Introduction to Computer Forensics
CSCI 3800
Lecture Notes
Chapter 16

Applying Forensic Science to Computers

- We are now ready to learn how to apply forensic science to the examination of single computers.
- We will be using the methodologies that we learned in Chapter 6 and Chapter 8.
- We will be using the following principles and techniques from forensic science:
    - Comparison
    - Classification,
    - Individualization, and
    - Evaluation of source.
- The steps to conduct the investigation are:
    - Preparation
    - Survey
    - Documentation
    - Preservation,
    - Examination
    - Analysis
    - Reconstruction, and
    - Reporting of results.
- Preparation:
    - We learned about this in chapter 6.
    - You need to make a "plan of attack" before you do anything else.
    - Look at your crime scene; see what digital evidence you may need to seize.
    - Determine how you will go about seizing the evidence: consent or warrant.
    - Plan how you will do the search: on site or in the lab.
    - What tools do you need to conduct the search?
    - Do you need any outside expertise?
    - Do you need to find the system admin to get passwords?
    - Who is in charge of ensuring chain of custody?
- Survey:
    - Again, we learned about this in chapter 6.
    - You have to be methodical about surveying your crime scene, make sure that you take the time to "find" all possible sources of digital evidence.
    - Basic search techniques are useful here: grid search, etc.
    - Don't forget to search for "supporting items" like manuals and peripherals.
    - Don't restrict your search to the "typical" computer, what about gaming systems, mobile phones, voip systems.
    - Follow the trail … I mean cable.
    - Some printers have internal hard-drives
- Documentation:

    - Remember that documentation is the MOST important part of a digital investigation.
    - Up to this point the purpose of documentation is the ensure the authenticity of the evidence and to document what evidence you have found.
    - Chain of custody: everyone that "touches" the evidence should be logged.
    - During the examination stage documentation is used to show the repeatability of the examination.
    - Case management is a part of documentation:
        - Document what actions are taken by the investigator.
        - Who is doing what.
        - Document the security of the evidence (usually part of the chain of custody).
- Preservation:
    - Don't forget that you might have seized more than just evidence: what about instrumentality? You must preserve all hardware seized.
    - When seizing hardware, you need to balance the need to not leave evidence behind with the need to conduct a thorough investigation in a timely fashion.
    - Ensure that the hardware is stored in a manor to preserve it (not too hot or cold, humidity factors, etc).
    - To turn off the computer or not (pull the plug?).
    - What about the contents of RAM?
    - How to preserve what is displayed on the computer? Photographs of the screen?
    - When preserving digital evidence ensure that it is kept "under lock and key."
    - Only extract the evidence that is needed.
    - When making copies of the evidence, make two!
    - Ensure that you get at least the data that a regular user can see.
    - Make sure that you are doing a bit-stream copy, not a "regular" copy? Why?
    - Should you use "clean" media to store your data on? What about a NAS?
- Examination/Analysis:
    - How "deep" of a forensic exam should you do?
    - Is the exam going to be conducted on site?
    - Must employee some form of filtering or data reduction due to the sheer volume of data today.
    - How do you do that?
    - Data recovery
    - What is the meaning of all of the data that you have isolated?
- Reconstruction:
    - Need a functional analysis of the computer. Can it actually do what you are saying it did?

    - Relational analysis.
    - Temporal analysis.
- Reporting:
    - How to present the evidence to someone (investigator, DA, judge).
    - How to right the report.
    - What order to put the information in.