Computer Forensics: Bringing the Evidence to Court

By: Cornell Walker

***Abstract*—Today the computer has impacted almost every facet of our lives and has become a major means of communication. One of the areas which has seen the most impact is how we maintain and store data. This data is stored in the form of logs, files, spreadsheets, or email to name a few. And along with the means to store this data, we have developed many techniques to retrieve this data.. Once retrieve, this data can be used to restore information, show a history, or used as evidence to arrive at a conclusion – even if the conclusion is within our courts. This paper takes a brief look at a new science that has developed as a result of the way we now store and maintain that data; "computer forensics," and how this new science has impacted court decision and rulings regarding computer records. The areas of concern are: cleanliness of the evidence and how does the court define "computer records."**

I. Introduction

Computers have become an important part of our lives and as such are involved in almost everything we do from paying bills to booking vacations. However, computer systems have also become the mainstay of criminal activity. And when the individuals involved are brought before the courts, innocence or guilt is basically decided by testimonies and evidence. Of the two areas, evidence is probably the area most key. And when it comes to "evidence" it is the accuracy of that evidence which may be the difference in determining the outcome of the trail.

Relying more and more on the evidence extracted from computer systems to bring about convictions has forged a new means of scientific investigation. The term used to coin this area of investigation is "computer forensics." It is an area of science that has come under the scrutiny of law enforcement, federal, state, and local government officials. And the reason for the scrutiny revolves around the "cleanliness" of the data being presented. Jerry Wegman, an Associate Professor of Business Law, states, "Computer forensics has developed as an indispensable tool for law enforcement. But in the digital world, as in the physical l world, the goals of law enforcement are balanced with the goals of maintaining personal liberty and privacy. Computer forensic investigators must be aware of the legal environment in which they work, or they risk having the evidence they obtain being ruled inadmissible."[1]

II. Computer Forensics Defined

Judd Robbins", An Explanation of Computer Forensics, definition of computer forensics is as follows: "Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud." [2]

Ms. Erin Kenneally further defines computer forensics by stating, "Since forensic science is the application of a scientific discipline to the law, the essence of all forensic disciplines concerns the principles applied to the detection, collection, preservation, and analysis of evidence to ensure its admissibility in legal proceedings. Computer forensics refers to the tools and techniques to recover, preserve, and examine data stored or transmitted in binary form." [3]

III. A Question of "Cleanliness"

As I stated earlier when it comes to the legal issues of computer forensics, we must focus on the "cleanliness" of the information being extracted. The computer forensics specialist must approach the retrieval process in a very detailed and methodical manner since any or all evidence

discovered can then be used or help during discovery, depositions, or actual litigation. Ryan Purita, one of the leading computer forensic experts in private practice in Canada, and states, “In order for results to hold up in court, the file system under investigation must remain unaltered. If a single file has a time stamp later than the date and time that the file system was surrendered as evidence, an opposing lawyer can call the entire investigation into question. "You screw one little thing up," Purita explains, "and everything else is gone" in the case.” [4]

Erin Kenneally echoes the importance of “evidence” collection and how meticulous and calculated steps should be taken during the retrieval of such evidence., “Whereas DNA analysis is performed on the original blood evidence, maintaining the sanctity of original evidence is a tenet of computer forensics, and analysis must be conducted on a copy of the original media (with a few, notable exceptions where circumstances preclude a copy being made)“ [5] She continues by stating, “Regardless of whether the discipline is computer forensics or fingerprinting, the driving question is not whether evidence exists but, rather, can investigators uncover and contextualize the evidence. Therefore, the challenges are: Where to look? What techniques will make the evidence apparent? And is the evidence admissible?”[6]

IV. The Government’s Approach to Computer Records

Currently the federal government has made attempts to define and rule on the process of reviewing and admitting computer records within the judicial system. These rulings can be viewed in their entirety in DOJ manual entitled "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation.” [7] In an excerpt of this manual entitled, “Computer Crime and Intellectual Property Section,” Orin S. Kerr, trial attorney, “…explains some of the important issues that can arise when the government seeks the admission of computer records under the Federal Rules of Evidence.”[8] The areas I found of importance, and the ones I will briefly review, are as follows: Computer data and how it is defined; Authenticity and the Alteration; Establishing the Reliability of Computer Programs; Identifying the Author of Computer-Stored Records; and The Best Evidence Rule.

V. Computer Records, “The Business Exception Rule”

Mr. Kerr notes that the focus of computer records within the federal courts have centered on their admissibility and whether these records fall within the “business records exception.” Fed. R. Evid. 803(6).[9]The court’s determination, or the “test” of admissibility, is confirmed based on previous cases tried in the courts: “*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); and *Capital Marine Supply v. M/V Roland Thomas II*, 719 F.2d 104, 106 (5th Cir. 1983). “[10] If the computer records of interest are submitted to the courts and fall within the rulings of the above cases, the courts will accept them as “business records” provided, “… they were kept pursuant to a routine procedure for motives that tend to assure their accuracy.” [11] Accordingly, the courts have defined "business" as business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

The courts are also aware, that as they become more familiar with computer information, that they must established a more precise definition as to the “type” of records being admitted. Orin states, “…computer records that contain text often can be divided into two categories: computer-generated records, and records that are merely computer-stored. *See People v. Holowko*, 486 N.E.2d 877, 878-79 (Ill. 1985). 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. If the records are admitted to prove the truth of the matter they assert, the offeror of the records must show circumstances indicating that the human statements contained in the record are reliable and trustworthy, *see* Advisory Committee Notes to Proposed Rule 801 (1972), and the records must be authentic. 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. Finally, a third category of computer records exists: some computer records are both computer-generated *and* computer-stored. "[12]

VI. Authenticity and the Alteration of Computer Records

One thing we do know regarding computers is that, without secure measures, the data stored on these machines can be easily changed. Lawyers are also aware of this fact and allegations as to the authenticity of the computer records will come into question. Ms. Kenneally states, "… the mutability of digital evidence facilitates legal challenges grounded in chain of-custody and evidence-tampering arguments "[13]

So how does the court approach the question of tampering and alteration? In the case of the "*United States v. Glasser*, 773 F.2d 1553, 1559 (11th Cir. 1985)" [14} the courts established the following: "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." [15]

So the courts threw the responsibility on to the opposing party…they must proved that the security provided was inadequate and that a better security system existed.

VII. Establishing the Reliability of Computer Programs in Regards to "Hearsay"

A similar challenge to that of Authenticity and Alteration is the question of the authenticity of the programs running the computer system. However, the courts resolved this situation in "*United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir. 1990)." [16] The courts ruled that the government could dismiss this challenge so long as "the government provides sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof[." [17]

But according to Mr. Kerr, the federal courts that evaluate the authenticity of computer-generated records often assume that the records contain hearsay, and then apply the business records exception. "*See, e.g., United States v. Linn*, 880 F.2d 209, 216 (9th Cir. 1989)." [18]

Hearsay is considered by the courts if the records in question contain the assertions of a person, whether or not processed by a computer. However, if there is only computer-generated data untouched by human hands, the courts stated the record cannot contain hearsay. If the latter is the case, (and for the records to be admissible), the government need only to establish the authenticity of the record and does not need to establish the hearsay exception rule.

VIII. Identifying the Author of Computer-Stored Records

Since computer-stored records consist of strings of zeros and ones, the author is not necessarily identified. If we bring in the internet factor we now have a certain amount of anonymity associated with the data. In '*United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998)' [19], the courts stated that "circumstantial evidence generally provides the key to establishing the authorship and authenticity of a computer record." [20]

IX. The Best Evidence Rule

In their efforts to apply the Best Evidence Rule, "…to prove content of a writing, recording, or photograph, the "original" writing, recording, or photograph is ordinarily required." Fed. R. Evid.

1002 [21], Prosecutors again argue that computer records in their original form, consists of zeros and ones. Therefore, how can a printout be considered an original since the final product is the result of "…manipulating the file through a complicated series of electronic and mechanical processes." [22]

The Federal Rules of Evidence addressed this issue in the following manner:

"[I]f data are stored in a computer or similar device, any printout or other output readable Fed. R. Evid. 1001(3). Thus, an accurate printout of computer data always satisfies the best evidence rule. *See Doe v. United States*, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992). According to the Advisory Committee Notes that accompanied this rule when it was first proposed, this standard was adopted for reasons of practicality. by sight, shown to reflect the data accurately, is an "original". [23]

X. Things the Forensic Specialist Must Consider

In their article, Legal Aspects of Digital Forensics, Daniel J. Ryan and Gal Shpantzer

suggests, "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." [24] "Legal Aspects of Digital Forensics Daniel J. Ryan Gal Shpantzer

Ryan and Shpantzer continue in their observations by reflecting on the Daubert v. Merrell Dow Pharmaceuticals, Inc., case, "…to even reach the point where specific competency questions are answered, digital evidence must survive the threshold test posed by *Daubert* of its competency as a class of evidence." [25]

In ruling on the Daubert case, 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." [26]

In other words, the court gave its suggestion of several factors to be considered:

a. whether the theories and techniques employed by the scientific expert have been tested;
b. whether they have been subjected to peer review and publication;
c. whether the techniques employed by the expert have a known error rate;
d. whether they are subject to standards governing their application; and
e. whether the theories and techniques employed by the expert enjoy widespread acceptance. [27]

By no means is the list above all inclusive and definitive. We must remember that testimonies may be admissible even where one or more of the factors are unsatisfied. Ryan and Shpantzer further make note that 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." [28] "So, digital forensic evidence proposed for admission in court must satisfy two conditions: it must be (1) relevant, arguably a very weak requirement, and (2) it must be "derived by the scientific method" and "supported by appropriate validation." [29]

XI. Conclusion

As the courts gain more and more experience regarding the definition of computer records and their submission as "evidence," it is obvious the forensic specialist has a major responsibility. He or she must take great care in extracting and consolidating all of the data he or she thinks will be pertinent to the lawyers and individuals they are working with. Christopher Wall and Jason Paroff, "Cracking the Computer Forensics Mystery," noted the following," According to the Sedona Conference, a legal and political thing tank founded for the purpose of establishing reasonable standards and principles for handling electronic evidence, "computer forensics is the use of specialized techniques for recovery, authentication , and analysis of electronic data when a case involves issues relating to reconstruction of computer usage, examination of residual data, authentication of data

by technical analysis or explanation o technical features of data and computer usage. Computer forensics requires specialized expertise that goes beyond normal data collection and preservation techniques available to end-users or system support personnel."[30]

But since no "standard" exist on how to properly retrieve data, what can the forensic specialist do, to better ensure the data retrieved is being presented in its 'purest" form? Quoting Matthew Meyers and March Rogers, "In other fields of study, (e.g., accounting and financial fraud investigation) there are methods used to ensure that the practice is credible and reliable, and that the individuals claiming to be professionals have met a certain criteria. In the accounting profession, there is the certified professional account (CPA) examination, as well as standards and methodologies for the accounting processes. These two key components give credibility to the field, as it shows an individual is qualified by examination (that requires several years of experience prior to qualifying to take the examination) and, that is possible to follow a procedure to come to the same results. Both these aspects are missing in the computer forensics field. The question now becomes: Is it possible for an approach similar to accounting to be applied to computer forensics, and if so, what should be required?"[31]

In an article by Ryan Leigland and Axel Krings, they state the following:
"Incidents of computer related crime continues to rise each year. The CERT Coordination Center reported over 135,000 incidents in 2003, a 67% increase from 2002. Consequently, the need for forensics techniques and tools to discover attacks is also rising. My forensic investigators have developed ad-hoc procedures for performing digital investigations. The informal nature of these procedures can prevent verification of the evidence collected, and may diminish the value of the evidence in legal proceedings." [32]

Dr. Robert Rowlingson, in his article "A Ten Step Process for Forensic Readiness," while not outlining answer or providing a step-by-step approach for standardization, may have provided a means to help those who may become involved in litigations (i.e. businesses corporate or government) to better prepare themselves . He states that most forensic investigations take place after the fact (the crime has been committed, now the quest for the evidence), but what should take place is what he terms "forensic readiness." Forensic readiness, according to Dr. Rowlingson is "…the ability of an organization to maximize it potential to use digital evidence while minimizing the costs of an investigation." [33]

Scott Stevens, in an article written for the New York Law Journal, agrees that early intervention is key," Perhaps more compelling are the technical and legal implications that recommend early computer forensics intercession."[34]

While there are some costs associated with this preparation, he states, "…there is the opportunity to actively collect potential evidence in the form of logfiles, emails, back-up disks, portable computers, network traffic records, and telephone records amongst others. This evidence may be collected in advance of a crime or dispute, and can be used to the benefit of the collecting organization." [35] To continue, " Being prepared to gather and use evidence can also have benefit as a deterrent. A good deal of crime is internal. Staff will know what the organization's attitude is toward the policing of corporate systems. They will know, or will hear rumors, as to what type of crimes may have been successfully or unsuccessfully committed, and what action may have been taken against staff. A company showing that it has the ability to catch and prosecute this type of insider attacker will dissuade them, much like the shop sign "***We always prosecute thieves.***" [36]

REFERENCES

[1] Wegman, Jerry, Computer Forensics: Admissibility of Evidence in Criminal Cases; Available: http://www.e-evidence.info/legal2.html

[2] Robbins, Judd An Explanation of Computer Forensics, PC Software Forensics; Available: http://knock-knock.com

[3] Kenneally, Erin, "Computer Forensics," ;login: The Magazine of Usenix & Sage, August 2002 Volume 27-number 4

[4] Byfield, Bruce, "IT Manager's Journal; Tracking the Evolution of IT; "The two-edged sword: Legal computer forensics and open source; Legal and Regulatory. Available: http://www.management.itmanagersjournal.com

[5] Kenneally, Erin, "Computer Forensics," ;login: The Magazine of Usenix & Sage, August 2002 Volume 27-number 4

[6] Kenneally, Erin, "Computer Forensics," ;login: The Magazine of Usenix & Sage, August 2002 Volume 27-number 4

[7] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)

[8] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[9] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[10] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[11] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[12] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[13] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[14] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[15] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[16] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[17] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[18] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[19] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[20] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[21] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[22] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[23] Kerr, Orin S., :Computer Records and the Federal Rules of Evidence; USA Bulletin (March 2001)
[24] Ryan, Daniel J., Shpantzer, George Washington University, “Legal Aspects of Digital Forensics” Available: http://www.danjryan.com
[25] Ryan, Daniel J., Shpantzer, George Washington University, “Legal Aspects of Digital Forensics” Available: http://www.danjryan.com
[26] Ryan, Daniel J., Shpantzer, George Washington University, “Legal Aspects of Digital Forensics” Available: http://www.danjryan.com
[27] Ryan, Daniel J., Shpantzer, George Washington University, “Legal Aspects of Digital Forensics” Available: http://www.danjryan.com
[28] Ryan, Daniel J., Shpantzer, George Washington University, “Legal Aspects of Digital Forensics” Available: http://www.danjryan.com
[29] Wall, Christopher and Paroff, Jason, “Cracking the Computer Forensics Mystery,” Utah Bar Journal, Available: http://www.krollontrack.com
[30] Meyers, Matthew and Rogers, Marc, “Computer Forensics: The Need for Standardization and Certification,” International Journal of Digital Evidence, Fall 2004, Volume 2; Available: http://www.ijde.org
[31] Ryan, Daniel J., Shpantzer, George Washington University, “Legal Aspects of Digital Forensics” Available: http://www.danjryan.com
[32] Leigland, Ryan, Krings, Axel W., “A Formalization of Digital Forensics,” International Journal of Digital Evidence; Fall 2004, Volume 3, Issue 2; Available: http://www.ijde.org
[33] Stevens, Scott, “Deploy Computer Forensics Early to Find the Smoking Gun,” New York Law Journal, Monday, March 31, 2003
[34] Rowlingson, Robert, Ph.D, “A Ten Step Process for Forensic Readiness,” International Journal of Digital Evidence,” Winter 2004, Volume 2, Issue 3; Available: http://www.ijde.org
[35] Rowlingson, Robert, Ph.D, “A Ten Step Process for Forensic Readiness,” International Journal of Digital Evidence,” Winter 2004, Volume 2, Issue 3; Available: http://www.ijde.org
[36] Rowlingson, Robert, Ph.D, “A Ten Step Process for Forensic Readiness,” International Journal of Digital Evidence,” Winter 2004, Volume 2, Issue 3; Available: http://www.ijde.org