“I Object… It’s Hearsay”

Hearsay and Evidence
in the
Computer Emergency Response Team (CERT)

Susan E.E.B. Sherman, Esq.

SANS Security Essentials
GSEC Practical Assignment
Version 1.4 Option 1
October 20, 2004

Abstract

The Computer Emergency Response Team (CERT) is responsible for computer-related information incident handling within a specific government Agency. Part of that mission is the inherent issue to provide support to law enforcement officials. CERT must provide evidence to those that are going to complete the law enforcement effort of an incident. The CERT staff is trained either as incident handlers, those that react to information about computer incidents/events or subject area experts, those that know specific areas of computer technology. Neither of these groups are experts in legal evidence nor have they had training in evidence preservation.

This paper will present the current Federal evidentiary laws concerning computer evidence and its relationship to hearsay and then apply the Federal law to the CERT information of a Federal Agency. Finally an actual incident's information will be reviewed as to the Federal Laws and the procedures involved and recommendations will be made. The Federal Agency will be called the Agency and all of its internal procedures are For Official Use Only so they are only referenced in this document and not quoted. Also, any indication of the Department or Agency is intended to be vague.

Federal Evidence Law

To determine the truth of an issue, the US Courts are based on testimony of witnesses to bring evidence to the person trying the facts. To provide the maximum information to the trier of fact, the witness will ideally be required to testify in person under oath and subject to cross-examination on something that he personally knows. It is when this ideal situation can't occur that problems develop – thus the Rules of Evidence apply. Since this paper is reviewing the evidence and hearsay laws and cases as applied to a Federal Agency, the Federal Rules of Evidence (incorporating the revisions that took effect Dec. 1, 2003) apply.

The general principle of the US Law system is that relevant evidence is admissible unless there are specific provisions that exclude it. "Relevant evidence" means evidence 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. [1]

There is a mismatch between these two principles. If a person has relevant testimony but cannot testify in person under oath, does this mean that what the person has as evidence is inadmissible in court? What if he tells a friend, can the friend testify for him if the friend can testify under oath and subject to cross-examination? But he does not personally know something, is that permitted?

We live in the 21st Century where computers know so much information - so we can add even more questions. If a computer "says" something, is that evidence? Can a computer be cross-examined? Can a computer provide evidence under oath? Does the computer "know" something and is it an original thought or something that is told to it? It is this "original thought" idea that is the basis of the major Federal Rule of Evidence exception and the doctrine of Hearsay.

Hearsay

"Hearsay" is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. [2] Many longstanding debates have occurred in the attempt to clarify what the federal rule meant by "statement", "declarant", "offered", "in evidence" and "truth of the matter asserted". What is a statement? A line on a computer report? A log entry? An email?

[1] Rule 401, Federal Rules of Evidence, Legal Information Institute, www.cornell.law.rules/fre/rules, October 2004

[2] Rule 801 c

A"statement" is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion. [3]

These terms become important in every evidence case, however in the case of computer based evidence, these terms become especially interesting. Although the Federal Rules of Evidence were originally written before the true thrust of computer evidence or E-Evidence[4] (termed by Kristin M. Nimsger and Alan E. Brill) was felt, the rules have been modified and expanded to include computer-related interests. Note that a “statement” must be from a person – not a computer. Can computers produce hearsay? Yes, but not alone. There must be an accomplice.

There are 2 kinds of E-Evidence: Computer-generated and Computer-stored. [5] Even the kinds of evidence require more evidence – specifically who created the content of the information.

Computer-generated records contain the output of computer instructions without manual intervention. This fails the hearsay definition listed above because in computer-generated records, a “person” is not making an assertion. So generally courts have not applied Hearsay standards to pure computer-generated records thus it is initially admissible in courts. This will include the output of programs, logs, receipts, reports, etc.

On the other hand, computer-stored information can be based on human generated contents. Emails, word processing files, and even the columns that people enter into spreadsheets have a human base. If the person that entered the information does not testify on it (and also be cross-examined in person and under oath on it), the computer-stored information is considered hearsay. If an attorney wants to enter an email into evidence, it would need the proper exception/exclusion to the Federal Rules of Evidence. There are 23 separate exceptions to hearsay, but concerning the computer business, there is only one that is important and two others that need to be mentioned.

The main exclusion used in E-Evidence in the Information Security area is Fed. R. Evid. 803(6), which states that business records are not hearsay:

> (6) **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

[3] Rule 801 c

[4] Brill, Alan E. et al “Unlocking, Discovering and Using Digital Evidence: A Practical Demonstration”, AMERICAN BAR ASSOCIATION SECTION OF SCIENCE & TECHNOLOGY LAW, August 10, 2003, 2003 San Francisco, www.abanet.org/scitech/annual/5.pdf , October 2004

[5] Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice July, 2002, http://www.cybercrime.gov/s&smanual2002.htm, October 2004

> regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record or data compilation[6]

The official Notes to the Rule 803 clarify the terms “regularly conducted business activity” showing why there is such a sense of reliability in the regular records that the business relies on it to run the business.

> The element of unusual reliability of business records is said to variously be supplied by systematic checking, by regularity and continuity which produce habits of precision, by actual experience of business in relying upon them or by a duty to make an accurate record as part of a continuing job or occupation.” [7]

So back to the example of E-Evidence. Computer records that are regularly collected and stored and are relied on to run a business seem to have a nice loophole in the Hearsay law as one of the exceptions.

As cited in the Search and Seizure manual[8], it is the underlying data in the computer’s memory that is the business records as defined in this area of the code. If the business (governmental or private) retains computer logs, email archives or reports of any kind in the course of ordinary duty and the business relies on the data for accuracy, then it can be entered into court without being subject to a hearsay challenge.

One other hearsay exclusion that can be considered by the Information Assurance professional is the “**Absence of entry in records kept in accordance with the provisions of paragraph (6)**.” [9] This states that if a record is regularly kept as part of business and it is missing, then that fact can be admitted into evidence. So if part of the regular ordinary business would be to keep a log file for the day’s firewall logs, and out of the last 180 days, one day is missing, it would be permitted without a hearsay challenge to be entered in court that the log record was missing. Further evidence would need to be shown as to what the missing record meant and how it became missing. It is the first Hearsay challenge that has been overcome.

These other issues, after Hearsay has been overcome, can also plague the Information Assurance professional. Although these issues are very rarely challenged in a court, it is the daily establishment of the processes that will uphold the occasional challenges that do occur in court.

[6] Rule 803(6)
[7] Federal Rules of Evidence Advisory Committee’s Comments About Hearsay, 'Lectric Law Library's stacks, www.lectlaw.com/files/crf08.htm, October 2004
[8] Searching and Seizing Computers
[9] Rule 803(7)

Best Evidence Rule

The Best Evidence Rule historically has said that the best evidence that can be offered in court is the original. But in the world of E-Evidence, digital photography, copier machines, computer generation, what is the original? Wouldn't it be a bunch of electrical pulses or lack of pulses usually represented by 1's and 0's?

The Federal Rules of Evidence did address this issue in Article X. CONTENTS OF WRITINGS, RECORDINGS, AND PHOTOGRAPHS:

> Rule 1001. (3) **Original**. An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".[10]

Thus the output from the computer in a "readable by sight" form is the original of the information found inside the computer.

Summaries

One final issue of admissibility is required to be addressed. Summarization. How much information could a computer store that could be presented in "readable by sight" form to be provided in evidence – pages, millions of pages? Isn't just about all information from the computer summarized bits and bytes in some way? As cited in the Search and Seizure manual[11], the courts have found that computer evidence isn't necessarily summarized. And even if it is a true summary, the Federal Rule of Evidence 1006 says, "The contents of voluminous writings, recordings, or photographs which cannot conveniently be examined in court may be presented in the form of a chart, summary, or calculation…" [12]

Other Evidence Tests

Now that the computer E-Evidence has passed the basic tests to be admissible in court, what can an Information Assurance professional do to make sure the information passes the other tests of evidence: Authentication (or Identification) and Reliability. These tests do apply to the computer data in total as it is stored in the system and then again how it is reported out of the computer.

Authentication or Identification

[10] Rule 1001 (3)
[11] Searching and Seizing Computers
[12] Rule 1006

This is the rule that makes sure the evidence is what the proponent claims it is.[13] Originally in the US Courts, a business expert had to be the one to introduce the computer records to the court and computer experts had to explain to the trier of fact how the computer worked. It was a question of trusting a computer. But now the Federal rules have made computer evidence more legitimate requiring that the witness introducing the computer records must have first hand knowledge of the relevant facts, not be a computer expert.[14] Of course certification of a computer professional with a minimum of a SANS GIAC certification of competence would always be persuasive in the issue of expertise. Questioning the computer records and the chain of custody of the information can challenge the authenticity. Who created the program that created the records and who had access to the computer once the information was gathered or determined?

The prime case on this issue is United States v. Whitaker 127 F.3d 602 (7th Cir. 1997) where the standard that absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record.[15] This means that just because the evidence **may** have been tampered with, doesn't mean that the issue **may** be brought up in court. This goes to the good faith requirement such as any attorney knows prior to bringing something up in court.

Reliability

Often computer programs are not reliable. The computers themselves will only do what the programs tell them to do and thus the human factor is introduced. If the program that creates the data report or records for the court is flawed, then ergo, the data itself could be found unreliable in a court of law. This is usually a self-authenticating issue. If the users of the computer programs rely on them to provide information, then the programs are considered reliable. However if past evidence of unreliability is entered, the entire information could be found to be unacceptable.

Another method of determining reliability, although a much tougher case to prove, would be to show what the computer was instructed to do and what it did. This is sort of a test for the computer programmer, operator and the attorney to prove that what was said was done. This is not an enviable position, but it may be necessary. Once again, the easiest way of developing reliability is like creating authenticity, do it slowly over time.

CERT

The Computer Emergency Response Team (CERT) is tasked with being responsible for computer-related information incident handling with the Agency.

[13] Rule 901(a)
[14] Searching and Seizing Computers
[15] Searching and Seizing Computers

The CERT has procedures developed for incident handling. While these procedures are constantly under review, the current procedures describe the forms, reports, and other documentation involved in incident handling. In addition there are directions in the procedures for telephone calls, emails and in-person visits. All of these could be potential evidence if the incident becomes a court case.

The three main documents and procedures have many of the same elements, but are directed at different audiences. The first is the Computer Incident Response Guide[16] that is provided to the computer users and the local Information Assurance Staffs at the locations where the systems are run and used. This document is a guide "intended to serve as a ready reference and working aid to assist field activities and elements in the management of computer incident response activities in accordance with the Policy." [17] Names have been changed to protect the identity of the organizations.

The second is the CERT Handling Procedures[18] which are only to be used by CERT personnel for dealing with an incident that is either discovered by the CERT personnel or is reported to the CERT through the channels set forth in the Computer Incident Response Guide.

The third document is the CERT Incident Analysis Procedures, which has a stated purpose "to determine the effect of a particular incident against an Agency network, in order to stop further damage and aid in the recovery process."[19] This is the procedures used to discover the evidence and it is only to be used by qualified incident handlers within the CERT organization.

1. Computer Incident Response Guide

This is the document that is provided to everyone, as it is everyone's responsibility to protect the Agency's assets. The Guide specifies, "Anyone who uses a system or network can be involved in a cyber incident."[20] After defining incidents and what to look for, the Guide boldly states that all Agency employees should report all confirmed or suspected security events and incidents. Then it gets down to the business of reporting. This is where the evidence chain starts. There is even an Annex B, which has Tools, Templates and Forms.

The first form is the basic form that is contained in the CERT Handling Procedures. It is entitled Computer Incident Report Form. Instructions on this form state that it needs to be completed immediately and then sent via Encrypted email to the CERT office.

[16] Computer Incident Response Guide, Agency,
[17] ibid
[18] CERT Handling Procedures
[19] CERT Incident Analysis Procedures
[20] ibid

From an evidence point of view, this document is electronic and stored in a computer but it is has data filled in by people so it is classified as Computer-stored evidence subject to hearsay challenges. But it is also computer-generated as it is emailed so certain fields on the email (like date, from location, to location) will be computer-generated as part of the email and thus not subject to hearsay challenges for those fields although it will require someone to bring it into evidence – someone with knowledge of the event, ideally the person who created the document.

Now where does the information that the individual gathers come from to be put in the form? Some fields are obvious such as the organization name, date and time that the incident was observed. Others such as the source IP, target IP and the technical incident can be determined by the person filling out the form with personal knowledge. The information varies so widely based on the type and scope of the incident that it cannot be addressed in this paper. Suffice it to say that there are a whole slew of hearsay and evidentiary challenges just there.

Once this document is emailed to the CERT, then the next procedure takes over in the evidence chain.

2. CERT Handling Procedures

The CERT Handling Procedures now kick in and are used by trained incident handlers working for the CERT. As stated in this document, "Tracking will include all events that you extract from Intrusion Detection Systems, firewall logs, referrals from external Agency sources, incidents escalated by site…" [21] All this will be both documented in the Incident Handling Spreadsheet on the shared drive and in the Computer Incident/Event Log Form. Also at this point an Incident Folder is created on a shared computer and "any supporting documentation" is put in the folder. The folder should contain a copy of all correspondence sent, log files, spreadsheets and the Action Log.

Incident Handling Spreadsheet

The Incident Handling Spreadsheet is a quick overview and tracking mechanism for the management to review incident status. Fields (such as date opened and closed, type of incident, site, source IP, analyst name, etc.) on the spreadsheet contain data provided either by the Computer Incident Report provided by the users/sites or from information ascertained by the CERT Incident Handlers. Although the information in the spreadsheet could be admissible in court (aside from the hearsay issues) it violates the spirit of the Best Evidence rule requiring originals.

Computer Incident/Event Log

[21] CERT Handling Procedure

This is the location of the most information about a computer incident. As usual there are many evidence issues. As each event is entered into the log with the date, time, initials of incident handler, and "Observation/Activity/Action Taken/Calls Received/Calls Made", a case can be built on evidence.

Incident Folder

Here is where the evidence is stored. Correspondence is saved here. These documents are the emails about the incident. As stated above, these computer-stored documents will have to have their content reviewed against the hearsay rules but the computer-generated fields (date/time stamps, to and from addresses) will be exempt from those reviews.

As for the computer logs, this is finally the location where the information is stored. Firewall and operating log files are taken from the compromised computer and copied here. How to gather this evidence without further compromising the computer and network and also preserving evidence is covered in the CERT Incident Analysis Procedures.

CERT Incident Analysis Procedures

The Incident Analysis Goal Procedures' goal is to develop a consistent methodology for the discovery of evidence. Specifically the goal is to "discover evidence that proves:

- What happened
- Where it happened
- When it happened
- Who did it
- How they did it" [22]

The Pre-Analysis section of this document provides the best evidence-oriented direction provided to the Agency concerning incidents. "Since it may not always be apparent at the beginning of an incident investigation what the outcomes will be, we must treat every investigation as if it will lead to a court case. This means that we must be careful to maintain a provable chain of custody."[23] Then the key steps are identified.

1. Contact Law Enforcement if it is one of a certain type of incidents. This is an important step and the CERT works closely with the law enforcement individuals assigned to this area. When contacting the officer, he will provide specific guidance on evidence collection or he will even take over the investigation at that point if he thinks it is needed. At that point, the evidence gathering is out of the hands of the CERT.
2. Contact the Agency's cabinet-level Headquarters for certain types of incidents. This step, which is required within a certain time frame for

[22] CERT Incident Analysis Procedures
[23] ibid

certain types of incidents, is there to allow a wider view if this type of incident is happening across multiple agencies.

3. Disconnect the system from the network and back it up. This is the prime evidence. A bit by bit image of the system or a clone is made before any investigation is done. This backup is the prime computer evidence that will be used later both in developing the full theory of the case and also proving what had happened. Directions are given in multiple operating systems for the backup: “dd” on a Unix system, “ghosting” on a Windows system are the prime methods. Other methods are listed as acceptable (cpio, tar, safeback, dump, encase, etc). Specifically the stated purpose is to get a full backup done before touching the system in any way. Now that’s evidence handling! This is also computer-generated evidence that will not be subject to hearsay challenges. And as long as the evidence is preserved on the backup and the person who created the backup will testify about the process and the tools used, this is solid evidence – best evidence.
4. Keep complete and accurate notes. This once again references the folder created above and the CERT Action Log.
5. Be on-site. This part of the document reminds the CERT Analyst that it is best to be on-site where the incident took place but also recognizes logistical and budgetary issues that may require the reliance on local site personnel. The other options are given. The first is to leave the compromised system live on the network so the analysis can be done remotely. This is possible with a properly configured firewall and TCP Wrappers. The final alternate is to replace the system and have it physically sent to CERT. Time is an issue on this option.

The rest of the CERT Incident Analysis Procedure is specific operating system instructions that are far too numerous to delve into here, but the stated goals of discovering evidence is what is focused on.

CERT Incident

The following is a summary of an actual CERT incident. No people names or locations or organization names are used.

The first indication of the issue was a CERT Analyst assigned to a specific location received an Intrusion Detection System (IDS) alert that an IP was infected (Nachi Ping Sweep accompanied by Smurf Attack). The actual IDS logs and alerts that were seen by the analyst were not stored anywhere at that time.

Contrary to policy, no Incident Folder was created. No incident number was assigned and the incident spreadsheet was not annotated. Initial correspondence was an email from the CERT Incident Analyst to the site Information Assurance Officer (IAO) identifying the IP and the alert. This would be considered a Record of regularly conducted activity exception to the hearsay rule as it was a record of an act or event made at or near the time by a person with knowledge. It is regular practice for Incident Handlers to communicate with the IAO's by email.

The IAO at the location did her work reviewing the incident and then reported back 8 days later what she did with concern. It was then that the CERT Incident Handler created the incident folder, assigned an incident number and entered information in the spreadsheet. The log was also started then. Although the initial email was inserted in the incident folder with the associated computer-generated information (date, time, from, to), all other information up to this point was subject to a hearsay challenge.

The incident log contained information that the Incident Handler entered concerning a phone call between the Incident Handler and the IAO. The IAO reported what had occurred in the preceding 8 days and the Incident Handler typed it all down in the log. Following that, 7 separate phone calls were documented between the CERT Incident Handler and either the IAO or a Law Enforcement officer over a two-day span. Once again this would be generally considered hearsay, as the info in the spreadsheet was not made by a person who had direct knowledge. This is the classic hearsay within hearsay. The business record of the log could get around the first challenge of hearsay because of the Business Records exception. The actual words attributed to the IAO and the Law Enforcement officer would still have a challenge against them.

Finally, when a resolution was reached on the incident and it was going to be closed by the Incident Handler, 11 days later, she attached to the incident folder a report that was generated by the IDS upon request by the CERT Incident Handler. This report, in its computer-generated form, would not be considered hearsay as it was computer-generated and therefore it would not be "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."[24] It would be considered evidence brought into the case by someone who knew the facts, in this case the Incident Handler. If there were challenges to the authenticity of the report, the Intrusion Detection Expert on the CERT staff could testify on how the IDS was configured and what the resulting report meant in terms of programming. She could also testify on the reliability of the IDS reports by showing how the Incident Handlers relied on them to conduct their daily business. The fact that the report was created 11 days later would be immaterial as the information that was the basis of the report was created when the incident was actually detected. Best Evidence standard would be achieved by the report out of the IDS tool.

Conclusion

[24] Rule 801 (c)

Evidence law and Hearsay law are a court issue. Incident Handling and the associated documentation are an Information Assurance issue. These two sides will collide on a regular basis in courts when there are high stakes. Education of both sides seems to be the best method of preventing rough collisions of the sides. The law side needs to understand what the processes are and then provide input into the procedures so that the Incident Handlers would know what is expected of them. The Incident Handlers need to know what is expected of them and then do it. The result would be solid evidence that the law enforcement community could use to complete and prosecute the incidents that are identified originally. This would allow a full closed circle.

List of References

“Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001”, Department of Justice, http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm

Brill, Alan E. et al “Unlocking, Discovering and Using Digital Evidence: A Practical Demonstration” American Bar Association Section of Science & Technology Law, August 10, 2003, 2003 San Francisco, www.abanet.org/scitech/annual/5.pdf

Capra, Daniel J., “Advisory Committee Notes to the Federal Rules of Evidence That May Require Clarification”, www.fjc.gov/public/pdf.nsf/lookup/Capra.pdf/$file/Capra.pdf, 1998

CERT Handling Procedures, Agency Document, Incident Response Handbook v3.1 -31Jul01.doc

CERT Incident Analysis Procedures, Agency Document, 15 May 2002

Computer Information Security Incident Response Guide, Agency Document, May 9, 2003

Federal Rules of Evidence Advisory Committee’s Comments About Hearsay, 'Lectric Law Library's stacks, www.lectlaw.com/files/crf08.htm, October 2004

Federal Rules of Evidence, Legal Information Institute, http://www.law.cornell.edu/rules/fre/rules.htm, October 2004

Incident Response Procedures for DMZ Incidents, Agency Document, March 25, 2003

Kerr, Orin S., Computer Records and the Federal Rules of Evidence, March 2001 http://www.cybercrime.gov/usamarch2001_4.htm

Nimsger, Kristin M. and Brill, Alan E., “LegalTimes – Looking Outside the Box” week of October 21, 2002 • VOL. XXV, NO. 41, American Bar Association Section of Science & Technology Law, August 10, 2003, 2003 San Francisco, www.abanet.org/scitech/annual/5.pdf

Paul, George L., “The “Authenticity Crisis” In Real Evidence” American Bar Association Section of Science & Technology Law, August 10, 2003, 2003 San Francisco, www.abanet.org/scitech/annual/5.pdf

Proposed 2004 Amendments to Federal Rules of Evidence, Amendments Effective December 1, 2004 (if approved by Supreme Court and absent congressional action to the contrary) http://www.legalpub.com/pages/proposed%202004%20amendments%20fre.htm, October 2004

Reviewing Events / Writing Incidents, Agency Draft Document, Nov. 18, 1999

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice July, 2002, http://www.cybercrime.gov/s&smanual2002.htm

Stansbury, Jim, "Archiving Event Logs" Practical Assignment 1.4b (amended August 29, 2002), http://www.sans.org/rr/papers/30/1002.pdf