

# Super timeline analysis:

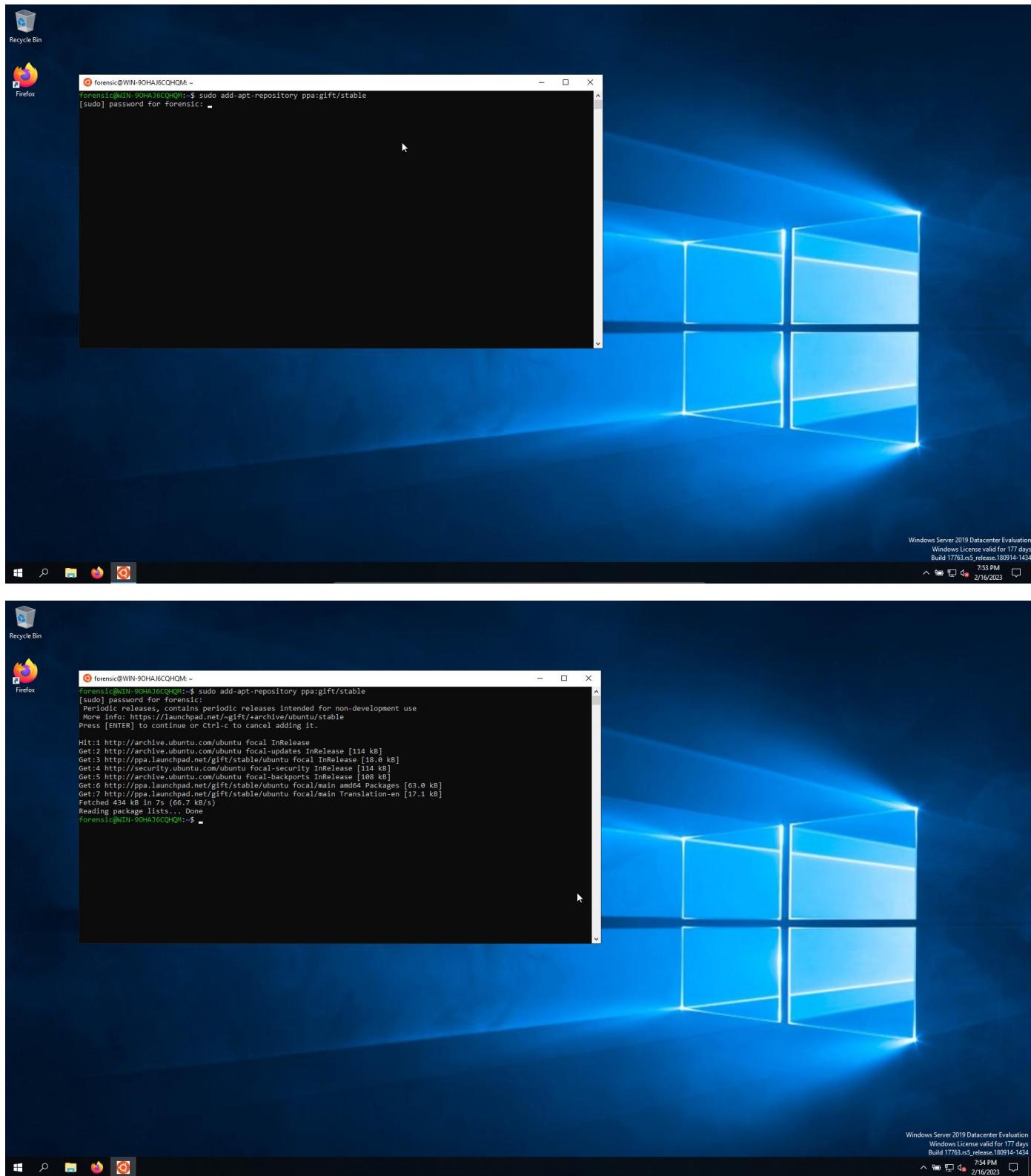
- Analysis process
- Preparing tools
- Memory timeline creation
- Disk timeline creation
- Merging timelines
- Super timeline view with Timeline explorer
- Analyzing malicious activity based on Super Timeline

## Analysis process

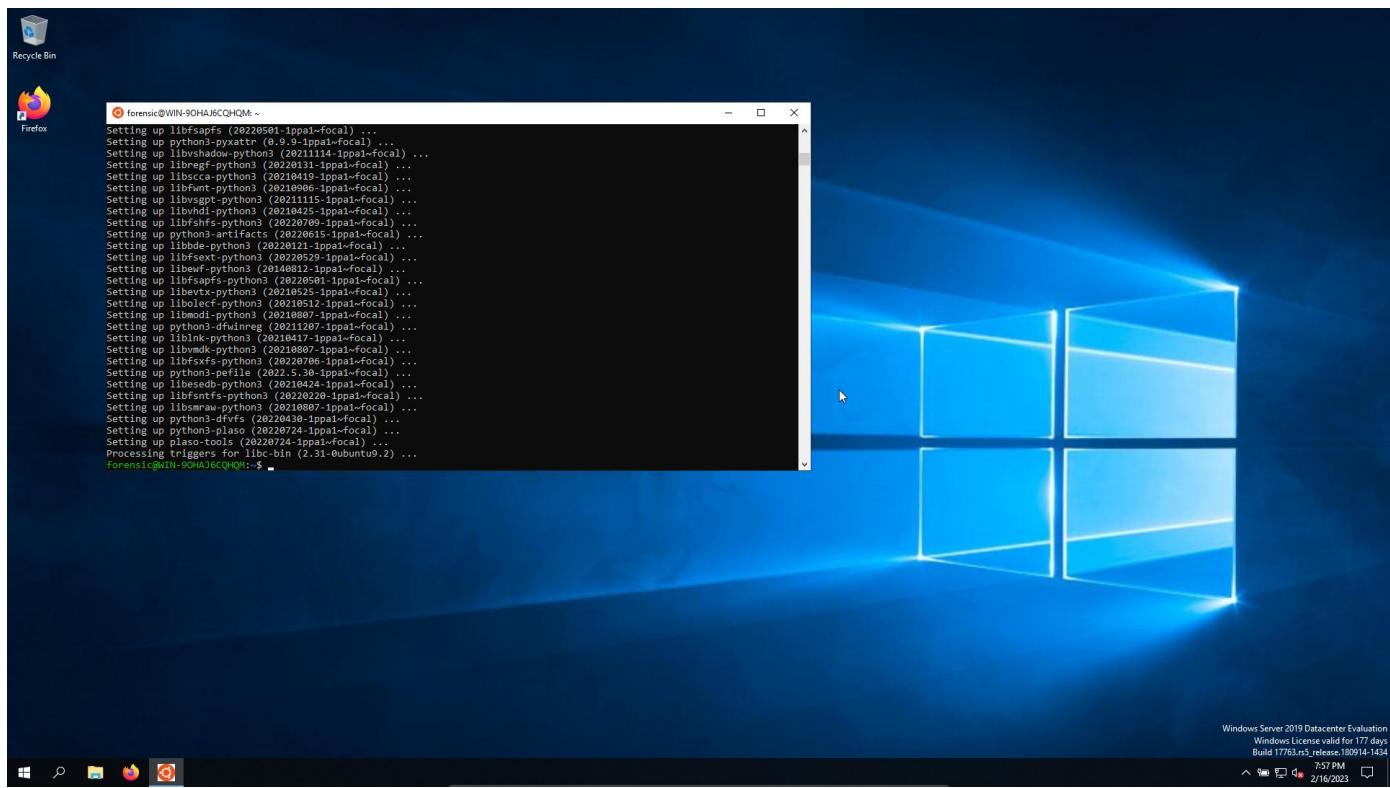
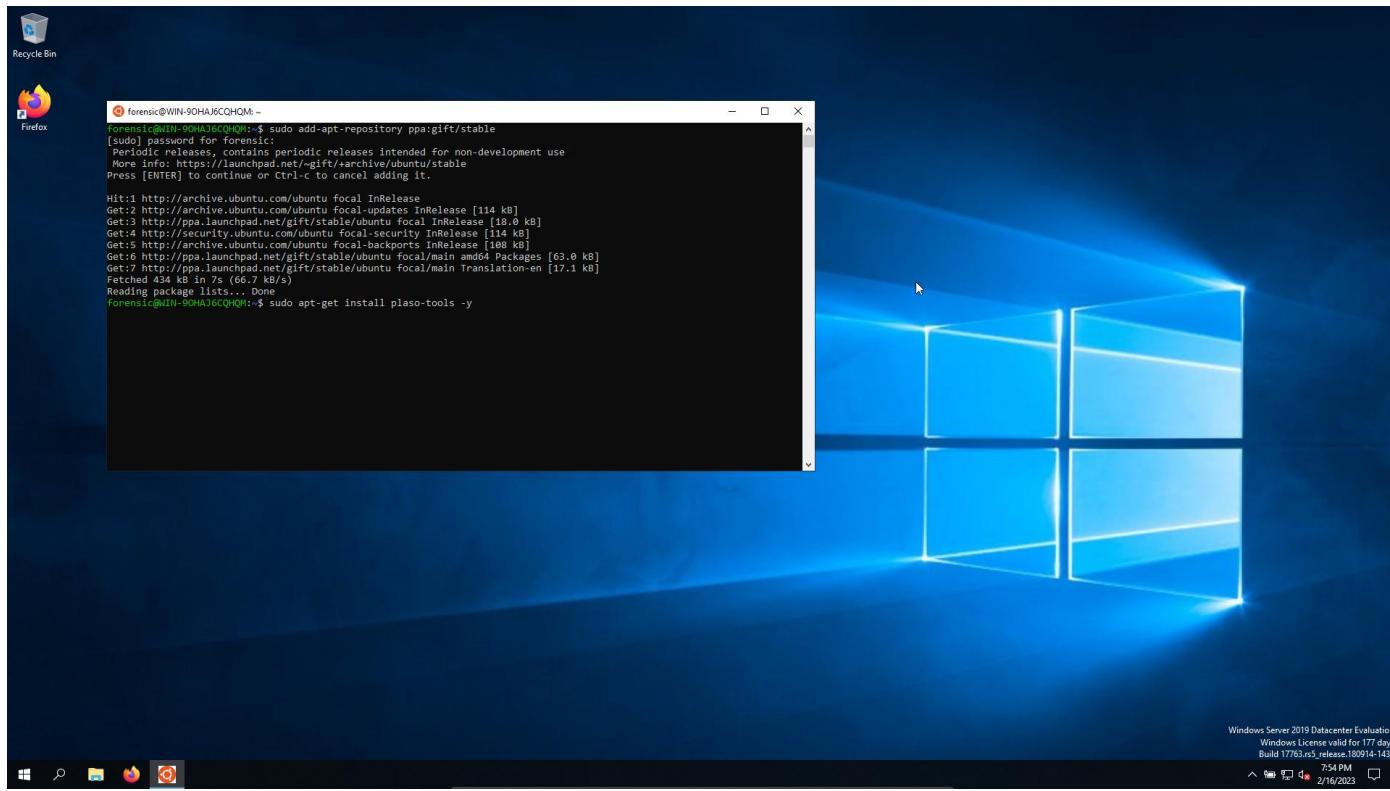
- Installing Plaso, Log2Timeline
- Prepare Evidence
  - Disk Image
  - Memory Image
- Use Tools:
  - Memory: generate bodyfile
  - Disk: generate plaso file
  - Merge files
  - Generate super timeline with psort tool

## Preparing tools

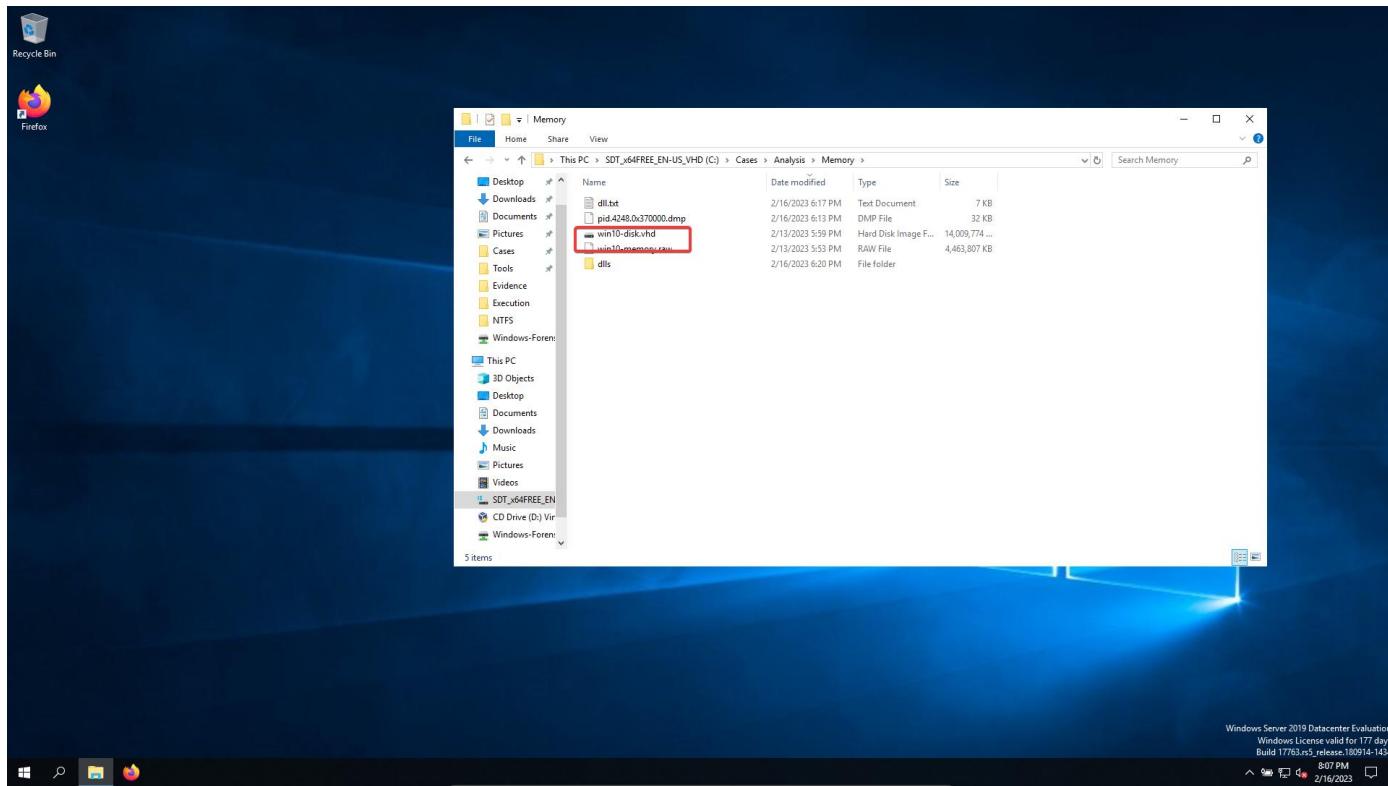
- Install Log2Timeline:
  - Add GIFT repository:



- Install plaso:

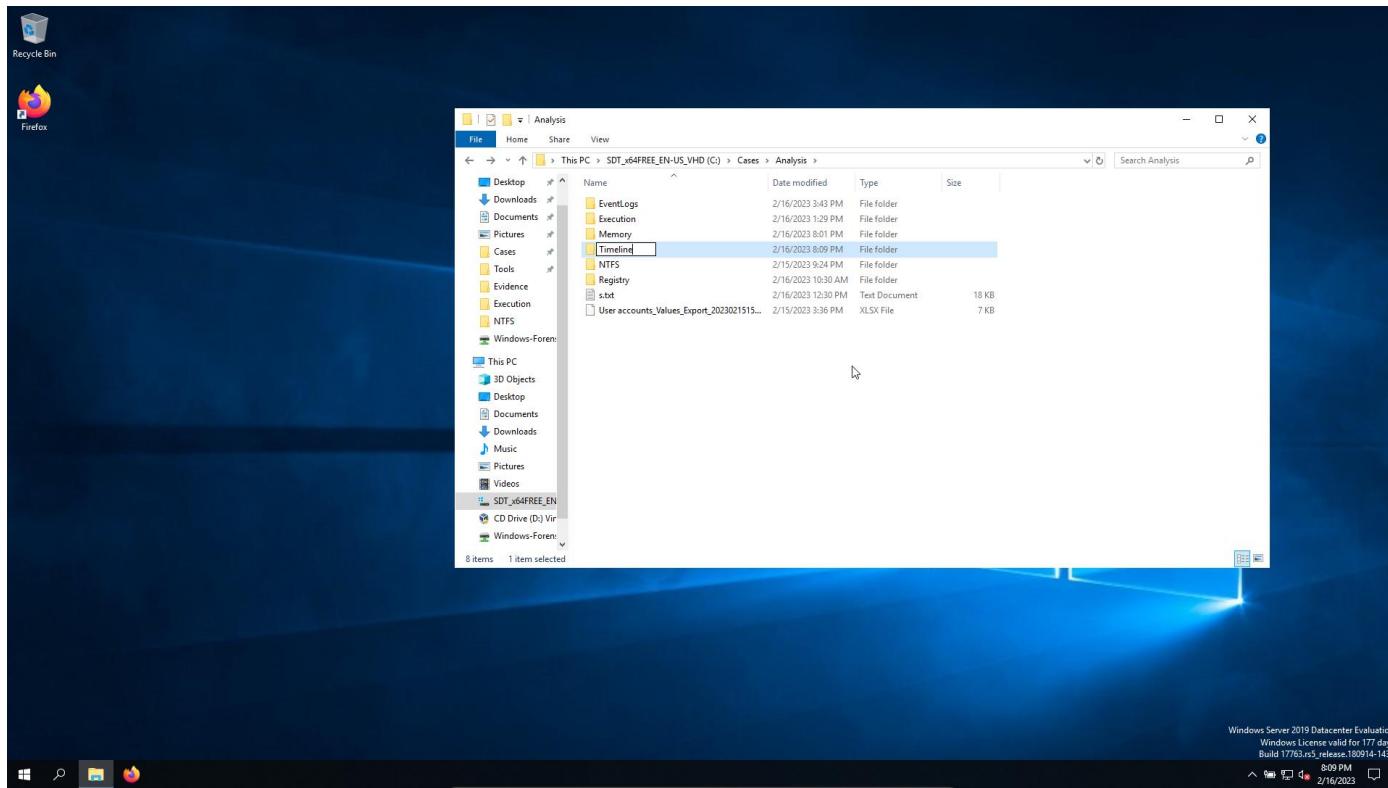


- Place memory and disk images under the same folder:  
C:\Cases\Analysis\Memory

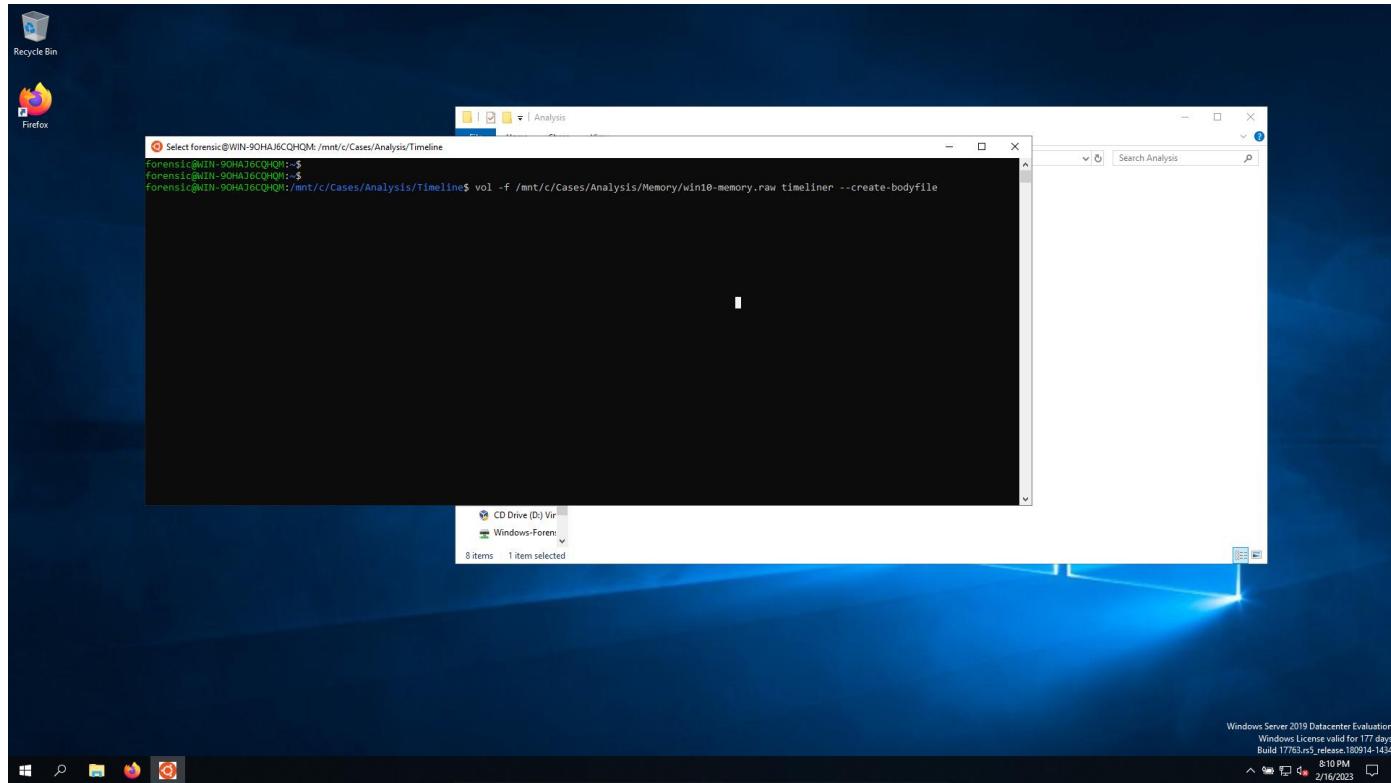


## Memory timeline creation

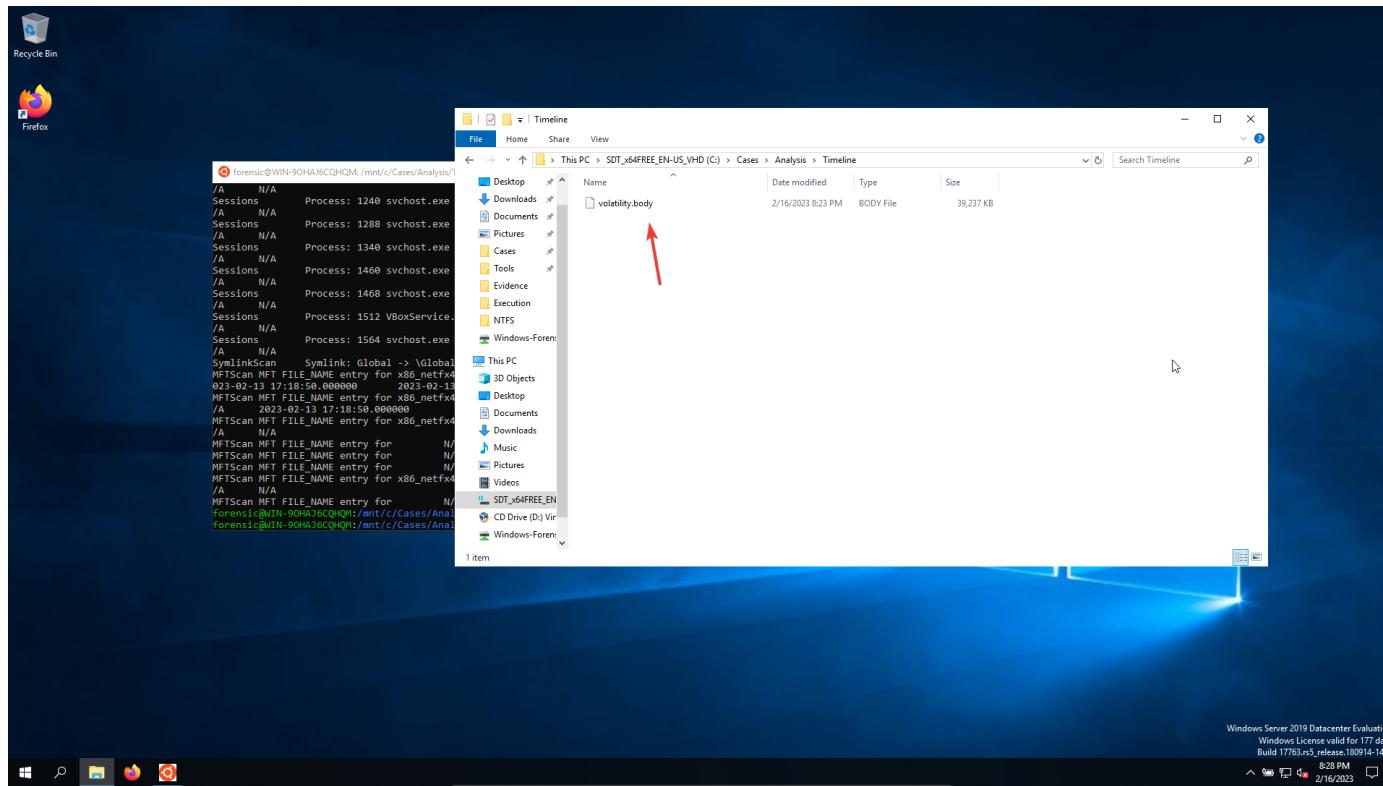
- Create folder Timeline in Analysis folder:



- Create bodyfile with volatility:



Analysis						
/A	N/A	Process: 1240 svchost.exe started by user NT AUTHORITY/LOCAL SERVICE	2023-02-14 03:11:28.000000	N/A	N/A	N/A
/A	N/A	Process: 1288 svchost.exe started by user NT AUTHORITY/LOCAL SERVICE	2023-02-14 03:11:28.000000	N/A	N/A	N/A
/A	N/A	Process: 1348 svchost.exe started by user NT AUTHORITY/LOCAL SERVICE	2023-02-14 03:11:28.000000	N/A	N/A	N/A
/A	N/A	Process: 1400 svchost.exe started by user WORKGROUP/MSEdgeWIN10\\$	2023-02-14 03:11:28.000000	N/A	N/A	N/A
/A	N/A	Process: 1468 svchost.exe started by user WORKGROUP/MSEdgeWIN10\\$	2023-02-14 03:11:28.000000	N/A	N/A	N/A
/A	N/A	Process: 1512 VBoxService.exe started by user WORKGROUP/MSEdgeWIN10\\$	2023-02-14 03:11:28.000000	N/A	N/A	N/A
/A	N/A	Process: 1564 svchost.exe started by user WORKGROUP/MSEdgeWIN10\\$	2023-02-14 03:11:28.000000	N/A	N/A	N/A
/A	N/A	SymlinkScan Symlink: Global -> [Global]?? 2023-02-14 03:11:28.000000 N/A N/A N/A				
MFTScan	MFT FILE_NAME entry for x86_ntfx4-mscorsec.dll_b03fsf7f1d50a3a_4.0.15744.161_none_280b5ffaac91ea55	-	2023-02-13 17:18:50.000000	2	N/A	N/A
MFTScan	MFT FILE_NAME entry for x86_ntfx4-mscorsec.dll_b03fsf7f1d50a3a_4.0.15744.161_none_280b5ffaac91ea55	-	2023-02-13 17:18:50.000000	N/A	N/A	N/A
MFTScan	MFT FILE_NAME entry for x86_ntfx4-mscorsec.dll_b03fsf7f1d50a3a_4.0.15744.161_none_280b5ffaac91ea55	-	2023-02-13 17:18:50.000000	N/A	N/A	N/A
MFTScan	MFT FILE_NAME entry for x86_ntfx4-mscorsec.dll_b03fsf7f1d50a3a_4.0.15744.161_none_280b5ffaac91ea55	-	2023-02-13 17:18:50.000000	N/A	N/A	N/A
/A	N/A	MFTScan MFT FILE_NAME entry for N/A 2023-02-13 17:26:52.000000 1601-01-01 00:00:37.000000 1609-01-11 05:32:53.000000				
MFTScan	MFT FILE_NAME entry for N/A N/A 1601-01-01 00:00:37.000000	1609-01-11 05:32:53.000000				
MFTScan	MFT FILE_NAME entry for N/A N/A 1601-01-01 00:00:37.000000	N/A				
MFTScan	MFT FILE_NAME entry for x86_ntfx4-mscorsec.dll_b03fsf7f1d50a3a_4.0.15744.161_none_280b5ffaac91ea55	-	N/A			
/A	N/A	MFTScan MFT FILE_NAME entry for N/A N/A N/A N/A				
Forensic@WIN-90HAJ6CQHQH: /mnt/c/Cases/Analysis/Timeline\$						
Forensic@WIN-90HAJ6CQHQH: /mnt/c/Cases/Analysis/Timeline\$						



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

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

File SOFTWARE SECURITY DEFAULT NTUSER.DAT SAMBA UnGzip bz2 bzip2 SYSTEM.txt T1053\_005\_OnLogon T1053\_005\_OnStartup volatility body

```

1 |#!PList - Process: 4 System (24744601464336) [0|0|0|0|0|0|0|0|0|0|1|1|1676342427
2 |#!PList - Process: 4 System (24744601464336) [0|0|0|0|0|0|0|0|0|0|1|1|1676342427
3 |#!PList - Process: 88 Registry (247446042374208) [0|0|0|0|0|0|0|0|0|0|1|1|16763424265
4 |#!PList - Process: 88 Registry (247446042374208) [0|0|0|0|0|0|0|0|0|0|1|1|1676344265
5 |#!PList - Process: 286 amdapi.exe (247446042374208) [0|0|0|0|0|0|0|0|0|0|1|1|1676344267
6 |#!PList - Process: 128 amssvc.exe (2474461004145289) [0|0|0|0|0|0|0|0|0|0|1|1|16763424267
7 |#!PList - Process: 392 coras.exe (2474461401675523) [0|0|0|0|0|0|0|0|0|0|1|1|16763424286
8 |#!PList - Process: 392 coras.exe (2474461401675523) [0|0|0|0|0|0|0|0|0|0|1|1|1676344206
9 |#!PList - Process: 480 coras.exe (2474461363642592) [0|0|0|0|0|0|0|0|0|0|1|1|16763424207
10 |#!PList - Process: 480 coras.exe (2474461363642592) [0|0|0|0|0|0|0|0|0|0|1|1|16763424206
11 |#!PList - Process: 480 coras.exe (2474461363642592) [0|0|0|0|0|0|0|0|0|0|1|1|16763424206
12 |#!PList - Process: 472 wininit.exe (2474461282919360) [0|0|0|0|0|0|0|0|0|0|1|1|16763442396
13 |#!PList - Process: 540 winlogon.exe (247446099667732) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
14 |#!PList - Process: 540 winlogon.exe (247446099667732) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
15 |#!PList - Process: 612 services.exe (2474461376468512) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
16 |#!PList - Process: 612 services.exe (2474461376468512) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
17 |#!PList - Process: 620 lsass.exe (247446124597376) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
18 |#!PList - Process: 620 lsass.exe (247446124597376) [0|0|0|0|0|0|0|0|0|0|1|1|1676344207
19 |#!PList - Process: 720 svchost.exe (247446138491649) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
20 |#!PList - Process: 720 svchost.exe (247446138491649) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
21 |#!PList - Process: 736 fonddrvhost.exe (247446098126209) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
22 |#!PList - Process: 736 fonddrvhost.exe (247446098126209) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
23 |#!PList - Process: 736 fonddrvhost.exe (247446098126209) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
24 |#!PList - Process: 744 fonddrvhost.exe (247446098142592) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
25 |#!PList - Process: 816 svchost.exe (247446098110016) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
26 |#!PList - Process: 816 svchost.exe (247446098101632) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
27 |#!PList - Process: 860 svchost.exe (247446098085249) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
28 |#!PList - Process: 860 svchost.exe (247446098085249) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
29 |#!PList - Process: 892 svchost.exe (247446098085249) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
30 |#!PList - Process: 996 dwm.exe (247446140133505) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
31 |#!PList - Process: 996 dwm.exe (247446140133504) [0|0|0|0|0|0|0|0|0|0|1|1|1676344287
32 |#!PList - Process: 372 svchost.exe (247446140133504) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
33 |#!PList - Process: 404 svchost.exe (247446140133504) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
34 |#!PList - Process: 654 svchost.exe (247446097712512) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
35 |#!PList - Process: 694 svchost.exe (247446097712512) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
36 |#!PList - Process: 694 svchost.exe (247446097712512) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
37 |#!PList - Process: 680 svchost.exe (247446097704320) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
38 |#!PList - Process: 680 svchost.exe (247446097704320) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
39 |#!PList - Process: 356 svchost.exe (247446140133504) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
40 |#!PList - Process: 1044 svchost.exe (247446140133504) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
41 |#!PList - Process: 1044 svchost.exe (247446097687936) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
42 |#!PList - Process: 1124 svchost.exe (247446140806528) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
43 |#!PList - Process: 1124 svchost.exe (247446140806528) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
44 |#!PList - Process: 1124 svchost.exe (247446140806528) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
45 |#!PList - Process: 1164 svchost.exe (24744614013289) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
46 |#!PList - Process: 1232 svchost.exe (247446141207936) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
47 |#!PList - Process: 1232 svchost.exe (247446141207936) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
48 |#!PList - Process: 1232 svchost.exe (247446141207936) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
49 |#!PList - Process: 1240 svchost.exe (24744614170672) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
50 |#!PList - Process: 1240 svchost.exe (24744614170672) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
51 |#!PList - Process: 1288 svchost.exe (24744614211220) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
52 |#!PList - Process: 1288 svchost.exe (24744614211220) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
53 |#!PList - Process: 1340 svchost.exe (24744642092928) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
54 |#!PList - Process: 1460 svchost.exe (24744642056064) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
55 |#!PList - Process: 1460 svchost.exe (24744642056064) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
56 |#!PList - Process: 1460 svchost.exe (24744642047872) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288
57 |#!PList - Process: 1460 svchost.exe (24744642047872) [0|0|0|0|0|0|0|0|0|0|1|1|1676344288

```

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Find... Find in Files... Ctrl+F Ctrl+Shift+F

Find Next Shift+F3 F3 [1]0[0]1[0]1[1][1676344267

Find Previous Shift+F3 [0]1[0]1[0]1[0][1][1676344267

Select and Find Next Ctrl+F3 [1]0[0]1[0]1[0][1][1676344265

Select and Find Previous Ctrl+Shift+F3 [0]1[0]1[0]1[0][1][1676344267

Find (Volatile) Next Ctrl+Alt+F3 [1]0[0]1[0]1[0][1][1676344267

Find (Volatile) Previous Ctrl+Alt+Shift+F3 [52]1[0]1[0]1[0]1[1][1676344266

Replace... Ctrl+R Ctrl+Alt+R Ctrl+M

Incremental Search Ctrl+Alt+R

Search Results Window F7

Next Search Result F4

Previous Search Result Shift+F4

Go to... Ctrl+B

Go to Matching Brace Ctrl+Alt+B

Select All Between Matching Braces Ctrl+Alt+Shift+B

Mark... Ctrl+M

Style All Occurrences of Token

Style On Token

Clear Style

Jump Up

Jump Down

Copy Styled Text

Bookmark

Find characters in range... Ctrl+Shift+M

Find in character range... Ctrl+Shift+M

|Palist - Process: 372 svchost.exe (24744609772896) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 684 svchost.exe (247446097712512) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 684 svchost.exe (247446097712512) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 680 svchost.exe (2474460977049320) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 356 svchost.exe (2474460977049320) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 356 svchost.exe (2474460977049320) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1044 svchost.exe (247446097687936) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1044 svchost.exe (247446097687936) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1124 svchost.exe (24744614080652) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1124 svchost.exe (24744614080652) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1164 svchost.exe (24744614101322) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1164 svchost.exe (24744614101322) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1232 svchost.exe (24744614207936) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1232 svchost.exe (24744614207936) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1240 svchost.exe (247446141740672) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1240 svchost.exe (24744614201120) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1340 svchost.exe (24744614209293) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1340 svchost.exe (24744614209293) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1460 svchost.exe (247446042056064) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1460 svchost.exe (247446042047872) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1468 svchost.exe (247446042047872) [0]1[0]1[0]1[1][1676344288]

Normal text file

length: 40,178,150 lines: 356,761 Ln: 20 Col: 78 Pos: 1,514 Unix (LF) UTF-8 INS

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Find... Find in Files... Ctrl+F Ctrl+Shift+F

Find Next Shift+F3 F3 [1]0[0]1[0]1[1][1676344267

Find Previous Shift+F3 [0]1[0]1[0]1[0][1][1676344267

Select and Find Next Ctrl+F3 [1]0[0]1[0]1[0][1][1676344265

Select and Find Previous Ctrl+Shift+F3 [0]1[0]1[0]1[0][1][1676344267

Find (Volatile) Next Ctrl+Alt+F3 [1]0[0]1[0]1[0][1][1676344267

Find (Volatile) Previous Ctrl+Alt+Shift+F3 [52]1[0]1[0]1[0]1[1][1676344266

Replace... Ctrl+R Ctrl+Alt+R Ctrl+M

Incremental Search Ctrl+Alt+R

Search Results Window F7

Next Search Result F4

Previous Search Result Shift+F4

Go to... Ctrl+B

Go to Matching Brace Ctrl+Alt+B

Select All Between Matching Braces Ctrl+Alt+Shift+B

Mark... Ctrl+M

Style All Occurrences of Token

Style On Token

Clear Style

Jump Up

Jump Down

Copy Styled Text

Bookmark

Find characters in range... Ctrl+Shift+M

Find in character range... Ctrl+Shift+M

|Palist - Process: 372 svchost.exe (24744609772896) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 684 svchost.exe (247446097712512) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 684 svchost.exe (247446097712512) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 680 svchost.exe (2474460977049320) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 356 svchost.exe (2474460977049320) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 356 svchost.exe (2474460977049320) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1044 svchost.exe (247446097687936) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1044 svchost.exe (247446097687936) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1124 svchost.exe (24744614080652) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1124 svchost.exe (24744614080652) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1164 svchost.exe (24744614101322) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1164 svchost.exe (24744614101322) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1232 svchost.exe (24744614207936) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1232 svchost.exe (24744614207936) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1240 svchost.exe (247446141740672) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1240 svchost.exe (247446141740672) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1240 svchost.exe (247446141740672) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1240 svchost.exe (24744614201120) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1340 svchost.exe (24744614209293) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1340 svchost.exe (24744614209293) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1460 svchost.exe (247446042056064) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1460 svchost.exe (247446042047872) [0]1[0]1[0]1[1][1676344288

|Palist - Process: 1468 svchost.exe (247446042047872) [0]1[0]1[0]1[1][1676344288]

Normal text file

length: 40,178,150 lines: 356,761 Ln: 20 Col: 78 Sel: 10 | 1 Unix (LF) UTF-8 INS

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Find... Find in Files... Ctrl+F Ctrl+Shift+F

Find Next Shift+F3 F3 [1]0[0]1[0]1[1][1676344267

Find Previous Shift+F3 [0]1[0]1[0]1[0][1][1676344267

Select and Find Next Ctrl+F3 [1]0[0]1[0]1[0][1][1676344265

Select and Find Previous Ctrl+Shift+F3 [0]1[0]1[0]1[0][1][1676344267

Find (Volatile) Next Ctrl+Alt+F3 [1]0[0]1[0]1[0][1][1676344267

Find (Volatile) Previous Ctrl+Alt+Shift+F3 [52]1[0]1[0]1[0]1[1][1676344266

Replace... Ctrl+R Ctrl+Alt+R Ctrl+M

Incremental Search Ctrl+Alt+R

Search Results Window F7

Next Search Result F4

Previous Search Result Shift+F4

Go to... Ctrl+B

Go to Matching Brace Ctrl+Alt+B

Select All Between Matching Braces Ctrl+Alt+Shift+B

Mark... Ctrl+M

Style All Occurrences of Token

Style On Token

Clear Style

Jump Up

Jump Down

Copy Styled Text

Bookmark

Find characters in range... Ctrl+Shift+M

Find in character range... Ctrl+Shift+M

|Replace

Find what: |||

Replace with: |||

Find Next

In selection

Replace

Replace All

Replace All in All Opened Documents

Closes

Backward direction

Match whole word only

Match case

Wrap around

Search Mode

Normal

Extended (N, Y, V, B, \w)

Regular expression

Transparency

On losing focus

Always

Normal text file

length: 40,178,150 lines: 356,761 Ln: 20 Col: 78 Sel: 10 | 1 Unix (LF) UTF-8 INS

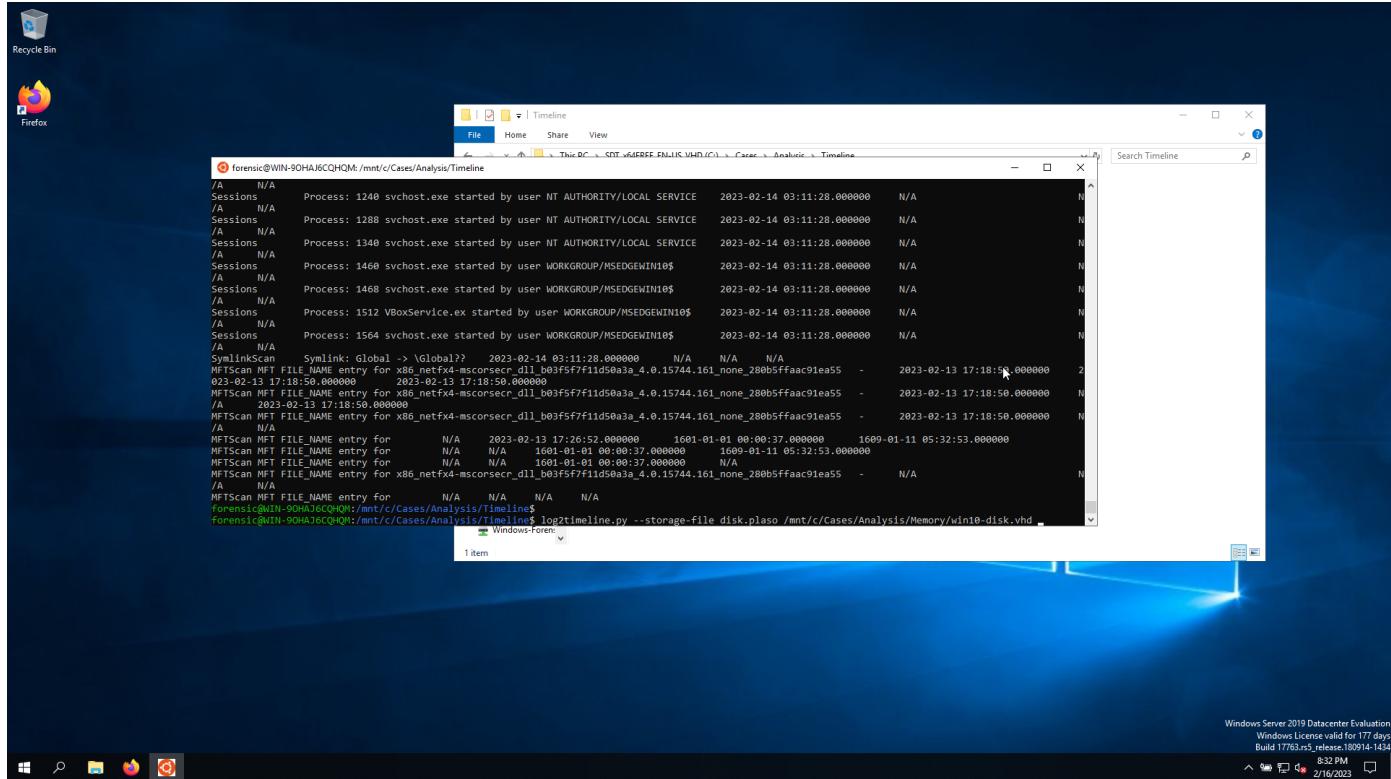
- Press two times, or until:

**Replace All: 0 occurrences were replaced in entire file**

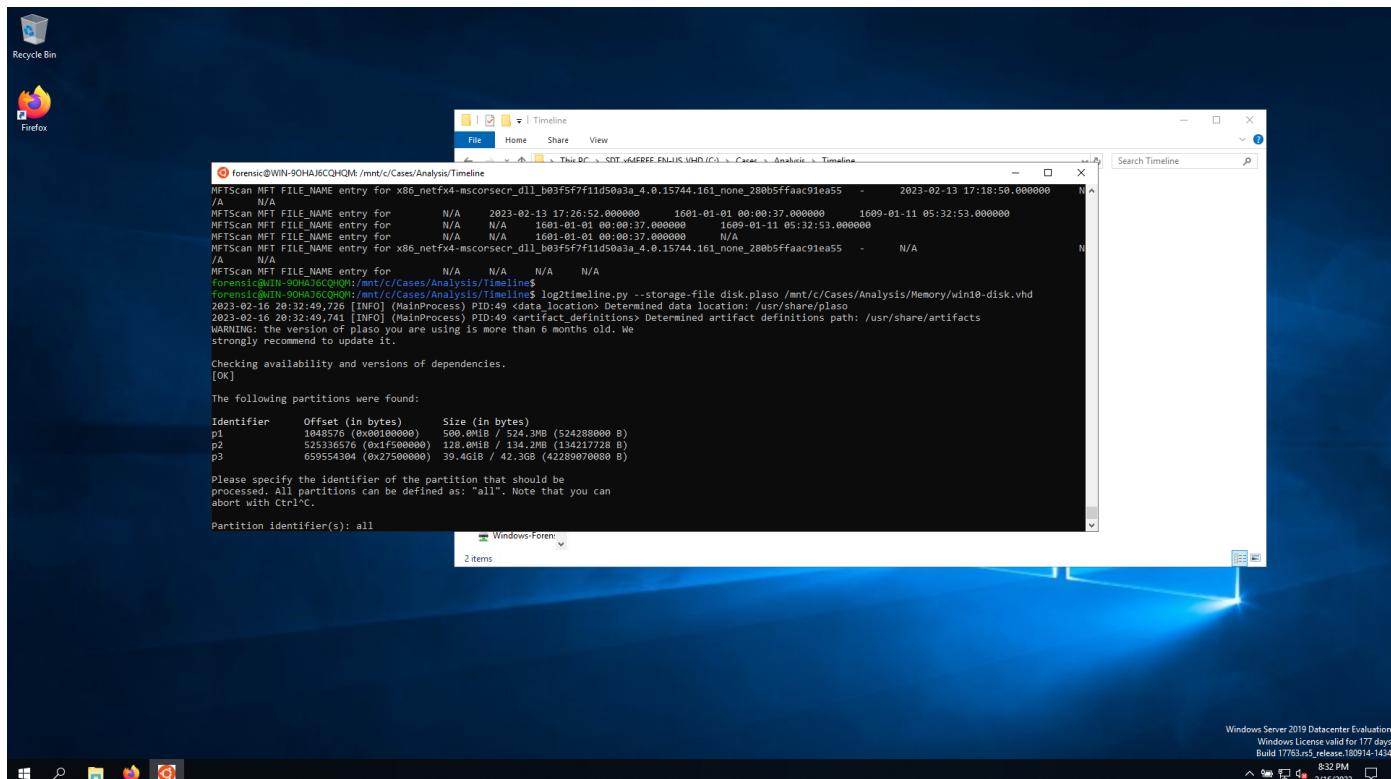
- Then save it.

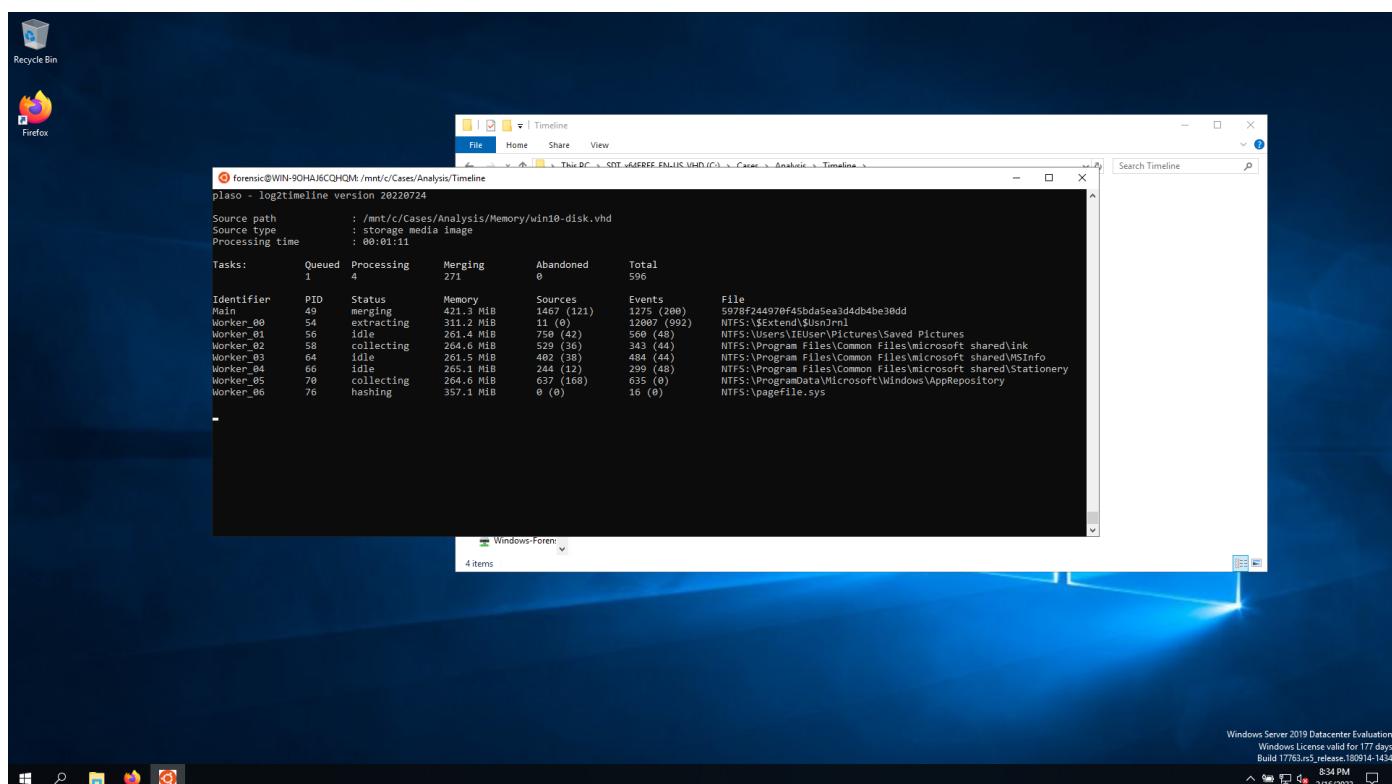
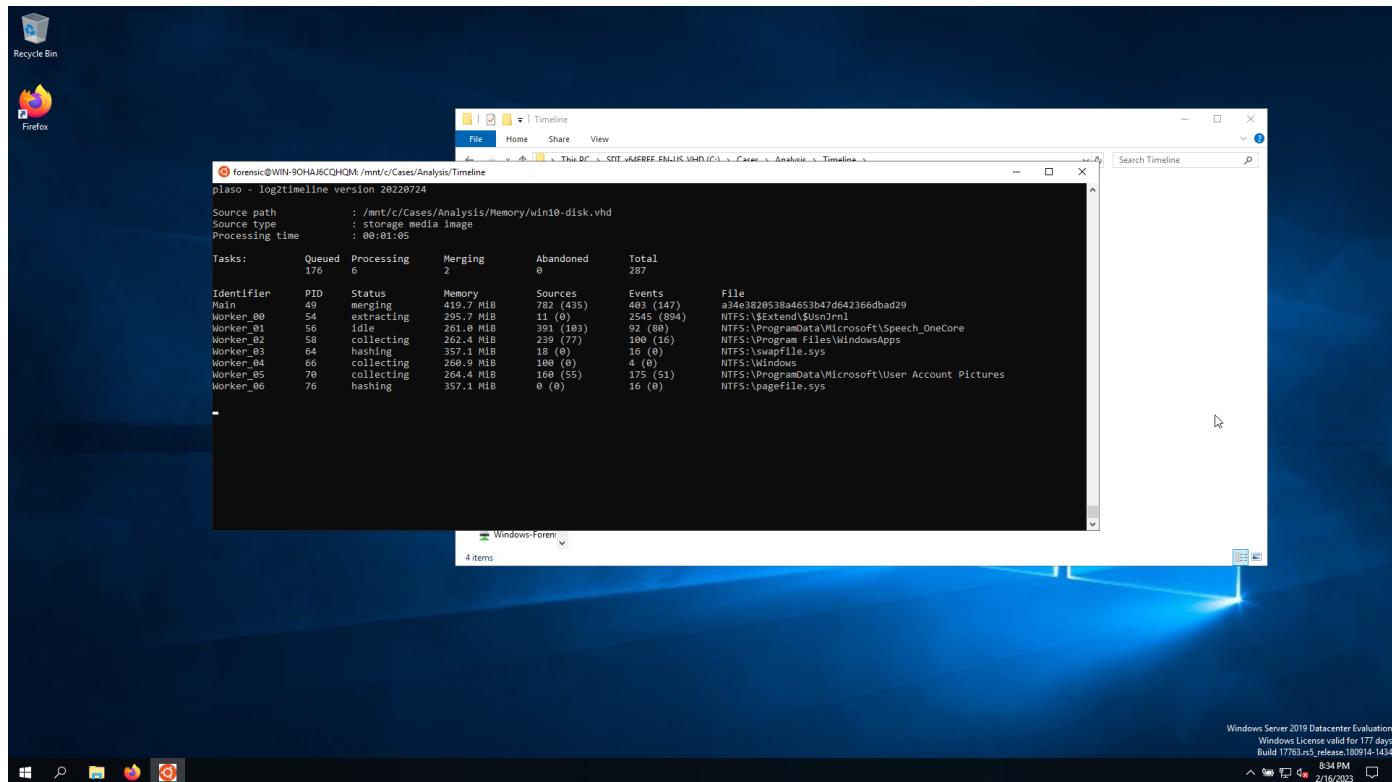
# Disk timeline creation

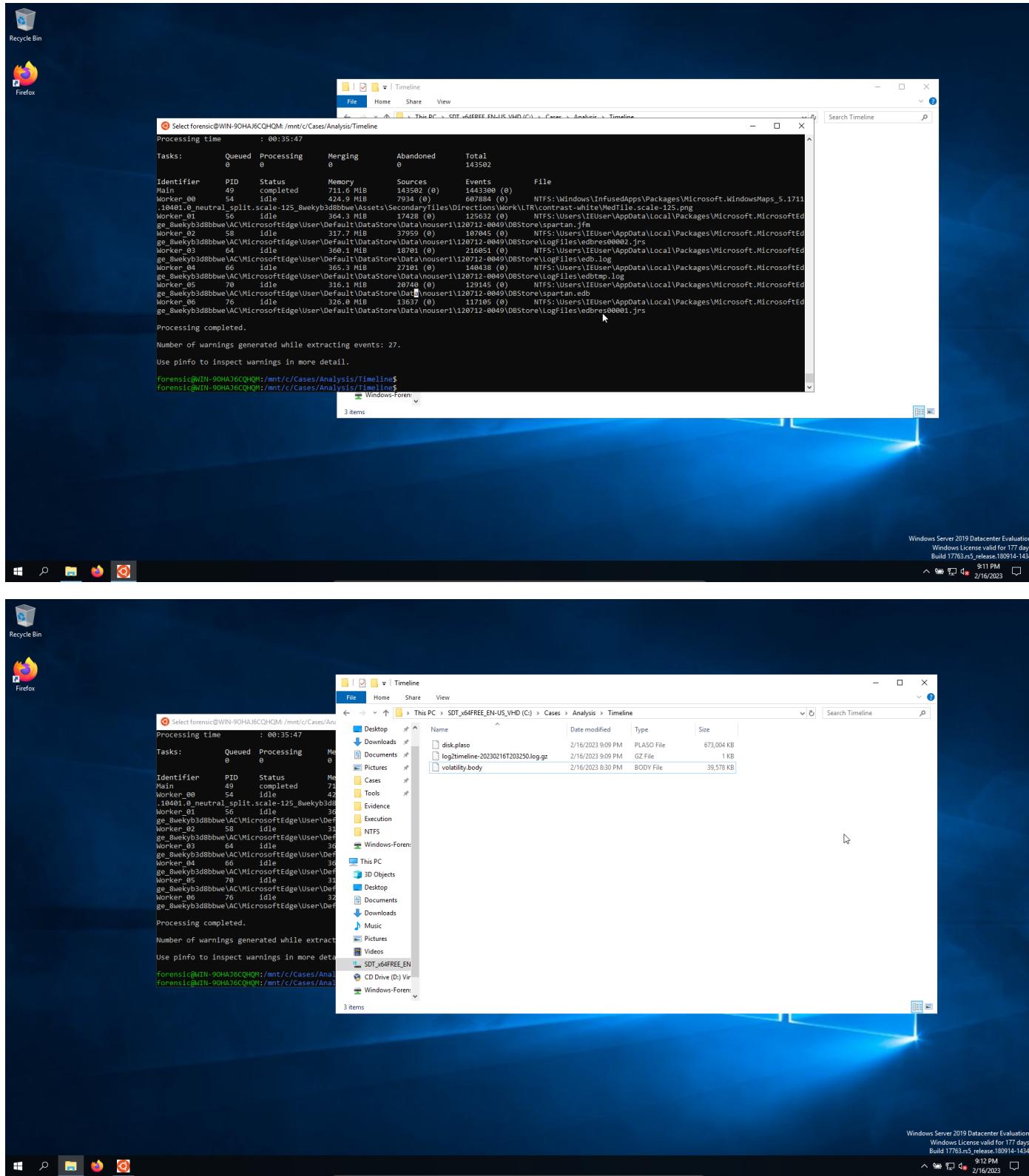
- Create .plaso file from .vhd:



- Input all:







- Print some information about the plaso file:

```

forensic@WIN-90HAJ6CQHOM:/mnt/c/Cases/Analysis/Timeline$ pinf
o.py disk.plaso
2023-02-16 21:13:01,685 [WARNING] [MainProcess] PID:83 <tools> This version of plaso is more than 6 months old.
WARNING: the version of plaso you are using is more than 6 months old. We
strongly recommend to update it.

***** Plaso Storage Information *****
Filename : disk.plaso
Format version : 0.220716
Serialization format : json

***** Sessions *****
Bea5f242-386c-4Fbc-b34D-25dbd43b8b40 : 2023-02-16T20:33:14.721014+00:00

***** Event sources *****
Total : 143502

***** Events generated per parser *****
Parser (plugin) name : Number of events
amcache : 277
appcompatcache : 488
bagman : 17
bam : 15
explorer_mountpoints2 : 6
explorer_programscache : 1
    filestat : 573755
        lnk : 572
        mylist_string : 1
        mylistex_string : 4
        mrulestext_and_shell_item : 5
        msie_webcache : 346
            msie_zone : 36
            networks : 44
olecf_automatic_descriptions : 58
    olecf_default : 125
olecf_document_summary : 8
    olecf_summary : 64
        oxml : 17
            pe : 10027
            prefetch : 674
            setupapi : 62
        shell_item : 462
        userassist : 34
            usnjhl : 277514
windows_boot : 1
    windows_run : 18
windows_sam_users : 16
windows_services : 581
windows_shutdown : 2
windows_task_cache : 426
windows_tbbzonem1 : 6
windows_tbbzonem2 : 6
windows_version : 4
    winevtx : 70442
    winlogon : 4
winreg_default : 468717
Total : 1443300

```

## Merging timelines

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

```
forensic@WIN-90HAJ6COHOM: /mnt/c/Cases/Analysis/Timeline
forensic@WIN-90HAJ6COHOM: /mnt/c/Cases/Analysis/Timeline$ log2timeline.py --parser=mactime --storage-file=disk.pisaso volatility.body

forensic@WIN-90HAJ6COHOM: /mnt/c/Cases/Analysis/Timeline
forensic@WIN-90HAJ6COHOM: /mnt/c/Cases/Analysis/Timeline$ log2Timeline version 20220724
pisaso - log2Timeline version 20220724

Source path      : /mnt/c/Cases/Analysis/Timeline/volatility.body
Source type     : single file
Processing time : 00:01:42

Identifier      PID    Status       Memory      Sources      Events      File
Main           87    completed    250.7 MB     1 (8)    1077427 (4230) 05:/mnt/c/Cases/Analysis/Timeline/volatility.body

Processing completed.

forensic@WIN-90HAJ6COHOM: /mnt/c/Cases/Analysis/Timeline$
```

```
forensic@WIN-90HAJ6CQHQH:~\mmt/c/Cases/Analysis/Timeline$ plaso - log2timeline version 20220724
Source path      : /mnt/c/Cases/Analysis/Timeline/volatility.body
Source type     : single file
Processing time : 00:01:42
Identifier      PID    Status       Memory      Sources   Events      File
Main          87    completed    250.7 MiB    1 (8)    1077427 (4230) OS:/mnt/c/Cases/Analysis/Timeline/volatility.body
Processing completed.

forensic@WIN-90HAJ6CQHQH:~\mmt/c/Cases/Analysis/Timeline$ ll
total 874268
drwxrwxrwx 1 forensic forensic      512 Feb 16 21:15 /
drwxrwxrwx 1 forensic forensic      512 Feb 16 20:09 disk/
-rw-rw-rwx 1 forensic forensic 854728512 Feb 16 21:17 disk.plaso*
-rw-rw-rwx 1 forensic forensic      400 Feb 16 21:09 log2timeline-20230216T203250.log.gz*
-rw-rw-rwx 1 forensic forensic      244 Feb 16 21:17 log2timeline-20230216T211544.log.gz*
-rw-rw-rwx 1 forensic forensic 40627393 Feb 16 20:30 volatility.body*
forensic@WIN-90HAJ6CQHQH:~\mmt/c/Cases/Analysis/Timeline$
```

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

```
forensic@WIN-90HAJ6CQHQH:~\mmt/c/Cases/Analysis/Timeline$ plaso - log2timeline version 20220724
Source path      : /mnt/c/Cases/Analysis/Timeline/volatility.body
Source type     : single file
Processing time : 00:01:42
Identifier      PID    Status       Memory      Sources   Events      File
Main          87    completed    250.7 MiB    1 (8)    1077427 (4230) OS:/mnt/c/Cases/Analysis/Timeline/volatility.body
Processing completed.

forensic@WIN-90HAJ6CQHQH:~\mmt/c/Cases/Analysis/Timeline$ ll
total 874268
drwxrwxrwx 1 forensic forensic      512 Feb 16 21:15 /
drwxrwxrwx 1 forensic forensic      512 Feb 16 20:09 disk/
-rw-rw-rwx 1 forensic forensic 854728512 Feb 16 21:17 disk.plaso*
-rw-rw-rwx 1 forensic forensic      400 Feb 16 21:09 log2timeline-20230216T203250.log.gz*
-rw-rw-rwx 1 forensic forensic      244 Feb 16 21:17 log2timeline-20230216T211544.log.gz*
-rw-rw-rwx 1 forensic forensic 40627393 Feb 16 20:30 volatility.body*
Forensic@WIN-90HAJ6CQHQH:~\mmt/c/Cases/Analysis/Timeline$ psort.py -o l2tcsv -w super-timeline.csv disk.plaso "date > '2023-02-12 00:00:00'"
```

```
forensic@WIN-90HAJ6CQHQ: /mnt/c/Cases/Analysis/Timeline
plaso - psort version 26228724

Storage file      : disk.plaso
Processing time   : 00:00:04

Events:    Filtered     In time slice    Duplicates    MACB grouped    Total
          0             0                 0               0                2528727

Identifier       PID  Status        Memory      Events      Tags      Reports
Main            91  exporting    127.2 MiB  0 (0)     0 (0)     0 (0)


```

```
forensic@WIN-9OHA4CQHOM:~\mnt/c
plaso - log2timeline version 20220724

Source path      : /mnt/c/Cases/Analysis/Evidence/win10-disk.vhd
Source type     : storage media image
Processing time  : 00:37:57

Tasks:          Queued    Processing    Merging    Abandoned    Total    140502
               0         0           0           0           0       140502

Identifier      PID   Status      Memory      Sources      Events      File
Main            2270 completed    666.0 MiB    143502 (0)    1443208 (0)    GZIP:\Users\IEUser\AppData\Local\Microsoft\OneDrive\logs\Personal\Install_2023-02-13_170828_584-68.loggz
Worker_00        2275 idle        369.1 MiB    17459 (0)     140828 (0)    GZIP:\Users\IEUser\AppData\Local\Microsoft\OneDrive\logs\Personal\StandaloneUpdate_2023-02-13_170759_4808-4612.loggz
Worker_01        2276 idle        430.2 MiB    17777 (0)     325365 (0)    NTFS:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Cache\b767b94ea5b957ab362bffdac8cd473da68be061c6C
Worker_02        2279 idle        353.2 MiB    15388 (0)     116636 (0)    NTFS:\Windows\ServiceProfiles\NetworkService\AppData\Local\Microsoft\Windows\DeliveryOptimization\Cache\b767b94ea5b957ab362bffdac8cd473da68be061c6C
F852174E-B10880E58D0444B2656A752E9372D0C8448871BAAG09F5EBFC360
Worker_03        2285 idle        362.7 MiB    32266 (0)     119719 (0)    NTFS:\Windows\SystemApps\Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3ddbbwe\23\common\monaco-editor\min\vs\language\typescript\lib\typescriptService
Worker_04        2287 idle        357.5 MiB    28600 (0)     372618 (0)    GZIP:\Users\IEUser\AppData\Local\Microsoft\OneDrive\logs\Personal\StandaloneUpdate_2023-02-13_170759_4808-4612.loggz
Worker_05        2293 idle        367.3 MiB    18977 (0)     127939 (0)    NTFS:\Windows\SystemApps\Microsoft.MicrosoftEdgeDevToolsClient_8wekyb3ddbbwe\23\common\monaco-editor\min\vs\language\typescript\src\worker.js
Worker_06        2297 idle        373.6 MiB    13682 (0)     240203 (0)    GZIP:\Users\IEUser\AppData\Local\Microsoft\OneDrive\logs\Personal\Update_2023-02-13_171153_6552-3608.loggz

Processing completed.

Number of warnings generated while extracting events: 27.

Use pinfo to inspect warnings in more detail.

Forensic@WIN-9OHA4CQHOM:~\mnt/c/Timeline\$ 11
total 39580
drwxrwxrwx 1 forensic forensic 512 Feb 16 23:18 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 16 23:18 [REDACTED]
drwxrwxrwx 1 forensic forensic 409527393 Feb 16 22:36 volatility.body*
[REDACTED]@WIN-9OHA4CQHOM:~\mnt/c/Timeline\$ cd ..
[REDACTED]@WIN-9OHA4CQHOM:~\mnt/c/Timeline\$ 11
ls: cannot read symbolic link 'Documents and Settings': Permission denied
ls: cannot access 'pagefile.sys': Permission denied
ls: 'System Volume Information': Permission denied
total 674610
drwxrwxrwx 1 forensic forensic 512 Feb 13 14:41 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 16 23:18 [REDACTED]
drwxr-xr-x 1 root          root   512 Feb 13 15:16 ../
drwxrwxrwx 1 forensic forensic 1 Sep 15 2018 BOOT0.txt*
drwxrwxrwx 1 forensic forensic 512 Sep 7 2019 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 13 14:38 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Sep 15 2018 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 16 10:08 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 16 10:08 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 16 10:08 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 13 14:40 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 13 14:40 [REDACTED]
drwxrwxrwx 1 forensic forensic 512 Feb 13 14:40 [REDACTED]
drwxrwxrwx 1 forensic forensic 4088432 Feb 16 23:16 bootmgr*
drwxrwxrwx 1 forensic forensic 690397184 Feb 16 23:16 disk_plaso*
drwxrwxrwx 1 forensic forensic 413 Feb 16 23:16 log2Timeline-20230216T223807.log.gz*
?????????? ?? ? ? ? pagefile.sys

[REDACTED]@WIN-9OHA4CQHOM:~\mnt/c\$
```

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

```
forensic@WN-90HA:~/COHM:/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)


```

```
forensic@WIN-90HAJ6CQHQH:/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    569.8 MiB  692328 (0)    0 (0)    0 (0)

Processing completed.
Forensic@WIN-90HAJ6CQHQH:/mnt/c$
```

```

forensic@WIN-9OHAJCQHQM:/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
Main 2345 completed 589.8 MiB 692328 (0)
Processing completed.
forensic@WIN-9OHAJCQHQM:/mnt/c$
```

Name	Date modified	Type	Size
Cases	2/15/2023 9:00 PM	File folder	
PerfLogs	9/15/2019 7:19 AM	File folder	
Program Files	2/16/2023 10:04 AM	File folder	
Program Files (x86)	2/16/2023 10:04 AM	File folder	
ProgramData	2/16/2023 10:04 AM	File folder	
Timeline	2/16/2023 11:18 PM	File folder	
Tools	2/13/2023 3:47 PM	File folder	
Users	2/13/2023 2:40 PM	File folder	
Windows	2/13/2023 2:40 PM	File folder	
diskplaso	2/16/2023 11:23 PM	PLASO File	835,904 KB
log2timeline-20230216T223807.log.gz	2/16/2023 11:16 PM	GZ File	1 KB
log2timeline-20230216T232127.log.gz	2/16/2023 11:23 PM	GZ File	1 KB
psort-20230216T232723.log.gz	2/16/2023 11:44 PM	GZ File	41 KB
super-timeline.csv	2/16/2023 11:44 PM	CSV File	279,171 KB

## Super timeline view with Timeline explorer

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

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

Line Tag Timestamp Source Des.. Source Name macb Inode Long Description

28 0001-01-01 00:00:00 System - N.. LOG ...b 48446 SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none>

32 0001-01-01 00:00:00 System - N.. LOG .a.. 48446 SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none>

1 2023-02-01 16:03:04 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wct2ABB.tmp Type: file

2 2023-02-06 14:41:58 File stat FILE ma..b 0 NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpnidm\5b50b566.png Type: file

3 2023-02-06 14:41:58 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpnidm\ed5d5d3ef.png Type: file

4 2023-02-07 18:53:57 MSIE WebCa.. WEBHIST m... 87721 URL: https://static-eecd.licdn.com/apc/trans.gif?151afe385c031e9ff23ad3419ed8ed1 Access count: 1 Sync count: 0 Filenam...

5 2023-02-07 18:53:57 MSIE WebCa.. WEBHIST m... 87721 URL: https://static-eecd.licdn.com/apc/trans.gif?30d092bea09847eC898b1a02ffcc6ed02 Access count: 1 Sync count: 0 Filenam...

6 2023-02-08 18:47:06 Windows Sh.. LNK ...b 87888 File size: 4096 File attribute flags: 0x00000010 Drive type: 0 Drive serial number: 0x00000000 Network path: \\VBoxSvr\MSEdge

7 2023-02-08 18:55:17 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wctD294.tmp Type: file

8 2023-02-08 19:43:28 PE Event PE ...b 91334 PE Type: Executable (EXE) Import hash: c2eff92437081e1fd6fc1e12e1d8b186

9 2023-02-09 08:42:55 File stat FILE macb 0 NTFS:\Users\IEUser\AppData\Local\Temp\BITF4AC.tmp Type: file

10 2023-02-09 20:19:21 Bodyfile FILE ma..b 0 MFTScan - MFT FILE\_NAME entry for wctCDF2.tmp Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:

11 2023-02-09 20:19:21 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wctCDF2.tmp Type: file

12 2023-02-10 21:37:51 MSIE WebCa.. WEBHIST m... 87721 URL: https://r.bing.com/rb/17jncnj1F1LrEdhNq7DoeCyhBssigCI.js?bu=Dx8oYm5xdGtlaKQBgAEoquE&or=m Access count: 4 Sync

13 2023-02-11 11:30:09 AppCompatC.. REG .... 43889 [HKEY\_LOCAL\_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 46 Path: SIGN.MEDIA=88A9CA Amd

14 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DeviceContainers.csv Type: file

15 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DevicePnps.csv Type: file

16 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DriveBinaries.csv Type: file

17 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DriverPackages.csv Type: file

18 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_ShortCuts.csv Type: file

19 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_UnassociatedFileEntries.csv Type: file

20 2023-02-11 12:31:13 File stat FILE m..c. 0 NTFS:\Users\IEUser\Desktop\PPW-main.zip Type: file

21 2023-02-11 14:04:31 Windows Sh.. LNK m... 87888 File size: 4096 File attribute flags: 0x00000010 Drive type: 0 Drive serial number: 0x00000000 Network path: \\VBoxSvr\MSEdge

22 2023-02-12 21:02:12 MSIE WebCa.. WEBHIST m... 87721 URL: https://onems-live.azureedge.net/api/settings-en-US/xml/settings-tipset?release=r4 Access count: 3 Sync count: 0 Filenam...

23 2023-02-13 00:00:00 File stat FILE .a.. 324613 TSK:\EFI\Boot\bootx64.efi Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

24 2023-02-13 00:00:00 File stat FILE .a.. 389 TSK:\EFI\Microsoft\Boot\BCD Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

25 2023-02-13 00:00:00 File stat FILE .a.. 398 TSK:\EFI\Microsoft\Boot\bootmgfw.efi Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

26 2023-02-13 07:33:59 PE Event PE ...b 93000 PE Type: Dynamic Link Library (DLL)

27 2023-02-13 07:34:00 PE Event PE ...b 92998 PE Type: Dynamic Link Library (DLL)

28 2023-02-13 09:05:52 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@Host: login.live.com Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 2 Cont

29 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@windowsDefender:/// Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 4 Cont

30 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@Host: This PC Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 5 Contain

31 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@https://login.live.com/oauth2\_desktop.srf?lc=1033 Access count: 2 Sync count: 0 Cached file s

32 2023-02-13 09:11:54 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@https://login.live.com/oauth2\_desktop.srf?lc=1033 Access count: 2 Sync count: 0 Cached file s

Total lines 475,070 | Visible lines 475,070 | Open files: 1 | Search options

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

Line Tag Timestamp Source Des.. Source Name macb Inode Long Description

28 0001-01-01 00:00:00 System - N.. LOG ...b 48446 SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none>

32 0001-01-01 00:00:00 System - N.. LOG .a.. 48446 SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none>

1 2023-02-01 16:03:04 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wct2ABB.tmp Type: file

2 2023-02-06 14:41:58 File stat FILE ma..b 0 NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpnidm\5b50b566.png Type: file

3 2023-02-06 14:41:58 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpnidm\ed5d5d3ef.png Type: file

4 2023-02-07 18:53:57 MSIE WebCa.. WEBHIST m... 87721 URL: https://static-eecd.licdn.com/apc/trans.gif?151afe385c031e9ff23ad3419ed8ed1 Access count: 1 Sync count: 0 Filenam...

5 2023-02-07 18:53:57 MSIE WebCa.. WEBHIST m... 87721 URL: https://static-eecd.licdn.com/apc/trans.gif?30d092bea09847eC898b1a02ffcc6ed02 Access count: 1 Sync count: 0 Filenam...

6 2023-02-08 18:47:06 Windows Sh.. LNK ...b 87888 File size: 4096 File attribute flags: 0x00000010 Drive type: 0 Drive serial number: 0x00000000 Network path: \\VBoxSvr\MSEdge

7 2023-02-08 18:55:17 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wctD294.tmp Type: file

8 2023-02-08 19:43:28 PE Event PE ...b 91334 PE Type: Executable (EXE) Import hash: c2eff92437081e1fd6fc1e12e1d8b186

9 2023-02-09 08:42:55 File stat FILE macb 0 NTFS:\Users\IEUser\AppData\Local\Temp\BITF4AC.tmp Type: file

10 2023-02-09 20:19:21 Bodyfile FILE ma..b 0 MFTScan - MFT FILE\_NAME entry for wctCDF2.tmp Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:

11 2023-02-09 20:19:21 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wctCDF2.tmp Type: file

12 2023-02-10 21:37:51 MSIE WebCa.. WEBHIST m... 87721 URL: https://r.bing.com/rb/17jncnj1F1LrEdhNq7DoeCyhBssigCI.js?bu=Dx8oYm5xdGtlaKQBgAEoquE&or=m Access count: 4 Sync

13 2023-02-11 11:30:09 AppCompatC.. REG .... 43889 [HKEY\_LOCAL\_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 46 Path: SIGN.MEDIA=88A9CA Amd

14 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DeviceContainers.csv Type: file

15 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DevicePnps.csv Type: file

16 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DriveBinaries.csv Type: file

17 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DriverPackages.csv Type: file

18 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_ShortCuts.csv Type: file

19 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_UnassociatedFileEntries.csv Type: file

20 2023-02-11 12:31:13 File stat FILE m..c. 0 NTFS:\Users\IEUser\Desktop\PPW-main.zip Type: file

21 2023-02-11 14:04:31 Windows Sh.. LNK m... 87888 File size: 4096 File attribute flags: 0x00000010 Drive type: 0 Drive serial number: 0x00000000 Network path: \\VBoxSvr\MSEdge

22 2023-02-12 21:02:12 MSIE WebCa.. WEBHIST m... 87721 URL: https://onems-live.azureedge.net/api/settings-en-US/xml/settings-tipset?release=r4 Access count: 3 Sync count: 0 Filenam...

23 2023-02-13 00:00:00 File stat FILE .a.. 324613 TSK:\EFI\Boot\bootx64.efi Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

24 2023-02-13 00:00:00 File stat FILE .a.. 389 TSK:\EFI\Microsoft\Boot\BCD Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

25 2023-02-13 00:00:00 File stat FILE .a.. 398 TSK:\EFI\Microsoft\Boot\bootmgfw.efi Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

26 2023-02-13 07:33:59 PE Event PE ...b 93000 PE Type: Dynamic Link Library (DLL)

27 2023-02-13 07:34:00 PE Event PE ...b 92998 PE Type: Dynamic Link Library (DLL)

28 2023-02-13 09:05:52 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@Host: login.live.com Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 2 Cont

29 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@windowsDefender:/// Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 4 Cont

30 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@Host: This PC Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 5 Contain

31 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@https://login.live.com/oauth2\_desktop.srf?lc=1033 Access count: 2 Sync count: 0 Cached file s

32 2023-02-13 09:11:54 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@https://login.live.com/oauth2\_desktop.srf?lc=1033 Access count: 2 Sync count: 0 Cached file s

Total lines 475,070 | Visible lines 475,070 | Open files: 1 | Search options

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

Line Tag Timestamp Source Des.. Source Name macb Inode Long Description

28 0001-01-01 00:00:00 System - N.. LOG ...b 48446 SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none>

32 0001-01-01 00:00:00 System - N.. LOG .a.. 48446 SSID: Network Description: Network Connection Type: Wired Default Gateway Mac: 52:54:00:12:35:02 DNS Suffix: <none>

1 2023-02-01 16:03:04 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wct2ABB.tmp Type: file

2 2023-02-06 14:41:58 File stat FILE ma..b 0 NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpnidm\5b50b566.png Type: file

3 2023-02-06 14:41:58 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Microsoft\Windows\Notifications\wpnidm\ed5d5d3ef.png Type: file

4 2023-02-07 18:53:57 MSIE WebCa.. WEBHIST m... 87721 URL: https://static-eecd.licdn.com/apc/trans.gif?151afe385c031e9ff23ad3419ed8ed1 Access count: 1 Sync count: 0 Filenam...

5 2023-02-07 18:53:57 MSIE WebCa.. WEBHIST m... 87721 URL: https://static-eecd.licdn.com/apc/trans.gif?30d092bea09847eC898b1a02ffcc6ed02 Access count: 1 Sync count: 0 Filenam...

6 2023-02-08 18:47:06 Windows Sh.. LNK ...b 87888 File size: 4096 File attribute flags: 0x00000010 Drive type: 0 Drive serial number: 0x00000000 Network path: \\VBoxSvr\MSEdge

7 2023-02-08 18:55:17 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wctD294.tmp Type: file

8 2023-02-08 19:43:28 PE Event PE ...b 91334 PE Type: Executable (EXE) Import hash: c2eff92437081e1fd6fc1e12e1d8b186

9 2023-02-09 08:42:55 File stat FILE macb 0 NTFS:\Users\IEUser\AppData\Local\Temp\BITF4AC.tmp Type: file

10 2023-02-09 20:19:21 Bodyfile FILE ma..b 0 MFTScan - MFT FILE\_NAME entry for wctCDF2.tmp Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:

11 2023-02-09 20:19:21 File stat FILE m..b 0 NTFS:\Users\IEUser\AppData\Local\Temp\wctCDF2.tmp Type: file

12 2023-02-10 21:37:51 MSIE WebCa.. WEBHIST m... 87721 URL: https://r.bing.com/rb/17jncnj1F1LrEdhNq7DoeCyhBssigCI.js?bu=Dx8oYm5xdGtlaKQBgAEoquE&or=m Access count: 4 Sync

13 2023-02-11 11:30:09 AppCompatC.. REG .... 43889 [HKEY\_LOCAL\_MACHINE\System\ControlSet001\Control\Session Manager\AppCompatCache] Cached entry: 46 Path: SIGN.MEDIA=88A9CA Amd

14 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DeviceContainers.csv Type: file

15 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DevicePnps.csv Type: file

16 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DriveBinaries.csv Type: file

17 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_DriverPackages.csv Type: file

18 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_ShortCuts.csv Type: file

19 2023-02-11 12:30:38 File stat FILE m..b 0 NTFS:\Users\IEUser\Desktop\PPW-main\amcache2\20230211043035\_Amcache\_UnassociatedFileEntries.csv Type: file

20 2023-02-11 12:31:13 File stat FILE m..c. 0 NTFS:\Users\IEUser\Desktop\PPW-main.zip Type: file

21 2023-02-11 14:04:31 Windows Sh.. LNK m... 87888 File size: 4096 File attribute flags: 0x00000010 Drive type: 0 Drive serial number: 0x00000000 Network path: \\VBoxSvr\MSEdge

22 2023-02-12 21:02:12 MSIE WebCa.. WEBHIST m... 87721 URL: https://onems-live.azureedge.net/api/settings-en-US/xml/settings-tipset?release=r4 Access count: 3 Sync count: 0 Filenam...

23 2023-02-13 00:00:00 File stat FILE .a.. 324613 TSK:\EFI\Boot\bootx64.efi Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

24 2023-02-13 00:00:00 File stat FILE .a.. 389 TSK:\EFI\Microsoft\Boot\BCD Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

25 2023-02-13 00:00:00 File stat FILE .a.. 398 TSK:\EFI\Microsoft\Boot\bootmgfw.efi Type: file Owner identifier: 0 Group identifier: 0 Mode: 0x777 Number of links: 1

26 2023-02-13 07:33:59 PE Event PE ...b 93000 PE Type: Dynamic Link Library (DLL)

27 2023-02-13 07:34:00 PE Event PE ...b 92998 PE Type: Dynamic Link Library (DLL)

28 2023-02-13 09:05:52 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@Host: login.live.com Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 2 Cont

29 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@windowsDefender:/// Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 4 Cont

30 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@Host: This PC Access count: 1 Sync count: 0 Cached file size: 0 Entry identifier: 5 Contain

31 2023-02-13 09:07:01 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@https://login.live.com/oauth2\_desktop.srf?lc=1033 Access count: 2 Sync count: 0 Cached file s

32 2023-02-13 09:11:54 MSIE WebCa.. WEBHIST m... 87721 URL: :2023021320230214: IEUser@https://login.live.com/oauth2\_desktop.srf?lc=1033 Access count: 2 Sync count: 0 Cached file s

Total lines 475,070 | Visible lines 475,070 | Open files: 1 | Search options

## Analyzing malicious activity based on Super Timeline

- Filter timestamps on the day of the cyber attack:

- Search ART-attack.ps1:

Timeline Explorer v1.3.0										
File Tools Tabs View Help										
super-timeline.csv										
Drag a column header here to group by that column										
Line	Tag	Timestamp	Source Desc.	Source Name	macb	Inode	Long Description	ART-attack.ps1	x	Find
37		2023-02-13 09:23:28	MSIE WebCa...	WEBHIST	m...	87721	URL: :2023012320230214: !IUser@file:///C:/Users/IEUser/Desktop/PwF-main/PwF-main/AtomicRedTeam/ART-attack.ps1 Access count: 1			
362841		2023-02-13 17:21:03	Bodyfile	FILE	macb		0 MFTScan - MFT FILE_NAME entry for ART-attack.ps1 Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:			
362904		2023-02-13 17:21:03	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE			
362905		2023-02-13 17:21:03	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE			
362906		2023-02-13 17:21:03	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_FILE_CREATE			
362907		2023-02-13 17:21:03	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA_EXTEND			
362908		2023-02-13 17:21:03	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA_EXTEND			
362909		2023-02-13 17:21:03	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE			
362910		2023-02-13 17:21:03	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE			
363206		2023-02-13 17:21:04	File entry...	FILE	ma.b	225	Name: PwF-main Long name: PwF-main NTFS file reference: 22968-2 Shell item path: <My Computer> \{bf4ffcc3a\}db2c\424c\b029-7fe99			
363213		2023-02-13 17:21:04	File entry...	FILE	ma.b	225	Name: PwF-main Long name: PwF-main NTFS file reference: 23026-2 Shell item path: <My Computer> \{bf4ffcc3a\}db2c\424c\b029-7fe99			
363220		2023-02-13 17:21:04	File entry...	FILE	ma.b	225	Name: ATOMIC_1 Long name: AtomicRedTeam NTFS file reference: 28668-2 Shell item path: <My Computer> \{bf4ffcc3a\}db2c\424c\b029-7fe99			
397054		2023-02-13 17:23:27	Windows Sh...	LNK	...a.	88253	File size: 3360 File attribute flags: 0x00000080 Drive type: 3 Drive serial number: 0x3a97874f Volume label: Local path: C:\			
397055		2023-02-13 17:23:27	Windows Sh...	LNK	...a.	225	File size: 3360 File attribute flags: 0x00000080 Drive type: 3 Drive serial number: 0x3a97874f Volume label: Local path: C:\			
397066		2023-02-13 17:23:28	Bodyfile	FILE	macb		0 MFTScan - MFT FILE_NAME entry for ART-attack.ps1!lnk Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:			
397070		2023-02-13 17:23:28	File entry...	FILE	...a.	88253	Name: ART-2.ps1 Long name: ART-attack.ps1!lnk NTFS file reference: 28674-2 Shell item path: <My Computer> \{bf4ffcc3a\}db2c\424c\b029-7fe99			
397084		2023-02-13 17:23:28	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_OBJECT_ID_CHANGE			
397085		2023-02-13 17:23:28	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_OBJECT_ID_CHANGE			
397086		2023-02-13 17:23:28	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1!lnk File reference: 225-2 Parent file reference: 87338-1 Update source: Update reason: USN_REASON_FILE_CREATE			
397087		2023-02-13 17:23:28	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1!lnk File reference: 225-2 Parent file reference: 87338-1 Update source: Update reason: USN_REASON_DATA_EXTEND			
397088		2023-02-13 17:23:28	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1!lnk File reference: 225-2 Parent file reference: 87338-1 Update source: Update reason: USN_REASON_DATA_EXTEND			
397089		2023-02-13 17:23:28	File stat	FILE	macb		0 NTFS: \Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\ART-attack.ps1.lnk Type: file			
397090		2023-02-13 17:23:28	MSIE WebCa...	WEBHIST	....	87721	URL: :2023012320230214: !IUser@file:///C:/Users/IEUser/Desktop/PwF-main/PwF-main/AtomicRedTeam/ART-attack.ps1 Access count: 1			
397091		2023-02-13 17:23:28	MSIE WebCa...	WEBHIST	....	87721	URL: Visited: !IUser@file:///C:/Users/IEUser/Desktop/PwF-main/PwF-main/AtomicRedTeam/ART-attack.ps1 Access count: 1 Sync count: 1			
397099		2023-02-13 17:23:28	MSIE WebCa...	WEBHIST	...a.	87721	URL: :2023012320230214: !IUser@file:///C:/Users/IEUser/Desktop/PwF-main/PwF-main/AtomicRedTeam/ART-attack.ps1 Access count: 1 Sync count: 1			
397100		2023-02-13 17:23:28	MSIE WebCa...	WEBHIST	ma...	87721	URL: Visited: !IUser@file:///C:/Users/IEUser/Desktop/PwF-main/PwF-main/AtomicRedTeam/ART-attack.ps1 Access count: 1 Sync count: 1			
397101		2023-02-13 17:23:28	OLECF Dest...	OLECF	m...	88253	Entry: 5 Pin status: Unpinned Hostname: msedgewin10 Path: C:\Users\IEUser\Desktop\PwF-main\PwF-main\AtomicRedTeam\ART-attack...			
397174		2023-02-13 17:23:33	Registry K...	REG	m...	87315	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs]@ps1 Index: 1 [MRU Value 2]: ART-attack...			
397175		2023-02-13 17:23:33	Registry K...	REG	m...	87315	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs]@ps1 Index: 1 [MRU Value 2]: Path: ART-attack...			
397180		2023-02-13 17:23:33	Registry K...	REG	m...	87315	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs]@ps1 Index: 1 [MRU Value 11]: Path: AtomicRedTeam\ART-attack...			
397228		2023-02-13 17:23:58	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA_TRUNCATED			
397229		2023-02-13 17:23:58	NTFS USN c...	FILE	...c.	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA_EXTEND			

#### - Search ART-attack:

#### - Execution of file:

Timeline Explorer v1.3.0									
File	Tools	Tabs	View	Help					
super-timeline.csv									
Drag a column header here to group by that column									
Line	Tag	Timestamp	Source Des...	Source Name	macb	Inode	Long Description	AUT-attack	x
▼	■	=	¶	¶	¶	=	¶		
397088		2023-02-13 17:23:28	NTFS USN ...	FILE	...	83391	ART-attack.ps1.lnk File reference: 225-2 Parent file reference: 87338-1 Update source: Update reason: USN_REASON_DATA_EXTEND		
397089		2023-02-13 17:23:28	File stat	FILE	macb		0 NTFS:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\ART-attack.ps1.lnk Type: file		
397090		2023-02-13 17:23:28	MSIE WebCa...	WEBHIST	....	87721	URL: :2023021320230214: IEUser@file:///C:/Users/IEUser/Desktop/PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1	Access count: 1	
397091		2023-02-13 17:23:28	MSIE WebCa...	WEBHIST	....	87721	URL: Visited: IEUser@file:///C:/Users/IEUser/Desktop/PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1	Access count: 1	Sync count: 1
397099		2023-02-13 17:23:28	MSIE WebCa...	WEBHIST	a...	87721	URL: :2023021320230214: IEUser@file:///C:/Users/IEUser/Desktop/PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1	Access count: 1	
397100		2023-02-13 17:23:28	MSIE WebCa...	WEBHIST	ma...	87721	URL: Visited: IEUser@file:///C:/Users/IEUser/Desktop/PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1	Access count: 1	Sync count: 1
397101		2023-02-13 17:23:28	OLECF Dest...	OLECF	m...	88253	Entry: 5 Pin status: Unpinned Hostname: msedgewin10 Path: C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1		
397136		2023-02-13 17:23:33	Bodyfile	FILE	macb		0 MFTScan - 213 FILE_NAME entry for ART-attack-cleanup.ps1.lnk Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:		
397143		2023-02-13 17:23:33	MSIE WebCa...	WEBHIST	....	87721	URL: :2023021320230214: IEUser@file:///C:/Users/IEUser/Desktop/PWF-main\PWF-main\AtomicRedTeam\ART-attack-cleanup.ps1	Access count: 1	
397144		2023-02-13 17:23:33	MSIE WebCa...	WEBHIST	....	87721	URL: Visited: IEUser@file:///C:/Users/IEUser/Desktop/PWF-main\PWF-main\AtomicRedTeam\ART-attack-cleanup.ps1	Access count: 1	Sync count: 1
397145		2023-02-13 17:23:33	NTFS USN ...	FILE	...	83391	ART-attack.cleanup.ps1 File reference: 28671-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_OBJEC		
397146		2023-02-13 17:23:33	NTFS USN ...	FILE	...	83391	ART-attack.cleanup.ps1 File reference: 28671-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_OBJEC		
397149		2023-02-13 17:23:33	NTFS USN ...	FILE	...	83391	ART-attack.cleanup.ps1.lnk File reference: 227-2 Parent file reference: 87338-1 Update source: Update reason: USN_REASON_FIL		
397150		2023-02-13 17:23:33	NTFS USN ...	FILE	...	83391	ART-attack.cleanup.ps1.lnk File reference: 227-2 Parent file reference: 87338-1 Update source: Update reason: USN_REASON_DAT		
397151		2023-02-13 17:23:33	NTFS USN ...	FILE	...	83391	ART-attack.cleanup.ps1.lnk File reference: 227-2 Parent file reference: 87338-1 Update source: Update reason: USN_REASON_DAT		
397160		2023-02-13 17:23:33	File stat	FILE	macb		0 NTFS:\Users\IEUser\AppData\Roaming\Microsoft\Windows\Recent\ART-attack-cleanup.ps1.lnk Type: file		
397169		2023-02-13 17:23:33	MSIE WebCa...	WEBHIST	a...	87721	URL: :2023021320230214: IEUser@file:///C:/Users/IEUser/Desktop/PWF-main\PWF-main\AtomicRedTeam\ART-attack-cleanup.ps1	Access count: 1	
397170		2023-02-13 17:23:33	MSIE WebCa...	WEBHIST	m...	87721	URL: Visited: IEUser@file:///C:/Users/IEUser/Desktop/PWF-main\PWF-main\AtomicRedTeam\ART-attack-cleanup.ps1	Access count: 1	Sync count: 1
397171		2023-02-13 17:23:33	OLECF Dest...	OLECF	m...	88253	Entry: 6 Pin status: Unpinned Hostname: msedgewin10 Path: C:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack-cleanup.ps1		
397174		2023-02-13 17:23:33	Registry K...	REG	...	87315	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs].ps1 Index: 1 [MRU Value 2]: ART-attack cle		
397175		2023-02-13 17:23:33	Registry K...	REG	...	87315	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs].ps1 Index: 1 [MRU Value 2]: Path: ART-atta		
397180		2023-02-13 17:23:33	Registry K...	REG	...	87315	[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs] Index: 1 [MRU Value 11]: Path: AtomicRedTeam		
397222		2023-02-13 17:23:57	NTFS USN ...	FILE	...	83391	ART-attack.cleanup.ps1 File reference: 28671-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA		
397223		2023-02-13 17:23:57	NTFS USN ...	FILE	...	83391	ART-attack.cleanup.ps1 File reference: 28671-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA		
397224		2023-02-13 17:23:57	NTFS USN ...	FILE	...	83391	ART-attack.cleanup.ps1 File reference: 28671-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA		
397225		2023-02-13 17:23:57	File stat	FILE	mac...		0 NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack-cleanup.ps1 Type: file		
397228		2023-02-13 17:23:58	NTFS USN ...	FILE	...	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA_TRUNCATI		
397229		2023-02-13 17:23:58	NTFS USN ...	FILE	...	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA_EXTEND		
397230		2023-02-13 17:23:58	NTFS USN ...	FILE	...	83391	ART-attack.ps1 File reference: 28674-2 Parent file reference: 28668-2 Update source: Update reason: USN_REASON_DATA_EXTEND		
397231		2023-02-13 17:23:58	File stat	FILE	m.c...		0 NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1 Type: file		
399108		2023-02-13 17:26:46	File stat	FILE	a...		0 NTFS:\Users\IEUser\Desktop\PWF-main\PWF-main\AtomicRedTeam\ART-attack.ps1 Type: file		

- Search for AtomicService.exe:

Timeline Explorer v1.3.0									
File Tools Tabs View Help									
super-timeline.csv									
Drag a column header here to group by that column									
Line	Tag	Timestamp	Source Des...	Source Name	macb	Inode	Long Description	atomicservice.exe	
=	=	=	=	=	=	=	=	x	Find
445658		2023-02-13 17:28:09	Bodyfile	FILE	macb		0 MFTScan - MFT FILE_NAME entry for <b>AtomicService.exe</b> Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:		
446875		2023-02-13 17:28:09	NTFS USN ...	FILE	...	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_FILE_CREAT		
446876		2023-02-13 17:28:09	NTFS USN ...	FILE	...	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEN		
446877		2023-02-13 17:28:09	NTFS USN ...	FILE	...	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEN		
446878		2023-02-13 17:28:09	NTFS USN ...	FILE	...	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO		
446879		2023-02-13 17:28:09	NTFS USN ...	FILE	...	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO		
446892		2023-02-13 17:28:09	File stat	FILE	...	84525	0 NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file		
446896		2023-02-13 17:28:09	WinEvtX	EVT	m..b		0 DLL! - DLL Load: Process 4248 AtomicService. Loaded <b>AtomicService.exe</b> (C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.		
449342		2023-02-13 17:28:30	Bodyfile	FILE	...	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['EXE'		
449376		2023-02-13 17:28:30	WinEvtX	EVT	m..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
449378		2023-02-13 17:28:30	WinEvtX	EVT	m..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
449385		2023-02-13 17:28:30	WinEvtX	EVT	m..b	83681	[7045 / 0x1b85] Provider identifier: {5595908d1-a6d7-4695-8e1e-26931d2012f4} Source Name: Service Control Manager Strings: ['Ata		
449386		2023-02-13 17:28:30	Registry K...	REG	...	43889	[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\AtomicTestService_CMD] Type: Service - Own Process (0x10) Start: Manual (3) I		
449388		2023-02-13 17:28:30	WinEvtX	EVT	m..b	84525	[13 / 0x0000] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['T103		
449389		2023-02-13 17:28:30	WinEvtX	EVT	m..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
449390		2023-02-13 17:28:30	WinEvtX	EVT	m..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
449391		2023-02-13 17:28:30	WinPrefetch	LOG	...	107815	Prefetch [ <b>ATOMICSERVICE.EXE</b> ] was executed - run count 1 path hints: \ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCD0341815D502		
449392		2023-02-13 17:28:30	File stat	FILE	...	0	NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file		
449512		2023-02-13 17:28:38	Bodyfile	FILE	macb		0 MFTScan - MFT FILE_NAME entry for <b>ATOMICSERVICE.EXE</b> 59E20F94.pf Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:		
449514		2023-02-13 17:28:38	NTFS USN ...	FILE	...	83391	<b>ATOMICSERVICE.EXE</b> -59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON		
449515		2023-02-13 17:28:38	NTFS USN ...	FILE	...	83391	<b>ATOMICSERVICE.EXE</b> -59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON		
449516		2023-02-13 17:28:38	NTFS USN ...	FILE	...	83391	<b>ATOMICSERVICE.EXE</b> -59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON		
449517		2023-02-13 17:28:38	File stat	FILE	macb		0 NTFS:\Windows\Prefetch\ATOMICSERVICE.EXE-59E20F94.pf Type: file		
451783		2023-02-13 17:56:59	WinEvtX	EVT	m..b	84525	[8 / 0x0008] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
451883		2023-02-13 17:56:59	File stat	FILE	...	83391	0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file		
451885		2023-02-13 17:56:59	NTFS USN ...	FILE	...	83391	<b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_FILE_CR		
451886		2023-02-13 17:56:59	NTFS USN ...	FILE	...	83391	<b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EX		
451887		2023-02-13 17:56:59	NTFS USN ...	FILE	...	83391	<b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EX		
451891		2023-02-13 17:56:59	File stat	FILE	mac		0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file		
451893		2023-02-13 17:56:59	WinEvtX	EVT	m..b	84525	[11 / 0x0000] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['Proc		

Timeline Explorer v1.3.0									
File Tools Tabs View Help									
super-timeline.csv									
Drag a column header here to group by that column									
Line	Tag	Timestamp	Source Des...	Source Name	macb	Inode	Long Description		atomicservice.exe
Y		=				=			x   Find
445658		2023-02-13 17:28:09	Bodyfile	FILE	macb	0	MFTScan - MFT FILE_NAME entry for <b>AtomicService.exe</b> Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:		
446875		2023-02-13 17:28:09	NTFS USN ...	FILE	...c.	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_FILE_CREAT		
446876		2023-02-13 17:28:09	NTFS USN ...	FILE	...c.	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEN		
446877		2023-02-13 17:28:09	NTFS USN ...	FILE	...c.	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEN		
446878		2023-02-13 17:28:09	NTFS USN ...	FILE	...c.	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO		
446879		2023-02-13 17:28:09	NTFS USN ...	FILE	...c.	83391	<b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO		
446892		2023-02-13 17:28:09	File stat	FILE	...cb	0	NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file		
446896		2023-02-13 17:28:09	WinEventX	EVT	m..b	84525	[1 / 0x000b] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['EXE'		
449342		2023-02-13 17:28:09	Bodyfile	FILE	...c..b	0	DLLIST - DLL Load: Process 4248 AtomicService_Loaded <b>AtomicService.exe</b> (C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe)		
449376		2023-02-13 17:28:09	File stat	FILE	...c..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
449378		2023-02-13 17:28:09	FILE OPENING	FILE	...c..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
449385		2023-02-13 17:28:09	WEB HISTORY	FILE	...c..b	85681	[7/845 /1085] Provider identifier: {555908d1-a6d7-4695-8e1e-26931d2012f4} Source Name: Service Control Manager Strings: ['Ato		
449386		2023-02-13 17:28:09	DELETED DATA	FILE	...c..b	43889	[KEY\LOCAL_MACHINE\System\ControlSet001\Services\AtomicService\CMD] Type: Service - Own Process (0x10) Start: Manual (3) I		
449388		2023-02-13 17:28:09	EXECUTION	FILE	...c..b	84525	[13 / 0x000d] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['T103		
449389		2023-02-13 17:28:09	Process (0x00000000)	FILE	...c..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
449390		2023-02-13 17:28:09	File stat	FILE	...c..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
449391		2023-02-13 17:28:09	LOG FILE	FILE	a...	10781	Prefetch [ <b>ATOMICSERVICE_EXE</b> ] was executed - run count 1 path hints: \ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F500CD3418150502F		
449392		2023-02-13 17:28:09	File stat	FILE	a...	0	NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file		
449512		2023-02-13 17:28:38	Bodyfile	FILE	macb	0	MFTScan - MFT FILE_NAME entry for <b>ATOMICSERVICE_EXE</b> -59E20F94.pf Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:		
449514		2023-02-13 17:28:38	NTFS USN ...	FILE	...c.	83391	<b>ATOMICSERVICE_EXE</b> -59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON		
449515		2023-02-13 17:28:38	NTFS USN ...	FILE	...c.	83391	<b>ATOMICSERVICE_EXE</b> -59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON		
449516		2023-02-13 17:28:38	NTFS USN ...	FILE	...c.	83391	<b>ATOMICSERVICE_EXE</b> -59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON		
449517		2023-02-13 17:28:38	File stat	FILE	macb	0	NTFS:\Windows\Prefetch\ATOMICSERVICE_EXE -59E20F94.pf Type: file		
451783		2023-02-13 17:56:59	WinEventX	EVT	m..b	84525	[8 / 0x0008] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'		
451883		2023-02-13 17:56:59	File stat	FILE	...b	0	NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file		
451885		2023-02-13 17:56:59	NTFS USN ...	FILE	...c.	83391	<b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_FILE_CR		
451886		2023-02-13 17:56:59	NTFS USN ...	FILE	...c.	83391	<b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EX		
451887		2023-02-13 17:56:59	NTFS USN ...	FILE	...c.	83391	<b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EX		
451891		2023-02-13 17:56:59	File stat	FILE	mac..	0	NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file		
451893		2023-02-13 17:56:59	WinEventX	EVT	m..b	84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['Proc		

Timestamp Is same day 2023-02-13 00:00:00 Edit Filter  
Total lines 475,070 Visible lines 30 Open Files: 1 Search options

Line	Tag	Timestamp	Source Des.	Source Name	macb	Inode	Long Description
445658		2023-02-13 17:28:09	Bodyfile	FILE	macb	0	MFTScan - MFT FILE_NAME entry for <b>AtomicService.exe</b> Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:
446875		2023-02-13 17:28:09	NTFS USN C...	FILE	...c	83391	<b>AtomicService.exe</b> File reference: 108643-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_FILE_CREATE
446876		2023-02-13 17:28:09	NTFS USN C...	FILE	...c	83391	<b>AtomicService.exe</b> File reference: 108643-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEN
446877		2023-02-13 17:28:09	NTFS USN C...	FILE	...c	83391	<b>AtomicService.exe</b> File reference: 108643-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEN
446878		2023-02-13 17:28:09	NTFS USN C...	FILE	...c	83391	<b>AtomicService.exe</b> File reference: 108643-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO
446879		2023-02-13 17:28:09	NTFS USN C...	FILE	...c	83391	<b>AtomicService.exe</b> File reference: 108643-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO
446892		2023-02-13 17:28:09	File stat	FILE	m...b		NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file
446896		2023-02-13 17:28:09	WinEvtX	EVT	m...b	84525 [1 / 0x000] Provider identifier: {5770385f-c2a4-e30-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['EXE'	
449342		2023-02-13 17:28:30	Bodyfile	FILE	m...b	0	DLLList - DLL Load: Process 4248 AtomicService. Loaded <b>AtomicService.exe</b> (C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.
449376		2023-02-13 17:28:30	WinEvtX	EVT	m...b	84525 [1 / 0x000] Provider identifier: {5770385f-c2a4-e30-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'	
449378		2023-02-13 17:28:30	WinEvtX	EVT	m...b	84525 [1 / 0x000] Provider identifier: {5770385f-c2a4-e30-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'	
449385		2023-02-13 17:28:30	WinEvtX	EVT	m...b	83681 [7045 / 0x1085] Provider identifier: {555908d1-a6d7-4695-8e1c-269312012f4} Source Name: Service Control Manager Strings: ['Ato	
449386		2023-02-13 17:28:30	Registry K...	REG	m...	43889 [HKEY_LOCAL_MACHINE\System\ControlSet001\Services\AtomicTestService\CMDO] Type: Service - Own Process (0x10) Start: Manual (3) I	
449388		2023-02-13 17:28:30	WinEvtX	EVT	m...b	84525 [13 / 0x000] Provider identifier: {5770385f-c2a4-e30-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['T103'	
449389		2023-02-13 17:28:30	WinEvtX	EVT	m...b	84525 [1 / 0x0001] Provider identifier: {5770385f-c2a4-e30-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'	
449390		2023-02-13 17:28:30	WinEvtX	EVT	m...b	84525 [1 / 0x0001] Provider identifier: {5770385f-c2a4-e30-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'	
449391		2023-02-13 17:28:30	WinPrefetch	LOG	...a	107815 Prefetch [ <b>ATOMICSERVICE.EXE</b> ] was executed - run count 1 path hints: ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F500CD341815D502F	
449392		2023-02-13 17:28:30	File stat	FILE	a...	0 NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file	
449512		2023-02-13 17:28:38	Bodyfile	FILE	macb	0	MFTScan - MFT FILE_NAME entry for <b>ATOMICSERVICE.EXE</b> 59E20F94.pf Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:
449514		2023-02-13 17:28:38	NTFS USN C...	FILE	...c	83391	<b>ATOMICSERVICE.EXE</b> _59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON
449515		2023-02-13 17:28:38	NTFS USN C...	FILE	...c	83391	<b>ATOMICSERVICE.EXE</b> _59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON
449516		2023-02-13 17:28:38	NTFS USN C...	FILE	...c	83391	<b>ATOMICSERVICE.EXE</b> _59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON
449517		2023-02-13 17:28:38	File stat	FILE	macb	0	NTFS:\Windows\Prefetch\ATOMICSERVICE.EXE\_59E20F94.pf Type: file
451783		2023-02-13 17:56:59	WinEvtX	EVT	m...b	84525 [8 / 0x008] Provider identifier: {5770385f-c2a4-e30-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['.'	
451883		2023-02-13 17:56:59	File stat	FILE	...b	0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4_0\UsageLogs\AtomicService.exe.log Type: file	
451885		2023-02-13 17:56:59	NTFS USN C...	FILE	...c	83391 <b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_FILE_CR	
451886		2023-02-13 17:56:59	NTFS USN C...	FILE	...c	83391 <b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EX	
451887		2023-02-13 17:56:59	NTFS USN C...	FILE	...c	83391 <b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EX	
451891		2023-02-13 17:56:59	File stat	FILE	mac	0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4_0\UsageLogs\AtomicService.exe.log Type: file	

A screenshot of the Volatility super-timeline interface. The top bar shows a search field with 'Timestamp Is same day 2023-02-13 00:00:00' and a checkbox. Below it is a navigation bar with icons for Windows, File, Machine, View, Input, Devices, Help, and Forensics-System (Volatility installed). The main area shows a timeline with several entries. At the bottom, there's a footer with 'Total lines 475,070 | Visible lines 30 | Open files: 1 | Search options' and a timestamp '11:57 PM 2/16/2023'.

- #### - Service creation:

Timeline Explorer v1.3.0	File	Tools	Tabs	View	Help	
super-timeline.csv						x
Drag a column header here to group by that column						
Tag	Timestamp	Source Des_	Source Name	macb	Inode	Long Description
2023-02-13 17:28:09	Bodyfile	FILE	macb			0 MFTScan - MFT FILE_NAME entry for <b>AtomicService.exe</b> Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:
2023-02-13 17:28:09	NTFS USN C_	FILE	...	83391	AtomicService.exe	File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_FILE_CREATE
2023-02-13 17:28:09	NTFS USN C_	FILE	...	83391	AtomicService.exe	File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
2023-02-13 17:28:09	NTFS USN C_	FILE	...	83391	AtomicService.exe	File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
2023-02-13 17:28:09	NTFS USN C_	FILE	...	83391	AtomicService.exe	File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
2023-02-13 17:28:09	NTFS USN C_	FILE	...	83391	AtomicService.exe	File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
2023-02-13 17:28:09	File stat	FILE	...	...		0 NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file
2023-02-13 17:28:09	WinEvent	EVT	m..b	84525	[1 / 0x000b]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['EXE' '2023-02-13T17:28:09Z' '108644-3']
2023-02-13 17:28:30	Bodyfile	FILE	...			0 DllList - DLL Load: Process 4248 AtomicService. Loaded <b>AtomicService.exe</b> (C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe)
2023-02-13 17:28:30	WinEvent	EVT	m..b	84525	[1 / 0x0001]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T17:28:30Z' '108644-3']
2023-02-13 17:28:30	WinEvent	EVT	m..b	84525	[1 / 0x0001]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T17:28:30Z' '108644-3']
2023-02-13 17:28:30	WinEvent	EVT	m..b	8367	[7045 / 0xb185]	Provider identifier: {555980d1-a6d7-4695-8e1c-26931d2812fa} Source Name: Service Control Manager Strings: ['AtomicTestService' '2023-02-13T17:28:30Z' '108644-3']
2023-02-13 17:28:30	Registry K_	REG	...	53889	[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\AtomicService_CMD]	Type: Service - Own Process (0x10) Start: Manual (3) Image path: \Windows\system32\services\AtomicService_CMD
2023-02-13 17:28:30	WinEvent	EVT	m..b	84525	[13 / 0x000d]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['T1083 T1080' '2023-02-13T17:28:30Z' '108644-3']
2023-02-13 17:28:30	WinEvent	EVT	m..b	84525	[1 / 0x0001]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T17:28:30Z' '108644-3']
2023-02-13 17:28:30	WinEvent	EVT	m..b	84525	[1 / 0x0001]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T17:28:30Z' '108644-3']
2023-02-13 17:28:30	File pref	LOG	a..	107819	Prefetch [ATOMICSERVICE.EXE] was executed - run count 1 path hints: \ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50CD0341815D5FD234CFB9016	
2023-02-13 17:28:30	File stat	FILE	...			0 NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file
2023-02-13 17:28:38	Bodyfile	FILE	macb			0 MFTScan - MFT FILE_NAME entry for <b>ATOMICSERVICE.EXE</b> -59E20F94.pf Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:
2023-02-13 17:28:38	NTFS USN C_	FILE	...	83391	ATOMICSERVICE.EXE-59E20F94.pf	File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_FILE_CREATE
2023-02-13 17:28:38	NTFS USN C_	FILE	...	83391	ATOMICSERVICE.EXE-59E20F94.pf	File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
2023-02-13 17:28:38	NTFS USN C_	FILE	...	83391	ATOMICSERVICE.EXE-59E20F94.pf	File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
2023-02-13 17:28:38	File stat	FILE	macb			0 NTFS:\Windows\Prefetch\ATOMICSERVICE.EXE-59E20F94.pf Type: file
2023-02-13 17:56:59	WinEvent	EVT	m..b	84525	[8 / 0x0008]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T17:56:59Z' '108644-3']
2023-02-13 17:56:59	File stat	FILE	...b			0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file
2023-02-13 17:56:59	NTFS USN C_	FILE	...	83391	AtomicService.exe	.log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_FILE_CREATE
2023-02-13 17:56:59	NTFS USN C_	FILE	...	83391	AtomicService.exe	.log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
2023-02-13 17:56:59	NTFS USN C_	FILE	...	83391	AtomicService.exe	.log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
2023-02-13 17:56:59	File stat	FILE	mac			0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file
2023-02-13 17:56:59	WinEvent	EVT	m..b	84525	[11 / 0x000b]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['ProcessHosting' '2023-02-13T17:56:59Z' '108644-3']

Total lines 475,070 Visible lines 30 Open files: 1 11:59 PM 2/16/2023

x [ ]  **Timestamp**  **Is same day** 2023-02-13 00:00:00 | Edit Filter  
C:\super-timeline.csv | Total lines 475,070 | **Visible lines 30** | Open files 1 | Search options

#### - Prefetch file execution:

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

atomicservice.exe x Find

Tag	Timestamp	Source Des..	Source Name	macb	Inode	Long Description
	2023-02-13 17:28:09	Bodyfile	FILE	macb		0 MFTScan - MFT FILE_NAME entry for <b>AtomicService.exe</b> Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:
	2023-02-13 17:28:09	NTFS USN c..	FILE	...	83391	AtomicService.exe File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_FILE_CREATE
	2023-02-13 17:28:09	NTFS USN c..	FILE	...	83391	AtomicService.exe File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
	2023-02-13 17:28:09	NTFS USN c..	FILE	...	83391	AtomicService.exe File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
	2023-02-13 17:28:09	NTFS USN c..	FILE	...	83391	AtomicService.exe File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
	2023-02-13 17:28:09	File stat	FILE	...	84525	0 MFTScan - MFT FILE_NAME entry for <b>AtomicService.exe</b> Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:
	2023-02-13 17:28:09	WinEvtX	EVT	m..b	84525 [1 / 0x000b]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['EXE' '2023-02-1']
	2023-02-13 17:28:30	Bodyfile	FILE	...	84525	0 DllList - DLL Load: Process 4248 AtomicService_Loaded <b>AtomicService.exe</b> (C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe) Size
	2023-02-13 17:28:30	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 17:28:30	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 17:28:30	Registry K..	REG	m...	83681 [7045 / 0x1b85]	Provider identifier: {555908d1-a6d7-4695-8e1e-26931d2012f4} Source Name: Service Control Manager Strings: ['AtomicTestSe']
	2023-02-13 17:28:30	WinEvtX	EVT	m..b	43889 [KEY_LOCAL_MACHINE\System\ControlSet001\Control\CMND] Type: Service - Own Process (0x10) Start: Manual (3) Image path	
	2023-02-13 17:28:30	WinEvtX	EVT	m..b	84525 [13 / 0x000d]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['T1031 T1050']
	2023-02-13 17:28:30	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 17:28:30	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 17:28:30	WinPrefetch	LOG	...	107815	Prefetch [ <b>ATOMICSERVICE.EXE</b> ] was executed - run count 1 path hints: \ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50CD03418150502F34C8F90168017404\ATOMICSVT1543.003\BIN\ATOMICSERVICE.EXE hash: 0x59E20F94 volume: 1 [serial number: 0xA97874F] device path: \VOLUME{01d3db4976cd072-3a97874F}]
	2023-02-13 17:28:30	File stat	FILE	...	0 NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe	Type: file
	2023-02-13 17:28:30	File file	FILE	macb	0 MFTScan - MFT FILE_NAME entry for <b>AtomicService.exe</b> Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:	
	2023-02-13 17:28:30	NTFS USN c..	FILE	...	83391 ATOMICSERVICE.EXE-59E20F94.pf	File reference: 107815-1 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_FILE_CREATE
	2023-02-13 17:28:30	NTFS USN c..	FILE	...	83391 ATOMICSERVICE.EXE-59E20F94.pf	File reference: 107815-1 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
	2023-02-13 17:28:30	File stat	FILE	macb	0 NTFS:\Windows\Prefetch\ATOMICSERVICE.EXE-59E20F94.pf	Type: file
	2023-02-13 17:28:30	NTFS USN c..	FILE	...	83391 ATOMICSERVICE.EXE-59E20F94.pf	File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
	2023-02-13 17:28:30	File stat	FILE	macb	0 NTFS:\Windows\Prefetch\ATOMICSERVICE.EXE-59E20F94.pf	Type: file
	2023-02-13 17:28:30	WinEvtX	EVT	m..b	84525 [8 / 0x0008]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-1']
	2023-02-13 17:28:30	NTFS USN c..	FILE	...	83391 ATOMICSERVICE.EXE-59E20F94.pf	File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
	2023-02-13 17:28:30	File stat	FILE	macb	0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log	Type: file
	2023-02-13 17:28:30	NTFS USN c..	FILE	...	83391 AtomicService.exe.log	File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_FILE_CREATE
	2023-02-13 17:28:30	NTFS USN c..	FILE	...	83391 AtomicService.exe.log	File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EXTEND
	2023-02-13 17:28:30	File stat	FILE	macb	0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log	Type: file
	2023-02-13 17:28:30	WinEvtX	EVT	m..b	84525 [11 / 0x000b]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['ProcessHostin']

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

atomicservice.exe x Find

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

atomicservice.exe x Find

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

atomicservice.exe x Find

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

atomicservice.exe x Find

## - Service information in registry:

Timeline Explorer v1.3.0						
File Tools Tasks View Help		super-timeline.csv				
Drag a column header here to group by that column						
Tag	Timestamp	Source Des...	Source Name	macb	Inode	Long Description
2023-02-13 17:28:09	Bodyfile	FILE	macb			0 MFTScan - MFT FILE_NAME entry for <b>AtomicService.exe</b> Owner identifier: 0 Group identifier: 0 Mode: 0 MD5: 83391
2023-02-13 17:28:09	NTFS USN C...	FILE	...	b		File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_FILE_CREATE
2023-02-13 17:28:09	NTFS USN C...	FILE	...	b		83391 <b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
2023-02-13 17:28:09	NTFS USN C...	FILE	...	b		83391 <b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
2023-02-13 17:28:09	NTFS USN C...	FILE	...	b		83391 <b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
2023-02-13 17:28:09	NTFS USN C...	FILE	...	b		83391 <b>AtomicService.exe</b> File reference: 108644-3 Parent file reference: 108643-3 Update source: Update reason: USN_REASON_BASIC_INFO_CHANGE
2023-02-13 17:28:09	File stat	FILE	...	b		0 NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file
2023-02-13 17:28:09	WinEventV	EVT	m..b			84525 [1 / 0x000b] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['EXE' '2023-01-01T00:00:00Z' '0']
2023-02-13 17:28:30	Bodyfile	FILE	...	b		0 DllList - DLL Load: Process 4248 AtomicService. Loaded <b>AtomicService.exe</b> (C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe) Size: 0x10000000
2023-02-13 17:28:30	WinEventV	EVT	m..b			84525 [1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T00:00:00Z' '0']
2023-02-13 17:28:30	WinEventV	EVT	m..b			84525 [1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T00:00:00Z' '0']
2023-02-13 17:28:30	WinEventV	EVT	m..b			83681 [7045 / 0x1B85] Provider identifier: {555908d1-a6d7-4695-8e10-269312021f4} Source Name: Service Control Manager Strings: ['AtomicTestService' '2023-02-13T00:00:00Z' '0']
2023-02-13 17:28:30	Registry K...	REG	...	a..		83889 \HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\AtomicTestService_CMDI Type: Service - Own Process (0x10) Start: Manual (3) Image path: \Windows\system32\services\AtomicTestService.exe
2023-02-13 17:28:30	WinEventV	EVT	m..b			84525 [13 / 0x0004] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['T1031' 'T1050' '2023-02-13T00:00:00Z' '0']
2023-02-13 17:28:30	WinEventV	EVT	m..b			84521 [1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T00:00:00Z' '0']
2023-02-13 17:28:30	WinEventV	EVT	m..b			84525 [1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T00:00:00Z' '0']
2023-02-13 17:28:30	WinPrefetch	LOC	...	a..		107619 <b>Prefetch\ATOMICSERVICE.EXE</b> was executed - run count 1 path hints: \ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F500CD341815D502F34CBF9016
2023-02-13 17:28:30	File stat	FILE	...	a..		0 NTFS:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe Type: file
2023-02-13 17:28:38	Bodyfile	FILE	macb			0 MFTScan - MFT FILE_NAME entry for <b>ATOMICSERVICE.EXE</b> -59E20F94.pf Owner identifier: 0 Group identifier: 0 Mode: 0 MD5: 83391
2023-02-13 17:28:38	NTFS USN C...	FILE	...	b		File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_FILE_CREATE
2023-02-13 17:28:38	NTFS USN C...	FILE	...	b		83391 <b>ATOMICSERVICE.EXE</b> -59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
2023-02-13 17:28:38	NTFS USN C...	FILE	...	b		83391 <b>ATOMICSERVICE.EXE</b> -59E20F94.pf File reference: 107815-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
2023-02-13 17:28:38	File stat	FILE	macb			0 NTFS:\Windows\Prefetch\ATOMICSERVICE.EXE-59E20F94.pf Type: file
2023-02-13 17:56:59	WinEventV	EVT	m..b			84525 [8 / 0x0008] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T00:00:00Z' '0']
2023-02-13 17:56:59	File stat	FILE	...	b		0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file
2023-02-13 17:56:59	NTFS USN C...	FILE	...	c..		83391 <b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_FILE_CREATE
2023-02-13 17:56:59	NTFS USN C...	FILE	...	c..		83391 <b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
2023-02-13 17:56:59	NTFS USN C...	FILE	...	c..		83391 <b>AtomicService.exe</b> .log File reference: 85375-10 Parent file reference: 64427-2 Update source: Update reason: USN_REASON_DATA_EXTEND USN_REASON_CHANGE
2023-02-13 17:56:59	File stat	FILE	mac..			0 NTFS:\Windows\System32\config\systemprofile\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\AtomicService.exe.log Type: file
2023-02-13 17:56:59	WinEventV	EVT	m..b			84525 [1 / 0x000b] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698ffbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['ProcessHost' '2023-02-13T00:00:00Z' '0']

Total lines 475,070 Visible lines 30 Open files: 1 Search options 1203 AM 2/17/2023

The screenshot shows the Timeline Explorer interface with a single timeline entry highlighted. The entry is for a super-timeline.csv file and details a registry key creation event.

**Timeline Entry Details:**

- Line #:** 449386
- Timestamp:** 2023-02-13 17:28:09
- Source Name:** REG
- Format:** winreg/windows\_services
- Extra:** name: AtomicTestService\_CMD; object\_name: LocalSystem; sha256\_hash: f39eb2b8d28a1d0630ddf6ca21715032b7e9308e670127ff520f997a298b5

**Timeline View:**

- Shows a list of events from 2023-02-13 17:28:09 to 2023-02-13 17:56:59.
- Events include: Bodyf (Line # 449386), NFTS (Timestamp 2023-02-13 17:28:30), NFTS (Time zone UTC), NFTS (macb m...), NFTS (Source name REG), File (Source description Registry Key - Service), File (Type Content Modification Time), Bodyf (User name -), WinEV (Host name -), WinEV (Short description HKEY\_LOCAL\_MACHINE\{System\ControlSet001\}Services\AtomicTestService\_CMD), WinEV (Long description [HKEY\_LOCAL\_MACHINE\{System\ControlSet001\}Services\AtomicTestService\_CMD]), WinEV (Type: Service - Own Process (0x10) Start: Manual (3) Image path: C:\AtomicRedTeam\atomicms\T1543.003\bin\AtomicService.exe Error control: Normal (1)), Regis, WinEV, WinEV, WinEV, WinEV, WinEV, WinEV, File, Bodyf, NFTS, NFTS, NFTS, NFTS, File, WinEV, File, NFTS, NFTS, NFTS, NFTS, NFTS.

**Bottom Status Bar:**

- atomicservice.exe
- x -
- Find

- Search notepad execution:

Drag a column header here to group by that column							notepad.exe	Find
Tag	Timestamp	Source Des..	Source Name	macb	Inode	Long Description		
	2023-02-13 17:03:28	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_SECURITY_CHANGE		
	2023-02-13 17:03:28	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_SECURITY_CHANGE		
	2023-02-13 17:03:43	Registry K..	REG	m...		83391 [KEY_LOCAL_MACHINE\Software\Microsoft\WindowsSelfHost\OneSettings] ContactF5S: [REG_SZ] false CostedConnectionInterval: [REG_DWORD] 1E		
	2023-02-13 17:05:02	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_SECURITY_CHANGE		
	2023-02-13 17:05:02	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_SECURITY_CHANGE		
	2023-02-13 17:09:48	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_SECURITY_CHANGE		
	2023-02-13 17:09:48	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_SECURITY_CHANGE		
	2023-02-13 17:11:30	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_SECURITY_CHANGE		
	2023-02-13 17:11:30	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_SECURITY_CHANGE		
	2023-02-13 17:17:23	File stat	FILE	...a.		0 NTFS:\Windows\SysWOW64\notepad.exe Type: file		
	2023-02-13 17:17:23	File stat	FILE	...a.		0 NTFS:\Windows\WinSxS\wow64\microsoft\windows-notepad_31bf3856ad364e35_10.0.17134.1_none_Seefc4250d8ae358\ notepad.exe Type: file		
	2023-02-13 17:22:41	Bodyfile	FILE	...b		0 PsList - Process: 7796 notepad.exe (247446052513152) Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:		
	2023-02-13 17:22:41	Bodyfile	FILE	...b		0 PsScan - Process: 7796 notepad.exe (247446052513152) Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:		
	2023-02-13 17:22:41	Registry K..	REG	...a.		87315 [KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorers\UserAssist\{CBF5FC0-ACE2-4FA4-9178-9926F41749EA}\Count] UserAss		
	2023-02-13 17:22:41	Registry K..	REG	m...		87315 [KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ApplicationAssociationToasts] AppX43nxtbyvps62jhe\spodpxz1n790\etc\_tif:		
	2023-02-13 17:22:41	WinPrefetch	LOG	....		88308 Prefetch [NOTEPAD.EXE] was executed - run count 5 point hints: \WINDOWS\SYSTEM32\NOTEPAD.EXE hash: 0xC5670914 volume: 1 [serial number: ]		
	2023-02-13 17:22:44	Bodyfile	FILE	m...		0 PsList - Process: 7796 notepad.exe (247446052513152) Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:		
	2023-02-13 17:22:44	Bodyfile	FILE	m...		0 PsScan - Process: 7796 notepad.exe (247446052513152) Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:		
	2023-02-13 17:22:44	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_TRUNCATED		
	2023-02-13 17:22:44	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND		
	2023-02-13 17:22:44	NTFS USN c..	FILE	...c.		83391 NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND		
	2023-02-13 17:22:45	Registry K..	REG	m...		87440 [KEY_CURRENT_USER\Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\MuiCache] C:\Program Files (x86)\Windows Media Player\		
	2023-02-13 17:22:45	Registry K..	REG	m...		87315 [KEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorers\FileExts_.ps1\OpenWithList] Index: 1 [MRU Value b]: powershell_i		
	2023-02-13 17:22:45	Registry K..	REG	m...		87440 [KEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\{52C64B7E]\@C:\Windows\system32\windowspowershell\v1.0\powershell.exe		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded ADVAPI32.dll (C:\Windows\System32\ADVAPI32.dll) Size 659456 Offset 140721145315328		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded COMCTL32.dll (C:\Windows\System32\COMCTL32.dll) Size 405968 Offset 1407211185110		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded CRYPTBASE.DLL (C:\Windows\system32\CRYPTBASE.DLL) Size 45056 Offset 1407211185110		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded FLTLIB.DLL (C:\Windows\System32\FLTLIB.DLL) Size 40960 Offset 140721124868988 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded GDI32.dll (C:\Windows\System32\GDI32.dll) Size 163840 Offset 140721146953728 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded IMM32.DLL (C:\Windows\System32\IMM32.DLL) Size 184320 Offset 140721177559048 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded IPHLPAPI.DLL (C:\Windows\system32\IPHLPAPI.DLL) Size 229376 Offset 14072113989120		

## - Suspicious DLL injected:

Drag a column header here to group by that column							notepad.exe	Find
Tag	Timestamp	Source Des..	Source Name	macb	Inode	Long Description		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded KERNEL32.DLL (C:\Windows\System32\KERNEL32.DLL) Size 729088 Offset 140721146036224		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded KERNELBASE.dll (C:\Windows\System32\KERNELBASE.dll) Size 2568192 Offset 1407211293		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded MSCIF.dll (C:\Windows\System32\MSCIF.dll) Size 1527808 Offset 140721143218176 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded MmCore.r.dll (C:\Windows\System32\MmCore.r.dll) Size 1175552 Offset 14072093972889		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded OLEAUT32.dll (C:\Windows\System32\OLEAUT32.dll) Size 794624 Offset 14072117814400		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded PROPSYS.dll (C:\Windows\System32\PROPSYS.dll) Size 1785856 Offset 14072106909696		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded RPCRT4.dll (C:\Windows\System32\RPCRT4.dll) Size 1196032 Offset 140721187192832 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded SHELL32.dll (C:\Windows\System32\SHLWAPI.DLL) Size 2133664 Offset 140721149640704		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded SHLWAPI.DLL (C:\Windows\System32\SHLWAPI.DLL) Size 331776 Offset 140721185751040		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded SPIPCL1.DLL (C:\Windows\system32\SSPIPCL1.DLL) Size 196608 Offset 140721123819520		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded Secur32.dll (C:\Windows\system32\Secur32.dll) Size 49152 Offset 14072123221760 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded T1085.001.dll (C:\AtomicRedTeam\atomics\T1085.001.dll) Size 1187		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded USER32.dll (C:\Windows\System32\USER32.dll) Size 1638400 Offset 140721184112640 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded WINSPPOOL.DRV (C:\Windows\System32\WINSPPOOL.DRV) Size 540672 Offset 140720836116480		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded bcrypt.dll (C:\Windows\System32\bcrypt.dll) Size 151552 Offset 140721119625216 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded bcryptPrimitives.dll (C:\Windows\System32\bcryptPrimitives.dll) Size 499712 Offset		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded cfgmgr32.dll (C:\Windows\System32\cfgmgr32.dll) Size 299008 Offset 14072112644096		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded clbcatq.dll (C:\Windows\System32\clbcatq.dll) Size 655360 Offset 14072118653742		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded combbase.dll (C:\Windows\System32\combbase.dll) Size 3289088 Offset 14072118770304		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded dwmapi.dll (C:\Windows\System32\dwmapi.dll) Size 167936 Offset 140721099243520 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded gdi32full.dll (C:\Windows\System32\gdi32full.dll) Size 1646592 Offset 140721131945		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded iertutil.dll (C:\Windows\System32\iertutil.dll) Size 2760704 Offset 14072094385766		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded kernel.appcore.dll (C:\Windows\System32\kernel.appcore.dll) Size 69632 Offset 1407		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded msvcrt.dll (C:\Windows\System32\msvcrt.dll) Size 651264 Offset 1407211257856		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded msvcr7.dll (C:\Windows\System32\msvcr7.dll) Size 647168 Offset 14072114754352		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded notepad.exe (C:\Windows\System32\notepad.exe) Size 266240 Offset 140700452585472		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded ntdll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 1970176 Offset 140721188765696 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded powrprof.dll (C:\Windows\System32\powrprof.dll) Size 311296 Offset 140721125326848		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded profapi.dll (C:\Windows\System32\profapi.dll) Size 126976 Offset 14072112493362		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded sechost.dll (C:\Windows\System32\sechost.dll) Size 372736 Offset 140721175396352		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded shcore.dll (C:\Windows\System32\shcore.dll) Size 692224 Offset 140721179866368 Owner		
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DLList - DLL Load: Process 3164 notepad.exe Loaded ucrtbase.dll (C:\Windows\System32\ucrtbase.dll) Size 1024000 Offset 14072114216966		

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

Timestamp Source Des... Source Name macb Inode Long Description

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded iertutil.dll (C:\Windows\system32\iertutil.dll) Size 2760704 Offset 14072094385766

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded kernel.appcore.dll (C:\Windows\System32\kernel.appcore.dll) Size 69632 Offset 1407211257856

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded msvcv\_win.dll (C:\Windows\System32\msvcv\_win.dll) Size 651264 Offset 1407211257856

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded msvcrt.dll (C:\Windows\System32\msvcrt.dll) Size 647168 Offset 140720452585472 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded notepad.exe (C:\Windows\System32\notepad.exe) Size 266240 Offset 140720452585472 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded ntdll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 1970176 Offset 140721188765696 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded powrprof.dll (C:\Windows\System32\powrprof.dll) Size 311296 Offset 140720951459840 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded profapi.dll (C:\Windows\System32\profapi.dll) Size 126976 Offset 140721124933632 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded sechost.dll (C:\Windows\System32\sechost.dll) Size 372736 Offset 140721175396352 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded shcore.dll (C:\Windows\System32\shcore.dll) Size 692224 Offset 140721179066368 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded ucrtbase.dll (C:\Windows\System32\ucrtbase.dll) Size 1024000 Offset 14072114216960

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded urlmon.dll (C:\Windows\System32\urlmon.dll) Size 1884160 Offset 140720951459840 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded uxtheme.dll (C:\Windows\System32\uxtheme.dll) Size 622592 Offset 140721096753152 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded win32u.dll (C:\Windows\System32\win32u.dll) Size 131072 Offset 140721125654528 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded windows.storage.dll (C:\Windows\System32\windows.storage.dll) Size 7393280 Offset 140720951459840

2023-02-13 17:28:32 Bodyfile FILE ...b 0 PsList - Process: 3164 notepad.exe (247446047105152) Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:

2023-02-13 17:28:32 Bodyfile FILE ...b 0 PsScan - Process: 3164 notepad.exe (247446047105152) Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:

2023-02-13 17:28:32 Bodyfile FILE ...b 0 Sessions - Process: 3164 notepad.exe started by user MSEDEGWIN10\IEUser Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:

2023-02-13 17:28:32 WinPrefetch LOG ...a... 88309 [Prefetch [NOTEPAD.EXE] was executed - run count 5 path hints: \WINDOWS\SYSTEM32\NOTEPAD.EXE hash: 0xC5670914 volume: 1 [serial number]]

2023-02-13 17:28:32 File stat FILE ...a... 0 NTFS:\Windows\System32\ notepad.exe Type: file

2023-02-13 17:28:32 File stat FILE ...a... 0 NTFS:\Windows\WinSxS\amd64\_microsoft-windows-notepad\_31bf3856ad364e35\_10.0.17134.1\_none\_549b19d2d92a15d\ notepad.exe Type: file

2023-02-13 17:28:32 WinVTX EVT m...b 84525 [1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698fbfd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13 17:28:32']

2023-02-13 17:28:41 NTFS USN c... FILE ...c. 83391 NOTEPAD.EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN\_REASON\_DATA\_TRUNCATI

2023-02-13 17:28:41 NTFS USN c... FILE ...c. 83391 NOTEPAD.EXE-C5670914.pf File reference: 88309-3 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 NOTEPAD.EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN\_REASON\_DATA\_EXTEND

2023-02-13 17:28:41 File stat FILE mac. 0 NTFS:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf Type: file

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded MPR.dll (C:\Windows\System32\MPR.dll) Size 106496 Offset 14072102833568 Owner ide

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded RMCLIENT.dll (C:\Windows\System32\RMCLIENT.dll) Size 135168 Offset 140721100161024

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded efsprt.dll (C:\Windows\System32\efsprt.dll) Size 729088 Offset 140720579936256 Owne

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded oleacc.dll (C:\Windows\System32\oleacc.dll) Size 438272 Offset 140720782966784 Owne

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded twinapi.appcore.dll (C:\Windows\System32\twinapi.appcore.dll) Size 1802240 Offset

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded wintypes.dll (C:\Windows\SYSTEM32\wintypes.dll) Size 1363968 Offset 140721057497088

Timestamp Is same day 2023-02-13 00:00:00

Total lines 475,070 Visible lines 87 Open files: 1 Search options

Ed Filter

## - Process created:

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

super-timeline.csv

Drag a column header here to group by that column

Timestamp Source Des... Source Name macb Inode Long Description

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded iertutil.dll (C:\Windows\system32\iertutil.dll) Size 2760704 Offset 14072094385766

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded kernel.appcore.dll (C:\Windows\System32\kernel.appcore.dll) Size 69632 Offset 1407211257856

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded msvcv\_win.dll (C:\Windows\System32\msvcv\_win.dll) Size 651264 Offset 1407211257856

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded msvcrt.dll (C:\Windows\System32\msvcrt.dll) Size 647168 Offset 140720452585472 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded notepad.exe (C:\Windows\System32\notepad.exe) Size 266240 Offset 140720452585472 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded ntdll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 1970176 Offset 140721188765696 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded powrprof.dll (C:\Windows\System32\powrprof.dll) Size 311296 Offset 140720951459840 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded profapi.dll (C:\Windows\System32\profapi.dll) Size 126976 Offset 140721124933632 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded sechost.dll (C:\Windows\System32\sechost.dll) Size 372736 Offset 140721175396352 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded shcore.dll (C:\Windows\System32\shcore.dll) Size 692224 Offset 140721179066368 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded ucrtbase.dll (C:\Windows\System32\ucrtbase.dll) Size 1024000 Offset 14072114216960

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded urlmon.dll (C:\Windows\System32\urlmon.dll) Size 1884160 Offset 140720951459840 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded uxtheme.dll (C:\Windows\System32\uxtheme.dll) Size 622592 Offset 140721096753152 0

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded win32u.dll (C:\Windows\System32\win32u.dll) Size 131072 Offset 140721125654528 Owne

2023-02-13 17:28:32 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded windows.storage.dll (C:\Windows\System32\windows.storage.dll) Size 7393280 Offset 140720951459840

2023-02-13 17:28:32 Bodyfile FILE ...b 0 PsList - Process: 3164 notepad.exe (247446047105152) Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:

2023-02-13 17:28:32 Bodyfile FILE ...b 0 PsScan - Process: 3164 notepad.exe (247446047105152) Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:

2023-02-13 17:28:32 Bodyfile FILE ...b 0 Sessions - Process: 3164 notepad.exe started by user MSEDEGWIN10\IEUser Owner identifier: 0 Group identifier: 0 Mode: 0 MD5:

2023-02-13 17:28:32 WinPrefetch LOG ...a... 88309 [Prefetch [NOTEPAD.EXE] was executed - run count 5 path hints: \WINDOWS\SYSTEM32\NOTEPAD.EXE hash: 0xC5670914 volume: 1 [serial number]]

2023-02-13 17:28:32 File stat FILE ...a... 0 NTFS:\Windows\System32\ notepad.exe Type: file

2023-02-13 17:28:32 File stat FILE ...a... 0 NTFS:\Windows\WinSxS\amd64\_microsoft-windows-notepad\_31bf3856ad364e35\_10.0.17134.1\_none\_549b19d2d92a15d\ notepad.exe Type: file

2023-02-13 17:28:32 WinVTX EVT m...b 84525 [1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698fbfd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13 17:28:32']

2023-02-13 17:28:41 NTFS USN c... FILE ...c. 83391 NOTEPAD.EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN\_REASON\_DATA\_TRUNCATI

2023-02-13 17:28:41 NTFS USN c... FILE ...c. 83391 NOTEPAD.EXE-C5670914.pf File reference: 88309-3 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 NOTEPAD.EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN\_REASON\_DATA\_EXTEND

2023-02-13 17:28:41 File stat FILE mac. 0 NTFS:\Windows\Prefetch\NOTEPAD.EXE-C5670914.pf Type: file

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded MPR.dll (C:\Windows\System32\MPR.dll) Size 106496 Offset 14072102833568 Owner ide

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded RMCLIENT.dll (C:\Windows\System32\RMCLIENT.dll) Size 135168 Offset 140721100161024

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded efsprt.dll (C:\Windows\System32\efsprt.dll) Size 729088 Offset 140720579936256 Owne

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded oleacc.dll (C:\Windows\System32\oleacc.dll) Size 438272 Offset 140720782966784 Owne

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded twinapi.appcore.dll (C:\Windows\System32\twinapi.appcore.dll) Size 1802240 Offset

2023-02-13 17:29:03 Bodyfile FILE ...b 0 DLList - DLL Load: Process 3164 notepad.exe Loaded wintypes.dll (C:\Windows\SYSTEM32\wintypes.dll) Size 1363968 Offset 140721057497088

Timestamp Is same day 2023-02-13 00:00:00

Total lines 475,070 Visible lines 87 Open files: 1 Search options

Ed Filter

## - Process injection code:

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

Timeline Explorer v1.3.0.0						
File	Tools	Tabs	View	Help		
super-timeline.csv						
Drag a column header here to group by that column						
Tag	Timestamp	Source Des...	Source Name	macb	Inode	Long Description
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded msvcr7.dll (C:\Windows\System32\msvcr7.dll) Size 647168 Offset 140721147543552 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded notepad.exe (C:\Windows\system32\notepad.exe) Size 266240 Offset 140700452585472 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded ntddll.dll (C:\Windows\SYSTEM32\ntdll.dll) Size 1970176 Offset 140721188765696 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded powrprof.dll (C:\Windows\System32\powrprof.dll) Size 311296 Offset 140721125326848 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded profapi.dll (C:\Windows\System32\profapi.dll) Size 126976 Offset 140721124933632 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded sechost.dll (C:\Windows\System32\sechost.dll) Size 372736 Offset 14072117596352 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded shcore.dll (C:\Windows\System32\shcore.dll) Size 692240 Offset 140721179066368 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded ucrtbase.dll (C:\Windows\System32\ucrtbase.dll) Size 1024000 Offset 14072114216968 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded uxtheme.dll (C:\Windows\System32\uxtheme.dll) Size 622592 Offset 140721096753152 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded win32u.dll (C:\Windows\System32\win32u.dll) Size 131072 Offset 140721125654528 Own
	2023-02-13 17:28:32	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded windows.storage.dll (C:\Windows\System32\windows.storage.dll) Size 7393280 Offset 140721125654528 Own
	2023-02-13 17:28:32	PsList	- Process:	3164	notepad.exe	(247446047105152) Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:
	2023-02-13 17:28:32	PsScan	- Process:	3164	notepad.exe	(247446047105152) Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:
	2023-02-13 17:28:32	Sessions	- Process:	3164	notepad.exe	→ started by user MSEDEWIN10\IEUser Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:
	2023-02-13 17:28:32	WinPrefetch	LOG	a...	88395	Prefetch [NOTEPAD_EXE] was executed - run count 5 path hints: \WINDOWS\SYSTEM32\NOTEPAD_EXE hash: 0xC5670914 volume: 1 [serial number: 1]
	2023-02-13 17:28:32	File stat	FILE	a...		0 NTFS:\Windows\System32\notepad.exe Type: file
	2023-02-13 17:28:32	File stat	FILE	a...		0 NTFS:\Windows\WinSxS\and64_microsoft-windows-notepad_31bf3b56ad364e35_10.0.17134.1_none_549b19d292a215d\notepad.exe Type: file
	2023-02-13 17:28:32	WinVTX	EVT	m...b	84525	[1 / 0x00001] Provider identifier: {5770385F-c22a-43e0-bf4c-06F5698Fbd9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' , '2023-02-
	2023-02-13 17:28:41	NTFS USN c...	FILE	..c.	83391	NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_TRUNCATION
	2023-02-13 17:28:41	NTFS USN c...	FILE	..c.	83391	NOTEPAD_EXE-C5670914.pf File reference: 88309-3 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	NOTEPAD_EXE-C5670914.pf File reference: 88309-3 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
	2023-02-13 17:28:41	File stat	FILE	mac...		0 NTFS:\Windows\Prefetch\NOTEPAD_EXE-C5670914.pf Type: file
	2023-02-13 17:29:03	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded MPR.DLL (C:\Windows\System32\MPR.dll) Size 106496 Offset 14072102833568 Owner id e
	2023-02-13 17:29:03	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded RMLCLIENT.dll (C:\Windows\System32\RMLCLIENT.dll) Size 135168 Offset 140721108161024
	2023-02-13 17:29:03	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded esfrwt.dll (C:\Windows\System32\esfrwt.dll) Size 729088 Offset 140720579936256 Own
	2023-02-13 17:29:03	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded oleacc.dll (C:\Windows\System32\oleacc.dll) Size 438272 Offset 140720782966784 Own
	2023-02-13 17:29:03	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded twinapi.appcore.dll (C:\Windows\System32\twinapi.appcore.dll) Size 1802240 Offset 14072105749708
	2023-02-13 17:29:03	Bodyfile	FILE	...b		0 DllList - DLL Load: Process 3164 notepad.exe Loaded win32p.dll (C:\Windows\System32\win32p.dll) Size 1363968 Offset 14072105749708
	2023-02-13 17:56:52	Background...	REG	a...	85289	[Device\HarddiskVolume3\Windows\System32\hotpad.exe [5-1-21-1058341133-2029417715-4019509128-1000]
	2023-02-13 17:56:58	Registry K...	REG	m...	43889	[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\bam\UserSettings\5-1-5-21-1058341133-2029417715-4019509128-1000] Microsoft.Microsoft

Timeline Explorer v1.3.0

File Tools Tab View Help

super-timeline.csv

Drag a column header here to group by that column

Tag	Timestamp	Source Des...	Source Name	macb	Inode	Long Description
	=					
<b>Details for super timeline entry, Line # 451093, Inode: 43889</b>						
	Line #	451093	Version	2		
	Timestamp	2023-02-13 17:56:58	File name	NTFS:\Windows\System32\config\SYSTEM		
	Time zone	UTC	Inode	43889		
	macb	m...	Notes	-		
	Source name	REG	Format	winreg/winreg_default		
	Source description	Registry Key	Extra	sha256 hash: f39eb2b8c28a1d0630dd6ca21715032b7e9308e6701271fc5201997a298b5		
	Type	Content Modification Time				
	User name	-				
	Host name	-				
	Short description	[HKEY_LOCAL_MACHINE\System\ControlSet001\Services\bam\UserSettings\5-1-5-21-1]				
	Long description	(HKEY_LOCAL_MACHINE\System\ControlSet001\Services\bam\UserSettings\5-1-5-21-1058341133-2092417715-4019509128-1000)				
		Microsoft.MicrosoftEdge_Bwelybjdbbwbe: [REG_BINARY] (24 bytes)				
		Microsoft.Windows.Shell_Cvnhnzbwyew: [REG_BINARY] (24 bytes)				
		Microsoft.Windows.Shell_Sequencerlock_cvnhnzbwyew: [REG_BINARY] (24 bytes)				
		Microsoft.Windows.ShellExperienceHost_cvnhnzbwyew: [REG_BINARY] (24 bytes)				
		Microsoft.Windows.Store_Bwelybjdbbwbe: [REG_BINARY] (24 bytes)				
		SequenceNumber: [REG_DWORD, LE] 19 Version: [REG_DWORD, LE] 1 \Device\Harddisk\Volume3\Windows\System32\ApplicationFrameHost.exe: [REG_BINARY] (24 bytes) \Device\Harddisk\Volume3\Windows\System32\OpenWith.exe: [REG_BINARY] (24 bytes) \Device\Harddisk\Volume3\Windows\System32\PowerShell\v1.0\powershell.exe: [REG_BINARY] (24 bytes) \Device\Harddisk\Volume3\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe: [REG_BINARY] (24 bytes) \Device\Harddisk\Volume3\Windows\System32\cmd.exe: [REG_BINARY] (24 bytes) \Device\Harddisk\Volume3\Windows\System32\notepad.exe: [REG_BINARY] (24 bytes) \Device\Harddisk\Volume3\Windows\explorer.exe: [REG_BINARY] (24 bytes) windows.immersivecontrolpanel_cvnhnzbwyew: [REG_BINARY] (24 bytes)				
		Show formatted				
		Show raw				
	Always on top	<input checked="" type="radio"/>				
					Previous record	Next record
	Background... REG	. . .	43889	Device\HarddiskVolume3\Windows\System32\notepad.exe	[5-1-5-21-1058341133-2092417715-4019509128-1000]	
	Timestamp	Is same day	2023-02-13 00:00:00			
					Total lines: 475,070	Visible lines: 87
					Open files: 1	Search options
						12:10 AM 2/17/2023

C:\super-timeline.csv

- Search for mavinject.exe:

Timeline Explorer v1.3.0.0						
File Tools Table View Help		super-timeline.csv				
Drag a column header here to group by that column						
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 Type
2023-02-13 17:28:32	WinETVK	EVT	m..b	84525 [1 / 0x0001]	Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698fbfd9}	Source Name: Microsoft-Windows-Symon Strings: [-] '2023-02-1
2023-02-13 17:28:32	WinPrefetch	LOG	.a..	107816	Prefetch [MAVINJECT.EXE] was executed - run count 1 path hints: \WINDOWS\SYSTEM32\MAVINJECT.EXE hash: 0x91AA51D2 volume: 1 [serial number]	
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

Tag	Timestamp	Source Des..	Source Name	macb	Inode	Long Description
File stat	2023-02-13 17:28:32	FILE	.a..		0	NTFS:\Windows\System32\mavinject.exe Type: file
File stat	2023-02-13 17:28:32	FILE	.a..		0	NTFS:\Windows\WinSxS\amd64_microsoft-windows-appmanagement-appvwow_31bf3856ad364e35_10.0.17134.1_none_98ba589f5b912b0d\mavinject.exe Type: file
WinEvtX	2023-02-13 17:28:32	EVT	m..b		84525	[1 / 0x0001] Provider identifier: {5770385f-c22a-43e0-bf4c-06f5698fb9d9} Source Name: Microsoft-Windows-Sysmon Strings: ['-' '2023-02-13T17:28:32Z' 'mavinject.exe']
WinPrefetch	2023-02-13 17:28:32	LOG	.a..		10776	Prefetch [MAVINJECT.EXE] was executed - run count 1 path hints: \WINDOWS\SYSTEM32\MAVINJECT.EXE volume: 1 [serial number: 1] [version: 1]
Bodyfile	2023-02-13 17:28:41	FILE	macb		83391	0 MFTScan - MFT FILE_NAME entry for MAVINJECT.EXE-91AA51D2.pf Owner identifier: 0 Group identifier: 0 Mode: 0 MDS:
NTFS USN c...	2023-02-13 17:28:41	FILE	...		83391	MAVINJECT.EXE-91AA51D2.pf File reference: 107816-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_FILE_CREATE
NTFS USN c...	2023-02-13 17:28:41	FILE	...		83391	MAVINJECT.EXE-91AA51D2.pf File reference: 107816-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
NTFS USN c...	2023-02-13 17:28:41	FILE	...		83391	MAVINJECT.EXE-91AA51D2.pf File reference: 107816-7 Parent file reference: 83680-1 Update source: Update reason: USN_REASON_DATA_EXTEND
File stat	2023-02-13 17:28:41	FILE	macb		0	NTFS:\Windows\Prefetch\MAVINJECT.EXE-91AA51D2.pf Type: file

File	Timestamp	Line	Content
super-timeline.csv	2023-02-13 17:28:32	449499	File Line # 449499, Inode: 84525

File	Timestamp	Line	Content
super-timeline.csv	2023-02-13 17:28:32	449499	File Line # 449499, Inode: 84525