the CART agent) was entitled to examine all of defendant's files to determine whether they contained items that fell within the scope of the warrant. In the course of doing so, he inadvertently discovered evidence of child pornography, which was clearly incriminating on its face."[260]

The court found *United States v. Carey* to be distinguishable, finding that the CART agent never abandoned his original search: "he was not commencing a new search when he opened the 'Teen' and 'Tiny Teen' subdirectories, rather, he was continuing his systematic search . . . without regard to file names or suffixes because he was aware that the materials that were the subject of the warrant could be hidden anywhere in defendant's files."[261] The *Gray* court was also not persuaded by the defense's argument that the CART agent knew the "Teen" and "Tiny Teen" subdirectories did not contain documents or other files related to hacker activity when he searched them because many of the files had ".jpg" extensions, indicating a picture file, and none of the materials covered by the warrant were believed to be pictures. In a strong affirmation of standard practice by many examiners, the court noted that the CART agent "would have been remiss not to search files with a '.jpg' suffix simply because such files are generally pictures files," based upon his experience that computer hackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories.[262]

In *United States v. Scott-Emuakpor,* [263] FBI and Secret Service agents investigating a bank fraud scheme obtained a warrant authorizing the seizure of "[a]ll documents purporting to offer an investment opportunity regarding Nigerian accounts or contract over-invoicing[,]" and "[a]ll records, including computer files, that disclose the names or addresses of persons solicited for any such investment." In the course of this search of the seized computers, the investigating agents came upon and seized a letter from a third party to the United States Embassy in London applying for a visa on behalf of defendant. The defendant, relying upon *United States v. Carey*, contended that given the warrant's very specific delineations, the letter to the Embassy should have been excluded, as it was not a document that disclosed "the names or addresses of persons

solicited for any such investment." The court upheld the search, finding that *Carey* was inapplicable as there was "no evidence that the agents examining the computer equipment knew that any particular file contained evidence of criminal activity other than the Nigerian fraud scheme." The court also determined that the seizure of the Embassy letter was appropriate as related evidence within the scope of the warrant because it tied Defendant to Intercorp and to England, a fact which the Government contended was central to the fraudulent scheme it intended to prove at trial.

In *United States v. Scott,*[264] Secret Service agents conducting a counterfeit securities investigation obtained a warrant authorizing the search of a the suspect's residence and seizure of items that constituted "evidence of criminal offenses, the fruits of crime, and the instrumentalities of criminal offenses."[265] Although the initial warrant did not specifically provide for the seizure of the computer files and equipment, the court held the seizure of two computers was proper as the officers had probable cause to believe the computers were being used as an instrumentality of criminal offenses, and thus the officers acted within the scope of the warrant.[266] In the course of examining the seized computers for information relating to the bank fraud investigation, the investigating agent conducted what the court describes as "a 'text string' mirror-image search of the computers' hard drives."[267] The investigating agent utilized EnCase for this process and his overall computer investigation.[268] The text string search resulted in numerous hits that, in conjunction with other independent information, led the agents to believe that the defendants may have been involved in additional crimes involving bank and tax fraud. On that basis, the agents sought and obtained a supplemental warrant authorizing the search of the computers for evidence of the additional crimes, which the court ultimately found to be supported by adequate probable cause.[269]

In *Wisconsin v. Schroeder,*[270] detectives conducting an investigation of online harassment and disorderly conduct were issued a search warrant to enter the defendant Schroeder's residence and seize his computer and related items in order to search for evidence of his having posted the Internet messages. Upon seizing the computer system, Schroeder indicated to the officers that there was child pornography on his computer. The computer was then sent to the state crime lab for analysis, where the officer who served the warrant informed the computer lab examiners that child pornography might be residing on the computer. In their search for evidence of online harassment, the lab examiners did find some pornographic pictures of children, at which point they stopped their search and sought a second search warrant to provide authority to search for child pornography on Schroeder's computer. Upon being issued the second warrant, the state crime lab examiners resumed the search and found more illicit pictures of minors, as well as evidence of the online harassment.

Schroeder sought to suppress the evidence of child pornography, asserting that the crime lab's initial discovery of the images did not legitimately fall under the plain view doctrine exception and thus the supplemental warrant represented "fruit of the poisonous tree." Schroeder contended that when the crime lab analyst first began to search the computer for evidence of harassment, he was also actively looking for child pornography even though there was no warrant for him to do so. Schroeder noted that after being told that there might be child pornography on the computer, the crime lab analyst opened files that had names suggestive of child pornography and thus was

"verifying" that the files did contain child pornography. According to Schroeder, "This additional step of opening and reviewing the folder to verify it contained child porn makes the search illegal."

The lab analyst testified, however, that when he searches a computer he systematically examines user-created files regardless of their names, in the event that a file has been renamed in order to conceal its contents. While systematically opening all user-created files, the lab analyst opened one containing images that he considered child pornography. At that point, he stopped his search and proceeded to obtain a supplemental warrant. He did not resume his search and find the rest of the contraband until after the issuance of the second search warrant. Thus, his initial discovery of child pornography occurred when he opened a file and saw a nude picture of a child appear on his monitor. Finding that the plain view doctrine did apply, the court noted "this was no different than an investigator opening a drawer while searching for drugs and seeing a nude picture of a child on top of a pile of socks."

The *Schroeder* court placed heavy reliance on *United States v. Gray*, and, like the *Gray* court, distinguished *United States v. Carey*. The Schroeder court noted, "[i]n *Gray*, as in the present case, the investigator stopped searching and obtained a second warrant. There, as here, the continued search for child pornography was authorized by the second warrant."

The Ninth Circuit has also neglected to adopt the *Carey* reasoning. In *United States v. Rossby*[271] the defendant had given his consent to a "complete search" of his office. [272] The police then included within the "complete search" a search of his computers. The Ninth Circuit stated that "[t]he district court did not clearly err in holding that [the defendant's] consent to search his office reasonably included consent to examine the contents of his laptop computers.[273] The Ninth Circuit was not persuaded by the defendant's reliance on *Carey* and noted that "even in the Tenth Circuit, *Carey* has been limited to its facts."[274]

In *United States v. Balon*[275], The Second Circuit addressed the technological problem caused by the *Carey* analysis. The defendant argued that the supervised release condition that authorized the monitoring of "all data" on his computer was overbroad, and that the probation officer should be limited to reviewing "only those actions or files that might indicate introduction of child pornography onto the computer."[276] The three-judge panel of the Second Circuit took a dim view of this line of reasoning:

> [I]f a computer user loads contraband data onto a computer, it would seem easy to label the files containing the data in innocuous ways, say, by disguising the file as a "word" or "excel" document and changing its filename to "communication to attorney" or "tax return info." To insulate the file from examination, the user need only change the letters at the end of the filename. It appears, therefore, that unless the probation officer is allowed to search these documents, a user could store huge amounts of illicit data on the computer without anyone being allowed to view it."[277]

One court that followed the *Carey* decision was a trial court in New York State in the case of *People v. Carratu*.[278] The defendant in *Carratu* was the focus of an investigation into criminal possession of illegal cable television access devices. The warrants in the case authorized searches for "devices capable of defeating the security and encryption system of a cable television operator . . . records relating to the purchase, sale, and transportation of such devices . . . as well as computers and computer diskettes used in connection with the illegal activity."[279] The Court described the forensic examination as follows:

> The initial procedure was to make a copy of the hard drive for each of the systems. . . . Then the directory for each of the hard drives was displayed, and the folders for each hard drive were listed alphabetically. Finally, the detective opened each folder and examined each user-generated file to determine whether it contained evidence pertaining to the illegal cable box operation. . . . In a folder labeled "Fake I.D." on the Sony hard drive, the detective observed image files of driver's licenses, social security cards, inspection stickers, and registration certificates.[280]

The *Carratu* Court closely followed the reasoning of *Carey*. The *Carratu* Court held that folders that are "ambiguously labeled" may be opened by an investigator searching for evidence of a specific crime.[281] However, with respect to folders that are not "ambiguously labeled," the Court reached a different conclusion:

> The court notes that the "Fake I.D." folder was not ambiguously labeled. To the contrary, the name of the folder clearly indicated that it likely contained false identification documents rather than documents or records concerning the sale of illegal cable boxes. . . . Thus, from mere inspection of the folder name [the detective] had probable cause to seek a further warrant authorizing a search of the Sony computer for evidence of possession of forged instruments. And, since the file extension names on the files within the Fake I.D. folder indicated that they likely contained images, they appeared not to contain the type of text files which were akin to the items sought by the warrant.[282]

In suppressing the evidence of false identification documents, the *Carratu* Court did not even consider the ease with which files could be purposefully named anything at all, or that file extensions can be easily changed. Under the reasoning of the *Carratu* Court, all a criminal would have to do to hide text documents is to name his folders something innocuous like "Family Photos" and change the file extensions to .gif or .jpg, and the evidence would be suppressible.

In *Frasier v. State*,[283] an appellate court in Indiana again distinguished *Carey*. In that case, the affidavit in support of a search warrant application set forth evidence related to marijuana possession and dealing, as well as child pornography.[284] Based upon the affidavit, the judge issued a search warrant that directed the police to enter the defendant's home and search for marijuana-related materials and equipment; the judge

specifically struck out from the draft affidavit the words "pornographic images depicting persons believed to be children." When the police executed the warrant, a detective noticed an icon labeled "Smoke" on the desktop of a personal computer located in a bedroom. The detective opened the file, and noticed that it contained drug-related materials. The detective then began opening documents listed in the "Documents" menu of the computer's "Start" menu. The first document opened contained an image the detective believed to be child pornography. The detective opened a few other files, which also appeared to contain child pornography. A warrant was then sought and obtained to search for evidence of child pornography on the computer.

In addressing the defendant's objection to the introduction of the evidence of child pornography, the *Frasier* court held that the plain view doctrine applied, and it specifically discussed *Carey* in great detail:

> The situation in *Carey* was similar to the one before us: the police had a warrant to search the defendant's computer for documentary evidence pertaining to the sale and distribution of controlled substances.
>
>   *   *   *   *   *
>
> [The *Carey* court stated that] "the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, *we do not need to reach it here.*" . . . [T]he essential holding of the *Carey* court was that the plain view exception was inapplicable because the officer expected to find the files. . . [A]ccording to the *Carey* court, the fact that the document was closed cannot be the touchstone of whether the plain view doctrine is applicable; rather, it is whether the discovery was inadvertent.
>
>   *   *   *   *   *
>
> We have our own concerns with the approach . . . suggested by the *Carey* court, which implies that the police must rely upon the label given to a file to determine its contents. A computer image file is not exactly the same as a physical photograph. . . . The image file must be "opened," i.e., read and interpreted by some program in order to render its contents into a humanly perceptible form, i.e., an image on the computer monitor. In this sense, a computer image file is akin to a photograph sealed in an envelope or folder. And the name given to the file is like a label stuck onto the envelope or folder. Although such a label might say "Tax Records," the photograph inside could be of a nude child. Likewise, a computer image file containing child pornography could easily be named "tax_records.xls," in an attempt to hide its actual contents. . . . An officer searching for one type of record on a computer should not be forced to rely upon the name given to a file, which might very well hide its actual contents. In order to find out what is contained in the file, it must necessarily be "opened" in some way to ascertain its contents.

In *People v. Pacifico B.* [285], a California court distinguished *Carey* in an unpublished decision. In the *Pacifico B.* case, the warrant authorized a search for photographs of the victim. The computer forensics investigator "was informed of the scope of the warrant, and was given a photograph of [the victim] so that he could recognize her. [He] opened all of the files on the hard drives, including files with the extension 'JPG' . . . [He] did not encounter any photographs of [the victim] but did see photographs of other children that were pornographic in nature. . . No supplemental warrant was acquired."[286] The defense, relying on *Carey* and *United States v. Turner* (cited above in Section 7.1 at footnote 165) sought to have the defendant's conviction reversed. The *Pacifico B.* court rejected the defense's arguments, and noted that:

> [T]he warrant in this case specified that a search be conducted for images of the victim. [The investigator] was thus acting within the scope of the warrant in opening the JPG files on defendant's hard drives to look for such images. And having properly opened those files pursuant to the warrant, the child pornography images [the investigator] ultimately encountered were appropriately characterized as being in plain view.[287]

Although the *Pacifico B.* case does not carry precedential value, those drafting search warrants may want to keep the court's reasoning in mind.

United States v. Hill[288] is a case from federal district court in California that does not specifically refer to *Carey*, but that clearly rejects the reasoning of the *Carey* court. The government expert in *Hill* had, "through a comprehensive computer analysis using 'EnCase' forensic software," discovered over 1,000 images of child pornography on two zip disks.[289] The defendant argued that the search warrant relied upon was overbroad "because it placed no limitations on the forensic examination of the [zip] disks that were seized."[290] The Court refused to limit the investigator's search of computer files:

> Defendant also argues that the warrant was overbroad because it did not define a "search methodology." He claims that the search should have been limited to certain files that are more likely to be associated with child pornography, such as those with a ".jpg" suffix (which usually identifies files containing images) or those containing the word "sex" or other key words.
>
> Defendant's proposed search methodology is unreasonable. "Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent." *United States v. Hunter,* 13 F.Supp.2d 574, 583 (D.Vt.1998). Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer.
>
> Forcing police to limit their searches to files that the suspect has labeled in a particular way would be much like saying police may not

seize a plastic bag containing a powdery white substance if it is labeled "flour" or "talcum powder." There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it. The ease with which child pornography images can be disguised--whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated--forecloses defendant's proposed search methodology.[291]

In the Matter of the Search of: 3817 W. West End,[292] the U.S. District Court, N.D. Illinois, held that when deciding to issue a warrant to seize and search a home computer, the court has the authority to require the investigating officer to use a search protocol to ensure that the search will not exceed constitutional bounds. The court noted that "[t]he capacity of a computer to store extraordinary volumes of information increases the risk that many documents will have nothing to do with the alleged criminal activity that creates the probable cause for a search and seizure."[293] Interestingly, the sophisticated search functionality of modern computer forensic software proved a double-edged sword in this case, as the Court explained that "[c]omputer technology affords a variety of methods by which the government may tailor a search to target on the documents which evidence the alleged criminal activity, including: limiting the search by date range, doing key word searches, limiting the search to text files or graphics files, and focusing on certain software programs."[294] Therefore, allowing the government to search a computer "without limitation and without standards… fails to satisfy the particularity requirement of the Fourth Amendment."[295]

In United States v. Maali,[296] defendants filed a motion to suppress evidence seized pursuant to a federal investigation into their employment and harboring of aliens and tax evasion. One objection lodged by defendants was that the government should have included a computer search strategy in its affidavit to obtain the warrant as recommended in a Department of Justice computer search manual. The Court held: "The better practice would have been to follow the DOJ guidelines in developing a search strategy and presenting that strategy to the magistrate judge, and the failure to do so is troubling. However, the lack of a detailed offsite search strategy does not render the warrants' computer search provisions insufficiently particular, and the computer search provisions otherwise satisfy the Fourth Amendment."[297]

Defendants also challenged the manner in which the computer hard drives were seized and copied. "The seized computer hard drives were copied or "mirrored" and the hard drives were returned to the Defendants approximately one week after the searches."[298] Citing United States v. Hill, the Court held the seizure of hard-drives permissible because the affidavit supporting the warrant explained the necessity of an off-site search of the hard drives. "[S]ome aspects of a computer search necessarily require a controlled environment and special techniques."[299]

As for the manner in which the hard drives were searched, the FBI computer analyst in the case compiled all "data records" from the 83 computer hard drives onto a master hard drive, "culling down" the search by eliminating all "program files." Defendants argued that this "culling down" was insufficiently particular and the agent

should have limited the search to specific data files. The Court disagreed, holding, "the computer search has not been shown to be constitutionally infirm… it has been recognized that seizure of superfluous computer files is virtually inevitable."[300]

Additionally, defendants argued that investigators should have retained records of the text string searches that they ran. Disagreeing, the Court held: "[a]s to the failure of the searchers to keep records of the text string searches that they ran, while the maintenance of a search log seems feasible and not terribly burdensome to the searchers, the lack of such a record does not in and of itself render the search unconstitutional, at least in the face of testimony from the agents that the text string searches that were run pertained to the issues and entities described in the warrant."[301]

In *State v. Bolsinger*,[302] and appellate case from Iowa, the defendant argued that the search of his computer hard drive went beyond the scope of the warrant. The trial court had rejected this argument, stating:

> The actual search of the computer was not overbroad. There was testimony by the officer that did the search that he uses a special software system that enables him to do keyword searches of the entire system. That software then pulls up all fields that have hits of that keyword in them and allows the officer to view a small section of the file. Several words before and after the keyword come up to allow the officer to see the context in which the word is being used. From there the officer is able to make a determination whether to open the file or not. In addition to seeing the context of the word, the software tells him what type of computer file it is in. This too gives him information in order to determine whether that file is within the bounds of the search warrant. The officer did not look at everything on the hard drive. Rather, the search was narrow in focus due to the utilization of the software system and professional judgment of the officer after viewing the word or words in context.[303]

Due in part to the "comprehensive safeguards taken by the police to limit their search of Bolsinger's computer to the items specified in the warrant" the Court of Appeals of Iowa affirmed the trial court.[304]

The Tenth Circuit itself has narrowly interpreted *Carey*, or sought to avoid its application, on at least two occasions. First, in *United States v. Riccardi,*[305] the defendant argued that the warrant that had authorized the search of his computer did not comply with the particularity requirement of *Carey*. In fact, the warrant was remarkably vague: it authorized the "seizure" of Riccardi's computer and the search of "all electronic and magnetic media stored within such devices." [306] When the investigating officer conducted his forensic examination of the computer using EnCase software, he found thumbnail images of child pornography.[307] Apparently aware of Tenth Circuit precedent, however, the officer then suspended the search in order to review the search warrant language. After a prosecutor assured the officer's supervisor that the child pornography found on the computer would be covered by the warrant, the officer continued the search. The Court held that because the "warrant in this case was

not limited to any particular files, or to any particular federal crime," it lacked the specificity required by *Carey* and its progeny.[308] However, the Court found that the good-faith exception applied:

> Even if the court finds the warrant to be facially invalid – as was the case here – it "must also review the text of the warrant and the circumstances of the search to ascertain whether the agents might have reasonably presumed it to be valid."
>
> *   *   *   *   *
>
> The officers remained within the terms of the warrant as well as the affidavit, and did not conduct a "fishing expedition" beyond the scope of the authorized investigation. They did not search for, or seize, any materials for which probable cause had not been shown. By consulting the prosecutor, they showed their good faith in compliance with constitutional requirements. Nor do we think the defect in the warrant was so flagrant or obvious that "the executing officers [could] not reasonably presume it to be valid."[309]

As a result, the Court upheld the defendant's conviction.

In another Tenth Circuit case, *United States v. Brooks*,[310] an FBI agent had conducted a search of the defendant's computer at the defendant's house and with the defendant's consent. Upon locating several contraband images, the agent shut down the computer and seized it, and subsequently obtained a warrant authorizing a forensic search of the defendant's three computers and other media; this search was conducted at a police laboratory.[311] The defendant moved to suppress the evidence discovered during the forensic search, arguing that the warrant for the search was not specific enough, in that it did not describe a specific search methodology. The Court disagreed, reasoning as follows:

> At the outset, we disagree with Brooks that the government was required to describe its specific search methodology. This court has never required warrants to contain a particularlized computer search strategy. We have simply held that officers must describe with particularity the *objects of their search*. . . .
>
> The question of whether the nature of computer forensic searches lends itself to predetermined search protocols is a difficult one. Given the numerous ways information is stored on a computer, openly and surreptiously, a search can be as much an art as a science. . . . [C]ourts will look to (1) the object of the search, (2) the types of files that may reasonably contain these objects, and (3) whether officers actually expand the scope of the search upon locating evidence of a different crime.[312]

The Court went on to explain that *Carey* does not "stand for the proposition that a

warrant is per se overbroad if it does not describe a specific search methodology."[313]

The defendant also made a second argument concerning the warrant, arguing that it was overbroad because its language (authorizing a search of the computers "for evidence of child pornography," and then identifying the things to be search as including "correspondence, including printed or handwritten letters, electronic text files, emails and instant messages") did not explicitly instruct the officers to look solely for those text files containing child pornography.[314] The Court rejected the argument, noting that "although the language of the warrant may, on first glance, authorize a broad, unchanneled search through Brooks's document files, as a whole, its language more naturally instructs officers to search those files only for evidence *related to child pornography*."[315]

In a recent federal case from the Eastern District of Wisconsin called *United States v. Calimlim*, the warrant, perhaps written with *Carey* in mind, specified detailed search methodologies to be used on any computers seized, including "[s]canning storage areas for deliberately hidden files [and] Performing key word searches in electronic storage areas to determine whether occurrence of language contained in such storage areas exist that pertain to the subject matter of the investigation."[316] The Court noted that one agent used EnCase software (and another forensic tool) and the other "utilized EnCase software to perform key word searches of the data in each computer."[317] The Magistrate Judge agreed that the keywords used by the agents demonstrated a reasonable effort to limit the search to items identified in the warrant.[318]

§ 7.4 Post-*Carey* Practice

In a nutshell, *Carey* provides that an investigator may not manually search through individual files in a concerted effort to obtain information outside a warrant's articulated scope. While not addressing *Carey*, the *United States v. Scott* decision provides an indication that text string searches performed across an entire hard drive or other form of media would not subject the examiner to questions of exceeding the scope of a warrant, as long as such text searches were generally within the course of the investigation delineated by the warrant. The *Calimlim* case reached a similar result. By logical extension, results from aggregate hash file analysis, signature mismatch analysis and other automated functions featured in EnCase software would provide a means for investigators to justifiably seek supplemental warrants to broaden searches for evidence of additional criminal activity. At the same time, investigators employing such practices would arguably be better insulated from charges that they conducted an unauthorized review of individual files to obtain probable cause for the supplemental warrant. EnCase software features several automated features, such as the categorization of the hash value of each file in a case, that can help identify suspect files. EnCase software also features a capability providing for an unlimited number of executable macros and filters, and an automated picture gallery displaying all known graphical images in a case. As these functions will presumably be enacted as a routine practice in the course of computer investigations, supplemental warrants based upon information obtained from the aggregate outputs of these automated processes would be within the scope of the Fourth Amendment. See, *United States v. Gray,*[319] (software providing thumbnail views of all files in a directory properly utilized as standard FBI CART practice).

The *Carey* court proposes that in future investigations, computer examiners should be required to "engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents." The court notes that law enforcement computer investigators "can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory." If the courts were to adopt such a "file sorting" requirement, EnCase software provides an excellent, if not sole, mechanism to comply with various computer file-sorting instructions from a magistrate.

Given the post-*Carey* caselaw, however, it certainly appears that most judges are becoming more sophisticated regarding computer evidence, as the discussion by the *Frasier* and *Hill* courts show. While *Carey* has not been directly overruled, there is a long body of cases that seek to distinguish the *Carey* holding, and the Tenth Circuit itself has narrowly construed it. As of November 2005, numerous cases have distinguished it, and others such as *Hill* have rejected its reasoning while not mentioning it by name. Certainly investigators located in the Tenth Circuit should be aware of the *Carey* holding and conform their actions to it, and investigators in New York State should be cognizant of the *Carratu* case (although *Carratu* is not, of course, binding precedent). However, there appears now to be little chance that the *Carey* reasoning will spread widely to other jurisdictions.

§ 7.5 Warrant Return Requirements and Other Warrant Issues

Reports from the field indicate that the majority of federal magistrates are now requiring that computer forensic analysis upon computer media seized from businesses be completed within specified time periods. "A search warrant must be executed and returned to the judge or commissioner who issues it within [the time frame specified in the warrant]; after the expiration of this time the warrant, unless executed, is void." *United States v. Brunnette*[320]. Thus, the failure to complete a computer forensic analysis within the time specified will likely result in the suppression of the evidence found in the course of the investigation. In *United States v. Brunnette*, the court excluded evidence obtained from a computer investigation that was not completed within the 60 day period prescribed by the warrant.[321] Further, as demonstrated by *Steve Jackson Games v. United States*[322] an agency may be exposed to civil liability for unreasonably retaining custody of seized computer media.

This is one area where EnCase software presents a double-edged sword for law enforcement. If all federal magistrates were educated as to the capabilities of the software, we would likely see further time constraints being placed upon the analysis of seized computer media. Courts have thus far analyzed this issue in the context of older computer forensic technology noting that "it is no easy task to search a well-laden hard drive by going through all of the information it contains, let alone to search through it

and the disks for information that may have been 'deleted.'" *United States v. Upham*,[323] (analyzing forensic processes utilized by U.S. Customs in early 1997, before the agency's adoption of EnCase software). The Court further states "if the images themselves could have been easily obtained through an on-site inspection, there might have been no justification for allowing the seizure of all computer equipment." In reviewing a 1995 forensic examination, the Court in *United States v. Hunter,*[324] opined, "until technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur." Similarly, in *United States v. Triumph Capital Group*, a federal case from 2002, the Court held that a forensic examination of a hard drive need not occur within the time period specified in Federal Rule of Criminal Procedure 41 for return of a search warrant; so long as the search is completed within a reasonable time, in need not be performed within ten days.[325] The Court's view was that "[c]omputer searches are not, and cannot be subject to any rigid time limit because they may involve much more information than an ordinary document search, more preparation and a greater degree of care in their execution."[326] Many observers, however, believe that it is only a matter of time before shorter warrant return requirements become the standard for computer examinations. For example, in the *United States v. Maali* case, discussed earlier in this chapter, the seized hard drives were returned to the defendants within one week.

A case that was decided in the other direction is *United States v. Gorrell*,[327] in which the warrant specified that the search of the defendant's home had to occur on or before January 10, 2003.[328] The search occurred prior to that date, and recovered two computers and a zip disk. The forensic analysis of the seized computer hard drives, however, was delayed until October 2003 "due to a backlog of similar requests."[329] The defendant argued that the recovered data was inadmissible due to the ten-month delay in processing. The Court rejected the defendant's argument, stating that "[t]he warrant did not limit the amount of time in which the government was required to complete its off-site forensic analysis of the seized items and the courts have not imposed such a prophylactic constraint on law enforcement."[330]

Although the *Gorrell* Court was lenient, other courts have taken a stricter approach. In *State v. Zinck*,[331] an unpublished decision from New Hampshire, the Court concluded that an eighteen-month delay in conducting a search of the defendant's computer was unreasonable. The Court distinguished *Habershaw* [discussed above in Chapter 6], noting that the *Habershaw* Court held that a supplementary search of a computer occurring four days after the return date required by the warrant (as occurred in *Habershaw*) was reasonable because the search originated within the time period mandated by the warrant.[332] In contrast, the *Zinck* Court held, "this is not a case where the length of time after the warrant's expiration is brief and justifiable due to the time constraints of a search initiated within the warrant's time frame. Nor is this a case where the volume of material necessitated an excessive amount of time to complete the search. Indeed, the State concedes that once the search was initiated it took just two weeks to complete."[333].

Another interesting warrant issue that was recently addressed is whether a law enforcement officer's affidavit in support of a search warrant should be held to the evidentiary standards applied to courtroom testimony. In *Cano v. State of Florida*,[334] a

deputy with twenty years of experience submitted an affidavit that addressed "the psychological profile of the typical person who commits repeated sex crimes involving one targeted child and those who involve themselves with child pornography on computers and the internet."[335] The defendant argued that evidence seized as a result of that warrant should be suppressed. The Court stated:

> In this case, the affidavit of the deputy described his experience and his knowledge or beliefs about the tendencies of child sexual offenders who utilize computers and cameras. We are not entirely convinced that the deputy provided expert testimony in his affidavit or that his testimony should be regarded as expert scientific evidence, but we make that assumption for purposes of this opinion. Neither the deputy nor the magistrate relied on this evidence to decide whether the young girl was a victim of sexual abuse or whether [the defendant] was the perpetrator. This evidence was utilized merely to determine the scope of the search and to conclude that the other evidence supporting the search was not stale.
>
>   *   *   *   *   *
>
> The type of thorough consideration given at trial to relevance or to the prejudicial effect of evidence versus its probative value is not feasible or appropriate when a magistrate issues a search warrant. The restrictive standards of *Frye*, while not entirely out of place when issuing a warrant, are not essential to that process. Moreover, the *Frye* approach to novel scientific evidence contemplates an adversarial hearing that occurs only when the opposing party objects to the evidence. This methodology is not particularly adaptable to the procedures used to obtain a search warrant . . .[336]

§ 7.6 Business Disruption Caused by the Seizure of Computers

One of the problems with seizing computers in the field for later forensic analysis is the extensive disruption caused to the party from whom the computers are seized, which can be particularly acute in the case of a business. In many instances, the computers from which evidence is gathered belong to a third party that has not been charged with a crime. *See, e.g.*, *State (Ohio) v. Morris*, discussed above in Chapter 6, in which law enforcement returned the original hard drive, which "belonged to a non-party . . . who used the computer in his business."[337] In these situations, law enforcement needs to be able to acquire the data in the field, so as not to unnecessarily harm innocent parties. In *Airtrans, Inc. v. Mead*,[338], the Sixth Circuit Court of Appeals addressed a claim by plaintiff that "[d]uring execution of the warrant, the agents seized records and disabled company computers, leaving AirTrans effectively unable to operate. . . After the search, AirTrans filed a § 1983 action against the defendants seeking compensation for its business losses."[339] In that case, AirTrans was the target of a criminal investigation, and the Court of Appeals found that there was no constitutional violation. Nevertheless, it would have been far easier for the government to collect the computer data on site, thereby obviating any claim of harm by plaintiff. As in the *Morris* and *Maali* (discussed above in Section 7.3) cases, the forensic image could readily serve the government's investigative purposes. The

case of *State v. Kaminski*[340] represents an example of the common misperception among law enforcement personnel and judges concerning the investigation of a computer system. In applying for a warrant to search the defendant's residence, the affiants stated to the Court "that to retrieve data from a computer system it is necessary for the entire system to be seized and submitted to a computer specialist for examination and analysis in a laboratory setting."[341] With current technology, that is no longer the case.

8

Complying with Discovery Requirements in Criminal Cases when Utilizing the EnCase Process

§ 8.0 Overview

One of the questions prosecutors and examiners routinely face in the field is complying with discovery requirements when the prosecution's computer evidence is contained within an EnCase image. This is a somewhat difficult issue due to the very nature of computer evidence. Printing out all the data on a 10-gigabyte hard drive would result in a stack of paper approximately 300 meters tall. Even worse, this data will be compromised unless properly handled with computer forensic software. The question then becomes, what is required to produce relevant computer evidence in the course of discovery?

There are several models for producing electronic evidence in the course of discovery that are employed by prosecutors and attorneys. Each have their own strengths and weaknesses, and the applicable statutes and discovery rules of the particular jurisdiction and preferences and discretion of the individual judge often determine which of the following models are most suitable.

§ 8.1 Production of Entire EnCase Images

Many attorneys choose to produce exact copies of the EnCase Evidence File, which is a complete physical image of an acquired drive. Often the prosecution will also produce the Case File, which contains the bookmarks, text-string searches, various notes and comments of the investigator, as well as other information. As much of the data contained within the Case File, such as the examiner's bookmarks and notations could be considered work product, it is within the discretion of the prosecutor to produce such evidence. Many prosecutors in the U.S. inform the defense that it should retain an expert who is familiar with the EnCase software. With EnCase software and the practice of computer forensics becoming more standard, there are an increasing number of experts in the private sector as well as Federal and State Public Defenders offices who are utilizing the software. As such, this option is becoming increasingly more feasible as the practice of computer forensics expands.

The advantage to this approach is that it ensures the defense cannot tamper with the evidence, at least without detection, and dispels any claim that the prosecution withheld evidence. For these reasons, this method of discovery is the most desirable. The disadvantage to this approach is that many defendants and their counsel still lack the expertise or means to purchase and utilize the EnCase software, although as noted above, this trend is decreasing.

§ 8.2 Production of Restored Drives

Another option is to provide a restored hard drive, which is a complete bootable clone of the original seized drive. EnCase software includes a feature that allows the examiner to easily restore an EnCase image to a separate drive. EnCase software will restore the seized drive onto a separate drive and verify the copy by a 128 bit, MD5 hash, which will match that of the original evidence, even if different sized media is utilized in the process. After receiving the discovery, the defense's retained expert can examine the evidence.

The advantage of this approach is that it provides the entirety of the evidence in a manner that most laypersons can access and view. However, the disadvantage of this approach is that deleted, temporary and buffer files, as well as key metadata are not viewable by simply booting the cloned drive. Also, once the defense boots the cloned drive, much of the evidence would change, including date stamps and writes to the swap file. As a result, the Defense may attempt to introduce, and not necessarily by intention, evidence that is not an accurate reflection of the data as it existed at the time the government seized the computer media. Of course, with the MD5 hash of the restored drive recorded, the prosecution would be able to detect that any changes were made to the restored drive by the defense.

§ 8.3 Production of Exported Files

Some prosecutors provide selected exported files and other information from the Evidence File, along with printouts of that information. Production of these files and blocks of selected data is achieved by transferring the information to a CD-ROM disk in a format that is easily viewable by counsel. The EnCase Report may also be produced. This option provides the exact information that the prosecution intends to introduce at trial in a convenient and easy to read format. By providing the electronic evidence on CD-ROM disks, the defense cannot tamper with the selected portions of the original evidence. Disadvantages of this process include potential claims that the production was too narrow and that potentially exculpatory documents were omitted. Many courts tend to prefer that document productions be comprehensive, as opposed to more limited productions that may not contain all relevant data.

§ 8.4 Supervised Examination

Where the Defense has retained an expert, another option is to permit the defense expert to access, under supervision of the investigating officer and/or a special master, an image of the original drives so that the expert can conduct a proper and non-invasive investigation. Ideally, the expert would utilize EnCase software to conduct the exam, but may be permitted access to the original drives or a properly restored clone for re-imaging with other non-invasive tools.

Section 4.4 summarizes a New Hampshire Federal District Court case where the prosecution offered to allow the Defense supervised access to a copy of the EnCase Evidence File, which contained images of child pornography. However, the Defense

contended that it required access to the original computer systems in question so that they could operate those computers and examine them in their native environment, and filed a formal written request for a Court order allowing such unfettered access to the "original" computer evidence. The Government filed a successful objection to the request, asserting that the "mirror image" created by the Special Agent is the proper way to preserve the original evidence. The Government asserted that merely turning on the computer, as the Defense requested, will change the state of the evidence by altering critical date stamps and potentially overwriting existing files and information.

The Court ruled that the Defense could only have access to the original computer systems if their expert created a proper forensic image under the supervision of the Special Agent. The Defense was barred from booting the original computer systems to their native operating systems.

§ 8.5 Production of EnCase Evidence Files to Defense Experts

A number of courts have required the prosecution to provide copies of EnCase evidence files to the defense. This approach is highly controversial in cases in which the computer evidence consists of contraband, such as child pornography, and in such cases the prosecution typically argues for the type of supervised examination described above in Section 8.4.

United States v. Hill,[342] a case from federal district court in California (described above in Chapter 7), is illustrative. In that case, the Court held that the government had to provide copies of the EnCase evidence files to the defense, reasoning as follows:

> The government intends to introduce into evidence "over 1,000 images of child pornography and/or child erotica," which it discovered on two 100 megabyte zip diskettes taken from defendant's home. The government's expert discovered the images through a comprehensive forensic computer analysis using "Encase" forensic software. Defendant wishes to obtain two "mirror image" copies of the computer media analyzed by the government's expert to allow his own expert to conduct a forensic analysis and his counsel to prepare his defense. The government opposes producing these items, offering instead to permit the defense to view the media in an FBI office and to conduct its analysis in the government's lab.

> *   *   *   *   *

> The court concludes that defendant will be seriously prejudiced if his expert and counsel do not have copies of the materials. Defense counsel has represented that he will have to conduct an in-depth analysis of the storage media in order to explore whether and when the various images were viewed, how and when the images were downloaded and other issues relevant to both guilt and sentencing. The court is persuaded that counsel cannot be expected to provide defendant with competent representation unless counsel and his

expert have ready access to the materials that will be the heart of the government's case.

> The government's proposed alternative -- permitting the defense expert to analyze the media in the government's lab at scheduled times, in the presence of a government agent -- is inadequate. The defense expert needs to use his own tools in his own lab. And, he cannot be expected to complete his entire forensic analysis in one visit to the FBI lab. It took defense counsel between two and three hours to quickly scroll through the 2,300 images in the Encase report, so it is likely to take the expert much longer than that to conduct a thorough analysis. Defendant's expert is located in another state, and requiring him to travel repeatedly between his office and the government's lab -- and obtain permission each time he does so -- is unreasonably burdensome. Moreover, not only does defendant's expert need to view the images, his lawyer also needs repeated access to the evidence in preparing for trial.[343]

The reasoning of the *Hill* Court was explicitly followed in *United States v. Frabizio*,[344] in which the defendant "moved for production of an image of the hard drive, as well as all 'Encase' files."[345] The government refused to produce any images it believed to be child pornography, but it did make those images available for inspection at an FBI facility. The Court rejected the government's approach; instead it adopted the same protective order used by the *Hill* Court, and noted that "there is no reason to think that defense counsel or her expert cannot be trusted to abide by the proposed protective order. It cannot be said -- at least credibly -- that the only defense counsel and experts to be trusted are those who were formerly employed by the government."[346]

In a recent unpublished opinion, a Minnesota appellate court affirmed the dismissal of a case because the prosecution had refused to turn over a forensic image of the defendant's hard drive, which the prosecution asserted contained child pornography.[347] Defense counsel had specifically requested a "forensically sound Image Copy of the hard-drive of the computer containing the alleged pornographic images, and all digital storage media including but not limited to Zip Discs, Jaz Discs, CD Rom, Tapes, Floppy Discs and any other storage media."[348] The prosecution "asserted its ongoing refusal to allow respondent to access the allegedly pornographic images, arguing that [among other things] federal law prohibits the dissemination of the images, even to defense counsel or respondent's expert."[349] The trial court dismissed the case because of the prosecution's recalcitrance, a decision that was upheld by the Court of Appeals.

United States v. Alexander[350] is another case in which the court ordered the production of a duplicate forensic image of a hard drive containing contraband to a defense expert. The Court dismissed the prosecution's concern regarding further dissemination of contraband, relying "on the efficacy of its orders to protect the public from further disclosure of the images."[351]

In the consolidation of two Tennessee child pornography prosecutions, *State v.*

Butler,[352] "[c]ounsel for both defendants filed motions for discovery, including requests that the State provide them with copies of the computer hard drives and 'other computer materials' for their independent examination and review. The State refused, offering to make the material available for examination by defense counsel and defense computer experts at the sheriff's department, but contending that it would constitute a violation of the sexual exploitation statute for the material to be removed from the custody and control of the sheriff's department."[353] The Court of Criminal Appeals of Tennessee held that the State was required to provide the defense with copies of the alleged pornographic materials, and that "so long it occurs in the context of the prosecution or defense under the statute," dissemination would not constitute a violation.[354] At the trial court, one of the defendants had argued that the State should be required to turn over the original hard drive, rather than a forensic image of the hard drive, alleging that "computer programs in existence did not create true mirror images."[355] The trial court rejected this argument, "requiring the State to provide Allen's counsel with a mirror image copy of the computer hard drive rather than the actual hard drive itself."[356]

§ 8.6 Discovery Referee in Civil Litigation Matters

Chapter 9 includes a discussion of a well-designed protocol proscribed by a Federal District Court for the discovery by computer forensic experts of electronic evidence contained on opponents' hard drives. In *Simon Property Group v. mySimon, Inc.*,[357] the court issued an order appointing a computer forensics expert as an officer of the court, enabling the expert to conduct the exam under court supervision as a neutral special master. By serving in such capacity, any attorney-client or other privileges would remain intact during the course of the neutral experts' examination, with the producing party afforded full opportunity to lodge objections to the production of evidence identified during the course of the examination. This particular special master model may be appropriate in some criminal case as well, particularly those involving seizure of computers from law firms or other businesses with sensitive material.

EnCase Enterprise Edition in Civil Discovery

§ 9.0 Overview

Years ago, in the days of command-line analysis utilities, attorneys typically employed computer forensic experts only in high-stakes, high-expense litigation or corporate investigation matters. Back then, many civil litigants resisted court-ordered computer discovery by convincing judges that a proper forensic analysis of a single hard drive would cost tens of thousands of dollars in expert fees. In the 1997 case *Alexander v. Federal Bureau of Investigation,*[358] for example, an IT specialist testified in a high-profile investigation of President Clinton that the examination of a single hard drive required approximately 265 hours. If a law firm were to retain an expert to conduct a similar task at an average standard rate of $300 per hour, the cost would nearly exceed $80,000 for the examination alone. It is thus no wonder that the *Alexander* case often found its way into briefs submitted by litigants seeking to quash an adversary's subpoena for the production of computer evidence. As recently as July 1999, counsel advanced the argument in one well-publicized federal litigation that e-mail discovery was "simply not feasible."[359]

Over the past few years, however, electronic discovery has become a standard part of the litigation process, fostered by a growing awareness amongst counsel and the bench that nearly all evidence is digital. "Rules 26(b) and 34 of the Federal Rules of Civil Procedure instruct that computer-stored information is discoverable under the same rules that pertain to tangible, written materials."[360] Indeed, "[n]ow that the key issues have been addressed and national standards are developing, parties and their counsel are fully on notice of their responsibility to preserve and produce electronically stored information."[361]

Thus, the trend over the past few years is that courts no longer tolerate the time-worn excuses often advanced by litigants resisting electronic discovery, such as high cost and extreme burden. This is particularly true with respect to large companies. The corollary to this trend, or perhaps its cause, is that the judiciary has become increasingly sophisticated about the technologies that can be brought to bear on electronic discovery. For example, Judge Scheindlin, author of the landmark *Zubulake* line of cases, laid out a technological procedure to guide counsel:

> To the extent that it may not be feasible for counsel to speak with every key player, given the size of a company or the scope of the lawsuit, counsel must be more creative. It may be possible to run a

system-wide keyword search; counsel could then preserve a copy of each "hit." Although this sounds burdensome, it need not be. Counsel does not have to review these documents, only see that they are retained. For example, counsel could create a broad list of search terms, run a search for a limited time frame, and then segregate responsive document. [FN75] When the opposing party propounds its document requests, the parties could negotiate a list of search terms to be used in identifying responsive documents, and counsel would only be obliged to review documents that came up as "hits" on the second, more restrictive search. The initial broad cut merely guarantees that relevant documents are not lost.

> FN75. It might be advisable to solicit a list of search terms from the opposing party for this purpose, so that it could not later complain about which terms were used.

In short, it is *not* sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched. This is not to say that counsel will necessarily succeed in locating all such sources, or that the later discovery of new sources is evidence of a lack of effort. But counsel and client must take *some reasonable steps* to see that sources of relevant information are located.[362]

With the advent of EnCase Enterprise software, this capability is available to every litigant, as it provides a much-improved platform for the search, collection, and analysis of digital data from multiple computers and servers located anywhere on a wide-area network.

§ 9.1   Computer Discovery is a Mandated and Routine Process

In the past, many enterprises embroiled in civil litigation in the US largely avoided court-ordered discovery of their networks for computer evidence on the grounds that such measures were overly broad, burdensome and expensive.[363] Alternatively, many litigants were able to shift the costs of electronic discovery to the party requesting the discovery. However, over the past few years the landscape shifted considerably, to the point where "[t]he discovery of electronic data . . . in today's world . . . includes virtually all cases."[364]

Setting the tone is a case from a few years ago, *In Re Bristol-Meyers Squibb Securities Litigation,*[365] in which the court unequivocally stated that as the vast majority of documentation now exists in electronic form, electronic evidence discovery should be considered a standard and routine practice going forward. A subsequent decision, *Residential Funding Corp. vs. DeGeorge Financial*[366] is a must-read for any attorney or consultant that practices in the area of computer evidence discovery. In that case, Residential Funding Corp (Residential) attempted to stave off its opponent's discovery

request for production of computer evidence by citing the prohibitive expense and technical difficulties involved in producing the requested emails and other computer documents. Residential's own expert professed to the court that "technical problems" prevented the timely and cost-effective retrieval of sought computer data. The Court, however, had no patience for Residential's obstruction, characterizing Residential's conduct as "purposeful sluggishness," and dropped a judicial bombshell by further commenting that it was unreasonable for Residential to continue to employ the services of its electronic discovery expert who admitted difficulty in getting the job done. The court granted DeGeorge's expert access to Residential's network, including desktops and backup tapes, and imposed harsh monetary and evidentiary sanctions against Residential for its bad faith conduct.

A federal district court in Connecticut, in *Pace v. Nat. Passenger RR Corp.*, a case involving the destruction of video evidence, discussed the *Residential Funding* opinion.[367] The *Pace* court described *Residential Funding* as holding that the knowing destruction of evidence, even if done negligently and without any intent to breach a duty to preserve, satisfies a finding of a culpable state of mind, such that an adverse inference can be drawn. In addition, the *Pace* court noted that *Residential Funding* applies to destruction of evidence prior to the institution of litigation, not merely to post-litigation disputes, as was the case in *Residential Funding.* "Indeed, the opinion makes clear that its standards apply to document destruction generally."

The *Residential* decision clearly illustrates that the alleged burden of computer evidence discovery is no longer a shield to compliance, and that permitting computer evidence to be destroyed can lead to sanctions or the drawing of an adverse inference. A federal magistrate judge noted, in a class-action sexual harassment case, that the defendant:

> had a duty to preserve the computer hard drives, e-mail accounts, and internet records of anyone who left the company who had been accused (formally or informally) of sexual harassment or misconduct. Or, if this were cost prohibitive, it could have searched the computer for sexually inappropriate of otherwise offensive material before destroying the other data it contained and reusing the computer.[368]

Thus, courts are becoming more sophisticated regarding the advanced technology, such as EnCase software, available to litigants for computer evidence preservation and retrieval. For example, the Court in the *Residential Funding* case had no patience for the "purposeful sluggishness" of a computer forensics consultant. Similarly, the *3817 W. West End* [see Section 7.3, above] Court highlighted the growing lack of judicial patience for unprepared or incompetent computer forensics "experts":

> When the Court raised the possibility of limiting the search to certain time periods, one of the government representatives stated that such a limitation would not be helpful since the file directory only shows when a document was last saved. The Court then asked the government technical expert whether that problem could not be overcome by examining the "metadata" in the computer files, which would show not

only the date a document was last saved, but also when the document was first created and (often times) the changes in the documents from the original draft to the final revision. The government technical expert made no response, leaving the Court with the firm impression that he was not familiar with a term that we would expect a computer expert to know.[369]

In another case, the Court ordered an examination of hard drives and even suggested specific search terms and time parameters![370] Several other courts have similarly issued decisions requiring expedient and full compliance with computer evidence discovery requests. (See *Antioch Co. vs. Scrapbook Borders, Inc.*[371]; *Tulip Computers International vs. Dell Computer*[372]). Moreover, courts continue to severely punish litigants who fail to preserver and/or alter computer evidence when a lawsuit is pending. *Metropolitan Opera Association v. Local 100, Hotel And Restaurant Employees Int'l Union*[373], is one of a strong line of cases that impose harsh penalties upon parties who fail to preserve computer evidence. In *Metropolitan Opera*, the court ordered what amounts to be a case-ending finding of liability as a litigation penalty after determining that the defendants improperly destroyed computer evidence in bad faith. One of the surest ways to lose a lawsuit these days is to have an opponent establish that you or your expert failed to preserve computer evidence while the lawsuit was pending, or worse, actively destroyed evidence, as in the *Kucala* case discussed in Chapter 6, above.

These cases establish that enterprises and their consultants responding to computer discovery must demonstrate technical and organizational competence in the ability to comply with subpoenas for production of relevant data and to properly preserve and acquire evidence. Courts will grant an enterprise the opportunity to produce the requested information themselves, but only if they demonstrate such technical and organizational competence by either retaining proficient computer forensics/e-discovery experts or having the appropriate resources and court-validated technology employed internally to get the job done. If not, the dilatory enterprise will likely find itself being visited by its opponent's experts in a widened and highly intrusive court-ordered on-site discovery effort, with often devastating court sanctions to boot.

§ 9.2 Spoliation

Failure to satisfy a party's preservation obligations [described below in Section 9.3] can lead directly to sanctions. Situations in which a party intentionally destroys information are straightforward for the courts to address. For instance, in *AdvantaCare Health Partners, L.P. v. Access IV*[374], Gary Dangerfield and Gwen Porter were employees of AdvantaCare who resigned and began a competing business called Access IV. AdvantaCare then hired a computer forensics expert who "determined that Dangerfield had accessed AdvantaCare's computer network and copied a large number of AdvantaCare's files prior to leaving, including files containing company policies and procedures, patient databases, employee lists, and contracts. The forensic [expert] also determined that Dangerfield tried to conceal his copying activities by deleting copied files from his hard drive."[375] Shortly thereafter, the Court entered a temporary restraining order that prohibited the defendants from using, copying, or destroying any

AdvantaCare data, and that required the defendants to permit AdvantaCare to make forensic copies of the hard drives and network servers of Access IV.[376] The Court described the defendants' response to the temporary restraining order:

> . . . [The defendants] were served with a copy of the TRO . . . at 4:20 pm on October 6, 2003. Early that evening, Dangerfield visited numerous websites, searching for computer data deletion software. At 9:00 pm, Dangerfield upgraded to BC Wipe, one of the strongest computer file deletion programs available. Between October 7, 2003 and October 10, 2003, Dangerfield deleted more than thirteen thousand files from his home computer using BC Wipe.[377]

Even after this activity was uncovered, the defendants failed to comply with the temporary restraining order, or with agreements they had made with plaintiffs concerning the deletion of AdvantaCare data. The Court entered evidentiary sanctions, ordering that "the trier of fact shall find that Defendants copied all of the files on Plaintiffs' computers" and awarded monetary sanctions of $20,000.[378]

Kucala Enterprises, Ltd. v. Auto Wax Co., Inc., discussed above in Chapter 6, likewise involved intentional evidence destruction. Similarly, in the fifth opinion issued in the *Zubulake* line of cases (described more fully below in Section 9.4), the Court noted that:

> UBS personnel unquestionably deleted relevant e-mails from their computers after August 2001, even though they had received at least two directions from counsel not to. Some of those e-mails were recovered (Zubulake has pointed to at least 45), but some--and no one can say how many--were not. And even those e-mails that were recovered were produced to Zubulake well after she originally asked for them.[379]

As a result, the Court issued a negative inference jury instruction, and ordered the defendant to pay the costs of any re-depositions of witnesses necessitated by the defendant's late production of responsive documents.[380]

The day after the fifth Zubulake opinion was issued, a federal district court in the District of Columbia addressed spoliation in *United States v. Philip Morris USA*.[381] The Court described the situation as follows:

> [On October 10, 1999, the Court issued an order] requiring preservation of "all documents and other records containing information which could be potentially relevant to the subject matter of this litigation." Despite this Order, Defendants Philip Morris and Altria Group deleted electronic mail ("email") which was over sixty days old, on a monthly systemwide basis for a period of at least two years after October 19, 1999. In February, 2002, Defendants became aware that there was inadequate compliance with [the Court's order], as well as its own internal document retention policies, and that some emails

relevant to this lawsuit were, in all likelihood, lost or destroyed. It was not until June 19, 2002, four months after learning about this serious situation, that Philip Morris notified the Court and the Government. Moreover, despite learning of the problem in February 2002, Philip Morris continued its monthly deletions of email in February and March of 2002.[382]

The Court found that the defendants' noncompliance with its order warranted the imposition of a sanction precluding all individuals who had failed to comply with the document retention program from testifying in any capacity at trial, as well as a monetary sanction of $2,750,000.[383] Although for Philip Morris USA, nearly three million dollars is not a significant sum, the case highlights the seriousness with which courts are addressing failures to meet preservation obligations with respect to electronic documents and data.

In *Mastercard International, Inc. v. Moulton,*[384] Mastercard had sued the defendants for copyright and trademark infringement. For four months after the filing of the lawsuit, the defendants failed to take any steps to preserve potentially relevant e-mails, and instead allowed their server to eliminate emails after twenty-one days in accordance with their existing practice.[385] The Court, although it refused to impose specific sanctions, noted the following:

> [W]e are not persuaded that defendants acted in bad faith, that is, for the express purpose of obstructing litigation. They appear simply to have persevered in their normal document retention practices, in disregard of their discovery obligations. The absence of bad faith, however, does not protect defendants from appropriate sanctions, since even simple negligence is a sufficiently culpable state of mind to justify a finding of spoliation.[386]

Notwithstanding the Moulton case, litigants must beware allowing normal email or other deletion systems to continue to operate, at least if the litigants have not preserved potentially relevant evidence by, for example, using EnCase Enterprise software. In *Mosaid Technolgies Inc. v. Samsung Electronic Co. Ltd.,*[387] the Court imposed a "spoliation inference"[388] and monetary sanctions against Samsung for destruction of electronic data. The Court described the case as follows:

> [A]fter the inception of this litigation in September 2001, Samsung never placed a "litigation hold" or "off switch" on its document retention policy concerning email. Unchecked, Samsung's automatic computer e-mail policy allowed e-mails to be deleted, or at least to become inaccessible, on a rolling basis. As a result, Samsung failed to produce a single technical e-mail in this highly technical patent litigation because none had been preserved.

<p style="text-align:center">*   *   *   *   *</p>

The duty to preserve potentially relevant evidence is an affirmative

obligation that a party may not shirk. **When the duty to preserve is triggered, it cannot be a defense to a spoliation claim that the party inadvertently failed to place a "litigation hold" or "off switch" on its document retention policy to stop the destruction of that evidence.** As discoverable information becomes progressively digital, e-discovery, including e-mails and other electronic documents, plays a larger, more crucial role in litigation. In this district, in October 2003, Local Civil Rule 26.1 was amended to include a section concerning discovery of digital information. *See* L. Civ. R. 26.1(d). Among other things, that rule requires counsel to investigate how a client's computers store digital information, to review with the client potentially discoverable evidence, and to raise the topic of e-discovery at the Rule 26(f) conference, including preservation and production of digital information. **Unless and until parties agree not to pursue e-discovery, the parties have an obligation to preserve potentially relevant digital information. Parties who fail to comply with that obligation do so at the risk of facing spoliation sanctions.**

Although Rule 26.1(d) was not in effect at the start of this litigation, Samsung was aware that it had a duty to preserve potentially discoverable evidence. It knew that its technical e-mails were potentially relevant to the claims and defenses existing in this lawsuit. And Samsung chose to do nothing about the spoliation of those e-mails. As a result, MOSAID has suffered prejudice from the nonproduction of countless e-mails because its ability to prove infringement, and other issues, has been potentially hindered.

In light of the above, the Court affirms the spoliation inference jury instruction and monetary sanctions imposed by Magistrate Judge Hedges. These are the least burdensome sanctions the Court can impose while still attempting to level what has become an uneven playing field.[389]

Of course, there is nothing wrong with having a set schedule for the deletion of email or other data. Once the duty to preserve attaches, however, the party must preserve potentially relevant documents. As stated by the *Mosaid Technologies* Court, "[t]he duty to preserve potentially relevant evidence is an affirmative obligation that a party may not shirk."[390] The often-overlooked crucial point is that it is only potentially relevant data that need be preserved. Irrelevant information need not be kept. In *Tantivy Communications, Inc. v. Lucent Technologies Inc.*, the Court described discovery obligations as follows: "[t]he party and its counsel should ensure that (1) all sources of relevant information are discovered, (2) relevant information is retained on a continuing basis, and (3) relevant non-privileged material is produced to the opposing party."[391] Again, irrelevant information plays no part in discovery. Using EnCase Enterprise software, a litigant can search for and preserve the potentially relevant data in a secure container (known as a Logical Evidence File), thereby satisfying its preservation obligation. With those obligations satisfied, the litigant arguably can then continue its normal document destruction processes.

One example of an aggressive document destruction process was described by the Court in the *Broccoli v. Echostar Communications Corp.*[392] case, as follows:

> Under Echostar's extraordinary email/document retention policy, the email system automatically sends all items in the user's "sent items" folder over seven days old to the user's "deleted items" folder, and all items in a user's "deleted items" folder over 14 days old are then automatically purged from the user's "deleted items" folder. The user's purged emails are not recorded or stored in any back up files. Thus, when 21-day-old emails are purged, they are forever unretrievable. The electronic files, including the contents of all folders, sub-folders, and all email folders, of former employees are also completely deleted 30 days after the employee leaves Echostar.[393]

In this case, the Court found that Echostar's preservation obligations attached as early as January 2001, but that Echostar did nothing to preserve potentially relevant data. The Court had little patience for this approach:

> Given Echostar's status as a large public corporation with ample financial resources, the court finds it indefensible that . . . basic personnel procedures and related documentation were lacking . . . [Echostar was] guilty of gross spoliation of evidence.[394]

Clearly, the Court's statement about Echostar's size and resources demonstrates the growing trend to hold litigants, particularly large companies, to the letter of the law with respect to meeting discovery obligations.

§ 9.3 Metadata

It is routinely acknowledged that metadata, if relevant to the case, is discoverable. (As an aside, it goes without saying that if metadata – or any other kind of information – is irrelevant, there is no obligation to preserve or produce it in discovery). The ABA's Civil Discovery Standards note that "[a] party requesting information in electronic form should also consider . . . asking for the production of metadata associated with the responsive data."[395] Similarly, the Sedona Principles comment that "[o]f course, if the producing party knows or should reasonably know that particular metadata is relevant to the dispute, it should be produced."[396] The judiciary is likewise cognizant of this fact. For example, in a case management order issued in 2005, a federal court in Louisiana used the following language:

> PRESERVATION OF EVIDENCE --- All parties and their counsel are reminded of their duty to preserve evidence that may be relevant to this action. The duty extends to documents, data, and tangible things . . . . "Documents, data, and tangible things" is to be interpreted broadly to include writings, records, files, correspondence, [etc.]. Information that serves to identify, locate, or link such material, such as file inventories, file folders, indices, and **metadata,** is also included in this

definition.[397]

Similarly, a federal district court in Illinois matter-of-factly discussed the discoverability of metadata as follows:

> "On April 25, 2003, WH-TV moved to compel Motorola to produce the files in electronic form. WH-TV stated that it was necessary to have the files in electronic form, because the electronic files contained "metadata" that are not printed on the hard copies. WH-TV also noted that having the files in electronic form would allow it to search them more easily. On May 2, 2003, this court granted WH-TV's motion to compel."[398]

Often, when faced with a preservation obligation or a discovery request, companies will gather potentially relevant electronic data by asking their employees to comb through their computers looking for information. While well-intentioned, perhaps, this activity has the effect of changing much of the key metadata associated with the potentially relevant data, since the employees are using the computer's operating system to gather information. Historically, in order to preserve the metadata of potentially relevant digital data, one had to make a forensic image of the entire hard drive, or at least a partition. There was no other way to preserve all of the relevant metadata. Fortunately, with the release of EnCase Version 5, individual files can be collected while preserving their metadata. This revolutionary advance is crucial for cases in which metadata contains potentially relevant information, and is an important part of a defensible electronic discovery process.

The recent class action case of *Williams v. Sprint/United Mgmt. Co.* is a landmark case with respect to metadata. The plaintiffs, a class of over 1700 former employees who had been terminated in a reduction-in-force, alleged that age was a determining factor in their terminations. The plaintiffs objected to the defendant's production in discovery of a redacted form of Excel spreadsheets that set forth various criteria concerning how individuals were selected for the reduction-in-force. "Defendant, prior to producing the electronic versions of the Excel spreadsheets, had utilized software to scrub the spreadsheets to remove the metadata."[399] The Court noted that "when I talk about electronic data, that includes the metadata."[400] After a thorough review of metadata and the relevant Sedona Principles, the Court held that:

> [W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, [FN68] the producing party should produce the electronic documents with their metadata intact, unless the party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order. [FN69] The initial burden with regard to the disclosure of the metadata would therefore be placed n the party to whom the request or order to produce is directed. The burden to object to the disclosure of metadata is appropriately placed on the party ordered to produce its electronic documents as they are ordinarily maintained because that party has access to the

metadata and is in the best position to determine whether producing it is objectionable. Placing the burden on the producing party is further supported by the fact that metadata is an inherent part of an electronic document, and its removal ordinarily requires an affirmative act by the producing party that alters the document.[401]

> FN68. This same reasoning would apply if the court ordered a party to produce the electronic documents as an "active file" or in their "native format."
>
> FN69. The same principle may apply when a party *requests* electronic documents be produced as they are maintained in the ordinary course of business, as an "active file," or in their "native format."

The approach used by the *Williams* Court, at least when it comes to the *preservation* of electronic data, virtually mandates the use of a collection process that does not alter or destroy the metadata. To the extent it becomes a model for other courts, employees combing through their electronic files using the computer's operating system may become a thing of the past.

§ 9.4   Employing a Defensible Process

A common thread in the spoliation cases discussed above is that the responding party was unable to convince the Court that its electronic discovery process was thorough and reasonable under the circumstances. It is black letter law that a party must take reasonable steps to preserve potentially relevant evidence when faced with pending litigation. When discussing electronic data, many commentators have noted that a litigant must suspend its normal document retention practices, which may call for the intentional deletion of electronic data (or paper documents, for that matter) as part of the normal course of business:

> The scope of a party's preservation obligation can be described as follows: Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents.[402]

Unlike paper documents, however, a company that uses computers destroys electronic data, *whether or nor it ceases the intentional deletion of files*. A computer will overwrite deleted files as part of its ordinary operation. Indeed, the simple act of turning on a computer can alter hundreds of files, including changing the metadata associated with files. As a result, the suspension of a party's document retention policies will not suspend the destruction of electronic data. Indeed, when it comes to electronic data, a party should take immediate steps to *preserve* data that is potentially relevant to the litigation. In other words, a litigant must take affirmative steps to preserve electronic data that may be relevant to pending litigation.

Of course, it is not reasonable to assume that a litigant will stop using computers in the context of its business, just so that potentially relevant information is preserved. In the past, a litigant at the outset of litigation would often send out an email to

employees, notifying them of the pending litigation. As highlighted above, however, this does not satisfy the litigant's preservation obligations; "[I]n short, it is *not* sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information."[403] Fortunately, however, with the advent of EnCase Enterprise Edition, technology is readily available to efficiently search and preserve electronic data contained on hard drives, servers, and other types of media, with minimal disruption of the litigant's business operations. For example, if a litigant becomes aware that litigation is likely to be commenced against it, it can use its network-enabled computer forensics capability to search its hard drives and servers in order to identify the drives on which information regarding that vendor is located. Thus, a litigant can, at the outset of litigation, significantly narrow the scope of the universe of potentially relevant data, thereby saving time and money, while concretely meeting its preservation obligations:

> [Along with cataloging any later-created documents in a separate electronic file, creating a forensic] mirror-image of the computer system taken at the time the duty to preserve attaches (to preserve documents in the state they existed at that time), creates a complete set of relevant documents.[404]

By preserving forensic images of the relevant electronic files, hard drives or servers, a litigant can blunt any subsequent charges of spoliation of evidence (which arise all too frequently in the context of electronic evidence). Indeed, a litigant may be able to continue to operate its automatic deletion systems, provided it has first preserved the potentially relevant data.

A recent case that highlights the benefits of employing a defensible process is *Williams v. Massachusetts Mutual Life Insurance Company,*[405] in which the plaintiff alleged the existence of an email that "'spelled out' a policy or practice by MassMutual of using disciplinary actions as a pretext for terminating minority employees."[406] When MassMutual did not produce the email, plaintiff filed a motion seeking "to have the court appoint a 'neutral' forensic computer expert to inspect Defendants' computer hard drives and/or electronics communication system in an attempt to recover the . . . e-mail message which he claims exists."[407] In refusing what the Court described as "an intrusion into an opposing party's information system," the Court noted that MassMutual had already performed its own computer forensics search and collection effort in response to the litigation.[408] The affidavit that MassMutual had submitted in support of its response to plaintiff's motion stated in part as follows:

> 2. Robert Bell is a member of the team of information security professionals [at MassMutual]. . . Mr. Bell has performed over seventy-five (75) investigations using Encase, the standard computer forensics software used by law enforcement and corporate security departments.
>
> 3. At the request of counsel for MassMutual, Mr. Bell . . . used Encase to search the hard drives of all personal computers assigned by MassMutual to the [relevant MassMutual

employees] from 2002 to the present, the e-mail boxes of [those employees] and relevant files on a local area network on which human resources personnel can store documents electronically.[409]

In contrast to the responding party's position in the *MassMutual* case, the defendant in *Mudron v. Brown & Brown, Inc.*[410] found itself in the unenviable position of being forced to allow the plaintiff's computer forensic expert to access the defendant's computers. The plaintiff "filed a motion for discovery sanctions and other relief alleging that he has been consistently denied electronic data."[411] The Court ordered that the defendant, who had presumably not conducted a computer forensic examination itself, had to allow plaintiff's computer forensic expert to access defendant's "computer drives to obtain forensic images."[412]

The recent high-profile case between Morgan Stanley and Ron Perelman concerning the sale of Sunbeam to Coleman[413] graphically illustrates the perils of failing to employ a defensible electronic data collection and preservation approach. In this fraud case, Morgan Stanley collected electronic documents itself, using software it had developed in-house, with dire consequences:

> [A Morgan Stanley employee] reported that . . . she and her team had **discovered that a flaw in the software they had written** had prevented [Morgan Stanley] from locating all responsive e-mail attachments. [She also] reported that [Morgan Stanley] discovered . . . that the date-range searches for e-mail users who had a Lotus Notes platform were flawed, so there were at least 7,000 additional e-mail messages that appeared to fall within the scope of [existing orders] . . .[414]

The judge viewed Morgan Stanley's failures as intentional. As described on the front page of the *Wall Street Journal*:

> As a result of what she described as Morgan Stanley's 'bad faith' actions, Judge Elizabeth Maass made an extraordinary legal decision: She told the jury it should simply assume the firm helped defraud Mr. Perelman.
> *   *   *   *   *
> Morgan Stanley is in serious trouble because of the way it mishandled an increasingly critical matter for companies: handing over email and other documents in legal battles. Lawsuits these days require companies to comb through electronic archives and are sometimes won or lost based on how the litigants perform these tasks.[415]

As of May 2005, Morgan Stanley was appealing the jury verdict, which totaled over $600 million of compensatory damages, and over $800 million of punitive damages. The lesson of the *Morgan Stanley* case is that using a "black-bag" approach that can't be explained to the Court and the other side – and hasn't been thoroughly tested or vetted in court – is unacceptable and unwise.

§ 9.5   Cost-Effective Searching of Data

Contrary to the assumptions of many, for a company with a network-enabled computer forensics capability, the cost of creating forensic images is nominal.   In addition to efficiently fulfilling its preservation obligations under the Federal Rules – including if necessary with respect to deleted files and metadata – a litigant with a networked computer forensics capability actually achieves numerous efficiencies by searching for relevant data and creating forensic images of the relevant machines. As noted by Judge Scheindlin of the Southern District of New York:

> Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved. This makes no sense. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.[416]

From a single network workstation, a litigant with EnCase® Enterprise Edition can simultaneously target several of its workstations on its network and within minutes view metrics on the size and types of files on a target workstation, conduct keyword searches for, and retrievals of, key documents, copy documents, and if necessary, image a target hard drive.   As a result, the litigant can efficiently identify responsive information, and can rapidly search any such data for privileged material, thereby saving it countless attorney hours (and the resulting expense) associated with traditional paper document review and the creation of privilege logs. In short, network-enabled computer forensics is fostering a revolution in terms of the feasibility of large-scale investigations. For instance, in a recent matter involving due diligence investigation for a merger and acquisition, enterprise computer forensics technology was effectively employed to search more than 5,000 computers distributed in dozens of locations worldwide in only four weeks.[417] The consultants involved completed the effort at a fraction of the costs of less advanced processes.

This contrasts with the approach taken by some litigation support specialists, who collect data from systems in the same general manner as any IT administrator would, by making logical copies of the data, often using the native software running on the target systems to acquire the data. At least one court has identified this approach as "minimalist," while noting that a computer forensics process is "more thorough."[418] A second common "minimalist" procedure involves simply asking the end users at an organization to provide all emails and electronic documents responsive to specific parameters, with little or no thought toward the proper collection, logging, and authentication of those documents, not to mention adequate employee compliance with the requests themselves. While these methodologies are not technically complicated, they are exceedingly vulnerable to challenges regarding the authenticity and completeness of the collected data.   When a "minimalist" non-forensic approach to collecting and analyzing computer data is employed, the proponent of that evidence faces the following risks and liabilities:

- The searched data is not thorough and complete
- The produced data cannot be properly authenticated
- Key metadata (file access times, modification dates, file origin and authorship info, etc.) will not be collected or correlated
- Data is not properly preserved and often inadvertently destroyed or altered
- Efforts to conceal or delete data will not be identified or remediated
- Counsel cannot demonstrate best practices and good faith compliance
- The investigation is expensive, untimely and highly disruptive of the responding company's business operations

In addition to the proper preservation and authentication of computer evidence, dozens of recently reported decisions (in addition to thousands of non-reported cases) dramatically demonstrate how critical electronic evidence is routinely identified when accurate and thorough computer forensics protocols are employed. A sampling of two published cases illustrates the growing frequency and import of computer forensics investigations.

In *Philip Morris USA, Inc. v. Otamedia Ltd.*[419], a computer forensic investigation was instrumental in establishing trademark infringement and unfair competition. In *Philip Morris*, the computer forensics expert established that the defendant improperly employed certain Internet domain names and manipulation of search engines to improperly sell plaintiff's products. Additionally, a separate computer forensics investigation successfully impeached the defendant's claims that the wrongful sales comprised of "merely a fraction" of the products sold, as the investigation revealed that the sales data produced by the defendant had been electronically manipulated through computer programming formulas specifically created to produce fraudulent results. When confronted with the computer forensics investigation results, the defendant conceded that its sales data was unreliable, and likely fraudulent.

In *People v. Superior Court*[420], a computer forensic investigation established that the defendant created five antedated letters on his computer. The investigation revealed that the letters — dated September 1, 1999, September 10, 1999, and November 17, 1999 — were actually created on March 9, 2000 in an elaborate attempt to backdate a contract and provide false information to investigators. As a result of the computer forensics evidence, the defendant was charged with perjury and intentionally offering falsified documents pursuant to a federal subpoena.

A common thread in each of these investigations is that, without computer forensics being used, rather than "minimalist" non-forensic methods, none of the dispositive evidence would have been identified, not to mention properly preserved and authenticated. As such, it is abundantly clear that computer forensics represents best practices for the collection and analysis of such data, and that counsel and their clients are at a severe disadvantage when computer forensics is omitted from their e-Discovery processes.

§ 9.6 Cost-Shifting

One of the bigger issues with respect electronic discovery is: who should pay for it? It has long been common practice for parties responding to discovery requests to argue that electronic discovery is too costly, and that the requesting party should therefore be required to pay the costs. Judge Scheindlin, in a series of opinions in the *Zubulake v. UBS Warburg* dispute,[421] set forth a new standard to be used in determining the propriety of cost-shifting. The plaintiff was a former highly-paid employee of defendant, and brought suit alleging gender discrimination, failure to promote, and retaliation. To support her claim, the plaintiff sought discovery of emails relating to her that were sent to or from five employees of defendant. The evidence resided only on defendant's back-up tapes, and retrieval was expected to be costly and time-consuming. The court stated that "[b]ecause it apparently recognizes that Zubulake is entitled to the requested discovery, UBS expends most of its efforts urging the court to shift the cost of production to 'protect [it] . . . from undue burden or expense.'"[422] Judge Scheindlin commented:

> The first question, however, is whether cost-shifting must be considered in every case involving the discovery of electronic data, which – in today's world – includes virtually all cases. In light of the accepted principle . . . that electronic evidence is no less discoverable than paper evidence, the answer is "No." The Supreme Court has instructed that "the presumption is that the responding party must bear the expense of complying with discovery requests . . ."
>
> *   *   *   *   *
>
> Many courts have automatically assumed that an undue burden or expense may arise simply because electronic evidence is involved. This makes no sense. Electronic evidence is frequently cheaper and easier to produce than paper evidence because it can be searched automatically, key words can be run for privilege checks, and the production can be made in electronic form obviating the need for mass photocopying.[423]

Judge Scheindlin held that if the data in question is accessible, it is not even appropriate to consider cost-shifting. For inaccessible data, Judge Scheindlin set forth a seven-factor balancing test that is significantly less likely to result in cost-shifting than previous tests.[424] In addition, the *Zubulake* line of cases eviscerates the argument that reviewing voluminous electronic evidence is too time-consuming or expensive: "once the data has been restored to an accessible format and responsive documents located, cost-shifting is no longer appropriate. . . . The point is simple: technology may increasingly permit litigants to reconstruct lost or inaccessible information, but once restored to an accessible form, the usual rules of discovery apply."[425]

Other federal courts have explicitly followed *Zubulake* with respect to the cost-shifting issue.[426] The import of *Zubulake* is clear: litigants can no longer count on being able to shift costs when electronic discovery is in issue.[427] Indeed, when it comes to searching and collecting computer data, as the Second Circuit has noted, "[t]he

technology . . . is constantly and rapidly changing."[428] As a result, a hard-and-fast rule in favor of cost-shifting makes no sense. As technology develops, even the recovery of "inaccessible" data may become inexpensive and commonplace. A recent New York case, *Weiller v. New York Life Insurance Co.,*[429] highlights the fact that litigants can no longer count on being able to shift costs, and that alleging high electronic discovery costs is unlikely to forestall discovery. According to the Court:

> [Plaintiff seeks] "[a]ll databases, electronic material, tape media, electronic media, hard drives, computer disks and documents" . . . **this request is proper, in light of today's technological realities** (e.g, *Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309 (S.D.N.Y. 2003)).

> Defendants attest that preservation of computer hard drives under the preservation order issued in the MDL resulted in a cost to defendants of more than $1,000,000.00. The court is not insensitive to the cost entailed in electronic discovery, and would, at the appropriate juncture, entertain an application by defendants to obligate plaintiff, the requesting party, to absorb all or a part of the cost of the e-discovery it seeks, or will seek, herein. . . . However, **the court will not constrain the production of possibly relevant evidence on account of the later need to allocate the cost."**[430]

Although the impact of the *Zubulake* decision has been widespread, a few state courts have neglected to follow it on state law grounds. In *Lipco Elec. Corp v. ASG Consulting Corp.*[431], defendant ASG Consulting objected to certain electronic discovery requests on the grounds that "extracting this information from its computer hard drive or back-up tapes would be extremely difficult, time consuming and expensive, "due to the customized, non-commercial software used to create the information. The New York state court analyzed cost-shifting as follows:

> [C]ost shifting of electronic discovery is not an issue in New York since the courts have held that, under [New York law], the party seeking discovery should incur the costs incurred in the production of discovery material need only determine whether the material is discoverable and whether the party seeking discovery is willing to bear the cost of production of the electronic material.
> *   *   *   *   *
> Until such time as [the plaintiffs] express a willingness to pay the costs to be incurred for the production of this data, the court will not direct its production.

Similarly, a California court relied on state law in deciding *Toshiba Am. Elec. Components, Inc. v. The Superior Court of Santa Clara County.*[432] The *Toshiba* case concerned the production of relevant evidence contained on more than 800 backup tapes and who should bear the costs of retrieving the data. The Court decided the case solely on California state-law grounds, referenced California Code of Civil Procedure Section 2031, [433] and stated that "our Legislature has identified the expense of translating data compilations into usable form as one that, in the public's interest, should

be placed upon the demanding party."[434] The Court stated that the requesting party could seek a protective order or file a motion to compel production if asked to pay costs that it finds unreasonable and unnecessary. The Court indicated that data sampling would be an appropriate test for determining necessity. Importantly, however, the *Toshiba* Court noted at the outset of its analysis that the parties did not dispute that the backup tapes constituted "data compilations" within the meaning of Section 2031(g)(1); whether other types of computer data, such as emails residing on an active server, would be viewed as "data compilations" is questionable. Indeed, even if Section 2031(g)(1) applies to a particular category of data, "the demanding party [must] bear only its *reasonable* expense and then only when translation is *necessary* to obtain usable data."[435] As a result, *Toshiba* is likely to impact only those cases in which back-up tapes or other thorny storage media are used.

§ 9.7 A Few Procedural Models

In addition to cost issues, computer evidence discovery in civil litigation has also been hampered in the past by a lack of streamlined procedural mechanisms to access computers in the custody or control of opposing litigants or other third parties. Unlike government investigators, who can often seize computers pursuant to warrant without advance notice, a civil litigant often gains accesses to opponent's computer systems only after weeks of protracted objections and discovery motions. The following five decisions each provide differing procedural models that provide excellent guidance in developing a electronic evidence discovery plan.

Simon Property Group

In June 2000 an Indiana U.S. District Court issued an order articulating a detailed discovery protocol for the examination of computers to recover relevant documents, including deleted files. In *Simon Property Group v. mySimon, Inc.*,[436] the court issued an order appointing Seattle-based Computer Forensics, Inc., (CFI) as an officer of the court and directing that CFI generate mirror images of 8 designated computers. The Court issued the order after the Plaintiff brought a motion to compel access to computers in the possession of defendants, who objected to making their computers available for forensic analysis. The following are some key portions of the *Simon Property* Court's order:

- The Court first ordered the plaintiff to select and agree to pay a computer forensics expert to serve as an officer of the court and ordered the defendants to identify all computers in question that may contain relevant documents. The Court also instructed the parties to meet and confer to draft a proposed order addressing the various details of the inspection process, objections and the transfer of information.

- When the parties failed to agree on a framework, the Court ordered that CFI would carry out the inspection and copying of data from defendant mySimon's designated computers. The Court instructed that all communications between CFI and plaintiff's counsel take place either in the presence of defendant's counsel or through written or electronic

communication with a copy to defendant's counsel.

- The Court mandated that within 14 days of the order CFI was "to inspect defendant's designated computers and create an exact copy or 'snapshot' of the hard drives of those computers." The Court noted that the inspection order did not apply to mySimon's computers and servers that actually provide defendant's Internet shopping services and instructed that the inspection be carried out in a manner minimizing disruption of and interference with mySimon's business, and that mySimon and its counsel shall cooperate in providing access to the designated computers.

- The Court mandated that within 28 days of the order CFI: 1) "recover from the designated computers all available word-processing documents, incoming and outgoing electronic mail messages, PowerPoint or similar presentations, spreadsheets, and other files, including but not limited to those files that were 'deleted'" from the 8 separate computers designated by defendants; 2) "provide such documents in a reasonably convenient form to defendant's counsel, along with, to the extent possible, (a) information showing when any recovered 'deleted' files were deleted, and (b) information about the deletion and the contents of deleted files that could not be recovered."

- The Court ordered that within six weeks of the order; 1) CFI "shall file a report with the court setting forth the scope of the work performed and describing in general terms (without disclosing the contents) the volume and types of records provided to defendant's counsel," and; 2) mySimon's counsel shall review the records for privilege and responsiveness, shall appropriately supplement their response to discovery requests, and shall send by overnight delivery to plaintiff's counsel all responsive and non-privileged documents and a privilege log reflecting which documents were withheld pursuant to the attorney-client privilege or work product immunity.

- The Court also directed that within 30 days after the final resolution of the case, CFI shall destroy the records copied from the designated computers and shall confirm such destruction to the satisfaction of mySimon.

Simon Property demonstrates that a large-scale computer forensic analysis can be performed within a reasonable period of time. Unlike the *Alexander v. F.B.I.* case, the EnCase process was utilized to carry out the order of the *Simon Property* court.[437] Additionally, the appointment of a single computer forensic consulting firm to act as special master is another important trend in civil litigation that better serves judicial economy and efficiency. The alternative of each party retaining separate partisan computer forensic experts only invites prolonged litigation through objections and extensive motions, whereas a single expert acting as special master can expedite the process by retaining custody of the evidence while providing the producing party an orderly means to address any claims of privilege. Further, with the computer forensic expert serving as a special master or officer of the court, any attorney-client or other

privileges would not be waived by virtue of a computer forensic image of the drives being made.

Trigon Insurance

Trigon Insurance Company vs. United States[438], employs much of the Simon Property model, but involves an important element of cost-shifting where the producing party was shown to have deleted files in bad faith. In *Trigon Insurance*, the insurance company brought an action against the government for recovery of federal income taxes and interest assessed and collected over a seven-year period. The government retained and designated experts, under Federal Rule of Civil Procedure 26(a), to provide opinions on the taxation issues in question. While conducting their analysis and preparing reports, the experts sent and received several e-mail communications to and from the government's litigation support consultant, Analysis Group/Economics ("Analysis Group"), including several draft versions of their expert reports. Trigon requested production of all documents reviewed by the testifying experts under Rule 26(a)(2). Upon searching for responsive documents, the government determined that many of the e-mail correspondence and draft reports had been deleted, and claimed that the information could not be recovered.

Not accepting the government's position, Trigon filed a motion seeking to compel the United States to hire an independent computer forensics expert to attempt to recover the allegedly deleted documents on the various computers of the testifying experts and Analysis Group. Trigon also sought to depose the testifying experts regarding the destruction of documents. The court, citing its inherent authority to fashion a remedy concerning the discovery process, ordered the appointment of an independent computer forensics expert, to be paid by the government, to attempt to recover the deleted computer files in question. The court rejected the government's contentions that Analysis Group and the experts properly deleted the documents pursuant to their ongoing records retention policies. The court determined that the government had a duty to inform its consulting experts and litigation support firm of its duty to preserve any and all records generated or relied upon by the testifying experts.

The computer forensic examination revealed that the experts and Analysis Group deleted extensive amounts of responsive information. While the computer forensic experts retrieved a substantial amount of the deleted information, at least some of that data could not be recovered. Finding that the government had improperly spoliated evidence, the court issued evidentiary sanctions in the form of adverse inferences concerning the substantive testimony and credibility of the government's experts, as well as monetary sanctions. The court determined that the electronic documents destroyed were important in testing the substantive ability of the expert's opinions and prejudiced Trigon by impairing its ability to cross-examine the government's experts.

There are several important lessons that litigators should learn from Trigon Insurance. First, in some circumstances a party may have an affirmative duty to conduct a computer forensics examination. In this case, this duty arose when the government's expert witnesses failed to retain discoverable electronic evidence, and thus the government was obligated to foot the bill for recovery efforts of an independent

computer forensics expert. Notably, the court determined that this duty to retain electronic documents overrode existing records retention policies.

Trigon Insurance also illustrates that sanctions for spoliation of electronic evidence should be imposed by the court where it is demonstrated that such spoliation of computer files took place. Additionally, while computer forensics examinations are essential for many reasons, *Trigon Insurance* illustrates the necessity of the procedure in order to determine and substantiate claims of spoliation. A computer forensics expert will be able to identify specific evidence that has been partially destroyed, while preserving the remainder of data in question through proper handling.

Rowe Entertainment v. The William Morris Agency

Rowe Entertainment v. The William Morris Agency[439], provides a good alternative model to Simon Property, while at the same time candidly addressing some of the technical challenges presented when trying and sleuth through several years of an organization's e-mails, all while dealing with privileged information. The protocols issued by the court are as follows:

> "Initially, the plaintiffs shall designate one or more experts who shall be responsible for isolating each defendant's e-mails and preparing them for review. The defendants shall have the opportunity to object to any expert so designated. The expert shall be bound by the terms of this order as well as any confidentiality order entered in the case.
>
> With the assistance and cooperation of the defendants' technical personnel, the plaintiffs' expert shall then obtain a mirror image of any hard drive containing e-mails as well as a copy of any back-up tape. The plaintiffs may choose to review a sample of hard drives and tapes in lieu of all such devices.
>
> Plaintiffs' counsel shall formulate a search procedure for identifying responsive e-mails and shall notify each defendant's counsel of the procedure chosen, including any specific word searches. Defendants' counsel may object to any search proposed by the plaintiffs.
>
> Once an appropriate search method has been established, it shall be implemented by the plaintiffs' expert. Plaintiffs' counsel may then review the documents elicited by the search on an attorneys'-eyes-only basis. The plaintiffs may choose the format for this review; they may, for example, view the documents on a computer screen or print out hard copy. Once plaintiffs' counsel have identified those e-mails they consider material to this litigation, however, they shall provide those documents to defendants' counsel in hard copy form with Bates stamps. The plaintiffs shall bear all costs associated with the production described thus far. However, the defendants shall pay for any procedures beyond those adopted by the plaintiffs, such as the creation of TIFF files.

Defendants' counsel shall then have the opportunity to review the documents produced in order to designate those that are confidential and assert any privilege. Any purportedly confidential or privileged document shall be retained on an attorneys'-eyes-only basis until any dispute about the designation is resolved. The fact that such a document has been reviewed by counsel or by the expert shall not constitute a waiver of any claim of privilege or confidentiality.

Should any defendant elect to review its database prior to production, it shall do so at its own expense. In that event, the defendant shall review those hard drives and back-up tapes selected by the plaintiffs and shall create copies from which privileged or confidential and unresponsive material has been deleted. The defendant shall then provide plaintiffs' counsel with each "redacted" hard drive or tape, together with a privilege log identifying the documents removed. The process would then continue as described above."

This process would be more efficient than the Simon Properties model. However, the "attorney's eyes only" provision is rather intrusive and may still compromise privileged information, despite the court's "no waiver" ruling. While this model may not be appropriate where privileged data may be more prevalent, it provides a good alternative to Simon Properties.

U.S. v. Regan

In *U.S. v. Regan*,[440] a federal district court grappled with the issue of how to permit computer forensic imaging of hard drives and media used by the defendant's attorneys. The defendant allegedly had tried to sell classified information to Iraq, Libya, and China, and had been indicted on several charges of attempted capital espionage. After finding non-privileged information in the defendant's jail cell, and having reason to suspect that the information was composed by defendant using the Court's computers that had been provided by the government for use by defendant's attorneys in the Courthouse Secure Classified Information Facility, the prosecution filed a motion to image a hard drive and certain floppy disks. The court, in granting the prosecution's motion, set forth a detailed procedure intended to protect any applicable attorney-client privilege. The court did not allow the FBI to conduct the search. Rather, the court referred the matter to a magistrate judge, with the instruction that a court-selected neutral computer forensics expert (with proper security clearances) should be hired to image the hard drive and search for four specific items. If the expert were to find the specified items, he or she would then provide the information in electronic and hard copy to the magistrate judge for review. The magistrate judge would report the expert's findings to all counsel and to the District Judge. The imaged hard drive was to be maintained in a secure location until a verdict was reached in the case, at which time the prosecution could seek leave to conduct a further search.

The *Regan* case is an excellent example of how concerns regarding overbroad searches or potential privilege issues can be resolved by using the power of computer

forensic software to narrow the items searched for, and how a neutral expert can be used to protect the concerns of both parties.

Each of the cases outlined above illustrate that accessing a computer system in question may involve several months of legal wrangling, with critical evidence possibly being overwritten in the meantime. As such, the following are some practice points that counsel should consider when it becomes clear that computer evidence is relevant to a case at hand.

- Issue a demand letter requesting preservation of all relevant computer evidence. An example form of a preservation letter is included below.
- Consider immediately proposing a stipulation to the opposing party along the lines of the *Simon Property* case. Such a measure would immediately enable an expert to access and image the computers in question and retain sole custody of the forensic evidence until the opposing party has had a full opportunity to review documents identified by the expert as relevant and address any objections with the court. For the producing party, the alternative may well be an order compelling production of hard drives and back-up tapes, which may contain confidential or proprietary information. See, for example, the case of *Renda Marine, Inc. v. U.S.,* in which the court ordered the government to produce, at its expense, back-up tapes and the hard drive of the relevant contracting officer, for inspection by the plaintiff's computer forensic expert, noting that plaintiff's "technicians can retrieve deleted email and search hard drives and email back-up tapes . . . limit[ing] their retrievals to document[s] and email relevant" to the case and the plaintiff.[441]
- Any proposed stipulation should include a provision that the parties preserve the integrity of all evidence contained on computer systems in the interim period prior to the inspection by the computer forensic experts. (*See, Illinois Tool Works, Inc. v. Metro Mark Products, Ltd*[442]). Ideally, preserving the integrity of the computer evidence means that the computers are not operated at all. While parties will invariably consider such a provision to be burdensome, this underscores that the relevant computer systems should be immediately identified and imaged at the outset of the litigation.
- If the opposing party is uncooperative, the court could consider evidentiary and/or monetary sanctions if an order similar to what you originally proposed for a stipulation is ultimately adopted after a noticed motion.
- Any objections to producing computers for inspection on burden or cost under the grounds set forth in *Alexander v. F.B.I.* should be countered with a discussion of more recently available computer forensic tools that provide significantly increased efficiency to the process.
- In particularly sensitive cases, counsel should consider bringing an *ex parte* motion for a temporary restraining order preventing the operation of relevant computer systems until they can be accessed and imaged.
- If the producing party is found to have engaged in improper deletion of computer evidence, request that the court shift the expert costs to the

party that caused the data deletion.

- A disadvantage to the special master approach is that counsel seeking the discovery may never have the opportunity to review the EnCase evidence file created by the special master expert to search for relevant information that the expert may have missed. Consider seeking permission from the court to obtain a copy of the evidence file for your own review and analysis.

§ 9.8 Example Form Letter Demanding Preservation of Computer Evidence

A letter demanding preservation of computer evidence is an important tactic in civil litigation, where a discovery order to access an opponent's computer systems may take weeks. Sending such a letter is important to establish notice that the recipient has a legal duty to preserve electronic evidence relevant to the case. Absent receiving such a letter, a company may be free to destroy electronic evidence in the normal course of business, especially if that company destroys such information pursuant to an established and ongoing electronic records retention policy.

Below is an example of the type of letter that should be utilized in the context of civil litigation in order to establish a duty and obligation on the part of the recipient to retain and preserve the identified electronic evidence. Seeking an emergency restraining order prohibiting such destruction is an even stronger measure, and should be considered in appropriate circumstances.

<DATE>

_____
_____
_____

Re: **Jane Doe v. XYZ Company**

Dear Sir or Madam:

As critical evidence in this matter exists in the form of electronic data contained in the computer systems of XYZ Company, this is a notice and demand that such evidence identified below in paragraphs 2 through 6 must be immediately preserved and retained by XYZ Company until further written notice from the undersigned. This request is essential, as a paper printout of text contained in a computer file does not completely reflect all information contained within the electronic file. Additionally, the continued operation of the computer systems identified herein will likely result in the destruction of relevant evidence due to the fact that electronic evidence can be easily altered, deleted or otherwise modified. The failure to preserve and retain the electronic data outlined in this notice constitutes spoliation of evidence and will subject XYZ Company to legal claims for damages and/or evidentiary and monetary sanctions.

1. For purposes of this notice, "Electronic Data" shall include, but not be limited to, all text files (including word processing documents), spread sheets, e-mail files and information concerning e-mail (including logs of e-mail history and usage, header information and "deleted" files), internet history files and preferences, graphical image files (including ".JPG, .GIF, .BMP and TIFF" files), data bases, calendar and scheduling information, computer system activity logs, and all file fragments and backup files containing Electronic Data.

2. Please preserve and retain all Electronic Data generated or received by _____.

3. Please preserve and retain all Electronic Data containing any information about _____.

4. Unless and until all potentially relevant Electronic Data has been preserved, XYZ Company must refrain from operating (or removing or altering fixed or external drives and media attached thereto) standalone personal computers, network workstations, notebook and/or laptop computers operated by _____.

5. XYZ Company must retain and preserve all backup tapes or other storage media, whether on-line or off-line, and refrain from overwriting or deleting information contained thereon, which may contain Electronic Data identified in paragraphs 2 through 4.

6. In order to alleviate any burden upon XYZ Company, the undersigned is prepared to immediately enlist the services of a computer forensic expert to image and examine all drives and media in the custody and control of XYZ company which may contain Electronic Data relevant to this matter. This can be accomplished in a manner outlined by the Court in *Simon Property Group v. mySimon, Inc.* 94 F.R.D. 639 (SD Ind. 2000), to ensure retention of all privileges while properly processing computer evidence as mandated by the court in *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*, 167 F.R.D. 90 (D.C. Col., 1996).

Please contact me if you have any questions regarding this request.

Sincerely,

_____

§ 9.9 Resources for Electronic Evidence Discovery

Computer forensics and electronic discovery in civil litigation is a quickly growing field. There are some important resources dedicated to this specific discipline, including the following:

- "Digital Discovery and e-Evidence" is a monthly publication published by Pike and Fischer, dedicated to computer forensics and electronic evidence discovery. The publication features articles, recent case synopsis, and other important developments involving electronic evidence discovery at the trial court level. Subscription info: (800) 255-8131 http://www.pf.com/ddeePD.asp

- http://californiadiscovery.findlaw.com/electronic_data_discovery.htm is a site maintained by a former San Francisco County Superior Court Commissioner. The site features a wealth of information, references, and links on electronic evidence discovery in California and other jurisdictions.

- www.kenwithers.com is a site maintained by a Federal Judicial Center research attorney. The FJC is dedicated to providing continuing education to the federal court bench and conducting research into emerging areas of the law of evidence and court procedure. Mr. Withers' is assigned by the FJC to the area of electronic evidence discovery, and his site is similarly dedicated to the subject, with numerous power point slides presented to judicial conferences, as well as several other links and resources.

- <u>Overly On Electronic Evidence In California</u> is a notable treatise on the subject, written by Michael Overly, and published by the West Group.

- <u>www.encase.com</u> The Guidance Software website contains numerous resources, including legal resources, message boards, whitepapers and other reference materials and links.

10

Employee Privacy and Workplace Searches of Computer Files and E-mail

§ 10.0 Overview

Electronic mail is all but firmly established as the primary form of workplace communication. In recent years, employment litigation and other cases involving alleged workplace misconduct routinely involve evidence in the form of e-mail or other computer-generated records created in the course of business. With most of a typical company's "documents" and other information existing in electronic form, employer monitoring, and in many cases, seizure of these files is becoming commonplace. In considering employee privacy in the context of monitoring of e-mail and other computer files, it is important to note that the rights of government employees may differ in many aspects from their counterparts in the private sector. For instance, the United States Constitution's Fourth Amendment restrictions on unreasonable searches and seizures afford potential additional protections for government employees who are subject to monitoring of their e-mail and computer files. As the Fourth Amendment only acts as a check on government actions,[443] the scope of the Amendment's protections for government workers' e-mail is limited, if at all, in application to non-government workers. Conversely, employer manuals and other written information setting forth company policy largely govern privacy rights in the commercial workplace. As such, workplace privacy issues in the private and public sector are addressed separately in this section.

§ 10.1 Employee Monitoring in the Private Sector

While an employer is generally prohibited by law from intercepting e-mail messages being transmitted over the internet,[444] monitoring employee e-mail, stored computer files, including Internet history files, are generally permitted in most states without written consent or notification. Connecticut and Delaware each require employers to obtain written consent from their employees or provide written notice to their employees before any such monitoring can take place.[445] A bill for a similar statute, dubbed the "Notice Electronic Monitoring Act" (S.2898) was introduced in Congress in July 2000, but never made it out of committee. Counsel should remain vigilant in monitoring any developments in the law at both the state and federal level.

In considering the propriety of employer monitoring of employee e-mail and computer files, the primary question concerns whether and to what extent written agreements and policies addressing such monitoring are in place. Written notification that their e-mail and computer files are subject to access by the employer generally governs whether an employee can claim a reasonable expectation of privacy in those files. These rules, in the form of written e-mail, Internet use and stored computer file policies, must limit employees' privacy expectations in their electronic communications

and stored computer files, but must do so consistently with laws that prohibit interceptions of electronic communications in transit. Moreover, it is important that these rules and policies are expressly acknowledged and consented to in writing by the employee.

<u>Balancing of Interests</u>

In determining an employee's privacy interests, the courts will balance the employer's interest against the reasonable privacy rights of the employee. Preventing theft of intellectual property and policing unauthorized activity are generally seen as compelling interests justifying an employer's reasonable monitoring activities. [446] Additionally, employers may potentially be held liable for an employee's online misconduct where the company's computer networks are the means for the offense.[447] Some legal experts have hypothesized that where an employee utilizes an employer's computer systems to engage in such activities as hacking, on-line harassment or copyright infringement, an employer may be liable for those activities.[448] In *Blakey v. Continental Airlines,[449]* the New Jersey Supreme Court found that Continental Airlines could be potentially liable for an employee's harassing postings on an internet bulletin board hosted by the airline for its employees. In reversing a lower court's order dismissing Blakey's complaint, the Court reasoned that since the company provided the Internet forum for employees' use, Continental had a duty to monitor e-mail postings to ensure that employees were not harassing one another. In another leading decision in this area, *Smyth v. Pillsbury Co.*, the Pennsylvania U.S. District Court determined that "a company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments."[450] Thus, with the employers' interest in preventing theft and unauthorized activity coupled with the possibility of third-party liability for *failing* to monitor the employees' on-line conduct usage, e-mail and Internet usage monitoring of employees is a critical, if not mandatory necessity for employers in the private sector.

Still, employers are wise to ensure that proper written notifications are in place. The case of *Muick v. Glenayre Electronics[451]* upheld the propriety of an employer's search of its employee's hard drive, but predicated the reasonableness on the existence of written notifications and existing company computer use polices. The Court's rationale in *Muick* is consistent with an emerging trend requiring these policies. Notably, the decision implies a different result had such written notifications not been in place.

While not clearly requiring a policy, in *United States v. Bailey*,[452] a federal district court in Nebraska held that the defendant, who signed on to his work computer through a "splash" screen that included a consent to search, "had no expectation of privacy in the work computer owned by someone else because every time he accessed the work computer he physically acknowledged that he was giving consent to search the computer. Such repeated warnings about consent to search, followed by such repeated acknowledgments, categorically and without more defeat [defendant]'s claim of privacy."[453] Thus, under the *Bailey* court's reasoning, an employer that requires its employees to sign on through a "consent to search" screen or warning is on solid grounds when conducting searches of an employee's hard drive.

<u>UK Approach</u>

In the UK, monitoring of employees has been addressed through national regulations. In 2003, the Employment Practices Data Protection Code, Part 3, was issued under the Data Protection Act of 1998. As in the U.S., real-time monitoring is generally forbidden. However, access to stored emails that have been opened is not prohibited.[454] If an employer wishes to monitor electronic communications, it should "establish a policy on their use and communicate it to workers."[455] The policy should set forth clearly the extent, if any, to which employees can use email or the Internet for non-business purposes.[456] Finally, when monitoring emails, employers should review only address and subject, "unless it is essential for a valid and defined reason to examine content."[457]

§ 10.2 The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986 (ECPA) is a federal statute that some contend has application to an employer's workplace e-mail monitoring activities. The ECPA includes two categories relevant to this discussion: Title I prohibits interception of messages in transit,[458] while Title II prohibits access to and disclosure of stored information. The "stored information" provision under title II has been narrowly construed to only apply to information in intermediate storage incident to transmission, such as an e-mail residing on a server prior to being retrieved by the recipient. Thus, the ECPA prohibits three types of intrusions into electronic communications: intercepting messages while they are in transit, accessing information in intermediate storage incident to transmission, and disclosing information at any point in the process.[459] While the ECPA may seem to provide employees with broad protection from e-mail monitoring, the Act contains several exceptions that sharply limit its scope. First, it is apparent that Congress did not intend the ECPA to govern the relations of employees to their employers, but rather intended to regulate intrusions by unauthorized outsiders into the electronic communications of organizations. As such, most commentators believe that the ECPA does not cover workplace local area networks (LANs) and thus provides no protection for employees when they send e-mail over their workplace computer network.[460] The language in the ECPA prohibiting disclosure of electronic communications only applies to those entities that provide electronic communication services "to the public,"[461] while intra-office networks offer services only to employees. Thus, under this construction of the ECPA, any e-mail sent by employees over a nonpublic network would not be subject to the Act.

Second, even if the ECPA did apply to proprietary LANs, the Act contains an exemption allowing access to stored communications when authorized by the entity providing electronic communications services.[462] On its face, this provision allows the network provider to access any stored communication that had been sent over the network without violating the ECPA. If an employer owns the network, it could then access all communications sent by employees. In *Bohach v. City of Reno,*[463] the plaintiffs, two police officers, sought an injunction preventing the City from continuing an internal affairs investigation. In rejecting the plaintiffs' claim that the investigators' violated the EPCA by retrieving the plaintiffs' pager messages stored on the City's telephone network, the court noted that the City was the provider of the electronic

communications service used by the officers.[464] It then held that "[section] 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage. Because the City is the provider of the 'service,' neither it nor its employees can be liable under § 2701."[465]

Employers should be aware that actually intercepting e-mail messages in transit, as opposed to accessing stored communications, would likely constitute a violation of the ECPA.[466] Interception is generally defined as the act of accessing a message or preventing it from reaching its destination at any point between the time the message is sent and the time the intended recipient receives it. To date, most courts have taken a narrower view of what constitutes "interception" of e-mail, establishing that under the ECPA, interception can only occur during the fraction of a second the message is actually traveling along the wires connecting computers.[467]

Fraser v. Nationwide Mutual Insurance Co.[468] is the latest case to hold that an employer's retrieval of an employee's e-mail from post-transmission storage does not constitute an "interception" under the ECPA. In *Eagle Investment Systems Corporation v. Tamm*,[469] the court similarly determined that no "interception" occurred when an employee obtained a stored e-mail from a co-worker without his consent.

In *Steve Jackson Games, Inc. v. United States Secret Service*, the Fifth Circuit addressed the issue of whether the seizure of a computer storing private e-mail that had been sent to an electronic bulletin board but not yet read by the recipients constituted an "intercept" proscribed by Title I of the ECPA. The court determined that such a seizure was not an interception because the e-mail was not being transferred but was instead in storage incidental to transmission.[470] Other courts have reached similar conclusions regarding the definition of interception as used in the ECPA.[471] However, at least one court has since determined that the viewing of information from a secure web page in intermediate storage prior to being read by its intended recipient constitutes an "interception."[472] These rulings indicate that e-mail could almost always be seized before it reached its intended recipient without being "intercepted" and thus triggering the tough restrictions of Title I of the ECPA.

§ 10.3 Other Important Considerations for Employers

The issue of employee monitoring is complex and the employers should seek the advice of their counsel when considering the implementation of a written policy governing these issues. The following are some additional important considerations for employers:

- Employers should monitor all developments in this rapidly developing area of law. In addition to the Connecticut and Delaware statutes,[473] the California legislature passed a law that would have mandated an employee's written consent among other requirements before an employer could monitor their employees' e-mail, Internet usage and stored computer files.[474] Only the somewhat unexpected veto of Governor Gray Davis blocked the enactment of the statute. Similar bills are being considered in other states and in the US Congress.

- In any event, employers should ensure that all employees are informed and consent in writing to any such monitoring activities. Proper written consent provides an exception to almost all existing laws governing employer monitoring in the United States.
- Employers and their counsel should be mindful of cases that hold employers liable for the wrongful conduct committed by an employee through the internet/network. This adds to the equation of the employer's interests of not only protecting their intellectual property and internal resources but also being charged with a duty to prevent wrongful on-line conduct of their employees.
- Employers should be consistent and even-handed in their monitoring activities in order to avoid common law invasion of privacy claims. An employee could in theory state a claim for improper monitoring if an ordinary reasonable person would find that the circumstances involved "a substantial and highly offensive invasion of privacy."[475] For instance, a targeted, non-routine search for incriminating electronic documents to provide a pretext for the termination of an employee may be construed as unreasonable by some courts.

§ 10.4 Monitoring of Government Employees

Federal, state, and municipal employers constitute a very large sector of the U.S. economy, and the federal government has established a goal of providing e-mail to every federal agency and promoting e-mail as the preferred method of conducting government business. In addition, the federal government has instituted an aggressive telecommuting program, which has encouraged extensive use of e-mail.[476] Included within these aggressive plans for digitizing the federal workplace are equally aggressive e-mail monitoring programs. [477] Unlike their private sector counterparts, federal employees are afforded a degree of protection under the Fourth Amendment's prohibition against unreasonable search and seizures.[478] However, those protections can also be substantially limited by the implementation of written policies and agreements that reduce an employee's reasonable expectations of privacy.[479]

United States v. Simons,[480] is a notable case that directly addresses issues of the monitoring and seizure a federal employee's computer files in the workplace. In *Simons,* systems administrators of the Foreign Bureau of Information Service (FBIS) division of the CIA searched an employee's hard drive over a remote network connection after routine network monitoring detected unauthorized Internet connections from his computer to sex-related websites. The FBIS previously instituted a written policy regarding Internet usage by employees stating that employees were to use the Internet for official government business only. The policy specifically prohibited accessing unlawful material and stated that "[u]sers shall . . . [u]nderstand FBIS will periodically audit, inspect, and/or monitor the user's Internet access as deemed appropriate." The record reflects three distinct levels at which FBIS, and then the CIA Office of the Inspector General (OIG), searched and ultimately seized Simons' computer files. First, FBIS investigators performed text searches across the network, resulting in numerous sex-related keyword "hits" originating from Simons' computer. The FBIS network administrator then remotely accessed and copied files from Simons' computer

to determine the existence of unauthorized downloaded Internet files. After determining that some downloaded images appeared to be child pornography, investigators from the CIA OIG directed Simons' hard drive be seized from his office without a warrant, despite their knowledge that Simons' computer likely contained images of child pornography.

Simons contended on appeal from his conviction that the FBIS's search of his computer files stored on his hard drive in his office over the network violated the Fourth Amendment. Simons further contended that the OIG's warrantless seizure of his hard drive also violated the Fourth Amendment. The court found the remote network searches of Simons' computer to be proper because, in light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet. Notably, the appellate court declined to recognize any privacy distinction between the network-wide keyword text searches (which Simons did not contest) and the subsequent remote search and seizure of files contained on Simon's hard drive (which Simons objected to).[481]

As far as the entry into Simons' office to seize his hard drive is concerned, the court found that as Simons did have a reasonable expectation of privacy in his office, the warrantless entry and seizure of Simons' computer potentially violated the Fourth Amendment absent the applicability of a specific exception to the warrant requirement.[482] While the FBIS's written policies addressed internet usage and network monitoring, the court found that the policies did not sufficiently address privacy expectations regarding computer files stored on the hard drives and other media actually contained within the employee's office.[483] However, citing the U.S. Supreme Court decision of *O'Connor v Ortega, supra,* the court held that a government employer's interest in "the efficient and proper operation of the workplace" justified the warrantless work-related search of Simons' computer, especially since the *O'Connor* Court held that when a government employer conducts a search pursuant to an investigation of work-related misconduct, the Fourth Amendment will be satisfied if the search is reasonable in its inception and its scope. A search normally will be reasonable at its inception "when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct."[484] Such searches will be considered permissible in its scope "when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of ... the nature of the [misconduct]."[485]

Obviously, the best practice for an investigator in this situation would be obtain a warrant, if feasible, prior to physically seizing a government employee's computer, as courts outside of the Fourth Circuit may not reach many of the conclusions of the *Simons* Court. Further, this case illustrates the importance of comprehensive written policies that not only address e-mail and network activity monitoring, but also the access of stored files on the employee's computer.

Although members of the military are government employees, their expectations of privacy may be less than civilian employees. In *U.S. v. Plush*[486], the U.S. Air Force Court of Criminal Appeals held that a military officer does not have a reasonable expectation of privacy in his work computer. Plush had brought his government-issued laptop computer into a government repair facility for repair of a cracked screen. While

performing routine maintenance on the computer, the staff sergeant in charge of computer maintenance noticed unusually large files in the recycle bin and temporary Internet files, including more than 1,200 graphics files, three of which contained sexually explicit photographs. This was the basis for an authorization for a subsequent forensic analysis of the laptop and two desktop computers that were located in Plush's office disks. The forensic analysis revealed that the three computers contained nearly 4,500 sexually explicit images. In denying an appeal of a conviction of conduct unbecoming of an officer, the Court stated that "the nature of military life provides members with a minimal expectation of privacy in government property, due to government ownership, the nonpersonal nature of military offices, and the inherent right of command to inspect property under its control."[487] The Court also noted that "Air Force policy requires the monitoring of telecommunications systems, including computers; Air Force policy provides that use of such equipment constitutes consent to monitoring; and Air Force policy further requires a notice and consent log-on banner to be installed on all computers."[488] As a result, the Court held that "the appellant could not reasonably have expected a right to privacy as to his laptop computer."[489]

In *United States v. Long*,[490] a case consistent with *Plush,* the United States Navy-Marine Corps Court of Criminal Appeals held that a computer network system administrator could properly turn over information about criminal activity only if such information was found during normal system maintenance. The administrator had testified that "there was no ongoing monitoring of the network at the time and that he specifically acted at the behest of law enforcement officials in retrieving the e-mails."[491] The Court opined:

> So long as [the computer network system administrator] conducts his activities through ongoing system monitoring or confines his searches to those necessitated to ensure that the system is operating properly and that no user is abusing the system or using the system in an unauthorized manner, the system administrator can also properly turn over any evidence of criminal conduct to the authorities. Once he becomes the agent of law enforcement, however, either through conducting a search for criminal activity at their request or by permitting them to participate actively in his monitoring and administering function, he loses that special status afforded him under the law and becomes equally subject to the requirements of the 4th Amendment regarding probable cause and proper search authorization.

> We conclude that it is reasonable, under the circumstances presented in this case, for an authorized user of the Government computer network to have a limited expectation of privacy in their e-mail communications sent and received via the Government network server. Specifically, while the e-mails may have been monitored for purposes of maintaining and protecting the system from malfunction or abuse, they were subject to seizure by law enforcement personnel only by disclosure as a result of monitoring or when a search was conducted in accordance with the principles enunciated in the 4th

Amendment.

We conclude that the appellant had a subjective expectation of privacy in the e-mails sent and received on her Government computer vis-à-vis law enforcement and that this expectation of privacy was reasonable. The military judge therefore erred in denying the defense motion to suppress the e-mails at trial.[492]

NOTES

[1] U.S. Federal Rule of Evidence 1001(1); Canada Evidence Act, Chapter C-5 sections 30(12), 31.8(b).

[2] Canada Evidence Act, Chapter C-5 section 31.1.

[3] *United States v. Siddiqui,* 235 F.3d 1318 (11th Cir. 2000) (Testimony of recipients sufficient to authenticate e-mails sent by defendant). *Laughner v. State*, 769 N.E.2d 1147 (Ind.App. 2002) (AOL Instant messages authenticated by the recipient).

[4] *Authentication of Computer-Generated Evidence In the United States Federal Courts*, (1995) 35 IDEA:J.L.& Tech. 437, 439.

[5] 200 F.3d 627 (9th Cir. 2000).

[6] *United States v. Tank, supra*, 200 F.3d at 629.

[7] *Id.* at 630.

[8] *Id., citing United States v. Black*, 767 F.2d 1334, 1342 (9th Cir. 1985).

[9] *Id.* at 631.

[10] *Id.*

[11] See also, *United States v. Whitaker,* 127 F.3d 595, 601(7th Cir. 1997).

[12] 2000 WL 288443 (W.D. Mich. 2000).

[13] 167 F.R.D. 90 (D.C. Col., 1996).

[14] *Gates Rubber Co.*, *supra*, 167 F.R.D. at 112.

[15] *Id.*

[16] 127 F.3d 595 (7th Cir. 1997).

[17] *Whitaker, supra,* 127 F.3d at 600-601.

[18] *Id*. at 600.

[19] *Id.*

[20] 771 N.E.2d 710 (Ind.App. 2002).

[21] *Bone v. State, supra,* 771 N.E.2d at 716.

[22] *Id.*

[23] *Id.* at 716-717.

[24] 205 Cal.App.3d 632 (1988).

[25] *People v. Lugashi, supra*, 205 Cal.App.3d at 636.

[26] *Lugashi,* at 641.

[27] *Id.*

[28] *Lugashi,* at 640

[29] *Id.*

[30] *Id.*

[31] *Id.*

[32] 55 Conn.App. 384, 739 A.2d 311 (1999).

[33] 678 A.2d 266, 292 N.J.Super. 11, (1996).

[34] 775 A.2d 189, 191, 341 N.J.Super. 241, 245 (2001).

[35] 949 S.W.2d 93 (1997).

[36] *Id*. at 100.

[37] *Id*. at 97.

[38] *Id*. at 99.

[39] 945 P.2d 367 (1997).

[40] *Id.* at 368.

[41] *Id* at 370.

[42] *Id.*

[43] 908 S.W.2d 598 (1995).

[44] 829 F.2d 757 (9th Cir. 1987).

[45] *Id*. at 759.

[46] Additionally, *Lugashi* is clearly an important case when seeking to introduce computer-generated evidence created or maintained by third party ISPs, businesses and other institutions.

[47] *United States v. Tank*, 200 F.3d 627 (9th Cir. 2000); *Wisconsin v. Schroeder,* 2000 WL 675942.

[48] *United States v. Whitaker*, 127 F.3d 595, 602 (7th Cir. 1997).

[49] *United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988); See also, *United States v. Glasser*, 773 F.2d 1553 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite

to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records.").

[50] *United States v. Tank*, supra, at 631 fn. 5.

[51] *Wisconsin v. Schroeder,* 2000 WL 675942 (Wis.App. 2000).

[52] See <u>Bonallo</u>, 858 F.2d at 1436.

[53] See, <u>e.g.</u>, *United States v. Moore*, 923 F.2d 910, 915 (1st Cir. 1991); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990); *People v. Lugashi*, 205 Cal.App.3d 632 (1988).

[54] Council of Europe's Convention on Cybercrime, Explanatory Report, ¶ 298.

[55] See *United States v. Campos*, 221 F.3d 1143, 1147 (10th Cir. 2000); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (upholding seizure of "[a]ny and all computer software and hardware, . . . computer disks, disk drives" in a child pornography case because "[a]s a practical matter, the seizure and subsequent off-premises search of the computer and all available disks was about the narrowest definable search and seizure reasonably likely to obtain the [sought after] images").

[56] 2003 WL 21000002 (N.D.Tex. 2003).

[57] 297 F.Supp.2d 1264 (D.Or. Oct. 20, 2003).

[58] *Id*. at 1268.

[59] *Id*. at 1268-69.

[60] *Id*. at 1269.

[61] *Id*. at 1275 (emphasis added).

[62] *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 at *16 (S.D.N.Y. Jul. 20, 2004); *see also Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 280) and *Zubulake v. UBS Warburg*, 2003 WL 22410619 (S.D.N.Y., Oct. 22, 2003).

[63] *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 at *8 (S.D.N.Y. Jul. 20, 2004)

[64] For a press account of the case, see:
http://icwales.icnetwork.co.uk/0100news/0200wales/tm_objectid=14367417&method=full&siteid=50082&headline=accountant-plotted-to-cheat-employers-of---pound-1-5m-name_page.html

[65] *Id*.

[66] 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993).

[67] *Frye v. United States*, 293 F. 1013 (D.C.Cir.1923).

[68] See, *United States v. Beasley*, 102 F.3d 1440, 1448 (8th Cir. 1996) (judicial notice taken of reliability of the PCR method of DNA typing).

[69] No. 99-2362-KHV, (D. Kansas).

[70] 526 U.S. 137, 119 S.Ct. 1167 (1999).

[71] *Daubert, supra*, 509 U.S. at 592-594, 113 S.Ct. 2786.

[72] See, e.g., *United States v. Liebert,* 519 F.2d 542, 547 (3rd Cir. 1975) (holding that computer evidence was admissible in criminal trial provided that prosecution lays a sufficient foundation to warrant a finding that such information is trustworthy and the defense is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence). See also, *United States v. Weatherspoon,* 581 F.2d 595, 598 (7th Cir. 1978).

[73] *SC Magazine,* April 2001, "Test Center- GETTING THE HARD FACTS." (Testing of Computer Forensics analysis tools reported in the leading publication in the IT Security industry. EnCase receives the highest rating over the other tested programs, noting: "If you work doing forensic analysis of media on a regular basis, you must have this tool.") *See also SC Magazine,* October 2003, "Group Test 1: Data Forensics," in which EnCase received a 5-star rating -- "**VERDICT:** Sets the standard for other forensic products. Definitely the best option for professional forensics investigations."

[74] In addition to the *SC Magazine* test reviews in 2001 and 2003 noted above, EnCase has received dozens of favorable reviews and mentions in industry publications, which are available for review and download at: http://www.encase.com/corporate/news/index.shtm

[75] *The Computer Paper*, December 2002, "Sherlock Holmes Meets Data."

[76] Sonoma County, California Superior Ct. no SCR28424.

[77] *SC Magazine*, April 2001, "Test Center- GETTING THE HARD FACTS"; *SC Magazine,* October 2003, "Group Test 1: Data Forensics."

[78] 162 F. Supp. 2d 1097, 1103 (D. Alaska 2001).

[79] The final report can be obtained from the National Institute of Justice web site at http://www.ojp.usdoj.gov/nij/pubs-sum/200031.htm.

[80] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993).

[81] *State of Washington v. Leavell* (Okanogan County, Washington Superior Ct. no. 00-1-0026-8).

[82] Judicial Notice is the act of a court recognizing the existence and truth of certain facts relevant to the case at bar. Such notice excuses a party from having the burden of establishing fact from necessity of producing formal proof.

[83] "Thus, evidence describing, for example, the process of creating x-rays, photographs, tape recordings, computer generated records, radar records, or scientific surveys when coupled with evidence showing that a particular process or system produces an accurate result when correctly employed and properly operated and that the process or system was in fact so employed and operated constitutes sufficient evidence that the result is what it purports to be." Wright & Miller, Fed.Prac.& Proc. Evid. § 6830; *Notes of the Advisory Committee* regarding Rule 901(b)(9); *see also*, *People v. Lugashi* (1988) 205 C.A.3d 352 (Data collection software program presumed accurate); *People v. Mormon* (1981) 97 Ill.App.3d 556, 422 N.E.2d 1065, 1073 (Data retrieval program presumed accurate) 17 J.Marshall Jour. Of Computer & Info. Law 411, 507-508 [Westlaw: 17 JMARJCIL 411]

[84] 526 U.S. 137, 119 S.Ct. 1167 (1999).

[85] An excellent discussion of this debate can be found at 31 *Federal Practice and Procedure* § 7114, Wright & Miller, (2000 Revision), where the authors identify an apparent conflict between the application of *Daubert* and 901(b)(9).

[86] *United States v. Downing,* 753 F.2d 1224, 1240, fn. 21, (3rd Cir. 1985).

[87] 127 F.3d 595 (7th Cir.1997).

[88] *United States v. Whitaker, supra,* 127 F.3d at 600.

[89] 18 F.3d 1461 (9th Cir. 1994).

[90] *United States v. Quinn, supra,* 18 F.3d at 1465.

[91] *Id.*

[92] 802 S.W.2d 429 (Tx. Ct. App. 1991).

[93] *Burleson v. State, supra,* 802 S.W.2d at 441.

[94] 71 Am.Jur. Trials 111 § 118 (1999).

[95] *Weisman v. Hopf-Himsel, Inc*., 535 N.E. 2d 1222, 1226 (Ind. Ct. App. 1st Dist. 1989); *People v. Bovio,* 455 N.E.2d 829, 833 (Ill. App 1983); *Burleson v. State*, *supra,* 802 S.W.2d at 441; *People v. Lombardi, 711 N.E.2d 426* (Ill. App 1999).

[96] *United States v. Liebert,* 519 F.2d 542, 547 (3rd Cir. 1975); *United States v. Weatherspoon,* 581 F.2d 595, 598 (7th Cir. 1978).

[97] *Logan v. State*, 2005 WL 2840283 (Ind.App. Oct. 31, 2005).

[98] *Id.* at *1.

[99] 2000 WL 288443 (W.D. Mich. 2000).

[100] *Galaxy Computer Services, Inc. v. Baker,* 325 B.R. 544 (E.D.Va. 2005).

[101] *Id.* at 562.

[102] *Id.* at 563 [Emphasis added].

[103] 257 F.3d 50 (1st Cir. 2001).

[104] Available at http://www.ncjrs.org/pdffiles1/nij/200031.pdf

[105] See http://www.encase.com/corporate/news/index.shtm for a comprehensive listing of peer review publications concerning EnCase.

[106] 200 F.3d 627, 630-631 (9th Cir. 2000).

[107] 135 F.Supp 207, fn. 1 (2001 D.Me.). According the prosecutor in *Dean*, EnCase was used in the examination and provided an effective means for presenting the results of the examination at trial.

[108] *Fed. R. Evid.* 1002.

[109] *Fed. R. Evid.* 1001(1).

[110] The treatise. *Overly On Electronic Evidence in California*, (1999) § 9.02; 9-3, comments on California Evidence Code section 255, an identical statute to Rule 1001(3), noting "The approach adopted in Evidence Code section 255 allows for the possibility that multiple or, even, an infinite number of originals may exist. Each time an electronic document is printed, a new 'original' is created."

[111] Civil Evidence Act 1995 (c.38) at § 8.

[112] *United States v. Crume*, 422 F.3d 728, 730-31 (8th Cir. 2005).

[113] *Broderick v. State,* 35 S.W.3d 67(2000).

[114] Section V.D.1, citing, *Doe v. United States, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992),*

[115] 1 F.3d 1274 (D.C. Cir 1993).

[116] *Armstrong v. Executive Office of The President, supra,* 1 F.3d at 1280,

[117] *Id.* (See also, *Recovery and Reconstruction of Electronic Mail as Evidence* (1997) 41 AMJUR POF 3d 1 §19 ["If the document is a computer printout of an e-mail message, the proponent is required to prove that the printout accurately reflects what is in the computer."])

[118] 135 F.Supp.2d 207, fn. 1. (D.Me.) According the prosecutor in *Dean*, EnCase was used in the examination and provided an effective means for presenting the results of the examination at trial.

[119] *United States v. Seifert,* 2005 WL 44749 (D.Minn. Jan 7, 2005).

[120] *Id.* at note 2.

[121] 960 F.Supp. 498, 501 (D.Mass. 1997).

[122] 111 F.Supp.2d 294 (S.D.NY 2000).

[123] *Whelan Associates, Inc. v. Jaslow Dental Laboratories, Inc.*, 797 F.2d 1222 (2d Cir. 1986) (Comprehensiveness and complexity of the file structures within the program made the file structures sufficiently informative to warrant copyright protection); *CMAX/Cleveland, Inc. v. UCR, Inc.*, 804 F. Supp. 337 (M.D. Ga. 1992); *DVD Copy Control Association v. McLaughlin*, No. CV 786804, 2000 WL 48512 (Cal. Super. Jan. 21, 2000).

[124] 777 N.E.2d at 886.

[125] *Id.*

[126] 777 N.E.2d at 887.

[127] 127 S.W.3d 309 (Tex.App. 2004).

[128] *Id.* at 311.

[129] *Id.* at 312.

[130] *Id.* at 313-14.

[131] *State v. Morris*, 2005 WL 356801 (Ohio App. 9 Dist. Feb. 16, 2005).

[132] *Id.* at *2 (emphasis added).

[133] *Taylor v. State*, *supra*, 93 S.W.3d 487, 507-08.

[134] Okanogan County Cause no. 00-1-0026-8.

[135] *Frye v. United States*, 293 F. 1013 (D.C. Cir. 1923).

[136] 90 Wash.App. 100; 950 P.2d 1024 (Wash. App. 1998).

[137] 2000 WL 288443 (W.D.Mich. 2000).

[138] Sonoma County, California Superior Ct. no SCR28424.

[139] *Frye*, *supra,* 293 F. 1013.

[140] *Daubert,* 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469.

[141] *People v. Rodriguez,* transcript of January 11, 2001 hearing, p 88, ln 27.

[142] 168 F.3d 532, 537 (1st Cir. 1999).

[143] See, e.g., *United States v. Liebert,* 519 F.2d 542, 547 (3rd Cir. 1975) (holding that computer evidence was admissible in criminal trial provided that prosecution lays a sufficient foundation to warrant a finding that such information is trustworthy and the defense is given the same opportunity to inquire into the accuracy of the computer system involved in producing such evidence). See also, *United States v. Weatherspoon,* 581 F.2d 595, 598 (7th Cir. 1978).

[144] Case No. CR01-13, District Court of Johnson County, Nebraska.

[145] Journal Entry and Order, Nov. 6, 2001, by District Court Judge Daniel Bryan, Jr..

[146] *Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.*, 2003 WL 21230605 (N.D.Ill., May 27, 2003).

[147] *See Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.*, 2003 WL 22433095 (N.D.Ill., Oct. 27, 2003).

[148] 297 F.Supp.2d 1264 (D.Or. Oct. 20, 2003).

[149] *Id.* at 1267.

[150] *Id.* at 1267-68.

[151] *Id.* at 1268.

[152] *Id.* at 1268-69.

[153] *Id.* at 1269.

[154] *Id.* at 1270.

[155] *Id.* at 1271.

[156] *Id.* at 1273.

[157] *Id.* at 1275 (emphasis added).

[158] 2004 WL 413273 (Ohio App. 4 Dist., Mar. 2, 2004).

[159] *Id.* at *1.

[160] *Id.* at *1.

[161] *Id.* at *2.

[162] *Id.* at *3.

[163] *Id.* at *20.

[164] *People v. Donath*, 2005 WL 850895 (Ill.App. 1 Dist. Apr. 13, 2005).

[165] *Id.* at *11.

[166] E-mail correspondence from Senior Special Agent Jarrod Winkle, May 16, 2005.

[167] *People v. Donath*, 2005 WL 850895 at *12-*13(Ill.App. 1 Dist. Apr. 13, 2005).

[168] *State v. Levie*, 695 N.W.2d 619, 624 (Minn. App. 2005).

[169] *Id.* at 622.

[170] *State v. Luther*, 105 P.3d 56, 58 (Wash.App. Div. 1 2005).

[171] *Id.*

[172] *Liebert Corp. v. Mazur*, 2005 WL 762954 (Ill.App. 1 Dist., 2005).

[173] *Id.*

[174] *Id.* at *5

[175] *Id.* at *6.

[176] *Id.* at *6.

[177] *Id.*

[178] *Id.* at *15-16.

[179] *Porath v. State*, 148 S.W.3d 402 (Tex.App.-Houston [14 Dist.], 2004).

[180] *Id.* at 406.

[181] *Id.* at 415.

[182] *People v. Zavala*, 2005 WL 605465 (Cal.App. 6 Dist. Mar. 16, 2005).

[183] *Id.* at *1.

[184] *People v. Upton*, 2004 WL 2075393 (Cal.App. 6 Dist. Sept. 17, 2004).

[185] *Id.* at *1.

[186] *State v. Howell,* 609 S.E.2d 417,419 (N.C.App. 2005).

[187] *Fridell v. State*, 2004 WL 2955227 (Tex. App. Dec. 22, 2004).

[188] *Id.* at *2-*3.

[189] *State v. McKinney* 699 N.W.2d 471, 2005 S.D. 73 (S.D. 2005).

[190] *Id.* at 480-81. In a telephone conversation on June23, 2005, Kevin Atkins told Gregg Smolar that he used EnCase software on this case.

[191] *United States v. Bass*, 411 F.3d 1198 (10th Cir. 2005).

[192] *Id.* at 1200.

[193] *Id.* at 1202.

[194] *United States v. Davis*, 61 M.J. 530 (Army Ct.Crim.App. 2005).

[195] *Id.* at 531, 537.

[196] Although the Cybercrime Arsenal package is offered to law enforcement, EnCase software itself is available to the public at large.

[197] *United States v. Long*, 425 F.3d 482, 484 (7th Cir. 2005).

[198] *Foust v. McFarland*, 698 N.W.2d 24 (Minn.App. 2005).

[199] Telephone conversation between Marl Lanterman and Gregg Smolar, July 5, 2005.

[200] *Foust v. McFarland*, 698 N.W.2d at 29.

[201] 2003 ABQB 212 (Mar. 7, 2003).

[202] 2003 ABPC 190 (Nov. 28, 2003).

[203] 2003 O.J. No. 5513 (Dec. 5, 2003).

[204] *Id.* at ¶ 3.

[205] *Id.*

[206] *Id.* at ¶ 14.

[207] *Id.* at ¶ 7.

[208] *Id.* at ¶ 15.

[209] *Id.* at ¶ 20.

[210] *Id.* at ¶ 65.

[211] Fed. Court, NSW Dist., N128 of 2003 (May 30, 2003).

[212] 2003 WL 22407255 (Fed. Court), N1161 of 2003 (Sept. 19, 2003).

[213] *Id.* at ¶¶ 1-3.

[214] *Id.* at ¶ 4.

[215] *Id.* at Annexure A.

[216] *Id.* at Order no. 3.

[217] *Id*. at Order no. 4.

[218] *Ler Wee Teang Anthony v. Public Prosecutor*, Court of Appeal, Criminal Appeal No. 27 of 2001 (April 19, 2002).

[219] The Supreme Court's judgment can be found at http://judis.nic.in/supremecourt/qrydisp.asp?tfnm=27092

[220] *See, e.g.*, http://www.tribuneindia.com/2005/20050805/main1.htm

[221] *See* http://www.chennaionline.com/colnews/newsitem.asp?NEWSID=%7B4A181E08-74B0-487D-910C-09C15658A43C%7D&CATEGORYNAME=NATIONAL

[222] *Horton v. California,* 496 U.S. 128, 134, 110 S.Ct. 2301, 2307, 110 L.Ed.2d 112 (1990).

[223] *United States v. Roberts*, 86 F.Supp.2d 678 (S.D.Tex 2000) (Warrantless search by Customs agents of the defendant's computer and zip disks constituted a routine export search, valid under the Fourth Amendment). This holding is specifically limited to border or export searches.

[224] *United States v. Turner,* 169 F.3d 84 (1ˢᵗ Cir. 1999) (Suppressing all evidence obtained from a warrantless search of suspect's computer files), See also, *United States v. Barth,* 26 F.Supp.2d 929, 935-936 (D.C. Tex. 1998)..

[225] *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999).

[226] U.S. Department of Justice, *Federal Guidelines for Searching and Seizing Computers* (1994) Note 12, at 89.

[227] *United States v. Hunter*, 13 F. Supp. 2d 574, 583 (D. Vt. 1998).

[228] 152 F.3d 1241 (10ᵗʰ Cir.1998).

[229] *United States v. Simpson, supra*, 153 F.2d at 1248.

[230] 168 F.3d 532 (1ˢᵗ Cir. 1999).

[231] *United States v. Upham*, supra, 168 F.3d at 535

[232] *Id.* at 537.

[233] See *Davis v. Gracey*, 111 F.3d 1472, 1480 (10th Cir.1997) (upholding seizure of computer and all files contained therein because probable cause supported seizure of computer as an instrumentality of the crime); *United States v. Kimbrough,* 69 F.3d 723, 727 (5ᵗʰ Cir 1995) (upholding warrant allowing seizure of "hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media-floppy disks, CD ROMs, tape systems and hard drive, other computer related operational equipment ... used to visually depict a minor engaging in sexually explicit conduct"); *United States v. Lamb*, 945 F. Supp. 441, 457-58 (N.D.N.Y. 1996) (finding e-mail messages discussing the transport of child pornography to have a sufficient nexus to the crime and thus subject to seizure).

[234] 119 F.3d 742, 745 (9ᵗʰ Cir. 1997).

[235] 58 F.3d 423, 426 (9th Cir.1995).

[236] *United States v. Kow*, supra, 58 F.3d 423 at 427.

[237] See *Marron v. United States*, 275 U.S. 192, 196, 47 S.Ct. 74, 76, 72 L.2d 231 (1927) (particularity requirement "prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.")

[238] 172 F.3d 1268 (10ᵗʰ Cir. 1999).

[239] *United States v. Carey*, *supra,* 172 F.3d at 1272-1273.

[240] *Id.,* at 1271.

[241] *Id.*

[242] *Id.*

[243] *Id.* at 1272.

[244] *Id.*

[245] *Id.* at 1274.

[246] *Id.* at 1273.

[247] *Id.* at 1275.

[248] *Id.* (citations omitted)

[249] *Id.*

[250] *Id.*, citing, Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J.L. & Tech. 75, 104 (1994).

[251] The court notes: "Although the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others, we do not need to reach it here." *Carey,* 172 F.3d at 1273.

[252] *Id.*

[253] Concurring opinion of Judge Baldock, *Carey*, 172 F.3d at 1277.

[254] 78 F.Supp.2d 524 (E.D.Va. 1999).

[255] *United States v. Gray, supra*, 78 F.Supp.2d at 526.

[256] *Id.* at 527.

[257] *Id.*

[258] *Id.*

[259] *Id.* at 528.

[260] *Id.* at 529, citing *United States v. Hunter, supra*, 13 F.Supp.2d at 584.

[261] *United States v. Gray*, supra, 78 F.Supp.2d at 530.

[262] *Id.* at 529.

[263] 2000 WL 288443 (W.D.Mich. 2000).

[264] 83 F.Supp.2d 187 (D.Mass 2000)

[265] *United States v. Scott, supra*, 183 F.Supp.2d at 195.

[266] *Id.* at 196.

[267] *Id.* at 197.

[268] Although the opinion does not reflect the type of software utilized, *the EnCase Legal Journal* confirmed with the investigating agent identified in the opinion that EnCase was used for the investigation. (March 28, 2000 telephone interview of USSS Special Agent Bruce Rittenour).

[269] *United States v. Scott, supra*, 183 F.Supp.2d at 197-198.

[270] 2000 WL 675942, Wisconsin Supreme Court Decision.

[271] 81 Fed. Appx. 109 (9ᵗʰ Cir. 2003)

[272] Id. at 110.

[273] Id.

[274] Id.

[275] 384 F.3d 38, 41 (2ⁿᵈ Cir. 2004).

[276] Id.

[277] Id. at 48.

[278] 194 Misc.2d 595, 755 N.Y.S.2d 800 (2003).

[279] 194 Misc.2d at 599, 755 N.Y.S.2d at 804.

[280] 194 Misc.2d at 602, 755 N.Y.S.2d at 806.

[281] 194 Misc.2d at 605, 755 N.Y.S.2d at 808.

[282] 194 Misc.2d at 605, 755 N.Y.S.2d at 808.

[283] 794 N.E.2d 449 (Ind. App. 2003).

[284] 794 N.E.2d 449, 452-54.

[285] 2004 WL 1427013 (Cal. Ct. of Appeal, June 25, 2004).

[286] *Id.* at *5.

[287] *Id. at *6.*

[288] 322 F.Supp. 1081 (C.D. Cal. 2004).

[289] *Id.* at 1091.

[290] *Id.* at 1084.

[291] *Id.* at 1090-91.

[292] *In re Search of: 3817 W. West End,* 321 F.Supp.2d 953 (N.D.Ill. 2004).

[293] *Id.*

[294] *Id.*

[295] *Id.*

[296] *United States v. Maali*, 346 F. Supp. 2d 1226 (M.D. Fla., 2004).

[297] *Id.* at 1247.

[298] *Id.* at 1236.

[299] *Id.* at 1264.

[300] *Id.* at 1265.

[301] *Id.*

[302] *State v. Bolsinger*, 2005 WL 756767 (Iowa App. Mar. 31, 2005).

[303] *Id. at *6.*

[304] *Id.*

[305] *United States v. Riccardi*, 405 F.3d 852 (10ᵗʰ Cir. April 19, 2005).

[306] *Id.* at 858.

[307] *Id.* The use of EnCase software was confirmed by Special Agent David Finch in a telephone conversation with Gregg Smolar of Guidance Software, Inc. on June 15, 2005.

[308] *Id.* at 862-63.

[309] *Id.* at 863-64.

[310] *United States v. Brooks*, 2005 WL 2767185 (10th Cir. Oct. 26, 2005).

[311] *Id.* at *2.

[312] *Id.* at *5 [Internal citations omitted; emphasis in original].

[313] *Id.*

[314] *Id.* at *6.

[315] *Id.* [Emphasis in original].

[316] *United States v. Calimlim*, 2005 WL 2922193 at *17 (E.D.Wis. Nov. 4, 2005).

[317] *Id.* at n. 4.

[318] *Id.* at *17.

[319] *Supra*, 78 F.Supp.2d at 526.

[320] 76 F.Supp.2d 30 (D.ME 1999), citing, *Sgro v. United States*, 287 U.S. 206, 210, 53 S.Ct. 138, 140, 77 L.Ed. 260 (1932).

[321] *supra*, 76 F.Supp.2d at 42.

[322] 36 F.3d 457, 462 (5th Cir. 1994).

[323] *supra*, 168 F.3d 532.

[324] *supra*, 13 F.Supp.2d at 583.

[325] *United States v. Triumph Capital Group*, 211 F.R.D. 31 (D.Conn. 2002).

[326] *Id.* at 66.

[327] *United States v. Gorrell*, 360 F.Supp.2d 48 (D.D.C. 2005).

[328] *Id.,* at n. 5.

[329] *Id.,* at 52.

[330] *Id.,* at n. 5.

[331] *State v. Zinck,* 2005 WL 551447 (N.H. Super. Ct. Feb. 4, 2005).

[332] *Id.* at *1-*2.

[333] *Id.* at *2.

[334] 884 So.2d 131 (Ct. of Appeal of Florida, 2004).

[335] *Id.* at 133.

[336] *Id.* at 135-36.

[337] *State v. Morris*, 2005 WL 356801 (Ohio App. 9 Dist. Feb. 16, 2005).

[338] *Airtrans, Inc. v. Mead*, 389 F.3d 594 (6th Cir. 2004).

[339] *Id.* at 596-97.

[340] *State v. Kaminski*, 2005 WL 1155112 (Conn.Super., Apr. 25, 2005).

[341] *Id.*

[342] 322 F.Supp. 1081 (C.D. Cal. 2004).

[343] *Id.* at 1091, 1092-93.

[344] 2004 WL 2397346 (D. Mass. Oct. 27, 2004).

[345] *Id.* at *1.

[346] *Id.* at *3.

[347] State of Minnesota v. Kandel, 2004 WL 1774781 (Minn.App. Aug. 10, 2004).

[348] *Id.* at *1.

[349] *Id.* at *2.

[350] 2004 WL 2095701 (E.D. Mich. Sept. 14, 2004)

[351] Id. at *10.

[352] *State v. Butler,* 2005 WL 735080 (Tenn.Crim.App. Mar 30, 2005).

[353] *Id.* at *1.

[354] *Id.* at *11.

[355] *Id.* at *2.

[356] *Id.* at *3.

[357] 194 F.R.D. 639 (S.D. Ind. 2000).

[358] 188 F.R.D. 111, 117 (1998 D.C. Cir).

[359] *Playboy Enterprises v. Welles*, 60 F.Supp.2d 1050, 1054 (S.D. CA 1999).

[360] *Rowe Entertainment, Inc. v. The William Morris Agency,* 2002 WL 975713 at *3 (S.D.N.Y. May 9, 2002).

[361] *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 at *16 (S.D.N.Y. Jul. 20, 2004).

[362] *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 at *8 (S.D.N.Y. Jul. 20, 2004) (emphasis in original).

[363] This is despite the fact that "it is a well accepted proposition that deleted computer files, whether they be emails or otherwise, are discoverable" (*Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002); *see also, Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) ("[C]omputer records, including records that have been 'deleted,' are documents discoverable under [Rule] 34)). In addition to deleted data, metadata is also discoverable. (*See* ABA's Civil Discovery Standard 29(b)(ii) ("A party requesting information in electronic form should also consider . . . asking for the production of metadata associated with the responsive data").

[364] *Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309, 317 (S.D.N.Y. 2003).

[365] 205 F.R.D. 437 (D. NJ 2002).

[366] 306 F.3d 99 (2nd Cir 2002).

[367] *Pace v. Nat. RR Passenger Corp.*, 2003 WL 22860317 (D. Conn., Dec. 1, 2003).

[368] *Wiginton v. CB Richard Ellis*, 2003 WL 22439865 (N.D. Ill., Oct. 27, 2003).

[369] *In re Search of: 3817 W. West End,* 321 F.Supp.2d at n.1 (internal citations and quotations omitted).

[370] *United States v. Andreozzi*, 2004 WL 2496722 (U.S. Army Court of Crim. Appeals, Nov. 4, 2004), in which the Court's Order specified that "the computer hard drives of Captain Travis . . . will be examined . . . Suggested examination time parameter should include from 1 April 1998 to 10 June 1998. Suggested examination terms are 'andreozzi' and 'enlisted,' or 'andreaozzi' and 'forum.'"

[371] 210 F.R.D. 645 (D Minn 2002).

[372] 2002 WL 818061 (D. Del. Apr. 30, 2002).

[373] 212 F.R.D. 178 (S.D.N.Y. 2003).

[374] 2004 WL 1837997 (N.D.Cal. Aug. 17, 2004).

[375] *Id.* at *1.

[376] *Id.*

[377] *Id.* at *2.

[378] *Id.* at *11.

[379] *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866 at *5 (S.D.N.Y. Jul. 20, 2004).

[380] *Id.* at *13.

[381] 327 F.Supp.2d 21 (D.D.C. July 21, 2004).

[382] *Id.* at 23-24.

[383] *Id.* at 26.

[384] 2004 WL 1393992 (S.D.N.Y. June 22, 2004).

[385] *Id.* at *3.

[386] *Id.* at *4.

[387] *Mosaid Technologies Inc. v. Samsung Electronics Co., Ltd.,* 348 F.Supp.2d 332 (D.N.J. Dec. 7, 2004).

[388] A "'spoliation inference' is an adverse inference that permits a jury to infer that "destroyed evidence might or would have been unfavorable to the position of the offending party." *Id.* at 336, *citing Scott v. IBM Corp.*, 196 F.R.D. 233 at 248 (D.N.J. 2000).

[389] *Id.* at 333, 339-340 (emphasis added).

[390] *Mosaid Technologies Inc. v. Samsung Electronics Co., Ltd.,* 348 F.Supp.2d 332, 333 (D.N.J. Dec. 7, 2004).

[391] *Tantivy Communications, Inc. v. Lucent Technologies Inc.*, 2005 WL 2860976 (E.D.Tex. Nov. 1, 2005).

[392] *Broccoli v. Echostar Communications Corp.*, 229 F.R.D. 506 (D.Md. 2005).

[393] *Id.* at 510.

[394] *Id.* at 512.

[395] ABA Civil Discovery Standard 29(b)(ii).

[396] *The Sedona Principles for Electronic Document Production*. Comment 12.a.

[397] *In re Vioxx Prods. Liab.y Litig.*, 2005 WL 756742 at *3 (E.D.La. Feb. 18, 2005) (emphasis added).

[398] Zenith Electronics Corp. v. WH-TV Broadcasting Corp., 2004 WL 1631676 at * 7 (N.D.Ill. July 19, 2004).

[399] *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 644 (D.Kan. 2005).

[400] *Id.*

[401] *Id.* at 652.

[402] *Zubulake v. UBS Warburg LLC*, 2003 WL 22410619, at *4 (S.D.N.Y. Oct. 22. 2003).

[403] *Zubulake v. UBS Warburg LLC*, 2004 WL 1620866, at *8 (S.D.N.Y. July 20, 2004).

[404] *Zubulake v. UBS Warburg LLC*, 2003 WL 22410619, at *3 (S.D.N.Y. Oct. 22. 2003).

[405] *Williams v. Massachusetts Mutual Life Insurance Co.*, 226 F.R.D. 144 (D. Mass. 2005)

[406] *Id.* at 145.

[407] *Id.*

[408] *Id.* at 146.

[409] Affidavit of Bruce Bonsall, available electronically on the PACER system (http://pacer.psc.uscourts.gov).

[410] *Mudron v. Brown & Brown, Inc.*, 2005 WL 645927 (N.D. Ill. Mar. 17, 2005).

[411] *Id.* at *4.

[412] *Id.*

[413] *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 674885 (Fla.Cir.Ct. Mar. 23, 2005).

[414] *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 at *4 (Fla.Cir.Ct. Mar. 1, 2005).

[415] Susanne Craig, "How Morgan Stanley Botched a Big Case by Fumbling Emails," *Wall Street Journal,* May 16, 2005.

[416] *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 318 (S.D.N.Y. 2003).

[417] eExaminer, August 2004; "Mission Impossible; 5,000 Computer Examinations in Four Weeks" www.guidancesoftware.com/corporate/examiner/2004-08.shtm

[418] *Tempco Electric Heater Corp. v. Temperature Engineering Co.*, 2004 WL 1254134 (N.D.Ill. 2004).

[419] 2004 WL 1878751 (S.D.N.Y. 2004).

[420] 2004 WL 1468698 (Cal.App.3d 2004).

[421] *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003); *see also Zubulake v. UBS Warburg LLC*, 216 F.R.D. 280 (S.D.N.Y. 280) and *Zubulake v. UBS Warburg*, 2003 WL 22410619 (S.D.N.Y., Oct. 22, 2003).

[422] 217 F.R.D. at 317.

[423] *Id.* at 317-18.

[424] *Id.* at 322.

[425] 216 F.R.D. at 291.

[426] See, e.g., *Open TV v. Liberate Technologies*, 219 F.R.D. 474 (N.D. Cal. 2003); *Hagemeyer North America, Inc. v. Gateway Data Sciences Corp.*, 222 F.R.D. 594 (E.D. Wis. 2004).

[427] The approach used in previous cases such as *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002) , was much more likely to result in cost-shifting.

[428] *United States v. Balon*, 384 F.3d 38, 41 (2nd Cir. 2004).

[429] *Weiller v. New York Life Insurance Co.*, 6 Misc.3d 1038 (A), 2004 WL 3245345 (N.Y.Sup. Mar. 16, 2005).

[430] *Id.* at *6 (emphasis added) (internal citations omitted).

[431] No. 8775/01, Supreme Court, Nassau County, New York, Aug. 18, 2004.

[432] 2004 WL 2757873 (Cal. App. 6 Dist. Dec. 3, 2004).

[433] The statute, Code of Civil Procedure §2031 (g)(I), provides that '[i]f necessary, the responding party at the reasonable expense of the demanding party shall, through detection devices, translate any data compilations in the demand into reasonably usable form."

[434] 2004 WL 2757873 at *6 (Cal. App. 6 Dist. Dec. 3, 2004).

[435] *Id.* at *5 (emphasis in original).

[436] *supra*, 194 F.R.D. 639.

[437] July 18, 2000 phone interview with Shawn Howell of Computer Forensics, Inc.

[438] 204 F.R.D. 277 (E.D.Va. 2001).

[439] 2002 WL 63190 (S.D.N.Y. Jan. 16, 2002).

[440] 281 F.Supp.2d 795 (E.D. Va. 2002).

[441] *Renda Marine, Inc. v. UnitedStates,* 58 Fed. Cl. 57 (Fed. Cl., 2003).

[442] 43 F.Supp.2d 951, 954 (E.D. Ill 1999).

[443] See, e.g., *Flagg Bros., Inc. v. Brooks*, 436 U.S. 149, 156 (1978) (stating that most constitutional rights "are protected only against infringement by governments"); *Jackson v. Metropolitan Edison Co*., 419 U.S. 345, 349 (1974) (describing "essential dichotomy" between deprivations of rights by state action and private conduct).

[444] See 18 U.S.C. §§ 1367, 2521, 3117, 3121-3127 (1994).

[445] Connecticut Public Act no. 98-142. There are exceptions under this statute where the employer has reasonable grounds to suspect that the employee is engaging in unlawful conduct or conduct creating a hostile workplace environment, and such monitoring may produce evidence of this misconduct. Del. Code, tit. 19, section 705. The only explicit exceptions under the Delaware law are for "processes that are designed to manage the type or volume of incoming or outgoing electronic mail or telephone voice mail or Internet usage, that are not targeted to monitor or intercept the electronic mail or telephone voice mail or Internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection"

[446] *Smyth v. Pillsbury Co*, 914 F.Supp. 97 (E.D. Pa. 1996).

[447] See, e.g. "Employer Liability for Employee Online Criminal Acts." *Federal Communications Law Journal*, (1999) 51 FCLJ 467.

[448] *Id.*

[449] 751 A.2d 538 (2000).

[450] *Smyth v. Pillsbury Co.*, *supra*, 914 F.Supp at 100.

[451] 280 F.3d 741 (2002).

[452] 272 F.Supp.2d 822 (D.Neb. 2003).

[453] *Id.* at 824.

[454] Employment Practices Data Protection Code § 3.3.2, available at: http://www.informationcommissioner.gov.uk/eventual.aspx?id=446

[455] Employment Practices Data Protection Code at § 3.3.1.

[456] *Id.*

[457] *Id.* at § 3.3.8.

[458] See 18 U.S.C. §§ 1367, 2521, 3117, 3121-3127 (1994).

[459] Yochai Benkler, "Rules of the Road for the Information Superhighway" § 1, § 20.3[1] (1996) (discussing effects of ECPA's passage).

[460] See, e.g., Michael D. Scott et al., Scott on Multimedia Law § 12.04 [[A] (2d ed. Supp. 1997) (asserting that ECPA "would not apply to corporate or other 'non-public' computer networks.... [A] company's review of e-mail transmitted through or stored on its computer system would not violate the ECPA"); Kent D. Stuckey et al., Internet and Online Law § 5.03[1] (Release 2 1998) (stating that ECPA "does not ... protect against employers monitoring the e-mail of their employees").

[461] 18 U.S.C. §§ 2511(3)(a), 2702(a)(1) (1994).

[462] See 18 U.S.C. § 2701(c)(1) (1994) (exempting all "conduct authorized...by the person or entity providing a wire or electronic communications service"). The provider of electronic communications services is known as the "network provider."

[463] 932 F. Supp. 1232 (D. Nev. 1996).

[464] See *Id.* at 1232. The officers had used the police department's alphanumeric paging system to send messages to each other. See *Id.* at 1233. The contents of these messages led to an internal affairs investigation of the officers.

[465] See *Id.* at 1236.

[466] *Steve Jackson Games, supra,* 36 F.3d at 463.

[467] *Steve Jackson Games*, *supra,* 36 F.3d at 463 (holding that seizure of e-mail sent to bulletin board but not yet read by intended recipients did not constitute unlawful interception). See also, *United States v. Reyes*, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) .

[468] 135 F.Supp.2d 623 (D. Penn. 2001).

[469] 2001 WL 576133 (D.Mass. May 22, 2001).

[470] *Steve Jackson Games, supra,* 36 F.3d at 463.

[471] See *United States v. Councilman*, 245 F. Supp.2d 319 (D. Mass. 2003); *Bohach v. City of Reno, supra,* 932 F. Supp. at 1235-36 ("The statutes therefore distinguish the 'interception' of an electronic communication at the time of transmission from the retrieval of such a communication after it has been put into 'electronic storage." '); *United States v. Reyes, supra*, 922 F. Supp. at 836 ("[T]he definitions [in the ECPA] thus imply a requirement that the acquisition of the data be simultaneous with the original transmission of the data.").

[472] *Konop v. Hawaiian Airlines, Inc.,* 236 F.3d 1035 (9th Cir.2001); opinion withdrawn, 262 F.3d 97 and superceded by 302 F.3d 868, (9th Cir. 2002). *Konop* initially created some concerns about a broader definition of "interception." However, and in response to these concerns, the opinion has been withdrawn and superceded.

[473] See § 9.01.

[474] California SB1016, sponsored by Debra Bowen, D-Redondo Beach.

[475] *Smyth v. Pillsbury Co.*, *supra*, 914 F.Supp at 100 (recognizing the theoretical possibility of such a claim).

[476] See, e.g., Mike Causey, *Telecommuting Today*, Wash. Post, July 8, 1997, at B2 .

[477] See, e.g., H.G. Reza, *The Few, the Proud, the Online*, L.A. Times (Orange County ed.), Dec. 25, 1997, at E1, available in LEXIS, News Library, LAT File.

[478] *O'Connor v. Ortega*, 480 U.S. 709, 715, 107 S.Ct. 1492, 1496 (1987) (a plurality decision); *Shields v. Burge*, 874 F.2d 1201, 1203-04 (7th Cir.1989).

[479] *O'Connor*, 480 U.S. at 717, 107 S.Ct. at 1497; 480 U.S. at 737, (Blackmun, J., dissenting).

[480] 206 F.3d 392 (4th Cir 2000).

[481] *Id.* at 398, fn. 9.

[482] *Id.* at 399-400.

[483] *United States v. Simons, supra*, 206 F.3d at 399, fn 10.
[484] *O'Connor*, 480 U.S. at 726, 107 S.Ct. at 1502.
[485] *Id*. (citing *New Jersey v. T.L.O.,* 469 U.S. 325, 342, 105 S.Ct. 733, (1985)).
[486] *United States v. Plush*, 2004 WL 2191813 (A.F. Ct. Crim. App. Sep. 21, 2004).
[487] *Id.* at *3 (internal citations and quotations omitted).
[488] *Id.*
[489] *Id.* at *4.
[490] *United States v. Long* 61 M.J. 539 (N.M.Ct.Crim.App. 2005).
[491] *Id.* at 543.
[492] *Id.* at 546.