Legal Aspects of Digital Forensics

Daniel J. Ryan
The George Washington University
Washington, D. C.
danjryan@gwu.edu

Gal Shpantzer
The George Washington University
Washington, D. C.
gal@pikpuk.com

ABSTRACT

Of the disciplines that comprise Information Assurance, digital forensics is perhaps the one most closely defined by legal requirements, and one whose growth and evolution is informed and guided by case law, regulatory changes, and the ability of cyberlawyers and digital forensics experts to take the products of forensic tools and processes to court. The tension between privacy rights and law enforcement's need to search and seize digital evidence sometimes mirrors, and frequently extends, the extant tensions inherent in rules of evidence. This legal foundation makes forensics tools and techniques for recovery, handling, analysis and preservation of digital evidence unique among the technical arcana of IA, as opposed to firewalls, anti-virus, routing, or intrusion detection, among others, where progress is made with much less scrutiny and guidance from legal scholars.

This paper seeks to explore some of the legal aspects of forensics as an art within IA. We start with a real-world case of an institution that suffered from a lack of forensic capability, moving on to a discussion of some of the most important court cases that guided the development of the field in the last two decades. Then we look ahead to some of the challenges looming for practitioners of digital forensics.

Categories and Subject Descriptors

K.5 Legal Aspects of Computing
K.5.2 Governmental Issues [Regulation]

Keywords

Digital evidence, computer forensics.

1. INTRODUCTION

Imagine that hackers have targeted your organization. In a series of attacks, your network is penetrated and the intruders install an illicit program that sends out derogatory messages about senior executives and managers in your organization to various committees with responsibility for overseeing the management of your organization, using the names of random members of your organization as the senders of the messages. Imagine that other attacks result in the destruction of valuable intellectual capital and digital assets resident on your systems and networks. A great deal of unfavorable publicity and embarrassment results.

But you have implemented a new intrusion detection system, and your sysop uses its audit logs to trace the intrusions back to a former member of your organization, aided and abetted by a current member. Law enforcement is notified and the two are arrested and charged with feloniously altering computer data, with willfully using your computer network without authority, with causing a computer to malfunction, and with other related crimes. Greatly relieved, the public relations department is directed to prepare and distribute a press release stating that the hackers have been caught and arrested, naming the culprits and quoting several of your executives regarding their nefarious activities.

Then lawyers for the alleged hackers mount their own attack – on the evidence your sysop gathered. They assert that your intrusion detection system is unproven technology, and that the evidence was not gathered, stored, or analyzed properly. At a preliminary hearing the judge rules that the evidence is insufficient to refer the case to a grand jury, and the charges are dropped. Within days, a multi-million dollar lawsuit is filed alleging defamation of character and false imprisonment. Attorneys for the "hackers" claim the two men suffered great embarrassment and damage to

their reputations, and that they lost jobs and money as a result of the charges filed against them -- charges that were later dropped. The suit claims your organization violated their civil rights, and that their prosecution was instigated out of malice without any legal or factual basis.

Is such a scenario realistic? This scenario is similar to what happened to George Mason University in a recent case. [1] The message? Lack of due care and attention to the legal rules surrounding the collection and uses of digital evidence can not only make the evidence worthless, it can leave investigators vulnerable to liability in countersuits.

2. THRESHOLD CONSIDERATIONS

As every Perry Mason fan knows, evidence, to be admissible in court, must be relevant, material and competent, and its probative value must outweigh any prejudicial effect. Digital evidence is not unique with regard to relevancy and materiality, but because it can be easily duplicated and modified, often without leaving any traces, digital evidence can present special problems related to competency. Moreover, to even reach the point where specific competency questions are answered, digital evidence must survive the threshold test posed by *Daubert* [2] of its competency as a class of evidence.

From 1923 until 1993, the admissibility of expert scientific evidence was controlled by a heuristic known as the Frye test after a District of Columbia Court of Appeals case [3] in which the test was first articulated. The Frye test held the expert scientific evidence was admissible only if the scientific community generally accepted the scientific principles upon which it was based. In Daubert, the Court held that Rule 702 of the Federal Rules of Evidence, adopted in 1973, supplanted Frye. Rule 702 provides: "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise." This implies that the scientific evidence proposed possesses the scientific validity to be considered competent as evidence if it is grounded in the methods and procedures of science.

There is no specific test that can be used to determine whether digital evidence possesses the requisite scientific validity. The Court in Daubert suggested several factors to be considered:

- whether the theories and techniques employed by the scientific expert have been tested;
- whether they have been subjected to peer review and publication;
- whether the techniques employed by the expert have a known error rate;
- whether they are subject to standards governing their application; and
- whether the theories and techniques employed by the expert enjoy widespread acceptance.[4]

These factors are not exhaustive and do not constitute "a definitive checklist or test."[5] Testimony may be admissible even where one or more of the factors are unsatisfied. The Court further clarified that the admissibility inquiry must focus "solely" on the expert's "principles and methodology," and "not on the conclusions that they generate."[6]

So, digital forensic evidence proposed for admission in court must satisfy two conditions: it must be (1) relevant [7], arguably a very weak requirement, and (2) it must be "derived by the scientific method" and "supported by appropriate validation."[8]

Digital forensics is, of course, highly technical, and therefore grounded in science: computer science, mathematics, physics, and so forth. It is also a discipline that requires knowledge of engineering, particularly electrical, mechanical and systems engineering. And applying the science and engineering in specific investigations is a complex process that requires professional judgment that is sometimes more art than science.

The question of applicability of *Daubert*-criteria and decisional processes to non-scientific expert evidence was addressed by the Supreme Court in *Kumho Tire Co. v. Carmichael*. [9] *Kuhmo Tire* extended the *Daubert* approach to assessing the reliability of expert testimony to all expert testimony, regardless of whether the proposed testimony was based on scientific principles, engineering principles, or "other specialized" knowledge. This avoided the very real problem of ambiguous decisions regarding whether proposed testimony was rejected because it was scientific but did not satisfy *Daubert* criteria, or because it was non-scientific and therefore not subject to *Daubert* analysis and yet was defective in some other way. In practice, the result is that every expert, including computer forensics experts, are now subject to challenge for reliability. Trial courts and counsel are required to seek indicia of reliability that is reasonably pertinent to the expert's field of expertise. Testing and verification of theories and techniques of digital forensics, peer review, existence of known error rates,

articulation of standards for digital forensics investigations, and differences of opinion among digital forensics experts regarding applicability and acceptance of tools and techniques are all areas that will be probed in such threshold determinations of admissibility. To the extent that digital forensics is more art than science, and less based on standards, it may have trouble surviving such a challenge.

3. ADMISSIBILITY OF DIGITAL EVIDENCE

If digital evidence survives the *Daubert* challenge, it may still have to surmount several competency hurdles concerning the collection, storage, processing and presentation of the evidence. Computers today come with or can be augmented to provide huge amounts of data storage. Gigabyte disk drives are common and a single computer may contain several such drives. Seizing and freezing can no longer be accomplished simply by burning a single CD-ROM. Failure to freeze the evidence prior to opening the files, coupled with the fact that merely opening the files changes them, can and has invalidated critical evidence. Then comes the problem of locating the relevant evidence within massive amounts of data. Wading through such volumes of information to find relevant evidence is a daunting task.

As daunting as these problems are, additional problems arise when we have to look beyond a single computer. In modern distributed computer architectures, the digital evidence we need may reside on many different servers and clients within the organization's IT infrastructure. The problems get even more difficult when the IT infrastructure is connected to the Internet, for then digital evidence may be spread across vast geographic distances and several sovereign jurisdictions.

Digital evidence requires a proper foundation for introduction, of course, but the courts do not require that digital evidence meet more stringent foundations than that required for other types of evidence. [10] Generally, introduction of digital evidence (or rather of computer printouts of digital evidence, since in digital form it would be useless to the trier of fact) is allowed "providing that the party offering the computer information lays a foundation sufficient to warrant a finding that such information is trustworthy and the opposing party is given the same opportunity to inquire into the accuracy of the computer and its input procedures as he has to inquire into the accuracy of written business records." [11] Arguments that digital evidence is inherently untrustworthy because it can easily and undetectably be modified have not been readily accepted in court. [12]

As with any evidence, testimony clearly establishing that the evidence has been under the control of responsible law enforcement personnel and trained investigators is required to assure the trier of fact that the evidence is complete and has not been changed. Attempts to introduce incomplete printouts of web pages have failed. [13]

Since digital evidence usually takes the form of a writing, or at least a form which can be analogized to a writing, it must be authenticated and satisfy the requirements of the Best Evidence Rule. [14] The Best Evidence Rule applies to information stored in computers. As a practical matter, of course, a disk or tape is not directly usable by the trier of fact. Rule 1001(3), therefore, provides that, "if data are stored in a computer or similar device, any printout readable by sight, shown to reflect the data accurately, is an 'original'." Rule 1003 also provides that a duplicate is admissible unless there is a genuine question as to the accuracy of the duplicate or if, for some reason, it would not be fair to admit the duplicate in lieu of the original. Proper handling and correct seizing and freezing by a computer forensics expert should eliminate any questions with regard to accuracy. The proponent of the evidence need not present testimony by a programmer, but should present some witness who can describe how information is processed through the computer and used by the organization.

With regard to hearsay, most courts have dealt with the objection to the introduction of computer records by relying on the business records exception. [15] Such an approach may work for audit logs, provided they satisfy the rule, which might not be the case for computer records collected as part of an investigation rather than as the result of a routine, periodic process. However, in *U. S. Hutson*, the court found to be admissible records that had been created specifically in support of litigation because the underlying data was entered into the computer pursuant to legitimate business purposes and in a timely manner. [16] Again, proper handling and processing by a computer forensics expert should eliminate problems that could affect admissibility. The International High-Tech Crime Conference in 1999 adopted the following guidelines to preserve admissibility of digital evidence:

- "Upon seizing digital evidence, action should not change that evidence.
- "When it is necessary for a person to access original digital evidence, that person must be forensically competent.

- "All activity relating to the seizure, access, storage or transfer of digital evidence must be fully documented, preserved and available for review.
- "An individual is responsible for all actions taken with respect to digital evidence while the digital evidence is in their possession. [sic]
- "Any agency that is responsible for seizing, accessing, storing or transferring digital evidence is responsible for compliance with these principles."[17]

4. DIGITAL WIRETAPS

Interception of message traffic as a means of espionage and law enforcement is an excellent way to gather information, but one that is very invasive of privacy. Consequently, wiretapping as a means of gathering evidence has presented special concerns and special problems for the legal system. [18] Collection of electronic evidence by telephone wiretap has been carefully controlled by the legal system through statutes such as the Wiretap Act, the Pen/Trap statute, and the Electronic Communications Privacy Act (ECPA), and numerous court cases. [19] As computerized telecommunications systems have increasingly borne the communications of governments, businesses and individuals, law enforcement and private litigants alike have turned to seeking digital evidence on-line, sometimes with interceptions that are analogous to telephone wiretaps. So it has become important to know what a "digital wiretap" is.

Computers communicate with a type of switching system that is entirely different from the type of system used in ordinary telephony. The Plain-Old-Telephone-System (POTS) uses circuit switching, setting up a virtual circuit that remains in existence for the duration of a call. Intercept means tapping into that virtual circuit and listening or recording the contents of the communication taking place on the circuit.

Computers communicate using a *packet switching system*. Thus, information that is to be transmitted from sender to recipient passes through many phases. First it is created by the sender. Then the information to be communicated is broken down into small packets that contain some portion of the contents of the communication as well as sender's and recipient's IP addresses and some accounting information. The packets are individually transmitted from the sender's computer to a nearby packet switch and then from switch to switch, at each being stored momentarily and then forwarded to the next available switch in the direction of their ultimate destination. Different packets may take different routes through the network as they travel from sender to recipient, depending on link availability and loading in the network. Upon receipt, the packets are reassembled into an exact replica of the original file. Thus, information passes through several stages of disassembly, storing and forwarding, and reassembly, before becoming available to the recipient. In addition to the store and forward mechanisms inherent in the packet switching system, at the applications level there may be additional storage intervals while a file is being composed and after receipt but before being opened by the recipient. Finally, the recipient may store the file for future reference for some period of time before deleting it. What, then, constitutes an *intercept* in this packetized world?

While the message is being drafted, it can be captured by keystroke capture software, as was the case when the F. B. I. surreptitiously placed such software on the computer of Nicodemo S. Scarfo to search for evidence of an illegal gambling and loan sharking operation. The software was designed to record keystrokes only when the computer was not using its modem to communicate with other computers. The court held that such capture was not a violation of the Wiretap Act. [20] Thus, capture during the creation phase is arguably not an intercept.

At the recipient's end, the U.S. District Court of New Hampshire in *Basil W. Thompson v. Anne M. Thompson, et al.,* ruled that accessing e-mail stored on a hard drive was not an "interception" under the Wiretap Act. [21] This outcome is consistent with previous case law, which has held that in order to qualify as an "interception," e-mail must be accessed "during transmission" [22] The court held that the acquisition of stored e-mail that are no longer in the process of being transferred is governed by the Electronic Communication Privacy Act's stored communications provisions.

Thus, both case law and statutory law seem to contemplate that interception implies that the data is in motion rather than at rest. But, of course, the very nature of a packet switching system stores the data for a while in each switch. Is that storage period subject to different rules than the motion period while the data travels to the next switch? A literal reading of the ECPA might suggest so. Section 2510 provides that " 'electronic storage' means - (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." Section 2701 sanctions anyone who intentionally exceeds an authorization to access ... and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage."

Nevertheless, *intercept* is broadly defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device," [23] leaving open the possibility that the courts could consider that data can be intercepted at any time between the senders execution of a send command and the recipient's opening of the communication. In dicta, the court in *Basil W. Thompson v. Anne M. Thompson, et al.,* even suggested that an ISP would be considered a "communications system" for the purposes of ECPA's definitions, much less a packet switch. [23]

An additional complication is introduced by the different treatment accorded recent data from that stored for longer periods. Access to recent communications (stored for less than one hundred and eighty days) requires a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant, while older communications can be accessed without notice to the subscriber or customer if a warrant is obtained as for recent communications, or with an administrative or grand jury subpoena if there is prior notice. Also with prior notice, a court order can be obtained for access based merely on "articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." [24]

So, for purposes of collection of digital evidence, we have to deal with at least four categories: interceptable or not interceptable and recent or older. Which category applies determines warrant requirements and other legal constraints on our ability to collect the data.

Of course there may be technical impediments to collection as well. Cryptography provides a powerful shield, making data unintelligible and therefore unusable. Of course, it must be correctly used, and the keys must be kept secure, or the cryptography can be undone, as happened when investigators analyzing data seized from the Aum Shinri Kyo cult that poisoned the Tokyo subway with nerve gas found the keys to the cults encrypted files on a floppy disk. [25] In the *Scarfo* case, the encryption was broken by surreptions collection of the key by a keystroke recorder. [26] To date only a handful of cases have been stopped dead in the water by encryption, but it remains a significant threat to forensic analysis.

Finally, there must be electronic access to the data sought for forensic analysis. To ensure access, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA), sometimes called the "Digital Telephony" bill. [27] CALEA was intended to "ensure that their systems are technically capable of enabling law enforcement agencies operating with proper legal authority to intercept individual telephone calls and to obtain certain 'call-identifying information.'" [28] Congress paid the hefty bill for the redesign of the POTS required by CALEA by reprogramming money from the intelligence community budget.

5. EMERGING PROBLEMS

As challenging as the profession of digital forensics has been to date, still more interesting problems are looming on the horizon. Computers are proliferating throughout modern society, and as their numbers grow, they change in size, shape, speed, and function. Once we gathered digital evidence from monolithic, stand-alone mainframes. Today we have PC's, supercomputers, distributed client-server networks, laptops, palmtops, and PDA's, all of which can, and do, provide digital evidence at times. We have networks that use twisted pairs, coaxial cables, fiber optic cables, radio, and infrared radiation to convey information. We have LAN's and WAN's. Digital evidence stored in one computer is readily available to a miscreant using another computer half a world, and several legal jurisdictions, away.

As computers become smaller, faster and cheaper, computers are increasingly embedded inside of other larger systems in ways that are not always obvious and allow information to be created, stored, processed and communicated in ways that are unprecedented. Consequently, digital evidence can arise in unexpected places and forms. Instrumentation of spaces for every purpose from environmental monitoring to interactive control of heart rhythms will mean that digital evidence will be even more difficult to collect and analyze, and harder to present in ways that the trier of fact can understand and use.

Computerized control systems manage banks, factories, retail inventories, air traffic control, hospitals, schools, corporations, and government organizations. Computers and their software programs are embedded in our cars, boats, trains and planes, in tools, equipment, and machinery, in telecommunications systems and public switched networks, even in our bodies. Each of them is a potential source of digital evidence, the collection, storage, analysis, and presentation of which is and will be constrained by evolving legal standards and constraints that we fail to understand at our peril.

REFERENCES

[1]http://www.washingtonpost.com/wp-srv/WPlate/1998-08/19/060l-081998-idx.html accessed 8/26/02.

[2] *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).

[3] *Frye v. United States*, 54 App. D. C. 46, 293 F. 1013 (1923).

[4] *Daubert* at 593.

[5] *Ibid*.

[6] *Daubert* at 595.

[7] "Relevant evidence" is defined as that which has "any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." Fed. R. Evid. 401.

[8] *Daubert* at 590.

[9] *Kuhmo Tire v. Carmichael*, 119 S.Ct. 37, 142 L.Ed.2d 29, 69 USLW 3228, (1998).

[10] See, for example, *U. S. v. Tank*, 200 F.3d 627 (9th Cir. 2000); *Perfect 10 v. Cybernet Ventures*, No. CV 01-2595LGB(SHX)2002 ILRWeb (P&F) 1411, 2002 WL 731721(U. S. D. C., C. D. CA, April 22, 2002); *U. S. v. Catabra,n* 836 F.2d 453,457 (9th Cir. 1988); *U. S. v. Miller*, 771 F.2nd 1219, 1237 (5th Cir. 1985); *U. S. v. Yong Brothers, Inc.*, 728 F.2d 682 (5th Cir. 1984).

[11] *U. S. v. Liebert*, 519 F.2d 542, 547 (3d Cir. 1975) *cert. denied* 423 U. S. 985 (1975).

[12] *U. S. v. Bonallo*, 858 F.2nd 1427,1436 (9th Cir. 1988).

[13] *State v. American Blast Fax, Inc*., No. 00CV933, 2002 WL 508330 (E. D. Mo, March 13, 2002)

[14] Fed. R. Evid. 1002.

[15]Fed. R. Evid. 803(6) states, "Records of regularly conducted activity. A memorandum, report, record, or data compilation, in any form, of 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 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."
See, e.g., *United States v. Cestnik*, 36 F.3d 904, 909-10 (10th Cir. 1994); *United States v. Moore*, 923 F.2d 910, 914 (1st Cir. 1991); *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990); *United States v. Catabran*, 836 F.2d 453, 457 (9th Cir. 1988); *Capital Marine Supply v. M/V Roland Thomas II*, 719 F.2d 104, 106 (5th Cir. 1983). From http://www.usdoj.gov/criminal/cybercrime/usamarch2001_4.htm accessed 8/26/02. See also *State v. Polanco*, 21251, 2002 WL 535804 (Conn. App., 2002).

[16] *U. S. v. Hutson*, 821 F.2nd 1015, 1020 (5th Cir. 1987).

[17] Louis Strydom, *Computer Evidence*, 2nd World Conference on the Investigation of Crime, ICC Durban, Dec. 2001.

[18] "Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping." Justice Louis Brandeis, *Olmstead v. United States*, 277 U.S. 438 (1928).

[19] The Wire Tap Act, also known as Title III, is 18 U. S. C. §§ 2510-22. The Pen Registers and Trap and Trace Devices statute is 18 U. S. C. §§ 3121-27. The Electronic Communications Privacy Act is 100 STAT. 1848, PUBLIC LAW 99-508, which *inter alia* amended the Wiretap Act and added 18 U. S. C. §§ 2701-10 dealing with stored communications. See also *Katz* ***v.*** *United States*, 389 U.S. 347; 88 S. Ct. 507; 19 L. Ed. 2d 576; 1967 U.S. LEXIS 2 (1967).

[20] Letter Opinion and Order, *United States v. Nicodemo S. Scarfo, et al.* Criminal Action No. 00-404 (NHP), U. S. District Court for the District of New Jersey, December 26, 2001.

[21] Order of the U.S. District Court for the District of New Hampshire in *Basil W. Thompson v. Anne M. Thompson, et al.,* Civil No. 02-091-M (May 30, 2002).

[22] See *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457 (5th Cir. 1994).

[23] E-Commerce Law Week, Issue 205, ©Copyright 2002, Steptoe & Johnson LLP.

[24] 18 U. S. C. § 2703(d)

[25] William Baugh and Dorothy Denning, *Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism*, U. S. Working Group on Organized Crime, National Strategy Information Center, 1997, p. 5.

[26] *United States v. Nicodemo S. Scarfo, et al.* Criminal Action No. 00-404 (NHP), U. S. District Court for the District of New Jersey.

[27] Communications Assistance for Law Enforcement Act of 1994, Pub. L. No. 103-414, 108 Stat. 4279.

[28] United States Telecom Association, et al., v. Federal Communications Commission and United States of America,