Evidence of program execution:

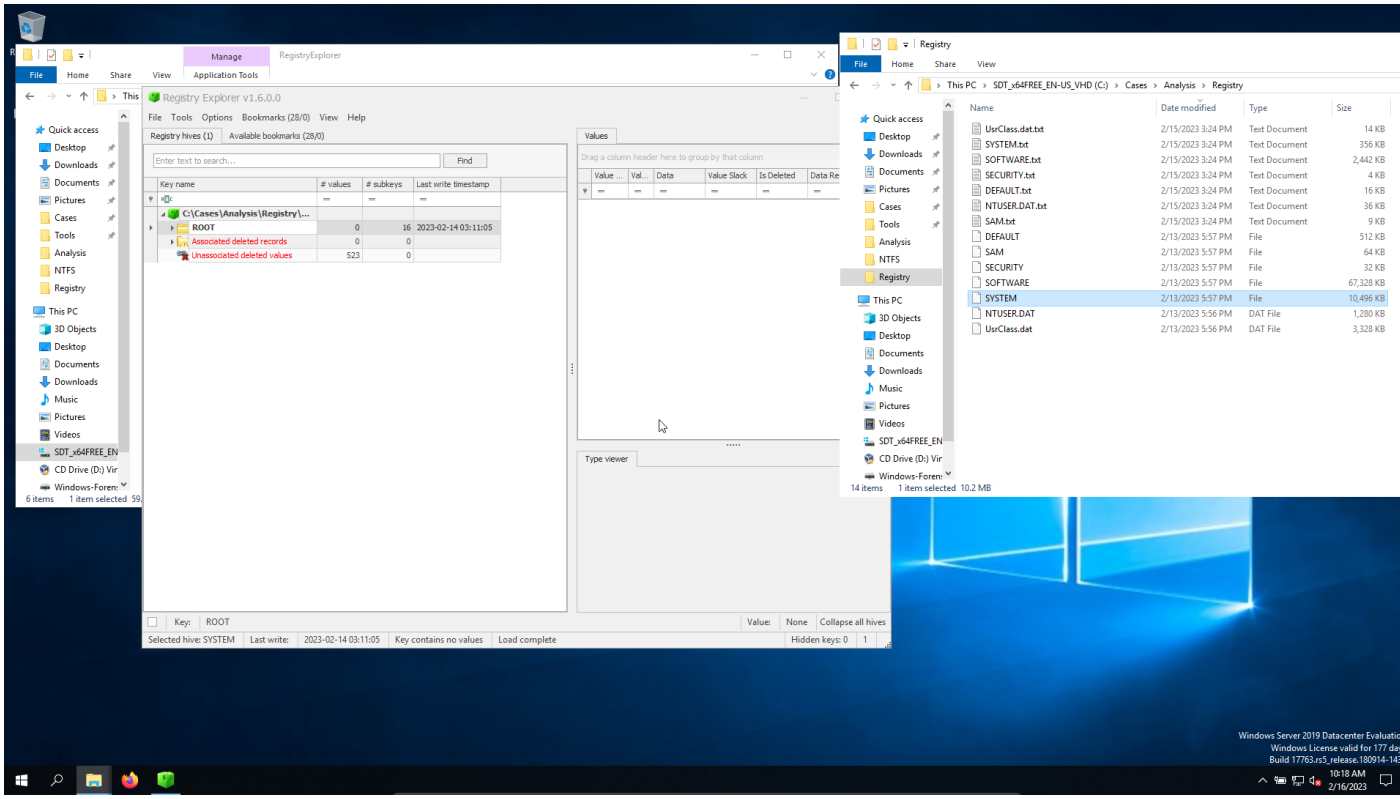
- Execution artifacts:
  - Background Activity Moderator (BAM)
  - Application Compatibility Cache (ShimCache)
  - Amcache
  - Prefetch
  - Prefetch Timeline-Analysis

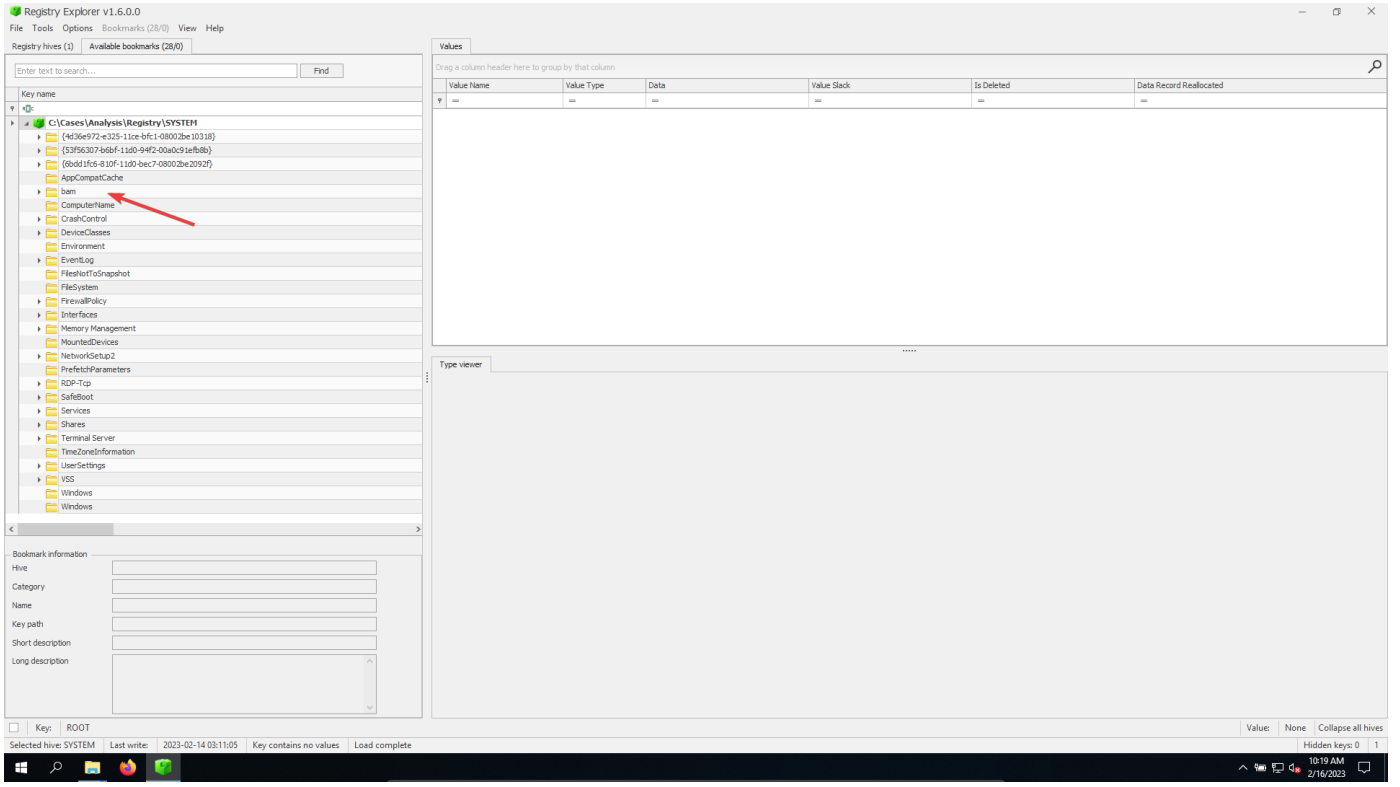
- Find :
  - What executables did BAM recorded for the user IEUser? Print execution date and time.
  - Cache entry position for:
    - AtomicService.exe
    - Mavinject.exe
  - SHA-1 for the AtomicService.exe record.

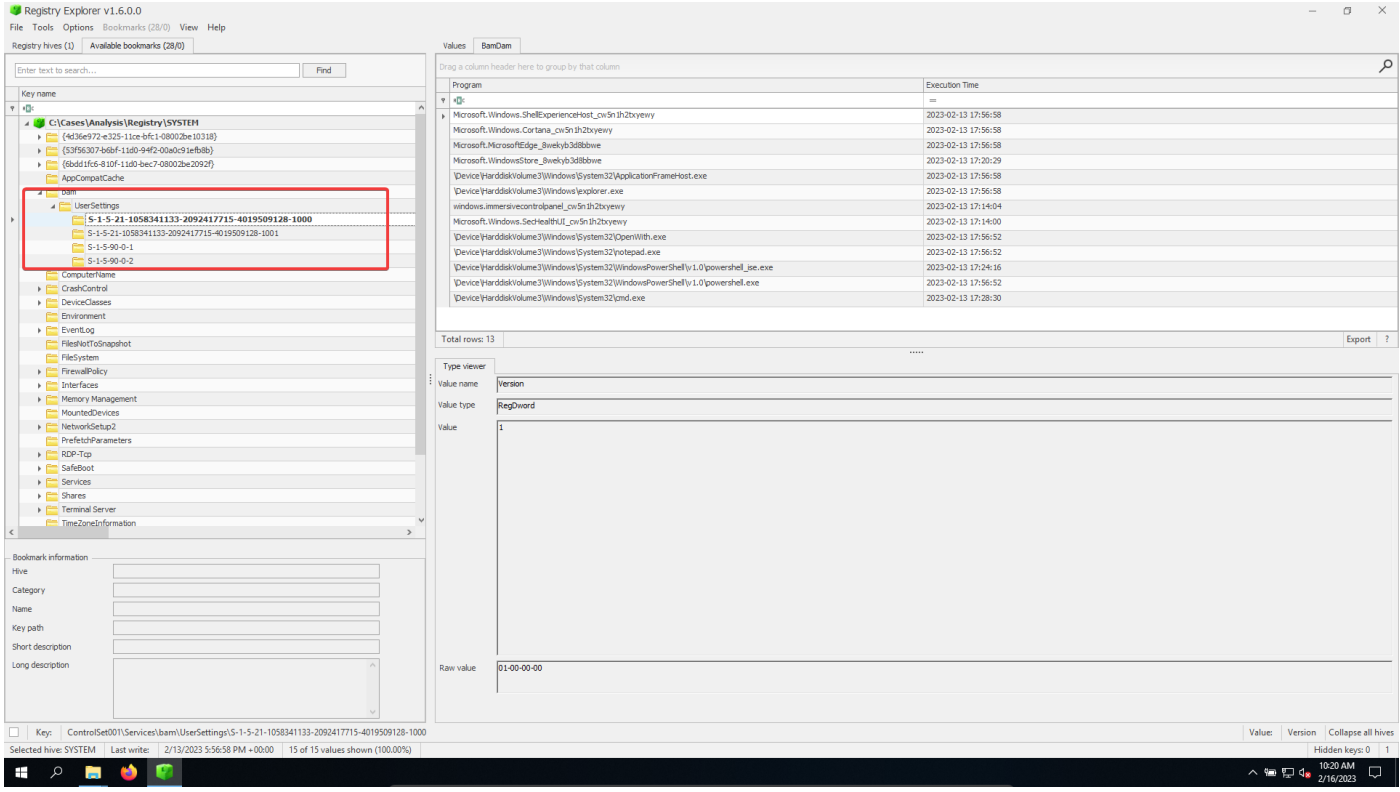
Background Activity Moderator (BAM)

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

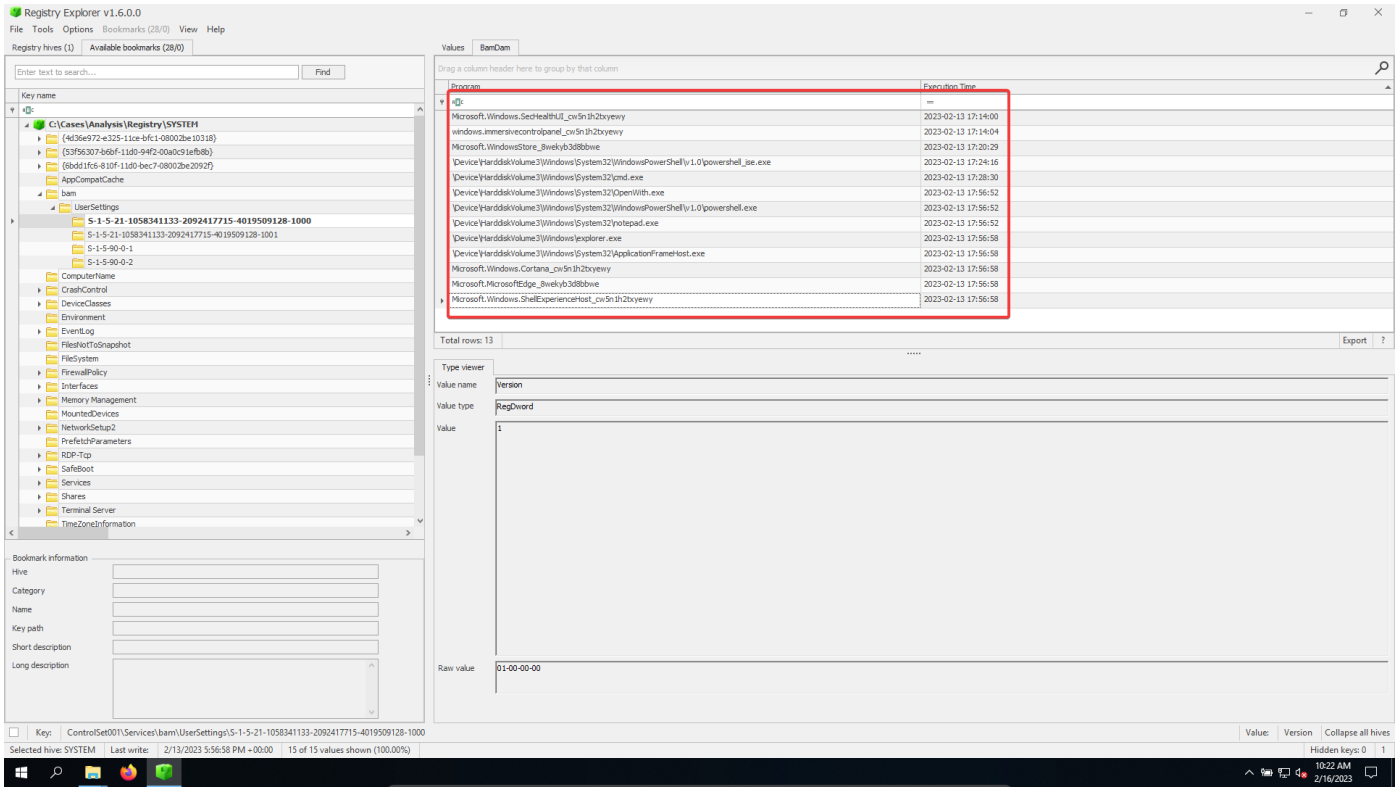
- FThe BAM records information about executables that have been ran on a system
- Open RegistryExplorer and upload SYSTEM registry hive:


Registry Explorer v1.6.0.0
File Tools Options Bookmarks (28/0) View Help
Registry hives (1)
Available bookmarks (28/0)
Enter text to search...
Find
Key name
values
subkeys
Last write timestamp
C:\Cases\Analysis\Registry\...
ROOT
Associated deleted records
Unassociated deleted values
Values
Drag a column header here to group by that column
Value ...
Val...
Data
Value Slack
Is Deleted
Data Re
Type viewer
Key: ROOT
Value: None
Collapse all hives
Selected hive: SYSTEM
Last write: 2023-02-14 03:11:05
Key contains no values
Load complete
Hidden keys: 0
Registry
This PC > SDT_x64FREE_EN-US_VHD (C:) > Cases > Analysis > Registry
Name
Date modified
Type
Size
UsrClass.dat.txt 2/15/2023 3:24 PM Text Document 14 KB
SYSTEM.txt 2/15/2023 3:24 PM Text Document 356 KB
SOFTWARE.txt 2/15/2023 3:24 PM Text Document 2,442 KB
SECURITY.txt 2/15/2023 3:24 PM Text Document 4 KB
DEFAULT.txt 2/15/2023 3:24 PM Text Document 16 KB
NTUSER.DAT.txt 2/15/2023 3:24 PM Text Document 36 KB
SAM.txt 2/15/2023 3:24 PM Text Document 9 KB
DEFAULT 2/13/2023 5:57 PM File 512 KB
SAM 2/13/2023 5:57 PM File 64 KB
SECURITY 2/13/2023 5:57 PM File 32 KB
SOFTWARE 2/13/2023 5:57 PM File 67,328 KB
SYSTEM 2/13/2023 5:57 PM File 10,496 KB
NTUSER.DAT 2/13/2023 5:56 PM DAT File 1,280 KB
UsrClass.dat 2/13/2023 5:56 PM DAT File 3,328 KB
14 items 1 item selected 10.2 MB
Windows Server 2019 Datacenter Evaluation
Windows License valid for 177 days
Build 17763.rs5_release.180914-1434
10:18 AM
2/16/2023

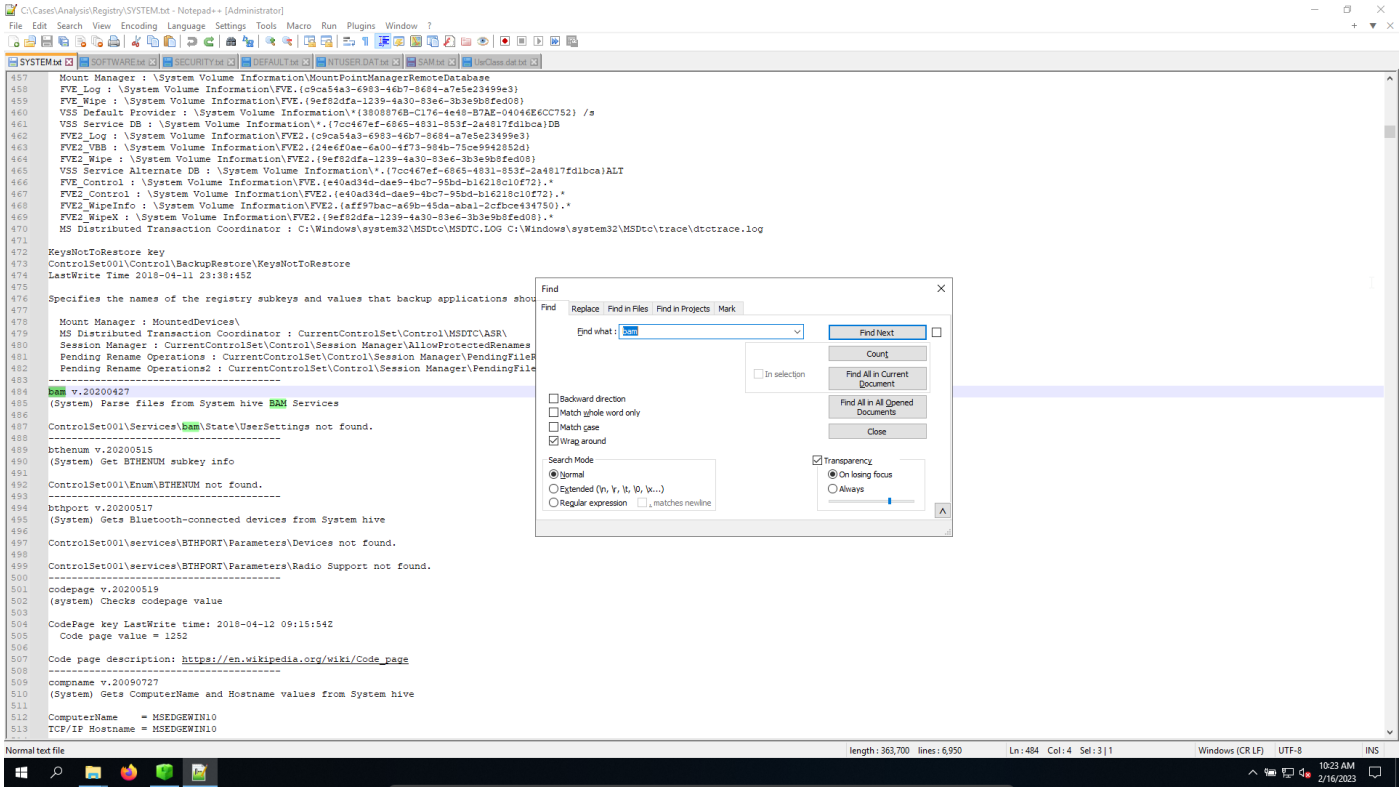

Registry Explorer v1.6.0.0
File Tools Options Bookmarks (28/0) View Help
Registry hives (1)
Available bookmarks (28/0)
Enter text to search...
Find
Key name
C:\Cases\Analysis\Registry\SYSTEM
{4d36e972-e325-11ce-bfc1-08002be10318}
{53f56307-b6bf-11d0-94f2-00a0c91efb8b}
{6bdd1fc6-810f-11d0-bec7-08002be2092f}
AppCompatCache
bam
ComputerName
CrashControl
DeviceClasses
Environment
EventLog
FilesNotToSnapshot
FileSystem
FirewallPolicy
Interfaces
Memory Management
MountedDevices
NetworkSetup2
PrefetchParameters
RDP-Tcp
SafeBoot
Services
Shares
Terminal Server
TimeZoneInformation
UserSettings
VSS
Windows
Windows
Bookmark information
Hive
Category
Name
Key path
Short description
Long description
Values
Drag a column header here to group by that column
Value Name
Value Type
Data
Value Slack
Is Deleted
Data Record Reallocated
Type viewer
Key: ROOT
Value: None
Collapse all hives
Selected hive: SYSTEM
Last write: 2023-02-14 03:11:05
Key contains no values
Load complete
Hidden keys: 0
10:19 AM
2/16/2023



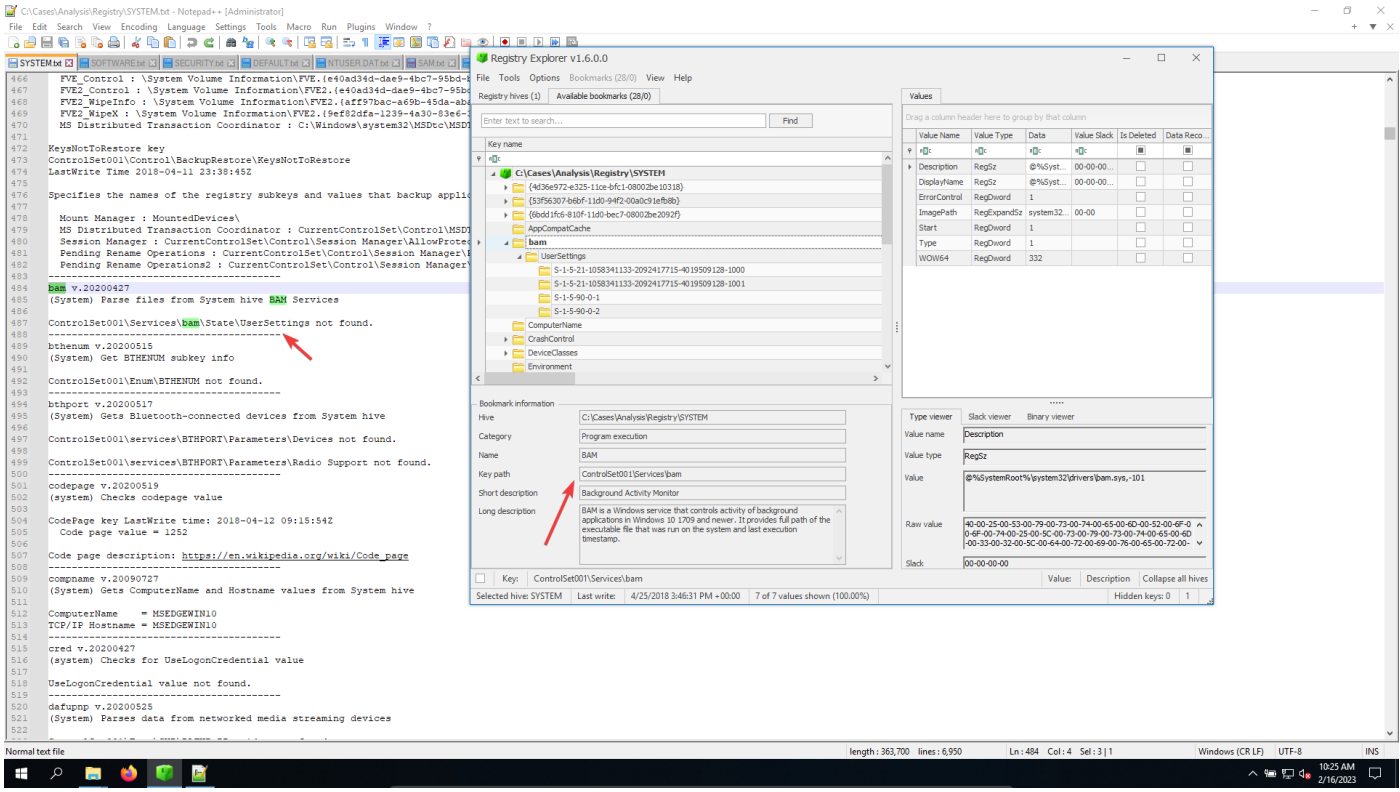
- These programs ran untill the shutdown of the system.



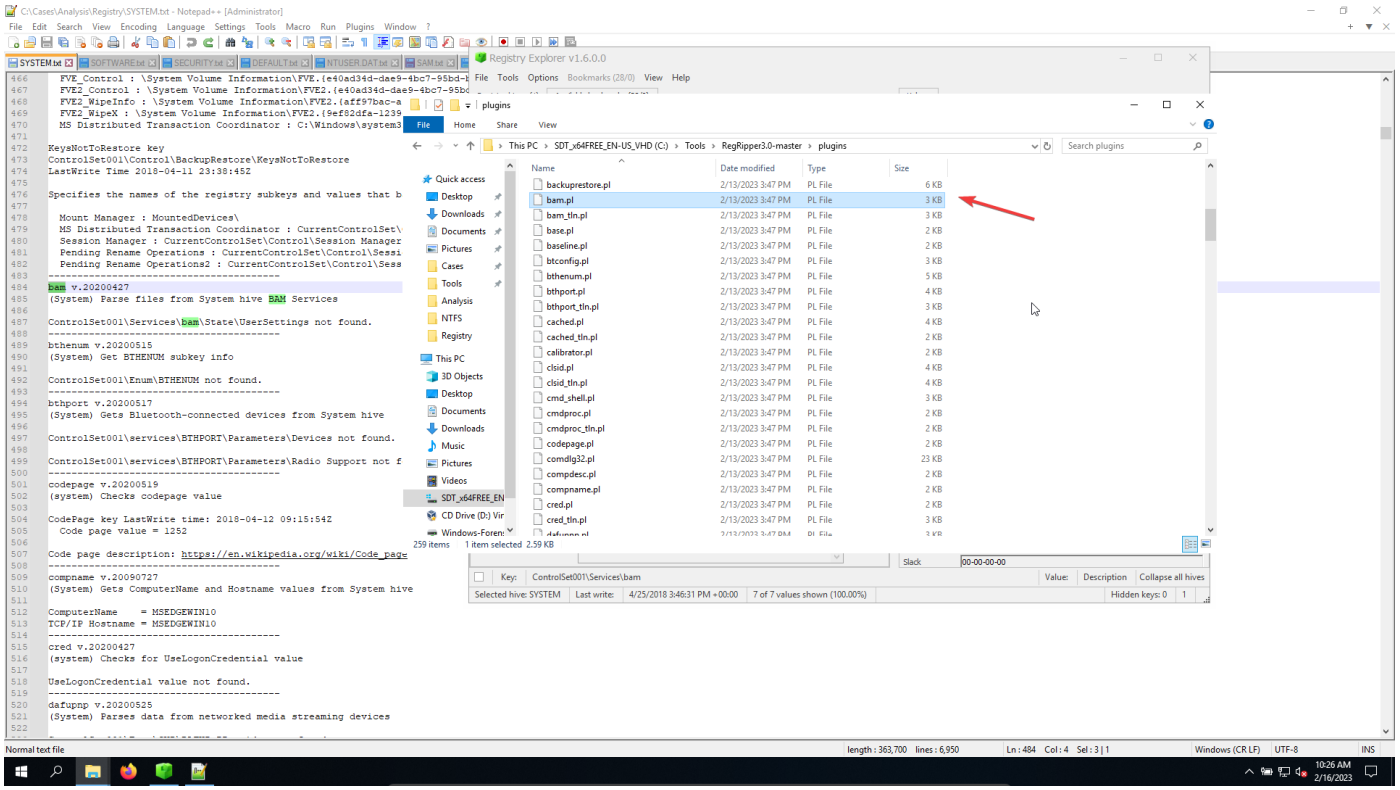
- You can use the .txt files too, it is easier to view or copy and paste.

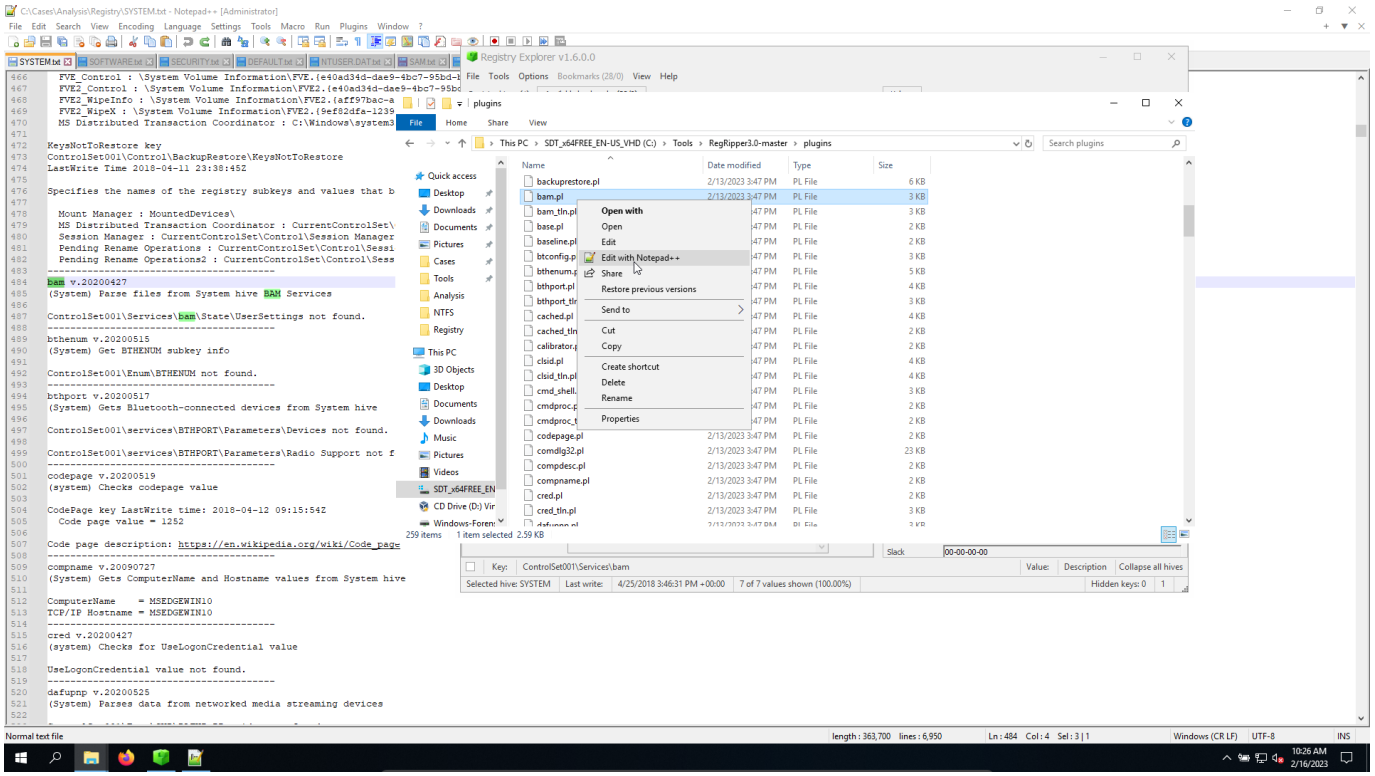


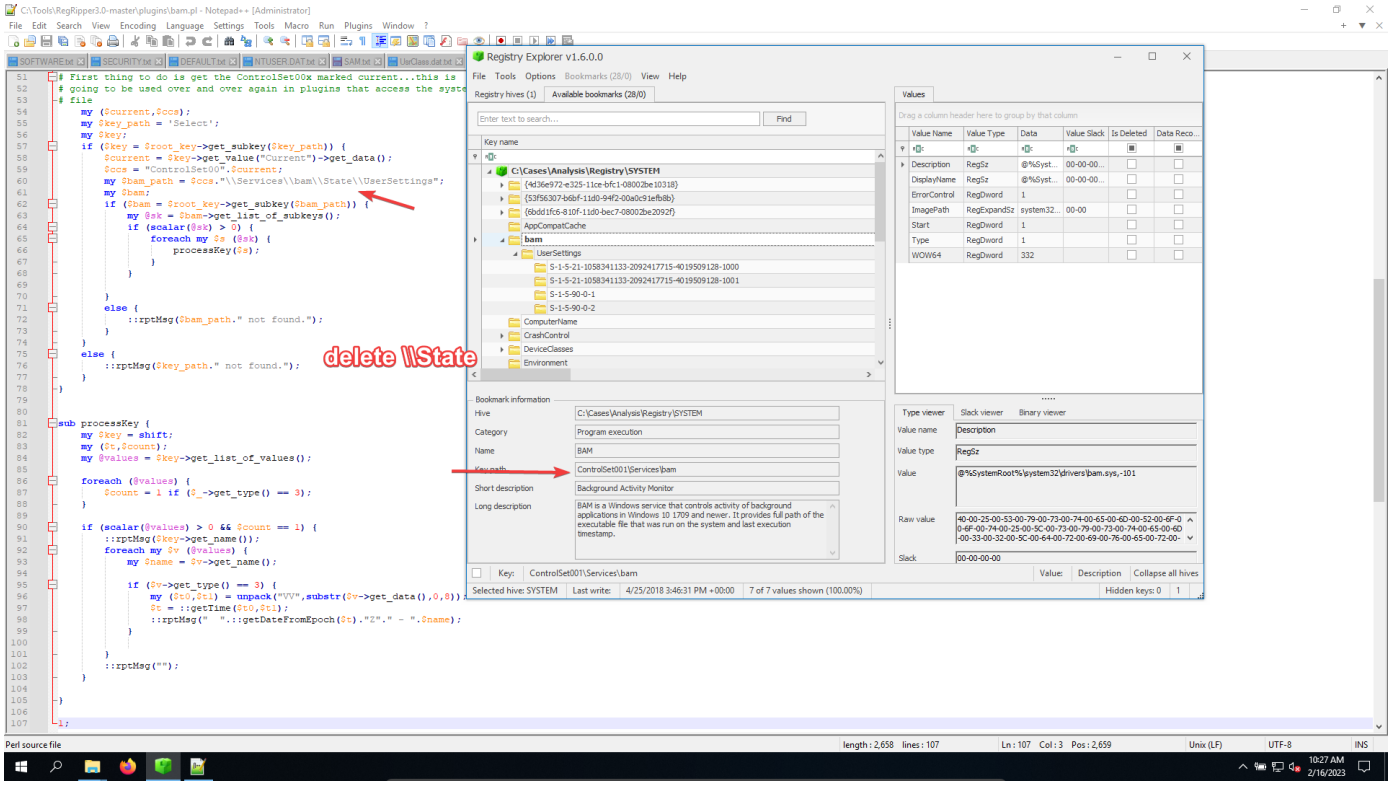
- In this case you can see that there is no output, that is why because the regripper pluggin does not look where it should:



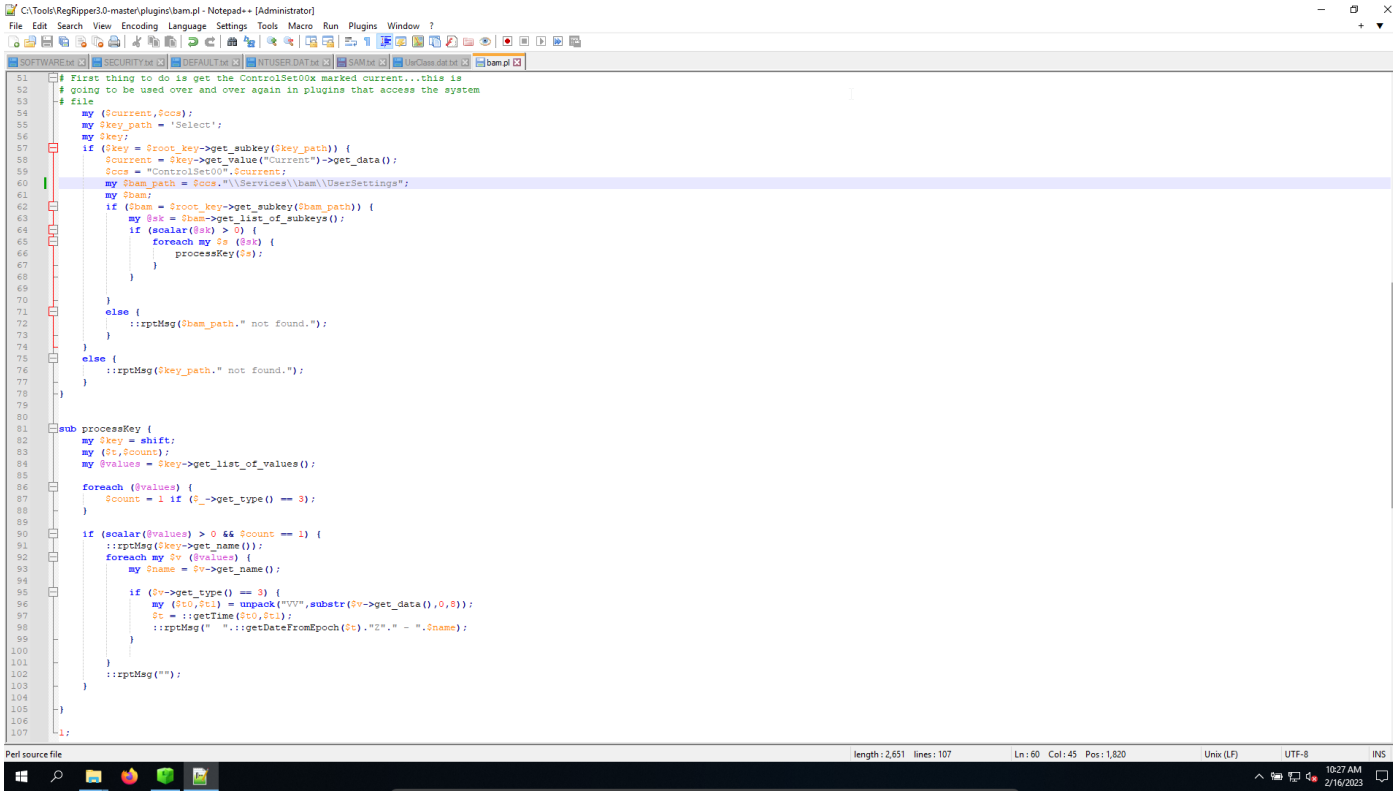
- We delete the SYSTEM.txt , change the path of the plugin to search for and redo the regripper cmd script to parse the SYSTEM.



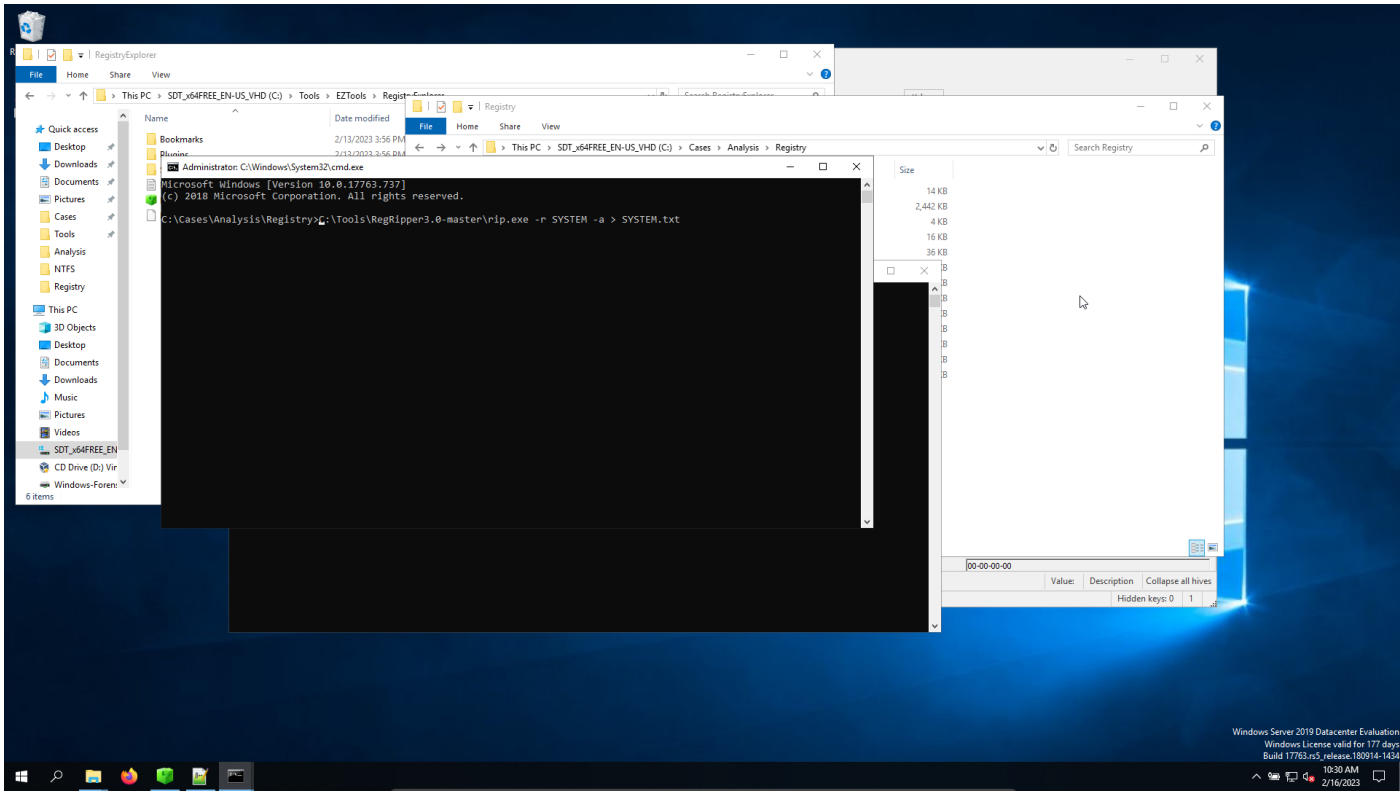


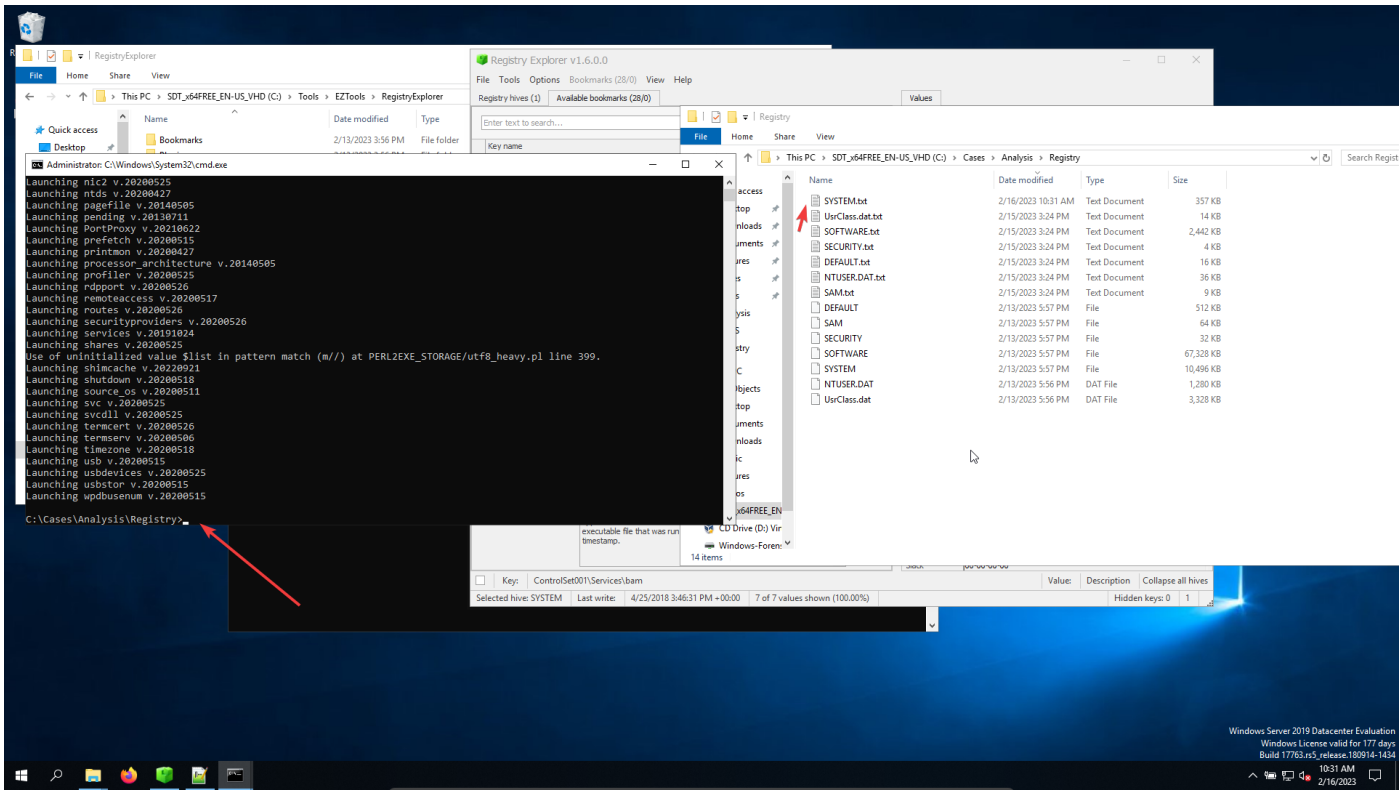


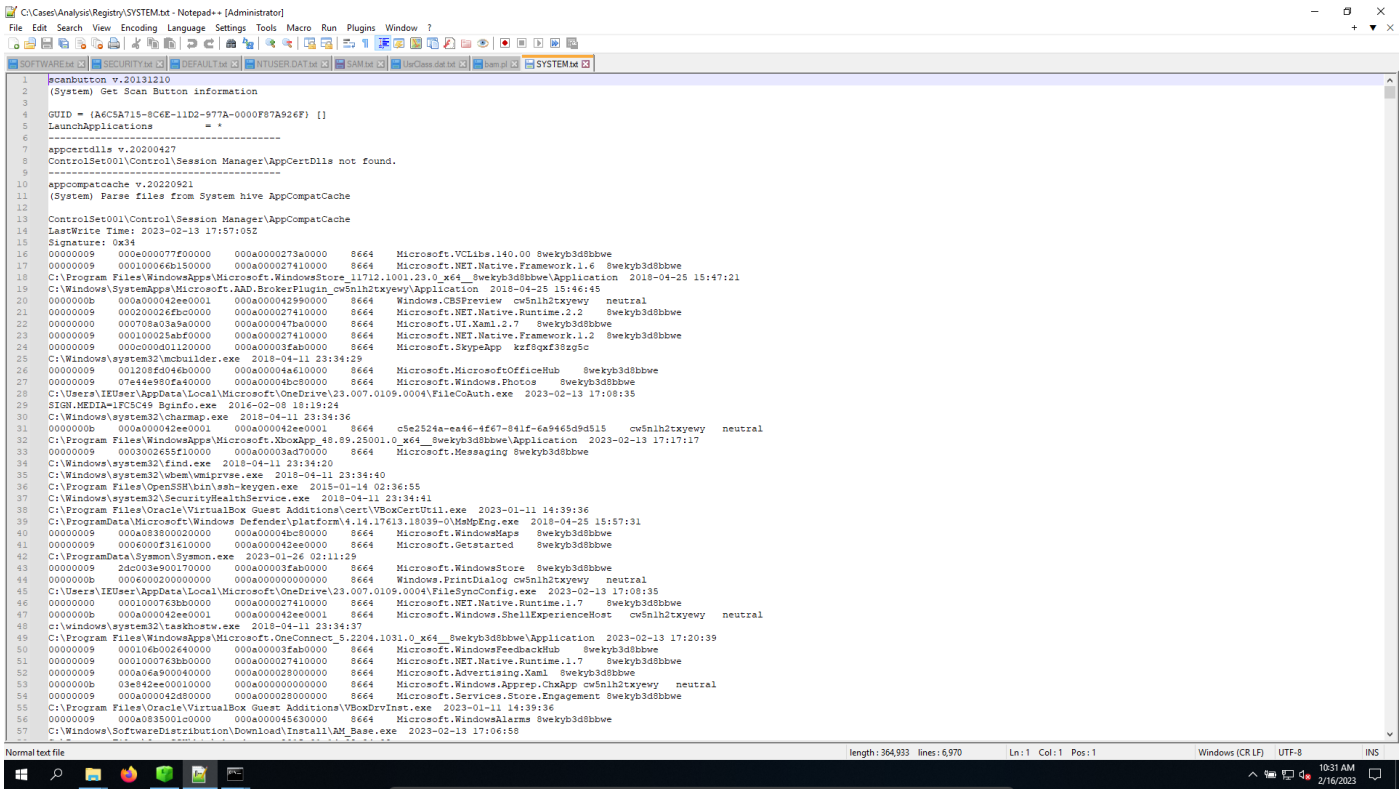

```
# First thing to do is get the ControlSet00x marked current...this is
# going to be used over and over again in plugins that access the syste
# file
    my ($current,$ccs);
    my $key_path = 'Select';
    my $key;
    if ($key = $root_key->get_subkey($key_path)) {
        $current = $key->get_value("Current")->get_data();
        $ccs = "ControlSet00".$current;
        my $bam_path = $ccs."\\Services\\bam\\State\\UserSettings";
        my $bam;
        if ($bam = $root_key->get_subkey($bam_path)) {
            my @sk = $bam->get_list_of_subkeys();
            if (scalar(@sk) > 0) {
                foreach my $s (@sk) {
                    processKey($s);
                }
            }

        }
        else {
            ::rptMsg($bam_path." not found.");
        }
    }
    else {
        ::rptMsg($key_path." not found.");
    }
}

sub processKey {
    my $key = shift;
    my ($t,$count);
    my @values = $key->get_list_of_values();

    foreach (@values) {
        $count = 1 if ($_->get_type() == 3);
    }

    if (scalar(@values) > 0 && $count == 1) {
        ::rptMsg($key->get_name());
        foreach my $v (@values) {
            my $name = $v->get_name();

            if ($v->get_type() == 3) {
                my ($t0,$t1) = unpack("VV",substr($v->get_data(),0,8));
                $t = ::getTime($t0,$t1);
                ::rptMsg("  ".::getDateFromEpoch($t)."Z"." - ".$name);
            }

        }
        ::rptMsg("");
    }

}

1;
```



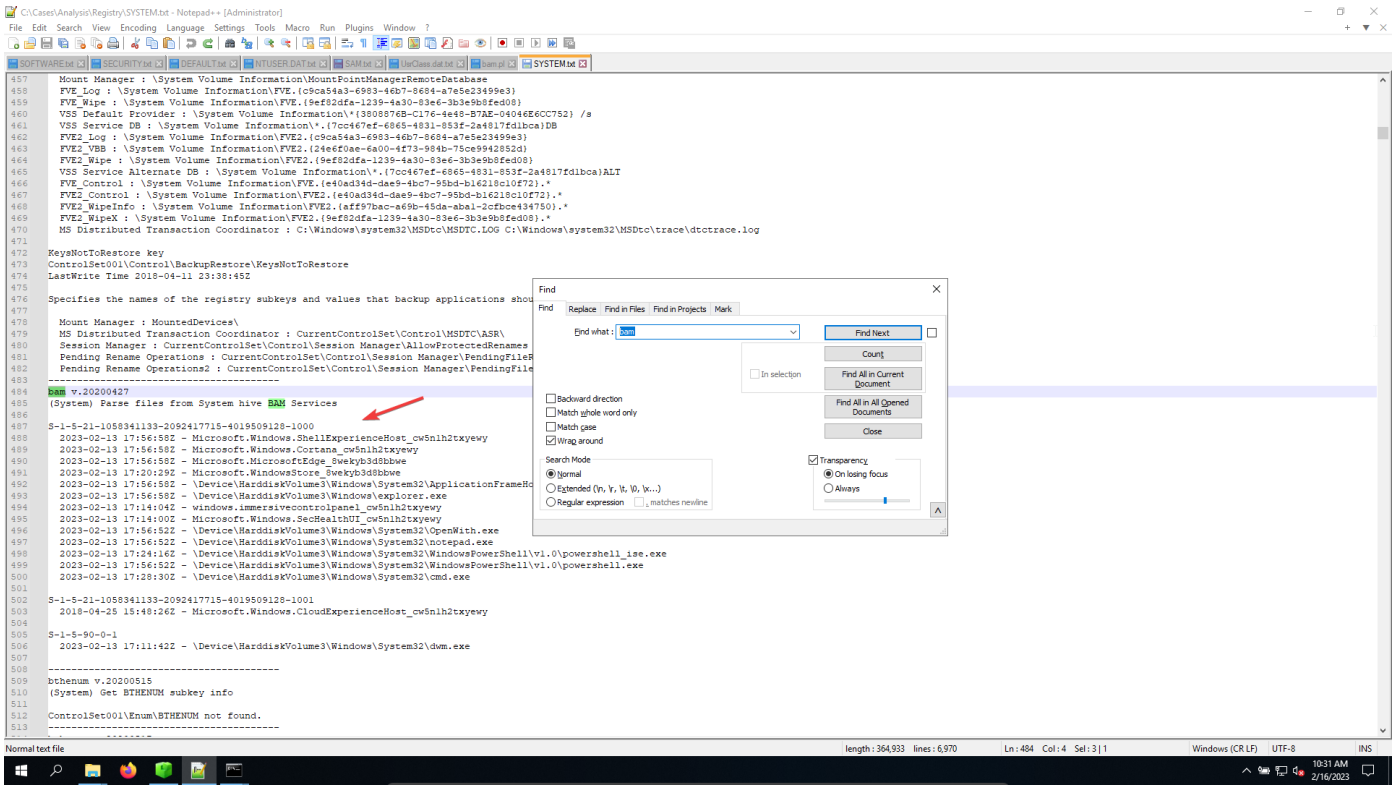
```
# First thing to do is get the ControlSet00x marked current...this is
# going to be used over and over again in plugins that access the system
# file
    my ($current,$ccs);
    my $key_path = 'Select';
    my $key;
    if ($key = $root_key->get_subkey($key_path)) {
        $current = $key->get_value("Current")->get_data();
        $ccs = "ControlSet00".$current;
        my $bam_path = $ccs."\\Services\\bam\\UserSettings";
        my $bam;
        if ($bam = $root_key->get_subkey($bam_path)) {
            my @sk = $bam->get_list_of_subkeys();
            if (scalar(@sk) > 0) {
                foreach my $s (@sk) {
                    processKey($s);
                }
            }

        }
        else {
            ::rptMsg($bam_path." not found.");
        }
    }
    else {
        ::rptMsg($key_path." not found.");
    }
}

sub processKey {
    my $key = shift;
    my ($t,$count);
    my @values = $key->get_list_of_values();

    foreach (@values) {
        $count = 1 if ($_->get_type() == 3);
    }

    if (scalar(@values) > 0 && $count == 1) {
        ::rptMsg($key->get_name());
        foreach my $v (@values) {
            my $name = $v->get_name();

            if ($v->get_type() == 3) {
                my ($t0,$t1) = unpack("VV",substr($v->get_data(),0,8));
                $t = ::getTime($t0,$t1);
                ::rptMsg("  ".::getDateFromEpoch($t)."Z"." - ".$name);
            }

        }
        ::rptMsg("");
    }

}

1;
```


Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Cases\Analysis\Registry>C:\Tools\RegRipper3.0-master\rip.exe -r SYSTEM -a > SYSTEM.txt


Administrator: C:\Windows\System32\cmd.exe
Launching nic2 v.20200525
Launching ntds v.20200427
Launching pagefile v.20140505
Launching pending v.20130711
Launching PortProxy v.20210622
Launching prefetch v.20200515
Launching printmon v.20200427
Launching processor_architecture v.20140505
Launching profiler v.20200525
Launching rdpport v.20200526
Launching remoteaccess v.20200517
Launching routes v.20200526
Launching securityproviders v.20200526
Launching services v.20191024
Launching shares v.20200525
Use of uninitialized value $list in pattern match (m//) at PERL2EXE_STORAGE/utf8_heavy.pl line 399.
Launching shimcache v.20220921
Launching shutdown v.20200518
Launching source_os v.20200511
Launching svc v.20200525
Launching svcdll v.20200525
Launching termcert v.20200526
Launching termserv v.20200506
Launching timezone v.20200518
Launching usb v.20200515
Launching usbdevices v.20200525
Launching usbstor v.20200515
Launching wpdbusenum v.20200515
C:\Cases\Analysis\Registry>
Registry Explorer v1.6.0.0
SYSTEM.txt
UsrClass.dat.txt
SOFTWARE.txt
SECURITY.txt
DEFAULT.txt
NTUSER.DAT.txt
SAM.txt
DEFAULT
SAM
SECURITY
SOFTWARE
SYSTEM
NTUSER.DAT
UsrClass.dat



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



- 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

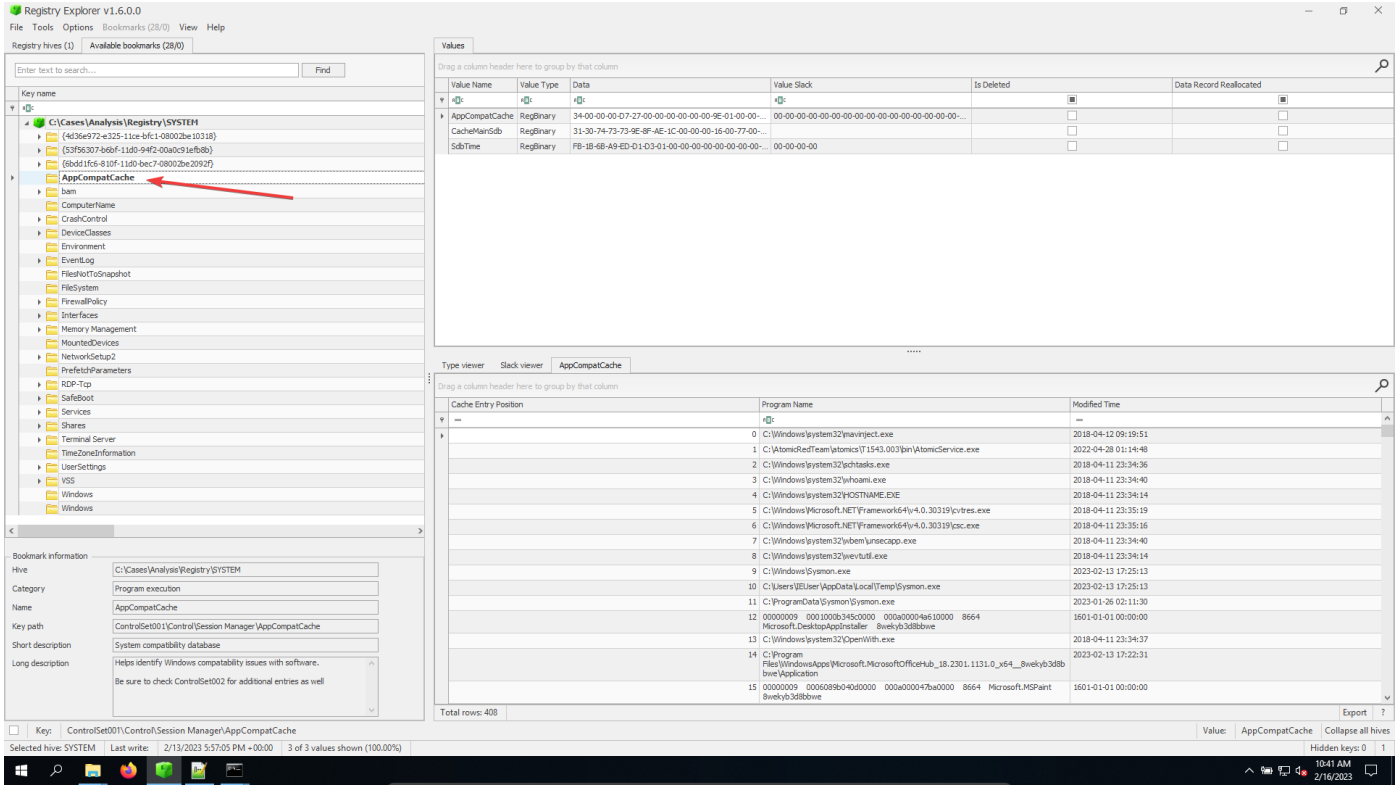
2023-02-13 17:56:58Z - \Device\HarddiskVolume3\Windows\System32\ApplicationFrameHost.exe

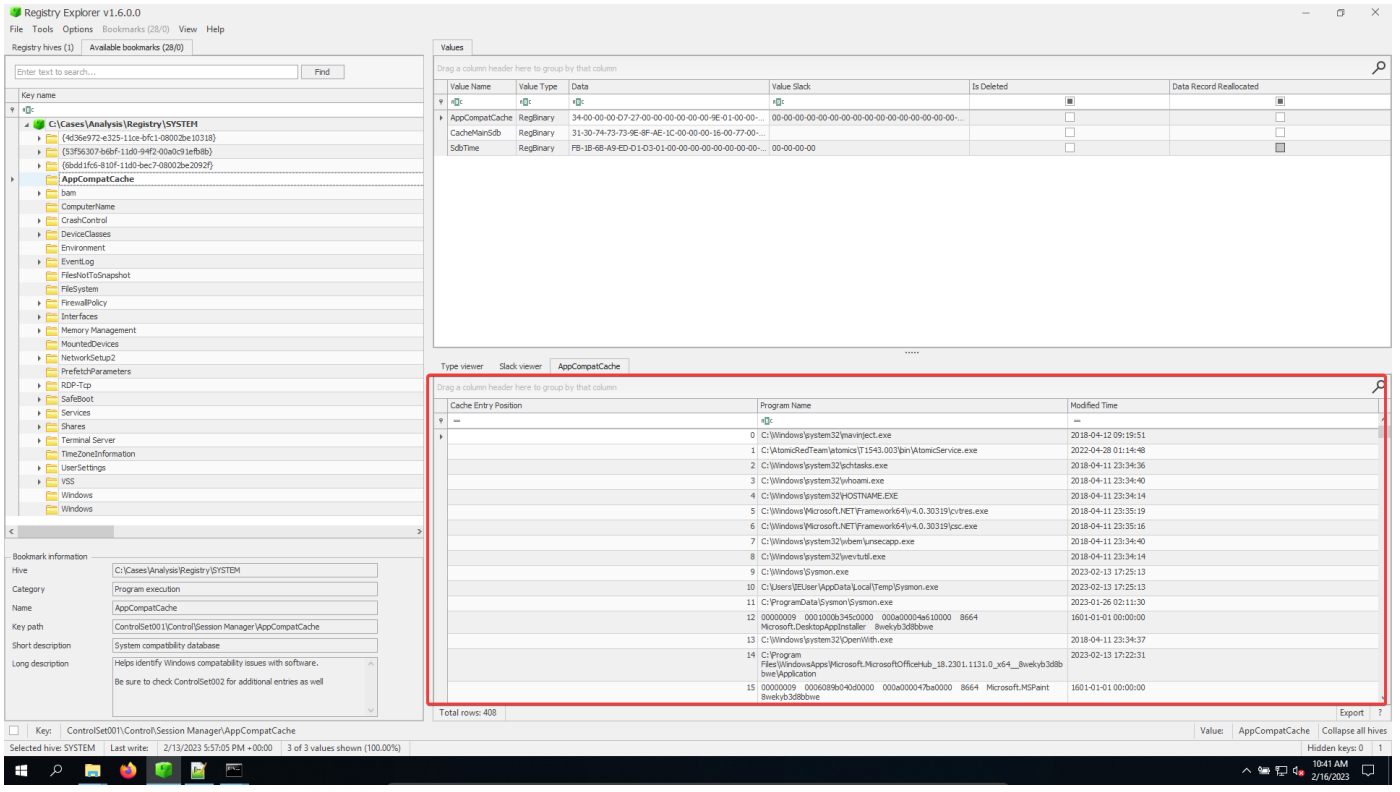
2023-02-13 17:56:52Z - \Device\HarddiskVolume3\Windows\System32\OpenWith.exe

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

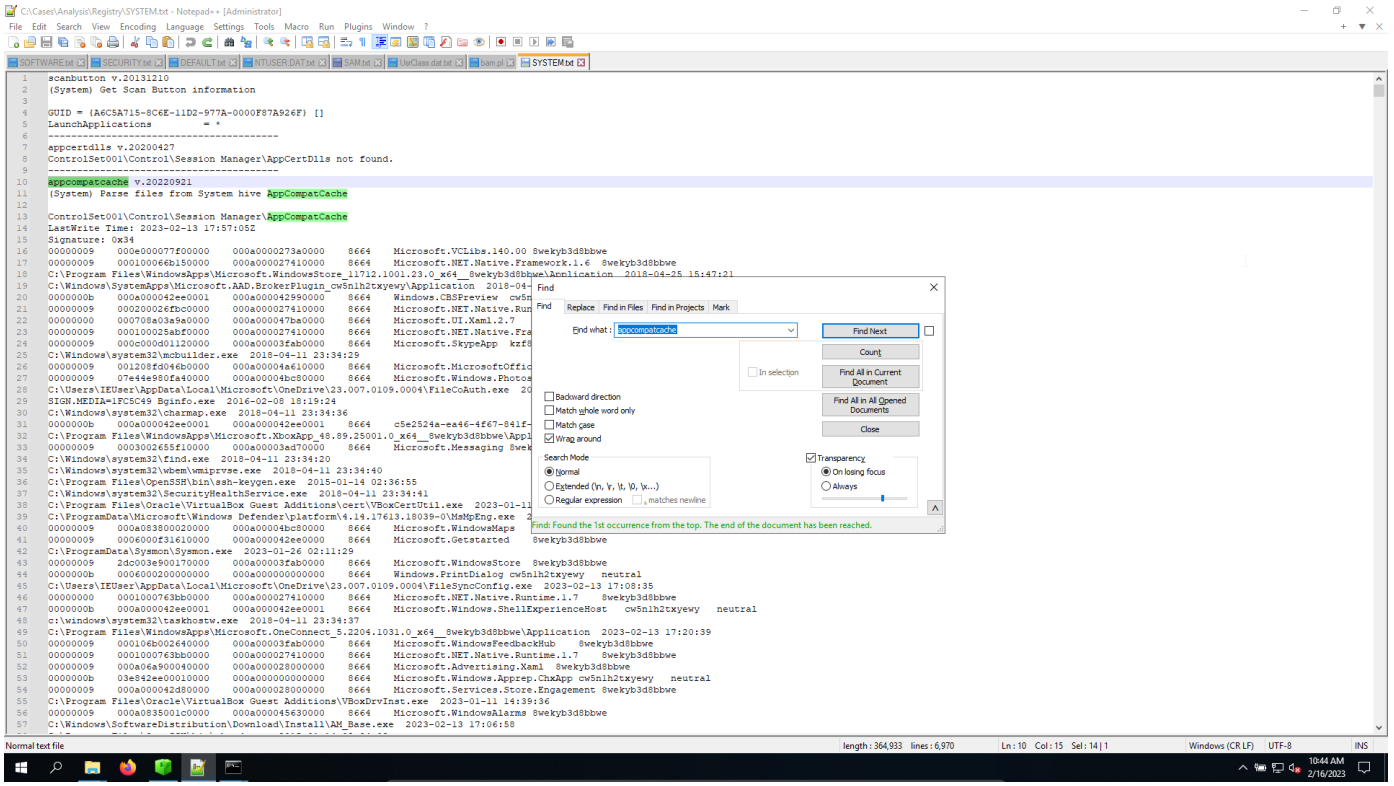
Application Compatibility Cache (ShimCache)

- You can find information related to ShimCache at:
  - 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:

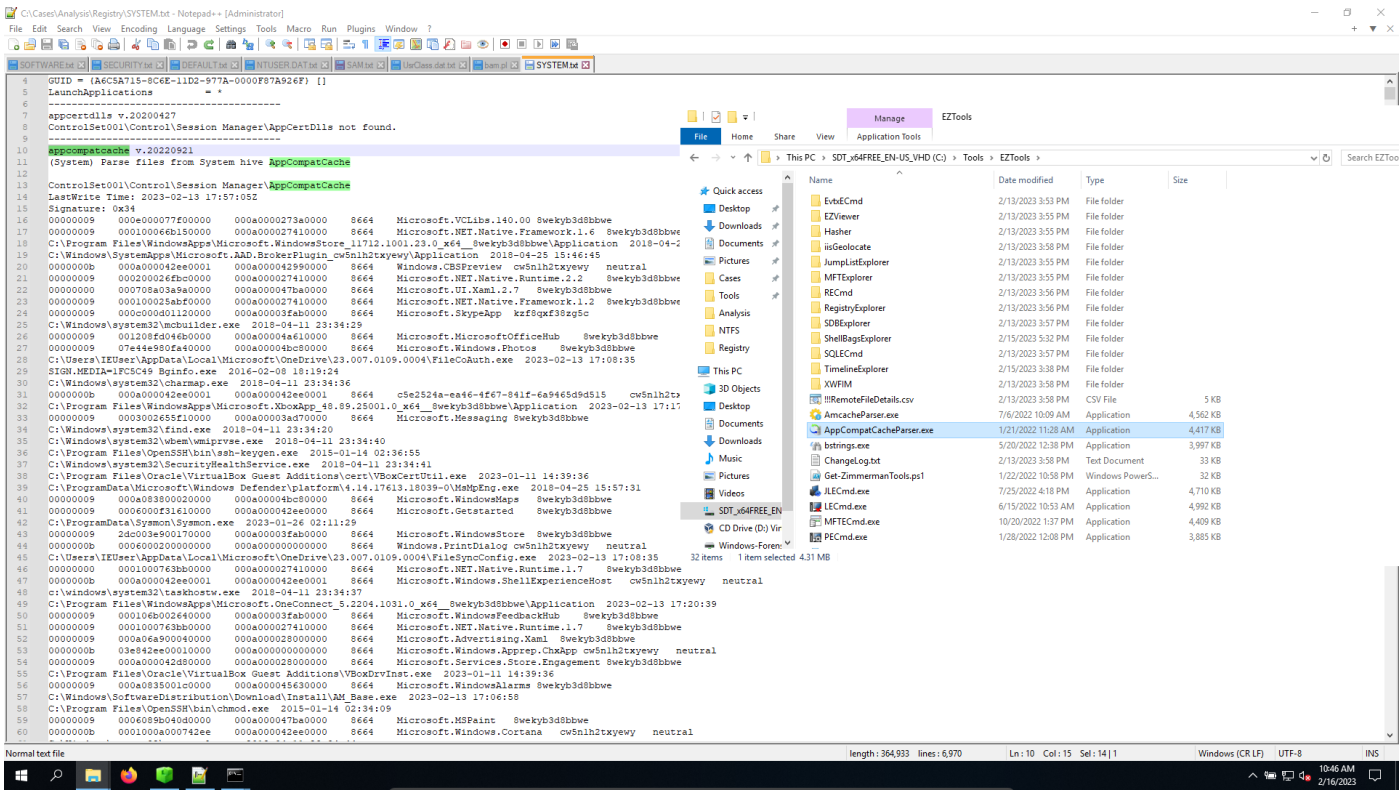




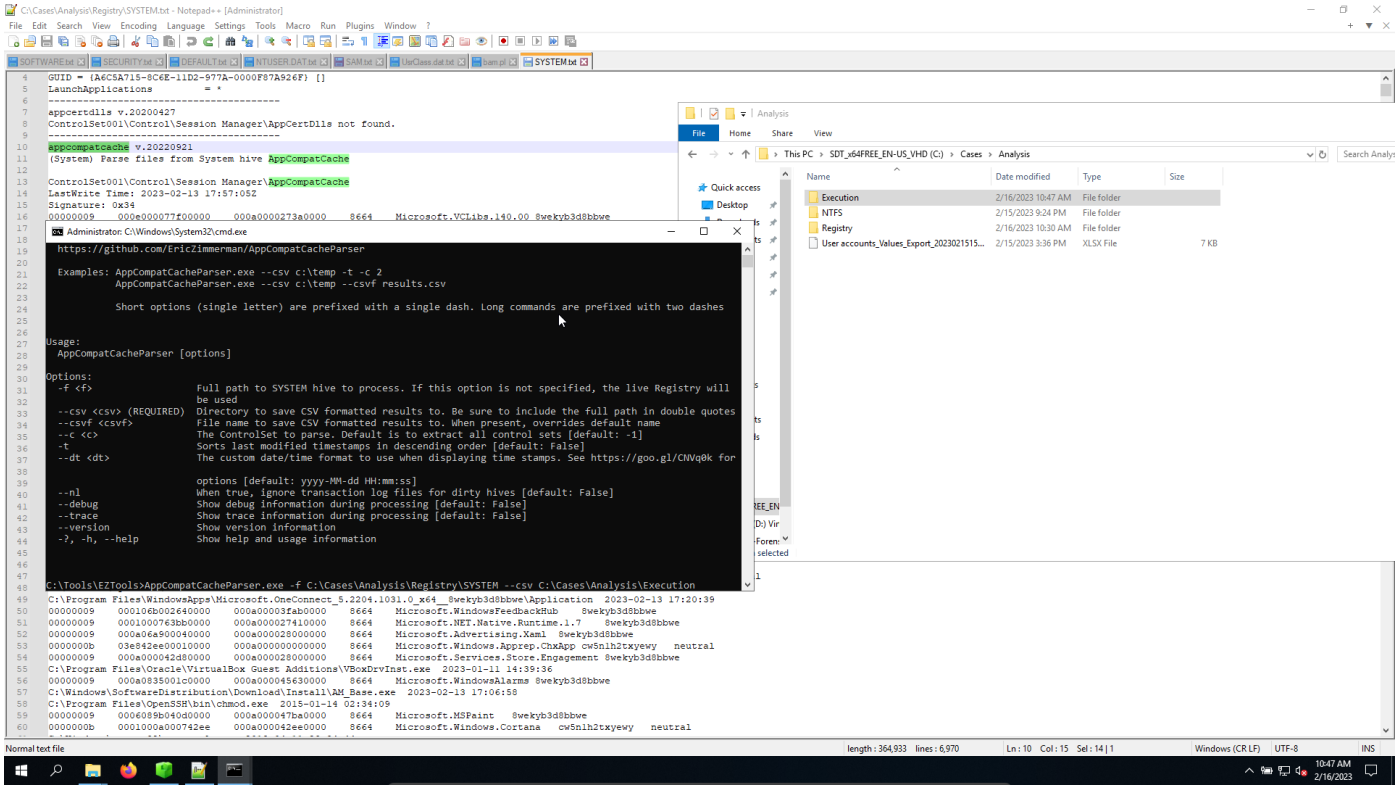
- Cache Entry Position shows the order of program execution.
- We can use different tools to get the same information in different formats.

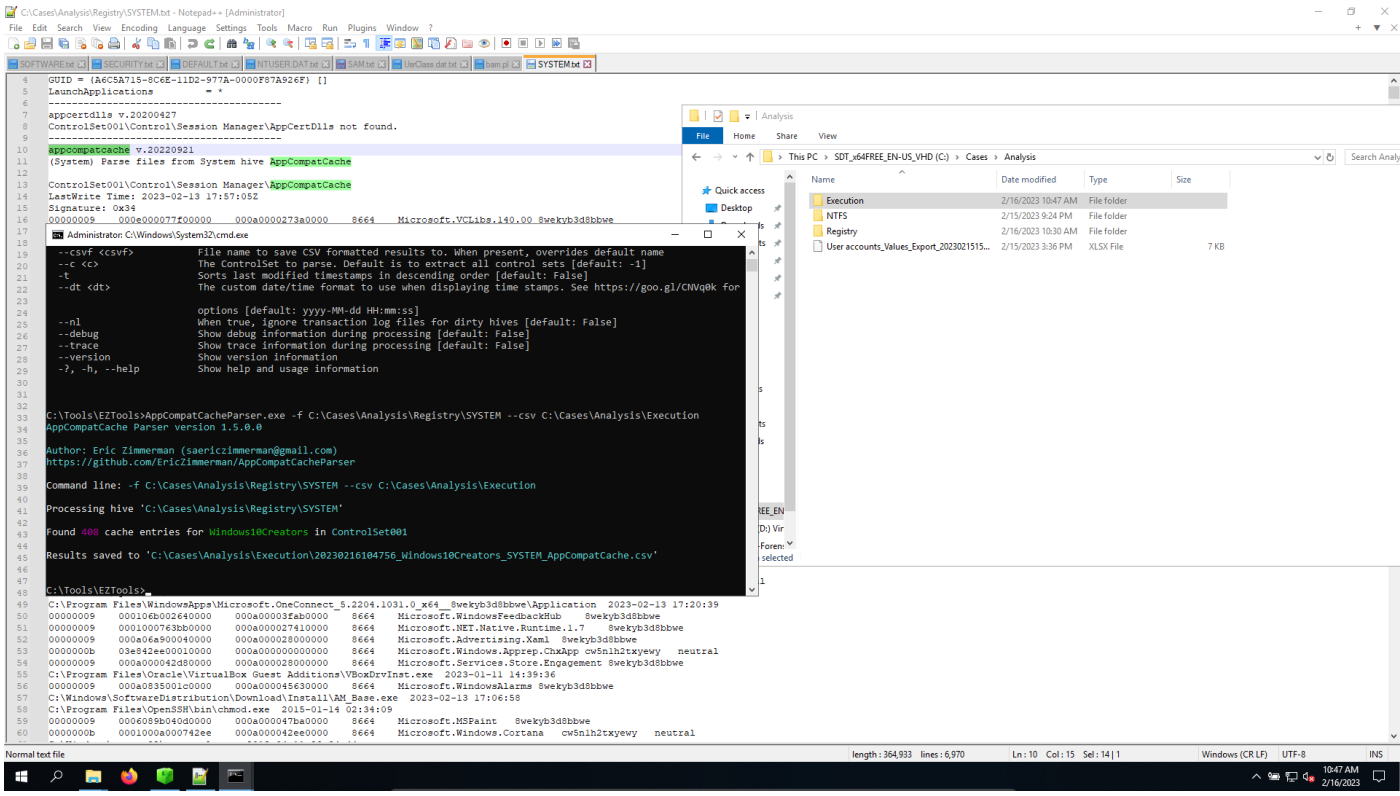


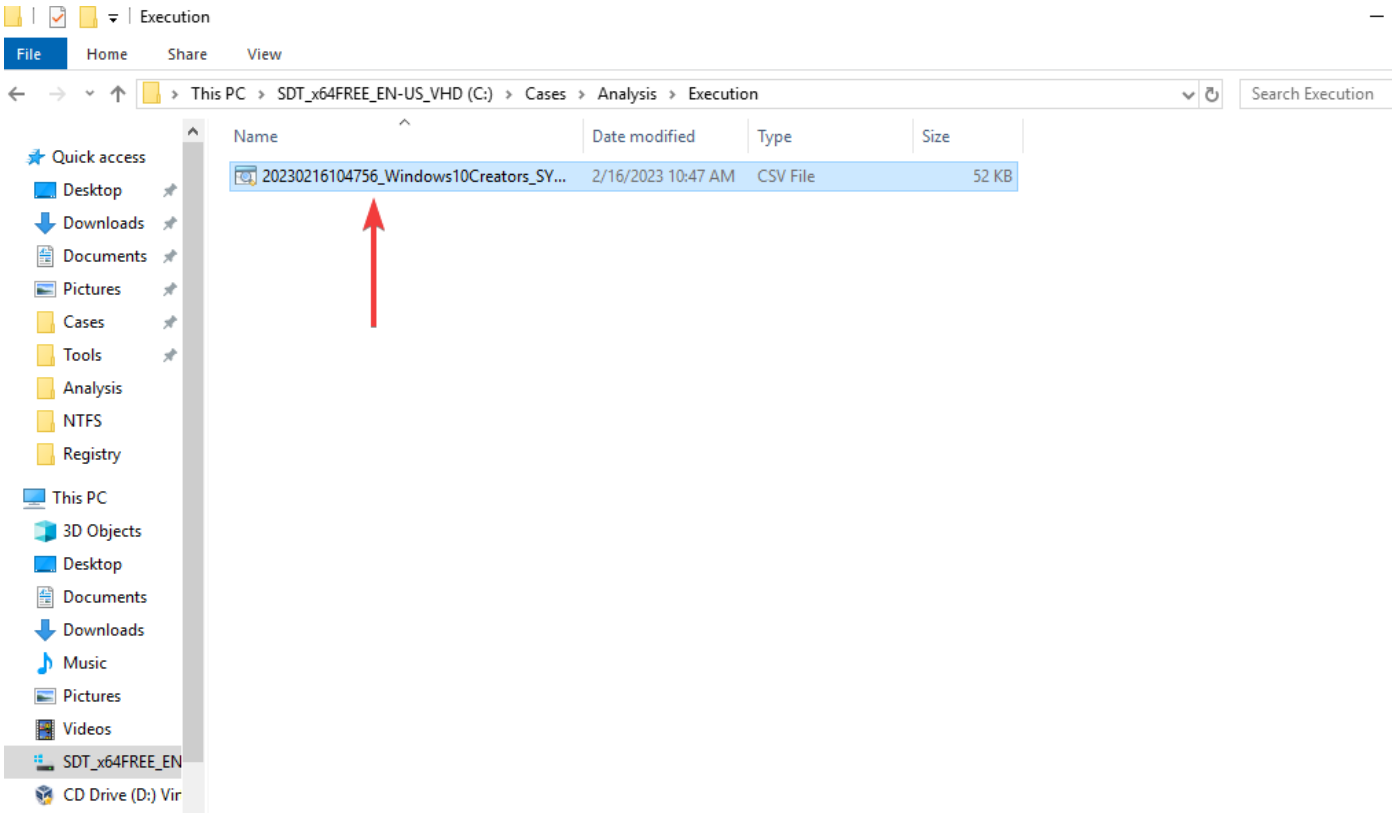
- We will use AppCompatCacheParser:

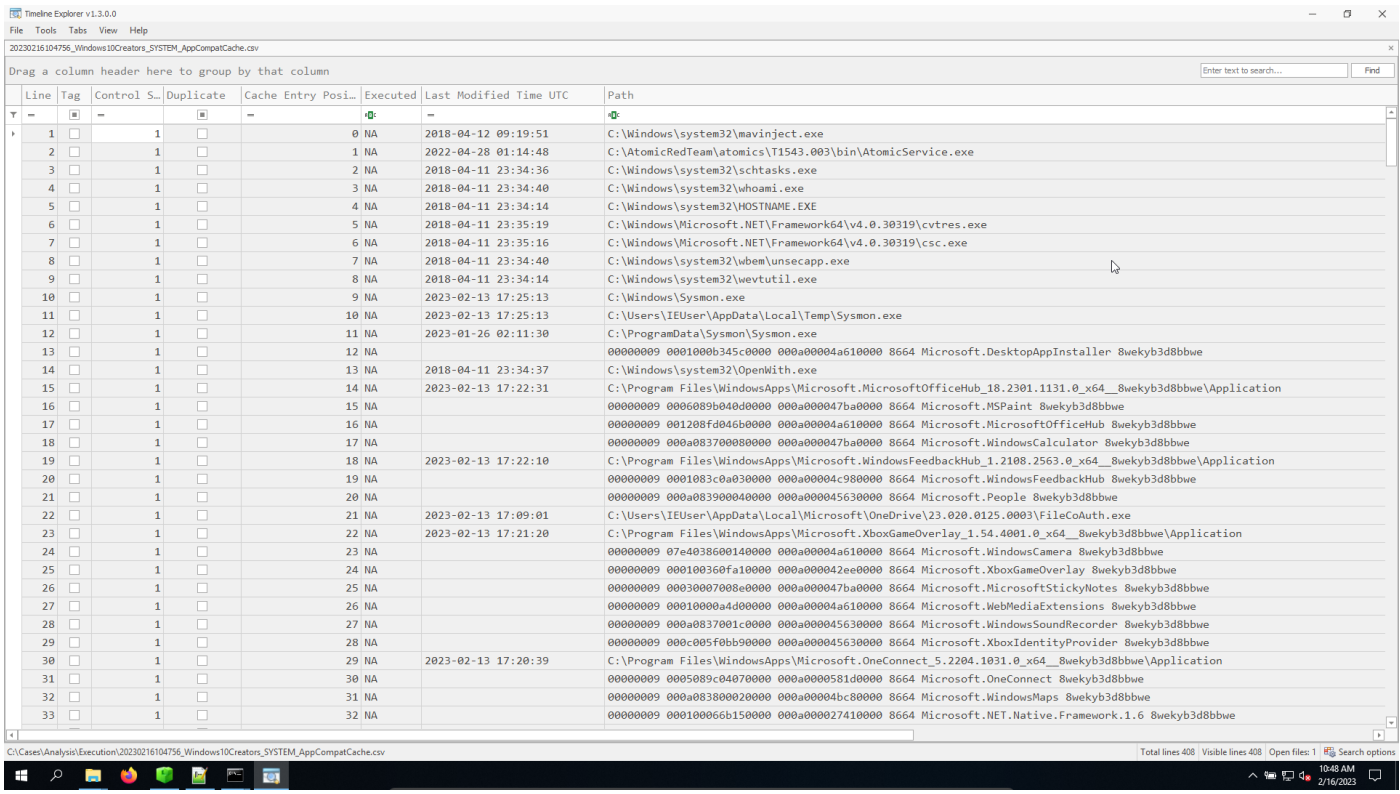


- Use it in the cmd:

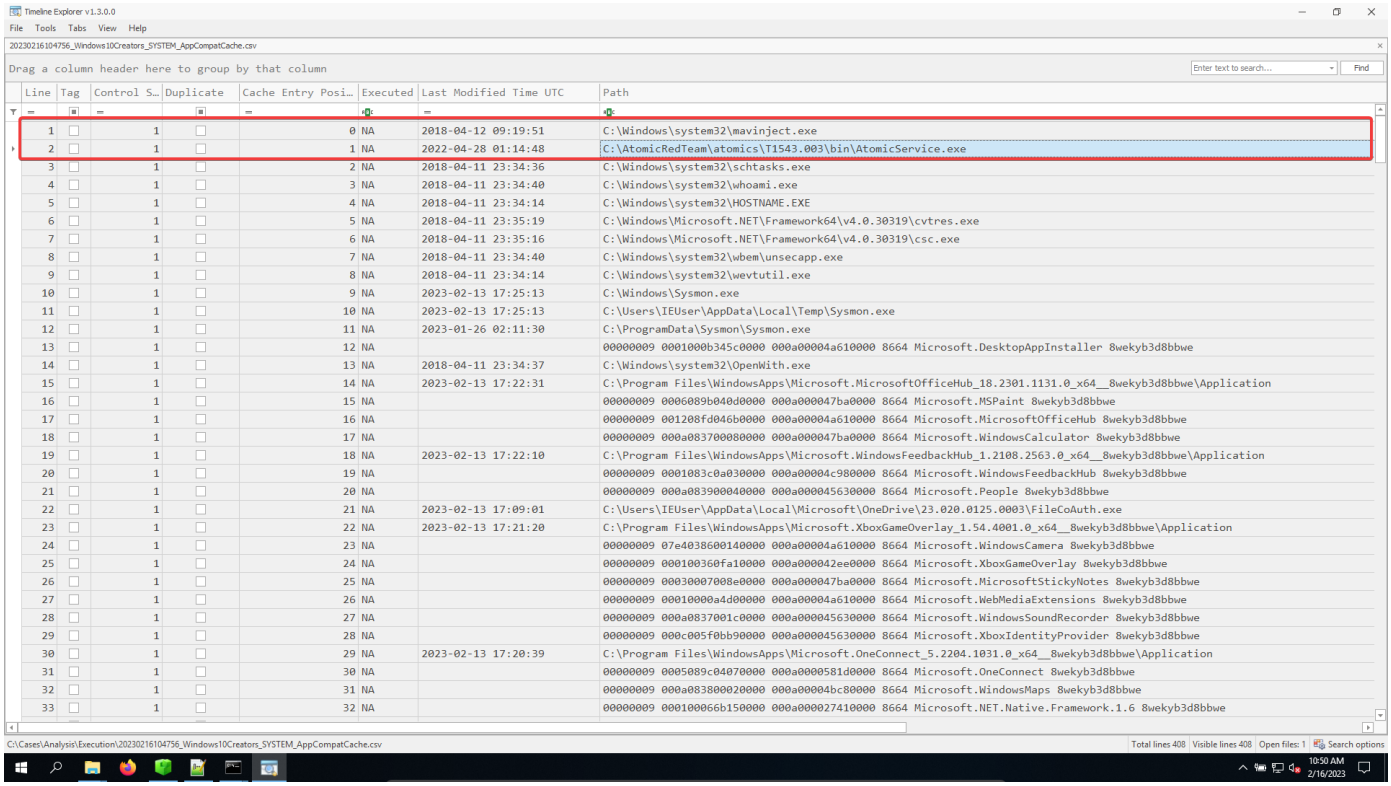

C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]
Administrator: C:\Windows\System32\cmd.exe
https://github.com/EricZimmerman/AppCompatCacheParser
Examples: AppCompatCacheParser.exe --csv c:\temp -t -c 2
AppCompatCacheParser.exe --csv c:\temp --csvf results.csv
Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
Usage:
AppCompatCacheParser [options]
Options:
-f <f> 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 <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
Analysis
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › Analysis
Name
Date modified
Type
Size
Execution
2/16/2023 10:47 AM
File folder
NTFS
2/15/2023 9:24 PM
File folder
Registry
2/16/2023 10:30 AM
File folder
User accounts_Values_Export_2023021515...
2/15/2023 3:36 PM
XLSX File
7 KB


C:\Cases\Analysis\Registry\SYSTEM.txt - Notepad++ [Administrator]
Administrator: C:\Windows\System32\cmd.exe
--csvf <csvf> File name to save CSV formatted results to. When present, overrides default name
-c <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 1.5.0.0
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>
Analysis
This PC › SDT_x64FREE_EN-US_VHD (C:) › Cases › Analysis
Name
Date modified
Type
Size
Execution
2/16/2023 10:47 AM
File folder
NTFS
2/15/2023 9:24 PM
File folder
Registry
2/16/2023 10:30 AM
File folder
User accounts_Values_Export_2023021515...
2/15/2023 3:36 PM
XLSX File
7 KB



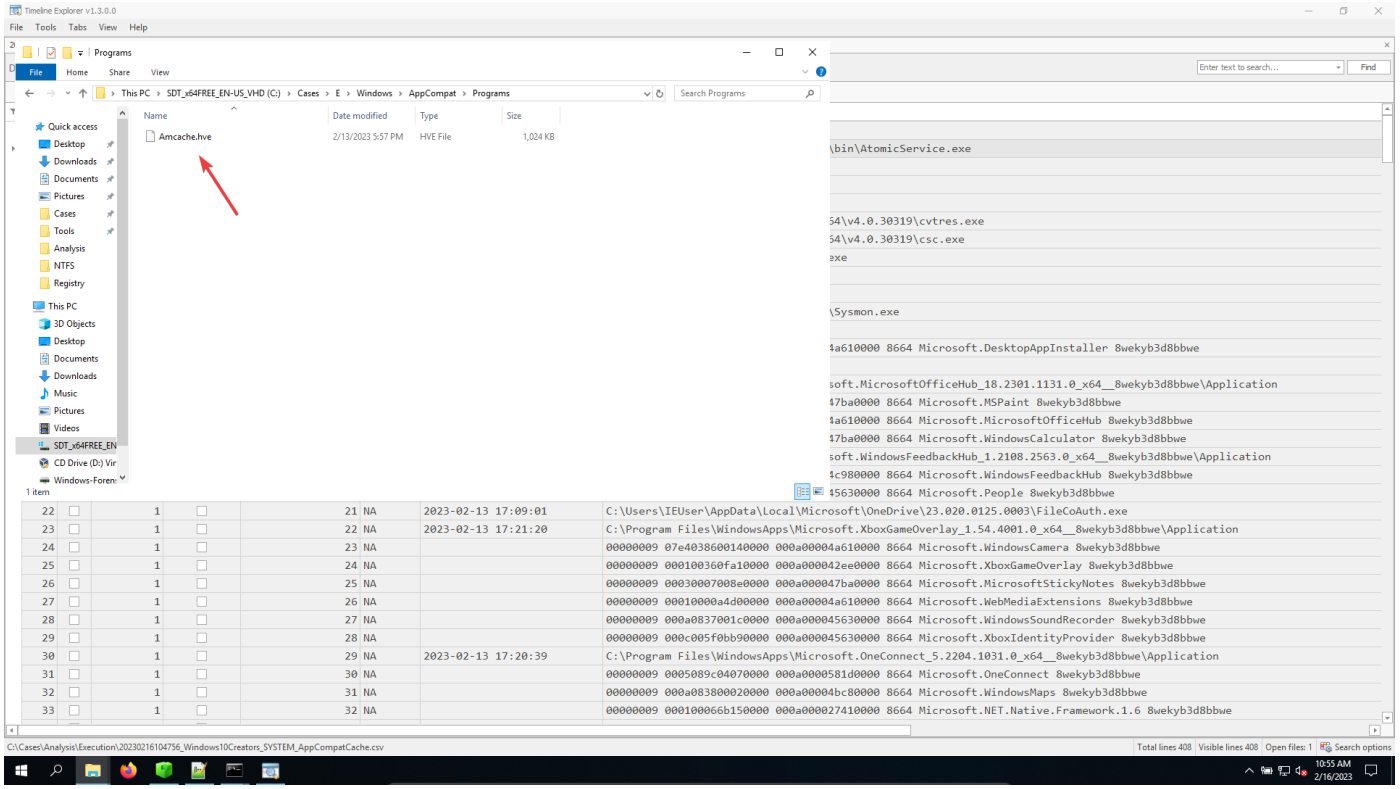


- Cache entry position for:
  - AtomicService.exe - 1
  - Mavinject.exe - 0

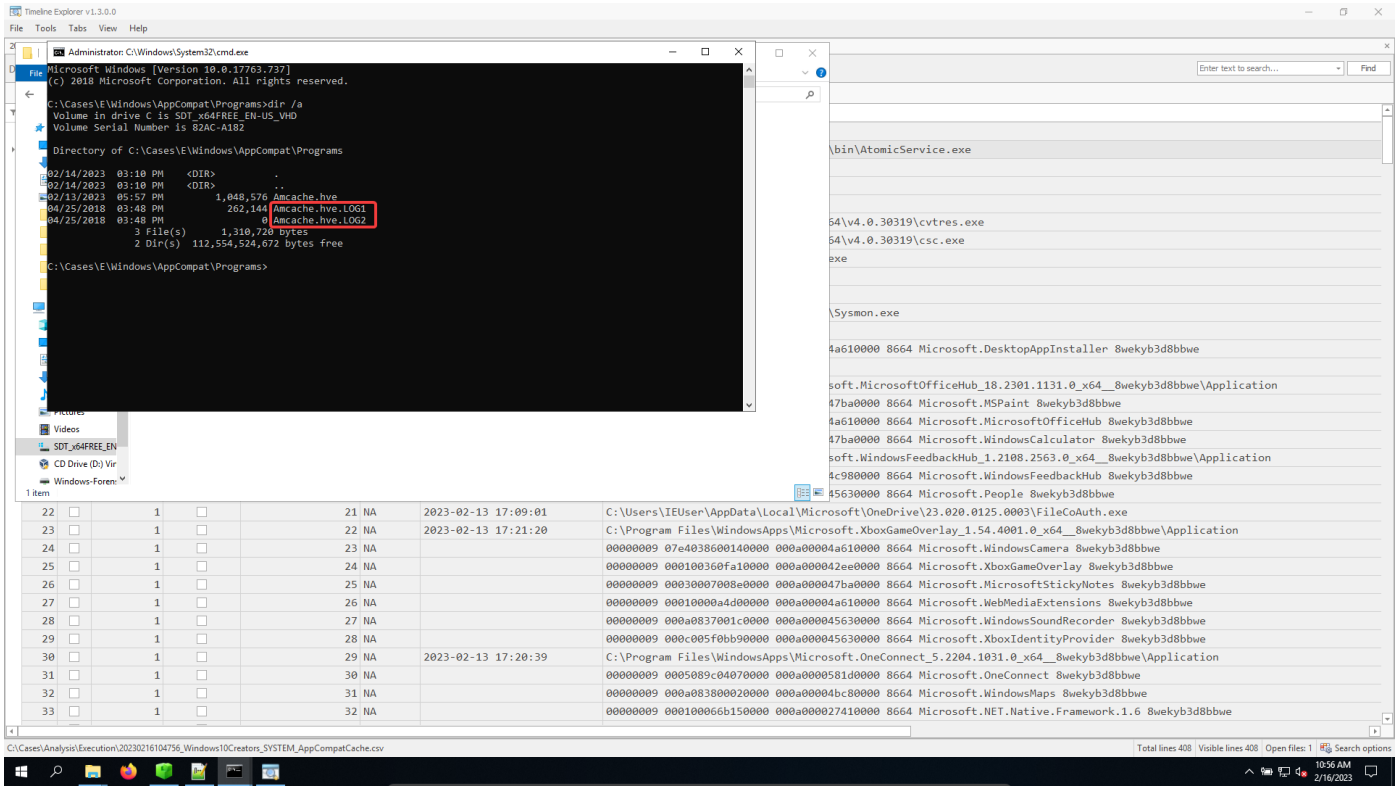


Amcache

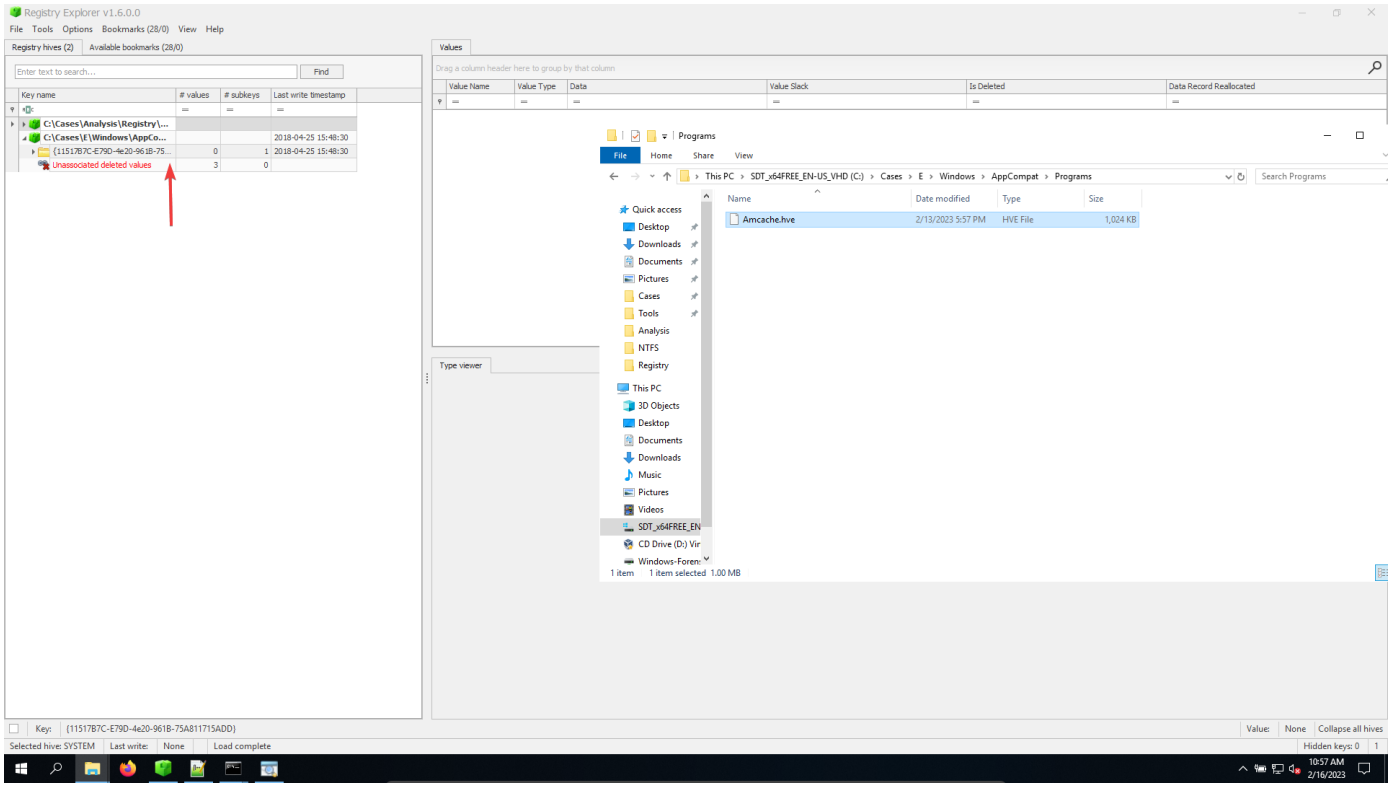
- You can find it at : C:\Windows\AppCompat\Programs\Amcache.hve
- Stores information about the user application experience.
- Location:

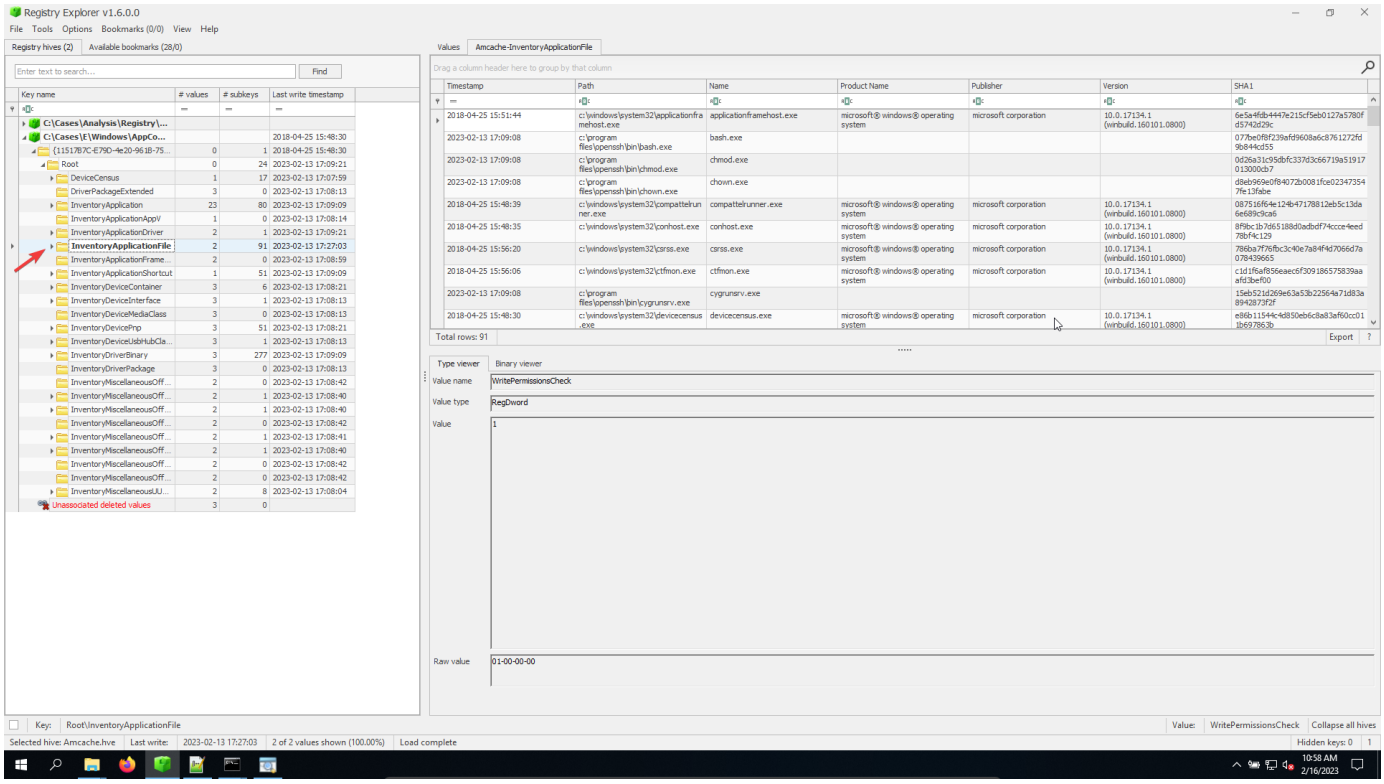


- There are two log files for Amcache.hve:

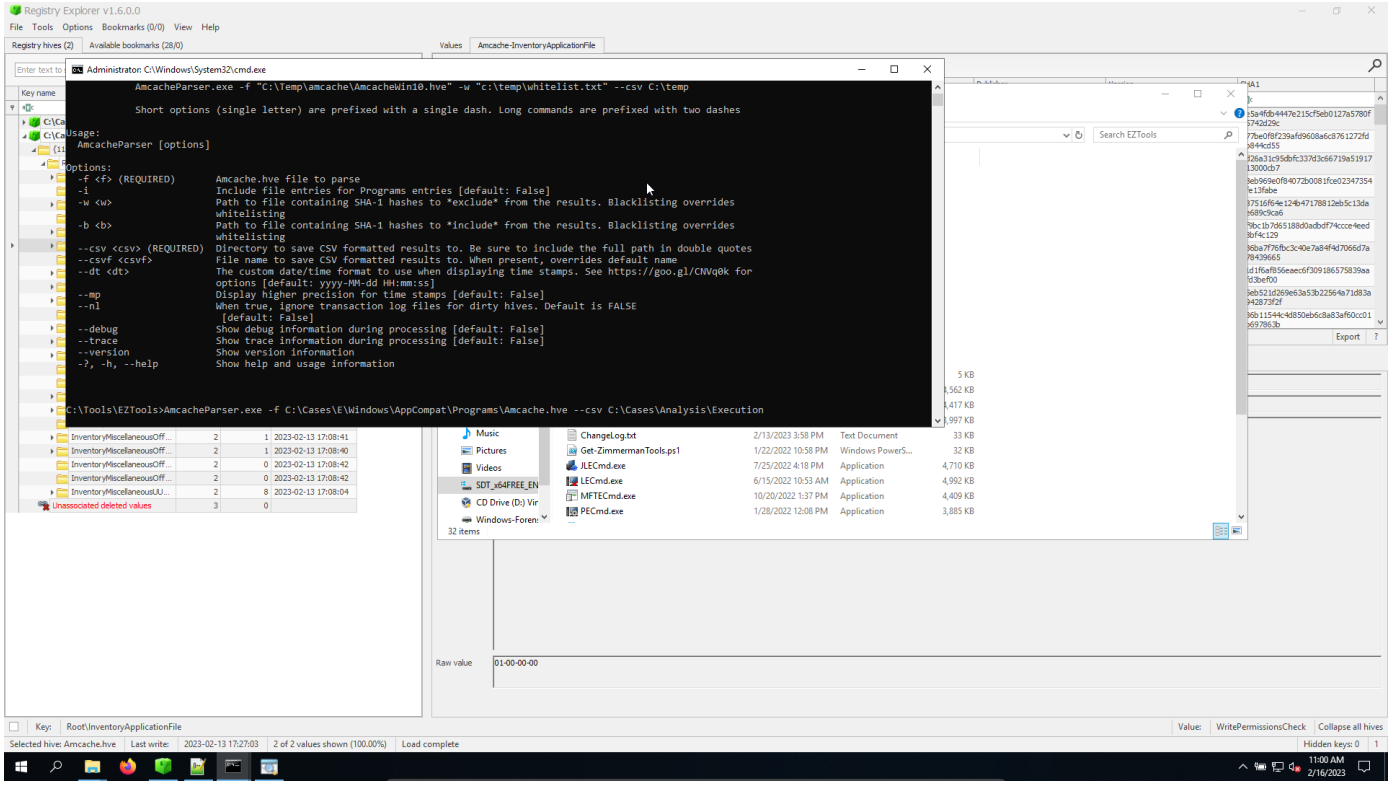


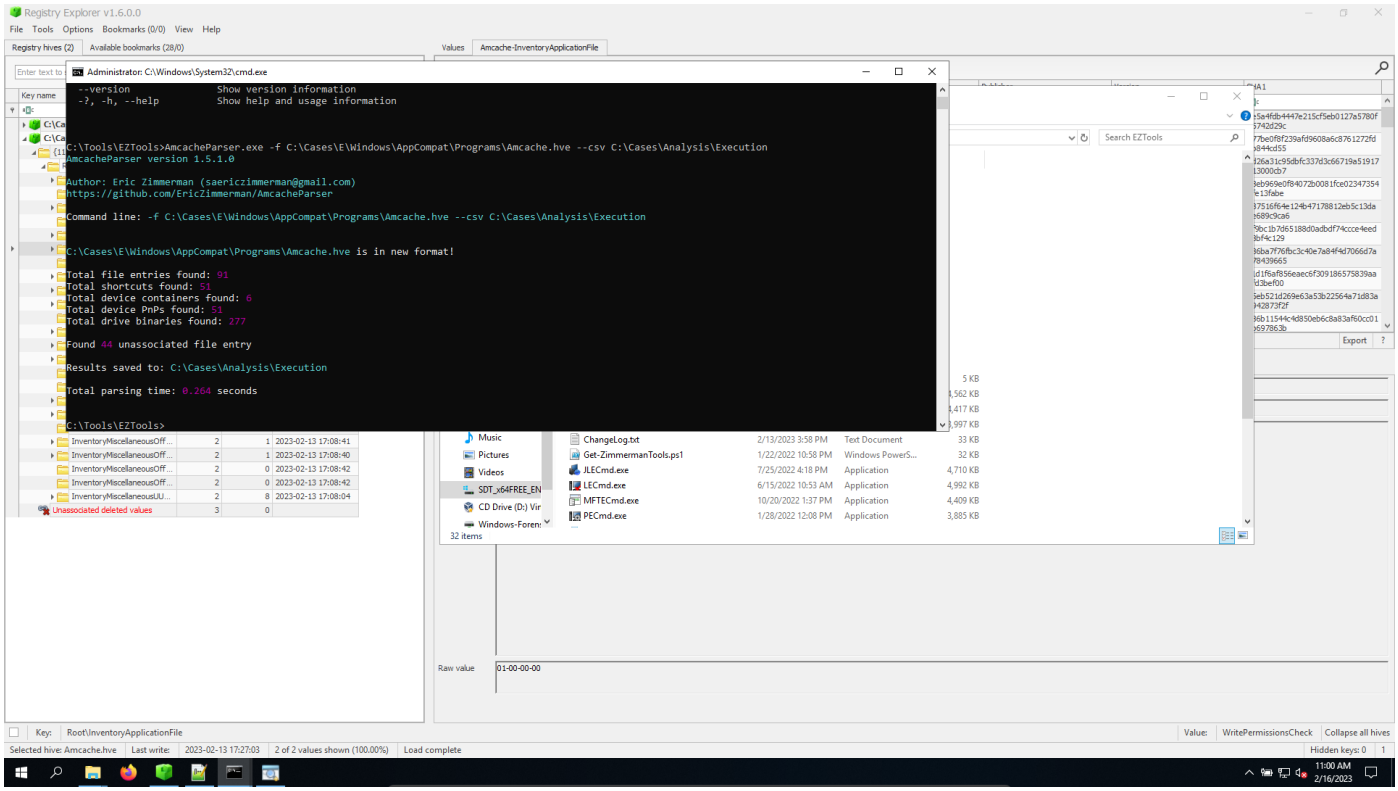
- Open it in registry Explorer:

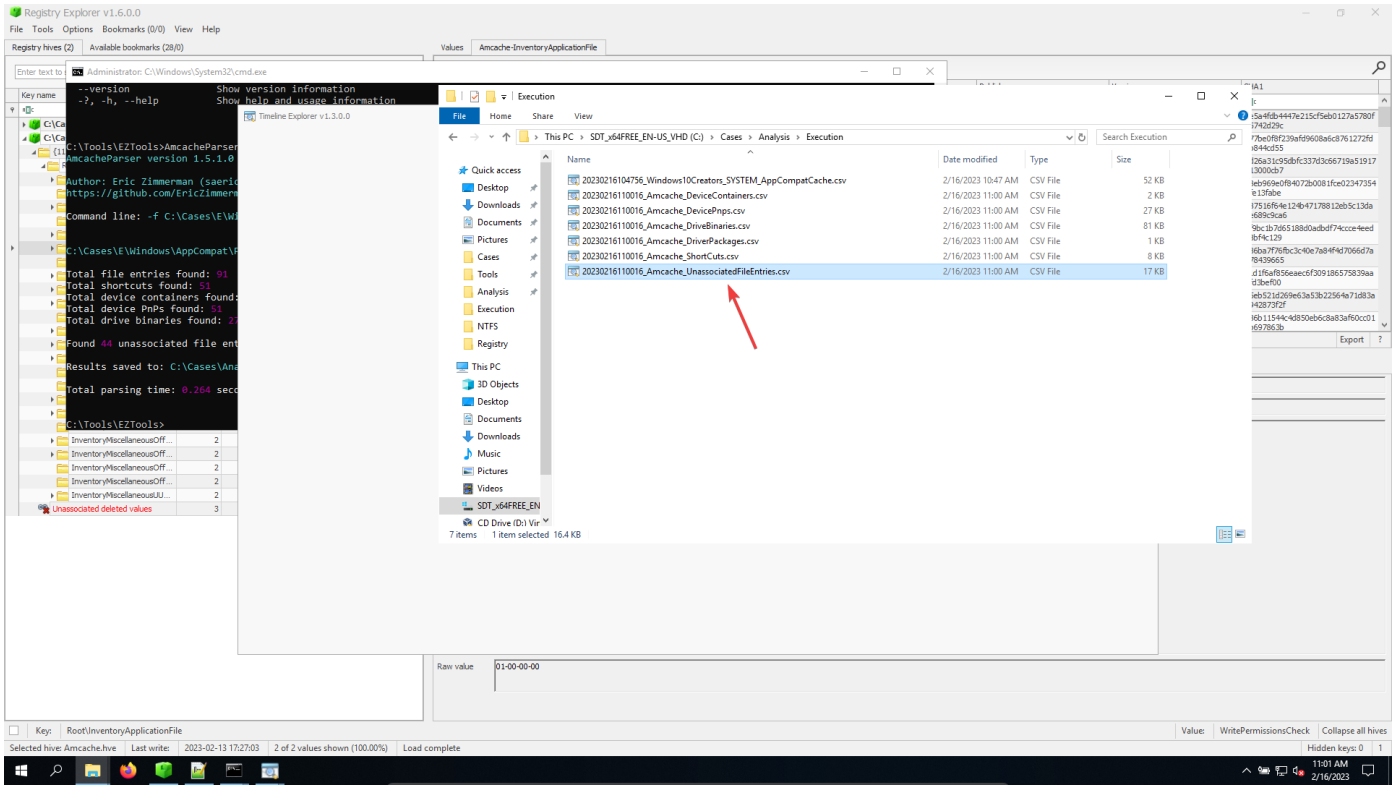


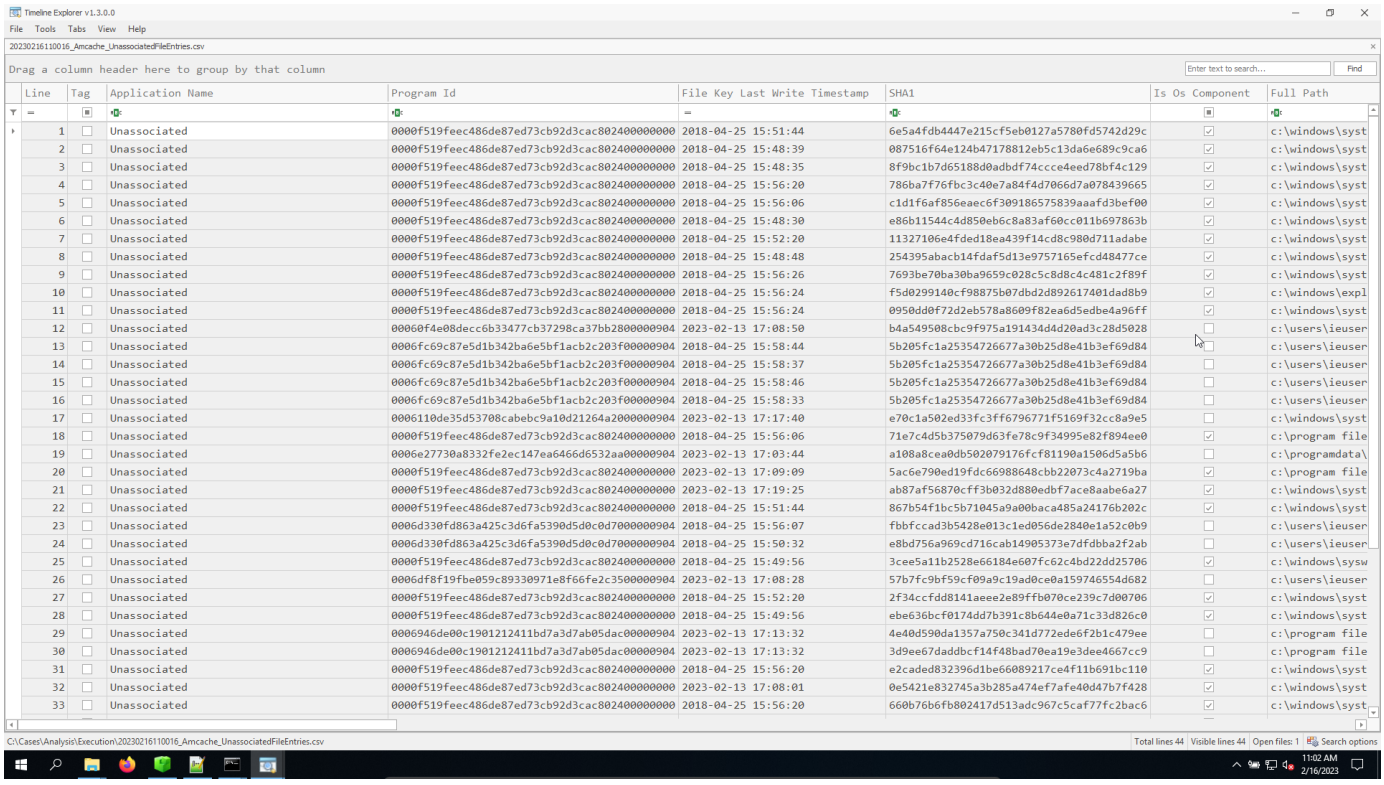


- AmcacheParser:


Registry Explorer v1.6.0.0
Administrator: C:\Windows\System32\cmd.exe
AmcacheParser.exe -f "C:\Temp\amcache\AmcacheWin10.hve" -w "c:\temp\whitelist.txt" --csv C:\temp
Short options (single letter) are prefixed with a single dash. Long commands are prefixed with two dashes
Usage:
AmcacheParser [options]
Options:
-f <f> (REQUIRED) Amcache.hve file to parse
-i Include file entries for Programs entries [default: False]
-w <w> Path to file containing SHA-1 hashes to *exclude* from the results. Blacklisting overrides whitelisting
-b <b> 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
--csvf <csvf> File name to save CSV formatted results to. When present, overrides default name
--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]
--mp Display higher precision for time stamps [default: False]
--nl When true, ignore transaction log files for dirty hives. Default is FALSE [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>AmcacheParser.exe -f C:\Cases\E\Windows\AppCompat\Programs\Amcache.hve --csv C:\Cases\Analysis\Execution


Registry Explorer v1.6.0.0
Administrator: C:\Windows\System32\cmd.exe
--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
AmcacheParser version 1.5.1.0
Author: Eric Zimmerman (saericzimmerman@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>



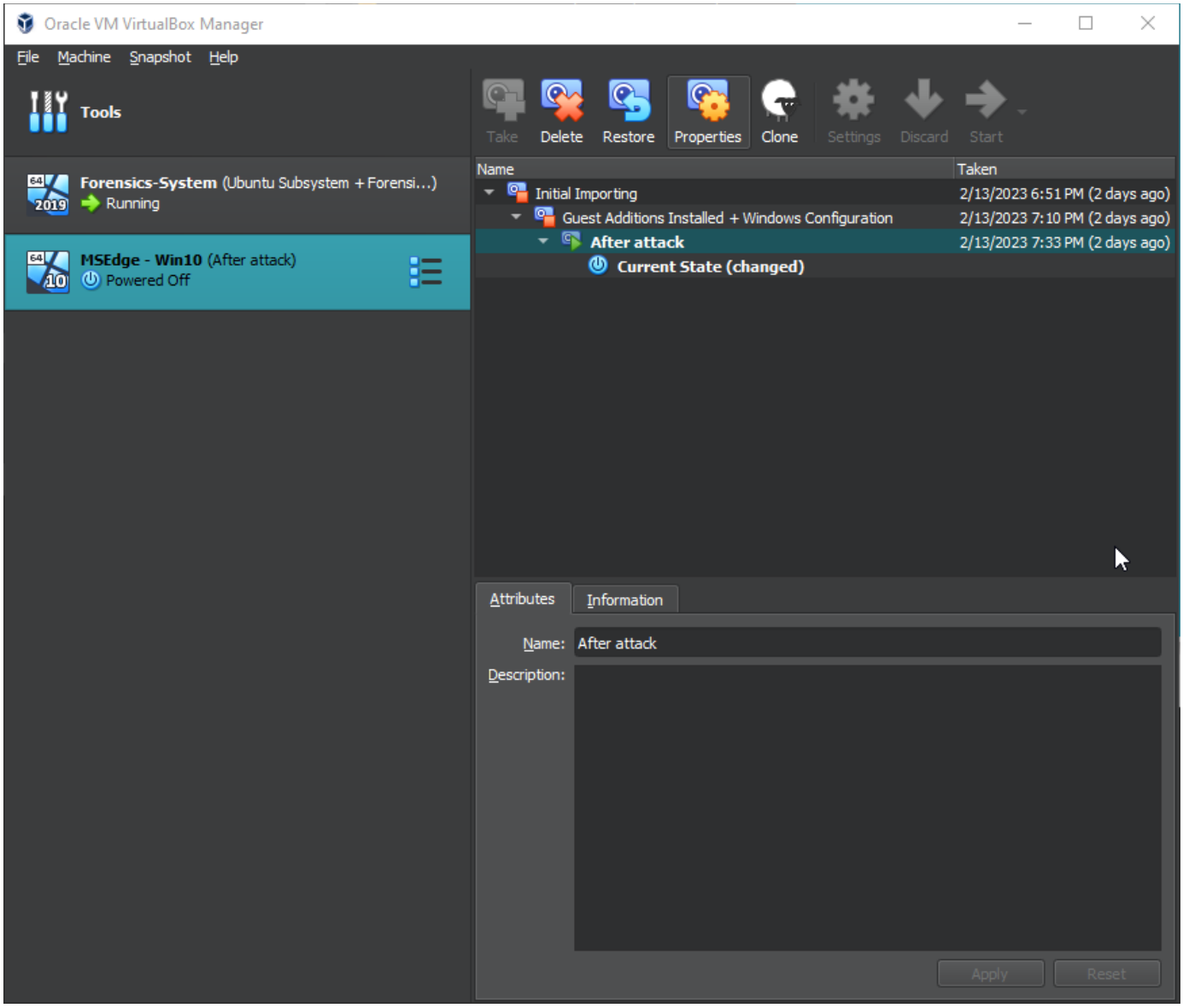


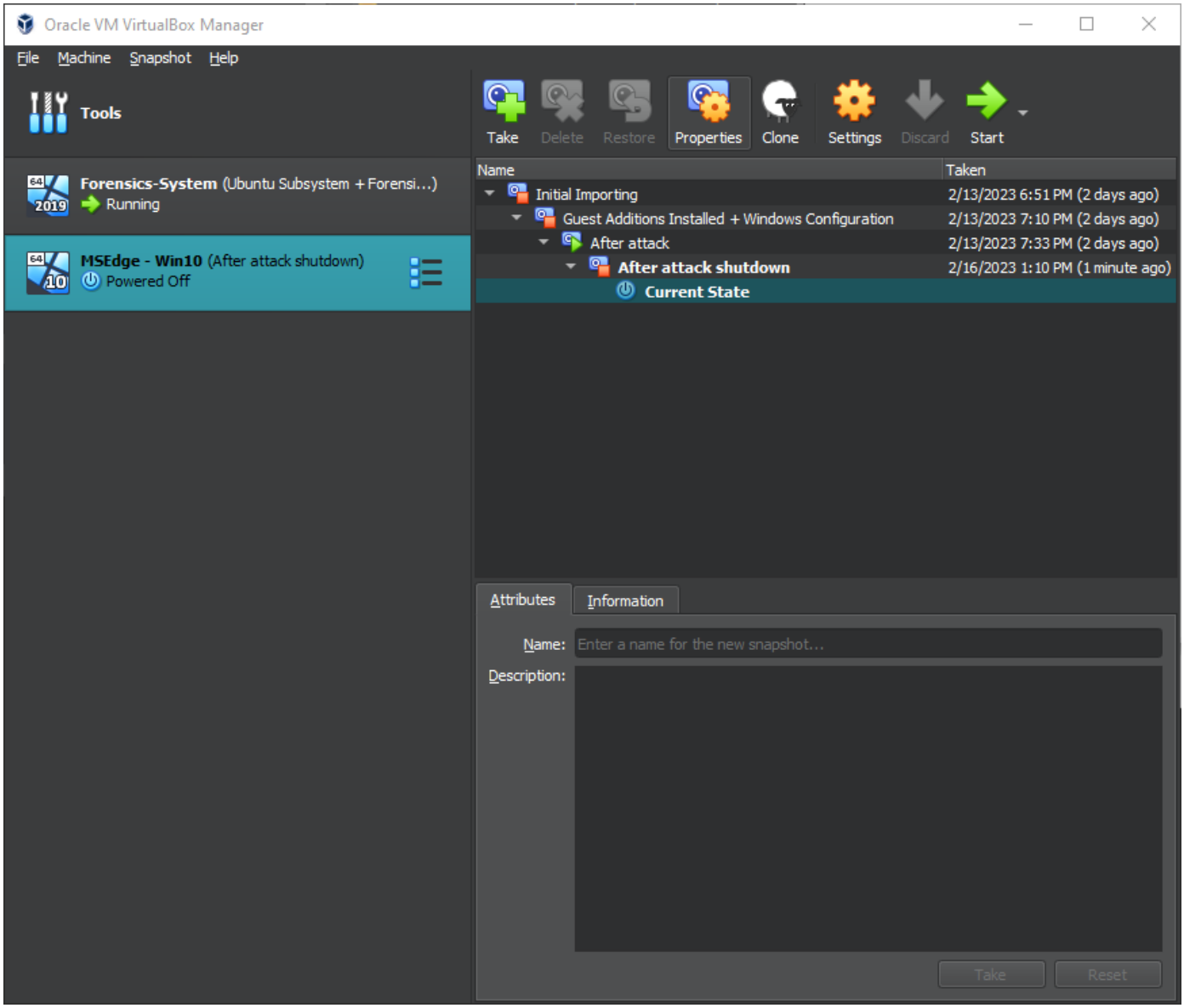
Line	Tag	Application Name	Program Id	File Key Last Write Timestamp	SHA1	Is Os Component	Full Path
1		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:51:44	6e5a4fdb4447e215cf5eb0127a5780fd5742d29c	☑	c:\windows\syst
2		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:48:39	087516f64e124b47178812eb5c13da6e689c9ca6	☑	c:\windows\syst
3		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:48:35	8f9bc1b7d65188d0adbdf74ccce4eed78bf4c129	☑	c:\windows\syst
4		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:56:20	786ba7f76fbc3c40e7a84f4d7066d7a078439665	☑	c:\windows\syst
5		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:56:06	c1d1f6af856eaec6f309186575839aaafd3bef00	☑	c:\windows\syst
6		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:48:30	e86b11544c4d850eb6c8a83af60cc011b697863b	☑	c:\windows\syst
7		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:52:20	11327106e4fded18ea439f14cd8c980d711adabe	☑	c:\windows\syst
8		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:48:48	254395abacb14fdaf5d13e9757165efcd48477ce	☑	c:\windows\syst
9		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:56:26	7693be70ba30ba9659c028c5c8d8c4c481c2f89f	☑	c:\windows\syst
10		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:56:24	f5d0299140cf98875b07dbd2d892617401dad8b9	☑	c:\windows\expl
11		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:56:24	0950dd0f72d2eb578a8609f82ea6d5edbe4a96ff	☑	c:\windows\syst
12		Unassociated	00060f4e08decc6b33477cb37298ca37bb2800000904	2023-02-13 17:08:50	b4a549508cbc9f975a191434d4d20ad3c28d5028	☐	c:\users\ieuser
13		Unassociated	0006fc69c87e5d1b342ba6e5bf1acb2c203f00000904	2018-04-25 15:58:44	5b205fc1a25354726677a30b25d8e41b3ef69d84	☐	c:\users\ieuser
14		Unassociated	0006fc69c87e5d1b342ba6e5bf1acb2c203f00000904	2018-04-25 15:58:37	5b205fc1a25354726677a30b25d8e41b3ef69d84	☐	c:\windows\syst
15		Unassociated	0006fc69c87e5d1b342ba6e5bf1acb2c203f00000904	2018-04-25 15:58:46	5b205fc1a25354726677a30b25d8e41b3ef69d84	☐	c:\users\ieuser
16		Unassociated	0006fc69c87e5d1b342ba6e5bf1acb2c203f00000904	2018-04-25 15:58:33	5b205fc1a25354726677a30b25d8e41b3ef69d84	☐	c:\users\ieuser
17		Unassociated	0006110de35d53708cabebc9a10d21264a2000000904	2023-02-13 17:17:40	e70c1a502ed33fc3ff6796771f5169f32cc8a9e5	☐	c:\windows\syst
18		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:56:06	71e7c4d5b375079d63fe78c9f34995e82f894ee0	☑	c:\program file
19		Unassociated	0006e27730a8332fe2ec147ea6466d6532aa00000904	2023-02-13 17:03:44	a108a8cea0db502079176fcf81190a1506d5a5b6	☐	c:\programdata\
20		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2023-02-13 17:09:09	5ac6e790ed19fdc66988648cbb22073c4a2719ba	☑	c:\program file
21		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2023-02-13 17:19:25	ab87af56870cff3b032d880edbf7ace8aabe6a27	☑	c:\windows\syst
22		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:51:44	867b54f1bc5b71045a9a00baca485a24176b202c	☑	c:\windows\syst
23		Unassociated	0006d330fd863a425c3d6fa5390d5d0c0d7000000904	2018-04-25 15:56:07	fbbfccad3b5428e013c1ed056de2840e1a52c0b9	☐	c:\users\ieuser
24		Unassociated	0006d330fd863a425c3d6fa5390d5d0c0d7000000904	2018-04-25 15:50:32	e8bd756a969cd716cab14905373e7dfdbba2f2ab	☐	c:\users\ieuser
25		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:49:56	3cee5a11b2528e66184e607fc62c4bd22dd25706	☑	c:\windows\sysw
26		Unassociated	0006df8f19fbe059c89330971e8f66fe2c3500000904	2023-02-13 17:08:28	57b7fc9bf59cf09a9c19ad0ce0a159746554d682	☐	c:\users\ieuser
27		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:52:20	2f34ccfdd8141aeee2e89ffb070ce239c7d00706	☑	c:\windows\syst
28		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:49:56	ebe636bcf0174dd7b391c8b644e0a71c33d826c0	☑	c:\windows\syst
29		Unassociated	00069946de00c1901212411bd7a3d7ab05dac00000904	2023-02-13 17:13:32	4e40d590da1357a750c341d772ede6f2b1c479ee	☐	c:\program file
30		Unassociated	00069946de00c1901212411bd7a3d7ab05dac00000904	2023-02-13 17:13:32	3d9ee67daddbcf14f48bad70ea19e3dee4667cc9	☐	c:\program file
31		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:56:20	e2caded832396d1be66089217ce4f11b691bc110	☑	c:\windows\syst
32		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2023-02-13 17:08:01	0e5421e832745a3b285a474ef7afe40d47b7f428	☑	c:\windows\syst
33		Unassociated	0000f519feec486de87ed73cb92d3cac802400000000	2018-04-25 15:56:20	660b76b6fb802417d513adc967c5caf77fc2bac6	☑	c:\windows\syst

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

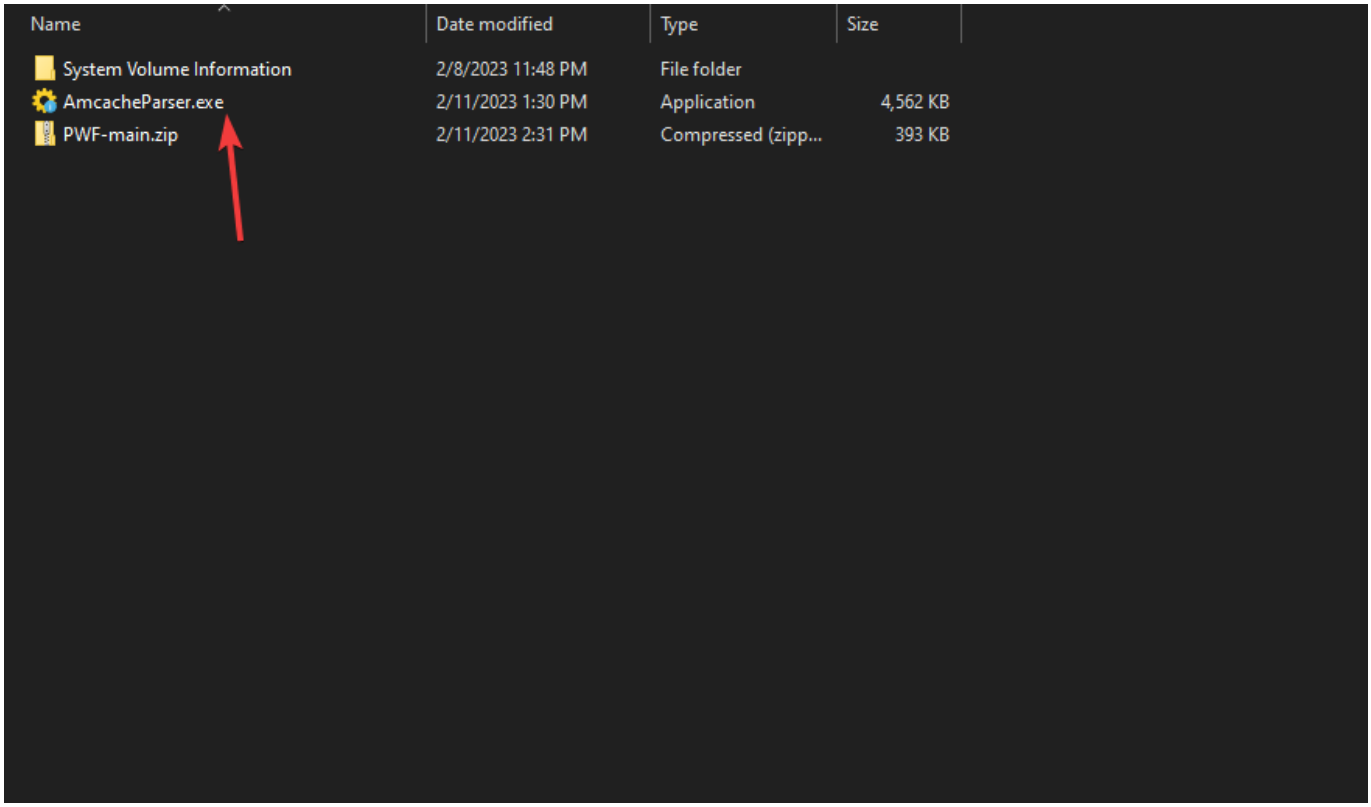
```
02/14/2023  03:10 PM    <DIR>          .
02/14/2023  03:10 PM    <DIR>          ..
02/13/2023  05:57 PM         1,048,576 Amcache.hve
04/25/2018  03:48 PM           262,144 Amcache.hve.LOG1
04/25/2018  03:48 PM                 0 Amcache.hve.LOG2
```

- We need to open the compromised system :

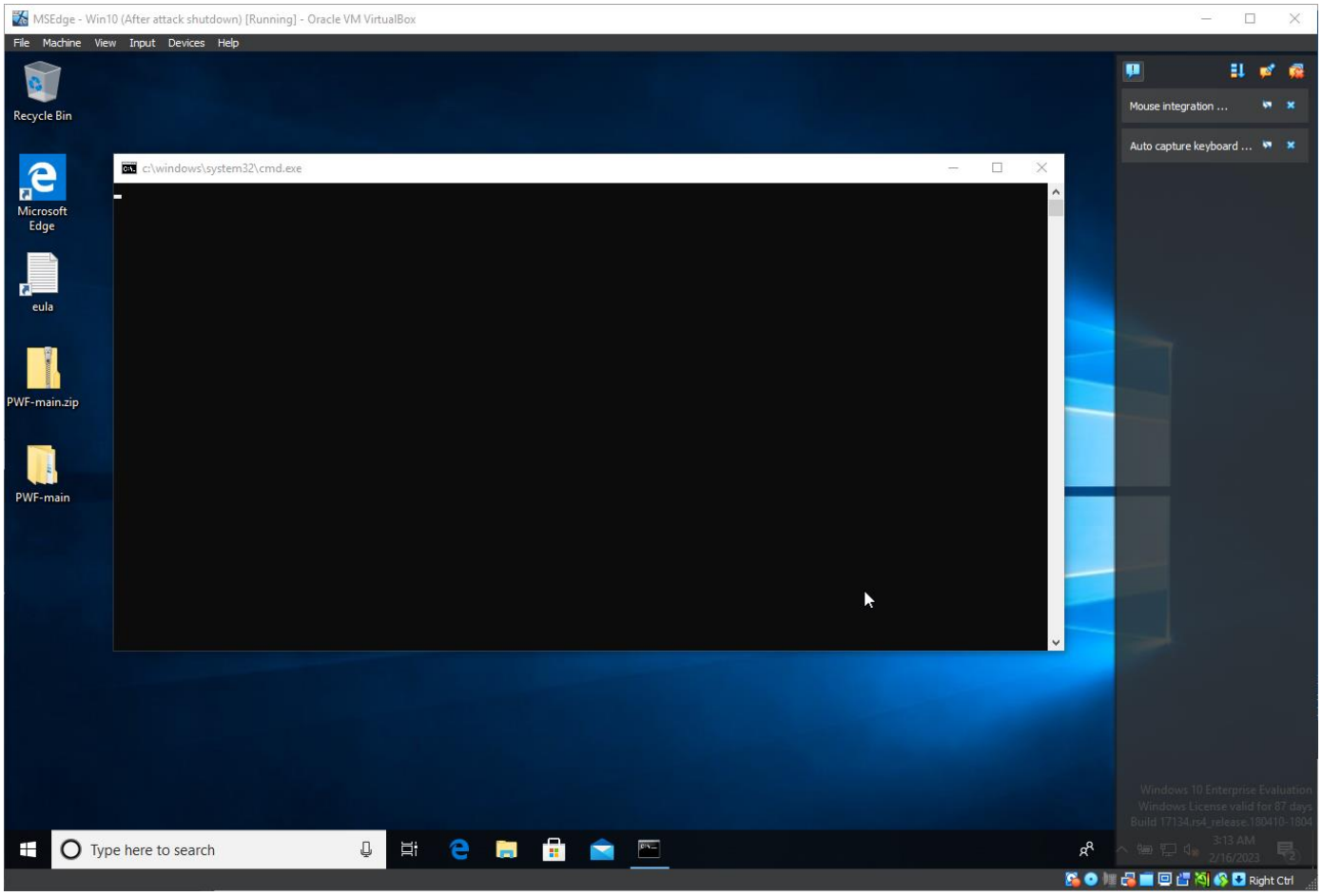


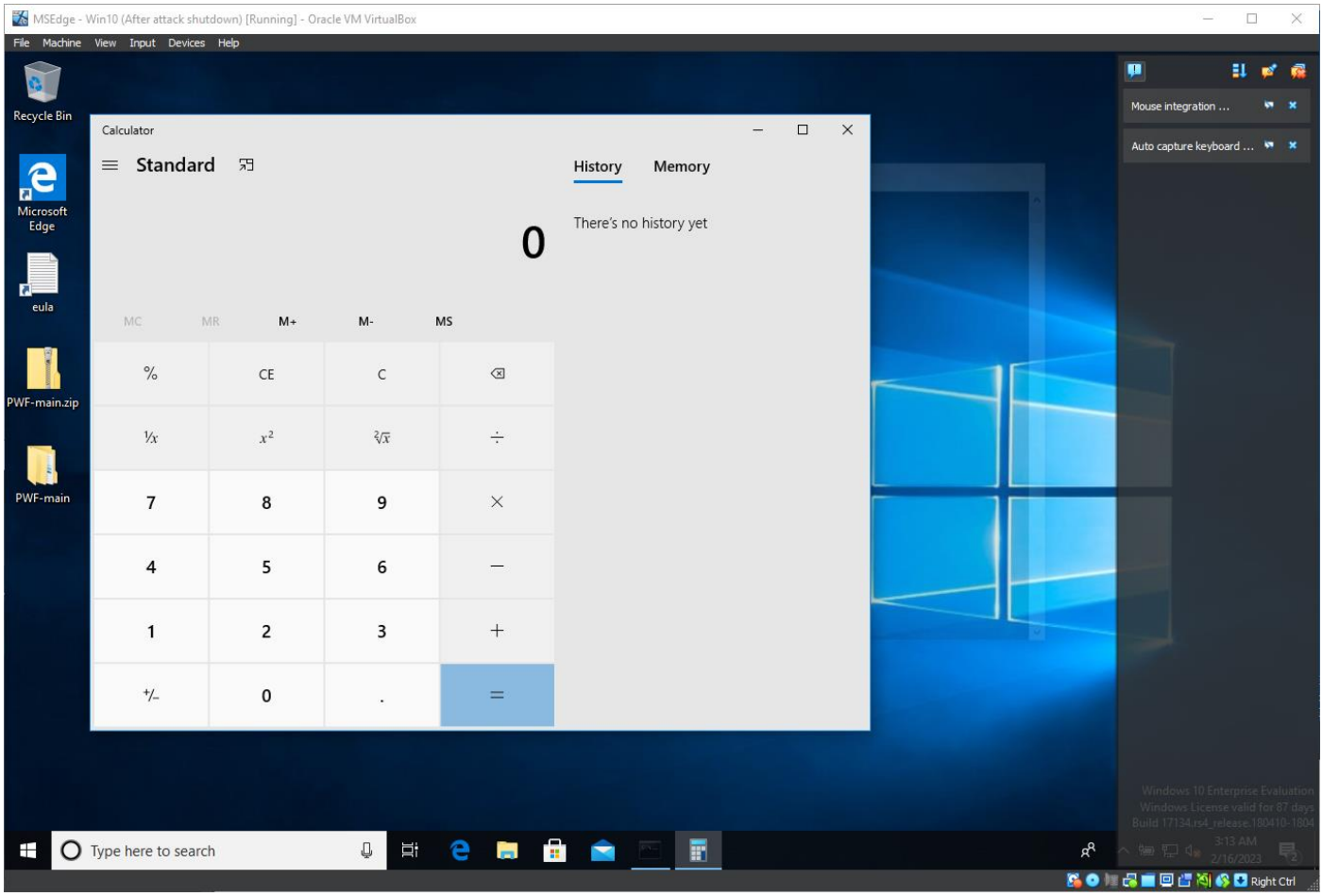


- AmcacheParser to put in the compromised system shared folder: https://f001.backblazeb2.com/file/EricZimmermanTools/AmcacheParser.zip

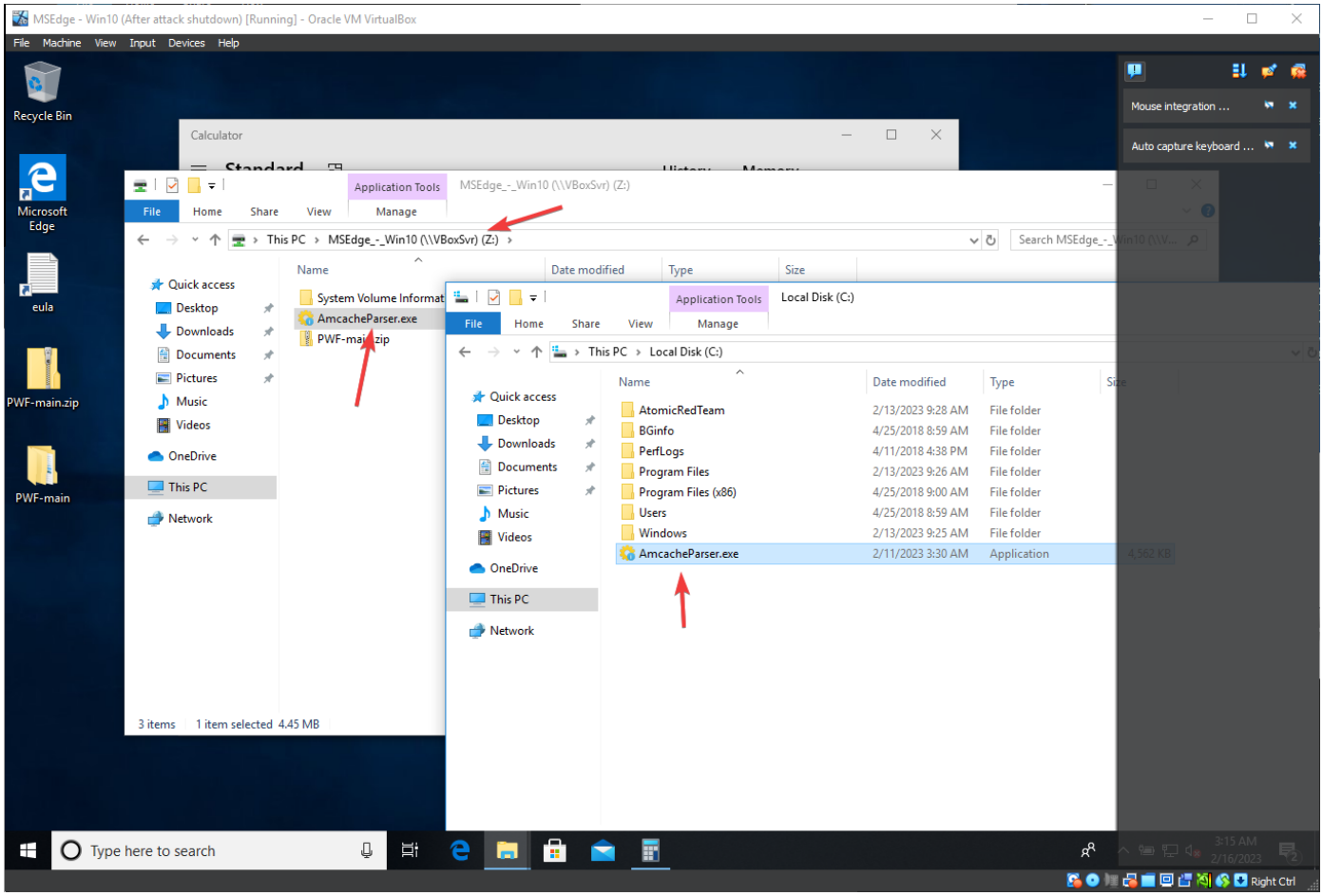


- Open compromised system. Typically you would disconnect from the network , the virtual machine , but there is nothing malicious in the virtual machine.
- Persistence techniques, following in the further analysis:

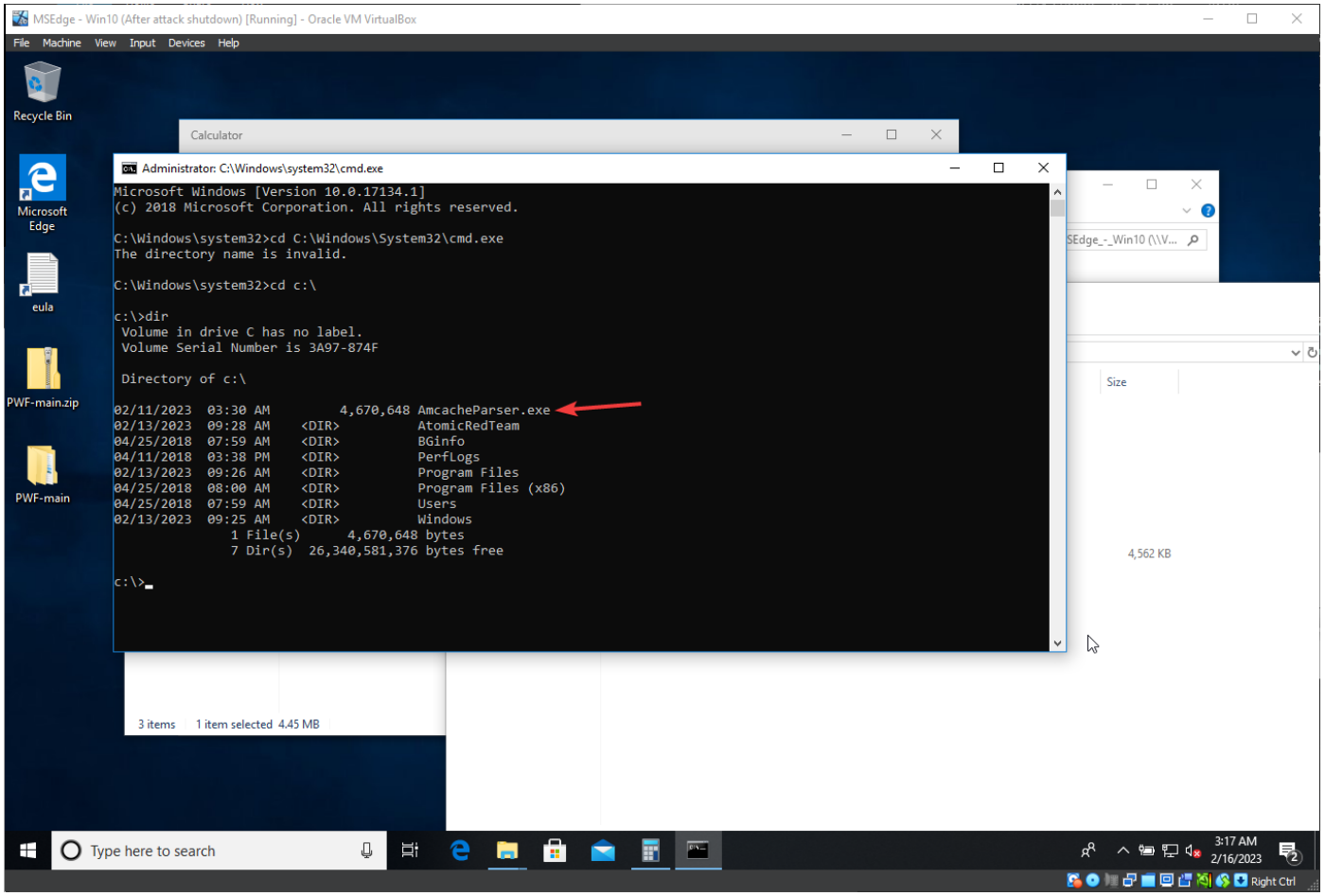

MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
c:\windows\system32\cmd.exe
Mouse integration ...
Auto capture keyboard ...
Type here to search
Windows 10 Enterprise Evaluation
Windows License valid for 87 days
Build 17134.rs4_release.180410-1804
3:13 AM
2/16/2023
Right Ctrl

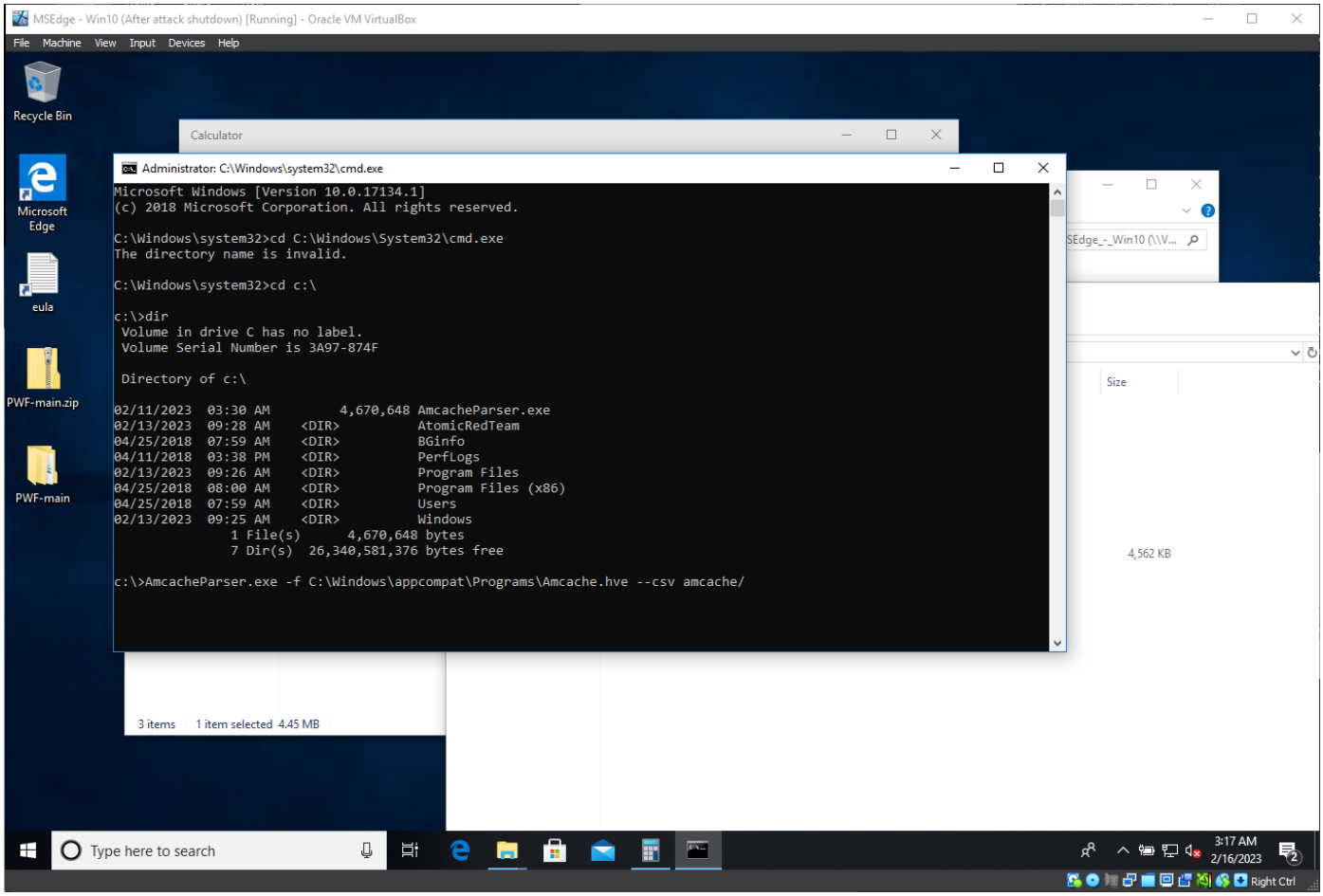


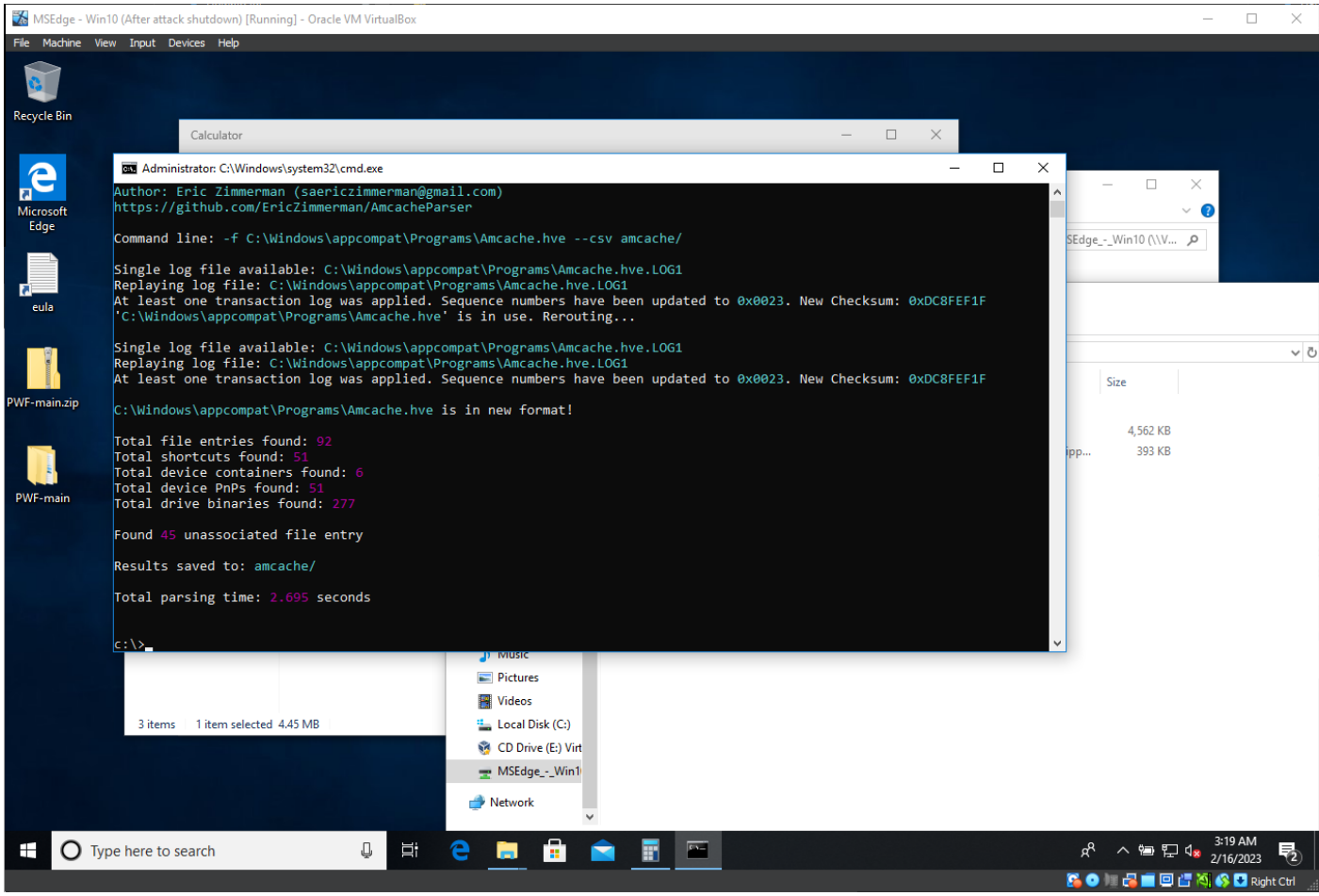
- Copy the file wherever you want



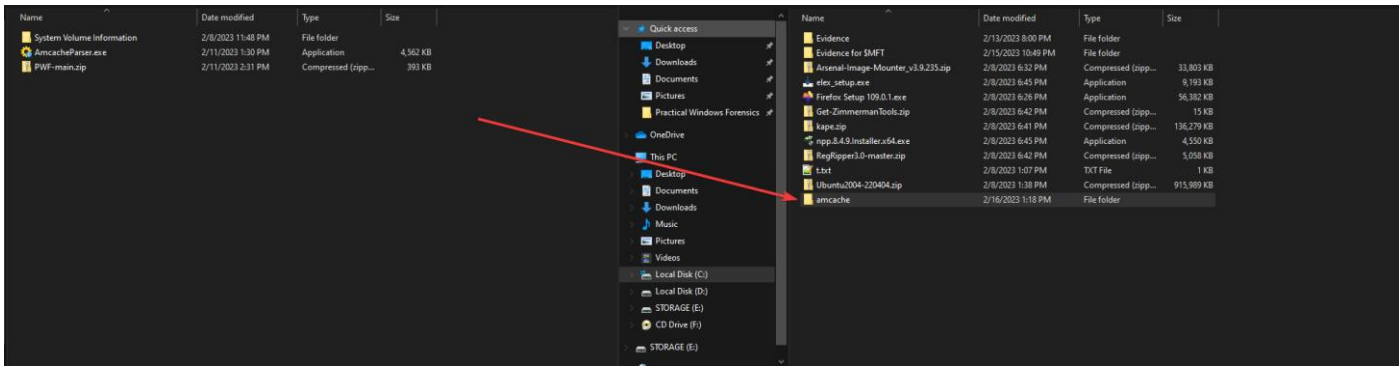
- Parse the amchache hive:


MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Calculator
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.1]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\Windows\System32\cmd.exe
The directory name is invalid.
C:\Windows\system32>cd c:\
c:\>dir
Volume in drive C has no label.
Volume Serial Number is 3A97-874F
Directory of c:\
02/11/2023 03:30 AM 4,670,648 AmcacheParser.exe
02/13/2023 09:28 AM <DIR> AtomicRedTeam
04/25/2018 07:59 AM <DIR> BGinfo
04/11/2018 03:38 PM <DIR> PerfLogs
02/13/2023 09:26 AM <DIR> Program Files
04/25/2018 08:00 AM <DIR> Program Files (x86)
04/25/2018 07:59 AM <DIR> Users
02/13/2023 09:25 AM <DIR> Windows
1 File(s) 4,670,648 bytes
7 Dir(s) 26,340,581,376 bytes free
c:\>
Size
4,562 KB
3 items 1 item selected 4.45 MB
Type here to search
3:17 AM
2/16/2023
Right Ctrl

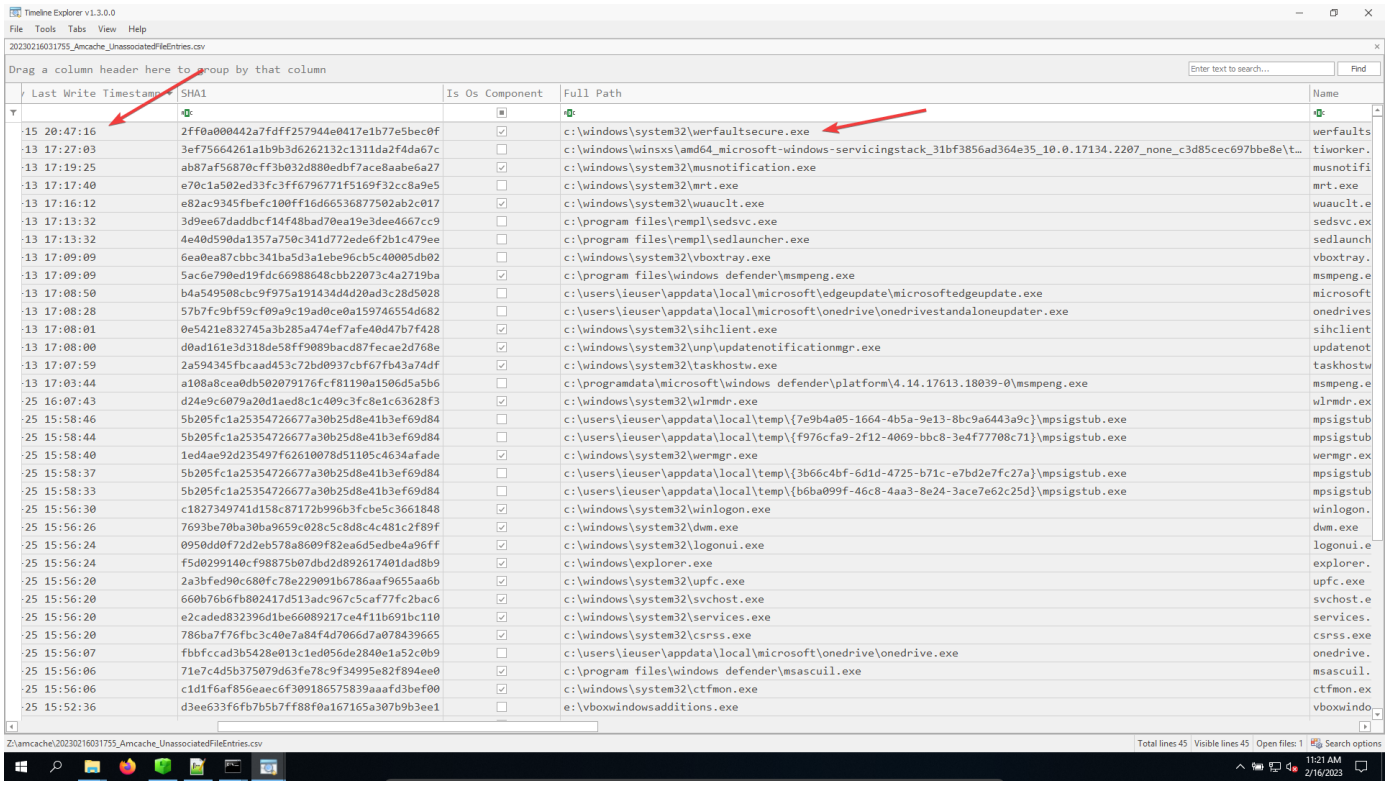

MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Calculator
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.1]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd C:\Windows\System32\cmd.exe
The directory name is invalid.
C:\Windows\system32>cd c:\
c:\>dir
Volume in drive C has no label.
Volume Serial Number is 3A97-874F
Directory of c:\
02/11/2023 03:30 AM 4,670,648 AmcacheParser.exe
02/13/2023 09:28 AM <DIR> AtomicRedTeam
04/25/2018 07:59 AM <DIR> BGinfo
04/11/2018 03:38 PM <DIR> PerfLogs
02/13/2023 09:26 AM <DIR> Program Files
04/25/2018 08:00 AM <DIR> Program Files (x86)
04/25/2018 07:59 AM <DIR> Users
02/13/2023 09:25 AM <DIR> Windows
1 File(s) 4,670,648 bytes
7 Dir(s) 26,340,581,376 bytes free
c:\>AmcacheParser.exe -f C:\Windows\appcompat\Programs\Amcache.hve --csv amcache/
Size
4,562 KB
3 items 1 item selected 4.45 MB
Type here to search
3:17 AM
2/16/2023
Right Ctrl



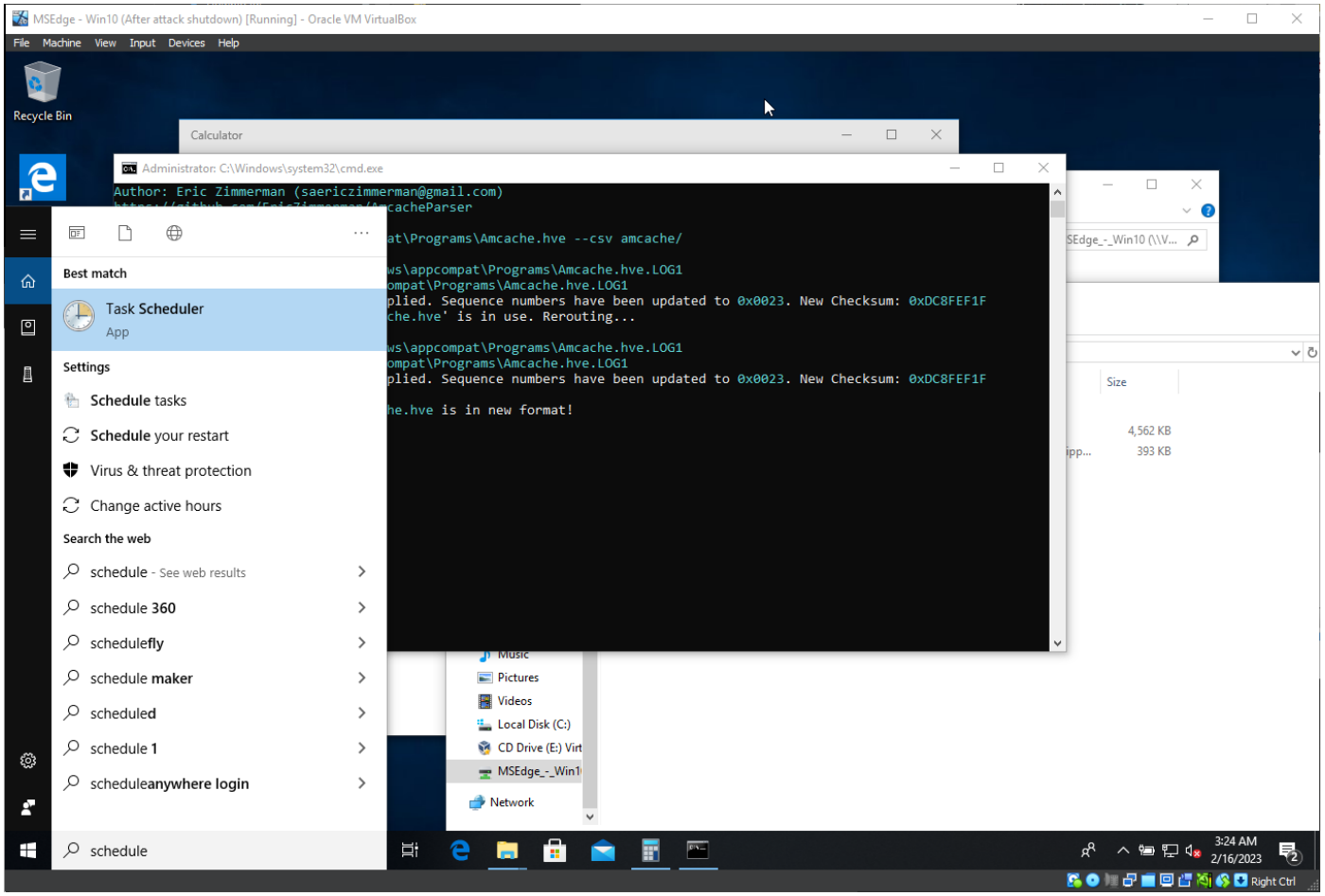
- Move it into the Forensic Workstation folder.

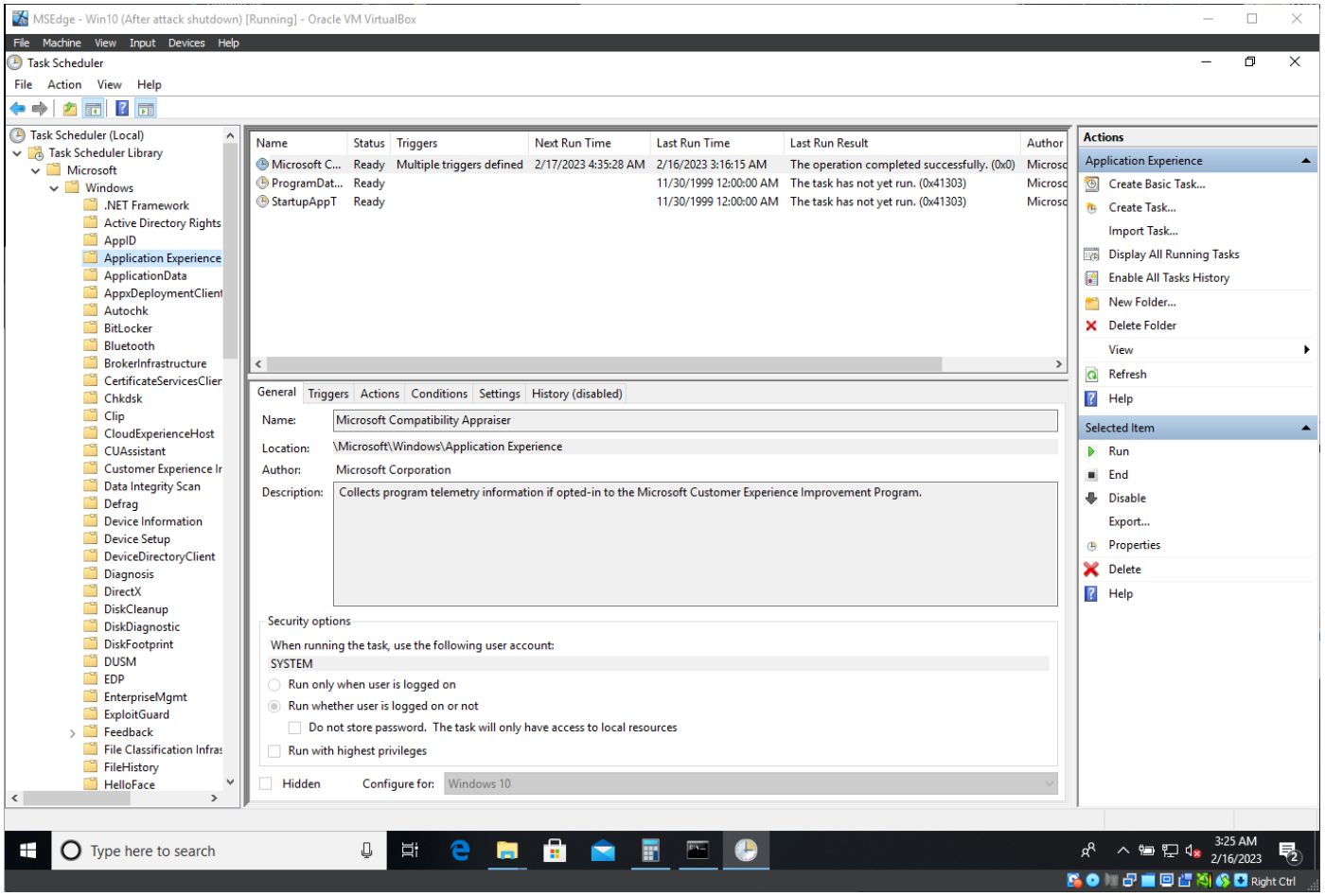


- Just one file added.

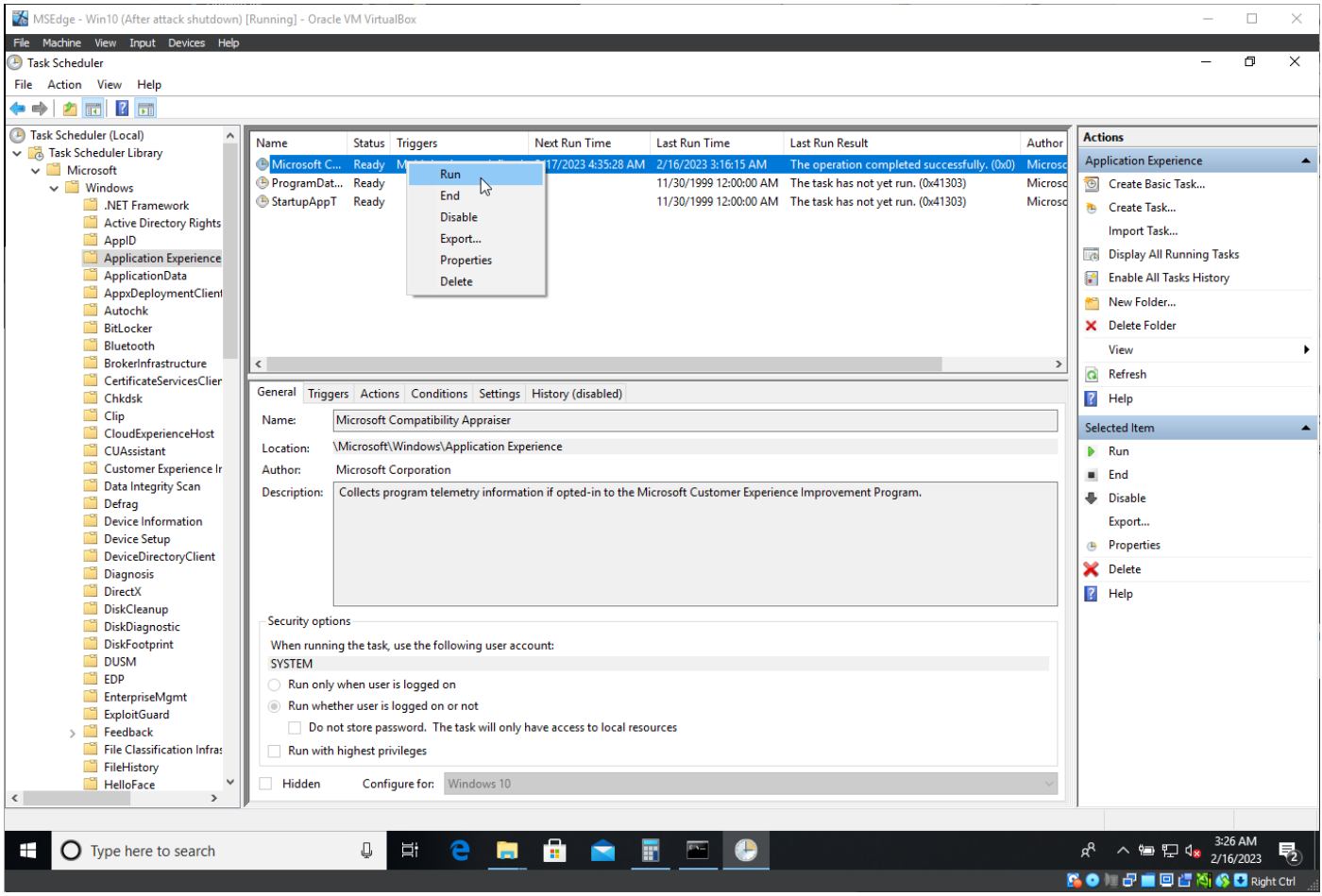


- According to : https://dfir.ru/2018/12/02/the-cit-database-and-the-syscache-hive/
- The executables are recorded in the Amcache when a particular “Microsoft Compatibility Appraiser” task is executed.
- Open Task Scheduler:

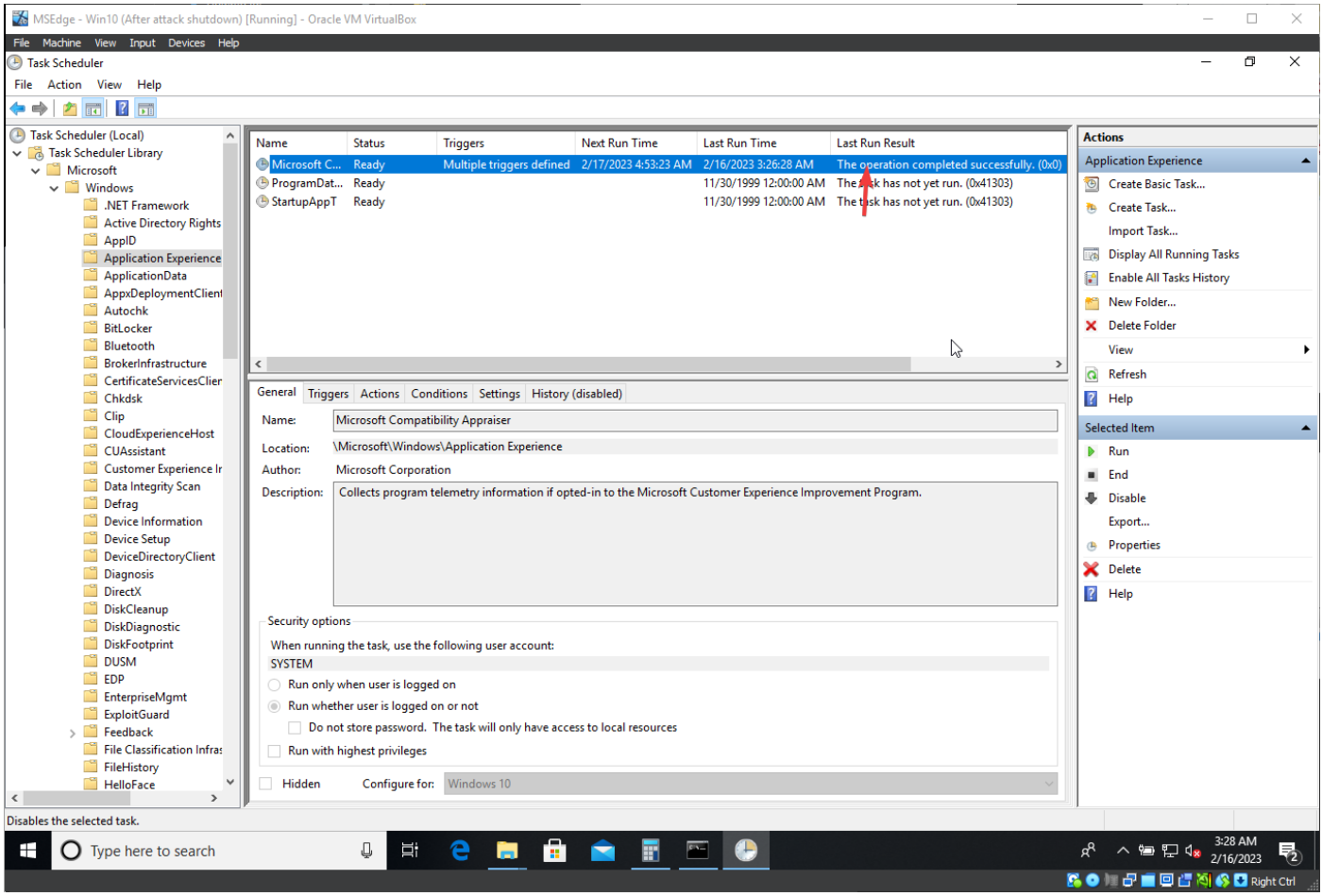

MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Calculator
Administrator: C:\Windows\system32\cmd.exe
Author: Eric Zimmerman (saericzimmerman@gmail.com)
at\Programs\Amcache.hve --csv amcache/
ws\appcompat\Programs\Amcache.hve.LOG1
ompat\Programs\Amcache.hve.LOG1
plied. Sequence numbers have been updated to 0x0023. New Checksum: 0xDC8FEF1F
che.hve' is in use. Rerouting...
ws\appcompat\Programs\Amcache.hve.LOG1
ompat\Programs\Amcache.hve.LOG1
plied. Sequence numbers have been updated to 0x0023. New Checksum: 0xDC8FEF1F
he.hve is in new format!
Best match
Task Scheduler
App
Settings
Schedule tasks
Schedule your restart
Virus & threat protection
Change active hours
Search the web
schedule - See web results
schedule 360
schedulefly
schedule maker
scheduled
schedule 1
scheduleanywhere login
schedule
Size
4,562 KB
393 KB
Music
Pictures
Videos
Local Disk (C:)
CD Drive (E:) Virt
Network
3:24 AM
2/16/2023
Right Ctrl



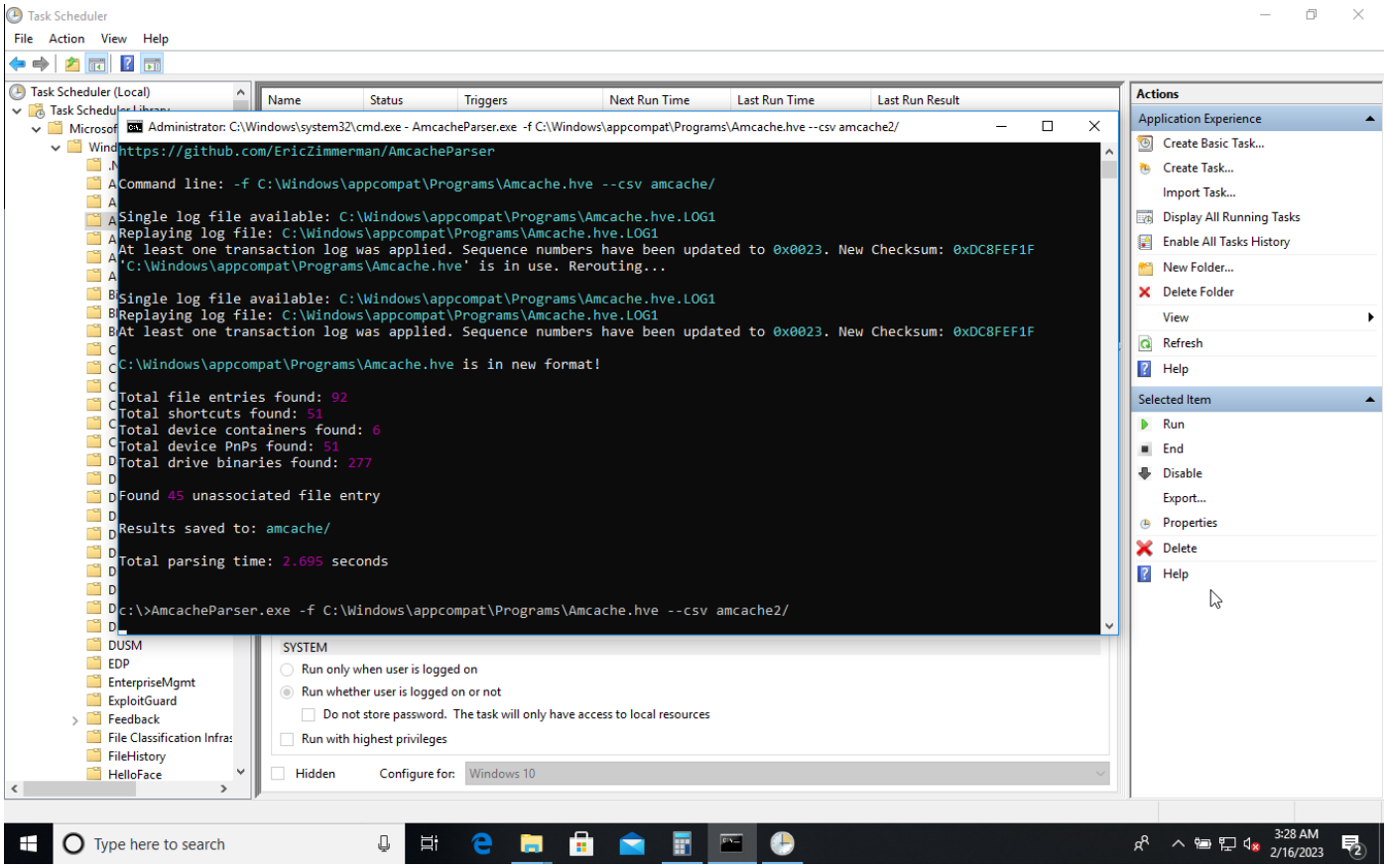
- Run the Microsoft Compatibility Appraiser task:



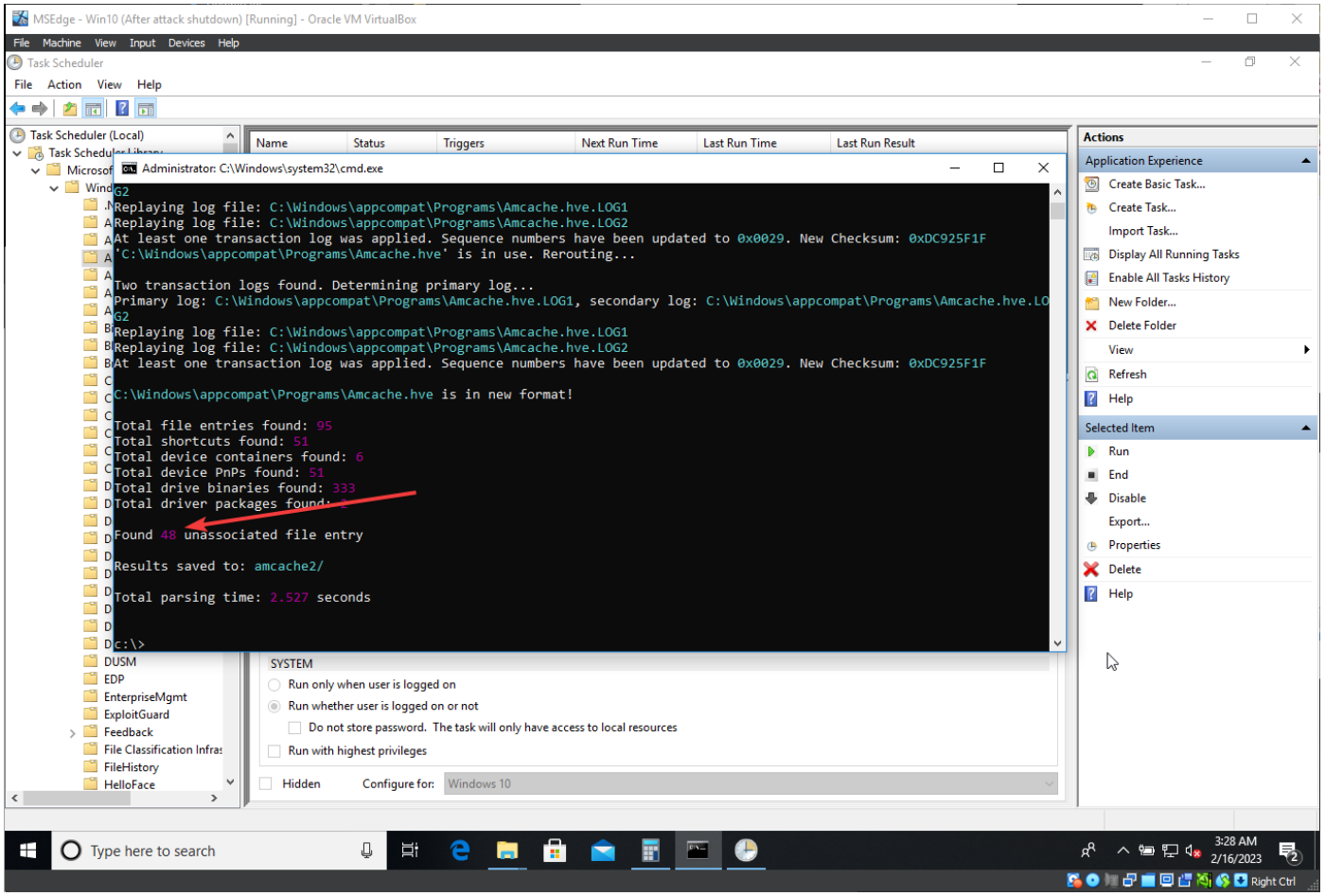
- Wait for it to finish.


MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Task Scheduler
File Action View Help
Task Scheduler (Local)
Task Scheduler Library
Microsoft
Windows
.NET Framework
Active Directory Rights
AppID
Application Experience
ApplicationData
AppxDeploymentClient
Autochk
BitLocker
Bluetooth
BrokerInfrastructure
CertificateServicesClier
Chkdsk
Clip
CloudExperienceHost
CUAssistant
Customer Experience Ir
Data Integrity Scan
Defrag
Device Information
Device Setup
DeviceDirectoryClient
Diagnosis
DirectX
DiskCleanup
DiskDiagnostic
DiskFootprint
DUSM
EDP
EnterpriseMgmt
ExploitGuard
Feedback
File Classification Infras
FileHistory
HelloFace
Name Status Triggers Next Run Time Last Run Time Last Run Result
Microsoft C... Ready Multiple triggers defined 2/17/2023 4:53:23 AM 2/16/2023 3:26:28 AM The operation completed successfully. (0x0)
ProgramDat... Ready 11/30/1999 12:00:00 AM The task has not yet run. (0x41303)
StartupAppT Ready 11/30/1999 12:00:00 AM The task has not yet run. (0x41303)
General Triggers Actions Conditions Settings History (disabled)
Name: Microsoft Compatibility Appraiser
Location: \Microsoft\Windows\Application Experience
Author: Microsoft Corporation
Description: Collects program telemetry information if opted-in to the Microsoft Customer Experience Improvement Program.
Security options
When running the task, use the following user account:
SYSTEM
Run only when user is logged on
Run whether user is logged on or not
Do not store password. The task will only have access to local resources
Run with highest privileges
Hidden
Configure for: Windows 10
Actions
Application Experience
Create Basic Task...
Create Task...
Import Task...
Display All Running Tasks
Enable All Tasks History
New Folder...
Delete Folder
View
Refresh
Help
Selected Item
Run
End
Disable
Export...
Properties
Delete
Help
Disables the selected task.
Type here to search
3:28 AM
2/16/2023
Right Ctrl

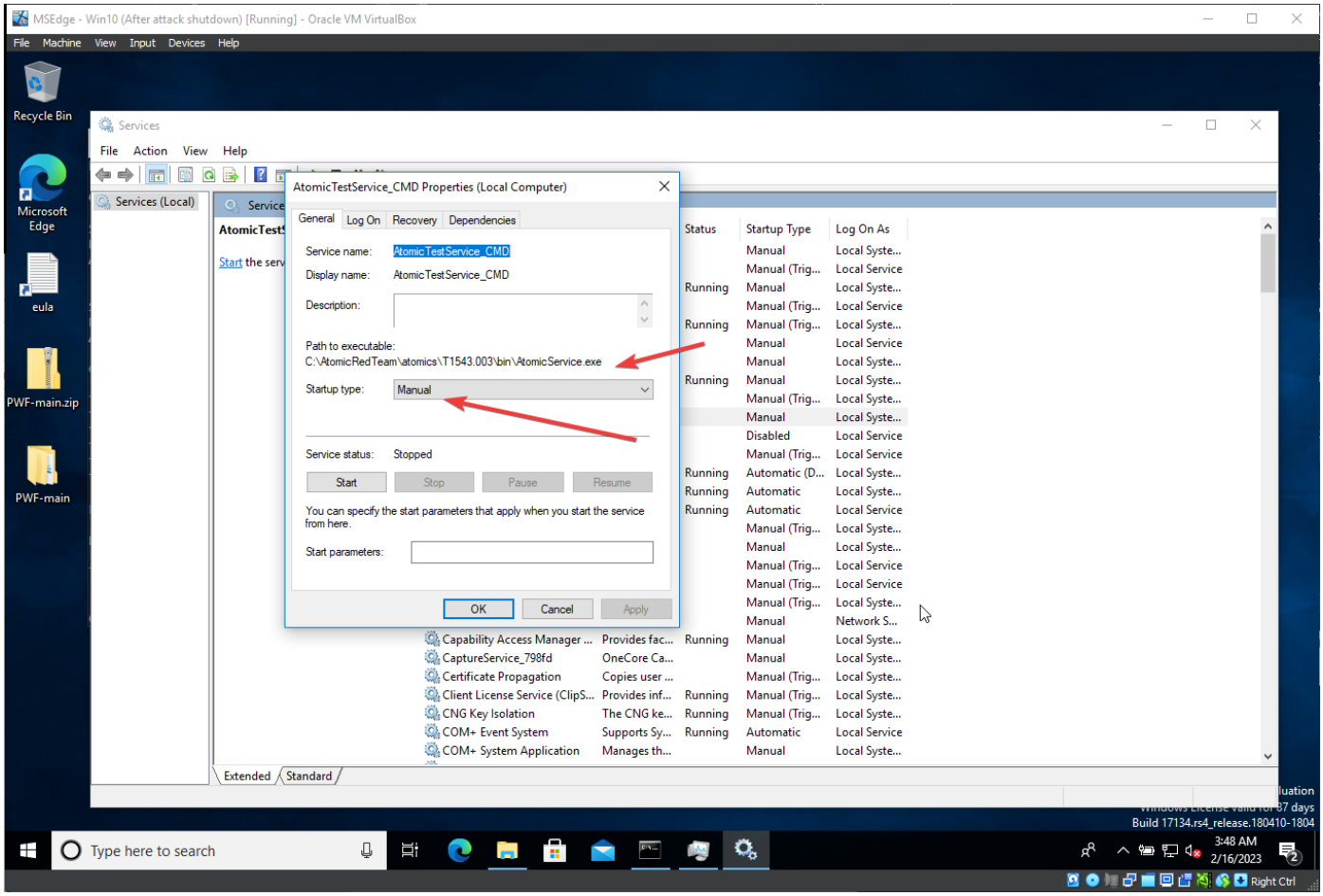
- Reparse it :

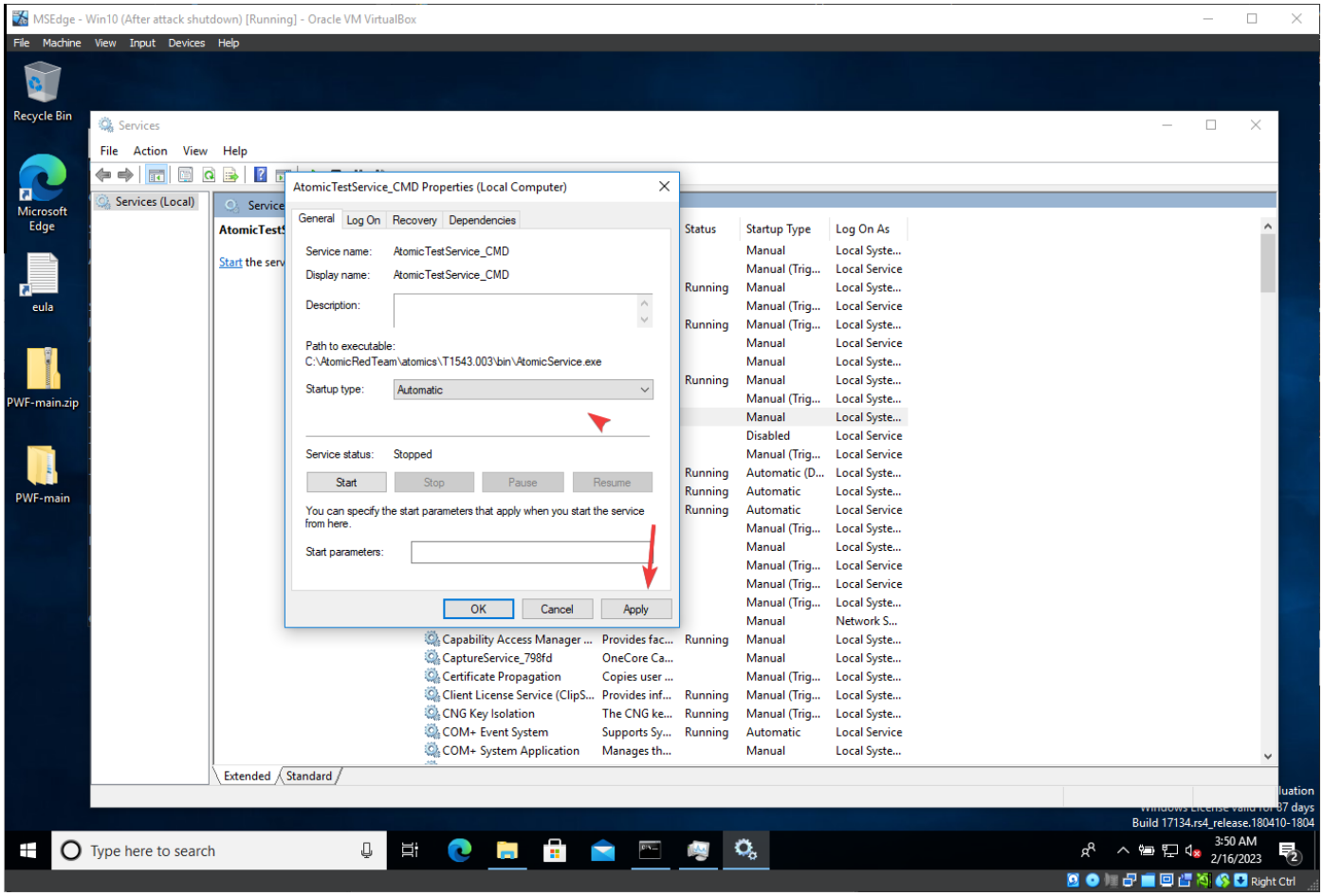


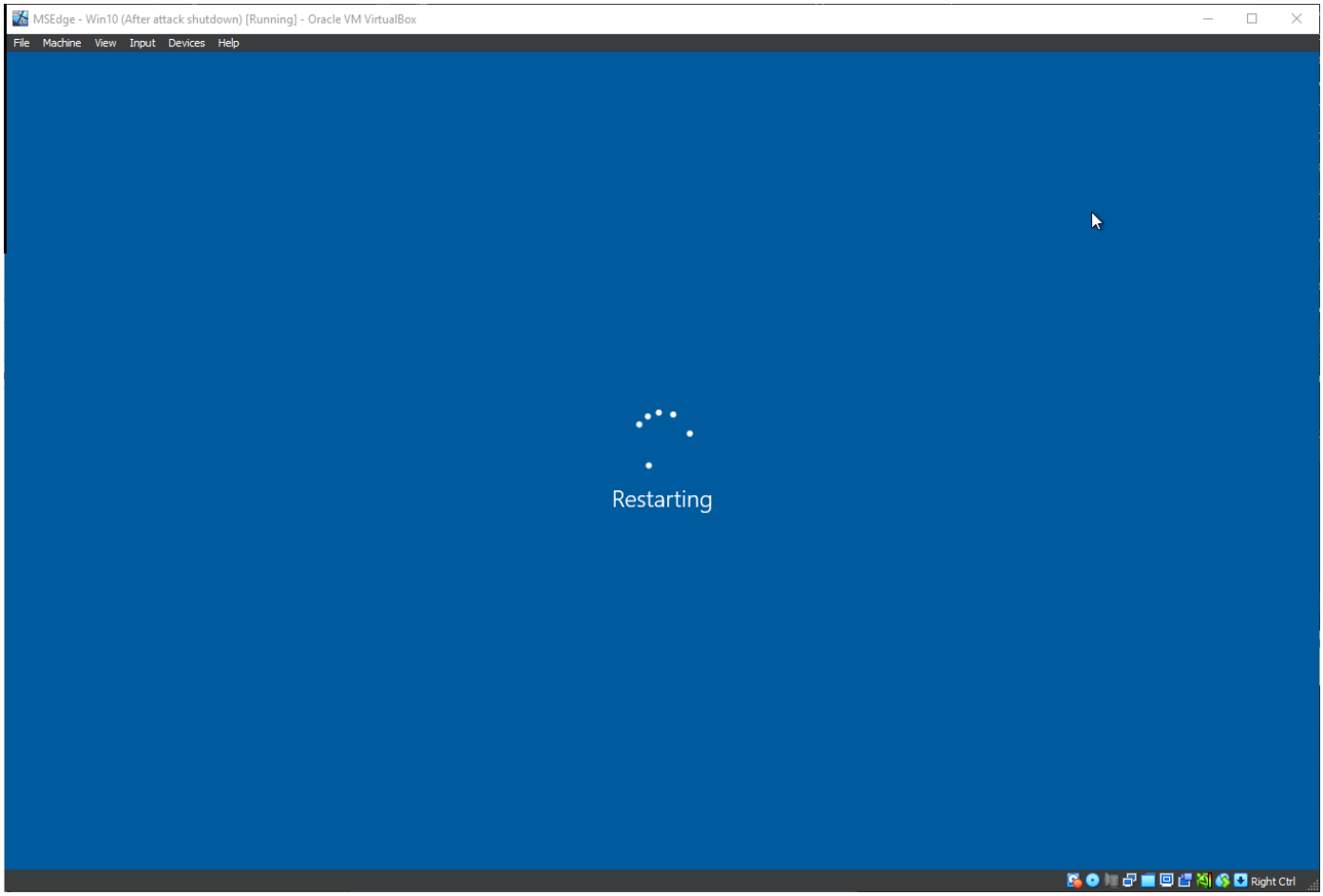
- The number changed:

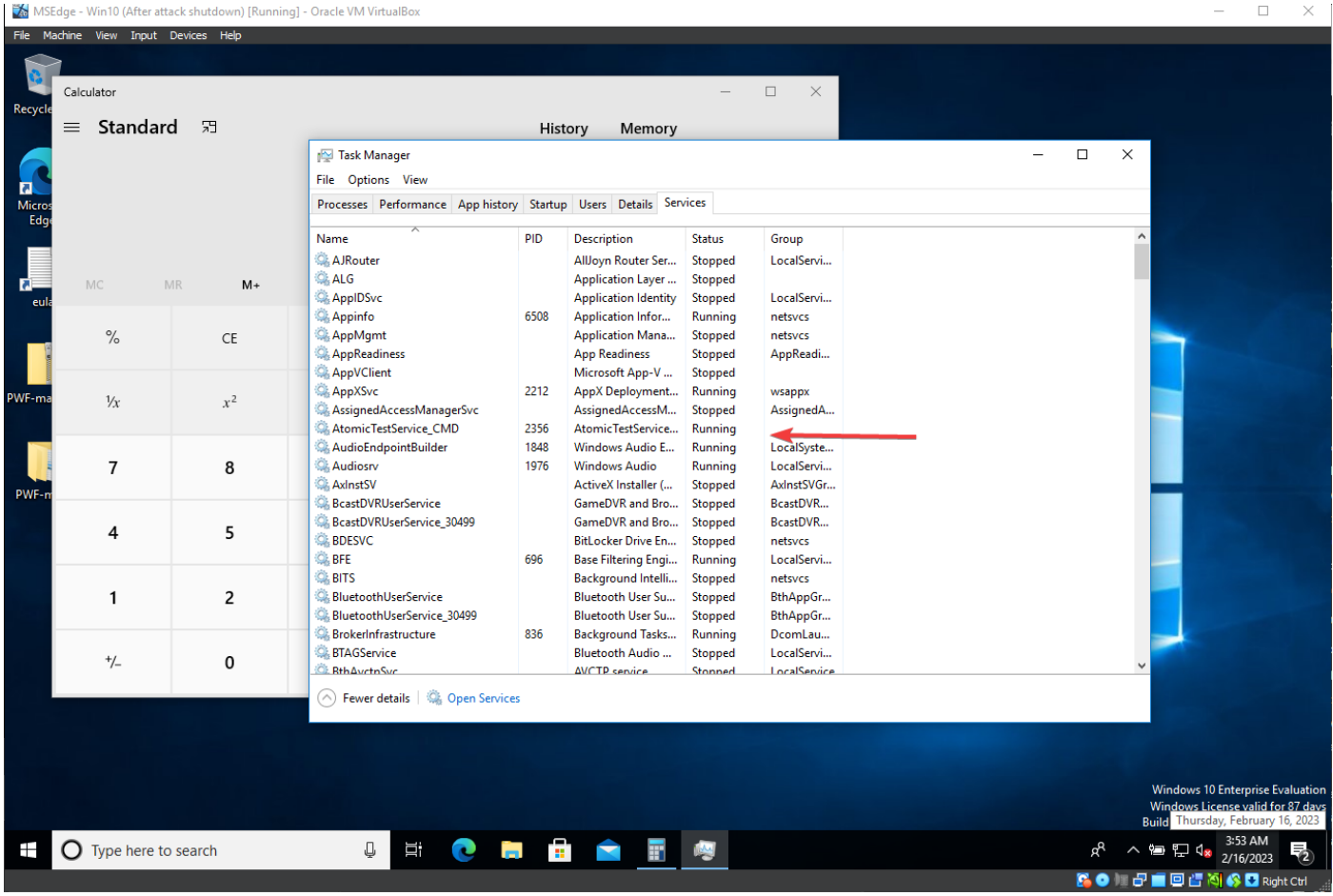


- Still no update.
- The service is actually loaded, but is set on startup manual. If we change the startup type to automatically and reboot the vm, update the task scheduler, parse the amcache, we should see it.

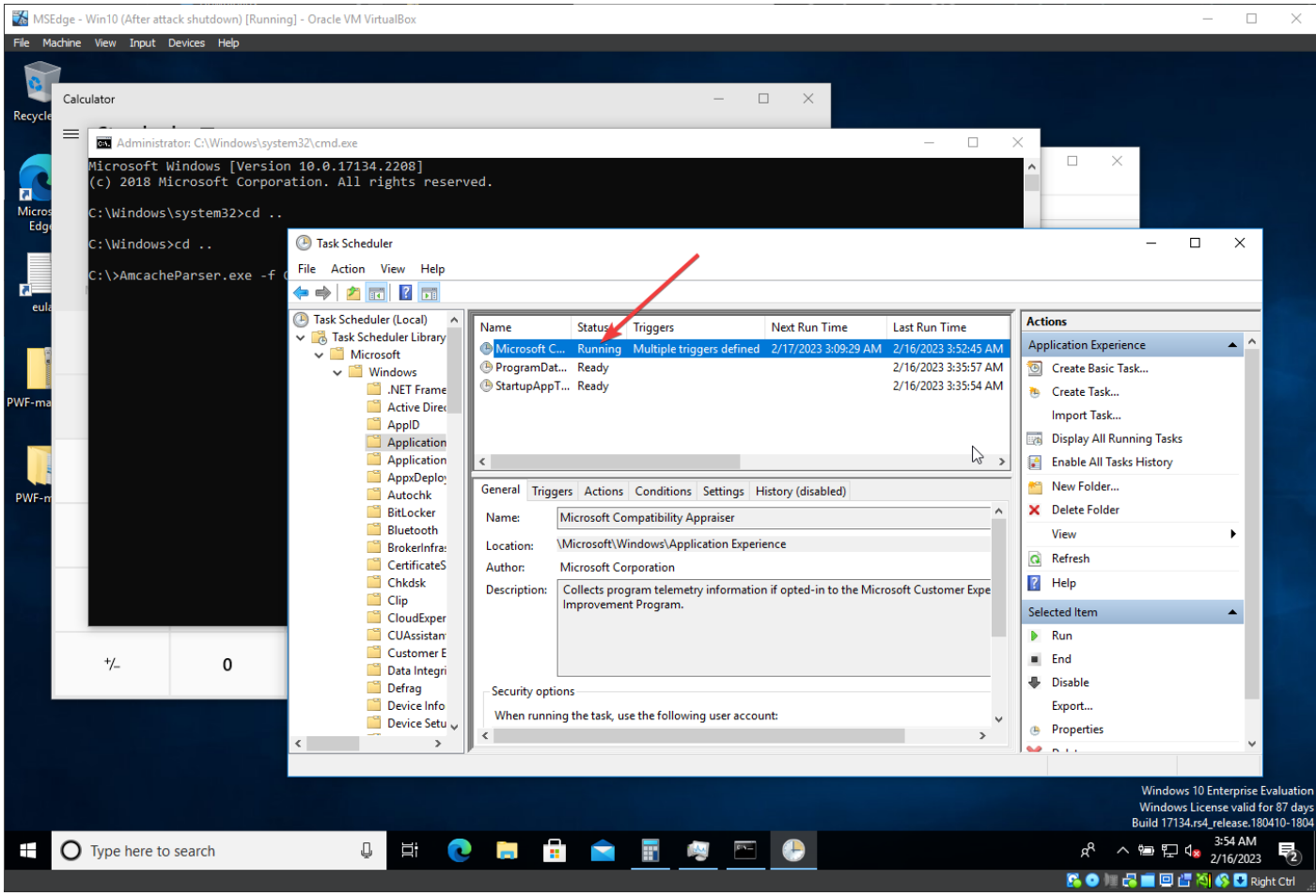

MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Services
File Action View Help
Services (Local)
AtomicTestService_CMD Properties (Local Computer)
General Log On Recovery Dependencies
Service name: AtomicTestService_CMD
Display name: AtomicTestService_CMD
Description:
Path to executable:
C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
Startup type: Manual
Service status: Stopped
Start Stop Pause Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK Cancel Apply
Status Startup Type Log On As
Capability Access Manager ... Provides fac... Running Manual Local Syste...
CaptureService_798fd OneCore Ca... Manual Local Syste...
Certificate Propagation Copies user ... Manual (Trig... Local Syste...
Client License Service (ClipS... Provides inf... Running Manual (Trig... Local Syste...
CNG Key Isolation The CNG ke... Running Manual (Trig... Local Syste...
COM+ Event System Supports Sy... Running Automatic Local Service
COM+ System Application Manages th... Manual Local Syste...
Extended Standard
Type here to search
3:48 AM
2/16/2023
Right Ctrl


MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Microsoft Edge
eula
PWF-main.zip
PWF-main
Services
File Action View Help
Services (Local)
AtomicTestService_CMD Properties (Local Computer)
General Log On Recovery Dependencies
Service name: AtomicTestService_CMD
Display name: AtomicTestService_CMD
Description:
Path to executable:
C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
Startup type: Automatic
Service status: Stopped
Start Stop Pause Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK Cancel Apply
Status Startup Type Log On As
Capability Access Manager ... Provides fac... Running Manual Local Syste...
CaptureService_798fd OneCore Ca... Manual Local Syste...
Certificate Propagation Copies user ... Manual (Trig... Local Syste...
Client License Service (ClipS... Provides inf... Running Manual (Trig... Local Syste...
CNG Key Isolation The CNG ke... Running Manual (Trig... Local Syste...
COM+ Event System Supports Sy... Running Automatic Local Service
COM+ System Application Manages th... Manual Local Syste...
Extended Standard
Type here to search
3:50 AM
2/16/2023
Right Ctrl

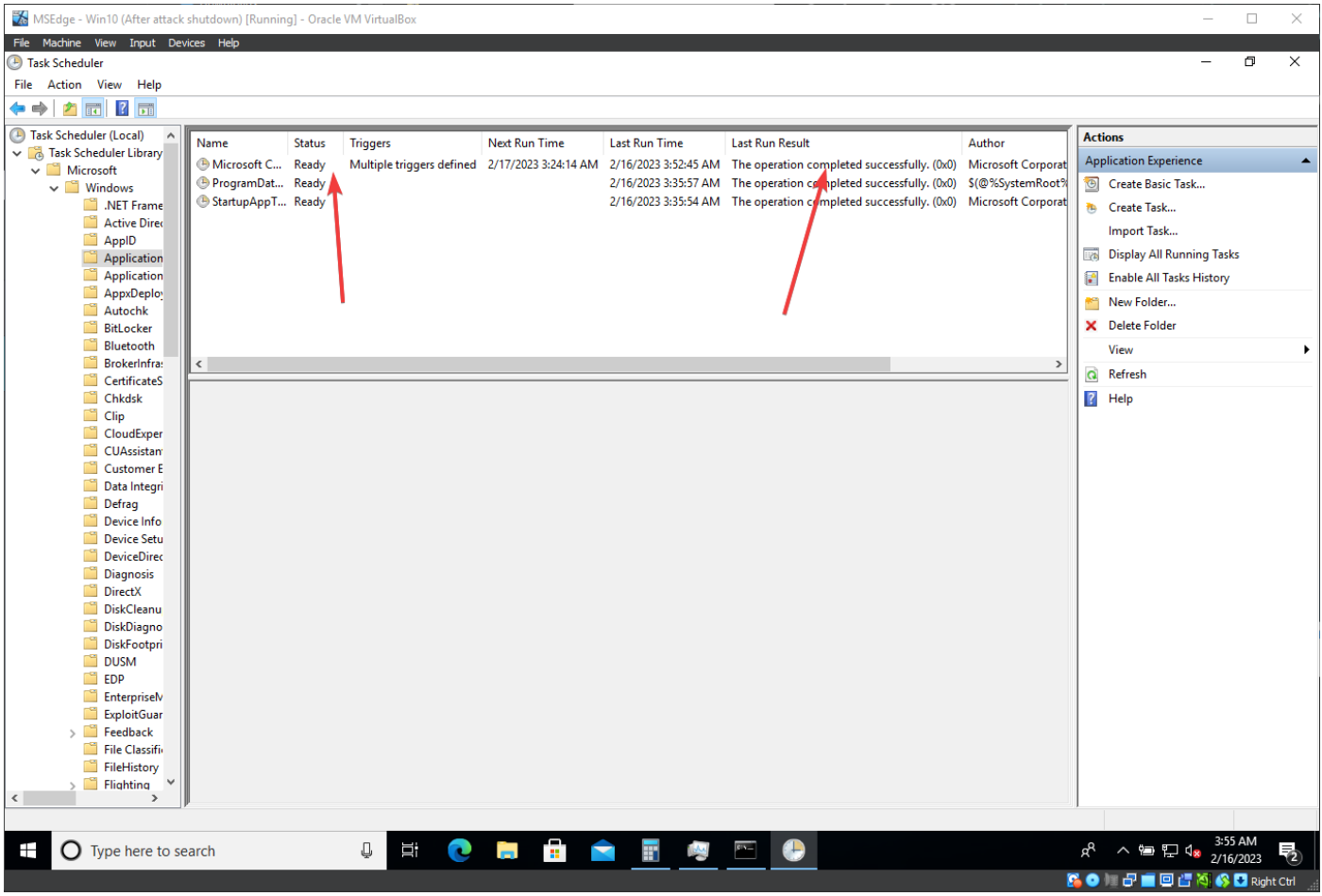

MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Restarting
Right Ctrl



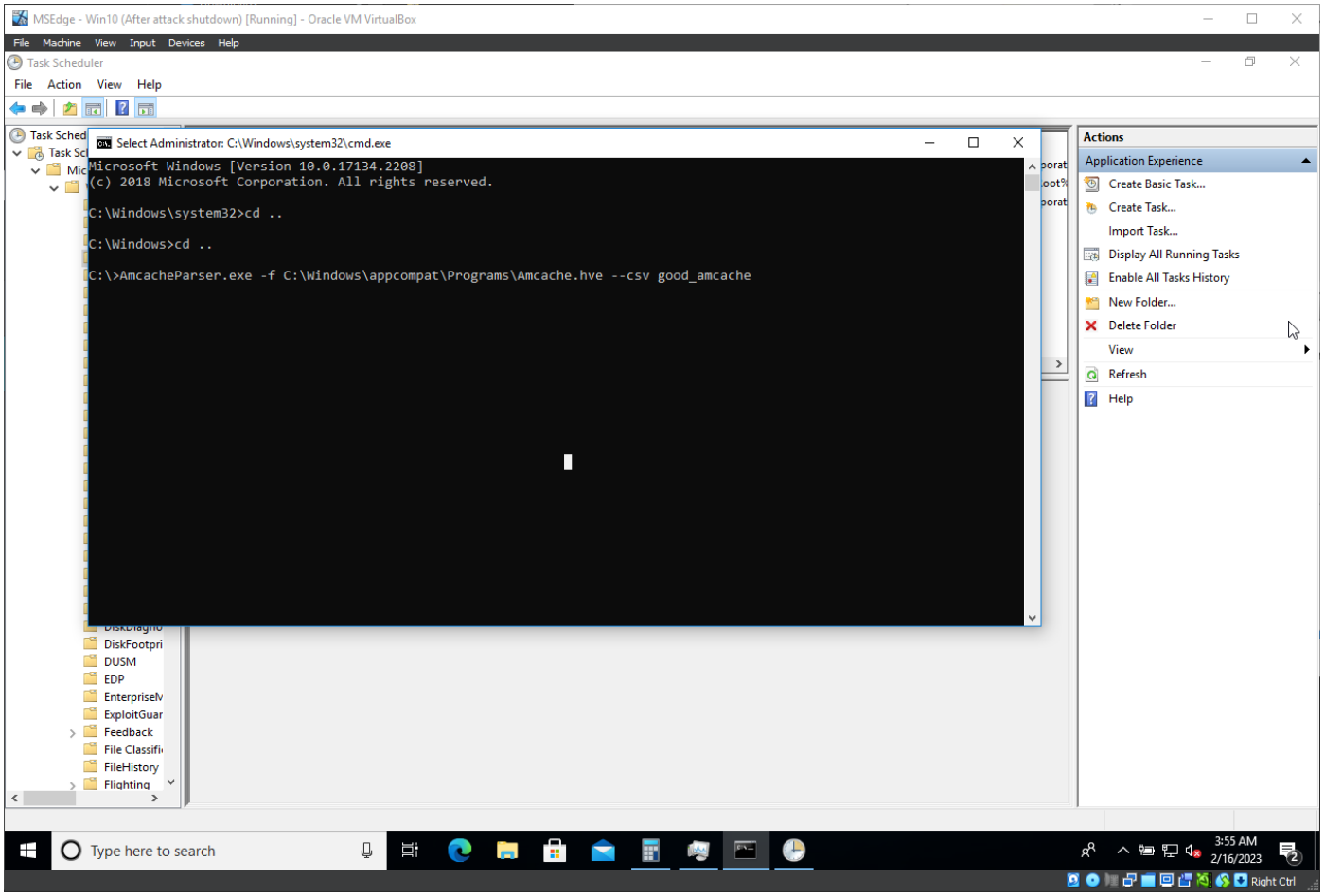
- It is already running.



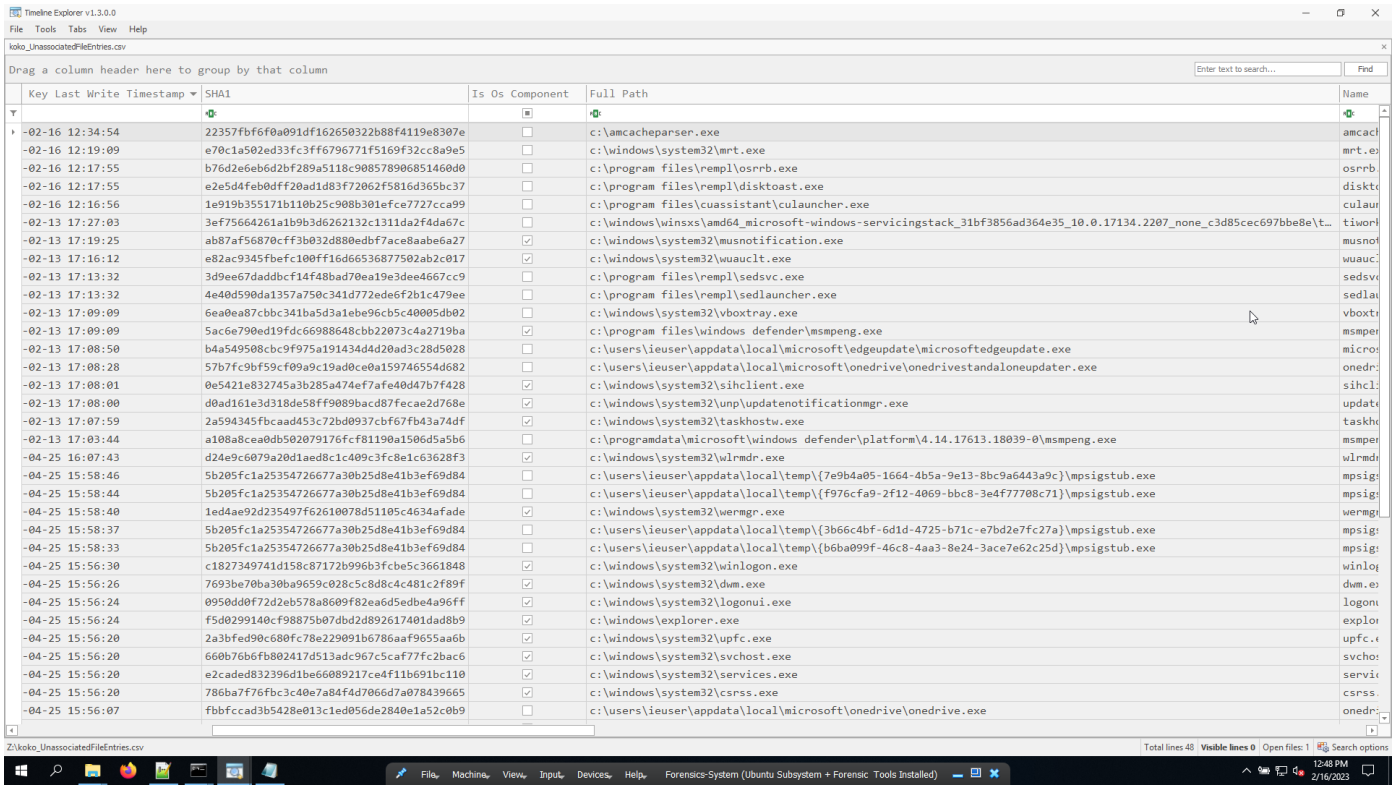
- We will wait until it finishes.


MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Task Scheduler
File Action View Help
Task Scheduler (Local)
Task Scheduler Library
Microsoft
Windows
Name Status Triggers Next Run Time Last Run Time Last Run Result Author
Microsoft C... Ready Multiple triggers defined 2/17/2023 3:24:14 AM 2/16/2023 3:52:45 AM The operation completed successfully. (0x0) Microsoft Corporat
ProgramDat... Ready 2/16/2023 3:35:57 AM The operation completed successfully. (0x0) $(@%SystemRoot%
StartupAppT... Ready 2/16/2023 3:35:54 AM The operation completed successfully. (0x0) Microsoft Corporat
Actions
Application Experience
Create Basic Task...
Create Task...
Import Task...
Display All Running Tasks
Enable All Tasks History
New Folder...
Delete Folder
View
Refresh
Help
Type here to search
3:55 AM
2/16/2023
Right Ctrl

- Execute:


MSEdge - Win10 (After attack shutdown) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Task Scheduler
File Action View Help
Select Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17134.2208]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Windows\system32>cd ..
C:\Windows>cd ..
C:\>AmcacheParser.exe -f C:\Windows\appcompat\Programs\Amcache.hve --csv good_amcache
Actions
Application Experience
Create Basic Task...
Create Task...
Import Task...
Display All Running Tasks
Enable All Tasks History
New Folder...
Delete Folder
View
Refresh
Help
DiskFootpri
DUSM
EDP
Feedback
FileHistory
Type here to search
3:55 AM
2/16/2023
Right Ctrl

- Run again:

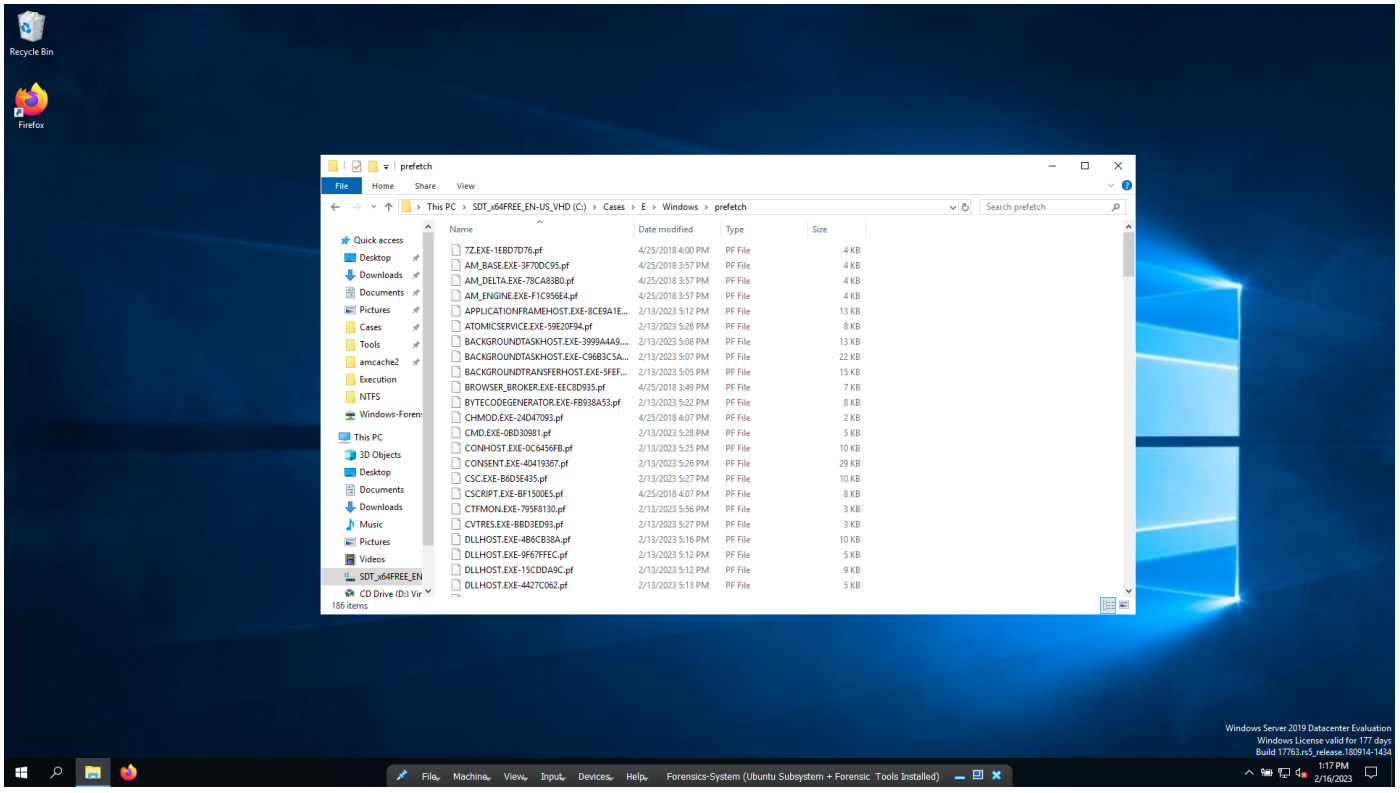

Timeline Explorer v1.3.0.0
File Tools Tabs View Help
koko_UnassociatedFileEntries.csv
Drag a column header here to group by that column
Key Last Write Timestamp
SHA1
Is Os Component
Full Path
Name
-02-16 12:34:54 22357fbf6f0a091df162650322b88f4119e8307e c:\amcacheparser.exe
-02-16 12:19:09 e70c1a502ed33fc3ff6796771f5169f32cc8a9e5 c:\windows\system32\mrt.exe
-02-16 12:17:55 b76d2e6eb6d2bf289a5118c908578906851460d0 c:\program files\rempl\osrrb.exe
-02-16 12:17:55 e2e5d4feb0dff20ad1d83f72062f5816d365bc37 c:\program files\rempl\disktoast.exe
-02-16 12:16:56 1e919b355171b110b25c908b301efce7727cca99 c:\program files\cuassistant\culauncher.exe
-02-13 17:27:03 3ef75664261a1b9b3d6262132c1311da2f4da67c c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.17134.2207_none_c3d85cec697bbe8e\t…
-02-13 17:19:25 ab87af56870cff3b032d880edbf7ace8aabe6a27 c:\windows\system32\musnotification.exe
-02-13 17:16:12 e82ac9345fbefc100ff16d66536877502ab2c017 c:\windows\system32\wuauclt.exe
-02-13 17:13:32 3d9ee67daddbcf14f48bad70ea19e3dee4667cc9 c:\program files\rempl\sedsvc.exe
-02-13 17:13:32 4e40d590da1357a750c341d772ede6f2b1c479ee c:\program files\rempl\sedlauncher.exe
-02-13 17:09:09 6ea0ea87cbbc341ba5d3a1ebe96cb5c40005db02 c:\windows\system32\vboxtray.exe
-02-13 17:09:09 5ac6e790ed19fdc66988648cbb22073c4a2719ba c:\program files\windows defender\msmpeng.exe
-02-13 17:08:50 b4a549508cbc9f975a191434d4d20ad3c28d5028 c:\users\ieuser\appdata\local\microsoft\edgeupdate\microsoftedgeupdate.exe
-02-13 17:08:28 57b7fc9bf59cf09a9c19ad0ce0a159746554d682 c:\users\ieuser\appdata\local\microsoft\onedrive\onedrivestandaloneupdater.exe
-02-13 17:08:01 0e5421e832745a3b285a474ef7afe40d47b7f428 c:\windows\system32\sihclient.exe
-02-13 17:08:00 d0ad161e3d318de58ff9089bacd87fecae2d768e c:\windows\system32\unp\updatenotificationmgr.exe
-02-13 17:07:59 2a594345fbcaad453c72bd0937cbf67fb43a74df c:\windows\system32\taskhostw.exe
-02-13 17:03:44 a108a8cea0db502079176fcf81190a1506d5a5b6 c:\programdata\microsoft\windows defender\platform\4.14.17613.18039-0\msmpeng.exe
-04-25 16:07:43 d24e9c6079a20d1aed8c1c409c3fc8e1c63628f3 c:\windows\system32\wlrmdr.exe
-04-25 15:58:46 5b205fc1a25354726677a30b25d8e41b3ef69d84 c:\users\ieuser\appdata\local\temp\{7e9b4a05-1664-4b5a-9e13-8bc9a6443a9c}\mpsigstub.exe
-04-25 15:58:44 5b205fc1a25354726677a30b25d8e41b3ef69d84 c:\users\ieuser\appdata\local\temp\{f976cfa9-2f12-4069-bbc8-3e4f77708c71}\mpsigstub.exe
-04-25 15:58:40 1ed4ae92d235497f62610078d51105c4634afade c:\windows\system32\wermgr.exe
-04-25 15:58:37 5b205fc1a25354726677a30b25d8e41b3ef69d84 c:\users\ieuser\appdata\local\temp\{3b66c4bf-6d1d-4725-b71c-e7bd2e7fc27a}\mpsigstub.exe
-04-25 15:58:33 5b205fc1a25354726677a30b25d8e41b3ef69d84 c:\users\ieuser\appdata\local\temp\{b6ba099f-46c8-4aa3-8e24-3ace7e62c25d}\mpsigstub.exe
-04-25 15:56:30 c1827349741d158c87172b996b3fcbe5c3661848 c:\windows\system32\winlogon.exe
-04-25 15:56:26 7693be70ba30ba9659c028c5c8d8c4c481c2f89f c:\windows\system32\dwm.exe
-04-25 15:56:24 0950dd0f72d2eb578a8609f82ea6d5edbe4a96ff c:\windows\system32\logonui.exe
-04-25 15:56:24 f5d0299140cf98875b07dbd2d892617401dad8b9 c:\windows\explorer.exe
-04-25 15:56:20 2a3bfed90c680fc78e229091b6786aaf9655aa6b c:\windows\system32\upfc.exe
-04-25 15:56:20 660b76b6fb802417d513adc967c5caf77fc2bac6 c:\windows\system32\svchost.exe
-04-25 15:56:20 e2caded832396d1be66088217ce4f11b691bc110 c:\windows\system32\services.exe
-04-25 15:56:20 786ba7f76fbc3c40e7a84f4d7066d7a078439665 c:\windows\system32\csrss.exe
-04-25 15:56:07 fbbfccad3b5428e013c1ed056de2840e1a52c0b9 c:\users\ieuser\appdata\local\microsoft\onedrive\onedrive.exe
Total lines 48 Visible lines 0
Forensics-System (Ubuntu Subsystem + Forensic Tools Installed)
12:48 PM
2/16/2023

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

None

Prefetch

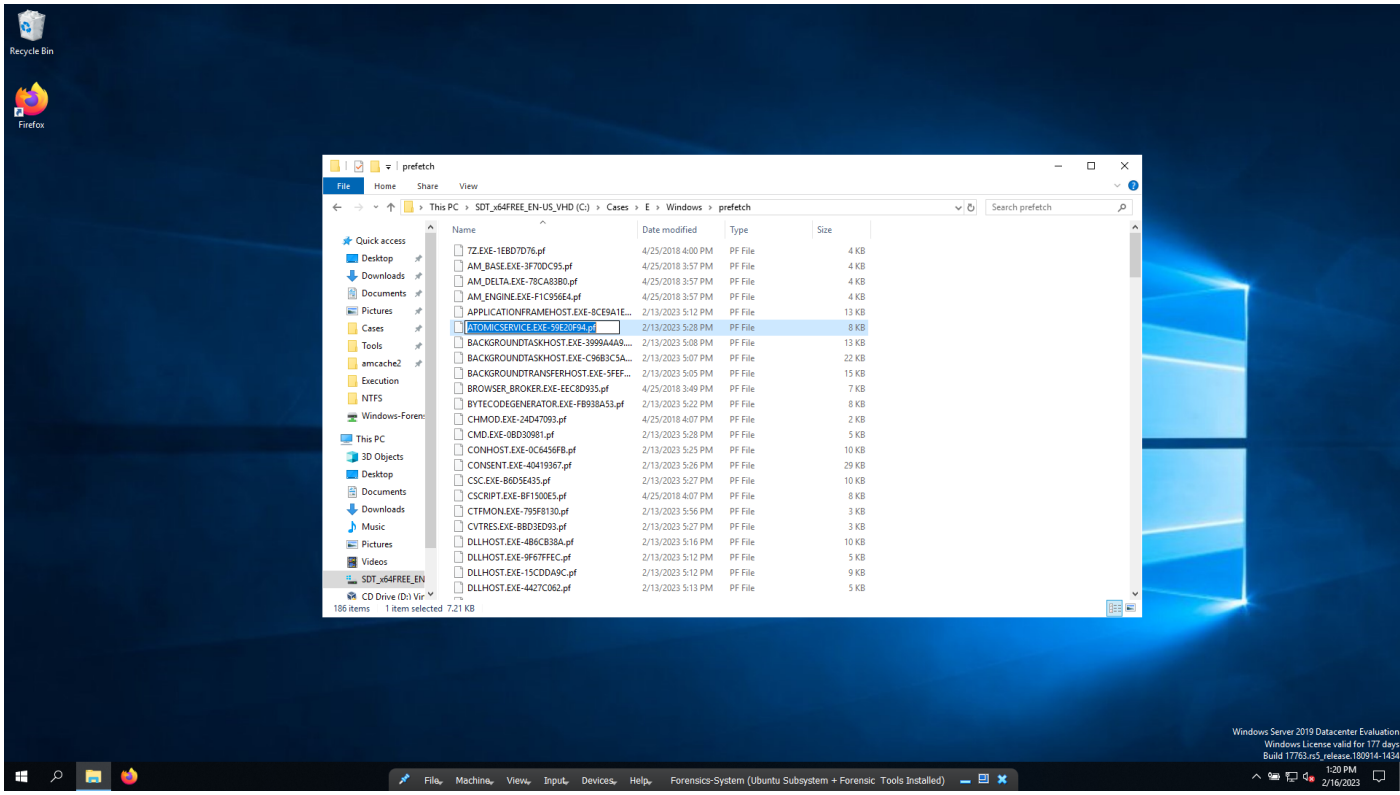
- The prefetch artifact is something that windows stores a prefetch file for every single application that executed.
- Location: C:\Windows\Prefetch*.pf
- Windows does this for preloading the store information from this files, from the disk into the memory to speed up the boots and startups of the applications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

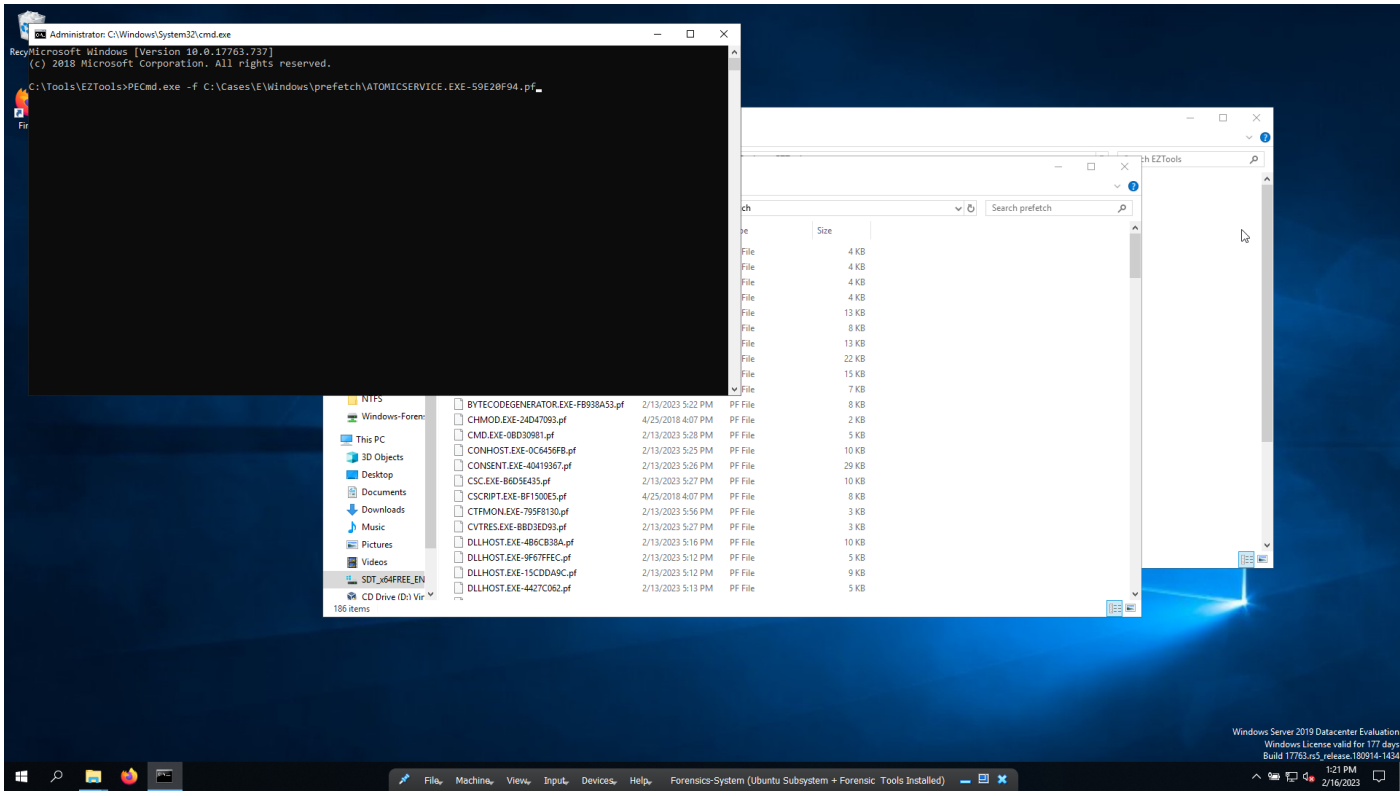


- Format is App-hash of location has been executed from.

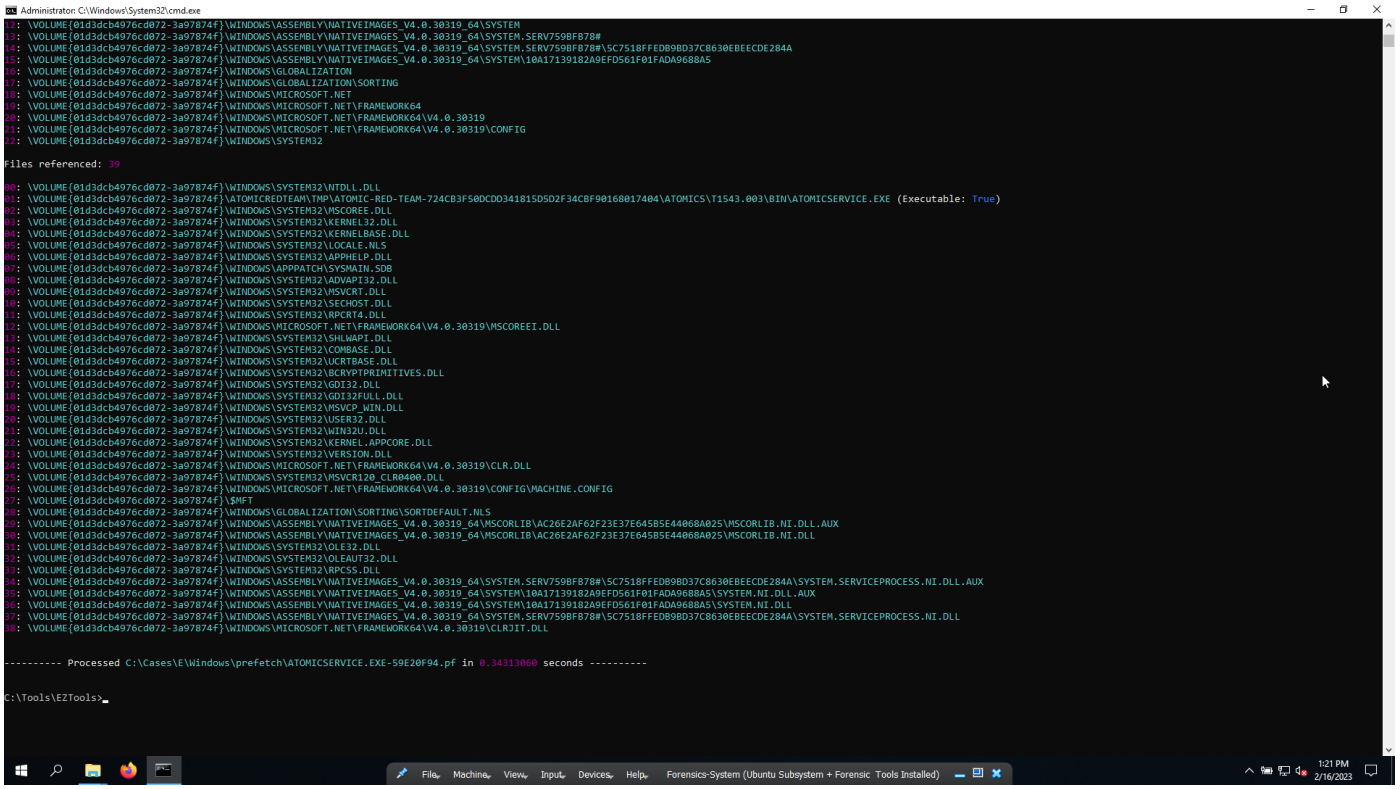
7Z.EXE-1EBD7D76.pf
AM_BASE.EXE-3F70DC95.pf
AM_DELTA.EXE-78CA83B0.pf
AM_ENGINE.EXE-F1C956E4.pf
APPLICATIONFRAMEHOST.EXE-8CE9A1E...
ATOMICSERVICE.EXE-59E20F94.pf
BACKGROUNDTASKHOST.EXE-3999A4A9....
BACKGROUNDTASKHOST.EXE-C96B3C5A...
BACKGROUNDTRANSFERHOST.EXE-5FEF...
BROWSER_BROKER.EXE-EEC8D935.pf
BYTECODEGENERATOR.EXE-FB938A53.pf

- 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
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 17:28:30

Volume information:

#0: Name: \VOLUME{01d3dcb4976cd072-3a97874f} Serial: 3A97874F Created: 2018-04-25 16:43:51 Directories: 23 File references: 63

Directories referenced: 23

00: \VOLUME{01d3dcb4976cd072-3a97874f}\ATOMICREDTEAM
01: \VOLUME{01d3dcb4976cd072-3a97874f}\ATOMICREDTEAM\TMP (Keyword True)
02: \VOLUME{01d3dcb4976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404 (Keyword True)
03: \VOLUME{01d3dcb4976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS (Keyword True)
04: \VOLUME{01d3dcb4976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003 (Keyword True)
05: \VOLUME{01d3dcb4976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN (Keyword True)
06: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS
07: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\APPPATCH
08: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\ASSEMBLY
09: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64
10: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\MSCORLIB
11: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\MSCORLIB\AC26E2AF62F23E37E645B5E44068A025
12: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM
13: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.SERV759BFB78#
14: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM.SERV759BFB78#\5C7518FFED89BD37C8630EBEECDE284A
15: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\ASSEMBLY\NATIVEIMAGES_V4.0.30319_64\SYSTEM\10A17139182A9EFD561F01FADA9688A5
16: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\GLOBALIZATION
17: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\GLOBALIZATION\SORTING
18: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\MICROSOFT.NET
19: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\MICROSOFT.NET\FRAMEWORK64
20: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\MICROSOFT.NET\FRAMEWORK64\V4.0.30319
21: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\MICROSOFT.NET\FRAMEWORK64\V4.0.30319\CONFIG
22: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32

Files referenced: 39

00: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\NTDLL.DLL
01: \VOLUME{01d3dcb4976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE (Executable: True)
02: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\MSCOREE.DLL
03: \VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\KERNEL32.DLL
```



- 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:

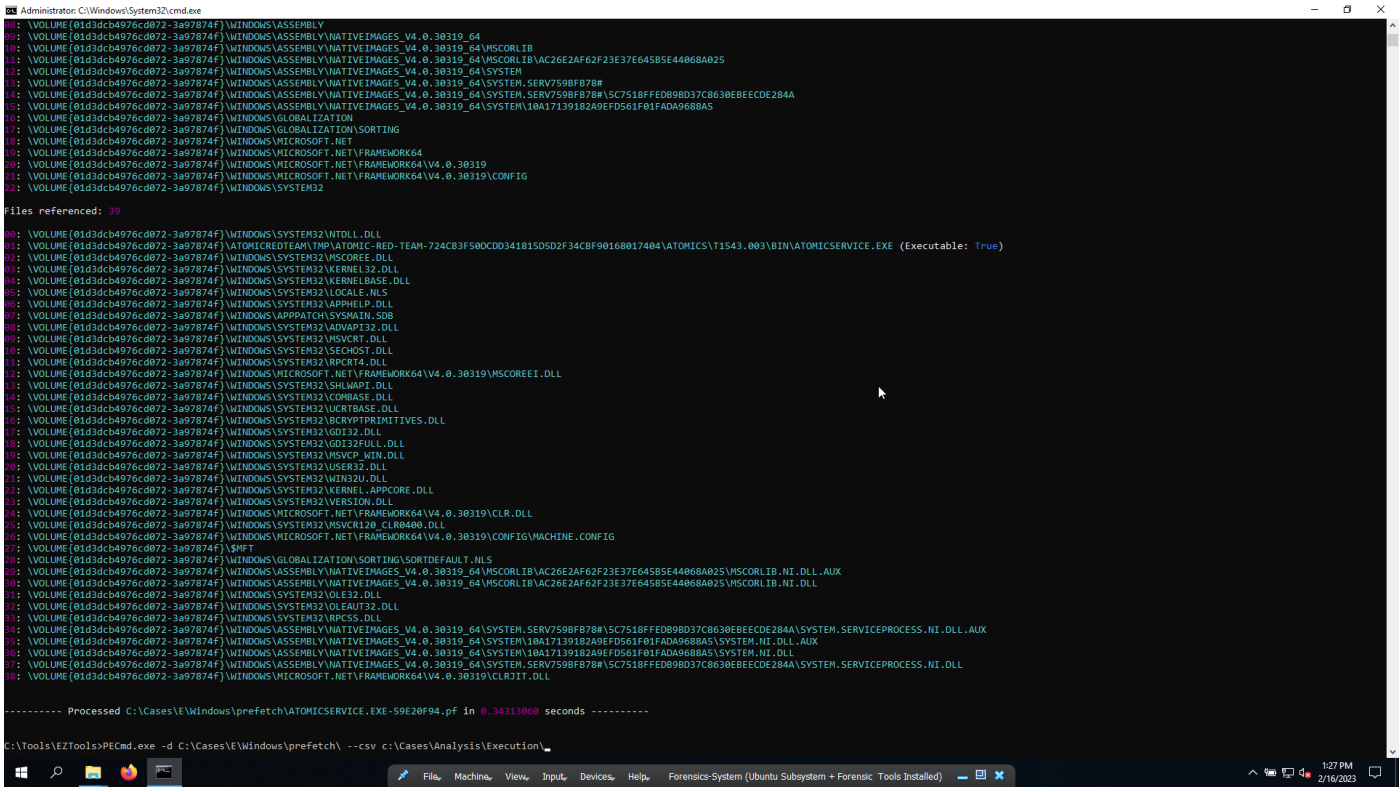
    Run count: 1

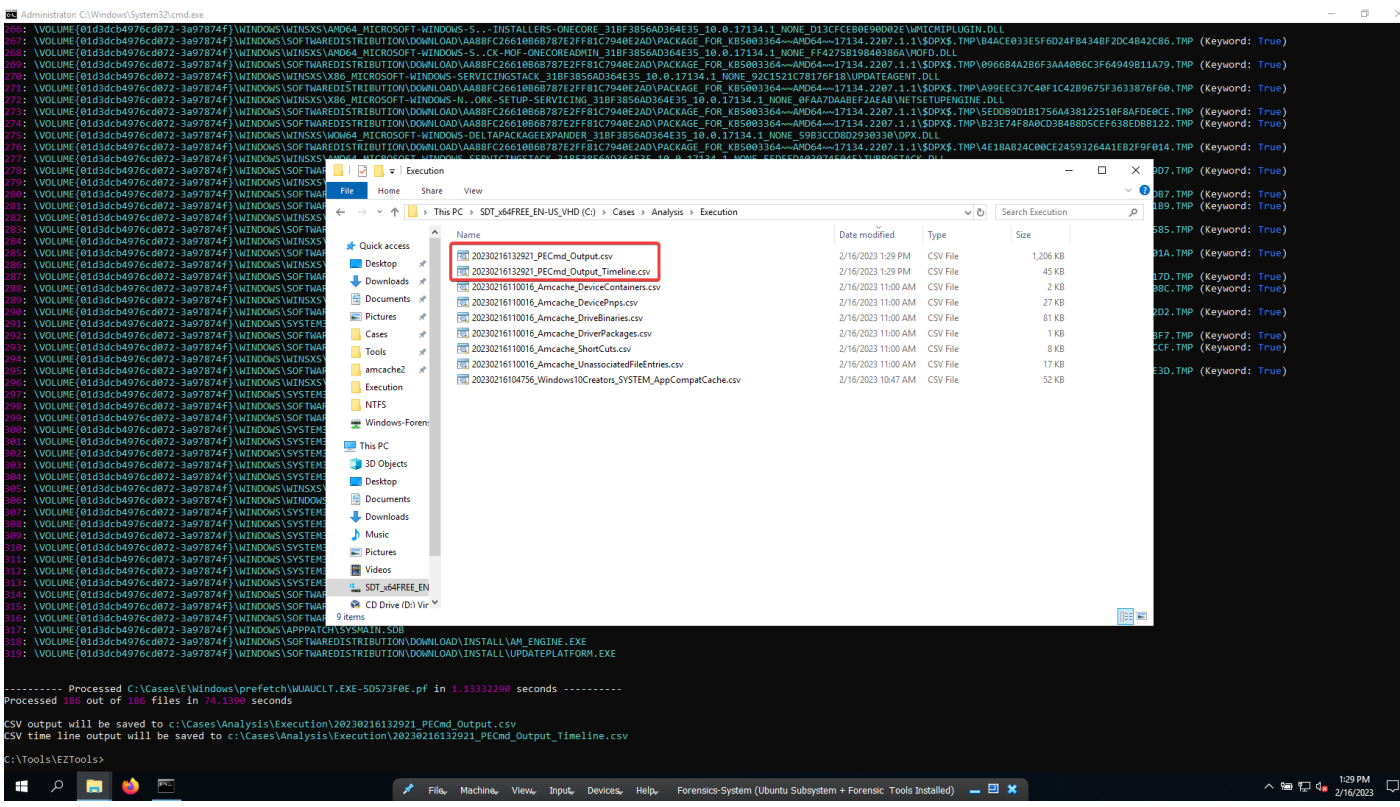
    Last run: 2023-02-13 17:28:30

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

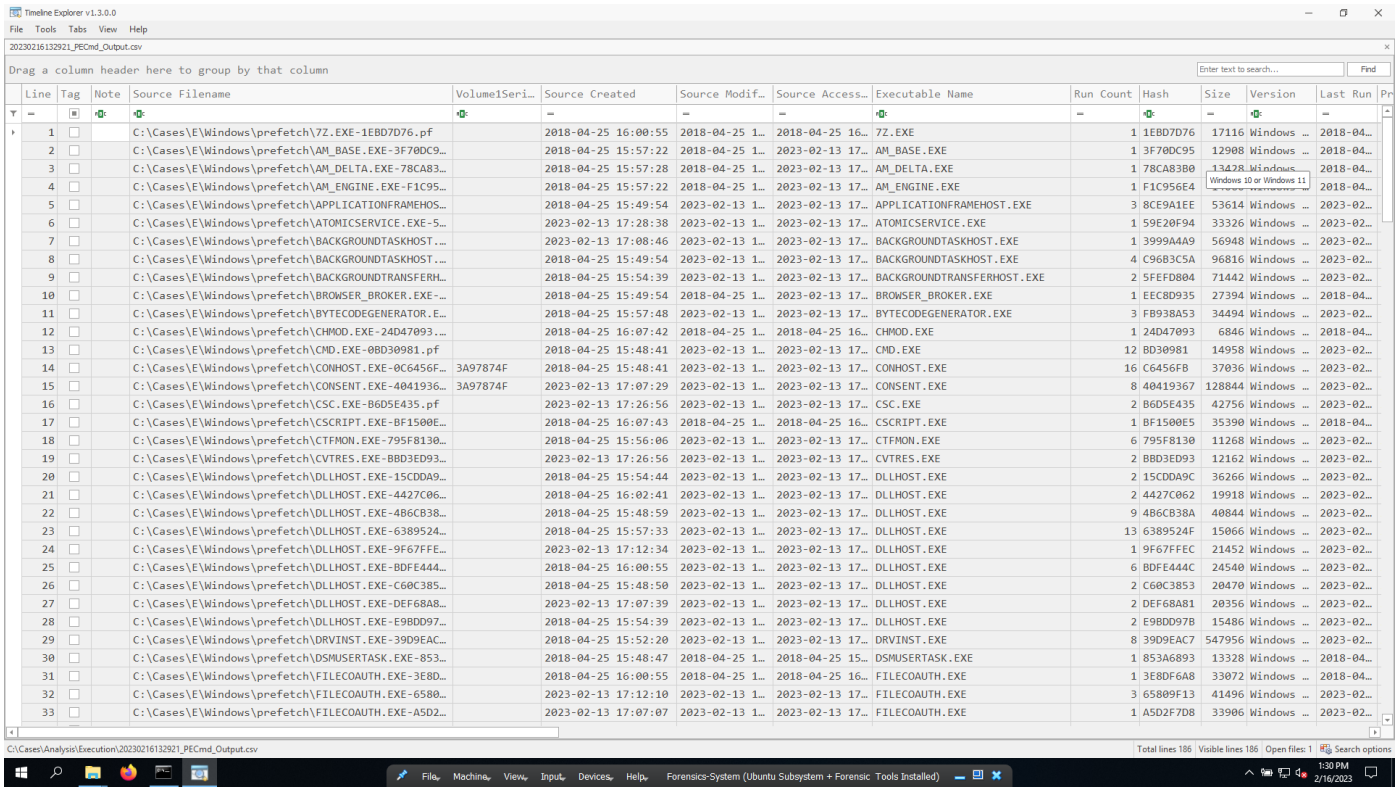
Prefetch Timeline-Analysis

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

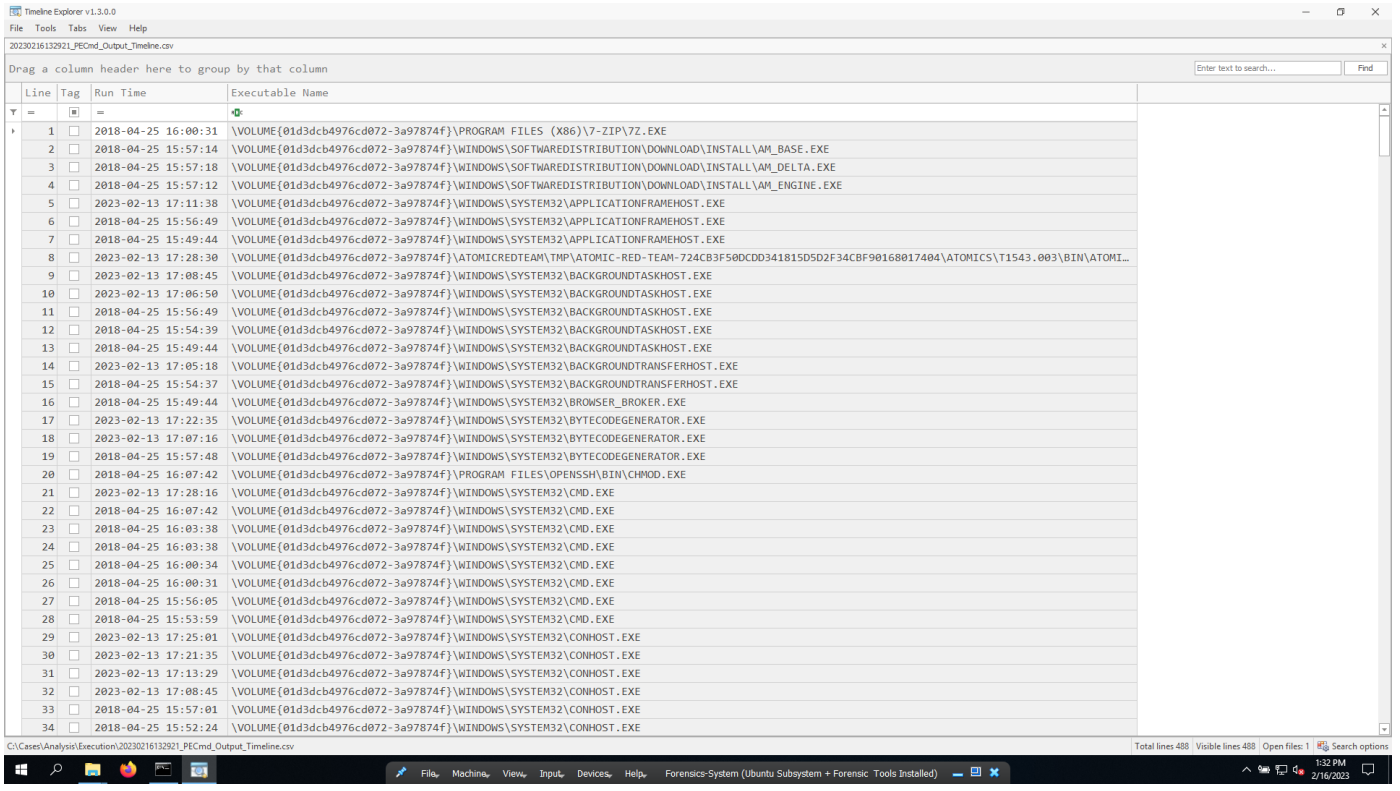




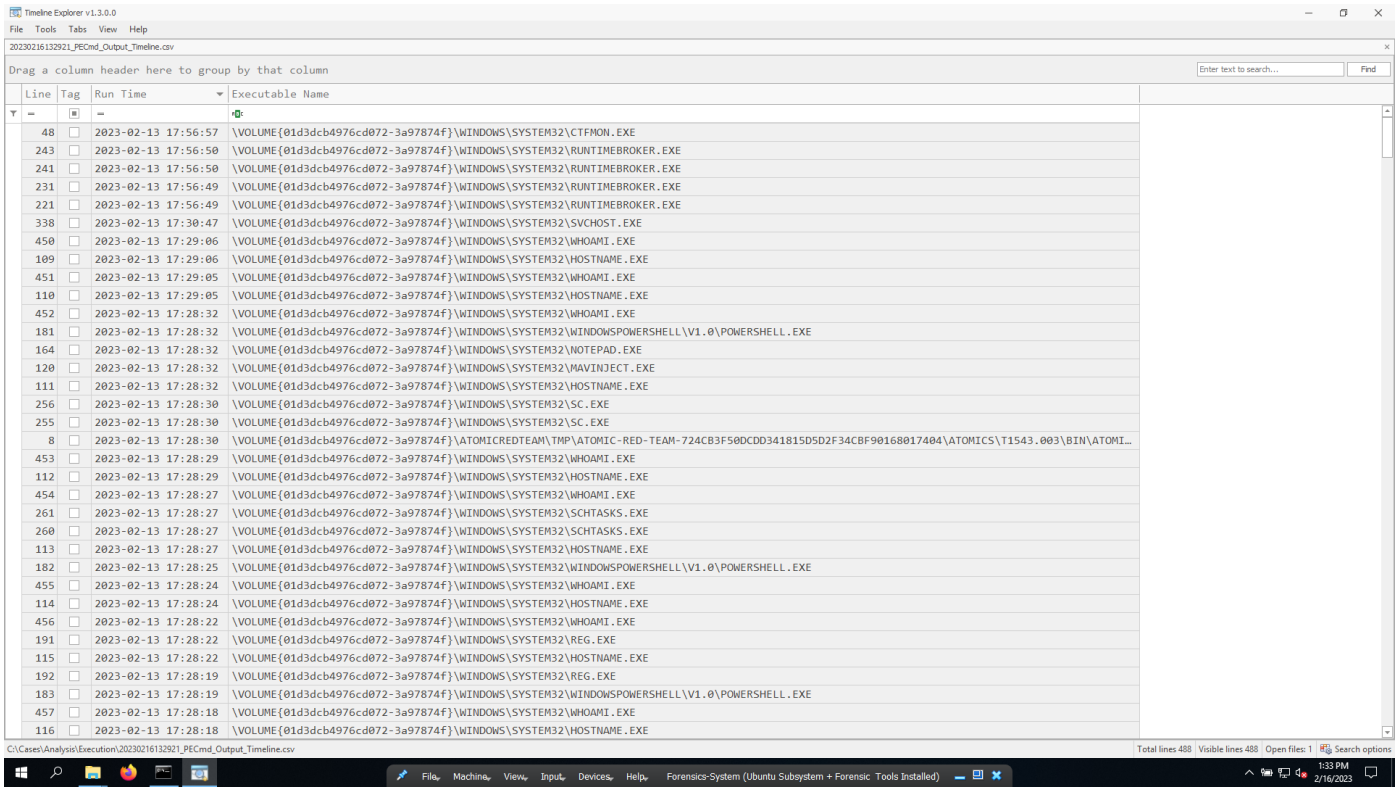
- Simple output:



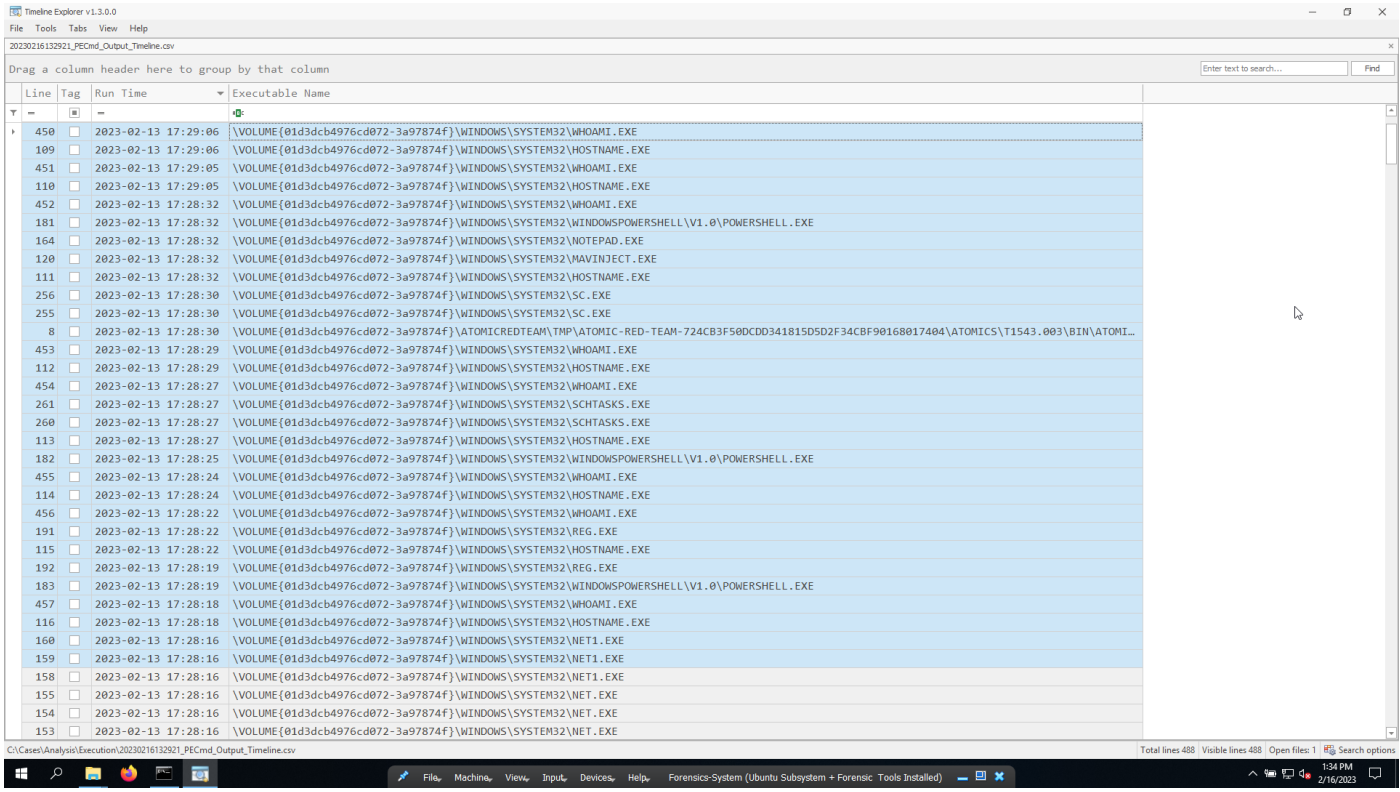
- Timeline output:



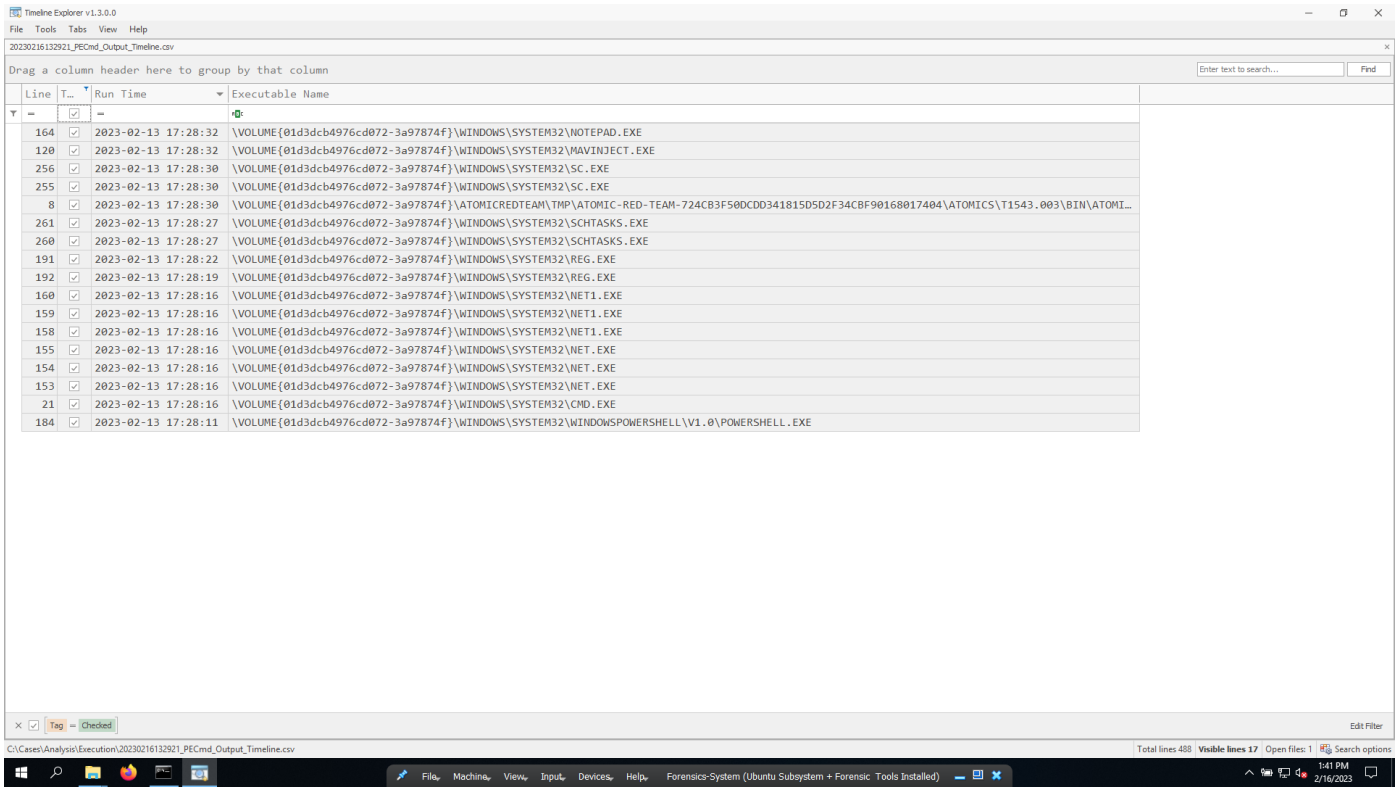
- Sort the output by runtime:



- Included in attack timeline:



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



- Executing Ascending – order

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\NOTEPAD.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\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{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\SC.EXE

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

\VOLUME{01d3dcb4976cd072-3a97874f}\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE

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

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\SCHTASKS.EXE

- Suspicious modifying or creating tasks.

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\REG.EXE

- Suspicious REG execution.

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\NET1.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\NET.EXE

- Suspicious NET and NET1 execution.

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\CMD.EXE

- Suspicious cmd execution.

\VOLUME{01d3dcb4976cd072-3a97874f}\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\POWERSHELL.EXE

- Suspicious powershell execution