

The Digital Evidence in the Information Era

By

Mohamed CHAWKI *

* LL.B, BA, LL.M, DU; Member of the Egyptian Council of State - PhD Researcher, School of Law, University of Lyon III – France.

Table of contents ¹

I. Introduction

II. The Rise of Digital Forensics and the Digital Evidence

- A. *Historical View.*
- B. *Classification of the Digital Evidence.*

III. Admissibility of the Digital Evidence

- A. *The Standard of Proof.*
- B. *Requirements of the IACIS.*

IV. Searching and Seizing the Digital Evidence

- A. *Items that Can Searched and/ or Seized.*
- B. *Searching with/without having a Search Warrant.*
- C. *Seizure of Digital Evidence.*

V. Conclusion

¹ An earlier version of this study was presented at the “Cybercrime Conference 2003”, organised by the Computer Crime Research Center (Zaporozhye, Ukraine) and the Transnational Crime and Corruption Center at the American University (Washington, DC, U.S).

I. Introduction

The Evidence is the foundation of any criminal case, including those involving cybercrimes. Searching, examining, collecting, and preserving this Evidence may differ from one law enforcement officer to another. However, these procedures are governed by laws and legislations that should be followed. Errors in gathering, developing, or presenting Evidence can have dire consequences on the trial. Generally speaking, an Evidence means “ *Information, whether in the form of personal testimony, the language of documents, or the production of material objects, that is given in legal investigation, to establish the fact or point in question*”.² Evidence is the mean by which the court is put in possession of the facts upon which it has to adjudicate. Unless there is a dispute as to particular facts there need to be no form evidence of them. Many potential disputes in actions can be resolved before evidence is required by appropriate pleadings, thus highlighting the real areas of dispute and shortening the trial. Evidence can include documents, testimony, and other objects. It can be classified into three categories:

- a) **Real or physical Evidence**, which consists of tangible objects that can be seen and touched.
- b) **A testamentary Evidence**, where the testimony of a witness can be given during a trial, based on a personal observation or experience.
- c) **Circumstantial Evidence**, which is based on a remark, or observation of realities that tends to support a conclusion, but not to prove it.

In criminal trials, the prosecution has to prove every element of its case beyond a reasonable doubt. In civil trials, on the other hand, a party has the burden only of proving his or her affirmative contentions by a preponderance of the Evidence. In recent years the problems of procuring Evidence have been eased somewhat by the introduction of broader discovery (i.e., disclosure) rules. In civil cases, these rules compel each party to a suit to allow the other to have access to its witnesses and to

² Oxford English Dictionary.

certain types of Evidence before the trial. In criminal cases, the judge has the discretionary power to order discovery; however, in any event, the prosecutor must release all exculpatory Evidence on request.

II. The Rise of the Digital Forensics and the Digital Evidence

As early as 1984, the FBI Laboratory and other law enforcement agencies began developing programs to examine computer Evidence. To properly address the growing demands of investigators and prosecutors in a structured and programmatic manner, the FBI established the Computer Analysis and Response Team (CART). In 1991, a new term; “Computer Forensics” was coined in the first training session held by the International Association of Computer Specialists (IACIS) in Portland, Oregon. It is the science whereby; experts extract data from computer media in such a way that it may be used in a court of law; it deals with the application of law to a science. In this case, the science involved is computer science and some refer to it as Forensic Computer Science. Computer forensics has also been described as the autopsy of a computer hard disk drive because specialized software tools and techniques are required to analyze the various levels at which computer data is stored after the fact. Since then, it has become a popular topic in technological circles and in the legal community, while the Digital forensic is the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of Digital Evidence derived from Digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations.

The domain of computer forensics involves collecting, preserving, seizing, analysing and presentation of computer-related Evidence utilizing secure, controlled methodologies and auditable procedures. These examinations involve the examination of computer media, such as floppy disks, hard disk drives, backup tapes, CD-ROM’s and any other media used to store data. The forensic specialist uses specialized software, not normally available to the general public. The examination will discover data that resides in a computer system, or recover deleted/ erased, encrypted or damaged file information and recover passwords, so that documents can be read. Any

or all of this information found during the analysis may or can be used during both criminal and civil litigation. Thus, this Evidence can be visible when stored in the mean of files saved on disks, or not visible, when it requires some sort of software to locate it.

Regarding computer related crimes cases, Evidences are classified into three main categories, according to SWGDE / IOCE standards:

- a) Digital Evidence, **where the information are stored or transmitted in electronic or magnetic form.**
- b) Physical items, **where the Digital information is stored, or transmitted through a physical media.**
- c) Data objects, **where the information are linked to physical items.**

III. Admissibility of the Digital Evidence

Generally speaking, there are three requirements for the Evidence to be admissible in the court. (A) Authentication, (B) the best Evidence rule, and (C) exceptions to the hearsay rule. Authentication means showing a true copy of the original, best Evidence means presenting the original, and the allowable exceptions are when a confession, business, or official records are involved. Authentication appears to be the most commonly used rule, but experts disagree over what is the most essential, or most correct, element of this in practice. Some say documentation (of what has been done); others say preservation (or integrity of the original); and still others say authenticity (the Evidence being what you say it is).

Good arguments could be made for the centrality of each, or all, as the standard in computer forensic law. In addition, the U.S. courts require the legality of the Evidence; it must be obtained in accordance with the laws governing search and seizure, including laws expressed in the U.S. and state legislations. Some legislation sets special rules to admissible the Digital Evidence. Starting by rule 401, the Evidence is defined '*as having 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*'. According to the rule n°402 of the federal rule of

Evidence , “*All relevant Evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authorities*”. Thus the Evidence which is not relevant is not admissible.

Where these rules are still not clear, there are some requirements and precautions that should be followed by investigators. The IACIS³ provides some of these requirements to its members, to ensure that competent, professional forensic examinations:

- a) Forensically sterile examination media must be used.
- b) The examination must maintain the integrity of the original media.
- c) Printouts, copies of data and exhibits resulting from the examination must be properly marked, controlled and transmitted.

IV. Searching and Seizing the Digital Evidence

The first successful step in searching and seizing the Digital Evidence is to know and understand well what will be searched and seized. Secondly, investigators and law enforcement officers doing these steps must have a warrant to search, which covers the location and description of the system. Thirdly, the Digital Evidence shall be well seized when it is located.

A: Items that can be searched and/or seized

When speaking about searching or seizing computers, we usually do not refer to the CPU (Central Processing Unit) only; computer is useless without the devices that allow for input (e.g., the Keyboard or the mouse) and output (e.g., a monitor or printer) of Information. These devices are known as “peripherals,” and they are an integral part of any “computer system”. It means [t]he input/output units and auxiliary storage units of a computer system, attached by cables to the central processing unit.

³ The International Association of Computer Investigative Specialists.

Thus, searching and seizing the Digital Evidence in computers will often refer to the hardware, software, and data contained in the main unit. Printers, external modems (attached by cable to the main unit), monitors, and other external attachments will be referred to collectively as “peripherals” and discussed individually where appropriate. When we are referring to both the computer and all attached peripherals as one huge package, we will use the term “computer system”. “Information” refers to all the information on a computer system, including both software applications and data. Software is the term used to describe all of the programs we use when we employ the computer for some task; it is usually delivered to us on either one or more small magnetic disks or CD-ROMs. There are two basic categories of software: system software and application software. System software consists of the programs that manage our operation of the computer; while application software consists of the programs that allow us to work on higher-level tasks. They all compose the Evidence searched. Hardware searches are not conceptually difficult. Like searching for weapons, the items sought are tangible. They occupy physical space and can be moved in familiar ways. Searches for data and software are far more complex. For purposes of clarity, these types of searches must be examined in two distinct groups: (1) searches where the information sought is on the computer at the search scene and (2) searches where the information sought has been stored off-site, and the computer at the search scene is used to access this off-site location.

In some cases, the distinction is insignificant, for example when the computer is part of a network. Although “property” is defined in Federal Rule of Criminal Procedure 41(h) to include “*documents, books, papers and other tangible objects*” (emphasis added), courts have held that intangible property such as information may be seized. In *United States v. Villegas*, 899 F.2d 1324, 1334-35 (2d Cir.), cert. denied, 498 U.S. 991 (1990), the Second Circuit noted that warrants had been upheld for intangible property such as telephone numbers called from a given phone line and recorded by a pen register, conversations overheard by means of a microphone touching a heating duct, the movement of property as tracked by location-monitoring beepers, and images seized with video cameras and telescopes. The court in *Villegas* upheld a warrant which authorized agents to search a cocaine factory and covertly take photographs without authorizing the seizure of any tangible objects.

When investigators are dealing with smaller networks, desktops PC and workstations an attempt to justify the taking of the whole system should be based on the following criteria. When an entire organization is pervasively involved in an ongoing criminal scheme, with little legitimate business, (in non-essential services) and Evidence of the crime is clearly present throughout the network, an entire system seizure might be proper. In small desktop situations, investigators should seize the whole system, after requesting to do so in the affidavit. Investigators seizing whole systems should justified it by wording their affidavits in such a way so as to refer to the computer as a “system”, dependant on set configurations to preserve “ best Evidence ” in a state of original configuration. This can and often does include peripherals, components, manuals, and software. In addition to the above, investigators should make every effort to lessen the inconvenience of an on-site search. Some estimates of manual data search and analyses are 1 megabyte for every 1hour of investigation work. Based on this equation, a 1-Gigabyte hard drive can take up to 1000 hours to fully examine. This equation assumes that each piece of data is decrypted, decoded, compiled, read, interpreted and printed out.

B: Having a search Warrant

A search warrant is a document signed by a magistrate giving law enforcement officers the authority to search a specific place for specific items that are particularly described in the warrant. A warrant must be based on another document called affidavit, which is signed under another oath by some person expressing the belief that certain items will be found at the location to be searched and giving facts that support the belief. We will be presenting an overview on the U.S. Constitution and other federal laws, as this will help in understanding the general theories governing this subject:

“ The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized”.

The Fourth Amendment is applicable when a “search” and a “seizure”, are occurring typically in a criminal case, with a subsequent attempt to use judicially what was seized. Whether there was a search and seizure within the meaning of the Amendment, whether a complainant’s interests were constitutionally infringed, will often turn upon consideration of his interest and whether it was officially abused. Its restrictions apply only to agents of the government such as the public employees, the public officials, and the police officers. A private party cannot violate a suspect’s Fourth Amendment rights.⁴

In order to search a specific location, a search warrant issued by a “judicial officer” or a “magistrate” should be obtained. Warrants to search computers which contain privileged information must meet the same requirements as warrants to search for and seize paper documents under similar conditions; that is, the warrant should be narrowly drawn to include only the data pertinent to the investigation, and that data should be described as specifically as possible. Since a broad search of computers used by confidential fiduciaries (e.g., attorneys or physicians) is likely to uncover personal information about individuals who are unconnected with the investigation, it is important to instruct any assisting forensic computer experts not to examine files about uninvolved third parties any more than absolutely necessary to locate and seize the information described in the warrant. The search warrant may normally authorize the seizure of a) contraband; b) anything which is the fruit of or has been used in the commission of any crime; c) anything other than documents which may constitute Evidence of any crime; d) Documents which may constitute Evidence of any crime.

C: Searching without having a search Warrant

As already explained, a search without a warrant is per se invalid. However, there are some well defined and well delineated exceptions to that rule. These exceptions as established by statutes include:

1. Consent Search

⁴ Also see in the United Kingdom *Roberts v Jump Knitwear* [1981] FSR 527 ; *Morton-Norwich Products Inc. V Intercen Ltd (No. 2)* [1981]FSR 337.

A consent search is a voluntary permission of the party who is being searched, or controlled to the officers. In this case, they search using this consent, even if they don't have a reason to believe that an offence has been committed. The consent should be always being voluntary; if it is obtained under threat, duress, or any shape of intimidation, it is considered non voluntary. Courts have held that the person, who gives the consent, must have the authority to do. For example, an employer can give the officers consent to search employees' computer, parents for their young minors, spouses, On the other hand, a landlord can't give consent to search a tenant's home. The courts normally consider the person giving this consent, and its scope. A consent search is a voluntary permission of the party who is being searched, or controlled to the officers. In this case, they search using this consent, even if they don't have a reason to believe that an offence has been committed. The consent should be always being voluntary; if it is obtained under threat, duress, or any shape of intimidation, it is considered non voluntary. Courts have held that the person, who gives the consent, must have the authority to do. For example, an employer can give the officers consent to search "employees' computer", parents for their young minors, spouses. On the other hand, a landlord can't give consent to search a tenant's home. The courts normally consider the person giving this consent, and its scope.

2) Exigent Circumstances

The second situation where searches can be done, without a warrant is the case of exigent circumstances. Under the "exigent circumstances" exception to the warrant requirement, agents can search without a warrant if the circumstances would cause a reasonable person to believe it to be necessary when destruction of Evidence is imminent, a warrantless seizure of that Evidence is justified if there is probable cause to believe that the item seized constitutes Evidence of criminal activity. If a target's screen is displaying Evidence which agents reasonably believe to be in danger, the "exigent circumstances" doctrine would justify downloading the information before obtaining a warrant. For example, agents may know that the incriminating data is not actually stored on the suspect's machine, but is only temporarily on line from a second network storage site in another building, city, or district.

Thus, even if the agents could secure the target's computer in front of them, someone could still electronically damage or destroy the data--either from the second computer where it is stored or from a third, unknown site. Of course, when agents know they must search and seize data from two or more computers on a wide-area network, they should, if possible, simultaneously execute separate search warrants. The court always regards the exigent circumstances; some courts have ruled that exigent circumstances did not exist if the law enforcement officers had time to obtain a warrant by telephone. *United States v. Patino*, 830 F.2d 1413, 1416 (7th Cir. 1987) (warrantless search not justified when officer had adequate opportunity to obtain telephone warrant during 30-minute wait for backup assistance; not permissible for agents to wait for exigency and then exploit it), cert. denied, 490 U.S. 1069 (1989).

3) Plain – View Search

In this exception, the law enforcement officer is in a place, where he/she can observe the Evidence in plain view. This normally happens, when the officers search for particular Evidence, and they come across a different one. To rely on this exception, the officer must be in a lawful position to observe the Evidence, and its incriminating character must be immediately apparent.

4) Border Searches

Law enforcement officers may search computers without a warrant and without probable cause as a condition of crossing the border or its “functional equivalent”. When determining the contents of international baggage and incoming international mail at the border. Border searches or international mail searches of diskettes, tapes, computer hard drives (such as laptops carried by international travellers), or other media should fall under the same rules which apply to incoming persons, documents, and international mail. On the other hand, this exception will not be applied to data transmitted electronically, or by other non-physical methods into the United States from other countries.

D: Seizure of Digital Evidence

The way in which we can seize the Digital Evidence differs from hardware to software. Investigators used to print the files and recopy them on floppy disks, or to seize all computer equipments and access the stored data from another location. Hardware searches are not conceptually difficult; they occupy physical space and can be moved in familiar ways. One of the best ways used nowadays is making a complete exact bit stream copy of the hard disk before shutting down the computer. These copies will be used to reconstruct the suspect disk and analyze it later. Searches for data and software are far more complex, specially to be accepted by the court. Before the Supreme Court's rejection of the "mere Evidence" rule in *Warden v. Hayden*, 387 U.S. 294, 300-301 (1967), courts were inconsistent in ruling whether records that helped to connect the criminal to the offence were instrumentalities of crime (and thus seizable), or were instead merely Evidence of crime (and thus not sizable). Indeed, several courts have concluded that, when it comes to documents, it is impossible to separate the two categories, stating that the distinction between mere Evidence and instrumentalities is wholly irrational, since, depending on the circumstances, the same 'papers and effects' may be 'mere Evidence' in one case and "instrumentality" in another.

Information could be found printed out on copies, this is very valuable as they display an earlier version of data that has since been altered or deleted, and this negates the suspects' defence. Also they may lead the investigators to a particular printer which in turn may be seizable. In some conditions, investigators, and law enforcement officers may find notes in manuals, on the equipment, near by the computer. These also are considered Evidence accepted by the courts. They may lead to beak a password finding a directory, operate software...etc. But since a broad search of computers used by confidential fiduciaries (e.g., attorneys or physicians) is likely to uncover personal information about individuals who are unconnected with the investigation, it is important to instruct any assisting forensic computer experts not to examine files about uninvolved third parties any more than absolutely necessary to locate and seize the information described in the warrant. Federal law recognizes some, but not all, of the common law testimonial privileges. Fed. R. Evid. 501.

Indeed, Congress has recognized a “special concern for privacy interests in cases in which a search or seizure for documents would intrude upon a known confidential relationship such as that which may exist between clergyman and parishioner; lawyer and client; or doctor and patient”, 42 U.S.C. § 2000aa-11(1) (3). At Congress’s direction, see 42 U.S.C. § 2000aa-11(a), the Attorney General has issued guidelines for federal officers who want to obtain documentary materials from disinterested third parties. 42 U.S.C. § 2000aa-11. Under these rules, they should not use a search warrant to obtain documentary materials believed to be in the private possession of a disinterested third party physician, lawyer, or clergyman where the material sought or likely to be reviewed during the execution of the warrant contains confidential information on patients, clients, or parishioners. 28 C.F.R. § 59.4(b). Also, the Congress has expressed a special concern for publishers and journalists in the Privacy Protection Act, 42 U.S.C. 2000aa. Generally speaking, agents may not search for or seize any “work product materials” (defined by statute) from someone “reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication”, 42 U.S.C. § 2000aa (a). In addition, as an even broader proposition, government officers cannot search for or seize “documentary materials” (also defined) from someone who possesses them in connection with a purpose to similarly publish. 42 U.S.C. § 2000aa (b). These protections do not apply to contraband, fruits of a crime, or things otherwise criminally possessed. 42 U.S.C. § 2000aa-7.

On October 26, 2001, President Bush signed the USA Patriot Act (USAPA) into law. With this law we have given sweeping new powers to both domestic law enforcement and international intelligence agencies and have eliminated the checks and balances that previously gave courts the opportunity to ensure that these powers were not abused. Most of these checks and balances were put into place after previous misuse of surveillance powers by these agencies, including the revelation in 1974 that the FBI and foreign intelligence agencies had spied on over 10,000 U.S. citizens, including Martin Luther King. The passage of this act resulted in many changes concerning information systems and Digital Evidence:

a) The explanation of search warrant concerning e-mail

communications, the warrant can apply even to records that are not in the district of the issuing court. b) The authority of federal courts is expanded, to allow issuance of pen register 'trap and trace devices' anywhere in the United States.

- b) Nowadays, records could be subpoenaed and obtained by search warrant from Internet services provided by cable companies, without even notifying the customer that the government wants to examine his records.
- c) Investigators can obtain a voicemail Evidence, to seize and listen to unopened voicemail messages stored with a third party provider, under a search warrant, rather than following previously difficult steps and process under a wiretap order.
- d) Penalties and sentences have been increased for offences involving damages and hacking computers. The scope of the law is now applied to computers that are even located in other countries, if US interstate or foreign commerce is affected.
- e) Investigators nowadays could subpoena certain records such as credit card numbers, and other payment information, addresses, and their session times and connection duration of customers from ISPs.
- f) Investigators are allowed to intercept voice wire communications as Evidence in cases.

V. Conclusion

We are only seeing the beginning of computer networking. Wireless networks are on the rise and computer hardware and software continues to become more portable and sophisticated. Technology that enables any appliance to be attached to a wireless network is becoming more popular. For instance Jini <<http://www.sun.com/jini>>, a flexible technology created by Sun Microsystemes, enables a single hand-held device to connect to several wireless networks simultaneously, providing individuals with a wide range of services including cellular phone service, Internet service, and proximity networks. These developments in wireless communication promise to change the way we do business and socialize. Additionally, these new technologies will enable new forms of cybercrime, creating new challenges for lawmakers and law enforcers. On such a base, individuals and organizations shall act to prepare for cybercrime

investigations i.e developing Digital Evidence Recovery Teams (DERT), creating policies and procedures, and sharing information and expertise.

References

- [1] D. TITTEL: Scene of the Cybercrime [U.S.A, Syngress], (2002).
- [2] E. CAESY: Digital Evidence and Computer Crime [California, Academic Press], (2000).
- [3] R. SLADE: Software Fornisics/ Collecting Evidence from the Scene of a Digital Crime [U.S.A, McGraw-Hill], (2004).
- [4] C. BOWERS: Forensic Dental Evidence: An Investigator's Handbook [U.S.A, Elsevier], (2004).
- [5] N. NEGROPONTE : Being Digital [N.Y, Negroponte], (1995).
- [6] C. REED : Computer Law [London, no Given Editor].
- [7] H. BILTZER, J. JACOBIA: Forensic Digital Imaging and Photography [U.K, Academic Press], (2002).
- [8] M. COLLINS : Body of Evidence : Crime Scene Investigation (2003).
- [9] The Role of Evidence in a Trial: <<http://www.slider.com/>>.
- [10] Computer Forensics Defined: <<http://www.forensics-intl.com/>>.
- [11] DOJ Computer Crime and Intellectual Property Section: <<http://www.cybercrime.gov>>.
- [12] International Journal of Digital Evidence: <<http://www.ijde.org/>>.
- [13] Federal Rules of Evidence: <<http://www.law.cornell.edu/>>.
- [14] The International Association of Computer Investigation: <<http://www.cops.org/>>.
- [15] High Technology Crime Investigation Association: <<http://htcia.org>>.
- [16] University of Dayton: cybercrimes: <<http://www.cybercrimes.net/>>.
- [17] Computer Forensics: <<http://www.computerforensics.com>>.

