

Windows Forensics- Part 3: File System & Execution Artifacts

Scope : Advanced File System Analysis & Program Execution Tracking

Now that we've analyzed **user behavior artifacts**, we'll dive deeper into **file system metadata and program execution evidence** to uncover **hidden activities and anti-forensic techniques**.

What We'll Cover in This Part

File System Artifacts

- **Master File Table (MFT)** : Complete file system metadata analysis
- **USN Journal** : File System change tracking
- **Background Activity Moderator (BAM)** : Background process tracking
- **AppCompatCache / Shimcache**: Applications compatibility records
- **AmCache** : Program execution metadata
- **Prefetch** : Application startup optimization data

Analysis Tools

- **MFTECmd**
- **Timeline Explorer**
- **Registry Explorer**
- **PECmd**
- **AmcacheParser**
- **Notepad++**

Investigation Goals

- Reconstruct complete file system timeline
- Track program execution history
- Recover deleted file evidence
- Identify malware persistence mechanisms

Session Objectives - Key Questions to Answer:

File Location & Identification:

- Which files are located in the AtomicRedTeam directory?
- What is the MFT Entry Number for "ART-attack.ps1"?

Timestamp Analysis:

- What are the MACB timestamps for "ART-attack.ps1"?
- Was "ART-attack.ps1" timestamped?

Deleted File Investigation:

- When was "deleteme_T1551.004" created and deleted?
- What was the Entry number for "deleteme_T1551.004"?
- Does "deleteme_T1551.004" still exist in the MFT?

1. Master File Table (MFT) Analysis

What is the MFT ?

The **Master File Table** is a **core NTFS database** storing **metadata about every file and folder on a disk**, including the MFT itself. It preserves file information even after deletion.

MFT Structure

- **Each entry = FILE record** (typically 1KB)
- **Contains attributes like database columns:**

Record Header: check flags to see if file is deleted, Sequence number helps track deleted files (deleted/in-use)

\$STANDARD_INFORMATION:

- **File Timestamps** (Created, Modified, Accessed, Entry Modified).
- **File permissions**

\$FILE_NAME: File names with additional timestamps

\$DATA: Where the actual content of the file is stored

- **If small** → stored inside the MFT (**Resident**)
- **If big** → points to clusters on disk (**Non-Resident**)

MFT Analysis with MFTECmd

Complete MFT Parsing

⇒ MFTECmd.exe -f C:\Users\NIZAR\Desktop\Cases\E\\$MFT --csv
C:\Users\NIZAR\Desktop\Cases\Analysis\ --csvf MFT.csv

The screenshot shows an Administrator Command Prompt window. The command entered is `MFTECmd.exe -f C:\Users\NIZAR\Desktop\Cases\E\$MFT --csv C:\Users\NIZAR\Desktop\Cases\Analysis\ --csvf MFT.csv`. The output indicates that 114,088 FILE records were found, with 6,680 free records, and a file size of 118MB. It also notes that the path to the analysis directory does not exist and is being created. The CSV output will be saved to `C:\Users\NIZAR\Desktop\Cases\Analysis\MFT.csv`. The process took 2.7896 seconds.

```
Administrator: Command Prompt
C:\Users\NIZAR\Desktop\Forensics Tools\Get-ZimmermanTools>MFTECmd.exe -f C:\Users\NIZAR\Desktop\Cases\E\$MFT --csv C:\Users\NIZAR\Desktop\Cases\Analysis\ --csvf MFT.csv
MFTECmd version 1.3.0.0

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

Command line: -f C:\Users\NIZAR\Desktop\Cases\E\$MFT --csv C:\Users\NIZAR\Desktop\Cases\Analysis\ --csvf MFT.csv

File type: Mft

Processed C:\Users\NIZAR\Desktop\Cases\E\$MFT in 2.7896 seconds

C:\Users\NIZAR\Desktop\Cases\E\$MFT: FILE records found: 114,088 (Free records: 6,680) File size: 118MB
Path to C:\Users\NIZAR\Desktop\Cases\Analysis\ doesn't exist. Creating...
CSV output will be saved to C:\Users\NIZAR\Desktop\Cases\Analysis\MFT.csv

C:\Users\NIZAR\Desktop\Forensics Tools\Get-ZimmermanTools>
```

Successfully executing *MFTECmd* to parse the *Master File Table* and generate *CSV* output for analysis

Key Investigation Questions & Findings

Some Atomic Red Team Files Discovered:

- **Invoke-atomicredteam**
- **Get-AtomicTechnique.ps1**
- **Install-atomicredteam.ps1**
- **Phant0m.exe**

Timeline Explorer v2.1.0

File Tools Tabs View Help

MFT.csv

Drag a column header here to group by that column

File Name Extension Is

Parent Path

File Name Extension Is

AtomicRedTeam

Find

LICENSE.txt

Private

.gitkeep

AtomicClassSchema.ps1

Get-PrereqExecutor.ps1

Get-TargetInfo.ps1

Invoke-CheckPrereqs.ps1

Invoke-ExecuteCommand.ps1

Invoke-KillProcessTree.ps1

Invoke-Process.ps1

Replace-InputArgs.ps1

Show-Details.ps1

Write-KeyValue.ps1

Write-PrereqResults.ps1

Public

Default-ExecutionLogger.psm1

Total lines 149,304 Visible lines 1,235 Open files: 1 Search options

Tag = Unchecked Edit Filter

C:\Users\NIZAR\Desktop\Cases\Analysis\MFT.csv

ENG US 11:14 AM 11/28/2025

- MFT analysis revealing files inside AtomicRedTeam folder including `Invoke-atomicredteam` and related attack scripts**

Timeline Explorer v2.1.0

File Tools Tabs View Help

MFT.csv

Drag a column header here to group by that column

Line Tag Entry Number Sequence Number Parent Entry Number Parent Sequence... In Use Parent Path File Name Extension Is

139615 ART-attack.ps1

139616 ART-attack.ps1:Zone.Identifier

Total lines 149,304 Visible lines 2 Open files: 1 Search options

ENG US 1:50 AM 11/28/2025

Tag = Unchecked Edit Filter

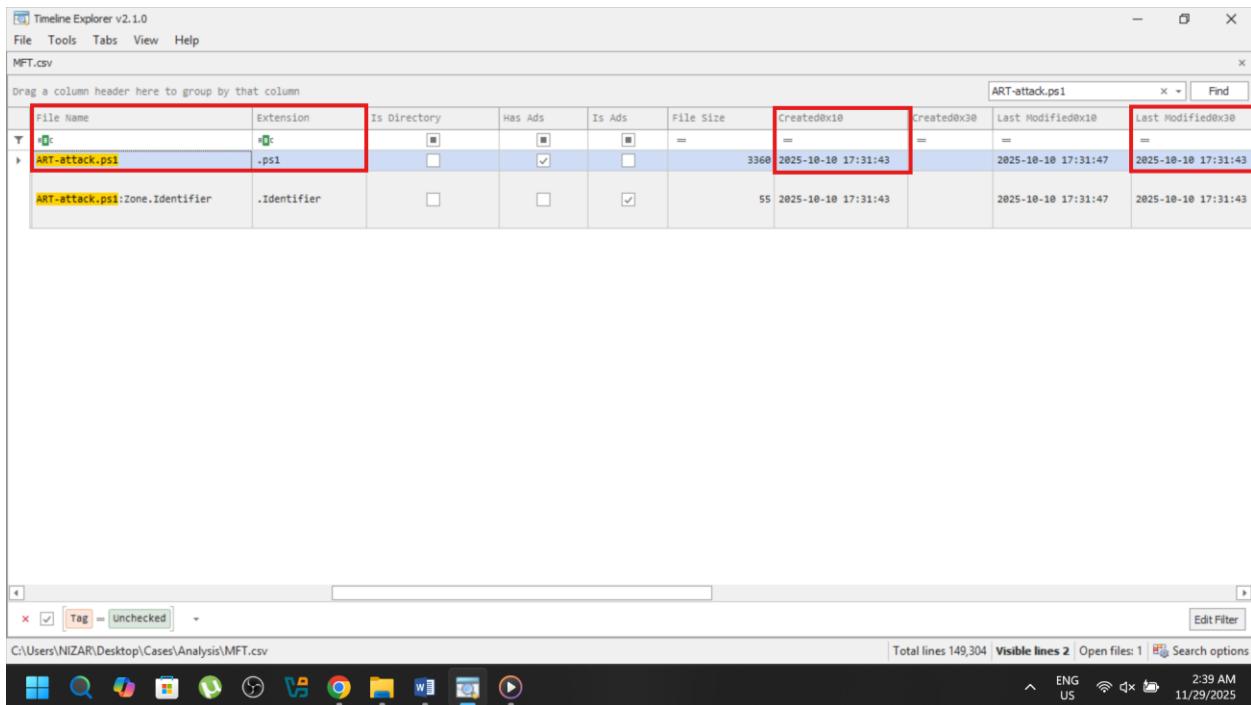
C:\Users\NIZAR\Desktop\Cases\Analysis\MFT.csv

MFT record showing Entry Number 111159 for ART-attack.ps1 file

What are the MACB timestamps for "ART-attack.ps1"?

Answer:

- **Modified:** 2024-10-10 17:31:47
- **Accessed:** 2025-10-10 17:31:43
- **Changed:** 2025-10-10 17:31:44
- **Born (Created):** 2025-10-10 17:31:43



File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created@0x10	Created@0x30	Last Modified@0x10	Last Modified@0x30
ART-attack.ps1	.ps1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	3360	2025-10-10 17:31:43		2025-10-10 17:31:47	2025-10-10 17:31:43
ART-attack.ps1:zone.Identifier	.Identifier	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	55	2025-10-10 17:31:43		2025-10-10 17:31:47	2025-10-10 17:31:43

MFT entry showing creation date and last modification date for ART-attack.ps1 file

Last Record Change@0x10	Last Record Change@0x30	Last Access@0x10	Last Access@0x30	Zone Id	Contents	Reparse Target	Reference Count	SI<FN	u Sec Zeros
2025-10-10 17:31:47	=	2025-10-10 17:31:44	=	2025-10-10 17:31:47	=	[ZoneTransfer] ZoneId=3 HostUrl=https://github.com/	1		
2025-10-10 17:31:47	=	2025-10-10 17:31:44	=	2025-10-10 17:31:47	=		1		
			2025-10-10 17:31:43						

Timeline Explorer v2.1.0
File Tools Tabs View Help
MFT.csv ART-attack.ps1 Find
Drag a column header here to group by that column
Last Record Change@0x10 Last Record Change@0x30 Last Access@0x10 Last Access@0x30 Zone Id Contents Reparse Target Reference Count SI<FN u Sec Zeros
2025-10-10 17:31:47 = 2025-10-10 17:31:44 = 2025-10-10 17:31:47 = [ZoneTransfer]
ZoneId=3 HostUrl=https://github.com/ 1
2025-10-10 17:31:47 = 2025-10-10 17:31:44 = 2025-10-10 17:31:47 = 2025-10-10 17:31:43 = 1
Total lines 149,304 Visible lines 2 Open files: 1 Search options
C:\Users\NIZAR\Desktop\Cases\Analysis\MFT.csv ENG US 2:41 AM 11/29/2025

MFT timestamps showing changed date and last accessed date for ART-attack.ps1

Note: The **3-second** difference between **0x10 (\$FILE_NAME)** and **0x30 (\$STANDARD_INFORMATION)** timestamps is normal system behavior and **does not indicate timestamping**.

When was "deleteme_T1551.004" created and deleted?

Initial Finding: File Not Found in Active MFT

Current Status:

- File not found in active MFT records
- Indicates file has been deleted from the file system

Next Step: USN Journal Analysis

Since the file doesn't appear in active **MFT records**, we need to examine the **USN Journal** to track its creation and deletion timeline.

What is the USN Journal ?

A Windows NTFS log that records all file system changes like **creations, modifications, and deletions** with timestamps **for forensic tracking**.

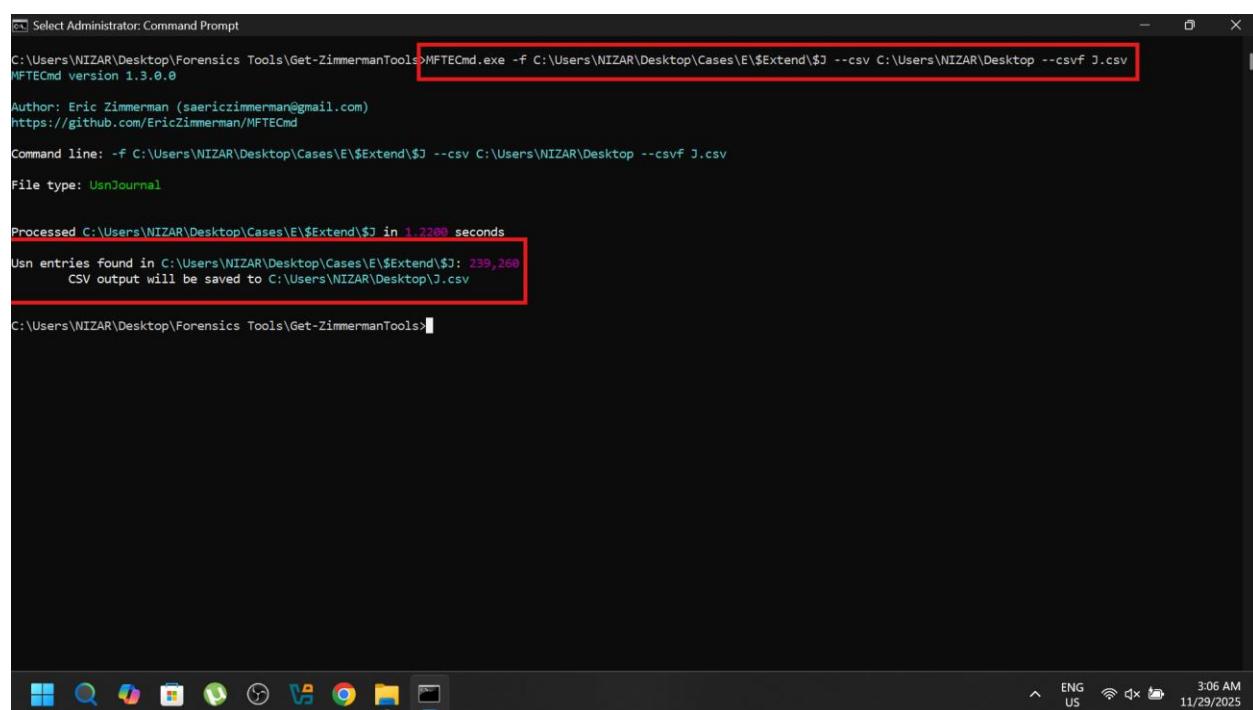
USN Journal Analysis Command:

⇒ MFTECmd.exe -f C:\Users\NIZAR\Desktop\Cases\E\\$Extend\$\\$J --csv
C:\Users\NIZAR\Desktop --csvf J.csv

What USN Journal Will Reveal:

- File creation timestamp
- File deletion timestamp
- Complete lifecycle of the deleted file
- File operations before deletion

Let's parse the USN Journal to uncover the file's history...



The screenshot shows a Windows Command Prompt window titled "Select Administrator: Command Prompt". The command entered is "MFTECmd.exe -f C:\Users\NIZAR\Desktop\Cases\E\\$Extend\$\\$J --csv C:\Users\NIZAR\Desktop --csvf J.csv". The output indicates the command is version 1.3.0.0, the author is Eric Zimmerman, and the file type is UsnJournal. It shows processing time of 1.2288 seconds and found 239,268 entries in the journal. The CSV output will be saved to C:\Users\NIZAR\Desktop\J.csv.

```
C:\Users\NIZAR\Desktop\Forensics Tools\Get-ZimmermanTools>MFTECmd.exe -f C:\Users\NIZAR\Desktop\Cases\E\$Extend$\$J --csv C:\Users\NIZAR\Desktop --csvf J.csv
MFTECmd version 1.3.0.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/MFTECmd

Command line: -f C:\Users\NIZAR\Desktop\Cases\E\$Extend$\$J --csv C:\Users\NIZAR\Desktop --csvf J.csv
File type: UsnJournal

Processed C:\Users\NIZAR\Desktop\Cases\E\$Extend$\$J in 1.2288 seconds
Usn entries found in C:\Users\NIZAR\Desktop\Cases\E\$Extend$\$J: 239,268
CSV output will be saved to C:\Users\NIZAR\Desktop\J.csv
```

Successfully executing MFTECmd to parse USN Journal (\$Extend\$J) for tracking file system changes and deleted files

- When was "deleteme_T1551.004" created and deleted?
- What was the Entry number for "deleteme_T1551.004"?

Answers:

File Creation:

2025-10-10 17:39:42 - FileCreate event in USN Journal

File Deletion:

2025-10-10 17:39:48 - FileDelete event in USN Journal

Entry Number:

112466

Key Finding:

- File lifespan: 6 seconds - Extremely short duration
- Rapid creation and deletion pattern suggests automated or scripted activity
- Potential anti-forensic technique to hide temporary files
- This short file lifespan indicates suspicious activity and possible evidence cleaning.

Line	Tag	Update Timestamp	Par...	Name	Exten...	Entry ..	Sequen...	Parent Entry Number	Par...	Update Seq.	Update Reasons	File At...	Source File
T	=	=	=	=	=	=	=	=	=	=	=	=	=
238235		2025-10-10 17:39:42		deleteme_T1551.004	.004	112466	6	46782	3	30296504	FileCreate	Archive	C:\Users\NIZAR\Desktop\Cas
238236		2025-10-10 17:39:42		deleteme_T1551.004	.004	112466	6	46782	3	30296600	FileCreate Close	Archive	C:\Users\NIZAR\Desktop\Cas
238265		2025-10-10 17:39:48		deleteme_T1551.004	.004	112466	6	46782	3	30300304	FileDelete Close	Archive	C:\Users\NIZAR\Desktop\Cas

USN Journal showing file *creation/deletion timeline* with corresponding entry numb

Does "deleteme_T1551.004" still exist in the MFT?

The file has been **deleted** from the system. The MFT entry is no longer in use. (Resident : False)

2. BAM Analysis (Background Activity Moderator)

What is BAM ?

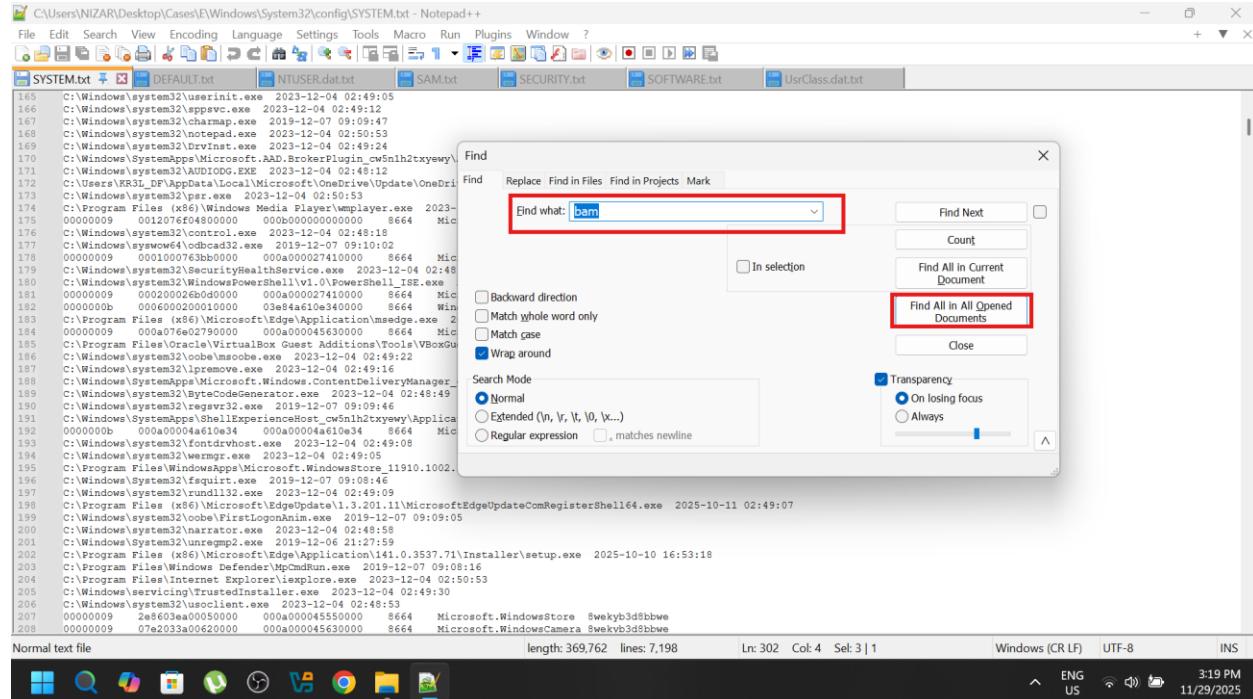
BAM is a Windows service that tracks background application execution for resource management, providing valuable forensic data on program execution.

Registry Location

⇒ **SYSTEM\CurrentControlSet\Services\bam\UserSettings\<SID>**

Investigation Questions:

- Which executables did BAM record for the target user (KR3L-DF) ?
- What were their last execution dates and times?
- Are there any suspicious or forensic tools executed?



A screenshot of Notepad++ showing a search dialog. The search term 'bam' is entered in the 'Find what:' field. The 'Find All In All Opened Documents' checkbox is checked. The search mode is set to 'Normal'. The results pane shows a list of registry entries from various files, including SYSTEM.txt, DEFAULT.txt, NTUSER.dat.txt, SAM.txt, SECURITY.txt, SOFTWARE.txt, and UsrClass.dat.txt. The entries are mostly paths to system DLLs and executables like 'kernel32.dll', 'user32.dll', 'ole32.dll', etc., with some specific BAM-related entries like 'C:\Windows\system32\bam.exe' and 'C:\Windows\system32\bam.dll'.

```
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\SYSTEM.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SYSTEM.txt DEFAULT.txt NTUSER.dat.txt SAM.txt SECURITY.txt SOFTWARE.txt UsrClass.dat.txt
165 C:\Windows\system32\userinit.exe 2023-12-04 02:49:05
166 C:\Windows\system32\seppsvc.exe 2023-12-04 02:49:12
167 C:\Windows\system32\charmap.exe 2019-12-07 09:09:47
168 C:\Windows\system32\notepad.exe 2023-12-07 02:50:53
169 C:\Windows\system32\vrctrl.exe 2023-12-04 02:49:24
170 C:\Windows\system32\Microsoft.ABD.Bcp0nFleGzJ5nh2txyewy
171 C:\Windows\system32\AUDIOLOG.EXE 2023-12-04 02:48:11
172 C:\Users\KR3L_DF\AppData\Local\Microsoft\OneDrive\Update\OneDri
173 C:\Windows\system32\iper.exe 2023-12-04 02:50:53
174 C:\Program Files (x86)\Windows Media Player\mplayer.exe 2023-
175 00000009 0012076f04800000 0000000000000000 8664 Mic
176 C:\Windows\system32\control.exe 2023-12-07 02:48:18
177 C:\Windows\system32\odbcad32.exe 2019-12-07 09:10:02
178 C:\Windows\system32\user32.dll 0000000000000000 8664 Mic
179 C:\Windows\system32\SecurityHealthService.exe 2023-12-04 02:48
180 C:\Windows\system32\WindowsPowerShellV1.0\powershell_ise.exe
181 00000009 000200026b0d0000 000a000027410000 8664 Mic
182 0000000b 0006000200010000 03e84a610e340000 8664 Win
183 C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe Mic
184 00000009 000a076e02790000 000a00045630000 8664
185 C:\Program Files\Oracle\VirtualBox\Guest Additions\Tools\VBoxGu
186 C:\Windows\system32\cmd.exe 2023-12-04 02:49:22
187 C:\Windows\system32\lprmove.exe 2023-12-04 02:49:16
188 C:\Windows\SystemApps\Microsoft.Windows.ContentDeliveryManager
189 C:\Windows\System32\ByteCodeGenerator.exe 2023-12-04 02:48:49
190 C:\Windows\System32\regsvr32.exe 2019-12-07 09:09:46
191 C:\Windows\SystemApps\ShellExperienceHost_cw5nh2txyewy\Appli
192 0000000b 000a0004a610e34 000a00004a610e34 8664 Mic
193 C:\Windows\system32\fontdrvhost.exe 2023-12-04 02:49:08
194 C:\Windows\system32\shell32.dll 2023-12-04 02:49:05
195 C:\Windows\system32\WindowsAppManifests\Manifests\11910.1002.
196 C:\Windows\System32\fiquirt.exe 2019-12-07 09:08:46
197 C:\Windows\System32\rundll32.exe 2023-12-04 02:49:09
198 C:\Program Files (x86)\Microsoft\Edge\update\1.3.201.11\MicrosoftEdgeUpdateComRegisterShell164.exe 2025-10-11 02:49:07
199 C:\Windows\System32\voobe\FirstLogonAnim.exe 2019-12-07 09:09:05
200 C:\Windows\system32\narrator.exe 2023-12-04 02:48:58
201 C:\Windows\System32\unrempp2.exe 2019-12-06 21:27:59
202 C:\Program Files (x86)\Microsoft\Edge\Application\msedge_0.3537.71\Installer\setup.exe 2025-10-10 16:53:18
203 C:\Windows\system32\explorer.exe 2019-12-07 09:08:16
204 C:\Program Files\Internet Explorer\explorer.exe 2023-12-04 02:50:53
205 C:\Windows\servicing\TrustedInstaller.exe 2023-12-04 02:49:30
206 C:\Windows\System32\useclient.exe 2023-12-04 02:48:53
207 00000009 2e8603ea00050000 000a00045550000 8664 Microsoft.WindowsStore_Swekyb3d8bbwe
208 00000009 07e2033a00620000 000a00045630000 8664 Microsoft.WindowsCamera_Swekyb3d8bbwe
Normal text file length: 369,762 lines: 7,198 Ln: 302 Col: 4 Sel: 3 | 1 Windows (CR LF) UTF-8 INS
ENG US 3:19 PM 11/29/2025
```

Using **Notepad++** to search for BAM registry entries across all parsed registry files

```

C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\SYSTEM.txt - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
SYSTEM.txt DEFAULT.txt NTUSER.dat.txt SAM.txt SECURITY.txt SOFTWARE.txt UsrClass.dat.txt
312
313 S-1-5-21-1767728838-24418769-4131373679-1001
314 2025-10-10 17:03:19Z - \Device\HarddiskVolume2\Windows\explorer.exe
315 2025-10-10 17:03:19Z - \Device\HarddiskVolume2\Windows\startmenuexperienceHost_cw5nh2txyewy
316 2025-10-10 17:03:19Z - Microsoft.Windows.ShellExperienceHost_cw5nh2txyewy
317 2025-10-10 17:02:35Z - Microsoft.Windows.ShellExperienceHost_cw5nh2txyewy
318 2025-10-10 17:13:43Z - \Device\HarddiskVolume2\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
319 2025-10-10 17:01:38Z - \Device\HarddiskVolume2\Program Files\Oracle\VirtualBox Guest Additions\Tools\VBoxDrvInst.exe
320 2025-10-10 17:03:46Z - \Device\HarddiskVolume2\Windows\System32\cmd.exe
321 2025-10-10 17:05:26Z - \Device\HarddiskVolume2\Windows\System32\applicationFrameHost.exe
322 2025-10-10 17:05:37Z - windows.immersivecontrolpanel_cw5nh2txyewy
323 2025-10-10 17:06:29Z - Microsoft.MicrosoftOfficeHub_8wekyb3d8bbwe
324 2025-10-10 17:05:45Z - Microsoft.Windows.Client.CBS_cw5nh2txyewy
325 2025-10-10 17:06:33Z - Microsoft.WindowsStore_8wekyb3d8bbwe
326
327 S-1-5-90-0-1
328 2025-10-10 17:03:19Z - \Device\HarddiskVolume2\Windows\System32\dwm.exe
329

Search results (12 hits)
Search "bam" (12 hits in 1 file of 7 searched) [Normal]
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\SYSTEM.txt (12 hits)
Line 302: bam v.20200427
Line 303: (System) Parse files from System hive BAM Services
Line 873: Name = bam
Line 874: Display = @%SystemRoot%\system32\drivers\bam.sys,-100
Line 875: ImagePath = system32\drivers\bam.sys
Line 5915: 2025-10-10 02:47:21Z,bam @%SystemRoot%\system32\drivers\bam.sys,-100,system32\drivers\bam.sys,Kernel driver,System Start,,@%SystemRoot%\system32\DriverStore\FileRepository\basicdisplay.inf_amd64_19e58b6267591a82\BasicDisplay.sys,Ker
Line 6008: 2025-10-10 17:02:45Z,BasicDisplay,,\SystemRoot\System32\DriverStore\FileRepository\basicdisplay.inf_amd64_d3f5994a67770b50\BasicDisplay.sys,Ker
Line 6038: 2025-10-10 17:02:30Z,BasicRender,,\SystemRoot\System32\DriverStore\FileRepository\basicrender.inf_amd64_d3f5994a67770b50\BasicRender.sys,Ker
Line 6253: 2019-12-07 09:15:07Z,BattC,,,,%SystemRoot%\system32\drivers\bam.sys,-101

Search "BAM" (12 hits in 1 file of 7 searched) [Normal]
Search "S-1-5-21-1767728838-24418769-4131373679-1001" (13 hits in 3 files of 7 searched) [Normal]
Search "BAM" (12 hits in 1 file of 7 searched) [Normal]

Normal text file length: 369,762 lines: 7,198 Ln: 302 Col: 4 Sel: 3 | 1 Windows (CR LF) UTF-8 INS
ENG US 3:20 PM 11/29/2025

```

BAM registry entries showing executed applications including explorer.exe, cmd.exe, and msedge.exe

BAM Analysis Results

Executables Recorded for User SID: **S-1-5-21-1767728838-24418769-4131373679-1001 (KR3L-DF)**

System & Application Executions:

- **explorer.exe** - 2025-10-10 17:03:19Z (**File Explorer**)
- **msedge.exe** - 2025-10-10 17:13:43Z (**Microsoft Edge**)
- **cmd.exe** - 2025-10-10 17:03:46Z (**Command Prompt**)
- **VBoxDrvInst.exe** - 2025-10-10 17:01:38Z (**VirtualBox Drivers**)

Windows System Processes:

- **StartMenuExperienceHost** - Start menu interactions
- **ShellExperienceHost** - Windows shell interface
- **ApplicationFrameHost** - Universal app hosting
- **ImmersiveControlPanel** - Settings application
- **Windows Search** - Search functionality

Store Applications:

- **Microsoft Office Hub** - Office applications
- **Windows Store** - App store access

Key Findings:

- **Normal system activity pattern observed**
- **No suspicious or forensic tools detected** in BAM records
- **Standard user workflow** with browser and system applications
- **VirtualBox components present** (expected in VM environment)
- **BAM analysis shows legitimate user activity without evidence of malicious tools.**

3. AppCompatCache/Shimcache Analysis

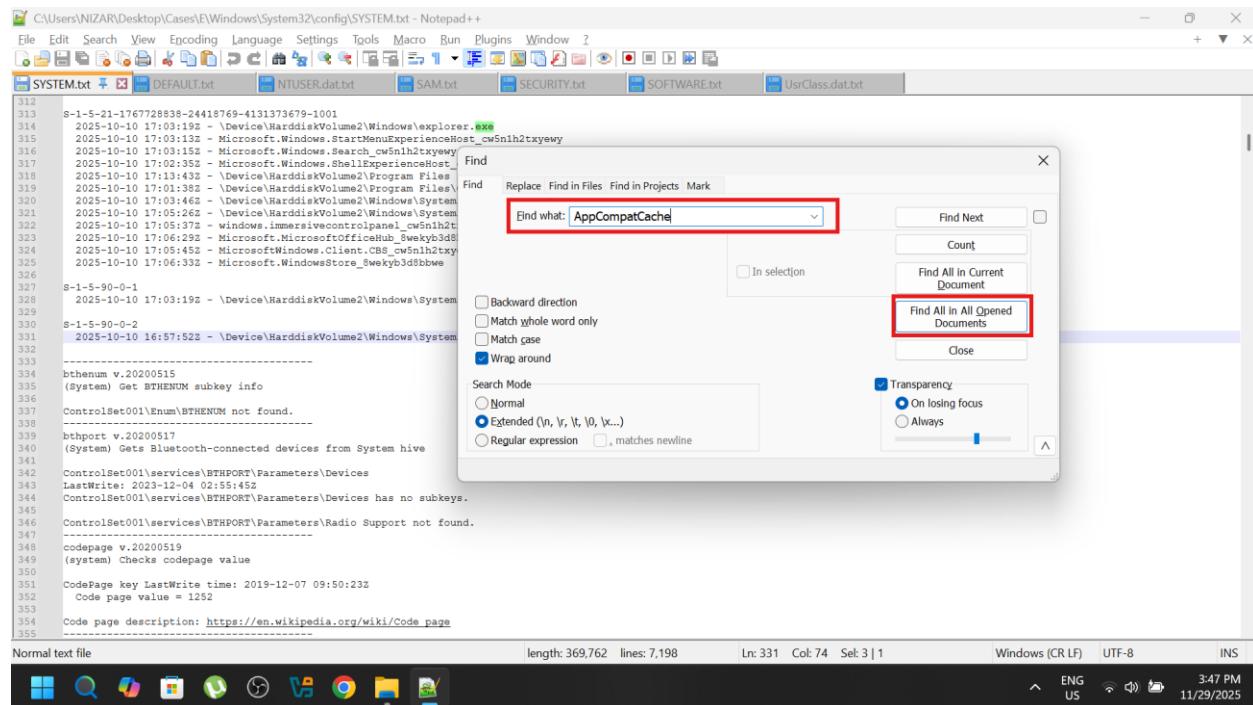
A Windows registry artifact that stores application compatibility data, creating a historical record of executables that Windows has encountered on the system.

Registry Location

⇒ SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

Key Characteristics:

- **Records executable file paths Windows has encountered**
- **Stores last modified time of files** (not execution time)
- **Provides historical record of program presence**
- **Not definitive proof of execution** (files can be copied without running)



Using Notepad++ to search for **AppCompatCache** entries across all registry files for application compatibility history

C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\SYSTEM.txt - Notepad++

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

SYSYEM.txt DEFAULT.txt NTUSER.dat.txt SAM.txt SECURITY.txt SOFTWARE.txt UsrClass.dat.txt

9
10 appcompatcache v.20220921
11 (System) Parse files from System hive AppCompatCache
12
13 ControlSet001\Control\Session Manager\AppCompatCache
14 LastWriteTime: 2023-12-04 02:51:09
15
Signature: 0x34
16 C:\Windows\system32\dgqladapterscache.exe 2023-12-04 02:48:43
17 C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe 2023-12-04 02:51:09
18 C:\Windows\system32\vlmrdr.exe 2023-12-04 02:49:29
19 00000000 03e84a610e340000 000a0002550000 8664 MicrosoftAAD.BrokerPlugin cw5nlh2txyewy neutral
20 00000000 000a0004a610e34 000a0004a610e34 8664 Microsoft.Windows.OBENetworkCaptivePortal cw5nlh2txyewy
21 00000009 000200026ac000000 000a000274100000 8664 Microsoft.NET.Native.Runtime.2.2 Swekyb3d8bbwe
22 00000000 03e84a610e340000 000a0002550000 8664 Microsoft.Windows.AssignedAccessLockApp cw5nlh2txyewy neutral
23 00000000 000a0004a610e34 000a0004a610e34 8664 Microsoft.Windows.PeopleExperienceHost cw5nlh2txyewy neutral
24 C:\Windows\system32\SppExtComObj.exe 2023-12-04 02:49:12
25 C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe 2023-12-04 02:49:16
26 C:\Windows\system32\SIU1.exe 2023-12-04 02:49:12
27 C:\Windows\system32\MSMScched.exe 2019-12-07 09:09:54
28 C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe 2023-12-04 02:51:09
29 C:\Windows\system32\wauclt.exe 2023-12-04 02:48:55
30 C:\Windows\system32\ClipReexec.exe 2023-12-04 02:48:01
31 00000000 03e84a610e340000 8664 NcslUpwApp Swekyb3d8bbwe neutral
32 00000009 00010000518bb0000 000a00045630000 8664 Microsoft.WebMediaExtensions Swekyb3d8bbwe
33 00000000 03e84a610e340000 000a000000000000 8664 Microsoft.XboxGameCallableUI cw5nlh2txyewy neutral
34 00000000 000a0004a610e34 000a0004a610e34 8664 Microsoft.Windows.XpuejectDialog cw5nlh2txyewy neutral
35 C:\Windows\Speech\Components\regisvr.exe 2019-12-07 09:08:58
36 C:\Windows\system32\dhm.exe 2023-12-04 02:49:02
37 C:\Windows\system32\SystemHealth\systray.exe 2019-12-07 09:08:41
38 00000009 2e30000000000000 000a00045550000 8664 Microsoft.StorePurchaseApp Swekyb3d8bbwe
39 00000000 000a0004a610e34 000a00038390000 8664 Microsoft.AsyncTextService Swekyb3d8bbwe
40 00000009 000a077207b40000 000a00045630000 8664 Microsoft.WindowsSoundRecorder Swekyb3d8bbwe
41 C:\Windows\system32\directxdataupdated.exe 2023-12-04 02:49:44
42 00000009 000000025990000 000a00045630000 8664 Microsoft.Getstarted Swekyb3d8bbwe
43 00000009 0001002e2af90000 000a00042ee0000 8664 Microsoft.XboxGameOverlay Swekyb3d8bbwe
44
Search results - (3 hits)
Search "AppCompatCache\r\n" (3 hits in 1 file of 7 searched) [Extended]
C:\Users\NIZAR\Desktop\Cases\E\Windows\System32\config\SYSTEM.txt (3 hits)
Line 11: (System) Parse files from System hive AppCompatCache
Line 13: ControlSet001\Control\Session Manager\AppCompatCache

AppCompatCache entries showing detected executables and their metadata in Notepad++ search results

AppCompatCache registry entries viewed in Registry Explorer showing cached executable information

Key Executables Detected:

System & Administration Tools:

- **cmd.exe** - Command Prompt - **Last Modified: 2023-12-04 02:48:51**
- **powershell.exe** - Windows PowerShell - **Last Modified: 2023-12-04 02:51:09**
- **regedit.exe** - Registry Editor - **Last Modified: 2023-12-04 02:50:12**
- **taskmgr.exe** - Task Manager - **Last Modified: 2023-12-04 02:48:59**
- **msinfo32.exe** - System Information - **Last Modified: 2023-12-04 02:50:17**
- **control.exe** - Control Panel - **Last Modified: 2023-12-04 02:48:18**

Virtualization Components:

- **VBoxDrvInst.exe** - VirtualBox Driver Installer - **Last Modified: 2025-08-13 20:13:36**
- **VBoxGuestInstallHelper.exe** - VirtualBox Guest Helpers - **Last Modified: 2025-08-13 20:13:38**
- **VBoxCertUtil.exe** - VirtualBox Certificate Utility - **Last Modified: 2025-08-13 20:13:30**

Network & Communication:

- **msedge.exe** - Microsoft Edge Browser - **Last Modified: 2025-10-09 06:52:49**
- **OneDrive.exe** - Cloud storage sync - **Last Modified: 2025-10-10 17:00:34**

Windows Store Apps:

- **Microsoft Store** applications - **Various timestamps**
- **Office Hub** components - **Various timestamps**
- **Media and entertainment apps** - **Various timestamps**

⚠️ LOLBins (Living Off the Land Binaries) Alert:

Note: Several legitimate processes detected could be used for **LOLBins attacks**:

- **cmd.exe & powershell.exe** - Command execution and scripting
- **regedit.exe** - Registry manipulation
- **msinfo32.exe** - System reconnaissance
- **control.exe** - System configuration changes

Analysis Summary:

- **No obvious malicious software detected**
- **Multiple LOLBins present that could be exploited**
- **Normal system administration activity mixed with potential attack vectors**
- **VirtualBox environment confirmed**
- **Standard user applications usage pattern**

Note : While no overt malware was found, the presence of multiple LOLBins requires correlation with other artifacts to rule out Living Off the Land attacks.

4. AmCache Analysis

What is AmCache?

AmCache is a **Windows registry** artifact that stores **comprehensive metadata** about **executables and applications that have been executed on a system**, providing valuable forensic data for incident investigations.

Registry Location

⇒ C:\Windows\AppCompat\Programs\Amcache.hve

What AmCache Contains :

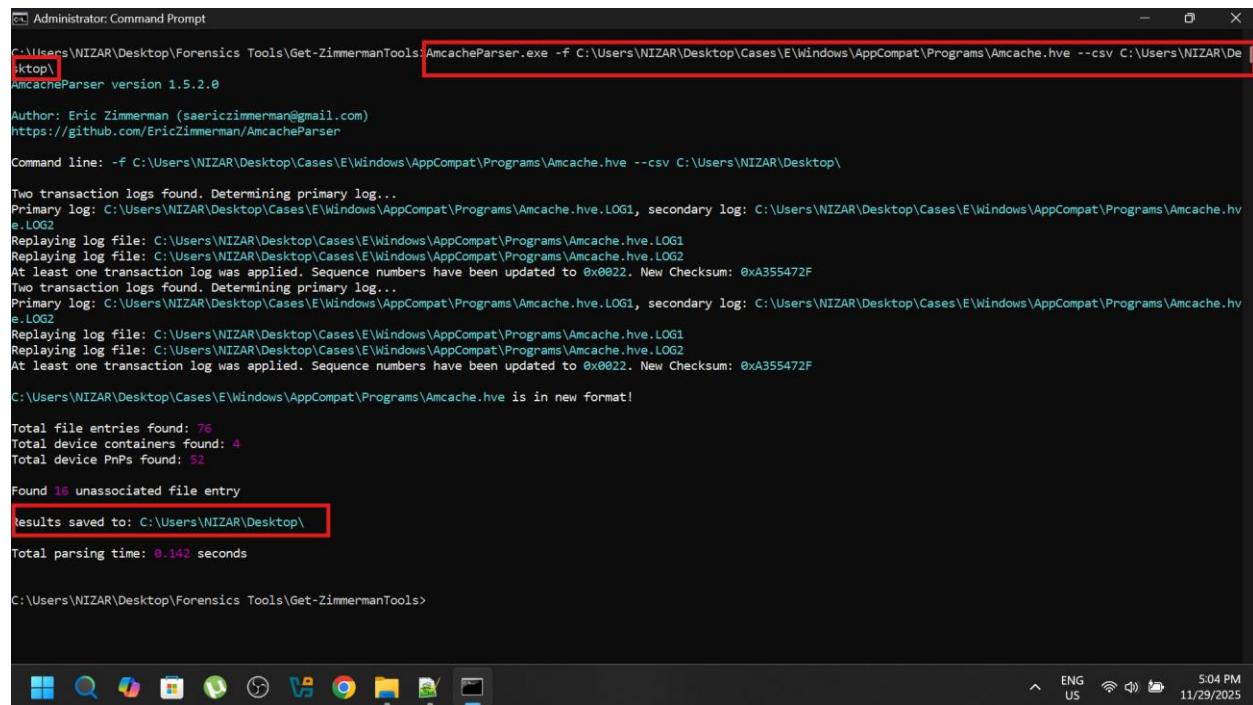
- **Executable metadata:** File paths, sizes, timestamps

- **SHA1 hashes** for file integrity verification
- **Program execution information and timestamps**
- **Software publisher details**
- **MRU (Most Recently Used) data**

Analysis Method :

Parse AmCache Hive :

⇒ **AmcacheParser.exe -f**
C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve --
csv C:\Users\NIZAR\Desktop



```

Administrator: Command Prompt
C:\Users\NIZAR\Desktop\Forensics Tools\Get-ZimmermanTools\AmcacheParser.exe -f C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve --csv C:\Users\NIZAR\Desktop\

AmcacheParser version 1.5.2.0

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

Command line: -f C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve --csv C:\Users\NIZAR\Desktop\

Two transaction logs found. Determining primary log...
Primary log: C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve.LOG1, secondary log: C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x0022. New Checksum: 0xA355472F
Two transaction logs found. Determining primary log...
Primary log: C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve.LOG1, secondary log: C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve.LOG2
Replaying log file: C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve.LOG1
Replaying log file: C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve.LOG2
At least one transaction log was applied. Sequence numbers have been updated to 0x0022. New Checksum: 0xA355472F

C:\Users\NIZAR\Desktop\Cases\E\Windows\AppCompat\Programs\Amcache.hve is in new format!

Total file entries found: 76
Total device containers found: 4
Total device PnPs found: 52

Found 16 unassociated file entry
results saved to: C:\Users\NIZAR\Desktop\

Total parsing time: 0.142 seconds

C:\Users\NIZAR\Desktop\Forensics Tools\Get-ZimmermanTools>

```

Successfully executing *AmcacheParser* to extract program execution data from *AmCache.hve* registry hive

20251129170435_Amcache_UnassociatedFileEntries.csv - Excel

	A	B	C	D	E	F	G
	ApplicationName	ProgramId	FileKeyLastWritten	SHA1	IsOsComponent	FullPath	Name
1	ApplicationName	ProgramId	FileKeyLastWritten	SHA1	True	c:\windows\system32\compattelrunner.exe	CompatTelRunner.exe
2	Unassociated	0000f519fee1 #####	92be78f15897d905538b36fbf015af29616cc49	43e2258320589c44ad6e809b59adb0d9695fc8d	True	c:\windows\system32\crss.exe	crss.exe
3	Unassociated	0000f519fee1 #####	e5c13895c71f575e845d93cdbed822569a09076	e27bffb384518ae3bb610e8a7335366836738acd	True	c:\windows\system32\devicecensus.exe	DeviceCensus.exe
4	Unassociated	0000f519fee1 #####	66bcca86d76dcfe2343aa25a342e830d2f7b34a	25e92edc0cab5e7446a302863802f3879b27bd9	True	c:\windows\system32\drvinst.exe	drvinst.exe
5	Unassociated	0000f519fee1 #####	93582a42d1248864dc40e8578b10db8fc4aac86	ce8669d8826c8795115d58c62e726ae53943dc9	False	c:\windows\system32\em.exe	EM.exe
6	Unassociated	0000f519fee1 #####	2ff161a1185b5716ade6b895127d561299e7cafe	895aa04ea5f6800232ae263b21a12b6ae0a63d	False	c:\windows\explorer.exe	explorer.exe
7	Unassociated	0000f519fee1 #####	445f1538365a88e029b357f4696f0e3ee50a1d8	79c9a666e776781578db55d1ca191c15e10b74e6	True	c:\program files (x86)\microsoft\edgeupdate\microsoftheadgeupdate\MicrosoftEdgeUpdate.exe	MicrosoftEdgeUpdate.exe
8	Unassociated	0000f519fee1 #####	99bf5030a015c2f5bea0ab7196b925f6b8d959f9	99bf5030a015c2f5bea0ab7196b925f6b8d959f9	False	c:\program files (x86)\microsoft\edge\application\msedge.exe	msedge.exe
9	Unassociated	0000f519fee1 #####	79c9a666e776781578db55d1ca191c15e10b74e6	79c9a666e776781578db55d1ca191c15e10b74e6	True	c:\users\kr3l_df\appdata\local\microsoft\onedrive\update\onedriveSetup.exe	OneDriveSetup.exe
10	Unassociated	0000f519fee1 #####	2ff161a1185b5716ade6b895127d561299e7cafe	2ff161a1185b5716ade6b895127d561299e7cafe	False	c:\windows\syswow64\onedrivesetup.exe	OneDriveSetup.exe
11	Unassociated	0000f519fee1 #####	895aa04ea5f6800232ae263b21a12b6ae0a63d	895aa04ea5f6800232ae263b21a12b6ae0a63d	False	c:\program files (x86)\microsoft\edgeupdate\install\{a8f496ab-4b47-46f7-875f-66c1d916-f77f\}setup.exe	setup.exe
12	Unassociated	0000f519fee1 #####	c747abb3f7bfd1eb0537892cefe99216071f690	c747abb3f7bfd1eb0537892cefe99216071f690	False	c:\program files (x86)\microsoft\edgeupdate\install\{66c1d916-f77f\}setup.exe	setup.exe
13	Unassociated	0006eec05d #####	445f1538365a88e029b357f4696f0e3ee50a1d8	445f1538365a88e029b357f4696f0e3ee50a1d8	True	c:\windows\system32\svchost.exe	svchost.exe
14	Unassociated	0000f519fee1 #####	79c9a666e776781578db55d1ca191c15e10b74e6	79c9a666e776781578db55d1ca191c15e10b74e6	True	c:\windows\system32\taskhost.exe	taskhostw.exe
15	Unassociated	0000f519fee1 #####	99bf5030a015c2f5bea0ab7196b925f6b8d959f9	99bf5030a015c2f5bea0ab7196b925f6b8d959f9	False	c:\windows\winsxs\amd64_microsoft-windows-servicingstack_31b710100000_6.3.9600.17765\TiWorker.exe	TiWorker.exe
16	Unassociated	0000f519fee1 #####			False		
17	Unassociated	0000f519fee1 #####					
18							
19							
20							
21							
22							

Complete *list of executables* and their metadata extracted from *AmCache.hve* registry hive

AmCache Update Behavior

Empty AmCache typically indicates either:

- Programs were never executed
- The hive hasn't been updated yet

AmCache updates primarily occur when:

- Binaries are executed
- Scheduled tasks run (like Application Experience service)

Proactive Investigation Step :

To ensure comprehensive data, I ran the Microsoft Compatibility Appraiser to force AmCache updates, allowing us to identify currently active malware.

Critical Finding

Malware Hash Identified: c51217ce3d1959e99886a567d21d0b97022bd6e3 (**AtomicService.exe**)

The screenshot shows the VirusTotal analysis interface for the file hash c51217ce3d1959e99886a567d21d0b97022bd6e3. The main summary indicates that 2/71 security vendors flagged the file as malicious. The file name "AtomicService.exe" is highlighted with a red box. Below the summary, the file details show it is a PE executable (4.00 KB) with various detection tags like "detect-debug-environment", "runtime-modules", "long-sleeps", "direct-cpu-clock-access", and "assembly". The "Community Score" is shown as 2/71. The "DETECTION" tab is selected. A green banner at the bottom encourages joining the community for additional insights and automation features.

The hash flagged as malicious in VirusTotal analysis

5. Prefetch Analysis

What is Prefetch?

Prefetch is a Windows optimization feature that speeds up application startup by storing execution data, creating valuable forensic artifacts that track program usage patterns.

Prefetch File Location:

⇒ C:\Windows\Prefetch*.pf

Forensic Value of Prefetch :

- Executable names and file paths
- First and last execution timestamps
- Execution count (how many times run)
- Referenced files/DLLs used by applications

- Volume information and file locations

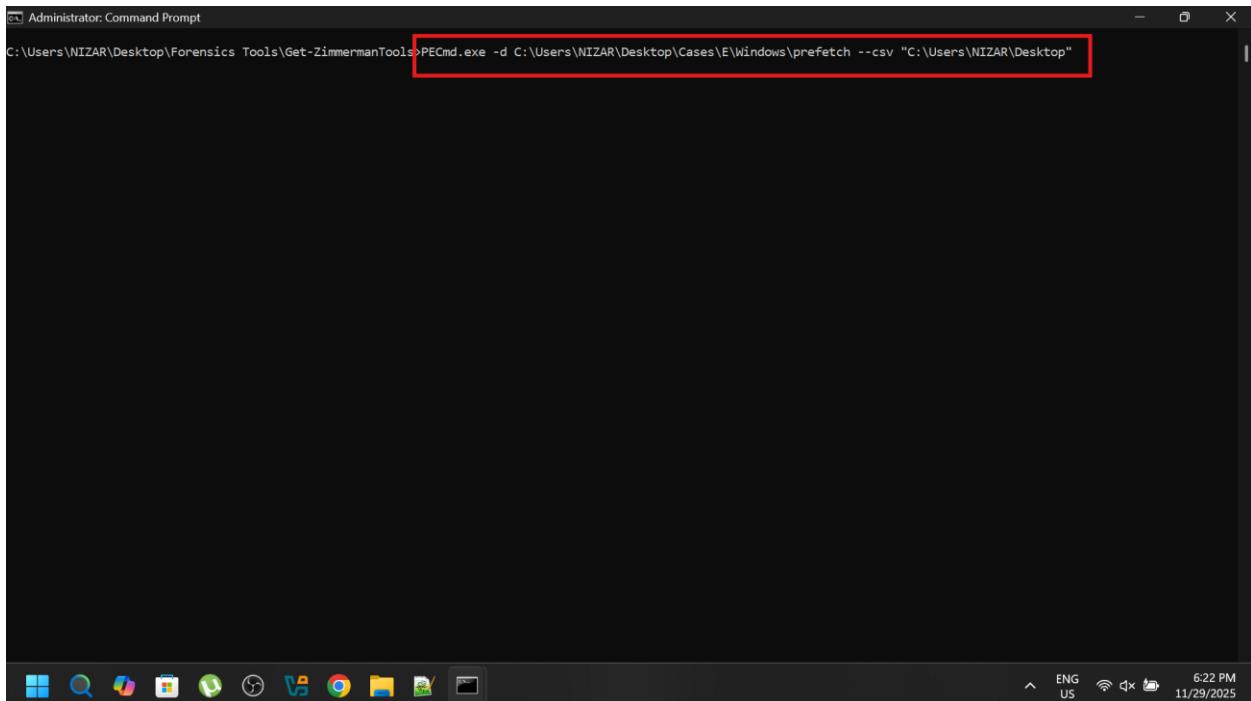
Key Characteristics :

- Desktop Windows only (not default on Server versions)
- Limited storage (128-1024 files, older ones overwritten)
- File naming: EXECUTABLE-RANDOMHASH.pf
- Different hash = different file location/path

Analysis Method :

Prefetch Parsing Command :

⇒ PECmd.exe -d C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch --csv "C:\Users\NIZAR\Desktop"



```
Administrator: Command Prompt
C:\Users\NIZAR\Desktop\Forensics Tools\Get-ZimmermanTools>PECmd.exe -d C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch --csv "C:\Users\NIZAR\Desktop"
```

Executing **PECmd** to parse Windows **Prefetch files** and generate execution timeline data

```

Administrator: Command Prompt
148: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\EN-US\NGCRECOVERY.DLL.MUI
149: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\EN-US\CRYPT32.DLL.MUI
150: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\C_28591.NLS
151: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SERVICEPROFILES\LOCALSERVICE\APPDATA\LOCAL\FONTCACHE\~FONTCACHE-FONTFACE.DAT
152: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SERVICEPROFILES\LOCALSERVICE\APPDATA\LOCAL\FONTCACHE\~FONTCACHE-S-1-5-21-1767728838-24418769-4131373679-1001.DAT
153: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\TZRES.DLL
154: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\EN-US\TZRES.DLL.MUI
155: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\XMLLITE.DLL
156: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\SXS.DLL
157: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\XMLHUB_18.1903.1152.0_X64_8WEKYB3D8BBWE\MOFFICE.BACKGROUNDTASKS.WINMD
158: \VOLUME{\01dc3a60e\095701-04ec23c2}\USERS\KR3L_DF\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\AC\MICROSOFT\INTERNET_EXPLORER\DOMSTORE\QQ8P2YQ\WMM.OFFICE[1].XML
159: \VOLUME{\01dc3a60e\095701-04ec23c2}\USERS\KR3L_DF\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\AC\MICROSOFT\CRYPTNETURLCACHE\METADATA\7423F88C7F265F00EFC08EA88C3BD45_AA1E858004EB816148CE81268683776
160: \VOLUME{\01dc3a60e\095701-04ec23c2}\PROGRAM FILES\WINDOWSAPPS\MICROSOFT.MICROSOFTOFFICEHUB_18.1903.1152.0_X64_8WEKYB3D8BBWE\AC\MICROSOFT\CRYPTNETURLCACHE\CONTENT\7423F88C7F265F00EFC08EA88C3BD45_AA1E858004EB816148CE81268683777
161: \VOLUME{\01dc3a60e\095701-04ec23c2}\USERS\KR3L_DF\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\AC\INETCACHE\I57JMAQQ\ERROR[1].CSS
162: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.APPLICATIONMODEL.WINMD
163: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.FOUNDATION.WINMD
164: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.SYSTEM.WINMD
165: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\APPCONTRACTS.DLL
166: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\WINMETADATA\WINDOWS.STORAGE.WINMD
167: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\WINDOWS.STATErepository.DLL
168: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\CDPRT.DLL
169: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\CDP.DLL
170: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\DISREG.DLL
171: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\MSVCP110_WIN.DLL
172: \VOLUME{\01dc3a60e\095701-04ec23c2}\USERS\KR3L_DF\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\AC\INETCACHE\J4CBW2KP\ODC_HOMEPAGEBIGARROW_LTR-060C245A73[1].PNG
173: \VOLUME{\01dc3a60e\095701-04ec23c2}\USERS\KR3L_DF\APPDATA\LOCAL\PACKAGES\MICROSOFT.MICROSOFTOFFICEHUB_8WEKYB3D8BBWE\AC\INETCACHE\MSIMGSIZ.DAT
174: \VOLUME{\01dc3a60e\095701-04ec23c2}\WINDOWS\SYSTEM32\WINDOWSCODECS.DLL

----- Processed C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\WIAHOST.EXE-DB8D8801.pf in 0.09705990 seconds -----
Processed 178 out of 178 files in 9.036 seconds

CSV output will be saved to C:\Users\NIZAR\Desktop\20251129162130_PECmd_Output.csv
CSV time line output will be saved to C:\Users\NIZAR\Desktop\20251129162130_PECmd_Output_Timeline.csv

```

C:\Users\NIZAR\Desktop\Forensics Tools\Get-ZimmermanTools>

ENG US 6:23 PM 11/29/2025

PECmd executed successfully, Prefetch analysis completed and CSV exported

20251129162130_PECmd_Output.csv - Excel							R		
1	SourceFilename	C	SourceCreated	D	SourceModified	E	SourceAccessed	F	ExecutableName
2	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\APPLICATIONFRAMEHOST.EXE-CCEE5F759.pf		10/10/2025 17:05		10/10/2025 17:05		11/29/2025 16:21		APPLICATIONFRAMEHOST.EXE
3	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\ATOMICSERVICE.EXE-94EEF3DF.pf		10/10/2025 17:37		10/10/2025 17:37		11/29/2025 16:21		ATOMICSERVICE.EXE
4	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\AUDIODG.EXE-BDFD3029.pf		10/10/2025 16:51		10/10/2025 17:41		11/29/2025 16:21		AUDIODG.EXE
5	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\BACKGROUNDTASKHOST.EXE-119C8B1B.pf		10/10/2025 16:51		10/10/2025 16:57		11/29/2025 16:21		BACKGROUNDTASKHOST.EXE
6	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\BACKGROUNDTASKHOST.EXE-9BA7511C.pf		10/10/2025 16:58		10/10/2025 17:32		11/29/2025 16:21		BACKGROUNDTASKHOST.EXE
7	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\BACKGROUNDTASKHOST.EXE-BB001E4D.pf		10/10/2025 17:05		10/10/2025 17:05		11/29/2025 16:21		BACKGROUNDTASKHOST.EXE
8	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\BACKGROUNDTRANSFERHOST.EXE-C9D9A465.pf		10/10/2025 16:59		10/10/2025 17:28		11/29/2025 16:21		BACKGROUNDTRANSFERHOST.EXE
9	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\BYTECODEGENERATOR.EXE-C1E9BCE6.pf		10/10/2025 17:05		10/10/2025 17:05		11/29/2025 16:21		BYTECODEGENERATOR.EXE
10	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\CMD.EXE-A481B364.pf		10/10/2025 17:37		10/10/2025 17:37		11/29/2025 16:21		CMD.EXE
11	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\CONHOST.EXE-1F3E9D7E.pf		10/10/2025 17:01		10/10/2025 17:39		11/29/2025 16:21		CONHOST.EXE
12	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\CONSENT.EXE-531BD9EA.pf		10/10/2025 16:57		10/10/2025 17:41		11/29/2025 16:21		CONSENT.EXE
13	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\CSCE.EXE-67679278.pf		10/10/2025 17:24		10/10/2025 17:35		11/29/2025 16:21		CSC.EXE
14	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\CRSS.EXE-3F4E1F7E.pf		10/10/2025 16:57		10/10/2025 16:57		11/29/2025 16:21		CRSS.EXE
15	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\CVTRES.EXE-F2B7602E.pf		10/10/2025 17:24		10/10/2025 17:35		11/29/2025 16:21		CVTRES.EXE
16	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\DLLHOST.EXE-28A8211F.pf		10/10/2025 16:51		10/10/2025 17:16		11/29/2025 16:21		DLLHOST.EXE
17	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\DLLHOST.EXE-504C779A.pf		10/10/2025 16:53		10/10/2025 17:04		11/29/2025 16:21		DLLHOST.EXE
18	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\DLLHOST.EXE-570206E5.pf		10/10/2025 16:52		10/10/2025 16:52		11/29/2025 16:21		DLLHOST.EXE
19	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\DLLHOST.EXE-5E46FA0D.pf		10/10/2025 16:51		10/10/2025 17:40		11/29/2025 16:21		DLLHOST.EXE
20	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\DLLHOST.EXE-766398D2.pf		10/10/2025 16:56		10/10/2025 17:03		11/29/2025 16:21		DLLHOST.EXE
21	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\DLLHOST.EXE-ABDE6D5B.pf		10/10/2025 16:51		10/10/2025 16:55		11/29/2025 16:21		DLLHOST.EXE
22	C:\Users\NIZAR\Desktop\Cases\E\Windows\prefetch\DLLHOST.EXE-BFD940A4.pf		10/10/2025 16:57		10/10/2025 16:57		11/29/2025 16:21		DLLHOST.EXE

Prefetch analysis showing ATOMICSERVICE.EXE execution, confirming Atomic Red Team tool usage

ENG US 6:24 PM 11/29/2025

RunTime	ExecutableName
10/10/2025 17:05	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\APPLICATIONFRAMEHOST.EXE
10/10/2025 17:37	\VOLUME\b6e0ec095701-04ec23\ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM-724CB3F50DCDD341815D5D2F34CBF90168017404\ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE
10/10/2025 17:40	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\AUDIODG.EXE
10/10/2025 17:33	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\AUDIODG.EXE
10/10/2025 17:16	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\AUDIODG.EXE
10/10/2025 16:51	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\AUDIODG.EXE
10/10/2025 16:57	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 16:51	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 17:32	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 17:03	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 16:58	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 17:05	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTASKHOST.EXE
10/10/2025 17:28	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTRANSFERHOST.EXE
10/10/2025 17:28	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTRANSFERHOST.EXE
10/10/2025 16:59	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BACKGROUNDTRANSFERHOST.EXE
10/10/2025 16:59	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BYTEXCODEGENERATOR.EXE
10/10/2025 17:05	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\BYTEXCODEGENERATOR.EXE
10/10/2025 17:37	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\CMD.EXE
10/10/2025 17:37	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\CONHOST.EXE
10/10/2025 17:37	\VOLUME\b6e0ec095701-04ec23\Windows\SYSTEM32\CONHOST.EXE

ATOMICSERVICE.EXE last executed at 2025-10-10 17:37:43 - confirming red team activity timestamp

Key Findings & Analysis :

1. Suspicious or Unusual Executables

ATOMICSERVICE.EXE was executed from:

- ⇒ \ATOMICREDTEAM\TMP\ATOMIC-RED-TEAM ... \ATOMICS\T1543.003\BIN\ATOMICSERVICE.EXE

- This path strongly suggests **Atomic Red Team**, a well-known adversary simulation framework used for testing security controls.

- **MITRE ATT&CK Technique: T1543.003 – Create or Modify System Process:** Windows Service

2. Powershell Activity

- CONHOST.EXE and POWERSHELL.EXE were executed multiple times.

- PowerShell is commonly used for legitimate administration but also for post-exploitation and lateral movement.

3. Scheduled Task Activity

SCHTASKS.EXE was launched via **CMD.EXE**, indicating **possible scheduled task creation or modification.**

4. User-Level Persistence Attempt

CMD.EXE referenced:

⇒ \USERS\KR3L_DF\APPDATA\ROAMING\MICROSOFT\WINDOWS\START
MENU\PROGRAMS\STARTUP\BATSTARTUP.BAT

This is a startup script location for persistence

5. Background Tasks Hosts & DLL Hosts

Multiple instances of **BACKGROUNDTASKHOST.EXE** and **DLLHOST.EXE** were launched, some associated with:

- Content Delivery Manager
- AAD Broker Plugin
- Microsoft Office Hub
- **These are typically legitimate but can be abused for code execution.**

6. Compilation Activity

CSC.EXE (C# Compiler) and **CVTRES.EXE** (Resource Converter) were executed, suggesting on-the-fly compilation of **C# code**, often seen **in offensive toolkits.**

7. Timeline of interest

- **Most activity** occurred between **16:51** and **17:41** on **2025-10-10**.
- Multiple **CONHOST.EXE** and **DLLHOST.EXE** instances suggest **interactive or scripted sessions.**