CS6004 - Assignment-2

Chamundeswari Arumugam
Professor
SSN College of Engineering, Chennai

September 2017

Assignment-2

- **Chapter 2-Data Acquisition**
  1. At a murder scene, you have started making an image of a computers drive. Youre in the back bedroom of the house, and a small fire has started in the kitchen. If the fire cant be extinguished, you have only a few minutes to acquire data from a 10 GB hard disk. Write one to two pages outlining your options for preserving the data.

  2. You need to acquire an image of a disk on a computer that cant be removed from the scene, and you discover that its a Linux computer. What are your options for acquiring the image? Write a brief paper specifying the hardware and software you would use.

  3. A bank has hired your firm to investigate employee fraud. The bank uses four 20 TB servers on a LAN. You are permitted to talk to the network administrator, who is familiar with where the data is stored. What diplomatic strategies should you use? Which acquisition method should you use? Write a two-page report outlining the problems you expect to encounter, explaining how to rectify them, and describing your solution. Be sure to address any customer privacy issues.

  4. You are investigating a case involving a 2 GB drive that you need to copy at the scene. Write one to two pages describing three options you have to copy the drive accurately. Be sure to include your software and media choices.

Assignment-2(Contd..)

- **Chapter 5 - Processing Crime and Incident Scenes**
  1. In the arson running case project, what information do you need about the crime scene and how the digital evidence was acquired? Review the memos you received from the Seattle Police Department and the Legatima Insurance Company, and write a short paper outlining what information might be missing and what you need to find out.

  2. Youre a detective for the local police. Thomas Brown, the primary suspect in a murder investigation, works at a large local firm and is reported to have two computers at work in addition to one at home. What do you need to do to gather evidence from these computers, and what obstacles can you expect to encounter during this process? Write a two- to three-page report stating what you would do if the company had its own Computer Forensics and Investigations Department and what you would do if the company did not.

  3. A murder in a downtown office building has been widely publicized. Youre a police detective and receive a phone call from a computer forensics investigator, Gary Owens, who says he has information that might relate to the murder case. Gary says he ran across a few files while investigating a policy violation at a company in the same office building. Considering the silver-platter doctrine, what procedures might you, as a public official, have to follow? Write a one-page paper detailing what you might do.

Assignment-2(Contd..)

- **Chapter 5 - Processing Crime and Incident Scenes (Contd..)**

4. Your spouse works at a middle school and reports rumors of a teacher, Zane Wilkens, molesting some students and taking illicit pictures of them. Zane allegedly viewed these pictures in his office. Your spouse wants you to take a disk image of Zanes computer and find out whether the rumors are true. Write a one- to two-page paper outlining how you would tell your spouse and school administrators to proceed. Also, explain why walking into Zanes office to acquire a disk image wouldnt preserve the integrity of the evidence.

5. As a computing investigator for your local sheriffs department, you have been asked to go with a detective to a local school that received a bomb threat in an anonymous e-mail. The detective already has information from a subpoena sent to the last known ISP where the anonymous e-mail originated, and the message was sent from a residence in the schools neighborhood. The detective tells you the school principal also stated that the schools Web server had been defaced by an unknown computer attacker. The detective has just obtained a warrant for the search and seizure of a computer at the residence the ISP identified. Prepare a list of what items should be included in an initial-response field kit to ensure the preservation of computer evidence when the warrant is carried out.

Assignment-2(Contd..)

- **Chapter 6 - Working with windows and DOS systems**
  1. For the arson running case project, decide whether youre going to work from the image or restore it to a drive. Next, determine the file system type, such as FAT32 or NTFS, and investigate whether any files used EFS or another encryption method. Write a short paper on your findings, and if any encryption methods were used, include a discussion of what forensics tools you could use to open those files.

  2. An employee suspects that his password has been compromised. He changed it two days ago, yet it seems someone has used it again. What might be going on?

Assignment-2(Contd..)

- **Chapter 7 - Current Computer Forensics Tools**
  1. For the arson running case project, the insurance company gives you an image file called Firestarter.dd (extracted to your work folder with the other project files for this chapter). Given the resources you determined you need in Chapter 3, describe the tools youll use to evaluate and analyze the image.

  2. On the Internet, research two popular GUI tools, Guidance Software EnCase and AccessData FTK, and compare their features to other products, such as ProDiscover (www.techpathways.com) and Ontrack EasyRecover Professional (www.ontrack.com/easyrecoveryprofessional). Create a chart outlining each tools current capabilities, and write a one- to two-page report on the features you found most beneficial for your lab.

  3. Research the forensics tools available for Mac OS and Linux. Are tools similar to Hex Workshop available for these OSs? Based on their documentation, how easy would validating these tools be? Select at least two tools, and write a one to two-page paper describing what you would do to validate them, based on what you have learned in this chapter.

  4. You need to establish a procedure for your corporation on how to verify a new forensics software package. Write two to three pages outlining the procedure you plan to use in your lab.

Assignment-2(Contd..)

- **Chapter 13 - Cell Phone and Mobile Device Forensics**
  1. You have been called in on a case involving a particular cell phone, but you dont have the equipment to conduct a forensics analysis of it. Do online research to find possible resources, and write a one- to two-page paper explaining what tools you could use to analyze the cell phone.

  2. For this project, you need access to a mobile forensics toolkit. Select a cell phone model for which you have no cable. After doing Internet research for possible options, write a plan for approaching the problem. Remember that you dont want to destroy data, so make sure you include a step to test the equipment before using it.