

Evidence of program execution:

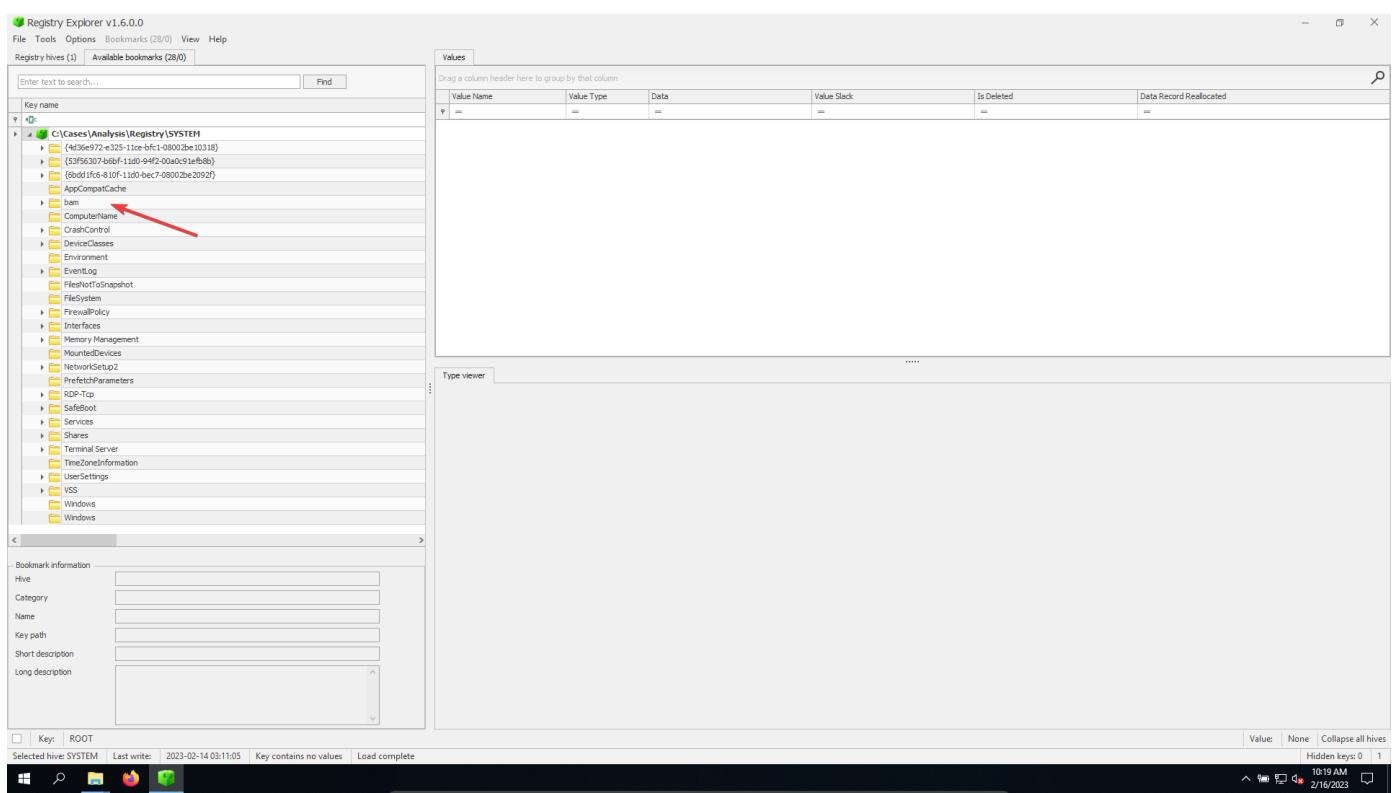
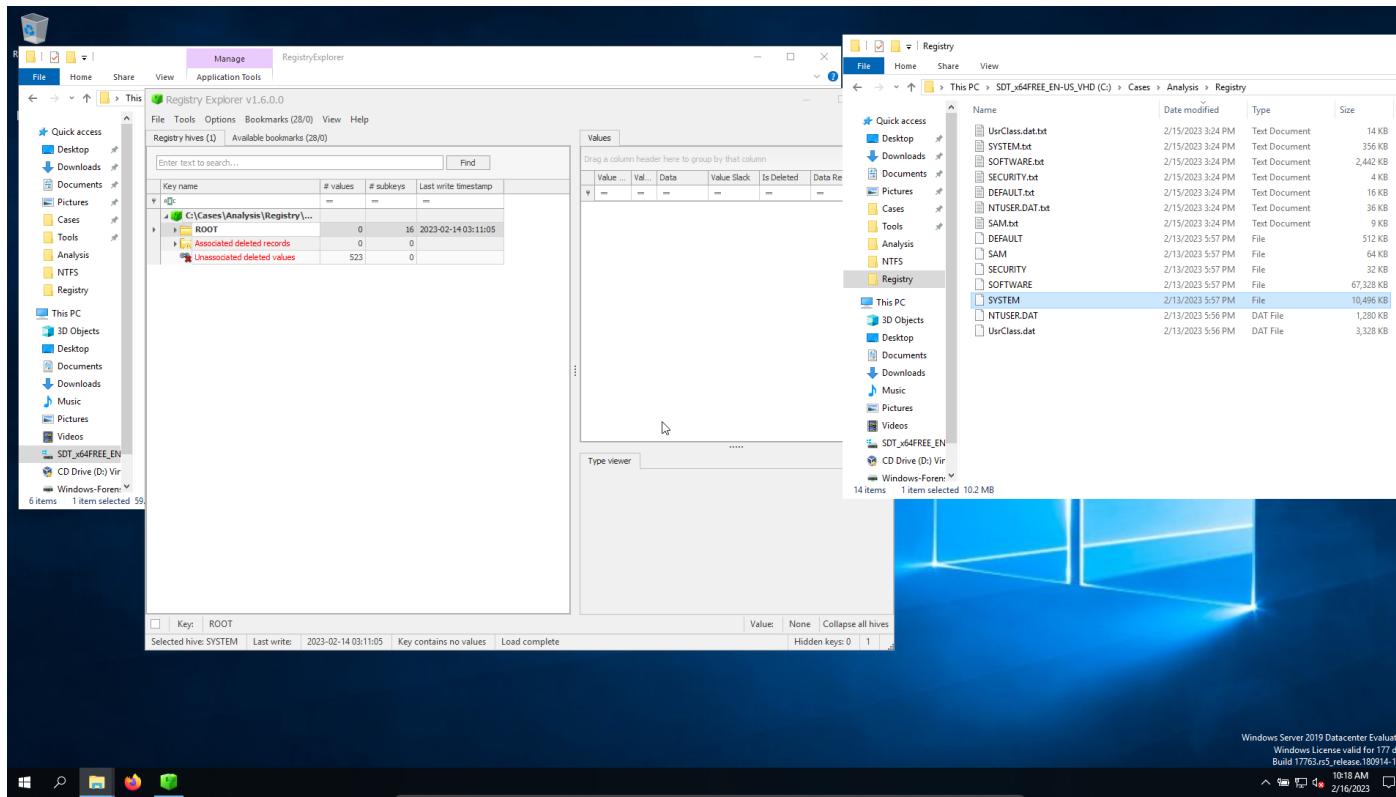
- Execution artifacts:
 - Background Activity Moderator (BAM)
 - Application Compatibility Cache (ShimCache)
 - Amcache
 - Prefetch
 - Prefetch Timeline-Analysis

- Find :
 - What executables did BAM recorded for the user IEUser?
Print execution date and time.
 - Cache entry position for:
 - AtomicService.exe
 - Mavinject.exe
 - SHA-1 for the AtomicService.exe record.

Background Activity Moderator (BAM)

- You can find the BAM in the registry:
 - HKLM\SYSTEM\CurrentControlSet\Services\bam\UserSettings

- FThe BAM records information about executables that have been ran on a system
- Open RegistryExplorer and upload SYSTEM registry hive:



Program	Execution Time
Microsoft.Windows.ShellExperienceHost_cw5n1h2byewy	2023-02-13 17:56:58
Microsoft.Windows.Cortana_cw5n1h2byewy	2023-02-13 17:56:58
Microsoft.MicrosoftEdge_swkeyb3dbbwe	2023-02-13 17:56:58
Microsoft.WindowsStore_swkeyb3dbbwe	2023-02-13 17:20:29
[Device]HarddiskVolume3\Windows\System32\ApplicationFrameHost.exe	2023-02-13 17:56:58
[Device]HarddiskVolume3\Windows\explorer.exe	2023-02-13 17:56:58
windows.immersivecontrolpanel_cw5n1h2byewy	2023-02-13 17:14:04
Microsoft.Windows.SeeHealHUI_cw5n1h2byewy	2023-02-13 17:14:00
[Device]HarddiskVolume3\Windows\System32\OpenWith.exe	2023-02-13 17:56:52
[Device]HarddiskVolume3\Windows\System32\Notespad.exe	2023-02-13 17:56:52
[Device]HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell_ie.exe	2023-02-13 17:24:16
[Device]HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2023-02-13 17:56:52
[Device]HarddiskVolume3\Windows\System32\cmd.exe	2023-02-13 17:28:30

Total rows: 13

Type viewer Value name: Version
Value type: RegDword
Value: 1
Raw value: 01-00-00

Key: ControlSet001\Services\bam\UserSettings\S-1-5-21-1058341133-2092417715-4019509128-1000
Selected hive: SYSTEM Last write: 2/13/2023 5:56:58 PM +00:00 15 of 15 values shown (100.00%)

- These programs ran until the shutdown of the system.

Program	Execution Time
Microsoft.Windows.SeeHealHUI_cw5n1h2byewy	2023-02-13 17:14:00
windows.immersivecontrolpanel_cw5n1h2byewy	2023-02-13 17:14:04
Microsoft.WindowsStore_swkeyb3dbbwe	2023-02-13 17:20:29
[Device]HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell_ie.exe	2023-02-13 17:24:16
[Device]HarddiskVolume3\Windows\System32\cmd.exe	2023-02-13 17:28:30
[Device]HarddiskVolume3\Windows\System32\OpenWith.exe	2023-02-13 17:56:52
[Device]HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2023-02-13 17:56:52
[Device]HarddiskVolume3\Windows\System32\Notespad.exe	2023-02-13 17:56:52
Microsoft.Windows.Cortana_cw5n1h2byewy	2023-02-13 17:56:58
Microsoft.MicrosoftEdge_swkeyb3dbbwe	2023-02-13 17:56:58
Microsoft.Windows.ShellExperienceHost_cw5n1h2byewy	2023-02-13 17:56:58

Total rows: 13

Type viewer Value name: Version
Value type: RegDword
Value: 1
Raw value: 01-00-00

Key: ControlSet001\Services\bam\UserSettings\S-1-5-21-1058341133-2092417715-4019509128-1000
Selected hive: SYSTEM Last write: 2/13/2023 5:56:58 PM +00:00 15 of 15 values shown (100.00%)

- You can use the .txt files too, it is easier to view or copy and paste.

```

C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad+ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SYSTEM.txt [ SOFTWARE.txt ] [ SECURITY.txt ] [ DEFAULT.txt ] [ NTUSER.DAT ] [ MISC.txt ] [ C:\Cases\Analysis\Registry\SYSTEM.dat ]
457 Mount Manager : \System Volume Information\MountPointManagerRemoteDatabase
458 FVE Log : \System Volume Information\FVE_{c9ca54a3-6933-4e67-8684-a7e5e23499e3}
459 FVE_Wipe : \System Volume Information\FVE_{fef82dfa-1239-4a30-83e6-3b3e9e98fe08}
460 VSS Default Provider : \System Volume Information\{3080876B-C176-4e48-B7AF-04046E6CC752} /a
461 VSS Service DB : \System Volume Information\FVE2_{f9ca84a3-6933-4e67-8684-a7e5e23499e3}
462 FVE2 Log : \System Volume Information\FVE2_{f9ca84a3-6933-4e67-8684-a7e5e23499e3}
463 FVE2_Wipe : \System Volume Information\FVE2_{fef82dfa-1239-4a30-83e6-3b3e9e98fe08}
464 FVE2_Wipe : \System Volume Information\FVE2_{fef82dfa-1239-4a30-83e6-3b3e9e98fe08}
465 VSS Service Alternate DB : \System Volume Information\{7cc467ef-6865-4831-833f-2a4917fd1bca} /ALT
466 FVE_Control : \System Volume Information\FVE2_{f9ca84a3-6933-4e67-8684-a7e5e23499e3}
467 FVE2_Control : \System Volume Information\FVE2_{f9ca84a3-6933-4e67-8684-a7e5e23499e3}
468 FVE2_Wipek : \System Volume Information\FVE2_{fef82dfa-1239-4a30-83e6-3b3e9e98fe08}.
469 MS Distributed Transaction Coordinator : C:\Windows\system32\MSDtc\MSDTC.LOG C:\Windows\system32\MSDtc\trace\dtctrace.log
470
471 KeysNotToRestore Key
472 ControlSet001\Control\BackupRestore\KeysNotToRestore
473 LastWrite Time 2018-04-11 23:38:52
474
475 Specifies the names of the registry subkeys and values that backup applications should ignore.
476
477 Mount Manager : MountedDevices
478 MS Distributed Transaction Coordinator : CurrentControlSet\Control\MSDTC\MSDTC
479 Session Manager : CurrentControlSet\Control\Session Manager\AllowForceLogonNames
480 Pending Rename Operations : CurrentControlSet\Control\Session Manager\PendingFileRename
481 Pending Rename Operations2 : CurrentControlSet\Control\Session Manager\PendingFileRename
482
483 -----
484 bam v.20200427
485 (System) Parse files from System hive BAM Services
486
487 ControlSet001\Services\bam\State\UserSettings not found.
488
489 bthenum v.20200515
490 (System) Get BTHENUM subkey info
491
492 ControlSet001\Enum\BTHENUM not found.
493
494 bthport v.20200517
495 (System) Gets Bluetooth-connected devices from System hive
496
497 ControlSet001\services\BTHPORT\Parameters\Devices not found.
498
499 ControlSet001\services\BTHPORT\Parameters\Radio Support not found.
500
501 codepage v.20200519
502 (system) Checks codepage value
503
504 CodePage key LastWrite time: 2018-04-12 09:15:54Z
505 Code page value = 1252
506
507 Code page description: https://en.wikipedia.org/wiki/Code\_page
508
509 compname v.20090727
510 (System) Gets ComputerName and Hostname values from System hive
511
512 ComputerName = MSEDEGEWIN10
513 TCP/IP Hostname = MSEDEGEWIN10

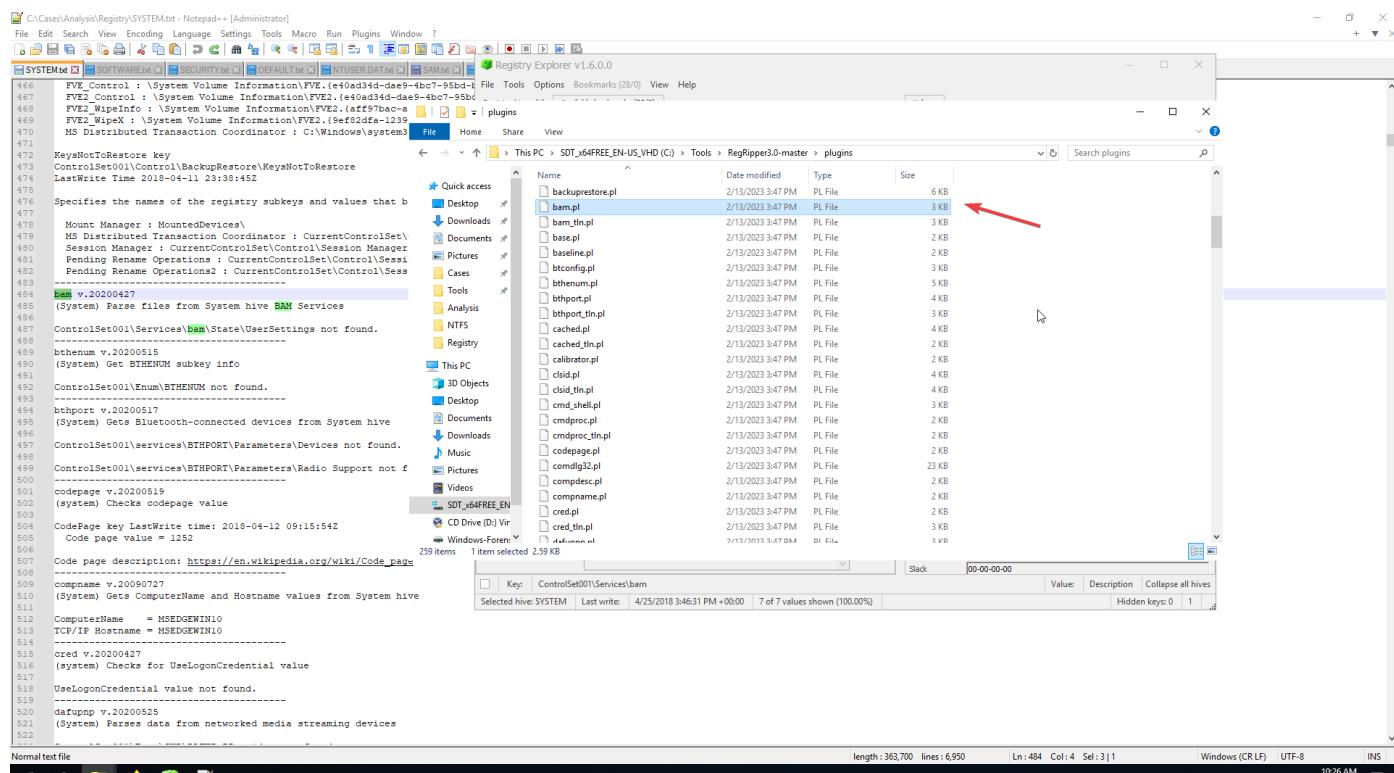
```

- In this case you can see that there is no output, that is why because the regripper plugin does not look where it should:

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Recd...
RegSz	@%Syst...	00-00-00			
Displayname	RegSz	@%Syst...	00-00-00		
ErrorControl	RegWord	1			
ImagePath	RegExpandSZ	system32	00-00		
Start	RegWord	1			
Type	RegWord	1			
WOW64	RegWord	32			

Selected hive: SYSTEM | Last write: 4/25/2018 3:46:31 PM +00:00 | 7 of 7 values shown (100.00%)

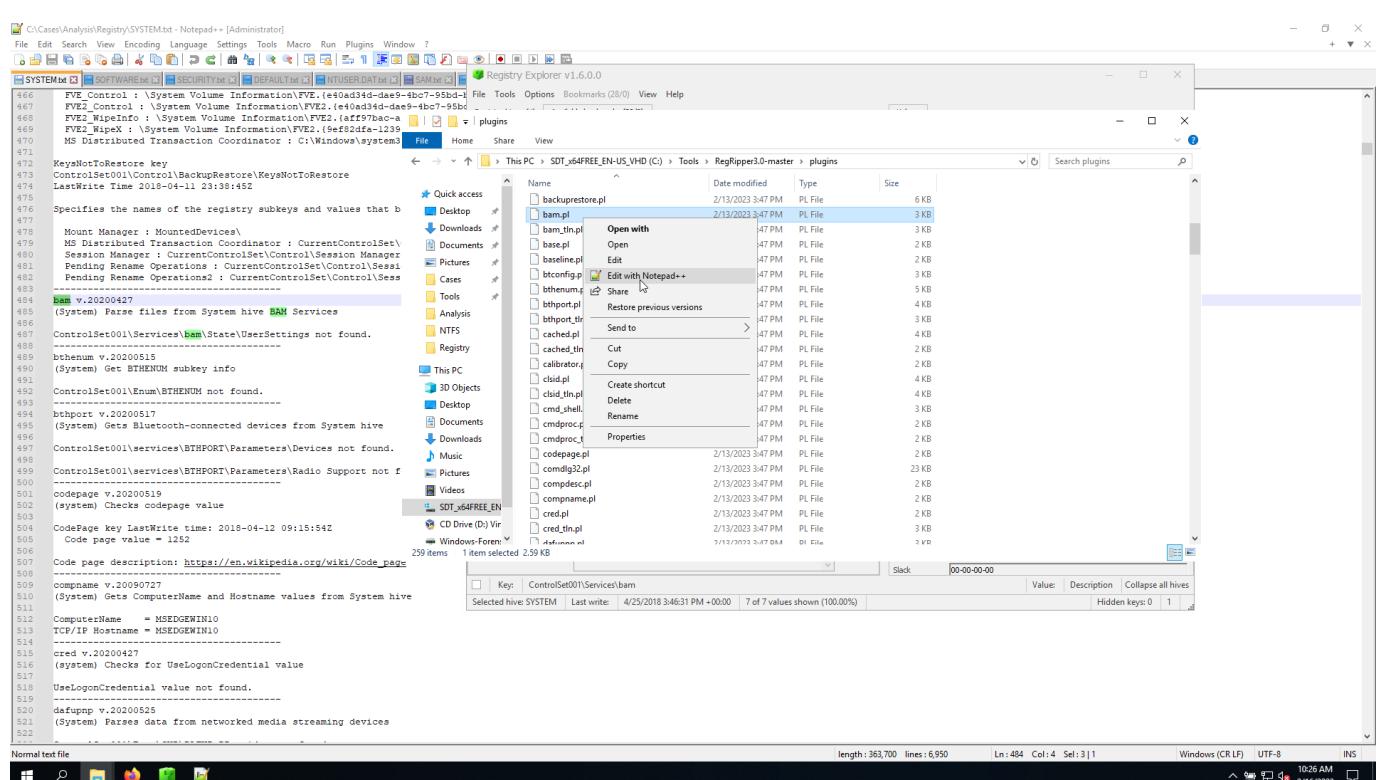
- We delete the SYSTEM.txt , change the path of the plugin to search for and redo the regripper cmd script to parse the SYSTEM.



```

466 FVE_Control : \System\Volume\Information\FVE.(e40ad34d-dae9-4bc7-5bd1-File Tools Options Bookmarks (28/0) View Help
467 FVE2_Control : \System\Volume\Information\FVE2.(e40ad34d-dae9-4bc7-5bd1-File Tools Options Bookmarks (28/0) View Help
468 FVE2_WipeInfo : \System\Volume\Information\FVE2.(aff979ac-a
469 FVE2_WipeX : \System\Volume\Information\FVE2.(9ef22dfa-1239-MS Distributed Transaction Coordinator : C:\Windows\system32
470
471 KeysNotToRestore Key
472 ControlSet001\Control\BackupRestore\KeysNotToRestore
473 LastWrite Time: 2018-04-11 23:38:45Z
474
475 Specifies the names of the registry subkeys and values that b
476
477 Mount Manager : MountedDevices\MS Distributed Transaction Coordinator : CurrentControlSet\Control\Session Manager Pending Rename Operations : CurrentControlSet\Control\Session Manager Pending Rename Operations2 : CurrentControlSet\Control\Session Manager
478
479 ControlSet001\Services\bam.State\UserSettings not found.
480
481 bthenum.v.20200515
482 (System) Get BTHENUM subkey info
483
484 ControlSet001\Enum\BTHENUM not found.
485
486 bthport.v.20200517
487 (System) Gets Bluetooth-connected devices from System hive
488
489 ControlSet001\services\BTHPORT\Parameters\Devices not found.
490
491 ControlSet001\services\BTHPORT\Parameters\Radio Support not f
492
493 codepage.v.20200519
494 (system) Checks codepage value
495
496 CodePage key LastWrite time: 2018-04-12 09:15:54Z
497 Code page value = 1252
498
499 Code page description: https://en.wikipedia.org/wiki/Code_Page
500
501 compname.v.20090727
502 (System) Gets ComputerName and Hostname values from System hive
503
504 ComputerName = MSEDEWIN10
505 TCP/IP Hostname = MSEDEWIN10
506
507 cred.v.20200427
508 (system) Checks for UseLogonCredential value
509 UseLogonCredential value not found.
510
511 datfump.v.20200525
512 (System) Parses data from networked media streaming devices
513
514
515
516
517
518
519
520
521
522

```



```

length: 363,700 lines: 6,950 Ln: 484 Col: 4 Sel: 3|1 Windows (CR LF) UTF-8 INS
10:26 AM 2/16/2023

```

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

Registry Explorer V1.6.0.0

Values

Value Name	Type	Data	Value Slack	Is Deleted	Data Rec...
Description	RegSz	@%Syst...	00-00-00-	<input type="checkbox"/>	<input type="checkbox"/>
DisplayName	RegSz	@%Syst...	00-00-00-	<input type="checkbox"/>	<input type="checkbox"/>
ErrorControl	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
ImagePath	RegExpandSz	system32...	00-00	<input type="checkbox"/>	<input type="checkbox"/>
Start	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
Type	RegDword	1		<input type="checkbox"/>	<input type="checkbox"/>
WOW64	RegDword	332		<input type="checkbox"/>	<input type="checkbox"/>

Bookmark information

Hive: C:\Cases\Analysis\Registry\SYSTEM

Category: Program execution

Name: BAM

Keywords: ControlSet001\Services\bam

Short description: Background Activity Monitor

Long description: BAM is a Windows service that controls activity of background applications in Windows 10 1709 and newer. It provides full path of the executable file that was run on the system and last execution timestamp.

Raw value: 40-00-25-00-53-00-79-00-73-00-74-00-65-00-60-00-52-00-6f-0

Slack: 00-00-00

Selected hive: SYSTEM Last write: 4/25/2018 3:46:31 PM +00:00 7 of 7 values shown (100.0%)

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

Per source file

```

51 # First thing to do is get the ControlSet00x marked current...this is
52 # going to be used over and over again in plugins that access the system
53 # file
54 my ($current,$ocs);
55 my $key_path = 'Select';
56 my $key;
57 if ($key = $root_key->get_subkey($key_path)) {
58   $ocs = $key->get_value("Current")->get_data();
59   my $bam_path = $ocs."\".(Services)\bam\state\userSettings";
60   my $bam;
61   if ($bam = $root_key->get_subkey($bam_path)) {
62     my @values = $bam->get_list_of_subkeys();
63     foreach my $s (@values) {
64       if (scalar($s) > 0) {
65         foreach my $k ($s) {
66           processKey($k);
67         }
68       }
69     }
70   } else {
71     ::rptMsg($bam_path." not found.");
72   }
73 } else {
74   ::rptMsg($key_path." not found.");
75 }
76 else {
77   ::rptMsg($key_path." not found.");
78 }
79
80 sub processKey {
81   my $key = shift;
82   my ($t,$count);
83   my @values = $key->get_list_of_values();
84
85   foreach (@values) {
86     $count += 1 if ($->get_type() == 3);
87   }
88
89   if (scalar(@values) > 0 && $count == 1) {
90     ::rptMsg($key->get_name());
91     foreach my $v (@values) {
92       my $name = $v->get_name();
93
94       if ($v->get_type() == 3) {
95         my ($t,$stl) = unpack("VV",substr($v->get_data(),0,8));
96         $t = ::getTime($t,$stl);
97         ::rptMsg(" ".$->getDateFromEpoch($t)."Z" . " - ". $name);
98       }
99     }
100   }
101   ::rptMsg("");
102 }
103
104
105
106
107
1;

```

length: 2,658 lines: 107 Ln: 107 Col: 3 Pos: 2,659 Unix (LF) UTF-8 INS

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

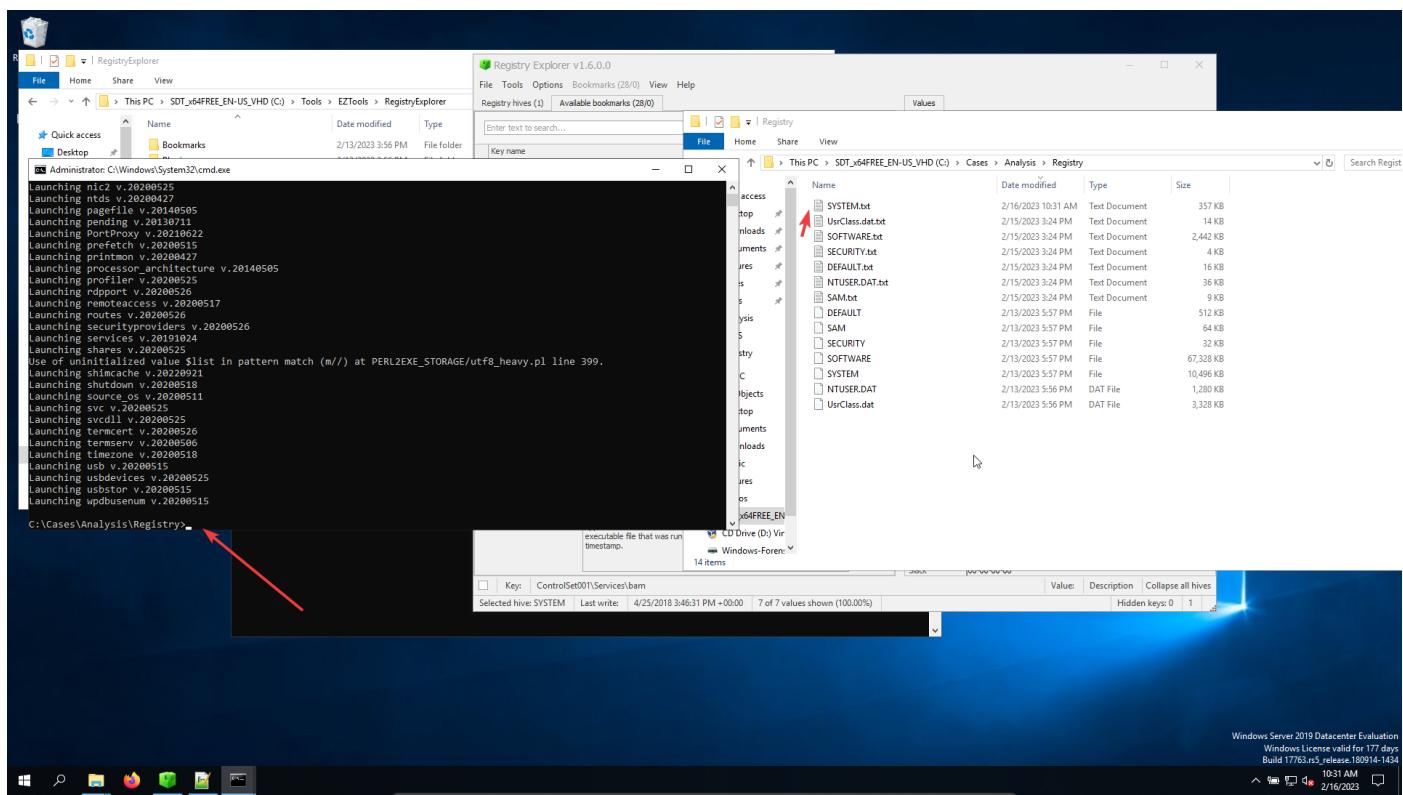
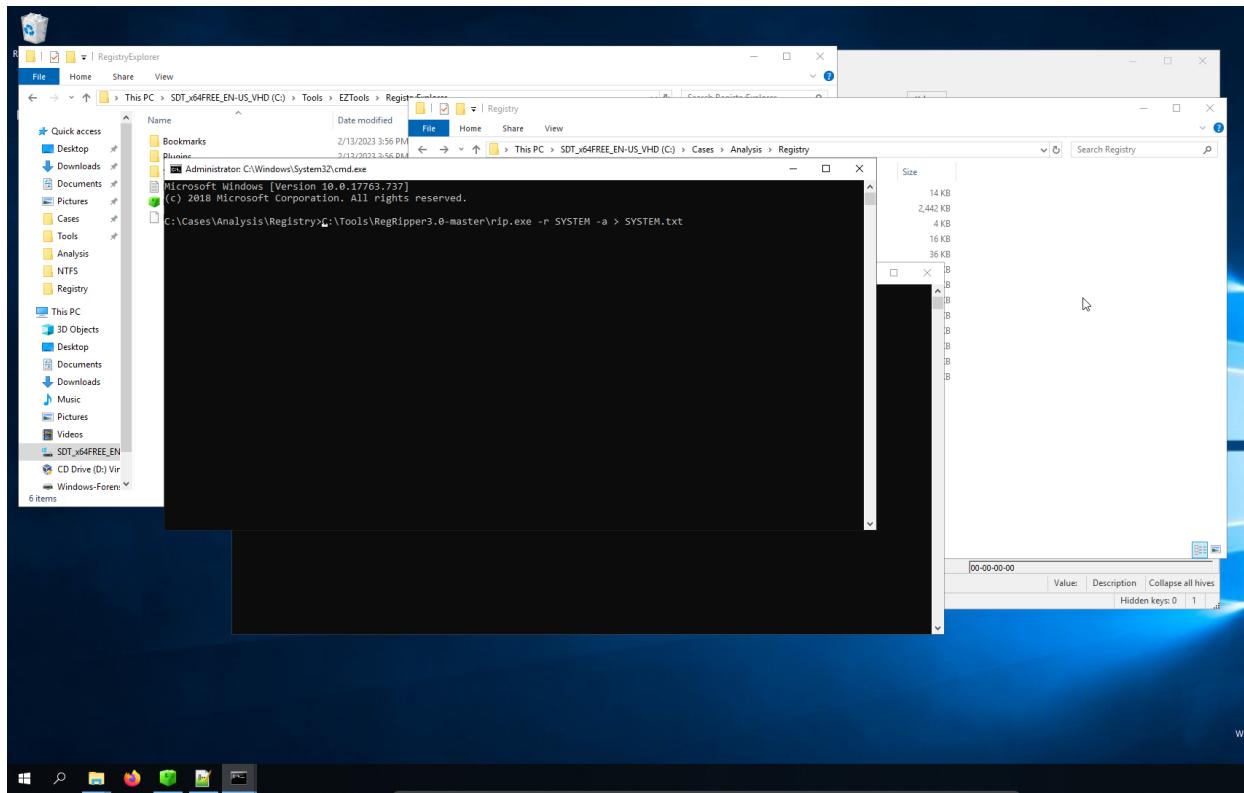
Per source file

```

51 # First thing to do is get the ControlSet00x marked current...this is
52 # going to be used over and over again in plugins that access the system
53 # file
54 my ($current,$ocs);
55 my $key_path = 'Select';
56 my $key;
57 if ($key = $root_key->get_subkey($key_path)) {
58   $ocs = $key->get_value("Current")->get_data();
59   my $bam_path = $ocs."\".(Services)\bam\state\userSettings";
60   my $bam;
61   if ($bam = $root_key->get_subkey($bam_path)) {
62     my @values = $bam->get_list_of_subkeys();
63     foreach my $s (@values) {
64       if (scalar($s) > 0) {
65         foreach my $k ($s) {
66           processKey($k);
67         }
68       }
69     }
70   } else {
71     ::rptMsg($bam_path." not found.");
72   }
73 } else {
74   ::rptMsg($key_path." not found.");
75 }
76 else {
77   ::rptMsg($key_path." not found.");
78 }
79
80 sub processKey {
81   my $key = shift;
82   my ($t,$count);
83   my @values = $key->get_list_of_values();
84
85   foreach (@values) {
86     $count += 1 if ($->get_type() == 3);
87   }
88
89   if (scalar(@values) > 0 && $count == 1) {
90     ::rptMsg($key->get_name());
91     foreach my $v (@values) {
92       my $name = $v->get_name();
93
94       if ($v->get_type() == 3) {
95         my ($t,$stl) = unpack("VV",substr($v->get_data(),0,8));
96         $t = ::getTime($t,$stl);
97         ::rptMsg(" ".$->getDateFromEpoch($t)."Z" . " - ". $name);
98       }
99     }
100   }
101   ::rptMsg("");
102 }
103
104
105
106
107
1;

```

length: 2,651 lines: 107 Ln: 60 Col: 45 Pos: 1,820 Unix (LF) UTF-8 INS



- Search for bam again, you should see the text now showing:

C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad+ [Administrator]

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

Software\Microsoft\Windows\CurrentVersion\Run

Security\SYSTEM

Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\BackupRestore

System\SYSTEM

```
457 Mount Manager : \System Volume Information\WormPointManagerRemoteDatabases
458 FVE_Log : \System Volume Information\FVE_{fc9ca5a3-6933-4ab7-8694-a7e5e23499e3}
459 FVE_Wipe : \System Volume Information\FVE_{fef52d2fa-1239-a430-83e-3b3e9b8fed08}
460 VSS Service Provider : \System Volume Information\{38088768-C176-4eb8-B7AE-04406ECC752} / s
461 VSS Service DB : \System Volume Information\{7cc4d7ef-68d5-4831-853f-2a4017fdbca1DB
462 FVE2_Log : \System Volume Information\FVE2_{f9a034d4-6439-4363-8684-7e67a58588}
463 FVE2_Wipe : \System Volume Information\FVE2_{c4ed60aa-e0a9-4733-860a-9e94922d2}
464 FVE2_Wipe : \System Volume Information\FVE2_{fef52d2fa-1239-a430-83e-3b3e9b8fed08}
465 VSS Service Alternate DB : \System Volume Information\{7cc067ef-68d5-4931-853f-2a4817fdbca1ALT
466 FVE_Control : \System Volume Information\{V.E.(e04ad3d4-dae5-4bc7-95bd-b16218c10f72).*
467 FVE2_Control : \System Volume Information\FVE2_{(e104ad3d4-dae5-4bc7-95bd-b16218c10f72).*
468 FVE2_Wipe : \System Volume Information\{FVE2_{f9a034d4-6439-4363-8684-7e67a58588}.*
469 FVE2_Wipe : \System Volume Information\{FVE2_{c4ed60aa-e0a9-4733-860a-9e94922d2}.*
470 MS Distributed Transaction Coordinator : C:\Windows\system32\MSDtc\MSDtc.LOG C:\Windows\system32\trace\dtctrace.log
471
472 KeysNotToRestore key
473 ControlSet001\Control\BackupRestore\KeysNotToRestore
474 LastWrite Time 2014-04-11 23:38:45Z
475
476 Specifies the names of the registry subkeys and values that backup applications should
477
478 Mount Manager : MountedDevices\*
479 MS Distributed Transaction Coordinator : CurrentControlSet\Control\MSDTC\MSDTC
480 Session Manager : CurrentControlSet\Control\Session Manager\AllowProtocolRenames
481 Pending Rename Operations : CurrentControlSet\Control\Session Manager\PendingFile
482 Pending Rename Operations2 : CurrentControlSet\Control\Session Manager\PendingFile
483
484 Ban v.20200427
485
486 (System) Parse files from System hive BAN Services
487
488 S-1-5-21-1058341133-2092417115-4019509128-1000
489 2023-02-13 17:56:58Z - Microsoft.Windows.ShellExperienceHost_cw5nh2txyewy
490 2023-02-13 17:56:58Z - Microsoft.Windows.Cortana_cw5nh2txyewy
491 2023-02-13 17:56:58Z - Microsoft.Windows.Controls_cw5nh2txyewy
492 2023-02-13 17:56:58Z - Microsoft.Windows.Devices.HarddiskVolume3\Windows\System32\ApplicationFrameHost_cw5nh2txyewy
493 2023-02-13 17:56:58Z - {Device\HarddiskVolume3\Windows\System32\explorer.exe}
494 2023-02-13 17:14:04Z - windows.immersivecontrolpanel_cw5nh2txyewy
495 2023-02-13 17:14:00Z - Microsoft.Windows.SecHealthUI_cw5nh2txyewy
496 2023-02-13 17:56:58Z - Microsoft.Windows.SystemUI_cw5nh2txyewy
497 2023-02-13 17:56:58Z - {Device\HarddiskVolume3\Windows\System32\OpenWith\ex
498 2023-02-13 17:24:16Z - {Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe
499 2023-02-13 17:56:52Z - {Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
500 2023-02-13 17:28:30Z - {Device\HarddiskVolume3\Windows\System32\cmd.exe
501
502 S-1-5-21-1058341133-2092417115-4019509128-1001
503 2018-04-25 15:48:26Z - Microsoft.Windows.CloudExperienceHost_cw5nh2txyewy
504
505 S-1-5-90-0-1
506 2023-02-13 17:11:42Z - {Device\HarddiskVolume3\Windows\System32\dum.exe
507
508
509 Bohemian V.20200515
510 [System] Get BTHENUM subkey info
511
512 ControlSet001\Enum\BTHENUM not found.
513
```

Normal text file

length: 364,933 lines: 6,970 Ln: 484 Col: 4 Sel: 3 | 1 Windows (CR LF) UTF-8

10:31 AM 2/16/2023

- What executables did BAM recorded for the user IEUser?
Print execution date and time.

S-1-5-21-1058341133-2092417715-4019509128-1000 – This is IEUser

2023-02-13 17:24:16Z -

\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell_ise.exe

2023-02-13 17:28:30Z - \Device\HarddiskVolume3\Windows\System32\cmd.exe

2023-02-13 17:56:52Z -

\Device\HarddiskVolume3\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

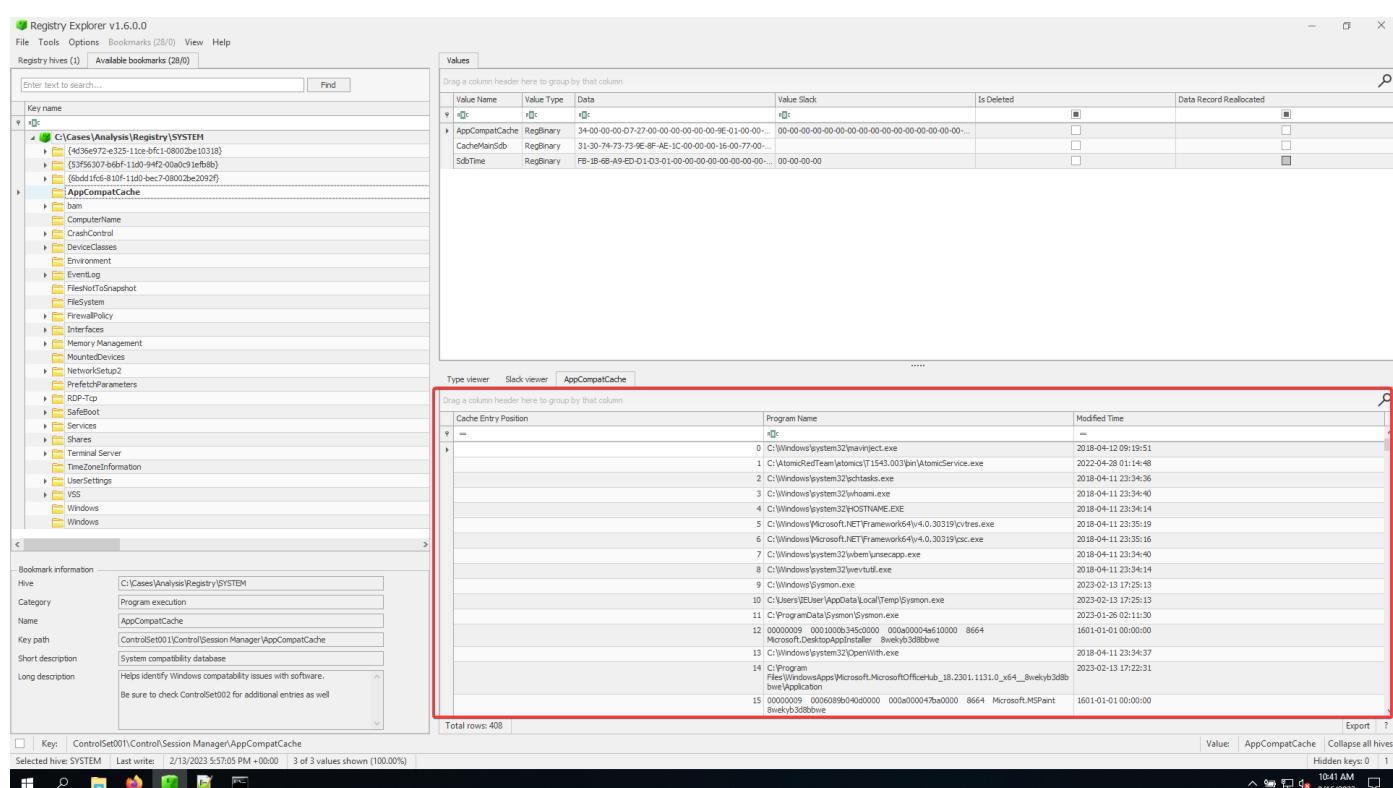
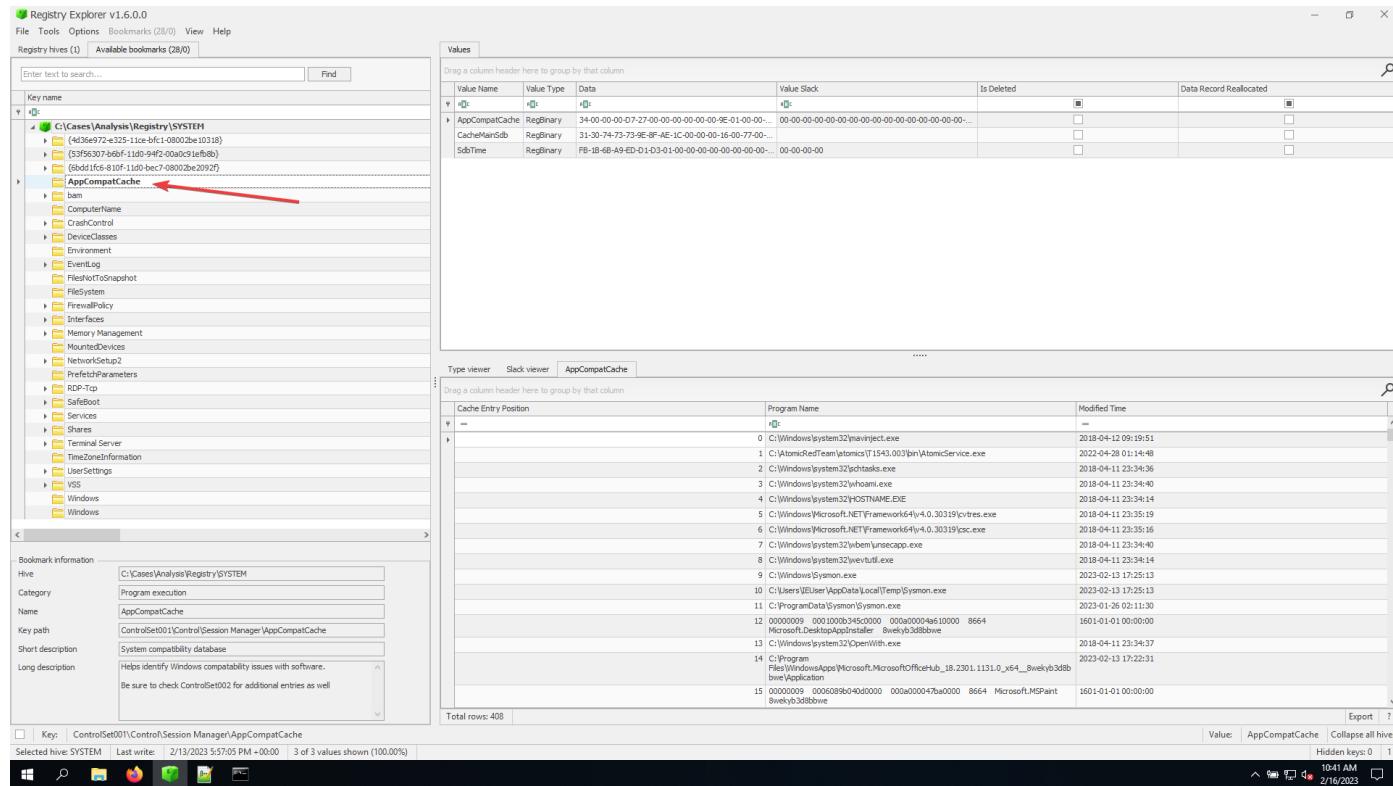
2023-02-13 17:56:58Z - \Device\HarddiskVolume3\Windows\System32\ApplicationFrameHost.exe

2023-02-13 17:56:52Z - \Device\HarddiskVolume3\Windows\System32\OpenWith.exe

2023-02-13 17:56:52Z - \Device\HarddiskVolume3\Windows\System32\notepad.exe

Application Compatibility Cache (ShimCache)

- You can find information related to ShimCache at:
 - o HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache
- The windows os stores information about application compatibility ofr backward compatibility reason, with all the programs . Remembers file metadata of executables and checks if it is backward compatible, if not , windows will load alternative code, for compatibility reasons
- This registry is written upon system shutdown
- Open registry explorer:



- Cache Entry Position shows the order of program execution.
 - We can use different tools to get the same information in different formats.

```

C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad+ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Software.hlp SECURITY.MSC DEFAULT.DAT SAM.BAK UserClass.dat BAK.ppt SYSTEM.txt

1 scanbutton v.20131120
2 (System) Get Scan Button information
3 GUID = {AEC5A715-8C6E-11D2-977A-0000F87A926F} []
4 LaunchApplications
5 =====
6 appcertdilis v.20200427
7 ControlSet001\Control\Session Manager\{AppCertDlIs not found.
8 =====
9 appcompatcache v.20220921
10 (System) Parse files from System hive AppCompatCache
11 =====
12 ControlSet001\Control\Session Manager\{AppCompatCache
13 LastWrite Time: 2023-02-13 17:17:05Z
14 Signature: 0x34
15 =====
16 00000009 00e000077f00000 00a0000273a0000 8664 Microsoft.VCLibs.140.00.Swekyb3dbbbwe
17 00000009 00100006b10000 00a000027410000 8664 Microsoft.NET.Native.Framework.1.6 Swekyb3dbbbwe
18 C:\Program Files\WindowsApps\Microsoft.WindowsStore_1712.1001.0_x64_Swekyb3dbbbwe\Application_2018-04-25_15:47:21
19 C:\Windows\SystemApps\Microsoft.BrokerPlugin_cw5nh1hxtwyewy\{AppCertDlIs not found.
20 00000009 000200026cb0000 00a000042940000 8664 Windows.CBSPreview_cw5nh1hxtwyewy
21 00000009 000200026cb0000 00a000027410000 8664 Microsoft.NET.Native.Run Find Replace Find in Files Find in Projects Mark End what: appcompatcache Find Next Count In selection Find All in Current Document Find All in All Opened Documents Close Transparency Normal Extended (N, Y, V, W...) Always Regular expression matches newline
22 00000009 000709a03a9e0000 00a000047b0000 8664 Microsoft.UI.Xaml.2.7
23 00000009 00100205abf0000 00a000027410000 8664 Microsoft.NET.Native.Fr
24 00000009 000200026cb0000 00a000042940000 8664 Microsoft.SkypeApp_kzf
25 C:\Windows\system32\msmbuild.exe 2018-04-11 23:34:25
26 00000009 00120002d046b0000 00a00004610000 8664 Microsoft.MicrosoftOffice
27 0744e990fa0000 00a00004bcb0000 8664 Microsoft.Windows.Photos
28 C:\Users\lEUZER\AppData\Local\Microsoft\OneDrive\23.007.0109.0004\FileCoAuth.exe 20
29 SIGN.MEDIA-1FC5C49 Bginfo.exe 2018-02-08 18:19:24
30 C:\Windows\system32\cmd.exe 2018-04-11 23:34:40
31 00000009 000200026cb0000 00a000042940000 8664 c5e2524a-ea46-4f67-814f-000000000000
32 C:\Program Files\WindowsApps\Microsoft.XboxApp_49.85200.1.0_x64_Swekyb3dbbbwe\Appl
33 00000009 0003002655f10000 00a00003d7000 8664 Microsoft.Messaging_Week
34 C:\Windows\system32\find.exe 2018-04-11 23:34:20
35 C:\Windows\system32\SearchHealthService.exe 2018-04-11 23:34:40
36 C:\Program Files\WindowsApps\Microsoft.ShellExperienceHost_begeyn.exe 2018-01-14 02:36:55
37 C:\Windows\system32\SecurityHealthService.exe 2018-04-11 23:34:41
38 C:\Program Files\Oracle\VirtualBox Guest Additions\vBoxOvfUtil.exe 2023-01-11 14:39:36
39 C:\ProgramData\Microsoft\Windows Defender\platform\4.14.17613.18039\0\Nshpng.exe 2
40 00000009 000a038300020000 00a000094eb0000 8664 Microsoft.WindowsMaps
41 00000009 000100026cb0000 00a00003d7000 8664 Microsoft.GetStarted Swekyb3dbbbwe
42 C:\ProgramData\Microsoft\Windows\Defender\platform\4.14.17613.18039\0\Nshpng.exe 2023-01-26 02:11:29
43 2d00000009 000100026cb0000 00a00003f3ab0000 8664 Microsoft.WindowsStore Swekyb3dbbbwe
44 00000009 0006000200000000 00a00003fb0000 8664 Windows.PrintDialog_cw5nh1hxtwyewy neutral
45 C:\Users\lEUZER\AppData\Local\Microsoft\OneDrive\23.007.0109.0004\FileSyncConfig.exe 2023-02-13 17:08:35
46 00000009 00100205abf0000 00a000027410000 8664 Microsoft.NET.Native.Runtime.1.7 Swekyb3dbbbwe
47 00000009 000200026cb0000 00a000042940000 8664 Microsoft.Windows.ShellExperienceHost_cw5nh1hxtwyewy neutral
48 c:\windows\system32\taskhostw.exe 2018-04-11 23:34:37
49 C:\Program Files\WindowsApps\Microsoft.OneConnect_5.2204.1031.0_x64_Swekyb3dbbbwe\Application 2023-02-13 17:20:39
50 00000009 00100205abf0000 00a00003f3ab0000 8664 Microsoft.FeedbackHub Swekyb3dbbbwe
51 00000009 0001000763b0000 00a000027410000 8664 Microsoft.NET.Native.Runtime.1.7 Swekyb3dbbbwe
52 00000009 000200026cb0000 00a000042940000 8664 Microsoft.Advertising.Xaml Swekyb3dbbbwe
53 03e842ee00100000 00a000028000000 8664 Microsoft.Windows.Advertising
54 00000009 000200028000000 00a000028000000 8664 Microsoft.Services.Store.Engagement Swekyb3dbbbwe
55 C:\Program Files\Oracle\VirtualBox Guest Additions\vBoxOvfInst.exe 2023-01-11 14:39:36
56 00000009 000a0383001c0000 00a000045630000 8664 Microsoft.WindowsAlarms Swekyb3dbbbwe
57 C:\Windows\SoftwareDistribution\Download\Install1\AM_Base.exe 2023-02-13 17:06:58

```

- We will use AppCompatCacheParser:

```

C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad+ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
Software.hlp SECURITY.MSC DEFAULT.DAT SAM.BAK UserClass.dat BAK.ppt SYSTEM.txt

4 GUID = {AEC5A715-8C6E-11D2-977A-0000F87A926F} []
5 LaunchApplications
6 =====
7 appcertdilis v.20200427
8 ControlSet001\Control\Session Manager\{AppCertDlIs not found.
9 =====
10 appcompatcache v.20220921
11 (System) Parse files from System hive AppCompatCache
12 =====
13 ControlSet001\Control\Session Manager\{AppCompatCache
14 LastWrite Time: 2023-02-13 17:17:05Z
15 Signature: 0x34
16 =====
17 00000009 0001000277f00000 00a0000273a0000 8664 Microsoft.VCLibs.140.00.Swekyb3dbbbwe
18 00000009 00100006b10000 00a000027410000 8664 Microsoft.NET.Native.Framework.1.6 Swekyb3dbbbwe
19 C:\Program Files\WindowsApps\Microsoft.WindowsStore_1712.1001.0_x64_Swekyb3dbbbwe\Application 2018-04-25_15:47:21
20 00000009 000200026cb0000 00a000042940000 8664 Windows.CBSPreview_cw5nh1hxtwyewy neutral
21 00000009 000200026cb0000 00a000027410000 8664 Microsoft.NET.Native.Run Find Replace Find in Files Find in Projects Mark End what: appcompatcache Find Next Count In selection Find All in Current Document Find All in All Opened Documents Close Transparency Normal Extended (N, Y, V, W...) Always Regular expression matches newline
22 00000009 000709a03a9e0000 00a000047b0000 8664 Microsoft.UI.Xaml.2.7
23 00000009 00100205abf0000 00a000027410000 8664 Microsoft.NET.Native.Fr
24 00000009 000200026cb0000 00a000042940000 8664 Microsoft.SkypeApp_kzf
25 C:\Windows\system32\msmbuild.exe 2018-04-11 23:34:25
26 00000009 00120002d046b0000 00a00004610000 8664 Microsoft.MicrosoftOffice
27 0744e990fa0000 00a00004bcb0000 8664 Microsoft.Windows.Photos Swekyb3dbbbwe
28 C:\Users\lEUZER\AppData\Local\Microsoft\OneDrive\23.007.0109.0004\FileCoAuth.exe 20
29 SIGN.MEDIA-1FC5C49 Bginfo.exe 2018-02-08 18:19:24
30 C:\Windows\system32\chmapp.exe 2018-04-11 23:34:36
31 00000009 000200026cb0000 00a000042940000 8664 c5e2524a-ea46-4f67-814f-000000000000
32 C:\Program Files\WindowsApps\Microsoft.XboxApp_49.85200.1.0_x64_Swekyb3dbbbwe\Application 2023-02-13 17:17:05Z
33 00000009 0003002655f10000 00a00003d7000 8664 Microsoft.Messaging_Week
34 C:\Windows\system32\find.exe 2018-04-11 23:34:20
35 C:\Windows\system32\SearchHealthService.exe 2018-04-11 23:34:40
36 C:\Program Files\WindowsApps\Microsoft.ShellExperienceHost_begeyn.exe 2018-01-14 02:36:55
37 C:\Windows\system32\SeamlessHealthService.exe 2018-04-11 23:34:41
38 C:\Program Files\WindowsApps\Microsoft.WindowsStore_1712.1001.0_x64_Swekyb3dbbbwe\{AppCertDlIs not found.
39 C:\ProgramData\Microsoft\Windows Defender\platform\4.14.17613.18039\0\Nshpng.exe 2023-01-11 14:39:36
40 00000009 00060002f313b0000 00a000042940000 8664 Microsoft.WindowsMaps Swekyb3dbbbwe
41 00000009 00060002f313b0000 00a000042940000 8664 Microsoft.GetStarted Swekyb3dbbbwe
42 C:\ProgramData\Microsoft\Windows\Defender\platform\4.14.17613.18039\0\Nshpng.exe 2023-01-26 02:11:29
43 2d00000009 0003e90170000 00a00003f3ab0000 8664 Microsoft.WindowsStore Swekyb3dbbbwe
44 00000009 000200026cb0000 00a000042940000 8664 Microsoft.FeedbackHub Swekyb3dbbbwe
45 C:\Users\lEUZER\AppData\Local\Microsoft\OneDrive\23.007.0109.0004\FileSyncConfig.exe 2023-02-13 17:08:35
46 00000009 0010000763b0000 00a000027410000 8664 Microsoft.NET.Native.Runtime.1.7 Swekyb3dbbbwe
47 00000009 000200026cb0000 00a000042940000 8664 Microsoft.Windows.ShellExperienceHost_cw5nh1hxtwyewy neutral
48 c:\windows\system32\taskhostw.exe 2018-04-11 23:34:37
49 C:\Program Files\WindowsApps\Microsoft.OneConnect_5.2204.1031.0_x64_Swekyb3dbbbwe\Application 2023-02-13 17:20:39
50 00000009 00100205abf0000 00a00003f3ab0000 8664 Microsoft.FeedbackHub Swekyb3dbbbwe
51 00000009 0001000763b0000 00a000027410000 8664 Microsoft.NET.Native.Runtime.1.7 Swekyb3dbbbwe
52 00000009 000200026cb0000 00a000042940000 8664 Microsoft.Advertising.Xaml Swekyb3dbbbwe
53 03e842ee00100000 00a000028000000 8664 Microsoft.Windows.Advertising
54 00000009 000200028000000 00a000028000000 8664 Microsoft.Services.Store.Engagement Swekyb3dbbbwe
55 C:\Program Files\Oracle\VirtualBox Guest Additions\vBoxOvfInst.exe 2023-01-11 14:39:36
56 00000009 000a0383001c0000 00a000045630000 8664 Microsoft.WindowsAlarms Swekyb3dbbbwe
57 C:\Windows\SoftwareDistribution\Download\Install1\AM_Base.exe 2023-02-13 17:06:58

```

- Use it in the cmd:

```
GUID = {AEC5A715-8C6E-11D2-977A-0000F87A926F} []
LaunchApplications =
-----
appcertd1s v.20200427
ControlSet001\Control\Session Manager\AppCertDlIs not found.

appcompatcache V.20220921
(System) Parse files from System hive AppCompatCache
ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: 2023-02-13 17:57:05Z
Signature: 0x34
00000009 00000007#00000 000a000273a0000 8664 Microsoft.VCLibs.140.00_Swekyb3d8bbwe
Administrator: C:\Windows\System32\cmd.exe
https://github.com/EricZimmerman/AppCompatCacheParser
Examples: AppCompatCacheParser.exe --csv c:\temp -t -2
AppCompatCacheParser.exe --csv c:\temp --csvf results.csv
Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
Usage:
AppCompatCacheParser [options]
Options:
-f <path> Full path to SYSTEM hive to process. If this option is not specified, the live Registry will be used
--csv <csv> (REQUIRED) Directory to save CSV Formatted results to. Be sure to include the full path in double quotes
--csvf <csvf> File name to save CSV Formatted results to. When present, overrides default name
--c <> The ControlSet to parse. Default is to extract all control sets [default: -1]
-t Sorts last modified timestamps in descending order [default: False]
--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]
--nl When true, ignore transaction log files for dirty hives [default: False]
--debug Show debug information during processing [default: False]
--trace Show trace information during processing [default: False]
--version Show version information
-?, -h, --help Show help and usage information
C:\Tools\EZTools>AppCompatCacheParser.exe -f C:\cases\Analysis\Registry\SYSTEM --csv C:\Cases\Analysis\Execution
C:\Program Files\WindowsApps\Microsoft.OneConnect_5.2204.1031_0_x64\OneConnect3d8bbwe\Application 2023-02-13 17:20:39
00000009 00010002640000 000a00003fab0000 8664 Microsoft.WindowsFeedbackHub_Swekyb3d8bbwe
00000009 0001000763bb0000 000a000027410000 8664 Microsoft.NET.Native.Runtime.1.7_Swekyb3d8bbwe
00000009 000a000049000000 000a000028000000 8664 Microsoft.Advertising.Xaml_Swekyb3d8bbwe
00000009 03e842ee00100000 000a000000000000 8664 Microsoft.Windows.AppPrep.ChxApp_cw5nlh2txyewy_neutral
00000009 000a000042d80000 000a000028000000 8664 Microsoft.Services.Store.Engagement_Swekyb3d8bbwe
55 C:\Program Files\Oracle\VirtualBox\Guest Additions\VBoxDrvInst.exe 2023-01-11 14:39:36
00000009 000a000045300000 000a0000045630000 8664 Microsoft.WindowsAlarms_Swekyb3d8bbwe
57 C:\Windows\SoftwareDistribution\Download\Install\AM_Base.exe 2023-02-13 17:06:58
C:\Program Files\OpenSSH\bin\chmod.exe 2015-01-14 02:34:09
59 00000009 0006089b04d0000 000a000047ba0000 8664 Microsoft.MSPaint_Swekyb3d8bbwe
60 0000000b 0001000a000742ee 000a000042ee0000 8664 Microsoft.Windows.Cortana_cw5nlh2txyewy_neutral
Normal text file
```

```
GUID = {AEC5A715-8C6E-11D2-977A-0000F87A926F} []
LaunchApplications =
-----
appcertd1s v.20200427
ControlSet001\Control\Session Manager\AppCertDlIs not found.

appcompatcache V.20220921
(System) Parse files from System hive AppCompatCache
ControlSet001\Control\Session Manager\AppCompatCache
LastWrite Time: 2023-02-13 17:57:05Z
Signature: 0x34
00000009 00000007#00000 000a000273a0000 8664 Microsoft.VCLibs.140.00_Swekyb3d8bbwe
Administrator: C:\Windows\System32\cmd.exe
https://github.com/EricZimmerman/AppCompatCacheParser
Examples: AppCompatCacheParser.exe --csv c:\temp -t -2
AppCompatCacheParser.exe --csv c:\temp --csvf results.csv
Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
Usage:
AppCompatCacheParser [options]
Options:
-f <path> Full path to SYSTEM hive to process. If this option is not specified, the live Registry will be used
--csv <csv> (REQUIRED) Directory to save CSV Formatted results to. Be sure to include the full path in double quotes
--csvf <csvf> File name to save CSV Formatted results to. When present, overrides default name
--c <> The ControlSet to parse. Default is to extract all control sets [default: -1]
-t Sorts last modified timestamps in descending order [default: False]
--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]
--nl When true, ignore transaction log files for dirty hives [default: False]
--debug Show debug information during processing [default: False]
--trace Show trace information during processing [default: False]
--version Show version information
-?, -h, --help Show help and usage information
C:\Tools\EZTools>AppCompatCacheParser.exe -f C:\Cases\Analysis\Registry\SYSTEM --csv C:\Cases\Analysis\Execution
AppCompatCache Parser version 1.5.0.6
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/AppCompatCacheParser
Command line: -f C:\Cases\Analysis\Registry\SYSTEM --csv C:\Cases\Analysis\Execution
Processing hive 'C:\Cases\Analysis\Registry\SYSTEM'
Found 408 cache entries for Windows10Creators in ControlSet001
Results saved to 'C:\Cases\Analysis\Execution\20230216104756_Windows10Creators_SYSTEM_AppCompatCache.csv'
C:\Tools\EZTools>
C:\Program Files\WindowsApps\Microsoft.OneConnect_5.2204.1031_0_x64\OneConnect3d8bbwe\Application 2023-02-13 17:20:39
50 00000009 00010002640000 000a00003fab0000 8664 Microsoft.WindowsFeedbackHub_Swekyb3d8bbwe
51 00000009 0001000763bb0000 000a000027410000 8664 Microsoft.NET.Native.Runtime.1.7_Swekyb3d8bbwe
52 00000009 000a000049000000 000a000028000000 8664 Microsoft.Advertising.Xaml_Swekyb3d8bbwe
53 00000009 03e842ee00100000 000a000000000000 8664 Microsoft.Windows.AppPrep.ChxApp_cw5nlh2txyewy_neutral
54 00000009 000a000042d80000 000a000028000000 8664 Microsoft.Services.Store.Engagement_Swekyb3d8bbwe
55 C:\Program Files\Oracle\VirtualBox\Guest Additions\VBoxDrvInst.exe 2023-01-11 14:39:36
56 00000009 000a000045300000 000a0000045630000 8664 Microsoft.WindowsAlarms_Swekyb3d8bbwe
57 C:\Windows\SoftwareDistribution\Download\Install\AM_Base.exe 2023-02-13 17:06:58
58 C:\Program Files\OpenSSH\bin\chmod.exe 2015-01-14 02:34:09
59 00000009 0006089b04d0000 000a000047ba0000 8664 Microsoft.MSPaint_Swekyb3d8bbwe
60 0000000b 0001000a000742ee 000a000042ee0000 8664 Microsoft.Windows.Cortana_cw5nlh2txyewy_neutral
Normal text file
```

Execution

File Home Share View

This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Execution

Quick access

- Desktop
- Downloads
- Documents
- Pictures
- Cases
- Tools
- Analysis
- NTFS
- Registry

This PC

- 3D Objects
- Desktop
- Documents
- Downloads
- Music
- Pictures
- Videos

SDT_x64FREE_EN

CD Drive (D:) Vir

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230216104756_Windows10Creators_SYSTEM_AppCompatCache.csv

Drag a column header here to group by that column

Line	Tag	Control S...	Duplicate	Cache Entry Posi...	Executed	Last Modified	Time UTC	Path
1				0	NA	2018-04-12	09:19:51	C:\Windows\system32\mavinject.exe
2				1	NA	2022-04-28	01:14:48	C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
3				1	NA	2018-04-11	23:34:36	C:\Windows\system32\schtasks.exe
4				1	NA	2018-04-11	23:34:40	C:\Windows\system32\whoami.exe
5				1	NA	2018-04-11	23:34:14	C:\Windows\system32\HOSTNAME.EXE
6				1	NA	2018-04-11	23:35:19	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
7				1	NA	2018-04-11	23:35:16	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
8				1	NA	2018-04-11	23:34:40	C:\Windows\system32\wbem\unseccapp.exe
9				1	NA	2018-04-11	23:34:14	C:\Windows\system32\wututil.exe
10				1	NA	2023-02-13	17:25:13	C:\Windows\Sysmon.exe
11				1	NA	2023-02-13	17:25:13	C:\Users\IEUser\AppData\Local\Temp\Syomon.exe
12				1	NA	2023-01-26	02:11:30	C:\ProgramData\Syomon\Syomon.exe
13				1	NA			00000009 0001000b345c0000 000a00004a610000 8664 Microsoft.DesktopAppInstaller 8wekyb3d8bbwe
14				1	NA	2018-04-11	23:34:37	C:\Windows\system32\OpenWith.exe
15				1	NA	2023-02-13	17:22:31	C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.2301.1131.0_x64_8wekyb3d8bbwe\Application
16				1	NA			00000009 000e009b04d00000 000a000047ba0000 8664 Microsoft.MSPaint 8wekyb3d8bbwe
17				1	NA			00000009 00120ef04d6b0000 000a000047ba0000 8664 Microsoft.MicrosoftOfficeHub 8wekyb3d8bbwe
18				1	NA			00000009 000a003700000000 000a000047ba0000 8664 Microsoft.WindowsCalculator 8wekyb3d8bbwe
19				1	NA	2023-02-13	17:22:10	C:\Program Files\WindowsApps\Microsoft.WindowsFeedbackHub_1.2108.2563.0_x64_8wekyb3d8bbwe\Application
20				1	NA			00000009 0001083c0a030000 000a00004c860000 8664 Microsoft.WindowsFeedbackHub 8wekyb3d8bbwe
21				1	NA			00000009 000a003900000000 000a000045630000 8664 Microsoft.People 8wekyb3d8bbwe
22				1	NA	2023-02-13	17:09:01	C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\23.020.0125.0003\FileCoAuth.exe
23				1	NA	2023-02-13	17:21:20	C:\Program Files\WindowsApps\Microsoft.XboxGameOverlay_1.54.4001.0_x64_8wekyb3d8bbwe\Application
24				1	NA			00000009 07e038600140000 000a00004a610000 8664 Microsoft.WindowsCamera 8wekyb3d8bbwe
25				1	NA			00000009 000100360fa10000 000a000042ee0000 8664 Microsoft.XboxGameOverlay 8wekyb3d8bbwe
26				1	NA			00000009 00030007008e0000 000a000047ba0000 8664 Microsoft.MicrosoftStickyNotes 8wekyb3d8bbwe
27				1	NA			00000009 000100004ad00000 000a00004a610000 8664 Microsoft.WebMediaExtensions 8wekyb3d8bbwe
28				1	NA			00000009 000a0037001c0000 000a000045630000 8664 Microsoft.WindowsSoundRecorder 8wekyb3d8bbwe
29				1	NA			00000009 000c005fb0b90000 000a000045630000 8664 Microsoft.XboxIdentityProvider 8wekyb3d8bbwe
30				1	NA	2023-02-13	17:20:39	C:\Program Files\WindowsApps\Microsoft.OneConnect_5.2204.1031.0_x64_8wekyb3d8bbwe\Application
31				1	NA			00000009 0005089c04070000 000a0000581d0000 8664 Microsoft.OneConnect 8wekyb3d8bbwe
32				1	NA			00000009 000a003800020000 000a00004bc80000 8664 Microsoft.WindowsMaps 8wekyb3d8bbwe
33				1	NA			00000009 000100066b150000 000a000027410000 8664 Microsoft.NET.Native.Framework.1.6 8wekyb3d8bbwe

Total lines: 408 | Visible lines: 408 | Open files: 1 | 10:48 AM | 2/16/2023

- Cache entry position for:
 - AtomicService.exe - 1
 - Mavinject.exe - 0

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

Enter text to search... Find

20230216104756_Windows10Creators_SYSTEM_AppCompatCache.csv

Drag a column header here to group by that column

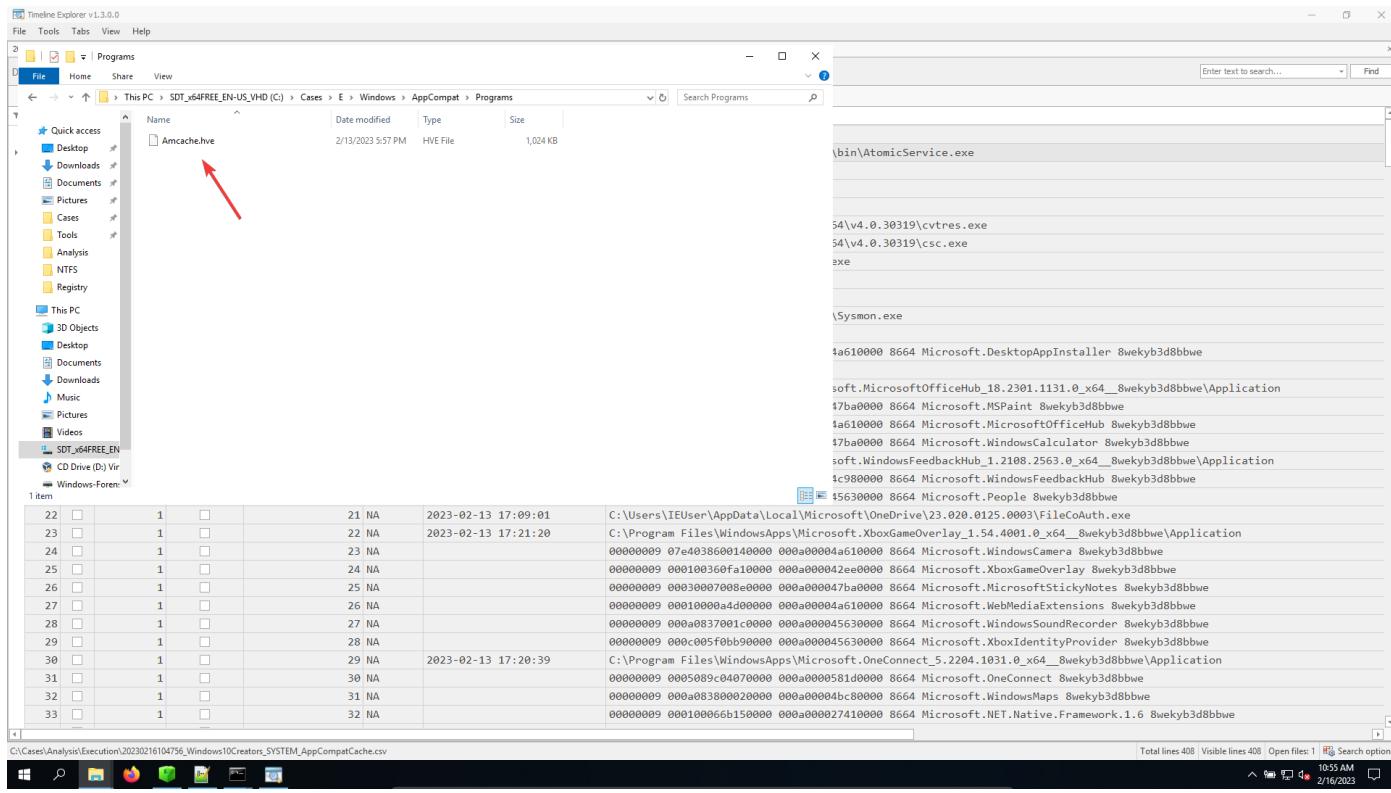
Line	Tag	Control S...	Duplicate	Cache Entry Posi...	Executed	Last Modified Time UTC	Path
1	□	1	□		0 NA	2018-04-12 09:19:51	C:\Windows\system32\mavinject.exe
2	□	1	□		1 NA	2022-04-20 01:14:48	C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
3	□	1	□		2 NA	2018-04-11 23:34:36	C:\Windows\system32\schtasks.exe
4	□	1	□		3 NA	2018-04-11 23:34:40	C:\Windows\system32\whoami.exe
5	□	1	□		4 NA	2018-04-11 23:34:14	C:\Windows\system32\HOSTNAME.EXE
6	□	1	□		5 NA	2018-04-11 23:35:19	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cvtres.exe
7	□	1	□		6 NA	2018-04-11 23:35:16	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe
8	□	1	□		7 NA	2018-04-11 23:34:40	C:\Windows\system32\wbem\unsecapp.exe
9	□	1	□		8 NA	2018-04-11 23:34:14	C:\Windows\system32\wevtutil.exe
10	□	1	□		9 NA	2023-02-13 17:25:13	C:\Windows\Systemmon.exe
11	□	1	□		10 NA	2023-02-13 17:25:13	C:\Users\IEUser\AppData\Local\Temp\Sysmon.exe
12	□	1	□		11 NA	2023-01-26 02:11:30	C:\ProgramData\Sysmon\Sysmon.exe
13	□	1	□		12 NA		00000009 001000b345c0000 000a00004a610000 8664 Microsoft.DesktopAppInstaller 8wekyb3d8bbwe
14	□	1	□		13 NA	2018-04-11 23:34:37	C:\Windows\system32\OpenWith.exe
15	□	1	□		14 NA	2023-02-13 17:22:31	C:\Program Files\WindowsApps\Microsoft.MicrosoftOfficeHub_18.2301.1131.0_x64_8wekyb3d8bbwe\Application
16	□	1	□		15 NA		00000009 0006089b040d0000 000a000047ba0000 8664 Microsoft.MSPaint 8wekyb3d8bbwe
17	□	1	□		16 NA		00000009 001208fd046b0000 000a00004a610000 8664 Microsoft.MicrosoftOfficeHub 8wekyb3d8bbwe
18	□	1	□		17 NA		00000009 000a0037000800000 000a000047ba0000 8664 Microsoft.WindowsCalculator 8wekyb3d8bbwe
19	□	1	□		18 NA	2023-02-13 17:22:10	C:\Program Files\WindowsApps\Microsoft.WindowsFeedbackHub_1.2108.2563.0_x64_8wekyb3d8bbwe\Application
20	□	1	□		19 NA		00000009 001083c0a030000 000a000049c980000 8664 Microsoft.WindowsFeedbackHub 8wekyb3d8bbwe
21	□	1	□		20 NA		00000009 000a00390000400000 000a000045630000 8664 Microsoft.People 8wekyb3d8bbwe
22	□	1	□		21 NA	2023-02-13 17:09:01	C:\Users\IEUser\AppData\Local\Microsoft\OneDrive\23.02.0125.0003\FileCoAuth.exe
23	□	1	□		22 NA	2023-02-13 17:21:20	C:\Program Files\WindowsApps\Microsoft.XboxGameOverlay_1.54.4001.0_x64_8wekyb3d8bbwe\Application
24	□	1	□		23 NA		00000009 07e4038600140000 000a00004a610000 8664 Microsoft.WindowsCamera 8wekyb3d8bbwe
25	□	1	□		24 NA		00000009 000100360fa10000 000a000042ee0000 8664 Microsoft.XboxGameOverlay 8wekyb3d8bbwe
26	□	1	□		25 NA		00000009 00030007008e0000 000a000047ba0000 8664 Microsoft.MicrosoftStickyNotes 8wekyb3d8bbwe
27	□	1	□		26 NA		00000009 000100004d400000 000a00004a610000 8664 Microsoft.WebMediaExtensions 8wekyb3d8bbwe
28	□	1	□		27 NA		00000009 000a0037001c0000 000a000045630000 8664 Microsoft.WindowsSoundRecorder 8wekyb3d8bbwe
29	□	1	□		28 NA		00000009 000c005f0bb90000 000a000045630000 8664 Microsoft.XboxIdentityProvider 8wekyb3d8bbwe
30	□	1	□		29 NA	2023-02-13 17:20:39	C:\Program Files\WindowsApps\Microsoft.OneConnect_5.2204.1931.0_x64_8wekyb3d8bbwe\Application
31	□	1	□		30 NA		00000009 0005089c04070000 000a0000581d0000 8664 Microsoft.OneConnect 8wekyb3d8bbwe
32	□	1	□		31 NA		00000009 000a003800020000 000a00004bc80000 8664 Microsoft.WindowsMaps 8wekyb3d8bbwe
33	□	1	□		32 NA		00000009 000100066b150000 000a000027410000 8664 Microsoft.NET.Native.Framework.1.6 8wekyb3d8bbwe

Total lines 408 Visible lines 408 Open files: 1 Search options

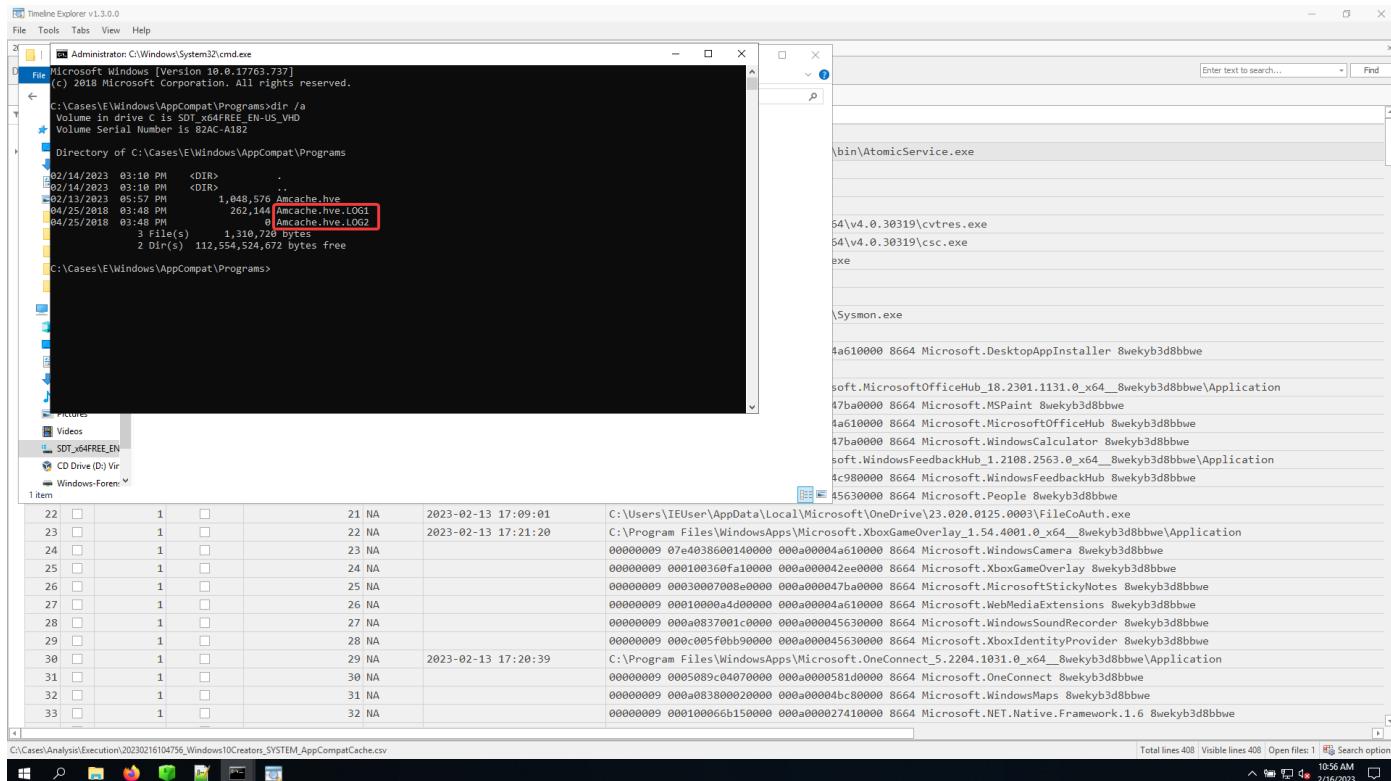
10:50 AM 2/16/2023

Amcache

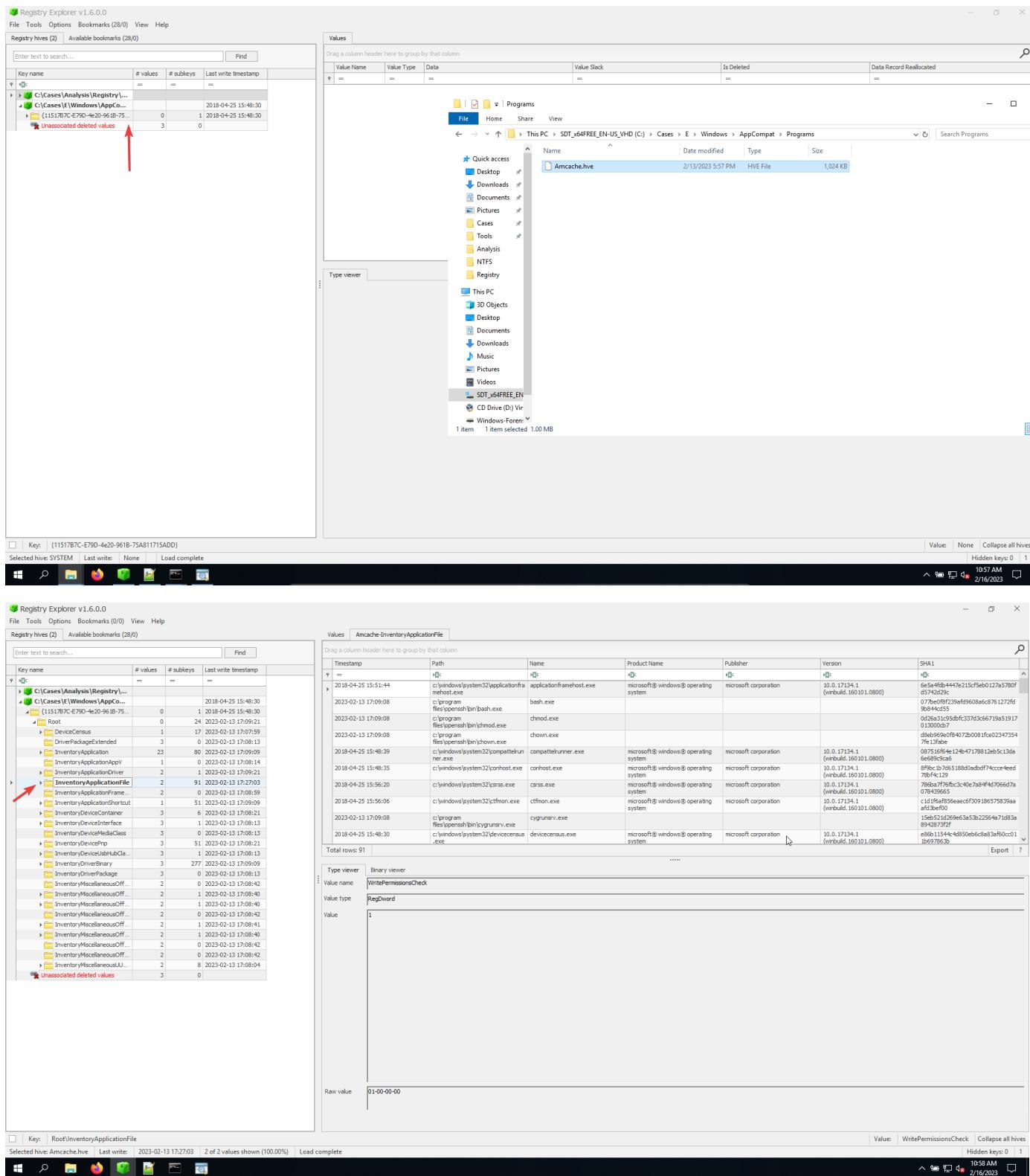
- You can find it at : **C:\Windows\AppCompat\Programs\Amcache.hve**
- Stores information about the user application experience.
- Location:



- There are two log files for Amcache.hve:



- Open it in registry Explorer:



- AmcacheParser:

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (0/0) View Help

Registry hives (2) Available bookmarks (28/0)

Enter text to search... Values Amcache-InventoryApplicationFile

Administrator: C:\Windows\System32\cmd.exe

```
AmcacheParser.exe -f "C:\Temp\amcache\AmcacheWin10.hve" -w "c:\temp\whitelist.txt" --csv C:\temp
AmcacheParser.exe [options]
  Options:
    -f <file> (REQUIRED) Amcache.hve file to parse
    -i <path> Include file entries for Programs entries [default: False]
    -W <path> Path to file containing SHA-1 hashes to *exclude* from the results. Blacklisting overrides whitelisting
    -b <path> Path to file containing SHA-1 hashes to *include* from the results. Blacklisting overrides whitelisting
    --csv <csv> (REQUIRED) Directory to save CSV formatted results to. Be sure to include the full path in double quotes
    --tsv <tsv> Save CSV formatted results to, when present, overrides default name
    --dt <date> The custom date/time format to use when displaying time stamps. See https://goo.gl/CHNq8K for options [default: yyyy-MM-dd HH:mm:ss]
    --mp Display higher precision for time stamps [default: False]
    --n1 When true, ignore transaction log files for dirty hives. Default is FALSE
    --debug Show detailed information during processing [default: False]
    --trace Show trace information during processing [default: False]
    --version Show version information
    -?, -h, --help Show help and usage information
```

C:\Tools\EZTools>AmcacheParser.exe -f C:\Cases\E\Windows\AppCompat\Programs\Amcache.hve --csv C:\Cases\Analysis\Execution

Path	Count	Time	Value
Inventory\MiscellaneousOff...	2	1	2023-02-13 17:08:41
Inventory\MiscellaneousOff...	2	1	2023-02-13 17:08:40
Inventory\MiscellaneousOff...	2	0	2023-02-13 17:08:42
Inventory\MiscellaneousOff...	2	0	2023-02-13 17:08:42
Inventory\MiscellaneousU...	2	8	2023-02-13 17:08:04
Unassociated deleted values	3	0	

Raw value: 01-00-00-00

5 KB
1,562 KB
1,417 KB
997 KB

Music Pictures Videos SDT_64FREE_EN CD Drive (D) Vir Windows-Forensics PE Cmd.exe

Changelog.txt Get-ZimmermanTools.ps1 JLCmd.exe LECmd.exe MFTECmd.exe PE Cmd.exe

2/13/2023 3:58 PM 1/22/2022 10:58 PM 7/25/2022 4:18 PM 6/15/2022 10:53 AM 10/20/2022 1:37 PM 1/28/2022 12:08 PM

Text Document Windows PowerShell Application Application Application Application Application

33 KB 32 KB 4,710 KB 4,992 KB 4,409 KB 3,885 KB

Values WritePermissionsCheck Collapse all hives

Selected hive: Amcache.hve Last write: 2023-02-13 17:27:03 2 of 2 values shown (100.00%) Load complete

11:00 AM 2/16/2023

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (0/0) View Help

Registry hives (2) Available bookmarks (28/0)

Enter text to search... Values Amcache-InventoryApplicationFile

Administrator: C:\Windows\System32\cmd.exe

```
--version Show version information
-?, -h, --help Show help and usage information
AmcacheParser version 1.5.1.0
Author: Eric Zimmerman (saeericzimmerman@gmail.com)
https://github.com/EricZimmerman/AmcacheParser
Command line: -f C:\Cases\E\Windows\AppCompat\Programs\Amcache.hve --csv C:\Cases\Analysis\Execution
C:\Cases\E\Windows\AppCompat\Programs\Amcache.hve is in new format!
Total file entries found: 91
Total shortcuts found: 51
Total device containers found: 6
Total device PnPs found: 51
Total drive binaries found: 277
Found 44 unassociated file entry
Results saved to: C:\Cases\Analysis\Execution
Total parsing time: 0.264 seconds
```

C:\Tools\EZTools>

Path	Count	Time	Value
Inventory\MiscellaneousOff...	2	1	2023-02-13 17:08:41
Inventory\MiscellaneousOff...	2	1	2023-02-13 17:08:40
Inventory\MiscellaneousOff...	2	0	2023-02-13 17:08:42
Inventory\MiscellaneousOff...	2	0	2023-02-13 17:08:42
Inventory\MiscellaneousU...	2	8	2023-02-13 17:08:04
Unassociated deleted values	3	0	

Raw value: 01-00-00-00

5 KB
1,562 KB
1,417 KB
997 KB

Music Pictures Videos SDT_64FREE_EN CD Drive (D) Vir Windows-Forensics PE Cmd.exe

Changelog.txt Get-ZimmermanTools.ps1 JLCmd.exe LECmd.exe MFTECmd.exe PE Cmd.exe

2/13/2023 3:58 PM 1/22/2022 10:58 PM 7/25/2022 4:18 PM 6/15/2022 10:53 AM 10/20/2022 1:37 PM 1/28/2022 12:08 PM

Text Document Windows PowerShell Application Application Application Application Application

33 KB 32 KB 4,710 KB 4,992 KB 4,409 KB 3,885 KB

Values WritePermissionsCheck Collapse all hives

Selected hive: Amcache.hve Last write: 2023-02-13 17:27:03 2 of 2 values shown (100.00%) Load complete

11:00 AM 2/16/2023

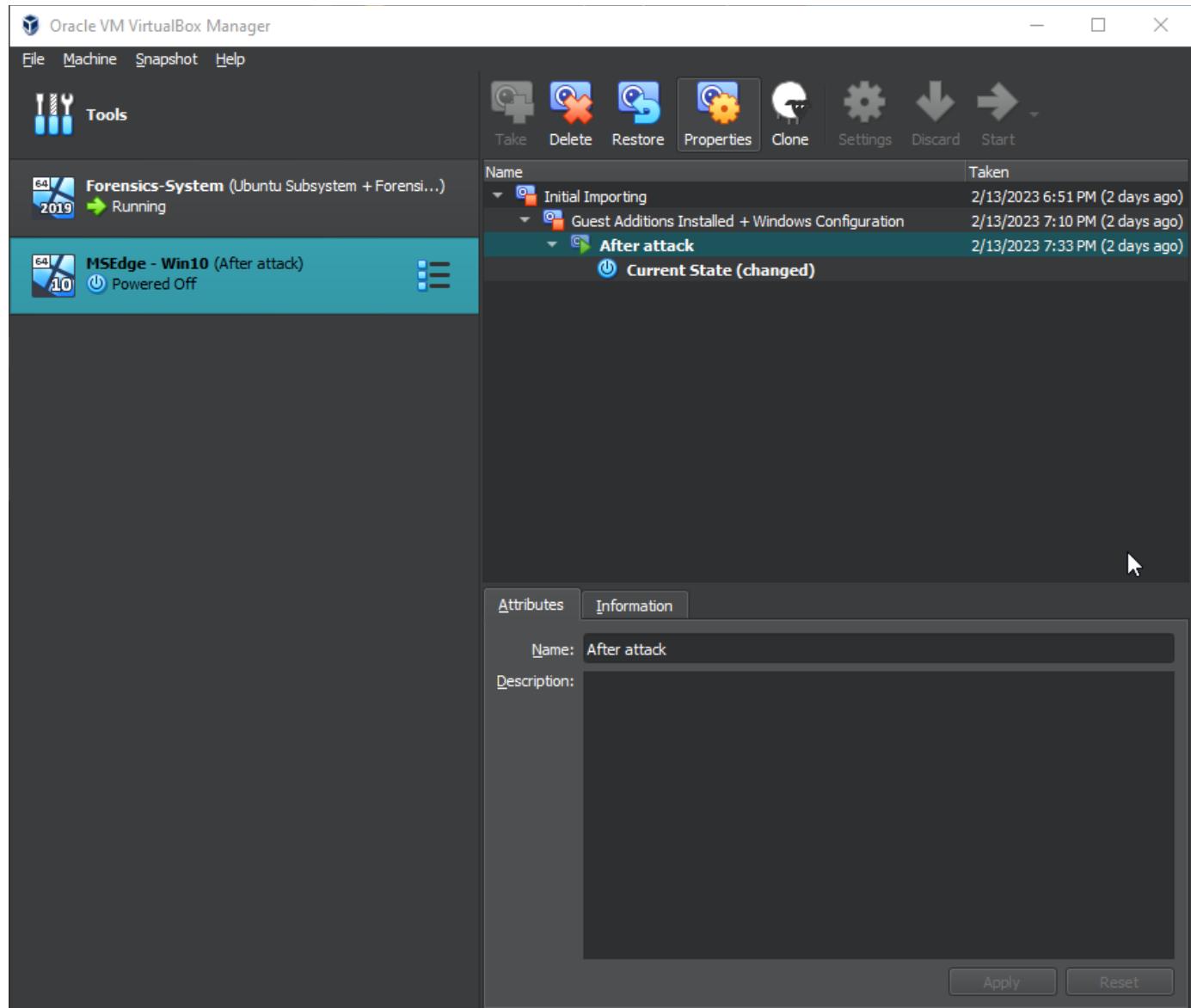
The screenshot shows a Windows desktop environment with several open windows:

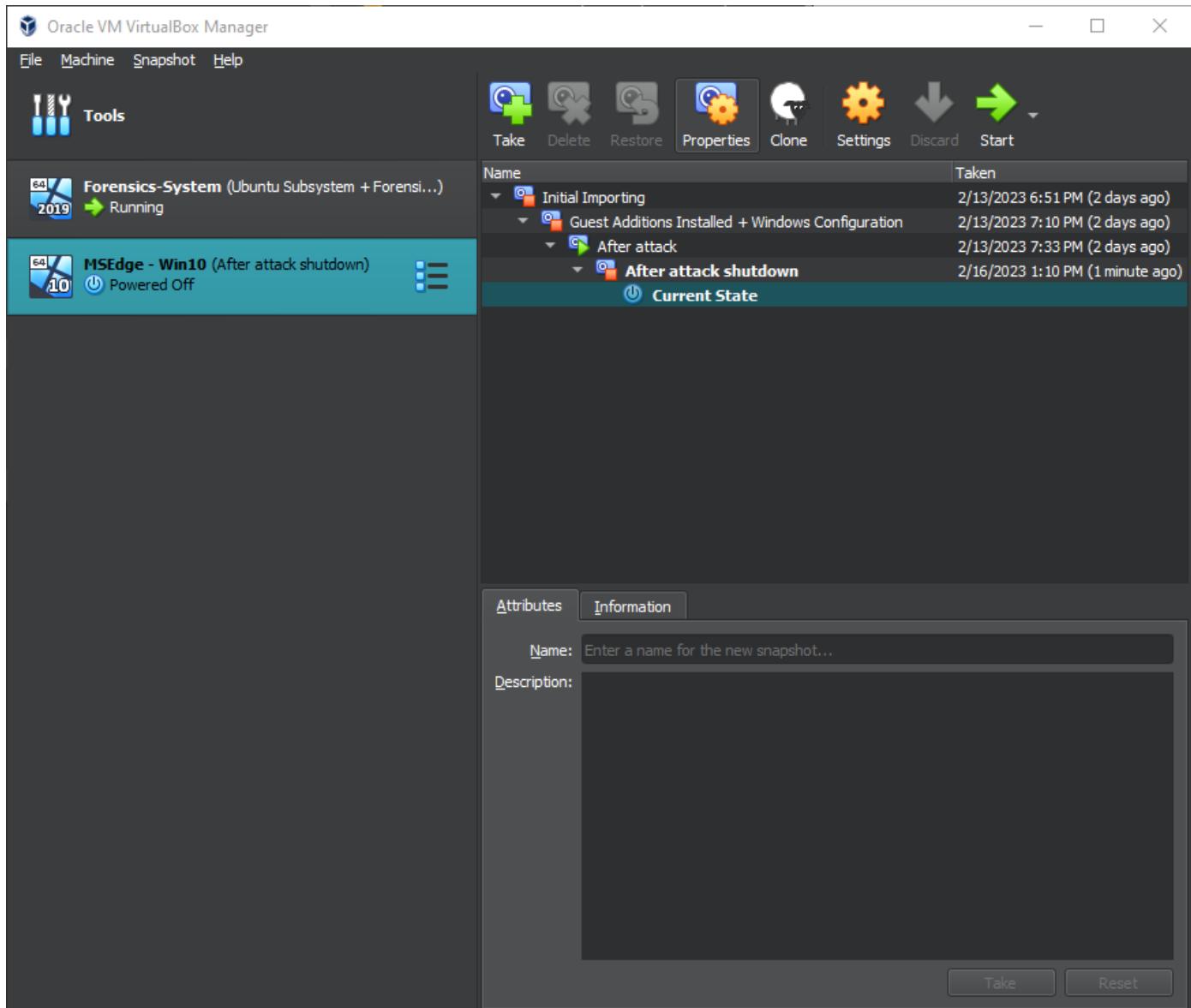
- Registry Explorer v1.6.0.0**: Shows the registry keys under `HKLM\Software\Amcache`. One key, `AmcacheParser version 1.5.1.0`, is expanded, showing its author (Eric Zimmerman) and command line.
- Timeline Explorer v1.3.0.0**: Shows a timeline of events. A specific entry, `20230216104756_Windows10Creators_SYSTEM_AppCompatCache.csv`, is highlighted.
- CSV File Viewer**: Displays the contents of the `Amcache_UnassociatedFileEntries.csv` file. The file contains numerous entries for unassociated files, each with columns for Line, Tag, Application Name, Program Id, File Key, Last Write Timestamp, SHA1, Is, Os, Component, and Full Path.
- Taskbar**: Shows various pinned icons and the system tray.

- We cannot see the Atomic service , maybe the transaction logs didn't merged with the Amcache.hve, but the date says otherwise:

```
02/14/2023 03:10 PM <DIR> .
02/14/2023 03:10 PM <DIR> ..
02/13/2023 05:57 PM 1,048,576 Amcache.hve
04/25/2018 03:48 PM 262,144 Amcache.hve.LOG1
04/25/2018 03:48 PM 0 Amcache.hve.LOG2
```

- We need to open the compromised system :

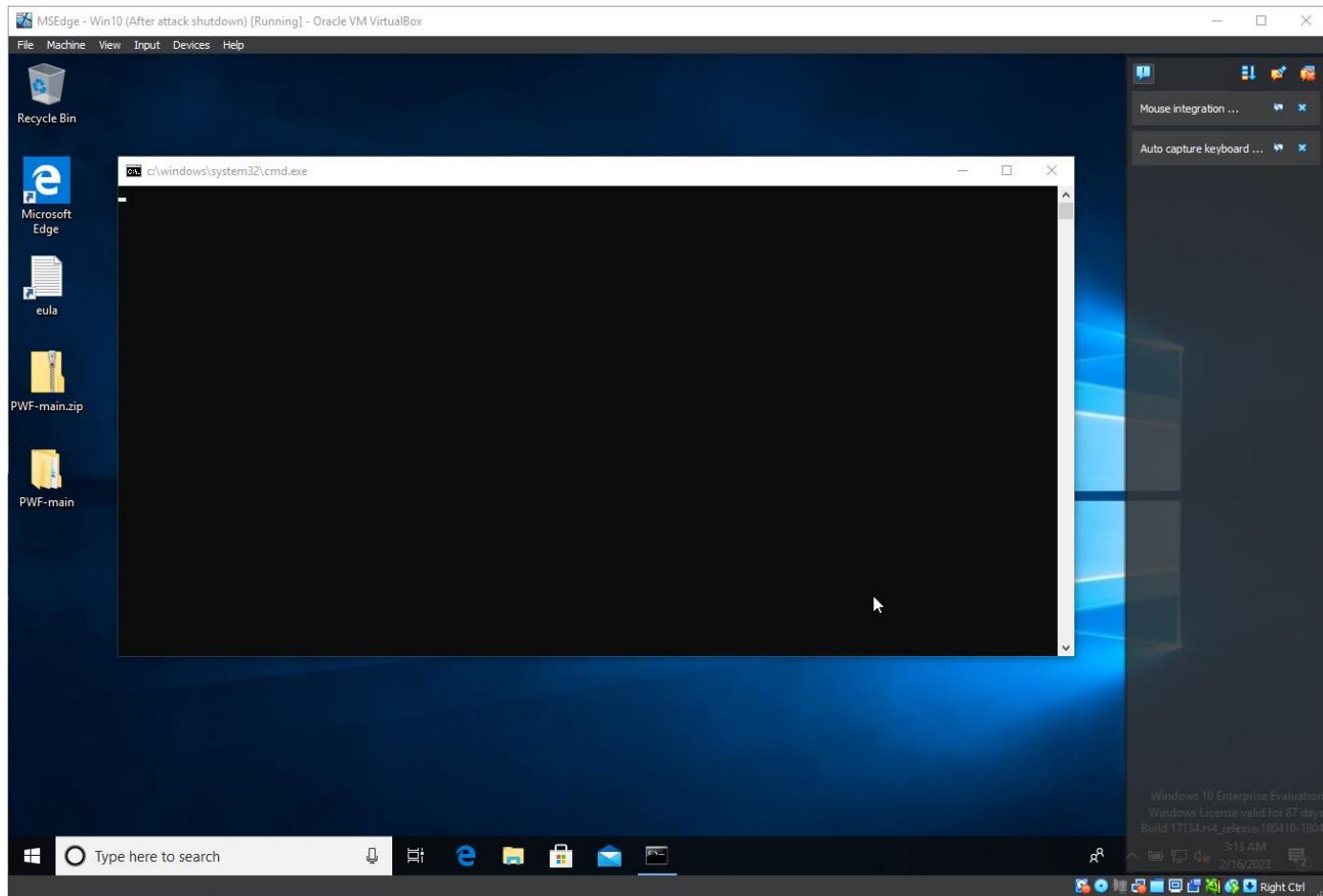


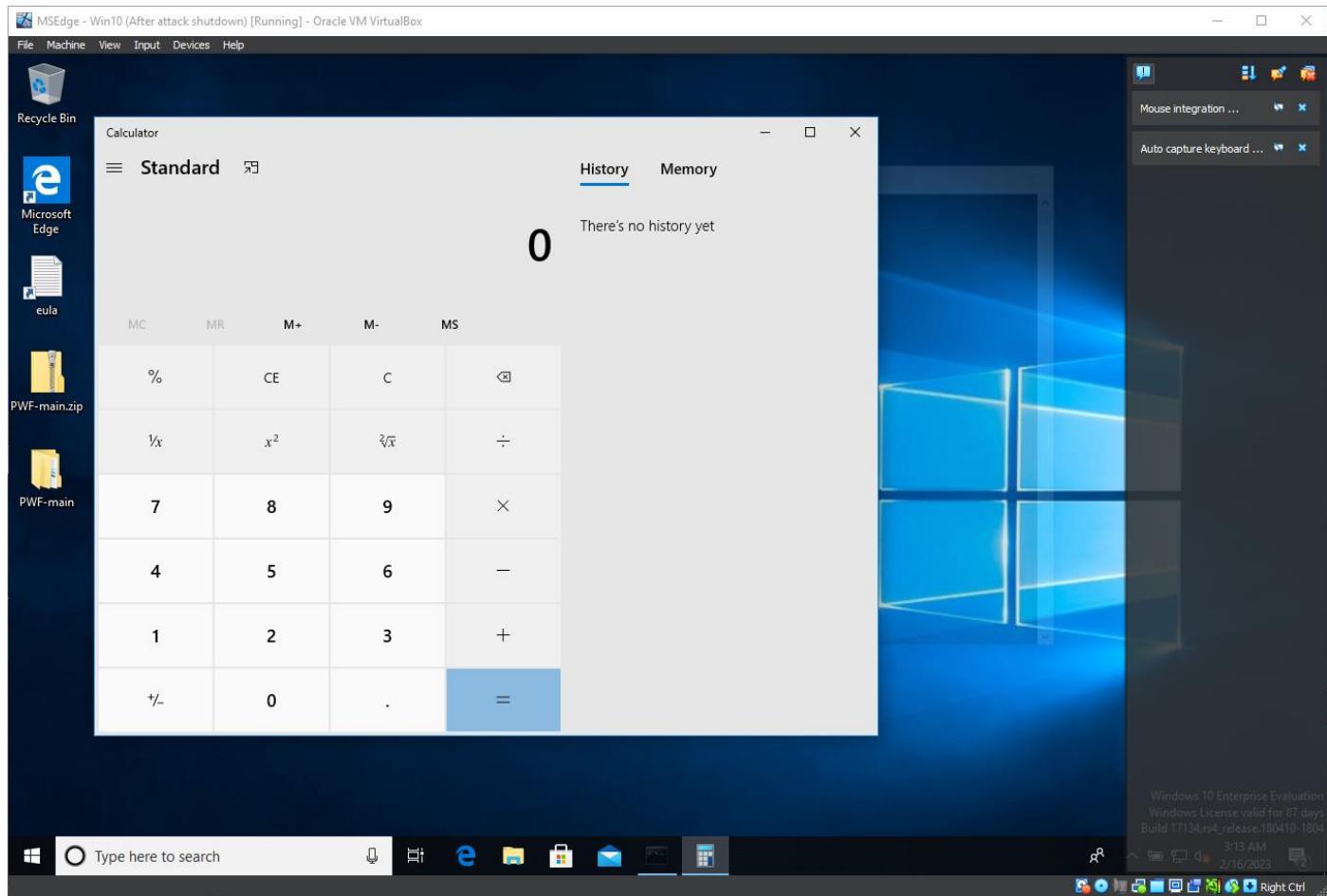


- AmcacheParser to put in the compromised system shared folder:
<https://f001.backblazeb2.com/file/EricZimmermanTools/AmcacheParser.zip>

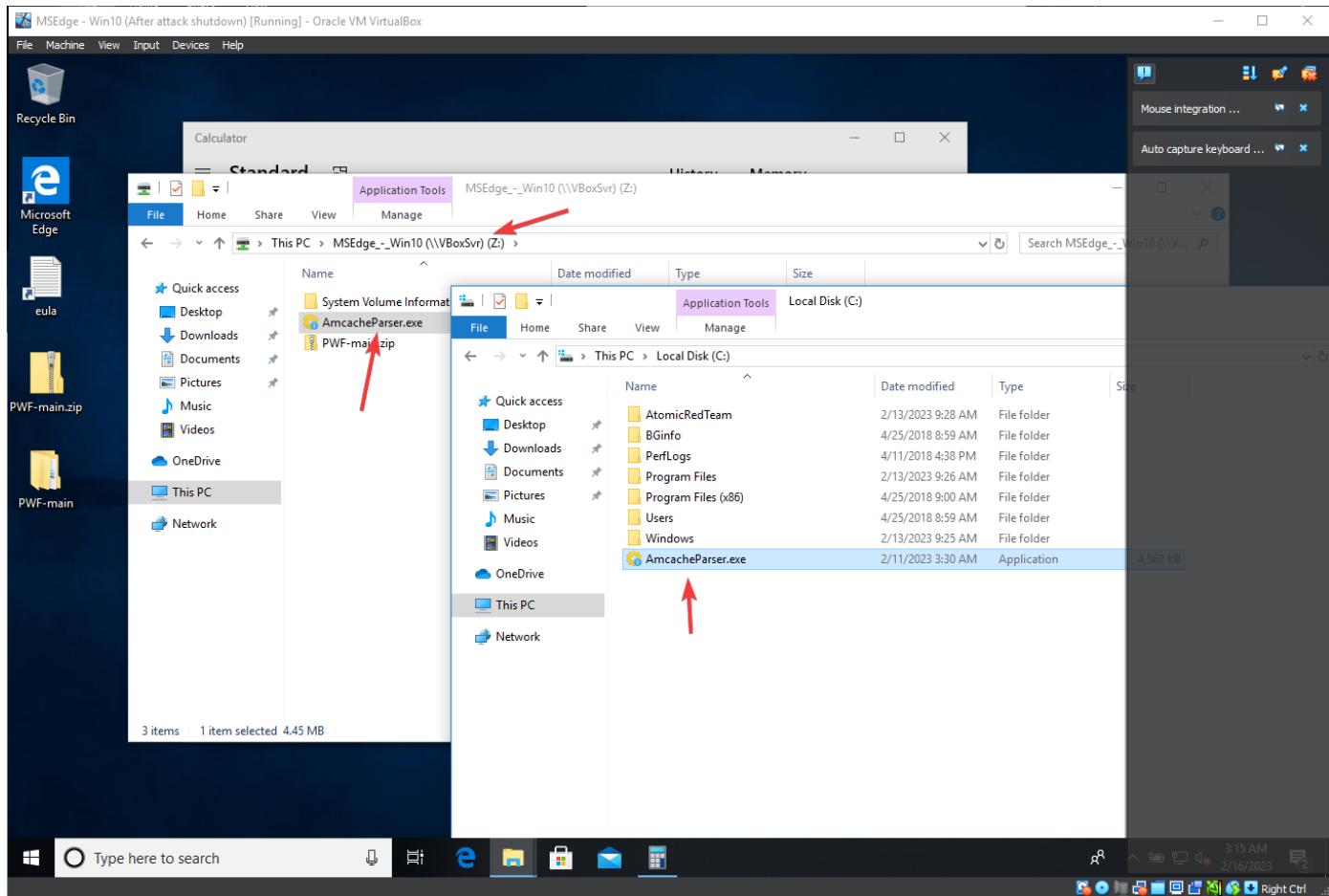
Name	Date modified	Type	Size
System Volume Information	2/8/2023 11:48 PM	File folder	
AmcacheParser.exe	2/11/2023 1:30 PM	Application	4,562 KB
PWF-main.zip	2/11/2023 2:31 PM	Compressed (zipp...)	393 KB

- Open compromised system. Typically you would disconnect from the network , the virtual machine , but there is nothing malicious in the virtual machine.
- Persistence techniques, following in the further analysis:

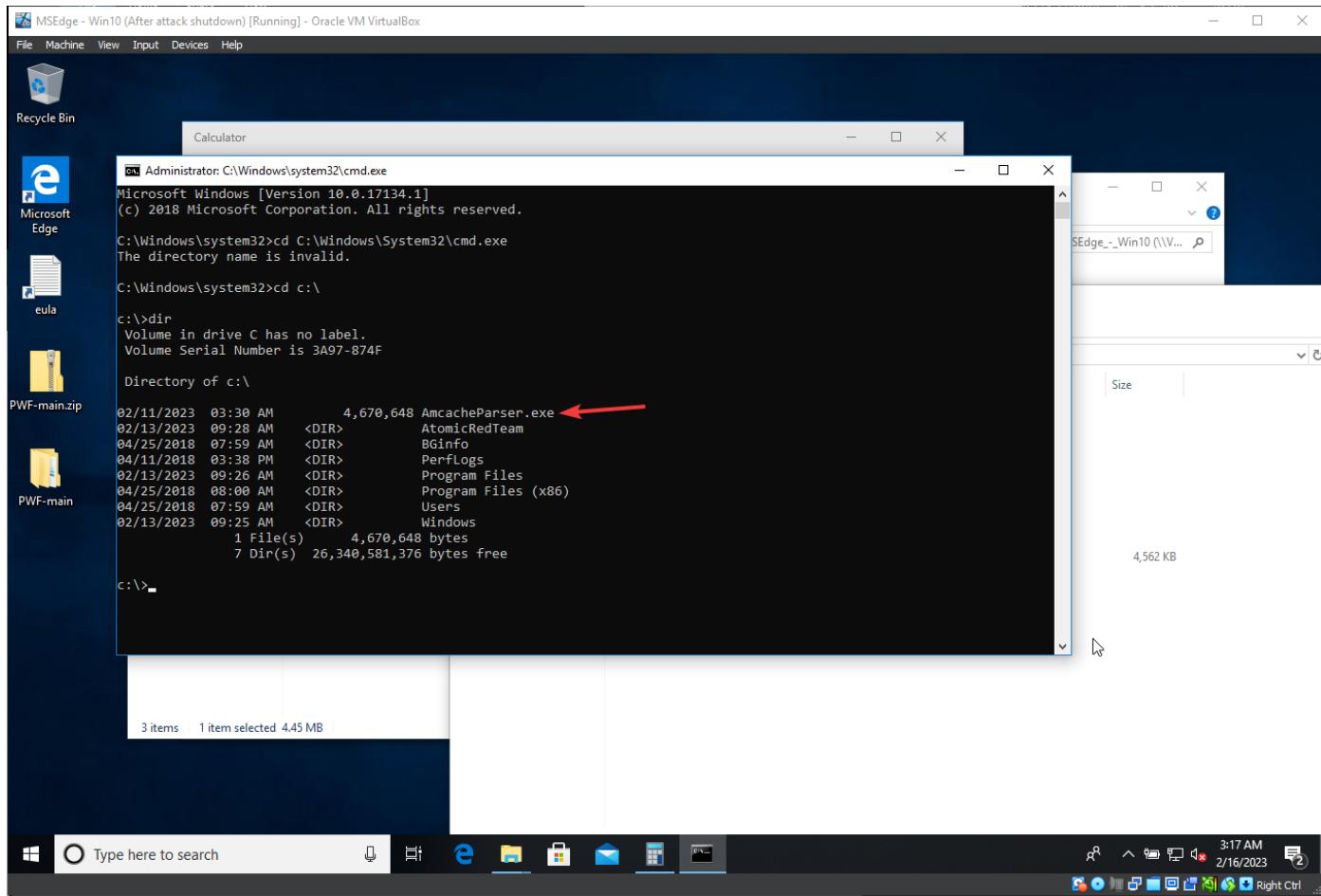


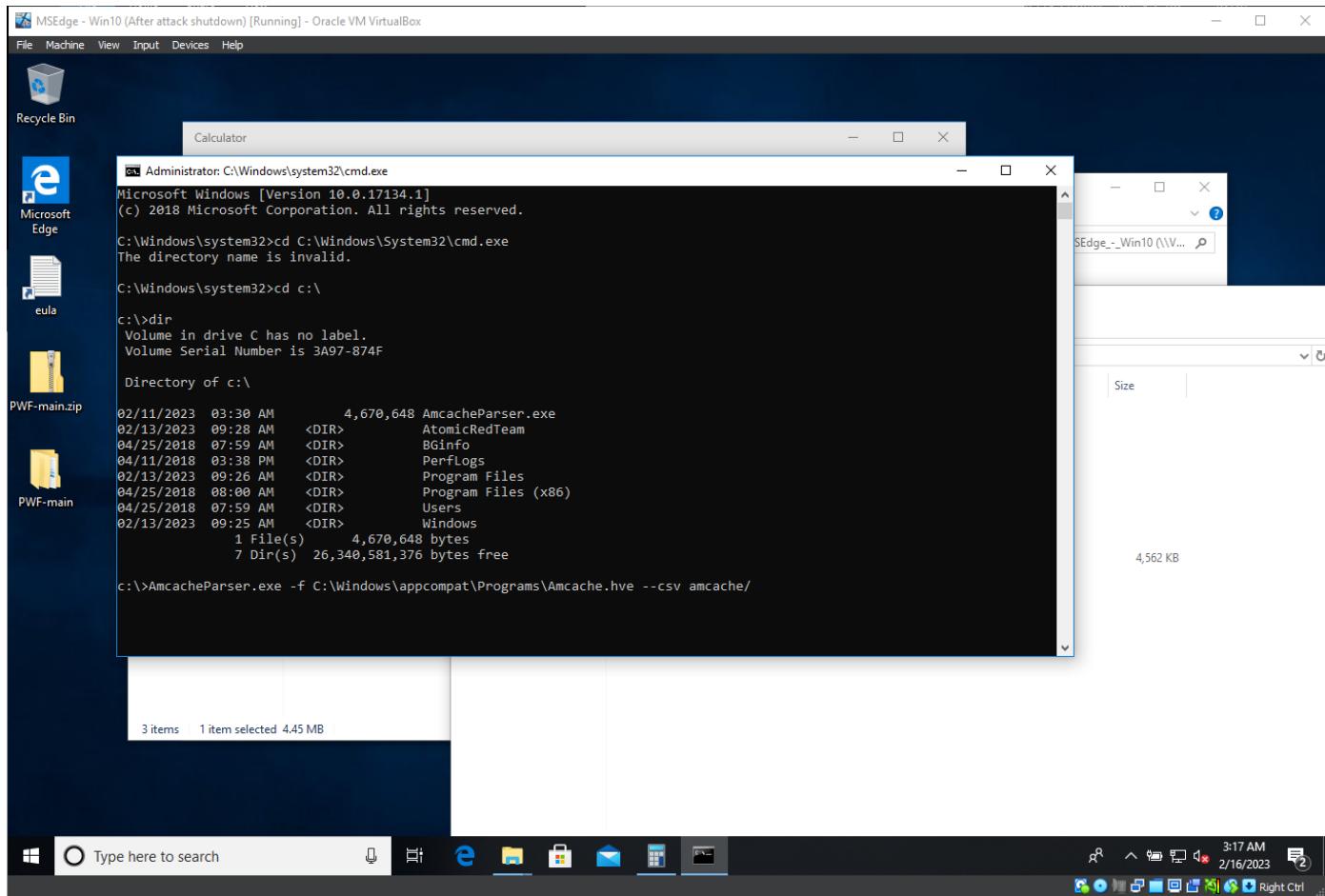


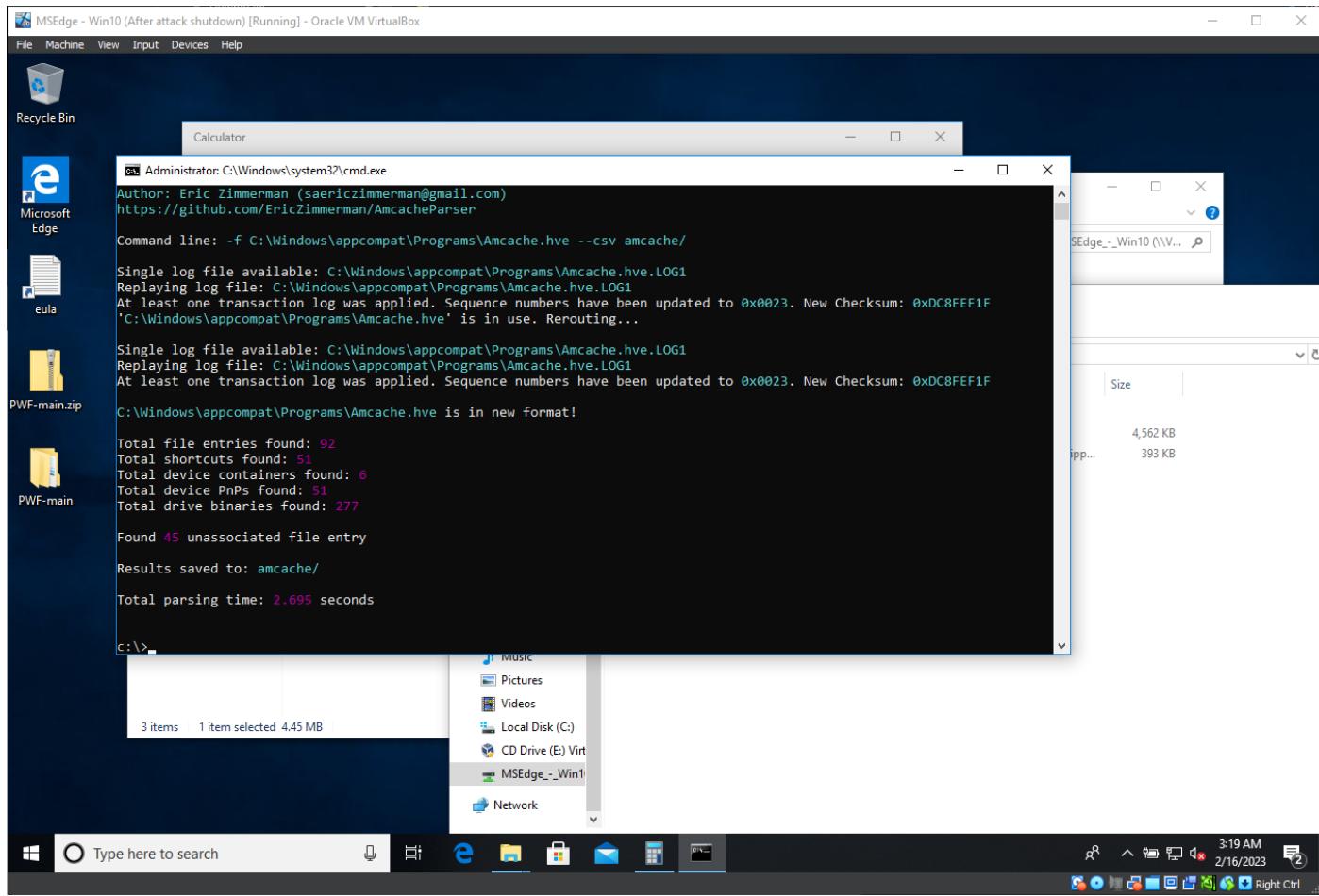
- Copy the file wherever you want



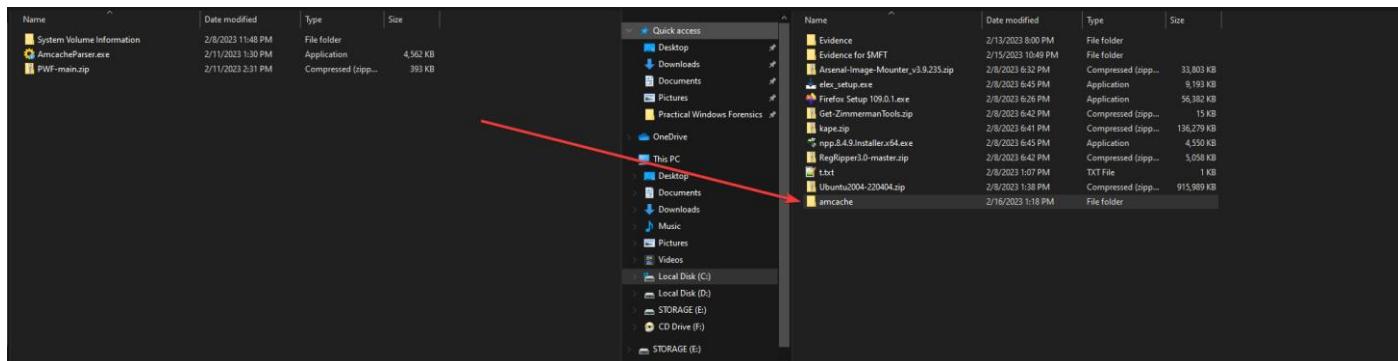
- Parse the amcache hive:







- Move it into the Forensic Workstation folder.



- Just one file added.

Timeline Explorer v1.3.0.0

File Tools Tabs View Help

20230216031755_Amcache_UnassociatedFileEntries.csv

Drag a column header here to group by that column

Enter text to search... Find

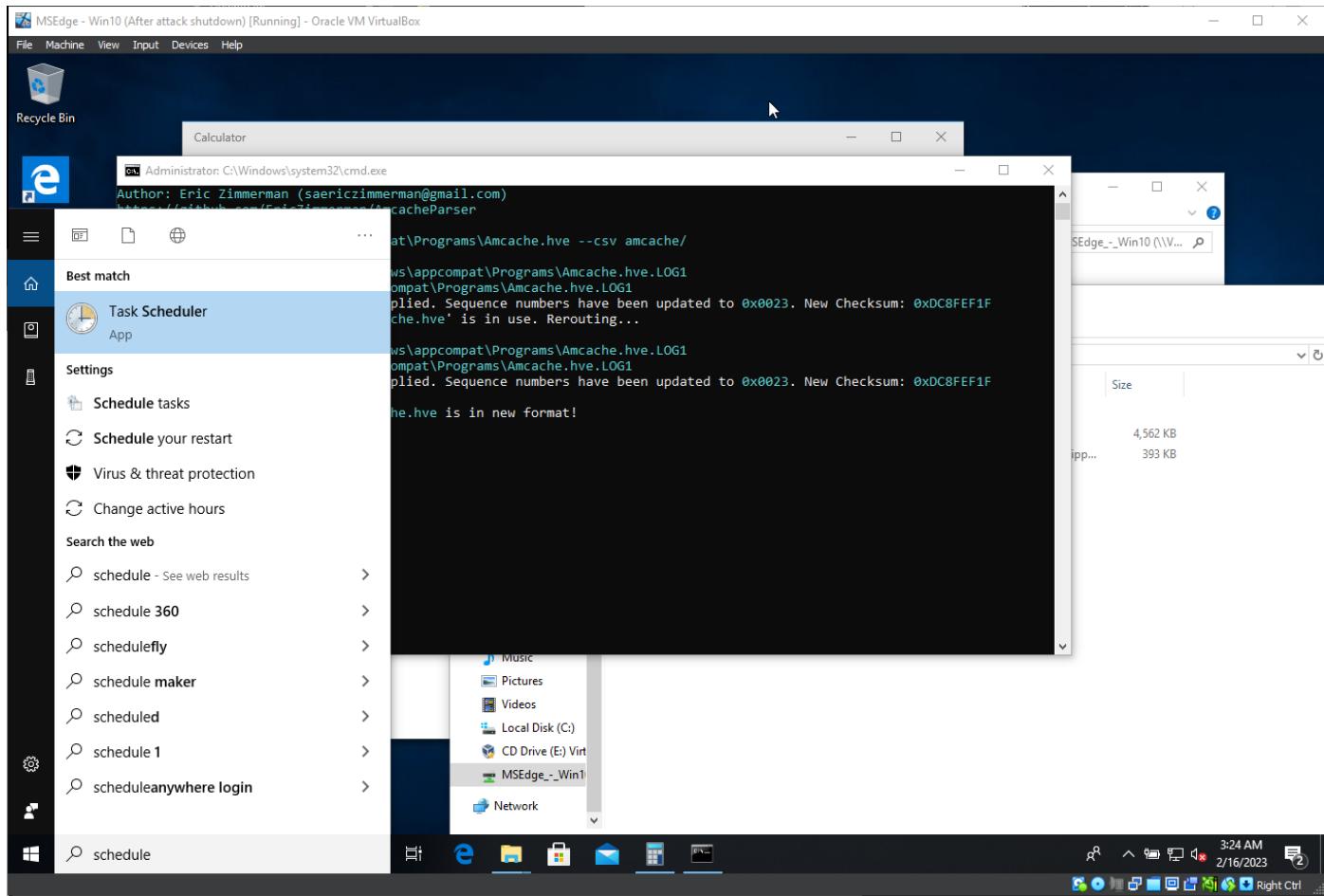
Last Write Timestamp	SHA1	Is Os Component	Full Path	Name
-15 20:47:16	2ff0a000442a7fdf257944e0417e1b77e5bec0f	<input checked="" type="checkbox"/>	c:\windows\system32\werfaultsecure.exe	werfaults
-13 17:27:03	3ef75664261a1b9b3d6262132c131da2f4da67c	<input type="checkbox"/>	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17134.2207_none_c3d85cec697bbe8etc...	mrt.exe
-13 17:19:25	ab87a56870cf3fb032d88edbf7ae8aabe627	<input checked="" type="checkbox"/>	c:\windows\system32\musnotification.exe	musnotifi
-13 17:17:40	e70c1a502ed33fcf3ff696771f5169f32cc8a9e5	<input type="checkbox"/>	c:\windows\system32\mrt.exe	wuauct.e
-13 17:16:12	e82ac9345fbefc100ff1d66536877502ab2c017	<input checked="" type="checkbox"/>	c:\windows\system32\wuauct.exe	sedsvc.ex
-13 17:13:32	3d9ee67daddcb1f4f4bbad70ea19e3dee4667cc9	<input type="checkbox"/>	c:\program files\rempl\sedsvc.exe	sedlauncher.exe
-13 17:13:32	4e40d590da1357a750e341d772e0ef62b1c479ee	<input type="checkbox"/>	c:\program files\rempl\sedlauncher.exe	vboxtray.
-13 17:09:09	6ea0ea87cbc341ba5d3a1be96cb5c40005db02	<input type="checkbox"/>	c:\windows\system32\vboxtray.exe	msmpeng.e
-13 17:09:09	5ac6e790de19fd66988648ccb22073c4a2719ba	<input checked="" type="checkbox"/>	c:\program files\windows defender\msmpeng.exe	microsoft
-13 17:08:50	b4a549508bc9f975a191434d420ad3c28d5028	<input type="checkbox"/>	c:\users\leuser\appdata\local\microsoft\edgeupdate\edgeupdate.exe	onedrives
-13 17:08:28	57b7fc9b59c0fa9a9c19adce0a159746554d682	<input type="checkbox"/>	c:\users\leuser\appdata\local\microsoft\onedrive\onedrivestandaloneupdater.exe	sihclient
-13 17:08:01	0e5421e832745a3b285a474ef7afe40d47b7f428	<input checked="" type="checkbox"/>	c:\windows\system32\sihclient.exe	updateandtaskhostw
-13 17:08:00	d0ad161e3d318de58ff9e89bacd87fecae2d768e	<input checked="" type="checkbox"/>	c:\windows\system32\updatenotificationmgr.exe	taskhostw
-13 17:07:59	2a594345fcada453c72bd937cbf6b43a74df	<input type="checkbox"/>	c:\windows\system32\taskhostw.exe	msmpeng.e
-13 17:03:44	a108a8cea0db502079176fcf81190a1506d5a5b6	<input type="checkbox"/>	c:\programdata\microsoft\windows defender\platform\4.14.17613.18039-0\msmpeng.exe	wlrmdr.ex
-25 16:07:43	d24e9c6079a20d1aed8c1c409c3fc8e1c63628f3	<input checked="" type="checkbox"/>	c:\windows\system32\wlrmdr.exe	mpsigtub
-25 15:58:46	5b205fc1a25354726677a30b25d8e41b3ef69d84	<input type="checkbox"/>	c:\users\leuser\appdata\local\temp\{7e9b4a05-1664-4b5a-9e13-8bc9a6443a9c}\mpsigtub.exe	mpsigtub
-25 15:58:44	5b205fc1a25354726677a30b25d8e41b3ef69d84	<input type="checkbox"/>	c:\users\leuser\appdata\local\temp\{976ca9-2f12-4069-bc8-3e4f77708c71}\mpsigtub.exe	wermgr.ex
-25 15:58:40	1ed4ae92d35497f62610078d5110c4634afade	<input checked="" type="checkbox"/>	c:\windows\system32\wermgr.exe	mpsigtub
-25 15:58:37	5b205fc1a25354726677a30b25d8e41b3ef69d84	<input type="checkbox"/>	c:\users\leuser\appdata\local\temp\{3b66c4bf-6d1d-4725-b71c-e7bd2efc27a}\mpsigtub.exe	mpsigtub
-25 15:58:33	5b205fc1a25354726677a30b25d8e41b3ef69d84	<input type="checkbox"/>	c:\users\leuser\appdata\local\temp\{b6ba099f-46c8-4aa3-8e24-3ace7e62c25d}\mpsigtub.exe	mpsigtub
-25 15:56:30	c1827349741d158c87172b9963fcbe53661848	<input checked="" type="checkbox"/>	c:\windows\system32\winlogon.exe	winlogon.
-25 15:56:26	7693be79ba30ba9659c028c5c8d8c4481c2f89f	<input checked="" type="checkbox"/>	c:\windows\system32\dwm.exe	dwm.exe
-25 15:56:24	0950dd0f772d2eb578a8699f82ea6d5edb4a96ff	<input checked="" type="checkbox"/>	c:\windows\system32\logonui.exe	logonui.e
-25 15:56:24	f5d0299140c989875b07db2d892617401dad8b9	<input checked="" type="checkbox"/>	c:\windows\explorer.exe	explorer.
-25 15:56:20	2a3bfed9c680f7c8e229901b6786aa9f9655aa6b	<input checked="" type="checkbox"/>	c:\windows\system32\upfc.exe	upfc.exe
-25 15:56:20	660b766fb882417d513ad967c5caf77fc2bac6	<input checked="" type="checkbox"/>	c:\windows\system32\svchost.exe	svchost.e
-25 15:56:20	e2cadef8323961be66089217ce4f11b691bc110	<input checked="" type="checkbox"/>	c:\windows\system32\services.exe	services.
-25 15:56:20	786ba7f76fb3c340e7a84fad7066d7a078439665	<input checked="" type="checkbox"/>	c:\windows\system32\csrss.exe	csrss.exe
-25 15:56:07	fbffccad3b5428e013:1ed056de2840e1a52c0b9	<input type="checkbox"/>	c:\users\leuser\appdata\local\microsoft\onedrive\onedrive.exe	onedrive.
-25 15:56:06	71e7c4d5b379079d63fe8c9f34995e82f894e0	<input checked="" type="checkbox"/>	c:\program files\windows defender\msascui.exe	msascui.l
-25 15:56:06	c1d1f6a9f856eae6f309186575839aaaf3be00	<input checked="" type="checkbox"/>	c:\windows\system32\ctfmon.exe	ctfmon.ex
-25 15:52:36	d3ee633f6fb7b5b7ff88f0167165a3079b93e1	<input type="checkbox"/>	c:\vboxwindosadditions.exe	vboxwindo

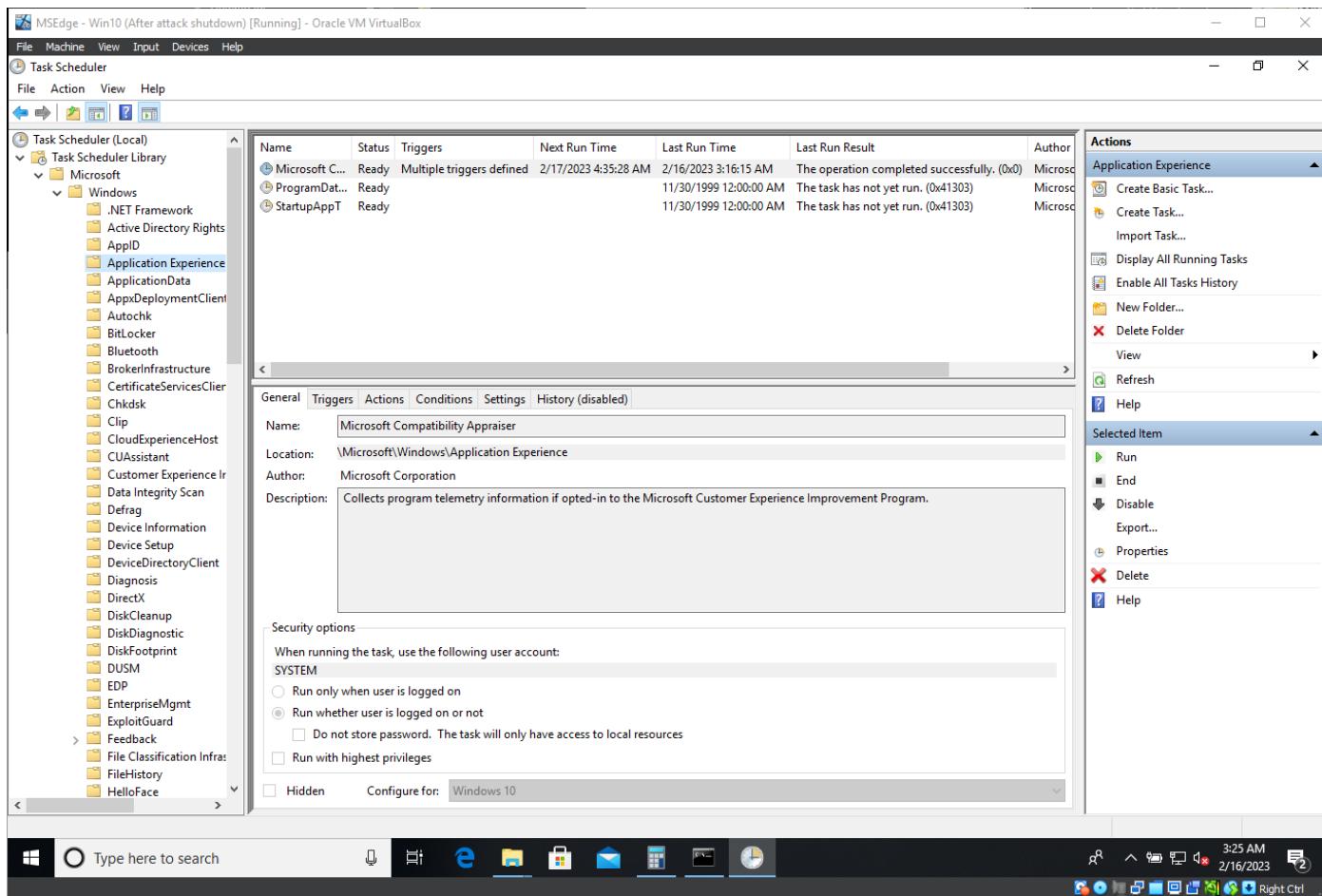
Total lines 45 Visible lines 45 Open files: 1 Search options

Z:\amcache\20230216031755_Amcache_UnassociatedFileEntries.csv

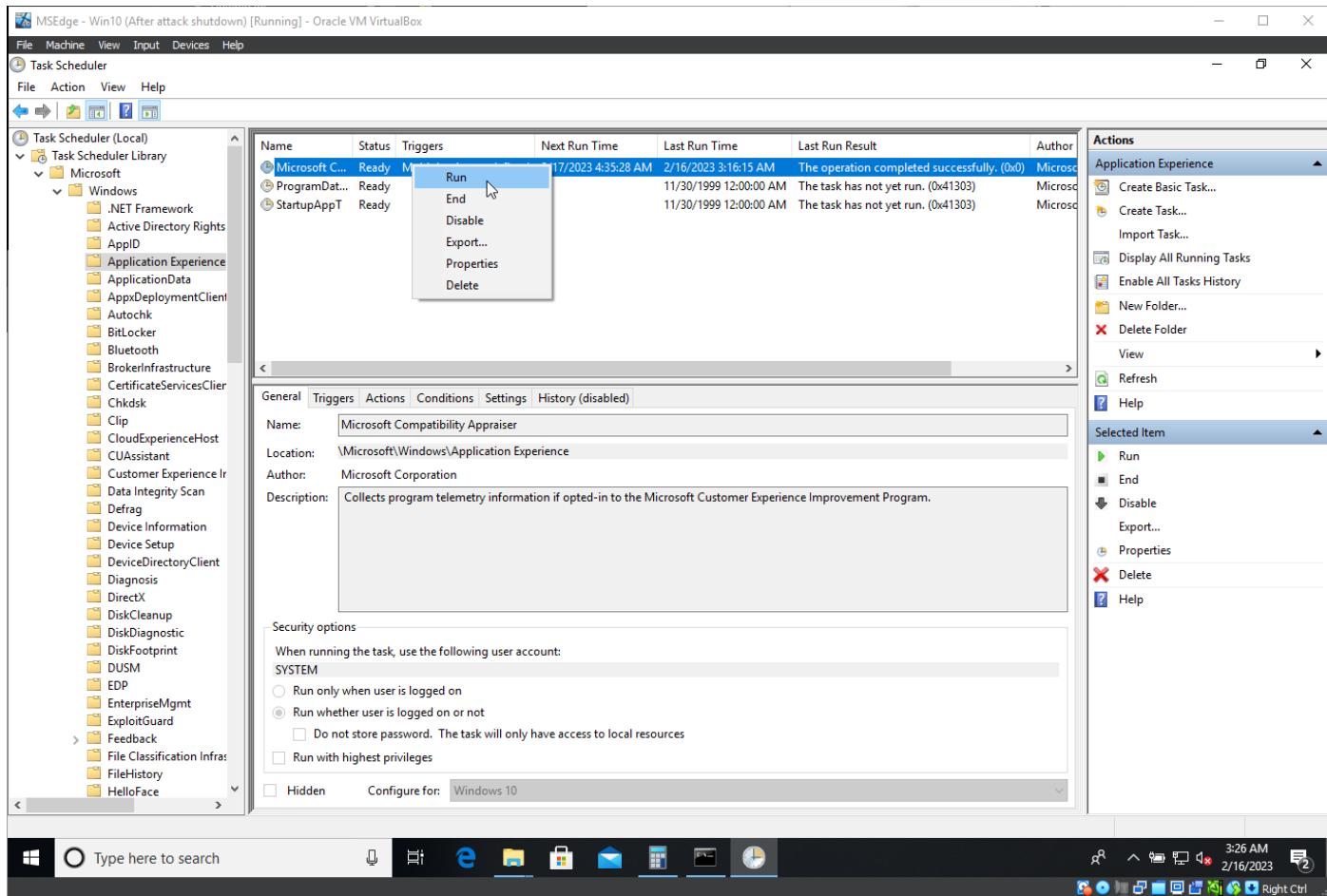
11:21 AM 2/16/2023

- According to : <https://dfir.ru/2018/12/02/the-cit-database-and-the-syscache-hive/>
- The executables are recorded in the Amcache when a particular “Microsoft Compatibility Appraiser” task is executed.
- Open Task Scheduler:

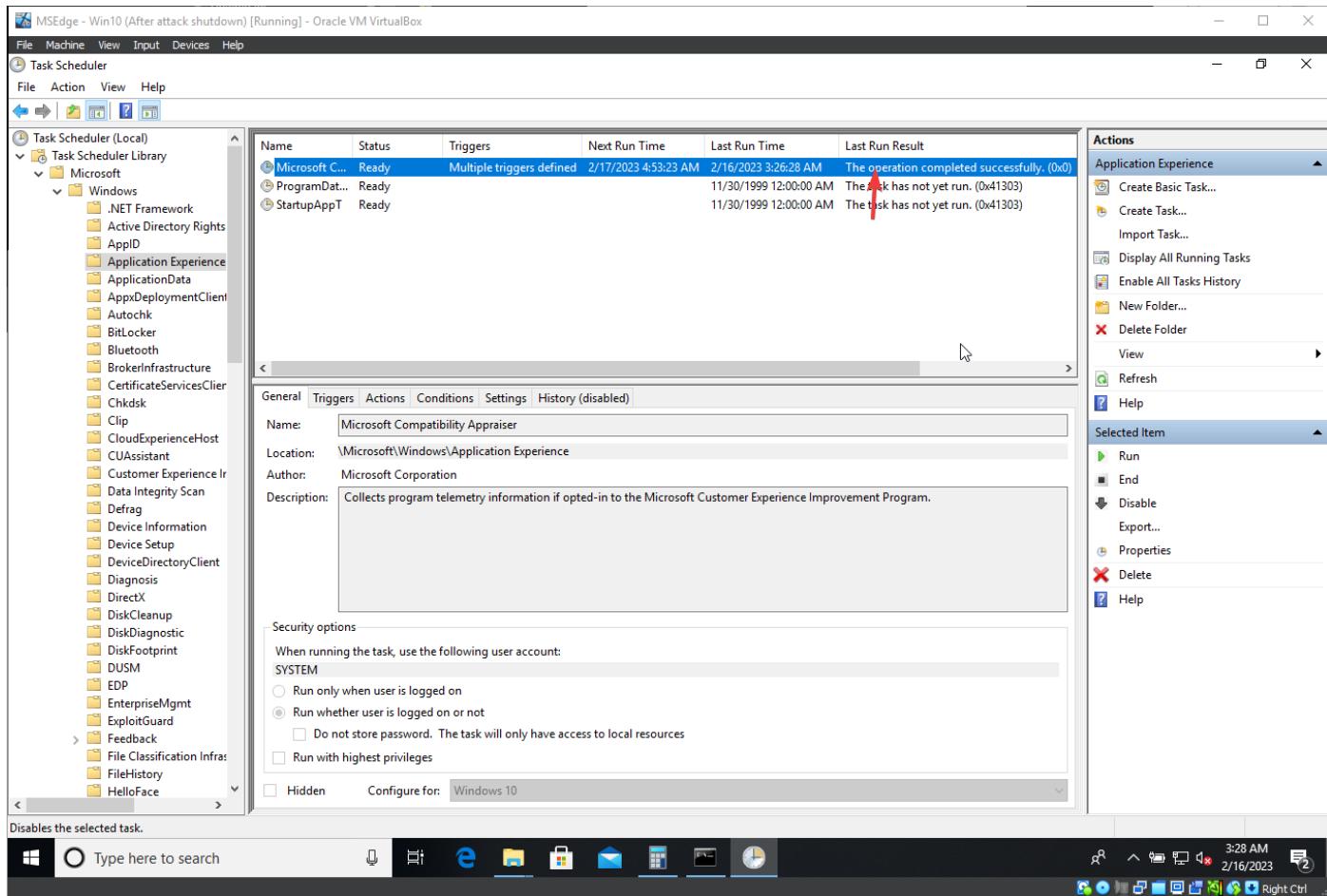




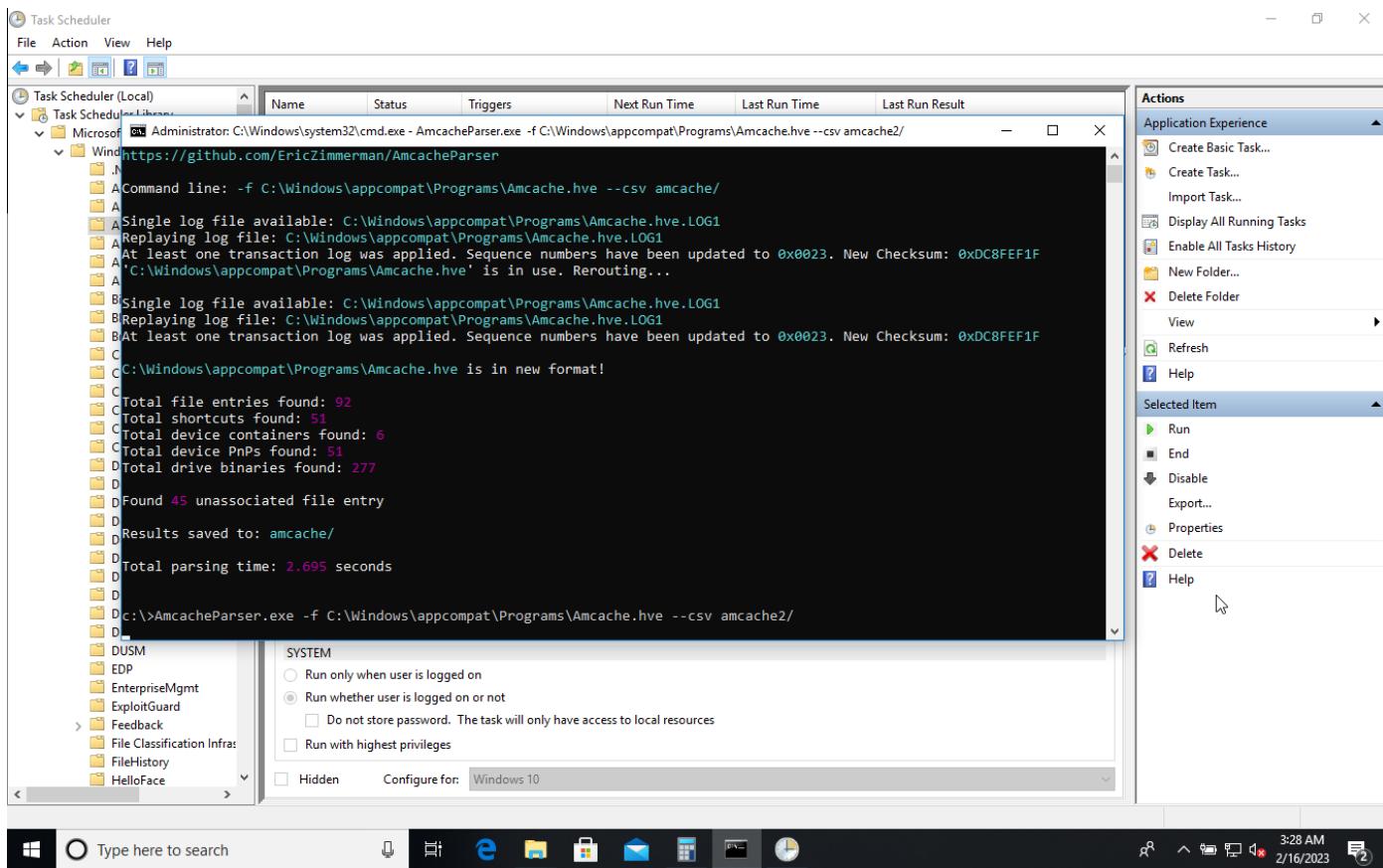
- Run the Microsoft Compatibility Appraiser task:



- Wait for it to finish.



- Reparse it :



- The number changed:

The screenshot shows the Windows Task Scheduler interface. A log entry from the command-line task 'Administrator: C:\Windows\system32\cmd.exe' is displayed. The log message indicates that the file 'amcache.hve' is in a new format and contains 48 unassociated file entries. A red arrow points to this specific line in the log output.

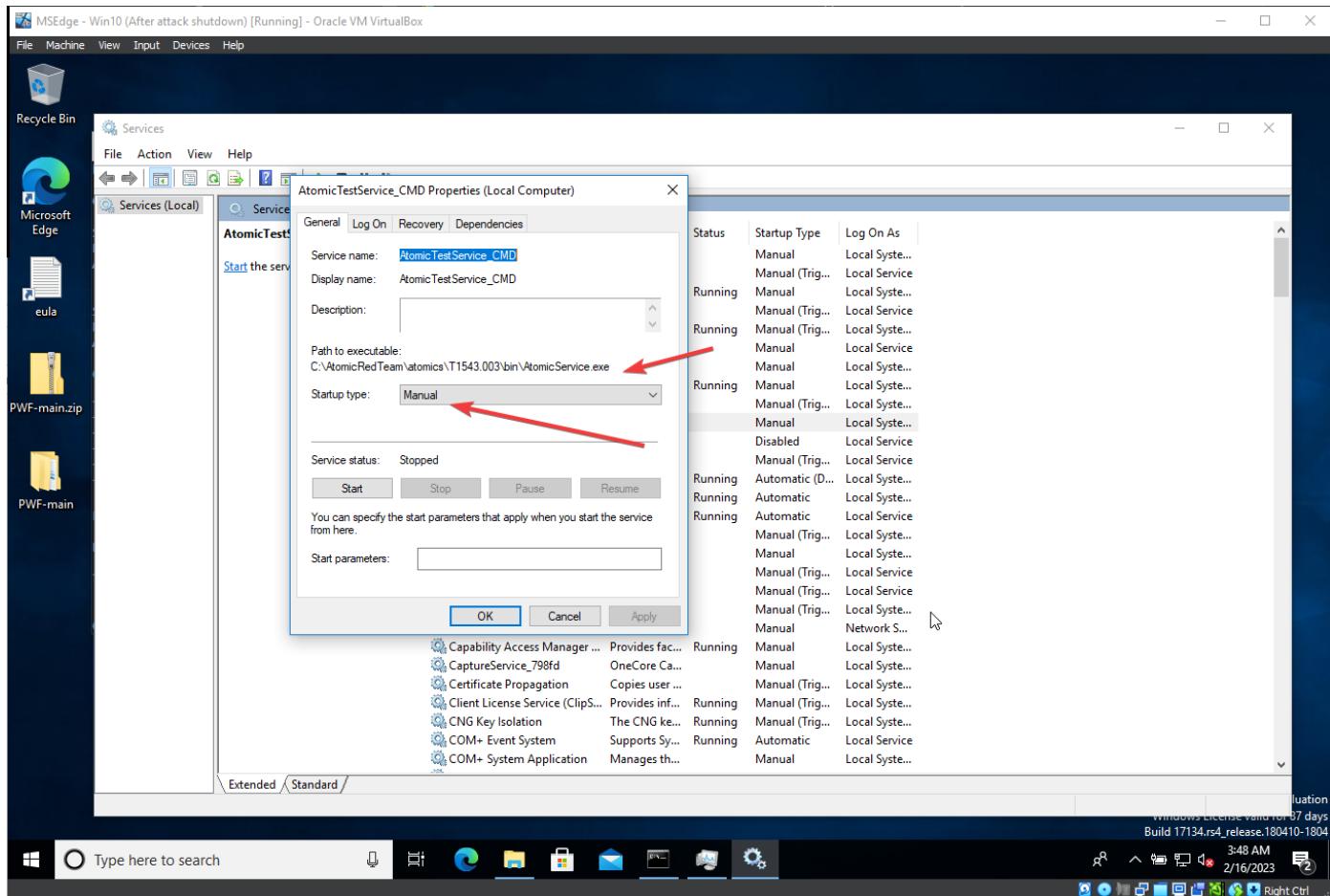
```
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x0029. New Checksum: 0xDC925F1F
'C:\Windows\appcompat\Programs\Amcache.hve' is in use. Rerouting...
Two transaction logs found. Determining primary log...
Primary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG1, secondary log: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
G2
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Windows\appcompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x0029. New Checksum: 0xDC925F1F
C
C:\Windows\appcompat\Programs\Amcache.hve is in new format!
C
Total file entries found: 95
C Total shortcuts found: 51
C Total device containers found: 6
C Total device PnPs found: 51
D Total drive binaries found: 333
D Total driver packages found: 2
D
D Found 48 unassociated file entry
D Results saved to: amcache2/
D Total parsing time: 2.527 seconds
D
D
D C:\>
D USM
D EDP
D EnterpriseMgmt
D ExploitGuard
D Feedback
D File Classification Infrastr
D FileHistory
D HelloFace
```

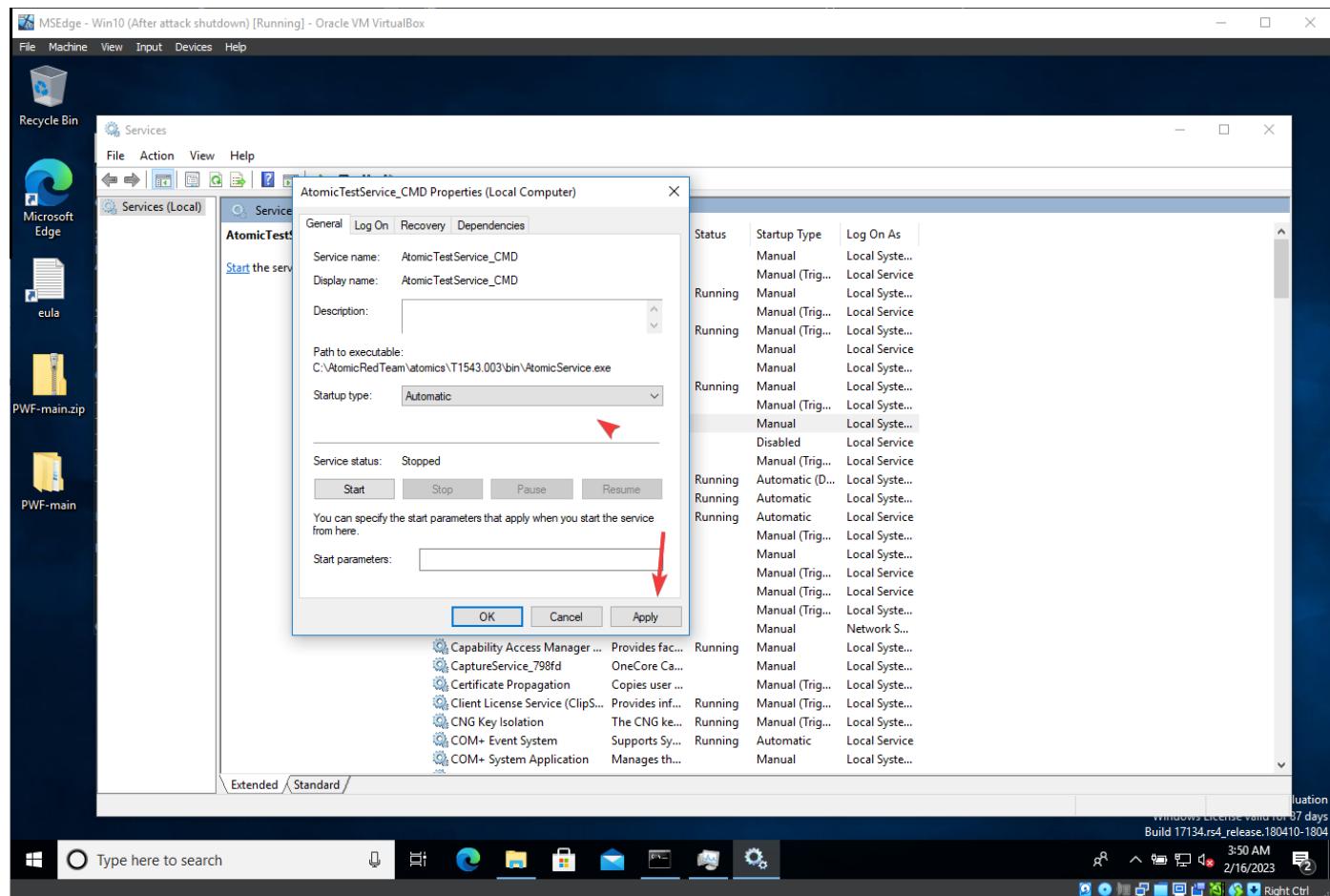
Below the log, there are configuration options for the task:

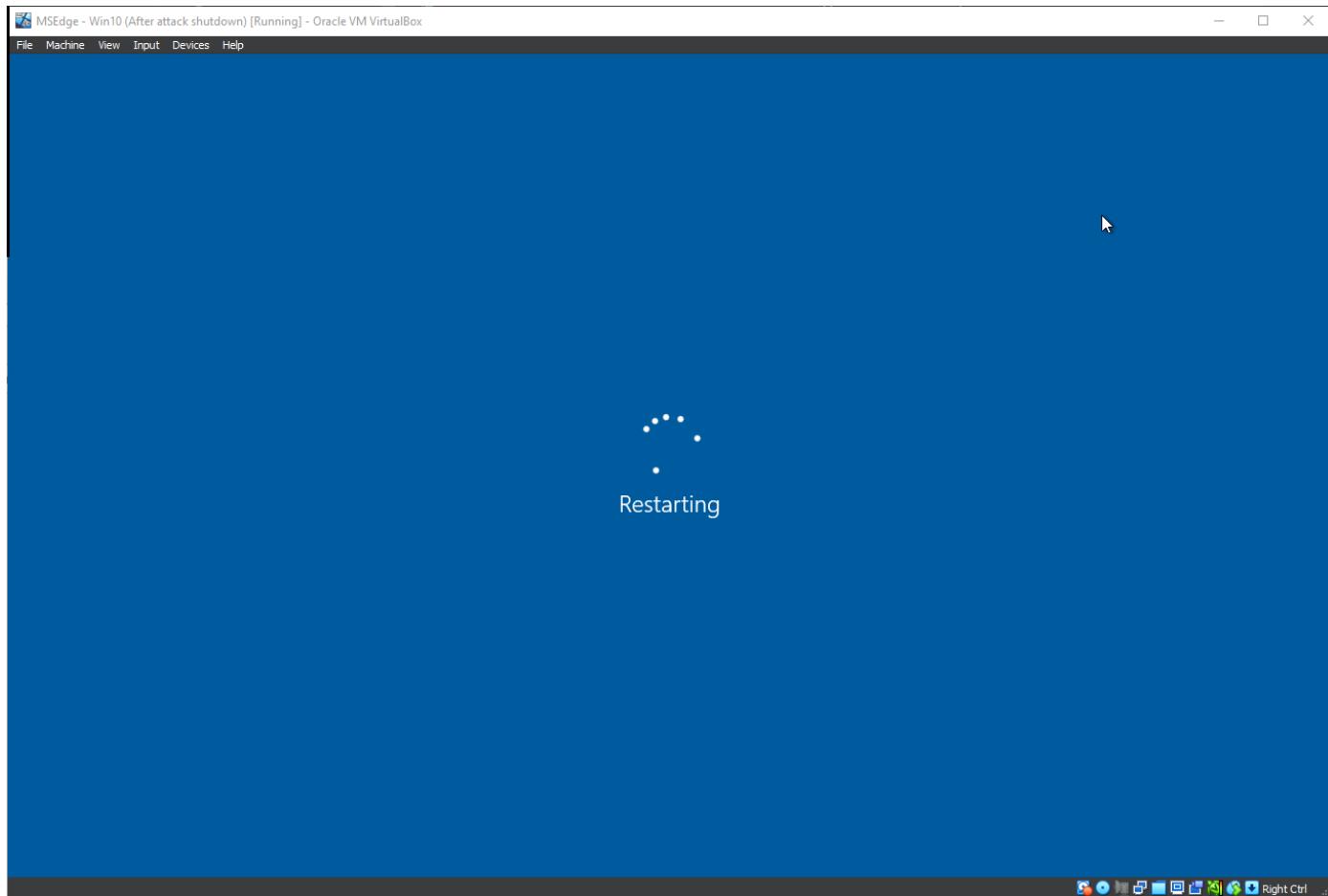
- Run only when user is logged on
- Run whether user is logged on or not (selected)
- Do not store password. The task will only have access to local resources
- Run with highest privileges
- Hidden
- Configure for: Windows 10

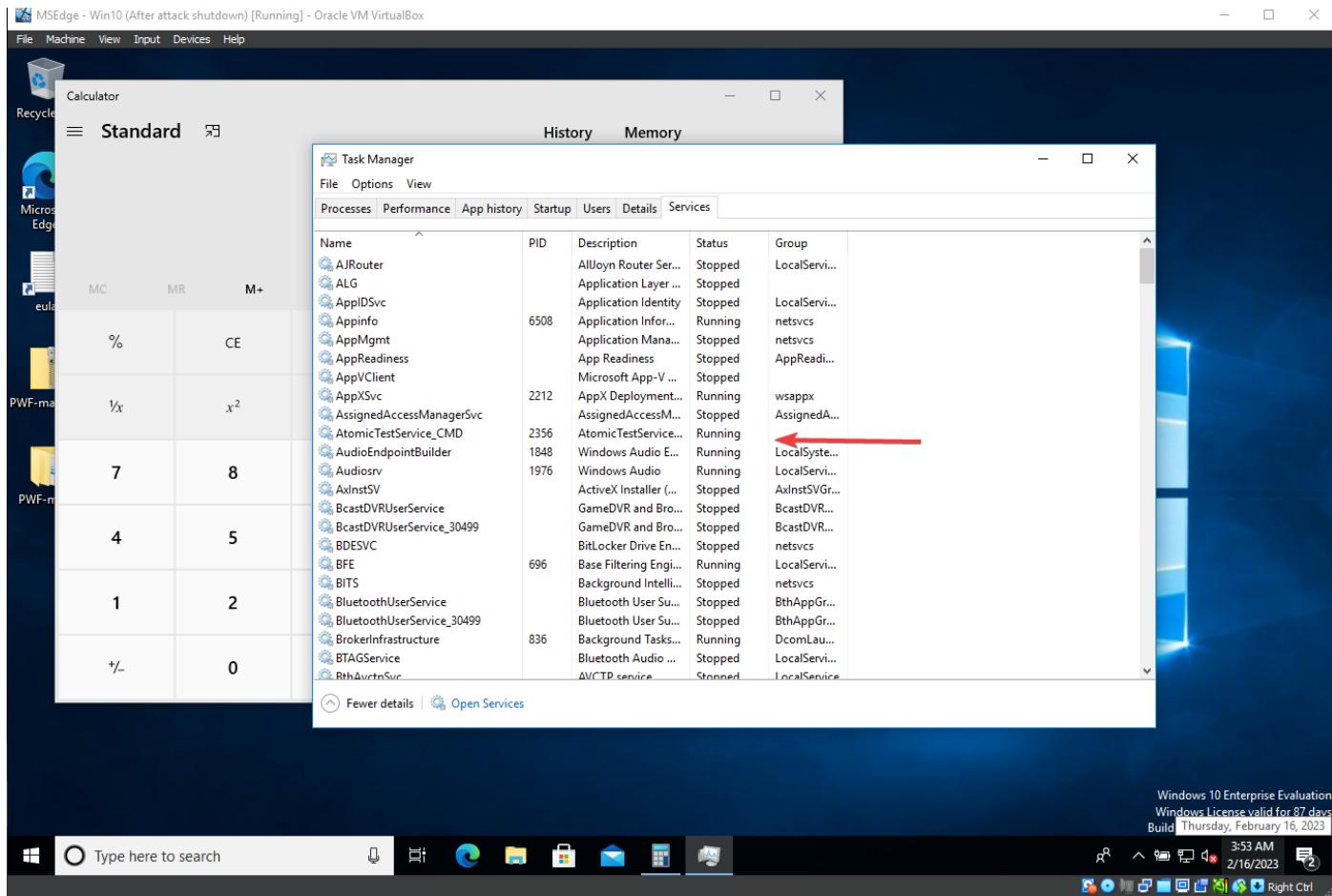
The Actions pane on the right lists various management options for the selected task.

- Still no update.
 - The service is actually loaded, but is set on startup manual. If we change the startup type to automatically and reboot the vm, update the task scheduler, parse the amcache, we should see it.

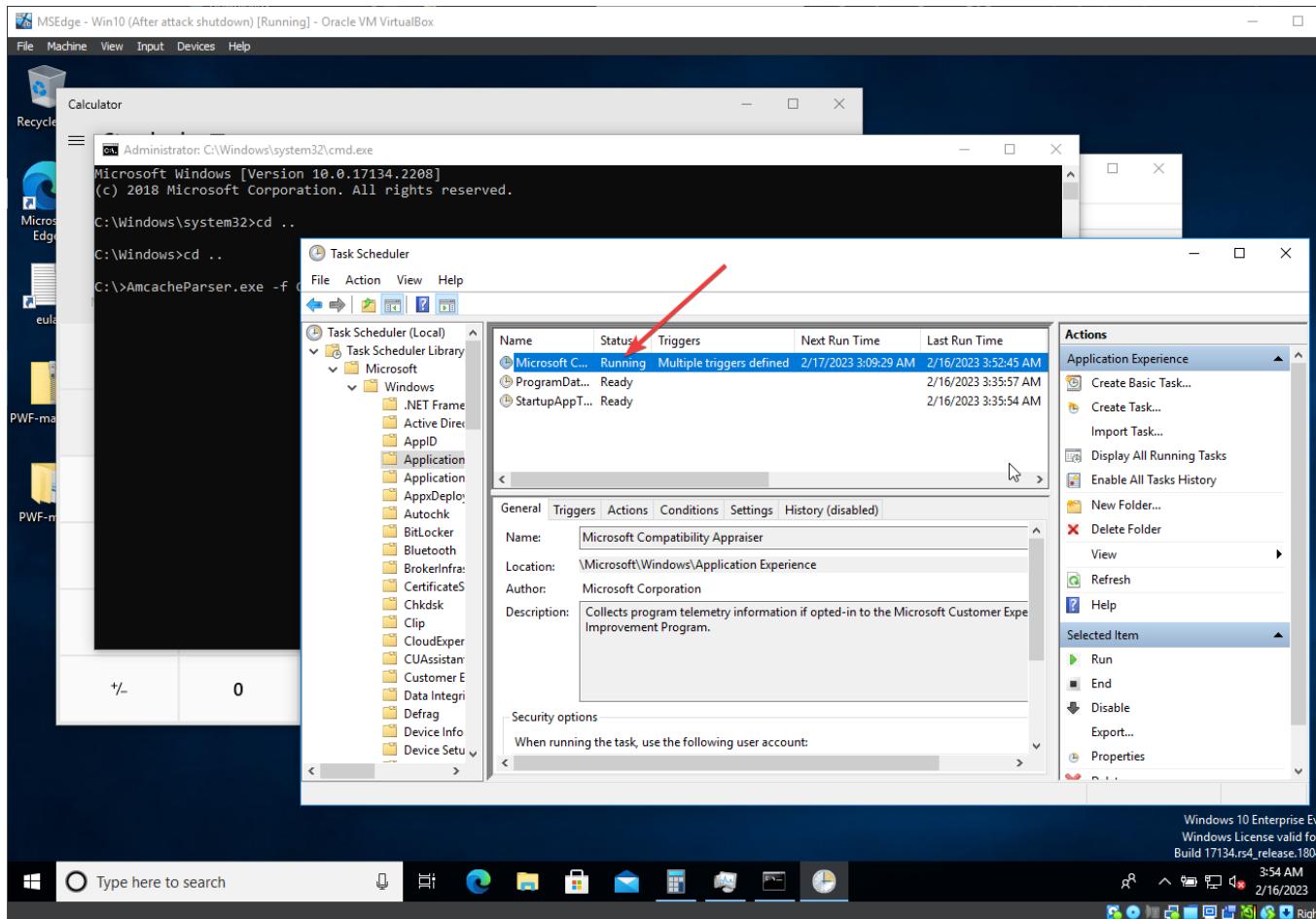




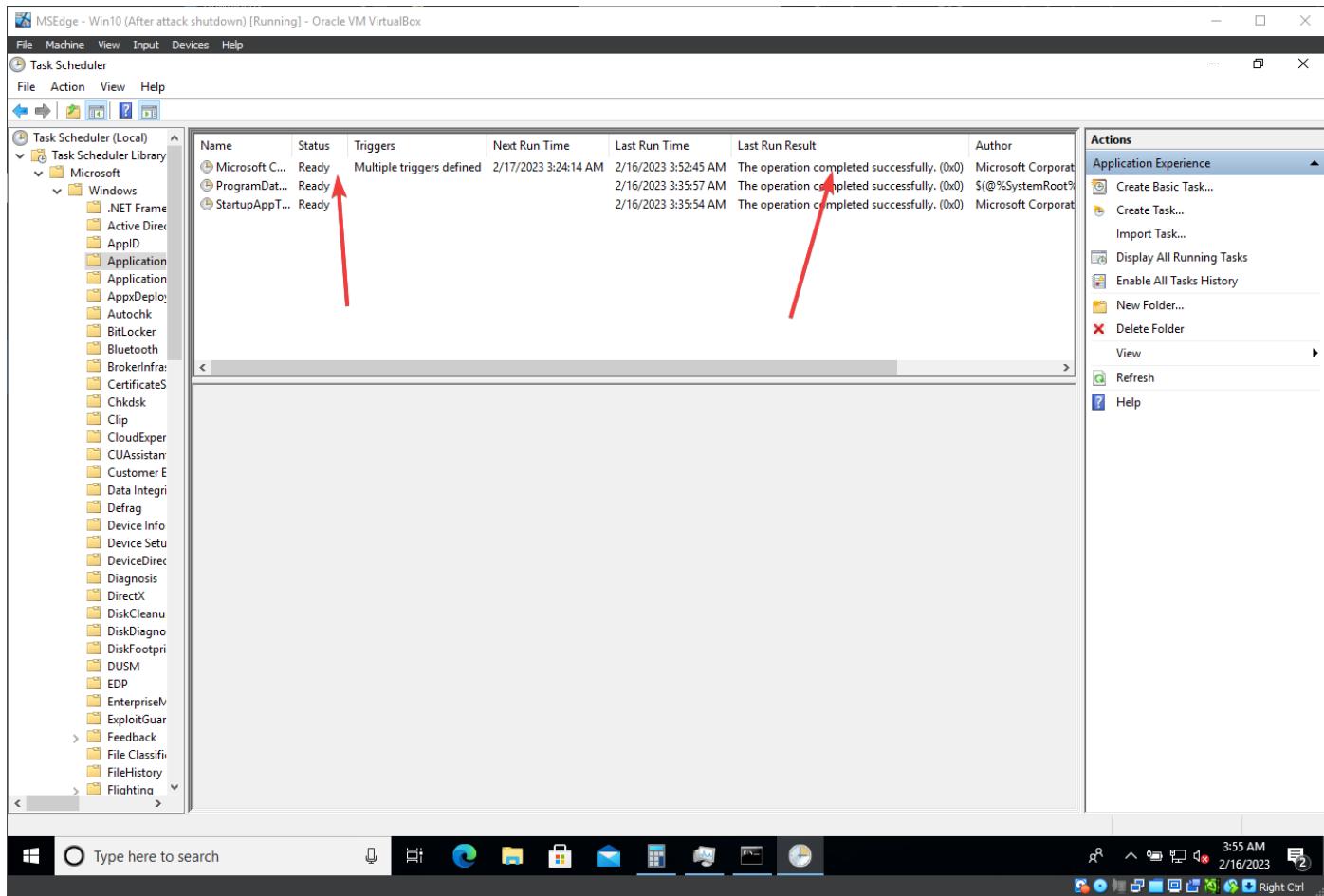




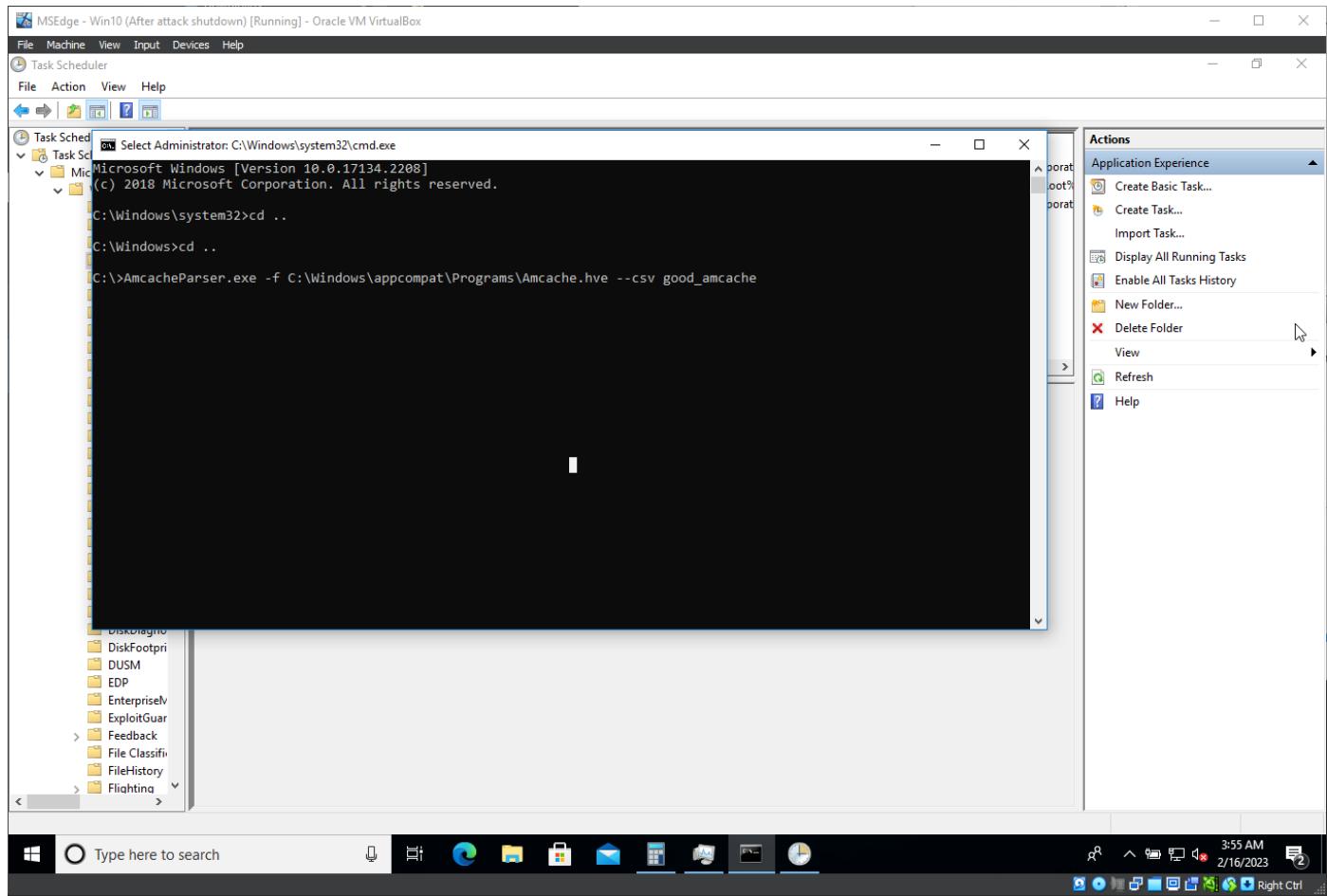
- It is already running.



- We will wait until it finishes.



- Execute:



- Run again:

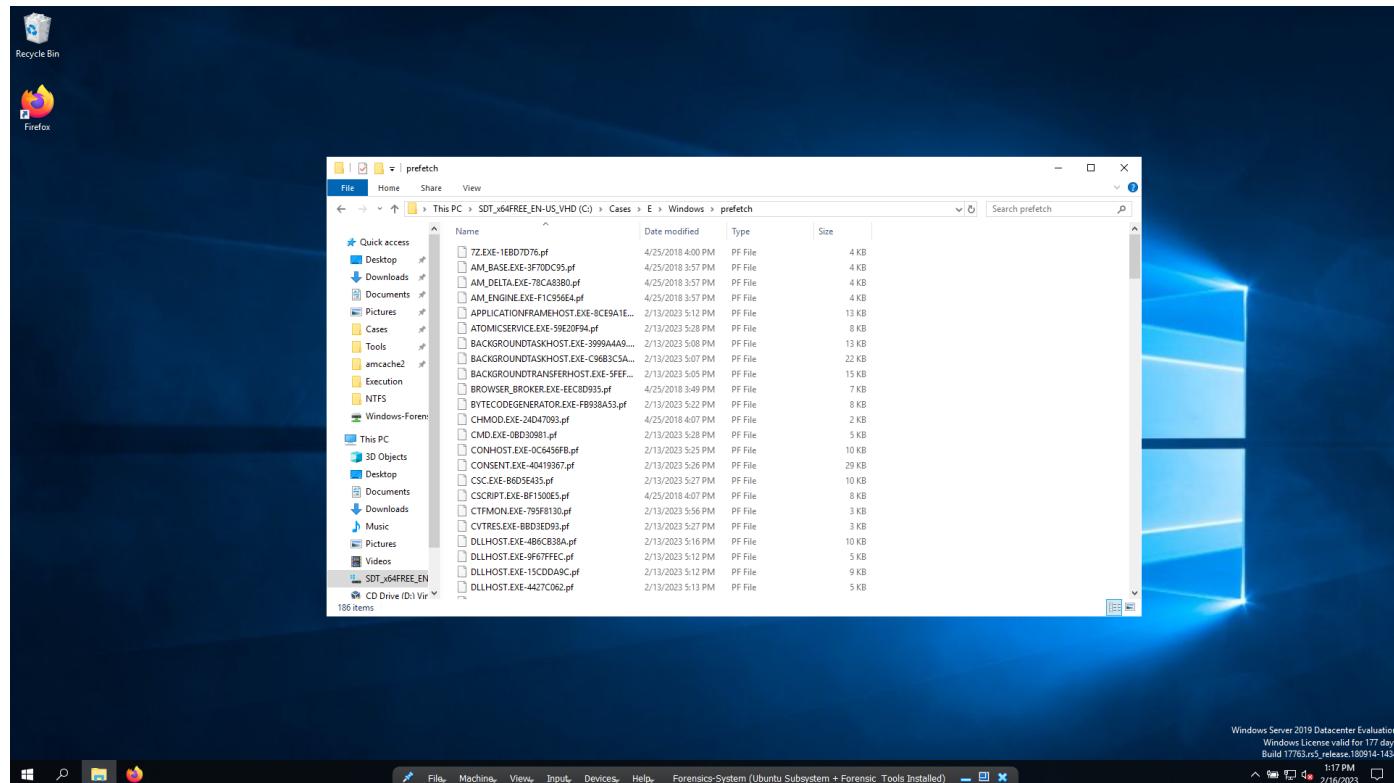
Key	Last Write	Timestamp	SHA1	Is Os Component	Full Path	Name
-02-16	12:34:54	22357fbff60a091df16265032b88f4119e8307e			c:\amcacheparser.exe	amacac
-02-16	12:19:09	e70c1a502ed33fc3ff76977f15169f32cc8a9e5			c:\windows\system32\mrt.exe	mrt.e
-02-16	12:17:55	b76d2e6eb62bf289a5118c908578906851460d0			c:\program files\rempl\osrrb.exe	osrrb.
-02-16	12:17:55	e2e5d4dfebb0ff2bad1d83f72062f816d365bc37			c:\program files\rempl\disktoast.exe	diskto
-02-16	12:16:56	1e919b355171b110b25c908b301efce7727cca99			c:\program files\cuassistant\culauncher.exe	culaur
-02-13	17:27:03	3ef75664261ab9b3d6262132c131da2f4da67c			c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856d364e35_10.0.17134.2207_none_c3d85cec697bbe8\...tiwori	tiwori
-02-13	17:19:25	ab87af56870cfc3b3d280edff7ace8aaabe6a27			c:\windows\system32\musnotification.exe	musnotof
-02-13	17:16:12	e82ac9345fbefc100ff16d6536877592ab2c017			c:\windows\system32\wuauclt.exe	wusuci
-02-13	17:13:32	3d9ee67daddbcf14f48bad70ea19e3de4667c9			c:\program files\rempl\sedsvc.exe	sedsv
-02-13	17:13:32	4e4bd590da1357a750c34d772edef2b1c479ee			c:\program files\rempl\sedlauncher.exe	sedla
-02-13	17:09:09	6ea0ea87cbbc341ba5d3a1be9cb5c40005db02			c:\windows\system32\vboxtray.exe	vboxtr
-02-13	17:09:09	5ac6e790eda19fdc6698648ccb22073c4a2719ba			c:\program files\windows defender\msmpeng.exe	msmpeng
-02-13	17:08:50	b4a549508cbcf9f75a191434d4d20ad3c28d028			c:\users\ieuser\appdata\local\microsoft\edgeupdate\microsoft\edgeupdate.exe	micro
-02-13	17:08:28	57b7fc9bf59cf09a9c19ad0ce0a159746554d682			c:\users\ieuser\appdata\local\microsoft\onedrive\onedrivestandaloneupdater.exe	onedr
-02-13	17:08:01	0e5421e832745a3b285a474ef7afe40d47bf428			c:\windows\system32\sihclient.exe	sihc
-02-13	17:08:00	d0ad161e3d318de58ff9089baed87fece2d768e			c:\windows\system32\unp\updatenotificationmgr.exe	update
-02-13	17:07:59	2a594345fcaad453c2b0d937cf67fb43a74df			c:\windows\system32\taskhost.exe	taskho
-02-13	17:03:44	a108a8ce9a0db502079176fcf81190a1906d5a5b6			c:\programdata\microsoft\windows defender\platform\4.14.17613.18039-0\msmpeng.exe	msmpeng
-04-25	16:07:43	d24e9c6079a20d1ae8d1c409c3fc8e1c63628f3			c:\windows\system32\wlrmldr.exe	wlrm
-04-25	15:58:46	5b205fc1a25354726677a30b25d8e41b3ef69d84			c:\users\ieuser\appdata\local\temp\{7e9b4a05-1664-4b5a-9e13-8bc9a6443a9c}\mpsigtstab.exe	mpsigt
-04-25	15:58:44	5b205fc1a25354726677a30b25d8e41b3ef69d84			c:\users\ieuser\appdata\local\temp\{f976cfa9-2f12-4069-bbc8-3e4f77708c71}\mpsigtstab.exe	mpsigt
-04-25	15:58:40	1ed4ae92d235497ff26210078d51105c4634afade			c:\windows\system32\wermgr.exe	wermgr
-04-25	15:58:37	5b205fc1a25354726677a30b25d8e41b3ef69d84			c:\users\ieuser\appdata\local\temp\{3b66c4bf-6d1d-4725-b71c-e7bd2e7fc27a}\mpsigtstab.exe	mpsigt
-04-25	15:58:33	5b205fc1a25354726677a30b25d8e41b3ef69d84			c:\users\ieuser\appdata\local\temp\{b6b0a99f-46c8-4aa3-8e24-3ace62c25d}\mpsigtstab.exe	mpsigt
-04-25	15:56:30	c1827349741d158c87172b9963fcbe5c3661848			c:\windows\system32\winlogon.exe	winlog
-04-25	15:56:26	7693be70ba30a9659c028c5c8d8c4481c2f89f			c:\windows\system32\dwm.exe	dwm.e
-04-25	15:56:24	0950dd0f72d2e5b78a809f82ead5d8ebe496ff			c:\windows\system32\logonui.exe	logoni
-04-25	15:56:24	f5d0299140c98875b7bd2d892617401dad8b9			c:\windows\explorer.exe	explor
-04-25	15:56:20	2a3bfed90c680fc78e229091b6786aa9f9655aa6b			c:\windows\system32\upfc.exe	upfc.e
-04-25	15:56:20	660b76b6fb02417d51a3dc967c5a77fc2bac6			c:\windows\system32\svchost.exe	svchost
-04-25	15:56:20	e2caded83239ed1be660089217cef11b691b1c110			c:\windows\system32\services.exe	servic
-04-25	15:56:20	786ba7f76fb3c340e7a84f4d7066d7a078439665			c:\windows\system32\csrss.exe	csrss
-04-25	15:56:07	fbffccad3b542e013c1ed056de2840e1a52c0b9			c:\users\ieuser\appdata\local\microsoft\onedrive\onedrive.exe	onedr

- Still no output of execution.
 - o SHA-1 for the AtomicService.exe record.

None

Prefetch

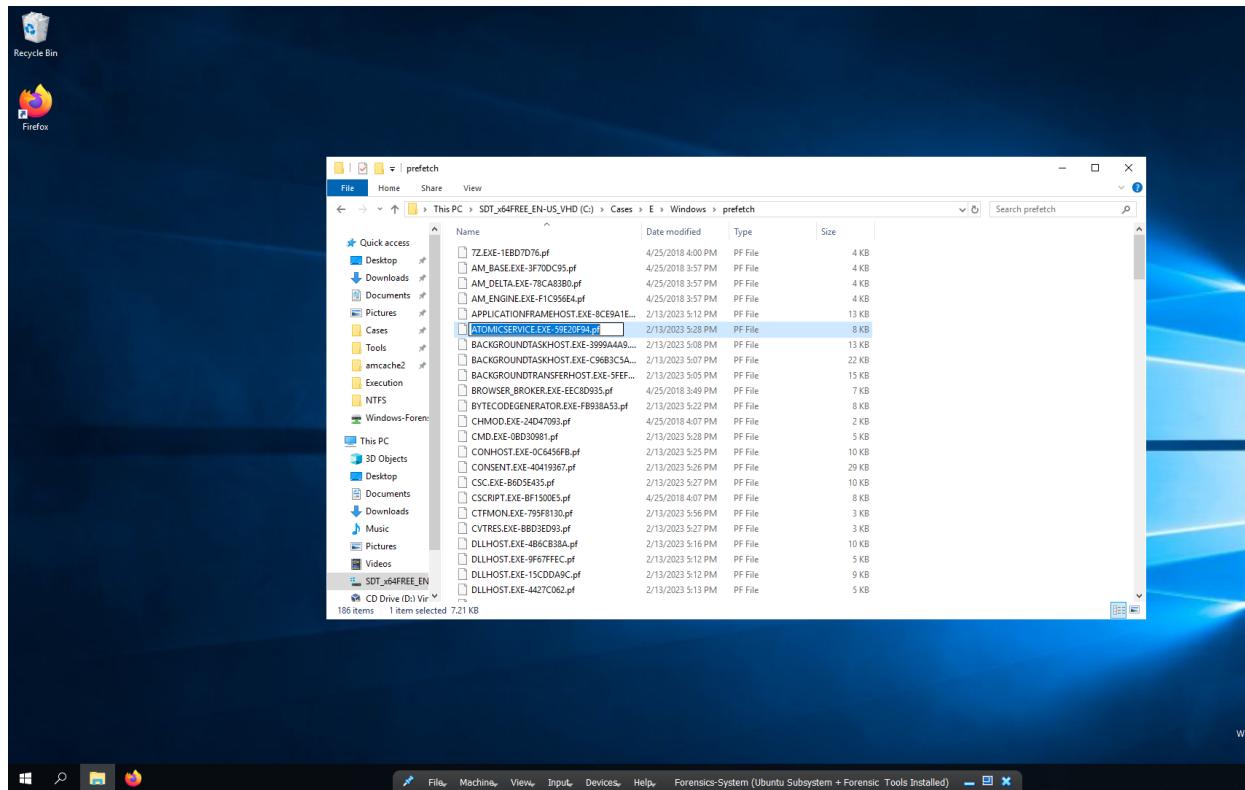
- The prefetch artifact is something that windows stores a prefetch file for every single application that executed.
- Location: C:\Windows\Prefetch*.pf
- Windows does this for preloading the store information from this files, from the disk into the memory to speed up the boots and startups of the applications , improving performance of loading applications .

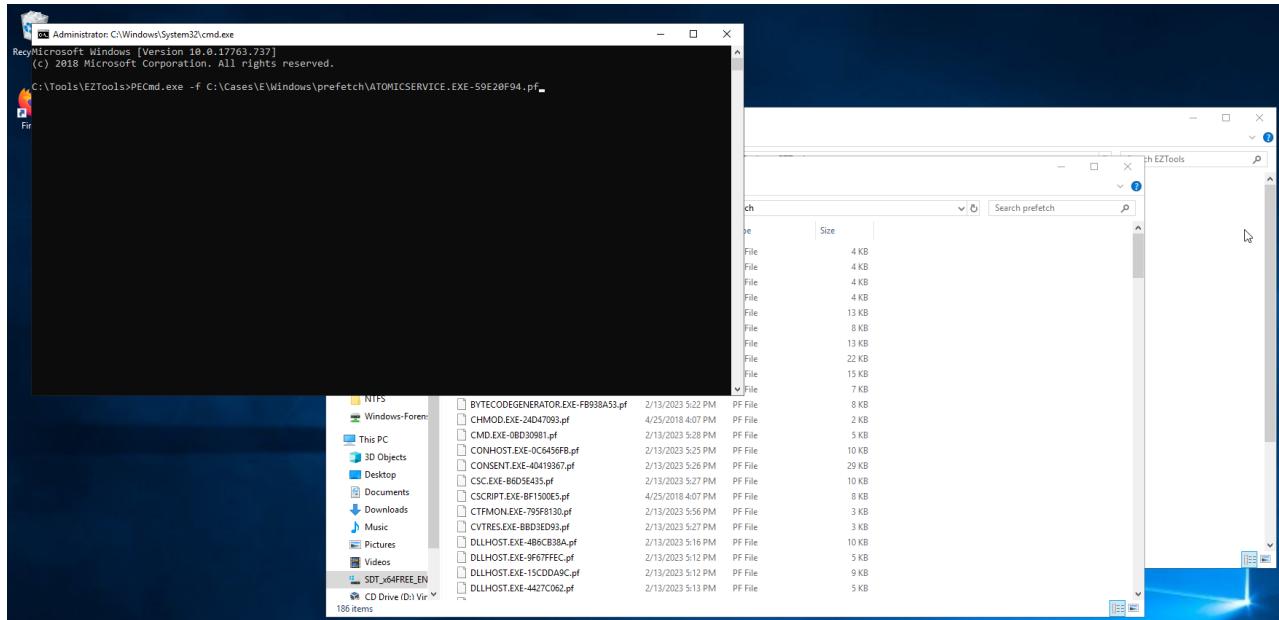


- Format is App-hash of location has been executed from.

- └ 7Z.EXE-1EBD7D76.pf
- └ AM_BASE.EXE-3F70DC95.pf
- └ AM_DELTA.EXE-78CA83B0.pf
- └ AM_ENGINE.EXE-F1C956E4.pf
- └ APPLICATIONFRAMEHOST.EXE-8CE9A1E...
- └ ATOMICSERVICE.EXE-59E20F94.pf
- └ BACKGROUNDTASKHOST.EXE-3999A4A9....
- └ BACKGROUNDTASKHOST.EXE-C96B3C5A...
- └ BACKGROUNDTRANSFERHOST.EXE-5FEF...
- └ BROWSER_BROKER.EXE-EEC8D935.pf
- └ BYTECODEGENERATOR.EXE-FB938A53.pf

- Parsing prefetch file with PECmd





```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\EZTools>PECmd.exe -f C:\Cases\E\Windows\prefetch\ATOMICSERVICE.EXE-59E20F94.pf

Windows Server 2019 Datacenter Evaluation
Windows License valid for 177 days
Build 17763.5_release.180914-1434
1:21 PM 2/16/2023

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 1:21 PM 2/16/2023

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Tools\EZTools>PECmd.exe -f C:\Cases\E\Windows\prefetch\ATOMICSERVICE.EXE-59E20F94.pf
PECmd version 1.5.0.0

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

Command line: -f C:\Cases\E\Windows\prefetch\ATOMICSERVICE.EXE-59E20F94.pf

Keywords: temp, tmp

Processing C:\Cases\E\Windows\prefetch\ATOMICSERVICE.EXE-59E20F94.pf

Created on: 2023-02-13 17:28:38
Modified on: 2023-02-13 17:28:38
Last accessed on: 2023-02-13 17:28:38

Executable name: ATOMICSERVICE.EXE
Hash: 59E20F94
File size (bytes): 33,326
Version: Windows 10 or Windows 11

Run count: 1
Last run: 2023-02-13 17:28:38

Volume information:

#0: Name: \VOLUME{01d3dcba976cd072-3a97874f} Serial: 3A97874F Created: 2018-04-25 16:43:51 Directories: 23 File references: 63

Directories referenced: 23

#0: \VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM
#1: \VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F580DC0D341815D02F34CBF90168017404 (Keyword True)
#2: \VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F580DC0D341815D02F34CBF90168017404\ATOMIC (Keyword True)
#3: \VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F580DC0D341815D02F34CBF90168017404\ATOMIC\T1543.003 (Keyword True)
#4: \VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F580DC0D341815D02F34CBF90168017404\ATOMIC\T1543.003\BIN (Keyword True)
#5: \VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F580DC0D341815D02F34CBF90168017404\ATOMIC\T1543.003\BIN\ (Keyword True)
#6: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS
#7: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\APPATCH
#8: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\ASSEMBLY\PRIVATE
#9: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVE\IMAGES_V4_0_30319_64
#10: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVE\IMAGES_V4_0_30319_64\MSCORLIB
#11: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVE\IMAGES_V4_0_30319_64\MSCORLIB\AC26E2AF62F23E37E645B5E44068A025
#12: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVE\IMAGES_V4_0_30319_64\SYSTEM\SERV798BF78F
#13: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVE\IMAGES_V4_0_30319_64\SYSTEM\SERV798BF78F\SC7510FFEBDB9BD37C8630E8EECDE284A
#14: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVE\IMAGES_V4_0_30319_64\SYSTEM\10A17139182A9EF0561F01FAD09688A5
#15: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\GLOBALIZATION
#16: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\GLOBALIZATION\SORTING
#17: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\MICROSOFT
#18: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\MICROSOFT.NET
#19: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\MICROSOFT.NET\NETFRAMEWORK64
#20: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\MICROSOFT.NET\NETFRAMEWORK64\V4_0_30319
#21: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\MICROSOFT.NET\NETFRAMEWORK64\V4_0_30319\CONFIG
#22: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32

Files referenced: 39

#0: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NTDLL.DLL
#1: \VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F580DC0D341815D02F34CBF90168017404\ATOMIC\T1543.003\BIN\ATOMICSERVICE.EXE (Executable: True)
#2: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\MSCOREE.DLL
#3: \VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\KERNEL32.DLL
```

```

Administrator: C:\Windows\System32\cmd.exe
1: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\SYSTEM
2: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\SYSTEM.SERV759BF878P
3: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\SYSTEM.SERV759BF878P\SC7518FFEDB9BD37C8630E8EECD284A
4: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\SYSTEM\16A17139182A9EFD561F01FADA9688A5
5: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\GLOBALIZATION
6: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\GLOBALIZATION\SORTING
7: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\MICROSOFT.NET
8: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSICLUSION\NETFRAMWORK64
9: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSICLUSION\NETFRAMWORK64\V4_0_30319\CONFIG
10: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSICLUSION\NETFRAMWORK64\V4_0_30319\CONFIG\CONFIG
11: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32
Files referenced: 39
12: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\NTDLL.DLL
13: \VOLUME{013dc4976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F500CD0341815D502F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE (Executable: True)
14: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\MSCOREE.DLL
15: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\KERNEL32.DLL
16: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\COMBASE.DLL
17: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\OLEAUT32.DLL
18: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\APPATCH\SYSMAIN.SOB
19: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\ADWAPI32.DLL
20: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\MSVCR7.DLL
21: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\SEHWRK.DLL
22: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\SHLWAPI.DLL
23: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\MSCOREEI.DLL
24: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\COMBASE.DLL
25: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\UCRTBASE.DLL
26: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\CRYPTBASE.DLL
27: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\CRYPTUI.DLL
28: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\GDI32.DLL
29: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\GDI32FULL.DLL
30: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\MSVCP_WIN.DLL
31: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\USER32.DLL
32: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\WIN32API.DLL
33: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\VERSION.DLL
34: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSICLUSION\CLR.DLL
35: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSICLUSION\MSVCR120_CLR0400.DLL
36: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSICLUSION\NETFRAMWORK64\V4_0_30319\CONFIG\MACHINE.CONFIG
37: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\GLOBALIZATION\SORTDEFAULT.NLS
38: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\MSCORLIB\AC26E2AF62F23E37E645B5E44068A025\MSCORLIB_NI.DLL.AUX
39: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\MSCORLIB\AC26E2AF62F23E37E645B5E44068A025\MSCORLIB_NI.DLL
40: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\SYSTEM32\OLEAUT32.DLL
41: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\SYSTEM.SERV759BF878P\SC7518FFEDB9BD37C8630E8EECD284A\SYSTEM_SERVICEPROCESS_NI.DLL.AUX
42: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\SYSTEM\16A17139182A9EFD561F01FADA9688A5\SYSTEM_NI.DLL
43: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSSEMBLY\NATIVEIMAGES_V4_0_30319_64\SYSTEM.SERV759BF878P\SC7518FFEDB9BD37C8630E8EECD284A\SYSTEM_SERVICEPROCESS_NI.DLL
44: \VOLUME{013dc4976cd072-3a97874f}\WINDOWS\VSICLUSION\NETFRAMWORK64\V4_0_30319\CLRUIT.DLL

----- Processed C:\Cases\E\Windows\prefetch\ATOMICSERVICE.EXE-59E20F94.pf in 0.3431366 seconds -----

C:\Tools\EZTools>

```

- If we have a prefetch file, the creation time will tell us when the program has been executed first:

Created on: 2023-02-13 17:28:38

- Run count tells us how many times did the application executed:

Run count: 1

Last run: 2023-02-13 17:28:30

- Windows keep track of the directories and files referenced by the executable

Prefetch Timeline-Analysis

- We can parse all the prefetch files to understand what happen, on a criminological order.

- #### - Simple output:

Timeline Explorer v1.3.0.0														Enter text to search...			Find	
Line	Tag	Note	Source	Filename	Volume1Seri...	Source Created	Source Modif...	Source Access...	Executable Name	Run Count	Hash	Size	Version	Last Run				
1	□		C:\Cases\E\Windows\prefetch\7Z.EXE-1EBD7D76.pf			2018-04-25 16:00:55	2018-04-25 1...	2018-04-25 16...	7Z.EXE	1	1EBD7D76	17116	Windows	2018-04...				
2	□		C:\Cases\E\Windows\prefetch\AM_BASE.EXE-3F78D9...			2018-04-25 15:57:22	2018-04-25 1...	2023-02-13 17...	AM_BASE.EXE	1	3F78D9C5	12988	Windows	2018-04...				
3	□		C:\Cases\E\Windows\prefetch\AM_DELTA.EXE-78CA83...			2018-04-25 15:57:22	2018-04-25 1...	2023-02-13 17...	AM_DELTA.EXE	1	78CA83B0	13428	Windows	2018-04...				
4	□		C:\Cases\E\Windows\prefetch\AM_ENGINE.EXE-F1C95...			2018-04-25 15:57:22	2018-04-25 1...	2023-02-13 17...	AM_ENGINE.EXE	1	F1C956E4	Windows 10 or Windows 11		2018-04...				
5	□		C:\Cases\E\Windows\prefetch\APPLICATIONFRAMEHOST...			2018-04-25 15:49:54	2023-02-13 1...	2023-02-13 17...	APPLICATIONFRAMEHOST.EXE	3	8CE9A1EE	53614	Windows	2023-02...				
6	□		C:\Cases\E\Windows\prefetch\ATOMICSERVICE.EXE-5...			2023-02-13 17:28:38	2023-02-13 1...	2023-02-13 17...	ATOMICSERVICE.EXE	1	59E20F94	33326	Windows	2023-02...				
7	□		C:\Cases\E\Windows\prefetch\BACKGROUNDTASKHOST....			2023-02-13 17:08:42	2023-02-13 1...	2023-02-13 17...	BACKGROUNDTASKHOST.EXE	1	3999AA0A	56948	Windows	2023-02...				
8	□		C:\Cases\E\Windows\prefetch\BACKGROUNDTASKHOST...			2018-04-25 15:49:54	2023-02-13 1...	2023-02-13 17...	BACKGROUNDTASKHOST.EXE	4	96816C5A	96816	Windows	2023-02...				
9	□		C:\Cases\E\Windows\prefetch\BACKGROUNDTRANSFERH...			2018-04-25 15:54:39	2023-02-13 1...	2023-02-13 17...	BACKGROUNDTRANSFERHOST.EXE	2	5FFEDB8A	71442	Windows	2023-02...				
10	□		C:\Cases\E\Windows\prefetch\BROWSER_BROKER.EXE-...			2018-04-25 15:49:51	2018-04-25 1...	2023-02-13 17...	BROWSER_BROKER.EXE	1	EEDBD935	27394	Windows	2018-04...				
11	□		C:\Cases\E\Windows\prefetch\BYTECODEGENERATOR.E...			2018-04-25 15:57:48	2023-02-13 1...	2023-02-13 17...	BYTECODEGENERATOR.EXE	3	F9B38A53	34494	Windows	2023-02...				
12	□		C:\Cases\E\Windows\prefetch\CHMOD.EXE-24D47093...			2018-04-25 16:07:42	2018-04-25 1...	2018-04-25 16...	CHMOD.EXE	1	24D47093	6846	Windows	2018-04...				
13	□		C:\Cases\E\Windows\prefetch\CMD.EXE-0BD30981.pf			2018-04-25 15:48:11	2023-02-13 1...	2023-02-13 17...	CMD.EXE	12	B030981	14958	Windows	2023-02...				
14	□		C:\Cases\E\Windows\prefetch\CONHOST.EXE-0C6456F...	3A97874F		2018-04-25 15:48:41	2023-02-13 1...	2023-02-13 17...	CONHOST.EXE	16	C6456FB	37036	Windows	2023-02...				
15	□		C:\Cases\E\Windows\prefetch\CONSENT.EXE-4041936...	3A97874F		2023-02-13 17:07:29	2023-02-13 1...	2023-02-13 17...	CONSENT.EXE	8	40419367	128844	Windows	2023-02...				
16	□		C:\Cases\E\Windows\prefetch\CSC.EXE-B605E435.pf			2023-02-13 17:26:56	2023-02-13 1...	2023-02-13 17...	CSC.EXE	2	B605E435	42756	Windows	2023-02...				
17	□		C:\Cases\E\Windows\prefetch\CSRCRIPT.EXE-BF1508E...			2018-04-25 16:07:43	2018-04-25 1...	2018-04-25 16...	CSRCRIPT.EXE	1	B1F508E5	35390	Windows	2018-04...				
18	□		C:\Cases\E\Windows\prefetch\CTFMON.EXE-795F8130...			2018-04-25 15:56:08	2023-02-13 1...	2023-02-13 17...	CTFMON.EXE	6	795F8130	11268	Windows	2023-02...				
19	□		C:\Cases\E\Windows\prefetch\CVTRES.EXE-BBD3E93...			2023-02-13 17:26:56	2023-02-13 1...	2023-02-13 17...	CVTRES.EXE	2	BBD3E93	12162	Windows	2023-02...				
20	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-15CDDA9...			2018-04-25 15:54:44	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	2	15CDCD9C	36266	Windows	2023-02...				
21	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-4427C06...			2018-04-25 16:02:41	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	2	4427C062	19918	Windows	2023-02...				
22	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-486CB38...			2018-04-25 15:48:59	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	9	486CB38A	40844	Windows	2023-02...				
23	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-6389524...			2018-04-25 15:57:33	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	13	6389524F	15066	Windows	2023-02...				
24	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-96F7FF...			2023-02-13 17:12:34	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	1	9F67FFEC	21452	Windows	2023-02...				
25	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-BDFE444...			2018-04-25 16:00:55	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	6	BDFE444C	24540	Windows	2023-02...				
26	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-C60C385...			2018-04-25 15:48:50	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	2	C60C3853	20470	Windows	2023-02...				
27	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-DEF68AB...			2023-02-13 17:07:30	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	2	DEF68AB1	20356	Windows	2023-02...				
28	□		C:\Cases\E\Windows\prefetch\DLHOST.EXE-E9BDD097...			2018-04-25 15:54:39	2023-02-13 1...	2023-02-13 17...	DLHOST.EXE	2	E9BDD097B	15486	Windows	2023-02...				
29	□		C:\Cases\E\Windows\prefetch\DRVINST.EXE-39D9EAC...			2018-04-25 15:52:20	2023-02-13 1...	2023-02-13 17...	DRVINST.EXE	8	39D9EAC7	547956	Windows	2023-02...				
30	□		C:\Cases\E\Windows\prefetch\DSMUSERTASK.EXE-853...			2018-04-25 15:48:47	2018-04-25 1...	2018-04-25 15...	DSMUSERTASK.EXE	1	853A6893	13328	Windows	2018-04...				
31	□		C:\Cases\E\Windows\prefetch\FILECOAUTH.EXE-3E8D...			2018-04-25 16:00:55	2018-04-25 1...	2018-04-25 16...	FILECOAUTH.EXE	1	3E8DF6A8	33072	Windows	2018-04...				
32	□		C:\Cases\E\Windows\prefetch\FILECOAUTH.EXE-6580...			2023-02-13 17:12:18	2023-02-13 1...	2023-02-13 17...	FILECOAUTH.EXE	3	65809F13	41496	Windows	2023-02...				
33	□		C:\Cases\E\Windows\prefetch\FILECOAUTH.EXE-A5D2...			2023-02-13 17:07:07	2023-02-13 1...	2023-02-13 17...	FILECOAUTH.EXE	1	A5D2F7D8	33986	Windows	2023-02...				

- Timeline output:

Timeline Explorer v1.3.0.0														Enter text to search...			Find	
Line	Run Time	Executable Name																
1	2018-04-25 16:00:31	\VOLUME{01d3dcba976cd072-3a97874f}\PROGRAM FILES (X86)\7-ZIP\7Z.EXE																
2	2018-04-25 15:57:14	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SOFTWARE DISTRIBUTION\DOWNLOAD\INSTALL\AM_BASE.EXE																
3	2018-04-25 15:57:18	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SOFTWARE DISTRIBUTION\DOWNLOAD\INSTALL\AM_DELTA.EXE																
4	2018-04-25 15:57:12	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SOFTWARE DISTRIBUTION\DOWNLOAD\INSTALL\AM_ENGINE.EXE																
5	2023-02-13 17:11:38	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\APPLICATIONFRAMEHOST.EXE																
6	2018-04-25 15:56:49	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\APPLICATIONFRAMEHOST.EXE																
7	2018-04-25 15:49:44	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\APPLICATIONFRAMEHOST.EXE																
8	2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BACKGROUND TASKHOST.EXE																
9	2023-02-13 17:08:45	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BACKGROUND TRANSFERHOST.EXE																
10	2023-02-13 17:06:50	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BACKGROUND TASKHOST.EXE																
11	2018-04-25 15:56:49	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BACKGROUND TASKHOST.EXE																
12	2018-04-25 15:54:39	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BACKGROUND TASKHOST.EXE																
13	2018-04-25 15:49:44	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BACKGROUND TASKHOST.EXE																
14	2023-02-13 17:05:18	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BACKGROUND TRANSFERHOST.EXE																
15	2018-04-25 15:54:37	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BACKGROUND TRANSFERHOST.EXE																
16	2018-04-25 15:49:44	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BROWSER_BROKER.EXE																
17	2023-02-13 17:23:35	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BYTECODEGENERATOR.EXE																
18	2023-02-13 17:07:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BYTECODEGENERATOR.EXE																
19	2018-04-25 15:57:48	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\BYTECODEGENERATOR.EXE																
20	2018-04-25 16:07:42	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE																
21	2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE																
22	2018-04-25 16:07:42	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE																
23	2018-04-25 16:03:38	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE																
24	2018-04-25 16:03:38	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE																
25	2018-04-25 16:00:34	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE																
26	2018-04-25 16:00:31	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE																
27	2018-04-25 15:56:05	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE																
28	2018-04-25 15:53:59	\VOLUME{01d3dcba976cd072-3a9																

Line	Tag	Run Time	Executable Name
48		2023-02-13 17:56:57	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CTFMON.EXE
243		2023-02-13 17:56:58	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE
241		2023-02-13 17:56:58	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE
231		2023-02-13 17:56:49	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE
221		2023-02-13 17:56:49	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE
338		2023-02-13 17:58:47	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SVCHOST.EXE
450		2023-02-13 17:29:06	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
109		2023-02-13 17:29:06	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
451		2023-02-13 17:29:05	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
110		2023-02-13 17:29:05	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
452		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
181		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
164		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NOTE PAD.EXE
120		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WAVINJECT.EXE
111		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
256		2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE
255		2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE
8		2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMI...
453		2023-02-13 17:28:29	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
112		2023-02-13 17:28:29	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
454		2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
261		2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE
260		2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE
113		2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
182		2023-02-13 17:28:25	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
455		2023-02-13 17:28:24	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
114		2023-02-13 17:28:24	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
456		2023-02-13 17:28:22	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
191		2023-02-13 17:28:22	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE
115		2023-02-13 17:28:22	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
192		2023-02-13 17:28:19	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE
183		2023-02-13 17:28:19	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
457		2023-02-13 17:28:18	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
116		2023-02-13 17:28:18	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE

Total lines 488 | Visible lines 488 | Open files: 1 | Search options
C:\Cases\Analysis\Execution\20230216132921_PECmd_Output_Timeline.csv

File Tools Tabs View Help File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 133 PM 2/16/2023

- Included in attack timeline:

Line	Tag	Run Time	Executable Name
450		2023-02-13 17:29:06	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
109		2023-02-13 17:29:06	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
451		2023-02-13 17:29:05	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
110		2023-02-13 17:29:05	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
452		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
181		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
164		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NOTE PAD.EXE
120		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WAVINJECT.EXE
111		2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
256		2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE
255		2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE
8		2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMI...
453		2023-02-13 17:28:29	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
112		2023-02-13 17:28:29	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
454		2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
261		2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE
260		2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE
113		2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
182		2023-02-13 17:28:25	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
455		2023-02-13 17:28:24	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
114		2023-02-13 17:28:24	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
456		2023-02-13 17:28:22	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
191		2023-02-13 17:28:22	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE
115		2023-02-13 17:28:22	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
192		2023-02-13 17:28:19	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE
183		2023-02-13 17:28:19	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE
457		2023-02-13 17:28:18	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WHOAMI.EXE
116		2023-02-13 17:28:18	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\HOSTNAME.EXE
160		2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE
159		2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE
158		2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE
155		2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE
154		2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE
153		2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE

Total lines 488 | Visible lines 488 | Open files: 1 | Search options
C:\Cases\Analysis\Execution\20230216132921_PECmd_Output_Timeline.csv

File Tools Tabs View Help File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 134 PM 2/16/2023

- We will select the executables that has been active at the time of the attack:

Line	Run Time	Executable Name
164	2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NOTE PAD.EXE
120	2023-02-13 17:28:32	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\MAVINJECT.EXE
256	2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE
255	2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE
8	2023-02-13 17:28:30	\VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE
261	2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE
260	2023-02-13 17:28:27	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE
191	2023-02-13 17:28:22	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE
192	2023-02-13 17:28:19	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE
166	2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE
159	2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE
158	2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE
155	2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE
154	2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE
153	2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE
21	2023-02-13 17:28:16	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE
184	2023-02-13 17:28:11	\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE

- Executing Ascending – order

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NOTE PAD.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\MAVINJECT.EXE

- Suspicious mavinject at the same timeframe as notepad.exe , this tool is usually used by attackers to inject code into processes.

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE

- Suspicious SC.exe is used to create windows services.

\VOLUME{01d3dcba976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE

- Suspicious ATOMICSERVICE.EXE executed, at the same timeframe as SC.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE

- Suspicious modifying or creating tasks.

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE

- Suspicious REG execution.

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE

- Suspicious NET and NET1 execution.

\VOLUME{01d3dcba976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE

- Suspicious cmd execution.

\VOLUME{01d3dcba976cd072-

3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE

- Suspicious powershell execution