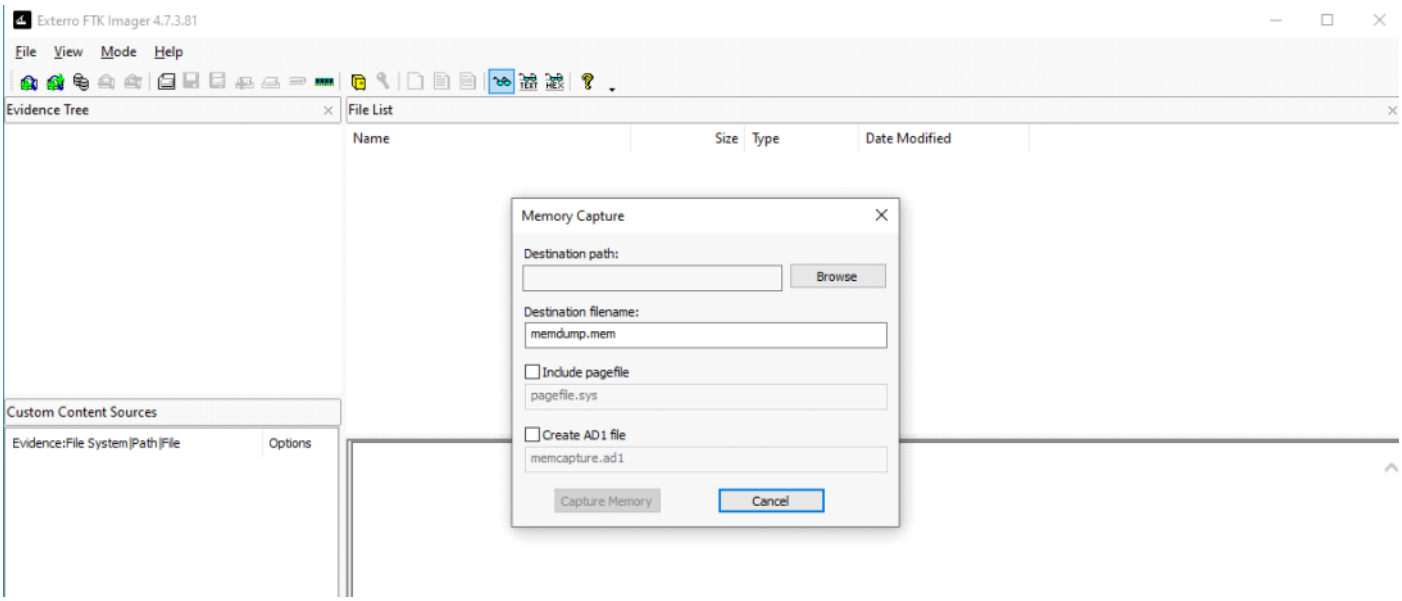
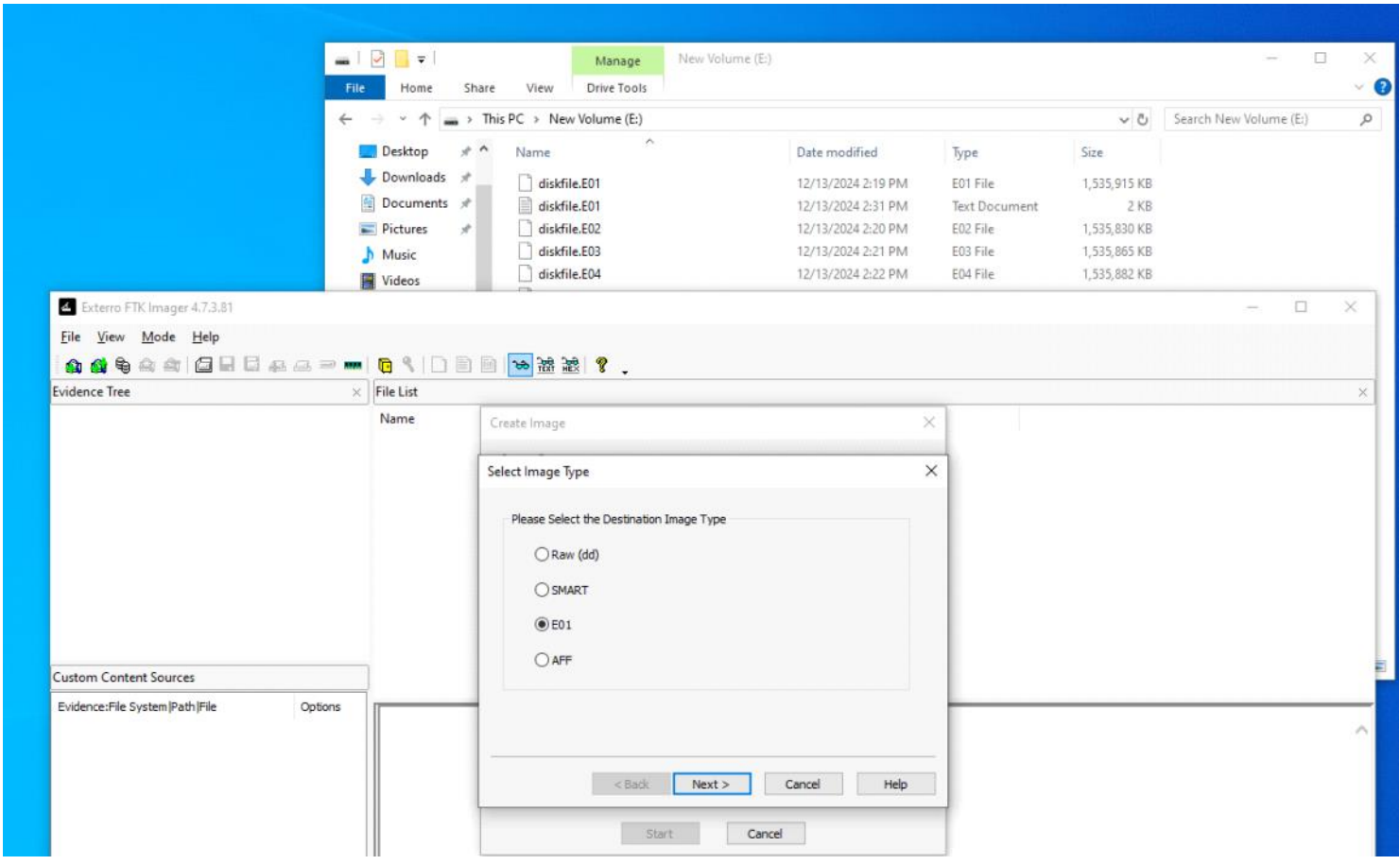
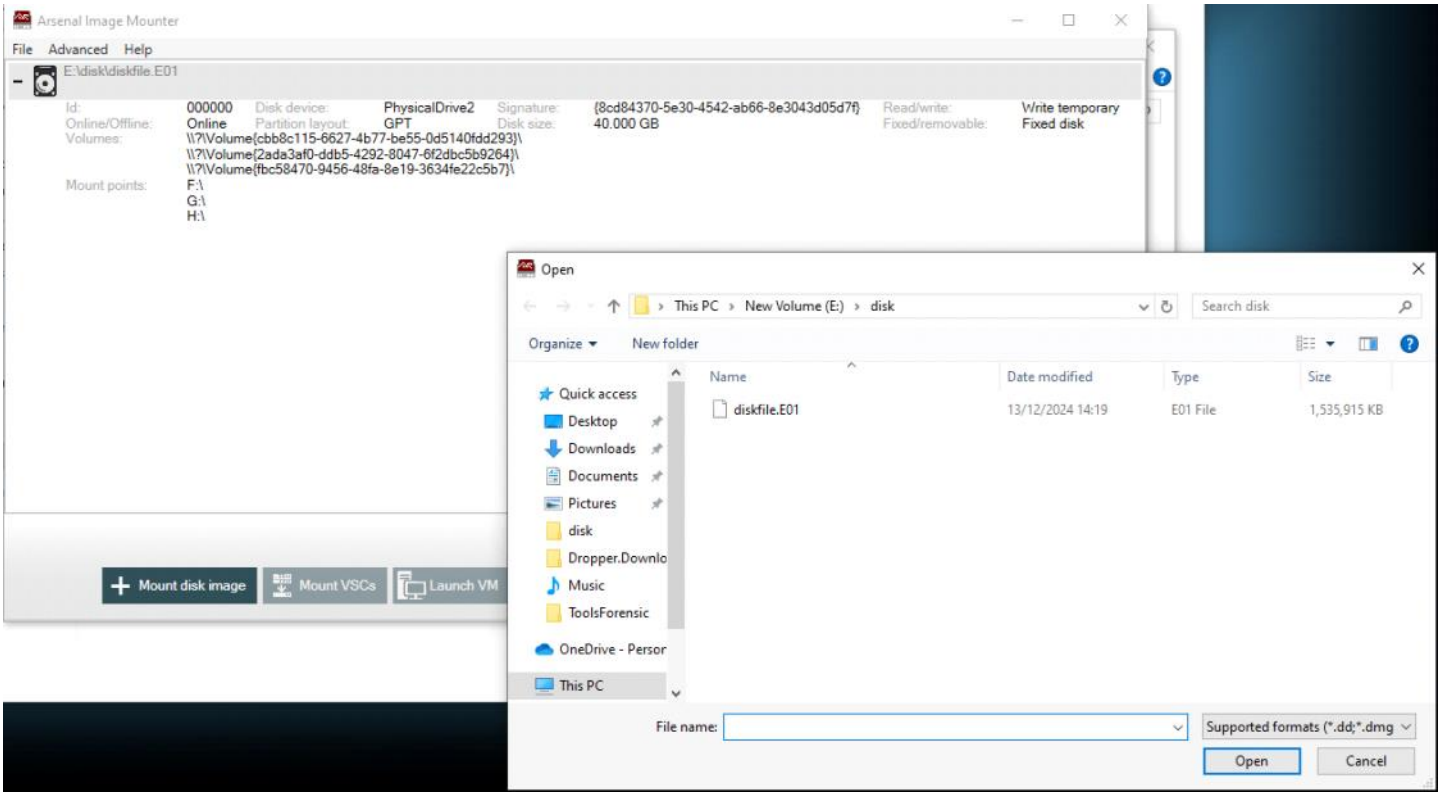
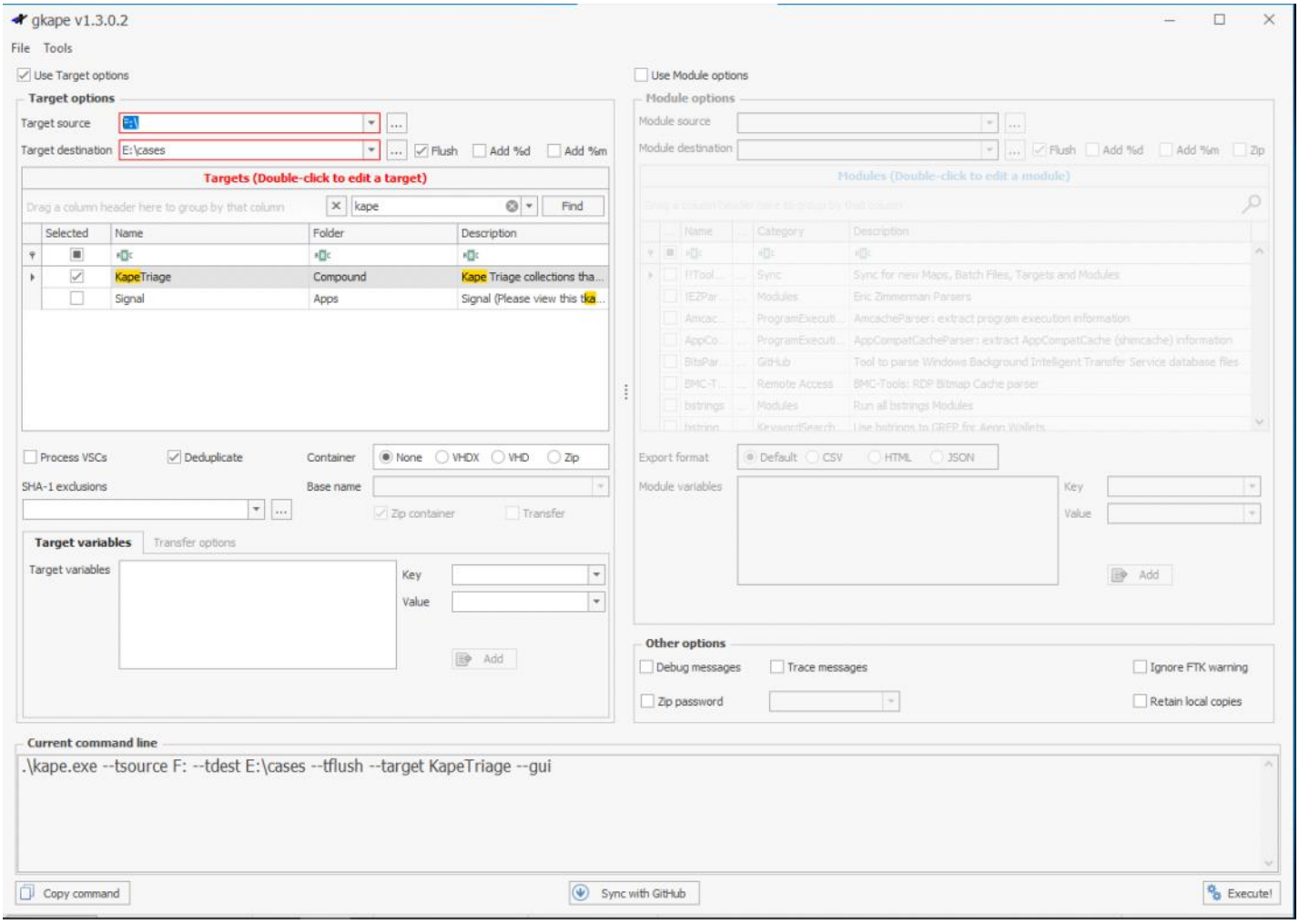




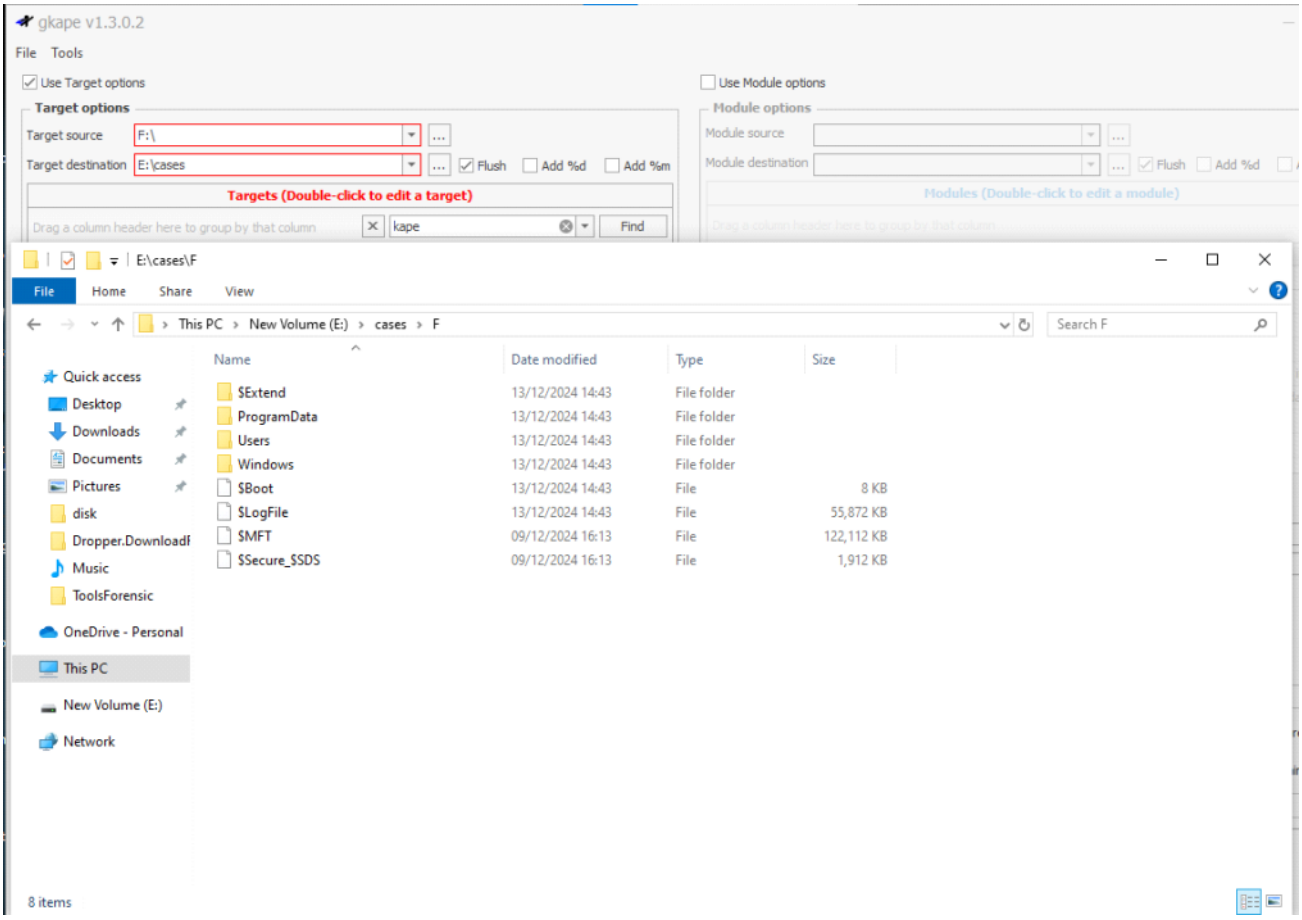
Mount the Image:



Kape Tiage on the mounted disk:



This will extract all the artifacts:

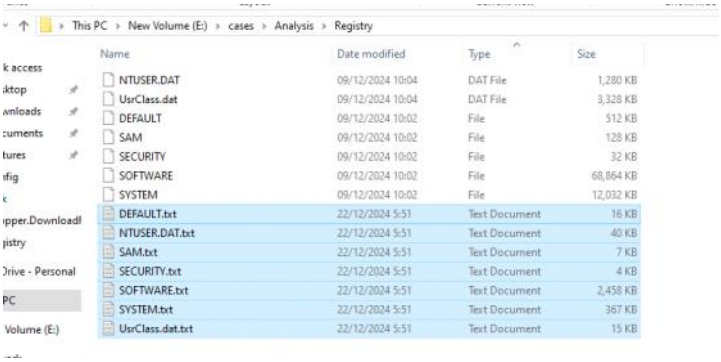

gkape v1.3.0.2
File Tools
Use Target options
Target options
Target source F:\
Target destination E:\cases
Flush Add %d Add %m
Targets (Double-click to edit a target)
Drag a column header here to group by that column
kape
Find
Use Module options
Module options
Module source
Module destination
Flush Add %d
Modules (Double-click to edit a module)
E:\cases\F
File Home Share View
This PC › New Volume (E:) › cases › F
Search F
Quick access
Desktop
Downloads
Documents
Pictures
disk
Dropper.Downloadf
Music
ToolsForensic
OneDrive - Personal
This PC
New Volume (E:)
Network
Name
Date modified
Type
Size
$Extend 13/12/2024 14:43 File folder
ProgramData 13/12/2024 14:43 File folder
Users 13/12/2024 14:43 File folder
Windows 13/12/2024 14:43 File folder
$Boot 13/12/2024 14:43 File 8 KB
$LogFile 13/12/2024 14:43 File 55,872 KB
$MFT 09/12/2024 16:13 File 122,112 KB
$Secure_$SDS 09/12/2024 16:13 File 1,912 KB
8 items

Registry

Sunday, 22 December 2024 17:27

Reg ripper command:

```
C:\Cases\Analysis\Registry>
C:\Cases\Analysis\Registry>
C:\Cases\Analysis\Registry>for /r %i in (*) do (C:\Tools\RegRipper\rip.exe -r %i -a > %i.txt)
```



This PC › New Volume (E:) › cases › Analysis › Registry

Name	Date modified	Type	Size
NTUSER.DAT	09/12/2024 10:04	DAT File	1,280 KB
UsrClass.dat	09/12/2024 10:04	DAT File	3,328 KB
DEFAULT	09/12/2024 10:02	File	512 KB
SAM	09/12/2024 10:02	File	128 KB
SECURITY	09/12/2024 10:02	File	32 KB
SOFTWARE	09/12/2024 10:02	File	68,864 KB
SYSTEM	09/12/2024 10:02	File	12,032 KB
DEFAULT.txt	22/12/2024 5:51	Text Document	16 KB
NTUSER.DAT.txt	22/12/2024 5:51	Text Document	40 KB
SAM.txt	22/12/2024 5:51	Text Document	7 KB
SECURITY.txt	22/12/2024 5:51	Text Document	4 KB
SOFTWARE.txt	22/12/2024 5:51	Text Document	2,458 KB
SYSTEM.txt	22/12/2024 5:51	Text Document	367 KB
UsrClass.dat.txt	22/12/2024 5:51	Text Document	15 KB

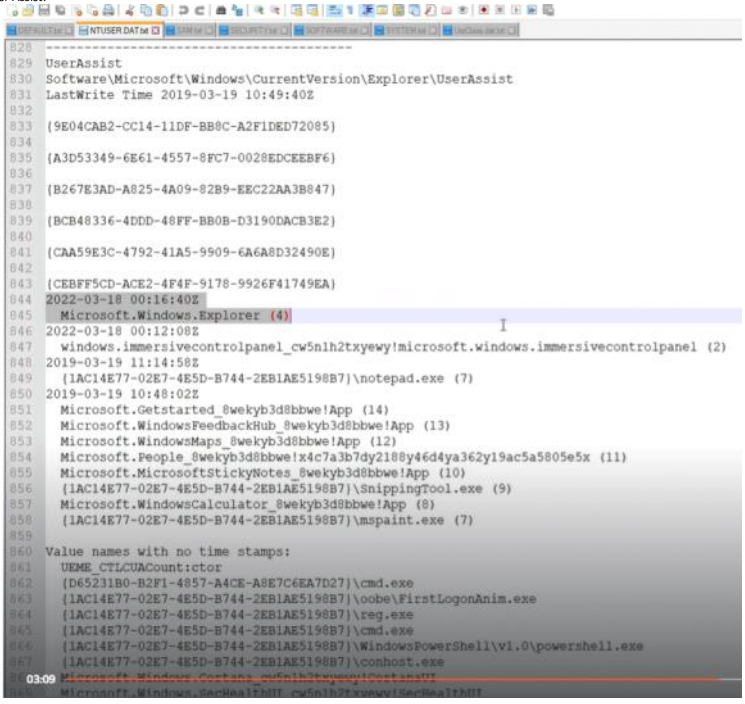
User Behavior

UserAssist - applications opened
RecentDocs - files and folders opened
Shellbags - locations browsed by the user
Open / Save MRU - files that were opened
Last-Visited MRU - applications used to open files

UserAssist:
NTUSER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

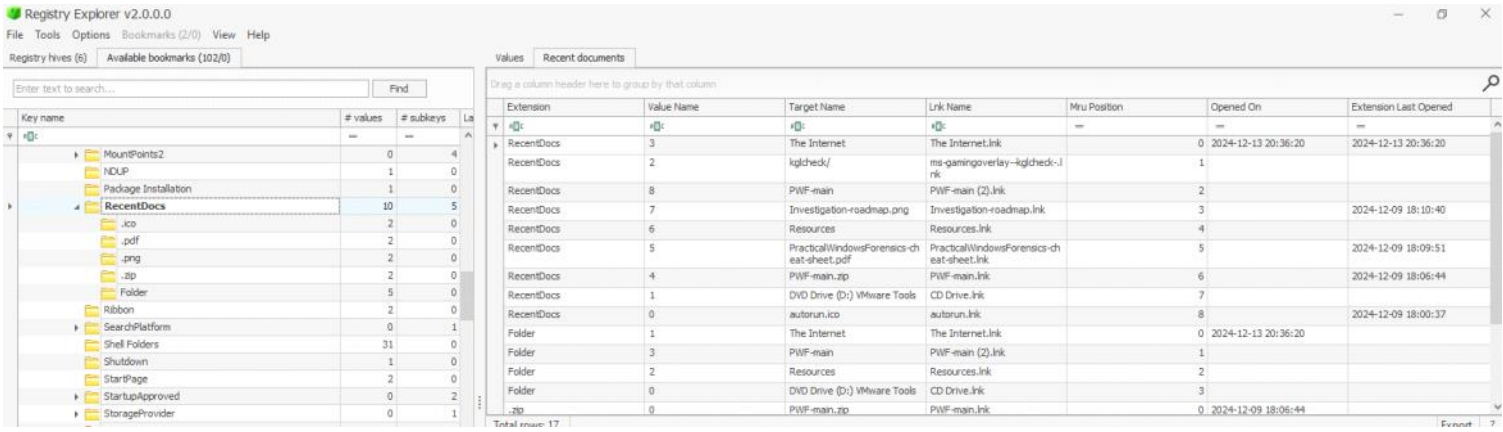
- {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} – A list of applications, files, links, and other objects that have been accessed.
- {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F} – Lists the shortcut links used to start programs

User Assist:

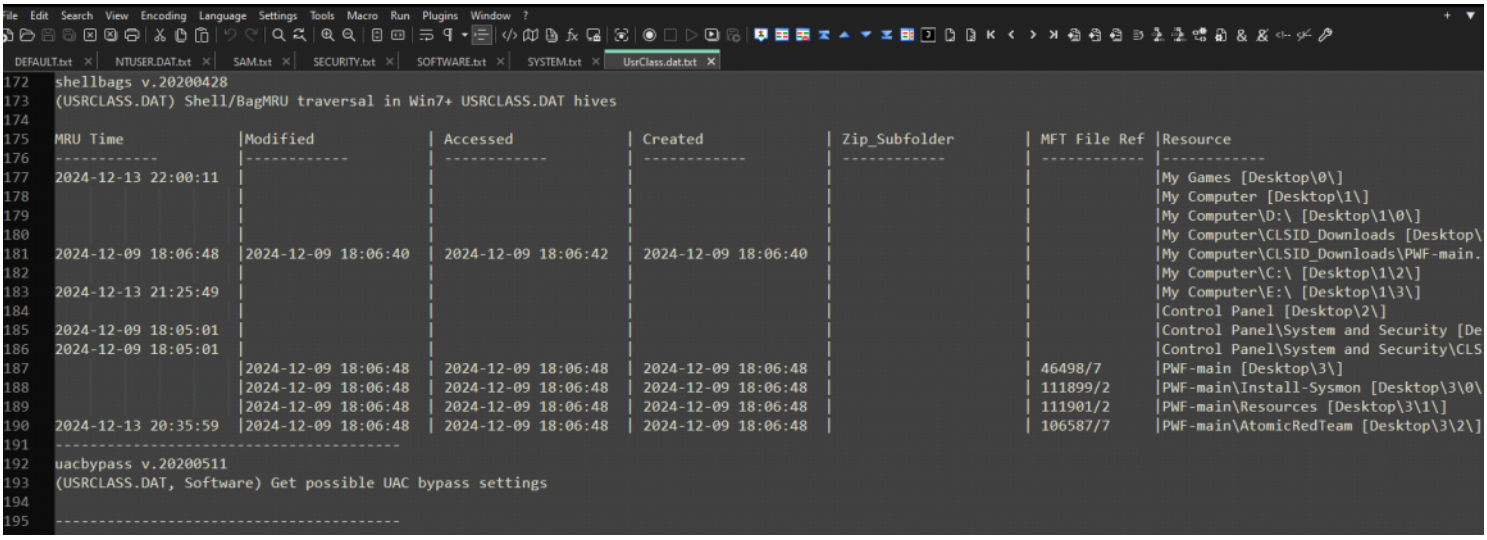


```
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2019-03-19 10:49:40Z

{9E04CAB2-CC14-11DF-BB8C-A2F1DED72085}

{A3D53349-6E61-4557-8FC7-0028EDCEEBF6}

{B267E3AD-A825-4A09-82B9-EEC22AA3B847}

{BCB48336-4DDD-48FF-BB0B-D3190DACB3E2}

{CAA59E3C-4792-41A5-9909-6A6A8D32490E}

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
2022-03-18 00:16:40Z
  Microsoft.Windows.Explorer (4)
2022-03-18 00:12:08Z
  windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel (2)
2019-03-19 11:14:58Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (7)
2019-03-19 10:48:02Z
  Microsoft.Getstarted_8wekyb3d8bbwe!App (14)
  Microsoft.WindowsFeedbackHub_8wekyb3d8bbwe!App (13)
  Microsoft.WindowsMaps_8wekyb3d8bbwe!App (12)
  Microsoft.People_8wekyb3d8bbwe!x4c7a3b7dy2188y46d4ya362y19ac5a5805e5x (11)
  Microsoft.MicrosoftStickyNotes_8wekyb3d8bbwe!App (10)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\SnippingTool.exe (9)
  Microsoft.WindowsCalculator_8wekyb3d8bbwe!App (8)
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\mspaint.exe (7)

Value names with no time stamps:
  UEME_CTLCUACount:ctor
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\cmd.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\oobe\FirstLogonAnim.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\reg.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\cmd.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\WindowsPowerShell\v1.0\powershell.exe
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\conhost.exe
```

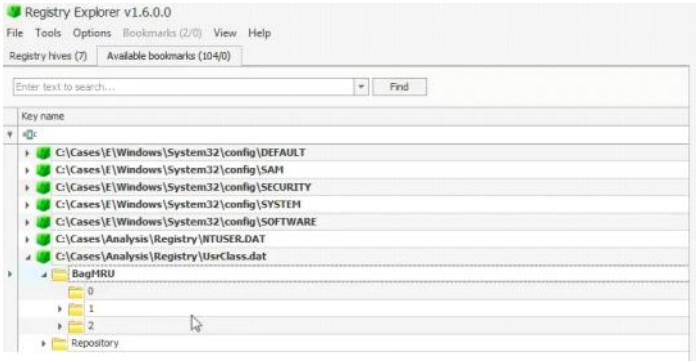
Recent docs:
NTUSER.DAT -> CurrentVersion -> Explorer -> RecentDocs



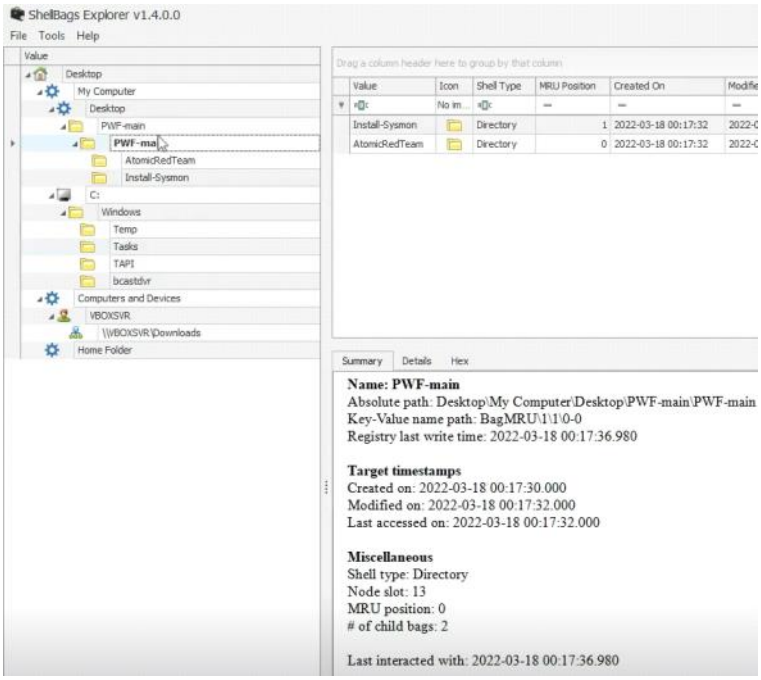
Shellbags:
Already parsed with reg ripper:



Or with reg explorer



Shellbag explorer -> open the USRCLASS.DAT


ShellBags Explorer v1.4.0.0
File Tools Help
Value
Desktop
My Computer
Desktop
PWF-main
PWF-main
AtomicRedTeam
Install-Sysmon
C:
Windows
Temp
Tasks
TAPI
bcastdvr
Computers and Devices
VBOXSVR
\\VBOXSVR\Downloads
Home Folder
Drag a column header here to group by that column
Value
Icon
Shell Type
MRU Position
Created On
Install-Sysmon
Directory
1
2022-03-18 00:17:32
AtomicRedTeam
Directory
0
2022-03-18 00:17:32
Summary
Details
Hex
Name: PWF-main
Absolute path: Desktop\My Computer\Desktop\PWF-main\PWF-main
Key-Value name path: BagMRU\1\1\0-0
Registry last write time: 2022-03-18 00:17:36.980
Target timestamps
Created on: 2022-03-18 00:17:30.000
Modified on: 2022-03-18 00:17:32.000
Last accessed on: 2022-03-18 00:17:32.000
Miscellaneous
Shell type: Directory
Node slot: 13
MRU position: 0
# of child bags: 2
Last interacted with: 2022-03-18 00:17:36.980

File System Analysis:

Sunday, 22 December 2024 19:16

```
FLARE-VM 22/12/2024  9:29:59.06
C:\ToolsForensic\Ericzimmerman\net6>MFTECmd.exe
Description:
  MFTECmd version 1.2.2.1

  Author: Eric Zimmerman (saericzimmerman@gmail.com)
  https://github.com/EricZimmerman/MFTECmd

  Examples: MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out" --csvf MyOutputFile.csv
            MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out"
            MFTECmd.exe -f "C:\Temp\SomeMFT" --json "c:\temp\jsonout"
            MFTECmd.exe -f "C:\Temp\SomeMFT" --body "c:\temp\bout" --bdl c
            MFTECmd.exe -f "C:\Temp\SomeMFT" --de 5-5
            MFTECmd.exe -f "C:\Temp\SomeMFT" --csv "c:\temp\out" --dr --fl
            MFTECmd.exe -f "c:\temp\SomeJ" --csv "c:\temp\out"
            MFTECmd.exe -f "c:\temp\SomeJ" -m "C:\Temp\SomeMFT" --csv "c:\temp\out"
            MFTECmd.exe -f "c:\temp\SomeBoot"
            MFTECmd.exe -f "c:\temp\SomeSecure_SDS" --csv "c:\temp\out"
            MFTECmd.exe -f "c:\temp\SomeI30" --csv "c:\temp\out"

            Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes

Usage:
  MFTECmd [options]

Options:
  -f <f>           File to process ($MFT | $J | $Boot | $SDS | $I30). Required
  -m <m>           $MFT file to use when -f points to a $J file (Use this to resolve parent path in $J CSV output)
  --json <json>    Directory to save JSON formatted results to. This or --csv required unless --de or --body is
                   specified
  --jsonf <jsonf>  File name to save JSON formatted results to. When present, overrides default name
  --csv <csv>      Directory to save CSV formatted results to. This or --json required unless --de or --body is
                   specified
  --csvf <csvf>    File name to save CSV formatted results to. When present, overrides default name
  --body <body>    Directory to save bodyfile formatted results to. --bdl is also required when using this option
  --bodyf <bodyf>  File name to save body formatted results to. When present, overrides default name
  --bdl <bdl>      Drive letter (C, D, etc.) to use with bodyfile. Only the drive letter itself should be provided
  --blf            When true, use LF vs CRLF for newlines [default: False]
  --dd <dd>        Directory to save exported $MFT FILE record. --do is also required when using this option
  --do <do>        Offset of the $MFT FILE record to dump as decimal or hex. Ex: 5120 or 0x1400 Use --de or --debug to
                   see offsets
  --de <de>        Dump full details for $MFT entry/sequence #. Format is 'Entry' or 'Entry-Seq' as decimal or hex.
                   Example: 5, 624-5 or 0x270-0x5.
  --dr             When true, dump $MFT resident files to dir specified by --csv or --json, in 'Resident' subdirectory.
                   Files will be named '<EntryNumber>-<SequenceNumber>_<FileName>.bin'
  --fls            When true, displays contents of directory from $MFT specified by --de. Ignored when --de points to a
                   file [default: False]
  --ds <ds>        Dump full details for Security Id from $SDS as decimal or hex. Example: 624 or 0x270
  --dt <dt>        The custom date/time format to use when displaying time stamps. See https://goo.gl/CNVq0k for
                   options [default: yyyy-MM-dd HH:mm:ss.fffffff]
```

Parse:

```
FLARE-VM 22/12/2024  9:30:04.87
C:\ToolsForensic\Ericzimmerman\net6>MFTECmd.exe -f E:\cases\F\$MFT --csv E:\cases\Analysis\NTFS --csvf MFT.csv
MFTECmd version 1.2.2.1

Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f E:\cases\F\$MFT --csv E:\cases\Analysis\NTFS --csvf MFT.csv

Warning: Administrator privileges not found!

File type: Mft

Processed E:\cases\F\$MFT in 1.5079 seconds

E:\cases\F\$MFT: FILE records found: 120,653 (Free records: 1,325) File size: 119.2MB
        CSV output will be saved to E:\cases\Analysis\NTFS\MFT.csv
```

Open the CSV file in Timeline Explorer:

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

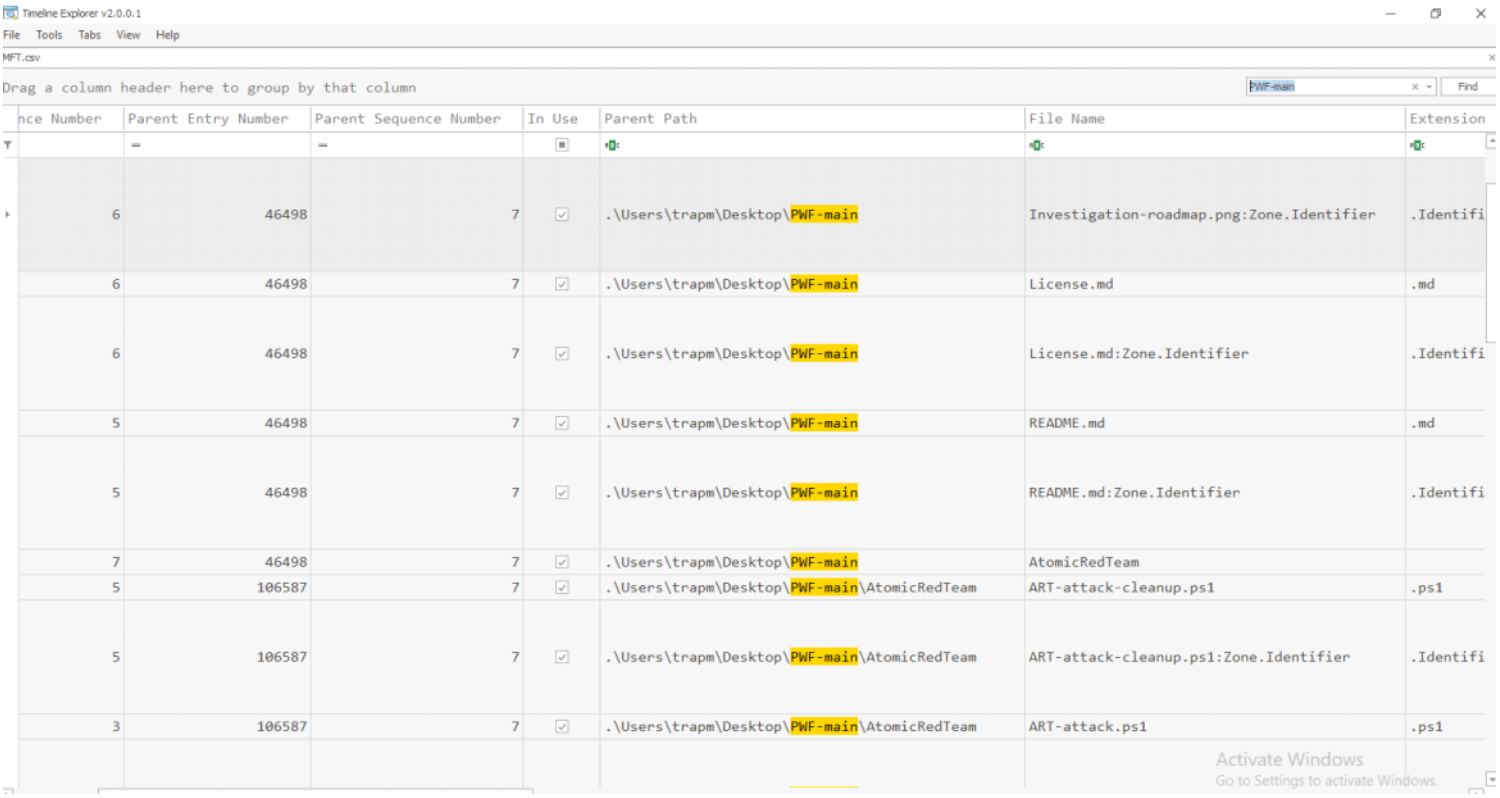
MFT.csv

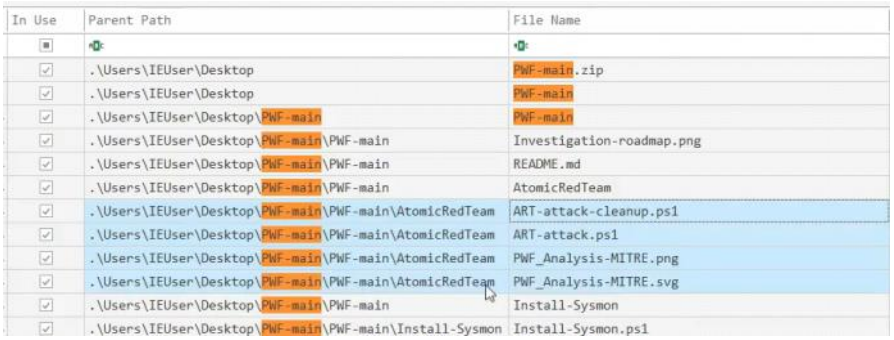
Drag a column header here to group by that column

Enter text to search... Find

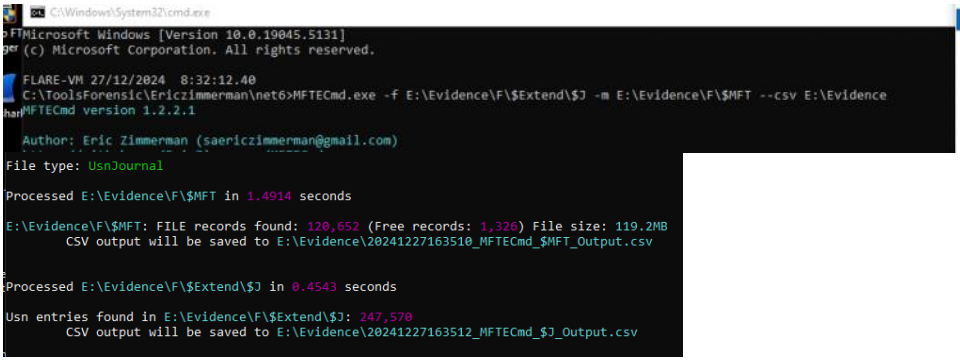
Line	Tag	Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name
1		0	1	5	5	☑	.	$MFT
2		1	1	5	5	☑	.	$MFTMirr
3		2	2	5	5	☑	.	$LogFile
4		3	3	5	5	☑	.	$Volume
5		4	4	5	5	☑	.	$AttrDef
6		5	5	5	5	☑	.	.
7		6	6	5	5	☑	.	$Bitmap
8		6	6	5	5	☑	.	$Bitmap:$SRAT
9		7	7	5	5	☑	.	$Boot
10		8	8	5	5	☑	.	$BadClus
11		8	8	5	5	☑	.	$BadClus:$Bad
12		9	9	5	5	☑	.	$Secure
13		9	9	5	5	☑	.	$Secure:$SDS
14		10	10	5	5	☑	.	$UpCase

Search for the file path we observed from Shallbags that was accessed as suspicious:

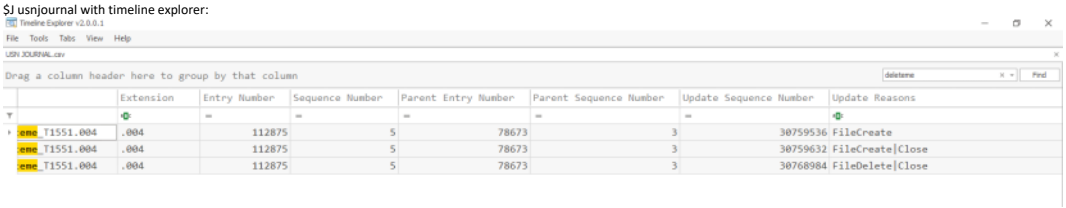




Parse MFT + USN journal:



$J usnjournal with timeline explorer:



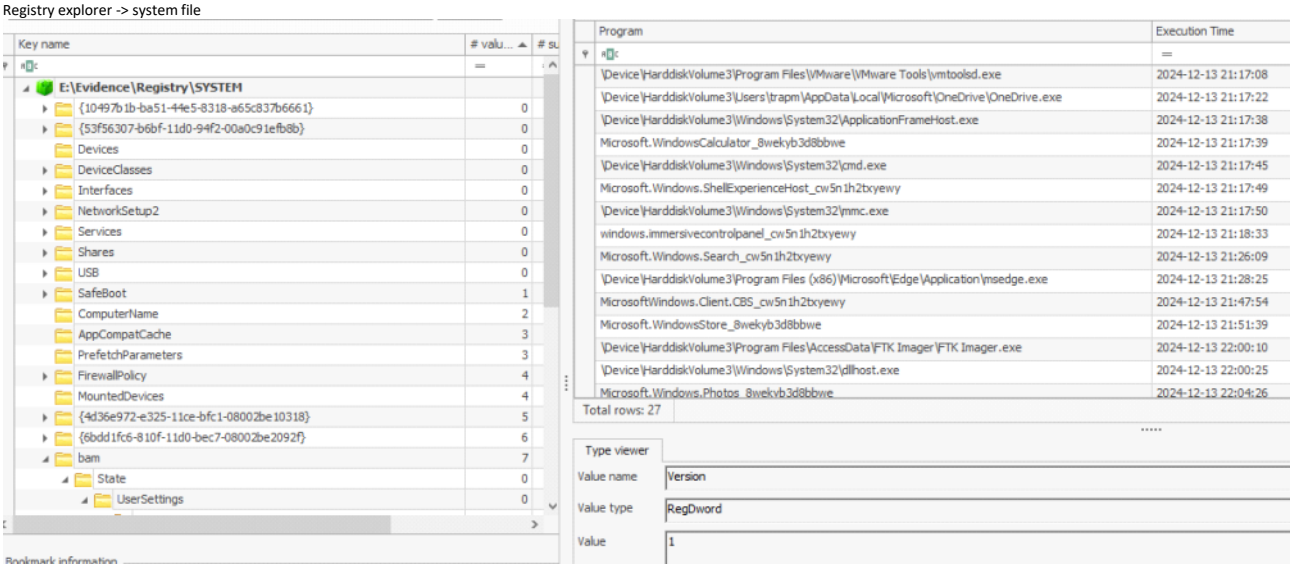
PWF: Disk Analysis Process

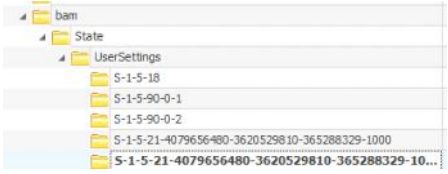
- System & User Information
  - Registry
- File Analysis
  - NTFS
- Evidence of Execution
  - BAM
  - ShimCache
  - Amcache
  - Prefetch
- Persistence Mechanisms
  - Run Keys
  - Startup Folder
  - Scheduled Tasks
  - Services
- Event Log Analysis

Background Activity Moderator (BAM)

Registry: *HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings*

Registry explorer -> system file





Also from reg ripper (search for BAM):

```
DEFAULT.txt | SAM.txt | SECURITY.txt | SOFTWARE.txt | SYSTEM.txt
318  ----------------------------------------
319  bam v.20200427
320  (System) Parse files from System hive BAM Services
321
322  S-1-5-18
323    2024-12-09 17:58:39Z - \Device\HarddiskVolume3\Windows\System32\oobe\FirstLogonAnim.exe
324
325  S-1-5-21-4079656480-3620529810-365288329-1000
326    2024-12-09 17:57:04Z - \Device\HarddiskVolume3\Windows\explorer.exe
327    2024-12-09 17:57:04Z - Microsoft.Windows.CloudExperienceHost_cw5n1h2txyewy
328    2024-12-09 17:57:03Z - Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy
329    2024-12-09 17:57:04Z - MicrosoftWindows.Client.CBS_cw5n1h2txyewy
330    2024-12-09 14:29:24Z - \Device\HarddiskVolume3\Windows\System32\CredentialUIBroker.exe
331
332  S-1-5-21-4079656480-3620529810-365288329-1001
333    2024-12-13 21:16:35Z - \Device\HarddiskVolume3\Windows\explorer.exe
334    2024-12-13 21:16:30Z - Microsoft.Windows.StartMenuExperienceHost_cw5n1h2txyewy
335    2024-12-13 21:26:09Z - Microsoft.Windows.Search_cw5n1h2txyewy
336    2024-12-13 21:17:38Z - \Device\HarddiskVolume3\Windows\System32\ApplicationFrameHost.exe
337    2024-12-13 21:51:39Z - Microsoft.WindowsStore_8wekyb3d8bbwe
338    2024-12-13 21:28:25Z - \Device\HarddiskVolume3\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
339    2024-12-09 18:00:50Z - \Device\HarddiskVolume3\Windows\System32\OpenWith.exe
340    2024-12-09 18:01:06Z - \Device\HarddiskVolume3\Windows\Temp\{4BDF1BCF-CA89-4013-9FC2-3E53434A314C}\.be\VC_redist.x64.exe
341    2024-12-13 21:17:08Z - \Device\HarddiskVolume3\Program Files\VMware\VMware Tools\vmtoolsd.exe
342    2024-12-13 21:47:54Z - MicrosoftWindows.Client.CBS_cw5n1h2txyewy
343    2024-12-13 22:00:25Z - \Device\HarddiskVolume3\Windows\System32\dllhost.exe
344    2024-12-13 21:17:49Z - Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy
345    2024-12-13 21:17:45Z - \Device\HarddiskVolume3\Windows\System32\cmd.exe
346    2024-12-13 21:17:50Z - \Device\HarddiskVolume3\Windows\System32\mmc.exe
347    2024-12-13 21:18:33Z - windows.immersivecontrolpanel_cw5n1h2txyewy
348    2024-12-09 18:03:58Z - \Device\HarddiskVolume3\Windows\System32\CredentialUIBroker.exe
349    2024-12-13 20:36:20Z - Microsoft.XboxGamingOverlay_8wekyb3d8bbwe
350    2024-12-13 21:04:36Z - Microsoft.Windows.SecHealthUI_cw5n1h2txyewy
351    2024-12-13 20:41:52Z - Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe
352    2024-12-13 21:06:11Z - \Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
353    2024-12-13 22:04:26Z - Microsoft.Windows.Photos_8wekyb3d8bbwe
354    2024-12-13 20:35:30Z - Microsoft.LockApp_cw5n1h2txyewy
355    2024-12-13 21:17:22Z - \Device\HarddiskVolume3\Users\trapm\AppData\Local\Microsoft\OneDrive\OneDrive.exe
356    2024-12-13 20:38:50Z - \Device\HarddiskVolume3\Windows\System32\notepad.exe
357    2024-12-13 21:06:13Z - \Device\HarddiskVolume3\Windows\System32\msiexec.exe
358    2024-12-13 22:00:10Z - \Device\HarddiskVolume3\Program Files\AccessData\FTK Imager\FTK Imager.exe
359    2024-12-13 21:17:39Z - Microsoft.WindowsCalculator_8wekyb3d8bbwe
```

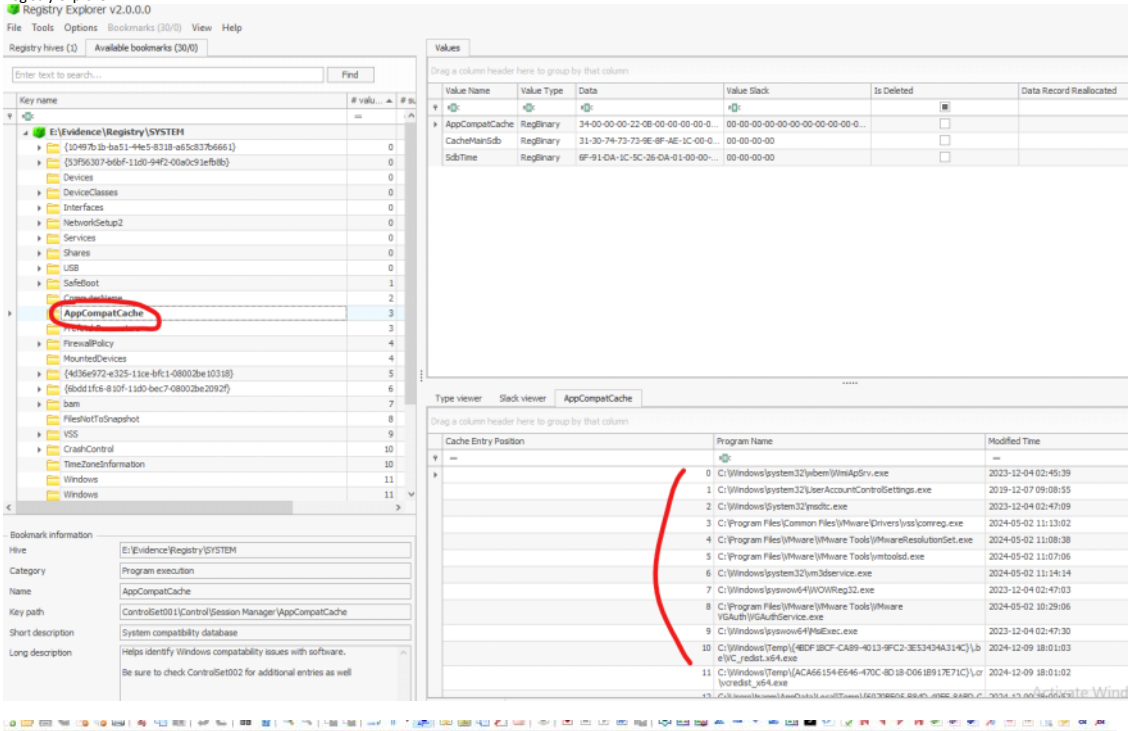
==========

Shimcache (can be used only if the system was shutdown after the incident)

Application Compatibility Cache ("AppCompatCache") / Shimcache

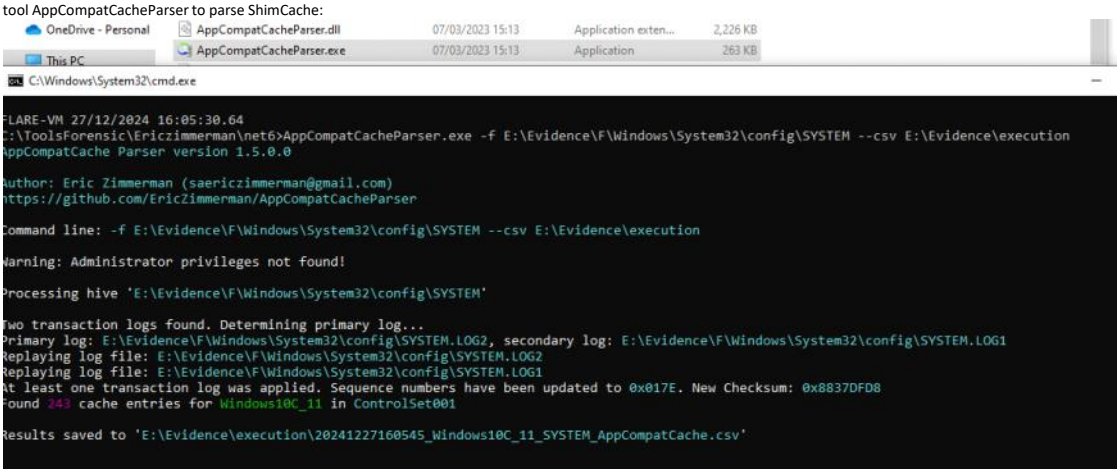
Registry: *HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache*

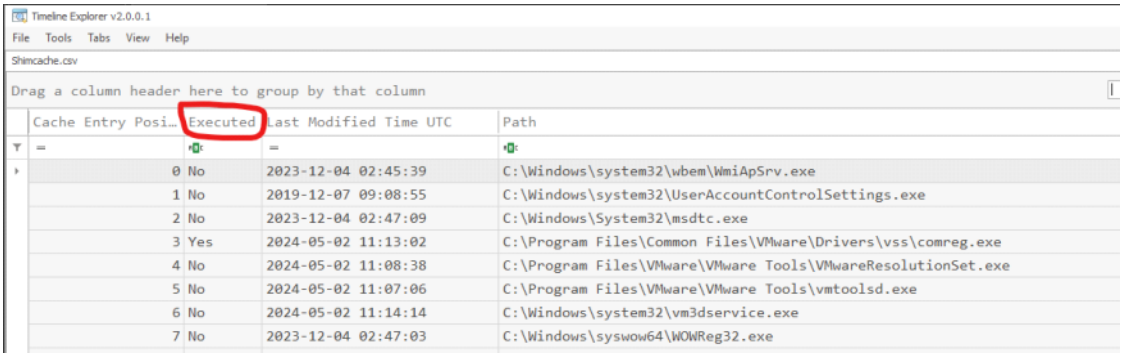
Registry explorer:




```
DEFAULT.txt | SAM.txt | SECURITY.txt | SOFTWARE.txt | SYSTEM.txt
5701
5702   subkey not found.
5703   ----------------------------------------
5704   shimcache v.20220921
5705   (System) Parse file refs from System hive AppCompatCache data
5706
5707   *** ControlSet001 ***
5708   ControlSet001\Control\Session Manager\AppCompatCache
5709   LastWrite Time: 2024-12-09 18:02:19Z
5710   Signature: 0x34
5711   0000000b    03e84a610e340000    000a000000000000    8664    Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy   neutral
5712   C:\Windows\system32\SppExtComObj.exe  2023-12-04 02:46:29
5713   C:\Program Files (x86)\Microsoft\EdgeUpdate\Install\{E1FED7E6-2FCA-49BD-B761-9E7929743348}\EDGEMITMP_B7BCF.tmp\setup.exe  2024-12
5714   00000009    000a000046b50000    000a000028000000    8664    Microsoft.Services.Store.Engagement_8wekyb3d8bbwe
5715   C:\Windows\system32\OOBE-Maintenance.exe  2023-12-04 02:45:39
5716   C:\Windows\system32\taskmgr.exe  2023-12-04 02:46:19
5717   C:\Windows\system32\regsvr32.exe  2019-12-07 09:09:46
5718   00000009    000a06aa34130000    000a00003fab0000    8664    Microsoft.GetHelp   8wekyb3d8bbwe
5719   SIGN.MEDIA=35EA298 setup64.exe  2024-05-02 10:35:41
5720   0000000b    000a00004a610e34    000a0000452b0000    8664    Microsoft.Windows.NarratorQuickStart    8wekyb3d8bbwe   neutral
5721   C:\Users\trapm\AppData\Local\Temp\{6070BE95-B84D-40FE-8ABD-C70B59F5A164}~setup\vcredist_x86.exe  2024-12-09 18:00:57
5722   C:\Program Files\Windows NT\Accessories\wordpad.exe  2023-12-04 02:48:06
```

tool AppCompatCacheParser to parse ShimCache:



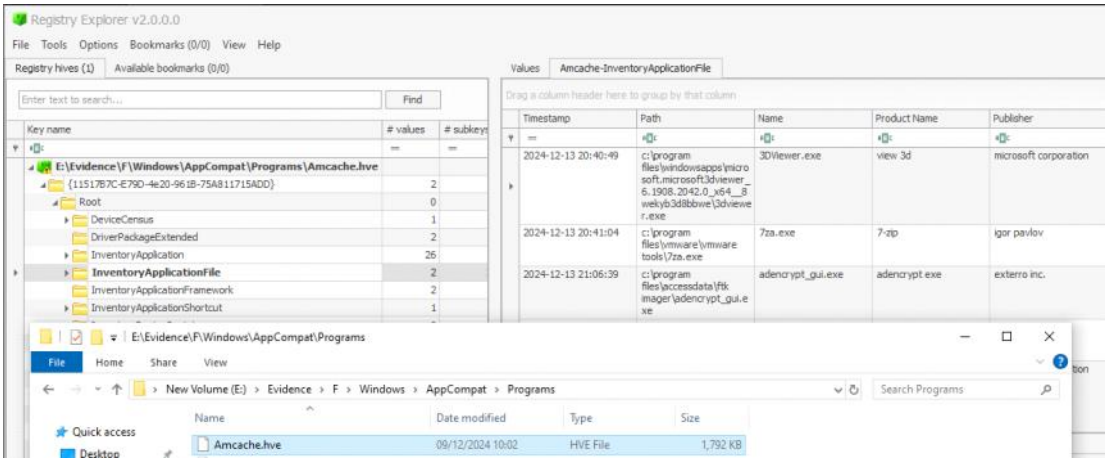


	Cache Entry Posi…	Executed	Last Modified Time UTC	Path
	=	=	=	
0	No	2023-12-04 02:45:39	C:\Windows\system32\wbem\WmiApSrv.exe	
1	No	2019-12-07 09:08:55	C:\Windows\system32\UserAccountControlSettings.exe	
2	No	2023-12-04 02:47:09	C:\Windows\System32\msdtc.exe	
3	Yes	2024-05-02 11:13:02	C:\Program Files\Common Files\VMware\Drivers\vss\comreg.exe	
4	No	2024-05-02 11:08:38	C:\Program Files\VMware\VMware Tools\VMwareResolutionSet.exe	
5	No	2024-05-02 11:07:06	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	
6	No	2024-05-02 11:14:14	C:\Windows\system32\vm3dservice.exe	
7	No	2023-12-04 02:47:03	C:\Windows\syswow64\WOWReg32.exe	

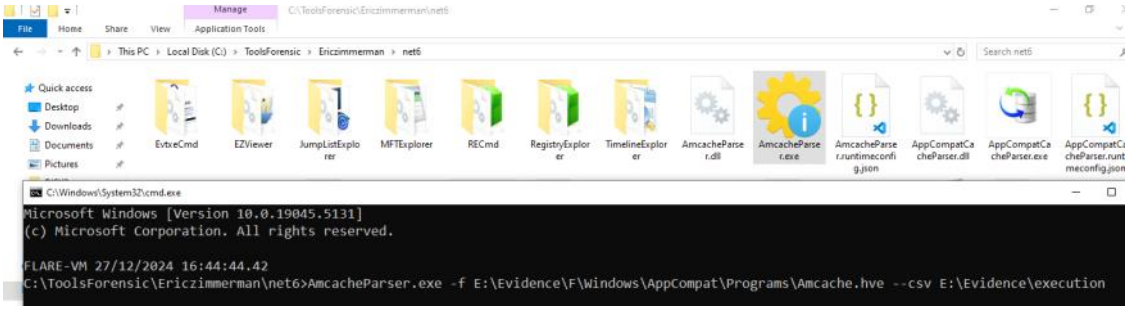
==========

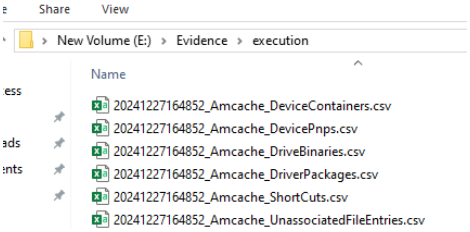
AmCache

Registry: *C:\Windows\AppCompat\Programs\Amcache.hve*



Amcache parser:





Can also Remove the Is Os Component for better view

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

20241227164852_Amcache_UnassociatedFileEntries.csv

Drag a column header here to group by that column

Enter text to search...

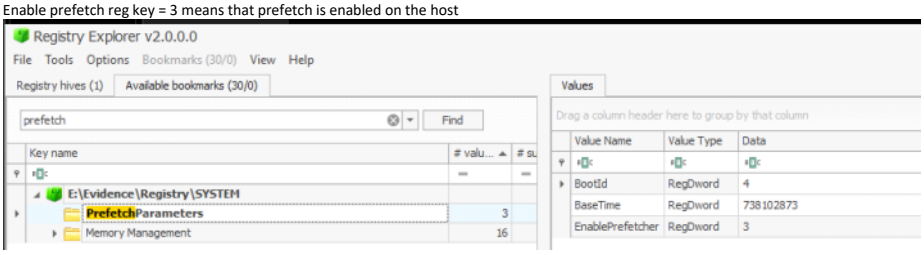
amp	SHA1	Is Os Component	Full Path
	c51217ce3d1959e99886a567d21d0b97022bd6e3	☐	c:\atomicredteam\atomics\t1543.003\bin\atomicservice.exe
	92be78f815897d905538b36fbf015af29616cc49	☑	c:\windows\system32\compattelrunner.exe
	1082c27ec39b3be995f34731d9d41ee9a2f04861	☐	c:\program files (x86)\microsoft\edgecore\131.0.2903.86\cookie_exporter.exe

==========

Prefetch

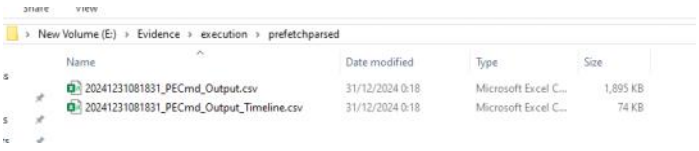
Path: *C:\Windows\Prefetch*.pf*

Enable prefetch reg key = 3 means that prefetch is enabled on the host



Parse Prefetch files:
Full folder with -d
Specific file with -f

```
FLARE-VM 31/12/2024  0:18:31.83
C:\ToolsForensic\Ericzimmerman\net6>PECmd.exe -d E:\Evidence\F\Windows\prefetch --csv E:\Evidence\execution\prefetchparsed
```



Tag the relevant processes and then enable tagging to display just them, this will build the event timeline:

Line	Tag	Run Time	Executable Name
286	☑	2022-03-18 00:25:52	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\NOTEPAD.EXE
197	☑	2022-03-18 00:25:52	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\MAVINJECT.EXE
383	☑	2022-03-18 00:25:36	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\SC.EXE
382	☑	2022-03-18 00:25:36	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\SC.EXE
18	☑	2022-03-18 00:25:36	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-MASTER\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE
386	☑	2022-03-18 00:25:32	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\SCHTASKS.EXE
385	☑	2022-03-18 00:25:32	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\SCHTASKS.EXE
315	☑	2022-03-18 00:25:13	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\REG.EXE
316	☑	2022-03-18 00:25:05	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\REG.EXE
276	☑	2022-03-18 00:24:47	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\NET1.EXE
275	☑	2022-03-18 00:24:47	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\NET1.EXE
274	☑	2022-03-18 00:24:47	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\NET1.EXE
269	☑	2022-03-18 00:24:47	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\NET.EXE
268	☑	2022-03-18 00:24:47	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\NET.EXE
267	☑	2022-03-18 00:24:47	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\NET.EXE
71	☑	2022-03-18 00:24:46	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\CMD.EXE
307	☑	2022-03-18 00:24:29	\VOLUME{01d4de8ba6e93c69-b4a6fec6}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE

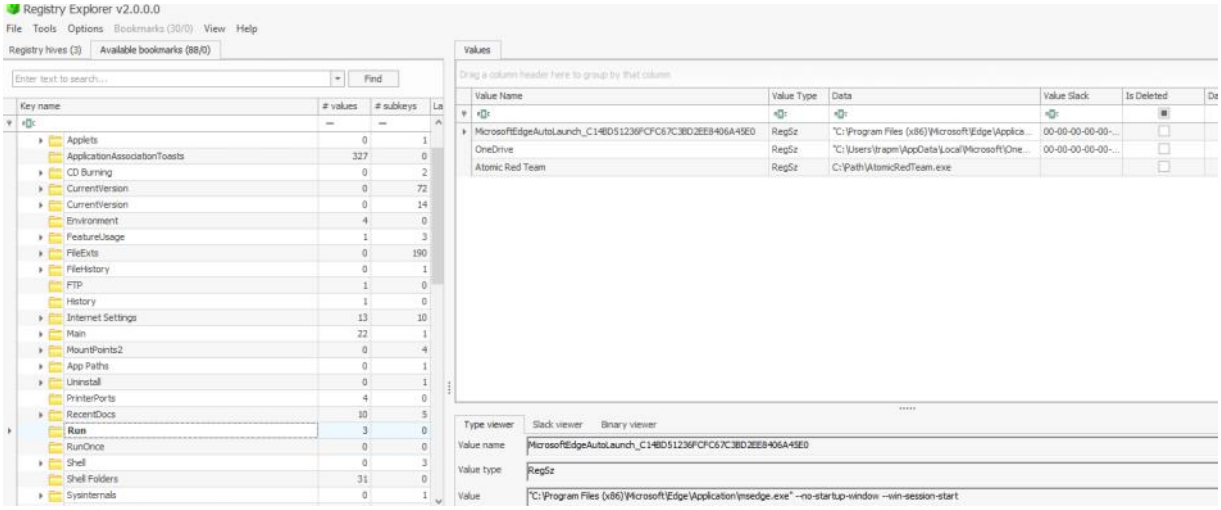
Persistence Mechanisms

Auto-Run Keys

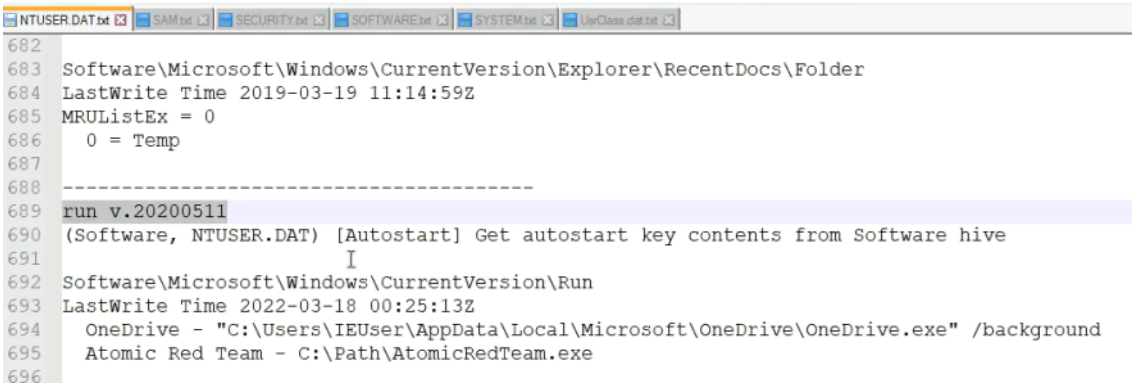
Registry:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

Reg explorer
Software and NTUSER hives:



Also from reg ripper:



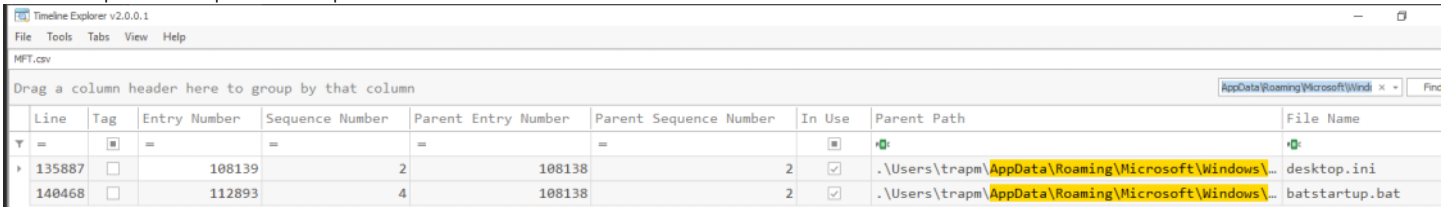
==========

Startup Folder

Paths:

C:\Users\[Username]\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

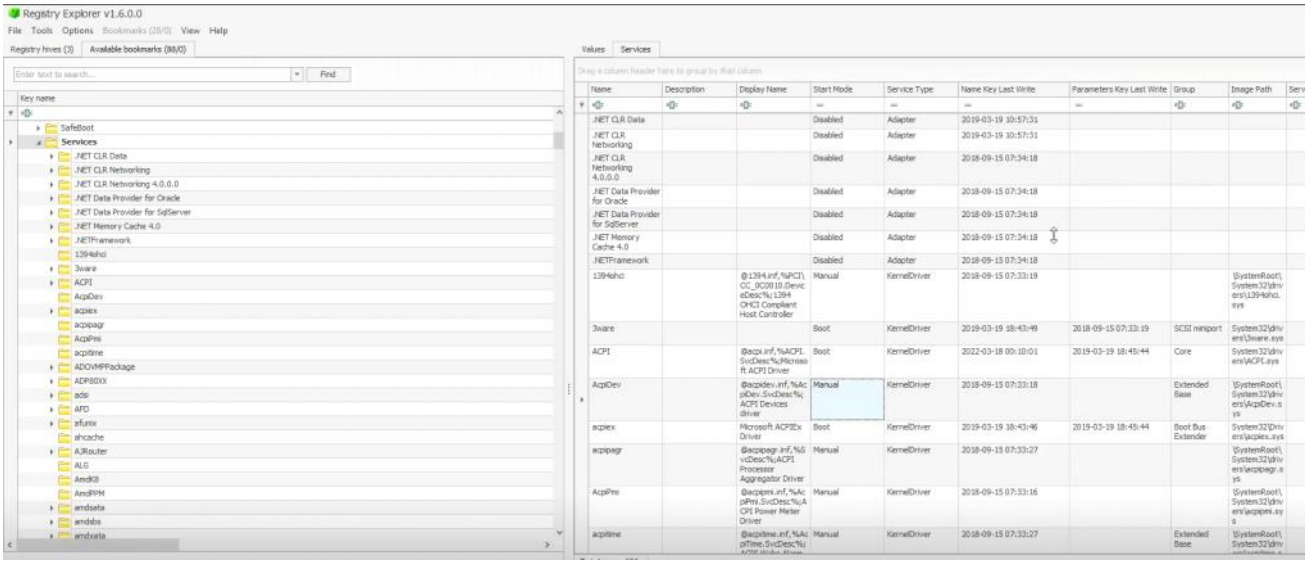
Search these paths of startup folders in the parsed MFT to see the files inside:

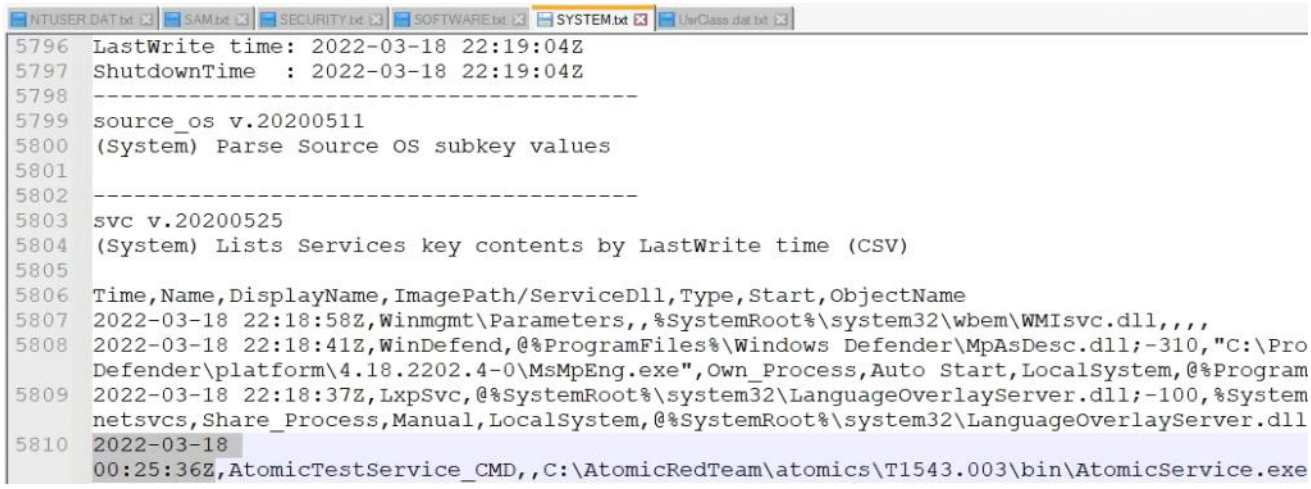


==========

Windows Services

Registry: *HKLM\SYSTEM\CurrentControlSet\Services*





==========

Scheduled Tasks

Registry:

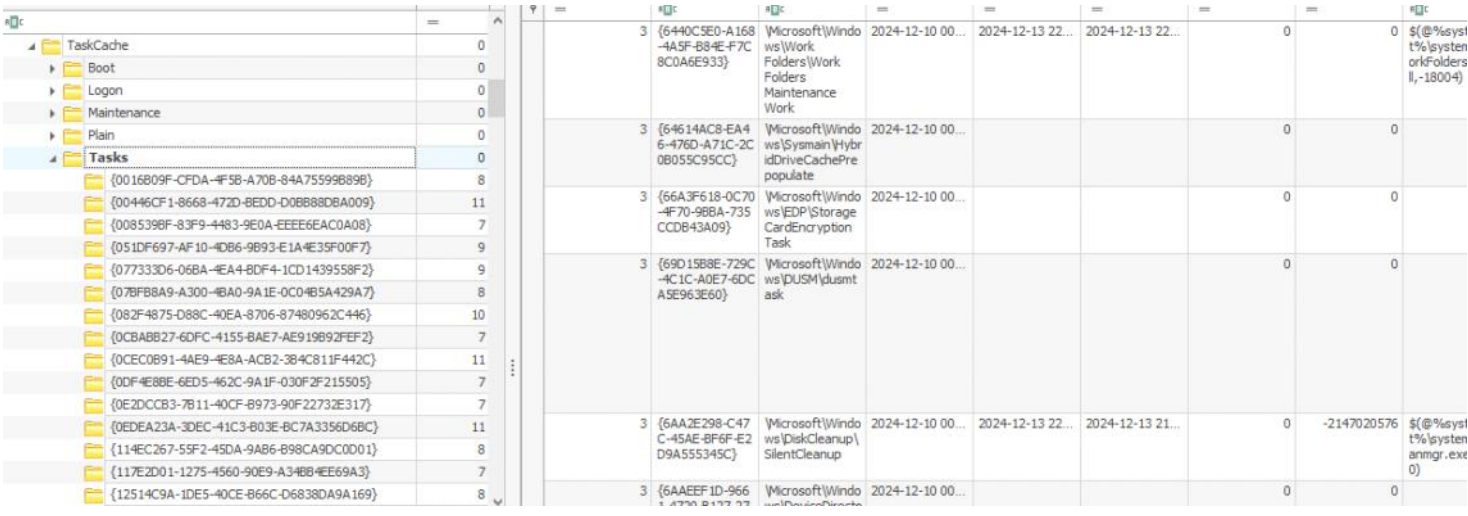
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree

Path:

C:\Windows\System32\Tasks

SOFTWARE -> TaskCache -> Tasks



Values | TaskCache

Drag a column header here to group by that column

Version	Key Name	Path	Created On	Last Start	Last Stop	Task State	Last Action R...	Source	Description	Security Desc...	Author
3	{D6CEA745-2EA0-47EC-9845-FA3565F6E8D1}	\T1053_005_OnStartup	2024-12-13 20:38:42	2024-12-13 2...	2024-12-13 2...	0	0				DESKTOP-AU5K958\Avior
3	{C46F43EC-26E2-49F7-8065-6C772C7E1534}	\T1053_005_OnLogon	2024-12-13 20:38:42	2024-12-13 2...	2024-12-13 2...	0	0				DESKTOP-AU5K958\Avior

DEFAULT.txt | SAM.txt | SECURITY.txt | SOFTWARE.txt | SYSTEM.txt

```
40080
40081   ----------------------------------------
40082   taskcache v.20200427
40083   (Software) Checks TaskCache\Tree root keys (not subkeys)
```

```
T1053_005_OnLogon
LastWrite: 2024-12-13 20:38:42Z
Id: {C46F43EC-26E2-49F7-8065-6C772C7E1534}
Task Reg Time: 2024-12-13 20:38:42Z
Task Last Run: 2024-12-13 21:16:13Z
Task Completed: 2024-12-13 21:17:45Z

T1053_005_OnStartup
LastWrite: 2024-12-13 20:38:42Z
Id: {D6CEA745-2EA0-47EC-9845-FA3565F6E8D1}
Task Reg Time: 2024-12-13 20:38:42Z
Task Last Run: 2024-12-13 21:15:50Z
Task Completed: 2024-12-13 21:17:45Z
```

The tasks are stored as xml file, so we can open them in any text editor:

E:\Evidence\F\Windows\System32\Tasks

File | Home | Share | View

New Volume (E:) › Evidence › F › Windows › System32 › Tasks ›

Quick access
- Desktop
- Downloads
- Documents
- Pictures
- DISK2
- Dropper.Downloadl
- Evidence
- Registry

Name	Date modified	Type	Size
Microsoft	27/12/2024 8:07	File folder	
MicrosoftEdgeUpdateTaskMachineCore	09/12/2024 6:20	File	4 KB
MicrosoftEdgeUpdateTaskMachineUA	09/12/2024 6:20	File	4 KB
OneDrive Reporting Task-S-1-5-21-40796...	13/12/2024 12:37	File	4 KB
OneDrive Standalone Update Task-S-1-5-...	13/12/2024 12:37	File	4 KB
T1053_005_OnLogon	13/12/2024 12:38	File	4 KB
T1053_005_OnStartup	13/12/2024 12:38	File	4 KB

E:\Evidence\F\Windows\System32\Tasks\T1053_005_OnStartup - Notepad++

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

DEFAULT.txt | SAM.txt | SECURITY.txt | SOFTWARE.txt | SYSTEM.txt | T1053_005_OnLogon | T1053_005_OnStartup

```
34    </Settings>
35    <Actions Context="Author">
36      <Exec>
37        <Command>cmd.exe</Command>
38        <Arguments>/c calc.exe</Arguments>
39      </Exec>
40    </Actions>
41    <Principals>
42      <Principal id="Author">
43        <UserId>S-1-5-18</UserId>
44        <RunLevel>LeastPrivilege</RunLevel>
45      </Principal>
46    </Principals>
47  </Task>
```

Memory Analysis

with Volatility3

Files:

Memory (volatile data)
hiberfil.sys
pagefile.sys
swapfile.sys

```
┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem windows.info.Info
Volatility 3 Framework 2.15.0
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0×f8004e413000
DTB     0×1ad000
Symbols file:///home/kali/Desktop/volatility/volatility3/volatility3/symbols/windows/ntkrnlmp.pdb/D9424FC4861E47C10FAD1B35DEC6DCC8-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0×f8004f022400
Major/Minor     15.19041
MachineType     34404
KeNumberProcessors      1
SystemTime      2024-12-13 21:06:30+00:00
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  10
NtMinorVersion  0
PE MajorOperatingSystemVersion  10
PE MinorOperatingSystemVersion  0
PE Machine      34404
PE TimeDateStamp        Mon Dec  9 11:07:51 2019
```

```
windows.pslist.PsList
                Lists the processes present in a particular windows memory image.
windows.psscan.PsScan
                Scans for processes present in a particular windows memory image.
windows.pstree.PsTree
                Plugin for listing processes in a tree based on their parent process ID.
```

```
┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem windows.pstree.PsTree
Volatility 3 Framework 2.15.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        Audit   Cmd     Path

4       0       System  0×ce8d08e83040  120     -       N/A     False   2024-12-09 18:02:30.000000 UTC  N/A     -       -       -
* 72    4       Registry        0×ce8d08ee3080  4       -       N/A     False   2024-12-09 18:02:26.000000 UTC  N/A     Registry        -       -
* 524   4       smss.exe        0×ce8d09ecb040  2       -       N/A     False   2024-12-09 18:02:30.000000 UTC  N/A     \Device\HarddiskVolume3\Windows
\System32\smss.exe      -       -
* 1540  4       MemCompression  0×ce8d08fb7040  58      -       N/A     False   2024-12-09 18:02:35.000000 UTC  N/A     MemCompression  -       -
628     616     csrss.exe       0×ce8d097dd080  9       -       0       False   2024-12-09 18:02:33.000000 UTC  N/A     \Device\HarddiskVolume3\Windows
\System32\csrss.exe     -       -
712     616     wininit.exe     0×ce8d0cc19080  1       -       0       False   2024-12-09 18:02:33.000000 UTC  N/A     \Device\HarddiskVolume3\Windows
\System32\wininit.exe   -       -
```

```
2080    824     AtomicService.  0×ce8d116c0340  3       -       0       False   2024-12-13 20:38:45.000000 UTC  N/A     Disabled
224     2944    notepad.exe     0×ce8d0d5be080  2       -       2       False   2024-12-13 20:38:49.000000 UTC  N/A     Disabled
```

Check for the parent process using PPID:

```
└─$ python3 vol.py -f memdump.mem windows.pslist --pid 2080
Volatility 3 Framework 2.15.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

2080    824     AtomicService.  0×ce8d116c0340  3       -       0       False   2024-12-13 20:38:45.000000 UTC  N/A     Disabled

┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem windows.pslist --pid 824
Volatility 3 Framework 2.15.0
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

824     712     services.exe    0×ce8d0cc78080  6       -       0       False   2024-12-09 18:02:33.000000 UTC  N/A     Disabled
```

Dump the file:

```
┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem windows.pslist --pid 2080 --dump
```

==========

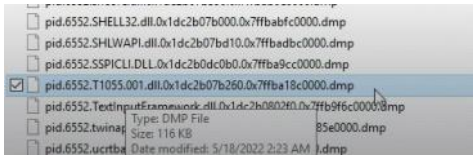
Investigate the dll injection on the notepad process:

```
┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem windows.dlllist --pid 224 > dll.txt
```

```
6552    notepad.exe 0x7ffbaa850000  0x4a000 cfgmgr32.dll     C:\Windows\System32\cfgmgr32.dll     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffbaa8a0000  0x74a000    windows.storage.dll C:\Windows\System32\windows.storage.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba9e00000  0x24000 profapi.dll C:\Windows\System32\profapi.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba9e30000  0x5d000 powrprof.dll     C:\Windows\System32\powrprof.dll     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba9de0000  0x11000 kernel.appcore.dll  C:\Windows\System32\kernel.appcore.dll  2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffbaa240000  0x17000 cryptsp.dll C:\Windows\System32\cryptsp.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffb96990000  0x279000    COMCTL32.dll
C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.379_none_05b83be8071c94a1\COMCTL32.dll 2022-03-18 00:25:52.000000  Disabl
6552    notepad.exe 0x7ffba6750000  0x1a8000    PROPSYS.dll C:\Windows\system32\PROPSYS.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffb964a0000  0x89000 WINSPOOL.DRV     C:\Windows\system32\WINSPOOL.DRV     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffbaa110000  0x26000 bcrypt.dll  C:\Windows\System32\bcrypt.dll  2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffb9fa10000  0x1d6000    urlmon.dll  C:\Windows\system32\urlmon.dll  2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffbadc20000  0xcb000 OLEAUT32.dll     C:\Windows\System32\OLEAUT32.dll     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba9340000  0x3d000 IPHLPAPI.DLL     C:\Windows\system32\IPHLPAPI.DLL     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffb9f760000  0x2a8000    iertutil.dll     C:\Windows\system32\iertutil.dll     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba97b0000  0xc000  CRYPTBASE.DLL    C:\Windows\system32\CRYPTBASE.DLL    2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffbaaff0000  0x2e000 IMM32.DLL    C:\Windows\System32\IMM32.DLL    2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba8230000  0x9c000 uxtheme.dll C:\Windows\System32\uxtheme.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffbad920000  0xa2000 clbcatq.dll C:\Windows\System32\clbcatq.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffb9da50000  0x107000    MrmCoreR.dll     C:\Windows\System32\MrmCoreR.dll     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffbad7a0000  0x16a000    MSCTF.dll    C:\Windows\System32\MSCTF.dll    2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba84b0000  0x2e000 dwmapi.dll  C:\Windows\system32\dwmapi.dll  2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffbaa260000  0x1db000    CRYPT32.dll C:\Windows\System32\CRYPT32.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba9dc0000  0x12000 MSASN1.dll  C:\Windows\System32\MSASN1.dll  2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffb83f00000  0xc6000 efswrt.dll  C:\Windows\System32\efswrt.dll  2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba48d0000  0x1a000 MPR.dll C:\Windows\System32\MPR.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba62c0000  0x153000    wintypes.dll     C:\Windows\SYSTEM32\wintypes.dll     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba85e0000  0x20d000    twinapi.appcore.dll C:\Windows\System32\twinapi.appcore.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba8590000  0x28000 RMCLIENT.dll     C:\Windows\System32\RMCLIENT.dll     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffb8f280000  0x6c000 oleacc.dll  C:\Windows\System32\oleacc.dll  2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffb9f6c0000  0x95000 TextInputFramework.dll  C:\Windows\System32\TextInputFramework.dll  2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba6420000  0x322000    CoreUIComponents.dll     C:\Windows\System32\CoreUIComponents.dll     2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba79d0000  0xe2000 CoreMessaging.dll   C:\Windows\System32\CoreMessaging.dll   2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba8e80000  0x31000 ntmarta.dll C:\Windows\SYSTEM32\ntmarta.dll 2022-03-18 00:25:52.000000  Disabled
6552    notepad.exe 0x7ffba18c0000  0x1d000 T1055.001.dll    C:\AtomicRedTeam\atomics\T1055.001\src\x64\T1055.001.dll    2022-03-18 00:25:53.000000  Disabled
6552    notepad.exe 0x7ffba44d0000  0xc000  Secur32.dll C:\Windows\system32\Secur32.dll 2022-03-18 00:25:53.000000  Disabled
6552    notepad.exe 0x7ffba9cc0000  0x2f000 SSPICLI.DLL C:\Windows\system32\SSPICLI.DLL 2022-03-18 00:25:53.000000  Disabled
```

Dump the dll:

```
┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem windows.dlllist --pid 224 --dump
```



==========

=====

Get the SIDs and users:

```
┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem windows.getsids --pid 2080 224
Volatility 3 Framework 2.15.0
Progress:  100.00               PDB scanning finished
PID     Process SID     Name

2080    AtomicService.  S-1-5-18         Local System
2080    AtomicService.  S-1-5-32-544     Administrators
2080    AtomicService.  S-1-1-0 Everyone
2080    AtomicService.  S-1-5-11        Authenticated Users
2080    AtomicService.  S-1-16-16384    System Mandatory Level
224     notepad.exe     S-1-5-21-4079656480-3620529810-365288329-1001   trapm
224     notepad.exe     S-1-5-21-4079656480-3620529810-365288329-513    Domain Users
224     notepad.exe     S-1-1-0 Everyone
224     notepad.exe     S-1-5-114       Local Account (Member of Administrators)
224     notepad.exe     S-1-5-32-544    Administrators
224     notepad.exe     S-1-5-32-545    Users
224     notepad.exe     S-1-5-4 Interactive
224     notepad.exe     S-1-2-1 Console Logon (Users who are logged onto the physical console)
224     notepad.exe     S-1-5-11        Authenticated Users
224     notepad.exe     S-1-5-15        This Organization
224     notepad.exe     S-1-5-113       Local Account
224     notepad.exe     S-1-5-5-0-1724277       Logon Session
224     notepad.exe     S-1-2-0 Local (Users with the ability to log in locally)
224     notepad.exe     S-1-5-64-10     NTLM Authentication
224     notepad.exe     S-1-16-12288    High Mandatory Level
```

==========

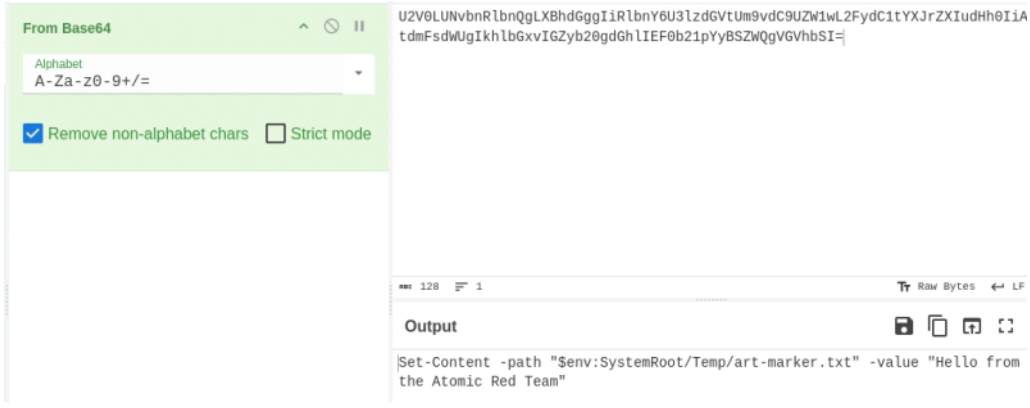
Suspicious Registry Key

```
iex ([Text.Encoding]::ASCII.GetString([Convert]::FromBase64String((gp 'HKCU:\Software\Classes
\AtomicRedTeam').ART
```

```
windows.registry.certificates.Certificates
                    Lists the certificates in the registry's Certificate Store.
  windows.registry.hivelist.HiveList
                    Lists the registry hives present in a particular memory image.
  windows.registry.hivescan.HiveScan
                    Scans for registry hives present in a particular windows memory image.
  windows.registry.printkey.PrintKey
                    Lists the registry keys under a hive or specific key value.
  windows.registry.userassist.UserAssist
                    Print userassist registry keys and information.
  windows.skeleton_key_check.Skeleton_Key_Check
                    Looks for signs of Skeleton Key malware
  windows.ssdt.SSDT   Lists the system call table.
```

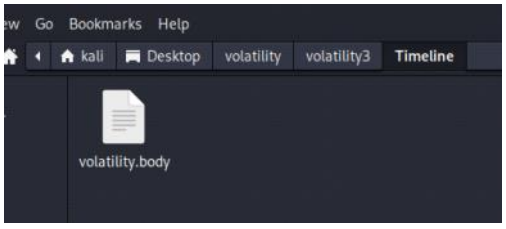
```
└─$ python3 vol.py -f memdump.mem windows.registry.hivelist
Volatility 3 Framework 2.15.0
Progress:  100.00               PDB scanning finished
Offset  FileFullPath    File output

0×8b09dce74000          Disabled
0×8b09dce89000  \REGISTRY\MACHINE\SYSTEM        Disabled
0×8b09dceed000  \REGISTRY\MACHINE\HARDWARE      Disabled
0×8b09dd8a4000  \Device\HarddiskVolume1\EFI\Microsoft\Boot\BCD  Disabled
0×8b09dd8f3000  \SystemRoot\System32\Config\SOFTWARE    Disabled
0×8b09e1321000  \SystemRoot\System32\Config\DEFAULT     Disabled
0×8b09e1366000  \SystemRoot\System32\Config\SECURITY    Disabled
0×8b09e6c05000  \SystemRoot\System32\Config\SAM Disabled
0×8b09e6cd0000  \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT        Disabled
0×8b09e0c19000  \SystemRoot\System32\Config\BBI Disabled
0×8b09e0c1d000  \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Disabled
0×8b09e71b1000  \??\C:\Users\trapm\ntuser.dat    Disabled
0×8b09e77e4000  \??\C:\Windows\AppCompat\Programs\Amcache.hve    Disabled
0×8b09e2ed4000  \??\C:\Users\trapm\ntuser.dat    Disabled
0×8b09e1288000  \??\C:\Users\trapm\AppData\Local\Microsoft\Windows\UsrClass.dat Disabled
```

```
┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem windows.registry.printkey --offset 0×8b09e1288000 --key AtomicRedTeam
Volatility 3 Framework 2.15.0
Progress:  100.00               PDB scanning finished
Last Write Time Hive Offset     Type    Key     Name    Data    Volatile

2024-12-13 20:38:27.000000 UTC  0×8b09e1288000  REG_SZ  \??\C:\Users\trapm\AppData\Local\Microsoft\Windows\UsrClass.dat\AtomicRedTeam   ART     "U2V0LUNvbnRl
bnQgLXBhdGggIiRlbnY6U3lzdGVtUm9vdC9UZW1wL2FydC1tYXJrZXIudHh0IiAtdmFsdWUgIkhlbGxvIGZyb20gdGhlIEF0b21pYyBSZWQgVGVhbSI="    False
```



Create timeline file from the full memory:

```
┌──(kali㉿kali)-[~/Desktop/volatility/volatility3]
└─$ python3 vol.py -f memdump.mem timeliner --create-bodyfiles
```



Make master timeline from full Disk image

```
And that is how you build a timeline using log2timeline...
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ log2timeline.py --storage-file disk.plaso /mnt/c/Cases/
2022-03-23T223835_ConsoleLog.txt  2022-03-23T223835_SkipLog.csv     E/                              win10-disk.raw
2022-03-23T223835_CopyLog.csv     Analysis/                        Notes.docx                      win10-disk.vhd
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ log2timeline.py --storage-file disk.plaso /mnt/c/Cases/win10-disk.raw
```

```
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ pinfo.py disk.plaso

************************* Plaso Storage Information *************************
            Filename : disk.plaso
      Format version : 20211121
Serialization format : json
---------------------------------------------------------------------------

********************************* Sessions *********************************
ad8839b4-9583-4854-a69a-248c7b326453 : 2022-06-08T00:29:25.907642+00:00
---------------------------------------------------------------------------
```

```
****************************** Event sources *******************************
Total : 158051
---------------------------------------------------------------------------

*********************** Events generated per parser ************************
          Parser (plugin) name : Number of events
---------------------------------------------------------------------------
                       amcache : 190
                appcompatcache : 344
                       bagmru : 21
                          bam : 14
          explorer_mountpoints2 : 4
         explorer_programscache : 1
                      filestat : 632137
                           lnk : 453
                mrulist_string : 1
             mrulistex_string : 2
mrulistex_string_and_shell_item : 3
                    msie_zone : 36
                     networks : 4
   olecf_automatic_destinations : 34
```

Add the volatility file to the disk file

```
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ log2timeline.py --parser=mactime --storage-file=disk.plaso volatility.body
```

Convert the file to CSV
The date is not must , this will return logs with timestamps only after 1-3-2022

```
forensics@WIN-BK1Q9542K3L:/mnt/c/Cases/Analysis/Timeline$ psort.py -o l2tcsv -w super-timeline.csv disk.plaso "date > '2022-03-01 00:00:00'"
```

Name	Date modified	Type	Size
disk.plaso	6/8/2022 2:46 AM	PLASO File	687,036 KB
log2timeline-20220608T002923.log.gz	6/8/2022 2:09 AM	GZ File	1 KB
log2timeline-20220608T024654.log.gz	6/8/2022 2:46 AM	GZ File	1 KB
psort-20220608T025005.log.gz	6/8/2022 2:56 AM	GZ File	44 KB
super-timeline.csv	6/8/2022 2:56 AM	CSV File	74,356 KB
volatility.body	6/7/2022 10:46 PM	BODY File	1,207 KB

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 Description	Source Name	macb	Inode	Long Description
915		0001-01-01 00:00:00	System - Network Co…	LOG	.a..	46357	SSID: Network Description: Network Connection Type: Wired D
1		2022-03-01 22:10:46	PE Event	PE	...b	126961	PE Type: Dynamic Link Library (DLL)
2		2022-03-01 22:10:47	PE Event	PE	...b	126963	PE Type: Dynamic Link Library (DLL)
3		2022-03-01 22:10:48	PE Event	PE	...b	126965	PE Type: Dynamic Link Library (DLL)
4		2022-03-01 22:10:49	PE Event	PE	...b	126967	PE Type: Dynamic Link Library (DLL)
5		2022-03-01 22:10:49	PE Event	PE	...b	126969	PE Type: Dynamic Link Library (DLL)
6		2022-03-01 22:10:50	PE Event	PE	...b	126971	PE Type: Dynamic Link Library (DLL)
7		2022-03-01 22:10:51	PE Event	PE	...b	126973	PE Type: Dynamic Link Library (DLL)
8		2022-03-01 22:10:52	PE Event	PE	...b	126975	PE Type: Dynamic Link Library (DLL)
9		2022-03-01 22:10:53	PE Event	PE	...b	126977	PE Type: Dynamic Link Library (DLL)
10		2022-03-01 22:11:00	PE Event	PE	...b	126979	PE Type: Dynamic Link Library (DLL)