



An NIJ Program hosted by UCF

*Digital Evidence in the Courtroom:
A Guide for Preparing Digital
Evidence for Courtroom Presentation*

MASTER DRAFT DOCUMENT

Revised March 12, 2003

The National Center for Forensic Science

Blank Page

Table of Contents

Introduction (to be drafted by the TWG) (p. 5-6)

Section A: 'Search and Seizure Issues' (pp. 7-19)

Section B: 'Integrity, Discovery, and Disclosure of Electronic Evidence (pp. 21-30)

Section C: 'Courtroom Preparation and Evidence Rules' (pp. 31-49)

Section D: 'Presentation of Digital Evidence' (pp. 51-59)

Appendices:

'Disclosure Rules of ECPA' (to be drafted by Section A)

'Sample Consent Form' (to be drafted by Section A)

Glossary (each sub-committee will be responsible for identifying/defining terms relevant to their sections)

Blank Page

Introduction¹

An oft-quoted statistic claims that it took radio 34 years to have 50 million listeners, television 13 years to secure 50 million viewers, and the Internet only 4 years to have 50 million users. Whether those statistics are completely accurate or not, there can be no doubt that new technology is adapted by large portions of the populace at an increasingly rapid pace.

One problem this creates is the technology becomes widespread long before society has developed a shared ethic governing its use and even longer before the legal system is adequately prepared to deal with the new technology.

Although computers and digital evidence have existed for more than 60 years, the age of computers on workers' desks, computers in the home, computers in children's bedrooms and computers in the hands of criminals is of much more recent vintage. As computers have spread into more hands, high technology crime has become far more prevalent.²

Child pornography cases, for example, for years, until the mid-1990s, involved magazines and real photographs. That started to change with the spread of the Internet so that now it is rare to find a child pornography case involving anything other than digital evidence (and occasionally printouts of the digital evidence.)

Digital evidence, once the province of classic "computer crime" cases like hacking and intrusion, is now being found in cases in every crime category – from harassment to homicide, from drug dealing to securities fraud. This rapid growth in the number of criminal cases involving digital evidence has all-too-often found law enforcement and the judiciary ill prepared to deal with the new issues created by this evidence.

This Guide is intended to help fill the gap between the level of current knowledge of digital evidence and the knowledge needed to successfully deal with digital evidence in the future. The Guide presents practical advice on dealing with digital evidence, from the acquisition of the evidence to the use of the evidence in court, including search and seizure issues, maintaining the integrity of digital evidence, disclosure and

¹ Designated members of the TWG will draft an 'Introduction.'

² High technology crimes may be defined as offenses that have been created or made possible by the advent of technology. They may also include traditional crimes that have been so transformed by computer technology that an understanding of that technology is essential to an understanding of the case.

High technology offenses include computer crimes (offenses in which the computer is the primary instrument used to facilitate the crime), computer-related crimes (computer used to facilitate the crime or to serve as a repository of evidence of a crime), and Internet-related crimes (Internet used to facilitate the crime). For a comprehensive list of examples, see the NIJ guide *Electronic Crime Scene Investigation: A Guide for First Responders*.

discovery, trial preparation, evidence rules and the presentation of digital evidence in the courtroom.

Section A: Search and Seizure Issues

1. Introduction

The **Wiretap Act**, the **Pen Register and Trap and Trace Statute**, the **Electronic Communications Privacy Act**, and the **Privacy Protection Act** are federal statutes governing access to and disclosure of certain types of information deemed deserving of special treatment by Congress. State constitutional and statutory provisions, industry-specific federal acts, and recent court decisions may provide additional rules in particular cases, although discussion of those sources of law are outside the scope of this guide.

These statutes impose rules on the gathering of certain types of evidence in the course of criminal investigations. Investigators and prosecutors should be familiar with these rules, since their breach may result in evidentiary challenges or civil suit. The fourth and fifth amendments to the federal Constitution also play significant roles in the course of an investigation.

Note: A comprehensive analysis of federal search and seizure issues, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, can be found at www.cybercrime.gov/searchmanual.htm.

2. Wiretap Act

Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2501 et seq.

The Wiretap Act focuses on the interception of the content of communications while the communications are in transit. Examples of such interceptions could include wiretapping a telephone, placing a listening device or ‘bug’ in a room to pick up conversations, and installing ‘sniffer’ software that captures a hacker’s instant messages. The Wiretap Act also governs the disclosure of intercepted communications.

The Wiretap Act generally and broadly prohibits anyone in the U.S. from intercepting the contents of wire, oral, or electronic communications unless one of several exceptions applies. As a basic rule, the Wiretap Act prohibits anyone who is not a participating party to a private communication from intercepting the communication between or among the participating parties using an ‘electronic, mechanical, or other device,’ unless one of several statutory exceptions applies.

One exception includes the issuance of a court order by a court of competent jurisdiction authorizing interception. The requirements to obtain such an order are substantial.

Violation of the Wiretap Act can itself constitute a crime and may lead to civil liability. In the case of wire and oral communications (i.e., communications of the human voice), violation of the Wiretap Act may result in the suppression of evidence. To ensure compliance with the Wiretap Act, agents and prosecutors should initially determine whether:

- The communication to be monitored is one of the protected communications defined in the statute.
- The proposed surveillance constitutes an ‘interception’ of the communications.

If both conditions are present, the agent or prosecutor should evaluate whether a statutory exception applies that permits the interception.

Note: Some states have versions of the Wiretap Act that are more restrictive than the federal act. The federal act does *not* pre-empt these laws unless federal agents are conducting the investigation. State and local law enforcement agents must comply with any such state act, even if there is no violation of the federal Wiretap Act.

3. Pen/Trap Statute

Pen Register and Trap and Trace Statute, 18 U.S.C. § 3121 *et seq.*

The Pen/Trap statute governs the real-time acquisition of dialing, routing, addressing, and signaling information relating to communications. Unlike the Wiretap Act, the Pen/Trap statute does not cover the acquisition of the content of communications; rather, it addresses the information about communications. Historically, the term ‘pen register’ refers to a device that records outgoing connection information. A ‘trap and trace’ device, on the other hand, records incoming connection information. For example, a pen register captures the telephone number dialed by an individual under surveillance, while a trap and trace device captures the telephone number of the party that is calling the individual under surveillance.

The Pen/Trap statute applies not only to telephone communications, but also Internet communications. For example, every e-mail communication contains ‘to’ and ‘from’ information. A pen/trap device captures such information in real-time.

The Pen/Trap statute generally forbids the nonconsensual real-time acquisition of non-content information about a wire or electronic communication, unless a statutory exception applies. Where there is no applicable exception to this prohibition, law enforcement agents must obtain a pen/trap order from the court before acquiring non-content information covered by the statute.

Note: Examples of requests for federal pen/trap orders may be found at *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (www.cybercrime.gov/searchmanual.htm). Some states have versions of the Pen/Trap statute that are more restrictive than the federal act. The federal act does *not* pre-empt these laws unless federal agents conduct the investigation. State and local law enforcement agents must comply with any such state act, even if there is no violation of the federal Pen/Trap statute.

4. ECPA

Electronic Communications Privacy Act, 18 U.S.C. § 2701 *et seq.*

The stored communications chapter of the Electronic Communications Privacy Act (ECPA) provides the customers and subscribers of certain communications service providers with privacy protections. This statute protects records held by providers about customers and subscribers (such as billing records), as well as files stored by the providers for customers and subscribers (such as e-mail or uploaded files). Depending on the type of provider, ECPA may dictate what type of legal process is necessary to compel a provider to disclose specific types of customer/subscriber information to law enforcement agents. ECPA also limits what a provider may and may not voluntarily disclose to others, including the government (see Appendix ‘X’ for a quick reference guide to the disclosure rules of ECPA).³

ECPA applies when the government agent seeks to obtain records about a customer or subscriber from a provider of communications services (e.g., an Internet Service Provider (ISP) or cellular phone provider). For example, ECPA applies when a government agent seeks to compel an ISP to turn over copies of a customer’s e-mail. ECPA does not apply when the agent seeks to obtain the same e-mail from the customer’s computer.

ECPA provides that the production of some information may be compelled by subpoena, some by court order, and some by search warrant. Generally, as the level of government process escalates from subpoena to 2703(d) order to search warrant, the information available under the less exacting standard is included at the higher level (e.g., a search warrant grants access to basic subscriber information, transactional information, and content of the stored communication).

³ Section A will be responsible for drafting this appendix.

Hint: Because providers may use different terms to describe the different types of data that they hold, it is advisable to consult with them on the preferred language when drafting the request.

A. Subscriber and Session Information: Subpoena

Under ECPA, a law enforcement agent may use a subpoena to obtain certain information listed in ECPA relating to the identity of a customer/subscriber, the customer/subscriber's relationship with the service provider, and basic session connection records. Specifically, a subpoena is effective to compel a service provider to disclose the following information on the customer/subscriber:

1. Name.
2. Address.
3. Local and long distance telephone connection records, or records of session times and durations.
4. Length of service (including start date) and types of service utilized.
5. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address.
6. The means and source of payment for such service (including any credit card or bank account number).

Notably, this list does not include extensive transaction-related records, such as logging information revealing the e-mail addresses of persons with whom a customer corresponded during prior sessions, or 'buddy lists.'

B. Other Non-Content Subscriber & Session Information: 2703(d) Order

A law enforcement agent will need to obtain a court order under 18 U.S.C. § 2703(d) to compel a provider to disclose more detailed records about the use of the services by a customer/subscriber. These records could include, for example:

1. Account activity logs that reflect what IP addresses the subscriber visited over time.
2. E-mail addresses of others from whom or to whom the subscriber exchanged e-mail.
3. 'Buddy lists.'

A law enforcement agent can also use 2703(d) order to compel a cellular telephone service provider to turn over, in real time, records showing the cell-site location information for calls made from a subscriber's cellular phone.

This information shows more of the subscriber's use of the system than that available by subpoena, but it does not include the content of the communications.

To obtain a 2703(d) order, law enforcement may go to any federal magistrate or district court with jurisdiction over the offense under investigation. State court judges authorized by the law of the state to enter orders authorizing the use of a pen/trap device may also issue 2703(d) orders. The application must offer 'specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.'

Note: In general, ECPA provides more privacy protection to the contents of communications and files stored with a provider than with records detailing the use of the service or the subscriber's identity. Please refer to *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (www.cybercrime.gov/searchmanual.htm) for examples of applications for an order under 2703(d).

C. Content of Stored Communications

ECPA distinguishes between communications in storage that have already been retrieved by the customer or subscriber, and those that have not. In addition, the statute distinguishes between retrieved communications that are held by a private provider (e.g., an employer who offers e-mail services to employees and contractors only) and those held by a provider that offers its services to the public generally.

1. Retrieved Communications Held by Private Provider: Subpoena

ECPA only applies to stored communications that a customer or subscriber has retrieved, but left on the server of the communication service provider, if the service provider offers those services to the public. If the provider does not offer those services to the public, there are no constraints imposed by ECPA on the right of the provider to disclose such information voluntarily. ECPA does not require any heightened or particular legal process to compel disclosure of such records.

For example, ECPA does not apply to a government request to compel an employer to produce the retrieved e-mail of a particular employee if the employer offers e-mail services and accounts to its employees but not to the public generally. The agent could instead use a subpoena or other process.

Note: ECPA may apply if the e-mail sought by the agent resides on the employer's server and has not yet been retrieved by the employee. In this instance, the rules discussed under Section 4.C.3 ('Unretrieved Communications: Search Warrant') apply (see below).

2. Retrieved Communications, Unretrieved Communications older than 180 Days, and Other Files Stored with a Public Provider: Subpoena or 2703(d), with Notice

ECPA *does* apply to stored communications that a customer or subscriber has retrieved (but left on the server of the communication service provider) if the service provider offers those services to the public. Such communications include text files, pictures, programs, or any other files that a customer may have stored on the public provider's system. Under the statute, such a provider is considered a 'remote computing service' and is not permitted to voluntarily disclose such content to the government.

A law enforcement agent may use either a subpoena or a 2703(d) court order to compel a public service provider to disclose the contents of stored communications retrieved by a customer or subscriber. The agent in either case, however, *must give prior notice to the customer or subscriber of the request*. Another provision in ECPA allows agents to delay the notice to the customer or subscriber when notice would jeopardize a pending investigation or endanger the life or physical safety of an individual. At the end of the delayed notice period, the agent must send a copy of the request or process to the customer or subscriber, along with a letter explaining the delay.

If the agent uses a subpoena to compel the disclosure of stored, retrieved communications from a public service provider, the agent may seek to delay notice for ninety days 'upon the execution of a written certification of a supervisory agent that there is reason to believe that notification of the existence of the subpoena may have an adverse result.' If the agent uses a 2703(d) order, the agent may seek permission from the court to delay notice as part of the application for the order.

Agents may also use a subpoena with prior notice, or a 2703(d) order with prior notice, to compel a service provider to disclose communications that are unretrieved but have been on the server more than 180 days. As a practical matter, most providers will not allow unretrieved messages to stay on a server unaccessed for such a long period.

Note: When a government agent seeks to compel a public service provider to produce the contents of communication, the agent must give notice to the customer or subscriber when using a subpoena or 2703(d) order. Notice may be delayed under appropriate circumstances. If using a search warrant or seeking non-content information, no notice is required.

3. Unretrieved Communications: Search Warrant

Unretrieved communications (including voice mail) held by the provider for 180 days or less have the highest level of protection available under ECPA. ECPA covers such communications whether the service provider is private or public. The service provider is generally not permitted to voluntarily disclose unretrieved communications to the government.

For example, under ECPA an e-mail sent to a customer is considered unretrieved if it resides on the server of the customer's provider (*i.e.*, an ISP or the customer's employer) waiting for the customer to log on and download the message. Once the customer downloads the e-mail (but leaves a copy on the server of the provider), the e-mail is deemed retrieved. Please refer to Section 4.C.1 ('Retrieved Communications Held by the Private Provider') for more detail about retrieved communications.

The agent may seek a search warrant, such as a warrant provided by 2703(a), to compel the production of unretrieved communications in storage with a service provider. No prior notice is required to the customer or subscriber.

D. Remedy: Civil Damages

Civil damages are the exclusive remedy for violation of EPCA. Except in cases where the constitutional rights have been infringed or suppression is provided by some other statute or source of law, evidence seized in violation of EPCA alone will not be suppressed.

5. PPA

Privacy Protection Act, 42 U.S.C. § 2000aa *et seq.*

The PPA limits law enforcement's use of a search warrant to search for or seize certain materials possessed by a person for disseminating a 'public communication' to the public. These protected materials may be either 'work product' (*i.e.*, materials created by the author/publisher) or 'documentary materials' (*i.e.*, any materials that document or support the work product).

For example, a person who is creating an online newsletter may possess interview notes that could be considered ‘documentary materials,’ whereas the text of the newsletter to be published could be considered ‘work product’ materials. The PPA applies only to law enforcement. If the material is covered by the PPA, law enforcement cannot use a search warrant to compel its production.

The PPA’s prohibition on the use of a search warrant does not apply in the following circumstances:

1. Materials searched for or seized are contraband, fruits, or instrumentalities of the crime.
2. There is reason to believe that the immediate seizure of such materials is necessary to prevent death or serious bodily injury.
3. There is probable cause to believe that the person possessing the materials has committed or is committing a criminal offense to which the materials relate (except for the possession of child pornography and certain government information, this exception does not apply where the mere possession of the materials constitutes the offense).

Where there is evidence relating to the crime located on a computer that also contains PPA protected materials, issues concerning proper scope and execution of a search warrant will arise. Recent court cases indicate that the courts are limiting the scope of PPA protection to people not suspected of committing a crime. In addition, there is no suppression remedy for non-constitutional violations of the PPA.

Note: For further information on the PPA, consult *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (www.cybercrime.gov/searchmanual.htm).

6. Constitutional Issues

Searches for digital evidence, like searches for other forms of evidence, are subject to the constraints of federal and state constitutional search and seizure laws and court rules. Traditional fourth amendment principles like those governing closed containers apply to digital evidence.

A. Does the Fourth Amendment Apply?

The fourth amendment protects individuals from unreasonable searches and seizures. There are two primary requirements for fourth amendment protections to be invoked:

- Is government action involved?
- Does the person affected have a reasonable expectation of privacy in the place or thing to be searched?

1. Government Action.

In most circumstances, government action is implicated when a government employee or agent conducts a search. Generally speaking, the fourth amendment's limitations do not apply to searches by private parties unless those searches are conducted at the direction of the government. Private parties who independently acquire evidence of a crime may turn it over to law enforcement (law enforcement may replicate the private search but not exceed the scope of the private search without a warrant or exception to the warrant requirement).

For example, if an employee discovers contraband files on a computer being repaired in a shop, the employee's subsequent release of information to law enforcement does not implicate the fourth amendment. In such a case, law enforcement may examine anything that the employee observed.

2. Reasonable Expectation of Privacy.

The fourth amendment applies when the searched party has an actual expectation of privacy in the thing searched, and then only if it is an expectation that society is prepared to recognize as reasonable. Some courts treat the computer as a "closed container" for fourth amendment purposes. In these jurisdictions, looking at the computer's sub-directories and files is akin to opening a closed container.

B. Satisfying Fourth Amendment Requirements

If the fourth amendment is implicated in the search at issue, then generally law enforcement must obtain a warrant unless an exception to the warrant requirement applies.

1. Warrantless Searches

There are several well-recognized exceptions to securing a warrant. While the following is not an exhaustive list, these examples provide some idea of how the common exceptions apply to the search and seizure of electronic evidence.

a. Consent

Consent is a valuable tool to the investigator. It can come from many sources, including a log-in banner, terms of use agreement, or company policy. Some considerations include:

1. A computer, like a shared apartment, can have multiple users. Users may consent to a search of their private area or common areas of the computer. Additional consent may be needed if the investigator encounters password-protected files. For example, in most cases, a parent can consent to a search of a minor child's computer.
2. Consent can be limited by subject matter, duration, and other parameters. Consent can be withdrawn at anytime. Attached is a suggested written consent to search/seize form (see Appendix 'X' for a sample consent form).⁴
3. The general rule is that a private-sector employer can consent to the search of an employee's workplace computer. The rules are far more complicated when the employer is the government.

Note: For further information on workplace consent rules, consult *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (www.cybercrime.gov/searchmanual.htm).

b. Exigent Circumstances

In order to prevent the destruction of evidence, an agent can seize an electronic storage device. In certain cases where there is an immediate danger of losing data, the agent may perform a limited search in order to preserve the status quo. Once the exigent circumstances cease to exist, so does the exception.

c. Search Incident to Arrest

A need to protect the safety of a law enforcement agent or to preserve evidence can justify a full search of an arrestee and the limited search of the arrest scene. This search incident to arrest can include a search through an electronic storage device, such as a cell phone or pager, held by the subject.

Note: Although a search incident to arrest may allow the search of electronic storage devices on the suspect, the arresting agent should take care to maintain the integrity of the evidence.

⁴ Section A will draft the appendix.

d. Inventory Search

The inventory search exception is intended to protect the property of a person in custody and guard against claims of damage or loss. Although untested, it is unlikely that the inventory search exception will allow a law enforcement agent to access digital evidence without a warrant.

e. Plain View Doctrine

The plain view exception may apply in some instances to the search for and seizure of electronic evidence. For this exception to apply, a law enforcement agent must legitimately be in the position to observe evidence, the incriminating character of which must be immediately apparent. Caution should be exercised when searching for digital evidence under the plain view exception. Rules vary between jurisdictions as to the nature of the permissible search.

2. Searches and Seizures Pursuant to Warrants

If none of the search warrant exceptions apply, and the fourth amendment is implicated in the search, law enforcement should secure a search warrant. Generally, the same warrant rules apply when preparing and executing a search warrant for digital evidence that applies in other investigations. Law enforcement agents should consider the following when preparing and executing search warrants for electronic evidence:

a. Describing Property

If the evidence sought is the computer itself (and the hardware is an instrumentality or the fruit of the crime or is contraband), then the warrant should describe the computer as the target of the search. If the evidence sought is information stored on a computer, then the warrant should describe the evidence of the crime sought and request the authority to seize the evidence in whatever form it may be stored, including any digital form.

Search warrants should also request the authority to search for system passwords and keys, since it may be impossible to access the system if it is password-protected or other encryption devices are in place.

<p>Note: For sample language, consult <i>Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations</i> (www.cybercrime.gov/searchmanual.htm).</p>
--

b. Conducting the Search

In some cases, the search of an electronic storage device can require significant technical knowledge and should be conducted by appropriate personnel. Such personnel should be supplied with a copy of the search warrant to ensure that the search is within the scope of the warrant.

In the course of conducting a search, a law enforcement agent may discover evidence of a crime outside the scope of the search warrant. In such an event, the agent should consider securing another warrant to expand the scope of the search.

Note: For a discussion of some of the issues concerning evidence collection, consult *Electronic Crime Scene Investigation: A Guide for First Responders* (www.ojp.usdoj.gov/nij).

c. Reasonable Accommodations

In some cases, it might be impractical to search the device onsite. If the device is to be searched offsite, the law enforcement agent should consider adding language to the warrant affidavit that justifies removal.

If the device is removed for an off-scene search, the search should be completed in a timely manner. Law enforcement may consider returning copies of seized data that is commingled with evidence of a crime to accommodate a reasonable request from suspects or third parties.

7. Privileged Information

In some instances, a law enforcement agent may have reason to believe that the place to be searched will have information that is considered “privileged” under statute or common law (e.g., when searching the office of a lawyer, doctor or member of the clergy). Before conducting the search, the agent should take care to identify the legal limitations that the jurisdiction may impose and comply with those limitations.

8. Resource List

- A. United States Department of Justice, Computer Crime Intellectual Property Section, (www.cybercrime.gov).
- B. National Association of Attorneys General (www.naag.org).
- C. National White Collar Crime Center (www.nw3c.org).

Blank Page

Section B: Integrity, Discovery, and Disclosure of Electronic Evidence

1. Introduction

Maintaining the integrity of electronic evidence throughout the process of examination presents different problems from the handling of traditional physical or documentary evidence. Some common problems are greatly exacerbated by the complexity of networked computers. This guide does not address the unique issues resulting from networked environments but focuses on selected issues of maintaining the integrity of information taken from stand-alone electronic media.

This guide assumes that the media that was seized has relevant information and the forensic procedures used to examine that media have not altered the evidence since it was seized. Ensuring that the chain of custody is intact after seizure is necessary but not sufficient to determining the authenticity of the data or evidence obtained from the forensic examination. It often provides no information whatsoever on who may have created or modified the electronic evidence before it was seized.

This guide assumes that only commercially recognized tools (i.e., tools recognized by the forensic community) would be used to acquire data from the source electronic device or media. Because the process used to acquire the data is itself electronic, both the evidence and the process may be subject to legal challenges. This may require additional expertise in order to authenticate the machine, applications, and forensic tools at issue. Refer to Section C ('Courtroom Preparation and Evidence Rules') for an in-depth treatment of the problem.

Investigators and prosecutors must recognize that in many, if not most, instances of computer-involved information, the information will have been handled, and quite possibly intentionally or unwittingly altered, *before the evidence is acquired by law enforcement*. This is particularly likely in the event of an intrusion or *access that exceeds authorization* leading to criminal mischief that is not immediately discovered, or one that is discovered and investigated by the victim before involving law enforcement. Information that is turned over to the prosecuting authorities for forensic examination by a victim may not be ultimately useful without a thorough and independent preliminary investigation into the authenticity and chain of custody of the proffered evidence.

Note: In evaluating this evidence, refer to the jurisdiction's statutes to identify possible crimes, including non-computer crime statutes that might be involved. Make a checklist of the elements that must be proved if this case goes to trial.

Sample questions that may need to be routinely asked about the evidence to be examined include:

- What evidence do you have that you were victimized by an unknown intruder or a known user who exceeded authorized access to the machines or data?
- What is the chronology of the access or changes in the data?
- What are the estimated damages?
- Who may be responsible for the incident?
- Why is this person (or these people) suspected?
- What is the impact to the business?
- Are computers and systems required to run the business?
- What first alerted you to the incident or loss?
- When did the incident first occur?
- When was the incident first discovered?
- Who has investigated the incident and what actions have been taken to identify, collect, preserve, or analyze the data and the devices involved?

Consult the earlier NIJ guides in this series for sample questions for specific kinds of computer-involved crimes (*Electronic Crime Scene Investigation: A Guide for First Responders* and *A Guide for the Forensic Examination of Digital Evidence*). These preliminary inquiries will be crucial for the prosecutor to be able to provide the necessary foundation and guarantees of trustworthiness for the ultimate evidence offered in the case. Without reasonable answers to these kinds of questions, the information originally received may not be admissible as evidence or useful in the development of admissible evidence. If the information is admitted into evidence, then the focus of the attack by the defense and concerns by the trial court will turn to the weight the evidence is accorded. Admissibility is only the first hurdle: credibility and persuasiveness of the evidence must still be assessed by the trier of fact as well.

2. Integrity of Data

The prosecutor must be able to demonstrate in court that the information obtained from the media is a true and accurate representation of the information originally contained in the media irrespective of whether the acquisition was done entirely by law enforcement or in part or entirely by a civilian witness or civilian victim.⁵

A. Chain of custody

There are two chains to consider: the physical item itself and the data.

1. **Physical items.** There are well-established procedures for handling the physical items, such as the computer, the PDA, or the cellular telephone. These procedures are outlined in the *Electronic Crime Scene Investigation, a Guide for First Responders* (www.ojp.usdoj.gov/nij).
2. **Data acquisition.** If the acquisition of the data is done in accord with best practices, concerns about chain of custody of the data contained in the forensic image become moot. Chain of custody issues unique to the acquisition of electronic evidence and the many issues that relate to the integrity of the evidence during the forensic examination itself are addressed in the forthcoming NIJ guide tentatively entitled *A Guide for the Forensic Examination of Digital Evidence* forthcoming.

B. Questions pertaining to the preliminary handling of digital evidence (pre law enforcement): the acquisition and examination processes.

Address these questions to both law enforcement agents and employees of private corporations (e.g., IT staff, security, etc.). Law enforcement agents often do not ask employees these questions after employees have provided evidence to agents. Allow sufficient time to collect and document answers before preparing an indictment or planning a trial. One advantage of inquiring about these issues when the police become involved in a case is that if the evidence is still on the system, and the original procedure used to gather the information was less than ideal, the police may be in a position to repeat the collection process or to resolve evidentiary issues if repeating the process is impracticable. Addressing these questions when the police are investigating the case reinforces adherence to following proper chain of custody procedures.

1. **What types of digital evidence have been collected?** For example, in a cyberstalking case, is there a hard copy (printed) version of the e-mail? Is there an electronic copy? Does it contain full header information?

⁵ Section B will add a topic sentence.

2. Who handled the evidence?

- a. Document the name and job function (e.g., layperson versus qualified personnel) of each individual who handled the digital evidence. Be aware that more than one person could be involved in this process.
- b. Identify everyone who had control of the digital evidence after it was examined and before it was given to law enforcement.

3. How was the digital evidence collected and stored?

- a. Identify any tools or methods used to collect the digital evidence.
- b. Determine who had access to the digital evidence after it was collected (anyone with access to the evidence should be considered part of the chain of custody). Account for all storage of data as well.

4. When was the evidence collected? Document the date and time when the evidence was collected (including a reference to time zone if necessary). Consider using a timeline to demonstrate the collection of evidence. Be aware that the collection of evidence might be an ongoing process.

5. Where was the evidence when it was collected?

- a. Geographical (e.g., ‘In what room? On what desk?’)
- b. Hardware
 1. What kind of machine/device held the digital evidence?
 2. Who had access to the machine/device?
 3. Who owned the machine/device?
 4. Is a serial number present?
 5. Was the machine/device a shared device?
 6. Was information retrieved from a network?
 7. Was information password-protected?
 8. Who had access to password-protected information?
- c. Offsite (e.g., servers – e-mail or remote – and web pages)

3. Building the Record to Make the Case

Thorough and accurate documentation is critical to the prosecutor's case. It is essential to establish both admissibility (under the principles discussed in Sections A and C of this guide) and the persuasive force of the evidence. A well-documented case is much more likely to result in a guilty plea. The previous section (B.2.B) describes the information law enforcement should gather to document the integrity⁶ of the data before law enforcement acquires it. Law enforcement also must thoroughly document their actions in respect to the data. General categories of such documentation include the following.

A. Search and Seizure

1. Document compliance with statutory requirements and limitations as discussed in Section A of this guide.
2. Document compliance with Fourth Amendment requirements as discussed in Section A of this guide.

B. Data Acquisition (please refer to the NIJ guides *Electronic Crime Scene Investigation: A Guide for First Responders* and *A Guide for the Forensic Examination of Digital Evidence*)

C. Data Examination (please refer to the NIJ guide *A Guide for the Forensic Examination of Digital Evidence*)

D. Data Storage (please refer to the NIJ guide *A Guide for the Forensic Examination of Digital Evidence*)

Will the examiner be qualified as a highly trained factual or expert? This decision will be discussed further in Section D of this guide.

E. Notes

<p>Note: Always retain notes related to the discovery and analysis of digital evidence. Such notes may prove invaluable if a case goes to trial.</p>

1. Preparation and storage of notes

Prepare and store notes used to write reports according to agency policy.

⁶ Define the term 'integrity.'

Because of the fragile nature of digital evidence, detailed and accurate documentation of the acquisition and examination process is critical. It is becoming a common occurrence to see the results of an analysis used in a trial; long after the analysis was performed. Attorneys may either challenge the analysis results, or request an additional analysis for evidence alleged to have been overlooked. These requests and/or allegations test the integrity of the entire examination process. In addition, a well-prepared and detailed examination log will prove invaluable to an examiner who may be called upon to re-examine the case.

The examiner should completely and accurately report the findings and results of the analysis of the digital evidence examination. Documentation is an ongoing process throughout the examination. Because of the fragile nature of digital evidence

2. Do not commingle notes from different cases.

Note: If notes exist, they may be discoverable, and prosecution must be notified.

F. Reports.

1. Prepare a detailed report as required by law (the requirements vary from jurisdiction and are different in civil and criminal proceedings).

- a. See FRCP 26 for federal civil matters.
- b. See FRCrP 16 for federal criminal matters.

2. Include the following in the report as required:

- a. Any permissible opinions the expert may render.
- b. The bases for any such opinion.
- c. The examiner's *curriculum vitae* (CV).
- d. Instances in which the examiner has been qualified as an expert. Be aware of any instances in which the examiner has been tendered as an expert but not qualified.

Note: An examiner not being offered as an expert may not be required under the law to produce a report. However, failure to adequately document pertinent information can affect the success of a prosecution. An expert cannot be an advocate.

4. Returning Original Evidence

After electronic evidence has been seized, defense attorneys may file motions for the return of the original evidence. Those motions may be filed before the examination has even been started.

A. Return of original evidence to defendants

There are a variety of reasons the defense may seek return of some or all of the electronic evidence before final adjudication. Some issues that may arise are outlined below.

1. Contraband

- a. If the original evidence has contraband, consider whether it is appropriate to return the original
- b. If the court, or local practice, determines that the original should not be provided to the defense, it may become necessary to provide the defense with access to the original or a forensic clone (i.e., think of the downstream consequences of winning a motion).

2. Stipulations

- a. Obtain stipulations when information is going to be returned. Remember that the stipulation needs to be obtained from the defendant – obtaining a stipulation from the owner of the data (e.g., a corporation) who is not the defendant is of no value (provide samples).⁷
- b. Anticipate that an ongoing business will eventually need its information returned. If the information is being obtained by search warrant, address this in the affidavit. The configuration of the evidence and the ability to obtain it will determine whether or not to seize the digital information. Stipulate whether the information was accurately seized from the company, which is not a party defendant (since it will not prove of any value for admitting the evidence).⁸

3. Privileged or proprietary information⁹

- a. Consider in advance whether the media to be seized contains proprietary or privileged information.

⁷ Section B will provide examples.

⁸ Consider revising this sentence.

⁹ Reviews this section to ensure accuracy of content.

- b. Consider obtaining a stipulation before seizing information from the target to avoid confiscating everything.
- c. Ensure that the prosecution team in advance addresses the issue of proprietary information when drafting the search warrant to avoid tainting the acquisition of evidence (consider the lessons of the Steve Jackson Games case and its interpretation of the PPA).
- d. Review the law on search and seizure to determine the appropriate process for including the procedures in the search warrant affidavit and whether the affidavit that details the process by which the search will be conducted must be included as one of the documents given to the representative of the business at the search warrant site.

Note: If evidence is mishandled, the examiner may end up destroying exculpatory material, or at the very least inviting unnecessary, time consuming, and expensive litigation over the possibility that exculpatory evidence was lost due to the government's mistakes in the collection or analysis process.

5. Obligations to Disclose Examination Results

The prosecution team has an obligation to provide evidence to the defense according to discovery rules. In addition, defense attorneys may seek to compel access to the evidence for examination by a defense examiner.

A. General Discovery

- 1. Provide a forensic clone of the evidence or make accommodations for the defense to examine the evidence in state custody.**
 - a. The defense may be entitled to the actual evidence or a copy (depending on the circumstances).
 - b. The defense may be entitled on the premises to examine the digital evidence.
 - 1) Provide defense with a clean computer for examining digital media (the computer should have no remnants from other cases).
 - 2) Provide defense with an appropriate space to review digital media.
- 2. Know the public document retention periods** (be aware that FOIA is sometimes used as a back door to get arguably relevant and material information).

- 3. Be aware of accreditation standards and laboratory policies, procedures or best practices to the extent they exist, both generally and for electronic evidence specifically.**

Determine whether they have been followed or there has been deviation. Understand the effect that any deviation may have on the case and be prepared to explain any deviation. Also, be aware that the policies, procedures, or best practices should be dynamic. The prosecution team must know which practices were applicable at the time the examination was conducted.

- 4. Know that discoverable material includes notes** (e.g., handwritten, tape recorded, computerized, e-mail, etc.) among the team members or informal sources of expertise on which you rely to get information
- 5. Identify all the examiners used to find the evidence.**

B. Exculpatory material

The prosecution team has an obligation to identify, preserve, and reveal exculpatory evidence to the defense. Those obligations vary according to jurisdiction, but typically require at a minimum that exculpatory evidence be made available to the defense in advance of trial and without a specific defense request. However, additional obligations may be imposed in different jurisdictions. The prosecutor should determine whether the examiner looked for all relevant evidence, including potentially exculpatory evidence. Failure to look for and report all relevant evidence may affect the credibility of the examiner's testimony, especially if additional information is found by a defense examination of the same media. Procedures should be in place to examine voluminous amounts of electronic evidence analogous to the sampling that a forensic accountant might do on books and records to satisfactorily conclude an audit of those records.

6. Resources

- High Tech Crime Task Forces
- NLETCs
- SEARCH
- NW3C
- Los Alamos Lab
- Search and Seizure Guidelines
- Prosecutors' Resource CD from NCTP
- NAAG website, with list of prosecutors
- NAC training classes (National Advocacy Center)
- HTCIA (and GMU conference of Mid Atlantic Chapter)
- FACT, Forensic Association of Computer Technologists

- Various Listservs – HTCIA, HTCC, IACIS, CFID
- DCITP
- FLETC
- POST (state by state)

Section C: Courtroom Preparation and Evidence Rules

1. Introduction

There are a variety of issues to keep in mind when preparing to present a case involving digital evidence. The most obvious point is that the presentation of digital evidence requires familiarity with new, specialized, evolving, and sometimes-complex technology. It therefore is essential that investigators and prosecutors:

- Take the time to acquire a basic working knowledge of the technical aspects of digital evidence in general
- Allow enough time to master the specific technical details of the case at hand

Because effective trial preparation begins at the outset of the investigation, the need for technical competence runs throughout the case. Those issues pertinent to the search for, seizure of, and chain of custody of digital evidence are discussed above in Sections A ('Search and Seizure Issues') and B ('Integrity, Discovery, and Disclosure of Electronic Evidence').

Section C will focus on three aspects of pretrial preparation:

- Preliminary considerations for the prosecutor when reviewing the scope of the investigation to date
- Effective pretrial communication between prosecutors, investigator, and forensic examiners.¹⁰
- Evidentiary issues (e.g., authentication and hearsay that arise in connection with digital evidence)

¹⁰ Define term 'Forensic Examiners'

2. Preliminary Considerations for Prosecutors

Ideally, a digital evidence case should be developed by a team consisting of the prosecutor, lead investigator, and the forensic examiner. Digital evidence cases often present special procedural and substantive issues. One of the prosecutor's first tasks upon being assigned the case is reviewing the scope of the investigation. Several key issues include:

A. Preparing and presenting an understandable theory of the case to the trier of fact.

B. Clarifying the nature of the technological issues.

1. Is the digital evidence associated with a 'high technology' crime?
2. Although the case might not involve a high technology crime, is digital evidence nevertheless an important aspect of the case? Or is digital evidence simply involved in the investigation or presentation of the case? (For example, a computer simulation or animation may be used to illustrate an expert's testimony in a homicide case).

C. Identifying and explaining the source and nature of the digital evidence in the case.

1. Are the computers storage devices for evidence of crime or are they contraband, evidence, or instrumentalities of crime themselves?
2. What hardware, software, operating systems, and system configurations were used by the target of the investigation or victim?
3. Was the evidence found on a stand-alone personal computer or a network?

D. Identifying potential sources of material digital evidence is a subject covered in Sections A and B of this guide.

During preparation for trial, it may become evident that specific additional sources should be investigated (e.g., backup files, log files, etc.).

E. Considering all appropriate charges (e.g., does a child pornography possession case also involve dissemination charges?).

3. Pretrial Communication

The prosecutor, investigator, and forensic examiner, in addition to working as a team during the investigation stage of a digital evidence case, should meet well in advance of trial to plan the presentation of the case. Several key issues include:

- A. Discussing any questions or points raised for clarification, further analysis, or investigation by the prosecutor's review of the case.
 - 1. Ensure familiarity with the specific technological aspects of the case.
 - 2. Review the experience and qualifications of the investigator and forensic examiner.
 - 3. Review the scope and limitations of the evidence.
 - 4. Read the reports prepared by the investigator and examiner before the meeting and use the meeting to clarify any points of uncertainty.
- B. Conducting a pretrial meeting with the investigator and forensic examiner to clarify the legal theory of the case, the elements of the crimes charged, and any anticipated defenses.
- C. Reviewing with the investigator and forensic examiner the likely scope and direction of direct and cross-examination.
- D. Distinguishing the types of digital evidence.

Three broad categories of digital evidence raise issues that are especially important to address in a pretrial meeting. Each category of evidence also involves clarifying whether a witness will offer fact or expert testimony.

1. Background evidence on technological issues.

Provide background evidence when necessary to enable the trier of fact to understand the technical issues in the case. Consider as examples asking the following tactical questions during the pretrial meeting:

- a. Will the forensic examiner be asked to provide general background testimony as well as testimony concerning the results of his or her analysis?
- b. Are there general technical issues that are not in dispute and, if so, can they be presented at the outset on a stipulated basis apart from the case-specific testimony?

- c. Does the use of metaphors to illustrate the technological issues present any legal complications? Using metaphors may have unintended consequences (e.g., referring to computers or computer files as ‘containers’ may have fourth amendment implications).
- d. Should a stipulated glossary of undisputed technical terms be provided to the trier of fact?

2. Substantive evidence.

The presentation of substantive evidence will raise tactical and technical considerations.

a. Tactical.

- Should e-mail messages or other digital evidence be presented in hard copy or on-screen?
- Will the jury be able to review hard copies of digital evidence in the jury room?
- Should all relevant files be offered or only specific examples? If all are offered, should all be discussed or only specific examples? How should sample files be selected (e.g., files in a child pornography case)?
- Digital evidence may include voluminous records for which summaries may be appropriate

Note: Live on-line activity at trial can be very unpredictable. Consider capturing the activity outside of court using a screen capture program and playing it back in court. If you must do a live demonstration, rehearse it carefully and anticipate what can go wrong.

b. Technical.

- How will technical glitches be addressed during trial (e.g., arrange for technical support, provide backup or hard copies, etc.)?
- Preparing the courtroom for presentation of digital evidence
 - Do the computers work?
 - Where are the wires located in the courtroom?
 - Are there enough outlets and do they work?

- Is there adequate and appropriate equipment?
- Notification of court security
- Notification of court reporter (e.g., if audio will be presented)
- Placement of monitors and lighting issues
- Presenting the evidence
 - Have clean copies of exhibits
 - Ensure adequate set-up time
 - Ensure stand-by mode, start-up screen, sound (if applicable) and screen savers are deactivated
 - Remember where equipment left off at last break (i.e., cueing)
 - Remember to protect the court record with descriptions of referenced exhibits
 - Provide jury notebooks or exhibit books
 - Consider whether to request jury note taking

3. Illustrative evidence.

In addition to the foregoing sets of tactical and technical issues, illustrative evidence may present additional considerations. For example:

- Consider which presentation media or combination of media will be most persuasive
- Should animation be presented in a fixed form with no ability to change the animation based on changed assumptions, or presented in a form in which it can be changed?
- Will such evidence need to be disclosed pretrial?

E. Considering pretrial rulings.

Because digital evidence may be unfamiliar and seem complex, consider resolving admissibility (e.g., of expert testimony) and presentation issues by pretrial motion. This serves the following goals:

- Avoids addressing those issues for the first time at trial before the jury
- Educates the court about technology-related issues
- Secures admission of evidence at trial
- Identifies potentially objectionable evidence

4. Evidentiary Considerations

A. Introduction

While the rules of evidence in state courts vary from jurisdiction to jurisdiction, many states' rules are modeled after the Federal Rules of Evidence ('FRE'). Because a state-by-state review is beyond the scope of these materials, this section is based primarily on the Federal Rules. Prosecutors should also consult whatever local rules apply.

Digital evidence, like any other kind of evidence, can present issues such as relevance, authentication, and hearsay. While these issues are resolved for the most part on the same basis as they are for other kinds of evidence, there are some points specific to digital evidence to keep in mind. In addition to the digital evidence itself, the presentation of digital evidence may involve expert testimony and its associated evidentiary issues. Although admissibility is ultimately a legal matter for the prosecutor to address, it may be helpful for the investigator and forensic examiner to have a basic grasp of what will be required to establish admissibility.

Evidentiary considerations may be affected by the nature and source of the digital evidence. For convenience, this section is organized as follows:

- Defining evidentiary terms (4.B)
- Pre-existing substantive evidence stored on a computer (4.C)
- Pre-existing substantive evidence generated by a computer (4.D)
- Substantive and illustrative computer-generated evidence prepared for trial (4.E)
- Expert testimony (4.F)

B. Defining evidentiary terms.

1. **Judicial Discretion ('Almost total').**

Trial judges exercise broad discretion when ruling on admissibility of evidence. Because digital evidence may be unfamiliar terrain for many trial judges, proponents should be knowledgeable about how the rules of evidence apply to new technologies.

2. **Relevance ('Does it help?').**

If the evidence helps to prove or disprove some fact that matters in the case, it normally will be admitted. The general approach of the Federal Rules is that '[a]ll relevant evidence is admissible,' unless some specific rule, statute, or constitutional provision excludes it (FRE 401). 'Relevant evidence' is broadly defined to mean 'evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more or less probable than it would be without the evidence' (FRE 401).

Of the various relevance-based objections, two are of particular concern.

a. Prejudice.

Relevant evidence may be excluded if the judge determines it is unduly prejudicial. It is unduly prejudicial if its 'probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues, or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence' (FRE 403). These potential objections should be kept in mind when considering offering computer-generated simulations or animations into evidence.

b. Other actions.

Objections to evidence of 'other crimes, wrongs, or acts' under FRE 404(b) can arise in digital evidence cases. However, such evidence may be admissible to prove 'motive, opportunity, intent, preparation, plan, knowledge, identity, or absence of mistake or accident.' For example, a child pornography case may involve multiple wrongful acts, only some of which have been charged. Evidence of uncharged acts may be admissible to prove knowledge or absence of mistake.

3. Authentication ('Is it what you say it is?').

The evidence offered must be shown to be what its proponent claims it is (FRE 901(a)). The proponent is not required to rule out all possibilities inconsistent with authenticity. The standard is a reasonable likelihood that the evidence is authentic.

4. Hearsay ('The preference for live testimony').

The rule against hearsay reflects a preference for having human statements introduced through live testimony in court, where the demeanor of the person making the statement (called the 'declarant') can be observed by the trier of fact and the declarant can be subjected to cross-examination. Digital evidence sometimes raises hearsay issues. A simplified but useful framework for considering hearsay problems follows:

a. Is it 'hearsay?'

1. Does the item fit within the 'core' definition of hearsay?

'Hearsay' is an out-of-court statement that is offered to prove the truth of the matter asserted in that statement (FRE 801(c)). If the statement is not offered to prove what it says, then it is not hearsay. For example, in a prosecution for credit fraud, computer printouts related to defendant's accounts, which were kept by the collections department of the credit card company, would meet the 'core' definition of hearsay because they would be offered to prove the truth of their contents. On the other hand, in a prosecution for on-line solicitation of a minor, the reply e-mails from the victim, if introduced simply to show contact between the defendant and victim rather than for the truth of their contents, would not meet the 'core' definition. They would be relevant for the fact that defendant received them, not for what they say.

Another issue, apart from whether the evidence is offered to prove the truth of the matter asserted, is whether it constitutes a 'statement' for hearsay purposes. A 'statement' is defined as '(1) an oral or written assertion, or (2) nonverbal conduct of a person, if it is intended by that person as an assertion' (FRE 801(a)). The critical question in that regard, as discussed below, is often whether the record is computer-generated (likely not a statement) or computer-stored (may include statements).

2. Even if the item falls within the 'core' definition of hearsay, is it nevertheless *exempted* from the definition of hearsay under the rules of evidence?

The Federal Rules of Evidence specify several categories of statements that, although offered to prove the truth of the matter asserted, are nevertheless deemed not to be hearsay. The most pertinent for present purposes is the category of ‘admissions’ (FRE 801(d)).

- b. If it is ‘hearsay,’ is it nevertheless admissible under one of the *exceptions*?

Even if the statement qualifies as hearsay, it may nevertheless be admissible under one of the numerous exceptions to the hearsay rule. The most common concerning digital evidence is the business records exception discussed below.

C. Pre-existing substantive evidence stored on a computer.

1. Distinguishing substantive from illustrative evidence and computer-stored from computer-generated evidence:

- a. Substantive versus illustrative.

As is the case with evidence in other forms, such as documents or live testimony, the principles applicable to the admissibility of digital evidence will depend in large part on where it comes from, how it was created, and the purpose for which it is offered. For present purposes, the term ‘substantive evidence’ refers to evidence introduced for what it helps to prove itself, as opposed to ‘illustrative evidence,’ which refers to evidence that illustrates testimony but does not by itself prove anything.

For example, computerized bank records in a credit card fraud case, e-mails in a cyber stalking case, and image files in a child pornography case are all substantive evidence. Each has substantive value in helping to prove an issue in the case. By contrast, a computer animation used to illustrate a witness’s testimony is offered to support the related substantive evidence (the testimony) rather than as proof of something itself.

- b. Computer-stored versus computer-generated.

Computer-stored evidence includes documents and other records that were created by a human being and that just happen to be stored in electronic form. Examples include word processing files, e-mail messages, and Internet chat room messages. This kind of evidence may raise both authentication and hearsay issues. Computer-generated evidence consists of the direct output of computer programs. Examples include the login record of an Internet Service Provider, automated telephone call records, and automatic teller receipts.

These records do raise authentication issues but are not properly regarded as hearsay because they are not the statement of a person. Finally, some records may contain a combination of computer-stored and computer-generated evidence. For example, a financial spreadsheet contains both the input data that originated from a person and the output of the computer program. Such evidence therefore presents both kinds of issues. Another category of evidence, computer-generated evidence prepared for trial, also presents distinct issues, and is discussed below.

2. Authentication of computer-stored substantive evidence.

Again, the authentication requirement simply means that the prosecution must show that the records stored in a computer are what the prosecution claims. Key issues usually center on identifying the author or authors of the computer-stored record and showing that it has not undergone significant change in any respect that matters in the case. Both of these points can often be shown through the chain of custody and other circumstantial evidence (some of which are discussed in Section B ('Integrity, Discovery, and Disclosure of Electronic Evidence')). Illustration (b)(1) of FRE 901 provides for authentication through 'testimony of [a] witness with knowledge,' that 'a matter is what it is claimed to be.'

Many courts have recognized that, while the witness called to establish authenticity must have personal knowledge of the facts about which he or she testifies, the witness need not have been the programmer of the computer in question or have knowledge of its maintenance and technical operation. For example, the computer-stored records of illegal drug transactions, found on a computer seized from the defendant's possession, could be authenticated by testimony from the investigating officer who seized the computer (showing that the computer was indeed found in the defendant's possession and that names used in the files matched those associated through other evidence with the drug transactions) and the examiner who recovered the files (showing that the records are actually those found on the computer).

In some cases, because of the relative anonymity of some computer-stored records (such as those involving Internet-related crimes), establishing authorship may depend largely on circumstantial evidence. For example, in a child pornography case involving Internet chat rooms, evidence obtained from the defendant's residence linking the defendant to his postings to the chat room, information the defendant gave to an undercover agent, and information obtained from the Internet Service Provider were sufficient to show authorship.

Technology is increasingly rendering authentication of digital evidence a simple and straightforward matter. Defendants will sometimes challenge authenticity by alleging that the computer records could have been altered after they were created.

Such arguments often emphasize the ease with which computer records may be modified. Under the ‘reasonable likelihood’ threshold for authentication, however, courts have generally not been receptive to such claims in the absence of specific evidence of alteration. Moreover, authentication of data may not necessarily be precluded by the use of examination software that alters non-essential data but does not effect significant changes to substantive data. For example, alteration of date and time stamps may be irrelevant in a given case.

Other input issues that may be raised, apart from the possibility of tampering, include the completeness of the record, the input procedures, and the input method (accurate data conversion). If these matters are genuinely in issue, the prosecution should be prepared to present witnesses to address them.

3. Hearsay and computer-stored substantive evidence.

If the computer-stored record contains statements made by a human being and is offered to prove the truth of the matter asserted in the statement, then the prosecution must consider the hearsay rule. As mentioned above, if the statement qualifies as an admission by a party-opponent, then FRE 801(d)(2) takes it out of the definition of hearsay and no exception is necessary. Also, the hearsay rule does not apply if the statement is not offered to prove the truth of the matter asserted.

As mentioned, the most common hearsay exception for computer-stored records is the business records exception, FRE 803(6). To establish the foundation for this exception, the prosecution should be prepared to show that:

- a. The computer equipment (hardware and software) on which it was stored is recognized as standard in the field.
- b. The data were entered in the regular course of business at or reasonably near the time of the occurrence of the event recorded.
- c. The sources on which the records were based, as well as the method and time of preparation, indicate that the records are trustworthy and their admission is justified.

This foundation may be established through the testimony of the custodian of the record or by a person who is familiar with the methods and systems through which it was prepared, even if that person does not have personal knowledge of the underlying facts contained in the record. In support of establishing trustworthiness, the prosecution might show:

- Company reliance on the data
- Protection of the accuracy of data entry

- Prevention of loss or alteration of the data while in storage
- Provision for integrity of data output

Note that there is considerable overlap between the foundation required for authentication and the foundation required to establish the availability of the hearsay exception. As noted above in connection with authentication, allegations of inaccuracies in a printout of computer records will not necessarily defeat admissibility provided an adequate foundation has been established. As is the case with non-computerized business records, the presence of some inaccuracies goes to the weight rather than the admissibility of the business record. Note also that, while records that are prepared solely for purposes of litigation may be challenged as untrustworthy, this limitation applies to the underlying data and not the printout of the record. Thus, preparation of a printout for purposes of litigation does not render it untrustworthy if the underlying data were entered and stored in the normal course of business.

For example, defendant was prosecuted for concealing assets during a bankruptcy proceeding and for destroying or concealing the bankrupt company's records. The trial court properly admitted computer printouts of the company's general ledgers, which contained inventory, payroll, and other accounting data entered by bookkeepers. The prosecution called the bookkeeper to testify that: the bookkeepers entered the data on a current basis, the printout accurately reflected the data, the printout was produced routinely each month, the data were regularly audited for accuracy, and the systems used were standard in the industry.

Note: Computer-stored records can involve two levels of hearsay. The act of data entry is itself an out-of-court 'statement' under FRE 801(a), but the result is usually the record kept in the regular course of business under FRE 803(6) as noted above. The underlying data entered may also contain hearsay 'statements,' which must qualify in turn for a hearsay exception or exemption.

4. Printouts of computer-stored substantive evidence

- a. Requirement of the original ('Best Evidence' Rule).

The so-called 'Best Evidence' Rule generally requires a party seeking to prove the contents of a writing, recording, or photograph to introduce the original writing, recording, or photograph unless some exception applies (FRE 1002).

Even though a printout of a computer-stored record might technically not be viewed as an original (especially since the ‘original’ data are simply a string of 1s and 0s), the ‘Best Evidence’ Rule does not present a problem if the printout accurately reflects the data. In recognition of the demands of practicality and common usage, the Federal Rules provide that ‘[i]f the 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”’ (FRE 1001(3)). This principle applies even if the duplicate originals have an inconsistent appearance (e.g., different fonts, margins, etc.).

b. ‘Summaries.’

Under FRE 1006, a party may present the contents of voluminous writings, recordings, or photographs, which cannot be conveniently examined in court, in the form of a chart, summary, or calculation -- subject to limitations such as making the originals or duplicates available to the other party for inspection or copying. A printout of a computer record is not automatically regarded as a ‘summary’ of that record. Digital evidence, of course, can be so voluminous that a summary of the data is required for convenience. For example, a summary of computerized invoices in a complex fraud case may be admissible if the limitations of FRE 1006 are met.

D. Pre-existing substantive evidence generated by a computer.

Some pre-existing computer records are generated by a computer program itself rather than human-created documents simply stored in electronic form. As used in this sense, the term ‘computer generated’ refers to the record itself rather than the printout. (Note that many courts will loosely refer to the printout as computer-generated regardless of whether the record being printed resulted from human data entry or was created by a computer algorithm). Examples of computer-generated records include automated telephone records, Internet Service Provider logs, and automatic teller records. Although some courts are beginning to recognize that not all computer evidence is alike, the proponent should be knowledgeable about the difference between computer-stored and computer-generated evidence. Correctly regarded, computer-generated evidence does raise authentication issues but is not hearsay. As a practical matter, this distinction may not make much difference at trial because of the overlap between authentication and establishment of the foundation for the business records exception.

1. Authentication of pre-existing substantive evidence generated by a computer.

Because computer-generated records are created directly by computer programs rather than by human input, authentication issues do not include identity of the records’ author.

The central authentication concerns instead are the reliability of the processing and output functions. Particularly pertinent to these concerns is FRE 901(b)(9), which provides for authentication by '[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.'

2. Hearsay and pre-existing substantive evidence generated by a computer.

As mentioned above, a record that is generated by a computer program is not properly regarded as hearsay. This is because it does not meet the definition of a 'statement' under FRE 801(a); it is neither 'an oral or written assertion' nor 'nonverbal conduct of a person if it is intended as an assertion.' Further, FRE 801(b) defines a 'declarant' as 'a person who makes a statement.' Some computer-generated records may have the appearance of a statement by a person, such as the 'You've got mail' prompt that signals the presence of unopened e-mail, but are actually merely the automatic output of the computer program.

The rationale for the hearsay rule – the preference for testing the trustworthiness of human assertions through in-court testimony subject to cross-examination and observation of witness demeanor by the trier of fact – does not apply to evidence generated directly by a machine or, for that matter, an animal. Thus, courts have long recognized that evidence such as the output of a Breathalyzer machine, a RADAR speed detection device, or a bloodhound's response to a scent all raise authentication issues but are not hearsay. Some courts have also similarly recognized that computer-generated records are not hearsay.

E. Substantive and illustrative computer-generated evidence prepared for trial.

1. Introduction.

The two kinds of digital evidence discussed above – computer-stored records and computer-generated records – existed in some form before the investigation and prosecution commenced. That form may have been digital, so that the evidence was reduced to hard copy for purposes of investigation and trial, but the underlying data existed beforehand. To that extent, substantive digital evidence is like any other kind of substantive evidence, such as fingerprints, biological samples, counterfeit currency, or a murder weapon.

Other kinds of evidence are prepared for purposes of trial. Some of these are illustrative rather than substantive. A common example would be the diagram of a building used to illustrate a witness's testimony. Such a diagram proves nothing by itself, but is used only to illustrate the testimony. Other kinds of evidence prepared for investigation and trial are substantive in that they do prove something independently of a witness's testimony.

An example would be photographs of a crime scene. Such evidence is 'demonstrative' rather than 'real.' It is relevant for what it depicts, but was not itself a thing involved in the transaction or occurrence that gave rise the prosecution.

Computer-generated evidence that is prepared for trial similarly can be either illustrative or substantive. A computer can be used to display any of the images formerly displayed by paper medium, such as a building floor plan (e.g., to show the positions of the perpetrator and witnesses in a robbery), an outline of the prosecution's case, or the highlights of an expert witness's testimony.

An example of a computer-generated static image used as substantive evidence would be a digital picture of the crime scene or of the perpetrator. Computers also allow manipulation of static images for emphasis and effect, such as zooming and highlighting, which formerly were done manually with paper images. Computer technology of course also allows the presentation of moving images. For example, a forensic pathologist might use animation to illustrate the trajectory of a bullet through a murder victim's body. Just as videotape technology allowed litigants to create vivid depictions, such as 'day-in-the-life' portrayals in personal injury cases, computer technology now also permits sophisticated 'recreations' of events and computer simulations.

2. Evidentiary issues.

a. Relevance.

The primary relevance concern with computer-generated evidence for trial is FRE 403, which confers broad discretion on the trial judge to exclude evidence on the grounds of unfair prejudice, confusion of issues, or misleading the jury. One concern might be that a computer-generated exhibit, especially an animated recreation or simulation, might make such a powerful impression on the trier of fact as to risk undue prejudice. A trial judge who admits a computer-generated exhibit over a FRE 403 objection might give the jury a limiting instruction, for example, about the purpose for which the exhibit is admitted.

b. Manner of interrogation.

The normal manner of proceeding on direct examination is to ask the witness specific, non-leading questions. Counsel using computer-generated exhibits at trial should take care to coordinate them with proper questioning of witnesses, and to establish the proper foundation, to avoid objections that the exhibit is essentially a lengthy narrative or in a sense leads the witness. These concerns are especially likely to arise if the evidence includes a 'voice-over' narration.

c. Authentication and other foundation issues.

Images simply used to illustrate a witness's testimony are relatively easy to authenticate, usually requiring only the witness's testimony that, based on personal knowledge, the image is a fair and accurate portrayal of what it represents. Digital photographs offered as pictures of a crime scene should normally be authenticated as are conventional photographs, unless some real concern arises regarding alteration. Requirements for recreations and simulations accompanying expert testimony may require the same foundation as the expert testimony itself (see 4.F, 'Expert Testimony,' below) to support the assumptions on which it rests plus testimony that the input and output parameters were correct. For example, common uses of simulations in civil cases are to portray airline disasters or automobile crashes. Authentication issues in such cases will focus on the extent to which input data correspond to actual events (in terms of accuracy and completeness) and the scientific validity of the mathematical model.

d. Hearsay.

1) Is it hearsay?

Whether the computer-generated evidence prepared for trial raises hearsay issues depends on the purpose for which it is introduced and on the nature of the evidence. A computer exhibit used simply to illustrate a witness's testimony – such as the computer image of a building floor plan or a computer diagram of a handgun – is not offered to prove the truth of the matter asserted. The exhibit itself is not offered to prove anything. It is offered only to illustrate the witness's testimony. As such, it is not hearsay. A digital photograph of a crime scene, while offered as substantive proof, is not a 'statement' but is instead only the direct output of a machine.

Recreations or simulations, on the other hand, may go beyond the testimony of the witness and thus constitute substantive evidence apart from a live witness's testimony. Hearsay problems may arise if the simulation is based on data not collected by the witness or a program not developed by the witness. With complex simulations, in which the output varies as a function both of the assumptions and the data, it is more difficult to argue that the output is not a 'statement' (i.e., the direct result of a machine's operation without human involvement).

2) Is an exception available?

If the computer-generated exhibit is deemed hearsay, its proponent will either have to find an applicable exception or some other way around the hearsay rule.

Several exceptions might apply to the input data: measurements, for example, might be regarded as ‘present sense impressions’ under FRE 803(1); other data might be taken from business records qualifying under FRE 803(6) or public records under FRE 803(8) (which, however, are subject to important limitations in criminal proceedings). However, even if the input data qualify under one of those exceptions, the hearsay rule may still apply to the operation of the program and the output function.

The proponent of the exhibit might also try to invoke the so-called ‘residual exception’ under FRE 807. This exception is subject to several limitations. The proponent must show that: the ‘statement’ is evidence of a material fact, is more probative of that fact than any other evidence the proponent could offer through reasonable efforts, and that admission of the evidence serves the purposes of the rules of evidence and the interests of justice. FRE 807 is also subject to a notice requirement.

Finally, a proponent of a computer animation or simulation prepared for trial might seek admission under FRE 703. Note, however, that the amendments enacted in 2000 to FRE 703 restrict the admissibility of otherwise inadmissible information relied on by the expert. Such evidence now is inadmissible unless the trial court finds that its ‘probative value in assisting the jury to evaluate the expert’s opinion substantially outweighs [its] prejudicial effect.’

F. Expert opinion testimony.

1. **Identifying the issues that will require an expert opinion** (See Section D.3).
2. **Identifying a qualified expert** (See Section D.3).
3. **Ensure that the qualified expert will use an admissible method**

There are a variety of tests governing the admission in court of the opinions of forensic experts. These tests are the *Frye* test (*Frye v. United States*, 54 App. D.C. 46, 293 F. 1013 (1923)), or the *Daubert* test (*Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993)), or some version thereof.

<p>Note: The admissibility of novel expert opinion testimony is typically resolved by pretrial motion. The prosecutor and the expert must prepare as carefully for these pretrial motions as for the trial itself.</p>

- In federal court, *Daubert* governs.

Daubert has replaced the *Frye* test (in federal court, and in many state courts) in favor of a test whereby the trial judge determines the admissibility of expert opinion testimony based on its relevance and the reliability of the underlying scientific techniques. The Court suggested that whether scientific expert opinion evidence will be helpful to the trier of fact may turn on whether 1) the scientific technique can be - and has been - tested, 2) it has been subjected to peer review and publication, 3) there is a known or potential rate of error, and 4) it has been generally accepted by the scientific community. The Court made clear in *Daubert* and in subsequent cases that this list is neither a rigid nor an exhaustive set of requirements.

Daubert is generally seen as the U.S. Supreme Court's suggestion that trial courts limit the admissibility of "junk science" and encourage the development of reliable scientific and technological forensic techniques. Recent changes to article seven of The Federal Rules of Evidence, governing the admissibility of expert opinion testimony, are based on *Daubert* and its progeny. *Kumho Tire Co., Ltd., v. Carmichael*, 526 U.S. 137 (1999), extended *Daubert* to technical areas other than those considered strictly scientific.

Technical expert opinion testimony is admissible under FRE 702 if "1) the testimony is based upon sufficient facts or data 2) the testimony is the product of reliable principles and methods, and 3) the witness had applied the principles and methods reliably to the case." FRE 702 as amended.

<p>Note: The law in this area continues to evolve. Numerous additional factors have been added to the four factors of <i>Daubert</i>.</p>
--

- Many states still use their versions of the *Frye* test

Frye set out a peer acceptance test whereby the admissibility of scientific techniques in court turned on the general acceptance of those techniques in the relevant scientific community. As the court stated in *Frye*, ". . . courts will go a long way in admitting expert testimony deduced from a well-recognized scientific principle or discovery, the thing from which the deduction is made must be sufficiently established to have gained general acceptance in the particular field in which it belongs" (note that under *Daubert*, general acceptance is only one of several factors for courts to consider).

As forensic examiners employ newer software, and newer versions of older software, in their examination of digital media, they may face *Frye* or *Daubert* challenges to that software. As examination techniques develop and as the expert witnesses deduce opinions about facts and evidence, “the thing from which the deduction is made must be sufficiently established” so as to be relevant and reliable in court.

Blank Page

Section D: Presentation of Digital Evidence

A trial involving digital evidence differs in two fundamental respects from most other trials. First, legal issues concerning the admissibility of digital evidence will nearly always arise. Those issues are discussed in Section C ('Courtroom Preparation and Evidence Rules'). Second, a trial involving digital evidence may involve complex or unfamiliar terms, issues, and concepts. Careful planning of how a case will be presented and how digital evidence will be used are essential to the successful outcome of a trial.

This section provides guidance in how to successfully present a case involving digital evidence.

1. Educating the audience

If a case is complex, educate the audience – both the judge and the jury – at every stage of the litigation process. Such education should address the following:

A. Daubert Expert Challenges and Pretrial Hearings.

B. *Voir Dire*.

C. Opening Statement.

D. Witness Testimony.

E. Making and Answering Objections.

F. Closing.

While it is important to bring the audience up to a minimum level of competency or understanding, do not make them experts: that is what experts are for. The general rule of prosecution is keep it simple and that holds especially true in the presentation of a case that is complex by nature. Let the defense make things complex. Consider which issues will be handled during case-in-chief and which to save for cross examination or rebuttal.

2. What needs to be proved/disproved?

Every case requires careful examination of the elements of the charges to ensure that convincing evidence will be presented as to each and every element. Digital evidence cases often require a determination by the prosecutor of what can and should be eliminated as reasonable explanations for the digital evidence. The key questions are:

- Is it necessary to disprove all alternative explanations?
- Can all reasonable alternative explanations be disproved?

A. Technical Anomalies

The nature of computer ‘incidents’ means that in some instances there will be no complete or clearly adequate explanation for a particular anomaly in the evidence or the time and money costs of explaining each anomaly will be prohibitive.

As computers and operating systems have become more complex, most network administrators and computer maintenance personnel limit their problem solving to the most frequently recurring problems. If a problem goes away upon rebooting and does not recur, it is a problem is not solved, even if there is no explanation for the problem. Computer experts accept the existence of unexplained ‘bugs’ or ‘glitches’ without doubting the validity of information stored or processed by computers.

Often there will be a conflict between the practical limits on what you want to or can prove or disprove and a defense attorney’s use of alternative explanations to create reasonable doubt.

B. Disproving Alternatives

What a prosecutor has to disprove depends on what issue is involved and the strength of the rest of the case.

When a crucial element is knowledge (e.g., in a possession of child pornography case), the prosecutor must be prepared to disprove defense claims that the pornography was stored on the defendant’s computer without his knowledge. The prosecutor does not need to disprove unreasonable alternatives (e.g., the pictures appeared on the defendant’s computer out of the ether).

When the hash values are different between the original evidence and the forensic copy, but there is an overwhelming amount of evidence on the computer (e.g., thousands of child porn pictures) the discrepancy in the hash values can be described and argued as irrelevant to the real issues in the case.

C. 'Timing is Everything'

When to rebut a defense is important. For example, if the defendant's knowledge of the contents of her/his computer will be crucial, it is sometimes wise to let the defendant raise the issue and allow the evidence (either through cross examination or rebuttal) rebut this claim, rather than asserting the disproof in the case-in-chief. A jury will often attach more importance to issues raised in the state's case, and hold the prosecutor to a higher standard than when the defense has raised the issue and the prosecutor is merely attacking the defense argument.

3. Expert Witnesses/Scientific Method Evidence

A. Deciding Whether a Technical Expert Witness is Needed

A major decision in cases that involve complex technology and extensive forensic examination of the digital evidence is whether to use an 'expert witness' (i.e., one qualified by special training, knowledge, or experience, to give an opinion). A witness can testify to extremely complex matters without having to qualify as an expert witness or be asked to give an expert opinion about a particular matter at issue in the case.

For example, in many cases involving digital evidence, either the investigator at the scene or an expert forensic examiner could testify as to how digital evidence was located. While the forensic examination process may involve a scientific method and the examiner may well have used experts skills and techniques, the only relevant issue at trial is whether the evidence in question was on the suspect's computer, not how it was located. Either it is or is not on the computer. For that question, the examiner is a fact witness.

Even if a scientific method was used to locate or identify evidence, unless an expert is giving an opinion based on that scientific method, the method does not have to meet the *Daubert* or *Frye* standard discussed in Section C ('Integrity, Discovery, and Disclosure of Electronic Evidence') above. If a metal detector was used to detect spent cartridges at a crime scene, there is no need to qualify the 'science' of metal detectors. Once the cartridge is found the issue focuses on the cartridge. Most cases involving digital evidence should be viewed similarly.

B. Using Technical Fact Witnesses and Expert Opinion Witnesses Effectively

In the metal detector example above, although an expert is not needed to explain how the cartridges or bullets were found, whether the lands and grooves on a particular bullet can be matched to a bullet fired from the suspect weapon will require the opinion of a qualified ballistics expert. Similarly, there may be situations in digital evidence cases when expert opinion testimony is needed.

When working with expert witnesses in digital evidence cases, pay special attention to the following:¹¹

- 1. Identifying a community of Qualified Technical Experts**
- 2. Explaining the issues in the case and the legal constraints for examining the available evidence**
- 3. Planning to Deal with a *Daubert* Gatekeeping Challenge**
- 4. Preparing the Witness for Trial**
 - a. Learning to tell technical stories
 - b. Making direct examination simple and interesting
 - c. Developing visual aides that teach complex concepts
 - d. Avoiding bias in demeanor and testimony
 - e. Preparing the witness for defense experts and theories
 - f. Helping experts draft their own reports
 - g. Preparing for cross-examination
 - h. Practice, practice, practice

4. Recurring Issues In Computer Crime Trials

While each digital evidence case will be different, there are some common issues that arise both with regard to the basic elements of the crimes charged and with regard to the nature of computers and computer networks. These include:

¹¹ Fred Smith will elaborate upon these points.

A. Identity

Although the digital evidence may show that a crime was committed from the defendant's computer, the prosecution may need to directly connect the defendant to the computer.

The defendant can be tied personally to information found on the computer in a variety of ways, including:

- Confession or admission
- Circumstantially (the defendant was the only resident at the computer location, the defendant is the registered user of the hardware or software)
- Substantive information on the computer uniquely within the defendant's knowledge
- Content analysis. The existence of unique similarities between the grammar, spelling, or other characteristics of the evidence and other writing known to have been authored by the defendant.

B. Knowledge

In some cases it may be necessary to show the defendant's knowledge of the digital evidence on the computer. For example, one common defense in possession of child pornography cases is the claim that the defendant was not aware the images were on his computer. Such a claim can often be disproved by:

- The number of such images found
- The directory structure. Were the pictures placed in directories that were logically related to the pictures (e.g., C:\Pictures\young\girls\sex.)?
- File names. Are the file names unique and do they accurately describe the contents of the files (e.g., 8yrold.jpg.baby.jpg)?
- Other indications on the computer of the defendant's interest in child pornography, such as newsgroup subscriptions, history of Internet activity, etc.

C. Chronology of Events

Time and date stamps on files can be powerful evidence tying the defendant to the computer and the computer to the crime. The evidence may show that time and date stamps have limitations:

- The accuracy of a computer's time and date stamps is directly dependent upon the accuracy of the computer's internal clock.
- Time and date stamps are tied to a particular time zone.
- Time and date stamps can be easily manipulated.

The accuracy or inaccuracy of a time/date stamp can be shown in a variety of ways, including:

1. Consistent offsets

Are the files consistently off by a specific amount of time or date (i.e., always one hour off or two days off.)? If so, there is a persuasive argument that the file times and dates can be adjusted by that offset and reflect accurate times/dates.

2. Internal file accuracy

Is the time/date on a file consistent with the contents of a file? For example, is the date stamp on a file consisting of a letter consistent with the date in the introductory portions of the letter?

3. E-mail header dates compared to time-date stamps assigned by the system.

On e-mail systems where e-mail is saved as individual files (or where e-mail has been copied to a file) is the time and date information contained in the header of the e-mail consistent with the time and date stamp the system assigned the file?

4. Compare known times and dates to system assigned times and dates

Were files downloaded from the victim at a known date and time? Do the files appear on the suspect's computer with time and date stamps consistent with that date and time?

5. Networked computer

Many networks are configured to automatically update a client's internal clock when the client is logged on. Is the computer in question a network computer? Are the clocks on computers on that network auto updated?

6. Patterns of file creation times and dates

Is there a cluster of files created at the same date/time? The relative date/time (i.e., all created at the same time) may be more important than the absolute date/time of creation.

7. Experiment

Use the suspect's hardware (but not the original drive) to create and alter files. Observe the discrepancies, if any, and compare to the evidence files.

5. Jury Instructions

- A. Do pattern jury instructions exist in the jurisdiction in question, or can approved instructions from other jurisdictions be adopted in this jurisdiction?

If no pattern instruction has been approved in a given jurisdiction, can instructions in analogous areas based on the elements of similar crimes be used? For example, burglary or trespass instructions may serve as models for a computer trespass case.

- B. Are there any special terms needing definition?

6. Jury Selection

Consider carefully the kind of jurors that would be best for a particular computer crime case involving the admission of complex or highly technical evidence. Investigators can assist prosecutors in thinking of appropriate questions and in considering the makeup of the overall panel and of individual jurors who are called. The goal is not to select technical experts to be jurors, but to find a few individuals who have sufficient experience using computers to be able to follow the technical testimony that must be presented in the course of the trial. Ideally one or more of these jurors will be able to become an advocate of the evidence that is presented to them during deliberations after the case has been presented.

- A. *Voir Dire*

Depending on the case, crucial information to obtain from potential jurors in *voir dire* may include:

- 1. What is their knowledge and experience level with computers?**
- 2. Do they view digital evidence with suspicion?**
- 3. Do they have strong views (one way or the other) about the specific crime being prosecuted?**

4. **Do they view victims of computer crimes, particularly business victims, as partially to blame?**
5. **What is their knowledge and experience level with the Internet, e-mail, and other specifics aspects of computers relevant to the case?**
6. **Has anyone ever been the victim of a crime similar to the one being prosecuted?**
7. **What security measures, if any, do they use for their own computer?**
8. **In intrusion cases, find out their views on privacy and assumption of the risk in using networked computers.**

B. Special Considerations for Computer Experts in the Jury Pool

Think of the problem of ending up with a computer expert on such a jury in the same way you would think about ending up with a doctor as a potential juror in a case in which medical testimony is relevant.

A doctor may be able to explain complicated medical concepts to fellow jurors, and a computer expert might be expected to lead the deliberations as to information technology issues in the case.

However, just as a doctor on the jury might require the government to over-prove the prosecution's case and to disprove totally immaterial matters, so might a computer expert substitute his or her knowledge for the evidence presented and dominate the deliberations concerning the forensic examinations and analyses.

7. Presenting complicated/technical issues

There are some methods of presenting complicated evidence, whether in digital evidence cases or other complex cases, which work well. These include:

- A. Using very simple analogies can explain general concepts (e.g., sending e-mail is like sending a postcard.

It goes from the mail box to the local post office through other post offices to the recipient's local post office and then to their mail box.). Keep in mind, however, that all analogies can have legal consequences.

- B. Define technical words in terms the jury can understand

C. Use pictures, drawings or graphs to demonstrate complex systems or concepts.

D. Build the knowledge of the jury through the opening statement and through each successive layer of the testimony of the witnesses.

Introduce them to simple concepts, explain those concepts in detail, and then move to more complex issues, which rely on understanding the initial concepts.

E. Where possible, relate the technology in the case to the technology the jurors indicated in *voir dire* they were familiar with or used.