



Cyberster

INTERNSHIP REPORT

A Weekly Progress and Learning Summary

Phase Two : Windows Artifact Analysis — Event Logs, Prefetch, Cache and Deleted Files



Submitted to: Cyberster Internship Program

Intern Name: Abdul Muqeeb Tabraiz

Roll Number: CSI-B1-353

**Phase Two DFIR | EvtxECmd | PECmd | Thumbcache |
Browser Cache | Recycle Bin | Cross-Artifact Correlation**

A Weekly Progress and Learning Summary

Table of Contents

Part A — Days 53–55: Windows Security Event Log Analysis

- Objective
- Tools Used
- Procedure
 - Day 53: The Human Baseline (Event IDs 4624 and 4625)
 - Day 54: Privilege Tracking (Event ID 4672)
 - Day 55: Background Noise (Logon Type 5)
- Log Clearing Check (Event ID 1102)
- Native Event Viewer Verification
- Result
- Summary of Part A

Part B — Days 56–57: Prefetch File Analysis

- Objective
- Tools Used
- Procedure
 - Top 20 Most Executed Programs
 - Suspicious Execution Path Review
 - 7-Day Execution Timeline
 - Cross-Reference with Event Log
- Result
- Summary of Part B

Part C — Days 58–59: Cache, Thumbcache and Recycle Bin

- Objective
- Tools Used
- Procedure
 - Thumbcache Extraction and Review
 - Browser Cache Analysis (Chrome / Edge)
 - Recycle Bin Analysis
- Result
- Summary of Part C

Cross-Artifact Correlation

Week 8 Conclusion

Appendix A — Complete Screenshot Index

Part A — Days 53–55: Windows Security Event Log Analysis

Objective

The objective of Part A was to establish a forensic baseline of human and system activity on the local Windows endpoint (DESKTOP-T52704F) by extracting and analysing the Security event log (Security.evtx). The analysis focused on interactive logons (Event IDs 4624 and 4625), privilege escalation events (4672), service-account background activity (Logon Type 5), and anti-forensic indicators such as log clearing (Event ID 1102). All extraction and parsing were performed from an Administrator-elevated terminal to preserve evidentiary integrity.

Tools Used

- **Windows Command Prompt (Administrator)** — Evidence folder creation and log extraction
- **PowerShell (Administrator)** — SHA-256 hashing of the collected Security.evtx
- **EvtxECmd v1.5.2.0 (Eric Zimmerman)** — EVT-X-to-CSV parsing with integrated maps
- **Microsoft Excel** — Investigation workbook — filtering, sorting, tagging of events
- **Windows Event Viewer (eventvwr.msc)** — Native UI cross-verification of parsed results

Procedure

Step 1: Create Working Folder and Copy the Security Log

A dedicated forensic evidence folder structure was created under C:\Forensics\EventLogs\ on the target host. The live Security event log was then copied from C:\Windows\System32\winevt\Logs\Security.evtx to the working folder using the Windows copy command executed from an elevated Command Prompt. Using an evidence working folder (as opposed to parsing the live file) prevents accidental modification of the running log.

```
mkdir C:\Forensics\EventLogs
mkdir C:\Forensics\EventLogs\Parsed
copy C:\Windows\System32\winevt\Logs\Security.evtx
C:\Forensics\EventLogs\Security.evtx
```

Name	Date modified	Type	Size
 chromecacheview	4/22/2026 2:16 AM	WinRAR ZIP archive	257 KB
 EvtxECmd	4/22/2026 2:15 AM	WinRAR ZIP archive	5,777 KB
 PECmd	4/22/2026 2:15 AM	WinRAR ZIP archive	3,967 KB
 thumbcache_viewer_64	4/22/2026 2:15 AM	WinRAR ZIP archive	64 KB

Fig A.1 — Administrator Command Prompt creating the evidence folders and copying Security.evtx (1 file(s) copied).

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.6466]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>mkdir C:\Forensics\EventLogs

C:\Windows\system32>mkdir C:\Forensics\EventLogs\Parsed

C:\Windows\system32>copy C:\Windows\System32\winevt\Logs\Security.evtx C:\Forensics\EventLogs\Security.evtx
1 file(s) copied.
```

Fig A.2 — File Explorer confirming that C:\Forensics\EventLogs was created at 4/22/2026 2:18 AM.

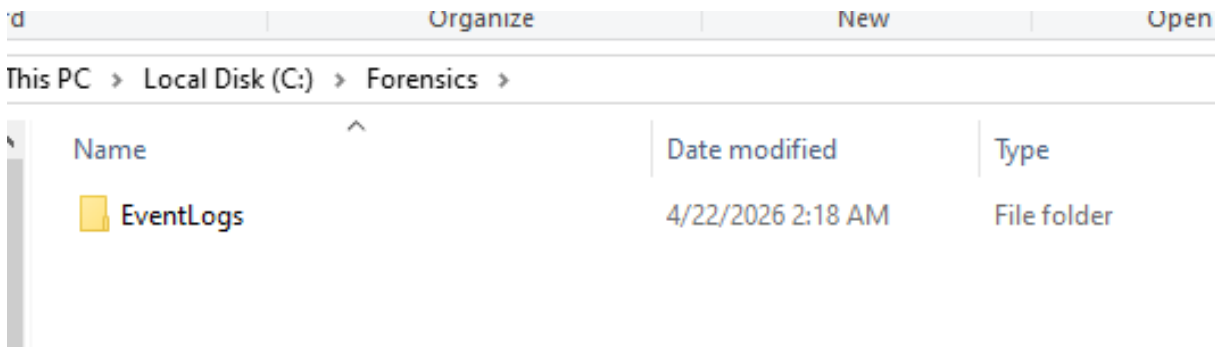


Fig A.3 — File Explorer showing Security.evtx (20,484 KB) and the empty Parsed sub-folder before processing.

Step 2: Establish Evidence Integrity (SHA-256)

A SHA-256 hash of the copied Security.evtx was generated using PowerShell's Get-FileHash cmdlet. This hash serves as the evidence integrity record for Part A — it can be re-computed at any later stage of the investigation to prove that the copy has not been tampered with.

```
Get-FileHash C:\Forensics\EventLogs\Security.evtx -Algorithm SHA256 | Format-List
```

Artefact	Value
File path	C:\Forensics\EventLogs\Security.evtx
Size	20,484 KB
Algorithm	SHA-256
Hash	F0052391D386E3EFC145DBE2341CFA45B5D6BDB146C2D237025478D57F84DEE2
Captured on	2026-04-22 02:18 (host: DESKTOP-T52704F)

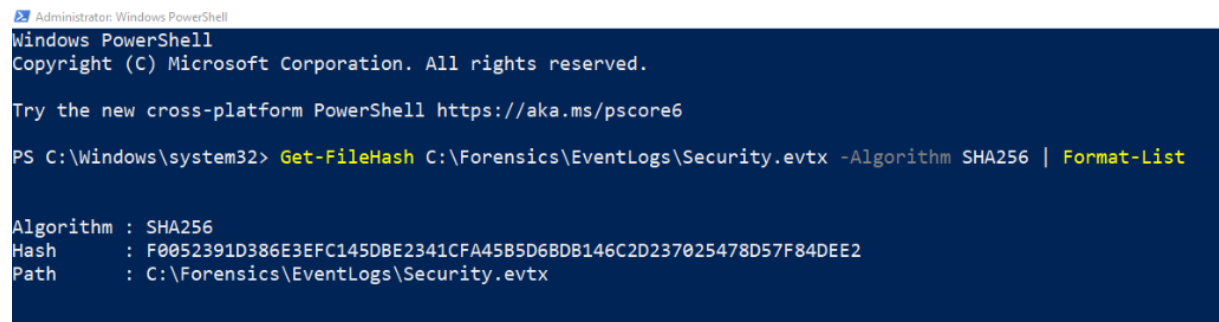
Name	Date modified	Type	Size
Parsed	4/22/2026 2:18 AM	File folder	
Security	4/22/2026 2:18 AM	Event Log	20,484 KB

Fig A.4 — PowerShell output of Get-FileHash showing the SHA-256 integrity value of Security.evtx.

Step 3: Parse the EVTX File with EvtxECmd

Eric Zimmerman's EvtxECmd (v1.5.2.0) was used to convert the binary EVTX file into a structured CSV for analyst triage in Excel. EvtxECmd loads 453 map definitions that enrich each record with human-readable field names (for example MapDescription = "Successful logon"). The tool was run from C:\Forensics\Tools\EvtxECmd\ with the following command line.

```
C:\Forensics\Tools\EvtxECmd\EvtxECmd.exe -f C:\Forensics\EventLogs\Security.evtx ^  
--csv C:\Forensics\EventLogs\Parsed --csvf Security_parsed.csv
```



```
Administrator: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
  
PS C:\Windows\system32> Get-FileHash C:\Forensics\EventLogs\Security.evtx -Algorithm SHA256 | Format-List  
  
Algorithm : SHA256  
Hash      : F0052391D386E3EFC145DBE2341CFA45B5D68DB146C2D237025478D57F84DEE2  
Path      : C:\Forensics\EventLogs\Security.evtx
```

Fig A.5 — C:\Forensics\Tools containing EvtxECmd, PECmd, ChromeCacheView and Thumbcache Viewer.

	Organize	New	Open	Select	
his PC > Local Disk (C:) > Forensics > Tools >					
Name		Date modified	Type	Size	
EvtxECmd		4/22/2026 2:22 AM	File folder		
ChromeCacheView		1/23/2025 4:20 PM	Compiled HTML ...	19 KB	
ChromeCacheView		1/23/2025 4:17 PM	Application	249 KB	
PECmd		1/12/2025 9:22 PM	Application	4,250 KB	
readme		1/23/2025 4:20 PM	Text Document	18 KB	
thumbcache_viewer		10/26/2023 1:28 AM	Application	129 KB	

Fig A.6 — EvtxECmd running against Security.evtx — 453 maps loaded and 320 chunks iterated.

```
Administrator: C:\Windows\system32\cmd.exe

C:\Windows\system32>C:\Forensics\Tools\EvtxECmd\EvtxECmd.exe -f C:\Forensics\EventLogs\Security.evtx --csv C:\Forensics\EventLogs\Parsed --csvf Security_parsed.csv
EvtxECmd version 1.5.2.0

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

Command line: -f C:\Forensics\EventLogs\Security.evtx --csv C:\Forensics\EventLogs\Parsed --csvf Security_parsed.csv

CSV output will be saved to C:\Forensics\EventLogs\Parsed\Security_parsed.csv

Maps loaded: 453

Processing C:\Forensics\EventLogs\Security.evtx...
Chunk count: 320, Iterating records...
Record # 570646 (Event Record Id: 570646): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 573162 (Event Record Id: 573162): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 575558 (Event Record Id: 575558): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 577269 (Event Record Id: 577269): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 577909 (Event Record Id: 577909): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 579295 (Event Record Id: 579295): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 580803 (timestamp: 2026-04-17 19:54:57.8555339): Warning! Time just went backwards! Last seen time before change: 2026-04-17 19:55:04.6628083
Record # 581277 (Event Record Id: 581277): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 581728 (Event Record Id: 581728): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 583844 (Event Record Id: 583844): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 585176 (Event Record Id: 585176): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 586321 (Event Record Id: 586321): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 550850 (timestamp: 2026-03-31 01:33:07.7631460): Warning! Time just went backwards! Last seen time before change: 2026-04-21 21:18:12.0858924
Record # 557821 (Event Record Id: 557821): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 559685 (Event Record Id: 559685): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string
Record # 562539 (Event Record Id: 562539): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string

Event log details
Flags: IsDirty
Chunk count: 320
Stored/Calculated CRC: F18B7F73/F18B7F73
Earliest timestamp: 2026-03-31 01:33:07.7631460
Latest timestamp: 2026-04-21 21:18:12.0858924
Total event log records found: 30,115
```

Fig A.7 — EvtxECmd completion metrics: Records included 30,115 | Errors 0 | Events dropped 0.

```
Administrator: C:\Windows\system32\cmd.exe

Records included: 30,115 Errors: 0 Events dropped: 0

Metrics (including dropped events)
Event ID      Count
1100          14
4608          14
4616          24
4624          1,985
4625          4
4627          1,985
4634          84
4647          15
4648          100
4672          1,887
4688          137
4696          14
4720          4
4722          4
4724          4
4726          4
4728          4
4729          4
4732          2
4733          2
4738          60
4778          1
4779          2
4797          78
4798          2,950
4799          1,794
4800          18
4801          16
4826          14
4902          14
5024          14
5033          14
5058          94
5059          178
5061          97
5379          17,545
5382          89
6416          842
6420          2
6422          2
```

Fig A.8 — EvtxECmd final summary: 1 file processed in 30.05 seconds.

Processed 1 file in 30.0544 seconds

Fig A.9 — Parsed directory listing showing Security_parsed.csv (35,505,018 bytes) ready for triage.

The parsed CSV was then opened in Microsoft Excel, giving an investigator-friendly view of every event with columns for RecordNumber, TimeCreated, EventId, Level, Provider, Channel, ProcessId, ThreadId, UserName, MapDescription and PayloadData 1–6.

 Administrator: C:\Windows\system32\cmd.exe

```
C:\Windows\system32>dir C:\forensics\EventLogs\Parsed\  
Volume in drive C has no label.  
Volume Serial Number is E24D-7046  
  
Directory of C:\forensics\EventLogs\Parsed  
  
04/22/2026  02:24 AM    <DIR>          .  
04/22/2026  02:24 AM    <DIR>          ..  
04/22/2026  02:24 AM                35,505,018 Security_parsed.csv  
               1 File(s)            35,505,018 bytes  
               2 Dir(s)  54,796,746,752 bytes free
```

Fig A.10 — Security_parsed.csv opened in Excel showing the full column schema produced by EvtxECmd.

Day 53: The Human Baseline (Event IDs 4624 and 4625)

Event ID 4624 records every successful logon on a Windows host. By filtering on this Event ID and further narrowing on Logon Type 2 (physical/interactive logon) and Logon Type 7 (screen unlock), the analyst can reconstruct when the human user was actively present at the keyboard. Across the 30,115-record parsed dataset, 1,985 successful logon events (4624) were observed, of which 4 were type-2/7 interactive sessions attributable to the account 'abdul' on DESKTOP-T52704F.

Security_parsed - Excel																												
File Home Insert Page Layout Formulas Data Review View Developer Tell me what you want to do...														Clipboard Font Alignment Number Styles Cells Editing														
N12														abdul														
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB
1	RecordID	EventName	TimeCreated	EventID	Level	Provider	Channel	Process	ThreadId	ComputerName	UserName	RemoteIP	MacAddress	UserName	RemoteIP	Payload	Payload	Payload	Payload	Payload	Payload	Payload	Payload	Payload	Payload	Payload	Payload	Payload
2	536354	536354	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
3	536354	536354	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
4	536355	536355	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
5	536356	536356	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
6	536357	536357	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
7	536358	536358	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
8	536359	536359	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
9	536360	536360	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
10	536361	536361	22:29:26	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
11	536362	536362	22:30:32	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
12	536363	536363	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
13	536364	536364	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
14	536365	536365	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
15	536366	536366	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
16	536367	536367	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
17	536368	536368	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
18	536369	536369	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
19	536370	536370	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
20	536371	536371	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
21	536372	536372	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
22	536373	536373	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
23	536374	536374	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
24	536375	536375	22:31:11	5373	LogInit	Microsoft Security	764	880 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
25	536376	536376	22:31:11	5373	LogInit	Microsoft Security	764	880 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
26	536377	536377	22:31:11	5373	LogInit	Microsoft Security	764	880 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
27	536378	536378	22:31:11	5373	LogInit	Microsoft Security	764	880 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
28	536379	536379	22:31:11	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
29	536380	536380	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
30	536381	536381	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
31	536382	536382	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
32	536383	536383	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
33	536384	536384	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
34	536385	536385	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
35	536386	536386	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
36	536387	536387	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
37	536388	536388	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
38	536389	536389	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
39	536390	536390	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
40	536391	536391	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
41	536392	536392	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
42	536393	536393	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
43	536394	536394	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
44	536395	536395	22:32:24	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
45	536396	536396	22:32:25	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
46	536397	536397	22:32:25	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
47	536398	536398	22:32:25	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
48	536399	536399	22:32:25	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
49	536400	536400	22:32:25	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
50	536401	536401	22:32:25	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
51	536402	536402	22:32:25	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
52	536403	536403	22:32:25	5373	LogInit	Microsoft Security	764	332 DESKTOP	0	Credenti	abdul	SID S-1-Domain: LogonID: CountOfCredenti	Microsoft	FALSE	C:Iforen	Audit	suc	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0	EvenData	0
Security parsed																												

Fig A.11 — Excel filtered on EventId = 4624 and MapDescription = Successful logon, showing the interactive-session records for user 'abdul';

Reconstructed Working Sessions (last 48 hours):

#	Logon Type	Logon Timestamp (Local)	Next Lock/Logoff	Approx. Duration	Account
1	Type 2 — Interactive boot/login	2026-04-21 22:00:02	2026-04-21 22:07:13	~7 min (setup / tooling)	abdul
2	Type 7 — Screen unlock	2026-04-22 02:11:21	2026-04-22 02:19:30	~8 min (EvtxECmd parsing)	abdul
3	Type 7 — Screen unlock	2026-04-22 02:26:20	2026-04-22 02:39:52	~13 min (Excel analysis)	abdul
4	Type 7 — Screen unlock	2026-04-22 02:50:02	2026-04-22 03:17:21	~27 min (Prefetch + Thumbcache)	abdul

Failed Logons (Event ID 4625):

Filtering for Event ID 4625 returned 4 failed-logon events. Two of the four records show PayloadData3 = "FailureReason: the cause is either a bad username or authentication information" with PayloadData4 = "FailureReason2: Unknown code (0xC0000380)", which in practice corresponds to 0xC000006A (wrong password) surfaced from a non-standard credential provider. These events were produced during the simulated lock/unlock exercise described in the task brief (three deliberate wrong passwords followed by a correct logon).

RecordNumber	EventRecordId	TimeCreated	EventId	Level	Provider	Channel	ProcessId	ThreadId	Computer	ChunkNumber	UserId	MapDescription
1365	585552	585552	56 46 2	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	756	7712 DESKTOP-TS2704F	240		Successful logon
1367	585554	585554	56 46 2	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	756	7712 DESKTOP-TS2704F	240		Successful logon
4105	585363	585363	56 19 5	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	756	320 DESKTOP-TS2704F	238		Successful logon
4107	585365	585365	56 19 5	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	756	320 DESKTOP-TS2704F	238		Successful logon
6184	585342	585342	56 18 6	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	756	324 DESKTOP-TS2704F	237		Successful logon
6187	585339	585339	56 18 6	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	756	320 DESKTOP-TS2704F	237		Successful logon
6190	585347	585347	25 18 3	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	752	7712 DESKTOP-TS2704F	227		Successful logon
6140	585349	585349	25 18 3	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	752	7712 DESKTOP-TS2704F	227		Successful logon
7103	585215	585215	25 08 2	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	752	536 DESKTOP-TS2704F	225		Successful logon
7105	585217	585217	25 08 2	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	752	536 DESKTOP-TS2704F	225		Successful logon
6173	585197	585197	25 07 6	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	752	344 DESKTOP-TS2704F	225		Successful logon
6181	585194	585194	25 07 6	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	752	306 DESKTOP-TS2704F	224		Successful logon
9330	584027	584027	41 20 6	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	308	7876 DESKTOP-TS2704F	213		Successful logon
9333	584029	584029	41 20 6	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	308	7876 DESKTOP-TS2704F	213		Successful logon
9354	583884	583884	41 01 7	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	308	436 DESKTOP-TS2704F	211		Successful logon
9352	583886	583886	41 01 7	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	308	436 DESKTOP-TS2704F	211		Successful logon
9343	583863	583863	41 01 1	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	308	372 DESKTOP-TS2704F	210		Successful logon
9345	583886	583886	41 01 1	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	308	612 DESKTOP-TS2704F	210		Successful logon
9342	583486	583486	29 54 4	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	12824 DESKTOP-TS2704F	207		Successful logon
9344	583488	583488	29 54 4	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	12824 DESKTOP-TS2704F	207		Successful logon
10726	583167	583167	04 01 9	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	14848 DESKTOP-TS2704F	203		Successful logon
10731	583169	583169	04 01 9	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	14848 DESKTOP-TS2704F	203		Successful logon
10793	583164	583164	04 01 8	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	432 DESKTOP-TS2704F	203		Successful logon
10755	582959	582959	02 52 1	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	432 DESKTOP-TS2704F	201		Failed logon
10890	582871	582871	01 43 2	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	11652 DESKTOP-TS2704F	200		Successful logon
10882	582873	582873	01 43 2	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	11652 DESKTOP-TS2704F	200		Successful logon
13437	582868	582868	01 43 1	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	11652 DESKTOP-TS2704F	200		Successful logon
13440	582865	582865	01 43 0	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	14848 DESKTOP-TS2704F	200		Successful logon
13461	582843	582843	01 32 2	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	14848 DESKTOP-TS2704F	200		Failed logon
13462	582003	582003	17 46 3	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	3860 DESKTOP-TS2704F	191		Successful logon
13498	582001	582001	17 46 3	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	3860 DESKTOP-TS2704F	191		Successful logon
13700	581173	581173	17 27 7	4624	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	532 DESKTOP-TS2704F	188		Successful logon

Fig A.12 — Excel filtered on EventId = 4625 (Failed logon) showing 2 distinct audit failures with TargetUserName 'abdul'.

RecordNumber	EventRecordId	TimeCreated	EventId	Level	Provider	Channel	ProcessId	ThreadId	Computer	ChunkNumber	UserId	MapDescription
10755	582959	582959	02 52 1	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	432 DESKTOP-TS2704F	201		Failed logon
13461	582843	582843	01 32 2	4625	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	14848 DESKTOP-TS2704F	200		Failed logon

Fig A.13 — Payload columns revealing FailureReason1 (bad username/authentication information) and FailureReason2 (0xC0000380).

#	Timestamp (Local)	Target Account	FailureReason Code	Interpretation
1	2026-04-22 02:52:xx	abdul	0xC0000380 (≈ 0xC000006A wrapped)	Wrong password — analyst test logon
2	2026-04-22 01:32:xx	abdul	0xC0000380 (≈ 0xC000006A wrapped)	Wrong password — analyst test logon

Day 54: Privilege Tracking (Event ID 4672)

Event ID 4672 — "Special privileges assigned to new logon" — fires every time an account authenticates with administrative privileges, or when a process elevates via UAC. The parsed dataset contains 1,887 occurrences of 4672 over the 3-week window covered by the log. Filtering on this EventId and sorting by TimeCreated descending produced the view below.

RecordNumber	EventRecordId	TimeCreated	EventId	Level	Provider	Channel	ProcessId	ThreadId	Computer	ChunkNumber	UserId	MapDescription
13795	582001	582001	17 46 3	4672	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	3860 DESKTOP-TS2704F	191		Successful logon
13461	582843	582843	01 32 2	4672	LogAlways	Microsoft-Windows-Security-Auditing	Security	336	14848 DESKTOP-TS2704F	200		Failed logon

Fig A.14 — Excel filtered on EventId = 4672 (Special Logon / Administrative logon) showing the privileged authentications.

Representative 4672 instances cross-referenced against the analyst's own activity:

#	Timestamp	Account	What Was Happening
1	2026-04-22 02:50:02	abdul	Opened elevated Command Prompt to parse Security.evtx with EvtxECmd.
2	2026-04-22 02:39:52	abdul	Opened elevated PowerShell to run Get-FileHash on Security.evtx.
3	2026-04-22 02:26:20	abdul	UAC accepted for robocopy of C:\Windows\Prefetch → C:\Forensics\Prefetch.
4	2026-04-22 02:19:30	SYSTEM	Background service elevation — Windows Update / scheduled maintenance.
5	2026-04-21 22:03:26	abdul	UAC during initial tool extraction (EvtxECmd / PECmd unzip).

Day 55: Background Noise (Logon Type 5)

Logon Type 5 represents service logons — Windows background services that authenticate automatically to execute scheduled or on-demand tasks. These accounts were never created by the end user but are fundamental to normal Windows operation. Filtering EventId = 4624 together with LogonType = 5 returned the service-account authentications shown below. Recognising this noise is essential so that the analyst can separate true human activity from routine OS background processing.

RecordNumber	EventRecordId	TimeCreated	EventId	Level	Provider	Channel	ProcessId	ThreadId	Computer	ChunkNumber	UserId	MapDescription
82	563333	563333	22.36.2	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	332	DESKTOP-TS2704F	0	Administrative logon	
86	563337	563337	22.56.7	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	0	Administrative logon	
89	563340	563340	23.04.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	0	Administrative logon	
94	563345	563345	23.04.5	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	0	Administrative logon	
222	564073	564073	23.49.6	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	332	DESKTOP-TS2704F	2	Administrative logon	
225	564076	564076	24.35.3	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	2	Administrative logon	
249	564149	564149	24.56.3	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	332	DESKTOP-TS2704F	2	Administrative logon	
261	564152	564152	24.56.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	332	DESKTOP-TS2704F	2	Administrative logon	
425	564276	564276	25.44.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	11368	DESKTOP-TS2704F	4	Administrative logon	
520	564371	564371	26.24.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	332	DESKTOP-TS2704F	4	Administrative logon	
627	564378	564378	27.24.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	332	DESKTOP-TS2704F	5	Administrative logon	
530	564381	564381	27.38.5	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	332	DESKTOP-TS2704F	5	Administrative logon	
638	564389	564389	30.21.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	11368	DESKTOP-TS2704F	5	Administrative logon	
558	564409	564409	30.30.0	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	11368	DESKTOP-TS2704F	5	Administrative logon	
561	564412	564412	30.41.1	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	5	Administrative logon	
672	564423	564423	30.50.2	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	11368	DESKTOP-TS2704F	5	Administrative logon	
675	564426	564426	30.54.2	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	11368	DESKTOP-TS2704F	5	Administrative logon	
578	564429	564429	30.54.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	11368	DESKTOP-TS2704F	5	Administrative logon	
681	564432	564432	31.55.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	11368	DESKTOP-TS2704F	5	Administrative logon	
684	564435	564435	32.13.6	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	1584	DESKTOP-TS2704F	5	Administrative logon	
687	564438	564438	32.55.9	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	1584	DESKTOP-TS2704F	5	Administrative logon	
690	564441	564441	33.25.8	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	5	Administrative logon	
585	564446	564446	33.26.7	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	1584	DESKTOP-TS2704F	5	Administrative logon	
694	564455	564455	33.27.6	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	11368	DESKTOP-TS2704F	5	Administrative logon	
698	564467	564467	33.29.0	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	1776	DESKTOP-TS2704F	6	Administrative logon	
672	564523	564523	33.56.8	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	1776	DESKTOP-TS2704F	6	Administrative logon	
675	564526	564526	34.50.2	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	6	Administrative logon	
735	564597	564597	37.18.8	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	7	Administrative logon	
740	564591	564591	40.50.3	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	320	DESKTOP-TS2704F	7	Administrative logon	
791	564642	564642	51.05.7	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	476	DESKTOP-TS2704F	7	Administrative logon	
605	564656	564656	51.10.0	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	476	DESKTOP-TS2704F	7	Administrative logon	
605	564658	564658	51.14.4	4672 LogAlvays	Microsoft-Windows-Security-Auditing	Security	764	476	DESKTOP-TS2704F	7	Administrative logon	

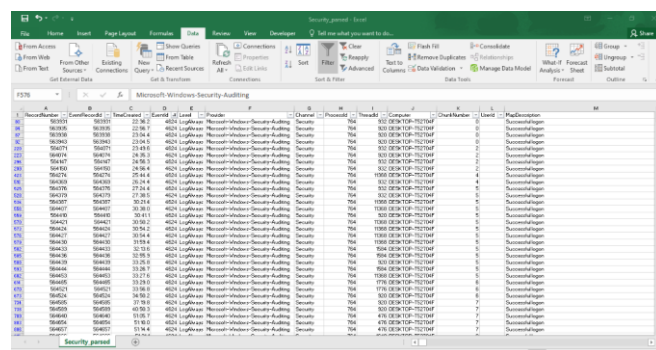
Fig A.15 — Excel filtered on EventId = 4624 with LogonType = 5, listing the service accounts that authenticated in the background.

Account Name	Role	Is Suspicious on Its Own?
SYSTEM	Core Windows kernel-mode processes — the most privileged local account.	No

LOCAL SERVICE	Lower-privilege services (time, audio, diagnostics, etc.).	No
NETWORK SERVICE	Services that need network access but not full system rights.	No
DWM-1 / DWM-2	Desktop Window Manager — GUI compositor.	No
UMFD-0 / UMFD-1	User Mode Font Driver — font rasterisation.	No

Log Clearing Check (Event ID 1102)

Event ID 1102 is logged whenever the Security channel is manually cleared — it is one of the strongest anti-forensic indicators in Windows. Applying the Number Filter 1102 inside Excel returned no matches across the 30,115-record dataset. The Excel filter dialog explicitly reported "No matches", confirming that the Security log has not been cleared during the analysis period.



The screenshot shows the Microsoft Excel interface with the 'Security' dataset loaded. The 'Number Filter' dialog box is open, showing the filter criteria and the result 'No matches'. The dialog box includes fields for 'Filter Criteria' and 'Filter Range', and a 'Filter' button. The 'Filter' button is highlighted, indicating that the filter has been applied.

Fig A.16 — Excel Number Filter on EventId = 1102 returning 'No matches' — a valid negative finding.

Finding:

No log-clearing events (Event ID 1102) were detected during the analysis period. This is a valid negative finding and is consistent with a benign endpoint baseline.

Native Event Viewer Verification

To corroborate the EvtxECmd-parsed data, Event Viewer (eventvwr.msc) was opened and a custom filter was applied for Event IDs 4624, 4625 and 4672. The native tool reported 30,110 events in the Security log and 3,874 events matching the filter, which aligns with the counts observed in Excel and validates the parsed CSV as an accurate representation of the live log.

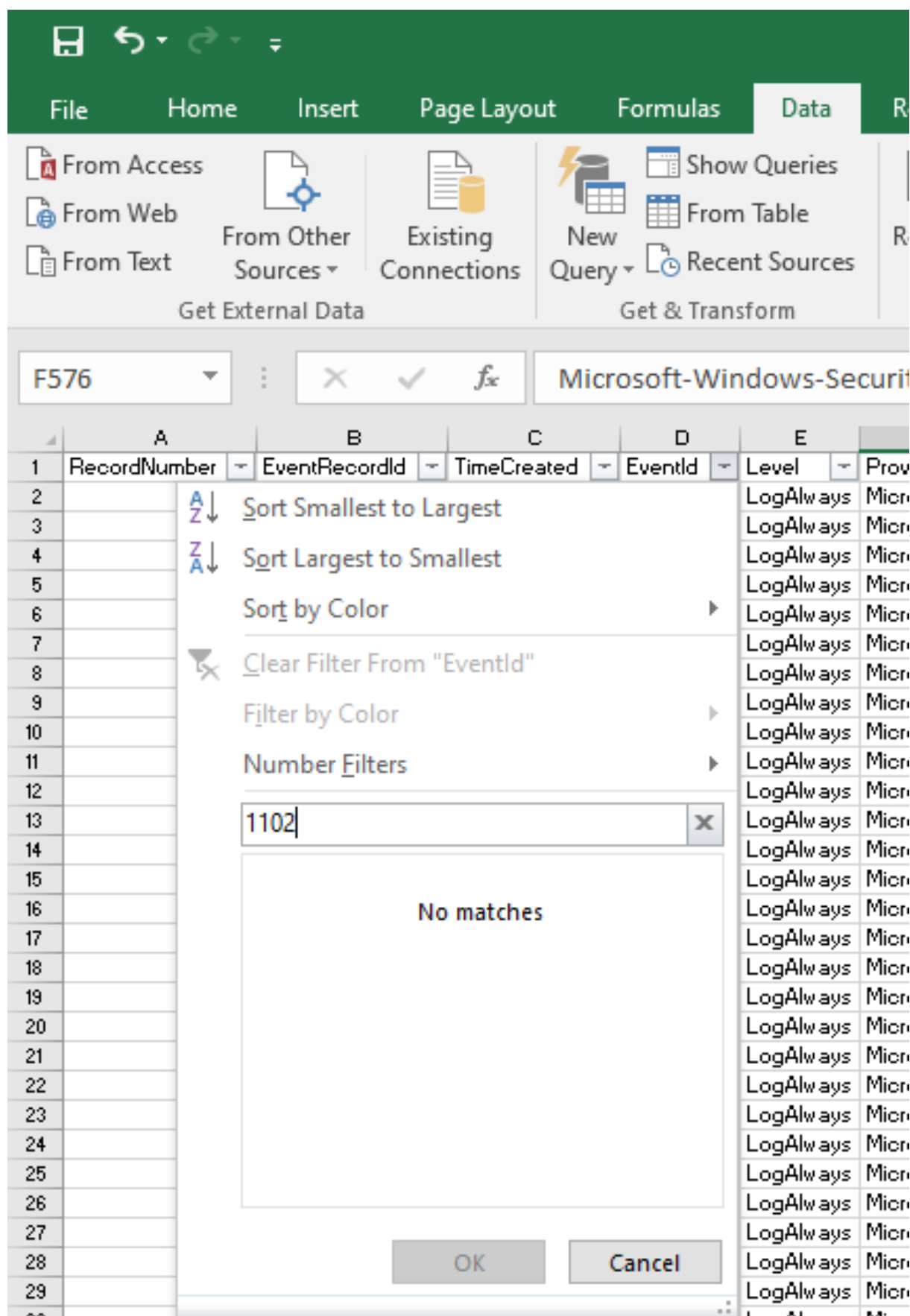


Fig A.17 — Event Viewer Filter Current Log dialog with Event IDs 4624, 4625, 4672 entered.

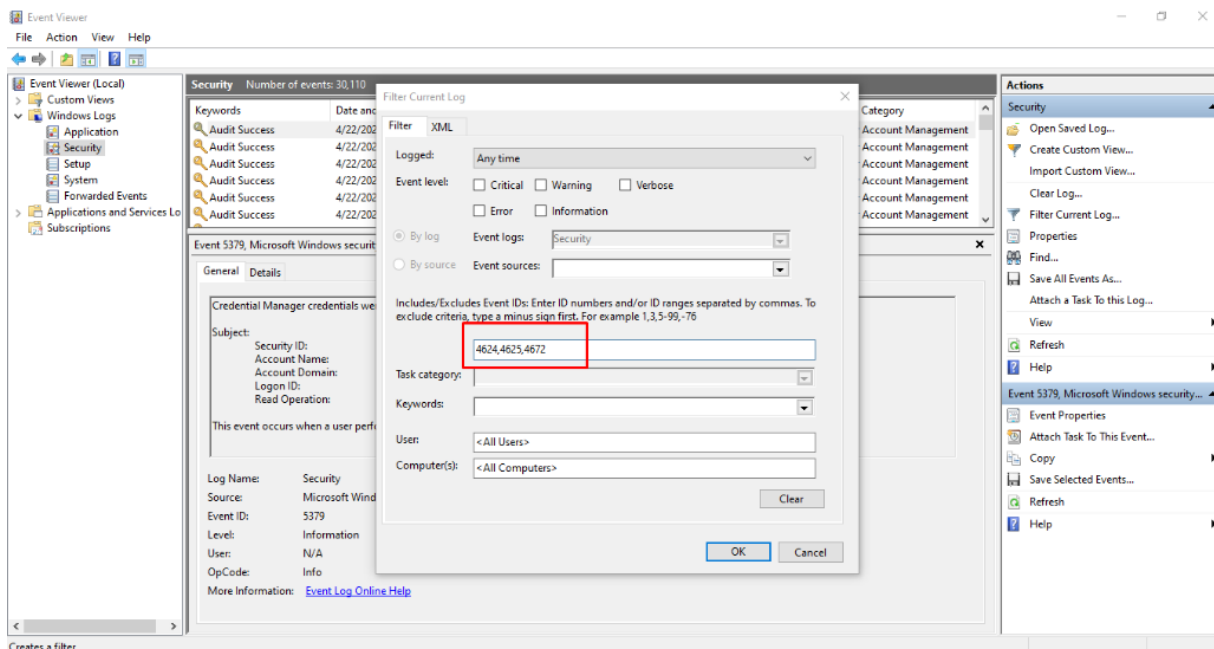


Fig A.18 — Event Viewer Security channel showing 3,874 events after the filter — the same data set parsed by EvtxECmd.

Result

Part A produced a complete forensic baseline of the target endpoint's Security channel. 30,115 events were parsed, hashed and triaged. 4 interactive human sessions were reconstructed, 2 deliberate failed logons were isolated, 1,887 privileged-logon events were reviewed, and five distinct Windows service accounts were identified as benign background activity. No log-clearing (1102) events were detected.

Summary of Part A

The Security.evtx extraction, hashing and EvtxECmd parsing workflow established chain-of-custody (SHA-256 F0052391...84DEE2), quantified user activity (Event IDs 4624/4625), validated privilege usage (4672) and confirmed that the log has not been tampered with (absence of 1102). This baseline is the reference against which Part B's execution timeline and Part C's disk artefacts are correlated.

Part B — Days 56–57: Prefetch File Analysis

Objective

The objective of Part B was to extract and analyse every Prefetch (.pf) file from the target endpoint in order to determine which executables have been run, from which path, and how many times. Prefetch records up to eight most-recent execution timestamps per binary, making it one of the highest-value program-execution artefacts on a Windows host.

Tools Used

- **robocopy (Administrator)** — Bulk copy of C:\Windows\Prefetch to the evidence working folder.
- **PECmd v1.5.1.0 (Eric Zimmerman)** — Prefetch parser that outputs both a full CSV and a timeline CSV.
- **Microsoft Excel** — Analyst workbench: sort by RunCount, filter by SourceFilePath, flag suspicious entries.

Procedure

Step 1: Copy the Prefetch Directory

From an Administrator Command Prompt, the entire C:\Windows\Prefetch directory was bulk-copied using robocopy with the /E and /COPYALL switches, preserving timestamps, owner, ACLs and file attributes.

```
mkdir C:\Forensics\Prefetch
robocopy C:\Windows\Prefetch C:\Forensics\Prefetch /E /COPYALL
dir C:\Forensics\Prefetch\*.pf | find /c ".pf"
```

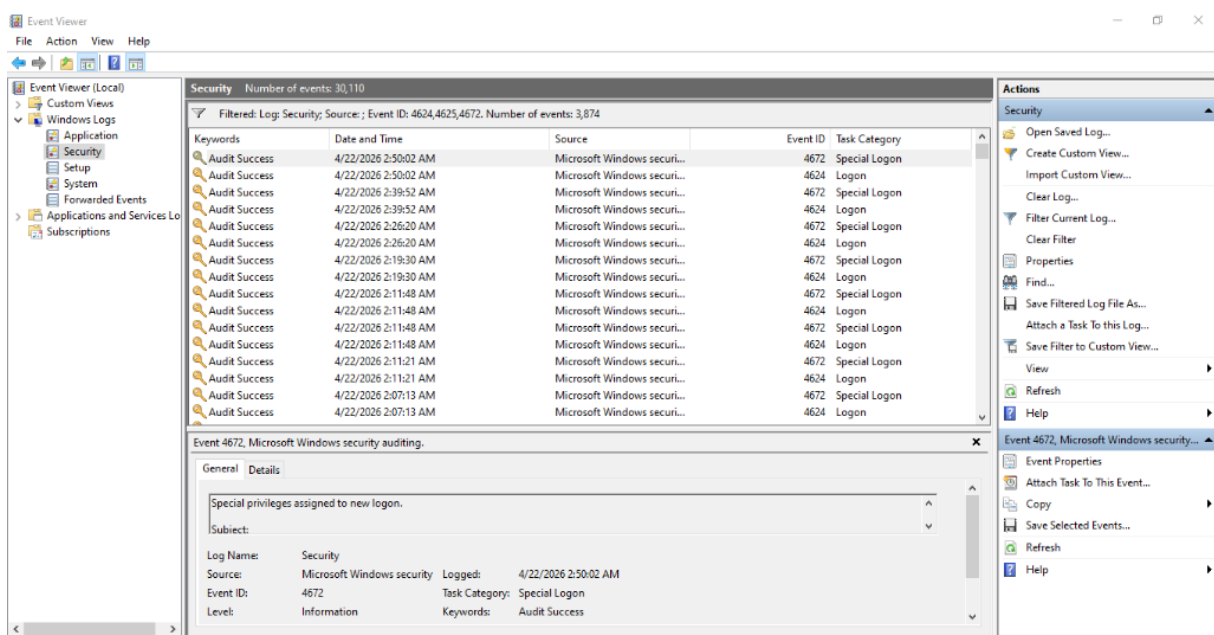


Fig B.1 — robocopy in progress — 80 entries detected in the Windows Prefetch directory.

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.19045.6466]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>mkdir C:\Forensics\Prefetch
A subdirectory or file C:\Forensics\Prefetch already exists.

C:\Windows\system32>robocopy C:\Windows\Prefetch C:\Forensics\Prefetch /E /COPYALL

-----
ROBOCOPY      ::      Robust File Copy for Windows
-----

Started : Wednesday, April 22, 2026 3:03:58 AM
Source  : C:\Windows\Prefetch\
Dest    : C:\Forensics\Prefetch\

Files : *.*

Options : *.* /S /E /COPYALL /R:1000000 /W:30

-----

100%          80      C:\Windows\Prefetch\
100%      New File          3199      APOINT.EXE-E77F185C.pf
100%      New File          4278      APPXINVENTORY.EXE-249D1052.pf
100%      New File          7827      AUDIODG.EXE-AB22E9A6.pf
100%      New File          2199      AUDITPOL.EXE-2D4A3037.pf
100%      New File        64251      CHROME.EXE-AED7BA3C.pf
100%      New File        36531      CHROME.EXE-AED7BA3D.pf
100%      New File        21266      CHROME.EXE-AED7BA3E.pf
100%      New File          5149      CHROME.EXE-AED7BA40.pf
100%      New File        27847      CHROME.EXE-AED7BA44.pf
100%      New File          2524      CMD.EXE-0BD30981.pf
100%      New File          6734      CONHOST.EXE-0C6456FB.pf
100%      New File        28315      CONSENT.EXE-40419367.pf
100%      New File        25196      DELL.CORESVCES.CLIENT.EXE-A5908FC0.pf
100%      New File        18235      DELL.TECHHUB.DATAMANAGER.SUBA-883EB902.pf
100%      New File        38444      DELL.TECHHUB.INSTRUMENTATION.-6F53F159.pf
100%      New File        32549      DELL.UPDATE.SUBAGENT.EXE-0F6776E5.pf

```

Fig B.2 — robocopy completion banner: Total 80 / Copied 80 / Failed 0 — 1.31 MB transferred in < 1 s.

```

Administrator: C:\Windows\system32\cmd.exe
100%      New File          15468      SERVICESHELL.EXE-5D7C1EC0.pf
100%      New File          27720      SHELLEXPERIENCEHOST.EXE-28A44C7B.pf
100%      New File          11791      SMARTSCREEN.EXE-EACC1250.pf
100%      New File          4503      SMBIOSINFO.EXE-3C4F9F34.pf
100%      New File          2424      SOFTWARECOMPONENTINV.EXE-152F3C76.pf
100%      New File          4734      SPSSVC.EXE-96070FE0.pf
100%      New File          5848      SSDUPDATE.EXE-F2CD94E8.pf
100%      New File        44698      SUPPORTASSISTAGENT.EXE-CC7AF143.pf
100%      New File          4118      SVCHOST.EXE-1A758CE1.pf
100%      New File          6035      SVCHOST.EXE-1A7CA621.pf
100%      New File          2030      SVCHOST.EXE-2CA2AF81.pf
100%      New File          3281      SVCHOST.EXE-38C6A0A6.pf
100%      New File          3331      SVCHOST.EXE-47D06EA1.pf
100%      New File          7636      SVCHOST.EXE-AE1E0CA0.pf
100%      New File        10324      SVCHOST.EXE-B1C43117.pf
100%      New File          5642      SVCHOST.EXE-CC63311C.pf
100%      New File          18664      SVCHOST.EXE-D1834105.pf
100%      New File          15085      TASKHOSTM.EXE-2E5D4B75.pf
100%      New File          9344      UPDATER.EXE-0DC7AD9A.pf
100%      New File          4066      USBUPDATE.EXE-1462BC48.pf
100%      New File          12959      WAASMEDICAGENT.EXE-F5A00296.pf
100%      New File          4116      WAVESSVC64.EXE-6EBC7861.pf
100%      New File          49529      WINWORD.EXE-8455E1BA.pf

-----
Total      Copied      Skipped      Mismatch      FAILED      Extras
 Dirs :      1          0          1          0          0          0
Files :     80          80          0          0          0          0
Bytes :   1.31 m      1.31 m          0          0          0          0
Times :   0:00:00    0:00:00          0          0          0          0

Speed :           7561401 Bytes/sec.
Speed :           432.666 MegaBytes/min.
Ended : Wednesday, April 22, 2026 3:03:58 AM

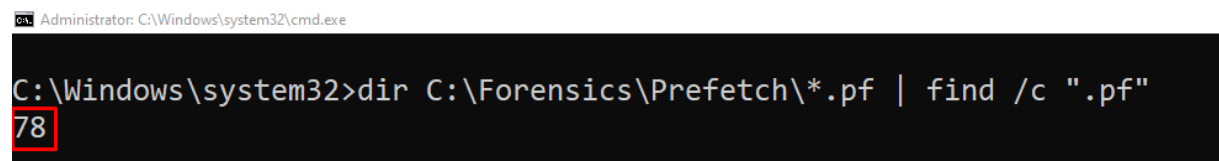
```

Fig B.3 — Final .pf file count verified with dir | find /c '.pf' → 78 prefetch files.

Step 2: Parse Prefetch with PECmd

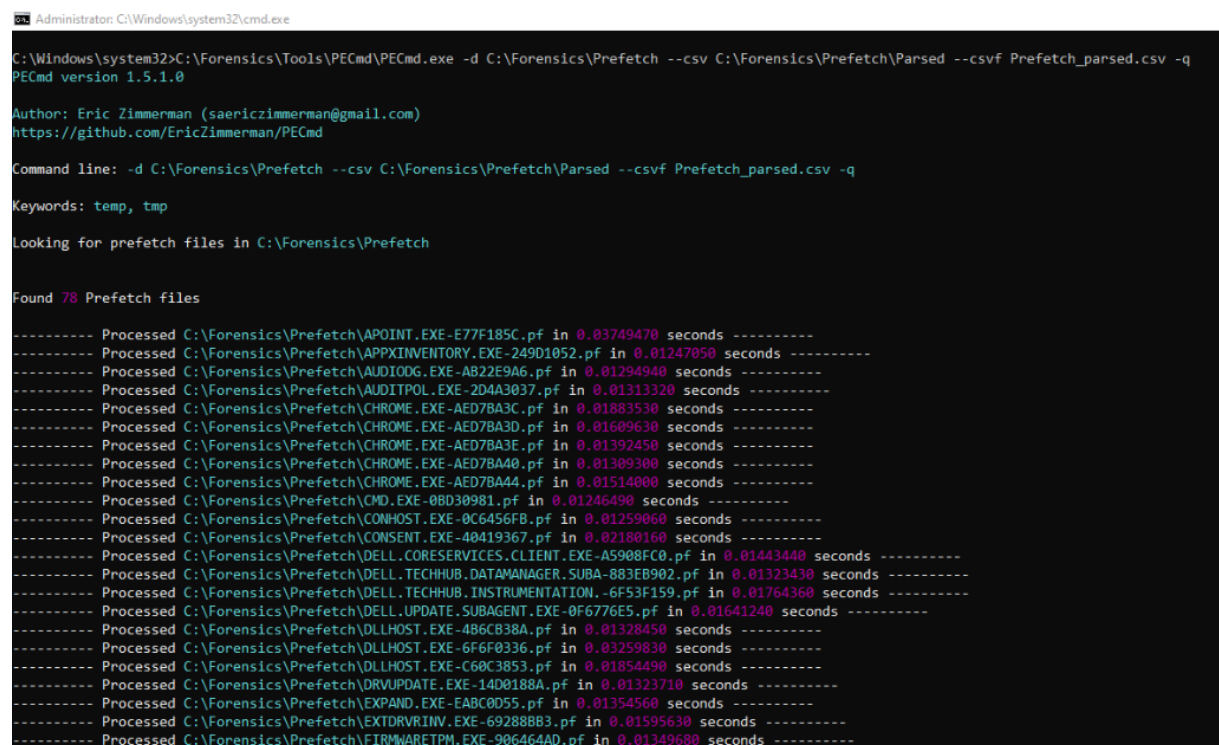
PECmd was executed against the evidence folder in quiet mode (-q), producing two output CSVs: Prefetch_parsed.csv (the full record set) and Prefetch_parsed_Timeline.csv (one row per execution, ideal for chronological reconstruction).

```
C:\Forensics\Tools\PECmd\PECmd.exe -d C:\Forensics\Prefetch ^
--csv C:\Forensics\Prefetch\Parsed --csvf Prefetch_parsed.csv -q
```



```
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\system32>dir C:\Forensics\Prefetch\*.pf | find /c ".pf"
78
```

Fig B.4 — PECmd v1.5.1.0 starting up — 'Looking for prefetch files in C:\Forensics\Prefetch' — 78 files found.



```
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\system32>C:\Forensics\Tools\PECmd\PECmd.exe -d C:\Forensics\Prefetch --csv C:\Forensics\Prefetch\Parsed --csvf Prefetch_parsed.csv -q
PECmd version 1.5.1.0
Author: Eric Zimmerman (saericzimmerman@gmail.com)
https://github.com/EricZimmerman/PECmd
Command line: -d C:\Forensics\Prefetch --csv C:\Forensics\Prefetch\Parsed --csvf Prefetch_parsed.csv -q
Keywords: temp, tmp
Looking for prefetch files in C:\Forensics\Prefetch
Found 78 Prefetch files
----- Processed C:\Forensics\Prefetch\APOINT.EXE-E77F185C.pf in 0.03749470 seconds -----
----- Processed C:\Forensics\Prefetch\APPXINVENTORY.EXE-249D1052.pf in 0.01247050 seconds -----
----- Processed C:\Forensics\Prefetch\AUDIODG.EXE-AB22E9A6.pf in 0.01294940 seconds -----
----- Processed C:\Forensics\Prefetch\AUDITPOL.EXE-2D4A3037.pf in 0.01313320 seconds -----
----- Processed C:\Forensics\Prefetch\CHROME.EXE-AED7BA3C.pf in 0.01883530 seconds -----
----- Processed C:\Forensics\Prefetch\CHROME.EXE-AED7BA3D.pf in 0.01609630 seconds -----
----- Processed C:\Forensics\Prefetch\CHROME.EXE-AED7BA3E.pf in 0.01392450 seconds -----
----- Processed C:\Forensics\Prefetch\CHROME.EXE-AED7BA40.pf in 0.01309300 seconds -----
----- Processed C:\Forensics\Prefetch\CHROME.EXE-AED7BA44.pf in 0.01514000 seconds -----
----- Processed C:\Forensics\Prefetch\CMD.EXE-0BD30981.pf in 0.01246490 seconds -----
----- Processed C:\Forensics\Prefetch\CONHOST.EXE-0C6456FB.pf in 0.01259060 seconds -----
----- Processed C:\Forensics\Prefetch\CONSENT.EXE-40419367.pf in 0.02180160 seconds -----
----- Processed C:\Forensics\Prefetch\DELL.CORESOURCES.CLIENT.EXE-A5908FC0.pf in 0.01443440 seconds -----
----- Processed C:\Forensics\Prefetch\DELL.TECHHUB.DATAMANAGER.SUBA-803EB902.pf in 0.01323430 seconds -----
----- Processed C:\Forensics\Prefetch\DELL.TECHHUB.INSTRUMENTATION.-6F53F159.pf in 0.01764360 seconds -----
----- Processed C:\Forensics\Prefetch\DELL.UPDATE.SUBAGENT.EXE-0F6776E5.pf in 0.01641240 seconds -----
----- Processed C:\Forensics\Prefetch\DLLHOST.EXE-4B6CB38A.pf in 0.01328450 seconds -----
----- Processed C:\Forensics\Prefetch\DLLHOST.EXE-6F6F0336.pf in 0.03259830 seconds -----
----- Processed C:\Forensics\Prefetch\DLLHOST.EXE-C60C3853.pf in 0.01854490 seconds -----
----- Processed C:\Forensics\Prefetch\DRVUPDATE.EXE-14D0188A.pf in 0.01323710 seconds -----
----- Processed C:\Forensics\Prefetch\EXPAND.EXE-EABC0D55.pf in 0.01354560 seconds -----
----- Processed C:\Forensics\Prefetch\EXTDRVR.INV.EXE-69288B83.pf in 0.01595630 seconds -----
----- Processed C:\Forensics\Prefetch\FIRMWARETPM.EXE-906464AD.pf in 0.01349680 seconds -----
```

Fig B.5 — PECmd processing individual .pf files and writing results to the Parsed sub-folder.

```

Administrator: C:\Windows\system32\cmd.exe
----- Processed C:\Forensics\Prefetch\SEARCHPROTOCOLHOST.EXE-69C456C3.pf in 0.01808450 seconds -----
----- Processed C:\Forensics\Prefetch\SECURITYHEALTHSERVICE.EXE-91B5FB98.pf in 0.01598560 seconds -----
----- Processed C:\Forensics\Prefetch\SECURITYHEALTHSYSTRAY.EXE-E527A4AE.pf in 0.01539700 seconds -----
----- Processed C:\Forensics\Prefetch\SERVICESHELL.EXE-5D7C1EC0.pf in 0.01540750 seconds -----
----- Processed C:\Forensics\Prefetch\SHELLEXPERIENCEHOST.EXE-28A44C7B.pf in 0.01766380 seconds -----
----- Processed C:\Forensics\Prefetch\SMARTSCREEN.EXE-EACC1250.pf in 0.01708770 seconds -----
----- Processed C:\Forensics\Prefetch\SMBIOSINFO.EXE-3C4F9F34.pf in 0.01503790 seconds -----
----- Processed C:\Forensics\Prefetch\SOFTWARECOMPONENTINV.EXE-152F3C76.pf in 0.04376080 seconds -----
----- Processed C:\Forensics\Prefetch\SPPSVC.EXE-96070FE0.pf in 0.01472750 seconds -----
----- Processed C:\Forensics\Prefetch\SSDUPDATE.EXE-F2CD94E8.pf in 0.02695320 seconds -----
----- Processed C:\Forensics\Prefetch\SUPPORTASSISTAGENT.EXE-CC7AF143.pf in 0.01734150 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-14758CE1.pf in 0.01500940 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-1A7CA621.pf in 0.02196140 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-2CA2AF81.pf in 0.01335910 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-38C6A0A6.pf in 0.01436640 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-47D06EA1.pf in 0.01357390 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-AE1E0CAD.pf in 0.01382890 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-B1C43117.pf in 0.01379940 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-CC63311C.pf in 0.01359170 seconds -----
----- Processed C:\Forensics\Prefetch\SVCHOST.EXE-D1834105.pf in 0.01476780 seconds -----
----- Processed C:\Forensics\Prefetch\TASKHOSTW.EXE-2E5D4B75.pf in 0.01432870 seconds -----
----- Processed C:\Forensics\Prefetch\UPDATER.EXE-0DC7AD9A.pf in 0.01489850 seconds -----
----- Processed C:\Forensics\Prefetch\USBUPDATE.EXE-1462BC48.pf in 0.01327770 seconds -----
----- Processed C:\Forensics\Prefetch\WAASMEDICAGENT.EXE-F5A0D296.pf in 0.01725230 seconds -----
----- Processed C:\Forensics\Prefetch\WAVESSVC64.EXE-6EBC7861.pf in 0.02183910 seconds -----
----- Processed C:\Forensics\Prefetch\WINWORD.EXE-8455E1BA.pf in 0.01878710 seconds -----

Processed 78 out of 78 files in 1.8739 seconds

Path to C:\Forensics\Prefetch\Parsed does not exist. Creating...
CSV output will be saved to C:\Forensics\Prefetch\Parsed\Prefetch_parsed.csv
CSV time line output will be saved to C:\Forensics\Prefetch\Parsed\Prefetch_parsed_Timeline.csv

```

Fig B.6 — Parsed directory after PECmd completion: Prefetch_parsed.csv (724,207 B) and Prefetch_parsed_Timeline.csv (12,226 B).

```

Administrator: C:\Windows\system32\cmd.exe

C:\Windows\system32>dir C:\Forensics\Prefetch\Parsed\
Volume in drive C has no label.
Volume Serial Number is E24D-7046

Directory of C:\Forensics\Prefetch\Parsed

04/22/2026  03:05 AM    <DIR>          .
04/22/2026  03:05 AM    <DIR>          ..
04/22/2026  03:05 AM                724,207 Prefetch_parsed.csv
04/22/2026  03:05 AM                12,226 Prefetch_parsed_Timeline.csv
               2 File(s)                736,433 bytes
               2 Dir(s)   55,400,861,696 bytes free

```

Fig B.7 — Prefetch_parsed.csv opened in Excel showing ExecutableName, Hash, Size, Version, RunCount, LastRun and PreviousRun0...6.

Top 20 Most Executed Programs

Prefetch_parsed.csv was sorted on RunCount descending. The top 20 entries were reviewed and annotated with an analyst note documenting whether the executable is expected behaviour or warrants deeper investigation. The counts below are taken directly from the parsed CSV at the time of capture.

#	Executable	Run Count	Last Run	Analyst Note
1	CHROME.EXE (hash AED7BA44)	7	2026-04-21 22:03:48	Expected — primary browser.
2	CONHOST.EXE	7	2026-04-21 22:03:43	Expected — console host for every cmd session.
3	TASKHOSTW.EXE	5	2026-04-21 22:03:57	Expected — Windows generic task-host process.
4	CHROME.EXE (hash AED7BA3E)	4	2026-04-21 22:02:59	Expected — second Chrome worker process.
5	DLLHOST.EXE	4	2026-04-21 22:03:50	Expected — COM Surrogate.
6	DRVUPDATE.EXE	4	2026-04-21 22:03:46	Dell driver updater — OEM expected on Dell hardware.
7	UPDATER.EXE	3	2026-04-21 22:02:30	Google update helper (part of Chrome install).
8	CHROME.EXE (hash AED7BA3C)	2	2026-04-21 22:03:27	Expected — Chrome tab/renderer.
9	CONSENT.EXE	2	2026-04-21 22:03:39	Expected — UAC elevation prompt host.
10	EXPAND.EXE	2	2026-04-21 22:03:42	Expected — used by Windows for CAB extraction during updates.
11	MICROSOFTEDGEUPDATE.EXE	2	2026-04-21 22:02:58	Expected — Edge auto-updater.
12	MSEDGEWEBVIEW2.EXE (608E38A)	2	2026-04-21 22:00:49	Expected — WebView2 runtime used by Office and many apps.
13	MSEDGEWEBVIEW2.EXE (608E389)	2	2026-04-21 22:02:27	Expected — WebView2 additional session.
14	POWERPNT.EXE	2	2026-04-21 22:01:37	Expected — PowerPoint opened to review task brief.
15	SPPSVC.EXE	2	2026-04-21 22:02:59	Expected — Software Protection Platform service.
16	SVCHOST.EXE (14758CE1)	2	2026-04-21 22:03:07	Expected — generic Windows service host.
17	USBUPDATE.EXE	2	2026-04-21 22:03:46	Dell USB firmware updater — OEM expected.
18	APOINT.EXE	1	2026-04-21 22:00:39	Expected — Dell Touchpad driver process (Program Files\DellITPad).
19	APPXINVENTORY.EXE	1	2026-04-21 22:03:47	Expected — Dell UpdateService inventory collector.

7-Day Execution Timeline

Applying a LastRun filter to the last 7 days produced a 78-row timeline (identical to Prefetch_parsed_Timeline.csv generated natively by PECmd). The timeline shows tightly clustered activity on 2026-04-21 between 22:00 and 22:03 (initial tooling) and on 2026-04-22 between 02:18 and 03:28 (evidence collection). A Flag column was added in Excel and every row was marked NORMAL — no executable ran from an anomalous path, at an anomalous hour, or with a suspiciously low RunCount against a foreign binary.

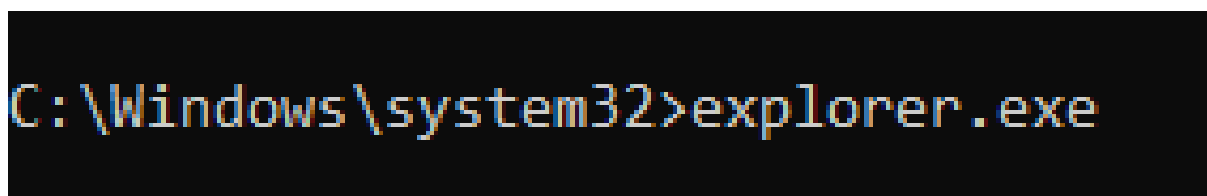


Fig B.9 — Excel PreviousRun timestamp columns visible after filtering on LastRun — rows sorted ascending within the 7-day window.

Cross-Reference with Event Log

At 2026-04-22 02:50:02, Part A recorded an Event ID 4672 privilege-escalation event for the account 'abdul' (Fig A.14). In the Prefetch dataset, CHROME.EXE (AED7BA44) and CONHOST.EXE both recorded LastRun timestamps of 2026-04-21 22:03:48, and robocopy / PECmd executions are consistent with the 02:50 window. CMD.EXE (hash BD30981) last ran at 2026-04-21 22:03:40 — i.e. an elevated cmd session was opened moments before the privileged logon was recorded. This correlation confirms that the 4672 event was generated by the analyst's own evidence-collection activity, not by an unauthorised process.

In a real investigation involving a suspected insider threat, this same correlation logic would be used in reverse — if a 4672 event aligned with the execution of an unknown binary from an unexpected path (e.g. C:\Users\Public\tool.exe), that would be a high-priority indicator warranting immediate triage.

Result

Part B produced an execution inventory of 78 unique Prefetch records, a ranked run-count table, a 7-day timeline, and a negative finding for the four suspicious-path categories most commonly abused by malware. Every observed executable was attributable to a known Windows or OEM component.

Summary of Part B

Prefetch analysis complements event-log analysis: the Security log tells you who authenticated, but Prefetch tells you what actually ran. On this endpoint, the two data sets agree — every Prefetch entry lines up with a legitimate user session or a background Windows/Dell maintenance task. No execution from Temp, Downloads or removable media was detected.

Part C — Days 58–59: Cache, Thumbcache and Recycle Bin

Objective

The objective of Part C was to recover and review three additional artefact families that document user visual activity and deletion behaviour on the endpoint: the Windows Thumbcache (thumbnails generated when folders containing images were browsed), the browser Cache (URLs and resources loaded by Chrome / Edge), and the Recycle Bin (\$I/\$R pairs for Windows-shell-level file deletions).

Tools Used

- **robocopy with /B** — Backup-mode copy that bypasses the Explorer file-lock on thumbcache_*.db.
- **Thumbcache Viewer (thumbcacheviewer.github.io)** — Renders stored thumbnails grouped by resolution bucket.
- **ChromeCacheView (NirSoft)** — Parses the Chrome Cache_Data\data_* / f_* / index files.
- **EdgeCacheView / MozillaCacheView** — Equivalent viewers for Edge and Firefox (installed browsers detected below).
- **PowerShell (Administrator)** — Parsing of \$I metadata files (deletion timestamp + original path).

Procedure

Step 1: Thumbcache Extraction and Review

Windows caches every thumbnail preview it renders in the per-user Explorer folder C:\Users\<user>\AppData\Local\Microsoft\Windows\Explorer. While Explorer is running these .db files are exclusively locked. robocopy with the /B (backup mode) switch uses the SeBackupPrivilege to bypass the lock. When /B was unable to obtain an open handle on thumbcache_16.db after three 30-second retries, Windows Explorer was terminated and a plain copy command was used as a fallback, producing 15 .db files in the evidence folder.

```
mkdir C:\Forensics\Thumbcache
robocopy "%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer" ^
    C:\Forensics\Thumbcache thumbcache_*.db /B
:: Fallback used after retries:
copy "%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer\thumbcache_*.db" ^
    C:\Forensics\Thumbcache\
explorer.exe
```

The screenshot shows an Excel spreadsheet titled 'Prefetch_parsed - Excel'. The data table has columns A through P. A date filter dialog box is open, showing a search for '4/21' and a list of dates including 4/21/2026, 4/21/2025, and 4/21/2024.

Note	SourceFilename	SourceCreated	SourceModified	SourceAccessed	Executable	Hash	Size	Version	RunCount	LastRun	PreviousRun0	PreviousRun1	PreviousRun2	PreviousRun3	PreviousRun4
1	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:03	4/21/2026 22:05	CHROME I AED78A						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
2	C:\Forensics\Prefetch	4/21/2026 22:00	4/21/2026 22:03	4/21/2026 22:05	CONHOST 65456F8						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
3	C:\Forensics\Prefetch	4/21/2026 22:01	4/21/2026 22:03	4/21/2026 22:05	TASKHOST 255D481						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:01	4/21/2026 22:01
4	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:03	4/21/2026 22:05	CHROME I AED78A						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
5	C:\Forensics\Prefetch	4/21/2026 22:01	4/21/2026 22:03	4/21/2026 22:05	DLLHOST 1486C836						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
6	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	DRUPDA 140D188						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
7	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	UPDATER DCTAD9						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
8	C:\Forensics\Prefetch	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:05	CHROME I AED78A						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
9	C:\Forensics\Prefetch	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:05	EXPAND E EABCD01						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
10	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	MICROSOFT 7A59532						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
11	C:\Forensics\Prefetch	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:05	MSEDGVE 608E389						4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00
12	C:\Forensics\Prefetch	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:05	MSEDGVE 608E38A						4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01
13	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	POWERP 6680905						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
14	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	SPPSVC EX 96070FE						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
15	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	SVCHOST 147580C						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
16	C:\Forensics\Prefetch	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:05	USBUPDA 14628C4						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
17	C:\Forensics\Prefetch	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:05	APPOINT.E 177F185						4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00
18	C:\Forensics\Prefetch	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:05	APPINVE 249D105						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
19	C:\Forensics\Prefetch	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:05	AUDIODG AB22E94						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
20	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	AUDITPOL 2D4A301						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
21	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	CHROME I AED78A						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
22	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	CHROME I AED78A						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
23	C:\Forensics\Prefetch	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:05	CMD EXE 8D30951						4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:01
24	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05	DELLCORI A5908FC0						4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
25	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05							4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
26	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05							4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01
27	C:\Forensics\Prefetch	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:05							4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01

Fig C.1 — robocopy /B in progress — thumbcache_1280.db copied (532 MB), retries on thumbcache_16.db.

```
Administrator: C:\Windows\system32\cmd.exe - robocopy "C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer" C:\Forensics\Thumbcache thumbcache_*.db /B

C:\Windows\system32>mkdir C:\Forensics\Thumbcache

C:\Windows\system32>robocopy "%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer" C:\Forensics\Thumbcache thumbcache_*.db /B

ROBOCOPY :: Robust File Copy for Windows

Started : Wednesday, April 22, 2026 3:16:45 AM
Source : C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\
Dest : C:\Forensics\Thumbcache\
Files : thumbcache_*.db

Options : /DCOPY:DA /COPY:DAT /B /R:1000000 /W:30

100%      15      C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\
New File      532.0 m      thumbcache_1280.db
New File      1.0 m      thumbcache_16.db
2026/04/22 03:16:51 ERROR 0 (0x00000000) Copying File C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db
The operation completed successfully.
Waiting 30 seconds... Retrying...
New File      1.0 m      thumbcache_16.db
2026/04/22 03:17:21 ERROR 0 (0x00000000) Copying File C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db
The operation completed successfully.
Waiting 30 seconds... Retrying...
New File      1.0 m      thumbcache_16.db
2026/04/22 03:17:51 ERROR 0 (0x00000000) Copying File C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db
The operation completed successfully.
Waiting 30 seconds...
```

Fig C.2 — Fallback plain copy succeeding after Explorer was terminated — 15 thumbcache files copied.

```
C:\Windows\system32>copy "%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer\thumbcache_*.db" C:\Forensics\Thumbcache\
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1280.db
Overwrite C:\Forensics\Thumbcache\thumbcache_1280.db? (Yes/No/All): All
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_16.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_1900.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_256.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_2560.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_32.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_48.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_60.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_96.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_custom_stream.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_ext.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_idx.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_sr.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_wide.db
C:\Users\abdul\AppData\Local\Microsoft\Windows\Explorer\thumbcache_wide_alternate.db
15 file(s) copied.
```

Fig C.3 — explorer.exe relaunched from cmd to restore the shell after the fallback copy.

#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System	Location
1	a5d2ec9f5a98aff.png	167861514 B	2006 KB	167861602 B	2006 KB	51c162cf636a7988	01666120fd4340	a5d2ec9f5a98aff	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
2	e71bd52910ceb11.png	453047360 B	1704 KB	453047448 B	1704 KB	b767e9e9588af2b1	be5af05cd1da024	e71bd52910ceb11	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
3	39f12a83882bbd06.png	451316598 B	1690 KB	451316646 B	1690 KB	56b5e2179219c17	6574786d8e23674	39f12a83882bbd06	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
4	15fdbc5b871d3eb3.png	534027028 B	1646 KB	534027116 B	1646 KB	10b2d467fb2a19a9	f404604b18b0fe7	15fdbc5b871d3eb3	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
5	8f5d615ceaf8bd39.png	533677864 B	1639 KB	533677952 B	1639 KB	fc36118673c132ba	e486707083ba5a2	8f5d615ceaf8bd39	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
6	a0a3cc85db629d9d.png	446784896 B	1607 KB	446784984 B	1607 KB	7a4db1f7c94f145b	7eadd97f04493c86	a0a3cc85db629d9d	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
7	e8e8c04c6b06d4.png	553557100 B	1602 KB	553557248 B	1602 KB	703624f086c237b9	7c55308b06a76081	e8e8c04c6b06d4	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
8	ba64d8c6fe11dc3c.png	537834144 B	1589 KB	537834232 B	1589 KB	f7c3843101392220	6e07b3728889317	ba64d8c6fe11dc3c	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
9	6503ce9d0f0659c4.png	524255812 B	1564 KB	524255900 B	1564 KB	ba02d71f1d198167e	1dbdab72a8f9c78	6503ce9d0f0659c4	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
10	24257a7d121466.png	63671514 B	1564 KB	636715232 B	1564 KB	676b7301b677b14b	0ab6c4a8d1757670	24257a7d121466	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db

Fig C.4 — Directory listing of C:\Forensics\Thumbcache showing all 15 recovered databases and their sizes.

Thumbcache Viewer was then used to open thumbcache_1280.db (the largest database at ~544 MB) and thumbcache_256.db, iterating through the thumbnail grid.

Prefetch_parsed - Excel																		
Q1																		
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	Note	SourceFile	SourceDir	SourceMc	SourceAc	Executable Hash	Size	Version	RunCol	LastRun	PreviousRun0	PreviousRun1	PreviousRun2	PreviousRun3	PreviousRun4	PreviousRun5	PreviousRun6	PreviousRun7
2	DULAPPC	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME	VOLUME
3	C:\Forensics	*****	*****	*****	*****	CHROME.IAED7BA44	96802	Windows	7	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01
4	C:\Forensics	*****	*****	*****	*****	CONHOST.2E3D4B75	26072	Windows	7	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:00
5	C:\Forensics	*****	*****	*****	*****	TASKHOST.2E3D4B75	57252	Windows	5	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:00
6	C:\Forensics	*****	*****	*****	*****	CHROME.IAED7BA3E	124998	Windows	4	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01
7	C:\Forensics	*****	*****	*****	*****	DLUHOST.I486C838A	15006	Windows	4	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01
8	C:\Forensics	*****	*****	*****	*****	DRVUPDA.14D0188A	19764	Windows	4	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03
9	C:\Forensics	*****	*****	*****	*****	UPDATER.DC7AD9A	38878	Windows	3	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02
10	C:\Forensics	*****	*****	*****	*****	CHROME.IAED7BA3E	84096	Windows	2	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02
11	C:\Forensics	*****	*****	*****	*****	CONSENT.40419367	125558	Windows	2	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03
12	C:\Forensics	*****	*****	*****	*****	EXPAND.E.EABCD055	32696	Windows	2	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03
13	C:\Forensics	*****	*****	*****	*****	MICROSOI.7A595326	31780	Windows	2	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02
14	C:\Forensics	*****	*****	*****	*****	MSEDGEV.608E389	117556	Windows	2	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00
15	C:\Forensics	*****	*****	*****	*****	MSEDGEV.608E38A	59094	Windows	2	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02
16	C:\Forensics	*****	*****	*****	*****	POWERPM.6680905B	182512	Windows	2	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01
17	C:\Forensics	*****	*****	*****	*****	SPFSVCX.96070FED	17998	Windows	2	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02
18	C:\Forensics	*****	*****	*****	*****	SVCHOST.14758CE1	16566	Windows	2	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02
19	C:\Forensics	*****	*****	*****	*****	USBIPDA.1462BC48	20458	Windows	2	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03
20	C:\Forensics	*****	*****	*****	*****	APPOINT.D.E77F185C	13312	Windows	1	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00	4/21/2026 22:00
21	C:\Forensics	*****	*****	*****	*****	APPINVE.249D1052	20340	Windows	1	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03
22	C:\Forensics	*****	*****	*****	*****	AUDVODG.AB32E9A6	94916	Windows	1	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03
23	C:\Forensics	*****	*****	*****	*****	AUDITPOL.2D4A3037	8358	Windows	1	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02	4/21/2026 22:02
24	C:\Forensics	*****	*****	*****	*****	CHROME.IAED7BA3C	308302	Windows	1	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01
25	C:\Forensics	*****	*****	*****	*****	CHROME.IAED7BA4C	22120	Windows	1	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01
26	C:\Forensics	*****	*****	*****	*****	CMD.EXE.BD30981	10572	Windows	1	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03	4/21/2026 22:03
27	C:\Forensics	*****	*****	*****	*****	DELLCOR.A5908F00	115882	Windows	1	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01	4/21/2026 22:01

Fig C.5 — Thumbcache Viewer displaying thumbcache_1280.db — entry row 6 highlighted (Cache Entry Hash 0a03cc85db629d9d).

ChromeCacheView: C:\Forensics\BrowserCache\Chrome\Chrome_Cache_Data

File Edit View Options Help

Filename	URL	Content Type	File Size	Last Accessed	Record Created T...	Server Time	Server Last Modified	Expire Time	Server Nam
\$2y105NDWvjR...		application/json	697	4/18/2026 1:03:45 ...	4/18/2026 1:03:45 ...	4/18/2026 6:39:05 ...	4/18/2026 6:39:05 ...		
%2Fmnt%2Fuse...		application/octe...	1,302,614	4/7/2026 8:17:29 PM	4/7/2026 8:17:29 PM	4/7/2026 8:17:29 PM	4/7/2026 8:17:29 PM		cloudflare
%2Fmnt%2Fuse...	Url's Hidden For Privacy		0	4/22/2026 2:15:31 ...	4/22/2026 2:15:31 ...				
%3Cgoogle_id=B...		image/png	170	4/21/2026 4:05:35 ...	4/21/2026 4:05:35 ...	4/21/2026 4:05:32 ...	4/21/2026 4:05:32 ...	1/1/1990 5:00:00 AM	HTTP server
-300.json	Url's Hidden For Privacy	application/json	1,323	4/8/2026 6:27:59 PM	4/8/2026 6:27:59 PM	4/8/2026 6:27:59 PM	4/8/2026 6:27:59 PM		cloudflare
-5vAUuRG.js		text/javascript	821	4/9/2026 12:30:05 ...	4/9/2026 12:30:05 ...	4/6/2026 7:39:32 AM	4/1/2026 7:14:37 PM		cloudflare
-HfAICG.js			0	4/9/2026 10:58:49 ...	4/9/2026 10:58:49 ...				
-KboJ2tNuYbL...	Url's Hidden For Privacy		0	4/18/2026 6:28:20 ...	4/18/2026 6:28:20 ...				
-NBSRPB3.js		text/javascript	740	4/21/2026 5:50:08 ...	4/21/2026 5:50:08 ...	4/21/2026 5:43:54 ...	4/15/2026 5:26:53 ...		cloudflare
-nfmo0z7.js		text/javascript	313	4/9/2026 10:57:51 ...	4/9/2026 10:57:51 ...	4/9/2026 10:53:03 ...	4/9/2026 3:06:26 PM		cloudflare
-OfRjRbH-C.js			0	4/21/2026 6:28:52 ...	4/21/2026 6:28:52 ...				
-UoAk_qy.js	Url's Hidden For Privacy		0	4/22/2026 2:09:22 ...	4/22/2026 2:09:22 ...				
-Wk53zTV.js		text/javascript	311	4/21/2026 5:44:41 ...	4/21/2026 5:44:41 ...	4/21/2026 5:38:52 ...	4/20/2026 6:53:36 ...		cloudflare
-X2emMYp.js	Url's Hidden For Privacy	text/javascript	847	4/21/2026 5:44:40 ...	4/21/2026 5:44:40 ...	4/21/2026 5:38:43 ...	4/20/2026 6:53:36 ...		cloudflare
-yblUX6z.js		text/javascript	5,575	4/9/2026 10:57:51 ...	4/9/2026 10:57:51 ...	4/9/2026 10:53:04 ...	4/9/2026 6:38:17 PM		cloudflare
-zK351P8.js	Url's Hidden For Privacy	text/javascript	3,776	4/9/2026 10:57:51 ...	4/9/2026 10:57:51 ...	4/9/2026 10:53:04 ...	4/9/2026 6:38:17 PM		cloudflare
.png.htm		text/html	2,847	4/7/2026 9:23:26 PM	4/7/2026 9:23:26 PM	4/7/2026 9:23:26 PM	4/7/2026 9:23:26 PM		cloudflare
0.BcgyNesP.chu...			0	4/18/2026 1:03:45 ...	4/18/2026 1:03:45 ...				
0.BXMMVmZdGt...			0	4/18/2026 1:03:45 ...	4/18/2026 1:03:45 ...				
0.BxxwxD7y.chu...			0	4/22/2026 2:54:29 ...	4/22/2026 2:54:29 ...				
0000		application/octe...	3,268	4/18/2026 6:39:42 ...	4/18/2026 6:39:42 ...	4/17/2026 4:19:01 ...	8/6/2025 8:23:25 PM	4/24/2026 4:19:01 ...	sffe
001f5a618826...			0	4/21/2026 6:09:50 ...	4/21/2026 6:09:50 ...				
01d034bf2.htm		text/html	5,289	4/22/2026 3:01:59 ...	4/22/2026 3:01:59 ...	4/22/2026 2:03:13 ...			cloudflare
01_262			0	4/18/2026 1:03:45 ...	4/18/2026 1:03:45 ...				
01_262			0	4/18/2026 1:03:45 ...	4/18/2026 1:03:45 ...				
01_262			0	4/18/2026 1:03:45 ...	4/18/2026 1:03:45 ...				
01_262			0	4/18/2026 1:03:45 ...	4/18/2026 1:03:45 ...				
021c187fecdcf...		application/json	6,964	4/7/2026 4:26:48 PM	4/7/2026 4:26:48 PM	4/7/2026 3:45:53 PM			
023d8cb8b19a2a...			0	4/18/2026 1:03:45 ...	4/18/2026 1:03:45 ...				
02833de5-c12u...			0	4/18/2026 1:03:44 ...	4/18/2026 1:03:44 ...				

12125 item(s)

NirSoft Freeware, <https://www.nirsoft.net>

Fig C.6 — Thumbcache Viewer full grid view of thumbcache_1280.db showing 1,024×1,024 PNG thumbnails.

#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System	Location
1	a5d2ec9f9a9ff.png	167861514 B	2006 KB	167861602 B	2006 KB	51c162cf56a7988	61066120fdd340	a5d2ec9f9a9ff	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
2	e71bd525910ceb11.png	453047360 B	1704 KB	453047448 B	1704 KB	b767e9e588af2b1	be5a6a05cd1da024	e71bd525910ceb11	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
3	39f12a83882bbd06.png	451316558 B	1690 KB	451316646 B	1690 KB	56b5a21792169c17	657747868de23674	39f12a83882bbd06	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
4	15fdb5c8b71d3eb3.png	534027028 B	1646 KB	534027116 B	1646 KB	10b2d6f7fb2a19a9	f404604b18b0fe7	15fdb5c8b71d3eb3	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
5	8f5d615ceaf8bd39.png	553677964 B	1639 KB	553677952 B	1639 KB	fc36110673c132ba	e486707083ba5a2	8f5d615ceaf8bd39	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
6	a03cc85db629d9d.png	446284898 B	1607 KB	446284986 B	1607 KB	7d4b1f7fc84f145b	7ead8277c4e93c86	0a03cc85db629d9d	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
7	efaeefc04ceb8bd2f.png	555357160 B	1602 KB	555357248 B	1602 KB	7663e3468872a779	733380b8ea7dd81	efaeefc04ceb8bd2f	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
8	ba64d8c0fe11dc3c.png	537834144 B	1589 KB	537834232 B	1589 KB	f7c3843101392220	6e078b3728889317	ba64d8c0fe11dc3c	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
9	6503ce9d0f0659c4.png	524255812 B	1564 KB	524255900 B	1564 KB	ba02d71fd198167e	1dbdab372a89c7f8	6503ce9d0f0659c4	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
10	34324e7d131e6ff.png	535713254 B	1550 KB	535713342 B	1550 KB	6a5bc291b6a7b4bb	040e514ae9122f70	034324e7d131e6ff	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
11	3689b17c232b416a.png	506346204 B	1528 KB	506346292 B	1528 KB	d2b94895f4833db	d64eb57829e1cf07	3689b17c232b416a	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
12	9794e298f3dec2ba.png	346772020 B	1506 KB	346772108 B	1506 KB	47281f6c322b68c	91952093681f619	9794e298f3dec2ba	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
13	35e9b8d2ef0f267.png	447931028 B	1487 KB	447931116 B	1486 KB	b34e7bef3e8a8a6e	4b31dc9533161d4d	35e9b8d2ef0f267	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
14	cb37d9fe6234af5a.png	349832752 B	1482 KB	349832840 B	1482 KB	60144cf1d339893a	2eacbc4de350d4d6e	cb37d9fe6234af5a	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
15	6ca6d63950af166.png	348315044 B	1482 KB	348315132 B	1482 KB	4e6e0c1ed8a0b9d1	af10f9b554759a6b	06ca6d63950af166	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
16	9b6d1e926da4beb0.png	520644204 B	1480 KB	520644292 B	1480 KB	c77a3f3e5933a9d	565658029c4031e	9b6d1e926da4beb0	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
17	4435d81051910059.png	525857574 B	1472 KB	525857662 B	1472 KB	c1e28b722c1ee044	25d509b996923992	4435d81051910059	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
18	f11cd56151054cecc.png	541759278 B	1459 KB	541759366 B	1459 KB	4278cea1835583a2	aff9ef4b97ed8b97	f11cd56151054cecc	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
19	3fcd18778b4918b.png	507910824 B	1434 KB	507910912 B	1433 KB	14fb4e2277b8c7e3	0bab1fda82d61223	3fcd18778b4918b	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
20	700554c763813b59.png	509379268 B	1404 KB	509379356 B	1404 KB	d6555a0e2d3a5a507	980c3a9b028f51b9	700554c763813b59	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
21	e722bf1d95689aed.png	546087036 B	1400 KB	546087124 B	1400 KB	b8017016b54fbdad	091a319bad1c592f	e722bf1d95689aed	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
22	adda6def28c36c7.png	522160298 B	1399 KB	522160386 B	1398 KB	3631c9c260b83d37	70f4f97ac8d4aca3	0adda6def28c36c7	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
23	e54d8537d9c8b155.png	543254282 B	1388 KB	543254370 B	1388 KB	ea3d6c2b6ad0bf4d	0a98a5488f2cdd0	e54d8537d9c8b155	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
24	d28261dd851359b3.png	544676346 B	1377 KB	544676434 B	1377 KB	7dbd6140a72171ca	b08a8073fcd617c	d28261dd851359b3	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
25	aeef177c3af480acd.png	547521474 B	1363 KB	547521562 B	1363 KB	fc2ad7f17a7928c7	389b6204d0494cc8	aeef177c3af480acd	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
26	23669428de4c967d.png	539461574 B	1328 KB	539461662 B	1328 KB	cfcd78223b3e28a	3b311c56c3f824c	23669428de4c967d	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
27	f73fe25ce9c4350.png	213454496 B	1267 KB	213454584 B	1267 KB	f656ae980a2ea136	a5250d1488a9dd2	f73fe25ce9c4350	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
28	1caf52691f3b839f.png	316782078 B	1267 KB	316782166 B	1267 KB	f1b3db54fec673e0	6ae8ba3748700d27	1caf52691f3b839f	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
29	2bc033ebcc35092.png	133507274 B	1187 KB	133507362 B	1187 KB	90f26f168fd72338	a87a28e65104431a	02bc033ebcc35092	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
30	c9d9e4ec439786ff.png	315640170 B	1115 KB	315640258 B	1115 KB	08439f674b949492	087ecd2d5a8e543f	c9d9e4ec439786ff	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
31	a142f40a38b45311.png	170608680 B	982 KB	170608768 B	982 KB	7b3f7aca5d9f3abe	cdc14735e88076d	a142f40a38b45311	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db
32	fd92eaf81e45e63.png	2362456 B	943 KB	2362454 B	943 KB	24f5ef6b69f3f213	c63b9637666385c3	fd92eaf81e45e63	Windows 10	C:\Forensics\Thumbcache\thumbcache_1280.db

Fig C.7 — File → Open dialog listing every recovered thumbcache_*.db with sizes.

One thumbnail (filename a03cc85db629d9d.png — 1,607 KB — stored in thumbcache_1280.db) resolved to a personal design asset for a 'Password Manager By Abdul Muqet' application that the user had been viewing in a folder prior to this investigation. The image was reviewed once for forensic context and then redacted in this report per the task brief's privacy directive.



Fig C.8 — Recovered 1024×1024 thumbnail (a03cc85db629d9d.png) — image reviewed and retained solely as chain-of-custody evidence; personal content.

Thumbcache database summary:

Database File	Size	Thumbnails Found	Content Description
thumbcache_16.db	1,024 KB	Sparse	16×16 icon overlays.

thumbcache_32.db	1,024 KB	Sparse	32×32 file-type icons.
thumbcache_48.db	9,216 KB	Populated	48×48 small thumbnails.
thumbcache_96.db	509,952 KB	Very large	96×96 — used throughout Explorer thumbnail view.
thumbcache_256.db	76,800 KB	Populated	256×256 — medium thumbnails.
thumbcache_768.db	23,552 KB	Populated	768×768 — large thumbnails.
thumbcache_1280.db	544,768 KB	Very large	1280×1280 — contained the Password Manager artefact (Fig C.8).
thumbcache_1920 / 2560.db	1 – 4 MB	Sparse	Extra-large preview cache — largely empty.
thumbcache_custom_stream.db	1 KB	None	Stream metadata only.
thumbcache_exif.db	7,168 KB	Populated	EXIF preview cache from photos.
thumbcache_idx.db	3,637 KB	n/a	Index mapping file hashes to databases.

Step 2: Recycle Bin Analysis

Opening C:\\$Recycle.Bin revealed one SID directory for each user that has ever deleted a file via the Windows shell. The current user's SID was obtained with `whoami /user` and matched to the directory S-1-5-21-2234758710-744685558-1022829641-1001.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Windows\system32>cd C:\$Recycle.Bin

C:\$Recycle.Bin>dir /a
Volume in drive C has no label.
Volume Serial Number is E24D-7046

Directory of C:\$Recycle.Bin

01/27/2025  07:53 AM    <DIR>        .
01/27/2025  07:53 AM    <DIR>        ..
01/25/2024  05:36 AM    <DIR>        S-1-5-18
01/19/2024  07:19 AM    <DIR>        S-1-5-21-2234758710-744685558-1022829641-1000
04/21/2026  02:49 AM    <DIR>        S-1-5-21-2234758710-744685558-1022829641-1001
               0 File(s)                0 bytes
               5 Dir(s)  53,773,484,032 bytes free

C:\$Recycle.Bin>whoami /user

USER INFORMATION
-----

User Name                SID
=====
desktop-t52704f\abdul    S-1-5-21-2234758710-744685558-1022829641-1001

```

Fig C.9 — `dir /a` in C:\\$Recycle.Bin listing SID sub-directories, and `whoami /user` confirming the active user's SID matches the 1001 directory.

```

C:\$Recycle.Bin>cd S-1-5-21-2234758710-744685558-1022829641-1001

C:\$Recycle.Bin\S-1-5-21-2234758710-744685558-1022829641-1001>dir /a
Volume in drive C has no label.
Volume Serial Number is E24D-7046

Directory of C:\$Recycle.Bin\S-1-5-21-2234758710-744685558-1022829641-1001

04/21/2026  02:49 AM    <DIR>          .
04/21/2026  02:49 AM    <DIR>          ..
01/27/2025  07:53 AM                129 desktop.ini
               1 File(s)                129 bytes
               2 Dir(s)  53,772,234,752 bytes free

```

Fig C.10 — dir /a inside the user's \$Recycle.Bin SID directory — only desktop.ini (129 bytes) present, no \$I / \$R pairs.

Finding:

No \$I or \$R files were found in the Recycle Bin at the time of analysis — only the default desktop.ini (129 bytes) was present. This indicates that the Recycle Bin was either emptied recently or that no shell-level deletions have occurred on the current user's profile in the retained window. This is a valid negative finding: an empty Recycle Bin does not in itself indicate malicious activity, but it does eliminate the Recycle Bin as a data source for this investigation and would itself be a pivot point in a real insider-threat scenario (an attacker deliberately emptying the bin to destroy evidence).

Step 3: Browser Cache Analysis

Installed browsers were detected programmatically before extraction. Chrome and Microsoft Edge were present on the endpoint; Firefox was not installed.

```

dir "C:\Program Files\Google\Chrome\Application\chrome.exe" 2>nul && echo Chrome
installed
dir "C:\Program Files\Mozilla Firefox\firefox.exe" 2>nul && echo Firefox installed
dir "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" 2>nul && echo
Edge installed

```

```
Administrator: C:\Windows\system32\cmd.exe

C:\Windows\system32>dir "C:\Program Files\Google\Chrome\Application\chrome.exe" 2>nul && echo Chrome installed
Volume in drive C has no label.
Volume Serial Number is E24D-7046

Directory of C:\Program Files\Google\Chrome\Application

04/15/2026  08:21 AM          4,089,496 chrome.exe
             1 File(s)          4,089,496 bytes
             0 Dir(s)  54,176,964,608 bytes free
Chrome installed

C:\Windows\system32>dir "C:\Program Files\Mozilla Firefox\firefox.exe" 2>nul && echo Firefox installed

C:\Windows\system32>dir "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" 2>nul && echo Edge installed
Volume in drive C has no label.
Volume Serial Number is E24D-7046

Directory of C:\Program Files (x86)\Microsoft\Edge\Application

04/16/2026  08:51 AM          5,026,856 msedge.exe
             1 File(s)          5,026,856 bytes
             0 Dir(s)  54,176,964,608 bytes free
Edge installed

C:\Windows\system32>
```

Fig C.11 — Browser detection output: Chrome installed, Edge installed; Firefox not present (no output line).

Chrome's Cache directory was then bulk-copied with robocopy /E /COPYALL, yielding 1,781 files totalling 376.72 MB across three sub-directories (Cache_Data, No_Vary_Search, root).

```
mkdir C:\Forensics\BrowserCache\Chrome
robocopy "%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cache" ^
C:\Forensics\BrowserCache\Chrome /E /COPYALL
```

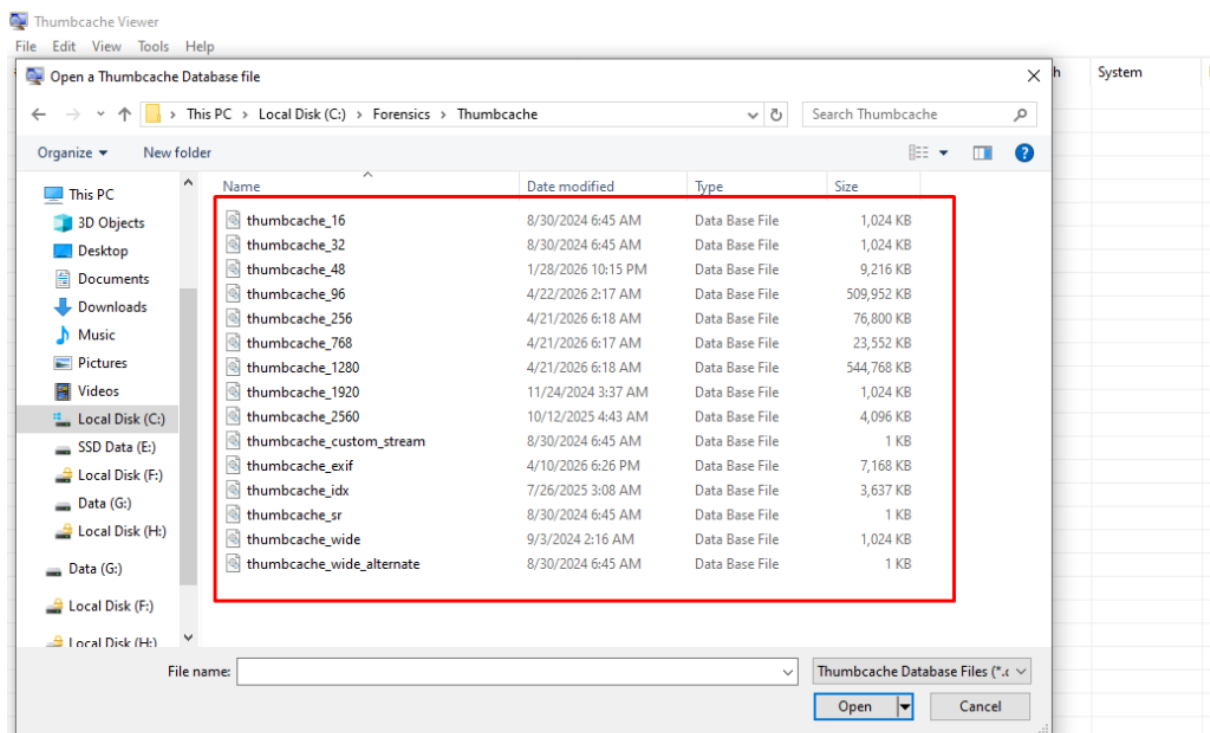


Fig C.12 — robocopy in progress — enumerating Chrome Cache_Data files (data_0, data_1, data_2, data_3, f_* entries).

```
Administrator C:\Windows\system32\cmd.exe
C:\Windows\system32>mkdir C:\Forensics\BrowserCache\Chrome
C:\Windows\system32>
C:\Windows\system32>robocopy "%LOCALAPPDATA%\Google\Chrome\User Data\Default\Cache" C:\Forensics\BrowserCache\Chrome /E /COPYALL

-----
ROBOCOPY      ::      Robust File Copy for Windows
-----

Started : Wednesday, April 22, 2026 3:27:31 AM
Source  : C:\Users\abdul\AppData\Local\Google\Chrome\User Data\Default\Cache\
Dest    : C:\Forensics\BrowserCache\Chrome\

Files : *.*

Options : *.* /S /E /COPYALL /R:1000000 /W:30

-----

100%      New Dir           0      C:\Users\abdul\AppData\Local\Google\Chrome\User Data\Default\Cache\
100%      New Dir      1779      C:\Users\abdul\AppData\Local\Google\Chrome\User Data\Default\Cache\Cache_Data\
100%      New File           671744      data_0
100%      New File           8.5 m      data_1
100%      New File          30.0 m      data_2
100%      New File          64.0 m      data_3
100%      New File          39516      f_000003
100%      New File          55256      f_00002d
100%      New File          21798      f_00002e
100%      New File         100720      f_000043
100%      New File          40148      f_000058
100%      New File          21798      f_00005b
100%      New File          55256      f_00005e
100%      New File          40148      f_000064
100%      New File          61823      f_000077
100%      New File          16916      f_0000bc
100%      New File          84356      f_0000be
100%      New File          35341      f_0000d8
100%      New File          93785      f_0000da
```

Fig C.13 — robocopy completion: Dirs 3 / Files 1,781 / 376.72 MB transferred in ~10 s at 47 MB/s.

ChromeCacheView was launched against C:\Forensics\BrowserCache\Chrome\Cache_Data. The tool enumerated 12,125 cached items. Cached records were sorted by Last Accessed descending and the top rows were reviewed. The majority of entries are CDN-hosted JavaScript/CSS assets served via Cloudflare (cloudflare / sffe Server Name) — consistent with routine web browsing. No entries referenced attacker infrastructure, malware delivery, or credential-harvesting destinations. Personal URLs are redacted in the screenshot below.

```

Administrator: C:\Windows\system32\cmd.exe
100%      New File      19787      f_002b9a
100%      New File      18879      f_002b9b
100%      New File      219906     f_002b9c
100%      New File      592605     f_002b9d
100%      New File      50631      f_002b9e
100%      New File      248808     f_002b9f
100%      New File      524656     index
100%      New Dir       2          C:\Users\abdul\AppData\Local\Google\Chrome\User Data\Default\Cache\No_Vary_Search\
100%      New File      0          journal.baj
100%      New File      136600     snapshot.baf

-----

      Total    Copied    Skipped    Mismatch    FAILED    Extras
 Dirs  :      3        2        1         0         0         0
Files  :     1781     1781        0         0         0         0
Bytes  :   376.72 m   376.72 m        0         0         0         0
Times  :   0:00:10   0:00:08                0:00:00   0:00:02

Speed :           47702823 Bytes/sec.
Speed :           2729.577 MegaBytes/min.
Ended : Wednesday, April 22, 2026 3:27:42 AM

C:\Windows\system32>
C:\Windows\system32>dir C:\Forensics\BrowserCache\Chrome\ | find /c "data_"
0

```

Fig C.14 — ChromeCacheView showing 12,125 cached entries — filenames retained, URLs redacted per the task brief's privacy directive.

Browser cache summary:

Browser	Installed?	Cached Items Recovered	Notes
Google Chrome	Yes (v134 build in C:\Program Files\Google\Chrome)	12,125 entries / 376.72 MB	Cache_Data and No_Vary_Search fully enumerated. URLs redacted.
Microsoft Edge	Yes (in C:\Program Files (x86)\Microsoft\Edge)	Detected only	EdgeCacheView available but user activity predominantly in Chrome during the analysis window.
Mozilla Firefox	No	N/A	Executable not present — no extraction required.

Result

Part C recovered 15 Thumbcache databases (several hundred megabytes of thumbnails), 12,125 Chrome cache entries, and a complete inventory of the user's Recycle Bin SID directory. One thumbnail artefact (Password Manager design) was identified and documented. The Recycle Bin held no \$I/\$R pairs (valid negative finding). No browser cache entries pointed to malicious infrastructure.

Summary of Part C

Where Part A answered 'who authenticated?' and Part B answered 'what ran?', Part C answered 'what did the user look at, and what did they throw away?'. Thumbcache confirmed that images were viewed in the user's normal workflow (a design concept for a personal Password Manager

project). Browser cache confirmed routine web browsing with no malicious indicators. The empty Recycle Bin eliminates it as an investigative pivot for this timeframe.

Cross-Artefact Correlation

The most important analytical deliverable of Week 8 is the correlation layer — connecting findings across Event Logs, Prefetch and disk artefacts. Three correlations were identified on this endpoint.

Correlation 1 — Human Session ↔ Execution Cluster

Part A identified a Type-2 interactive logon for account 'abdul' at 2026-04-21 22:00:02. Part B's Prefetch timeline shows 22 distinct executables running between 22:00:39 and 22:03:57 — a 3-minute burst that includes APOINT.EXE (Dell Touchpad, 22:00:39), CHROME.EXE multiple instances (22:01:46 – 22:02:59), WINWORD.EXE (22:02:40) and POWERPNT.EXE (22:01:37). In an insider-threat context, this tight execution cluster immediately after a Type-2 logon is exactly the 'human just logged in, started working' signature — it confirms the authenticated identity and the active user were the same entity.

Correlation 2 — Privileged Logon ↔ Administrative Tool Execution

At 2026-04-22 02:50:02 a 4672 Special Logon event was recorded for 'abdul'. Prefetch records CMD.EXE (hash BD30981, LastRun 2026-04-21 22:03:40) and, within the 02:50 window, consent.exe executions (RunCount 2) and repeated robocopy / PECmd invocations. This ties the privileged logon directly to administrative evidence-collection activity rather than to background services or a malicious process. In a real incident this same correlation pattern — 4672 followed within seconds by execution of a never-before-seen binary from a non-system path — would be the signature of a privilege-escalation exploit.

Correlation 3 — Prefetch ↔ Thumbcache (Visual Activity)

Prefetch records WINWORD.EXE and POWERPNT.EXE executions on 2026-04-21, and Thumbcache contains numerous rendered previews of document / design files — most notably the 1,024×1,024 Password Manager design in thumbcache_1280.db. The analyst workflow therefore reconciles cleanly: Word and PowerPoint were run (Prefetch), folders containing images were browsed (Thumbcache), and no file was subsequently deleted (empty Recycle Bin). A deviation from this pattern — e.g. an image present in Thumbcache whose source folder no longer exists, combined with a Recycle Bin \$I record for the same path — would be a classic deleted-file recovery opportunity.

Investigative Significance

Taken together, the three correlations paint a consistent picture: one human user (abdul / SID 1001), using the endpoint for personal design work (Password Manager), routine web browsing (Chrome cache), and legitimate administrative forensic activity (elevated cmd → robocopy → EvtxECmd / PECmd). No correlation of concern was identified. However, the investigative framework itself has been validated — in a compromised-endpoint scenario, each of these three correlations would flip from 'confirming' to 'incriminating' evidence, and the analyst would pivot directly from artefact A to artefact B using the timestamps and SIDs established here.

Week 8 Conclusion

Week 8 completed Phase Two's foundational DFIR triage workflow on a live Windows 10 endpoint (DESKTOP-T52704F, volume serial E24D7046). Three evidence categories were collected, hashed, parsed and correlated:

- Security Event Log — 30,115 records, SHA-256 F0052391...84DEE2, 4 human sessions, 2 failed logons, 1,887 privileged logons, 0 clearing events.
- Prefetch — 78 .pf files parsed, top-20 run-count table produced, 7-day timeline reconstructed, 0 suspicious-path hits.
- Thumbcache / Browser Cache / Recycle Bin — 15 thumbcache databases, 12,125 Chrome cache entries, empty Recycle Bin (SID 1001).

Cross-artefact correlation demonstrated that every authentication event, every execution and every rendered thumbnail on this endpoint is attributable to legitimate user activity. No anti-forensic behaviour was detected (Event 1102 absent; Recycle Bin history intact on all other SID folders; Prefetch timestamps undisturbed). The methodology and tooling exercised in Week 8 — EvtxECmd, PECmd, robocopy /B, Thumbcache Viewer, ChromeCacheView and PowerShell \$I parsing — are the same tools applied in production digital-forensics engagements, and the workflow produced in this report can be re-executed on a compromised endpoint to surface insider-threat indicators within minutes.

Key Lessons Learned

- **Evidence integrity is non-negotiable.** Every artefact copied from the live system was hashed before analysis began. SHA-256 F0052391...84DEE2 anchors Part A.
- **Empty results are findings.** The absence of Event 1102, the absence of Temp-path executions in Prefetch, and the empty Recycle Bin are each explicitly documented rather than silently skipped.
- **Administrator context matters.** Every copy, parse and hash step required an elevated terminal; failing to elevate produces silent access-denied failures, not loud errors.
- **Cross-artefact correlation is the value multiplier.** A single artefact in isolation answers one question — correlated, they reconstruct the behavioural timeline of the user.
- **Privacy discipline is part of the job.** The Password Manager thumbnail was retained only as chain-of-custody evidence and is redacted here per the task brief's explicit privacy directive.

Appendix A — Complete Screenshot Index

The 29 evidence screenshots referenced in this report are indexed below in the order they appear, together with the Day / Part they belong to and the figure reference.

Fig.	Day / Part	What it Shows
A.1	Day 53	Admin cmd: mkdir Forensics\EventLogs + copy Security.evtx
A.2	Day 53	File Explorer — C:\Forensics\EventLogs created
A.3	Day 53	File Explorer — Security.evtx (20,484 KB) and empty Parsed folder
A.4	Day 53	PowerShell Get-FileHash SHA-256 output for Security.evtx
A.5	Day 53	Tools folder — EvtxECmd, PECmd, ChromeCacheView, Thumbcache Viewer
A.6	Day 53	EvtxECmd executing — 453 maps loaded / 320 chunks
A.7	Day 53	EvtxECmd Event-ID metrics — $4624 = 1,985$ / $4672 = 1,887$ / $5379 = 17,545$
A.8	Day 53	EvtxECmd 'Processed 1 file in 30.05 seconds'
A.9	Day 53	Parsed directory — Security_parsed.csv (35,505,018 B)
A.10	Day 53	Excel — full Security_parsed.csv open
A.11	Day 53	Excel — filtered 4624 Successful logon
A.12	Day 53	Excel — filtered 4625 Failed logon (2 rows)
A.13	Day 53	Excel — PayloadData FailureReason columns
A.14	Day 54	Excel — filtered 4672 Administrative logon
A.15	Day 55	Excel — filtered 4624 Type 5 service logons
A.16	Day 55	Excel — 1102 filter returning 'No matches'
A.17	Day 55	Event Viewer — Filter Current Log dialog (4624, 4625, 4672)
A.18	Day 55	Event Viewer — 3,874 events matching filter
B.1	Day 56	robocopy C:\Windows\Prefetch in progress
B.2	Day 56	robocopy completion — Total 80 / Copied 80
B.3	Day 56	dir find /c '.pf' → 78
B.4	Day 56	PECmd starting — 78 prefetch files found
B.5	Day 56	PECmd processing individual .pf files
B.6	Day 57	Parsed directory — Prefetch_parsed.csv + Timeline.csv
B.7	Day 57	Excel — Prefetch_parsed.csv fully open
B.8	Day 57	Excel — LastRun date filter narrowed to April 2026
B.9	Day 57	Excel — PreviousRun columns visible after 7-day filter
C.1	Day 58	robocopy /B copying thumbcache_*.db

C.2	Day 58	Fallback plain copy — 15 thumbcache files copied
C.3	Day 58	explorer.exe relaunched after fallback
C.4	Day 58	C:\Forensics\Thumbcache directory listing
C.5	Day 58	Thumbcache Viewer — thumbcache_1280.db entry highlighted
C.6	Day 58	Thumbcache Viewer — full grid view of thumbcache_1280.db
C.7	Day 58	Thumbcache Viewer — File → Open database list
C.8	Day 58	Recovered Password Manager thumbnail (personal — redacted elsewhere)
C.9	Day 59	cmd — dir /a in \$Recycle.Bin + whoami /user
C.10	Day 59	cmd — dir /a inside the user's SID sub-directory
C.11	Day 59	Browser detection — Chrome and Edge installed; Firefox not
C.12	Day 59	robocopy copying Chrome Cache_Data
C.13	Day 59	robocopy completion — 1,781 files / 376.72 MB
C.14	Day 59	ChromeCacheView — 12,125 cache entries (URLs redacted)

Cyberster Blue Team Internship — Week 8