Super timeline analysis:

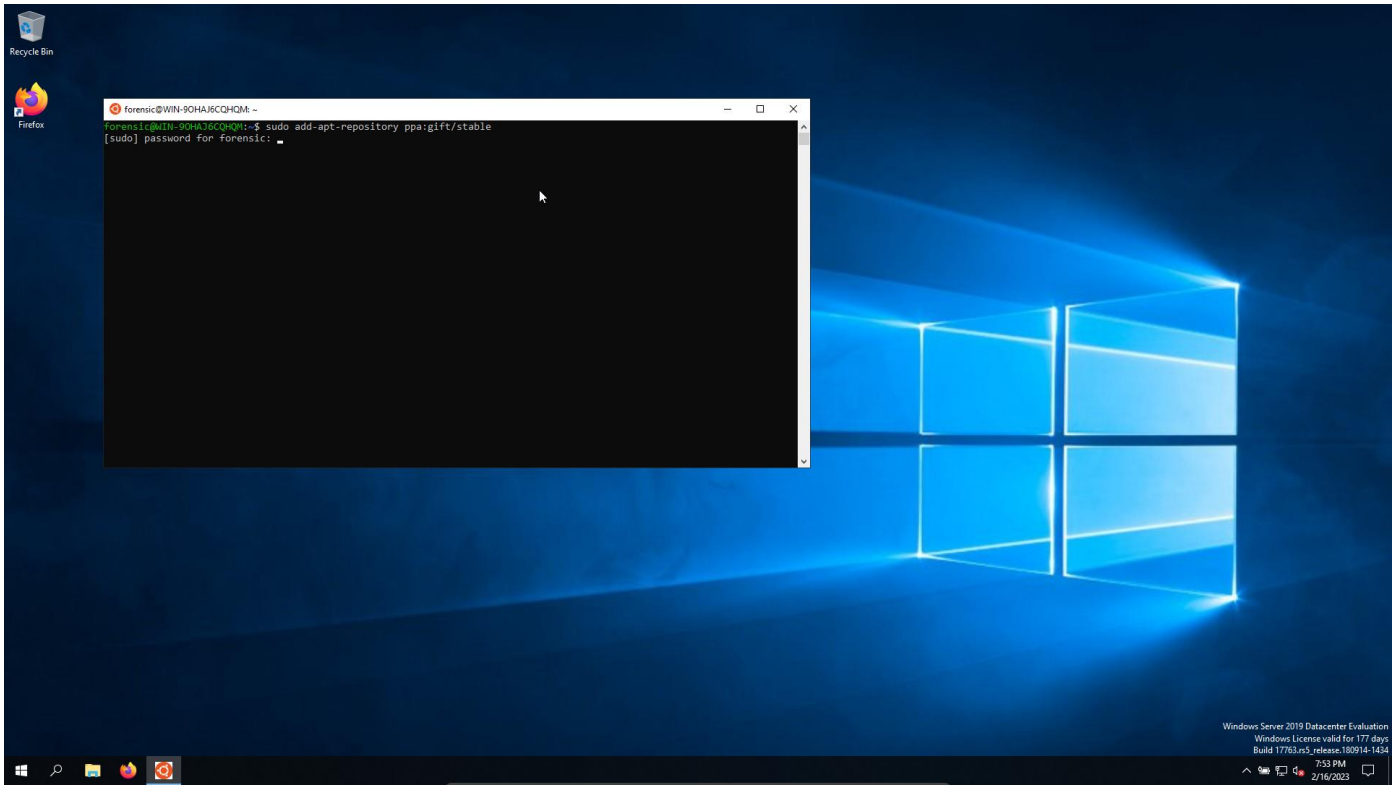
- Analysis process
- Preparing tools
- Memory timeline creation
- Disk timeline creation
- Merging timelines
- Super timeline view with Timeline explorer
- Analyzing malicious activity based on Super Timeline

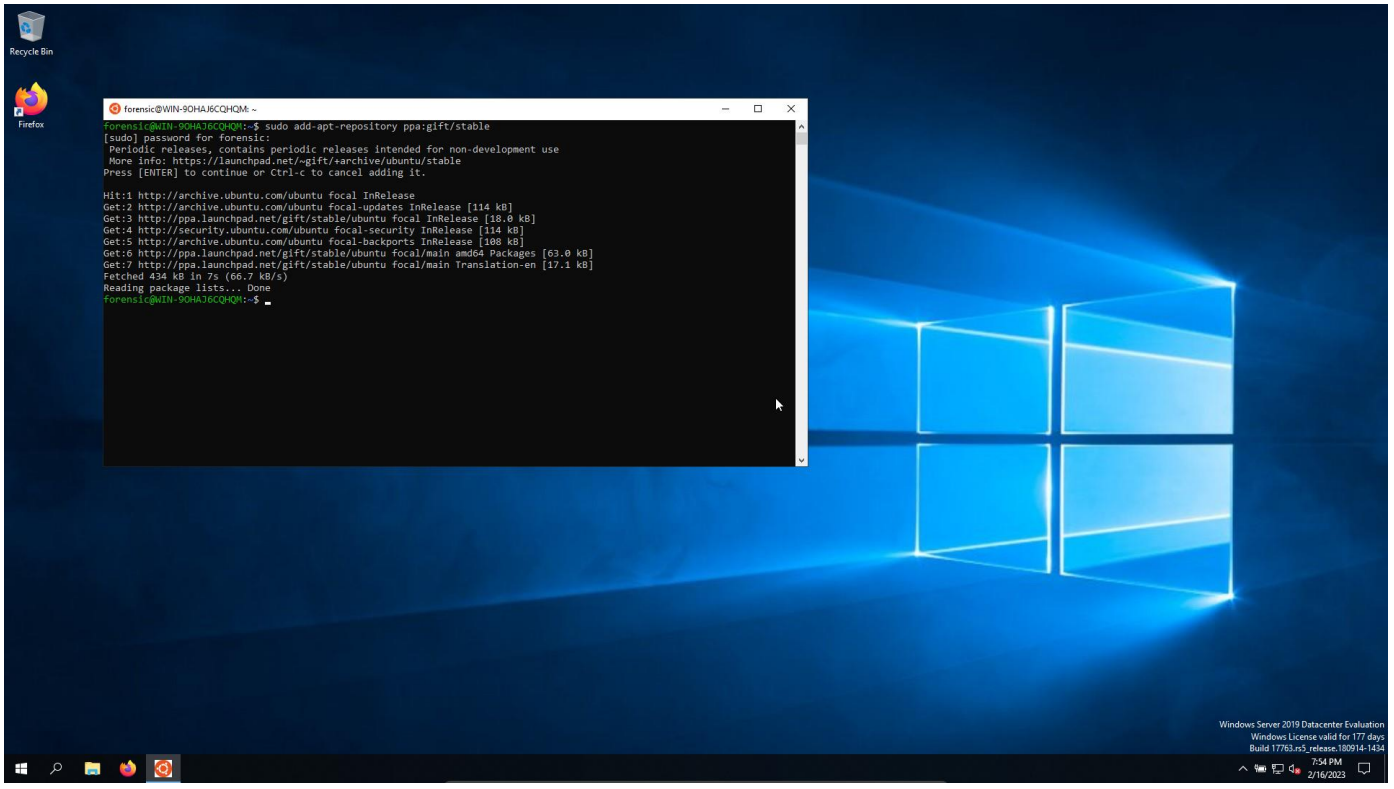
Analysis process

- Installing Plaso, Log2Timeline
- Prepare Evidence
    - Disk Image
    - Memory Image
- Use Tools:
    - Memory: generate bodyfile
    - Disk: generate plaso file
    - Merge files
    - Generate super timeline with psort tool

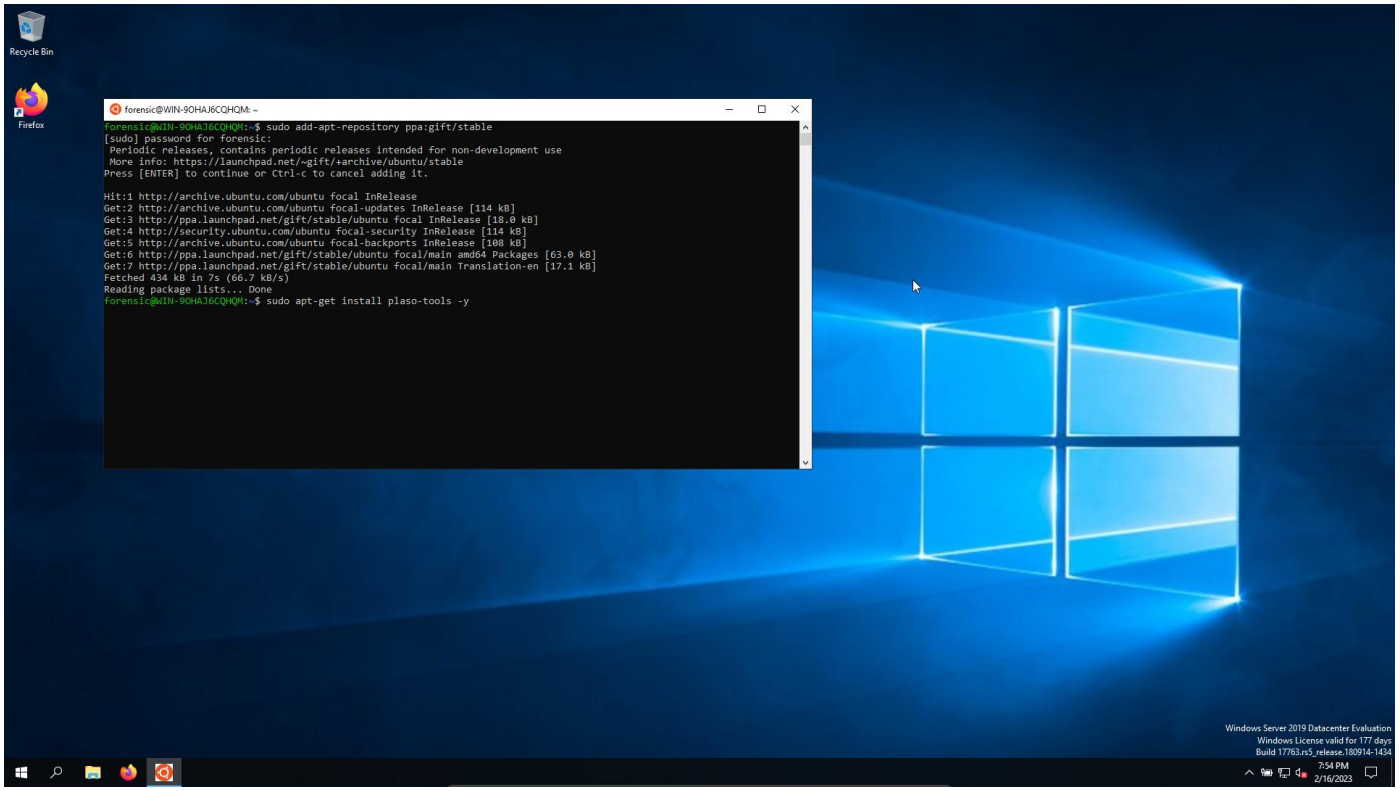
Preparing tools

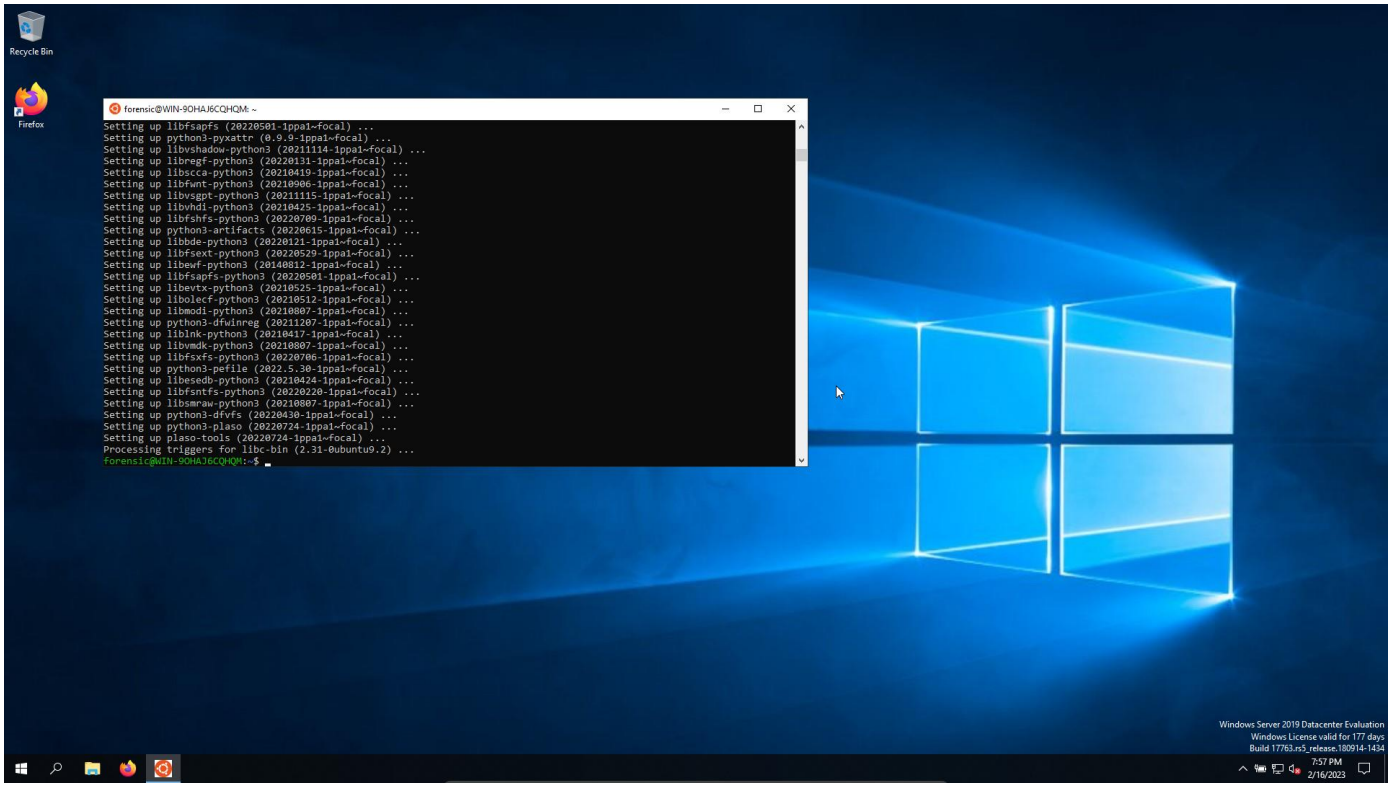
- Install Log2Timeline:
    - Add GIFT repository:



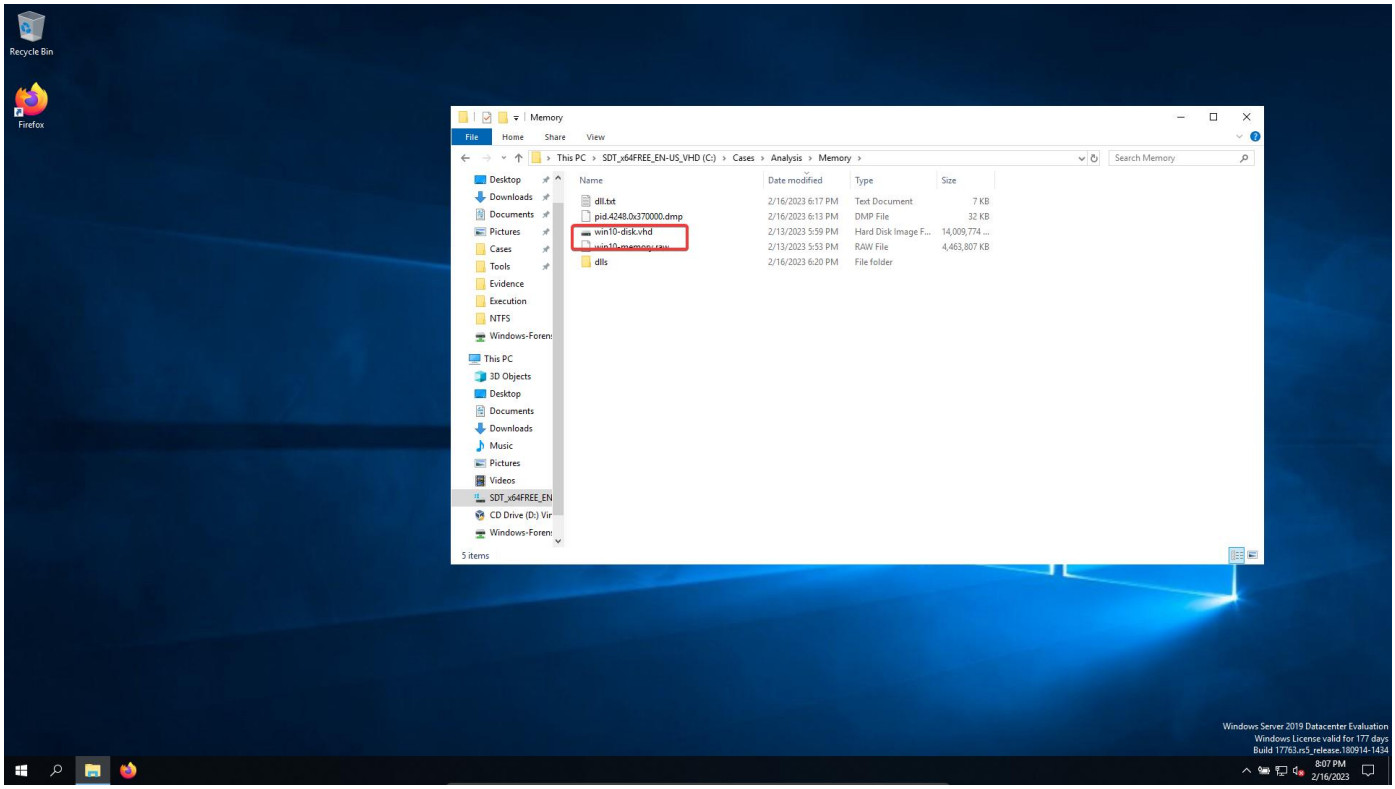


- Install plaso:



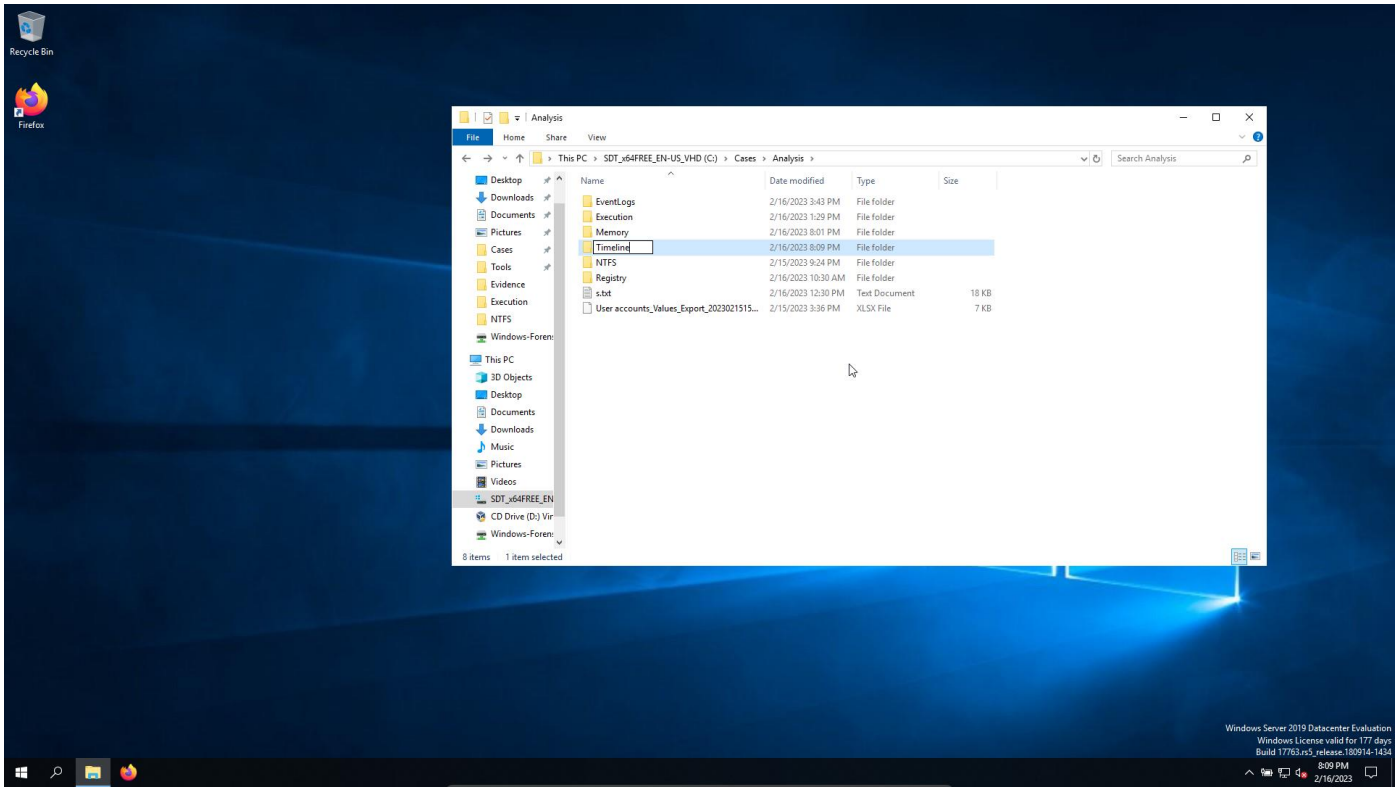


- Place memory and disk images under the same folder: C:\Cases\Analysis\Memory

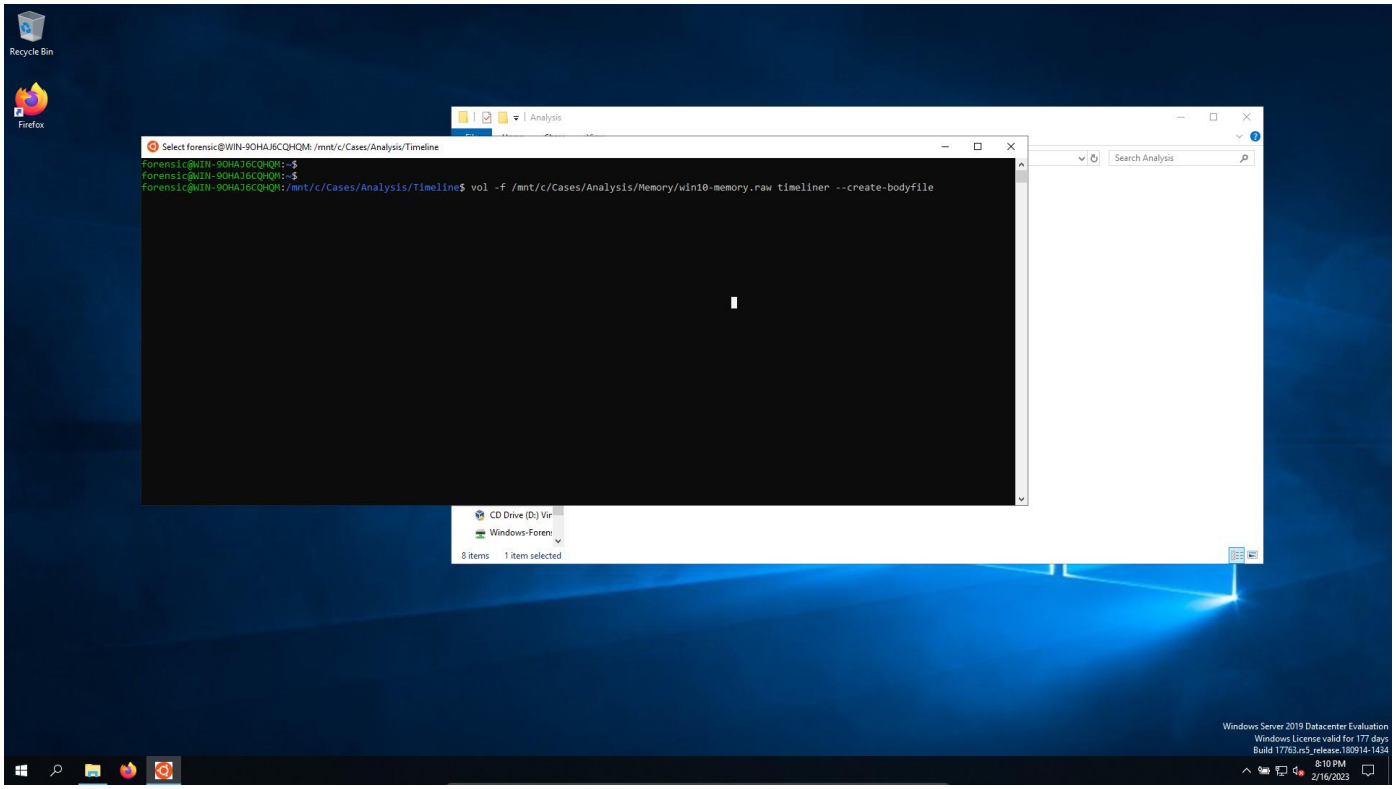


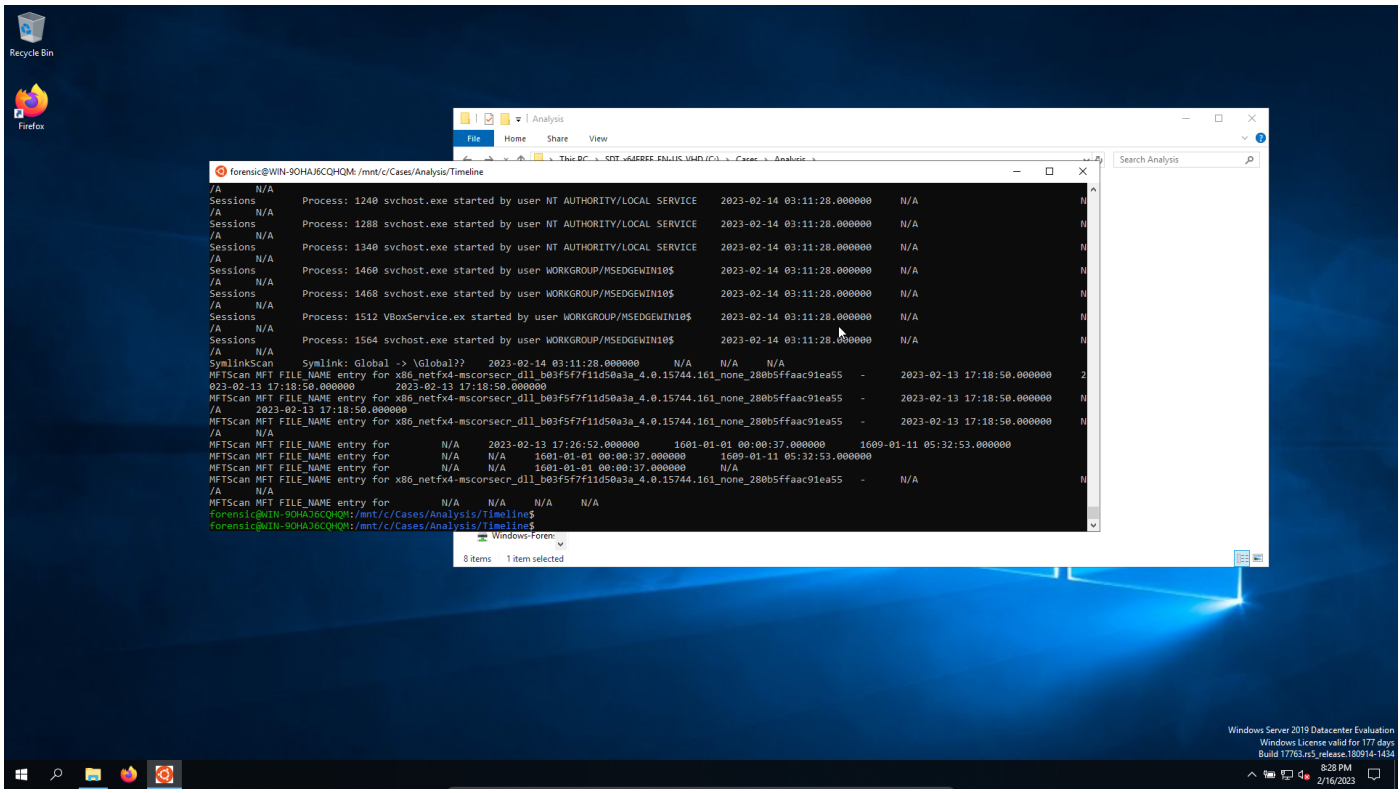
Memory timeline creation

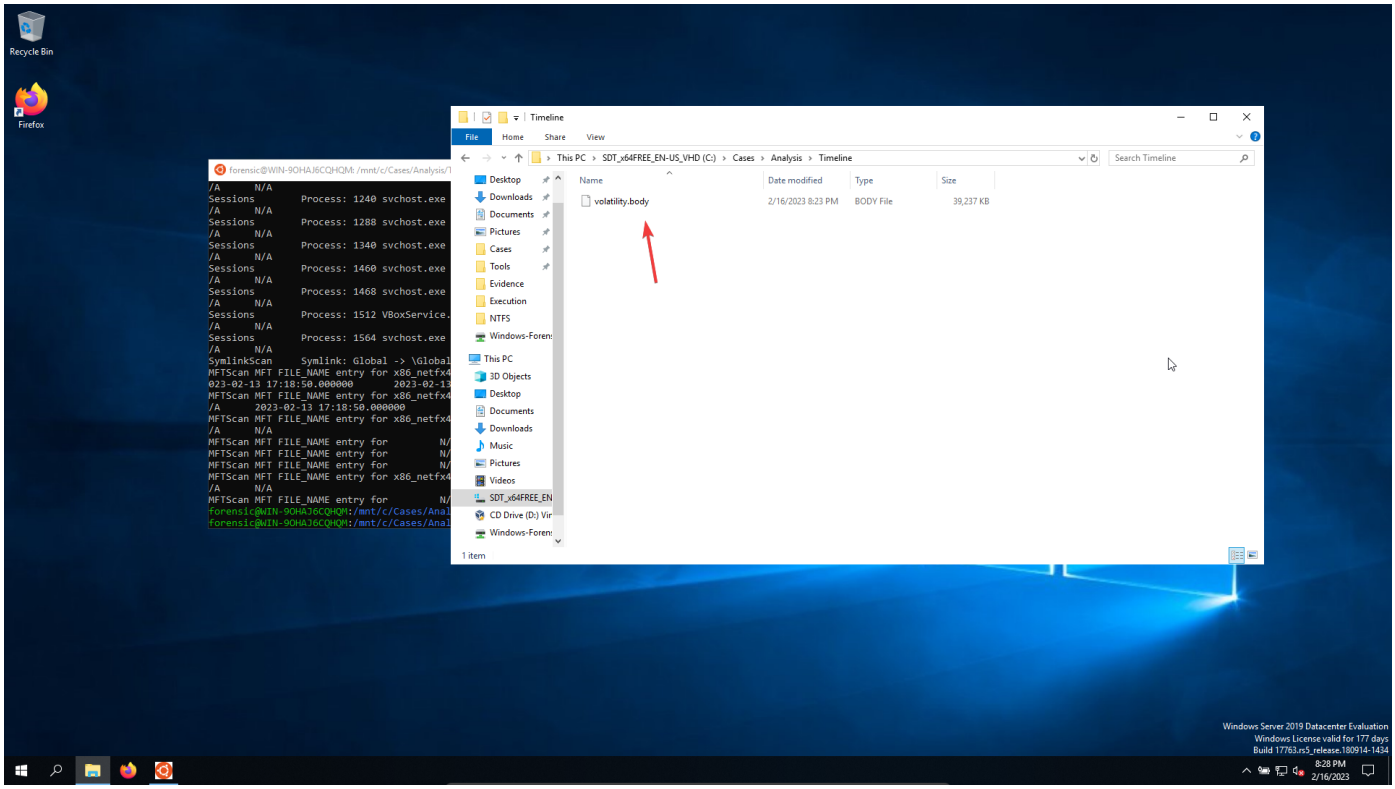
- Create folder Timeline in Analysis folder:



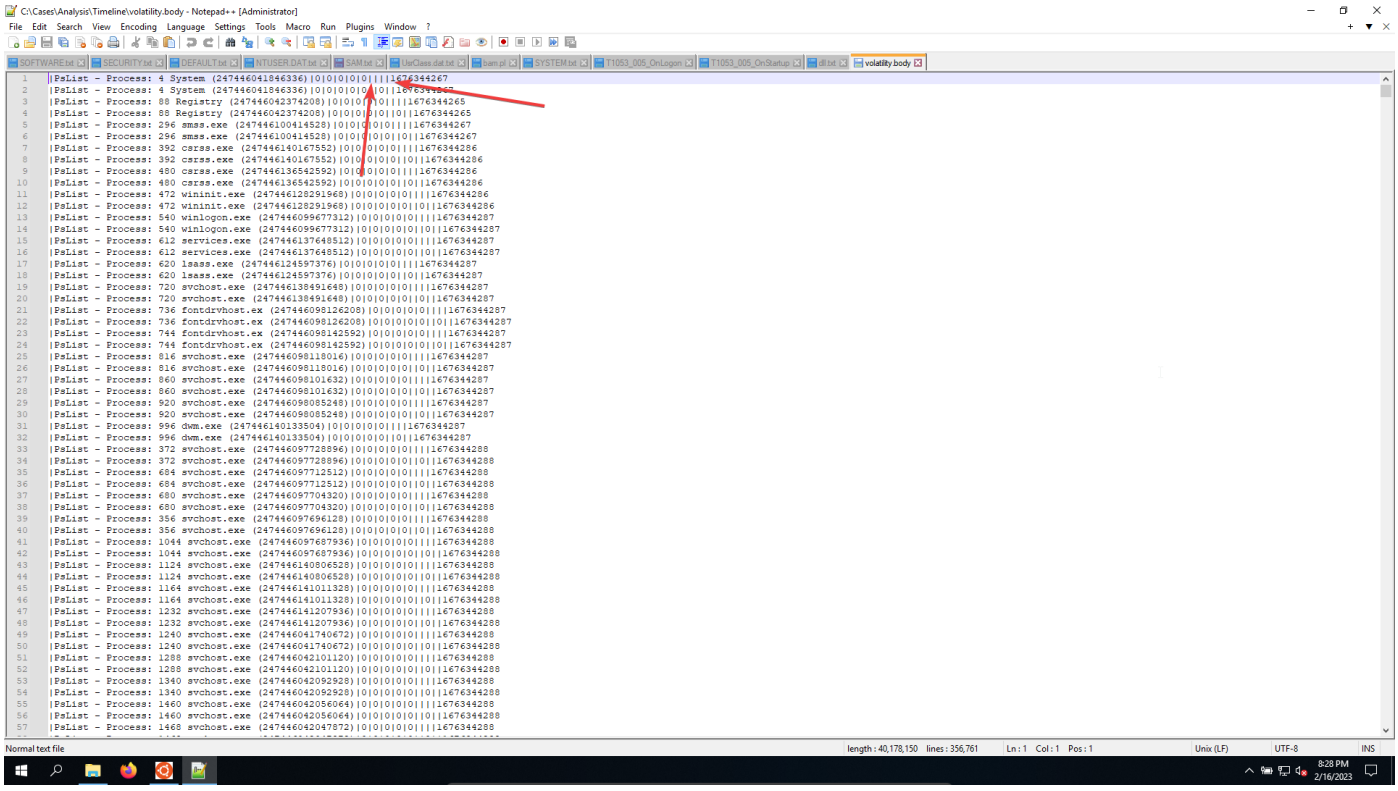
- Create bodyfile with volatility:

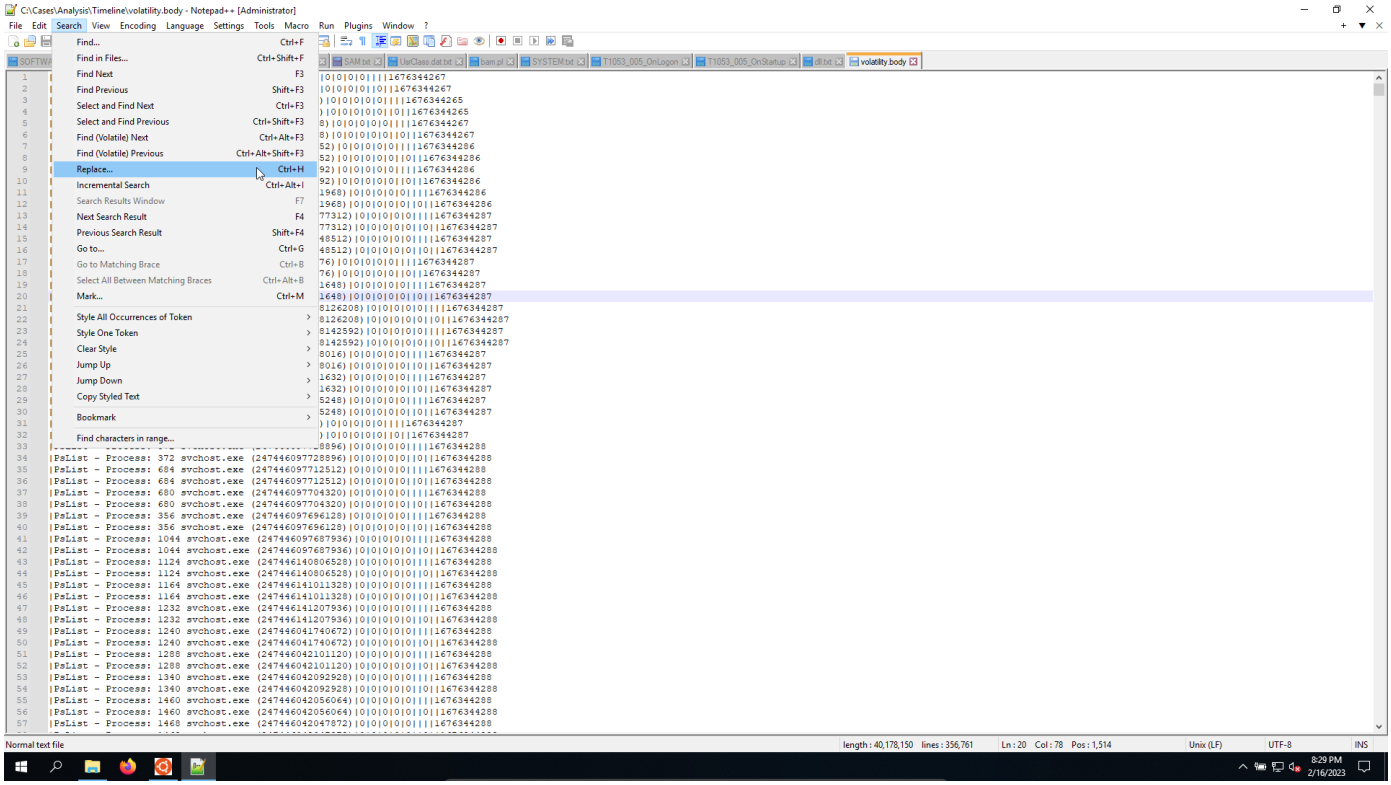


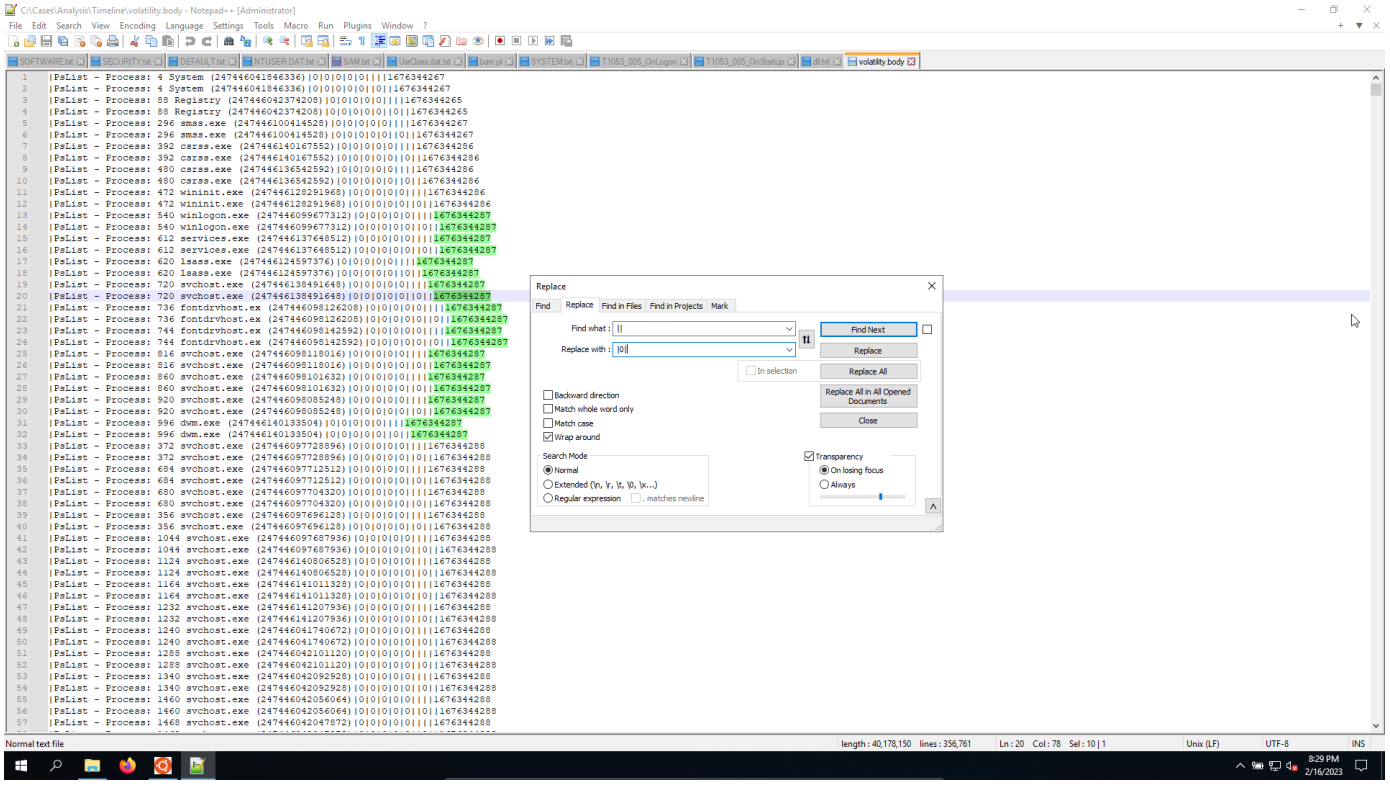




- Open it with notepad++ and change data representation:







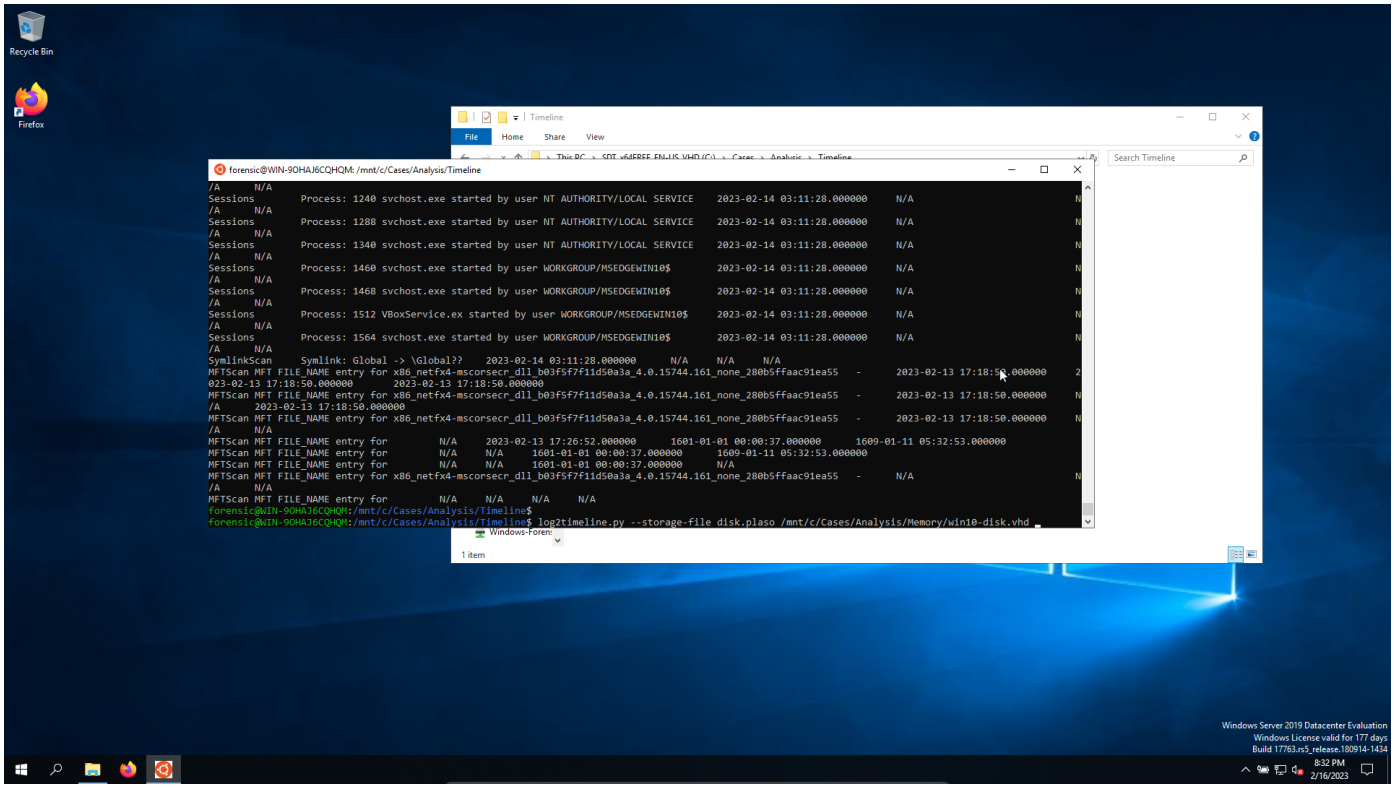
- Press two times, or untill:

  Replace All: 0 occurrences were replaced in entire file

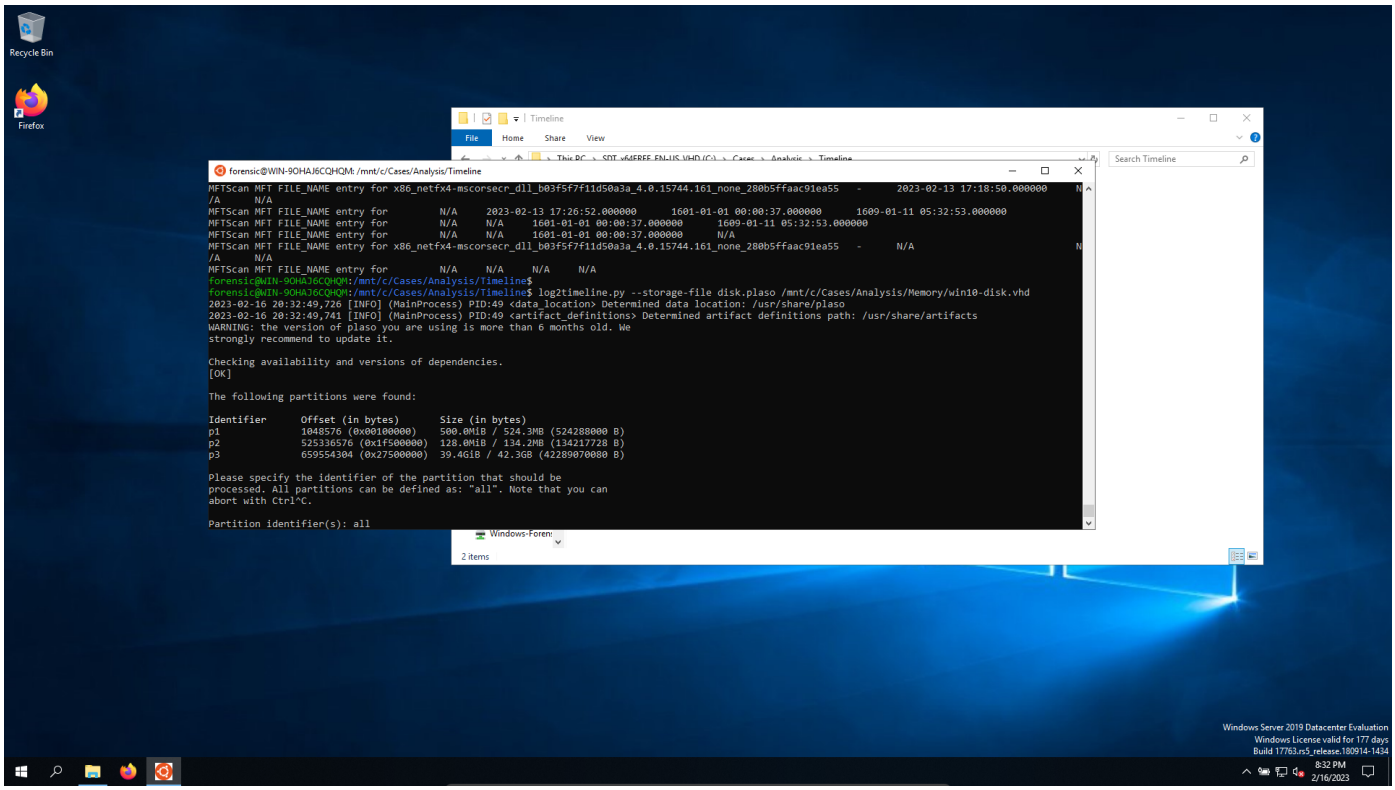
- Then save it.

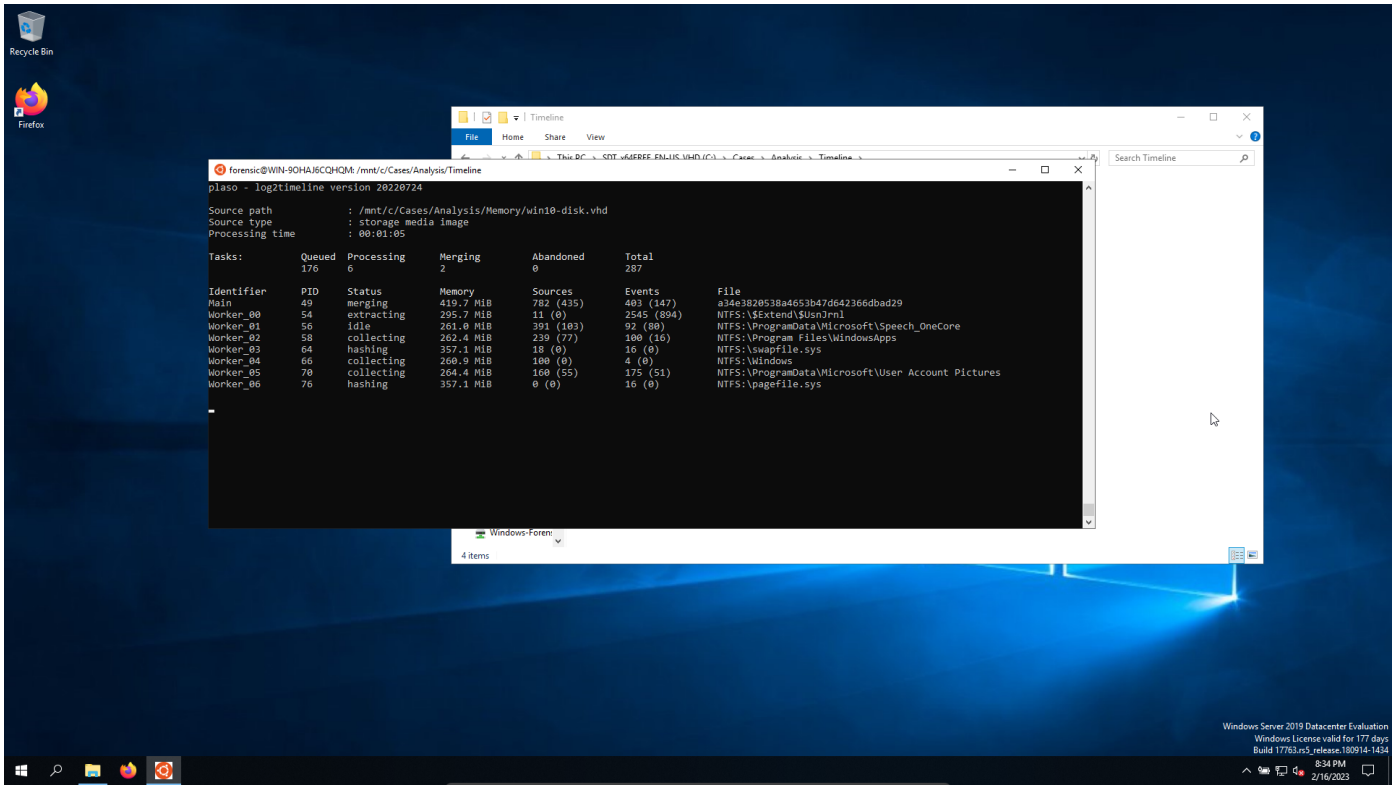
Disk timeline creation

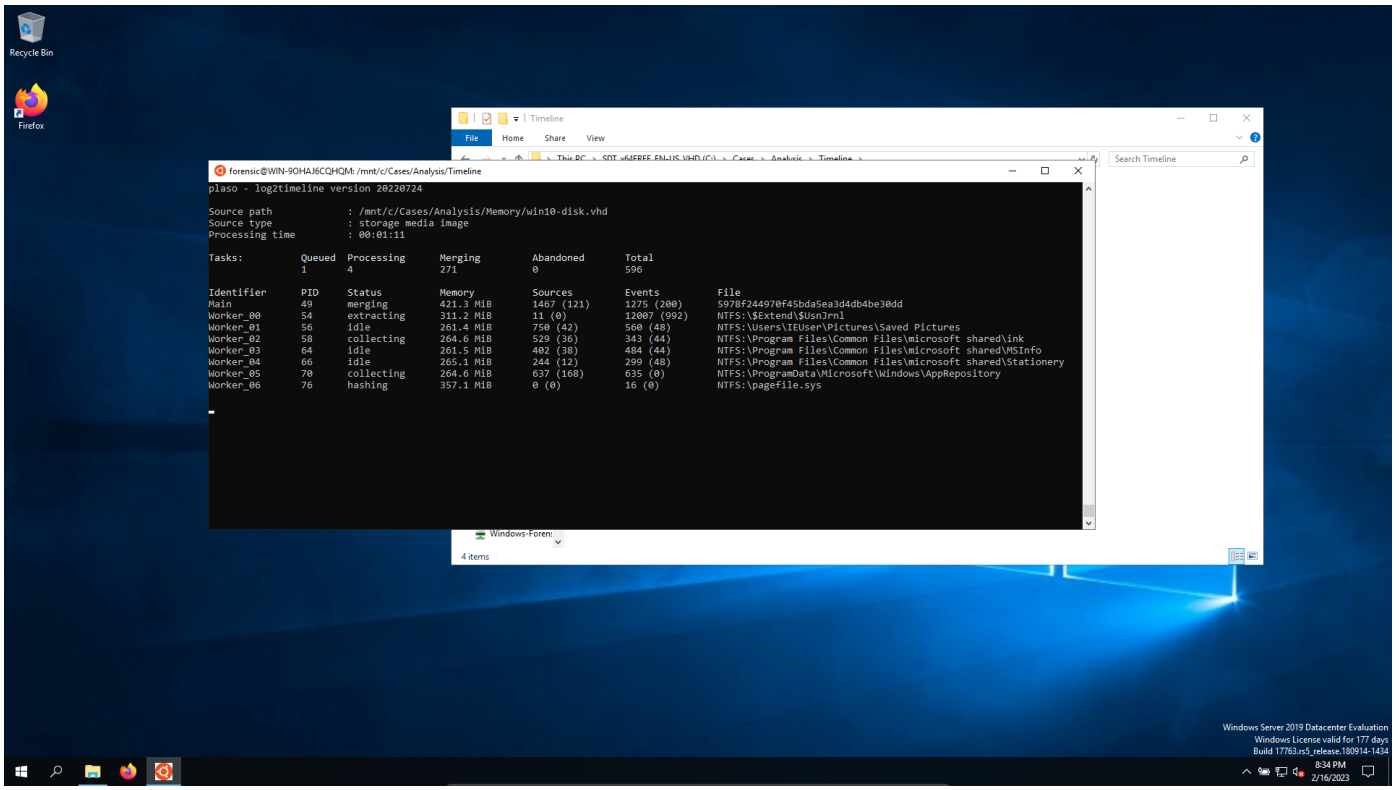
- Create .plaso file from .vhd:

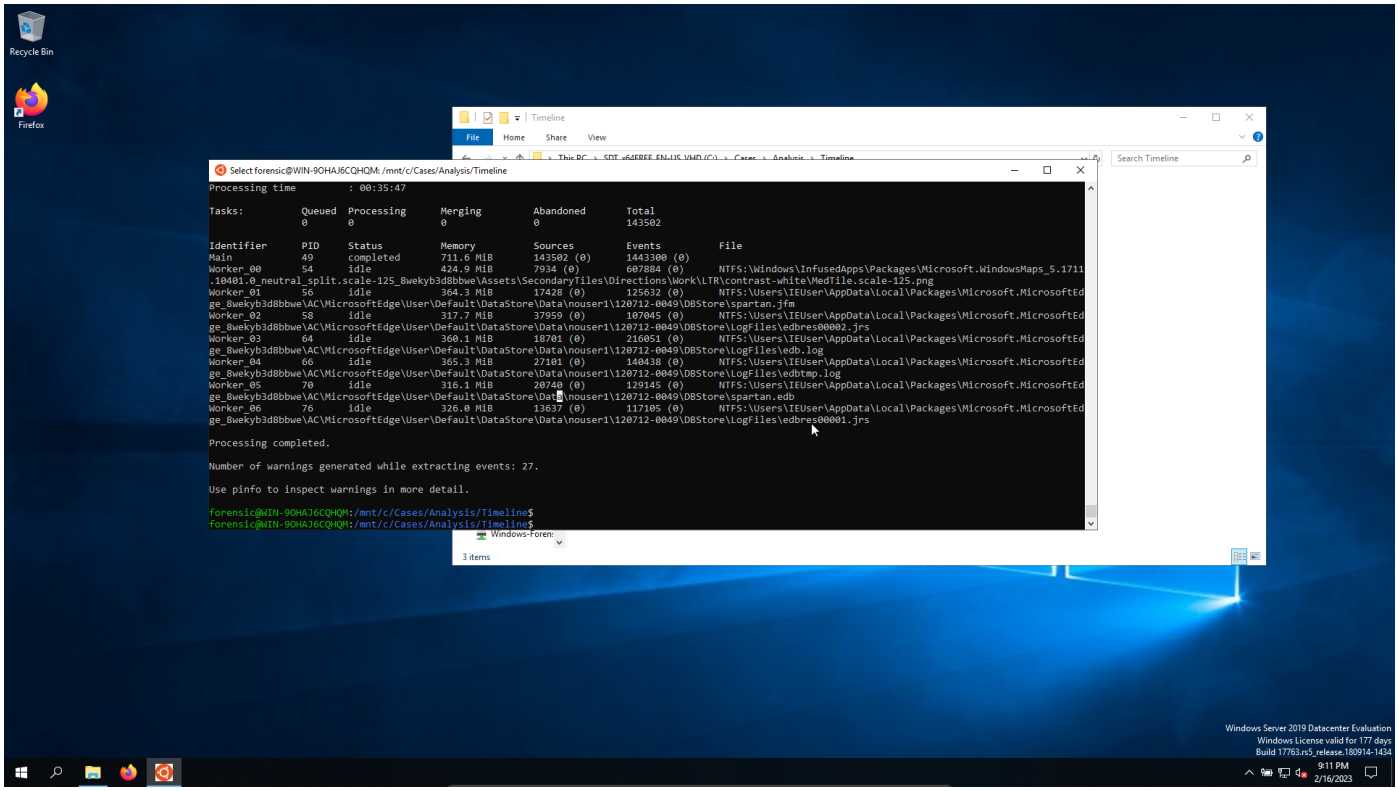


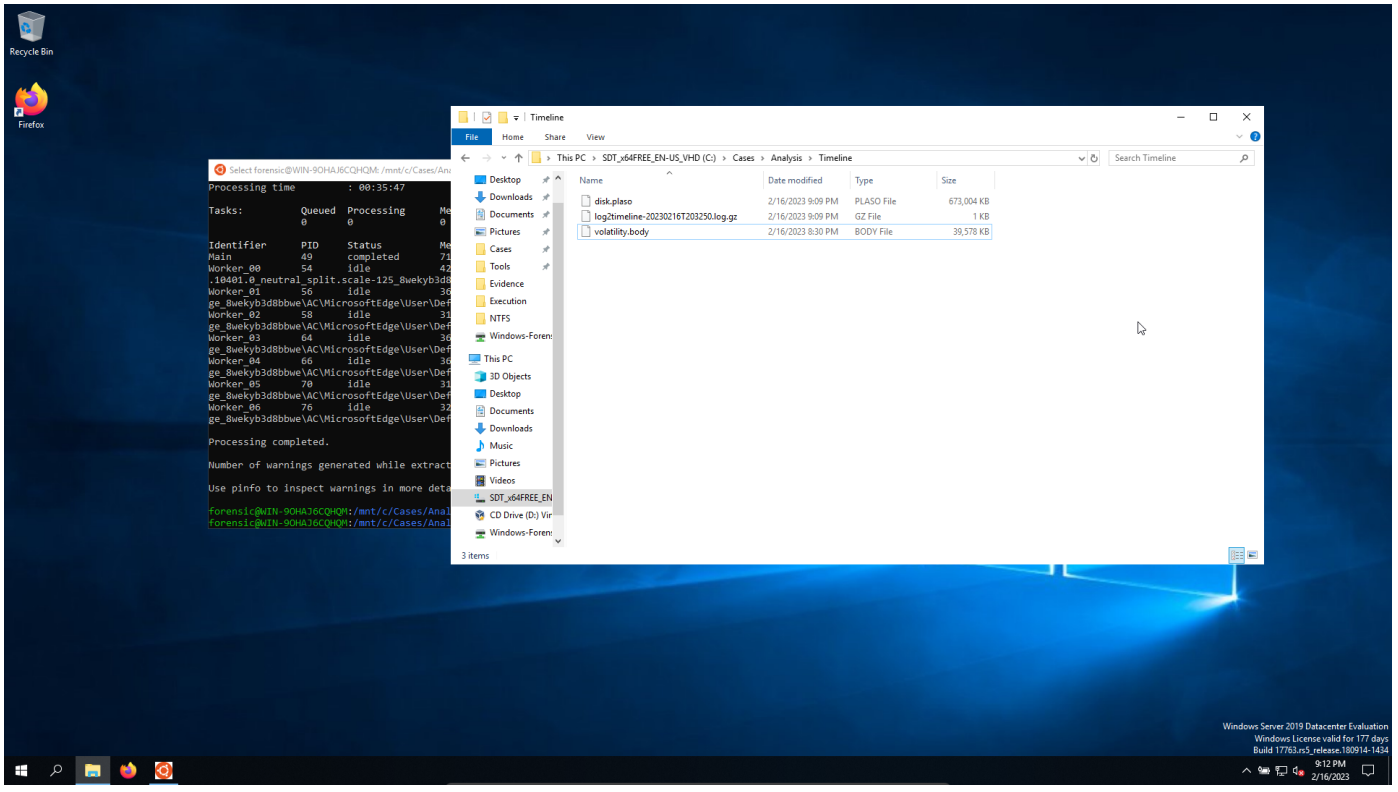
- Input all:



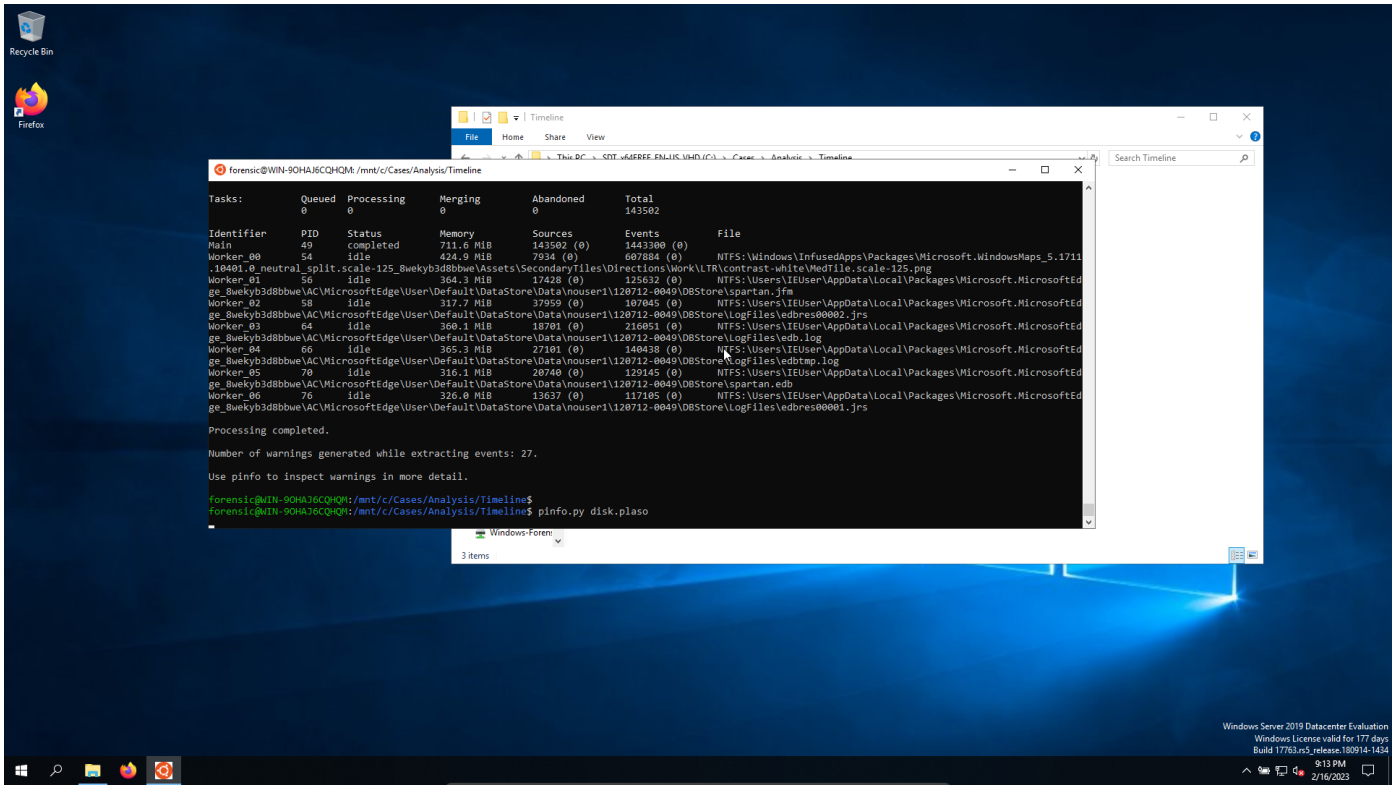

Recycle Bin
Firefox
Timeline
File
Home
Share
View
Search Timeline
4 items
forensic@WIN-9OHAJ6CQHQM: /mnt/c/Cases/Analysis/Timeline
plaso - log2timeline version 20220724
Source path : /mnt/c/Cases/Analysis/Memory/win10-disk.vhd
Source type : storage media image
Processing time : 00:01:05
Tasks: Queued Processing Merging Abandoned Total
176 6 2 0 287
Identifier PID Status Memory Sources Events File
Main 49 merging 419.7 MiB 782 (435) 403 (147) a34e3820538a4653b47d642366dbad29
Worker_00 54 extracting 295.7 MiB 11 (0) 2545 (894) NTFS:\$Extend\$UsnJrnl
Worker_01 56 idle 261.0 MiB 391 (103) 92 (80) NTFS:\ProgramData\Microsoft\Speech_OneCore
Worker_02 58 collecting 262.4 MiB 239 (77) 100 (16) NTFS:\Program Files\WindowsApps
Worker_03 64 hashing 357.1 MiB 18 (0) 16 (0) NTFS:\swapfile.sys
Worker_04 66 collecting 260.9 MiB 100 (0) 4 (0) NTFS:\Windows
Worker_05 70 collecting 264.4 MiB 160 (55) 175 (51) NTFS:\ProgramData\Microsoft\User Account Pictures
Worker_06 76 hashing 357.1 MiB 0 (0) 16 (0) NTFS:\pagefile.sys
Windows Server 2019 Datacenter Evaluation
Windows License valid for 177 days
Build 17763.rs5_release.180914-1434
8:34 PM
2/16/2023

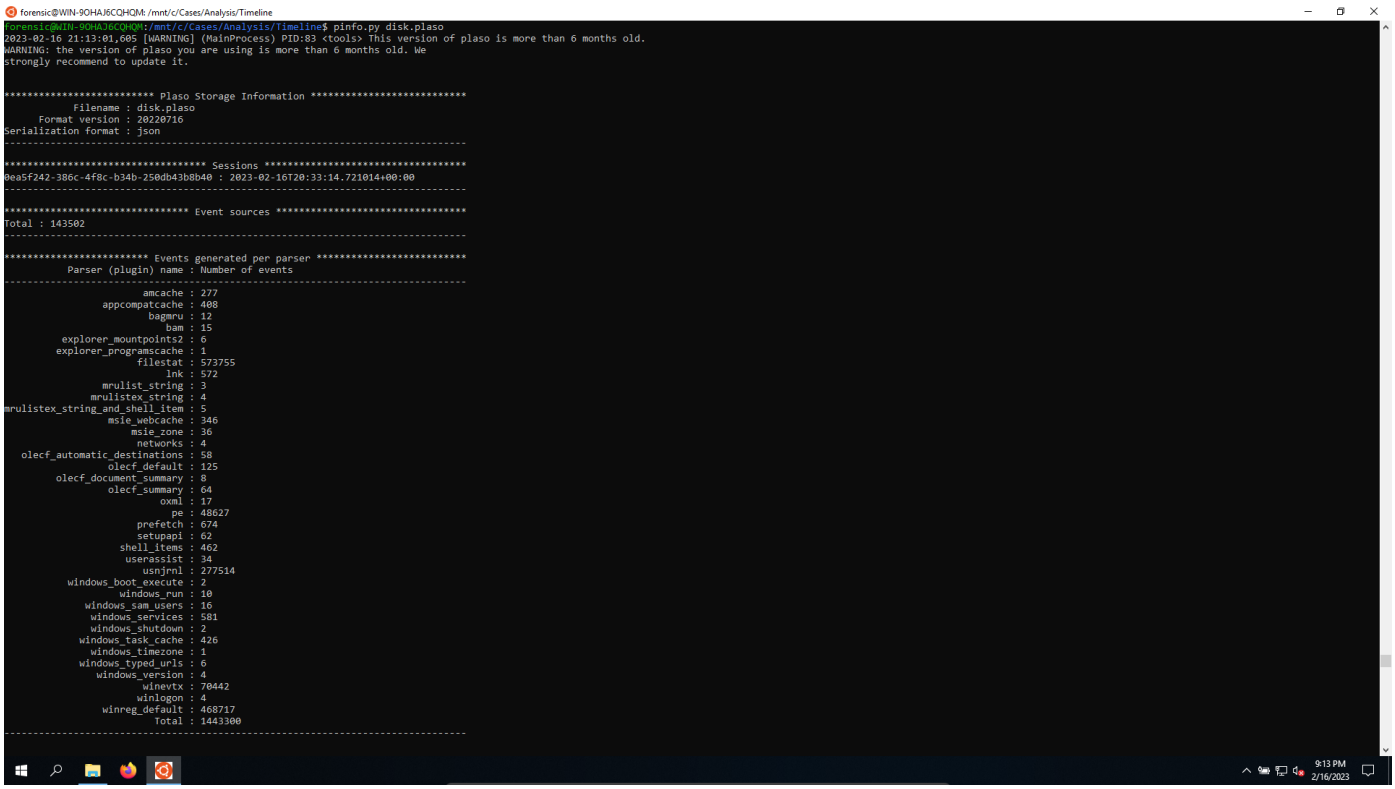

Recycle Bin
Firefox
Timeline
File
Home
Share
View
Search Timeline
4 items
forensic@WIN-9OHAJ6CQHQM: /mnt/c/Cases/Analysis/Timeline
plaso - log2timeline version 20220724
Source path : /mnt/c/Cases/Analysis/Memory/win10-disk.vhd
Source type : storage media image
Processing time : 00:01:11
Tasks: Queued Processing Merging Abandoned Total
1 4 271 0 596
Identifier PID Status Memory Sources Events File
Main 49 merging 421.3 MiB 1467 (121) 1275 (200) 5978f244970f45bda5ea3d4db4be30dd
Worker_00 54 extracting 311.2 MiB 11 (0) 12007 (992) NTFS:\$Extend\$UsnJrnl
Worker_01 56 idle 261.4 MiB 750 (42) 560 (48) NTFS:\Users\IEUser\Pictures\Saved Pictures
Worker_02 58 collecting 264.6 MiB 529 (36) 343 (44) NTFS:\Program Files\Common Files\microsoft shared\ink
Worker_03 64 idle 261.5 MiB 402 (38) 484 (44) NTFS:\Program Files\Common Files\microsoft shared\MSInfo
Worker_04 66 idle 265.1 MiB 244 (12) 299 (48) NTFS:\Program Files\Common Files\microsoft shared\Stationery
Worker_05 70 collecting 264.6 MiB 637 (168) 635 (0) NTFS:\ProgramData\Microsoft\Windows\AppRepository
Worker_06 76 hashing 357.1 MiB 0 (0) 16 (0) NTFS:\pagefile.sys
Windows Server 2019 Datacenter Evaluation
Windows License valid for 177 days
Build 17763.rs5_release.180914-1434
8:34 PM
2/16/2023





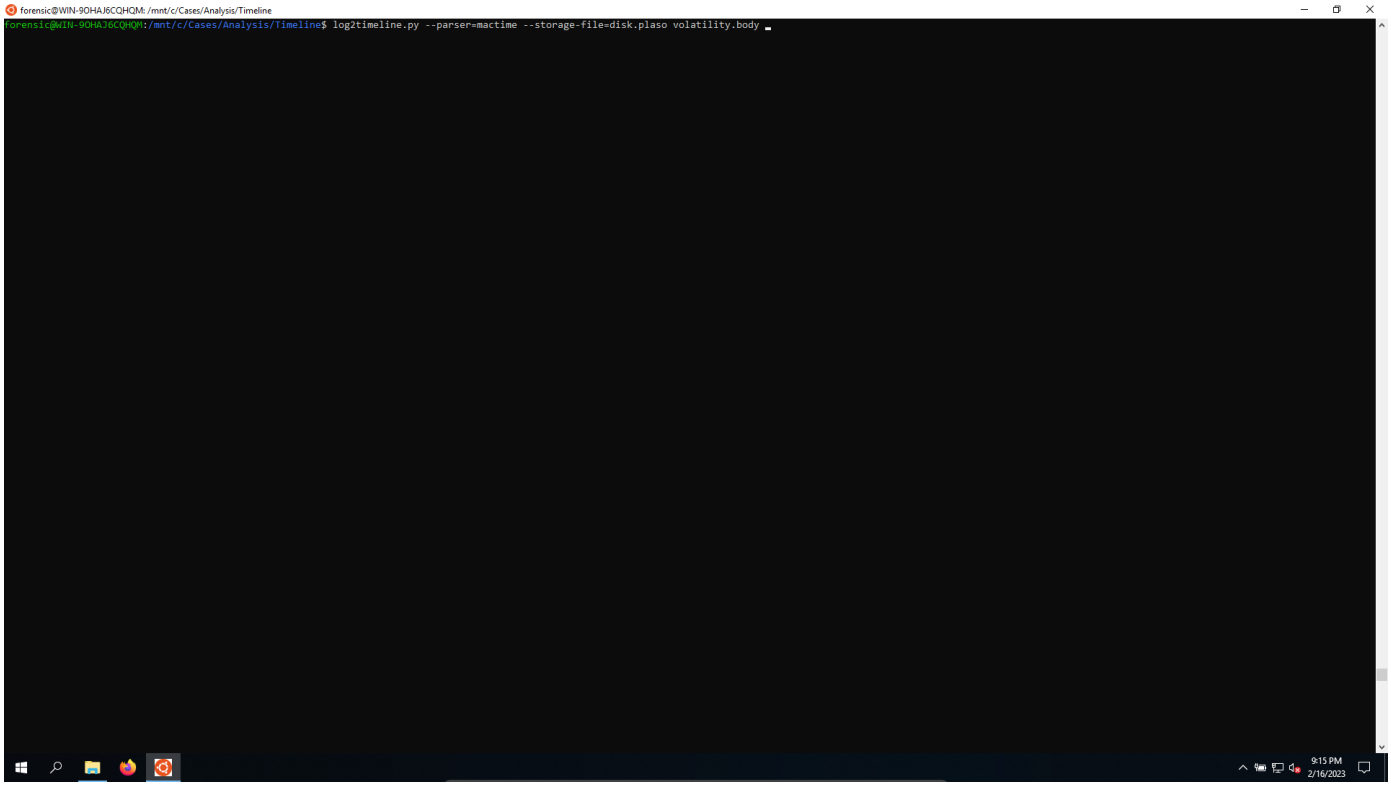
- Print some information about the plaso file:

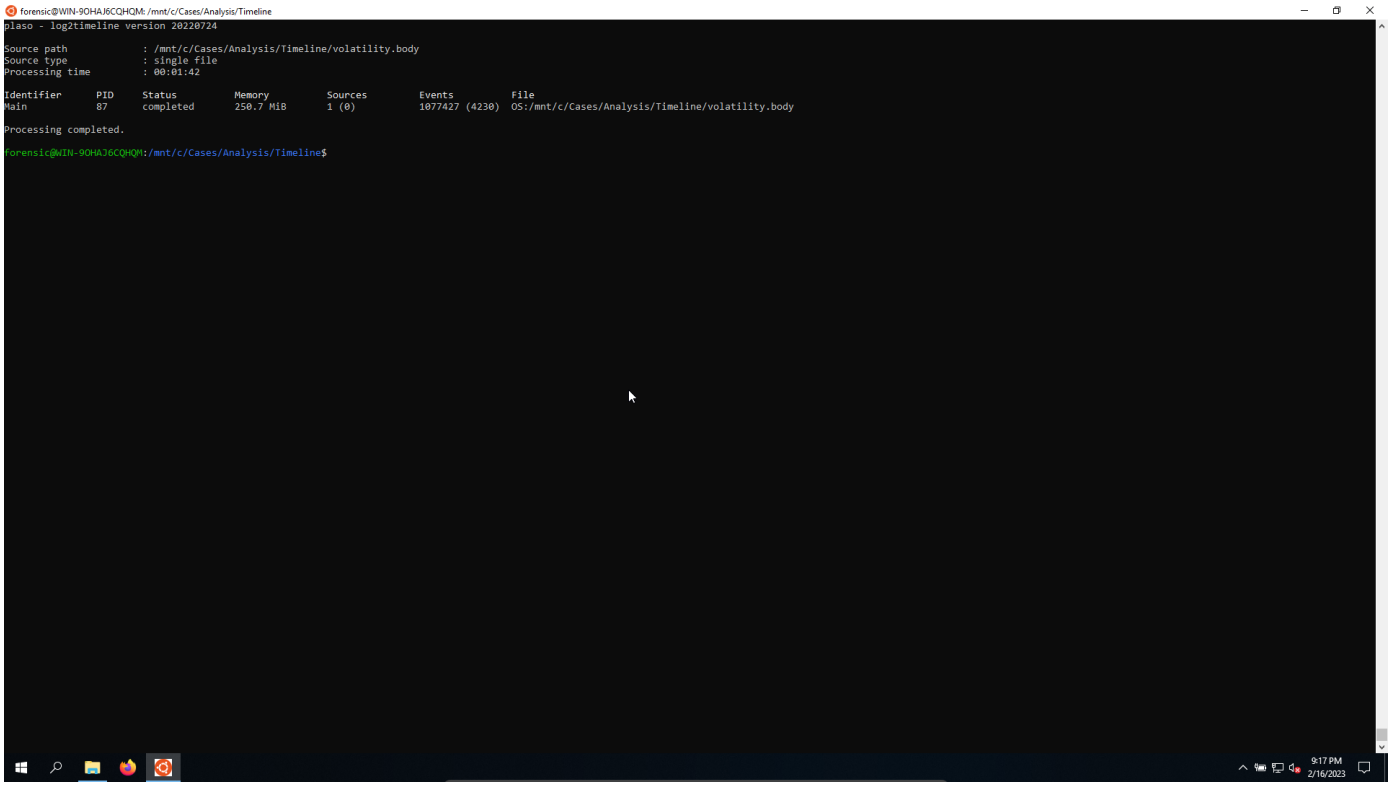


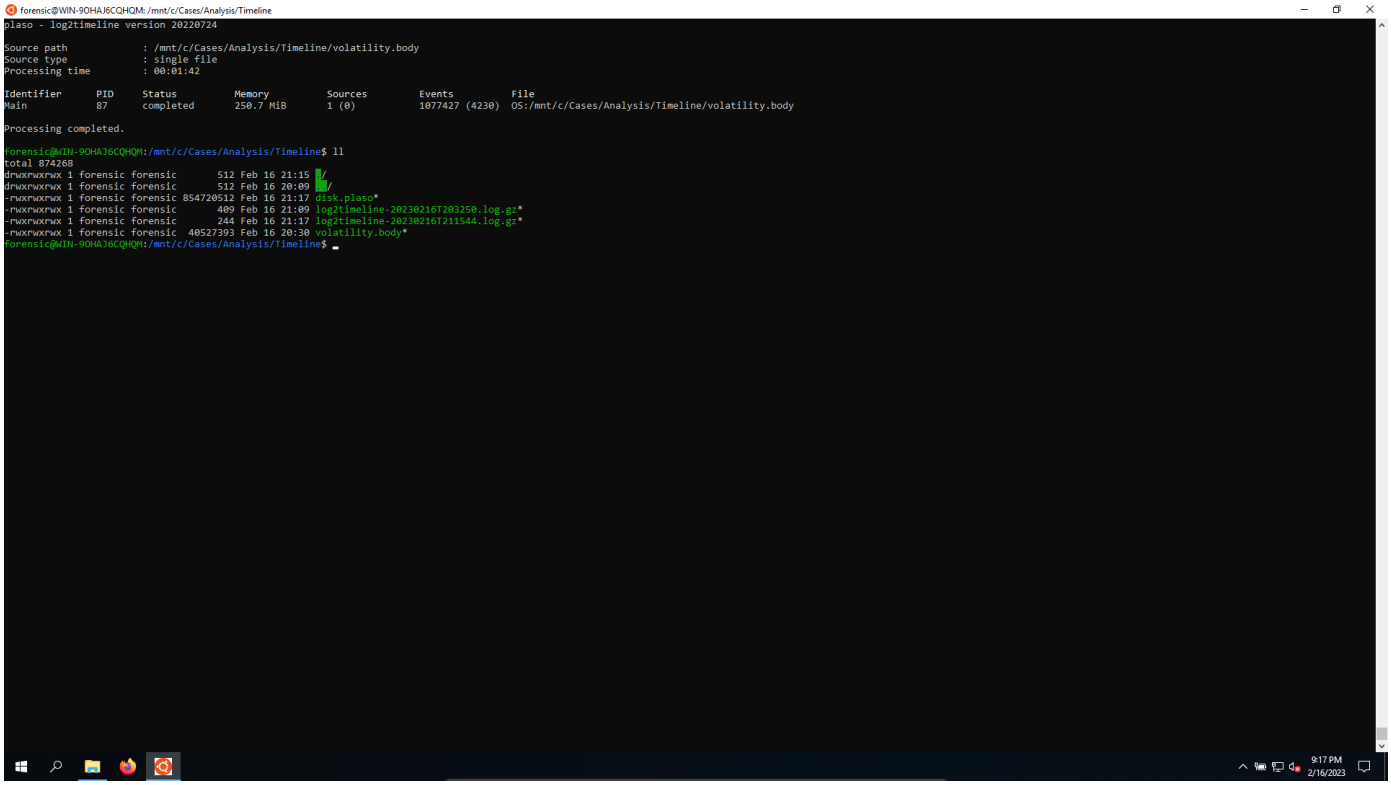


Merging timelines

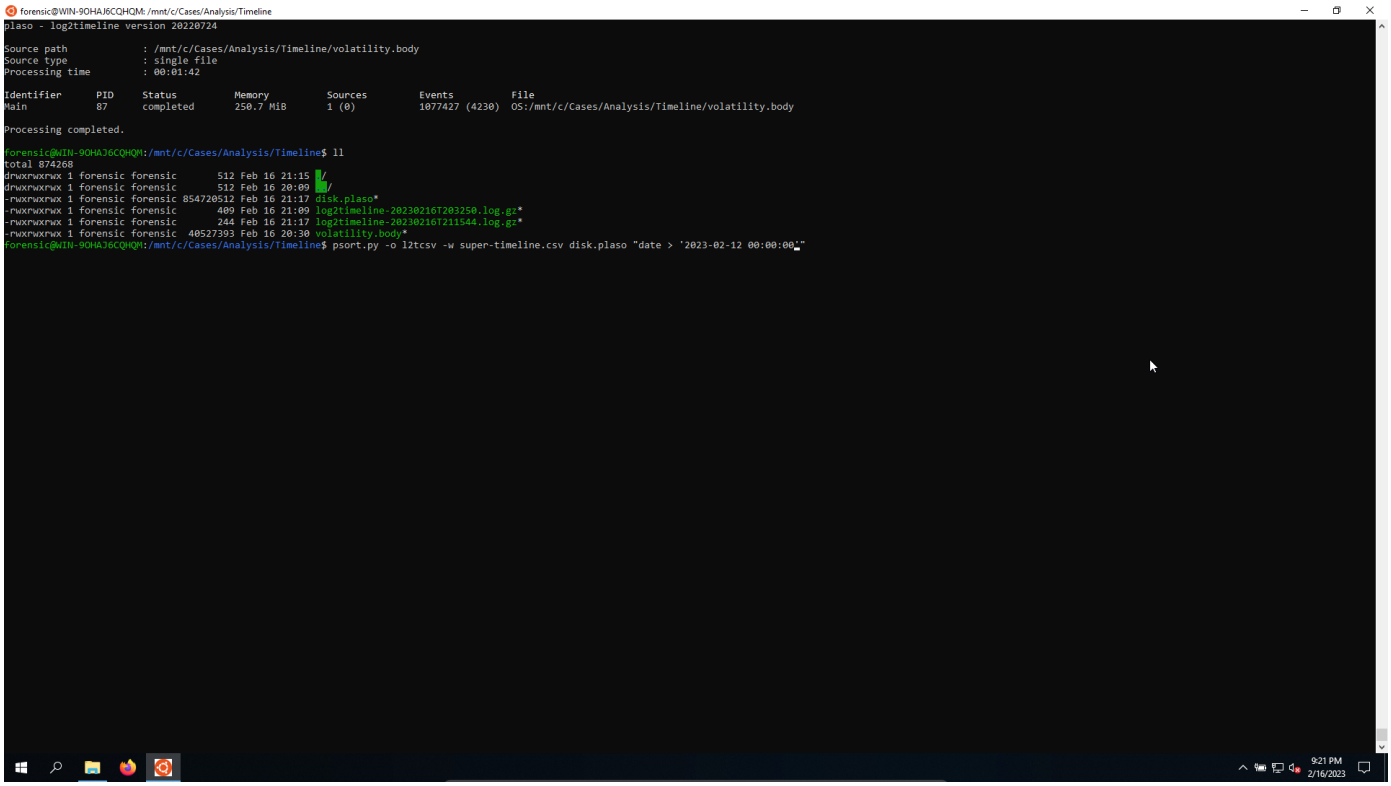
- Merging the two files with mactime, take bodyfile and merge it in the plaso file:

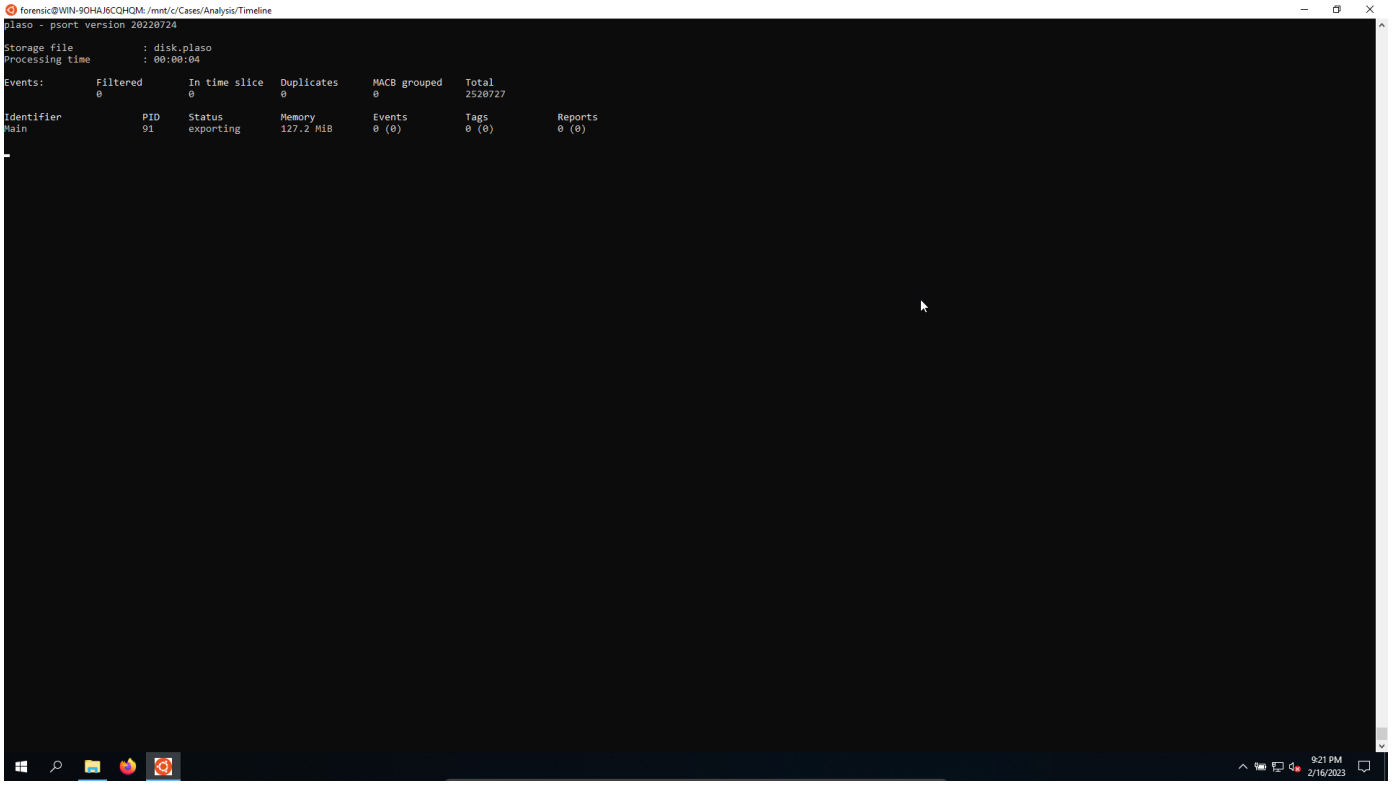


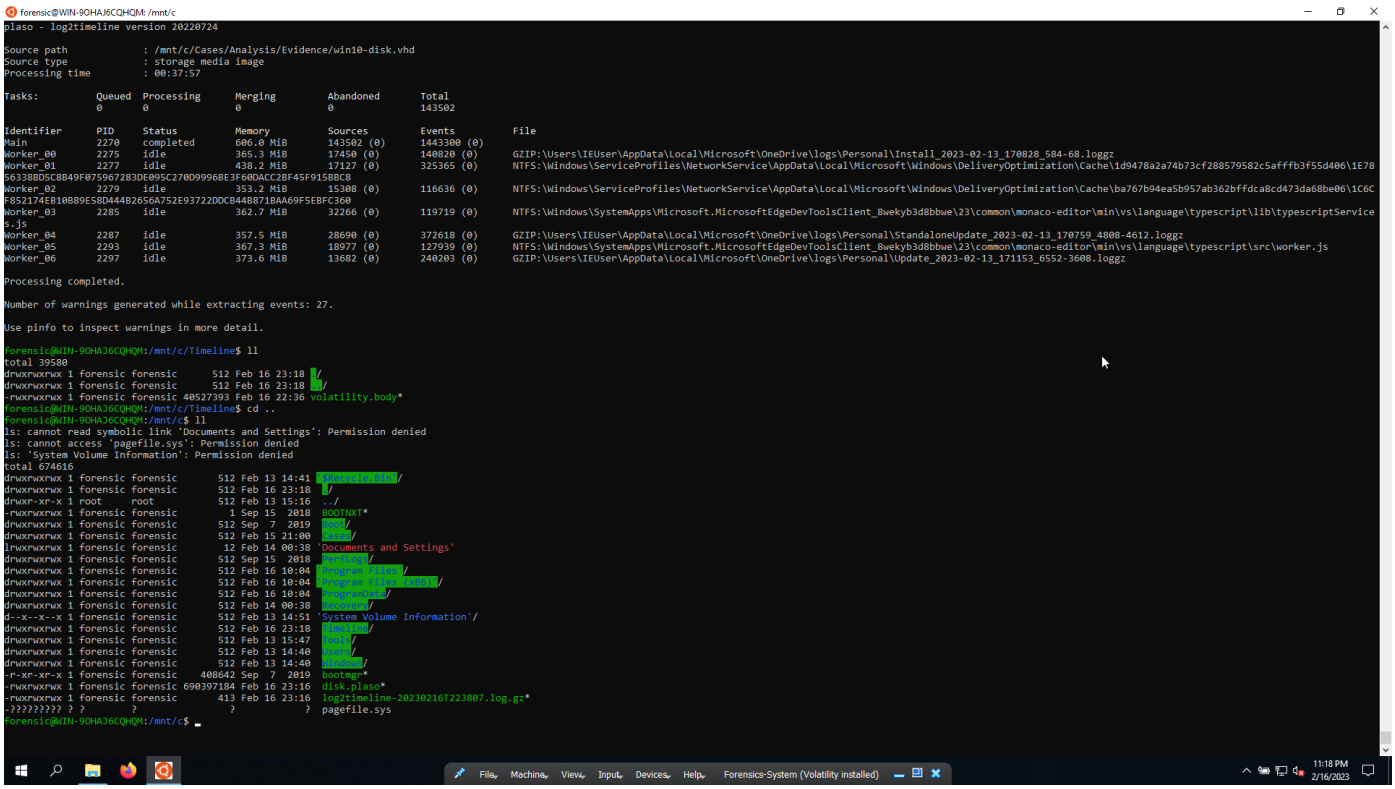




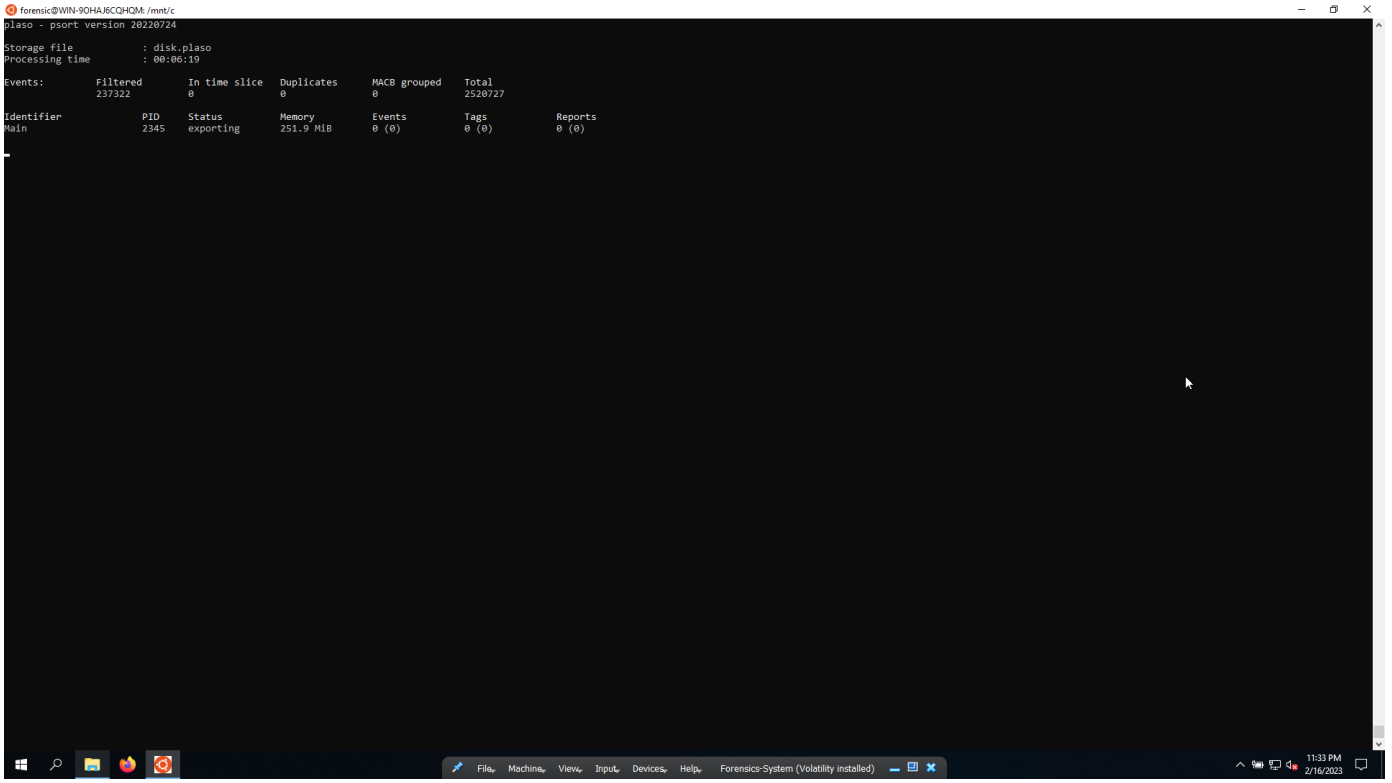
- Convert plaso file to csv and input the date when the attack happened:

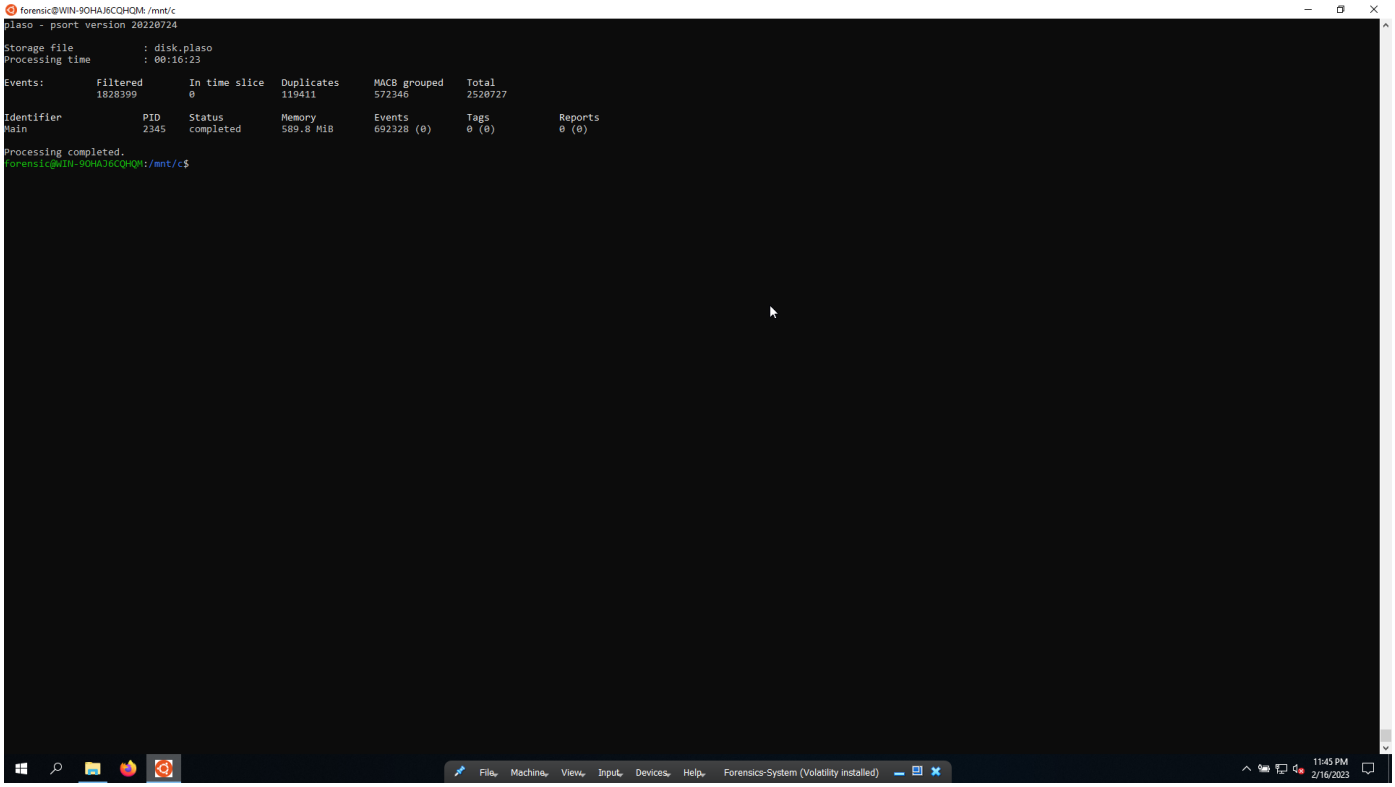


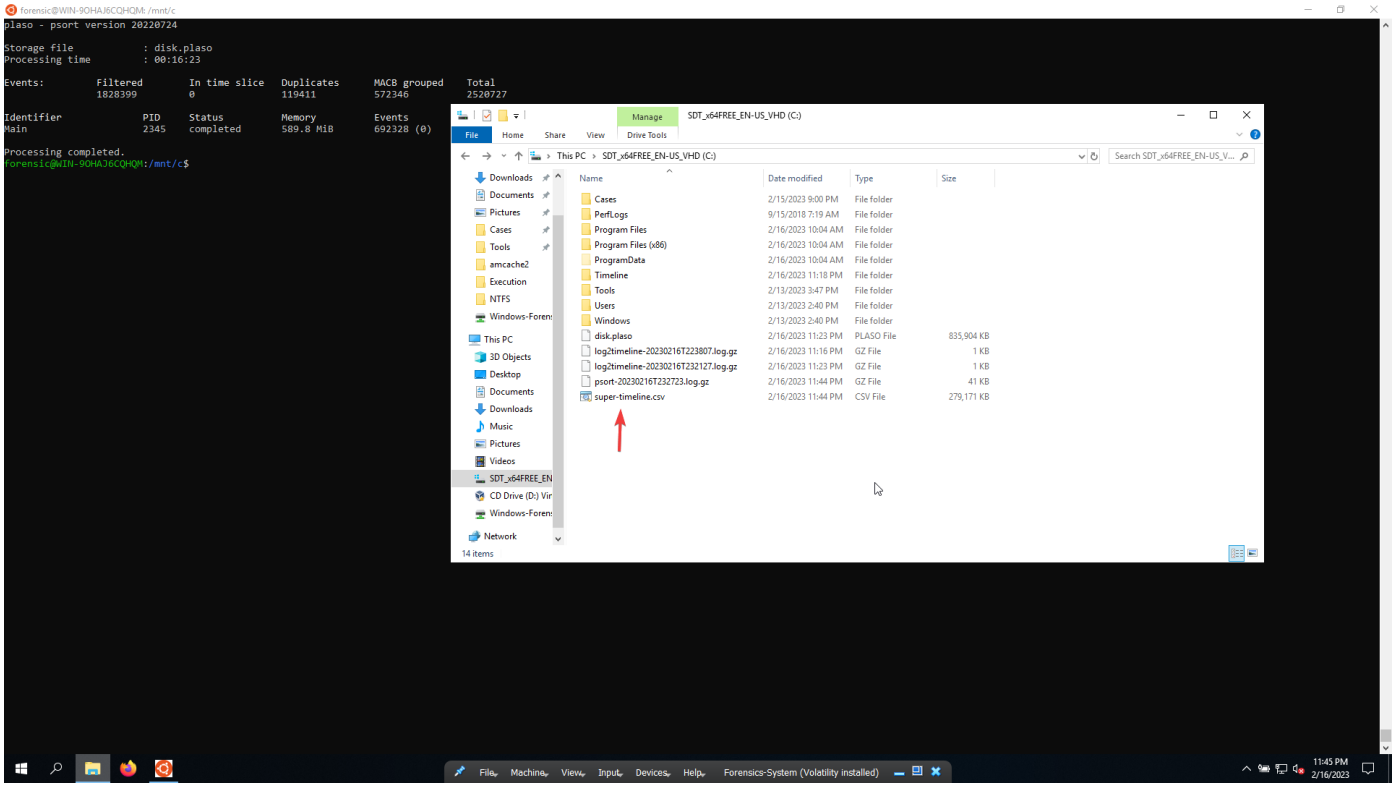




- If the memory doesn’t increase or values changing, just wait a little more, it has a cold start.

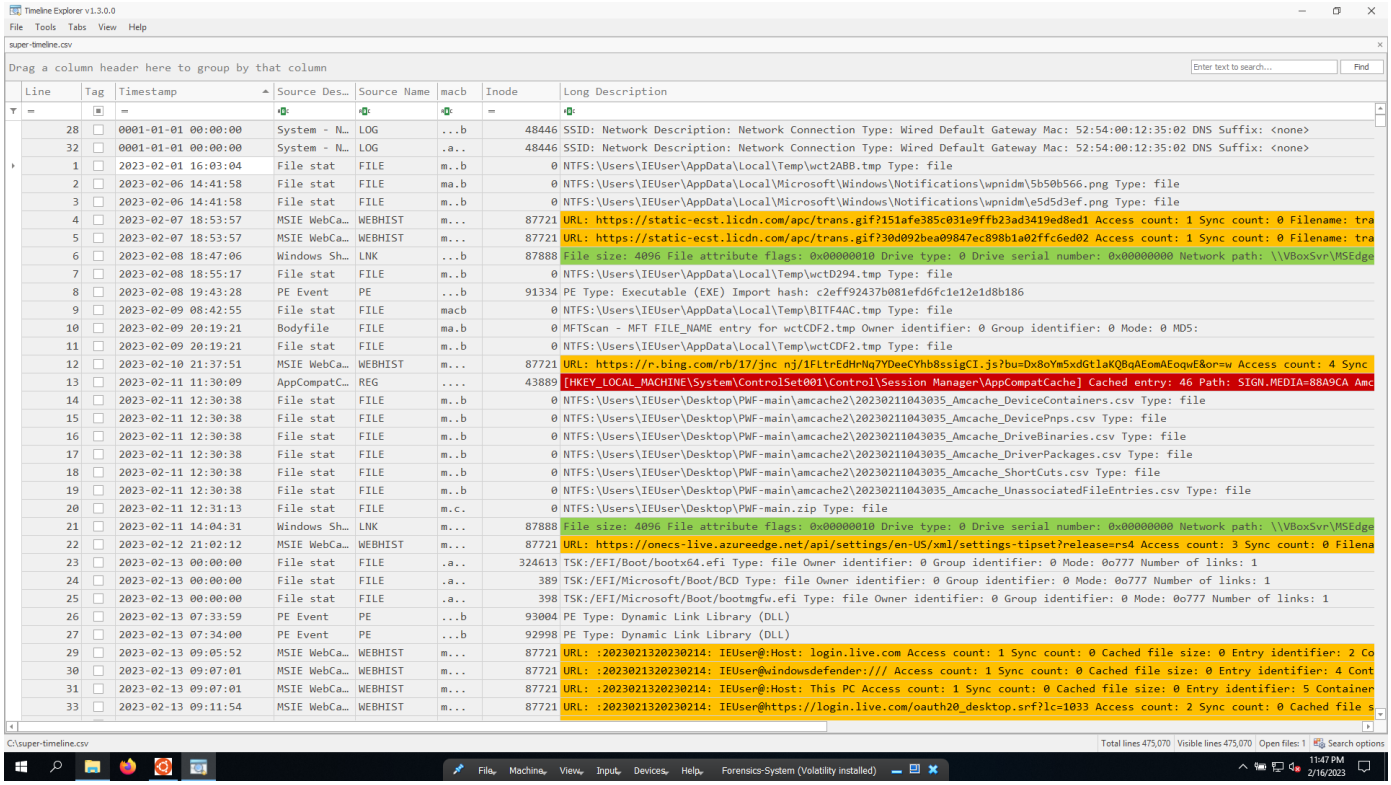

forensic@WIN-9OHAJ6CQHQM: /mnt/c
plaso - psort version 20220724
Storage file : disk.plaso
Processing time : 00:06:19
Events: Filtered In time slice Duplicates MACB grouped Total
237322 0 0 0 2520727
Identifier PID Status Memory Events Tags Reports
Main 2345 exporting 251.9 MiB 0 (0) 0 (0) 0 (0)
File Machine View Input Devices Help Forensics-System (Volatility installed)
11:33 PM
2/16/2023

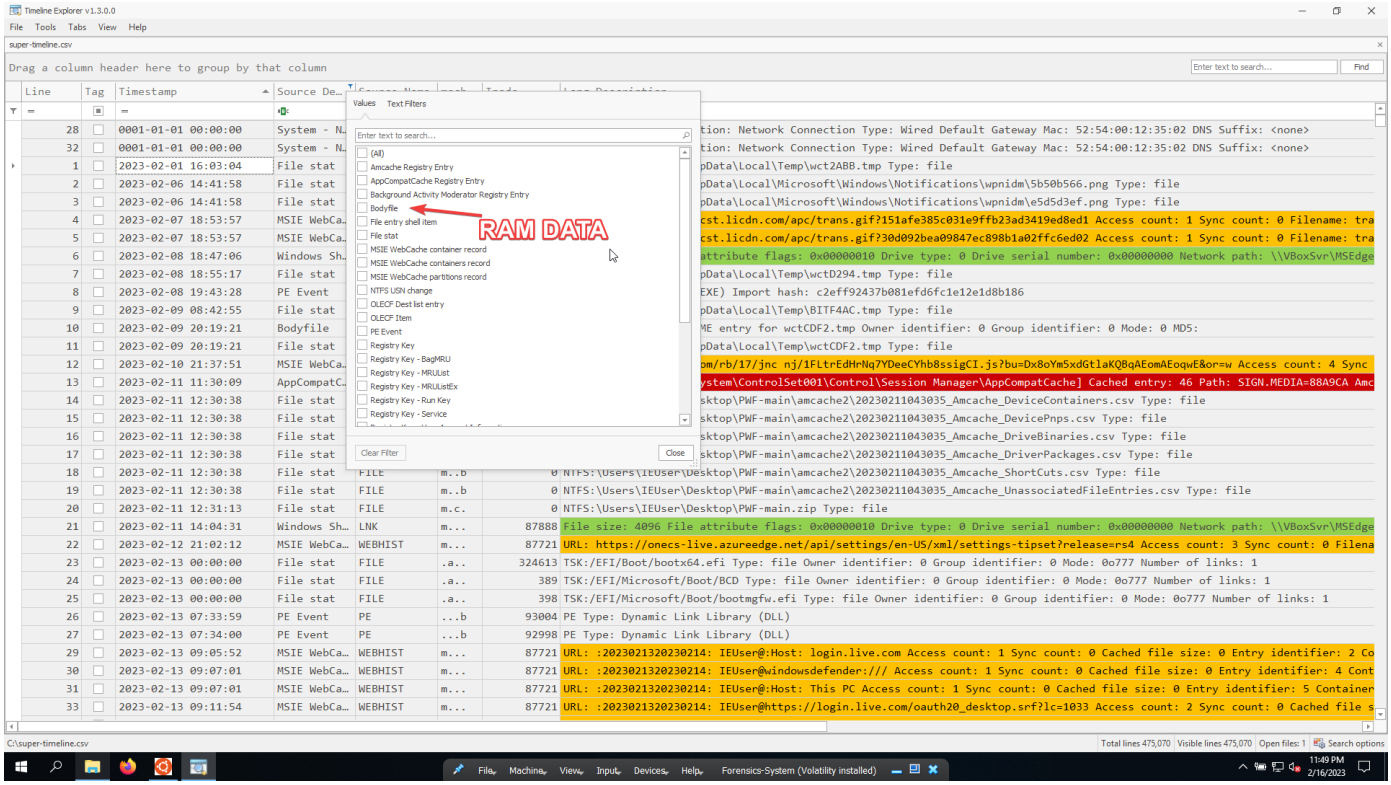

forensic@WIN-9OHAJ6CQHQM: /mnt/c
plaso - psort version 20220724
Storage file : disk.plaso
Processing time : 00:16:23
Events: Filtered In time slice Duplicates MACB grouped Total
1828399 0 119411 572346 2520727
Identifier PID Status Memory Events Tags Reports
Main 2345 completed 589.8 MiB 692328 (0) 0 (0) 0 (0)
Processing completed.
forensic@WIN-9OHAJ6CQHQM:/mnt/c$
File Machine View Input Devices Help Forensics-System (Volatility installed)
11:45 PM
2/16/2023



Super timeline view with Timeline explorer

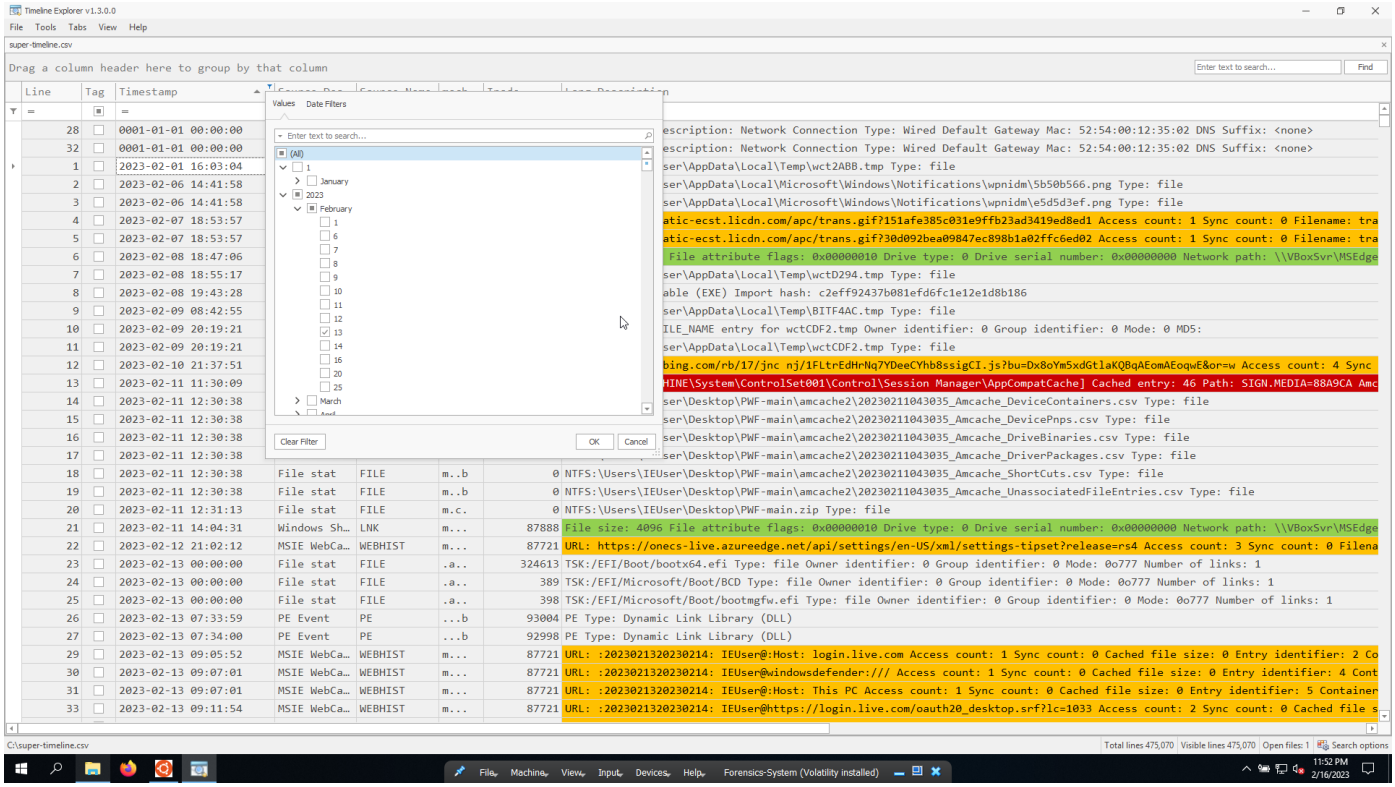
- A super timeline is a combination of disk and memory timelines.

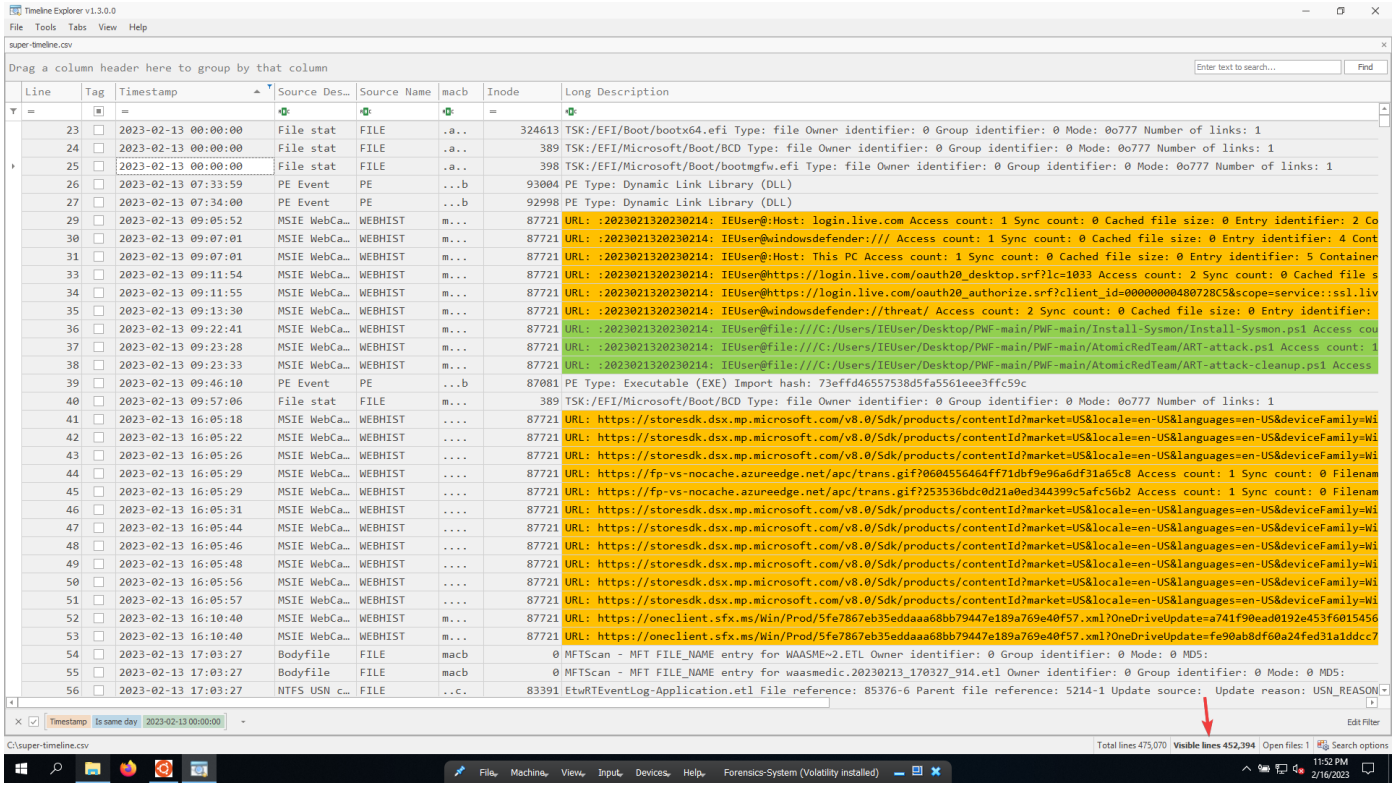




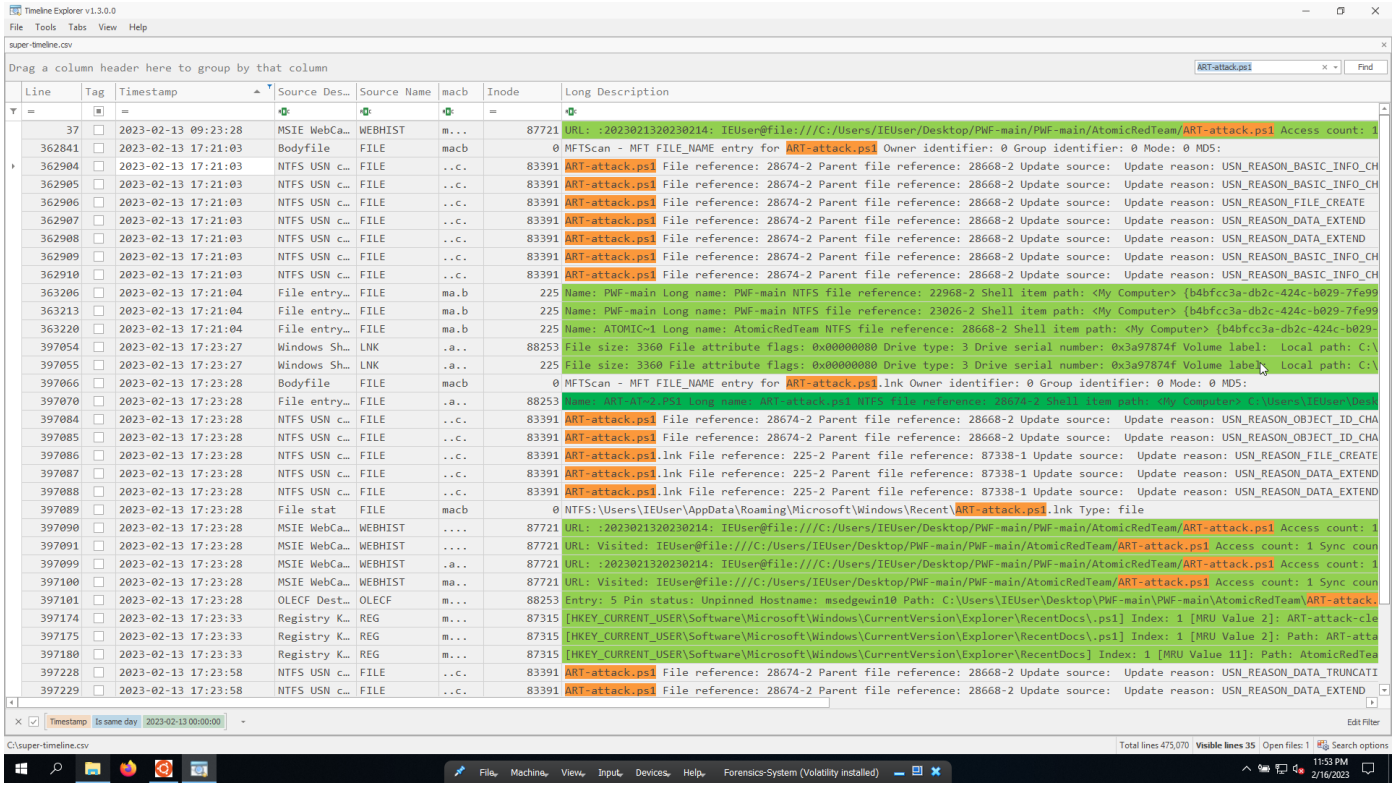
Analyzing malicious activity based on Super Timeline

- Filter timestamps on the day of the cyber attack:

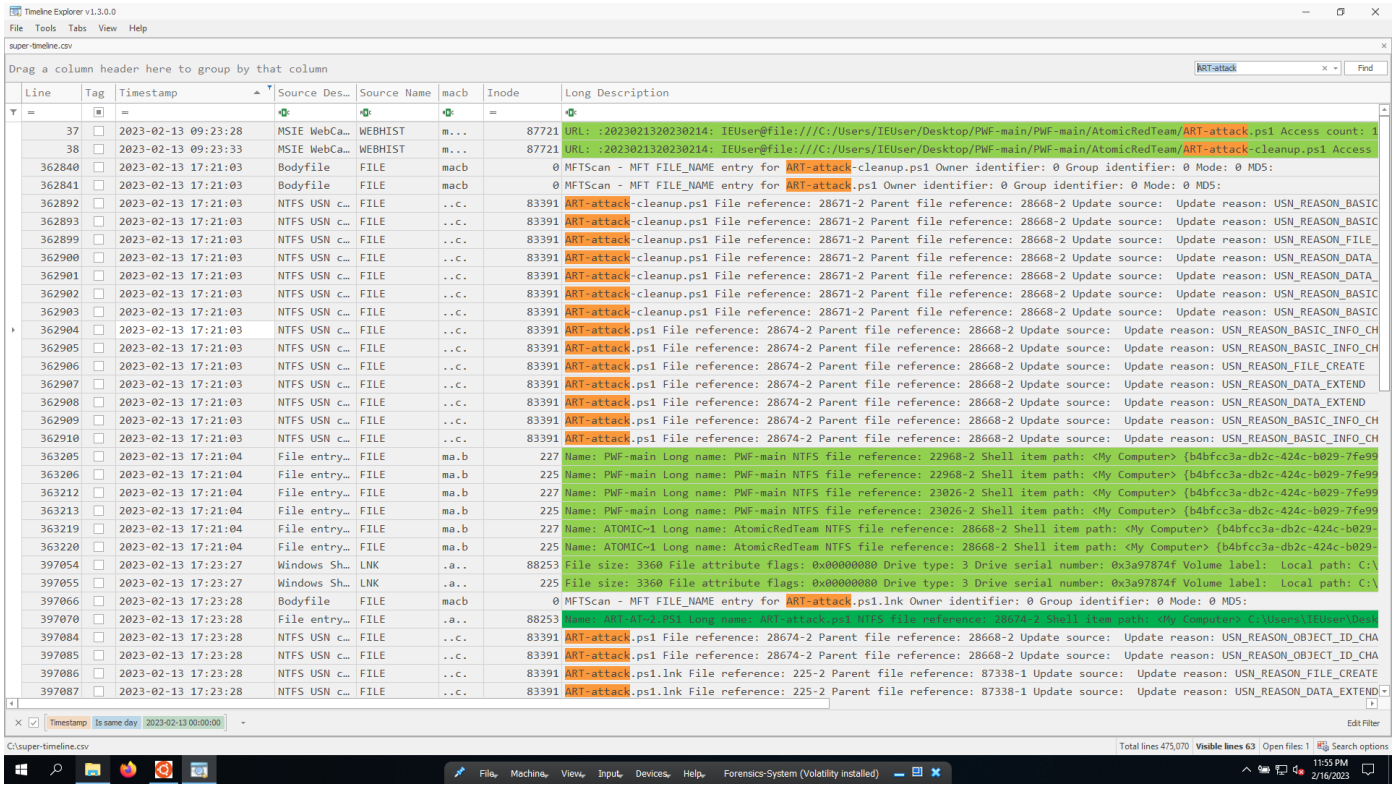




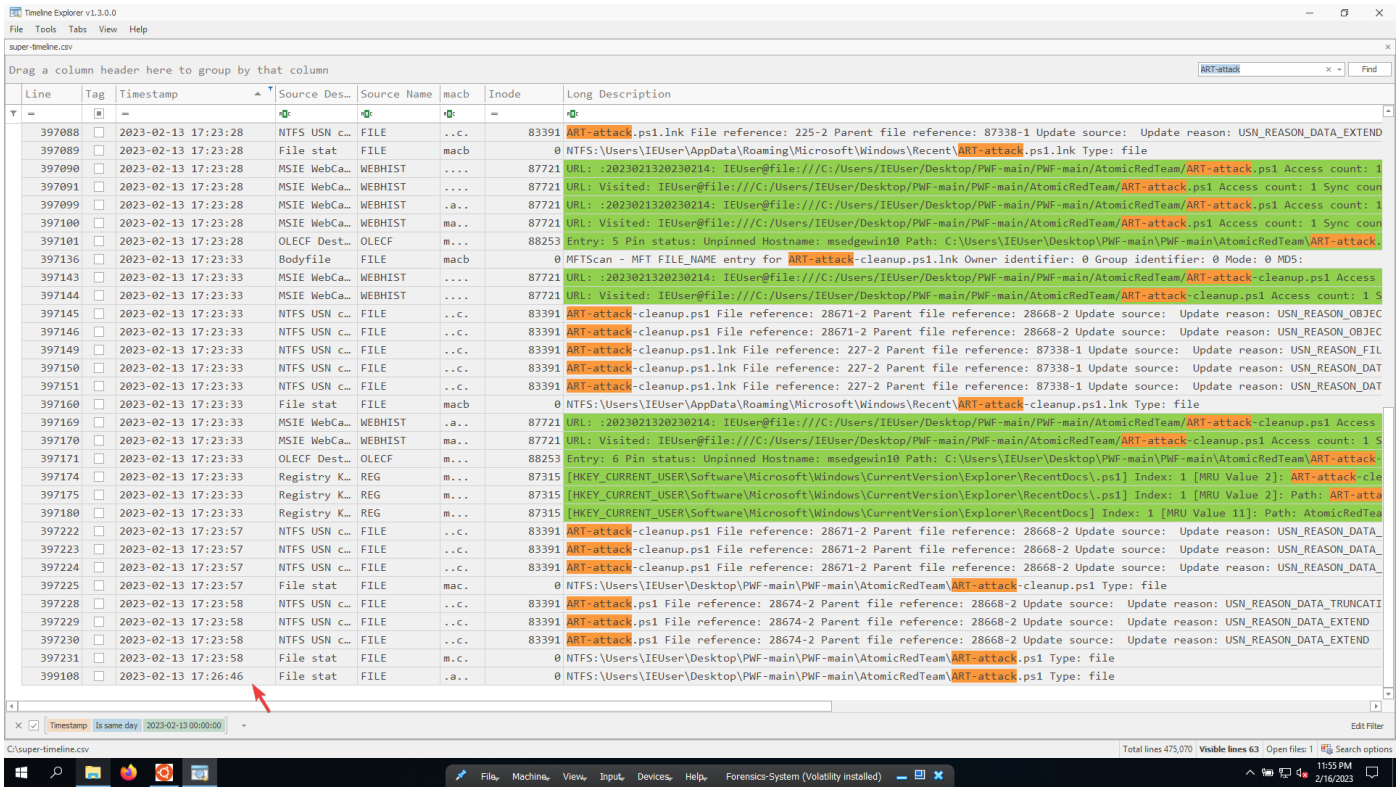
- Search ART-attack.ps1:



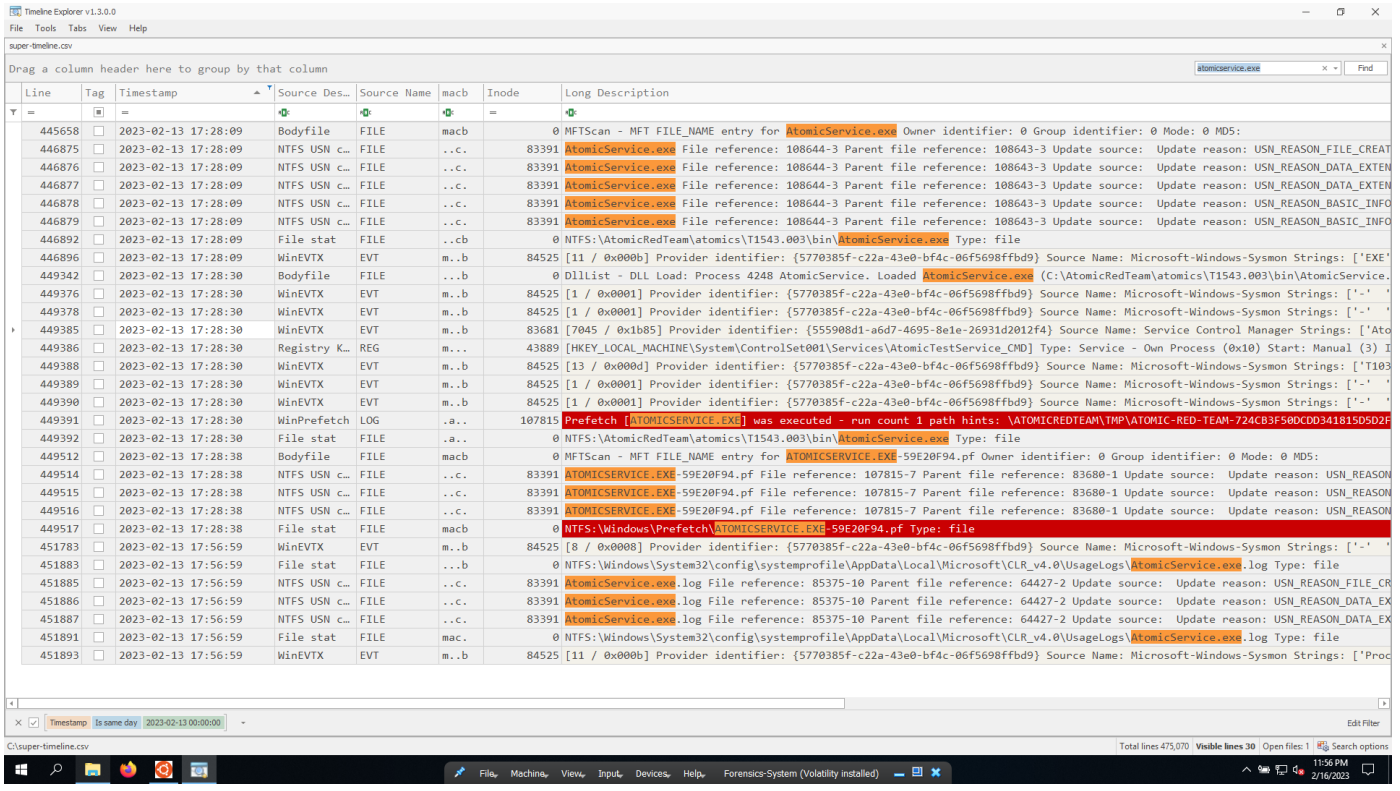
- Search ART-attack:

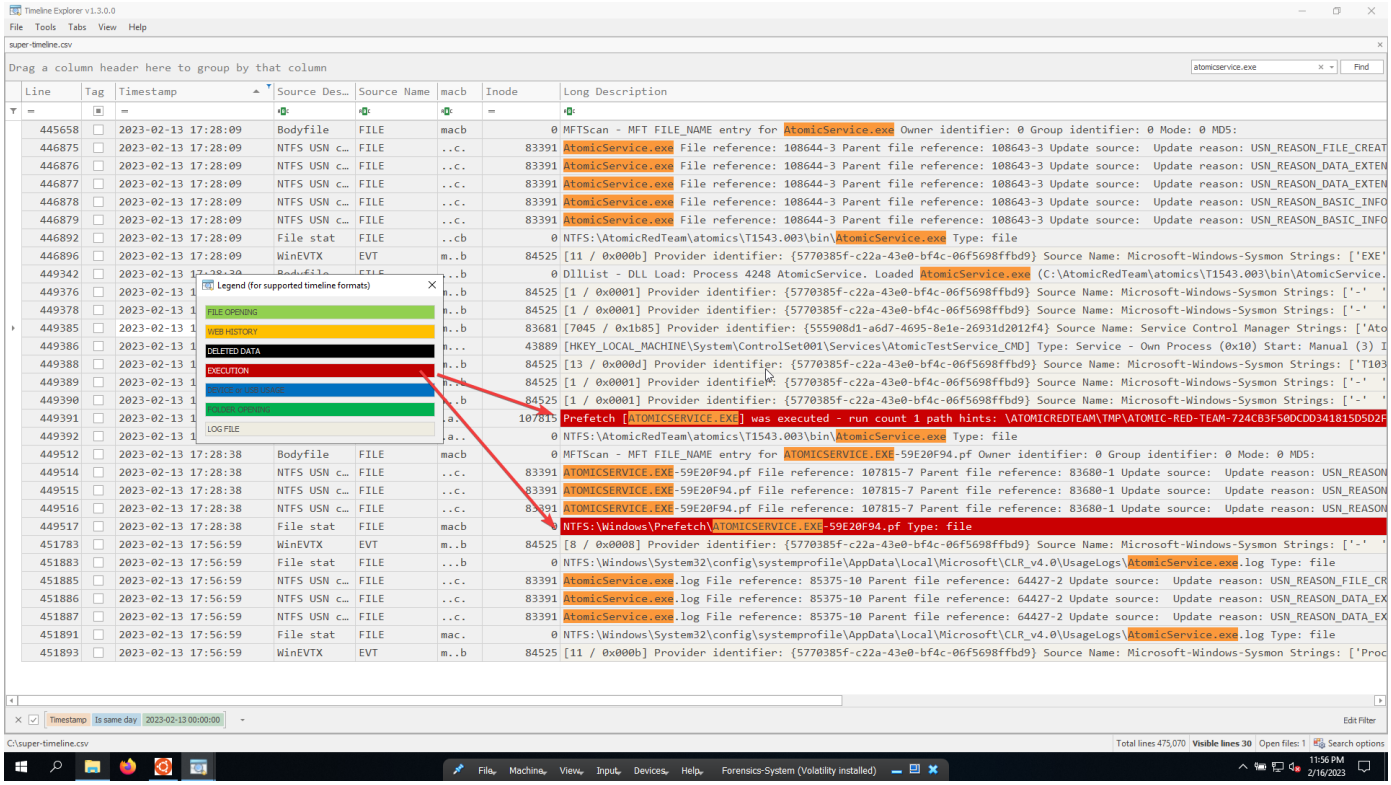


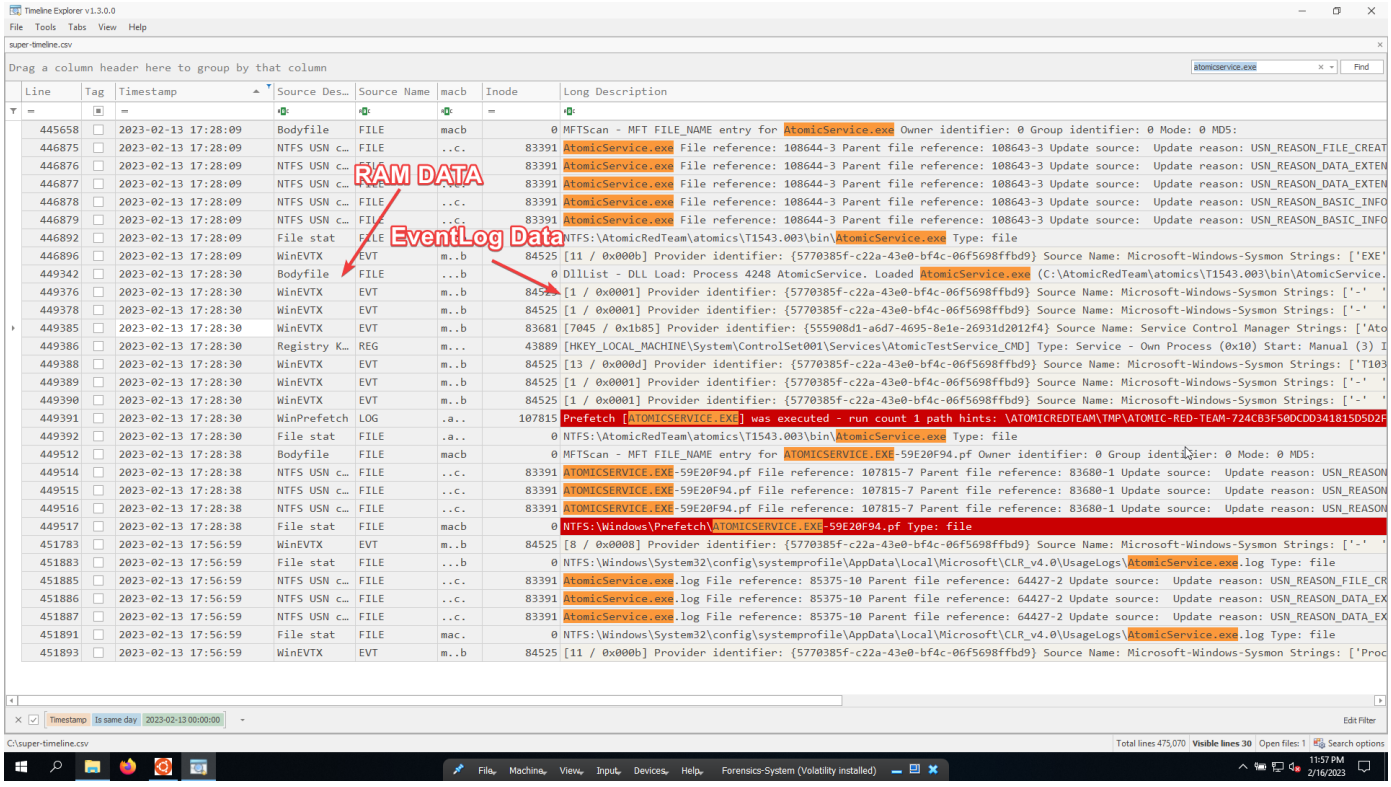
- Execution of file:



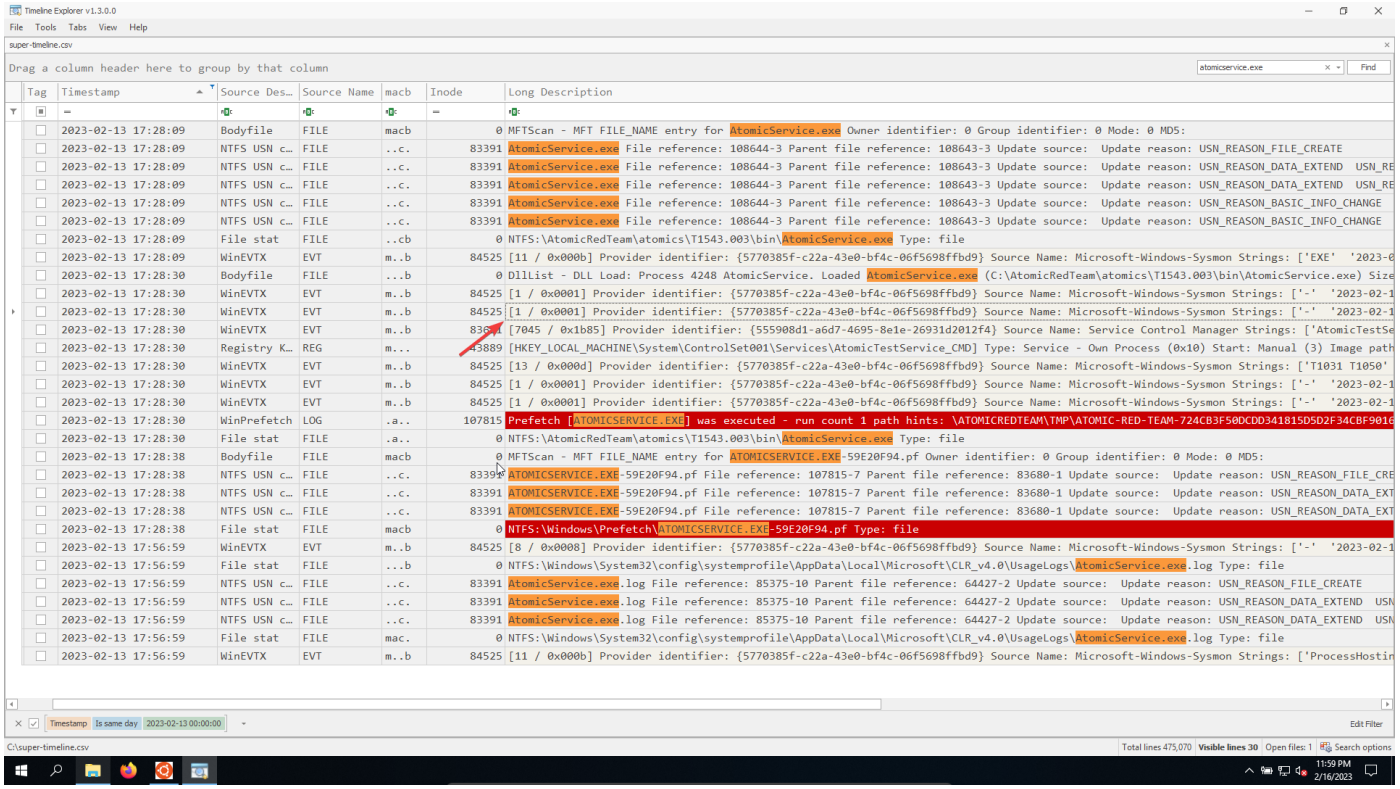
- Search for AtomicService.exe:

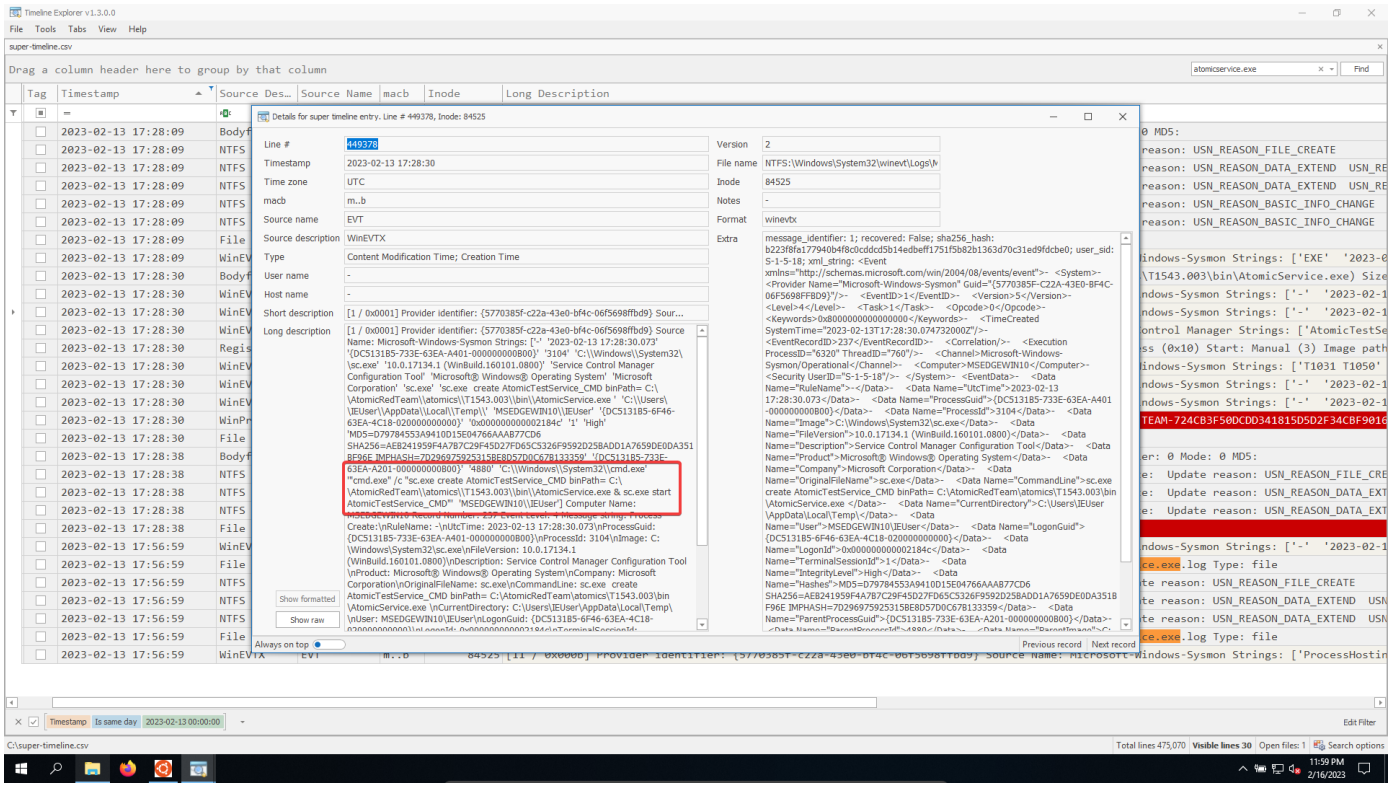




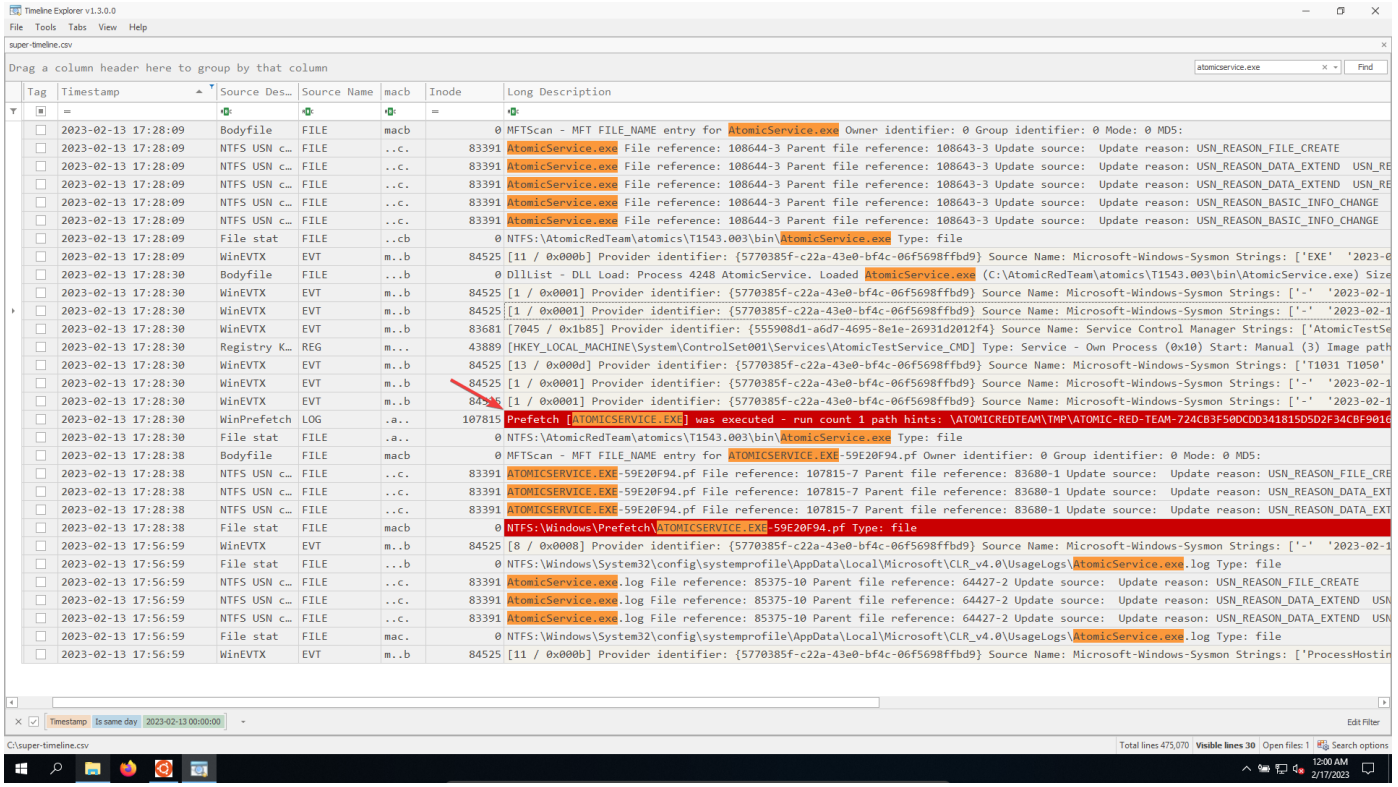


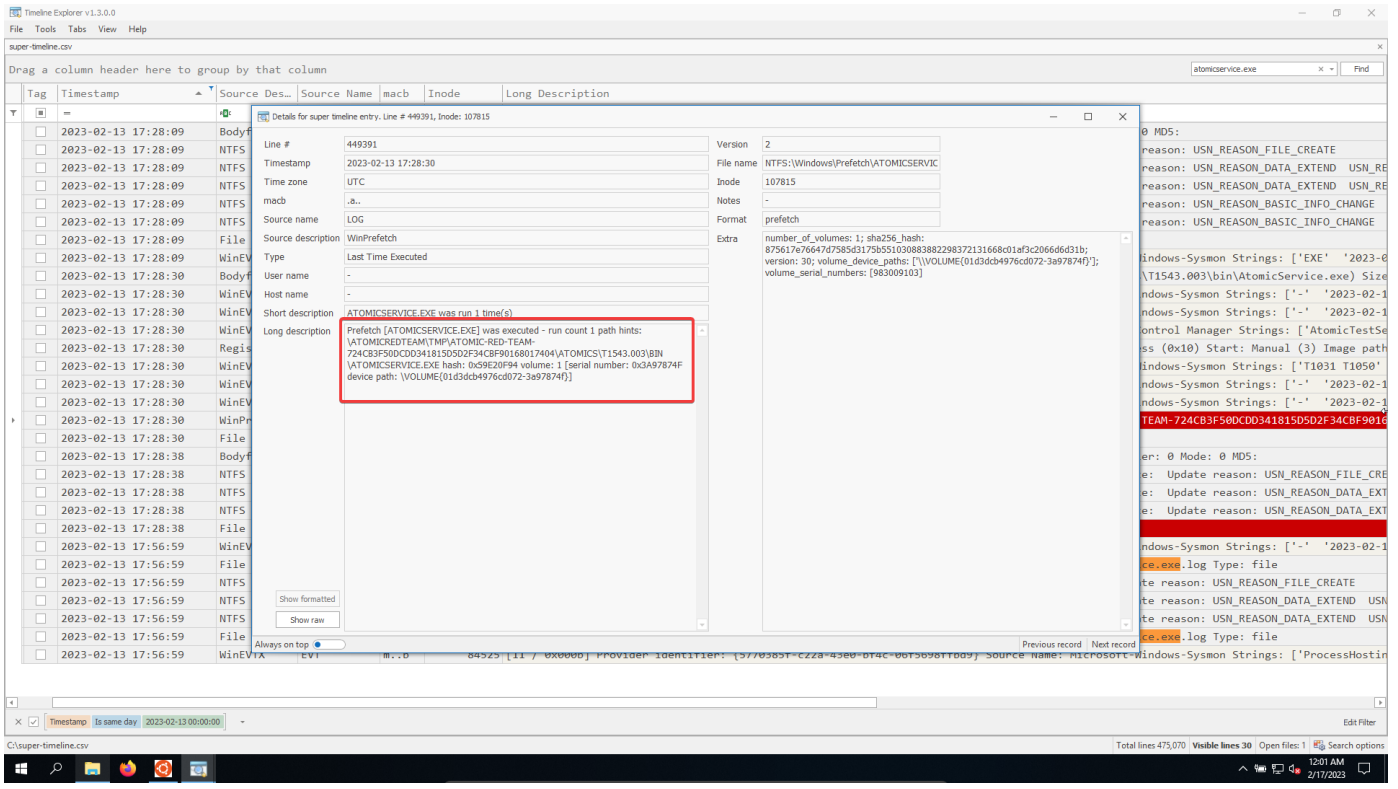
- Service creation:



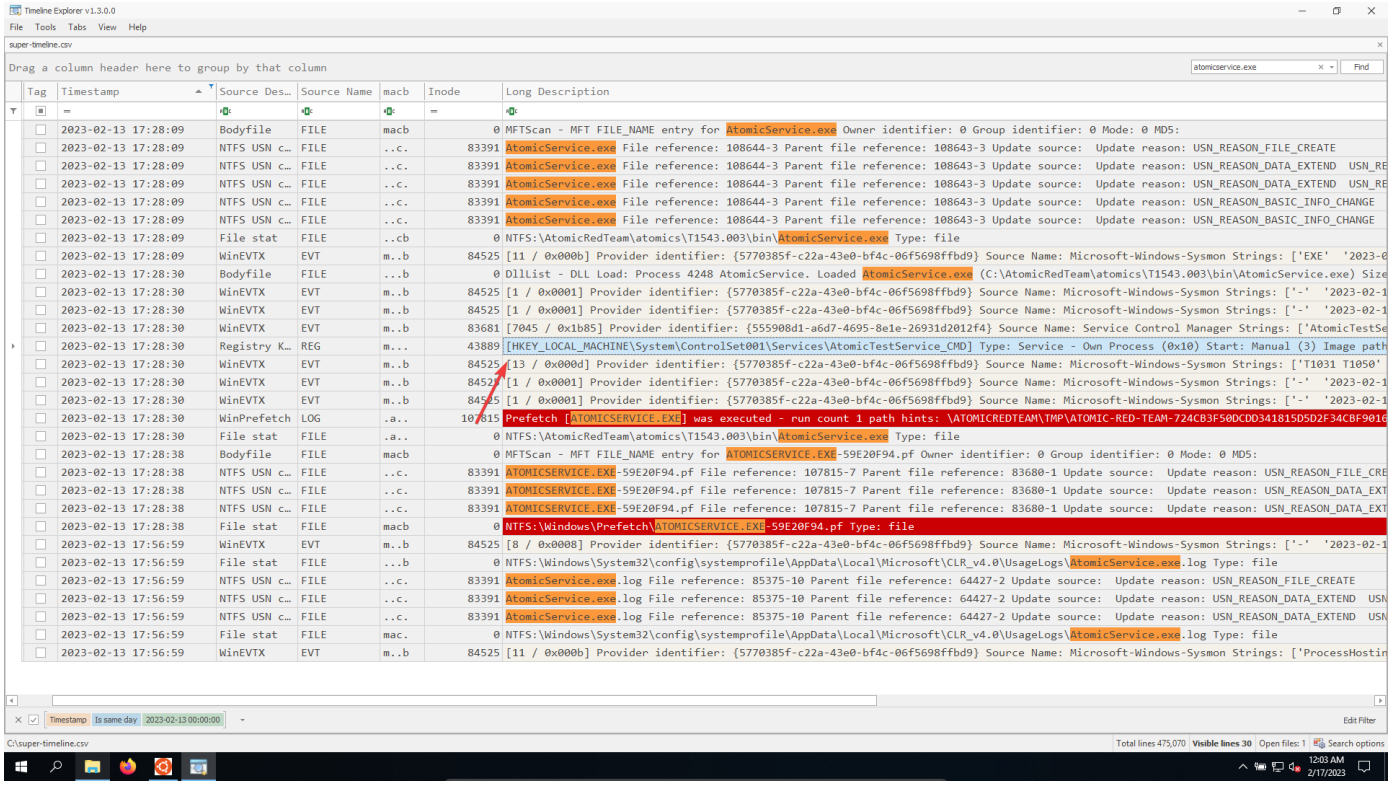


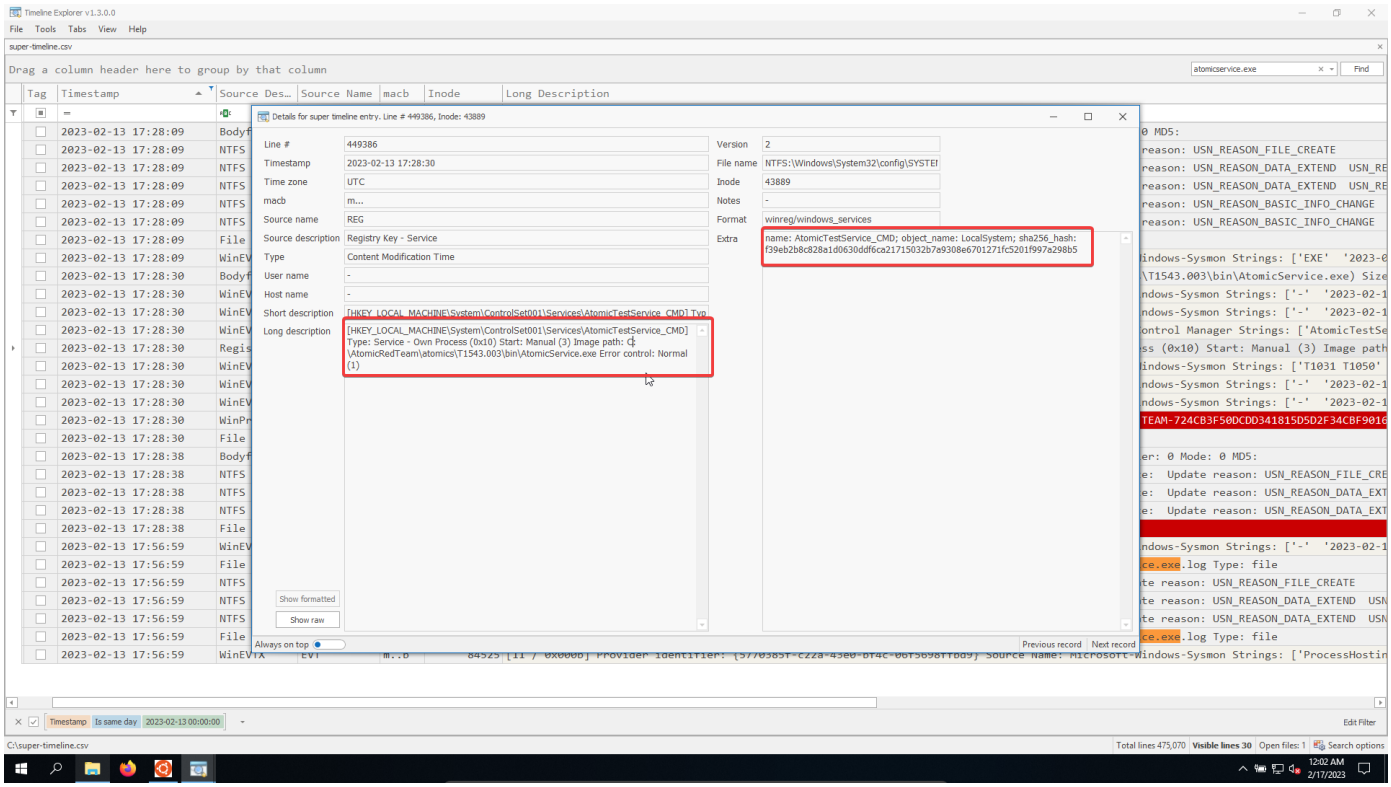
- Prefetch file execution:



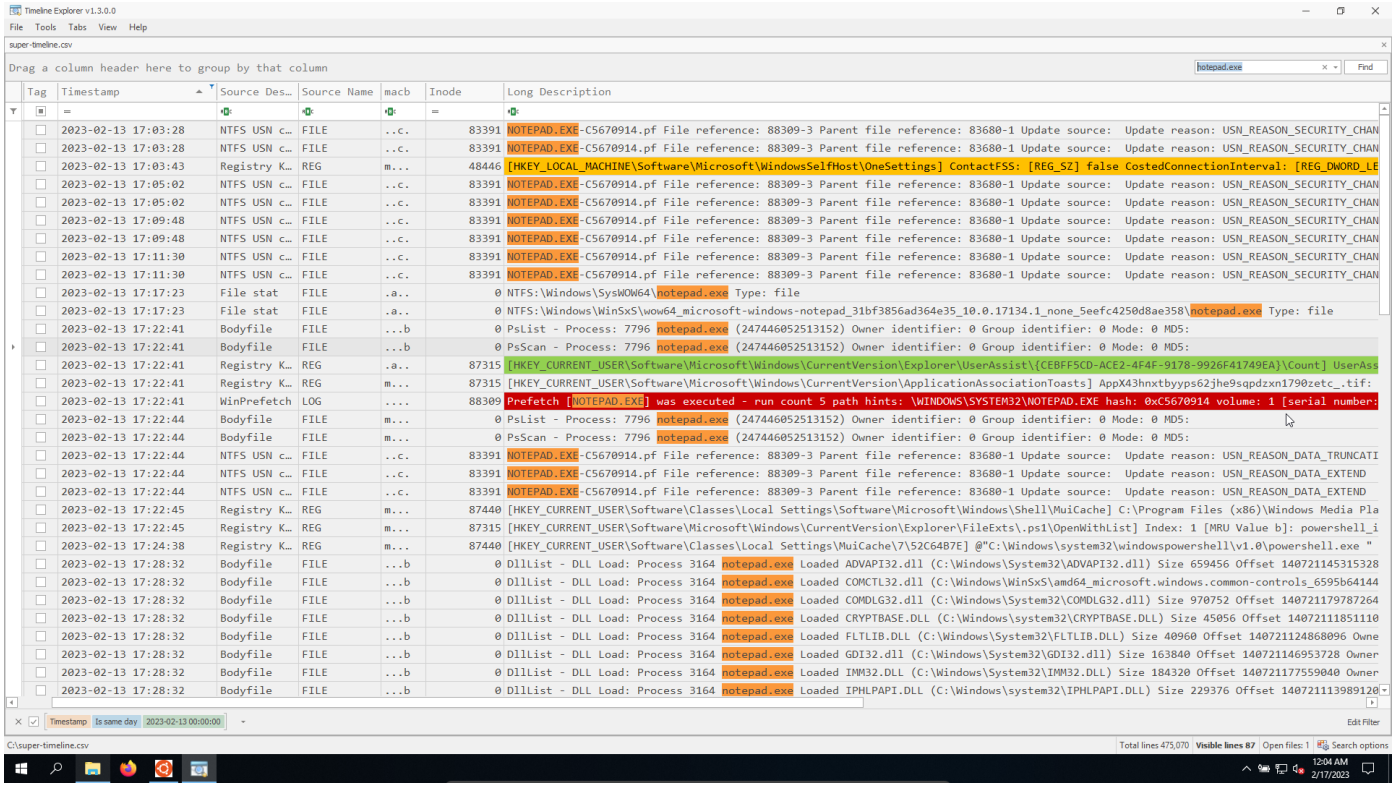


- Service information in registry:

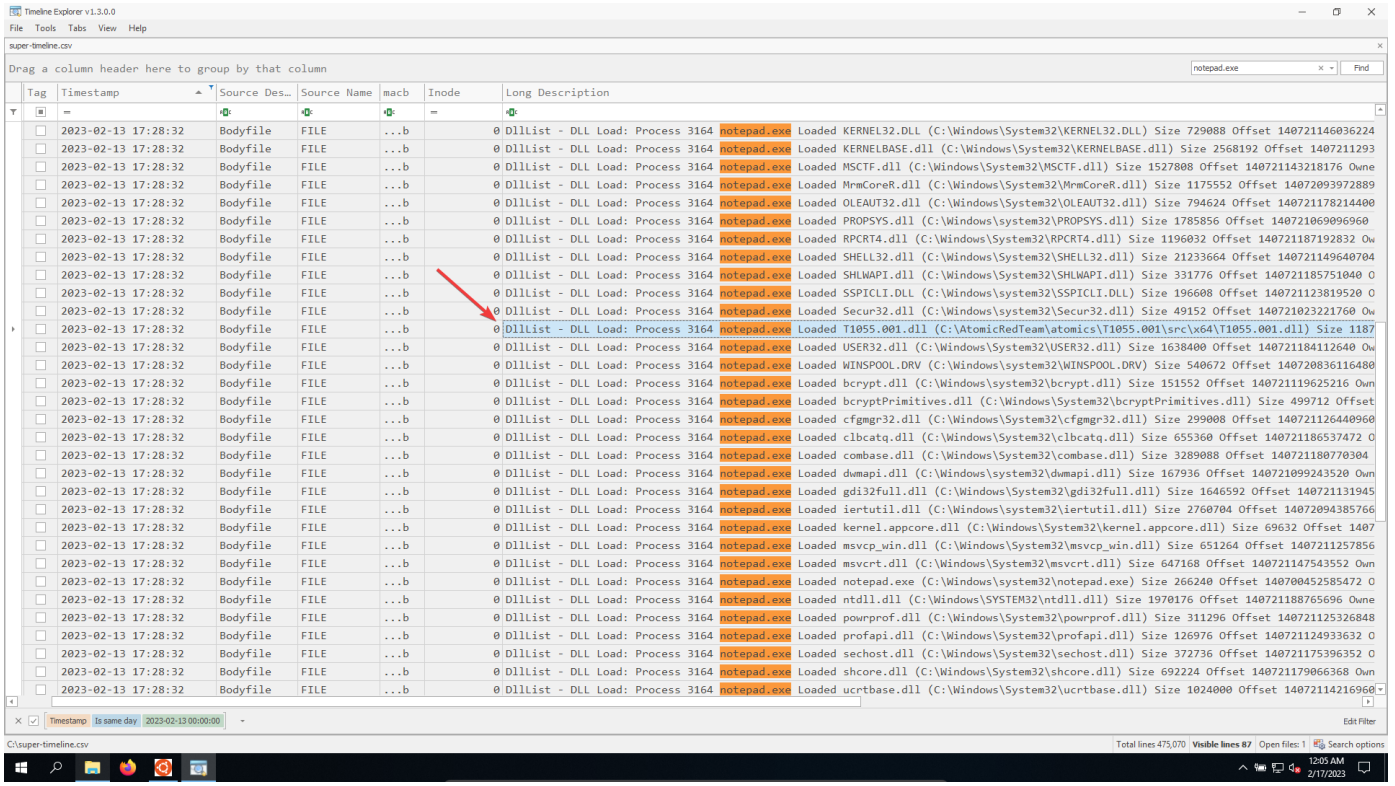


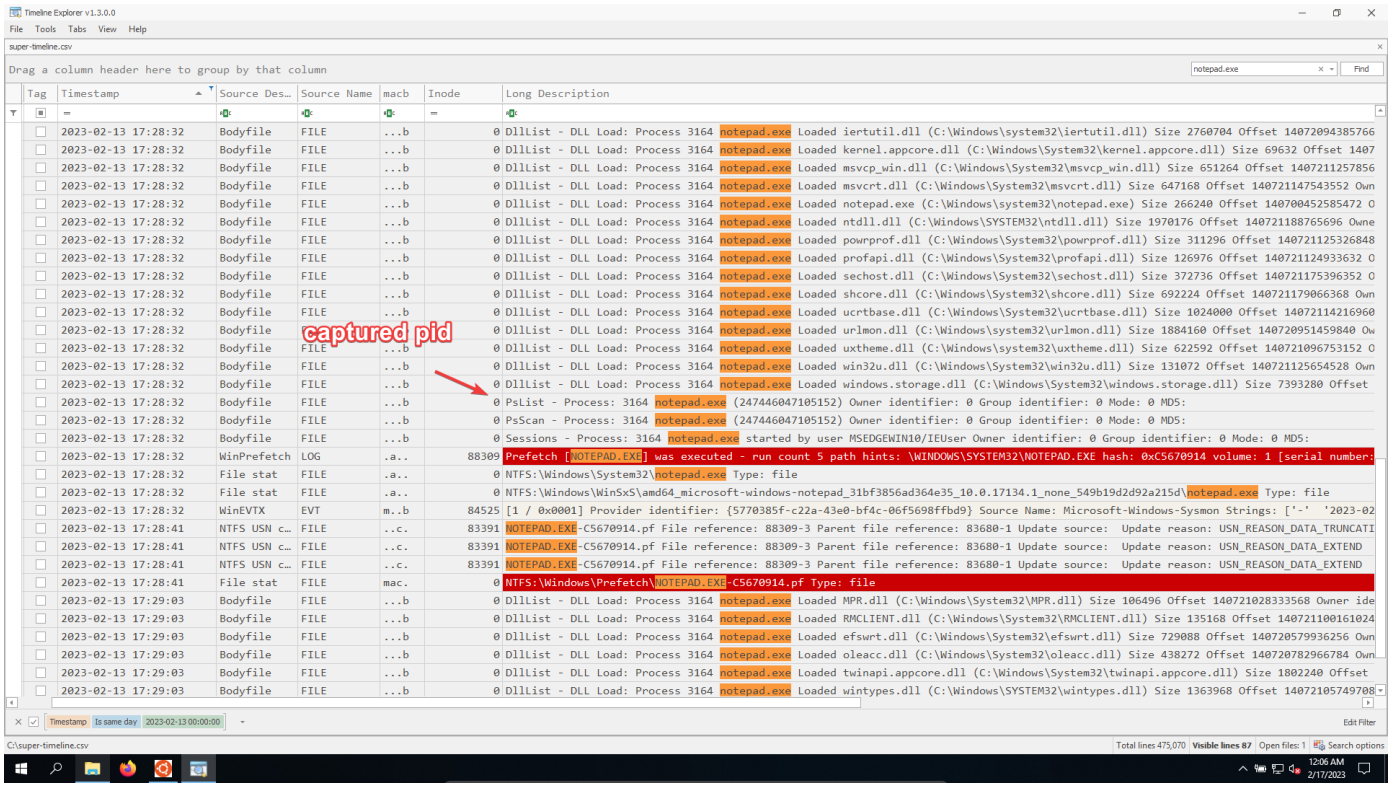


- Search notepad execution:

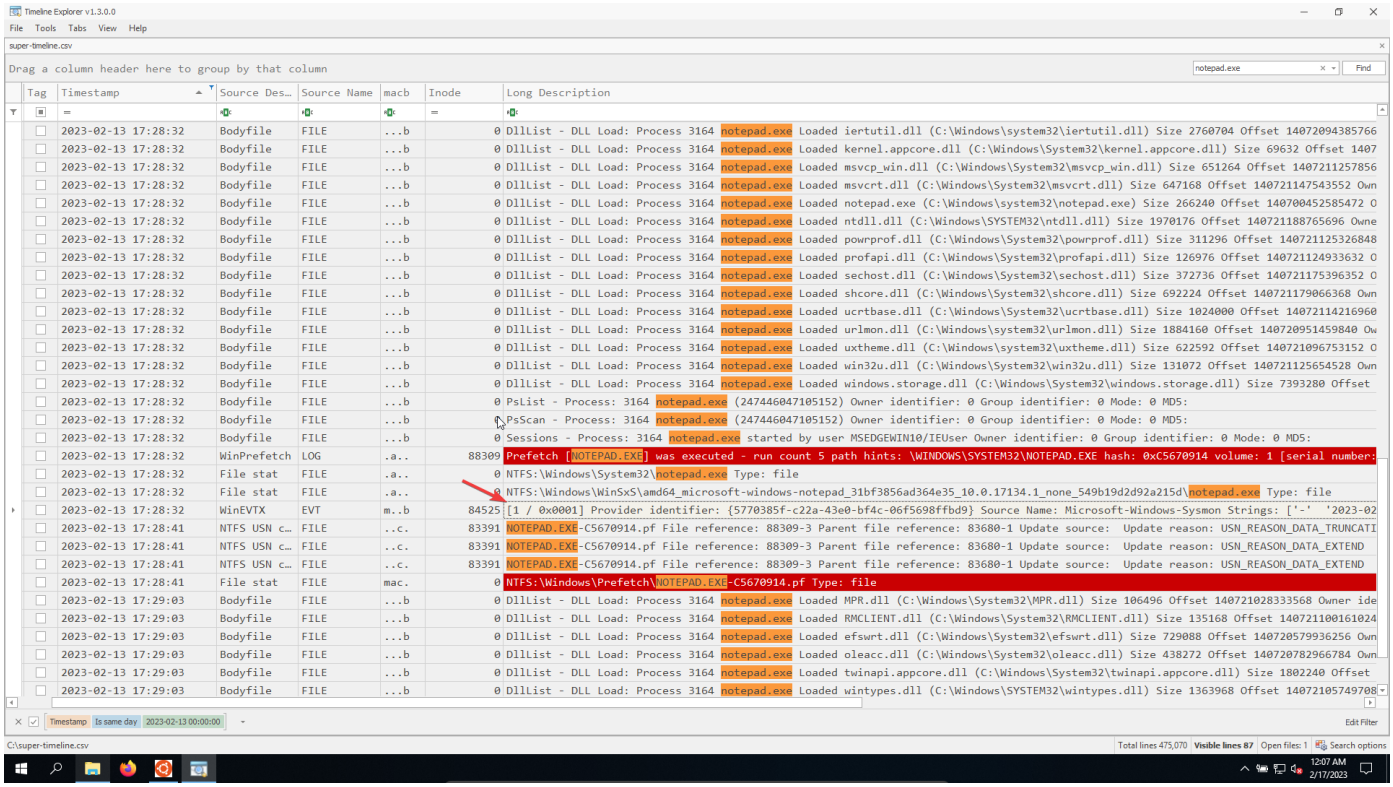


- Suspicious DLL injected:

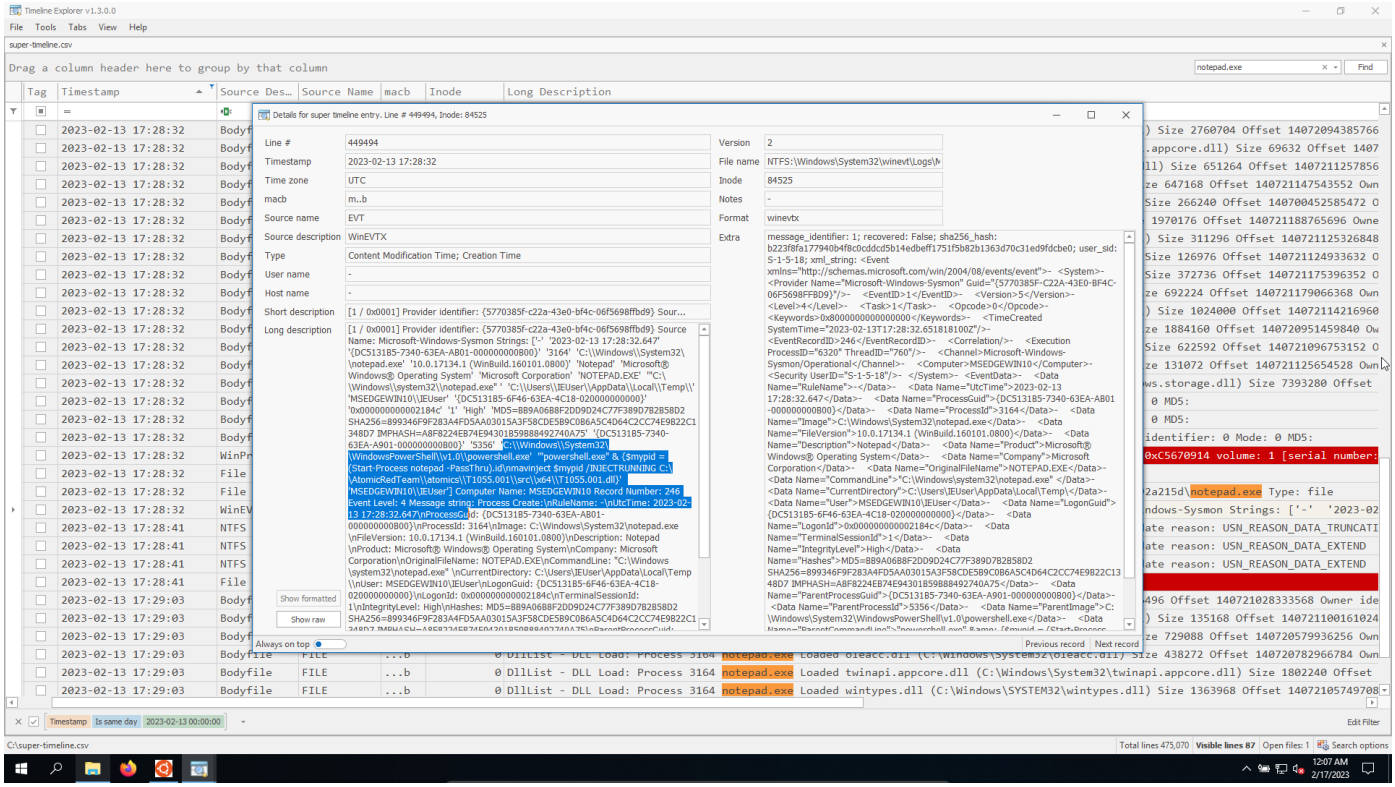




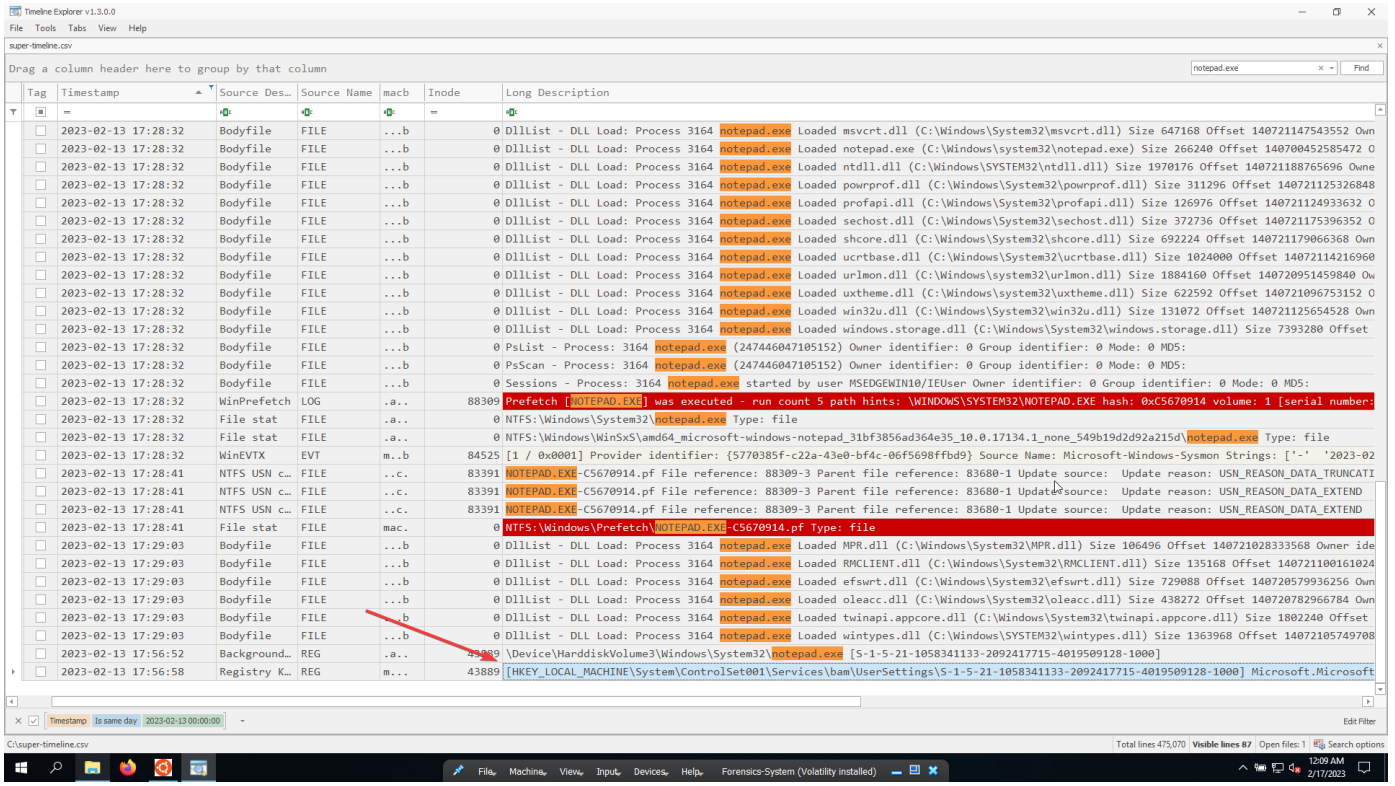
- Process created:

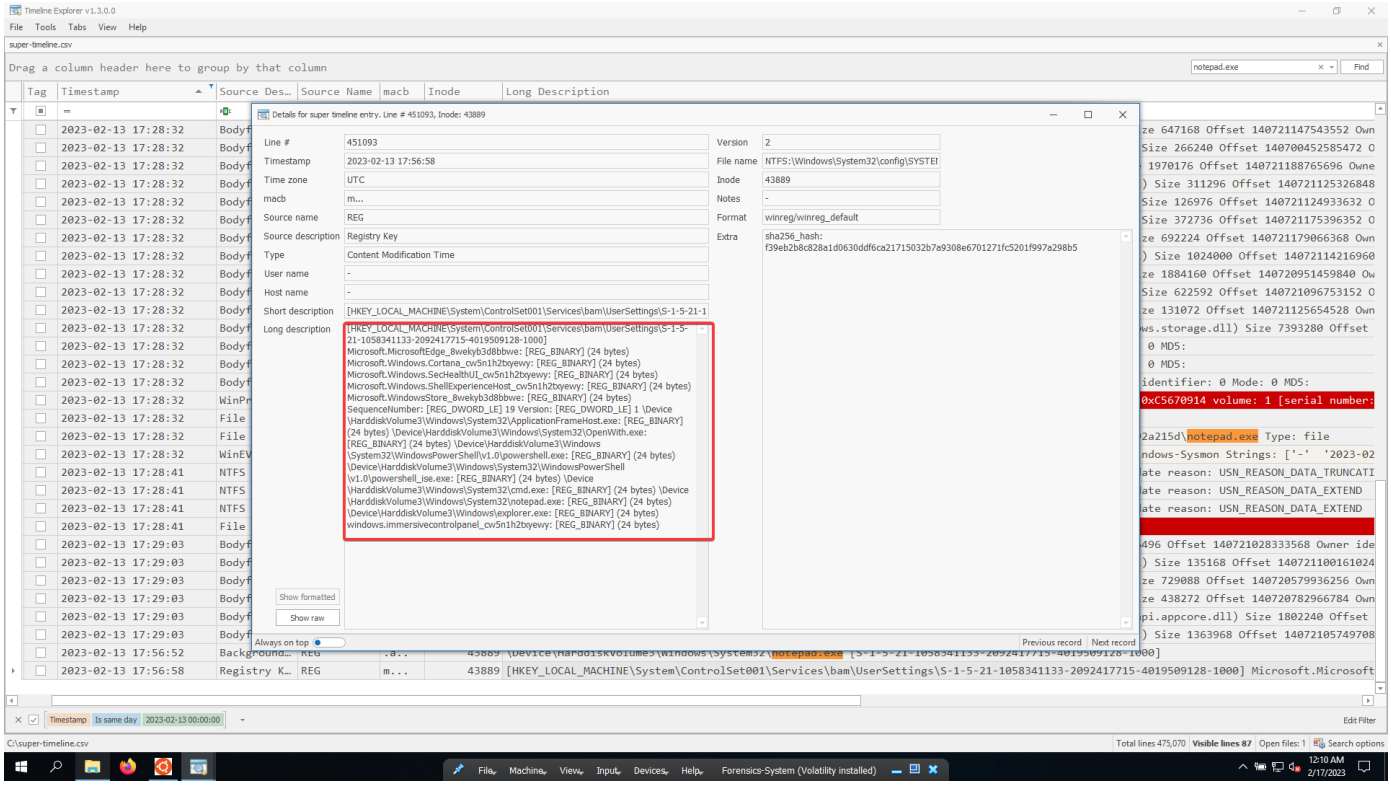


- Process injection code:

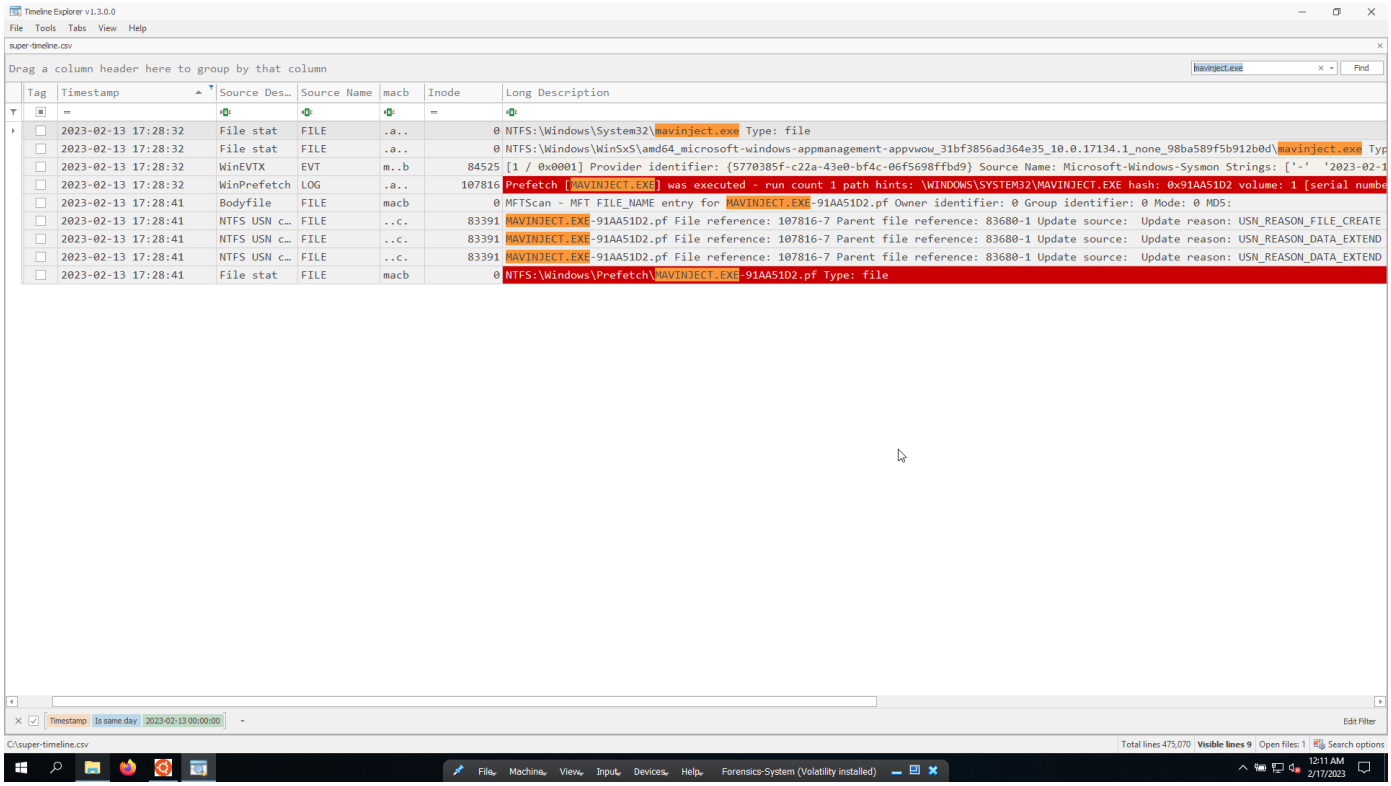


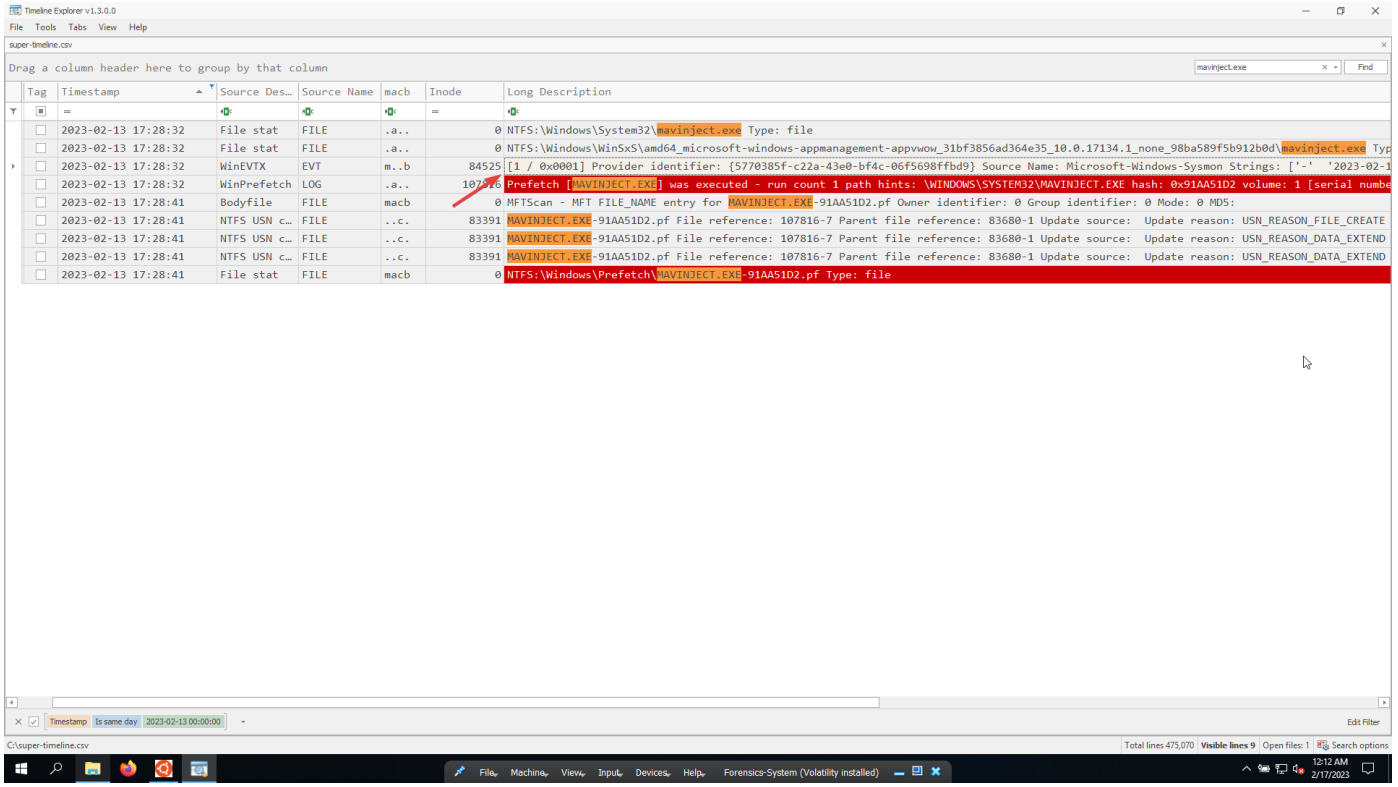
- Bam recorded last runtime of particular processes, before shutdown. It captured all the running processes that were active at that time:

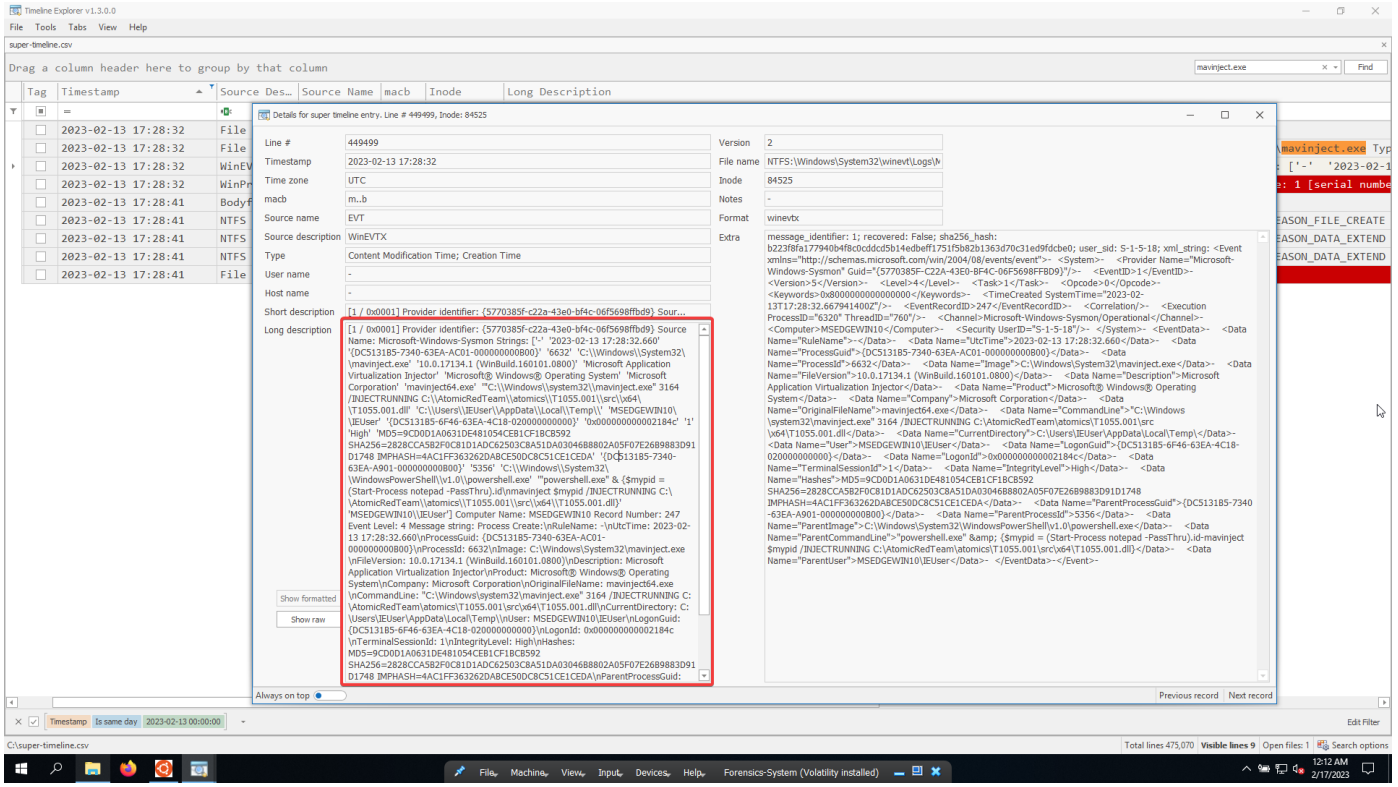




- Search for mavinject.exe:




Timeline Explorer v1.3.0.0
File Tools Tabs View Help
super-timeline.csv
Drag a column header here to group by that column
mavinject.exe
Find
Tag | Timestamp | Source Des... | Source Name | macb | Inode | Long Description
2023-02-13 17:28:32 | File stat | FILE | .a.. | 0 | NTFS:\Windows\System32\mavinject.exe Type: file
2023-02-13 17:28:32 | File stat | FILE | .a.. | 0 | NTFS:\Windows\WinSxS\amd64_microsoft-windows-appmanagement-appvwow_31bf3856ad364e35_10.0.17134.1_none_98ba589f5b912b0d\mavinject.exe Typ
2023-02-13 17:28:32 | WinEVTX | EVT | m..b | 84525 | [1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-1
2023-02-13 17:28:32 | WinPrefetch | LOG | .a.. | 107516 | Prefetch [MAVINJECT.EXE] was executed - run count 1 path hints: \WINDOWS\SYSTEM32\MAVINJECT.EXE hash: 0x91AA51D2 volume: 1 [serial numbe
2023-02-13 17:28:41 | Bodyfile | FILE | macb | 0 | MFTScan - MFT FILE_NAME entry for MAVINJECT.EXE-91AA51D2.pf Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:
2023-02-13 17:28:41 | NTFS USN c... | FILE | ..c. | 83391 | MAVINJECT.EXE-91AA51D2.pf File reference: 107816-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_FILE_CREATE
2023-02-13 17:28:41 | NTFS USN c... | FILE | ..c. | 83391 | MAVINJECT.EXE-91AA51D2.pf File reference: 107816-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
2023-02-13 17:28:41 | NTFS USN c... | FILE | ..c. | 83391 | MAVINJECT.EXE-91AA51D2.pf File reference: 107816-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
2023-02-13 17:28:41 | File stat | FILE | macb | 0 | NTFS:\Windows\Prefetch\MAVINJECT.EXE-91AA51D2.pf Type: file
Timestamp | Is same day | 2023-02-13 00:00:00
Edit Filter
C:\super-timeline.csv
Total lines 475,070 | Visible lines 9 | Open files: 1 | Search options
File Machine View Input Devices Help Forensics-System (Volatility installed)
12:12 AM
2/17/2023


Timeline Explorer v1.3.0.0
File Tools Tabs View Help
super-timeline.csv
Drag a column header here to group by that column
mavinject.exe
Find
Tag | Timestamp | Source Des... | Source Name | macb | Inode | Long Description
Details for super timeline entry. Line # 449499, Inode: 84525
Line # 449499
Timestamp 2023-02-13 17:28:32
Time zone UTC
macb m..b
Source name EVT
Source description WinEVTX
Type Content Modification Time; Creation Time
User name -
Host name -
Short description [1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Sour...
Long description
[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13 17:28:32.660' '{DC513185-7340-63EA-AC01-000000000B00}' '6632' 'C:\\Windows\\System32\\mavinject.exe' '10.0.17134.1 (WinBuild.160101.0800)' 'Microsoft Application Virtualization Injector' 'Microsoft® Windows® Operating System' 'Microsoft Corporation' 'mavinject64.exe' '"C:\\Windows\\system32\\mavinject.exe" 3164 /INJECTRUNNING C:\\AtomicRedTeam\\atomics\\T1055.001\\src\\x64\\T1055.001.dll' 'C:\\Users\\IEUser\\AppData\\Local\\Temp\\' 'MSEDGEWIN10\\IEUser' '{DC513185-6F46-63EA-4C18-020000000000}' '0x00000000002184c' '1' 'High' 'MD5=9CD0D1A0631DE481054CEB1CF1BCB592 SHA256=2828CCA5B2F0C81D1ADC62503C8A51DA030468B802A05F07E26B9883D91D1748 IMPHASH=4AC1FF363262DABCE50DC8C51CE1CEDA' '{DC513185-7340-63EA-A901-000000000B00}' '5356' 'C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe' '"powershell.exe" & {$myid = (Start-Process notepad -PassThru).id\nmavinject $myid /INJECTRUNNING C:\\AtomicRedTeam\\atomics\\T1055.001\\src\\x64\\T1055.001.dll}' 'MSEDGEWIN10\\IEUser'] Computer Name: MSEDGEWIN10 Record Number: 247 Event Level: 4 Message string: Process Create:\nRuleName: -\nUtcTime: 2023-02-13 17:28:32.660\nProcessGuid: {DC513185-7340-63EA-AC01-000000000B00}\nProcessId: 6632\nImage: C:\Windows\System32\mavinject.exe\nFileVersion: 10.0.17134.1 (WinBuild.160101.0800)\nDescription: Microsoft Application Virtualization Injector\nProduct: Microsoft® Windows® Operating System\nCompany: Microsoft Corporation\nOriginalFileName: mavinject64.exe\nCommandLine: "C:\Windows\system32\mavinject.exe" 3164 /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll\nCurrentDirectory: C:\Users\IEUser\AppData\Local\Temp\\nUser: MSEDGEWIN10\IEUser\nLogonGuid: {DC513185-6F46-63EA-4C18-020000000000}\nLogonId: 0x00000000002184c\nTerminalSessionId: 1\nIntegrityLevel: High\nHashes: MD5=9CD0D1A0631DE481054CEB1CF1BCB592 SHA256=2828CCA5B2F0C81D1ADC62503C8A51DA030468B802A05F07E26B9883D91D1748 IMPHASH=4AC1FF363262DABCE50DC8C51CE1CEDA\nParentProcessGuid:
Show formatted
Show raw
Always on top
Version 2
File name NTFS:\Windows\System32\winevt\Logs\M
Inode 84525
Notes -
Format winevtx
Extra
message_identifier: 1; recovered: False; sha256_hash: b223f8fa177940b4f8c0cddcd5b14edbeff1751f5b82b1363d70c31ed9fdcbe0; user_sid: S-1-5-18; xml_string: <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">- <System>- <Provider Name="Microsoft-Windows-Sysmon" Guid="{5770385F-C22A-43E0-BF4C-06F5698FFBD9}"/>- <EventID>1</EventID>- <Version>5</Version>- <Level>4</Level>- <Task>1</Task>- <Opcode>0</Opcode>- <Keywords>0x8000000000000000</Keywords>- <TimeCreated SystemTime="2023-02-13T17:28:32.6679414002"/>- <EventRecordID>247</EventRecordID>- <Correlation/>- <Execution ProcessID="6320" ThreadID="760"/>- <Channel>Microsoft-Windows-Sysmon/Operational</Channel>- <Computer>MSEDGEWIN10</Computer>- <Security UserID="S-1-5-18"/>- </System>- <EventData>- <Data Name="RuleName">-</Data>- <Data Name="UtcTime">2023-02-13 17:28:32.660</Data>- <Data Name="ProcessGuid">{DC513185-7340-63EA-AC01-000000000B00}</Data>- <Data Name="ProcessId">6632</Data>- <Data Name="Image">C:\Windows\System32\mavinject.exe</Data>- <Data Name="FileVersion">10.0.17134.1 (WinBuild.160101.0800)</Data>- <Data Name="Description">Microsoft Application Virtualization Injector</Data>- <Data Name="Product">Microsoft® Windows® Operating System</Data>- <Data Name="Company">Microsoft Corporation</Data>- <Data Name="OriginalFileName">mavinject64.exe</Data>- <Data Name="CommandLine">"C:\Windows\system32\mavinject.exe" 3164 /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll</Data>- <Data Name="CurrentDirectory">C:\Users\IEUser\AppData\Local\Temp\</Data>- <Data Name="User">MSEDGEWIN10\IEUser</Data>- <Data Name="LogonGuid">{DC513185-6F46-63EA-4C18-020000000000}</Data>- <Data Name="LogonId">0x00000000002184c</Data>- <Data Name="TerminalSessionId">1</Data>- <Data Name="IntegrityLevel">High</Data>- <Data Name="Hashes">MD5=9CD0D1A0631DE481054CEB1CF1BCB592 SHA256=2828CCA5B2F0C81D1ADC62503C8A51DA030468B802A05F07E26B9883D91D1748 IMPHASH=4AC1FF363262DABCE50DC8C51CE1CEDA</Data>- <Data Name="ParentProcessGuid">{DC513185-7340-63EA-A901-000000000B00}</Data>- <Data Name="ParentProcessId">5356</Data>- <Data Name="ParentImage">C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe</Data>- <Data Name="ParentCommandLine">"powershell.exe" & {$myid = (Start-Process notepad -PassThru).id-mavinject $myid /INJECTRUNNING C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll</Data>- <Data Name="ParentUser">MSEDGEWIN10\IEUser</Data>- </EventData></Event>
Previous record
Next record
Timestamp | Is same day | 2023-02-13 00:00:00
Edit Filter
C:\super-timeline.csv
Total lines 475,070 | Visible lines 9 | Open files: 1 | Search options
File Machine View Input Devices Help Forensics-System (Volatility installed)
12:12 AM
2/17/2023