CHAPTER 3

Digital Evidence in the Courtroom

Eoghan Casey

> … the law and the scientific knowledge to which it refers often serve different purposes. Concerned with ordering men's conduct in accordance with certain standards, values, and societal goals, the legal system is a prescriptive and normative one dealing with the "ought to be." Much scientific knowledge, on the other hand, is purely descriptive; its "laws" seek not to control or judge the phenomenon of the real world, but to describe and explain them in neutral terms.
>
> Korn (1966)

CONTENTS

Duty of Experts 51
Admissibility 56
Levels of Certainty in Digital Forensics ...68
Direct Versus Circumstantial Evidence 72
Scientific Evidence ...73
Presenting Digital Evidence 75

The purpose of a courtroom is to administer justice, and the role of digital investigators in this context is to present supporting facts and probabilities. As such, courts depend on the trustworthiness of digital investigators and their ability to present technical evidence accurately; it is their duty to present findings in a clear, factual, and objective manner. They must resist the influence of others' opinions and avoid jumping to conclusions. There is no place for advocacy or judgmental assertions in a digital investigator's professional work product, whether that be testimony or expert reports.

In addition to requiring digital investigators to be honest and forthright, courts are concerned with the authenticity of the digital evidence they present. Individuals processing evidence must realize that, in addition to being pertinent, evidence must meet certain standards to be admitted. It is easy enough to claim that a bloody glove was found in a suspect's home, but it is another matter to prove it. When guilt or innocence hangs in the balance, the proof that evidence is authentic and has not been tampered with becomes essential. The U.S. Federal Rules of Evidence, the UK Police and Criminal Evidence Act (PACE) and the Civil Evidence Act, and similar rules of evidence in other countries were established to help evaluate evidence. For instance, before admitting evidence, a court will generally ensure that it is relevant and will evaluate it to determine if that is what its proponent claims, if the evidence is hearsay, if it is unduly prejudicial, and if the original is required or a copy is sufficient. A failure to consider these issues from the outset may cause evidence to be excluded, potentially losing the case.

Digital Evidence and Computer Crime, Third Edition

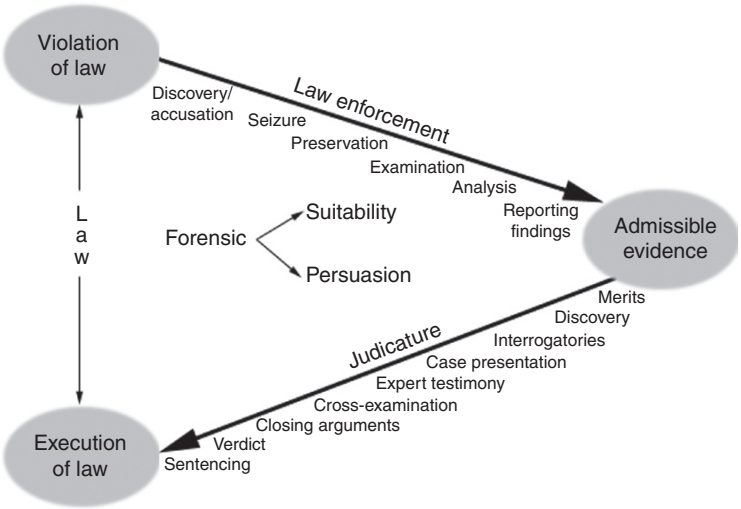

FIGURE 3.1
Overview of case/incident resolution process.

The process of determining if wrongdoing has occurred and whether punitive measures are warranted is depicted in Figure 3.1 to help digital investigators see the placement of their activities relative to other necessary events. At the outset of an investigation, there is some form of suspicion, alert, or accusation. Ideally, the investigation will proceed to information gathering and proper evidence handling and analysis, leading to a clear and precise explanation of facts in expert testimony. Although actual investigations rarely follow such an orderly path, this linear representation is useful for structuring procedures and formalizing the case management process. In practice, investigations can be nonlinear, such as performing some basic analysis in the collection stage or returning to the collection step when analysis leads to additional evidence.

The collection or seizure phase of a digital investigation, having someone on the search team who is trained to handle digital evidence can reduce the number of people who handle the evidence, thereby streamlining the presentation of the case and minimizing the defense opportunities to impugn the integrity of the evidence. Additionally, having standard operating procedures, continuing education, and clear policies helps to maintain consistency and prevent contamination of evidence. Given the ease with which digital evidence can be altered, the importance of procedures and the use of only trained personnel to handle and examine the evidence cannot be overstated.

This chapter provides an overview of the major issues that arise when digital evidence is presented in court, including the duty of experts, resisting preconceived theories and the influence of others, admissibility, uncertainty, and

presentation of digital evidence. This chapter is not intended as legal advice, and competent legal advice should be sought to address specific issues in a case and to ensure that nuances of the law are considered. There are many complexities and nuances associated with the admissibility of evidence. The process of preparing a case for trial is time consuming and expensive and may not result in a satisfactory outcome, particularly if there is insufficient evidence or evidence was handled improperly. Also, before deciding to take legal action, organizations must consider if they are required to disclose information about their systems that may be sensitive (e.g., network topology, system configuration information, and source code of custom monitoring tools) and other details about their operations that they may not want to make public.

3.1 DUTY OF EXPERTS

In general terms, experts have a duty to present the objective, unbiased truth of the matter before the court. It is not their role to advocate for one side; that burden is on the attorneys. The UK Criminal Procedure Rules (CPR) specifically address this issue with the following statements:

1. An expert must help the court to achieve the overriding objective by giving objective, unbiased opinion on matters within his expertise.
2. This duty overrides any obligation to the person from whom he receives instructions or by whom he is paid.
3. This duty includes an obligation to inform all parties and the court if the expert's opinion changes from that contained in a report served as evidence or given in a statement.[1]

There are many factors that can divert experts from their duty, despite the best intentions. It is the human condition to have emotional reactions, harbor prejudices, and be subject to other subtle influences. However, to be an effective digital investigator and expert witness, it is necessary to be more self-aware and resistant to subtle influences like bias, emotion, and greed. The following sections discuss the most common pitfalls to be avoided.

3.1.1 Resisting Influences

Digital investigators are often pressured, both subtly and overtly, to concentrate on specific areas of inquiry and to reach conclusions that are favorable to a particular party. Some cases and the nature of the evidence uncovered (digital or otherwise) will take digital investigators to emotional limits, testing their resolve. Members of law enforcement who conducted an investigation to apprehend a defendant may be required to present digital evidence objectively

[1] Explanations of these rules are available at [redacted].

in court and may have the duty to identify weaknesses in a prosecution case. Computer security professionals in the private sector often have to investigate longtime coworkers and cases in all sectors can involve brutal abuse of innocent victims, inciting distraught individuals and communities to strike out at the first available suspect. The effectiveness of the investigative process depends upon high levels of objectivity applied at all stages. A good digital investigator must resist such influences and remain objective in the most trying situations.

Clients, whether they are individuals or companies, will believe firmly in their cause and may present their position stridently. When a client tells a digital investigator how dishonest the other party is or presents the case in a way that is intended to garner sympathy, the digital investigator must resist any urge to form opinions about the case based on these emotional factors.

Attorneys have a responsibility to build the strongest case for their client. Therefore, it is to be expected that attorneys will ask a digital investigator whether a conclusion that is favourable to their client can be supported by the evidence. Digital investigators must be extremely firm on what conclusions the evidence supports to avoid being swayed by an attorney trying to push the limits of the evidence.

Digital investigators can also be influenced by the pressures of their peers. Certain organizations prohibit their members from working for the defense in criminal cases. The refusal to perform criminal defense work shows a clear bias that is not based on evidence in a case. As a result, digital investigators who accept this restriction will have difficulty defending their objectivity when challenged in the courtroom.

If a prime suspect emerges as an investigation progresses, digital investigators must resist the urge to formally assert that an individual is guilty, even though it is an investigator's duty to champion the truth.

PRACTITIONER'S TIP

A digital investigator can say; "I found images of children being sexually abused on the computer used by the defendant. I have investigated the possibility that a third party may have had access to the computer via a Trojan, have run certain tests, and have found no trace to support this hypothesis." This statement does not assert that the defendant is guilty of the offense of possessing child pornography. At the same time, this statement considers the possibility that a third party may have had access to the defendant's computer, but that there is no evidence of such access. Ultimately, it is for the court to consider the totality of the evidence, not just one digital investigator's testimony, to reach a decision.

A common error is to use a verification methodology, focusing on a likely suspect and trying to fit the evidence around that individual. When a prime

suspect has been identified and a theory of the offense has been formed, experienced investigators will try to prove themselves wrong. Implicating an individual is not the job of investigators—this is for the courts to decide and unlike scientific truth, legal truth is judgment based as discussed in Section 3.2.

3.1.2 Avoiding Preconceived Theories

Trained, experienced investigators will begin by considering whether a crime or infraction has actually occurred. For instance, when log files indicate that an employee misused a machine but he adamantly denies it, a digital investigator should carefully examine the logs for signs of error.

CASE EXAMPLE

An employee was suspected of unauthorized access to the root account on a critical UNIX server on the basis of entries in the sulog. Careful inspection of the system indicated that the utmp/wtmp log was corrupt, causing erroneous entries in the sulog. If the digital investigator was aware that such erroneous log entries were possible, the misunderstanding could have been avoided and a full-blown investigation would not have been necessary.

Similarly, when a large amount of data is missing on a computer and an intruder is suspected, digital investigators should determine if the damage is more consistent with disk corruption than an intrusion. In one case, a suicide note on a computer raised concern because it had a creation date after the victim's death. It transpired that the computer clock was incorrect and the note was actually written before the suicide.

When an investigator has ruled out innocent explanation, the focus shifts toward determining what happened, where, when, and how, who was involved, and why. The process by which digital evidence is uncovered and applied to these issues involves several steps covered in Part 2 (Digital Investigations) of this text, each employing strict protocols, proven methods, and, in some cases, trusted tools. The success of this process depends heavily on the experience and skill of the digital investigators, forensic analysts, and crime scene technicians who must collaborate to piece the evidence together and develop a convincing account of the offense.

The very traits that make good digital investigators may lead them to depend on experience instead of individual case-related facts, resulting in unfounded conclusions. Individuals with inquiring minds and an enthusiasm for apprehending offenders may begin to form theories about what might have occurred the moment they learn about an alleged crime, before examining available evidence. Even experienced investigators are prone to forming such preconceived theories because they are inclined to approach a case in the same way as they have approached past cases, knowing that their previous work was upheld.

Hans Gross, one of this century's preeminent criminologists, put it best in the following quotation:

> Nothing can be known if nothing has happened; and yet, while still awaiting the discovery of the criminal, while yet only on the way to the locality of the crime, one comes unconsciously to formulate a theory doubtless not quite void of foundation but having only a superficial connection with the reality; you have already heard a similar story, perhaps you have formerly seen an analogous case; you have had an idea for a long time that things would turn out in such and such a way. This is enough; the details of the case are no longer studied with entire freedom of mind. Or a chance suggestion thrown out by another, a countenance which strikes one, a thousand other fortuitous incidents, above all losing sight of the association of ideas end in a preconceived theory, which neither rests on juridical reasoning nor is justified by actual facts.
>
> **(Gross, 1924)**

As experience increases and methods employed are verified, the accuracy of these "predictions" or "investigator's intuition" may improve. Conjecture based upon experience has its place in effective triage but should not be relied upon to the exclusion of rigorous investigative measures. The investigative process demands that each case be viewed as unique, with its own set of circumstances and exhibits. Letting the evidence speak for itself is particularly important when offenders take steps to misdirect investigators by staging a crime scene or concealing evidence.

The main risk of developing full hypotheses before closely examining available evidence is that investigators will impose their preconceptions during evidence collection and analysis, potentially missing or misinterpreting a critical clue simply because it does not match their notion of what occurred. For instance, when recovering a deleted file named "pornlyr5.gif" depicting a naked baby, an investigator might impose a first letter on the file that indicates "pornlyr5.gif" rather than "bornlyr5.gif". Instead, if the original file name is not recoverable, a neutral character such as "_" should be used to indicate that the first letter is unknown.

This caveat also applies to the scientific method from which the investigative process borrows heavily. At the foundation of both is the tenet that no observation or analysis is free from the possibility of error. Simply trying to validate an assertion increases the chance of error—the tendency is for the analysis to be skewed in favor of the hypothesis. Conversely, on developing many theories, an investigator is owned by none, and by seeking evidence to disprove each hypothesis, the likelihood of objective analysis increases (Popper, 1959). Therefore, the most effective way to counteract preconceived theories is to employ a methodology that compels digital investigators to find flaws in their theories, a practice known as *falsification*.

3.1.3 Scientific Truth and Legal Judgment

Generally, in the prosecutorial environment, theories based upon scientific truth are subordinate to legal judgment and digital investigators must accept the ruling of the court. For instance, in common law countries, the standard of proof for criminal prosecutions is *beyond a reasonable doubt* and for civil disputes it is the *balance of probabilities.* Legal judgment is influenced by ideas like fairness and justice, and the outcome may not conform to the scientific truth. In a trial, the object is to assess the case as a whole to determine whether there is sufficient proof of guilt. The decision on the facts is specific to that trial. In "science," we are trying to identify rules that are universally true. In nearly all trials, scientific and technical evidence is only part of the total picture. A court may convict an individual even if the case is weak or some evidence suggests innocence.

> Most forensic scientists accept the reality that while truthful evidence derived from scientific testing is useful for establishing justice, justice may nevertheless be negotiated. In these negotiations, and in the just resolution of conflict under the law, truthful evidence may be subordinated to issues of fairness, and truthful evidence may be manipulated by forces beyond the ability of the forensic scientist to control or perhaps even to appreciate fully.
>
> **(Thornton, 1997)**

Digital investigators must generally accept an attorney's decision not to proceed with a case or not to disclose certain evidence. However, in some instances, investigators will face an ethical dilemma if they feel that a miscarriage of justice has occurred. An investigator may be motivated to disclose information to the media, or to assist in a follow-up investigation, but such choices must be made with great care because a repeated tendency to disagree with the outcome of an investigation or become a whistleblower could ruin an investigator's credibility and even expose him/her to legal action.

CASE EXAMPLE (NEW MEXICO, 2005)

Shawn Carpenter was a computer security professional at Sandia National Laboratories who realized that intruders from China were gaining unauthorized access to Sandia's network and stealing sensitive information. He began to track the intruders and "hack back" into systems they were using to store tools and stolen data. On one of these systems, Carpenter found files that had been stolen from U.S. government systems and he brought the problem to the attention of his supervisors. After failing to get anyone at Sandia to inform other victim organizations that they were under attack and that their data were being stolen, Carpenter took matters into his own hands. He became a secret informant for the FBI, providing them with details about the attackers. When Sandia discovered that Carpenter had done this, they fired him. Subsequently, after several years of legal battles, Sandia was compelled to pay Carpenter over $5 million in damages.

Employment of a rigorous investigative process may uncover unpopular or even difficult to believe truths that will be rejected by less objective people. Digital

investigators may be confronted with a difficult choice—of renouncing such truth or facing the consequences of holding an unpopular belief. It is the duty of investigators to unwaveringly assert the truth even in the face of opposition. This is not intended to suggest that science is infallible. The fact is that science is still advancing and previous theories are being replaced by better ones. For instance, DNA analysis has largely replaced blood typing in forensic serology, and although the technique of blood typing was valid, it was not conclusive enough to support some of the convictions based upon evidence derived from that analysis alone. This weakness can be shown in dramatic fashion by the existence and success of the Innocence Project,[2] which is using results of DNA analysis to overturn wrongful convictions based on less than conclusive ABO blood typing and enzyme testing.

When preparing for the final step of the investigative process (the decision or verdict), it is important to keep in mind that discrepancies between legal judgment and theories based on scientific truth may arise from a lack of understanding on the part of the decision makers. The court process differs from scientific peer review, where reviewers are qualified to understand and comment on relevant facts and methods with credibility. When technical evidence supporting theories based on scientific truth is presented to a group of reviewers who are not familiar with the methods used, misunderstandings and misconceptions may result. To minimize the risk of such misunderstandings, the investigative process and the evidence uncovered to support prosecution must be presented clearly to the court as discussed at the end of this chapter. A clear presentation of findings is also necessary when the investigative process is presented to decision makers who are in charge of civilian and military network operations. However, investigators may find this situation easier as decision makers in these domains often have some familiarity with methods and tools employed in forensic investigations for computer and network defense.

3.2 ADMISSIBILITY

The concept of admissibility is a simple one. Courts need to determine whether evidence is "safe" to put before a jury and will help provide a solid foundation for making a decision in the case. In practice, admissibility is a set of legal tests carried out by a judge to assess an item of evidence. This assessment process can become complicated, particularly when the evidence was not handled properly or has traits that make it less reliable or more prejudicial. Some jurisdictions have rules relating to admissibility that are formal and sometimes inflexible, while other jurisdictions give judges more discretion.

---

[2] [redacted].

In 2007, a case in Maryland dealt with the admissibility of digital evidence specifically and provided general guidelines for reaching a decision.

> [I]t can be expected that electronic evidence will constitute much, if not most, of the evidence used in future motions practice or at trial, [and] counsel should know how to get it right on the first try [Lorraine v. Markel Am. Ins. Co., 2007 WL 1300739 (D. Md., May 4, 2007) [redacted]].

In this case, both parties offered copies of e-mail messages that could not be authenticated properly. The magistrate judge would not admit the e-mail messages, noting that unauthenticated e-mails are a form of computer-generated evidence that pose evidential issues. The magistrate outlined five issues that must be considered when assessing whether digital evidence will be admitted:

1. Relevance
2. Authenticity
3. Not hearsay or admissible hearsay
4. Best evidence
5. Not unduly prejudicial

Although some of these issues may not be applicable in certain instances, each must be considered.

Other issues that may prevent digital evidence from being admitted by courts are improper handling and illegal search and seizure. Although courts have been somewhat lenient in the past on improper handling of digital evidence, more challenges are being raised relating to evidence handling procedures as more judges and attorneys become familiar with digital evidence. Courts are much less forgiving of illegal search and seizure of evidence.

3.2.1 Search Warrants

The most common mistake that prevents digital evidence from being admitted by courts is that it is obtained without authorization. Generally, a warrant is required to search and seize evidence. As discussed in Chapter 4, the Fourth Amendment requires that a search warrant be secured before law enforcement officers can search a person's house, person, papers, and effects. To obtain a warrant, investigators must demonstrate probable cause and detail the place to be searched and the persons or things to be seized. More specifically, investigators have to convince a judge or magistrate that, in all probability:

1. a crime has been committed;
2. evidence of crime is in existence; and
3. the evidence is likely to exist at the place to be searched.

Search warrants in the United Kingdom and other European countries can be more loosely defined than in the United States. In the United Kingdom, for instance, there are several kinds of warrants (e.g., a specific premises warrant, all-premises warrant, and multiple entry warrant), and they do not have to specify what things will be seized.

The main exceptions that can allow a warrantless search in the United States are plain view, consent, and exigency. If investigators see evidence in plain view, they can seize it provided they have obtained access to the area validly. By obtaining consent to search, investigators can perform a search without a warrant but care must be employed when obtaining consent to reduce the chance of the search being successfully challenged in court.

PRACTITIONER'S TIP

In practice, many searches are conducted with consent. One of the biggest problems with consensual searches is that digital investigators must cease the search when the owner withdraws consent. However, digital investigators may be able to use the evidence gathered from a consensual search to establish probable cause and obtain a search warrant.

CASE EXAMPLE (UNITED STATES V. TURNER, 1999)

Law enforcement officers obtained permission from the defendant to search his home for evidence relating to a sexual assault of one of his neighbors. During the search, an investigator looked at Turner's computer and identified child pornography. Turner was indicted for possessing child pornography but filed a suppression hearing to exclude the computer files on the ground that he had not consented to the search of his computer and it was not objectively reasonable for the detective to have concluded that evidence of the sexual assault—the stated object of the consent search—would be found in files with such labels as "young" or "young with breasts."

Regarding exigency, a warrantless search can be made for any emergency threatening life and limb or in which digital evidence is imminently likely to be altered or destroyed. In the latter circumstances, it might be necessary to seize the computing device immediately to reduce the potential of destruction of evidence. After the digital evidence is preserved, it is generally prudent to obtain a warrant to conduct a forensic examination of the digital evidence.

PRACTITIONER'S TIP

Once a search warrant is obtained, there is generally a limited amount of time to execute the search. Therefore, it is prudent to obtain a search warrant only after sufficient preparations have been made to perform the search in the allotted time period. Any evidence obtained under an expired search warrant may not be admissible.

There are four questions that investigators must consider when searching and seizing digital evidence:

1. Does the Fourth Amendment and/or the Electronic Communications Privacy Act (ECPA) apply to the situation?
2. Have the Fourth Amendment and/or ECPA requirements been met?
3. How long can investigators remain at the scene?
4. What do investigators need to reenter?

When addressing these questions, remember that the ECPA prohibits anyone, not just the government, from unlawfully accessing or intercepting electronic communications, whereas the Fourth Amendment applies only to the government.

Even when investigators are authorized to search a computer, they must maintain focus on the crime under investigation. For instance, in United States v. Carey (1998), the investigator found child pornography on a machine while searching for evidence of drug-related activity but the images were inadmissible because they were outside of the scope of the warrant.

One approach to dealing with this issue is to obtain another search warrant for that crime when evidence of another crime is discovered.

CASE EXAMPLE (UNITED STATES V. GRAY, 1999)

During an investigation into Montgomery Gray's alleged unauthorized access to National Library of Medicine computer systems, the FBI obtained a warrant to seize four computers from Gray's home and look for information downloaded from the library. While examining Gray's computers, a digital investigator found pornographic images in directories named "teen" and "tiny teen," halted the search, and obtained a second warrant to search for pornography.

CASE EXAMPLE (WISCONSIN V. SCHROEDER, 1999)

While investigating an online harassment complaint made against Keith Schroeder, a digital investigator found evidence relating to the harassment complaint on his computer and noticed some pornographic pictures of children. A second warrant was obtained, giving the digital investigator authority to look for child pornography on Schroeder's computer. Schroeder was charged with 19 counts of possession of child pornography and convicted on 18 counts after a jury trial. For the harassment, Schroeder was tried in a separate proceeding for unlawful use of a computer and disorderly conduct.

However, in 2009, the U.S. 9th Circuit Court recommended stricter controls for forensic analysis of digital evidence, challenging the concept of plain view in the digital dimension and suggesting approaches to reduce the risk of associated privacy violations (U.S. v. CDT).

3.2.2 Authentication of Digital Evidence

As discussed in Chapter 1, courts generally ask if the recovered evidence is the same as the originally seized data when considering whether digital evidence

is admissible. To demonstrate that digital evidence is authentic, it is generally necessary to satisfy the court that it was acquired from a specific computer and/or location, that a complete and accurate copy of digital evidence was acquired, and that it has remained unchanged since it was collected. In some cases it may also be necessary to demonstrate that specific information is accurate, such as dates associated with a particular file that is important to the case. The reliability of digital evidence clearly plays a critical role in the authentication process, as discussed in more detail later in this chapter.

Chain of custody and integrity documentation are important for demonstrating the authenticity of digital evidence. Proper chain of custody demonstrates that digital evidence was acquired from a specific system and/or location, and that it was continuously controlled since it was collected. Thus, proper chain of custody documentation enables the court to link the digital evidence to the crime. Incomplete documentation can result in confusion over where the digital evidence was obtained and can raise doubts about the trustworthiness of the digital evidence.

Integrity documentation helps demonstrate that digital evidence has not been altered since it was collected. In situations where the hash value of digital evidence differs from the original, it may be possible to isolate the altered portions and verify the integrity of the remainder. For example, bad sectors on a hard drive generally cause the hash value calculated for the drive to change each time it is computed. Documenting the location of bad sectors will help a digital investigator determine whether they are allocated to files that are important to the case. In addition, the hash values of individual files that are important to the case can be compared with those on the original hard drive to ensure that specific files are not impacted by the bad sectors.

When there are concerns that digital evidence was mishandled and that potentially exculpatory information was destroyed, courts may still decide to admit the evidence. In one case, digital investigators inadvertently booted the evidential computer but were able to satisfy the court that the digital evidence could still be trusted.

CASE EXAMPLE (UNITED STATES V. BUNTY, 2008)

U.S. Customs and Border Protection agents inspected Patrick Bunty's two laptops and various storage media when he arrived in Philadelphia from London and found images of child pornography. The agents used a government-owned computer to open files on Bunty's storage media, and attempted to examine the contents of his laptops. When they instructed Bunty to provide access to his laptops, he entered an incorrect password on one of the laptops that locked the laptop and prevented the agents from examining its contents at that time. In court, Bunty argued that the evidence should not be admitted in part because the government had not created forensic duplicates of the media prior to their inspection. The court held that the evidence was admissible, concluding that the government's handling of the evidence was in good faith and that their alterations of the evidence were not sufficient to exclude the evidence.

In some cases, the opposing party will attempt to cast doubt on more malleable forms of digital evidence, such as logs of online chat sessions.

CASE EXAMPLE (MICHIGAN V. MILLER, 2001)

In 2000, e-mail and AOL instant messages provided the compelling evidence to convict Sharee Miller of conspiring to kill her husband and abetting the suicide of the admitted killer (Jerry Cassaday) she had seduced with the assistance of the Internet. Miller carefully controlled the killer's perception of her husband, going so far as to masquerade as her husband to send the killer offensive messages. In this case, the authenticity of the AOL instant messages was questioned in light of the possibility that such an online conversation could be staged (Bean, 2003).

CASE EXAMPLE (UNITED STATES V. TANK, 1998)

In United States v. Tank, a case related to the Orchid/Wonderland Club investigation, the defendant argued that the authenticity and relevance of Internet chat logs were not adequately established. One of the points the defense argued was that the chat logs could be easily modified. The prosecution used a number of witnesses to establish that the logs were authentic. The court held that "printouts of computer-generated logs of 'chat room' discussions may be established by evidence showing how they were prepared, their accuracy in representing the conversations, and their connection to the defendant."

The case of United States v. Tank is significant because it is one of the first to deal with the authentication of chat logs. However, some feel that there are still questions about the authenticity and reliability of Internet chat logs that have not been addressed. On Internet Relay Chat (IRC), for example, in addition to the chat channel window, there may be important information in other areas of an IRC client such as the status window and private chat or fserve windows. As it is not possible for one investigator to view every window simultaneously, digital investigators must rely heavily on the logs for an account of what occurred. In some instances, investigators have been able to compensate for a lack of documentation by testifying that the evidence being presented is authentic and reliable. Of course, it is best to have solid documentation.

3.2.3 Reliability of Digital Evidence

To authenticate digital evidence, it may also be necessary to assess its reliability. There are two general approaches to assessing whether digital evidence can be relied upon in court. The first approach is to focus on whether the computer that generated the evidence was functioning normally, and the other approach is to examine the actual digital evidence for evidence of tampering and other damage.

In the past, the majority of legislation in the United States and United Kingdom followed the first approach, instructing courts to evaluate computer-generated records on the basis of the reliability of the system and process

that generated the records. For instance, the section in the Federal Rules of Evidence 901 (b) (9) titled "Requirement of Authentication or Identification" includes "evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result." In the United Kingdom, under Section 69 of PACE, there was a formal requirement for a positive assertion that the computer systems involved were working properly. The rationale for this approach is that, because records of this type are not the counterpart of a statement by a human declarant, which should ideally be tested by cross-examination of that declarant, they should not be treated as hearsay, but rather their admissibility should be determined on the basis of the reliability and accuracy of the process involved (Strong, 1992).

However, the reliability of a particular computer system or process is difficult to assess and, in practice, courts are not well equipped to assess the reliability of computer systems or processes. The increasing variety and complexity of computer systems make it "increasingly impractical to examine (and therefore certify) all the intricacies of computer operation" (Castell, 1990). Furthermore, requiring programmers and system designers to establish that computer systems are reliable at the lowest level is untenable, "overburdening already crowded courts with hordes of technical witnesses" (People v. Lugashi, 1988). An added difficulty in certifying a computer or even a specific process is that even a process that is generally reliable can malfunction under certain circumstances. Computer systems can have unforeseen operating errors, occasionally resulting in data corruption or catastrophic crashes. Therefore, it is not safe to presume that mechanical instruments were in order at the material time. Furthermore, because programs can be upgraded to fix bugs and modify functionality, it is not safe to assume that a particular process on the current system functioned in the same way at the time of the offense. This approach also breaks down when the computer system in question is under the control of the perpetrator. It is not feasible to rigidly categorize types of evidence in general—it is not valid to claim that all NT event logs are reliable. These logs can be tampered with and there may be signs of tampering such as deleted log entries in a computer intrusion case. Even if it were possible to determine that a computer system or process is generally reliable, this does not necessarily imply that the evidence at hand has not been tampered with to conceal a crime or misdirect investigators.

In 1997, the UK Law Commission recommended the repeal of Section 69 of PACE (Law Commission, 1997), noting the difficulties in assessing the reliability of computer systems, and criticizing Section 69 of PACE because it required a complex certification of the system even when there is no sign that the evidence might be unreliable, and it failed to address the major causes of inaccuracy in digital evidence.

> Without section 69, a common law presumption comes into play: In the absence of evidence to the contrary, the courts will presume that mechanical instruments were in order at the material time. Where a party sought to rely on the presumption, it would not need to lead evidence that the computer was working properly on the occasion in question unless there was evidence that it may not have been in which case the party would have to prove that it was (beyond reasonable doubt in the case of the prosecution, and on the balance of probabilities in the case of the defence). The principle has been applied to such devices as speedometers and traffic lights. … We are satisfied that the presumption of proper functioning would apply to computers, thus throwing an evidential burden on to the opposing party, but that that burden would be interpreted in such a way as to ensure that the presumption did not result in a conviction merely because the defence had failed to adduce evidence of malfunction which it was in no position to adduce.
>
> **(UK Law Commission, 1997)**

In 2001, as a result of these difficulties, Section 69 of PACE was largely abandoned, but it can still be useful when considering the reliability of computer-generated business records.

Even when there is a reasonable doubt regarding the reliability of digital evidence, this does not necessarily make it inadmissible, but will reduce the amount of weight it is given by the court. For instance, if there is concern that the evidence was tampered with prior to collection, this doubt may reduce the weight assigned to the evidence. In several cases, attorneys have argued that digital evidence was untrustworthy simply because there was a theoretical possibility that it could have been altered or fabricated. However, as judges become more familiar with digital evidence, they are requiring evidence to support claims of untrustworthiness. As noted in the U.S. Department of Justice Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations manual:

> Absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record. See Whitaker, 127 F.3d at 602 (declining to disturb trial judge's ruling that computer records were admissible because allegation of tampering was "almost wild-eyed speculation … [without] evidence to support such a scenario"); United States v. Bonallo, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness."); United States v. Glasser, 773 F.2d 1553, 1559 (11th Cir. 1985) ("The existence of an air-tight security system [to prevent tampering] is not, however, a prerequisite to the admissibility of computer printouts. If such a prerequisite did exist, it would become virtually impossible to admit computer-generated records; the party

> opposing admission would have to show only that a better security system was feasible.") … the government may need to disclose "what operations the computer had been instructed to perform [as well as] the precise instruction that had been given" if the opposing party requests. United States v. Dioguardi, 428 F.2d 1033, 1038 (C.A.N.Y. 1970). Notably, once a minimum standard of trustworthiness has been established, questions as to the accuracy of computer records "resulting from … the operation of the computer program" affect only the weight of the evidence, not its admissibility. United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988).
>
> **(USDOJ, 2002)**

In general, when assessing the reliability of digital evidence, it is more effective to focus on the evidence itself rather than the reliability of the process that created it. Rather than trying to assert that a specific computer or process is generally reliable, it is more effective to identify malicious tampering and destruction of a given item of digital evidence. For instance, identifying and isolating falsified records in a specific log file or bad sectors on a hard drive enable fact-finders to rely on the remaining reliable data.

3.2.4 Best Evidence

When dealing with the contents of a writing, recording, or photograph, courts sometimes require the original evidence. The original purpose of this rule was to ensure that decisions made in court were based on the best available information. With the advent of photocopiers, scanners, computers, and other technology that can create effectively identical duplicates, copies became acceptable in place of the original, unless "a genuine question is raised as to the authenticity of the original or the accuracy of the copy or under the circumstances it would be unfair to admit the copy in lieu of the original" (Best Evidence Rule).

Because an exact duplicate of most forms of digital evidence can be made, a copy is generally acceptable. In fact, presenting a copy of digital evidence is usually more desirable because it eliminates the risk that the original will be accidentally altered. Even a paper printout of a digital document may be considered equivalent to the original unless important portions of the original are not visible in printed form. For example, a printed Microsoft Word document does not show all of the data embedded within the original file such as edits and notes.

3.2.5 Hearsay

Digital evidence might not be admitted if it contains hearsay because the speaker or author of the evidence is not present in court to verify its truthfulness.

> Evidence is hearsay where a statement in court repeats a statement made out of court in order to prove the truth of the content of the out of court statement. Similarly, evidence contained in a document is hearsay

> if the document is produced to prove that statements made in court are true. The evidence is excluded because the crucial aspect of the evidence, the truth of the out of court statement (oral or documentary), cannot be tested by cross-examination.
>
> **(Hoey, 1996)**

For instance, an e-mail message may be used to prove that an individual made certain statements, but cannot be used to prove the truth of the statements it contains. Therefore, although Larry Froistad sent a message to an e-mail list indicating that he killed his daughter, investigators needed a confession and other evidence to prove this fact (see Chapter 10 for case details). The Canadian case against Pecciarich provides an interesting example of what may be considered hearsay in the context of online activities.

CASE EXAMPLE (REGINA V. PECCIARICH, 1995)

Pecciarich was initially charged with one count of distributing obscene pictures and one count of distributing child pornography by using his personal computer to upload files to a computer bulletin board where others could download the files. The bulletin board was examined remotely, only allowing investigators to testify that they had seen many files on the bulletin board that contained the suspect's code name "Recent Zephyr" and had downloaded a few of them.

Mr. Blumberg testified that the graphic or pictorial files Moppet 1.GIF through Moppet 4.GIF were downloaded by him on September 20, 1993, all exhibiting on screen a printed statement that they were uploaded by Recent Zephyr on dates in August and September 1993. A sample description of MOPPET 01 was "A Gateway original GIF! Two with girls fully nude and a younger one without panties, and just pulling off the top!" He testified that all remaining files specified in count 2 of the information were seen on either the Gateway or another bulletin board such as "Scruples," and all were identified as having been uploaded by Recent Zephyr on August 3, 1993. Only certain ones were downloaded and stored, due to time and space limitations. … Other files purportedly uploaded by Recent Zephyr were seen on many bulletin boards, and sometimes identified as associated with the company names "Yes Software" and "UCP Software."

On appeal, the judge overturned the distribution charges stating that, "the statements from the bulletin 'uploaded by Recent Zephyr' accompanied by a date in August or September 1993, are pure hearsay and therefore not evidence of uploading or of the date specified." This decision appears to have been influenced by the description of the bulletin board, leading the court to believe that the data could not be relied upon. In cross-examination, Blumberg acknowledged that even if a subscriber to the bulletin board uploaded the images, the systems operator could alter any data on the system, including removing clothing, "drawing in" body parts including genitalia, and inserting the words "uploaded by Recent Zephyr." Blumberg even acknowledged that an imposter could upload materials onto the bulletin board in the name of another subscriber, using his telephone number without his knowledge; however, in testimony, which was less than crystal clear, Blumberg explained that a system of callback verification may or may not pick up on the false identity of the uploader.

The court upheld the charge of possession despite the defense argument that the evidence used to attribute the documents to Pecciarich was also hearsay.

> Defense counsel argues that proof of authorship is not possible unless the documents are used in violation of the hearsay rule—namely to prove the truth of their message that the creator is "Recent Zephyr." However, rather than for truth, I have used the documents as pieces of original circumstantial evidence that the accused and the name "Recent Zephyr" are so frequently linked in a meaningful way as to create the logical inference that they are the same person.

Proving that someone distributed materials online is challenging and generally requires multiple data points that enable the court to connect the dots back to the defendant beyond a reasonable doubt. In Regina v. Pecciarich, although there was only a theoretical possibility of evidence tampering, the judge had little confidence in the digital evidence and believed that the date-time stamps on the bulletin board were hearsay even though the computer probably generated them (technically, hearsay only applies to human statements). The judge might have been skeptical of these date-time stamps because they were observed remotely through the bulletin board interface rather than collected directly from the system's hard drive. More corroborating evidence such as creation and modification times of the relevant files on the bulletin board system's hard drive and telephone records showing when the suspect had accessed the bulletin board may have helped prove distribution to the satisfaction of the court. A list of bulletin board user names with associated addresses and telephone numbers was presented to show that the defendant's telephone number was associated with the Recent Zephyr user name. However, the court determined that it could not be used "to show that the accused and Recent Zephyr have the same telephone number and city of residence. Such use would clearly be for the truth of the contents, and thus would violate the hearsay rule." Furthermore, lists of users cannot demonstrate that the defendant had connected to the bulletin board at the times the images in question were uploaded.

3.2.6 Hearsay Exceptions: Business Records

There are several exceptions to the hearsay rule to accommodate evidence that portrays events quite accurately and that is easier to verify than other forms of hearsay. For instance, the U.S. Federal Rules of Evidence specify that records of regularly conducted activity are not excluded by the hearsay rule:

> A memorandum, report, record, or data compilation, in any form, or acts, events, conditions, opinions or diagnoses, made at or near the time by, or from information transmitted by a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the

> regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testimony of the custodian or other qualified witness, unless the source of the information or the method or circumstances of preparation indicate lack of trustworthiness. The term "business" as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

The Irish Criminal Evidence Act, 1992, has a similar exception in Section 5(1):

> … information contained in a document shall be admissible in any criminal proceedings as evidence of any fact therein of which direct oral evidence would be admissible if the information
>
> **a.** Was compiled in the ordinary course of a business.
> **b.** Was supplied by a person (whether or not he so compiled it and is identifiable) who had, or may reasonably be supposed to have had, personal knowledge of the matters dealt with.
> **c.** In the case of information in nonlegible form that has been reproduced in permanent legible form, as reproduced in the course of the normal operation of the reproduction system concerned.

Although some courts evaluate all computer-generated data as business records under the hearsay rule, this approach may be inappropriate when a person was not involved. In fact, computer-generated data may not be considered hearsay at all because they do not contain human statements or they do not assert a fact but simply document an act. The USDOJ manual (USDOJ, 2002) clearly described the difference between digital evidence that is computer generated versus that which is computer stored:

> The difference hinges upon whether a person or a machine created the records' contents. Computer-stored records refer to documents that contain the writings of some person or persons and happen to be in electronic form. E-mail messages, word processing files, and Internet chat room messages provide common examples. As with any other testimony or documentary evidence containing human statements, computer-stored records must comply with the hearsay rule. … In contrast, computer-generated records contain the output of computer programs, untouched by human hands. Log-in records from Internet service providers, telephone records, and ATM receipts tend to be computer-generated records. Unlike computer-stored records, computer-generated records do not contain human "statements," but only the output of a computer program designed to process input following a defined algorithm. … The evidentiary issue is no longer whether a human's out-of-court statement was truthful and accurate (a question

> of hearsay), but instead whether the computer program that generated the record was functioning properly (a question of authenticity).

For example, in the English case of R. v. Governor of Brixton Prison, *ex parte* Levin (1997) (3 All E.R. 289) the House of Lords considered whether computer printouts were inadmissible because they were hearsay. In this case, Levin was charged for unauthorized access to the computerized fund transfer service of Citibank in New Jersey, USA, and making fraudulent transfers of funds from the bank to accounts that he or his associates controlled.

Lord Hoffman concluded that the printouts were not hearsay:

> The hearsay rule, as formulated in Cross and Tapper on Evidence (8th Ed., 1995), p. 46, states that "an assertion other than one made by a person while giving oral evidence in the proceedings is inadmissible as evidence of any fact asserted." The print-outs are tendered to prove the transfers of funds which they record. They do not assert that such transfers took place. They record the transfers themselves, created by the interaction between whoever purported to request the transfers and the computer programme in [New Jersey]. The evidential status of the print-outs is no different from that of a photocopy of a forged cheque (p. 239).

However, data that depend on humans for their accuracy, such as entries in a database that are derived from information provided by an individual, are covered under the business record exception if they meet the above description.

More courts are likely to acknowledge the distinction between computer-generated and computer-stored records as they become familiar with digital evidence and as more refined methods for evaluating the reliability of computer-generated data become available.

3.3 LEVELS OF CERTAINTY IN DIGITAL FORENSICS

Analysis of digital evidence requires interpretation that forms the basis of any conclusions reached. Digital investigators should be able to estimate and describe the level of certainty underlying their conclusions to help fact-finders determine what weight to attach. However, the field of digital forensics does not currently have formal mathematics or statistics to evaluate levels of certainty associated with digital evidence. There is currently a lack of consistency in the way that the reliability or accuracy of digital evidence is assessed, partly because of the complexity and multiplicity of computer systems. Furthermore, the level of certainty that digital investigators assign to their findings is influenced by their knowledge and experience.

Computers can introduce errors and uncertainty in various ways, including in the time and location of events. The system clock on a computer can be incorrect, and date-time stamps can be interpreted incorrectly. The source IP address of network traffic may be assigned to a proxy device rather than the actual originating computer, and GPS coordinates on a mobile device or satellite navigation system can be inaccurate.

Consider the example of IIS Web server logs showing unauthorized access to a server via a VPN concentrator:

```
2009-04-03 02:38:10 W3SVC1 10.10.10.50 GET /images/snakeoil3.jpg—80—
192.168.1.1 Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1) 200 0 0
```

An inexperienced digital investigator may reach a conclusion, on the basis of this log entry, that the connection to the Web server occurred at 02:38 on the morning of April 4, 2009, from a computer with IP address 192.168.1.1. A more experienced digital investigator will have less confidence that this log entry is accurate and may not be willing to reach a conclusion without further corroborating information. The system clock of the server could be incorrect, resulting in the date-time stamp in the log entry being incorrect. Furthermore, the date-time stamp could be configured with a time zone in either Universal Standard Time (UTC) or local time. Therefore, without additional information, a digital investigator cannot ascertain whether this event occurred on April 03, 2009, at 02:38 UTC or on April 02, 2009, at 22:38 EDT (UTC—0400). Of course, these potential errors can be addressed by documenting the system clock time and the time zone configuration, but origination uncertainty can be more problematic. In the above example, the attacker was connecting through a VPN configured with the private, nonroutable IP address 192.168.1.1,[3] so the IP address of the attacker's computer is not provided in this log and may not be on the same local area network or even in the same geographical region as the server. The level of certainty in the time and source of the attack recorded in the above log entry is a combination of these (and possibly other) uncertainties. However, it is not clear how the individual uncertainties interact or how they can be combined to estimate the overall level of certainty. Given the number of unknowns in the equation, this problem is effectively indeterminate. So, it is necessary to estimate uncertainty in a heuristic manner.

3.3.1 Defining Levels of Certainty

When describing the level of certainty associated with a particular finding, some digital investigators use an informal system of degrees of likelihood that can be used in both the affirmative and negative sense: (1) almost definitely, (2) most probably, (3) probably, (4) very possibly, and (5) possibly. However, a digital

[3] See Chapter 21 for coverage of different kinds of IP addresses and other aspects of networks that are relevant to digital investigators.

investigator may use these terms differently, potentially leading to inconsistency and confusion. Some digital investigators use the term *likely* to express a lower level of certainty than *probably*, whereas others treat these terms as synonyms. Some digital investigators say that the evidence "suggests" that something is in the realm of possibility and that the evidence "indicates" that something is probable. There is clearly a need for a more formal and consistent method of referring to the relative certainty of different types of digital evidence.

PRACTITIONER'S TIP

Many digital investigators use the terminology "is consistent with" inappropriately to mean that an item of digital evidence might have been due to a certain action or event. For many people, to say that something is consistent with something else means that the two things are identical, without any differences. To avoid confusion, digital investigators are encouraged only to state that something is consistent with something else if the two things are the same and to otherwise use the terminology "is compatible with."

The Certainty Scale in Table 3.1 is proposed as a tool to formalize the process by which digital investigators assign a level of certainty to conclusions that are based on digital evidence. Although digital investigators could conceivably assign a C-value to each piece of evidence they have analyzed, that approach

Table 3.1 A Proposed Scale for Categorizing Levels of Certainty in Digital Evidence

Certainty Level	Description/Indicators	Commensurate Qualification
C0	Evidence contradicts known facts	Erroneous/incorrect
C1	Evidence is highly questionable	Highly uncertain
C2	Only one source of evidence is not protected against tampering	Somewhat uncertain
C3	The source(s) of evidence are more difficult to tamper with but there is not enough evidence to support a firm conclusion or there are unexplained inconsistencies in the available evidence	Possible
C4	(a) Evidence is protected against tampering or (b) evidence is not protected against tampering but multiple, independent sources of evidence agree	Probable
C5	Agreement of evidence from multiple, independent sources that are protected against tampering. However, small uncertainties exist (e.g., temporal error and data loss)	Almost certain
C6	The evidence is tamperproof or has a high statistical confidence	Certain

can add confusion rather than clarity. It is more effective to assign a C-value to each conclusion that is based on one or more pieces of digital evidence. Although these C-values are still subjective and do not correspond to a specific percentage of confidence, using a more formal assessment process such as the Certainty Scale compels digital investigators to consider carefully the strengths and weaknesses of available evidence and associated conclusions.

Several examples of how a C-value can be used to clarify the level of certainty associated with a particular conclusion are provided here:

- C6 level of certainty: Files containing known child pornography were found on the defendant's computer, on the basis of hash values of the files matching known child pornography and a visual inspection of the file contents.
- C5 level of certainty: IP address, user account, and automatic number identification (ANI) information are all linked to the defendant and his home. Monitoring Internet traffic indicates that criminal activity is coming from the house. The multiple independent sources of digital evidence indicate that the activity almost certainly originated from the suspect's home.
- C4 level of certainty: Multiple items of evidence on the defendant's computer link him to the identity theft targeting the victim, including e-mail on May 31, 2010, confirming a Visa credit card in the victim's name, USBank online loan application completed in victim's name, and a cash advance on a MasterCard credit card in the victim's name.
- C0 level of certainty: The conclusion that Julie Amero intentionally accessed pornography Web sites while in the classroom is contradicted by evidence that pornographic pop-ups appearing on the computer were the result of an automated "spyware" program on the computer.

When digital investigators have a low level of confidence in available digital evidence, they may not be able to reach a conclusion without additional corroborating information.

One major advantage of this Certainty Scale is that it is flexible enough to assess the evidential weight of both the process that generated a piece of digital evidence and its contents, which may be documents or statements. Another major advantage of this Certainty Scale is that it is nontechnical and therefore easily understood by nontechnical people such as those found in most juries. Although it may be necessary at some stage to ask the court to consider the complexities of the systems involved, it is invaluable to give them a general sense of the level of certainty they are dealing with and to help them decide what evidential weight to give the evidence. Only focusing on the complexities, without providing a nontechnical overview, can lead to confusion and poor decisions.

One disadvantage of the Certainty Scale is that it is subjective—digital investigators must use their judgment when assigning certainty values. As such, different digital investigators may reach a similar conclusion but assign different levels of certainty based on their knowledge and experience.

Ultimately, it is hoped that this Certainty Scale will point to areas that require additional attention in digital evidence research. Debate over C-values in specific cases may reveal that certain types of evidence are less reliable than was initially assumed. For some types of digital evidence, it may be possible to identify the main sources of error or uncertainty and develop analysis techniques for evaluating or reducing these influences. For other types of digital evidence, it may be possible to identify all potential sources of error or uncertainty and develop a more formal model for calculating the level of certainty for this type of evidence.

3.4 DIRECT VERSUS CIRCUMSTANTIAL EVIDENCE

Direct evidence establishes a fact. Circumstantial evidence may suggest one. It is a common misconception that digital evidence cannot be direct evidence because of its separation from the events it represents. However, digital evidence can be used to prove facts. For example, if the reliability of a computer system is at issue, showing the proper functioning of that specific system is direct evidence of its reliability, whereas showing the proper functioning of an identical system is circumstantial.

Although digital evidence is generally only suggestive of human activities, circumstantial evidence may be as weighty as direct evidence and digital evidence can be used to firmly establish facts. For example, a computer log on record is direct evidence that a given account was used to log in to a system at a given time but is circumstantial evidence that the individual who owns the account was responsible. Somebody else might have used the individual's account and other evidence would be required to prove that he/she actually logged in to the system. It may be sufficient to demonstrate that nobody else had access to the individual's computer or password. Alternately, other sources of digital evidence such as building security logs may indicate that the account owner was the only person in the vicinity of the computer at the time of the log on.

Consider intellectual property theft as another example. Even if nobody saw the defendant taking the proprietary data, it may be sufficient to show that the data in his/her possession are the same as the proprietary data and that he/she had the opportunity for access. So, there is nothing inherently wrong with circumstantial evidence. Given enough circumstantial evidence, the court may not require direct evidence to convict an individual of a crime.

3.5 SCIENTIFIC EVIDENCE

In addition to challenging the admissibility of digital evidence directly, tools and techniques used to process digital evidence have been challenged by evaluating them as scientific evidence. Because of the power of science to persuade, courts are careful to assess the validity of a scientific process before accepting its results. If a scientific process is found to be questionable, this may influence the admissibility or weight of the evidence, depending on the situation.

In most U.S. states, novel scientific evidence is evaluated using four criteria developed in Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993). These criteria are as follows:

1. Whether the theory or technique can be (and has been) tested.
2. Whether there is a high known or potential rate of error, and the existence and maintenance of standards controlling the technique's operation.
3. Whether the theory or technique has been subjected to peer review and publication.
4. Whether the theory or technique enjoys "general acceptance" within the relevant scientific community.

Thus far, digital evidence processing tools and techniques have withstood scrutiny when evaluated as scientific evidence. However, the complexity and rate of change of technology leave limited time for testing and evaluating forensic tools and techniques. Bugs have been found in various digital evidence processing tools that can lead to incorrect or incomplete findings. Digital investigators may disagree on the interpretation of digital evidence based on their differing experience with and testing of the computer systems involved.

PRACTITIONER'S TIP

Given the complexity of modern computer systems, it is not unusual for digital investigators to encounter unexpected and undocumented behaviors during a forensic analysis of digital evidence. Such behaviors can cause unwary digital investigators to reach incorrect conclusions that can have a significant impact on a case, sometimes leading to false accusations. Thorough testing with as similar an environment to the original as possible can help avoid such mistakes and resolve differences in interpretation of digital evidence. Provided digital investigators can replicate the actions that led to the digital evidence in question, they can generally agree on what the evidence means. When it is not possible to replicate the exact environment or digital evidence under examination, digital investigators may need to rely on their understanding of the systems involved, which is where differences of opinion can arise.

To reduce the risk of mistakes, misinterpretations, missed evidence, and the resulting miscarriages of justice that may result from such errors, it is desirable to assess the reliability of commonly used tools. Testing techniques or tools and

determining error rates are challenging not just in the digital realm. Although many types of forensic examinations have been evaluated using the criteria set out in Daubert, the testing methods have been weak. "The issue is not whether a particular approach has been tested, but whether the sort of testing that has taken place could pass muster in a court of science" (Thornton, 1997). Also, error rates have not been established for most types of forensic examinations, largely because there are no good mechanisms in place for determining error rates. Fingerprinting, for example, has undergone recent controversy (Specter, 2002). Although the underlying concepts are quite reliable, in practice, there is much room for error. Errors are not simply caused by flaws in underlying theory but also in its application. This problem applies to the digital realm and can be addressed with increased standards and training.

The problems relating to admissibility and understanding of scientific evidence have become sufficiently complicated to require new approaches. In the United Kingdom and Ireland, law reform commissions have published recommendations on how to address challenges relating to admissibility of scientific evidence in general, and digital evidence in specific (Irish Law Reform Commission, 2009; UK Law Commission, 2009).

One approach that has been suggested to reduce the complexity of tool testing is to allow people to see the source code for critical components of the software (Carrier, 2002). Providing programmers around the world with source code allows tool testers to gain a better understanding of the program and increases the chances that bugs will be found. It is acknowledged that commercial tool developers will want to keep some portions of their programs private to protect their competitive advantage. However, certain operations, such as copying data from a hard drive, are sufficiently common and critical to require an open standard. Ultimately, given the complexity of computer systems and the tools used to examine them, it is not possible to eliminate or even quantify the errors, uncertainties, and losses and digital investigators must validate their own results using multiple tools.

When the source code is not available, another form of validation is performed—verifying the results by examining evidence using another tool to ensure that the same results are obtained. Formal testing is being performed by the National Institute of Standards and Technology (NIST) and some organizations and individuals perform informal tests. However, given the rate at which computer technology is changing, it is difficult for testers to keep pace and establish error rates for the various tools and systems. Additionally, tool testing does not account for errors introduced by digital investigators through misapplication or misinterpretation. Therefore, the most effective approach to validating results and establishing error rates is through peer review—that is, to have another digital investigator double-check findings using multiple tools to ensure that the results are reliable and repeatable.

An alternate approach to assessing the scientific validity of tools and techniques used to process digital evidence is to convene a prehearing meeting of the experts (Sommer, 2009). Some jurisdictions and international tribunals require opposing experts to submit a joint report summarizing the findings that everyone agrees on and explaining the areas of disagreement. In addition, opposing experts may be required to present evidence concurrently to decision makers, with questions being posed from attorneys, judges, and opposing experts. This process is sometimes called *hot tubbing* and allows for a degree of debate between experts. This just-in-time approach to peer review of scientific evidence has the potential to address new forensic analysis methods in a timely manner, enabling digital investigators to keep pace with changes in technology and handle novel situations that may arise in a specific case.

3.6 PRESENTING DIGITAL EVIDENCE

Digital investigators are commonly asked to testify or produce a written summary of their findings in the form of an affidavit or expert report. Testifying or writing a report is one of the most important stages of the investigative process because, unless findings are communicated clearly in writing, others are unlikely to understand or make use of them.

3.6.1 Expert Reports

A well-rendered report that clearly outlines the digital investigator's findings can convince the opposition to settle out of court, while a weakly rendered report can fuel the opposition to proceed to trial. Assumptions and lack of foundation in evidence result in a weak report. Therefore, it is important to build solid arguments by providing supporting evidence and demonstrating that the explanation provided is the most reasonable one.

Whenever possible, digital investigators should support assertions in their reports with multiple independent sources of evidence to ensure that any potential weakness in one source of digital evidence does not undermine an otherwise valid conclusion. They should clearly state how and where all evidence was found, to help decision makers to interpret the report and to enable another competent digital investigator to verify results. Including important items of digital evidence as figures or attachments can be useful when testifying in court as it may be necessary to refer to the supporting evidence when explaining findings in the report. Presenting alternative scenarios and demonstrating why they are less reasonable and less compatible with the evidence can help strengthen key conclusions. Explaining why other explanations are unlikely or impossible demonstrates that the scientific method was applied—that an effort was made to disprove the given conclusion but that it withstood critical scrutiny.

PRACTITIONER'S TIP

Careful use of language is needed to present digital evidence and associated conclusions as precisely as possible. Imprecise use of language in an expert report can give decision makers the wrong impression or create confusion. Therefore, digital investigators should carefully consider the level of certainty in their conclusions and should qualify their findings and conclusions appropriately.

If there is no evidence to support an alternative scenario, digital investigators should clearly state whether it is more likely that relevant evidence was missed or simply not present. If digital evidence was altered after it was collected, digital investigators must mention this in their reports, explaining the cause of the alterations and weighing their impact on the case (e.g., negligible or severe).

In short, a formal report of forensic findings should give readers all of the information they need to evaluate the evidence and associated conclusions. The following is a sample report structure:

- *Introduction*: Provide an overview of the case, the relevance of the evidential media being examined, who requested the forensic analysis, and what was requested. In addition, the introduction should provide the bona fides of those who performed the work, including a summary of relevant experience and training. A full CV can be provided as an attachment to the report.
- *Evidence Summary*: Describe the items of digital evidence that were analyzed, providing details that uniquely identify such as make, model, and serial number. Also consider including MD5 values, photographs, laboratory submission numbers, details of when and where the evidence was obtained, from whom the evidence was obtained and its condition (note signs of damage or tampering), and processing methods and tools.

The following sample evidence summary section describes two evidential mobile devices:

The items listed below are not necessarily all evidence submitted in the case, but reflect the media where the reported evidence was found/located.

MD-001-001 (Suspect)
HTC Dash (GSM), model S620
FCC-ID: NM8EXCA
IMEI: 355634020485402
S/N: SZ830FE01566
IMSI: 234545647568
ICCID: 98645634246
MD_001-002 (Suspect)

(*Continued*)

Motorola RAZR (CDMA), model V3m
ESN: 02003591013
Phone number: 540-555-3322
Note: Device screen was damaged and nonfunctional

The mobile devices were labeled with reference numbers (MD_001-001 & MD_001-002). The report will refer to this designation when talking about information found on said storage media. Both devices were acquired in a forensic laboratory environment that prevented the devices from communicating with the network. Forensic acquisitions of MD_001_001 were performed using XRY, Cellebrite, and XACT. Forensic acquisitions of MD_001_002 were performed using BitPim and MobileForensics. Whenever feasible, all findings were verified by performing a manual examination of the evidential devices.

- *Examination Summary*: Provide an overview of the critical findings relating to the investigation. Think of this as the executive summary, with any recommendations or conclusions in short form. This section is intended for decision makers who may not have time to read the full report and just need to know the primary results of the forensic analysis. In certain situations, it is advisable to summarize tools used to perform the examination, how important data were recovered (e.g., decryption and undeletion), and how irrelevant files were eliminated (e.g., using NSRL hash sets). Whenever feasible, use the same language in the examination summary as is used in the body of the report to avoid confusion and to help the attentive reader associate the summary with the relevant section in the detailed description.
- *File System Examination*: When dealing with storage media, provide an inventory of files, directories, and recovered data that are relevant to the investigation with important characteristics such as path names, date-time stamps, MD5 values, and physical sector location on disk. Note any unusual absences of data that may be an indication of data destruction, such as mass deletion, reformatting, or wiping.
- *Forensic Analysis and Findings*: Provide a detailed description of the forensic analysis performed and the resulting findings, along with supporting evidence. Any detailed forensic analysis of particular items that requires an extensive description can be provided in a separate subsection. The report should clearly specify the location where each referenced item was found, enabling others to replicate and verify the results in the future. In addition to describing important findings in the report, it can be more clear and compelling to show a photograph, screenshot, or printout of the evidence. Describe and interpret temporal, functional, and relational analysis and other analyses performed such as evaluation of source and digital stratigraphy.
- *Conclusions*: A summary of conclusions should follow logically from previous sections in the report and should reference supporting evidence.

> It is important not to jump to conclusions or make statements about innocence or guilt. Conclusions must be objective and be based on fact. Let the evidence speak for itself and avoid being judgmental.

If certain exhibits such as diagrams, tables, or printouts are too cumbersome to include in the body of the report, they can be attached as numbered appendices along with a glossary with definitions of technical terms used in the report.

In the United Kingdom, information that must be provided in an expert report is described in the Criminal Procedure Rules and includes the following:

- The expert's qualifications, relevant experience, and accreditation.
- The substance of all facts given to the expert which are material to the opinions expressed in the report or upon which those opinions are based.
- A summary of conclusions.

In addition, the UK Criminal Procedure Rule indicates that, where there is a range of opinion on the matters dealt with in the report, the range of opinion should be explained and the basis for the expert's own opinion should be provided with any necessary caveats (UK Ministry of Justice, 2010).

In addition to presenting the facts in a case, digital investigators are generally expected to interpret the digital evidence in the final report. Interpretation involves opinion and every opinion rendered by an investigator has a statistical basis. Therefore, in a written report, the investigator should clearly indicate the level of certainty he/she has in each conclusion and piece of evidence to help the court assess what weight to give them. Digital investigators commonly express degrees of likelihood using a range of terms such as (1) almost definitely, (2) most probably, (3) probably, (4) very possibly, and (5) possibly. Use of these terms in a forensic report can have a significant bearing on a case, particularly when a judge or jury has to decide whether the defendant is guilty beyond a reasonable doubt in a criminal case, or that the preponderance of evidence indicates guilt in a civil matter.

In addition to preparing a final, full-blown, technical report, digital investigators may be required to write reports for less technical decision makers. For instance, managers in an organization may need to know what transpired to help them determine the best course of action. The public relations department may need details to relay to shareholders. Attorneys may need a summary report to help them focus on key aspects of the case and develop search or arrest warrants or interview and trial strategy. A measure of hard work and creativity is required to create clear, nontechnical representations of important aspects in a case such as timelines, relational reconstructions, and functional analyses. However, the effort required to generate such representations is necessary to give attorneys, juries, and other decision makers the best chance of understanding important details and making informed decisions.

3.6.2 Testimony

Proper preparation for trial makes all the difference. For digital investigators, preparing for trial can involve meeting with attorneys in the case to review the forensic findings, address any questions or concerns, and discuss how the information will be presented in court. Scripting direct examination or rehearsing it may not be permitted in some contexts, but some discussion with the attorney ahead of time is generally permissible and provides an opportunity to identify areas that need further explanation and to anticipate questions that the opposition might raise during cross-examination. Keep in mind that attorneys are generally extremely busy getting many other aspects of a case ready for trial and may not have much time or attention to devote to the digital dimension. Do not assume that the attorneys can understand or recall the most important aspects of the digital forensic findings. In the days prior to the trial, and even during the trial, digital investigators must be prepared to give the attorneys what they need as quickly and concisely as possible.

When digital investigators first take the stand, they must first be accepted as an expert by the court. During this process, called *voir dire*, digital investigators will generally be asked to provide a summary of their qualifications and experience and, in some cases, will be asked questions about their training, credentials, etc. After this process, the court will decide whether to accept the digital investigator as an expert who can testify in the case.

When on the stand, the most important thing is to convey the facts as clearly as you can to all in attendance. Do not rush. Attempting to hurry through testimony could make a bad impression or worse, cause digital investigators to make a mistake. Digital investigators should take time to consider the question and answer it correctly the first time. Speak clearly and loud enough for at least the jury to hear, if not the entire courtroom.

During cross-examination, attorneys often attempt to point out flaws and details that were overlooked by the digital investigator. The most effective response to this type of questioning is to be prepared with clear explanations and supporting evidence. In some cases, the goal of the opposing counsel may be to raise doubts about digital forensic findings. Therefore, digital investigators should not expect the questions to be straightforward or even comprehensible. What seems like a nontech-savvy lawyer trying to muddle through technical findings may be a very savvy trial lawyer. Besides trying to create confusion in relation to the findings, asking a vague question may be a tactic to get the digital investigator to answer questions that the attorney had not thought of himself/herself. As a rule, never guess what an attorney is trying to ask. If a question seems unclear, ask the attorney to repeat it or rephrase it to clarify what is being asked. It is also advisable to pause before answering questions to give your attorney time to express objections. When objections are raised,

carefully consider why the attorney is objecting before answering the question. If prompted to answer a complex question with simply "Yes" or "No," inform the court that you do not feel that you can adequately address the question with such a simplistic answer but follow the direction of the court. Above all, be honest.

If a digital investigator does not know the answer to a question, it is okay to say "I don't know." Digital investigators can stick to solid evidence and avoid less certain speculation. Before agreeing to a statement in cross-examination, consider it carefully. The opposing counsel may not be stating a fact when asking a question like "Isn't it true that my client was not in possession of the mobile device at the time of the crime?" Knowing the facts of the case and being able to deliver them in response to a misleading question may discourage further attempts to catch the testifying digital investigator off guard.

In addition to presenting findings, digital investigators may be required to explain how the evidence was handled and analyzed to demonstrate chain of custody and thoroughness of methods. Digital investigators may also be asked to explain underlying technical aspects in a relatively nontechnical way, such as how files are deleted and recovered and how tools acquire and preserve digital evidence. Simple diagrams depicting these processes are strongly recommended.

It can be difficult to present digital evidence in even the simplest of cases. In direct examination, the attorney usually needs to refer to digital evidence and display it for the trier of fact (e.g., judge or jury). This presentation can become confusing and counterproductive, particularly if materials are voluminous and not well arranged. For instance, referring to printed pages in a binder is difficult for each person in a jury to follow, particularly when it is necessary to flip forward and backward to find exhibits and compare items. Such disorder can be reduced by arranging exhibits in a way that facilitates understanding and by projecting data onto a screen to make it visible to everyone in the court.

Displaying digital evidence with the tools used to examine and analyze it can help clarify details and provide context, taking some of the weight of explaining off the digital investigator. Some digital investigators place links to exhibits in their final reports, enabling them to display the reports onscreen during testimony and efficiently display relevant evidence when required. However, it is important to become familiar with the computer that will be used during the presentation to ensure a smooth testimony. Visual representations of timelines, locations of computers, and other fundamental features of a case also help provide context and clarity. Also, when presenting technical aspects of digital evidence such as how files are recovered or how log-on records are generated, first give a simplified, generalized example and then demonstrate how this applies to the evidence in the case.

The risk of confusion increases when multiple computers are involved and it is not completely clear where each piece of evidence originated. Therefore, make every effort to maintain the context of each exhibit, noting which computer or floppy disk it came from and the associated evidence number. Also, when presenting reconstructions of events on the basis of large amounts of data such as server logs or telephone records, provide simplified visual depictions of the main entities and events rather than just presenting the complex data. It should not be necessary to fumble through pages of notes to determine the associated computer or evidence number. Also, refer to exhibit numbers during testimony rather than saying, "this e-mail" or "that print screen."

Digital investigators may need to refer back to their work on a case years later and are often required to provide all notes related to their work and possibly different versions of an edited/corrected report. In the United Kingdom, there is a process called *disclosure* that aims to make the discovery process more streamlined and transparent, requiring the prosecution to provide all relevant material to the defense.[4] To facilitate such review or *disclosure*, it is helpful to organize any screenshots or printouts (initialed, dated, and numbered) of important items found during examination. For instance, create a neatly written index of all screenshots and printouts.

3.7 SUMMARY

The foundation of any case involving digital evidence is proper evidence handling. Therefore, the practice of seizing, storing, and accessing evidence must be routine to the point of perfection. Standard operating procedures with forms are a key component of consistent evidence handling, acting as both memory aids for digital investigators and documentation of chain of custody. Also, training and policies should provide digital investigators with a clear understanding of acceptable evidence handling practices and associated laws.

Verifying that evidence was handled properly is only the first stage of assessing its reliability. Courts may also consider whether digital evidence was altered before, during, or after collection, and whether the process that generated the evidence is reliable. Claims of tampering generally require some substantiation before they are seriously considered. Someone familiar with the system in question, who can testify that the computer was operating normally at the time, can generally address questions regarding the process that generated a given piece of digital evidence. Digital investigators are encouraged to consider

[4] More details regarding disclosure are available from the United Kingdom Crown Prosecution Service: [redacted]. The part of particular interest to experts is Appendix K: [redacted].

the degree of certainty in each conclusion that is based on digital evidence. A tool to help formalize the process by which digital investigators assign a level of certainty to conclusions that are based on digital evidence is provided in Table 3.1. If there are significant doubts about the reliability of relevant computer systems and processes, the court may decide to give the associated digital evidence less weight in the final decision.

On the stand, digital investigators may be asked to testify to the reliability of the original evidence and the collection and analysis systems and processes, and to assert that they personally established the chain of custody and forensically preserved the data. An unexplained break in the chain of custody could be used to exclude evidence. An understanding of direct versus circumstantial evidence, hearsay, and scientific evidence is necessary to develop solid conclusions and to defend those conclusions and the associated evidence on the stand. A failure to understand these concepts can weaken a digital investigator's conclusions and testimony. For instance, interpreting circumstantial evidence as though it were direct evidence, or basing conclusions on hearsay, could undermine a digital investigator's findings and credibility.

Ultimately, digital investigators must present their findings in court to a nontechnical audience. As with any presentation, the key to success is preparation, preparation, and more preparation. Be familiar with all aspects of the case, anticipate questions, rehearse answers, and prepare visual presentations to address important issues. Although this requires a significant amount of effort, keep in mind that someone's liberty might be at stake.

REFERENCES

Carrier, B. (2002). Open Source Digital Forensics Tools: The Legal Argument. Available from [redacted].

Casey, E. (2002). Error, uncertainty and loss in digital evidence. *International Journal of Digital Evidence, 1*(2). Available from [redacted].

Castell, S. (1990). Evidence and authorisation: Is EDI (electronic data interchange) legally reliable? *Computer Law and security report 2*, *6*(5).

Gross, H. (1924). *Criminal Investigation*. London: Sweet & Maxwell.

Guidance Software (2001–2002). EnCase legal journal (2nd ed.). Available from [redacted].

Hoey, A. (1996). *Analysis of the police and criminal evidence act, s.69—computer generated evidence*. Web Journal of Current Legal Issues, in association with Blackstone Press Ltd.

Irish Law Reform Commission. (2009). *Documentary and electronic evidence (LRC CP 57-2009)*.

Law Commission. (1997). Evidence in criminal proceedings: hearsay and related topics. Law Commission Report 245. Available from [redacted].

Mattel, M., Blawie, J. F., & Russell, A. (2000). *Connecticut law enforcement guidelines for computer systems and data search and seizure*. State of Connecticut Department of Public Safety and Division of Criminal Justice.

National Center for Forensic Science. (2003). *Digital evidence in the courtroom: a guide for preparing digital evidence for courtroom presentation*. Washington, DC: Mater Draft Document, U.S. Department of Justice, National Institute of Justice. Available from [redacted].

Specter, M. (2002). Do fingerprints lie?: The gold standard of forensic evidence is now being challenged. *The New Yorker*, May 27, 2002. Available from [redacted]

Strong, J. W. (1992). McCormick on Evidence. 4th edition, West Group.

Thornton, J. I. (1997). The general assumptions and rationale of forensic identification. In D. L. Faigman, D. H. Kaye, M. J. Saks, & J. Sanders (Eds.), *Modern scientific evidence: the law and science of expert testimony* (Vol. 2). St. Paul, MN: West Publishing Company.

UK Law Commission. (2009). The admissibility of expert evidence in criminal proceedings in England and Wales: a new approach to the determination of evidentiary reliability. Consultation Paper No. 190.

United States Department of Justice. (2002). Searching and seizing computers and obtaining electronic evidence in criminal investigations. Available from [redacted].

Cases

Bean, M. (2003). Mich. v. Miller: sex, lies and murder. Court TV. Available from [redacted].

Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993). 509 U.S. 579, 113 S.Ct. 2786, 125 LEd.2d 469.

Korn, H. (1966). Law, fact, and science in the courts. 66 *Columbia Law Review* 1080, 1093–1094.

Lorraine v. Markel Am. Ins. Co. (2007). WL 1300739 (D. Md., May 4, 2007). Available from [redacted].

Michigan v. Miller. (2001). 7th Circuit Court, Michigan.

People v. Lugashi. (1988). Appeals court, California (205 Cal. App.3d 632). Case Number B025012.

R. v. Governor of Brixton Prison, *ex parte* Levin. (1997). 3 All E. R. 289.

Regina v. Pecciarich. (1995). 22 O.R. (3d) 748, Ontario Court, Canada. Available from [redacted].

UK Ministry of Justice. (2010). *Criminal procedure rules, part 33—expert evidence*. Available from [redacted].

United States v. Bunty. (2008). WL 2371211 E.D. Pa. June 10, 2008.

United States v. Carey. (1998). Appeals Court, 10th Circuit. Case Number 98-3077. Available from [redacted].

United States v. Gray. (1999). District Court, Eastern District of Virginia, Alexandria division. Case Number 99-326-A.

United States v. Tank. (1998). Appeals Court, 9th Circuit. Case Number 98-10001. Available from [redacted].

United States v. Turner. (1999). Appeals Court, 1st Circuit. Case Number 98-1258. Available from [redacted].

Wisconsin v. Schroeder. (1999). Appeals Court, Wisconsin. Case Number 99-1292-CR. Available from [redacted].