CMPSCI 590F Digital Forensics Assignment 3: Introduction to Digital Forensics

Vinitra Ramasubramaniam

February 8, 2017

1 List an advantage and a disadvantage of working with digital evidence, as compared to physical evidence.

One advantage of working with digital evidence as compared to physical evidence is that usually forensic analysts work on bit-for-bit copies of the data instead of the original data. Thus, multiple copies are available to be worked on simultaneously by many people and in case of any corruption in the copied data, one can always restore the data again to the original. This is however not possible with most physical evidence because there is no unlimited supply of it (for example, DNA evidence or fibers).
One disadvantage of working with digital evidence as compared to physical evidence is that most digital evidence is circumstantial (except for photo or video) where as physical evidence like DNA or fiber evidence can individually link the perpetrator.

2 Describe a scenario where a 4-5 pieces of digital evidence are linked together using Locard's exchange principle. For example, a non-digital version with just two pieces of evidence might read: upon entering a house, one leaves some DNA from skin cells, and take some carpet fibers. (They are linked by the suspect, whose shoes contain fibers that match those from the crime scene, and whose DNA presumably matches that found at the scene.) You can go farther with digital evidence from all the systems involved (for example: server logs; local computer caches; and so on). For each piece of evidence in your example, state whether you are able to determine class or individual characteristics.

Consider an unauthorized user who intends to steal your email password stored in a file on your computer by copying the file to a remote site. It may seem like he/she did not leave any direct evidence of the theft because no files were changed. However, if file access logs are available, a record will be made of the file access. Even if no log files are maintained, system calls, and network logs at the ISP level might provide evidence related to the unauthorized access. Moreover, if the thief uses this stolen password to access your email, the IP address he is accessing your email from will be logged in your email provider's server logs.
The file access logs and system calls might provide the class characteristics. The ISP network logs and IP address in the email provider's server logs might be able to identify the individual

through the registered IP although it is possible that that particular individual didn't commit the crime.

3 Using the hypothetical case of Anne Adams from the first few lectures, give three examples of inferred conclusions using the three types of reasoning described in Lecture 03, listing the specific assumptions you are making in each example. Don't simply repeat the examples given in lecture; generate at least one new conclusion!

From analyzing the EXIF data of deleted image in adams.dd, we see that the GPS coordinates correspond to a location within Acme's building. Here are the reasonings, based on this observation.
Abductive Reasoning:
I observe that the EXIF properties contain Acme?s GPS coordinates, and it is likely that such information was captured by the Canon Camera automatically when the picture was clicked at Acme; therefore, this picture was taken while Anne was at Acme.
Deductive Reasoning:
I assume that Canon Camera always automatically fills in a image's properties with the EXIF GPS coordinates; therefore, we can deduce that this image was taken while Adams was at Acme.
Inductive Reasoning:
From my repeated experience, I hypothesize that the EXIF GPS always automatically captures the GPS coordinates of when the picture was taken; therefore, we can infer that this picture is a instance of my hypothesis and that this image was taken geographically inside Acme.

4 Find and report the title and URL for a validation report (for example, as published by the National Institute of Standards and Technology) that focuses on a digital forensics tool (software or hardware).

Title - Test Results for Graphic File Carving Tool: FTK v4.1
URL - `http://www.dhs.gov/sites/default/files/publications/508_Test%20Report_NIST_FTK%20v4.1%20Test_%20August%202015_Final.pdf`

5 Some examinations of cell phones for evidence use the phone's interface to gather information about the address book, recent calls, and so on. In other words, investigators simply press buttons on the phone to browse through and gather evidence from the phone book, SMS text messages application, and so on. List and explain one advantage and one disadvantage of using this approach (as opposed to, say, imaging the phone's contents and performing more in-depth forensics on the image).

The advantage of using the interface to gather information is that if no tool supports imaging the phone's contents, then information has to be gathered by physically interacting with the phone's interface directly.
The disadvantage of using the phone's interface to gather evidence is that the any potential could be easily erased or modified as we are directly interacting with the phone. Also any physical evidence left on the phone, for example, fingerprints or DNA would be contaminated with our physical interaction with the phone.