Lab #2 - Assessment Worksheet

Documenting a Workstation Configuration using Common Forensic Tools

Course Name and Number:
CYBS 7359 Digital Forensics

Student Name:
Natnael Kebede

Instructor Name:
Dr. Renita Murimi

Lab Due Date:
2/9/2020

Lab Assessment Questions

1. What is the main purpose of a software tool like WinAudit in computer forensics?

   the main purpose of a software tool like WinAudit in computer is to generate an inventory of software, licenses, security settings, hardware, and network settings of a workstation or server system.

2. Which item(s) generated by WinAudit would be of critical importance in a computer forensic investigation?

   Items generated by WinAudit that would be of critical importance in a computer forensic investigation are:

   Installed software,
   Software versions,
   Event logs,
   Security Settings,
   Groups and User accounts,
   Open ports, and
   Network configuration settings

3. Could you run WinAudit from a flash drive or any other external media? If so, why is this important during a computer forensic investigation?

Yes one can run WinAudit from a flash drive or any other external media. This is important because WinAudit is then able to be ran against Imaged drives without affecting the drive integrity as it is done through standalone execution rather than being installed on the system

4. Why would you use a tool like DevManView while performing a computer forensic investigation?

We use a use a tool like DevManView while performing a computer forensic investigation because it allows one it to gather a comprehensive list of all devices and their properties which can uncover hidden devices or detailed asset identification lists while also running from a single executable file, maintaining drive integrity. Additionally it is able to sort information found and identify and retrieve information quickly.

5. Which item(s) available from DevManView would be of critical importance in a computer forensic investigation?

Items available by DevManView that would be of critical importance in a computer forensic investigation are:

Suspicious device listings,
Flash drives or other external media,
"Driver registry time" matching the time of the suspected compromise, and
Drivers hidden from the operating system

6. What tool similar to DevManView is already present in Microsoft Windows systems?

The tool that is similar to DevManView that is already present in Microsoft Windows systems is Windows Device Manager.

7. Why would someone use a Hex editor during a forensic investigation?

One would use a Hex editor during a forensic investigation to view data about a suspicious file or hidden file that may not be visible using a regular text editor. Additionally, it can enable the investigator to drill into specific file types to make sure the file isn't malicious.

8. What “clue” in the Frhed examination of challenge.123 led you to the correct extension for that file?

The first line in the Hex code that indicates the file type of PDF: PDF-1.5 led me to the correct extension for that file.

9. Describe the contents of the challenge.pdf file, and the application in which it opens.

The challenge.pdf file is a PDF file which opens in Adobe Reader and it details out the Virtual Security Cloud Labs update for version 3.0 made available during Summer 2017. It also consists of an image and text describing the new change

10. Why do you need to keep evidence unaltered?

We need to keep evidence unaltered so that it can be used as evidence in a court of law and is s admissible.