ETHICAL HACKING TECHNOLOGIES

**Lab Work 3: Malware activity analysis**

Resources and tools

1. Memory (RAM) dump image; raw file.
2. Volatility - working memory (RAM) analysis software (<https://www.volatilityfoundation.org/releases>).
3. Any other software or tools can be used.

Using cybercrime investigation tool (<https://www.volatilityfoundation.org/releases-vol3> and/or <https://www.volatilityfoundation.org/releases> ), answer the questions below:

1 Can you identify the exact date and time (time must be in your time zone) when the memory dump was made?

|  |  |  |
| --- | --- | --- |
| Title (image) | Data | Time |
| Image local date and time | 2016-09-07 | 17:26:21 +0300 |

2. Can you identify the operating system from the working memory image?

|  |  |
| --- | --- |
| Title (image) | Operating system or family |
| AS Layer1 | WindowsAMD64PagedMemory (Kernel AS) – it is Windows |

3. Can you provide information about the number of processors or cores (CPU Core)?

|  |  |
| --- | --- |
| Title (image) | CPU Core |
| Number of Processors | 4 |

4. Can you identify the date and time of launch of applications linked to cloud services (data caches) on the memory image (the time must be in your time zone)?

|  |  |  |
| --- | --- | --- |
| Title (programmes) | Date of launch | Start-up time |
| googledrivesyn | 2016-09-07 | 17:17:50 UTC+3 |
| googledrivesyn | 2016-09-07 | 17:18:08 UTC+3 |
| BoxSync.exe | September 7, 2016 | 17:17:34 UTC+3 |

5. Can you identify the date and time of the start of the application that was used for email on the memory image (the time must be based on your time zone)?

|  |  |  |
| --- | --- | --- |
| Title (program’s) | Date of launch | Start-up time |
| thunderbird.ex | 2016-09-07 | 17:18:07 UTC+3 |

6. Can you identify on the memory image where or which (possible) e-mail is read by the user?

|  |  |  |
| --- | --- | --- |
| Title (program’s) | IP address, port | Note (to which email service provider you can assign) |
| IMAP over SSL/TLS (IMAPS), email client software or webmail interface | **Local address:** 192.168.0.200:49297  **Foreign Address:** 74.125.133.109:993 | Gmail (or another email service provider supporting IMAP over SSL) |
| IMAP over SSL/TLS (IMAPS), email client software or webmail interface | **Local address:** 192.168.0.200:49335  **Foreign Address:** 74.125.133.109:993 | Gmail (or another email service provider supporting IMAP over SSL) |

7. Can you determine what the partitions are and/or what encrypted partitions ("partitions") have been mounted

A screen shot of a computer

Description automatically generated

|  |
| --- |
|  |
| **Title** | **Connected from** | **Connected to** | **Note** |
| 0x0000000000466670 | Harddisk0Partition1 | \Device\HarddiskVolume1 | Our title is the offset |
| 0x00000000005a12c0 | Harddisk0Partition2 | \Device\HarddiskVolume2 | Our title is the offset |
| 0x00000000005e69c0 | E: | \Device\HarddiskVolume3 | Our title is the offset |
| 0x00000000008099c0 | HarddiskVolumeShadowCopy3 | \Device\HarddiskVolumeShadowCopy3 | Our title is the offset |
| 0x000000000085b060 | C: | \Device\HarddiskVolume2 | Our title is the offset |
| 0x000000000085b440 | STORAGE#Volume#{d9bf91ef-ba45-11e3-8c91-806e6f6e6963} | \Device\HarddiskVolume4 | Our title is the offset |
| 0x000000000085b900 | HarddiskVolumeShadowCopy2 | \Device\HarddiskVolumeShadowCopy2 | Our title is the offset |
| 0x000000000085bc40 | Volume#{2f97230b-b101-11e3-8c91-806e6f6e6963} | \Device\HarddiskVolume2 | Our title is the offset |
| 0x000000000085bdf0 | HarddiskVolumeShadowCopy3 | \Device\HarddiskVolumeShadowCopy3 | Our title is the offset |
| 0x000000000085bfe0 | HarddiskVolumeShadowCopy1 | \Device\HarddiskVolumeShadowCopy1 | Our title is the offset |
| 0x0000000000860220 | HarddiskVolumeShadowCopy2 | \Device\HarddiskVolumeShadowCopy2 | Our title is the offset |
| 0x000000000093a4a0 | Volume#{2f97230b-b101-11e3-8c91-806e6f6e6963} | \Device\HarddiskVolume1 | Our title is the offset |
| 0x000000000093a910 | STORAGE#Volume#{d9bf91ef-ba45-11e3-8c91-806e6f6e6963} | \Device\HarddiskVolume2 | Our title is the offset |
| 0x000000000098d4c0 | BootDevice | \Device\HarddiskVolume2 | Our title is the offset |
| 0x00000000009b81a0 | Volume#{a8c6939e-87e6-11e0-9f4b-806e6f6e6963} | \Device\HarddiskVolume3 | Our title is the offset |
| 0x00000000009c0410 | HarddiskVolume3 | \Device\HarddiskVolume3 | Our title is the offset |
| 0x00000000009f6380 | Partition2 | \Device\HarddiskVolume2 | Our title is the offset |
| 0x0000000000ac5530 | Partition1 | \Device\HarddiskVolume1 | Our title is the offset |
| 0x0000000000ac5af0 | Volume#{a8c6939e-87e6-11e0-9f4b-806e6f6e6963} | \Device\HarddiskVolume4 | Our title is the offset |
| 0x0000000000ac5f30 | Partition4 | \Device\HarddiskVolume4 | Our title is the offset |
| 0x0000000000af2b40 | X: | \Device\HarddiskVolume4 | Our title is the offset |
| 0x0000000000bd03a0 | STORAGE#Volume#{d9bf91ef-ba45-11e3-8c91-806e6f6e6963} | \Device\HarddiskVolume1 | Our title is the offset |
| 0x0000000000bd0720 | STORAGE#Volume#{d9bf91ef-ba45-11e3-8c91-806e6f6e6963} | \Device\HarddiskVolume3 | Our title is the offset |
| 0x0000000000bd0b90 | HarddiskVolume1 | \Device\HarddiskVolume1 | Our title is the offset |
| 0x0000000004320530 | Harddisk0Partition4 | \Device\HarddiskVolume4 | Our title is the offset |
| 0x00000000044337a0 | HarddiskVolume4 | \Device\HarddiskVolume4 | Our title is the offset |
| 0x0000000004433e60 | Harddisk0Partition3 | \Device\HarddiskVolume3 | Our title is the offset |
| 0x00000000044e85b0 | HarddiskVolumeShadowCopy1 | \Device\HarddiskVolumeShadowCopy1 | Our title is the offset |
| 0x0000000006062810 | Partition3 | \Device\HarddiskVolume3 | Our title is the offset |
| 0x0000000006062890 | HarddiskVolume2 | \Device\HarddiskVolume2 | Our title is the offset |
| 0x000000001ab2a450 | Harddisk1Partition1 | \Device\HarddiskVolume5 | Our title is the offset |
| 0x000000001d4ee600 | Partition1 | \Device\HarddiskVolume5 | Our title is the offset |
| 0x000000002191b8d0 | F: | \Device\HarddiskVolume5 | Our title is the offset |
| 0x0000000025d2de60 | HarddiskVolume5 | \Device\HarddiskVolume5 | Our title is the offset |
| 0x000000002cf7e6f0 | STORAGE#Volume#{d9bf91ef-ba45-11e3-8c91-806e6f6e6963} | \Device\HarddiskVolume5 | Our title is the offset |
| 0x000000004d7aa6b0 | Volume#{a8c6939e-87e6-11e0-9f4b-806e6f6e6963} | \Device\HarddiskVolume5 | Our title is the offset |

8. Can you list the software (at least 5) that the computer user may have used in the process of outputting the files?

|  |  |  |  |
| --- | --- | --- | --- |
| Eil.  No. | Name (software) | Evidence | Note (if necessary to explain the choice) |
| 1 | conhost.exe | Conhost.exe is the Command Line Host for Windows, which creates console windows to display output from command line applications and . bat files. | Conhost.exe is the Command Line Host for Windows, which creates console windows to display output from command line applications and . bat files. |
| 2 | BoxSync.exe | Box Sync is a file synchronization and sharing software, therefore, user may have used it to synchronize and output files to cloud storage | Box Sync is a file synchronization and sharing software, therefore, user may have used it to synchronize and output files to cloud storage |
| 3 | iexplore.exe | Internet Explorer is a web browser, therefore, the user may have used it to access online platforms where files could be uploaded or downloaded | Internet Explorer is a web browser, therefore, the user may have used it to access online platforms where files could be uploaded or downloaded |
| 4 | explorer.exe | Windows File Explorer is commonly used to navigate files and folders on the system, including copying, moving, and deleting files, which could involve outputting files to specific locations. | Windows File Explorer is commonly used to navigate files and folders on the system, including copying, moving, and deleting files, which could involve outputting files to specific locations. |
| 5 | googledrivesyn | Google Drive is a file synchronization and sharing software, therefore, user may have used it to synchronize and output files to cloud storage | Google Drive is a file synchronization and sharing software, therefore, user may have used it to synchronize and output files to cloud storage |
|  |  |  |  |

9 Can you determine the IP address assigned to the computer (please make a note where this assumption is made)?

|  |  |
| --- | --- |
| IP address | Note |
| 192.168.0.200 | I know it is private IP, but still |

10. Can you identify the information of the libraries (1-3) in the image?

|  |  |  |  |
| --- | --- | --- | --- |
| Name (file) | Name (Companies that created the library) | File version | Product version |
| sqlite3.dll | Robert Simpson, et al. | 1.0.94.0 | 1.0.94.0 |
| bcryptPrimitives.dll | Microsoft Corporation | 6.3.9600.16384 | 6.3.9600.16384 |
| python27.dll | Python Software Foundation | 2.7.9150.1013 | 2.7.9150.1013 |

11. Can you determine what software took the image of the memory and when (the time must be in your time zone)?

|  |  |  |
| --- | --- | --- |
| Title (program) | Data | Time |
| DumpIt.exe | 2016-09-07 | 17:26:01 UTC+3 |