TP03: HDD Analysis with Autopsy

1. Before we begin

In this **Practice**, we'll download a HDD image and analyse it using SleuthKit/Autopsy Framework.

2. What we'll learn

- ⊡ How to mount a hard disk image on Autopsy.
- ⊡ How to use Autopsy to analyse HDD image files (Applying to Greg Schardt scenario).

3. Autopsy[1]

Autopsy is an open source GUI-based digital forensics program that examines and analyzes both hard drives and smart phones effectively. Autopsy is popular among thousands of users worldwide in order to explore what actually happened in the computer.

4. How to mount a hard disk image on Autopsy

You should refer to Autopsy course Lab (Slides 06 to 12)

5. How to use Autopsy to analyse HDD image files

The Grec Schart scenario is as follows:

"On 09/20/04, a Dell CPi notebook computer, serial # VLQLW, was found abandoned along with a wireless PCMCIA card and an external homemade 802.11b antennae. It is suspected that this computer was used for hacking purposes, although cannot be tied to a hacking suspect, G=r=e=g S=c=h=a=r=d=t. (The equal signs are just to prevent web crawlers from indexing this name; there are no equal signs in the image files.) Schardt also goes by the online nickname of "Mr. Evil" and some of his associates have said that he would park his vehicle within range of Wireless Access Points (like Starbucks and other T-Mobile Hotspots) where he would then intercept internet traffic, attempting to get credit card numbers, usernames & passwords. Find any hacking software, evidence of their use, and any data that might have been generated. Attempt to tie the computer to the suspect, G=r=e=g S=c=h=a=r=d=t. A DD image and a EnCase image of the abandoned computer have already been made."

[1] https://www.sleuthkit.org/autopsy/

The mission for us is to analyze this Encase Image and answer around 24 questions that solve this case. The questions are also provided by the same people who provided this Hacking Case to us. The questions about this case are:

1. Where is the image Hash?
2. What operating system was installed on the computer ?
3. Who is the registered owner?
4. What is the OS install date?
5. What is the computer account name?
6. How many accounts are recorded?
7. What is the account name of the user who mostly uses the computer?
8. Who was the last user to logon to the computer?
9. When was the last recorded computer shutdown date/time?
10. Find the installed programs that may be used for hacking ?
11. Are there any interesting files on the computer?
12. List the network cards used by this computer?
13. How we can prove that Greg Schardt is Mr. Evil and is also the administrator of this computer?
14. Display the IP address and MAC address of the computer?
15. What is the SMTP email address and its password for Mr. Evil?
16. What are the NNTP (News Servers or netNews) settings for Mr. Evil? And What the installed program that shows this information ?
17. List 5 newsgroups that Mr. Evil has subscribed to?
18. What are the user settings that were shown when Mr. Evil was online on mIRC chat program?
19. What are IRC channels that the user of this computer accessed?
20. Ethereal, a popular “sniffing” program that can be used to intercept data, What is the name of the file that contains the intercepted data?
21. What the type of wireless computer has been used by the victim?
22. What websites was the victim accessing?
23. How many executable files are in the recycle bin?
24. How many files are actually reported to be deleted by the file system?