

Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual

By Christopher L. T. Brown

Christopher L. T. Brown
clbrown@TechPathways.com
Technology Pathways LLC
703 First Street
Coronado, CA. 92118
619-435-0906

1. Introduction

This paper is intended to provide an overview of the procedural aspects of searching and seizing computers as evidence in the work place. The paper starts off by examining the DoJ 2001 Search and Seizure Manual as it relates to non-warranted searches then provides guidance on the physical aspects of seizure and analysis. Please note that this paper is not intended to be legal advice, always consult legal counsel for such advice.

a. The DoJ SSM Defined

- Written in 1994 with supplements in 1997 and 1999, complete rewrite in 2001 due to expansive use of computers and the Internet.
- Provides Guidance and Advice on Searching & Seizing Computers.
- Intended to offer assistance.
- Not intended to be the authority, does not represent the official position of the DOJ and is not Regulatory.

b. Why you should RTFM (read the fine manual)

- Provides clear Fourth Amendment discussion
- Gives the reader a good overview of past court decisions surrounding computer crimes and computer evidence.
- If you are, or may become involved in searching or seizing computer or electronic evidence, this manual is a must read.

2. Searching and Seizing Computers with a Warrant

While usually only law enforcement officials will become involved in Search and Seizure with a warrant, it is helpful to understand the Fourth Amendment as it relates to computer storage devices.

a. The Fourth Amendment -

"Reasonable Expectation of Privacy in Computers as Storage Devices" - "To determine whether an individual has a reasonable expectation of privacy in information stored in a computer; it helps to treat the computer like a closed container such as a briefcase or file cabinet. The Fourth Amendment generally prohibits law enforcement from accessing and viewing information stored in a computer without a warrant if it would be prohibited from opening a closed container and examining its contents in the same situation."

Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual

By Christopher L. T. Brown

3. Warrantless & Workplace Searches

Private and workplace warrantless searches are acceptable as long as you follow guidelines.

- a. Private Searches - "The Fourth Amendment does not apply to searches conducted by private parties who are not acting as agents of the government" (United States v. Hall 1998 - Computer Repairman & Child Porn)
- b. Private v. Government searches have a broad range of definitions
- c. Other issues such as Consent, Third-Party Consent, Spouses, Parents and network administrators.
- d. Occur often in computer cases and raise unusually complicated legal issues.
- e. O'Connor v. Ortega 1987 - The legality of warrantless workplace searches depends on subtle factual distinctions such as whether the workplace is public sector or private sector and whether employment policies exist that authorize a search, and whether the search is work-related.
- f. Banners are important in the workplace. See SSM appendix for wording and use.

4. Legal Aspects Evidence

Here are some common challenges to computer evidence and how to mitigate them.

- a. Important issues when seeking the admission of computer records under the Federal Rules of Evidence.
- b. The courts have indicated that computer records generally can be admitted as business records if they were kept pursuant to a routine procedure for motives that tend to assure their accuracy.
- c. Authentication - Before a party may move for admission of a computer record or any other evidence, the proponent must show that it is authentic.
- d. Challenges to the authenticity of computer records often take on one of 3 forms:
 - Were the forms or records altered? - Chain of Custody is important to this challenge.
 - Was the Program that generated the forms or data reliable? - Generally easy to determine.
 - Authenticity or identity of their author. - Circumstantial evidence generally provides the key to establishing the authorship and authenticity of a computer record.
- e. To help mitigate authenticity challenges security professionals who handle computer evidence should always:

Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual

By Christopher L. T. Brown

- Ensure proper chain of custody is maintained
- Carefully select forensics tools
- Maintain proper use of forensics tools
- Provide extensive documentation

f. The Civil Side of Computer Forensics

- Civil Discover is the means by which both parties in a civil case obtain relevant "**information**" from each other
- Federal Rules pertaining to discovery define information as "Documents and Data Compilations".
- It is important to understand this definition is broad in scope.
- The information requested in the civil discovery process does not need to be admissible evidence, only needs to lead to admissible evidence.
- The production of civil discovery evidence can be broken down into four phases:
 - Identification - This is the phase in which the types, source and location of all documents and sources must be identified.
 - Preservation - This phase ensures integrity of data and records. As you might expect electronic records and data can easily be destroyed unintentionally through normal operations.
 - Filtering - In many cases a database or other type of electronic media will contain privileged, or non-related data which is not required by discovery. In these cases the data is filtered out in preparation for production.
 - Production - The documents and/or data is presented to the requesting party.
- Note the forensics four step process is derived from these phases of civil discovery
- As you might expect, complying with civil discovery can be very expensive.
- Analyzing data provided by discovery can be more expensive.
-

5. Collecting and Handling Evidence (The technical stuff)

If you are going to collect and analyze computer evidence, do it right so it can be used.

a. Be Informed

- Computer Forensics is as much an art as a science and while common sense will take you a long way, nothing can replace a well informed technician. You will find many means by which to become and stay informed in the References and Resources section of this guide.
- It would be a mistake for technicians new to the computer forensics field to neglect developing a good understanding of the legal aspects of forensics sciences prior to performing technical investigations. This type of error can prove

Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual

By Christopher L. T. Brown

devastating to the case by rendering some, or all evidence collected inadmissible. One of the best guides on the legal aspects of computer forensics is the DoJs Search and Seizure Manual. Of course you should always contact legal representation if you have questions regarding the legal issues search and seizure.

b. Standard Practices & Documentation

- While all data collection cases are unique, all examiners should develop standard practices and follow them. These standard practices will help ensure that all data collected is collected, analyzed and preserved in the same manner. A publication considered by many as a good guideline for developing standard practices is "The Good Practices Guide for Computer Based Evidence", published by the Association of Chief Police Officers in the United Kingdom.
- One of the most important aspects of standard practices is documentation. Documentation of exactly what you did and when during every fact of an investigation cannot be over emphasized. If litigation occurs as the result of your search and seizure you may be asked to testify as much as a year or more later. Documentation will make this process much less painful.
- Documentation should contain technical aspects of the computer such as operating system settings, BIOS settings, applications installed locally, hardware configuration and user passwords if available.
- Additional environment documentation will be needed if the computer seized is installed in a network where servers are utilized for logon, data storage, and applications. This documentation should include logon scripts, policy settings and access rights.
- In addition to the technical documentation it is a good idea to keep a running log of your actions, observations. Don't forget to include specific dates and times. This will help you write a summary report if needed later, or just a good memory jogger if you are asked to testify later.

c. Computer Shutdown - To pull the plug or not

- One of the greatest debates surrounding what is known as "Evidence Dynamics" is how to shutdown the computer you are about to seize. Evidence Dynamics can be defined as "Any event that changes or destroys evidence in any way during the processing of the case". Of course there are many other aspects to Evidence Dynamics, but computer shutdown is one of the most actively debated. One side of the debate is if you properly shutdown the computer system with procedures designed for that operating system then you can feel safe

Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual

By Christopher L. T. Brown

that the file system will be kept intact. In some operating systems improper shutdown could damage the file system. The other side of the debate is the school of thought that the suspect computer could be "rigged" to go through a series of file damaging procedures if not shut down in a special way. It is because of this that some security professionals recommend pulling the plug. Consider that if even a minor amount of file integrity is lost due to an improper shutdown, bit stream analysis of the drive would not be hindered. On a windows NT/2000 system registry settings can be made to flush the page file upon shutdown which may remove valuable information in its self.

- No mater how you look at it, there is no absolutely correct answer. Experience, type of operating system, as well as, other issues will help make the decision.

d. Maintain Chain of Custody

- Create a Chain-of-Custody form and manage it vigilantly. The idea behind Chain-of-Custody is simple. Keep track of anyone who has accessed the evidence from this point forward.
- Your Chain-of-Custody should include:
 1. Who Has physical possession
 2. Why They have physical possession
 3. Where They have physical possession
 4. Any Comments
 5. Signature
- If the evidence is changing possession then the releasing person and the gaining person should sign the document.

e. Physical Storage

- Keep all evidence under lock and key and know who has access. Under ideal circumstances only one person, "you" will have access.

f. Imaging the Evidence Drives

- It has long been standard practice within the computer forensics community to use some type of imaging technique to image original evidence drives for subsequent analysis.
- Some benefits to this technique include:
 1. Limiting access to original evidence
 2. Allowing technicians to run the imaged evidence environment without risk of modifying the original evidence
 3. Allowing technicians to use a variety of analysis tools on the imaged evidence without risk of modifying the original evidence

Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual

By Christopher L. T. Brown

4. Save time by allowing multiple technicians to perform analysis on multiple images of the original evidence

- As you can see, working on an image is a good idea. The key to successful imaging and analysis of an evidence disk is to ensure that you can attest that the results have not been modified or do not vary. It is recommended that you create a bit stream image the evidence drives utilizing forensics software that meets the mandatory requirements and assertions found in version 3.1.6 of the NIST Disk Imaging Tool Specification. Additionally, a new shrink-wrapped drive should be used for the image drive, a process often referred to as using a "forensically clean" drive.
- Ensure a cryptographically or mathematically sound checksum is created to maintain authenticity of disk image.
- Label and maintain Chain-of-Custody for the original evidence and all images.
- The imaged drive will become your working evidence. It is from here that you should perform all examinations and analysis.

g. Evidence Examination

- Evidence examination is the point we seek to find out if there is any true evidence useful to law enforcement and the legal process. An art as much as a science, evidence examination procedures can be as varied as platforms and installations.
- No matter what type of case you are working on, once you have imaged the evidence drives, you can outline your procedures as follows:
 1. Find out what you are looking for. You may need to help establish this question.
 2. If you are working with a legal team during the discovery process get involved early so you can help to ensure all the possible data sources are collected. This will change somewhat from case to case. In some cases you will be looking for graphic files, in others the information will reside in email and document files.
 3. Create a system report. Some cases may require a detailed report as to the status of the system. Include items such as applications installed. Directory structure, recent web sites visited viruses, Trojans, etc.
 4. Recover any deleted files and slack space from the media.
 5. On system drives it is often helpful to delete known files such as system drivers, executables and support files. That is, of course if you are only searching for data and not analyzing the performance and characteristics of the system. You may find it useful to create and maintain known file checksums to aid in this process.

Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual

By Christopher L. T. Brown

6. Identify and decrypt any encrypted files.
 7. Convert any file formats needed to prepare for searching and indexing. This step may include extracting email files.
 8. Conduct Search.
 9. If needed index results and prepare report for third party analysis hash values should be created for files of interest.
 10. Individual files may need to be organized and numbered as evidence if intended to be admitted into court.
- There are many tools available and you will most likely use more than one to achieve the steps outlined above. Don't forget that authenticity can be questioned based on the applications utilized. The use of well known and professional software tools is a must. The Resources section of this document contains links to many well known and commonly used tools.
 - As in every step before, create extensive documentation of your examination process as well as the results.

6. References

- a. Department of Justice Search & Seizure Manual dated January 2001 - Online at http://www.cybercrime.gov/searching.html#FED_GUID
- b. Computer Forensics Incident Response Essentials by Warren G. Kruse II and Jay G. Heiser. Published by Addison Wesley
- c. Handbook of Computer Crime Investigation - Forensic Tools and Technology by Eoghan Casey, et al. Published by Academic Press
- d. Computer Incident Response - Scott Grace - <http://www.sans.org/infosecFAQ/incident/IRCF.htm>

7. Agencies, Contacts & Resources

- a. US Attorney's Office - <http://www.usDoJ.gov/ag/>
- b. FBI Laboratory Computer Analysis and Response Team - <http://www.fbi.gov/hq/lab/org/cart.htm>
- c. DOJ Electronic Evidence Resource List - http://www.ojp.usDoJ.gov/nij/cybercrime_resources.htm
- d. NCIS Computer Crimes - <http://www.ncis.navy.mil/activities/CompCrim/CompCrim.html>
- e. HTCIA (High Technology Computer Investigation Association) - <http://htcia.org/>
- f. Good list of Technology Lawyers and Law Firms - <http://www.kuesterlaw.com/>

Procedural Aspects of Obtaining Computer Evidence with Highlights from the DoJ Search & Seizure Manual

By Christopher L. T. Brown

- g. Computer Forensics Online Magazine - <http://www.shk-dplc.com/cfo/>
- h. CyberCrime - <http://www.cybercrime.gov/>
- i. Technology Pathways LLC - <http://www.TechPathways.com>
- j. Computer Forensics Tool Testing List Server(cftt@yahoogroups.com)

This group is for discussing and coordinating computer forensics tool testing. Testing methodologies will be discussed, as well as the results of testing various tools. The ultimate goal of these tests is to ensure that tools used by computer forensics examiners are providing accurate and complete results.

This discussion group is open to all individuals in the field who are interested in participating in the testing of computer forensics tools.

To learn more about the cftt group, please visit
<http://groups.yahoo.com/group/cftt>

- k. Forensics List Server(forensics@securityfocus.com)

The FORENSICS mailing list is a discussion mailing list for the topic of technical and process methodologies for the application of computer forensics. The discussion is centered on such things as:

Technical Methodology for the Application of Computer Forensics. This is not system or software specific and is open for wide discussion. This discussion will be centered on such things as:

- Audit trail analysis. (Technical)
- General post mortem analysis. (Technical)
- Products and tools for use in this field. (Technical)

To learn more about the Forensics group, please visit
<http://www.securityfocus.com/cgi-bin/forums.pl>