Computer forensics is a discipline dedicated to the collection of computer evidence for judicial purposes. Those who practice computer forensics should be very familiar with the laws of evidence in their relevant jurisdictions so that they may correctly employ the proper procedures, tools and methodologies used to collect and process computer evidence. While there has been some excellent research and writing on search and seizure and privacy issues related to computer data, there has been comparatively little guidance on the authentication and presentation of electronic evidence at trial.

Computer investigation experts uncertain of what the law required often received unclear direction from counsel who were equally unfamiliar with the complex technical issues and nuances that must be applied to the laws of evidence. Consequently, there has been no clear consensus on issues such as what is required to establish a sufficient foundation for computer evidence, whether a computer forensic investigator is considered a scientific expert, and how the Best Evidence rule applies to computer data.

In response to these concerns, Guidance Software launched The EnCase Legal Journal ("ELJ"), which is provided with two goals in mind. First, the ELJ reports on recent trial court developments involving EnCase® software as well as notable court decisions involving computer evidence in general. Secondly, the ELJ 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.

The ELJ 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
# Table of Contents

New in December 2003 Revision .......................................................................................................................... 4

## Authentication of Computer Evidence

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>§1.0</td>
<td>Overview</td>
<td>5</td>
</tr>
<tr>
<td>§1.1</td>
<td>Authentication of Computer Data</td>
<td>5</td>
</tr>
<tr>
<td>§1.2</td>
<td>Authentication of the Recovery Process</td>
<td>7</td>
</tr>
<tr>
<td>§1.3</td>
<td>Authentication of the EnCase Recovery Process</td>
<td>11</td>
</tr>
<tr>
<td>§1.4</td>
<td>Challenges to Foundation Must Have Foundation</td>
<td>12</td>
</tr>
<tr>
<td>§1.5</td>
<td>Evidentiary Authentication Within the EnCase Enterprise Process</td>
<td>12</td>
</tr>
</tbody>
</table>

## Validation of Computer Forensic Tools

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>§2.0</td>
<td>Overview</td>
<td>16</td>
</tr>
<tr>
<td>§2.1</td>
<td>Frye/Daubert Standard</td>
<td>16</td>
</tr>
<tr>
<td>§2.2</td>
<td>Computer Forensics as an Automated Process</td>
<td>20</td>
</tr>
<tr>
<td>§2.3</td>
<td>Commercial vs. Custom Forensic Software and Authentication Issues</td>
<td>22</td>
</tr>
</tbody>
</table>

## Expert Witness Testimony

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>§3.0</td>
<td>Overview</td>
<td>25</td>
</tr>
<tr>
<td>§3.1</td>
<td>Threshold Under Rule 702</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>DIRECT EXAMINATION -- PRE-TRIAL EVIDENTIARY HEARING</td>
<td>27</td>
</tr>
<tr>
<td></td>
<td>DIRECT EXAMINATION FOR THE PRESENTATION OF COMPUTER EVIDENCE BEFORE A JURY</td>
<td>33</td>
</tr>
</tbody>
</table>

## The Best Evidence Rule

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>§4.0</td>
<td>Overview</td>
<td>41</td>
</tr>
<tr>
<td>§4.1</td>
<td>“Original” Electronic Evidence</td>
<td>41</td>
</tr>
<tr>
<td>§4.2</td>
<td>Presenting Electronic Evidence at Trial</td>
<td>43</td>
</tr>
<tr>
<td>§4.3</td>
<td>Compression And the Best Evidence Rule</td>
<td>45</td>
</tr>
<tr>
<td>§4.4</td>
<td>United States v. Naparst – The EnCase Evidence File Validated As Best Evidence</td>
<td>46</td>
</tr>
</tbody>
</table>

## Legal Analysis of the EnCase Evidence File

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>§5.0</td>
<td>Overview</td>
<td>50</td>
</tr>
<tr>
<td>§5.1</td>
<td>Evidence File Format</td>
<td>50</td>
</tr>
<tr>
<td>§5.2</td>
<td>CRC and MD5 Hash Value Storage and Case Information Header</td>
<td>51</td>
</tr>
<tr>
<td>§5.3</td>
<td>Chain of Custody Documentation</td>
<td>52</td>
</tr>
<tr>
<td>§5.4</td>
<td>The Purpose of Sterile Media and The EnCase Process</td>
<td>53</td>
</tr>
<tr>
<td>§5.5</td>
<td>Analyzing The Evidence File Outside of the EnCase Process</td>
<td>53</td>
</tr>
<tr>
<td>Challenges to EnCase and Other Litigated EnCase Issues</td>
<td>56</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>----</td>
<td></td>
</tr>
<tr>
<td>Matthew Dickey v. Steris Corporation</td>
<td>57</td>
<td></td>
</tr>
<tr>
<td>State of Washington v. Leavell</td>
<td>58</td>
<td></td>
</tr>
<tr>
<td>People v. Rodriguez</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>People v. Merken</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.</td>
<td>62</td>
<td></td>
</tr>
<tr>
<td>I. Newsgroups:</td>
<td>64</td>
<td></td>
</tr>
<tr>
<td>II. What is a JPEG?</td>
<td>66</td>
<td></td>
</tr>
<tr>
<td>III. Continued Review of Kevin Habershaw’s Computer</td>
<td>66</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Search and Seizure Issues and EnCase</th>
<th>70</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 7.0 Overview</td>
<td>70</td>
</tr>
<tr>
<td>§ 7.1 Computer Files and the Plain View Doctrine</td>
<td>70</td>
</tr>
<tr>
<td>§ 7.2 United States v. Carey</td>
<td>72</td>
</tr>
<tr>
<td>§ 7.3 Post-Carey Case Law</td>
<td>74</td>
</tr>
<tr>
<td>§ 7.4 Post-Carey Practice</td>
<td>78</td>
</tr>
<tr>
<td>§ 7.5 Warrant Return Requirements</td>
<td>80</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Complying with Discovery Requirements when Utilizing the EnCase Process</th>
<th>81</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 8.0 Overview</td>
<td>81</td>
</tr>
<tr>
<td>§ 8.1 Production of Entire EnCase Images</td>
<td>81</td>
</tr>
<tr>
<td>§ 8.2 Production of Restored Drives</td>
<td>82</td>
</tr>
<tr>
<td>§ 8.3 Production of Exported Files</td>
<td>82</td>
</tr>
<tr>
<td>§ 8.4 Supervised Examination</td>
<td>82</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EnCase As a Process for Civil Litigation Computer Discovery</th>
<th>84</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 9.0 Overview</td>
<td>84</td>
</tr>
<tr>
<td>§ 9.3 Example Form Letter Demanding Preservation of Computer Evidence</td>
<td>93</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Employee Privacy and Workplace Searches of Computer Files and E-mail</th>
<th>97</th>
</tr>
</thead>
<tbody>
<tr>
<td>§ 10.0 Overview</td>
<td>97</td>
</tr>
<tr>
<td>§ 10.1 Employee Monitoring in the Private Sector</td>
<td>97</td>
</tr>
<tr>
<td>§ 10.2 The Electronic Communications Privacy Act of 1986</td>
<td>99</td>
</tr>
<tr>
<td>§ 10.3 Other Important Considerations for Employers</td>
<td>100</td>
</tr>
<tr>
<td>§ 10.4 Monitoring of Government Employees</td>
<td>101</td>
</tr>
</tbody>
</table>
New in December 2003 Revision

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

Section 1.5: Added new section: “§ 1.5 Evidentiary Authentication Within the EnCase Enterprise Process

Section 2.1: Revised to include discussion of testing conducted by the National Institute of Standards and Technology (“NIST”).

Section 2.1: Revised to include direct testimony concerning the NIST testing.

Section 4.1: Revised to include brief discussion of standard in civil matters in the UK.

Chapter 6: Added detailed discussion of Kucala Enterprises, Ltd. v. Auto Wax Co., Inc., 2003 WL 21230605 (N.D.Ill. May 27, 2003), as well as brief discussions of cases from Canada (Regina v. Cox), Australia (Sony Music Entertainment (Australia) Ltd. v. Univ. of Tasmania, et al.), and Singapore (Ler Wee Teang Anthony v. Public Prosecutor), each of which accept evidence gathered using EnCase.


Section 7.4: Revised to include brief discussion of post-Carey case law.


§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. 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 evidence 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.” Under these statutes, a printout of an e-mail message can often be authenticated simply through direct testimony from the recipient or the author.

The US Federal Courts have thus far addressed the authentication of computer-generated evidence based upon Rule 901(a), much in the same manner as statutes that have existed before computer usage became widespread. United States v. Tank, 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. 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. 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." 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.

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."

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). 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 the
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 and other
Litigated Cases Addressing the Validity of the EnCase Process.

§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 forensic 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.”

In a similar decision, *Bone v. State*, 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. 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." 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.

*People v. Lugashi* 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.

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. 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.

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."\textsuperscript{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.\textsuperscript{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.”\textsuperscript{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 \textit{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.”\textsuperscript{31}

It should be noted that there are some factors and aspects of the \textit{Lugashi} decision that may not be completely applicable to computer forensics. For instance, \textit{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 \textit{Lugashi}, while courts would likely apply increased scrutiny to records generated by a law enforcement investigator or retained party expert. However, certain aspects of the \textit{Lugashi} decision seem applicable to questions regarding what is required to establish a proper foundation for evidence obtained from a computer forensic examination. (See also \textit{Federal Deposit Insurance Corporation v. Carabetta}\textsuperscript{32} [similar facts and holding to \textit{Lugashi}]; \textit{Hahnemann University Hosp. v. Dudnick}\textsuperscript{33}; \textit{Garden State Bank v. Graef}\textsuperscript{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.

\textit{Bray v. Bi-State Development Corp.}\textsuperscript{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. 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." 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."

In State of Arizona v. Rivers, 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. 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. 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. The court relied on the case of Ly v. State of Texas, 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*, 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. 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 these 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 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.

**NOTE:** See Chapter 6 For a Detailed Analysis of Reported Appellate Decisions and Other Litigated Cases Addressing the Validity of the EnCase Process.
by the program. This means that the examiner should ideally have received training on EnCase, 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 500,000+ 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 is designed to address these challenges presented by real-
time enterprise investigations. Importantly, EnCase Enterprise operates at the disk
level, allowing EnCase 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, 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.”

For these reasons, many law enforcement agencies in the United States and
throughout the world are employing EnCase Enterprise Edition 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.

Of course, because EnCase Enterprise 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 does not itself make any writes to the target drive during the exam, nor are
files altered in any way when viewed or copied by EnCase.

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, 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 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.

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 addresses this equation on three fronts. First, EnCase Enterprise, 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, even if the investigator had wanted to do so. Secondly, the elaborate, role-based security apparatus of the Enterprise Edition 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 environment and the resulting Evidence Files are encrypted with 128-bit AES encryption. In addition, when creating Evidence Files, EnCase Enterprise calculates CRC and MD5 checksums in the same manner as the standalone forensic version.

Positive Software v. New Century Mortgage

*Positive Software Solutions Inc. v. New Century Mortgage,* is a U.S. federal court case in which EnCase Enterprise Edition 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 "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 Edition or otherwise find that the forensic imaging that was conducted using EnCase Enterprise Edition 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."

While EnCase Enterprise has been used in hundreds of investigations to date, the Positive Software case is notable as it is a published decision that deals with evidence produced by EnCase Enterprise Edition, and implicitly accepts the process.
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,\textsuperscript{57} is an important federal 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\textsuperscript{58} 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.”\textsuperscript{59}

We have seen Daubert/Frye raised in most concerted challenges to EnCase. However, a corporate defendant advocating the EnCase-based evidence in Mathew Dickey v. Steris Corporation\textsuperscript{60} (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 meets the standards under both Rule 901 and Daubert,\textsuperscript{61} the recent 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 recent notable challenges to EnCase 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.”

Under the first prong of the test, courts have expressly noted that EnCase 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. Further, many agencies have tested EnCase in their labs before standardizing their agents with the software. Importantly, the widespread adoption of EnCase 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, recent publications have featured EnCase as the highest-rated tool in testing and comparisons among other commercially available software tools.

These reviews are among several industry publications featuring EnCase, 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 favorably. Among the more notable articles is the IEEE Computer Society publication, Computer Magazine, which featured a “case study” of the EnCase technology and reported on its widespread use and acceptance in the computer forensics community. 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.

A recent and 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.

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*, a recent case in Sonoma County, California where EnCase was subjected to a *Frye* analysis, the District Attorney investigator referenced in his testimony the above-mentioned IEEE Computer Society article and others currently available in the Newswire section of the Guidance Software website. 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. While all software programs contain bugs to varying degrees, the various tests and extensive usage of EnCase 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 or that performed by his/her agency. In the most detailed and documented published testing results of computer forensic software to date, *SC Magazine* notes that EnCase “outperformed all the other tools” that were tested by the magazine.

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*, 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, often they had not published their results. Additionally, test 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. Recently, however, the published testing landscape has changed considerably. In 2003 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.” (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 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 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 properly verified the imaged media in all such test scenarios.

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

- EnCase 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 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.” EnCase is without question the most widely used computer forensic process in the field. Over three thousand law enforcement agencies and companies worldwide employ EnCase for their computer investigations. In addition, EnCase has over eleven thousand users and Guidance Software trains over three thousand five hundred individuals annually in the use of EnCase. 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 is a commercially available tool with widespread general acceptance. Counsel should consider seeking judicial notice from the court of several of the Daubert factors as applied to EnCase, including its general acceptance, the fact that is commercially available and subject to widespread peer review.

§ 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. 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, 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.

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.” The court in United States v. Whitaker 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.

In United States v. Quinn, 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.” 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. In Burleson v. State, 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.\textsuperscript{84}

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.

\textbf{NOTE:} Please See Chapter 6 For a Detailed Analysis of State v. Cook and other Litigated Cases Addressing the Validity of the EnCase Process.

EnCase 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, 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 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 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."\(^{85}\)

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.\(^{86}\) 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.”\(^{87}\)

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 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 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.
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, 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. However, 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.”

However, it is not uncommon for an examiner to be asked to interpret the recovered data. The case of *United States v. Hilton* 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. PREFACE

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. BACKGROUND

[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

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. AUTHENTICATING THE ENCASE PROCESS UNDER RULE 901

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. ADDRESSING DAUBERT FACTORS
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. 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/O 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.91
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.95)

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 “[i]f 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 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 with them into Court for a more 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.93

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. BACKGROUND
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.

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

D. RECOVERY OF FILES “DELETED” FROM MULTIPLE 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 as 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. EVIDENCE FROM SWAP FILES

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 Defendant’s 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. EVIDENCE FOUND IN FILE SLACK
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.]

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. EVIDENCE OF WINDOWS METAFILES RECOVERED FROM UNALLOCATED CLUSTERS

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.
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 and Canada that essentially requires that, absent some exceptions, the original of a writing must be admitted 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 provides that “[t]o prove the content of a writing, recording or photograph, the original writing, recording or photograph is required….” Notably, electronic evidence falls under the Federal Rules definition of “documents.” 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 “[i]f 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.” 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.\textsuperscript{97}

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. A Texas Appellate Court recently ruled that an image copy of a hard drive qualifies as an "original" for the purposes of the Best Evidence Rule.\textsuperscript{98} The issue of whether an EnCase Evidence File suffices as an “original” under the Best Evidence Rule was recently 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.”\textsuperscript{99} This certainly is true in general. However, in Armstrong v. Executive Office of The President,\textsuperscript{100} 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.”\textsuperscript{101} 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.”\textsuperscript{102}

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 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 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.\textsuperscript{103} 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.
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.

§ 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." 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*, 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
Compression technology allows EnCase 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 in the same manner as uncompressed Evidence Files. EnCase 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 “[i]f 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 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
() Cr.: 00-11-1-M
()
(Harold Naparst

GOVERNMENT’S OBJECTION TO DEFENDANT’S MOTION FOR ACCESS TO COMPUTER EVIDENCE

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 January 14, 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.

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

\(^{1}\)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).
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
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 in either a DOS environment, or in a Windows environment, where a specially designed hardware write-blocking device is utilized. The ability of EnCase 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 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 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 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 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 38\textsuperscript{th} 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 is stored in a footer to the Evidence File and becomes part of the documentation of the evidence.

Throughout the examination process, EnCase 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 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 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](image)

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 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 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. 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, and EnCase will automatically report a verification error if the Case Info File is tampered with or altered in any way.

<table>
<thead>
<tr>
<th>EnCase Report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Case:</strong> CIN Investigation</td>
</tr>
<tr>
<td><strong>Evidence Number “2000-11-2”</strong></td>
</tr>
<tr>
<td>File &quot;C:\EnCase\Quantum.E01&quot; was acquired by Sheldon at 05/22/00 05:50:44PM. The computer system clock read: 05/22/00 05:50:46PM.</td>
</tr>
<tr>
<td><strong>Acquisition Notes:</strong></td>
</tr>
<tr>
<td>Copyright 2000 Guidance Software, Inc..</td>
</tr>
<tr>
<td><strong>File Integrity:</strong></td>
</tr>
<tr>
<td>Completely Verified, 0 Errors. Acquistion Hash: 7E75AB52735960245330533EAA246A6A Verification Hash: 7E75AB52735960245330533EAA246A6A</td>
</tr>
</tbody>
</table>

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 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 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 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.

§ 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, 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 generates and records concurrent to acquisition can only be read and reported by EnCase. The continual verification by EnCase 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 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. EnCase is a carefully designed process 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 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 can be independently verified by disk utilities such as the Norton tools when utilizing the precise disk location information automatically provided by EnCase. 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 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 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. 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 is not designed to mount or “crack” other proprietary file images.
Challenges to EnCase and Other Litigated EnCase Issues

Computer forensic investigators throughout the world utilize EnCase for the seizure, analysis and court presentation of computer evidence. With over 8,000 licensed users, computer evidence processed with EnCase 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. 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 even fewer instances — namely two — 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 the their subject jurisdiction, while providing compelling “persuasive authority” everywhere else. In addition, recently courts in Canada, Australia, and Singapore have published decisions accepting evidence gathered using EnCase.

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

**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.” 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 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.” The court also specifically noted that the investigator was trained in the use of the EnCase. 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."\textsuperscript{109}

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).

\textit{Taylor v. State}

\textit{Taylor v. State}, 93 S.W.3d 487 (2002 Tex.App) is another recent appellate decision that addresses the EnCase software, although not to the same degree as \textit{Cook}. Taylor involved several different issues on appeal, most of which did not involve EnCase. The issue that did address EnCase 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.\textsuperscript{110} 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 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.

\textit{Matthew Dickey v. Steris Corporation}

The first known instance of a “serious” challenge to the use of EnCase 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 would be allowed, overruling objections from the Plaintiff. In \textit{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 \textit{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. 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. 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, 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 where the defense brought an unsuccessful suppression motion to exclude from trial all computer evidence obtained through a forensic investigation utilizing EnCase. 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 was essentially providing “expert testimony” and that the defense was unable to cross-examine the government witness in detail regarding how EnCase works and how it was developed; and 2) That EnCase should be subject to a Frye 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, and that EnCase 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, 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 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. The Court determined that EnCase 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 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, which
was addressed at length in Vol. 1, issue 3 of the Journal. 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 where the court
subjected EnCase to 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 should be
subject to a Frye 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 state courts, while Daubert, a
variation of Frye, but based upon the same basis principles, 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, but there is no
known record of such tests being applied to the concept of computer forensics.

Upon the conclusion of the hearing, the defense conceded that EnCase was an
"appropriate and accepted" methodology under the Frye test for recovering computer
evidence. After finally admitting that EnCase 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 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 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 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 as a valid and accepted process.

United States v. Habershaw

In United States v. Habershaw, 2001 WL 1867803 (2002 D.Mass.), the court upheld the legality of a computer search by a computer forensic expert, David Papagiris, over the defendant’s objections. While not reflected in the court’s published opinion, EnCase was used by the experts for both the prosecution and the defense. The expert report submitted to the court by David Papagiris 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. Papagiris then conducted a computer forensics analysis of the hard drive, finding a great deal of incriminating evidence.

There are several compelling rulings and lesions 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 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. Pagagiris arrived on the scene and saved the day. The expert report submitted to the court by Papagiris (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. Papagiris’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. Pagagiris was able to show that while files were accessed during the time when the case agent was on the scene, but before Mr. Papagiris 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 Papagiris. 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. Papagaris 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 (May 1999 Calif. Sup.Ct., San Francisco), 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 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 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.

This development is potentially significant in light of the legal requirements for the admission of electronic evidence and the “best evidence rule,” as further discussed below. 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 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.\textsuperscript{120}

\textit{Kucala Enterprises, Ltd. v. Auto Wax Co., Inc.}

In this recent civil case, the issue was not the acceptability of evidence gathered with EnCase. Rather, the magistrate judge addressed the use of a wiping program, Evidence Eliminator, by the plaintiff.\textsuperscript{121} 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 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 propriety 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.\textsuperscript{122} 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.
Other Jurisdictions

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 in *Regina v. Cox* 123. In that child pornography case, the Royal Canadian Mounted Police had used EnCase 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 is used, and ruled that the images and the forensic report produced by EnCase were relevant evidence, but that the software itself was a tool used by experts, and not evidence.

Similarly, the Federal Court of Australia recently addressed EnCase software in *Sony Music Entertainment (Australia) Ltd. v. Univ. of Tasmania, et al.*, 124 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 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 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.”

In 2002 an appellate court in Singapore, in upholding a murder conviction, relied on evidence recovered through the use of EnCase. 125 The Techno Forensic Branch of the Technology Crime Division of the Criminal Investigation Department of the Singapore Police had used EnCase 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.
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. Ne wsgroups:

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 a 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...
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 newsgroups 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
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 --
§ 7.0 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. The plain view doctrine, for example, is an area that becomes more complex as EnCase allows forensic examiners to view, sort and manage many more files than previously possible with command line utilities.

The remote preview function of EnCase 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 their computer if the preliminary exam can be done quickly and without “impounding” their 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 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. 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 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. 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. 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.'" 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.

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 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. In United States v. Upham, 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. The court noted that from a legal standpoint, the recovery of deleted files is "no different that decoding a coded message lawfully seized or pasting together scraps of a torn-up ransom note."

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. In United States v. Lacy, 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, 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. 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.

§ 7.2 United States v. Carey

The case of United States v. Carey 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." 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. 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. 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. 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." 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." 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."

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.” 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.”

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.'(citations)
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.”

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.” 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.” 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.155 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.”156 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.”157

§ 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 another court has addressed the Plain View Doctrine in the context a forensic text string search of computer files but without a discussion Carey. These decisions provide some indications as to the impact of the Carey decision.

In United States v. Gray,158 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.159 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.160 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. 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.” 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.

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.”

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.” 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.

In United States v. Scott-Emuakpor, 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, 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.” 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. 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.” The investigating agent utilized EnCase for this process and his overall computer investigation. 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.

In Wisconsin v. Schroeder, 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.”

In Frasier v. State, 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. 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.

§ 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. By logical extension, results from aggregate hash file analysis, signature mismatch analysis and other automated functions featured in EnCase 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 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 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*,177 (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 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 judges are becoming more sophisticated regarding computer evidence, as the discussion by the *Frasier* court shows. While *Carey* has not been directly overruled, there is a long body of cases that seek to distinguish the *Carey* holding. As of December 2003, fourteen cases have distinguished *Carey*; not one has followed it. Certainly investigators located in the Tenth Circuit should be aware of the *Carey* holding and conform their actions to it. However, there appears now to be little chance that the *Carey* reasoning will spread to other jurisdictions.
§ 7.5 Warrant Return Requirements

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, often 30 days. "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. 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. Further, as demonstrated by Steve Jackson Games v. United States, an agency may be exposed to civil liability for unreasonably retaining custody of seized computer media.

This is one area where EnCase presents a double-edged sword for law enforcement. If all federal magistrates were educated as to the capabilities of the software, we would unfortunately see further time constraints being placed upon the analysis of seized computer media. (This is one reason why this publication is privately disseminated). 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 an the disks for information that may have been ‘deleted.’" United States v. Upham, (analyzing forensic processes utilized by U.S. Customs in early 1997, before the agency’s adoption of EnCase). 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, opined, “until technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur.”

Thus, it is only a matter of time before warrant return requirements of 10 days or less become the standard for computer examinations. A clear example is the Southern District of the 9th Circuit (San Diego) where magistrates are now routinely mandating on-site computer examinations when issuing warrants to be executed at business establishments. Not coincidently, the San Diego Regional Computer Forensics Lab resides in the Southern District of the 9th Circuit, and the capabilities and expertise of the lab are widely known by the local bench.
Complying with Discovery Requirements 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 typical 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 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 includes a feature that allows the examiner to easily restore an EnCase image to a separate drive. EnCase version 2.11+ 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. This approach is essentially the only option where the computer evidence consists of contraband, such as child pornography. Ideally, the expert would utilize EnCase 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 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., 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 As a Process for Civil Litigation
Computer Discovery

§ 9.0 Overview

A few years ago, in the days of command-line analysis utilities, attorneys typically employed computer forensic experts only in high-stakes, high-expense litigation and corporate investigation matters. Back then, many civil litigants resisted court-ordered computer discovery by convincing judges that a proper forensic analysis of a four GB hard drive would cost upwards of $40,000.00 in expert fees. In the 1997 case *Alexander v. Federal Bureau of Investigation*, 184 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 recent as July 1999, counsel advanced the argument in one well-publicized federal litigation that e-mail discovery was “simply not feasible.” 185

EnCase has played an important role in the recent expansion and acceptance of computer forensics consulting by providing a much more efficient process. The few government agencies that still rely on command-line analysis utilities as their principal tool set may have understandable reasons to do so. Concerning business and litigation consulting, however, where fees often exceed $300 per hour, no justification exists for primarily utilizing command-line utilities for forensic analysis. Previously, even though civil trial lawyers recognized the importance of computer evidence discovery involving the assistance of computer forensic experts, these enormous financial constraints generally limited the practice to only the most well financed lawsuits. However, EnCase now provides a much-improved platform for the forensic investigation and recovery of data from computers.

However, we unfortunately still hear on occasion complaints about astronomical bills from consultants who examined only 10 or 15 GBs of data. Such scenarios are not only a disservice to the clients; they are harmful to our industry by discouraging electronic evidence discovery and potentially creating bad law. The EnCase-using majority can enjoy a distinct competitive advantage by assuring their existing and potential clients that they employ the latest generation of computer forensic software.
§ 9.1 Courts Now Treat Computer Discovery as a Mandated and Routine Process

Until recently, 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. However, some very important decisions in the past year have dramatically shifted the e-discovery landscape. Setting the tone is the case of In Re Bristol-Meyers Squibb Securities Litigation,\(^\text{186}\) where the court unequivocally states 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\(^\text{187}\) 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 e-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.

Recently, 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.\(^\text{188}\) 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. Recently, 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. 189

Thus, courts are becoming more sophisticated regarding the sophisticated technology, such as EnCase, available to litigants for computer evidence preservation and retrieval. Several other courts have recently issued decisions consistent with this trend of requiring expedient and full compliance with computer evidence discovery requests. (See, Antioch Co. vs. Scrapbook Borders, Inc. 190, Tulip Computers International vs. Dell Computer 191). Moreover, courts continue to severely punish litigants who fail to preserve and/or alter computer evidence when a lawsuit is pending. Metropolitan Opera Association v. Local 100, Hotel And Restaurant Employees Int’l Union 192, 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 Section 6, above..

These cases establish that enterprises and their consultants responding to computer discovery must demonstrate technical and organizational competence in the ability to complying with subpoenas for production of the relevant data and to properly preserve and acquire the 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/EED experts or having the appropriate resources and court-validated technology employed internally to get the job done. Among the 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 Improved 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 four 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., 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. Additionally, the appointment of a single computer forensic consulting firm to act as special master is another important recent 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 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* 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.

**Zubulake**

Judge Shira Scheindlin, in a series of opinions in the *Zubulake v. UBS Warburg* dispute, 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, 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.’” 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.

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. 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.”

**U.S. v. Regan**

In *U.S. v. Regan*, 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 backup 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, backup 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 backup tapes... limit[ing] their retrievals to document[s] and email relevant” to the case and the plaintiff.203

• 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\textsuperscript{204}). 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 \textit{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.

\section*{§ 9.3 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.

\texttt{<DATE>}

\texttt{______________}

\texttt{©2001-2004 Guidance Software, Inc. 93 December 2003}
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. 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,

_____________
§ 9.4 Law Firms and Computer Forensics

Many law firms are moving beyond simply retaining computer forensics experts by training their own IT staff, associates and paralegals in the practice of computer forensics analysis. These progressive firms are working in conjunction with their computer forensics experts by conducting their own or supplementary low level analysis, and leaving the imaging and higher level analysis to their experts. Attorneys and other members of the firm should never be in a position of collecting evidence in a pending or potential litigation matter, unless they do not intend to represent the client at trial and thus will be able to testify as material witnesses.

Under this model, the law firm obtains the Evidence Files and Case files (with the case bookmarks, text searches and hits, etc) from their experts, enabling the firm to view in full context all the evidence, search hits and bookmarks created by the expert. While the expert obviously has superior technical expertise, it is often difficult for the expert to decipher the importance of recovered information. A random bit of text in file slack may mean nothing to the expert, but may be very important information to the attorney, who has a much better command of the facts in any given case.

Young associates and paralegals in large law firms typically review thousands of pages of documents each day in complex litigation matters. A natural progression of this practice, already seen in some law firms, involves tech savvy attorneys and paralegals conducting their own computer forensics analysis. This enables the law firm personnel to review their own “boxes of documents” as they normally do in other litigation.

In addition to computer forensic analysis, many law firms use Encase as a document management tool, as modern-age discovery is often produced on hard drives, CD-ROMs, and zip disks. A growing number of firms have discovered that imaging these hard drives and other media allows them consolidate all the data into one “case”, thereby taking advantage of the information management and analysis capabilities of the EnCase software, such as keyword searches, bookmarks, the report, file sorting, and for images, the gallery view.

With information being exchanged on many forms of computer media and computer files, many law firms are also turning to computer forensics software for information assurance compliance. If an attorney is providing information stored on computer media to a third party, that media should be reviewed with computer forensic software to insure that there is no privileged information or other confidential client data residing in a “deleted” file, slack or unallocated space. The same is true for certain compound files such as Word documents and Excel spreadsheets, where computer forensic software can analyze and recover prior revisions and other normally hidden information contained within such compound files.
§ 9.4 Resources for Electronic Evidence Discovery

Computer forensics in civil litigation (also referred to as “electronic evidence discovery”) is a new but 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/law_business_digitaldisc.asp

- http://californiadiscovery.findlaw.com/El_disco.htm is a site maintained by a 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.

- Overly On Electronic Evidence In California is a notable treatise on the subject, written by Michael Overly, and published by the West Group. This informative work discusses electronic discovery evidence in depth, and also addresses issues related to the authentication of computer evidence.

- www.encase.com The Guidance Software website contains numerous resources, including legal resources, message boards, whitepapers and other reference materials and links.
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, 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, 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 before any such monitoring can take place. 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.

Balancing of Interests

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. 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. 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. In Blakey v. Continental Airlines, 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.” Thus, with the employers’ interest in preventing theft and unauthorized activity coupled with the possibility of third 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 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, 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
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.

**UK Approach**

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. If an employer wishes to monitor electronic communications, it should “establish a policy on their use and communicate it to workers.” The policy should set forth clearly the extent, if any, to which employees can use email or the Internet for non-business purposes. Finally, when monitoring emails, employers should review only address and subject, “unless it is essential for a valid and defined reason to examine content.”

§ 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, 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. 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. The language in the ECPA prohibiting disclosure of electronic communications only applies to those entities that provide electronic communication services “to the public,” 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. 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*, 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 ECPA 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. 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."

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. 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.

*Fraser v. Nationwide Mutual Insurance Co.* 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*, 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. Other courts have reached similar conclusions regarding the definition of interception as used in the ECPA. However, at least one court in a more recent decision has 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." 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, 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. 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 recent 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.” 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. Included within these aggressive plans for digitizing the federal workplace are equally aggressive e-mail monitoring programs. Unlike their private sector counterparts, federal employees are afforded a degree of protection under the Fourth Amendment’s prohibition against unreasonable search and seizures. 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.

United States v. Simons 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).

As far as the entry into Simons’ office to seize his hard drive, 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. 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. 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.” 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]."
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.
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.)


5 200 F.3d 627 (9th Cir. 2000), United States v. Tank, supra, 200 F.3d at 629

6 Id. at 630

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

8 Id. at 631

9 Id.

10 Id.

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


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


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.


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

36 Id. at 100

37 Id. at 97

38 Id. at 99


40 Id. at 368.

41 Id. at 370

42 Id

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

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, 775 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
52 See Bonallo, 858 F.2d at 1436.
53 See, e.g., 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)
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 defensible search and seizure reasonably likely to obtain the [sought after] images")
57 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed.2d 469 (1993)
58 Frye v. United States, 293 F. 1013 (D.C.Cir.1923).
59 See, United States vs. Beasley, 102 F.3d 1440, 1448 (8th Cir. 1996) (judicial notice taken of reliability of the PCR method of DNA typing).
63 See discussion at 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). United States v. Weatherspoon, 581 F.2d 595, 598 (7th Cir. 1978) (same)
64 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.”
65 In addition to the recent SC Magazine test review noted above, EnCase has received dozens of favorable reviews and mentions in industry publications, which are available for review and download at: www.guidancesoftware.com/corporate/Press%20Room/2002index.shtm
67 Sonoma County, California Superior Ct. no SCR28424.
69 162 F. Supp. 2d 1097, 1103 (D. Alaska 2001)
70 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
71 (Daubert, 113 S.Ct. 2797, 125 L.Ed.2d 483.)
72 State of Washington v. Leavell (Okanogan County, Washington Superior Ct. no. 00-1-0026-8)
73 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.
74 “-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. Lagash (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]
75 526 U.S. 137, 119 S.Ct. 1167 (1999)
An excellent discussion of this debate can be found at *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)*.

*United States v. Downing* 753 F.2d 1224, 1240, fn. 21, (3rd Cir. 1985)

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

*United States v. Whitaker*, supra, 127 F.3d at 600

18 F.3d 1461 (9th Cir. 1994)

*United States v. Quinn*, supra, 18 F.3d at 1465

Id.


*United States v. Liebert*, 519 F.2d 542, 547 (3rd Cir. 1975); *United States v. Weatherspoon*, 519 F.2d 547, 549 (7th Cir. 1978).

Id.

18 F.3d 1461 (9th Cir. 1994)

*United States v. Liebert*, 519 F.2d 542, 547 (3rd Cir. 1975); *United States v. Weatherspoon*, 581 F.2d 595, 598 (7th Cir. 1978).

Id.

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


1 F.3d 1274 (D.C. Cir 1993)

*Armstrong v. Executive Office of The President*, supra, 1 F.3d at 1280

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.”])

135 F. Supp. 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.

*Fed. R. Evid.* 1002

*Fed. R. Evid.* 1001(1)

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.”

Civil Evidence Act 1995 (c.38) at § 8.


777 N.E.2d at 886

Id.

777 N.E.2d at 887

*Taylor v. State*, supra, 93 S.W.3d 487, 507-08

Okanogan County Cause no. 00-1-0026-8

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

90 Wash.App. 100; 950 P.2d 1024

Sonoma County, California Superior Ct. no SCR28424.

Frye v. United States, supra.


168 F.3d 532, 537 (1st Cir. 1999)

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). United States v. Weatherspoon, 581 F.2d 595, 598 (7th Cir. 1978) (same)


Let Wee Teang Anthony v. Public Prosecutor, Court of Appeal, Criminal Appeal No. 27 of 2001 (April 19, 2002).


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.


United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999)


152 F.3d 1241 (10th Cir.1998)

United States v. Simpson, supra, 153 F.2d at 1248.

168 F.3d 532 (1999)

United States v. Upham, supra, 168 F.3d at 535

Id. at 537.

See Davis v. Gracye, 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).

119 F.3d 742, 745 (9th Cir. 1997)

58 F.3d 423, 426 (9th Cir.1995)

United States v. Kow, supra, 58 F.3d 423 at 427

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.”)

172 F.3d 1268 (10th Cir. 1999)

United States v. Carey, supra, 172 F.3d at 1272-1273.

Id., at 1271

Id.

Id.

Id. at 1272

Id.

Id. at 1274

Id. at 1273

Id. at 1275

Id.
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, at 1273.

Concurring opinion of Judge Baldock, Carey, at 1277

Id. at 196.
Id. at 197

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).

United States v. Scott, supra, 183 F.Supp.2d at 197-198
2000 WL 675942, Wisconsin Supreme Court Decision
794 N.E.2d 449, 452-54.
supra, 78 F.Supp.2d at 526
supra, 76 F.Supp.2d at 42
36 F.3d 457, 462 (5th Cir. 1994)
supra, 168 F.3d 532
supra, 13 F.Supp.2d at 583
194 F.R.D. 639 (SD Ind. 2000)
188 F.R.D. 111, 117 (1998 D.C. Cir)
Playboy Enterprises v. Welles, 60 F.Supp.2d 1050, 1054 (S.D. CA 1999)
306 F.3d 99 (2nd Cir 2002)
210 F.R.D. 645 (D Minn 2002)
2002 WL 818061 (D DE 2002)
212 F.R.D. 178 (S.D.N.Y. 2003),
supra, 194 F.R.D. 639
July 18, 2000 phone interview with Shawn Howell of Computer Forensics, Inc.
204 F.R.D. 277 (E.D.Va. 2001)
2002 WL 63190 (S.D.N.Y.)
217 F.R.D. at 317.
See 217 F.R.D. at 322.
201 216 F.R.D. at 291.
204 43 F.Supp.2d 951, 954 (E.D. Ill 1999)
207 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”
210 See Id.
211 751 A.2d 538
212 Smyth v. Pillsbury Co., supra, 914 F.Supp at 100.
213 272 F.3d 741 (2002)
217 Employment Practices Data Protection Code at § 3.3.1.
218 Employment Practices Data Protection Code at § 3.3.1.
219 Employment Practices Data Protection Code at § 3.3.8.
222 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”).
224 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."
226 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.
227 See Id. at 1236
228 Steve Jackson Games, supra, 36 F.3d at 463
229 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); United States v. Reyes, 922 F. Supp. 818, 836-37 (S.D.N.Y. 1996) (same).
231 36 F.3d at 463
232 Steve Jackson Games, supra, 36 F.3d at 463
at the time of transmission from the retrieval of such a communication after it has been put into ‘electronic storage.”

234 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.”).

236 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.

235 See § 9.01

236 California SB1016, sponsored by Debra Bowen, D-Redondo Beach.

237 Smyth v. Pillsbury Co., supra, 914 F.Supp at 100 (recognizing the theoretical possibility of such a claim).


241 O’Connor, 480 U.S. at 717, 107 S.Ct. 1492; id. at 737, 107 S.Ct. 1492 (Blackmun, J., dissenting).

242 206 F.3d 392 (4th Cir 2000)

243 Id. at 398, fn. 9.

244 Id. at 399-400.

245 United States v. Simons, supra, 206 F.3d at 399, fn 10.

246 Id. at 726, 107 S.Ct. 1492

247 Id. (citing New Jersey v. T.L.O., 469 U.S. 325, 342, 105 S.Ct. 733, (1985)).