|[USER ASSIST]|: By using the timeline we analysis the different entry specially for the User Assist. We can look the activity part of the forensic analysis. We get all the entry at the RAM if not power shutdown of the affected machine. If we look at the different entry, then will get clear picture about the attack and correlation with forensic. We have discussed some of cases part of this home lab.

2020-08-30 20:21:19 UTC+0000|[USER ASSIST]| Microsoft.Windows.GettingStarted| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 14/FocusCount: 21/TimeFocused: 0:07:00.500000

From the USER Assist part when the windows open and it's fresh memory. It started at 2020-08-30. We observer how much time the windows open, how many executables are open and how much time it open.

2020-08-30 20:21:19 UTC+0000|[USER ASSIST]| %windir%\system32\displayswitch.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 13/FocusCount: 19/TimeFocused: 0:06:20.500000

The registry entry and the user is net user and time is 6 minutes & 20.5 seconds.

2020-08-30 20:21:19 UTC+0000|[USER ASSIST]| %windir%\system32\calc.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 12/FocusCount: 17/TimeFocused: 0:05:40.500000

From that we get some observation about the Calculator use. How long and how many times they are open. Like it opens 17 times 12 times it was open and 5 times it was close. It was available 5 minutes 40.5 seconds.

2020-08-30 20:21:19 UTC+0000|[USER ASSIST]| Microsoft.Windows.StickyNotes| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 11/FocusCount: 15/TimeFocused: 0:05:00.500000

From that we observe about the sticky notes, like how long and how many times they are open. Like it opens 15 times, and available on screen 11 times and 4 times it was close. It was available 5 minutes.

2020-08-30 20:21:19 UTC+0000|[USER ASSIST]| %windir%\system32\SnippingTool.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 10/FocusCount: 13/TimeFocused: 0:04:20.500000

It gives the inside about the snipping tools uses. It was used 04 minutes & 20.5 second. It was open 13 sites and focusing in 10 times and 3 times it's not uses

2020-08-30 20:21:19 UTC+0000|[USER ASSIST]| %windir%\system32\mspaint.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 9/FocusCount: 11/TimeFocused: 0:03:40.500000

From that we see Calculator open how long and how many times they are open. Like it opens 17 times 12 times it was open and 5 times it was close. It was available 5 minutes 40.5 seconds.

2020-08-30 20:21:19 UTC+0000|[USER ASSIST]| Microsoft.Windows.RemoteDesktop| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 6/FocusCount: 5/TimeFocused: 0:01:40.500000

From that we see Calculator open how long and how many times they are open. Like it opens 17 times 12 times it was open and 5 times it was close. It was available 5 minutes 40.5 seconds.

2020-08-30 20:21:19 UTC+0000|[USER ASSIST]| %windir%\system32\magnify.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 5/FocusCount: 3/TimeFocused: 0:01:00.500000

From that we see Calculator open how long and how many times they are open. Like it opens 17 times 12 times it was open and 5 times it was close. It was available 5 minutes 40.5 seconds.

1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| Microsoft.Windows.ControlPanel| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 0/FocusCount: 5/TimeFocused: 0:00:18.142000

From that we see Calculator open how long and how many times they are open. Like it opens 17 times 12 times it was open and 5 times it was close. It was available 5 minutes 40.5 seconds.

1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| %ProgramFiles%\Google\Update\GoogleUpdate.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 0/FocusCount: 1/TimeFocused: 0:00:46.957000

It takes almost 46.9 minutes for the Google update at the registry. It is single time open and always open

2020-08-30 20:27:07 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Desktop\7z1900-x64.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:03.043000

7z1900-x64.exe is executed at the power shell.

2020-08-30 20:31:05 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Desktop\Wireshark-win64-3.2.3.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 2/TimeFocused: 0:00:15.976000
Wireshark was installed.

2020-08-30 20:31:29 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Desktop\AccessData_FTK_Imager-_4.3.0.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:00.500000

FTK manager was installed

2020-08-30 20:31:34 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Desktop\npp.7.8.5.Installer.x64.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:13.058000

npp.7.8.5.Installer.x64.exe was installed at the Desktop.

1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| {6D809377-6AF0-444B-8957-A3773F02200E}\Notepad++\notepad++.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 0/FocusCount: 3/TimeFocused: 0:00:03.433000

Notepad++ was in open for 03.43 seconds

1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| {6D809377-6AF0-444B-8957-A3773F02200E}\Wireshark\npcap-0.9989.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 0/FocusCount: 3/TimeFocused: 0:00:24.571000

1970-01-01 00:00:00 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Downloads\dotNetFx40_Full_setup.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 0/FocusCount: 0/TimeFocused: 0:00:01.217000

dotNetFx40_Full_setup.exe is executed at the machine.

2020-11-04 03:01:07 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Downloads\Oct 2019\OCT 12\invoice1.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:00.500000

Run the invoice1.exe executed from C:\Users\MjolnirTraining\Downloads\Oct 2019\OCT 12 . Which is malware & run at 2020-11-04 03:01:07

2020-11-04 03:01:13 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Downloads\Oct 2019\OCT 12\pred-steal.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:00.500000

pred-steal.exe executed from C:\Users\MjolnirTraining\Downloads\Oct 2019\OCT 12 at the registry. Which is malware & run at 2020-11-04 03:01:13

2020-11-04 03:01:18 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Downloads\Oct 2019\19075-NYPD.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:00.500000

NYPD.exe executed from C:\Users\MjolnirTraining\Downloads\Oct 2019\OCT 12 at the registry. Which is malware & run at 2020-11-04 03:01:18

2020-11-04 03:01:41 UTC+0000|[USER ASSIST]| C:\Users\MjolnirTraining\Downloads\Oct 2019\OCT 12\run-last.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:00.500000

Run-last.exe executed from C:\Users\MjolnirTraining\Downloads\Oct 2019\OCT 12 at the registry. Which is malware & run at 2020-11-04 03:01:41

2020-11-04 03:02:01 UTC+0000|[USER ASSIST]| {6D809377-6AF0-444B-8957-A3773F02200E}\AccessData\FTK Imager\FTK Imager.exe| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 3/TimeFocused: 0:05:48.536000

Run the the \AccessData\FTK Imager\FTK Imager.exe for taking the memory dump at 2020-11-04 03:02:01

2020-11-04 03:02:49 UTC+0000|[USER ASSIST]| Microsoft.AutoGenerated.{C1C6F8AC-40A3-0F5C-146F-65A9DC70BBB4}| Registry: \??\C:\Users\MjolnirTraining\ntuser.dat /ID: N/A/Count: 1/FocusCount: 0/TimeFocused: 0:00:13.682000

[SHIMCACHE]: Shimcahce contains every single entry of the windows machine. It stores all the log from its start date. Every entry is given The Shimcache tracks metadata such as the full file path, last modified date, and file size but only contains the information prior to the system's last startup, as current entries are stored only in memory. The events in Shimcache.hve are listed in chronological order with the most recent event first and can be used in timelines to recreate and determine malicious activities. It focus on the time stamp of entry

[CMHIVE]: Hive is a data warehouse system for Hadoop that facilitates easy data summarization, ad-hoc queries, and the analysis of large datasets stored in Hadoop compatible file systems. Hive provides a mechanism to project structure onto this data and query the data using a SQL-like language called HiveQL.