

CJS 528: Introduction to Computer Forensics and Electronic Discovery

Doug White, PhD, CISSP, CCE, PI

Spring 2009

Purpose of this course

- Expose you to techniques used to examine basic computer technology
- Make you aware of how important electronic evidence can be
- Make you aware of the need for trained examiners
- Make you capable of conducting a basic investigation
- Make you aware of the dangers of mishandling electronic evidence.

Lab Work

- Course Requires Access Data FTK.
- This requires a dongle but will run on any machine if you have the dongle. However, this will only be required for maybe one case so the demo should work fine.
- You **MUST NOT** make illegal copies of FTK (although that would be a tricky problem).
- FTK is available as a demo for anyone, free.

Lab Work 2

- You will need a machine where you can work. GSB is an open lab for students in Security courses. Your ID should be enabled. There are courses in here MTR night, but otherwise you can get in.
- There will be some classtime available for casework but it will not be sufficient.

Lab Work 3

- FTK 1.82 is the best choice for this class.
- Do not attempt to use FTK 2.0 or FTK 2.1.
- If you would rather work with other software, there is no problem with that.

Grading in 528

- Case grades are done based on the approach used by CCE to grade exams. This means you may get really bad scores if you turn in bad cases. Your case grade for the class is based on IMPROVEMENT meaning you listen to the advice you get and improve. This lets my grades be more focused and gets your attention.

Website

- <http://cisweb.rwu.edu/dwhite>
- all materials are under CJS 528 for this class.

Phil's Tip Sheet

- <http://cisweb.rwu.edu/dwhite/rwclasses/cjs528/philstips.pdf>
- Please read this and the other case writing notes and then ask questions.
- We will also discuss in class of course.

Why Forensics is Important

- Consider the BTK case.
- What Expert Witnesses Do
- The danger of losing evidence or clues when line officers are not in tune with forensics.
- Finding the hidden answers
- Development and Preservation of Evidence

So what do Forensic Examiners Do?

- Consider this simple case:
 - A guy is selling drugs
 - His brother is helping him with the money laundering
 - They only communicate by cell phones and chat in MSIM.
 - Where is the evidence they worked together? How can you indict the launderer?
- Consider this simple case
 - A CEO orders a CFO to NOT report some critical information.
 - The CFO claims this happened via email

Examiners:

- Collect and Preserve Electronic Evidence
- Examine Electronic Evidence to determine it's viability
- Develop Electronic Evidence for use in prosecution/defense or civil trials
- Analyze evidence being developed by the other side.
- Testify

Being an Expert!

- In order to testify in court you are either a witness, an officer of the court, or an expert.

Frye (rule 702-706)

- Frye is a case that affects experts:
- “If scientific, technical, or other specialized knowledge will assist the trier of fact to understand 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, if
- (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.”

What does Frye mean?

- If you are “qualified” and you use an excepted means of analysis, you and your opinion should be admitted.
 - Example:
 - You have a PhD in Statistics
 - You perform a correlation analysis of sex and salary and find that there is a high correlation between being male and making a lot of money at company X. You also find there is a negative correlation between being female and making a lot of money at Company X.

Frye

- So, you should be admitted and your method should be acceptable so under Frye you should be ok.

There is a problem with Frye

- This advocates that you have to use only methods that are widely accepted and basically creates a big mess since attorneys can challenge virtually any person or method.

Daubert

- Daubert advocates four things:
 - 1. whether the methodology can be (and has been) tested;
 - 2. whether the theory or techniques has been subjected to peer review and publication;
 - 3. the known or potential rate of error; and
 - 4. “general acceptance” of the theory or methodology within a relevant scientific community.
- But leaves it to the trial judge to decide.

Reference Work

- <http://www.lewis-roberts.com/downloads/Evidence%20&%20Experts.pdf>

So acting as an expert

- Different courts have different requirements so be advised by your attorney.
- Some states now have new issues facing examiners (the PI issue will be discussed later).

Materials

- Typically, material is analyzed and then developed into a written analysis of the situation that provides two key components:
 - A Summation which contains all critical components simplified for a quick read and highlights key areas or an answer to a question.
 - An analysis which contains details of all materials as well as full disclosure of key evidence.

Process

- I usually make notes in a notepad file.
- Start the notepad file with
- .LOG on the first line and it will always insert the date and time.

Notepad

- .LOG
- 11:00 AM 1/20/2008
- case notes on the San Juan Group case.
- Evidence in the form of one Western Digital Hard Drive with serial number 19213214346 was received and photographed by Doug White (photo is P1).
- Evidence was documented and a receipt was given to officer Molo.
- Drive was stored in evidence locker
- 11:02 AM 1/23/2008
- Drive was retrieved from locker and imaging was conducted by Doug White. Two images were made onto sterile media and all there items were returned to the locker.

Understanding Discoverability

- Everything you write down in a case is discoverable.
- That means if you write, “I don’t know what I am doing” in a notebook and they subpoena that notebook, you will have to surrender it.
- Remember this when you make case notes, recordings, videos, etc.
 - Suspicious omissions usually look bad (see. Nixon, R. M.)

Case Preparation

- Your writeups will have two parts:
 - Summation – Contains an overview of what you have found but omits all the details. This is a document that is designed for non-experts to read and draw conclusions from based on the facts you have developed.
 - Analysis – Contains every last detail about the case. This is likely organized in one of several ways depending on your approach. The approach you use is likely important and can provide a competitive advantage to your firm.

Summations

- Do NOT attempt to draw conclusions
- Do NOT make assumptions
- Do stress key evidence (IYHO)
- Do emphasize critical components that “push” your case.
- If there is a tie-in, be sure and illustrate it clearly
- Do understand that what you write is a Court Document and may become evidence.
- Do understand that anything you write down in a case is subpoenaable.

Summations, cont.

- In your summation, you should refer to specifics in the analysis section by page number.
 - “4,067 known child pornographic images were recovered from the media belonging to the subject. All items are found on media DVD 20080120-0001 to 20070120-0010. File names and hashes are found on pp. 657-678 of this document.”

Analysis

- Do overanalyze everything. Omit no detail.
- Do Include your evidence log
- Do include your official notes
- Do include all information that *MAY* be relevant to the case.
- Do **NOT** assume things are irrelevant but you may exclude things that are common.

Analysis 2

- Analysis may also include reporting from FTK.
- Analysis may contain exhibits, tables, illustrations, or any other material relevant to your data analysis.

Approach

- Is my approach required?
- NO! You can take your own approach but be prepared to defend it.

Approaches

- It is typical to put large numbers of files on CD or DVD and refer to them by case number, media number, and item number (e.g. 20080120-0001-0001).
- For class, you can just assume you do this and refer to it as if you did. I already have the files so don't waste media.

Understanding

- I realize you are not an examiner and may not have the technical background to do full investigations.
- It is not expected you will achieve perfection and it is not necessary to do well in the class. It is expected that your form and style will be outstanding even if you miss something in the case. This is, of course, completely unrealistic.

Appendices

- Glossary of Key Terms – any term you use that might not be understood by someone on the street.
- Evidence Log (from notepad or other source)
- Evidence Trace – Tag number references for all evidence in the document. This may contain physical references such as serial numbers, photos, and other material you deem to voluminous to include in the Analysis narrative.
- Chain of custody.

Appendices 2

- License Information
- FTK logs and printouts
- Standard Business Practices (template)
 - Logging policy
 - Evidence Maintenance policy
 - Licensing policy
 - Sterile Media Policy
- Equipment Used (types etc.)

Critical Information

- This document will become OFFICIAL, that means if you screw up, it cannot be changed and will be used against you.
- You must be prepared to TESTIFY that the document is accurate and complete and you should be aware of what you are saying. (Example of the C++ Code Error)

Class Information

- Grammar, Style, and Thoroughness (including your re-writes and proofing) will be considered in grading your projects. Particular focus will be placed on your summation but the Analysis will be reviewed as well to match information.
- Typos, Spelling errors, and other mistakes that can easily be corrected and caught with software will result in large deductions.
- Mistakes in analysis are not as important (that's why you are taking a class) although in real life they would be critical. I will be more strict about analysis as the class proceeds.

Class Assumptions

- Doug will act as all roles in the case. Doug is NOT AN ATTORNEY nor is Doug an OFFICER OF THE COURT. Advice given to students in this class is a matter of Doug's opinion and does not represent any sort of accurate depiction of the law in Rhode Island or any other locale. If you have legal questions about forensics, contact your attorney or the officer presiding over your case for official responses before you attempt to perform any forensic analysis on real evidence.

Issues for Forensics Experts

- CCE and Credentials
- Equipment Purchase
 - Analysis Machines
 - Disk Drives (of many types)
 - Tape Drives(of many types)
 - Imaging Devices
- Software Licenses and Maintenance
 - Access Data (accessdata.com)
 - Encase (guidancesoftware.com)
 - Sleuthkit.org
- Insurance and Liability

Cases in Class

- Software you may want to use
 - Crackers
 - Hex Editors
 - Open Office (openoffice.org)
 - Other software that coordinates reporting (but most of this costs a lot of money).
- I do not need to be able to conduct YOUR analysis, I just have to be able to interpret your reports.

Cases, cont.

- There are 3 small cases in the class and 3 large cases.
- Be prepared to spend a great deal of time on the analysis

Policy 1

- Sterile Media Policy – Secure Technology, LLC. sterilizes all media upon receipt of such media using the following techniques:
 - 1) All hard drives are processed using wiper (lic. On file) to write zeros to every bit on the drive. The drive is then validated using the checksum zero technique outlined in White and Rea, 2008. Drives then have ports covered in evidence tape, are placed in anti-static bags sealed with tape marked “sterile” and the drives are locked in a storage cabinet until needed.

Policy 1, cont.

- Sterile Media Policy
 - 2) Secure Technology, LLC. does not use RW media for any purposes only R type CD and DVD media.
 - 3) Imaging machines exist in airgapped states and are never connected to networks. Imaging machines run from CD based or DVD based operating systems and have only sterile media installed.
 - 4) Evidence media is never connected to or used in work machines, only hashed images.

Sterile Media

- You need to sanitize all media, even NEW MEDIA! You should document this in your files as a standard practice. I will get you a copy of White and Rea, 2008 as soon as it comes out in print for your use.
- Killdisk.com has a free certified tool. Wiper is included on the USBboot disk available to you. Other tools exist. I would avoid free stuff in practice but in class it is fine.

Why do you need clean media?

- Is it possible:
 - That the files being used to prosecute were on this disk before my client obtained it
 - That the files on this disk are left over from some other case you did?

So what does sanitized media mean?

- The legendary DOD wipe – a pass of 0s to every bit, a pass of 1's to every bit, a random 0 or 1 to every bit. Repeat 7 times.
- This is very time consuming but will hold up.
- Doug's paper can illustrate another approach using logic.
 - One pass of all 0's
 - checksum the disk (this adds up all the bits)
 - If the total is 0, this should be sterile media.

A brief explanation of two key things

- You must sanitize the PHYSICAL media not LOGICAL media
 - PHYSICAL Media is the entire physical disk from byte 0000 0000 0000 0000 to byte ffff ffff ffff ffff. That is every single bit on the entire disk.
 - Logical media are drive partitions so that you might have a C: drive, a D: Drive and some other space that is unpartitioned on a disk.
 - If you only sterilize the C: drive, guess what, D and everything else is still there.
 - BE SURE YOU SANITIZE PHYSICAL DISKS

A Warning

- If you wipe something, it is wiped for good. I do drive wipes on a machine which has no other media in it and boot it from a CD. This way I don't accidentally wipe out something important.
- So, don't try this at home.

You need a policy

- One of your policies should be a policy about sterile media which details your policy and how it is maintained.
- Typically:
 - Sterilize media
 - write protect the media
 - put evidence tape over the drive ports so it can't be connected without removing the tape
 - Document it by serial number in your logs
 - Store in safe place until needed.
 - Be sure and note in your case log that evidence was imaged to sterile media and note the media numbers.

So why?

- Sterile media are used to store copies of evidence. NEVER NEVER NEVER work on actual evidence since it can be changed in the process of looking at it.
- Images are created a bit at a time by some sort of imaging tool that copies every single bit onto another piece of media.
- The evidence drive should have a write protection device in place to ensure you don't accidentally write to it.
- The image can then be used to examine or make more copies.
- Always make two images wherever possible since it may be difficult to get access to the evidence again.