Final

Instructions: Each question must have a screenshot with its answer. Please number the answers with the number of the question it corresponds to too. Each question will again be valued at 2 points.

1. What is the md5 and SHA256 hash of the forensic image named “classfinal.E01”?
   1. fb53f55a35c2daebfa78847329172f8c
   2. b4488accdb1600cf2ce527e4b89d36e4f6579d577673274d583f2368efd8e506
2. Which volumes contained the boot and filesystem (NTFS)
   1. Volume 2,3, and 4 all had a boot file, but Volume 2 and 3 were NTFS, and Volume 2 was the only one that had a boot folder.
3. What operating system is this machine?
   1. Windows 10
4. What datetime was this machine created?
   1. 2024-01-30 19:41:02 EST
5. Who is the main user of this system?
   1. ClassVM
6. What version of autopsy is on this device?
   1. Autopsy v.4.21.0

Using the Data Artifacts tabs

1. In the web downloads, how many items were downloaded. Provide the URL, name of the file, type of file and a hash.
   1. 2 downloads both the same
   2. <https://d1kpmuwb7gvu1i.cloudfront.net/AccessData_FTK_Imager_4.7.1.exe>
   3. AccessData\_FTK\_Imager\_4.7.1.exe
   4. Executable
   5. MD5: c19fd670a497951fdcc5b979e5b9a73e

|  |
| --- |
|  |

1. Using web searches which browser was used to conduct searches?
   1. Microsoft Edge
2. Was the user looking for malicious websites?
   1. Yes, one site in particular named “malware bazaar” and depending on their preferences, they also looked up anime pictures.
3. Is there an email in Autofill, please provide the email address and who it may belong to?
   1. Yes, [raymond.garayparavisini@gmail.com](mailto:raymond.garayparavisini@gmail.com)
   2. My CYBR 4400 professor; Ray G
4. At what time was a USB tablet attached to the device, please provide the device id along with the datetime?
   1. 2024-04-20 17:38:41 EDT
   2. 5&12c8f4c0&0&1

Using Analysis results

1. In the interesting items, Autopsy believes there are some suspicious files, named and what autopsy believe they are? Additionally provide the hashes of the files
   1. Gdbus.exe
      1. Encryption program
      2. MD5: 778d815bd7f02ec51425744665c988d9
      3. SHA-256: ccb14fedb5b0ba3f99bfa41ce2f06938974ebea633a4b869e602db636d7bcbb4
   2. Ch01ProjDataFiles(1).zip
      1. Possible Zip Bomb
      2. MD5: c3d7217427123cddf0c8ae4ae35754d6
      3. SHA-256: a7e03af545c463e061478d2ca837388da896eb42b0b5aa0b7ac24c742e23b002

Forensic Analysis

1. On the user ClassVm’s Desktop there is a file named “7z2301-x64.exe”? Hash the file and tell me what the file is used for?
   1. MD5: e5788b13546156281bf0a4b38bdd0901
   2. SHA-256: 26cb6e9f56333682122fafe79dbcdfd51e9f47cc7217dccd29ac6fc33b5598cd
   3. File archiver with a high compression ratio; identified as suspicious
2. On the Desktop there is a folder named EZTOOLs, find the tools in the folders and name 5 tools that would be useful to a forensic analyst? Hash the files
   1. TimelineExplorer
   2. ShellBagsExplorer
   3. RegistryExplorer
   4. SDBExplorer
   5. JumpListExplorer
3. Find the folder name Registry Explorer, export the tool and export a registry from the machine to use. Use 3 bookmarks from the tool and provide the information? You can use multiple registries as well.
   1. I used the NTUSER.dat registry and came across 31 bookmarks. 3 of which are:
      1. 7-Zip; application discussed earlier
      2. Accounts; business and personal account
      3. RecentDocs; various recent documents one being the EZtools folder
4. Export the windows event log known as “Windows Powershell.evtx”, is there anything suspicious that ran using powershell?
   1. I don’t believe there was anything suspicious ran through powershell

Using Volatility 2.6 or 3

1. Identify the correct profile for the memory capture?
   1. Windows 10 64 bit
2. What module do you use to identify the profile?
   1. Windows.info.Info
3. What modules can you use to see the processes that were running?
   1. Windows.pslist.PsList
4. Can you see any network connections that were established?
   1. Yes, one from javaw.exe
5. Are there any modules that would assist with MBR or the MFT in volatility?
   1. Yes, mbrparser
   2. Yes, mftparser for volatility 2 but not for 3

Bonus Questions

1. What tool did I use to create the memory capture? Take a screenshot of the button and point to it?
   1. FTK imager

Screenshots:

1. A screenshot of a computer

   Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated2.

3.

A screenshot of a computer

Description automatically generated

4.

A screenshot of a computer

Description automatically generated

5.

A screenshot of a computer

Description automatically generated

6.A screenshot of a computer

Description automatically generated

7.

A screenshot of a computer

Description automatically generated

8.A screenshot of a computer

Description automatically generated

9.

A screenshot of a computer

Description automatically generated

10.

A screenshot of a computer

Description automatically generated

11.

A screenshot of a computer

Description automatically generated

12.

A screenshot of a computer

Description automatically generated

13.

A screenshot of a computer

Description automatically generated

14.

A screenshot of a computer

Description automatically generated

15.

A screenshot of a computer

Description automatically generated

16.

A screenshot of a computer

Description automatically generated

17.

A screenshot of a computer

Description automatically generated

18.

A screenshot of a computer

Description automatically generated

19.

A screenshot of a computer

Description automatically generated

20.

A screen shot of a computer screen

Description automatically generated

21.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

22.

A screenshot of a computer

Description automatically generated