Midterm CYBR4400 Spring 2024

The following questions go over autopsy and FTK Imager. Please provide screenshots of the where you got the answers, how you got the answers or the area in the tool you went to get the answer. You may need to use the internet to figure out usage of a tool or to identify a specific location of artifacts. This simulates the everyday job of Digital Forensic Analyst. From answering questions to researching they may not know fully. Good Luck!

1. Is the forensic image hash E6DC06EFFDCAD74548E37323A66DBF54?
   1. No it’s 2079a64c5fcac3752d6fa8ce357420c0
2. What are the two most commonly use forensic image formats?
   1. RAW and E01
3. What type of filesystem and Operating System is the forensic image (ex. NTFS)?
   1. NTFS and Windows
4. Which volume contains the filesystem?
   1. 2 and 3
5. In autopsy, what must you wait for in order to be able to conduct string searches?
   1. You have to wait for ingest to complete
6. Who is the main User on this device? (provide the name of the user account)
   1. Kevin L Brown
7. How many items are in the Recent Documents section?
   1. 32
8. Looking at the Recycle Bin, can you tell me the name of the file(s) there? (Please list)
   1. $RBES280.txt
   2. $RBIPQHF.txt
   3. $RMJB96W.jpg
   4. $RQW4YOY.txt
9. What are the hash of the files in the Recycle Bin?
   1. 15b317a756a0afdc6741d420156bcbb8
   2. 33a193bb6c67c3ea791188216c66457a
   3. a428ad2d68ad56c82bd6296acfe61f32
   4. 2a5101fe9c212a44620c764b79dc933b
10. Are there any file(s) that may be confidential? (pay attention to what is being asked)
    1. Yes, there were keyword matches for the for the word confidential but I found 1 text document titled Johnypneumoic.txt that stated it was confidential in nature
11. Was there anything downloaded from the internet? If Yes, list the items. (maybe need to track actual file name of file if deleted)
    1. Hyabusa-main.zip
    2. Jownload.jfif
    3. Ninja-kamui-2.avif
    4. Jacker.jpg
12. Was there malware downloaded?
    1. no
13. Can you categorize the items in the documents folder? Name the categories based on file extensions
    1. Yes,
       1. .htm, html, .doc, .xls, .ppt, .pdf, .txt, .rtf
14. Exporting the registry files, specifically “Ntuser.dat”, use regedit –f on command line to read it and identify any suspicious keys and values? (research to find out where the file exists)
    1. C:\windows\system32\config
15. In the Pictures folder, is there anything weird? And if yes, what? (Please evaluate all contents)
    1. There’s a weird archive folder with two .txt files disguised as jpg files one with the keyword confidential
16. Provide the hashes for anything identified in the previous question, if there was nothing identified then provide that as the answer.
    1. 15b317a756a0afdc6741d420156bcbb8
    2. 2a5101fe9c212a44620c764b79dc933b
    3. a428ad2d68ad56c82bd6296acfe61f32
17. What directory contains the Windows Events logs? (Can use google)
    1. C:\Windows\system32\config folder
18. In FTK imager, what is the name of the of the button use to acquire a forensic image?
    1. Image mounting
19. Can you mount an image on top a Drive that is already occupied? (can you mount an image on C:, if it already exists)
    1. no
20. When mounting an image with FTK Imager, what is the default mount method?
    1. physical

Extra Credit

Using the forensic image provided for the midterm, use any forensic tool listed below and provided screenshot of success using the tool.

* KAPE
* Hayabusa
* Chainsaw

A computer screen shot of a black screen

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated