

|  |  |
| --- | --- |
| **Corporation** | **OSION Corporation** |
| **Project** | **Cyber-attack forensic analysis** |
| **Instructor** | **Andy Reid** |

|  |  |
| --- | --- |
| **Investigator Name** | **Darsh Solanki** |
| **Date** | **January 26, 2024** |

* Lab Activity I: File System Information

FILE SYSTEM INFORMATION:

1. I started by navigating to the File System information category in the Navigation pane.
2. I noted the “ID” value for the system, which serves as the beginning of the Security Identifier (SID) for the user accounts.

A white background with black numbers

Description automatically generated

Figure 1: SID.

1. I examined the drive geometry and file system information, checking for a Volume Name which is “System Reserved”, and I determined that it is a “hard drive”. Because, in drive type its written Fixed.



Figure 2: Volume name.



Figure 3: Drive type.

1. After, I tagged this information as “System Information” by right clicking on it. Then it will show you the options which one of them is tag.

A screenshot of a computer

Description automatically generated

Figure 4: Tag.

1. I then cleared all filters.

PARTITIONING SCHEME:

1. I switched to file System Explorer.
2. After clicking on drive 01-01.E01, I examined the Partition 1, Partition 2, and Unpartitioned Space in the evidence pane.
3. Then I moved to Unpartitioned Space, I navigated to offset 446 in HEX view, highlighting 16 bytes for the first partition.

A screenshot of a computer

Description automatically generated

Figure 5: 16 bytes and offset 446 in HEX.

* I identified the partition type using the first byte it is 80 – Bootable partition. There are other partition which is 00 – Non-Bootable partition.

1. Again I cleared all filters.

* Lab Activity II: Decoding SAM Values

1. In the user account section, I clicked on the Orion account, and noted the SID ending in -1001.
2. In next step I followed the like which provided in location which took me to registry view.

A screenshot of a computer

Description automatically generated

Figure 6: Registry view.

1. In registry view, I clicked on the F value I observed the value listed and HEX view.

A screenshot of a computer code

Description automatically generated

Figure 7: F value.

1. I decoded the last login timestamp from Offset 8 to 15 in the HEX code.

A screenshot of a computer

Description automatically generated

Figure 8: Decoded Last Login timestamp.

* It is on 2/22/2021 at 11:20:08 AM.

1. I cleared all filters and returned to Artifacts Explorer.

* Lab Activity III: OS and Timezone Information and User Accounts

OPERATING SYSTEM INFORMATION:

1. In Artifacts Explorer, I selected the Operating System Information category.
2. I chose the entry with Windows 10 Pro and Build Number 18363.

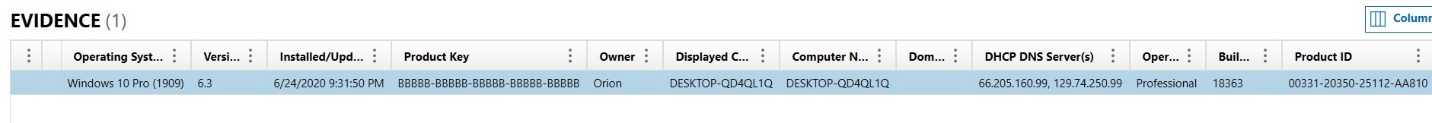


Figure 9: Windows 10 pro entry.

1. I noted the system and software files in the details pane.

A screenshot of a computer information

Description automatically generated

Figure 10: Details pane.

1. I followed the source link which is provided in location, and I observed related entries.

A screenshot of a computer

Description automatically generated

Figure 11: Evidence pane.

1. After clicking on ControlSet001\Control\Windows, I checked the Shutdown Time HEX code, and I decoded it.

A screenshot of a computer

Description automatically generated

Figure 12: HEX code.

1. I noted the value for the last shutdown Date/Time.

A close up of numbers

Description automatically generated

Figure 13: Last Shutdown Date/Time.

1. After that, I created a new artifact under EXAMINER DEFINED -> File snippets and tagged as “Last Shtdown Hex code.”

A screenshot of a computer

Description automatically generated

Figure 14: Tag Last Shutdown Hex Code.

1. I cleared my all filters.

TIMEZONE INFORMATION:

1. In the Time zone information category, I selected the item specifying US Eastern Standard Time.

A screenshot of a computer

Description automatically generated

Figure 15: US Eastern Standard Time.

1. I noted parsed data form system and software registry files.

A screenshot of a computer

Description automatically generated

Figure 16: Details pane.

1. I observed entries when I followed like on location of time zone information, and I returned to artifacts explorer.
2. In the next step, I added the Time Zone information artifact to the “System Information” tag.

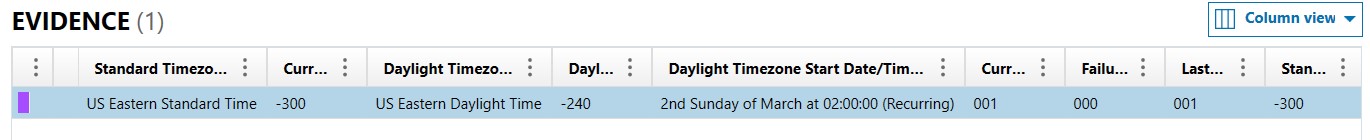


Figure 17: Time zone Information tag.

USER ACCOUNTS:

1. I selected the user account category; in this I sorted by the Security Identifier column.

A screenshot of a computer

Description automatically generated

Figure 18: SID column.

1. How many user created accounts are there and what are the RIDs of their SIDs?

* There are only 1 user account which is created and its RIDs is -1001 and SIDs is S-1-5-21-556966577-351287299-1074535340.

1. How many times has this account been logged into?

* 70 times.

1. Is the account password protected?

* Yes.

1. Has the user ever entered an incorrect password when attempting to log in? If so, when?

* Yes user have entered an incorrect password, on 2/21/2021 at 7:22:38 PM.

A screenshot of a computer

Description automatically generated