ACTIVITY - AUTOPSY

Steps:

1. Download and install the Autopsy,
2. Download the Mantooth.E01 image
3. Start your investigation using Autopsy
4. Write a Case Narrative Digital Forensics Examiner
5. Report Document and describe your process (with screenshot) to answer the following questions.

QUESTIONS

1. What is the image hash?
2. What operating system was used on the computer?
3. When was the install date?
4. What is the timezone settings?
5. Who is the registered owner?
6. What is the computer account name?
7. What is the primary domain name?
8. When was the last recorded computer shutdown date/time?
9. How many accounts are recorded (total number)?
10. What is the account name of the user who mostly uses the computer?
11. Who was the last user to logon to the computer?

12. A search for the name of “Wes Mantooth” reveals multiple hits. One of these proves that Wes Mantooth is the administrator of this computer. What file is it?
13. List the network cards used by this computer
14. Find installed programs that may be used for Digital forensics/hacking.
15. Which Email client is used by Mantooth?
16. How many executable files are in the recycle bin?
17. How many files are actually reported to be deleted by the file system?
18. Are there any viruses on the computer?
19. There is encryption software installed on the Mantooth computer?
20. What the most visited Internet domain and how many times it was visited ?