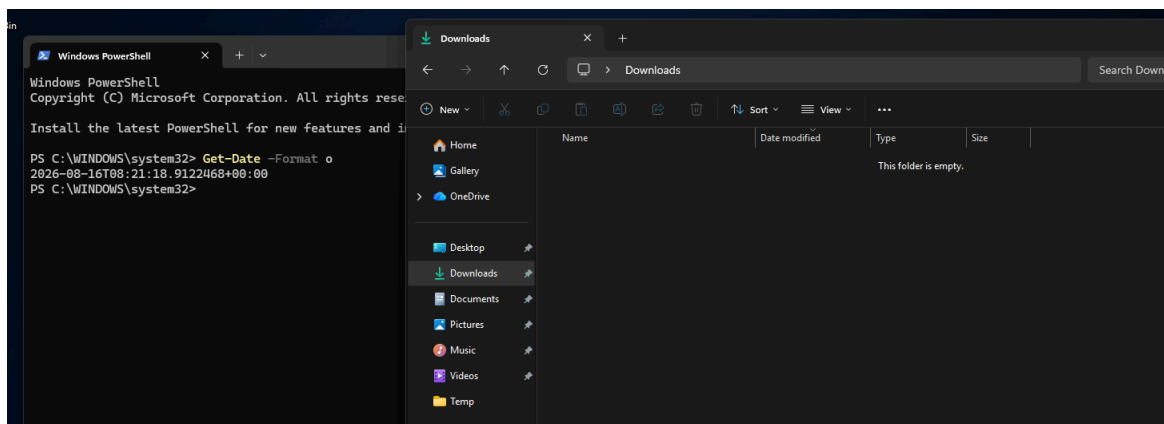
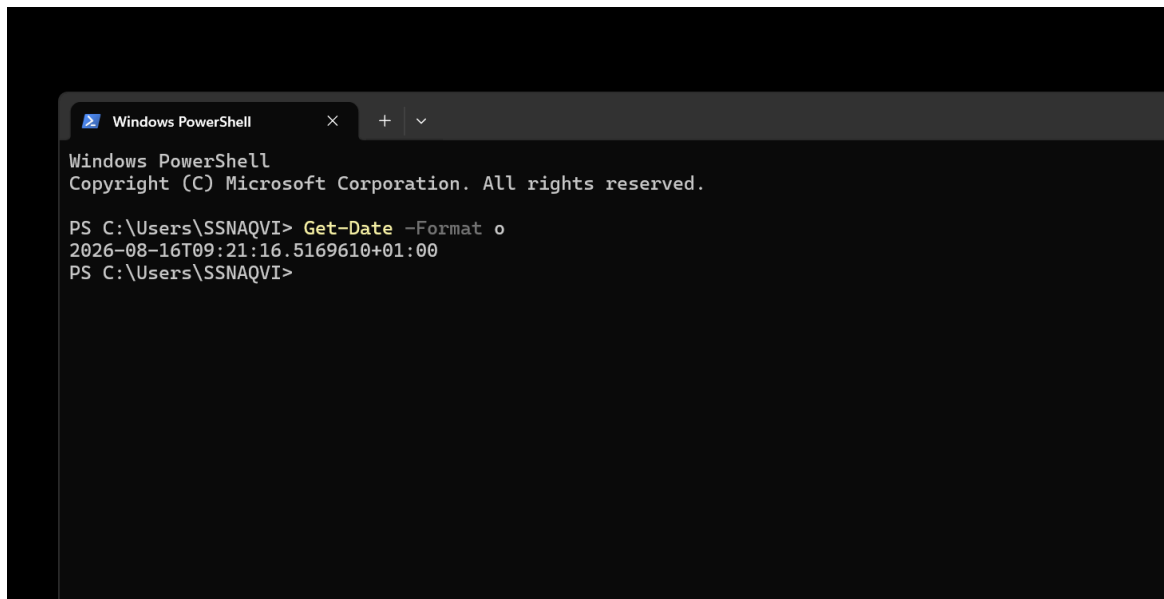




PRACTICAL

Last edited by	 Saqlain Naqvi
Status	Not started

▼ PRE SCN



```
$script:log = @()
```

```

function Log-Action {
    param([Parameter(Mandatory)][string]$id, [Parameter
(Mandatory)][string]$phase, [string]$note = '')
    $ts = Get-Date -Format o
    $script:log += [PSCustomObject]@{Action=$id; Phase=
$phase; UTC=$ts; Note=$note}
    Write-Host "$id $phase $ts $note"
}

function Save-Log {
    param([Parameter(Mandatory)][string]$Scenario, [Para
meter(Mandatory)][string]$Run, [string]$Path = 'C:\DISS_
TESTDATA')
    if (-not (Test-Path $Path)) { New-Item -ItemType Dir
ectory -Path $Path -Force | Out-Null }
    $file = Join-Path $Path "$Scenario-$Run-action-log.c
sv"
    $script:log | Export-Csv -Path $file -NoTypeInformat
ion
    Write-Host "Wrote $($script:log.Count) rows to $fil
e"
}

function Show-Log { $script:log | Format-Table -AutoSize
}

```

▼ SCN 1

```

PS C:\WINDOWS\system32> Log-Action A01 start "Open Edge"
A01 start 2026-08-16T08:58:59.4033339+00:00 Open Edge
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-16T08:59:41.3408270+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Download C
hrome"
A02 start 2026-08-16T09:00:13.7821730+00:00 Download Chr
ome
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-16T09:00:50.7262753+00:00

```

```
PS C:\WINDOWS\system32> Log-Action A03 start "Download WinRAR"
A03 start 2026-08-16T09:01:04.9746597+00:00 Download WinRAR
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-16T09:01:40.7449125+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Download VLC"
A04 start 2026-08-16T09:01:54.1119760+00:00 Download VLC
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-16T09:02:53.4331131+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Download Adobe Reader"
A05 start 2026-08-16T09:03:16.4195277+00:00 Download Adobe Reader
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-16T09:03:40.9418651+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Download Zoom"
A06 start 2026-08-16T09:03:59.5274415+00:00 Download Zoom
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-16T09:05:04.7044270+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Download Notepad++"
A07 start 2026-08-16T09:05:30.3951715+00:00 Download Notepad++
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-16T09:06:06.1802774+00:00
PS C:\WINDOWS\system32> Log-Action A08 start "Download Chrome Edge"
A08 start 2026-08-16T09:06:40.1540236+00:00 Download Chrome Edge
PS C:\WINDOWS\system32> Log-Action A08 end
A08 end 2026-08-16T09:06:51.5894190+00:00
PS C:\WINDOWS\system32> Log-Action A09 start "Open Downloads"
A09 start 2026-08-16T09:07:18.2189427+00:00 Open Downloads
```

```
ds
PS C:\WINDOWS\system32> Log-Action A09 end
A09 end 2026-08-16T09:07:34.3116590+00:00
PS C:\WINDOWS\system32> Log-Action A10 start "Install Chrome"
A10 start 2026-08-16T09:07:54.3956577+00:00 Install Chrome
PS C:\WINDOWS\system32> Log-Action A10 end
A10 end 2026-08-16T09:09:20.1974816+00:00
PS C:\WINDOWS\system32> Log-Action A11 start "Install WinRAR"
A11 start 2026-08-16T09:09:44.3129259+00:00 Install WinRAR
PS C:\WINDOWS\system32> Log-Action A11 end
A11 end 2026-08-16T09:10:03.7232064+00:00
PS C:\WINDOWS\system32> Log-Action A12 start "Install VLC"
A12 start 2026-08-16T09:10:25.3472610+00:00 Install VLC
PS C:\WINDOWS\system32> Log-Action A12 end
A12 end 2026-08-16T09:11:13.3732424+00:00
PS C:\WINDOWS\system32> Log-Action A13 start "Install Adobe Reader"
A13 start 2026-08-16T09:11:33.2293594+00:00 Install Adobe Reader
PS C:\WINDOWS\system32> Log-Action A13 end
A13 end 2026-08-16T09:17:18.5298004+00:00
PS C:\WINDOWS\system32> Log-Action 14 start "Install Zoom"
14 start 2026-08-16T09:17:42.2585285+00:00 Install Zoom
PS C:\WINDOWS\system32> Log-Action 14 end
14 end 2026-08-16T09:18:26.7579035+00:00
PS C:\WINDOWS\system32> Log-Action 15 start "Install Notepad++"
15 start 2026-08-16T09:18:45.4184013+00:00 Install Notepad++
PS C:\WINDOWS\system32> Log-Action 15 end
15 end 2026-08-16T09:19:19.5501357+00:00
PS C:\WINDOWS\system32> Show-Log
```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-16T08:58:59.4033339+00:00	Open Edge
A01	end	2026-08-16T08:59:41.3408270+00:00	
A02	start	2026-08-16T09:00:13.7821730+00:00	Download Chrome
A02	end	2026-08-16T09:00:50.7262753+00:00	
A03	start	2026-08-16T09:01:04.9746597+00:00	Download WinRAR
A03	end	2026-08-16T09:01:40.7449125+00:00	
A04	start	2026-08-16T09:01:54.1119760+00:00	Download VLC
A04	end	2026-08-16T09:02:53.4331131+00:00	
A05	start	2026-08-16T09:03:16.4195277+00:00	Download Adobe Reader
A05	end	2026-08-16T09:03:40.9418651+00:00	
A06	start	2026-08-16T09:03:59.5274415+00:00	Download Zoom
A06	end	2026-08-16T09:05:04.7044270+00:00	
A07	start	2026-08-16T09:05:30.3951715+00:00	Download Notepad++
A07	end	2026-08-16T09:06:06.1802774+00:00	
A08	start	2026-08-16T09:06:40.1540236+00:00	Download Close Edge
A08	end	2026-08-16T09:06:51.5894190+00:00	
A09	start	2026-08-16T09:07:18.2189427+00:00	Open Downloads
A09	end	2026-08-16T09:07:34.3116590+00:00	
A10	start	2026-08-16T09:07:54.3956577+00:00	Install Chrome
A10	end	2026-08-16T09:09:20.1974816+00:00	
A11	start	2026-08-16T09:09:44.3129259+00:00	Install WinRAR
A11	end	2026-08-16T09:10:03.7232064+00:00	
A12	start	2026-08-16T09:10:25.3472610+00:00	Install VLC
A12	end	2026-08-16T09:11:13.3732424+00:00	

```

A13      start 2026-08-16T09:11:33.2293594+00:00 Install A
dobe Reader
A13      end    2026-08-16T09:17:18.5298004+00:00
14       start 2026-08-16T09:17:42.2585285+00:00 Install Z
oom
14       end    2026-08-16T09:18:26.7579035+00:00
15       start 2026-08-16T09:18:45.4184013+00:00 Install N
otepad++
15       end    2026-08-16T09:19:19.5501357+00:00

```

```

PS C:\WINDOWS\system32> Save-Log -Scenario S01 -Run R01
Wrote 30 rows to C:\DISS_TESTDATA\S01-R01-action-log.csv
PS C:\WINDOWS\system32>

```

```

PS C:\WINDOWS\system32> Log-Action A01 start "Open Edge"
A01 start 2026-08-16T08:58:59.4033339+00:00 Open Edge
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-16T08:59:41.3408270+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Download Chrome"
A02 start 2026-08-16T09:00:13.7821730+00:00 Download Chrome
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-16T09:00:50.7262753+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Download WinRAR"
A03 start 2026-08-16T09:01:04.9746597+00:00 Download WinRAR
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-16T09:01:40.7449125+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Download VLC"
A04 start 2026-08-16T09:01:54.1119760+00:00 Download VLC
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-16T09:02:53.4331131+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Download Adobe Reader"
A05 start 2026-08-16T09:03:16.4195277+00:00 Download Adobe Reader
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-16T09:03:40.9418651+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Download Zoom"
A06 start 2026-08-16T09:03:59.5274415+00:00 Download Zoom
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-16T09:05:04.7044270+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Download Notepad++"
A07 start 2026-08-16T09:05:30.3951715+00:00 Download Notepad++
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-16T09:06:06.1802774+00:00
PS C:\WINDOWS\system32> Log-Action A08 start "Download Close Edge"
A08 start 2026-08-16T09:06:40.1540236+00:00 Download Close Edge
PS C:\WINDOWS\system32> Log-Action A08 end
A08 end 2026-08-16T09:06:51.5894190+00:00
PS C:\WINDOWS\system32> Log-Action A09 start "Open Downloads"
A09 start 2026-08-16T09:07:18.2189427+00:00 Open Downloads
PS C:\WINDOWS\system32> Log-Action A09 end
A09 end 2026-08-16T09:07:34.3116590+00:00
PS C:\WINDOWS\system32> Log-Action A10 start "Install Chrome"
A10 start 2026-08-16T09:07:54.3956577+00:00 Install Chrome
PS C:\WINDOWS\system32> Log-Action A10 end
A10 end 2026-08-16T09:09:20.1974816+00:00
PS C:\WINDOWS\system32> Log-Action A11 start "Install WinRAR"
A11 start 2026-08-16T09:09:44.3129259+00:00 Install WinRAR
PS C:\WINDOWS\system32> Log-Action A11 end
A11 end 2026-08-16T09:10:03.7232064+00:00
PS C:\WINDOWS\system32> Log-Action A12 start "Install VLC"
A12 start 2026-08-16T09:10:25.3472610+00:00 Install VLC
PS C:\WINDOWS\system32> Log-Action A12 end
A12 end 2026-08-16T09:11:13.3732424+00:00
PS C:\WINDOWS\system32> Log-Action A13 start "Install Adobe Reader"
A13 start 2026-08-16T09:11:33.2293594+00:00 Install Adobe Reader
PS C:\WINDOWS\system32> Log-Action A13 end
A13 end 2026-08-16T09:17:18.5298004+00:00
PS C:\WINDOWS\system32> Log-Action 14 start "Install Zoom"
14 start 2026-08-16T09:17:42.2585285+00:00 Install Zoom
PS C:\WINDOWS\system32> Log-Action 14 end
14 end 2026-08-16T09:18:26.7579035+00:00
PS C:\WINDOWS\system32> Log-Action 15 start "Install Notepad++"
15 start 2026-08-16T09:18:45.4184013+00:00 Install Notepad++
PS C:\WINDOWS\system32> Log-Action 15 end
15 end 2026-08-16T09:19:19.5501357+00:00

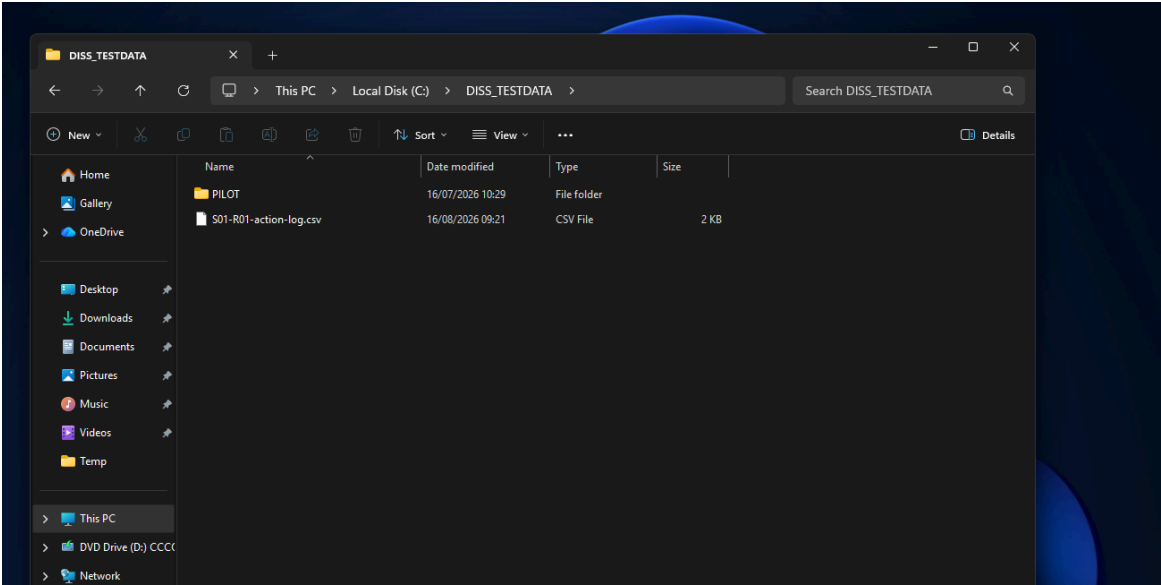
```

```
10 end 2026-08-16T09:19:19.0001537+00:00
PS C:\WINDOWS\system32> Show-Log

Action Phase UTC Note
-----
A01 start 2026-08-16T08:58:59.4033339+00:00 Open Edge
A01 end 2026-08-16T08:59:41.3408270+00:00
A02 start 2026-08-16T09:00:13.7821730+00:00 Download Chrome
A02 end 2026-08-16T09:00:50.7262753+00:00
A03 start 2026-08-16T09:01:04.9746597+00:00 Download WinRAR
A03 end 2026-08-16T09:01:40.7449125+00:00
A04 start 2026-08-16T09:01:54.1119760+00:00 Download VLC
A04 end 2026-08-16T09:02:53.4331131+00:00
A05 start 2026-08-16T09:03:16.4195277+00:00 Download Adobe Reader
A05 end 2026-08-16T09:03:40.9418651+00:00
A06 start 2026-08-16T09:03:59.5274415+00:00 Download Zoom
A06 end 2026-08-16T09:05:04.7044270+00:00
A07 start 2026-08-16T09:05:30.3951715+00:00 Download Notepad++
A07 end 2026-08-16T09:06:06.1802774+00:00
A08 start 2026-08-16T09:06:40.1540236+00:00 Download Close Edge
A08 end 2026-08-16T09:06:51.5894190+00:00
A09 start 2026-08-16T09:07:18.2189427+00:00 Open Downloads
A09 end 2026-08-16T09:07:34.3116590+00:00
A10 start 2026-08-16T09:07:54.3956577+00:00 Install Chrome
A10 end 2026-08-16T09:09:20.1974816+00:00
A11 start 2026-08-16T09:09:44.3129259+00:00 Install WinRAR
A11 end 2026-08-16T09:10:03.7232064+00:00
A12 start 2026-08-16T09:10:25.3472610+00:00 Install VLC
A12 end 2026-08-16T09:11:13.3732424+00:00
A13 start 2026-08-16T09:11:33.2293594+00:00 Install Adobe Reader
A13 end 2026-08-16T09:17:18.5298004+00:00
14 start 2026-08-16T09:17:42.2585285+00:00 Install Zoom
14 end 2026-08-16T09:18:26.7579035+00:00
15 start 2026-08-16T09:18:45.4184013+00:00 Install Notepad++
15 end 2026-08-16T09:19:19.5501357+00:00

PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32> Save-Log -Scenario S01 -Run R01
Wrote 30 rows to C:\DISS_TESTDATA\S01-R01-action-log.csv
PS C:\WINDOWS\system32> |
```



```

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scripts> .\scenario-acquire.ps1 -Scenario S01 -Run R01
[Acquire] S01-R01 offline acquisition starting
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'S01-R01-POST' -> DISS-Win11-25H2-Testbed-000002.vmdk
[Acquire] Mounting DISS-Win11-25H2-Testbed-000002.vmdk via aim_cli (DiscUtils, read-only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (419 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 27,332,608 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 0 bytes (exit 1)
ok NTUSER.DAT.LOG2 0 bytes (exit 1)
ok UsrClass.dat 2,097,152 bytes (exit 1)
ok UsrClass.dat.LOG1 196,608 bytes (exit 1)
ok UsrClass.dat.LOG2 0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,631,488 bytes (exit 1)
ok SOFTWARE 82,051,072 bytes (exit 1)
ok Amcache.hve 2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA-256 manifest
[Acquire] S01-R01 acquisition complete
Snapshot : S01-R01-POST (DISS-Win11-25H2-Testbed-000002.vmdk)
Mount : AIM device 000000 at H: (dismounted)
Files : 433 (136.67 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\artefacts\supporting\raw\S01-R01\acquisition-manifest.csv

Landing zones:
prefetch 419 files -> D:\UOW\SEM3\msc-diss-7csef001w\artefacts\prefetch\raw\S01-R01
eventlogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\artefacts\event-logs\raw\S01-R01
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\artefacts\shellbags\raw\S01-R01
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\artefacts\supporting\raw\S01-R01
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scripts>

```

▼ SCN2

```

PS C:\WINDOWS\system32> Log-Action A01 start "Iter 1 - l
aunch notepad.exe"
A01 start 2026-08-17T18:29:49.1777234+00:00 Iter 1 - lau
nch notepad.exe
PS C:\WINDOWS\system32> Log-Action A01 end "Iter 1"
A01 end 2026-08-17T18:30:33.0938169+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A02 start "Iter 1 - l
aunch calc.exe"
A02 start 2026-08-17T18:31:04.7225649+00:00 Iter 1 - lau
nch calc.exe
PS C:\WINDOWS\system32> Log-Action A02 end "Iter 1"
A02 end 2026-08-17T18:31:45.2024379+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A03 start "Iter 1 - l
aunch chrome.exe"
A03 start 2026-08-17T18:32:04.4030101+00:00 Iter 1 - lau
nch chrome.exe
PS C:\WINDOWS\system32> Log-Action A03 end "Iter 1"
A03 end 2026-08-17T18:33:09.1857753+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A04 start "Iter 1 - l

```

```

aunch winrar.exe"
A04 start 2026-08-17T18:34:14.6204594+00:00 Iter 1 - lau
nch winrar.exe
PS C:\WINDOWS\system32> Log-Action A04 end "Iter 1"
A04 end 2026-08-17T18:34:56.3893021+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A05 start "Iter 1 - l
aunch vlc.exe"
A05 start 2026-08-17T18:35:36.5951694+00:00 Iter 1 - lau
nch vlc.exe
PS C:\WINDOWS\system32> Log-Action A05 end "Iter 1"
A05 end 2026-08-17T18:36:48.1358539+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A06 start "Iter 1 - l
aunch notepad++.exe"
A06 start 2026-08-17T18:37:22.9443129+00:00 Iter 1 - lau
nch notepad++.exe
PS C:\WINDOWS\system32> Log-Action A06 end "Iter 1"
A06 end 2026-08-17T18:38:29.5511548+00:00 Iter 1
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Iter 2 - l
aunch notepad.exe"
A01 start 2026-08-17T18:39:53.8103100+00:00 Iter 2 - lau
nch notepad.exe
PS C:\WINDOWS\system32> Log-Action A01 end "Iter 2"
A01 end 2026-08-17T18:41:17.2682232+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A02 start "Iter 2 - l
aunch calc.exe"
A02 start 2026-08-17T18:42:07.4629662+00:00 Iter 2 - lau
nch calc.exe
PS C:\WINDOWS\system32> Log-Action A02 end "Iter 2"
A02 end 2026-08-17T18:43:32.0363790+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A03 start "Iter 2 - l
aunch chrome.exe"
A03 start 2026-08-17T18:44:01.6092203+00:00 Iter 2 - lau
nch chrome.exe
PS C:\WINDOWS\system32> Log-Action A03 end "Iter 2"

```

```
A03 end 2026-08-17T18:44:44.5670525+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A04 start "Iter 2 - l
aunch winrar.exe"
A04 start 2026-08-17T18:45:18.1439736+00:00 Iter 2 - lau
nch winrar.exe
PS C:\WINDOWS\system32> Log-Action A04 end "Iter 2"
A04 end 2026-08-17T18:46:10.5444002+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A05 start "Iter 2 - l
aunch vlc.exe"
A05 start 2026-08-17T18:46:36.5960948+00:00 Iter 2 - lau
nch vlc.exe
PS C:\WINDOWS\system32> Log-Action A05 end "Iter 2"
A05 end 2026-08-17T18:47:33.0180341+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A06 start "Iter 2 - l
aunch notepad++.exe"
A06 start 2026-08-17T18:47:58.0501524+00:00 Iter 2 - lau
nch notepad++.exe
PS C:\WINDOWS\system32> Log-Action A06 end "Iter 2"
A06 end 2026-08-17T18:48:46.0748833+00:00 Iter 2
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Iter 3 - l
aunch notepad.exe"
A01 start 2026-08-17T18:49:24.5375847+00:00 Iter 3 - lau
nch notepad.exe
PS C:\WINDOWS\system32> Log-Action A01 end "Iter 3"
A01 end 2026-08-17T18:50:10.9622410+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A02 start "Iter 3 - l
aunch calc.exe"
A02 start 2026-08-17T18:50:31.7721332+00:00 Iter 3 - lau
nch calc.exe
PS C:\WINDOWS\system32> Log-Action A02 end "Iter 3"
A02 end 2026-08-17T18:51:15.7449713+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A03 start "Iter 3 - l
aunch chrome.exe"
A03 start 2026-08-17T18:51:37.0617019+00:00 Iter 3 - lau
nch chrome.exe
```

```

PS C:\WINDOWS\system32> Log-Action A03 end "Iter 3"
A03 end 2026-08-17T18:52:23.9539301+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A04 start "Iter 3 - l
aunch winrar.exe"
A04 start 2026-08-17T18:52:52.0921476+00:00 Iter 3 - lau
nch winrar.exe
PS C:\WINDOWS\system32> Log-Action A04 end "Iter 3"
A04 end 2026-08-17T18:53:48.5170544+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A05 start "Iter 3 - l
aunch vlc.exe"
A05 start 2026-08-17T18:54:12.9288188+00:00 Iter 3 - lau
nch vlc.exe
PS C:\WINDOWS\system32> Log-Action A05 end "Iter 3"
A05 end 2026-08-17T18:54:58.7541132+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A06 start "Iter 3 - l
aunch notepad++.exe"
A06 start 2026-08-17T18:55:19.0676523+00:00 Iter 3 - lau
nch notepad++.exe
PS C:\WINDOWS\system32> Log-Action A06 end "Iter 3"
A06 end 2026-08-17T18:56:16.1809529+00:00 Iter 3
PS C:\WINDOWS\system32> Show-Log

```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-17T18:29:49.1777234+00:00	Iter 1 - launch notepad.exe
A01	end	2026-08-17T18:30:33.0938169+00:00	Iter 1
A02	start	2026-08-17T18:31:04.7225649+00:00	Iter 1 - launch calc.exe
A02	end	2026-08-17T18:31:45.2024379+00:00	Iter 1
A03	start	2026-08-17T18:32:04.4030101+00:00	Iter 1 - launch chrome.exe
A03	end	2026-08-17T18:33:09.1857753+00:00	Iter 1
A04	start	2026-08-17T18:34:14.6204594+00:00	Iter 1 - launch winrar.exe
A04	end	2026-08-17T18:34:56.3893021+00:00	Iter 1
A05	start	2026-08-17T18:35:36.5951694+00:00	Iter 1 - launch vlc.exe

```

A05    end    2026-08-17T18:36:48.1358539+00:00 Iter 1
A06    start 2026-08-17T18:37:22.9443129+00:00 Iter 1 -
launch notepad++.exe
A06    end    2026-08-17T18:38:29.5511548+00:00 Iter 1
A01    start 2026-08-17T18:39:53.8103100+00:00 Iter 2 -
launch notepad.exe
A01    end    2026-08-17T18:41:17.2682232+00:00 Iter 2
A02    start 2026-08-17T18:42:07.4629662+00:00 Iter 2 -
launch calc.exe
A02    end    2026-08-17T18:43:32.0363790+00:00 Iter 2
A03    start 2026-08-17T18:44:01.6092203+00:00 Iter 2 -
launch chrome.exe
A03    end    2026-08-17T18:44:44.5670525+00:00 Iter 2
A04    start 2026-08-17T18:45:18.1439736+00:00 Iter 2 -
launch winrar.exe
A04    end    2026-08-17T18:46:10.5444002+00:00 Iter 2
A05    start 2026-08-17T18:46:36.5960948+00:00 Iter 2 -
launch vlc.exe
A05    end    2026-08-17T18:47:33.0180341+00:00 Iter 2
A06    start 2026-08-17T18:47:58.0501524+00:00 Iter 2 -
launch notepad++.exe
A06    end    2026-08-17T18:48:46.0748833+00:00 Iter 2
A01    start 2026-08-17T18:49:24.5375847+00:00 Iter 3 -
launch notepad.exe
A01    end    2026-08-17T18:50:10.9622410+00:00 Iter 3
A02    start 2026-08-17T18:50:31.7721332+00:00 Iter 3 -
launch calc.exe
A02    end    2026-08-17T18:51:15.7449713+00:00 Iter 3
A03    start 2026-08-17T18:51:37.0617019+00:00 Iter 3 -
launch chrome.exe
A03    end    2026-08-17T18:52:23.9539301+00:00 Iter 3
A04    start 2026-08-17T18:52:52.0921476+00:00 Iter 3 -
launch winrar.exe
A04    end    2026-08-17T18:53:48.5170544+00:00 Iter 3
A05    start 2026-08-17T18:54:12.9288188+00:00 Iter 3 -
launch vlc.exe
A05    end    2026-08-17T18:54:58.7541132+00:00 Iter 3
A06    start 2026-08-17T18:55:19.0676523+00:00 Iter 3 -

```

launch notepad++.exe

A06 end 2026-08-17T18:56:16.1809529+00:00 Iter 3

PS C:\WINDOWS\system32> Save-Log -Scenario 2

Wrote 36 rows to C:\DISS_TESTDATA\scenario2_actions.csv

```
PS C:\WINDOWS\system32> Log-Action A01 start "Iter 1 - launch notepad.exe"
A01 start 2026-08-17T18:29:49.1777234+00:00 Iter 1 - launch notepad.exe
PS C:\WINDOWS\system32> Log-Action A01 end "Iter 1"
A01 end 2026-08-17T18:30:33.0938169+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A02 start "Iter 1 - launch calc.exe"
A02 start 2026-08-17T18:31:04.7225649+00:00 Iter 1 - launch calc.exe
PS C:\WINDOWS\system32> Log-Action A02 end "Iter 1"
A02 end 2026-08-17T18:31:45.2024379+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A03 start "Iter 1 - launch chrome.exe"
A03 start 2026-08-17T18:32:04.4030101+00:00 Iter 1 - launch chrome.exe
PS C:\WINDOWS\system32> Log-Action A03 end "Iter 1"
A03 end 2026-08-17T18:33:09.1857753+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A04 start "Iter 1 - launch winrar.exe"
A04 start 2026-08-17T18:34:14.6204594+00:00 Iter 1 - launch winrar.exe
PS C:\WINDOWS\system32> Log-Action A04 end "Iter 1"
A04 end 2026-08-17T18:34:56.3893021+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A05 start "Iter 1 - launch vlc.exe"
A05 start 2026-08-17T18:35:36.5951694+00:00 Iter 1 - launch vlc.exe
PS C:\WINDOWS\system32> Log-Action A05 end "Iter 1"
A05 end 2026-08-17T18:36:48.1358539+00:00 Iter 1
PS C:\WINDOWS\system32> Log-Action A06 start "Iter 1 - launch notepad++.exe"
A06 start 2026-08-17T18:37:22.9443129+00:00 Iter 1 - launch notepad++.exe
PS C:\WINDOWS\system32> Log-Action A06 end "Iter 1"
A06 end 2026-08-17T18:38:29.5511548+00:00 Iter 1
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Iter 2 - launch notepad.exe"
A01 start 2026-08-17T18:39:53.8103100+00:00 Iter 2 - launch notepad.exe
PS C:\WINDOWS\system32> Log-Action A01 end "Iter 2"
A01 end 2026-08-17T18:41:17.2682232+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A02 start "Iter 2 - launch calc.exe"
A02 start 2026-08-17T18:42:07.4629662+00:00 Iter 2 - launch calc.exe
PS C:\WINDOWS\system32> Log-Action A02 end "Iter 2"
A02 end 2026-08-17T18:43:32.0363790+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A03 start "Iter 2 - launch chrome.exe"
A03 start 2026-08-17T18:44:01.6092203+00:00 Iter 2 - launch chrome.exe
PS C:\WINDOWS\system32> Log-Action A03 end "Iter 2"
A03 end 2026-08-17T18:44:44.5670525+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A04 start "Iter 2 - launch winrar.exe"
A04 start 2026-08-17T18:45:18.1439736+00:00 Iter 2 - launch winrar.exe
PS C:\WINDOWS\system32> Log-Action A04 end "Iter 2"
A04 end 2026-08-17T18:46:10.5444002+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A05 start "Iter 2 - launch vlc.exe"
A05 start 2026-08-17T18:46:36.5960948+00:00 Iter 2 - launch vlc.exe
PS C:\WINDOWS\system32> Log-Action A05 end "Iter 2"
A05 end 2026-08-17T18:47:33.0180341+00:00 Iter 2
PS C:\WINDOWS\system32> Log-Action A06 start "Iter 2 - launch notepad++.exe"
A06 start 2026-08-17T18:47:58.0501524+00:00 Iter 2 - launch notepad++.exe
PS C:\WINDOWS\system32> Log-Action A06 end "Iter 2"
A06 end 2026-08-17T18:48:46.0748833+00:00 Iter 2
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Iter 3 - launch notepad.exe"
A01 start 2026-08-17T18:49:24.5375847+00:00 Iter 3 - launch notepad.exe
PS C:\WINDOWS\system32> Log-Action A01 end "Iter 3"
A01 end 2026-08-17T18:50:10.9622410+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A02 start "Iter 3 - launch calc.exe"
A02 start 2026-08-17T18:50:31.7721332+00:00 Iter 3 - launch calc.exe
PS C:\WINDOWS\system32> Log-Action A02 end "Iter 3"
A02 end 2026-08-17T18:51:15.7449713+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A03 start "Iter 3 - launch chrome.exe"
A03 start 2026-08-17T18:51:37.0617019+00:00 Iter 3 - launch chrome.exe
PS C:\WINDOWS\system32> Log-Action A03 end "Iter 3"
A03 end 2026-08-17T18:52:23.9539301+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A04 start "Iter 3 - launch winrar.exe"
A04 start 2026-08-17T18:52:52.0921476+00:00 Iter 3 - launch winrar.exe
PS C:\WINDOWS\system32> Log-Action A04 end "Iter 3"
A04 end 2026-08-17T18:53:48.5170544+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A05 start "Iter 3 - launch vlc.exe"
A05 start 2026-08-17T18:54:12.9288188+00:00 Iter 3 - launch vlc.exe
PS C:\WINDOWS\system32> Log-Action A05 end "Iter 3"
A05 end 2026-08-17T18:54:58.7541132+00:00 Iter 3
PS C:\WINDOWS\system32> Log-Action A06 start "Iter 3 - launch notepad++.exe"
A06 start 2026-08-17T18:55:19.0676523+00:00 Iter 3 - launch notepad++.exe
PS C:\WINDOWS\system32> Log-Action A06 end "Iter 3"
A06 end 2026-08-17T18:56:16.1809529+00:00 Iter 3

```

```

A06 end 2026-08-17T18:56:16.1809529+00:00 Iter 3
PS C:\WINDOWS\system32> Show-Log

Action Phase UTC                                     Note
-----
A01 start 2026-08-17T18:29:49.1777234+00:00 Iter 1 - launch notepad.exe
A01 end 2026-08-17T18:30:33.0938169+00:00 Iter 1
A02 start 2026-08-17T18:31:04.7225649+00:00 Iter 1 - launch calc.exe
A02 end 2026-08-17T18:31:45.2024379+00:00 Iter 1
A03 start 2026-08-17T18:32:04.4030101+00:00 Iter 1 - launch chrome.exe
A03 end 2026-08-17T18:33:09.1857753+00:00 Iter 1
A04 start 2026-08-17T18:34:14.6204594+00:00 Iter 1 - launch winrar.exe
A04 end 2026-08-17T18:34:56.3893021+00:00 Iter 1
A05 start 2026-08-17T18:35:36.5951694+00:00 Iter 1 - launch vlc.exe
A05 end 2026-08-17T18:36:48.1358539+00:00 Iter 1
A06 start 2026-08-17T18:37:22.9443129+00:00 Iter 1 - launch notepad++.exe
A06 end 2026-08-17T18:38:29.5511548+00:00 Iter 1
A01 start 2026-08-17T18:39:53.8103100+00:00 Iter 2 - launch notepad.exe
A01 end 2026-08-17T18:41:17.2682232+00:00 Iter 2
A02 start 2026-08-17T18:42:07.4629662+00:00 Iter 2 - launch calc.exe
A02 end 2026-08-17T18:43:32.0363790+00:00 Iter 2
A03 start 2026-08-17T18:44:01.6092203+00:00 Iter 2 - launch chrome.exe
A03 end 2026-08-17T18:44:44.5670525+00:00 Iter 2
A04 start 2026-08-17T18:45:18.1439736+00:00 Iter 2 - launch winrar.exe
A04 end 2026-08-17T18:46:10.5444002+00:00 Iter 2
A05 start 2026-08-17T18:46:36.5960948+00:00 Iter 2 - launch vlc.exe
A05 end 2026-08-17T18:47:33.0180341+00:00 Iter 2
A06 start 2026-08-17T18:47:58.0501524+00:00 Iter 2 - launch notepad++.exe
A06 end 2026-08-17T18:48:46.0748833+00:00 Iter 2
A01 start 2026-08-17T18:49:24.5375847+00:00 Iter 3 - launch notepad.exe
A01 end 2026-08-17T18:50:10.9622410+00:00 Iter 3
A02 start 2026-08-17T18:50:31.7721332+00:00 Iter 3 - launch calc.exe
A02 end 2026-08-17T18:51:15.7449713+00:00 Iter 3
A03 start 2026-08-17T18:51:37.0617019+00:00 Iter 3 - launch chrome.exe
A03 end 2026-08-17T18:52:23.9539301+00:00 Iter 3
A04 start 2026-08-17T18:52:52.0921476+00:00 Iter 3 - launch winrar.exe
A04 end 2026-08-17T18:53:48.5170544+00:00 Iter 3
A05 start 2026-08-17T18:54:12.9288188+00:00 Iter 3 - launch vlc.exe
A05 end 2026-08-17T18:54:58.7541132+00:00 Iter 3
A06 start 2026-08-17T18:55:19.0676523+00:00 Iter 3 - launch notepad++.exe
A06 end 2026-08-17T18:56:16.1809529+00:00 Iter 3

PS C:\WINDOWS\system32> Save-Log -Scenario 2
Wrote 36 rows to C:\DISS_TESTDATA\scenario2_actions.csv
PS C:\WINDOWS\system32> 0_

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 2
[Acquire] scenario2 offline acquisition starting (single-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario2_post' -> DISS-Win11-25H2-Testbed-000004.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_2
[Acquire] Mounting DISS-Win11-25H2-Testbed-000004.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (439 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 29,429,760 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 0 bytes (exit 1)
ok NTUSER.DAT.LOG2 524,288 bytes (exit 1)
ok UsrClass.dat 2,097,152 bytes (exit 1)
ok UsrClass.dat.LOG1 458,752 bytes (exit 1)
ok UsrClass.dat.LOG2 0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,631,488 bytes (exit 1)
ok SOFTWARE 82,051,072 bytes (exit 1)
ok Amcache.hve 2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario2 acquisition complete
Snapshot : scenario2_post (DISS-Win11-25H2-Testbed-000004.vmdk)
Mount : AIM device 000000 at H: (dismounted)
Files : 453 (139.91 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_2\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 439 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_2\artefacts\prefetch
eventLogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_2\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_2\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_2\artefacts\supporting

```

▼ SCN3

```

$root = 'C:\DISS_TESTDATA\scenario3_nav'
New-Item -ItemType Directory -Force -Path "$root\level1_
a\level2_a\level3_a\level4_a\level5_a" | Out-Null
New-Item -ItemType Directory -Force -Path "$root\level1_
b" | Out-Null
Get-ChildItem -Recurse $root | Select-Object FullName

```

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> $root = 'C:\DISS_TESTDATA\scenario3_nav'
PS C:\WINDOWS\system32> New-Item -ItemType Directory -Force -Path "$root\level1_a\level2_a\level3_a\level4_a\level5_a" | Out-Null
PS C:\WINDOWS\system32> New-Item -ItemType Directory -Force -Path "$root\level1_b" | Out-Null
PS C:\WINDOWS\system32> Get-ChildItem -Recurse $root | Select-Object FullName

FullName
-----
C:\DISS_TESTDATA\scenario3_nav\level1_a
C:\DISS_TESTDATA\scenario3_nav\level1_b
C:\DISS_TESTDATA\scenario3_nav\level1_a\level2_a
C:\DISS_TESTDATA\scenario3_nav\level1_a\level2_a\level3_a
C:\DISS_TESTDATA\scenario3_nav\level1_a\level2_a\level3_a\level4_a
C:\DISS_TESTDATA\scenario3_nav\level1_a\level2_a\level3_a\level4_a\level5_a

PS C:\WINDOWS\system32> $script:log = @()
PS C:\WINDOWS\system32> function Log-Action { param([Parameter(Mandatory)][string]$id,[Parameter(Mandatory)][string]$phase,[string]$note='')
>> $ts = Get-Date -Format o
>> $script:log += [PSCustomObject]@{Action=$id;Phase=$phase;UTC=$ts;Note=$note}
>> Write-Host "$id $phase $ts $note"
>> }
PS C:\WINDOWS\system32> function Save-Log { param([Parameter(Mandatory)][int]$Scenario,[int]$Run=0,[string]$Path='C:\DISS_TESTDATA')
>> if (-not (Test-Path $Path)) { New-Item -ItemType Directory -Path $Path -Force | Out-Null }
>> $filename = if ($Run -eq 0) { "scenario${Scenario}_actions.csv" } else { "scenario${Scenario}_run${Run}_actions.csv" }
>> $file = Join-Path $Path $filename
>> $script:log | Export-Csv -Path $file -NoTypeInformation
>> Write-Host "Wrote $($script:log.Count) rows to $file"
>> }
PS C:\WINDOWS\system32> |

```

```
PS C:\WINDOWS\system32> Log-Action A01 start "Open File Explorer"
A01 start 2026-08-18T07:20:32.2498331+00:00 Open File Explorer
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-18T07:20:52.8260083+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Navigate to C:\DISS_TESTDATA\scenario3_nav"
A02 start 2026-08-18T07:21:32.4661894+00:00 Navigate to C:\DISS_TESTDATA\scenario3_nav
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-18T07:21:48.2794905+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Double click level1_a"
A03 start 2026-08-18T07:22:48.8216265+00:00 Double click level1_a
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-18T07:23:01.4267588+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Double click level2_a"
A04 start 2026-08-18T07:23:20.4930525+00:00 Double click level2_a
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-18T07:23:33.6090316+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Double click level3_a"
A05 start 2026-08-18T07:23:49.2029690+00:00 Double click level3_a
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-18T07:24:04.1414477+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Double click level4_a"
A06 start 2026-08-18T07:24:18.7615493+00:00 Double click level4_a
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-18T07:24:37.2755628+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Double click level5_a"
```

```

A07 start 2026-08-18T07:24:52.9573385+00:00 Double click
level5_a
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-18T07:25:09.9162370+00:00
PS C:\WINDOWS\system32> Log-Action A08 start "Close Expl
orer"
A08 start 2026-08-18T07:25:24.8416827+00:00 Close Explor
er
PS C:\WINDOWS\system32> Log-Action A08 end
A08 end 2026-08-18T07:25:37.8058899+00:00
PS C:\WINDOWS\system32> $script:log | Format-Table -Auto
Size

```

Action	Phase	UTC	Note
-----	-----	----	----
A01	start	2026-08-18T07:20:32.2498331+00:00	Open File Explorer
A01	end	2026-08-18T07:20:52.8260083+00:00	
A02	start	2026-08-18T07:21:32.4661894+00:00	Navigate to C:\DISS_TESTDATA\scenario3_nav
A02	end	2026-08-18T07:21:48.2794905+00:00	
A03	start	2026-08-18T07:22:48.8216265+00:00	Double click level1_a
A03	end	2026-08-18T07:23:01.4267588+00:00	
A04	start	2026-08-18T07:23:20.4930525+00:00	Double click level2_a
A04	end	2026-08-18T07:23:33.6090316+00:00	
A05	start	2026-08-18T07:23:49.2029690+00:00	Double click level3_a
A05	end	2026-08-18T07:24:04.1414477+00:00	
A06	start	2026-08-18T07:24:18.7615493+00:00	Double click level4_a
A06	end	2026-08-18T07:24:37.2755628+00:00	
A07	start	2026-08-18T07:24:52.9573385+00:00	Double click level5_a
A07	end	2026-08-18T07:25:09.9162370+00:00	
A08	start	2026-08-18T07:25:24.8416827+00:00	Close Explorer

A08 end 2026-08-18T07:25:37.8058899+00:00

```
PS C:\WINDOWS\system32> Save-Log -Scenario 3
Wrote 16 rows to C:\DISS_TESTDATA\scenario3_actions.csv
PS C:\WINDOWS\system32>
```

```
Windows PowerShell
PS C:\WINDOWS\system32> Log-Action A01 start "Open File Explorer"
A01 start 2026-08-18T07:20:32.2498331+00:00 Open File Explorer
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-18T07:20:52.8260083+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Navigate to C:\DISS_TESTDATA\scenario3_nav"
A02 start 2026-08-18T07:21:32.4661894+00:00 Navigate to C:\DISS_TESTDATA\scenario3_nav
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-18T07:21:48.2794905+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Double click level1_a"
A03 start 2026-08-18T07:22:48.8216265+00:00 Double click level1_a
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-18T07:23:01.4267588+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Double click level2_a"
A04 start 2026-08-18T07:23:20.4930525+00:00 Double click level2_a
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-18T07:23:33.6090316+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Double click level3_a"
A05 start 2026-08-18T07:23:49.2029690+00:00 Double click level3_a
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-18T07:24:04.1414477+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Double click level4_a"
A06 start 2026-08-18T07:24:18.7615493+00:00 Double click level4_a
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-18T07:24:37.2755628+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Double click level5_a"
A07 start 2026-08-18T07:24:52.9573385+00:00 Double click level5_a
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-18T07:25:09.9162370+00:00
PS C:\WINDOWS\system32> Log-Action A08 start "Close Explorer"
A08 start 2026-08-18T07:25:24.8416827+00:00 Close Explorer
PS C:\WINDOWS\system32> Log-Action A08 end
A08 end 2026-08-18T07:25:37.8058899+00:00
```

```
PS C:\WINDOWS\system32> $script:log | Format-Table -AutoSize

Action Phase UTC Note
-----
A01 start 2026-08-18T07:20:32.2498331+00:00 Open File Explorer
A01 end 2026-08-18T07:20:52.8260083+00:00
A02 start 2026-08-18T07:21:32.4661894+00:00 Navigate to C:\DISS_TESTDATA\scenario3_nav
A02 end 2026-08-18T07:21:48.2794905+00:00
A03 start 2026-08-18T07:22:48.8216265+00:00 Double click level1_a
A03 end 2026-08-18T07:23:01.4267588+00:00
A04 start 2026-08-18T07:23:20.4930525+00:00 Double click level2_a
A04 end 2026-08-18T07:23:33.6090316+00:00
A05 start 2026-08-18T07:23:49.2029690+00:00 Double click level3_a
A05 end 2026-08-18T07:24:04.1414477+00:00
A06 start 2026-08-18T07:24:18.7615493+00:00 Double click level4_a
A06 end 2026-08-18T07:24:37.2755628+00:00
A07 start 2026-08-18T07:24:52.9573385+00:00 Double click level5_a
A07 end 2026-08-18T07:25:09.9162370+00:00
A08 start 2026-08-18T07:25:24.8416827+00:00 Close Explorer
A08 end 2026-08-18T07:25:37.8058899+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 3
Wrote 16 rows to C:\DISS_TESTDATA\scenario3_actions.csv
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32> cd D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\a
```

```

cquire_artefacts.ps1 -Scenario 3
[Acquire] scenario3 offline acquisition starting (single
-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,
SeSecurityPrivilege
[Acquire] Resolved 'scenario3_post' -> DISS-Win11-25H2-T
estbed-000003.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\s
cenarios\scenario_3
[Acquire] Mounting DISS-Win11-25H2-Testbed-000003.vmdk v
ia aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to ass
ign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (362 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
26,284,032 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%40per
ational.evtx      69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok NTUSER.DAT
2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1
458,752 bytes (exit 1)
    ok NTUSER.DAT.LOG2
425,984 bytes (exit 1)
    ok UsrClass.dat
2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1

```

```

344,064 bytes (exit 1)
  ok   UsrClass.dat.LOG2
483,328 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
  ok   SYSTEM
13,369,344 bytes (exit 1)
  ok   SOFTWARE
82,051,072 bytes (exit 1)
  ok   Amcache.hve
2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario3 acquisition complete
  Snapshot : scenario3_post (DISS-Win11-25H2-Testbed-000
003.vmdk)
  Mount    : AIM device 000000 at H: (dismounted)
  Files    : 376 (135.43 MB total)
  Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\sc
enario_3\artefacts\supporting\acquisition_manifest.csv

Landing zones:
  prefetch      362 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_3\artefacts\prefetch
  eventLogs     5 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_3\artefacts\event_logs
  shellbags     6 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_3\artefacts\shellbags
  supporting    3 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_3\artefacts\supporting
  evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_3\evaluation

```

```

Copyright (c) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> cd D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 3
[Acquire] scenario3 offline acquisition starting (single-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario3_post' -> DISS-Win11-25H2-Testbed-000003.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_3
[Acquire] Mounting DISS-Win11-25H2-Testbed-000003.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (362 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx 26,284,032 bytes (exit 1)
    ok System.evtx 2,166,784 bytes (exit 1)
    ok Application.evtx 2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
    ok NTUSER.DAT 2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1 458,752 bytes (exit 1)
    ok NTUSER.DAT.LOG2 425,984 bytes (exit 1)
    ok UsrClass.dat 2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1 344,064 bytes (exit 1)
    ok UsrClass.dat.LOG2 483,328 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
    ok SYSTEM 13,369,344 bytes (exit 1)
    ok SOFTWARE 82,051,072 bytes (exit 1)
    ok Amcache.hve 2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario3 acquisition complete
    Snapshot : scenario3_post (DISS-Win11-25H2-Testbed-000003.vmdk)
    Mount : AIM device 000000 at H: (dismounted)
    Files : 376 (135.43 MB total)
    Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_3\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 362 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_3\artefacts\prefetch
eventLogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_3\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_3\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_3\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_3\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

▼ SCN4

| RUN 1

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\scenario4_prepare_usb.ps1
Source HelloWorld.exe hash OK: 0C1F7FDF4A47F67D36042559E0B2B91E557CC1DD12B097BB78BA01EC7182954A

```

USB storage devices attached to the host:

```

Disk 2: General UDisk (3.75 GB) VID=(?) PID=(?) Serial=6&38E547A7&2&_&0

```

Enter the Disk number of the DISS-USB stick to WIPE and REFORMAT: 2

About to WIPE Disk 2 (General UDisk, 3.75 GB).

Type YES to proceed: YES
Wiping and reformatting via diskpart ...
Formatted. Volume root: H: Label: DISS-USB FS: NTFS
HelloWorld.exe staged and verified: 0C1F7FDF4A47F67D3604
2559E0B2B91E557CC1DD12B097BB78BA01EC7182954A

Wrote identity to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\evaluation\usb_identity.txt

Scenario 4 DISS-USB identity

Captured: 2026-08-22T11:15:50Z

Host: SKYNET

User: SSNAQVI

Disk index: 2
Model: General UDisk USB Device
Size (GB): 3.75
PNPDeviceID: USBSTOR\DISK&VEN_GENERAL&PROD_UDISK&REV_5.00\6&38E547A7&2&_&0
VID: (unknown)
PID: (unknown)
Serial (PnP): 6&38E547A7&2&_&0
Hardware ID: USB\VID_(unknown)&PID_(unknown)

Drive letter: H:
Volume label: DISS-USB
Filesystem: NTFS
Volume serial: B0920497

Payload:

Path: \PORTABLE\HelloWorld.exe
SHA-256: 0C1F7FDF4A47F67D36042559E0B2B91E557CC1D
D12B097BB78BA01EC7182954A
Source: scenarios/scenario_4/setup/HelloWorld.exe

Same physical stick across Run 1, Run 2, Run 3 (per catalogue).

Prep complete. Next steps:

1. Safely eject the stick from the host (system tray, Eject DISS-USB).
2. Revert the VM to baseline_pre_scenarios, power on, sign in.
3. Physically plug the stick back in, then VM > Removable Devices > Connect.
4. Load logger, execute A01 to A07, Save-Log -Scenario 4 -Run 1.

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\scenario4_prepare_usb.ps1
Source HelloWorld.exe hash OK: 0C1F7FDF4A47F67D36042559E0B2B91E557CC1DD12B097BB78BA01EC7182954A

USB storage devices attached to the host:
  Disk 2: General UDisk (3.75 GB) VID=(?) PID=(?) Serial=6&38E547A7&2&_&0

Enter the Disk number of the DISS-USB stick to WIPE and REFORMAT: 2

About to WIPE Disk 2 (General UDisk, 3.75 GB).
Type YES to proceed: YES
Wiping and reformatting via diskpart ...
Formatted. Volume root: H: Label: DISS-USB FS: NTFS
HelloWorld.exe staged and verified: 0C1F7FDF4A47F67D36042559E0B2B91E557CC1DD12B097BB78BA01EC7182954A

Wrote identity to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\evaluation\usb_identity.txt

Scenario 4 DISS-USB identity
Captured: 2026-08-22T11:15:50Z
Host: SKYNET
User: SSNAQVI

Disk index: 2
Model: General UDisk USB Device
Size (GB): 3.75
PNPDeviceID: USBSTOR\DISK&VEN_GENERAL&PROD_UDISK&REV_5.00\6&38E547A7&2&_&0
VID: (unknown)
PID: (unknown)
Serial (PnP): 6&38E547A7&2&_&0
Hardware ID: USB\VID_(unknown)&PID_(unknown)

Drive letter: H:
Volume label: DISS-USB
Filesystem: NTFS
Volume serial: B0920497

Payload:
  Path: \PORTABLE\HelloWorld.exe
  SHA-256: 0C1F7FDF4A47F67D36042559E0B2B91E557CC1DD12B097BB78BA01EC7182954A
  Source: scenarios/scenario_4/setup/HelloWorld.exe
  Same physical stick across Run 1, Run 2, Run 3 (per catalogue).

Prep complete. Next steps:
  1. Safely eject the stick from the host (system tray, Eject DISS-USB).
  2. Revert the VM to baseline_pre_scenarios, power on, sign in.
  3. Physically plug the stick back in, then VM > Removable Devices > Connect.
  4. Load logger, execute A01 to A07, Save-Log -Scenario 4 -Run 1.
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>
```

```
E:\PORTABLE\HelloWorld.exe X + v
=====
MSc Cyber Security and Forensics Project (7CSEF001W.2)
University of Westminster
=====

Author       : Syed Muhammad Saqlain Abbas (W21634541)
Repository   : github.com/dx7er/msc-diss-7csef001w
Scenario     : Scenario 4 (USB attach, browse, execute)

Purpose
This executable is a controlled forensic payload for the
dissertation testbed. It is staged on a prepared USB stick
(volume label DISS-USB) at \PORTABLE\HelloWorld.exe and
launched from Windows Explorer during scenario execution.

Running it produces correlated artefacts across the three
classes examined in this dissertation:
* Prefetch          HELLOWORLD.EXE-*.pf
* Event Logs        Security 4688 process creation
* ShellBags         BagMRU entry for the USB \PORTABLE\ path

It performs no network activity, writes no files and makes
no registry changes. Output is limited to this console.

Runtime
Host       : disstestbedvm
User       : disstestbedvm\dfanalyst
Started at : 2026-08-22 11:49:07 UTC

=====
Press Enter to close this window.
=====
```

```
PS C:\WINDOWS\system32> Log-Action A01 start "USB attach
via VMWARE Removable devices Connect"
A01 start 2026-08-22T11:45:27.8438961+00:00 USB attach v
ia VMWARE Removable devices Connect
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-22T11:45:57.5349729+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Open Explo
rer, navigate to USB root"
A02 start 2026-08-22T11:46:25.9479536+00:00 Open Explo
r, navigate to USB root
PS C:\WINDOWS\system32> Start-Process explorer.exe "<USB
>:\"
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-22T11:47:31.2898622+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Navigate t
o \PORTABLE\ directory inside USB root"
A03 start 2026-08-22T11:48:02.2528992+00:00 Navigate to
\PORTABLE\ directory inside USB root
PS C:\WINDOWS\system32> Log-Action A03 end
```

```

A03 end 2026-08-22T11:48:19.7328556+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Launching
Helloworld exe from directory"
A04 start 2026-08-22T11:49:03.1365232+00:00 Launching He
lloworld exe from directory
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-22T11:49:49.0046039+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Eject USB
from Explorer"
A05 start 2026-08-22T11:50:10.1839565+00:00 Eject USB fr
om Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-22T11:50:32.4201798+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Disconnect
USB from guest in VMWare Removable Devices"
A06 start 2026-08-22T11:50:59.8384977+00:00 Disconnect U
SB from guest in VMWare Removable Devices
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-22T11:51:30.4501965+00:00
PS C:\WINDOWS\system32> Show-Log

```

Action	Phase	UTC	Note
-----	-----	----	----
A01	start	2026-08-22T11:45:27.8438961+00:00	USB attac
			h via VMWARE Removable devices Connect
A01	end	2026-08-22T11:45:57.5349729+00:00	
A02	start	2026-08-22T11:46:25.9479536+00:00	Open Expl
			orer, navigate to USB root
A02	end	2026-08-22T11:47:31.2898622+00:00	
A03	start	2026-08-22T11:48:02.2528992+00:00	Navigate
			to \PORTABLE\ directory inside USB root
A03	end	2026-08-22T11:48:19.7328556+00:00	
A04	start	2026-08-22T11:49:03.1365232+00:00	Launching
			Helloworld exe from directory
A04	end	2026-08-22T11:49:49.0046039+00:00	
A05	start	2026-08-22T11:50:10.1839565+00:00	Eject USB
			from Explorer
A05	end	2026-08-22T11:50:32.4201798+00:00	

```
A06      start 2026-08-22T11:50:59.8384977+00:00 Disconnect USB from guest in VMWare Removable Devices
A06      end    2026-08-22T11:51:30.4501965+00:00
```

```
PS C:\WINDOWS\system32> Save-Log -Scenario 4 -Run 1
Wrote 12 rows to C:\DISS_TESTDATA\scenario4_run1_actions.csv
```

```
>> Write-Host Log Cleared
>> }
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "USB attach via VMWARE Removable devices Connect"
A01 start 2026-08-22T11:45:27.8438961+00:00 USB attach via VMWARE Removable devices Connect
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-22T11:45:57.5349729+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Open Explorer, navigate to USB root"
A02 start 2026-08-22T11:46:25.9479536+00:00 Open Explorer, navigate to USB root
PS C:\WINDOWS\system32> Start-Process explorer.exe "<USB>:\"
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-22T11:47:31.2898622+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Navigate to \PORTABLE\ directory inside USB root"
A03 start 2026-08-22T11:48:02.2528992+00:00 Navigate to \PORTABLE\ directory inside USB root
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-22T11:48:19.7328556+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Launching Hellowworld exe from directory"
A04 start 2026-08-22T11:49:03.1365232+00:00 Launching Hellowworld exe from directory
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-22T11:49:49.0046039+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Eject USB from Explorer"
A05 start 2026-08-22T11:50:10.1839565+00:00 Eject USB from Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-22T11:50:32.4201798+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Disconnect USB from guest in VMWare Removable Devices"
A06 start 2026-08-22T11:50:59.8384977+00:00 Disconnect USB from guest in VMWare Removable Devices
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-22T11:51:30.4501965+00:00
```

```
A06 end 2026-08-22T11:51:30.4501965+00:00
PS C:\WINDOWS\system32> Show-Log

Action Phase UTC                                     Note
-----
A01      start 2026-08-22T11:45:27.8438961+00:00 USB attach via VMWARE Removable devices Connect
A01      end   2026-08-22T11:45:57.5349729+00:00
A02      start 2026-08-22T11:46:25.9479536+00:00 Open Explorer, navigate to USB root
A02      end   2026-08-22T11:47:31.2898622+00:00
A03      start 2026-08-22T11:48:02.2528992+00:00 Navigate to \PORTABLE\ directory inside USB root
A03      end   2026-08-22T11:48:19.7328556+00:00
A04      start 2026-08-22T11:49:03.1365232+00:00 Launching Hellowworld exe from directory
A04      end   2026-08-22T11:49:49.0046039+00:00
A05      start 2026-08-22T11:50:10.1839565+00:00 Eject USB from Explorer
A05      end   2026-08-22T11:50:32.4201798+00:00
A06      start 2026-08-22T11:50:59.8384977+00:00 Disconnect USB from guest in VMWare Removable Devices
A06      end   2026-08-22T11:51:30.4501965+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 4 -Run 1
Wrote 12 rows to C:\DISS_TESTDATA\scenario4_run1_actions.csv
PS C:\WINDOWS\system32>
```

```
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 4 -Run 1
[Acquire] scenario4_run1 offline acquisition starting (multi-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,
```

```
SeSecurityPrivilege
[Acquire] Resolved 'scenario4_run1_post' -> DISS-Win11-2
5H2-Testbed-000009.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\s
cenarios\scenario_4\run_1
[Acquire] Mounting DISS-Win11-25H2-Testbed-000009.vmdk v
ia aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to ass
ign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (355 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
26,284,032 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%40per
ational.evtx 1,118,208 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok NTUSER.DAT
2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1
0 bytes (exit 1)
    ok NTUSER.DAT.LOG2
0 bytes (exit 1)
    ok UsrClass.dat
2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1
556,032 bytes (exit 1)
    ok UsrClass.dat.LOG2
0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
```

```
cache.hve
  ok    SYSTEM
13,369,344 bytes (exit 1)
  ok    SOFTWARE
82,051,072 bytes (exit 1)
  ok    Amcache.hve
2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario4_run1 acquisition complete
  Snapshot : scenario4_run1_post (DISS-Win11-25H2-Testbed-000009.vmdk)
  Mount    : AIM device 000000 at I: (dismounted)
  Files    : 369 (135.18 MB total)
  Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\supporting\acquisition_manifest.csv
```

Landing zones:

```
  prefetch      355 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\prefetch
  eventLogs      5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\event_logs
  shellbags      6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\shellbags
  supporting     3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\supporting
  evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\evaluation
```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 4 -Run 1
[Acquire] scenario4_run1 offline acquisition starting (multi-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario4_run1_post' -> DISS-Win11-25H2-Testbed-000009.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1
[Acquire] Mounting DISS-Win11-25H2-Testbed-000009.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (355 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 26,284,032 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 1,118,208 bytes (exit 1)
ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 0 bytes (exit 1)
ok NTUSER.DAT.LOG2 0 bytes (exit 1)
ok UsrClass.dat 2,097,152 bytes (exit 1)
ok UsrClass.dat.LOG1 556,032 bytes (exit 1)
ok UsrClass.dat.LOG2 0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,369,344 bytes (exit 1)
ok SOFTWARE 82,051,072 bytes (exit 1)
ok Amcache.hve 2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario4_run1 acquisition complete
Snapshot : scenario4_run1_post (DISS-Win11-25H2-Testbed-000009.vmdk)
Mount : AIM device 000000 at I: (dismounted)
Files : 369 (135.18 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 355 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\prefetch
eventlogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

RUN 2

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "USB attach
via VMWare Removable devices Connect"
A01 start 2026-08-22T20:33:34.0129820+00:00 USB attach v
ia VMWare Removable devices Connect
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-22T20:34:16.0830726+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Open Explo
rer, navigate to USB root"
A02 start 2026-08-22T20:34:34.0027278+00:00 Open Explo
r, navigate to USB root
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-22T20:34:49.6367617+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Navigate t
o \PORTABLE\ directory inside USB root"
A03 start 2026-08-22T20:35:20.2501771+00:00 Navigate to

```

```

\PORTABLE\ directory inside USB root
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-22T20:35:31.8434524+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Launching
Helloworld exe from directory"
A04 start 2026-08-22T20:35:43.6480516+00:00 Launching He
llowworld exe from directory
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-22T20:36:01.0050002+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Eject USB
from Explorer"
A05 start 2026-08-22T20:36:14.5251225+00:00 Eject USB fr
om Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-22T20:36:36.0165618+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Disconnect
USB from guest in VMWare Removable Devices"
A06 start 2026-08-22T20:36:47.3257862+00:00 Disconnect U
SB from guest in VMWare Removable Devices
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-22T20:37:10.2296287+00:00
PS C:\WINDOWS\system32> Show-Log

```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-22T20:33:34.0129820+00:00	USB attac
			h via VMWare Removable devices Connect
A01	end	2026-08-22T20:34:16.0830726+00:00	
A02	start	2026-08-22T20:34:34.0027278+00:00	Open Expl
			orer, navigate to USB root
A02	end	2026-08-22T20:34:49.6367617+00:00	
A03	start	2026-08-22T20:35:20.2501771+00:00	Navigate
			to \PORTABLE\ directory inside USB root
A03	end	2026-08-22T20:35:31.8434524+00:00	
A04	start	2026-08-22T20:35:43.6480516+00:00	Launching
			Helloworld exe from directory
A04	end	2026-08-22T20:36:01.0050002+00:00	
A05	start	2026-08-22T20:36:14.5251225+00:00	Eject USB

from Explorer

```
A05      end      2026-08-22T20:36:36.0165618+00:00
A06      start 2026-08-22T20:36:47.3257862+00:00 Disconnect USB from guest in VMWare Removable Devices
A06      end      2026-08-22T20:37:10.2296287+00:00
```

```
PS C:\WINDOWS\system32> Save-Log -Scenario 4 -Run 2
Wrote 12 rows to C:\DISS_TESTDATA\scenario4_run2_actions.csv
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "USB attach via VMWare Removable devices Connect"
A01 start 2026-08-22T20:33:34.0129820+00:00 USB attach via VMWare Removable devices Connect
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-22T20:34:16.0830726+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Open Explorer, navigate to USB root"
A02 start 2026-08-22T20:34:34.0027278+00:00 Open Explorer, navigate to USB root
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-22T20:34:49.6367617+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Navigate to \PORTABLE\ directory inside USB root"
A03 start 2026-08-22T20:35:20.2501771+00:00 Navigate to \PORTABLE\ directory inside USB root
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-22T20:35:31.8434524+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Launching Hellowworld exe from directory"
A04 start 2026-08-22T20:35:43.6480516+00:00 Launching Hellowworld exe from directory
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-22T20:36:01.0050002+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Eject USB from Explorer"
A05 start 2026-08-22T20:36:14.5251225+00:00 Eject USB from Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-22T20:36:36.0165618+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Disconnect USB from guest in VMWare Removable Devices"
A06 start 2026-08-22T20:36:47.3257862+00:00 Disconnect USB from guest in VMWare Removable Devices
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-22T20:37:10.2296287+00:00
```

```
PS C:\WINDOWS\system32> Show-Log

Action Phase UTC                                     Note
-----
A01      start 2026-08-22T20:33:34.0129820+00:00 USB attach via VMWare Removable devices Connect
A01      end 2026-08-22T20:34:16.0830726+00:00
A02      start 2026-08-22T20:34:34.0027278+00:00 Open Explorer, navigate to USB root
A02      end 2026-08-22T20:34:49.6367617+00:00
A03      start 2026-08-22T20:35:20.2501771+00:00 Navigate to \PORTABLE\ directory inside USB root
A03      end 2026-08-22T20:35:31.8434524+00:00
A04      start 2026-08-22T20:35:43.6480516+00:00 Launching Hellowworld exe from directory
A04      end 2026-08-22T20:36:01.0050002+00:00
A05      start 2026-08-22T20:36:14.5251225+00:00 Eject USB from Explorer
A05      end 2026-08-22T20:36:36.0165618+00:00
A06      start 2026-08-22T20:36:47.3257862+00:00 Disconnect USB from guest in VMWare Removable Devices
A06      end 2026-08-22T20:37:10.2296287+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 4 -Run 2
Wrote 12 rows to C:\DISS_TESTDATA\scenario4_run2_actions.csv
PS C:\WINDOWS\system32>
```

```
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 4 -Run 2
[Acquire] scenario4_run2 offline acquisition starting (m
```

```

ulti-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,
SeSecurityPrivilege
[Acquire] Resolved 'scenario4_run2_post' -> DISS-Win11-2
5H2-Testbed-000011.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\s
cenarios\scenario_4\run_2
[Acquire] Mounting DISS-Win11-25H2-Testbed-000011.vmdk v
ia aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to ass
ign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (353 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
26,284,032 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%4oper
ational.evtx      69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok NTUSER.DAT
2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1
393,216 bytes (exit 1)
    ok NTUSER.DAT.LOG2
0 bytes (exit 1)
    ok UsrClass.dat
2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1
0 bytes (exit 1)
    ok UsrClass.dat.LOG2

```

```

556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
    ok    SYSTEM
13,369,344 bytes (exit 1)
    ok    SOFTWARE
81,264,640 bytes (exit 1)
    ok    Amcache.hve
2,359,296 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario4_run2 acquisition complete
    Snapshot : scenario4_run2_post (DISS-Win11-25H2-Testbe
d-000011.vmdk)
    Mount    : AIM device 000000 at I: (dismounted)
    Files    : 367 (133.7 MB total)
    Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\sc
enario_4\run_2\artefacts\supporting\acquisition_manifes
t.csv

Landing zones:
    prefetch      353 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_4\run_2\artefacts\prefetch
    eventLogs      5 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_4\run_2\artefacts\event_logs
    shellbags      6 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_4\run_2\artefacts\shellbags
    supporting     3 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_4\run_2\artefacts\supporting
    evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_4\run_2\evaluation

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 4 -Run 2
[Acquire] scenario4_run2 offline acquisition starting (multi-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario4_run2_post' -> DISS-Win11-25H2-Testbed-000011.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2
[Acquire] Mounting DISS-Win11-25H2-Testbed-000011.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (353 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 26,284,032 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and Usrclass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 393,216 bytes (exit 1)
ok NTUSER.DAT.LOG2 0 bytes (exit 1)
ok UsrClass.dat 2,097,152 bytes (exit 1)
ok UsrClass.dat.LOG1 0 bytes (exit 1)
ok UsrClass.dat.LOG2 556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,369,344 bytes (exit 1)
ok SOFTWARE 81,264,640 bytes (exit 1)
ok Amcache.hve 2,359,296 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario4_run2 acquisition complete
Snapshot : scenario4_run2_post (DISS-Win11-25H2-Testbed-000011.vmdk)
Mount : AIM device 000000 at I: (dismounted)
Files : 367 (133.7 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 353 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\artefacts\prefetch
eventlogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\evaluation

```

RUN 3

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "USB attach
via VMWare Removable devices Connect"
A01 start 2026-08-22T21:00:15.5161211+00:00 USB attach v
ia VMWare Removable devices Connect
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-22T21:00:53.8302074+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Open Explo
rer, navigate to USB root"
A02 start 2026-08-22T21:01:07.7229492+00:00 Open Explo
r, navigate to USB root
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-22T21:01:30.0491603+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Navigate t
o \PORTABLE\ directory inside USB root"
A03 start 2026-08-22T21:01:51.1499791+00:00 Navigate to
\PORTABLE\ directory inside USB root
PS C:\WINDOWS\system32> Log-Action A03 end

```

```

A03 end 2026-08-22T21:02:22.9418681+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Launching
Helloworld exe from directory"
A04 start 2026-08-22T21:02:40.7948915+00:00 Launching He
llowworld exe from directory
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-22T21:03:01.1768956+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Eject USB
from Explorer"
A05 start 2026-08-22T21:03:10.5061649+00:00 Eject USB fr
om Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-22T21:03:31.8561588+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Disconnect
USB from guest in VMWare Removable Devices"
A06 start 2026-08-22T21:03:39.3021083+00:00 Disconnect U
SB from guest in VMWare Removable Devices
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-22T21:03:55.2412075+00:00
PS C:\WINDOWS\system32> Show-Log

```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-22T21:00:15.5161211+00:00	USB attac
			h via VMWare Removable devices Connect
A01	end	2026-08-22T21:00:53.8302074+00:00	
A02	start	2026-08-22T21:01:07.7229492+00:00	Open Expl
			orer, navigate to USB root
A02	end	2026-08-22T21:01:30.0491603+00:00	
A03	start	2026-08-22T21:01:51.1499791+00:00	Navigate
			to \PORTABLE\ directory inside USB root
A03	end	2026-08-22T21:02:22.9418681+00:00	
A04	start	2026-08-22T21:02:40.7948915+00:00	Launching
			Helloworld exe from directory
A04	end	2026-08-22T21:03:01.1768956+00:00	
A05	start	2026-08-22T21:03:10.5061649+00:00	Eject USB
			from Explorer
A05	end	2026-08-22T21:03:31.8561588+00:00	

```
A06      start 2026-08-22T21:03:39.3021083+00:00 Disconnect USB from guest in VMWare Removable Devices
A06      end    2026-08-22T21:03:55.2412075+00:00
```

```
PS C:\WINDOWS\system32> Save-Log -Scenario 4 -Run 3
Wrote 12 rows to C:\DISS_TESTDATA\scenario4_run3_action
s.csv
```

```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "USB attach via VMWare Removable devices Connect"
A01 start 2026-08-22T21:00:15.5161211+00:00 USB attach via VMWare Removable devices Connect
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-22T21:00:53.8302074+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Open Explorer, navigate to USB root"
A02 start 2026-08-22T21:01:07.7229492+00:00 Open Explorer, navigate to USB root
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-22T21:01:30.0491603+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Navigate to \PORTABLE\ directory inside USB root"
A03 start 2026-08-22T21:01:51.1499791+00:00 Navigate to \PORTABLE\ directory inside USB root
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-22T21:02:22.9418681+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Launching Hellowworld exe from directory"
A04 start 2026-08-22T21:02:40.7948915+00:00 Launching Hellowworld exe from directory
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-22T21:03:01.1768956+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Eject USB from Explorer"
A05 start 2026-08-22T21:03:10.5061649+00:00 Eject USB from Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-22T21:03:31.8561588+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Disconnect USB from guest in VMWare Removable Devices"
A06 start 2026-08-22T21:03:39.3021083+00:00 Disconnect USB from guest in VMWare Removable Devices
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-22T21:03:55.2412075+00:00
```

```
PS C:\WINDOWS\system32> Show-Log

Action Phase UTC                                     Note
-----
A01      start 2026-08-22T21:00:15.5161211+00:00 USB attach via VMWare Removable devices Connect
A01      end   2026-08-22T21:00:53.8302074+00:00
A02      start 2026-08-22T21:01:07.7229492+00:00 Open Explorer, navigate to USB root
A02      end   2026-08-22T21:01:30.0491603+00:00
A03      start 2026-08-22T21:01:51.1499791+00:00 Navigate to \PORTABLE\ directory inside USB root
A03      end   2026-08-22T21:02:22.9418681+00:00
A04      start 2026-08-22T21:02:40.7948915+00:00 Launching Hellowworld exe from directory
A04      end   2026-08-22T21:03:01.1768956+00:00
A05      start 2026-08-22T21:03:10.5061649+00:00 Eject USB from Explorer
A05      end   2026-08-22T21:03:31.8561588+00:00
A06      start 2026-08-22T21:03:39.3021083+00:00 Disconnect USB from guest in VMWare Removable Devices
A06      end   2026-08-22T21:03:55.2412075+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 4 -Run 3
Wrote 12 rows to C:\DISS_TESTDATA\scenario4_run3_actions.csv
PS C:\WINDOWS\system32>
```

```
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\a
cquire_artefacts.ps1 -Scenario 4 -Run 3
[Acquire] scenario4_run3 offline acquisition starting (m
ulti-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,
SeSecurityPrivilege
```

```
[Acquire] Resolved 'scenario4_run3_post' -> DISS-Win11-25H2-Testbed-000010.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3
[Acquire] Mounting DISS-Win11-25H2-Testbed-000010.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (349 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
26,284,032 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%4operational.evtx
69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
    ok NTUSER.DAT
2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1
0 bytes (exit 1)
    ok NTUSER.DAT.LOG2
642,048 bytes (exit 1)
    ok UsrClass.dat
2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1
0 bytes (exit 1)
    ok UsrClass.dat.LOG2
0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
```

```

    ok    SYSTEM
13,369,344 bytes (exit 1)
    ok    SOFTWARE
81,264,640 bytes (exit 1)
    ok    Amcache.hve
2,359,296 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario4_run3 acquisition complete
    Snapshot : scenario4_run3_post (DISS-Win11-25H2-Testbed-000010.vmdk)
    Mount      : AIM device 000000 at I: (dismounted)
    Files      : 363 (133.36 MB total)
    Manifest   : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\supporting\acquisition_manifest.csv

Landing zones:
    prefetch      349 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\prefetch
    eventLogs      5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\event_logs
    shellbags      6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\shellbags
    supporting      3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\supporting
    evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\evaluation

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\Acquire_artefacts.ps1 -Scenario 4 -Run 3
[Acquire] scenario4_run3 offline acquisition starting (multi-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario4_run3_post' -> DISS-Win11-25H2-Testbed-000010.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3
[Acquire] Mounting DISS-Win11-25H2-Testbed-000010.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (349 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx 26,284,032 bytes (exit 1)
    ok System.evtx 2,166,784 bytes (exit 1)
    ok Application.evtx 2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%40operational.evtx 69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
    ok NTUSER.DAT 2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1 0 bytes (exit 1)
    ok NTUSER.DAT.LOG2 642,048 bytes (exit 1)
    ok UsrClass.dat 2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1 0 bytes (exit 1)
    ok UsrClass.dat.LOG2 0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
    ok SYSTEM 13,369,344 bytes (exit 1)
    ok SOFTWARE 81,264,640 bytes (exit 1)
    ok Amcache.hve 2,359,296 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario4_run3 acquisition complete
Snapshot : scenario4_run3_post (DISS-Win11-25H2-Testbed-000010.vmdk)
Mount : AIM device 000000 at I: (dismounted)
Files : 363 (133.36 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 349 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\prefetch
eventlogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

▼ SCN5

```

PS C:\WINDOWS\system32> $root = 'C:\DISS_TESTDATA\scenario5_delete'
PS C:\WINDOWS\system32> $file = Join-Path $root 'scenario5_target.txt'
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> New-Item -ItemType Directory -Force -Path $root | Out-Null
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> $stagedUtc = (Get-Date).ToUniversalTime().ToString('o')
PS C:\WINDOWS\system32> $body = @(
>>     'Scenario 5 deletion target file.',
>>     "Staged (UTC): $stagedUtc",
>>     'This file is created by scenario5_prepare_file.ps1 before scenario execution.',
>>     'It is deleted to the Recycle Bin during A02 and permanently removed during A05.'
>> ) -join "`r`n"

```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-Content -Path $file -Value
$body -Encoding UTF8 -NoNewline
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Write-Host "Scenario 5 target st
aged at $file"
Scenario 5 target staged at C:\DISS_TESTDATA\scenario5_d
elete\scenario5_target.txt
PS C:\WINDOWS\system32> Get-Item $file | Select-Object F
ullName, Length, LastWriteTimeUtc

```

```

FullName                                     L
Length LastWriteTimeUtc
-----
-----
C:\DISS_TESTDATA\scenario5_delete\scenario5_target.txt
239 18/08/2026 08:24:25

```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> $sha = (Get-FileHash -Algorithm
SHA256 -Path $file).Hash
PS C:\WINDOWS\system32> Write-Host "SHA-256: $sha"
SHA-256: 1C35C35716B56C77AA468AA10EA252DCB1C5922200BB7CC
308E4076C43817E89
PS C:\WINDOWS\system32> Write-Host ""

```

```

PS C:\WINDOWS\system32> Write-Host "Record the following
in the ground_truth.csv (Note or ObservedOutcome colum
n):"
Record the following in the ground_truth.csv (Note or Ob
servedOutcome column):
PS C:\WINDOWS\system32> Write-Host "  StagedUTC : $stage
dUtc"
    StagedUTC : 2026-08-18T08:24:25.3992832Z
PS C:\WINDOWS\system32> Write-Host "  SHA256      : $sha"
    SHA256      : 1C35C35716B56C77AA468AA10EA252DCB1C5922200
BB7CC308E4076C43817E89

```

```

PS C:\WINDOWS\system32> $root = 'C:\DISS_TESTDATA\scenario5_delete'
PS C:\WINDOWS\system32> $file = Join-Path $root 'scenario5_target.txt'
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> New-Item -ItemType Directory -Force -Path $root | Out-Null
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> $stagedUtc = (Get-Date).ToUniversalTime().ToString('o')
PS C:\WINDOWS\system32> $body = @(
>> 'Scenario 5 deletion target file.',
>> "Staged (UTC): $stagedUtc",
>> 'This file is created by scenario5_prepare_file.ps1 before scenario execution.',
>> 'It is deleted to the Recycle Bin during A02 and permanently removed during A05.'
>> ) -join "`n"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-Content -Path $file -Value $body -Encoding UTF8 -NoNewline
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Write-Host "Scenario 5 target staged at $file"
Scenario 5 target staged at C:\DISS_TESTDATA\scenario5_delete\scenario5_target.txt
PS C:\WINDOWS\system32> Get-Item $file | Select-Object FullName, Length, LastWriteTimeUtc

FullName                                     Length LastWriteTimeUtc
-----
C:\DISS_TESTDATA\scenario5_delete\scenario5_target.txt 239 18/08/2026 08:24:25

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> $sha = (Get-FileHash -Algorithm SHA256 -Path $file).Hash
PS C:\WINDOWS\system32> Write-Host "SHA-256: $sha"
SHA-256: 1C35C35716B56C77AA468AA10EA252DCB1C5922200BB7CC308E4076C43817E89
PS C:\WINDOWS\system32> Write-Host ""

PS C:\WINDOWS\system32> Write-Host "Record the following in the ground_truth.csv (Note or ObservedOutcome column):"
Record the following in the ground_truth.csv (Note or ObservedOutcome column):
PS C:\WINDOWS\system32> Write-Host "  StagedUTC : $stagedUtc"
  StagedUTC : 2026-08-18T08:24:25.3992832Z
PS C:\WINDOWS\system32> Write-Host "  SHA256 : $sha"
  SHA256 : 1C35C35716B56C77AA468AA10EA252DCB1C5922200BB7CC308E4076C43817E89
PS C:\WINDOWS\system32>

```

```

PS C:\WINDOWS\system32> $script:log = @()
PS C:\WINDOWS\system32> function Log-Action {
>>     param([Parameter(Mandatory)][string]$id, [Parameter(Mandatory)][string]$phase, [string]$note = '')
>>     $ts = Get-Date -Format o
>>     $script:log += [PSCustomObject]@{ Action = $id; Phase = $phase; UTC = $ts; Note = $note }
>>     Write-Host "$id $phase $ts $note"
>> }
PS C:\WINDOWS\system32> function Save-Log {
>>     param([Parameter(Mandatory)][int]$Scenario, [int]$Run = 0, [string]$Path = 'C:\DISS_TESTDATA')
>>     if (-not (Test-Path $Path)) { New-Item -ItemType Directory -Path $Path -Force | Out-Null }
>>     $filename = if ($Run -eq 0) { "scenario${Scenario}_actions.csv" } else { "scenario${Scenario}_run${Run}_actions.csv" }
>>     $file = Join-Path $Path $filename
>>     $script:log | Export-Csv -Path $file -NoTypeInfo
>>     Write-Host "Wrote $($script:log.Count) rows to $file"
}

```

```
>> }
PS C:\WINDOWS\system32> function Show-Log { $script:log
| Format-Table -AutoSize }
```

```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> $script:log = @()
PS C:\WINDOWS\system32> function Log-Action {
>> param([Parameter(Mandatory)][string]$id, [Parameter(Mandatory)][string]$phase, [string]$note = '')
>> $ts = Get-Date -Format o
>> $script:log += [PSCustomObject]@{ Action = $id; Phase = $phase; UTC = $ts; Note = $note }
>> Write-Host "$id $phase $ts $note"
>> }
PS C:\WINDOWS\system32> function Save-Log {
>> param([Parameter(Mandatory)][int]$Scenario, [int]$Run = 0, [string]$Path = 'C:\DISS_TESTDATA')
>> if (-not (Test-Path $Path)) { New-Item -ItemType Directory -Path $Path -Force | Out-Null }
>> $filename = if ($Run -eq 0) { "scenario${Scenario}_actions.csv" } else { "scenario${Scenario}_run${Run}_actions.csv" }
>> $file = Join-Path $Path $filename
>> $script:log | Export-Csv -Path $file -NoTypeInformation
>> Write-Host "Wrote $($script:log.Count) rows to $file"
>> }
PS C:\WINDOWS\system32> function Show-Log { $script:log | Format-Table -AutoSize }
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32> $root = 'C:\DISS_TESTDATA\scenario5_delete'
PS C:\WINDOWS\system32> $file = Join-Path $root 'scenario5_target.txt'
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> New-Item -ItemType Directory -Force -Path $root | Out-Null
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> $stagedUtc = (Get-Date).ToUniversalTime().ToString('o')
PS C:\WINDOWS\system32> $body = @(
>> 'Scenario 5 deletion target file.',
>> "Staged (UTC): $stagedUtc",
>> 'This file is created by scenario5_prepare_file.ps1 before scenario execution.',
>> 'It is deleted to the Recycle Bin during A02 and permanently removed during A05.'
>> ) -join "`r`n"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Set-Content -Path $file -Value $body -Encoding UTF8 -NoNewline
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Write-Host "Scenario 5 target staged at $file"
```

Scenario 5 target staged at C:\DISS_TESTDATA\scenario5_delete\scenario5_target.txt

```
PS C:\WINDOWS\system32> Get-Item $file | Select-Object FullName, Length, LastWriteUtc
```

```
FullName                                                    L
Length LastWriteUtc
-----
-----
C:\DISS_TESTDATA\scenario5_delete\scenario5_target.txt
239 18/08/2026 08:24:25
```

```
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32> $sha = (Get-FileHash -Algorithm SHA256 -Path $file).Hash
```

```
PS C:\WINDOWS\system32> Write-Host "SHA-256: $sha"
```

```
SHA-256: 1C35C35716B56C77AA468AA10EA252DCB1C5922200BB7CC308E4076C43817E89
```

```
PS C:\WINDOWS\system32> Write-Host ""
```

```
PS C:\WINDOWS\system32> Write-Host "Record the following in the ground_truth.csv (Note or ObservedOutcome column):"
```

```
Record the following in the ground_truth.csv (Note or ObservedOutcome column):
```

```
PS C:\WINDOWS\system32> Write-Host "  StagedUTC : $stage dUtc"
```

```
    StagedUTC : 2026-08-18T08:24:25.3992832Z
```

```
PS C:\WINDOWS\system32> Write-Host "  SHA256      : $sha"
```

```
    SHA256      : 1C35C35716B56C77AA468AA10EA252DCB1C5922200BB7CC308E4076C43817E89
```

```
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32>
```

```
PS C:\WINDOWS\system32> $script:log = @()
```

```
PS C:\WINDOWS\system32> function Log-Action {
```

```
>>     param([Parameter(Mandatory)][string]$id, [Paramet
```

```

er(Mandatory)][string]$phase, [string]$note = '')
>>     $ts = Get-Date -Format o
>>     $script:log += [PSCustomObject]@{ Action = $id; Phase = $phase; UTC = $ts; Note = $note }
>>     Write-Host "$id $phase $ts $note"
>> }
PS C:\WINDOWS\system32> function Save-Log {
>>     param([Parameter(Mandatory)][int]$Scenario, [int]$Run = 0, [string]$Path = 'C:\DISS_TESTDATA')
>>     if (-not (Test-Path $Path)) { New-Item -ItemType Directory -Path $Path -Force | Out-Null }
>>     $filename = if ($Run -eq 0) { "scenario${Scenario}_actions.csv" } else { "scenario${Scenario}_run${Run}_actions.csv" }
>>     $file = Join-Path $Path $filename
>>     $script:log | Export-Csv -Path $file -NoTypeInfo
>>     Write-Host "Wrote $($script:log.Count) rows to $file"
>> }
PS C:\WINDOWS\system32> function Show-Log { $script:log | Format-Table -AutoSize }
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Open Explorer, navigate to C:\DISS_TESTDATA\scenario5_delete"
A01 start 2026-08-18T08:28:55.0928112+00:00 Open Explorer, navigate to C:\DISS_TESTDATA\scenario5_delete
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-18T08:29:23.8882133+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Delete scenario_5_target.ttx file to recycle Bin"
A02 start 2026-08-18T08:29:59.2350831+00:00 Delete scenario_5_target.ttx file to recycle Bin
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-18T08:30:21.2951788+00:00

```

```

PS C:\WINDOWS\system32> Log-Action A03 start "Open recycle Bin from Desktop"
A03 start 2026-08-18T08:30:48.4415559+00:00 Open recycle Bin from Desktop
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-18T08:31:05.5195679+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Empty Recycle bin"
A04 start 2026-08-18T08:32:13.2597613+00:00 Empty Recycle bin
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-18T08:32:30.3289214+00:00
PS C:\WINDOWS\system32> Show-log

```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-18T08:28:55.0928112+00:00	Open Explorer, navigate to C:\DISS_TESTDATA\scenario5_delete
A01	end	2026-08-18T08:29:23.8882133+00:00	
A02	start	2026-08-18T08:29:59.2350831+00:00	Delete scenario_5_target.ttx file to recycle Bin
A02	end	2026-08-18T08:30:21.2951788+00:00	
A03	start	2026-08-18T08:30:48.4415559+00:00	Open recycle Bin from Desktop
A03	end	2026-08-18T08:31:05.5195679+00:00	
A04	start	2026-08-18T08:32:13.2597613+00:00	Empty Recycle bin
A04	end	2026-08-18T08:32:30.3289214+00:00	

```

PS C:\WINDOWS\system32> Save-Log -Scenario 5
Wrote 8 rows to C:\DISS_TESTDATA\scenario5_actions.csv

```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Open Explorer, navigate to C:\DISS_TESTDATA\scenario5_delete"
A01 start 2026-08-18T08:28:55.0928112+00:00 Open Explorer, navigate to C:\DISS_TESTDATA\scenario5_delete
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-18T08:29:23.8882133+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Delete scenario_5_target.ttx file to recycle Bin"
A02 start 2026-08-18T08:29:59.2350831+00:00 Delete scenario_5_target.ttx file to recycle Bin
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-18T08:30:21.2951788+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Open recycle Bin from Desktop"
A03 start 2026-08-18T08:30:48.4415559+00:00 Open recycle Bin from Desktop
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-18T08:31:05.5195679+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Empty Recycle bin"
A04 start 2026-08-18T08:32:13.2597613+00:00 Empty Recycle bin
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-18T08:32:30.3289214+00:00
PS C:\WINDOWS\system32> Show-log

Action Phase UTC                                     Note
-----
A01 start 2026-08-18T08:28:55.0928112+00:00 Open Explorer, navigate to C:\DISS_TESTDATA\scenario5_delete
A01 end 2026-08-18T08:29:23.8882133+00:00
A02 start 2026-08-18T08:29:59.2350831+00:00 Delete scenario_5_target.ttx file to recycle Bin
A02 end 2026-08-18T08:30:21.2951788+00:00
A03 start 2026-08-18T08:30:48.4415559+00:00 Open recycle Bin from Desktop
A03 end 2026-08-18T08:31:05.5195679+00:00
A04 start 2026-08-18T08:32:13.2597613+00:00 Empty Recycle bin
A04 end 2026-08-18T08:32:30.3289214+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 5
Wrote 8 rows to C:\DISS_TESTDATA\scenario5_actions.csv
PS C:\WINDOWS\system32>

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\a
cquire_artefacts.ps1 -Scenario 5
[Acquire] scenario5 offline acquisition starting (single
-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,
SeSecurityPrivilege
[Acquire] Resolved 'scenario5_post' -> DISS-Win11-25H2-T
estbed-0000005.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\s
cenarios\scenario_5
[Acquire] Mounting DISS-Win11-25H2-Testbed-0000005.vmdk v
ia aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to ass
ign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (347 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
26,284,032 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)

```

```

    ok    Microsoft-Windows-DriverFrameworks-UserMode%40per
ational.evtx          69,632 bytes (exit 1)
    ok    Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok    NTUSER.DAT
2,359,296 bytes (exit 1)
    ok    NTUSER.DAT.LOG1
0 bytes (exit 1)
    ok    NTUSER.DAT.LOG2
0 bytes (exit 1)
    ok    UsrClass.dat
2,097,152 bytes (exit 1)
    ok    UsrClass.dat.LOG1
118,784 bytes (exit 1)
    ok    UsrClass.dat.LOG2
0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
    ok    SYSTEM
13,369,344 bytes (exit 1)
    ok    SOFTWARE
81,264,640 bytes (exit 1)
    ok    Amcache.hve
2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario5 acquisition complete
    Snapshot : scenario5_post (DISS-Win11-25H2-Testbed-000
005.vmdk)
    Mount    : AIM device 000000 at H: (dismounted)
    Files    : 361 (133.08 MB total)
    Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\sc
enario_5\artefacts\supporting\acquisition_manifest.csv

Landing zones:
    prefetch    347 files -> D:\UOW\SEM3\msc-diss-7csef00

```

```

1w\scenarios\scenario_5\artefacts\prefetch
    eventLogs          5 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_5\artefacts\event_logs
    shellbags          6 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_5\artefacts\shellbags
    supporting          3 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_5\artefacts\supporting
    evaluation (dir)    -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_5\evaluation
PS D:\UOW\SEM3\msc-diss-7csef00\scripts\scenarios>

```

```

PS D:\UOW\SEM3\msc-diss-7csef00\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 5
[Acquire] scenario5 offline acquisition starting (single-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario5_post' -> DISS-Win11-25H2-Testbed-000005.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef00\scenarios\scenario_5
[Acquire] Mounting DISS-Win11-25H2-Testbed-000005.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (347 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx                26,284,032 bytes (exit 1)
    ok System.evtx                  2,166,784 bytes (exit 1)
    ok Application.evtx             2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode\40Operational.evtx 69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition\4Diagnostic.evtx             69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UserClass.dat + transaction logs)
    ok NTUSER.DAT                   2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1              0 bytes (exit 1)
    ok NTUSER.DAT.LOG2              0 bytes (exit 1)
    ok UserClass.dat                2,097,152 bytes (exit 1)
    ok UserClass.dat.LOG1           118,784 bytes (exit 1)
    ok UserClass.dat.LOG2           0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
    ok SYSTEM                       13,369,344 bytes (exit 1)
    ok SOFTWARE                     81,264,640 bytes (exit 1)
    ok Amcache.hve                  2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario5 acquisition complete
    Snapshot : scenario5_post (DISS-Win11-25H2-Testbed-000005.vmdk)
    Mount : AIM device 000000 at H: (dismounted)
    Files : 361 (133.08 MB total)
    Manifest : D:\UOW\SEM3\msc-diss-7csef00\scenarios\scenario_5\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch      347 files -> D:\UOW\SEM3\msc-diss-7csef00\scenarios\scenario_5\artefacts\prefetch
eventLogs     5 files -> D:\UOW\SEM3\msc-diss-7csef00\scenarios\scenario_5\artefacts\event_logs
shellbags     6 files -> D:\UOW\SEM3\msc-diss-7csef00\scenarios\scenario_5\artefacts\shellbags
supporting    3 files -> D:\UOW\SEM3\msc-diss-7csef00\scenarios\scenario_5\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef00\scenarios\scenario_5\evaluation
PS D:\UOW\SEM3\msc-diss-7csef00\scripts\scenarios>

```

▼ SCN6

scenario6_actions.csv: 14 rows at C:\DISS_TESTDATA\scenario6_actions.csv

Action Phase UTC

Note

```

-----
A01    start 2026-08-18T16:01:16.4425738+00:00 sign out
A01    end   2026-08-18T16:03:04.5888220+00:00
A02    start 2026-08-18T16:03:13.9407560+00:00 sign in
A02    end   2026-08-18T16:03:19.2614473+00:00
A03    start 2026-08-18T16:03:58.4140382+00:00 lock
A03    end   2026-08-18T16:04:10.4977752+00:00
A04    start 2026-08-18T16:06:11.4983459+00:00 waited  1
0+ s
A04    end   2026-08-18T16:06:19.7487530+00:00
A05    start 2026-08-18T16:06:25.7417692+00:00 unlock
A05    end   2026-08-18T16:06:31.2554635+00:00
A06    start 2026-08-18T16:06:37.5681022+00:00 sign out
again
A06    end   2026-08-18T16:07:48.0474197+00:00
A07    start 2026-08-18T16:07:53.2762345+00:00 sign in
A07    end   2026-08-18T16:07:57.3376702+00:00

```

```

Copyright (C) Microsoft Corporation. All Rights Reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\WINDOWS\system32> Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass -Force
PS C:\WINDOWS\system32> . C:\DISS_TESTDATA\scenario6_log.ps1
PS C:\WINDOWS\system32> Log-Action6 A06 end
A06 end 2026-08-18T16:07:48.0474197+00:00
PS C:\WINDOWS\system32> Log-Action6 A07 start "sign in"
A07 start 2026-08-18T16:07:53.2762345+00:00 sign in
PS C:\WINDOWS\system32> Log-Action6 A07 end
A07 end 2026-08-18T16:07:57.3376702+00:00
PS C:\WINDOWS\system32> Finalise-Scenario6Log
scenario6_actions.csv: 14 rows at C:\DISS_TESTDATA\scenario6_actions.csv

```

Action	Phase	UTC	Note
A01	start	2026-08-18T16:01:16.4425738+00:00	sign out
A01	end	2026-08-18T16:03:04.5888220+00:00	
A02	start	2026-08-18T16:03:13.9407560+00:00	sign in
A02	end	2026-08-18T16:03:19.2614473+00:00	
A03	start	2026-08-18T16:03:58.4140382+00:00	lock
A03	end	2026-08-18T16:04:10.4977752+00:00	
A04	start	2026-08-18T16:06:11.4983459+00:00	waited 10+ s
A04	end	2026-08-18T16:06:19.7487530+00:00	
A05	start	2026-08-18T16:06:25.7417692+00:00	unlock
A05	end	2026-08-18T16:06:31.2554635+00:00	
A06	start	2026-08-18T16:06:37.5681022+00:00	sign out again
A06	end	2026-08-18T16:07:48.0474197+00:00	
A07	start	2026-08-18T16:07:53.2762345+00:00	sign in
A07	end	2026-08-18T16:07:57.3376702+00:00	

```
PS C:\WINDOWS\system32> _
```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\a
cquire_artefacts.ps1 -Scenario 6
[Acquire] scenario6 offline acquisition starting (single
-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,

```

```
SeSecurityPrivilege
[Acquire] Resolved 'scenario6_post' -> DISS-Win11-25H2-Testbed-000007.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_6
[Acquire] Mounting DISS-Win11-25H2-Testbed-000007.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (365 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
26,284,032 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%4operational.evtx
69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
    ok NTUSER.DAT
2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1
0 bytes (exit 1)
    ok NTUSER.DAT.LOG2
613,376 bytes (exit 1)
    ok UsrClass.dat
2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1
556,032 bytes (exit 1)
    ok UsrClass.dat.LOG2
556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
```

```

cache.hve
  ok    SYSTEM
13,369,344 bytes (exit 1)
  ok    SOFTWARE
81,264,640 bytes (exit 1)
  ok    Amcache.hve
2,359,296 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario6 acquisition complete
  Snapshot : scenario6_post (DISS-Win11-25H2-Testbed-000
007.vmdk)
  Mount    : AIM device 000000 at H: (dismounted)
  Files    : 379 (134.68 MB total)
  Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\sc
enario_6\artefacts\supporting\acquisition_manifest.csv

Landing zones:
  prefetch      365 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_6\artefacts\prefetch
  eventLogs     5 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_6\artefacts\event_logs
  shellbags     6 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_6\artefacts\shellbags
  supporting    3 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_6\artefacts\supporting
  evaluation (dir)      -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_6\evaluation

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 6
[Acquire] scenario6 offline acquisition starting (single-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario6_post' -> DISS-Win11-25H2-Testbed-000007.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_6
[Acquire] Mounting DISS-Win11-25H2-Testbed-000007.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (365 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 26,284,032 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 0 bytes (exit 1)
ok NTUSER.DAT.LOG2 613,376 bytes (exit 1)
ok UsrClass.dat 2,097,152 bytes (exit 1)
ok UsrClass.dat.LOG1 556,032 bytes (exit 1)
ok UsrClass.dat.LOG2 556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,369,344 bytes (exit 1)
ok SOFTWARE 81,264,640 bytes (exit 1)
ok Amcache.hve 2,359,296 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario6 acquisition complete
Snapshot : scenario6_post (DISS-Win11-25H2-Testbed-000007.vmdk)
Mount : AIM device 000000 at H: (dismounted)
Files : 379 (134.68 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_6\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 365 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_6\artefacts\prefetch
eventlogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_6\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_6\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_6\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_6\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

▼ SCN7

| RUN 1

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch Notepad++ from Start"
A01 start 2026-08-23T00:12:41.8472939+00:00 Launch Notepad++ from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-23T00:13:11.3463174+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Type Scenario 7 test content with UTC marker"
A02 start 2026-08-23T00:13:46.1641971+00:00 Type Scenario 7 test content with UTC marker

```

```

PS C:\WINDOWS\system32> [DateTime]::UtcNow.ToString("o")
2026-08-23T00:13:50.9282394Z
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-23T00:14:45.5349817+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "File menu,
Save As"
A03 start 2026-08-23T00:16:00.4150626+00:00 File menu, S
ave As
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-23T00:16:43.1342829+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Closing No
tepad++"
A04 start 2026-08-23T00:17:00.1499416+00:00 Closing Note
pad++
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-23T00:17:12.1615278+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Opening Do
cuments folder using File Explorer"
A05 start 2026-08-23T00:17:51.5442012+00:00 Opening Docu
ments folder using File Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-23T00:18:09.2064932+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Viewing th
e file created"
A06 start 2026-08-23T00:18:29.3549913+00:00 Viewing the
file created
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-23T00:18:42.8143908+00:00
PS C:\WINDOWS\system32> Log-Action "Closing File explore
r and Applications"

```

```

cmdlet Log-Action at command pipeline position 1
Supply values for the following parameters:
phase:
Log-Action : Cannot bind argument to parameter 'phase' b
ecause it is an empty string.
At line:1 char:1
+ Log-Action "Closing File explorer and Applications"

```

```
+ ~~~~~
+ CategoryInfo          : InvalidData: (:) [Log-Action], ParameterBindingValidationException
+ FullyQualifiedErrorId : ParameterArgumentValidationErrorEmptyStringNotAllowed,Log-Action
```

```
PS C:\WINDOWS\system32> Log-Action A07 start "Closing File explorer and Applications"
```

```
A07 start 2026-08-23T00:19:29.1974677+00:00 Closing File explorer and Applications
```

```
PS C:\WINDOWS\system32> Log-Action A07 end
```

```
A07 end 2026-08-23T00:19:44.8953935+00:00
```

```
PS C:\WINDOWS\system32> Show-Log
```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-23T00:12:41.8472939+00:00	Launch Notepad++ from Start
A01	end	2026-08-23T00:13:11.3463174+00:00	
A02	start	2026-08-23T00:13:46.1641971+00:00	Type Scenario 7 test content with UTC marker
A02	end	2026-08-23T00:14:45.5349817+00:00	
A03	start	2026-08-23T00:16:00.4150626+00:00	File menu, Save As
A03	end	2026-08-23T00:16:43.1342829+00:00	
A04	start	2026-08-23T00:17:00.1499416+00:00	Closing Notepad++
A04	end	2026-08-23T00:17:12.1615278+00:00	
A05	start	2026-08-23T00:17:51.5442012+00:00	Opening Documents folder using File Explorer
A05	end	2026-08-23T00:18:09.2064932+00:00	
A06	start	2026-08-23T00:18:29.3549913+00:00	Viewing the file created
A06	end	2026-08-23T00:18:42.8143908+00:00	
A07	start	2026-08-23T00:19:29.1974677+00:00	Closing File explorer and Applications
A07	end	2026-08-23T00:19:44.8953935+00:00	

```
PS C:\WINDOWS\system32> Save-Log -Scenario 7 -Run 1
Wrote 14 rows to C:\DISS_TESTDATA\scenario7_run1_action
S.CSV
```

```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch Notepad++ from Start"
A01 start 2026-08-23T00:12:41.8472939+00:00 Launch Notepad++ from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-23T00:13:11.3463174+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Type Scenario 7 test content with UTC marker"
A02 start 2026-08-23T00:13:46.1641971+00:00 Type Scenario 7 test content with UTC marker
PS C:\WINDOWS\system32> [DateTime]::UtcNow.ToString("o")
2026-08-23T00:13:50.9282394Z
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-23T00:14:45.5349817+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "File menu, Save As"
A03 start 2026-08-23T00:16:00.4150626+00:00 File menu, Save As
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-23T00:16:43.1342829+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Closing Notepad++"
A04 start 2026-08-23T00:17:00.1499416+00:00 Closing Notepad++
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-23T00:17:12.1615278+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Opening Documents folder using File Explorer"
A05 start 2026-08-23T00:17:51.5442012+00:00 Opening Documents folder using File Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-23T00:18:09.2064932+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Viewing the file created"
A06 start 2026-08-23T00:18:29.3549913+00:00 Viewing the file created
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-23T00:18:42.8143908+00:00
PS C:\WINDOWS\system32> Log-Action "Closing File explorer and Applications"

cmdlet Log-Action at command pipeline position 1
Supply values for the following parameters:
phase:
Log-Action : Cannot bind argument to parameter 'phase' because it is an empty string.
At line:1 char:1
+ Log-Action "Closing File explorer and Applications"
+ ~~~~~
+ CategoryInfo          : InvalidData: (:) [Log-Action], ParameterBindingValidationException
+ FullyQualifiedErrorId : ParameterArgumentValidationErrorEmptyStringNotAllowed,Log-Action

PS C:\WINDOWS\system32> Log-Action A07 start "Closing File explorer and Applications"
A07 start 2026-08-23T00:19:29.1974677+00:00 Closing File explorer and Applications
PS C:\WINDOWS\system32> Log-Action A07 end
```

```
PS C:\WINDOWS\system32> Show-Log

Action Phase UTC Note
-----
A01 start 2026-08-23T00:12:41.8472939+00:00 Launch Notepad++ from Start
A01 end 2026-08-23T00:13:11.3463174+00:00
A02 start 2026-08-23T00:13:46.1641971+00:00 Type Scenario 7 test content with UTC marker
A02 end 2026-08-23T00:14:45.5349817+00:00
A03 start 2026-08-23T00:16:00.4150626+00:00 File menu, Save As
A03 end 2026-08-23T00:16:43.1342829+00:00
A04 start 2026-08-23T00:17:00.1499416+00:00 Closing Notepad++
A04 end 2026-08-23T00:17:12.1615278+00:00
A05 start 2026-08-23T00:17:51.5442012+00:00 Opening Documents folder using File Explorer
A05 end 2026-08-23T00:18:09.2064932+00:00
A06 start 2026-08-23T00:18:29.3549913+00:00 Viewing the file created
A06 end 2026-08-23T00:18:42.8143908+00:00
A07 start 2026-08-23T00:19:29.1974677+00:00 Closing File explorer and Applications
A07 end 2026-08-23T00:19:44.8953935+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 7 -Run 1
Wrote 14 rows to C:\DISS_TESTDATA\scenario7_run1_actions.csv
PS C:\WINDOWS\system32>
```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\a
cquire_artefacts.ps1 -Scenario 7 -Run 1
[Acquire] scenario7_run1 offline acquisition starting (m
ulti-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,
SeSecurityPrivilege
[Acquire] Resolved 'scenario7_run1_post' -> DISS-Win11-2
5H2-Testbed-000013.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\s
cenarios\scenario_7\run_1
[Acquire] Mounting DISS-Win11-25H2-Testbed-000013.vmdk v
ia aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to ass
ign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (435 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
28,381,184 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%40per
ational.evtx 69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok NTUSER.DAT
2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1
0 bytes (exit 1)
    ok NTUSER.DAT.LOG2
0 bytes (exit 1)
    ok UsrClass.dat
2,097,152 bytes (exit 1)

```

```

    ok    UsrClass.dat.LOG1
131,072 bytes (exit 1)
    ok    UsrClass.dat.LOG2
0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
    ok    SYSTEM
13,631,488 bytes (exit 1)
    ok    SOFTWARE
82,051,072 bytes (exit 1)
    ok    Amcache.hve
2,883,584 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario7_run1 acquisition complete
    Snapshot : scenario7_run1_post (DISS-Win11-25H2-Testbe
d-000013.vmdk)
    Mount    : AIM device 000000 at I: (dismounted)
    Files    : 449 (138.24 MB total)
    Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\sc
enario_7\run_1\artefacts\supporting\acquisition_manifes
t.csv

Landing zones:
    prefetch    435 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_1\artefacts\prefetch
    eventLogs    5 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_1\artefacts\event_logs
    shellbags    6 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_1\artefacts\shellbags
    supporting    3 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_1\artefacts\supporting
    evaluation (dir)    -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_1\evaluation

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 7 -Run 1
[Acquire] scenario7_run1 offline acquisition starting (multi-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario7_run1_post' -> DISS-Win11-25H2-Testbed-000013.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1
[Acquire] Mounting DISS-Win11-25H2-Testbed-000013.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (435 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx 28,381,184 bytes (exit 1)
    ok System.evtx 2,166,784 bytes (exit 1)
    ok Application.evtx 2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
    ok NTUSER.DAT 2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1 0 bytes (exit 1)
    ok NTUSER.DAT.LOG2 0 bytes (exit 1)
    ok UsrClass.dat 2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1 131,072 bytes (exit 1)
    ok UsrClass.dat.LOG2 0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
    ok SYSTEM 13,631,488 bytes (exit 1)
    ok SOFTWARE 82,051,072 bytes (exit 1)
    ok Amcache.hve 2,883,584 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario7_run1 acquisition complete
Snapshot : scenario7_run1_post (DISS-Win11-25H2-Testbed-000013.vmdk)
Mount : AIM device 000000 at I: (dismounted)
Files : 449 (138.24 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 435 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\artefacts\prefetch
eventlogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

RUN 2

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch Notepad++ from Start"
A01 start 2026-08-23T00:44:57.2501249+00:00 Launch Notepad++ from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-23T00:45:16.0593664+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Type Scenario 7 test content with UTC marker"
A02 start 2026-08-23T00:45:24.9437676+00:00 Type Scenario 7 test content with UTC marker
PS C:\WINDOWS\system32> [DateTime]::UtcNow.ToString("o")
2026-08-23T00:45:30.7524214Z
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-23T00:46:12.6501306+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "File menu,

```

```

Save As in Docuemts folder"
A03 start 2026-08-23T00:46:28.5554324+00:00 File menu, S
ave As in Docuemts folder
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-23T00:47:11.6984992+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Closing No
tepad++"
A04 start 2026-08-23T00:47:18.7779816+00:00 Closing Note
pad++
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-23T00:47:27.3329881+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Opening Do
cuments folder using File Explorer"
A05 start 2026-08-23T00:47:37.3494337+00:00 Opening Docu
ments folder using File Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-23T00:47:43.3238789+00:00
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-23T00:48:03.8506739+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Viewing th
e file created"
A06 start 2026-08-23T00:48:12.9043877+00:00 Viewing the
file created
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-23T00:48:28.2100048+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Closing F
ile explorer and Applications"
A07 start 2026-08-23T00:48:41.2656526+00:00 Closing File
explorer and Applications
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-23T00:48:52.2702621+00:00
PS C:\WINDOWS\system32> Show-Log

```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-23T00:44:57.2501249+00:00	Launch No tepad++ from Start
A01	end	2026-08-23T00:45:16.0593664+00:00	

A02 start 2026-08-23T00:45:24.9437676+00:00 Type Scenario 7 test content with UTC marker
A02 end 2026-08-23T00:46:12.6501306+00:00
A03 start 2026-08-23T00:46:28.5554324+00:00 File menu, Save As in Documents folder
A03 end 2026-08-23T00:47:11.6984992+00:00
A04 start 2026-08-23T00:47:18.7779816+00:00 Closing Notepad++
A04 end 2026-08-23T00:47:27.3329881+00:00
A05 start 2026-08-23T00:47:37.3494337+00:00 Opening Documents folder using File Explorer
A05 end 2026-08-23T00:47:43.3238789+00:00
A05 end 2026-08-23T00:48:03.8506739+00:00
A06 start 2026-08-23T00:48:12.9043877+00:00 Viewing the file created
A06 end 2026-08-23T00:48:28.2100048+00:00
A07 start 2026-08-23T00:48:41.2656526+00:00 Closing File explorer and Applications
A07 end 2026-08-23T00:48:52.2702621+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 7 -Run 2
Wrote 15 rows to C:\DISS_TESTDATA\scenario7_run2_actions.csv

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch Notepad++ from Start"
A01 start 2026-08-23T00:44:57.2501249+00:00 Launch Notepad++ from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-23T00:45:16.0593664+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Type Scenario 7 test content with UTC marker"
A02 start 2026-08-23T00:45:24.9437676+00:00 Type Scenario 7 test content with UTC marker
PS C:\WINDOWS\system32> [DateTime]::UtcNow.ToString("o")
2026-08-23T00:45:30.7524214Z
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-23T00:46:12.6501306+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "File menu, Save As in Docuemts folder"
A03 start 2026-08-23T00:46:28.5554324+00:00 File menu, Save As in Docuemts folder
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-23T00:47:11.6984992+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Closing Notepad++"
A04 start 2026-08-23T00:47:18.7779816+00:00 Closing Notepad++
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-23T00:47:27.3329881+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Opening Documents folder using File Explorer"
A05 start 2026-08-23T00:47:37.3494337+00:00 Opening Documents folder using File Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-23T00:47:43.3238789+00:00
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-23T00:48:03.8506739+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Viewing the file created"
A06 start 2026-08-23T00:48:12.9043877+00:00 Viewing the file created
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-23T00:48:28.2100048+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Closing File explorer and Applications"
A07 start 2026-08-23T00:48:41.2656526+00:00 Closing File explorer and Applications
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-23T00:48:52.2702621+00:00

```

```

PS C:\WINDOWS\system32> Show-Log

Action Phase UTC Note
-----
A01 start 2026-08-23T00:44:57.2501249+00:00 Launch Notepad++ from Start
A01 end 2026-08-23T00:45:16.0593664+00:00
A02 start 2026-08-23T00:45:24.9437676+00:00 Type Scenario 7 test content with UTC marker
A02 end 2026-08-23T00:46:12.6501306+00:00
A03 start 2026-08-23T00:46:28.5554324+00:00 File menu, Save As in Docuemts folder
A03 end 2026-08-23T00:47:11.6984992+00:00
A04 start 2026-08-23T00:47:18.7779816+00:00 Closing Notepad++
A04 end 2026-08-23T00:47:27.3329881+00:00
A05 start 2026-08-23T00:47:37.3494337+00:00 Opening Documents folder using File Explorer
A05 end 2026-08-23T00:47:43.3238789+00:00
A05 end 2026-08-23T00:48:03.8506739+00:00
A06 start 2026-08-23T00:48:12.9043877+00:00 Viewing the file created
A06 end 2026-08-23T00:48:28.2100048+00:00
A07 start 2026-08-23T00:48:41.2656526+00:00 Closing File explorer and Applications
A07 end 2026-08-23T00:48:52.2702621+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 7 -Run 2
Wrote 15 rows to C:\DISS_TESTDATA\scenario7_run2_actions.csv
PS C:\WINDOWS\system32>

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\a
cquire_artefacts.ps1 -Scenario 7 -Run 2
[Acquire] scenario7_run2 offline acquisition starting (m
ulti-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,
SeSecurityPrivilege
[Acquire] Resolved 'scenario7_run2_post' -> DISS-Win11-2
5H2-Testbed-000014.vmdk

```

```
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\s
cenarios\scenario_7\run_2
[Acquire] Mounting DISS-Win11-25H2-Testbed-000014.vmdk v
ia aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to ass
ign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (435 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
28,381,184 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%40per
ational.evtx 69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok NTUSER.DAT
2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1
0 bytes (exit 1)
    ok NTUSER.DAT.LOG2
0 bytes (exit 1)
    ok UsrClass.dat
2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1
0 bytes (exit 1)
    ok UsrClass.dat.LOG2
556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
    ok SYSTEM
13,631,488 bytes (exit 1)
```

```

    ok    SOFTWARE
82,051,072 bytes (exit 1)
    ok    Amcache.hve
2,883,584 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario7_run2 acquisition complete
    Snapshot : scenario7_run2_post (DISS-Win11-25H2-Testbed-000014.vmdk)
    Mount      : AIM device 000000 at I: (dismounted)
    Files      : 449 (138.65 MB total)
    Manifest   : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\supporting\acquisition_manifest.csv

Landing zones:
    prefetch      435 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\prefetch
    eventLogs      5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\event_logs
    shellbags      6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\shellbags
    supporting      3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\supporting
    evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 7 -Run 2
[Acquire] scenario7_run2 offline acquisition starting (multi-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario7_run2_post' -> DISS-Win11-25H2-Testbed-000014.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2
[Acquire] Mounting DISS-Win11-25H2-Testbed-000014.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (435 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 28,381,184 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 0 bytes (exit 1)
ok NTUSER.DAT.LOG2 0 bytes (exit 1)
ok UsrClass.dat 2,097,152 bytes (exit 1)
ok UsrClass.dat.LOG1 0 bytes (exit 1)
ok UsrClass.dat.LOG2 556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,631,488 bytes (exit 1)
ok SOFTWARE 82,051,072 bytes (exit 1)
ok Amcache.hve 2,883,584 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario7_run2 acquisition complete
Snapshot : scenario7_run2_post (DISS-Win11-25H2-Testbed-000014.vmdk)
Mount : AIM device 000000 at I: (dismounted)
Files : 449 (138.65 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 435 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\prefetch
eventlogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

RUN 3

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch Notepad++ from Start"
A01 start 2026-08-23T01:37:10.1304310+00:00 Launch Notepad++ from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-23T01:37:36.8891773+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Type Scenario 7 test content with UTC marker"
A02 start 2026-08-23T01:37:48.3483141+00:00 Type Scenario 7 test content with UTC marker
PS C:\WINDOWS\system32> [DateTime]::UtcNow.ToString("o")
2026-08-23T01:37:55.7549893Z
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-23T01:38:25.0915857+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "File menu, Save As in Documents folder"

```

```

A03 start 2026-08-23T01:38:37.6191033+00:00 File menu, S
ave As in Docuemts folder
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-23T01:39:37.8602035+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Closing No
tepad++"
A04 start 2026-08-23T01:39:47.1060939+00:00 Closing Note
pad++
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-23T01:40:00.4118549+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Opening Do
cuments folder using File Explorer"
A05 start 2026-08-23T01:40:11.7039072+00:00 Opening Docu
ments folder using File Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-23T01:40:33.2715870+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Viewing th
e file created"
A06 start 2026-08-23T01:40:45.3515071+00:00 Viewing the
file created
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-23T01:40:57.2474867+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Closing Fi
le explorer and Applications"
A07 start 2026-08-23T01:41:06.9556496+00:00 Closing File
explorer and Applications
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-23T01:41:25.5465528+00:00
PS C:\WINDOWS\system32> Show-Log

```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-23T01:37:10.1304310+00:00	Launch No
			tepad++ from Start
A01	end	2026-08-23T01:37:36.8891773+00:00	
A02	start	2026-08-23T01:37:48.3483141+00:00	Type Scen
			ario 7 test content with UTC marker
A02	end	2026-08-23T01:38:25.0915857+00:00	

```

A03    start 2026-08-23T01:38:37.6191033+00:00 File men
u, Save As in Docuemts folder
A03    end    2026-08-23T01:39:37.8602035+00:00
A04    start 2026-08-23T01:39:47.1060939+00:00 Closing N
otepad++
A04    end    2026-08-23T01:40:00.4118549+00:00
A05    start 2026-08-23T01:40:11.7039072+00:00 Opening D
ocuments folder using File Explorer
A05    end    2026-08-23T01:40:33.2715870+00:00
A06    start 2026-08-23T01:40:45.3515071+00:00 Viewing t
he file created
A06    end    2026-08-23T01:40:57.2474867+00:00
A07    start 2026-08-23T01:41:06.9556496+00:00 Closing F
ile explorer and Applications
A07    end    2026-08-23T01:41:25.5465528+00:00

```

```

PS C:\WINDOWS\system32> Save-Log -Scenario 7 -Run 3
Wrote 14 rows to C:\DISS_TESTDATA\scenario7_run3_action
s.csv
PS C:\WINDOWS\system32>

```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch Notepad++ from Start"
A01 start 2026-08-23T01:37:10.1304310+00:00 Launch Notepad++ from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-23T01:37:36.8891773+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Type Scenario 7 test content with UTC marker"
A02 start 2026-08-23T01:37:48.3483141+00:00 Type Scenario 7 test content with UTC marker
PS C:\WINDOWS\system32> [DateTime]::UtcNow.ToString("o")
2026-08-23T01:37:55.7549893Z
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-23T01:38:25.0915857+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "File menu, Save As in Docuemts folder"
A03 start 2026-08-23T01:38:37.6191033+00:00 File menu, Save As in Docuemts folder
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-23T01:39:37.8602035+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Closing Notepad++"
A04 start 2026-08-23T01:39:47.1060939+00:00 Closing Notepad++
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-23T01:40:00.4118549+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Opening Documents folder using File Explorer"
A05 start 2026-08-23T01:40:11.7039072+00:00 Opening Documents folder using File Explorer
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-23T01:40:33.2715870+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Viewing the file created"
A06 start 2026-08-23T01:40:45.3515071+00:00 Viewing the file created
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-23T01:40:57.2474867+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Closing File explorer and Applications"
A07 start 2026-08-23T01:41:06.9556496+00:00 Closing File explorer and Applications
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-23T01:41:25.5465528+00:00

```

```

PS C:\WINDOWS\system32> Show-Log

Action Phase UTC Note
-----
A01 start 2026-08-23T01:37:10.1304310+00:00 Launch Notepad++ from Start
A01 end 2026-08-23T01:37:36.8891773+00:00
A02 start 2026-08-23T01:37:48.3483141+00:00 Type Scenario 7 test content with UTC marker
A02 end 2026-08-23T01:38:25.0915857+00:00
A03 start 2026-08-23T01:38:37.6191033+00:00 File menu, Save As in Documents folder
A03 end 2026-08-23T01:39:37.8602035+00:00
A04 start 2026-08-23T01:39:47.1060939+00:00 Closing Notepad++
A04 end 2026-08-23T01:40:00.4118549+00:00
A05 start 2026-08-23T01:40:11.7039072+00:00 Opening Documents folder using File Explorer
A05 end 2026-08-23T01:40:33.2715870+00:00
A06 start 2026-08-23T01:40:45.3515071+00:00 Viewing the file created
A06 end 2026-08-23T01:40:57.2474867+00:00
A07 start 2026-08-23T01:41:06.9556496+00:00 Closing File explorer and Applications
A07 end 2026-08-23T01:41:25.5465528+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 7 -Run 3
Wrote 14 rows to C:\DISS_TESTDATA\scenario7_run3_actions.csv
PS C:\WINDOWS\system32>

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 7 -Run 3
[Acquire] scenario7_run3 offline acquisition starting (multi-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario7_run3_post' -> DISS-Win11-25H2-Testbed-000012.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3
[Acquire] Mounting DISS-Win11-25H2-Testbed-000012.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (431 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
28,381,184 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%40operational.evtx
69,632 bytes (exit 1)

```

```

    ok    Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok    NTUSER.DAT
2,359,296 bytes (exit 1)
    ok    NTUSER.DAT.LOG1
0 bytes (exit 1)
    ok    NTUSER.DAT.LOG2
376,832 bytes (exit 1)
    ok    UsrClass.dat
2,097,152 bytes (exit 1)
    ok    UsrClass.dat.LOG1
0 bytes (exit 1)
    ok    UsrClass.dat.LOG2
556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
    ok    SYSTEM
13,631,488 bytes (exit 1)
    ok    SOFTWARE
82,051,072 bytes (exit 1)
    ok    Amcache.hve
2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario7_run3 acquisition complete
    Snapshot : scenario7_run3_post (DISS-Win11-25H2-Testbe
d-000012.vmdk)
    Mount    : AIM device 000000 at I: (dismounted)
    Files    : 445 (138.79 MB total)
    Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\sc
enario_7\run_3\artefacts\supporting\acquisition_manifes
t.csv

Landing zones:
    prefetch    431 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_3\artefacts\prefetch

```

```

eventLogs      5 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_3\artefacts\event_logs
shellbags      6 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_3\artefacts\shellbags
supporting     3 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_3\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_7\run_3\evaluation

```

```

4 evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 7 -Run 3
[Acquire] scenario7_run3 offline acquisition starting (multi-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario7_run3_post' -> DISS-Win11-25H2-Testbed-000012.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3
[Acquire] Mounting DISS-Win11-25H2-Testbed-000012.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (431 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 28,381,184 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 0 bytes (exit 1)
ok NTUSER.DAT.LOG2 376,832 bytes (exit 1)
ok UsrClass.dat 2,097,152 bytes (exit 1)
ok UsrClass.dat.LOG1 0 bytes (exit 1)
ok UsrClass.dat.LOG2 556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,631,488 bytes (exit 1)
ok SOFTWARE 82,051,072 bytes (exit 1)
ok Amcache.hve 2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario7_run3 acquisition complete
Snapshot : scenario7_run3_post (DISS-Win11-25H2-Testbed-000012.vmdk)
Mount : AIM device 000000 at I: (dismounted)
Files : 445 (138.79 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 431 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\artefacts\prefetch
eventLogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

▼ SCN8

```

PS C:\WINDOWS\system32> Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass -Force
PS C:\WINDOWS\system32> $script:log = @()
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> function Log-Action {
>>     param(
>>         [Parameter(Mandatory)][string]$id,

```

```

>>         [Parameter(Mandatory)][string]$phase,
>>         [string]$note = ''
>>     )
>>     $ts = Get-Date -Format o
>>     $script:log += [PSCustomObject]@{
>>         Action = $id
>>         Phase  = $phase
>>         UTC    = $ts
>>         Note   = $note
>>     }
>>     Write-Host "$id $phase $ts $note"
>> }
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> function Save-Log {
>>     param(
>>         [Parameter(Mandatory)][int]$Scenario,
>>         [int]$Run = 0,
>>         [string]$Path = 'C:\DISS_TESTDATA'
>>     )
>>     if (-not (Test-Path $Path)) {
>>         New-Item -ItemType Directory -Path $Path -For
ce | Out-Null
>>     }
>>     if ($Run -eq 0) {
>>         $filename = "scenario${Scenario}_actions.csv"
>>     } else {
>>         $filename = "scenario${Scenario}_run${Run}_ac
tions.csv"
>>     }
>>     $file = Join-Path $Path $filename
>>     $script:log | Export-Csv -Path $file -NoTypeInfor
mation
>>     Write-Host "Wrote $($script:log.Count) rows to $f
ile"
>> }
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> function Show-Log { $script:log
| Format-Table -AutoSize }

```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> function Reset-Log { $script:log
= @(); Write-Host "Log cleared" }
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Write-Host "Logger ready. Use: L
og-Action A01 start 'desc' / Log-Action A01 end"
Logger ready. Use: Log-Action A01 start 'desc' / Log-Act
ion A01 end
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch cm
d.exe from Start"
A01 start 2026-08-18T20:18:10.8212766+00:00 Launch cmd.e
xe from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-18T20:18:29.1424002+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "cmd: whoam
i"
A02 start 2026-08-18T20:18:49.0700644+00:00 cmd: whoami
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-18T20:18:58.3249610+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "cmd: dir
C:\Windows"
A03 start 2026-08-18T20:19:26.3738517+00:00 cmd: dir
C:\Windows
PS C:\WINDOWS\system32> Log-Action A03 end "dir C:\Windo
ws"
A03 end 2026-08-18T20:20:00.8904413+00:00 dir C:\Windows
PS C:\WINDOWS\system32> Log-Action A04 start "Close cmd"
A04 start 2026-08-18T20:20:14.2935150+00:00 Close cmd
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-18T20:20:25.2050958+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Launch pow
ershell"
A05 start 2026-08-18T20:20:48.4442687+00:00 Launch power

```

```

shell
PS C:\WINDOWS\system32> Log Action A05 end
Log : The term 'Log' is not recognized as the name of a
cmdlet, function, script file, or operable program. Chec
k the
spelling of the name, or if a path was included, verify
that the path is correct and try again.
At line:1 char:1
+ Log Action A05 end
+ ~~~
    + CategoryInfo          : ObjectNotFound: (Log:Strin
g) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-18T20:21:19.8578361+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "PS: Get-Pr
ocess"
A06 start 2026-08-18T20:21:44.9943674+00:00 PS: Get-Proc
ess
PS C:\WINDOWS\system32> Log-Action A06 end "Get-Process"
A06 end 2026-08-18T20:22:32.9225135+00:00 Get-Process
PS C:\WINDOWS\system32> Log-Action A07 start "Close powe
rshell"
A07 start 2026-08-18T20:22:49.7719866+00:00 Close powers
hell
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-18T20:23:00.0246629+00:00
PS C:\WINDOWS\system32> Show-Log

```

Action	Phase	UTC	Note
-----	-----	---	----
A01	start	2026-08-18T20:18:10.8212766+00:00	Launch cm
			d.exe from Start
A01	end	2026-08-18T20:18:29.1424002+00:00	
A02	start	2026-08-18T20:18:49.0700644+00:00	cmd: whoa
			mi
A02	end	2026-08-18T20:18:58.3249610+00:00	

```

A03      start 2026-08-18T20:19:26.3738517+00:00 cmd: dir
C:\Windows
A03      end    2026-08-18T20:20:00.8904413+00:00 dir C:\Wi
ndows
A04      start 2026-08-18T20:20:14.2935150+00:00 Close cmd
A04      end    2026-08-18T20:20:25.2050958+00:00
A05      start 2026-08-18T20:20:48.4442687+00:00 Launch po
wershell
A05      end    2026-08-18T20:21:19.8578361+00:00
A06      start 2026-08-18T20:21:44.9943674+00:00 PS: Get-P
rocess
A06      end    2026-08-18T20:22:32.9225135+00:00 Get-Proce
ss
A07      start 2026-08-18T20:22:49.7719866+00:00 Close pow
ershell
A07      end    2026-08-18T20:23:00.0246629+00:00

```

```

PS C:\WINDOWS\system32> Save-Log -Scenario 8
Wrote 14 rows to C:\DISS_TESTDATA\scenario8_actions.csv
PS C:\WINDOWS\system32>

```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch cmd.exe from Start"
A01 start 2026-08-18T20:18:10.8212766+00:00 Launch cmd.exe from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-18T20:18:29.1424002+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "cmd: whoami"
A02 start 2026-08-18T20:18:49.0700644+00:00 cmd: whoami
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-18T20:18:58.3249610+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "cmd: dir C:\Windows"
A03 start 2026-08-18T20:19:26.3738517+00:00 cmd: dir C:\Windows
PS C:\WINDOWS\system32> Log-Action A03 end "dir C:\Windows"
A03 end 2026-08-18T20:20:00.8904413+00:00 dir C:\Windows
PS C:\WINDOWS\system32> Log-Action A04 start "Close cmd"
A04 start 2026-08-18T20:20:14.2935150+00:00 Close cmd
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-18T20:20:25.2050958+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Launch powershell"
A05 start 2026-08-18T20:20:48.4442687+00:00 Launch powershell
PS C:\WINDOWS\system32> Log-Action A05 end
Log : The term 'Log' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the
spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ Log Action A05 end
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Log:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-18T20:21:19.8578361+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "PS: Get-Process"
A06 start 2026-08-18T20:21:44.9943674+00:00 PS: Get-Process
PS C:\WINDOWS\system32> Log-Action A06 end "Get-Process"
A06 end 2026-08-18T20:22:32.9225135+00:00 Get-Process
PS C:\WINDOWS\system32> Log-Action A07 start "Close powershell"
A07 start 2026-08-18T20:22:49.7719866+00:00 Close powershell
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-18T20:23:00.0246629+00:00

```

```

A07 end 2026-08-18T20:23:00.0246629+00:00
PS C:\WINDOWS\system32> Show-Log

Action Phase UTC Note
-----
A01 start 2026-08-18T20:18:10.8212766+00:00 Launch cmd.exe from Start
A01 end 2026-08-18T20:18:29.1424002+00:00
A02 start 2026-08-18T20:18:49.0700644+00:00 cmd: whoami
A02 end 2026-08-18T20:18:58.3249610+00:00
A03 start 2026-08-18T20:19:26.3738517+00:00 cmd: dir C:\Windows
A03 end 2026-08-18T20:20:00.8904413+00:00 dir C:\Windows
A04 start 2026-08-18T20:20:14.2935150+00:00 Close cmd
A04 end 2026-08-18T20:20:25.2050958+00:00
A05 start 2026-08-18T20:20:48.4442687+00:00 Launch powershell
A05 end 2026-08-18T20:21:19.8578361+00:00
A06 start 2026-08-18T20:21:44.9943674+00:00 PS: Get-Process
A06 end 2026-08-18T20:22:32.9225135+00:00 Get-Process
A07 start 2026-08-18T20:22:49.7719866+00:00 Close powershell
A07 end 2026-08-18T20:23:00.0246629+00:00

PS C:\WINDOWS\system32> Save-Log -Scenario 8
Wrote 14 rows to C:\DISS_TESTDATA\scenario8_actions.csv
PS C:\WINDOWS\system32>

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\a
cquire_artefacts.ps1 -Scenario 8
[Acquire] scenario8 offline acquisition starting (single
-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege,
SeSecurityPrivilege
[Acquire] Resolved 'scenario8_post' -> DISS-Win11-25H2-T
estbed-0000006.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\s
cenarios\scenario_8
[Acquire] Mounting DISS-Win11-25H2-Testbed-0000006.vmdk v
ia aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to ass
ign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (350 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
26,284,032 bytes (exit 1)
    ok System.evtx

```

```

2,166,784 bytes (exit 1)
  ok Application.evtx
2,166,784 bytes (exit 1)
  ok Microsoft-Windows-DriverFrameworks-UserMode%4oper
ational.evtx      69,632 bytes (exit 1)
  ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
  ok NTUSER.DAT
2,359,296 bytes (exit 1)
  ok NTUSER.DAT.LOG1
458,752 bytes (exit 1)
  ok NTUSER.DAT.LOG2
0 bytes (exit 1)
  ok UsrClass.dat
2,097,152 bytes (exit 1)
  ok UsrClass.dat.LOG1
0 bytes (exit 1)
  ok UsrClass.dat.LOG2
556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
  ok SYSTEM
13,369,344 bytes (exit 1)
  ok SOFTWARE
82,051,072 bytes (exit 1)
  ok Amcache.hve
2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario8 acquisition complete
  Snapshot : scenario8_post (DISS-Win11-25H2-Testbed-000
006.vmdk)
  Mount    : AIM device 000000 at H: (dismounted)
  Files    : 364 (134.81 MB total)
  Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\sc
enario_8\artefacts\supporting\acquisition_manifest.csv

```

Landing zones:

```
prefetch      350 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\prefetch
eventLogs     5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\event_logs
shellbags     6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\shellbags
supporting    3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\evaluation
```

```
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 8
[Acquire] scenario8 offline acquisition starting (single-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario8_post' -> DISS-Win11-25H2-Testbed-000006.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8
[Acquire] Mounting DISS-Win11-25H2-Testbed-000006.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (350 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 26,284,032 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 458,752 bytes (exit 1)
ok NTUSER.DAT.LOG2 0 bytes (exit 1)
ok UsrClass.dat 2,097,152 bytes (exit 1)
ok UsrClass.dat.LOG1 0 bytes (exit 1)
ok UsrClass.dat.LOG2 556,032 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,369,344 bytes (exit 1)
ok SOFTWARE 82,051,072 bytes (exit 1)
ok Amcache.hve 2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario8 acquisition complete
Snapshot : scenario8_post (DISS-Win11-25H2-Testbed-000006.vmdk)
Mount : AIM device 000000 at H: (dismounted)
Files : 364 (134.81 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch      350 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\prefetch
eventLogs     5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\event_logs
shellbags     6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\shellbags
supporting    3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_8\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>
```

▼ SCN9

```
# =====
# Scenario 9 ground-truth logger (paste into elevated Po
werShell)
# Author: Syed Muhammad Saqlain Abbas (W21634541)
# =====

$script:log = @()

function Log-Action {
    param(
        [Parameter(Mandatory)][string]$id,
        [Parameter(Mandatory)][string]$phase,
        [string]$note = ''
    )
    $ts = Get-Date -Format o
    $script:log += [PSCustomObject]@{
        Action = $id
        Phase  = $phase
        UTC    = $ts
        Note   = $note
    }
    Write-Host "$id $phase $ts $note"
}

function Save-Log {
    param(
        [Parameter(Mandatory)][int]$Scenario,
        [int]$Run = 0,
        [string]$Path = 'C:\DISS_TESTDATA'
    )
    if (-not (Test-Path $Path)) {
        New-Item -ItemType Directory -Path $Path -Force
    }
    Out-Null
}
```

```

        if ($Run -eq 0) {
            $filename = "scenario${Scenario}_actions.csv"
        } else {
            $filename = "scenario${Scenario}_run${Run}_actions.csv"
        }
        $file = Join-Path $Path $filename
        $script:log | Export-Csv -Path $file -NoTypeInformation
        Write-Host "Wrote $($script:log.Count) rows to $file"
    }

    function Show-Log {
        $script:log | Format-Table -AutoSize
    }

    function Reset-Log {
        $script:log = @()
        Write-Host "Log cleared"
    }

    Write-Host ""
    Write-Host "Logger loaded. Use: Log-Action A01 start 'description'"
    Write-Host "                                Log-Action A01 end"
    Write-Host "At end: Save-Log -Scenario 9"
    Write-Host ""

```

```

PS C:\WINDOWS\system32> Log-Action A01 start "Launch chrome from Start"
A01 start 2026-08-20T09:03:38.9508369+00:00 Launch chrome from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-20T09:04:00.2928116+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Navigate to UoW website"
A02 start 2026-08-20T09:04:39.0965454+00:00 Navigate to

```

UoW website

```
PS C:\WINDOWS\system32> Log-Action A02 end
```

A02 end 2026-08-20T09:05:26.0291188+00:00

```
PS C:\WINDOWS\system32> Log-Action A03 start "Navigate to  
bbc & Open first headline"
```

A03 start 2026-08-20T09:06:05.2543776+00:00 Navigate to
bbc & Open first headline

```
PS C:\WINDOWS\system32> Log-Action A03 end
```

A03 end 2026-08-20T09:06:55.7464559+00:00

```
PS C:\WINDOWS\system32> Log-Action A04 start "Open digital  
forensics in wikipedia & scroll"
```

A04 start 2026-08-20T09:08:06.9725021+00:00 Open digital
forensics in wikipedia & scroll

```
PS C:\WINDOWS\system32> Log-Action A04 end
```

A04 end 2026-08-20T09:09:33.6047258+00:00

```
PS C:\WINDOWS\system32> Log-Action A05 start "Download a  
sample pdf from File Examples"
```

A05 start 2026-08-20T09:11:32.4760836+00:00 Download a s
ample pdf from File Examples

```
PS C:\WINDOWS\system32> Log-Action A05 end
```

A05 end 2026-08-20T09:12:45.0613492+00:00

```
PS C:\WINDOWS\system32> Log-Action A06 start "Close Chro  
me"
```

A06 start 2026-08-20T09:12:58.1006619+00:00 Close Chrome

```
PS C:\WINDOWS\system32> Log-Action A06 end
```

A06 end 2026-08-20T09:13:08.8947172+00:00

```
PS C:\WINDOWS\system32> Log-Action A07 start "Open Downl  
oads using File Explorer"
```

A07 start 2026-08-20T09:13:40.0627768+00:00 Open Downloa
ds using File Explorer

```
PS C:\WINDOWS\system32> Log-Action A07 end
```

A07 end 2026-08-20T09:13:58.3102803+00:00

```
PS C:\WINDOWS\system32> Log-Action A08 start "Close File  
Explorer"^C
```

```
PS C:\WINDOWS\system32> Log-Action A08 start "Close File  
Explorer"
```

A08 start 2026-08-20T09:14:53.2520509+00:00 Close File E
xplorer

```
PS C:\WINDOWS\system32> Log-Action A08 end
A08 end 2026-08-20T09:15:02.0637490+00:00
PS C:\WINDOWS\system32> Save-Log -Scenario 9
Wrote 16 rows to C:\DISS_TESTDATA\scenario9_actions.csv
```

```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Log-Action A01 start "Launch chrome from Start"
A01 start 2026-08-20T09:03:38.9508369+00:00 Launch chrome from Start
PS C:\WINDOWS\system32> Log-Action A01 end
A01 end 2026-08-20T09:04:00.2928116+00:00
PS C:\WINDOWS\system32> Log-Action A02 start "Navigate to UoW website"
A02 start 2026-08-20T09:04:39.0965454+00:00 Navigate to UoW website
PS C:\WINDOWS\system32> Log-Action A02 end
A02 end 2026-08-20T09:05:26.0291188+00:00
PS C:\WINDOWS\system32> Log-Action A03 start "Navigate to bbc & Open first headline"
A03 start 2026-08-20T09:06:05.2543776+00:00 Navigate to bbc & Open first headline
PS C:\WINDOWS\system32> Log-Action A03 end
A03 end 2026-08-20T09:06:55.7464559+00:00
PS C:\WINDOWS\system32> Log-Action A04 start "Open digital forensics in wikipedia & scroll"
A04 start 2026-08-20T09:08:06.9725021+00:00 Open digital forensics in wikipedia & scroll
PS C:\WINDOWS\system32> Log-Action A04 end
A04 end 2026-08-20T09:09:33.6047258+00:00
PS C:\WINDOWS\system32> Log-Action A05 start "Download a sample pdf from File Examples"
A05 start 2026-08-20T09:11:32.4760836+00:00 Download a sample pdf from File Examples
PS C:\WINDOWS\system32> Log-Action A05 end
A05 end 2026-08-20T09:12:45.0613492+00:00
PS C:\WINDOWS\system32> Log-Action A06 start "Close Chrome"
A06 start 2026-08-20T09:12:58.1006619+00:00 Close Chrome
PS C:\WINDOWS\system32> Log-Action A06 end
A06 end 2026-08-20T09:13:08.8947172+00:00
PS C:\WINDOWS\system32> Log-Action A07 start "Open Downloads using File Explorer"
A07 start 2026-08-20T09:13:40.0627768+00:00 Open Downloads using File Explorer
PS C:\WINDOWS\system32> Log-Action A07 end
A07 end 2026-08-20T09:13:58.3102803+00:00
PS C:\WINDOWS\system32> Log-Action A08 start "Close File Explorer"
PS C:\WINDOWS\system32> Log-Action A08 start "Close File Explorer"
A08 start 2026-08-20T09:14:53.2520509+00:00 Close File Explorer
PS C:\WINDOWS\system32> Log-Action A08 end
A08 end 2026-08-20T09:15:02.0637490+00:00
PS C:\WINDOWS\system32> Save-Log -Scenario 9
Wrote 16 rows to C:\DISS_TESTDATA\scenario9_actions.csv
PS C:\WINDOWS\system32>
```

File Explorer

```
PS C:\WINDOWS\system32> cd D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 9
[Acquire] scenario9 offline acquisition starting (single -run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario9_post' -> DISS-Win11-25H2-Testbed-000008.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios\scenario_9
[Acquire] Mounting DISS-Win11-25H2-Testbed-000008.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
```

```
    ok  Prefetch folder (440 files, exit 1)
[Acquire] Copying 5 event log channels
    ok  Security.evtx
29,429,760 bytes (exit 1)
    ok  System.evtx
2,166,784 bytes (exit 1)
    ok  Application.evtx
2,166,784 bytes (exit 1)
    ok  Microsoft-Windows-DriverFrameworks-UserMode%4oper
ational.evtx      69,632 bytes (exit 1)
    ok  Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok  NTUSER.DAT
2,359,296 bytes (exit 1)
    ok  NTUSER.DAT.LOG1
253,952 bytes (exit 1)
    ok  NTUSER.DAT.LOG2
0 bytes (exit 1)
    ok  UsrClass.dat
2,097,152 bytes (exit 1)
    ok  UsrClass.dat.LOG1
0 bytes (exit 1)
    ok  UsrClass.dat.LOG2
0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
    ok  SYSTEM
13,631,488 bytes (exit 1)
    ok  SOFTWARE
82,051,072 bytes (exit 1)
    ok  Amcache.hve
2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario9 acquisition complete
    Snapshot : scenario9_post (DISS-Win11-25H2-Testbed-000
```

```

008.vmdk)
Mount      : AIM device 000000 at H: (dismounted)
Files      : 454 (139.3 MB total)
Manifest   : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\supporting\acquisition_manifest.csv

Landing zones:
  prefetch      440 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\prefetch
  eventLogs      5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\event_logs
  shellbags      6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\shellbags
  supporting      3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\supporting
  evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\evaluation

```

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> cd D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios> .\acquire_artefacts.ps1 -Scenario 9
[Acquire] scenario9 offline acquisition starting (single-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario9_post' -> DISS-Win11-25H2-Testbed-000008.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9
[Acquire] Mounting DISS-Win11-25H2-Testbed-000008.vmdk via aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at H:
[Acquire] Copying Windows\Prefetch\ (recursive)
  ok Prefetch folder (440 files, exit 1)
[Acquire] Copying 5 event log channels
  ok Security.evtx 29,429,760 bytes (exit 1)
  ok System.evtx 2,166,784 bytes (exit 1)
  ok Application.evtx 2,166,784 bytes (exit 1)
  ok Microsoft-Windows-DriverFrameworks-UserMode%4Operational.evtx 69,632 bytes (exit 1)
  ok Microsoft-Windows-Partition%4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UserClass.dat + transaction logs)
  ok NTUSER.DAT 2,359,296 bytes (exit 1)
  ok NTUSER.DAT.LOG1 253,952 bytes (exit 1)
  ok NTUSER.DAT.LOG2 0 bytes (exit 1)
  ok UserClass.dat 2,097,152 bytes (exit 1)
  ok UserClass.dat.LOG1 0 bytes (exit 1)
  ok UserClass.dat.LOG2 0 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
  ok SYSTEM 13,631,488 bytes (exit 1)
  ok SOFTWARE 82,051,072 bytes (exit 1)
  ok Amcache.hve 2,621,440 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario9 acquisition complete
Snapshot : scenario9_post (DISS-Win11-25H2-Testbed-000008.vmdk)
Mount : AIM device 000000 at H: (dismounted)
Files : 454 (139.3 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\supporting\acquisition_manifest.csv

Landing zones:
  prefetch      440 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\prefetch
  eventLogs      5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\event_logs
  shellbags      6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\shellbags
  supporting      3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\artefacts\supporting
  evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_9\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w\scripts\scenarios>

```

▼ SCN10

```
At line:1 char:3
+ . C:\DISS_TESTDATA\scenario10_log.ps1
+ ~~~~~
+ CategoryInfo          : SecurityError: (:) [], PSSecurityException
+ FullyQualifiedErrorId : UnauthorizedAccess

PS C:\WINDOWS\system32> Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass -Force
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> . C:\DISS_TESTDATA\scenario10_log.ps1
PS C:\WINDOWS\system32> Init-Scenario10Log
Initialised C:\DISS_TESTDATA\scenario10_actions.csv
PS C:\WINDOWS\system32> Log-Action10 PRE start "Baseline Pre Scenario VM, User signed In"
PRE start 2026-08-26T22:29:34.1132373+00:00 Baseline Pre Scenario VM, User signed In
PS C:\WINDOWS\system32> Log-Action10 A01 start "VM Shutdown: start -> power -> shutdown"
LogAction10 : The term 'LogAction10' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name,
or if a path was included, verify that the path is correct and try again.
At line:1 char:1
+ LogAction10 A01 start "VM Shutdown: start -> power -> shutdown"
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (LogAction10:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

PS C:\WINDOWS\system32> Log-Action10 A01 start "VM Shutdown: start -> power -> shutdown"
A01 start 2026-08-26T22:31:30.5434606+00:00 VM Shutdown: start -> power -> shutdown
PS C:\WINDOWS\system32>
```

scenario10_actions.csv: 9 rows at C:\DISS_TESTDATA\scenario10_actions.csv

Action	Phase	UTC	Note
-----	-----	---	----
PRE	start	2026-08-26T22:29:34.1132373+00:00	Baseline Pre Scenario VM, User signed In
A01	start	2026-08-26T22:31:30.5434606+00:00	VM Shutdown: start -> power -> shutdown
A01	end	2026-08-26T22:35:22.1917322+00:00	session terminated on shutdown; end time approximated
A02	start	2026-08-26T22:36:06.7201594+00:00	VM powered off; host UTC = 2026-08-26T22:31:55.2974385Z
A02	end	2026-08-26T22:36:40.4713894+00:00	
A03	start	2026-08-26T22:37:10.8989126+00:00	VM powered on; host UTC = 2026-08-26T22:34:18.9453068Z
A03	end	2026-08-26T22:37:18.8779222+00:00	VM POST reached
A04	start	2026-08-26T22:39:09.8379272+00:00	Wait 90s for post-boot
A04	end	2026-08-26T22:41:24.5365010+00:00	post boot settle completed

```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> . C:\DISS_TESTDATA\scenario10_log.ps1
PS C:\WINDOWS\system32> Log-Action10 A01 end "session terminated on shutdown; end time approximated"
A01 end 2026-08-26T22:35:22.1917322+00:00 session terminated on shutdown; end time approximated
PS C:\WINDOWS\system32> Log-Action10 A02 start "VM powered off; host UTC = 2026-08-26T22:31:55.2974385Z"
A02 start 2026-08-26T22:36:06.7201594+00:00 VM powered off; host UTC = 2026-08-26T22:31:55.2974385Z
PS C:\WINDOWS\system32> Log-Action10 A02 end
A02 end 2026-08-26T22:36:40.4713894+00:00
PS C:\WINDOWS\system32> Log-Action10 A03 start "VM powered on; host UTC = 2026-08-26T22:34:18.9453068Z"
A03 start 2026-08-26T22:37:10.8989126+00:00 VM powered on; host UTC = 2026-08-26T22:34:18.9453068Z
PS C:\WINDOWS\system32> Log-Action10 A03 end "VM POST reached"
A03 end 2026-08-26T22:37:18.8779222+00:00 VM POST reached
PS C:\WINDOWS\system32> Log-Action10 A04 start "Wait 90s for post-boot"
A04 start 2026-08-26T22:39:09.8379272+00:00 Wait 90s for post-boot
PS C:\WINDOWS\system32> Start-Sleep -Seconds 90
PS C:\WINDOWS\system32> Log-Action10 A04 end "post boot settle completed"
A04 end 2026-08-26T22:41:24.5365010+00:00 post boot settle completed
```

```
PS C:\WINDOWS\system32> Finalise-Scenario10Log
scenario10_actions.csv: 9 rows at C:\DISS_TESTDATA\scenario10_actions.csv

Action Phase UTC Note
-----
PRE start 2026-08-26T22:29:34.1132373+00:00 Baseline Pre Scenario VM, User signed In
A01 start 2026-08-26T22:31:30.5434606+00:00 VM Shutdown: start -> power -> shutdown
A01 end 2026-08-26T22:35:22.1917322+00:00 session terminated on shutdown; end time approximated
A02 start 2026-08-26T22:36:06.7201594+00:00 VM powered off; host UTC = 2026-08-26T22:31:55.2974385Z
A02 end 2026-08-26T22:36:40.4713894+00:00
A03 start 2026-08-26T22:37:10.8989126+00:00 VM powered on; host UTC = 2026-08-26T22:34:18.9453068Z
A03 end 2026-08-26T22:37:18.8779222+00:00 VM POST reached
A04 start 2026-08-26T22:39:09.8379272+00:00 Wait 90s for post-boot
A04 end 2026-08-26T22:41:24.5365010+00:00 post boot settle completed

PS C:\WINDOWS\system32>
```

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> [DateTime]::UtcNow.ToString('o')
2026-08-26T22:31:55.2974385Z
PS C:\WINDOWS\system32> [DateTime]::UtcNow.ToString('o')
2026-08-26T22:34:18.9453068Z
PS C:\WINDOWS\system32>
```

```
PS D:\UOW\SEM3\msc-diss-7csef001w> .\scripts\scenarios\acquire_artefacts.ps1 -Scenario 10 -AimCli 'D:\UOW\SEM3\Tools\Arsenal-Image-Mounter-v3.13.368\aim_cli.exe'
[Acquire] scenario10 offline acquisition starting (single-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario10_post' -> DISS-Win11-25H2-Testbed-000015.vmdk
```

```
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\s
cenarios\scenario_10
[Acquire] Mounting DISS-Win11-25H2-Testbed-000015.vmdk v
ia aim_cli (DiscUtils, read only, online)
[Acquire] Waiting for mount to attach and Windows to ass
ign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
    ok Prefetch folder (345 files, exit 1)
[Acquire] Copying 5 event log channels
    ok Security.evtx
26,284,032 bytes (exit 1)
    ok System.evtx
2,166,784 bytes (exit 1)
    ok Application.evtx
2,166,784 bytes (exit 1)
    ok Microsoft-Windows-DriverFrameworks-UserMode%40per
ational.evtx 69,632 bytes (exit 1)
    ok Microsoft-Windows-Partition%4Diagnostic.evtx
69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UsrClass.da
t + transaction logs)
    ok NTUSER.DAT
2,359,296 bytes (exit 1)
    ok NTUSER.DAT.LOG1
0 bytes (exit 1)
    ok NTUSER.DAT.LOG2
0 bytes (exit 1)
    ok UsrClass.dat
2,097,152 bytes (exit 1)
    ok UsrClass.dat.LOG1
556,032 bytes (exit 1)
    ok UsrClass.dat.LOG2
524,288 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Am
cache.hve
    ok SYSTEM
13,369,344 bytes (exit 1)
```

```

    ok    SOFTWARE
81,264,640 bytes (exit 1)
    ok    Amcache.hve
2,359,296 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario10 acquisition complete
    Snapshot : scenario10_post (DISS-Win11-25H2-Testbed-00
0015.vmdk)
    Mount      : AIM device 000000 at I: (dismounted)
    Files      : 359 (133.81 MB total)
    Manifest   : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\sc
enario_10\artefacts\supporting\acquisition_manifest.csv

Landing zones:
    prefetch    345 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_10\artefacts\prefetch
    eventLogs    5 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_10\artefacts\event_logs
    shellbags    6 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_10\artefacts\shellbags
    supporting    3 files -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_10\artefacts\supporting
    evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef00
1w\scenarios\scenario_10\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w>

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w> .\scripts\scenarios\acquire_artefacts.ps1 -Scenario 10 -AimCli 'D:\UOW\SEM3\Tools\Arsenal-Image-Mounter-v3.13.368\aim_cli.exe'
[Acquire] scenario10 offline acquisition starting (single-run)
[Acquire] Enabled SeBackupPrivilege, SeRestorePrivilege, SeSecurityPrivilege
[Acquire] Resolved 'scenario10_post' -> DISS-Win11-25H2-Testbed-000015.vmdk
[Acquire] Landing under D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10
[Acquire] Mounting DISS-Win11-25H2-Testbed-000015.vmdk via aim_cli (Diskutils, read only, online)
[Acquire] Waiting for mount to attach and Windows to assign drive letters...
[Acquire] Mounted: AIM device 000000, NTFS at I:
[Acquire] Copying Windows\Prefetch\ (recursive)
ok Prefetch folder (345 files, exit 1)
[Acquire] Copying 5 event log channels
ok Security.evtx 26,284,032 bytes (exit 1)
ok System.evtx 2,166,784 bytes (exit 1)
ok Application.evtx 2,166,784 bytes (exit 1)
ok Microsoft-Windows-DriverFrameworks-UserMode\40Operational.evtx 69,632 bytes (exit 1)
ok Microsoft-Windows-Partition\4Diagnostic.evtx 69,632 bytes (exit 1)
[Acquire] Copying user hives (NTUSER.DAT and UserClass.dat + transaction logs)
ok NTUSER.DAT 2,359,296 bytes (exit 1)
ok NTUSER.DAT.LOG1 0 bytes (exit 1)
ok NTUSER.DAT.LOG2 0 bytes (exit 1)
ok UserClass.dat 2,097,152 bytes (exit 1)
ok UserClass.dat.LOG1 556,032 bytes (exit 1)
ok UserClass.dat.LOG2 524,288 bytes (exit 1)
[Acquire] Copying system hives (SYSTEM, SOFTWARE) and Amcache.hve
ok SYSTEM 13,369,344 bytes (exit 1)
ok SOFTWARE 81,264,640 bytes (exit 1)
ok Amcache.hve 2,359,296 bytes (exit 1)
[Acquire] Dismounting AIM device
[Acquire] Computing SHA 256 manifest
[Acquire] scenario10 acquisition complete
Snapshot : scenario10_post (DISS-Win11-25H2-Testbed-000015.vmdk)
Mount : AIM device 000000 at I: (dismounted)
Files : 359 (133.81 MB total)
Manifest : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\artefacts\supporting\acquisition_manifest.csv

Landing zones:
prefetch 345 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\artefacts\prefetch
eventlogs 5 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\artefacts\event_logs
shellbags 6 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\artefacts\shellbags
supporting 3 files -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\artefacts\supporting
evaluation (dir) -> D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\evaluation
PS D:\UOW\SEM3\msc-diss-7csef001w>

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w> .\scripts\analysis\extract_artefacts.ps1 -Scenario 10
Cleaning existing analysis folder: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\analysis

```

```

Root folder: GUID: 4
Directory: 6
Drive letter: 1

Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\artefacts\shellbags\UserClass.dat

Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\analysis\shellbags\0_UserClass.csv

-----

Processing complete!

Processed 2 files in 0.44 seconds!
Total ShellBags found: 11

=====
Extraction complete for Scenario 10
=====

File                                         SizeKB
----
event_logs\20260826225351 EvtxECmd_Output.csv 32645.1
prefetch\scenario_10_prefetch.csv          3175
prefetch\scenario_10_prefetch_Timeline.csv 120.8
shellbags\ISBECmd_Messages.txt             2.4
shellbags\NTUSER.csv                       0.2
shellbags\UserClass.csv                    2

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w> .\scripts\analysis>window_filter.ps1 -Scenario 10

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w> .\scripts\analysis>window_filter.ps1 -Scenario 10

=====
Window-filtering Scenario 10
Ground truth : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\evaluation\ground_truth.csv
Pad (each side) : +/-2 s
Output : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_10\analysis\windowed
=====

Built 4 windows from ground truth (pad +/-2s):

Action Note                                     StartUtc      EndUtc      DurationSec
-----
A01 VM Shutdown: start -> power -> shutdown    22:31:28.543  22:35:24.191    235.65
A02 VM powered off; host UTC = 2026-08-26T22:31:55.2974385Z 22:36:04.720  22:36:42.471     37.75
A03 VM powered on; host UTC = 2026-08-26T22:34:18.9453068Z  22:37:08.898  22:37:20.877     11.98
A04 Wait 90s for post-boot                      22:39:07.837  22:41:26.536    138.7

[1 of 2] Prefetch Timeline
1212 timeline rows -> 67 rows kept

[2 of 2] EVTX events
30863 EVTX rows -> 881 rows kept

[extra] ShellBags copy-through (not time-filtered by design)
NTUSER.csv: 0 rows
UserClass.csv: 11 rows

=====
Scenario 10 windowing complete
=====

File                                     SizeKB Rows
----
windows.csv                             0.5      4
event_logs\events_windowed.csv          1024.1  881
prefetch\scenario_10_prefetch_Timeline_windowed.csv 6.6      67
shellbags\NTUSER.csv                    0.2      0
shellbags\UserClass.csv                  2       11

PS D:\UOW\SEM3\msc-diss-7csef001w>

```

▼ Analysis

- Tools Installation
 - <https://ericzimmerman.github.io/>

```
Invoke-WebRequest -Uri "https://download.ericzimmermanstools.com/Get-ZimmermanTools.zip" -OutFile "Get-ZimmermanTools.zip"
```

```
Expand-Archive -Path "Get-ZimmermanTools.zip" -DestinationPath "." -Force
```

```
.\Get-ZimmermanTools.ps1 -Dest D:\UOW\SEM3\Tools\ZimmermanTools
```

```

PS D:\UOW\SEM3\Tools\ZimmermanTools> Invoke-WebRequest -Uri "https://download.ericzimmermanstools.com/Get-ZimmermanTools.zip" -OutFile "Get-ZimmermanTools.zip"
PS D:\UOW\SEM3\Tools\ZimmermanTools> Expand-Archive -Path "Get-ZimmermanTools.zip" -DestinationPath "." -Force

```

```
PS D:\UOW\SEM3\Tools\ZimmermanTools> .\Get-ZimmermanTools.ps1 -Dest D:\UOW\SEM3\Tools\ZimmermanTools
```

This script will discover and download all available programs from <https://ericzimmerman.github.io> and download them to D:\UOW\SEM3\Tools\ZimmermanTools

A file will also be created in D:\UOW\SEM3\Tools\ZimmermanTools that tracks the signature of each file, so rerunning the script will only download new versions.

To redownload, remove lines from or delete the CSV file created under D:\UOW\SEM3\Tools\ZimmermanTools and rerun. Enjoy!

Use -NetVersion to control which version of the software you get (4 or 9). Default is 9. Use 0 to get all

```
* Getting available programs...
* Files to download: 27
* Downloaded Get-ZimmermanTools.zip (Size: 16,555)
* D:\UOW\SEM3\Tools\ZimmermanTools\net9 does not exist. Creating...
* Downloaded AmcacheParser.zip (Size: 2,337,170) (net 9)
* Downloaded AppCompatCacheParser.zip (Size: 2,290,113) (net 9)
* Downloaded bstrings.zip (Size: 2,006,525) (net 9)
* Downloaded EvtxECmd.zip (Size: 3,943,680) (net 9)
* Downloaded EZViewer.zip (Size: 91,506,373) (net 9)
* Downloaded JLECmd.zip (Size: 3,011,582) (net 9)
* Downloaded JumpListExplorer.zip (Size: 91,163,135) (net 9)
* Downloaded LECmd.zip (Size: 3,066,762) (net 9)
* Downloaded MFTECmd.zip (Size: 2,841,312) (net 9)
* Downloaded MFTEExplorer.zip (Size: 91,404,340) (net 9)
```

```
9)
* Downloaded PECmd.zip (Size: 2,279,692) (net 9)
* Downloaded RBCmd.zip (Size: 1,690,356) (net 9)
* Downloaded RecentFileCacheParser.zip (Size: 1,599,633) (net 9)
* Downloaded RECmd.zip (Size: 4,725,547) (net 9)
* Downloaded RegistryExplorer.zip (Size: 97,927,381) (net 9)
* Downloaded rla.zip (Size: 2,210,699) (net 9)
* Downloaded SDBExplorer.zip (Size: 91,393,982) (net 9)
9)
* Downloaded SBECmd.zip (Size: 3,177,325) (net 9)
* Downloaded ShellBagsExplorer.zip (Size: 93,561,020) (net 9)
* Downloaded SQLECmd.zip (Size: 7,440,410) (net 9)
* Downloaded SrumECmd.zip (Size: 2,063,275) (net 9)
* Downloaded SumECmd.zip (Size: 1,728,470) (net 9)
* Downloaded TimelineExplorer.zip (Size: 91,772,972) (net 9)
* Downloaded VSCMount.zip (Size: 1,679,576) (net 9)
* Downloaded WxTCmd.zip (Size: 6,078,718) (net 9)
* Downloaded iisGeolocate.zip (Size: 30,766,979) (net 9)
9)

* Saving downloaded version information to D:\UOW\SEM3\Tools\ZimmermanTools\!!!RemoteFileDetails.csv
```

```

PS D:\UOW\SEM3\Tools\ZimmermanTools> Invoke-WebRequest -Uri "https://download.ericzimmerman.com/Get-ZimmermanTools.zip" -OutFile "Get-ZimmermanTools.zip"
PS D:\UOW\SEM3\Tools\ZimmermanTools> Expand-Archive -Path "Get-ZimmermanTools.zip" -DestinationPath "." -Force
PS D:\UOW\SEM3\Tools\ZimmermanTools> .\Get-ZimmermanTools.ps1 -Dest D:\UOW\SEM3\Tools\ZimmermanTools

This script will discover and download all available programs
from https://ericzimmerman.github.io and download them to D:\UOW\SEM3\Tools\ZimmermanTools

A file will also be created in D:\UOW\SEM3\Tools\ZimmermanTools that tracks the signature of each file,
so rerunning the script will only download new versions.

To redownload, remove lines from or delete the CSV file created under D:\UOW\SEM3\Tools\ZimmermanTools and rerun. Enjoy!

Use -NetVersion to control which version of the software you get (4 or 9). Default is 9. Use 9 to get all

* Getting available programs...
* Files to download: 27
* Downloaded Get-ZimmermanTools.zip (Size: 16,555)
* D:\UOW\SEM3\Tools\ZimmermanTools\net9 does not exist. Creating...
* Downloaded AmcacheParser.zip (Size: 2,337,170) (net 9)
* Downloaded AppCompatCacheParser.zip (Size: 2,290,113) (net 9)
* Downloaded bstrings.zip (Size: 2,006,525) (net 9)
* Downloaded EvtxECmd.zip (Size: 3,943,680) (net 9)
* Downloaded EZViewer.zip (Size: 91,586,373) (net 9)
* Downloaded JLECmd.zip (Size: 3,011,502) (net 9)
* Downloaded JumpListExplorer.zip (Size: 91,163,135) (net 9)
* Downloaded LECmd.zip (Size: 3,866,762) (net 9)
* Downloaded MFTECmd.zip (Size: 2,841,312) (net 9)
* Downloaded MFTEExplorer.zip (Size: 91,404,340) (net 9)
* Downloaded PECmd.zip (Size: 2,279,692) (net 9)
* Downloaded RBCmd.zip (Size: 1,690,356) (net 9)
* Downloaded RecentFileCacheParser.zip (Size: 1,599,633) (net 9)
* Downloaded RmCmd.zip (Size: 4,725,507) (net 9)
* Downloaded RegistryExplorer.zip (Size: 97,927,381) (net 9)
* Downloaded rla.zip (Size: 2,210,699) (net 9)
* Downloaded SDBExplorer.zip (Size: 91,393,982) (net 9)
* Downloaded SBECmd.zip (Size: 3,177,325) (net 9)
* Downloaded ShellBagsExplorer.zip (Size: 93,561,020) (net 9)
* Downloaded SQLECmd.zip (Size: 7,440,410) (net 9)
* Downloaded SrumECmd.zip (Size: 2,863,275) (net 9)
* Downloaded SumECmd.zip (Size: 1,720,470) (net 9)
* Downloaded TimelineExplorer.zip (Size: 91,772,972) (net 9)
* Downloaded VSCMount.zip (Size: 1,679,576) (net 9)
* Downloaded WxTCmd.zip (Size: 6,078,718) (net 9)
* Downloaded iisGeolocate.zip (Size: 30,766,979) (net 9)

* Saving downloaded version information to D:\UOW\SEM3\Tools\ZimmermanTools\!!!RemoteFileDetails.csv
PS D:\UOW\SEM3\Tools\ZimmermanTools>

```

- Scenario 1
 - Parsing Prefetch with PECmd

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1> D:\UOW\SEM3\Tools\ZimmermanTools\net9\PECmd.exe -d .\artefacts\prefetch --csv .\analysis\prefetch -q
PECmd version 2026.5.0

```

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

Command line: -d .\artefacts\prefetch --csv .\analysis\prefetch -q

Warning: Administrator privileges not found!

Keywords: temp, tmp

Looking for prefetch files in .\artefacts\prefetch

Found 413 Prefetch files

```
----- Processed .\artefacts\prefetch\151.0.79
22.138_CHROME_INSTALL-FFDC6407.pf in 0.03313070 se
conds -----
----- Processed .\artefacts\prefetch\ACROBAT.
EXE-F94F9B29.pf in 0.02532590 seconds -----
----- Processed .\artefacts\prefetch\ACROBAT.
EXE-F94F9B2A.pf in 0.02216370 seconds -----
----- Processed .\artefacts\prefetch\ACROBAT.
EXE-F94F9B30.pf in 0.01425850 seconds -----
----- Processed .\artefacts\prefetch\ADNOTIFI
CATIONMANAGER.EXE-E7F9E8B8.pf in 0.02675900 second
s -----
----- Processed .\artefacts\prefetch\ADOBEAR
M.EXE-F9223367.pf in 0.01705310 seconds -----
----- Processed .\artefacts\prefetch\ADOBEARM
HELPER.EXE-C537EF0C.pf in 0.00750580 seconds -----
-----
----- Processed .\artefacts\prefetch\ADOBEARM
HELPER.EXE-FA58E1EF.pf in 0.01385850 seconds -----
-----
----- Processed .\artefacts\prefetch\ADOBEARM
_UCB.EXE-C04E772A.pf in 0.00704780 seconds -----
---
----- Processed .\artefacts\prefetch\ADOBECOL
LABSYNC.EXE-A30339B6.pf in 0.00669110 seconds ----
-----
----- Processed .\artefacts\prefetch\AM_BASE.
EXE-3F70DC95.pf in 0.00656360 seconds -----
----- Processed .\artefacts\prefetch\AM_BASE_
PATCH1.EXE-B2ACC39D.pf in 0.00533920 seconds -----
-----
----- Processed .\artefacts\prefetch\AM_DELT
A.EXE-78CA83B0.pf in 0.00619020 seconds -----
----- Processed .\artefacts\prefetch\AM_ENGIN
E.EXE-F1C956E4.pf in 0.00661250 seconds -----
----- Processed .\artefacts\prefetch\AM_ENGIN
```

```

E_PATCH_1.1.26060.300-49F3FAFB.pf in 0.00537560 se
conds -----
----- Processed .\artefacts\prefetch\APPACTIO
NS.EXE-D77D7F4C.pf in 0.00650740 seconds -----
-
----- Processed .\artefacts\prefetch\APPLICAT
IONFRAMEHOST.EXE-8CE9A1EE.pf in 0.00780040 seconds
-----
----- Processed .\artefacts\prefetch\ARMSVC.E
XE-A68AEAE4.pf in 0.00829600 seconds -----
----- Processed .\artefacts\prefetch\AUDIODG.
EXE-AB22E9A6.pf in 0.00671630 seconds -----
----- Processed .\artefacts\prefetch\AUDITPO
L.EXE-2D4A3037.pf in 0.00576920 seconds -----
----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-4589797A.pf in 0.00682690 seconds -
-----
----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-51333CCD.pf in 0.00586080 seconds -
-----
----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-652FD708.pf in 0.00661840 seconds -
-----
----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-7807DBFD.pf in 0.00624670 seconds -
-----
----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-94B29EA3.pf in 0.00719110 seconds -
-----
----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-BB08D488.pf in 0.00804380 seconds -
-----
----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-CAD1DF16.pf in 0.00845470 seconds -
-----
----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-D416BD78.pf in 0.00664680 seconds -
-----

```

```

----- Processed .\artefacts\prefetch\BACKGROU
NDTASKHOST.EXE-E093C3F5.pf in 0.00694300 seconds -
-----
----- Processed .\artefacts\prefetch\BACKGROU
NDTRANSFERHOST.EXE-2B373A4D.pf in 0.00607980 secon
ds -----
----- Processed .\artefacts\prefetch\BACKGROU
NDTRANSFERHOST.EXE-6A9B5922.pf in 0.00617510 secon
ds -----
----- Processed .\artefacts\prefetch\BACKGROU
NDTRANSFERHOST.EXE-E7B7D877.pf in 0.00900040 secon
ds -----
----- Processed .\artefacts\prefetch\BDEUISR
V.EXE-7BC33651.pf in 0.00621680 seconds -----
----- Processed .\artefacts\prefetch\CHRMSTP.
EXE-A45CB8FE.pf in 0.00614580 seconds -----
----- Processed .\artefacts\prefetch\CHRMSTP.
EXE-A45CB902.pf in 0.00784820 seconds -----
----- Processed .\artefacts\prefetch\CHROME.E
XE-AED7BA3C.pf in 0.01482920 seconds -----
----- Processed .\artefacts\prefetch\CHROME.E
XE-AED7BA3D.pf in 0.01761800 seconds -----
----- Processed .\artefacts\prefetch\CHROME.E
XE-AED7BA3E.pf in 0.00884570 seconds -----
----- Processed .\artefacts\prefetch\CHROME.E
XE-AED7BA40.pf in 0.00660300 seconds -----
----- Processed .\artefacts\prefetch\CHROME.E
XE-AED7BA45.pf in 0.00852070 seconds -----
----- Processed .\artefacts\prefetch\CHROME.E
XE-AED7BA47.pf in 0.00594940 seconds -----
----- Processed .\artefacts\prefetch\CHROME.E
XE-AED7BA4A.pf in 0.00528880 seconds -----
----- Processed .\artefacts\prefetch\CHROMESE
TUP.EXE-A7F215CA.pf in 0.00738260 seconds -----
--
----- Processed .\artefacts\prefetch\CMD.EXE-
0BD30981.pf in 0.00596200 seconds -----
----- Processed .\artefacts\prefetch\COMPATTE

```

```

LRUNNER.EXE-B7A68ECC.pf in 0.00700660 seconds ----
-----
----- Processed .\artefacts\prefetch\CONHOST.
EXE-0C6456FB.pf in 0.00964020 seconds -----
----- Processed .\artefacts\prefetch\CONSENT.
EXE-40419367.pf in 0.00777760 seconds -----
----- Processed .\artefacts\prefetch\CPINSTC
U.EXE-3BDE08CA.pf in 0.00681010 seconds -----
----- Processed .\artefacts\prefetch\CSRSS.EX
E-F3C368CB.pf in 0.00764140 seconds -----
----- Processed .\artefacts\prefetch\CTFMON.E
XE-795F8130.pf in 0.00681030 seconds -----
----- Processed .\artefacts\prefetch\DATAEXCH
ANGEHOST.EXE-8B66795C.pf in 0.00786340 seconds ---
-----
----- Processed .\artefacts\prefetch\DEFRAG.E
XE-3D9E8D72.pf in 0.00654950 seconds -----
----- Processed .\artefacts\prefetch\DIRECTXD
ATABASEUPDATER.EXE-7B8AED66.pf in 0.00736190 secon
ds -----
----- Processed .\artefacts\prefetch\DISMHOS
T.EXE-89B7E4B6.pf in 0.00795120 seconds -----
----- Processed .\artefacts\prefetch\DISMHOS
T.EXE-9ED88D89.pf in 0.00800020 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-074772BA.pf in 0.00651810 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-16537BE1.pf in 0.02198900 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-1A12D5C8.pf in 0.03027970 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-1BAE06BB.pf in 0.01380080 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-47BE07DC.pf in 0.01622210 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-6F625E57.pf in 0.03004930 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-742E0212.pf in 0.04396500 seconds -----

```

```

----- Processed .\artefacts\prefetch\DLLHOST.
EXE-7D5CE0CA.pf in 0.00793640 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-810B6BBE.pf in 0.01322920 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-895D23F2.pf in 0.01136280 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-A6DA1980.pf in 0.01811030 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-B6ED8881.pf in 0.01192420 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-C7F45418.pf in 0.00859910 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-CF58F4A8.pf in 0.00735000 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-DEEF2761.pf in 0.00856490 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-ECDCE3C.pf in 0.00863160 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-F6E270D2.pf in 0.00936970 seconds -----
----- Processed .\artefacts\prefetch\DLLHOST.
EXE-F7FC6593.pf in 0.00623600 seconds -----
----- Processed .\artefacts\prefetch\DRVINST.
EXE-39D9EAC7.pf in 0.01514700 seconds -----
----- Processed .\artefacts\prefetch\DSMUSER
ASK.EXE-853A6893.pf in 0.01389970 seconds -----
--
----- Processed .\artefacts\prefetch\DWM.EXE-
314E93C5.pf in 0.00784010 seconds -----
----- Processed .\artefacts\prefetch\ELEVATIO
N_SERVICE.EXE-84F3CFD3.pf in 0.00655350 seconds --
-----
----- Processed .\artefacts\prefetch\ELEVATIO
N_SERVICE.EXE-9F002A1E.pf in 0.00843030 seconds --
-----
----- Processed .\artefacts\prefetch\EXPLORE
R.EXE-54012F5E.pf in 0.00667080 seconds -----
----- Processed .\artefacts\prefetch\F65B37D7

```

```

-6CC3-45AC-8082-D0A15-A612753A.pf in 0.00790220 se
conds -----
----- Processed .\artefacts\prefetch\FILECOAU
TH.EXE-2FD9EA81.pf in 0.00807480 seconds -----
-
----- Processed .\artefacts\prefetch\FILECOAU
TH.EXE-8B04AFD8.pf in 0.01861550 seconds -----
-
----- Processed .\artefacts\prefetch\FILECOAU
TH.EXE-C81C0747.pf in 0.01714580 seconds -----
-
----- Processed .\artefacts\prefetch\FILECOAU
TH.EXE-DEBD4FBE.pf in 0.01497720 seconds -----
-
----- Processed .\artefacts\prefetch\FILECOAU
TH.EXE-E761558A.pf in 0.01810410 seconds -----
-
----- Processed .\artefacts\prefetch\FILESYNC
CONFIG.EXE-1EF029AA.pf in 0.02141630 seconds -----
-----
----- Processed .\artefacts\prefetch\FILESYNC
CONFIG.EXE-3104F3A4.pf in 0.02535830 seconds -----
-----
----- Processed .\artefacts\prefetch\FILESYNC
CONFIG.EXE-8C7A3841.pf in 0.02536950 seconds -----
-----
----- Processed .\artefacts\prefetch\FILESYNC
CONFIG.EXE-BE4D831B.pf in 0.01492500 seconds -----
-----
----- Processed .\artefacts\prefetch\FILESYNC
CONFIG.EXE-F25FA88D.pf in 0.02301660 seconds -----
-----
----- Processed .\artefacts\prefetch\FIRSTLOG
ONANIM.EXE-FA0BF656.pf in 0.02078360 seconds -----
-----
----- Processed .\artefacts\prefetch\FODHELPE
R.EXE-7F1ED892.pf in 0.02528330 seconds -----
----- Processed .\artefacts\prefetch\FONTDRVH

```

```

OST.EXE-8152304A.pf in 0.02797930 seconds -----
--
----- Processed .\artefacts\prefetch\FSQUIRT.
EXE-A8FF1DEB.pf in 0.02091720 seconds -----
----- Processed .\artefacts\prefetch\FULLTRUS
TNOTIFIER.EXE-CE8718CD.pf in 0.01715770 seconds --
-----
----- Processed .\artefacts\prefetch\GAMEBARF
TSERVER.EXE-06BA06F5.pf in 0.02544400 seconds ----
-----
----- Processed .\artefacts\prefetch\GENVALOB
J.EXE-12FC6795.pf in 0.02217080 seconds -----
----- Processed .\artefacts\prefetch\IDENTITY
_HELPER.EXE-2ABE7119.pf in 0.02464430 seconds ----
-----
----- Processed .\artefacts\prefetch\IDENTITY
_HELPER.EXE-92061327.pf in 0.03103030 seconds ----
-----
----- Processed .\artefacts\prefetch\INSTALLE
R.EXE-4EA35968.pf in 0.02250480 seconds -----
----- Processed .\artefacts\prefetch\INSTALLE
R.EXE-D59100F1.pf in 0.02225720 seconds -----
----- Processed .\artefacts\prefetch\IPCONFI
G.EXE-BFEC2AD0.pf in 0.02401520 seconds -----
----- Processed .\artefacts\prefetch\LOCKAPP.
EXE-4802742B.pf in 0.01845400 seconds -----
----- Processed .\artefacts\prefetch\LOGONU.
EXE-F639BD7E.pf in 0.02555090 seconds -----
----- Processed .\artefacts\prefetch\LPREMOV
E.EXE-570BDFF7.pf in 0.02081390 seconds -----
----- Processed .\artefacts\prefetch\MANAGE-B
DE.EXE-5D45B44A.pf in 0.01603260 seconds -----
-
----- Processed .\artefacts\prefetch\MICROSOF
T.SHAREPOINT.EXE-D515E8F9.pf in 0.02027980 seconds
-----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGEUPDATE.EXE-3531B324.pf in 0.02102140 seconds

```

```

-----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGEUPDATE.EXE-7A595326.pf in 0.01451240 seconds
-----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGEUPDATE.EXE-BE4DC3BA.pf in 0.02634660 seconds
-----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGEUPDATESETUP_X86_-2C61688C.pf in 0.01397250 se
conds -----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGEUPDATESETUP_X86_-600FA732.pf in 0.02673780 se
conds -----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGEUPDATESETUP_X86_-86BF8FAF.pf in 0.01621380 se
conds -----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGE_X64_150.0.4078.-27F27894.pf in 0.01208860 se
conds -----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGE_X64_150.0.4078.-8538F89C.pf in 0.01215270 se
conds -----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGE_X64_151.0.4129.-2B9767EC.pf in 0.00856370 se
conds -----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGE_X64_151.0.4129.-37A435BE.pf in 0.00847380 se
conds -----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGE_X64_151.0.4129.-3AA12C42.pf in 0.00724490 se
conds -----
----- Processed .\artefacts\prefetch\MICROSOF
TEDGE_X64_151.0.4129.-C50F0A38.pf in 0.00910770 se
conds -----
----- Processed .\artefacts\prefetch\MMC.EXE-
410C5F73.pf in 0.00845640 seconds -----
----- Processed .\artefacts\prefetch\MOBSYNC.
EXE-B307E1CC.pf in 0.02017980 seconds -----

```

```

----- Processed .\artefacts\prefetch\M0FCOMP.
EXE-5225C32D.pf in 0.02534820 seconds -----
----- Processed .\artefacts\prefetch\MONOTIFI
CATIONUX.EXE-23180524.pf in 0.02134400 seconds ---
-----
----- Processed .\artefacts\prefetch\MONOTIFI
CATIONUX.EXE-62024999.pf in 0.01656300 seconds ---
-----
----- Processed .\artefacts\prefetch\MOUSOCOR
EWORKER.EXE-3EF8346A.pf in 0.02131560 seconds ----
-----
----- Processed .\artefacts\prefetch\MOUSOCOR
EWORKER.EXE-44A01CE7.pf in 0.01403290 seconds ----
-----
----- Processed .\artefacts\prefetch\MPAM-D_B
D_1.455.131.0.EXE-3A9BB306.pf in 0.02093640 second
s -----
----- Processed .\artefacts\prefetch\MPCMDRU
N.EXE-2C9109F9.pf in 0.02208170 seconds -----
----- Processed .\artefacts\prefetch\MPCMDRU
N.EXE-53D6BCA3.pf in 0.01769460 seconds -----
----- Processed .\artefacts\prefetch\MPCMDRU
N.EXE-D97D4C20.pf in 0.01353710 seconds -----
----- Processed .\artefacts\prefetch\MPDEFEND
ERCORESERVICE.EXE-066E134E.pf in 0.02401540 second
s -----
----- Processed .\artefacts\prefetch\MPDEFEND
ERCORESERVICE.EXE-EFA342B9.pf in 0.01537070 second
s -----
----- Processed .\artefacts\prefetch\MPRECOVE
RY.EXE-0EE3DE78.pf in 0.01899420 seconds -----
-
----- Processed .\artefacts\prefetch\MPRECOVE
RY.EXE-F2041713.pf in 0.02522690 seconds -----
-
----- Processed .\artefacts\prefetch\MPSIGSTU
B.EXE-0D70515F.pf in 0.02200420 seconds -----
----- Processed .\artefacts\prefetch\MPSIGSTU

```

```

B.EXE-12C529AD.pf in 0.07636820 seconds -----
----- Processed .\artefacts\prefetch\MPSIGSTU
B.EXE-16581E9A.pf in 0.02277890 seconds -----
----- Processed .\artefacts\prefetch\MPSIGSTU
B.EXE-5D0450B3.pf in 0.02145300 seconds -----
----- Processed .\artefacts\prefetch\MPSIGSTU
B.EXE-E6B2483B.pf in 0.02364860 seconds -----
----- Processed .\artefacts\prefetch\MRT.EXE-
46668014.pf in 0.01828310 seconds -----
----- Processed .\artefacts\prefetch\MSCORSV
W.EXE-16B291C4.pf in 0.15558780 seconds -----
----- Processed .\artefacts\prefetch\MSCORSV
W.EXE-8CE1A322.pf in 0.01896670 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25F9A.pf in 0.01603320 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25F9B.pf in 0.02030970 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25F9C.pf in 0.01913640 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25F9E.pf in 0.01419730 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25FA3.pf in 0.01973710 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25FA4.pf in 0.01783770 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25FA5.pf in 0.02324010 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25FA7.pf in 0.01931850 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25FA8.pf in 0.02100340 seconds -----
----- Processed .\artefacts\prefetch\MSEDGE.E
XE-37D25FAA.pf in 0.02186680 seconds -----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-0ABB0366.pf in 0.01888540 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-0ABB0367.pf in 0.02344430 seconds -----

```

```

-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-0ABB0368.pf in 0.01916900 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-0ABB036A.pf in 0.02247130 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-0ABB0370.pf in 0.01247660 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-0ABB0371.pf in 0.02641180 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-0ABB0373.pf in 0.02260300 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-0ABB0374.pf in 0.01898610 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-1FED5E1E.pf in 0.01876870 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-1FED5E28.pf in 0.01819040 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-226B385B.pf in 0.02108940 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-226B3863.pf in 0.02001430 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-226B3864.pf in 0.01737160 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-226B3867.pf in 0.03404330 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE

```

```

BVIEW2.EXE-35087E8B.pf in 0.01915880 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-35087E8C.pf in 0.02755150 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-35087E8D.pf in 0.01453140 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-35087E8F.pf in 0.01418590 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-35087E96.pf in 0.02438290 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-35087E98.pf in 0.01221770 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-4CB30793.pf in 0.01888010 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-4CB30794.pf in 0.02585530 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-4CB30796.pf in 0.01701610 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-4CB3079D.pf in 0.01412180 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-4CB3079F.pf in 0.01704380 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-4CB8B388.pf in 0.01895860 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEdgeWE
BVIEW2.EXE-4CB8B389.pf in 0.01728050 seconds -----
-----

```

```
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-4CB8B38C.pf in 0.01367120 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-DF78B31A.pf in 0.02101940 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-DF78B31B.pf in 0.01783390 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-DF78B323.pf in 0.02270030 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-DF78B324.pf in 0.02071070 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-DF78B326.pf in 0.02176650 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-DF78B327.pf in 0.02521140 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-E34645C7.pf in 0.02195210 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-E34645C9.pf in 0.02442210 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-E34645CB.pf in 0.02612400 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-E34645D1.pf in 0.02140890 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-E34645D2.pf in 0.01677770 seconds -----
-----
----- Processed .\artefacts\prefetch\MSEDGEWE
BVIEW2.EXE-E34645D5.pf in 0.03011050 seconds -----
```

```

-----
----- Processed .\artefacts\prefetch\MSIEB6E.
TMP-6F471F13.pf in 0.01283680 seconds -----
----- Processed .\artefacts\prefetch\MSIEXEC.
EXE-8FFB1633.pf in 0.01879780 seconds -----
----- Processed .\artefacts\prefetch\MSIEXEC.
EXE-CDBFC0F7.pf in 0.03061040 seconds -----
----- Processed .\artefacts\prefetch\MSMPENG.
EXE-21B1E0B5.pf in 0.06000900 seconds -----
----- Processed .\artefacts\prefetch\MSMPENG.
EXE-558DCD36.pf in 0.00924320 seconds -----
----- Processed .\artefacts\prefetch\MSMPENG.
EXE-57141DF0.pf in 0.00886630 seconds -----
----- Processed .\artefacts\prefetch\NGEN.EXE
-4A8DA13E.pf in 0.00669750 seconds -----
----- Processed .\artefacts\prefetch\NGEN.EXE
-734C6620.pf in 0.00769420 seconds -----
----- Processed .\artefacts\prefetch\NGENTAS
K.EXE-0E6CEC17.pf in 0.00817920 seconds -----
----- Processed .\artefacts\prefetch\NGENTAS
K.EXE-849BFD75.pf in 0.00773380 seconds -----
----- Processed .\artefacts\prefetch\NISSRV.E
XE-36A5B16E.pf in 0.00782960 seconds -----
----- Processed .\artefacts\prefetch\NISSRV.E
XE-CEA330BB.pf in 0.00702010 seconds -----
----- Processed .\artefacts\prefetch\NOTEPAD.
EXE-DDF178E9.pf in 0.00907890 seconds -----
----- Processed .\artefacts\prefetch\NPP.8.9.
6.2.INSTALLER.X64.EXE-8F84A84E.pf in 0.02641160 se
conds -----
----- Processed .\artefacts\prefetch\OLKFULLT
RUSTEXECUTOR.EXE-6CEE7F9F.pf in 0.02049160 seconds
-----
----- Processed .\artefacts\prefetch\ONEDRIV
E.EXE-D76FABD0.pf in 0.02490690 seconds -----
----- Processed .\artefacts\prefetch\ONEDRIV
E.SYNC.SERVICE.EXE-7389B2F0.pf in 0.02665010 secon
ds -----

```

```

----- Processed .\artefacts\prefetch\ONEDRIVE.SYNC.SERVICE.EXE-C709AD1C.pf in 0.01718750 seconds -----
----- Processed .\artefacts\prefetch\ONEDRIVE.SYNC.SERVICE.EXE-CA481341.pf in 0.01607940 seconds -----
----- Processed .\artefacts\prefetch\ONEDRIVE.SYNC.SERVICE.EXE-E6D73D4B.pf in 0.01700320 seconds -----
----- Processed .\artefacts\prefetch\ONEDRIVE.SETUP.EXE-2F4C4906.pf in 0.02189960 seconds -----
-----
----- Processed .\artefacts\prefetch\ONEDRIVE.SETUP.EXE-E5884418.pf in 0.01824700 seconds -----
-----
----- Processed .\artefacts\prefetch\OPENCONSOLE.EXE-5C87B3C6.pf in 0.02194990 seconds -----
--
----- Processed .\artefacts\prefetch\OPENWITH.EXE-8B50D58B.pf in 0.03095470 seconds -----
----- Processed .\artefacts\prefetch\POWERCFG.EXE-954C9186.pf in 0.01405330 seconds -----
----- Processed .\artefacts\prefetch\POWERSHELL.EXE-AE8EDC9B.pf in 0.02740170 seconds -----
-
----- Processed .\artefacts\prefetch\POWERSHELL.EXE-CA1AE517.pf in 0.02148780 seconds -----
-
----- Processed .\artefacts\prefetch\RAREXTINSTALLER.EXE-E36B143E.pf in 0.02099950 seconds ----
-----
----- Processed .\artefacts\prefetch\READER_EN_R9BVLF8K_INSTALL.EX-FFF35C41.pf in 0.02380770 seconds -----
----- Processed .\artefacts\prefetch\REGSVR32.EXE-03D3FB87.pf in 0.01870810 seconds -----
----- Processed .\artefacts\prefetch\REGSVR32.EXE-B31EC963.pf in 0.01688100 seconds -----

```

```

----- Processed .\artefacts\prefetch\RUNDLL3
2.EXE-27E52A2D.pf in 0.01558050 seconds -----
----- Processed .\artefacts\prefetch\RUNDLL3
2.EXE-36D847E4.pf in 0.01237670 seconds -----
----- Processed .\artefacts\prefetch\RUNDLL3
2.EXE-6F26928C.pf in 0.01266200 seconds -----
----- Processed .\artefacts\prefetch\RUNDLL3
2.EXE-75313621.pf in 0.02483590 seconds -----
----- Processed .\artefacts\prefetch\RUNDLL3
2.EXE-ABDD26A5.pf in 0.01351990 seconds -----
----- Processed .\artefacts\prefetch\RUNDLL3
2.EXE-BE8830B6.pf in 0.01580000 seconds -----
----- Processed .\artefacts\prefetch\RUNDLL3
2.EXE-C0159C27.pf in 0.02866870 seconds -----
----- Processed .\artefacts\prefetch\RUNONCE.
EXE-BD8A4C8F.pf in 0.01600380 seconds -----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-0725D89A.pf in 0.03422100 seconds -----
-----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-1C911A7E.pf in 0.01480730 seconds -----
-----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-2C5A250C.pf in 0.01407610 seconds -----
-----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-359F036E.pf in 0.02247350 seconds -----
-----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-3E0B5307.pf in 0.01625240 seconds -----
-----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-4551A062.pf in 0.01435610 seconds -----
-----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-463D1322.pf in 0.02185130 seconds -----
-----
----- Processed .\artefacts\prefetch\RUNTIMEB

```

```

ROKER.EXE-4B570750.pf in 0.02048370 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-50503558.pf in 0.02561310 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-679BDFB7.pf in 0.01720180 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-734B97AA.pf in 0.01818540 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-74648FC2.pf in 0.02059900 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-824A470C.pf in 0.01435480 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-8657B60D.pf in 0.01725260 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-8E498C90.pf in 0.01499850 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-94F69FEA.pf in 0.02966420 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-9E81A438.pf in 0.02013100 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-A2AE195E.pf in 0.01370520 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-ACF4B348.pf in 0.01758530 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-B2BB82C3.pf in 0.01410140 seconds -----
----

```

```

----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-B3420CE1.pf in 0.02543870 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-BD9F1C99.pf in 0.02209830 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-C6B81CFE.pf in 0.01747090 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-E6FD6E45.pf in 0.03705520 seconds -----
----
----- Processed .\artefacts\prefetch\RUNTIMEB
ROKER.EXE-F63AE499.pf in 0.02553840 seconds -----
----
----- Processed .\artefacts\prefetch\SDBINST.
EXE-49E8B208.pf in 0.02089260 seconds -----
----- Processed .\artefacts\prefetch\SDIAGNHO
ST.EXE-B3171AA1.pf in 0.01607650 seconds -----
-
----- Processed .\artefacts\prefetch\SEARCHFI
LTERHOST.EXE-44162447.pf in 0.03064820 seconds ---
-----
----- Processed .\artefacts\prefetch\SEARCHHO
ST.EXE-219561B2.pf in 0.02167850 seconds -----
-
----- Processed .\artefacts\prefetch\SEARCHHO
ST.EXE-6487E6F2.pf in 0.02576000 seconds -----
-
----- Processed .\artefacts\prefetch\SEARCHIN
DEXER.EXE-1CF42BC6.pf in 0.01931980 seconds -----
----
----- Processed .\artefacts\prefetch\SEARCHPR
OTOCOLHOST.EXE-69C456C3.pf in 0.02397320 seconds -
-----
----- Processed .\artefacts\prefetch\SECURITY
HEALTHHOST.EXE-06344EE9.pf in 0.02002330 seconds -
-----

```

```

----- Processed .\artefacts\prefetch\SECURITY
HEALTHHOST.EXE-114869E6.pf in 0.01460680 seconds -
-----
----- Processed .\artefacts\prefetch\SECURITY
HEALTHHOST.EXE-5F9A48BB.pf in 0.02110680 seconds -
-----
----- Processed .\artefacts\prefetch\SECURITY
HEALTHSERVICE.EXE-91B5FB98.pf in 0.02535840 second
S -----
----- Processed .\artefacts\prefetch\SECURITY
HEALTHSETUP.EXE-554F8020.pf in 0.01964200 seconds
-----
----- Processed .\artefacts\prefetch\SECURITY
HEALTHSETUP.EXE-E57E89CA.pf in 0.01650450 seconds
-----
----- Processed .\artefacts\prefetch\SECURITY
HEALTHSYSTRAY.EXE-E527A4AE.pf in 0.01680590 second
S -----
----- Processed .\artefacts\prefetch\SETUP.EX
E-104E171A.pf in 0.01614780 seconds -----
----- Processed .\artefacts\prefetch\SETUP.EX
E-208AF6E5.pf in 0.01568950 seconds -----
----- Processed .\artefacts\prefetch\SETUP.EX
E-9A26F6C5.pf in 0.02985330 seconds -----
----- Processed .\artefacts\prefetch\SETUP.EX
E-B3DEB2A8.pf in 0.02149500 seconds -----
----- Processed .\artefacts\prefetch\SETUP.EX
E-B3DEB2AC.pf in 0.02458400 seconds -----
----- Processed .\artefacts\prefetch\SETUP.EX
E-F19BB198.pf in 0.02520900 seconds -----
----- Processed .\artefacts\prefetch\SETUP64.
EXE-6C6157AB.pf in 0.01759920 seconds -----
----- Processed .\artefacts\prefetch\SHELLEXP
ERIENCEHOST.EXE-408EBC4F.pf in 0.01938680 seconds
-----
----- Processed .\artefacts\prefetch\SHELLEXP
ERIENCEHOST.EXE-E14F1772.pf in 0.01414480 seconds
-----

```

```

----- Processed .\artefacts\prefetch\SHOWAPPP
ICKERFORPDF.EXE-29859212.pf in 0.01367460 seconds
-----
----- Processed .\artefacts\prefetch\SIHCLIEN
T.EXE-98C47F6C.pf in 0.03798160 seconds -----
----- Processed .\artefacts\prefetch\SINGLECL
IENTSERVICESUPDATER.E-E9F25D12.pf in 0.02134280 se
conds -----
----- Processed .\artefacts\prefetch\SLUI.EXE
-3E441AEE.pf in 0.01657940 seconds -----
----- Processed .\artefacts\prefetch\SMARTSCR
EEN.EXE-EACC1250.pf in 0.01229660 seconds -----
--
----- Processed .\artefacts\prefetch\SOFTLAND
INGTASK.EXE-A93C9879.pf in 0.01287250 seconds ----
-----
----- Processed .\artefacts\prefetch\SPPEXTCO
MOBJ.EXE-7D45A1AB.pf in 0.01285810 seconds -----
---
----- Processed .\artefacts\prefetch\SPPSVC.E
XE-96070FE0.pf in 0.01176530 seconds -----
----- Processed .\artefacts\prefetch\STARTMEN
UEXPERIENCEHOST.EXE-3A8E567A.pf in 0.02114800 seco
nds -----
----- Processed .\artefacts\prefetch\STOREDES
KTOPEXTENSION.EXE-8825CB35.pf in 0.01401060 second
s -----
----- Processed .\artefacts\prefetch\STOREDES
KTOPEXTENSION.EXE-911C1E74.pf in 0.02043030 second
s -----
----- Processed .\artefacts\prefetch\STOREDES
KTOPEXTENSION.EXE-B3EC9917.pf in 0.02478540 second
s -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-09F4AEA4.pf in 0.02010600 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-117C4441.pf in 0.02021360 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.

```

```

EXE-1454AA18.pf in 0.02539870 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-19B557B1.pf in 0.01782670 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-1B73F444.pf in 0.01665250 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-26F10090.pf in 0.02586490 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-2A35E6EF.pf in 0.01627370 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-2C8D0E2C.pf in 0.01625900 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-2F9E5F3D.pf in 0.02106640 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-31E42122.pf in 0.02466350 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-3CF81F86.pf in 0.02138420 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-41084AF7.pf in 0.02827820 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-44191FB8.pf in 0.02326560 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-4B98D760.pf in 0.01977820 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-4BD0A607.pf in 0.02195880 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-4D0E9C8C.pf in 0.02396630 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-502A129B.pf in 0.01676530 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-529F9AC1.pf in 0.02071180 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-58520C26.pf in 0.01478240 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-59780EBF.pf in 0.01561710 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-5F87ABED.pf in 0.03362050 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.

```

```
EXE-62105D0D.pf in 0.03064340 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-677C0885.pf in 0.01627550 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-6867B1E5.pf in 0.01818590 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-6A4A44E7.pf in 0.01995130 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-73D024B2.pf in 0.02109130 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-764FA25C.pf in 0.01857480 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-77C41F85.pf in 0.01819850 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-7962F060.pf in 0.02250200 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-7AAD9645.pf in 0.02251450 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-84F32335.pf in 0.02092530 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-852EC587.pf in 0.02490570 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-8CE690C0.pf in 0.02053040 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-952637C2.pf in 0.03019150 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-9A28EB78.pf in 0.01017400 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-9EB5DE68.pf in 0.00575210 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-A21A7EFE.pf in 0.02138170 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-AA89143F.pf in 0.00909140 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-B18C213B.pf in 0.00765360 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.  
EXE-BC826E0F.pf in 0.00958200 seconds -----  
----- Processed .\artefacts\prefetch\SVCHOST.
```

```

EXE-BE3D0421.pf in 0.01875880 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-C2DA4F6F.pf in 0.02183350 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-C38EF8DD.pf in 0.01750550 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-C625B657.pf in 0.02755180 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-C88A2A3B.pf in 0.02153380 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-D2385079.pf in 0.03211700 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-D5481872.pf in 0.02212890 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-D8C907E1.pf in 0.02092070 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-DDF1360E.pf in 0.02345730 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-DF14C859.pf in 0.01526230 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-E5CD0034.pf in 0.02597410 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-EA9BB143.pf in 0.02102760 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-EBBF67E6.pf in 0.02562570 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-F952D9A9.pf in 0.02470160 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-FA38241C.pf in 0.01535930 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-FB759C0F.pf in 0.02769180 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-FC42C687.pf in 0.02100270 seconds -----
----- Processed .\artefacts\prefetch\SVCHOST.
EXE-FC46CD61.pf in 0.01603680 seconds -----
----- Processed .\artefacts\prefetch\SYSTEMIN
F0.EXE-3EAAF1C2.pf in 0.02101650 seconds -----
-

```

```

----- Processed .\artefacts\prefetch\SYSTEMSE
TTINGS.EXE-AD6D6913.pf in 0.02555790 seconds ----
-----
----- Processed .\artefacts\prefetch\SYSTEMSE
TTINGSADMINFLOWS.EXE-F74198E7.pf in 0.02631940 sec
onds -----
----- Processed .\artefacts\prefetch\TASKHOST
W.EXE-2E5D4B75.pf in 0.01849350 seconds -----
----- Processed .\artefacts\prefetch\TASKKIL
L.EXE-BE180FC8.pf in 0.02094000 seconds -----
----- Processed .\artefacts\prefetch\TIWORKE
R.EXE-C741055F.pf in 0.02661740 seconds -----
----- Processed .\artefacts\prefetch\TIWORKE
R.EXE-D1C044D3.pf in 0.02352050 seconds -----
----- Processed .\artefacts\prefetch\TRUSTEDI
NSTALLER.EXE-766EFF52.pf in 0.02093890 seconds ---
-----
----- Processed .\artefacts\prefetch\UIEORCHE
STRATOR.EXE-C4670673.pf in 0.02134450 seconds ----
-----
----- Processed .\artefacts\prefetch\UIEORCHE
STRATOR.EXE-C9987E34.pf in 0.01524840 seconds ----
-----
----- Processed .\artefacts\prefetch\UIEORCHE
STRATORSTUB.EXE-83FF9FFA.pf in 0.01818510 seconds
-----
----- Processed .\artefacts\prefetch\UNINSTAL
L.EXE-73AE4314.pf in 0.02145010 seconds -----
----- Processed .\artefacts\prefetch\UPDATEPL
ATFORM.AMD64FRE.EXE-804667A0.pf in 0.02101330 seco
nds -----
----- Processed .\artefacts\prefetch\UPDATEPL
ATFORM.EXE-CE2B2ACB.pf in 0.05282990 seconds ----
-----
----- Processed .\artefacts\prefetch\UPDATER.
EXE-A67BCD0A.pf in 0.02865420 seconds -----
----- Processed .\artefacts\prefetch\UPDATER.
EXE-B5E7C409.pf in 0.01829700 seconds -----

```

```

----- Processed .\artefacts\prefetch\UPFC.EXE
-89D4FAEB.pf in 0.01633660 seconds -----
----- Processed .\artefacts\prefetch\USER00BE
BROKER.EXE-65584ADF.pf in 0.02829760 seconds -----
-----
----- Processed .\artefacts\prefetch\USOCLIEN
T.EXE-4ADC110B.pf in 0.01959610 seconds -----
----- Processed .\artefacts\prefetch\VCREDIST
_X64.EXE-2FCEC7CA.pf in 0.02017690 seconds -----
---
----- Processed .\artefacts\prefetch\VCREDIST
_X64.EXE-EB72154A.pf in 0.02230620 seconds -----
---
----- Processed .\artefacts\prefetch\VCREDIST
_X86.EXE-215F1F4E.pf in 0.03111880 seconds -----
---
----- Processed .\artefacts\prefetch\VCREDIST
_X86.EXE-7375DF65.pf in 0.02244930 seconds -----
---
----- Processed .\artefacts\prefetch\VC_REDIS
T.X64.EXE-6FE859E3.pf in 0.02216010 seconds -----
----
----- Processed .\artefacts\prefetch\VC_REDIS
T.X86.EXE-FDDBA21E.pf in 0.02099650 seconds -----
----
----- Processed .\artefacts\prefetch\VDS.EXE-
2FCA9D16.pf in 0.01392110 seconds -----
----- Processed .\artefacts\prefetch\VDSLDR.E
XE-50179B50.pf in 0.02449530 seconds -----
----- Processed .\artefacts\prefetch\VERCLSI
D.EXE-AB0FD091.pf in 0.02016610 seconds -----
----- Processed .\artefacts\prefetch\VGAUTHSE
RVICE.EXE-779D9D39.pf in 0.02298360 seconds -----
----
----- Processed .\artefacts\prefetch\VLC-3.0.
23-WIN32.EXE-BF857A3D.pf in 0.01976630 seconds ---
-----
----- Processed .\artefacts\prefetch\VLC-CACH

```

```

E-GEN.EXE-5C78127E.pf in 0.02375720 seconds -----
-----
----- Processed .\artefacts\prefetch\VMT00LS
D.EXE-90328040.pf in 0.02366230 seconds -----
----- Processed .\artefacts\prefetch\VMWAREERE
SOLUTIONSET.EXE-38A925F2.pf in 0.02229280 seconds
-----
----- Processed .\artefacts\prefetch\VMWARETO
OLBOXCMD.EXE-FB464DC1.pf in 0.01556220 seconds ---
-----
----- Processed .\artefacts\prefetch\VSSVC.EX
E-6C8F0C66.pf in 0.01843110 seconds -----
----- Processed .\artefacts\prefetch\WAASMEDI
CAGENT.EXE-21F161ED.pf in 0.01904720 seconds -----
-----
----- Processed .\artefacts\prefetch\WERFAUL
T.EXE-8EE1E6D7.pf in 0.02578530 seconds -----
----- Processed .\artefacts\prefetch\WERMGR.E
XE-BE3A79B5.pf in 0.02161270 seconds -----
----- Processed .\artefacts\prefetch\WERMGR.E
XE-F439C551.pf in 0.01372730 seconds -----
----- Processed .\artefacts\prefetch\WEVTUTI
L.EXE-1E154F39.pf in 0.01288410 seconds -----
----- Processed .\artefacts\prefetch\WHOAMI.E
XE-9D378AFE.pf in 0.01606670 seconds -----
----- Processed .\artefacts\prefetch\WIDGETS.
EXE-93188904.pf in 0.01494400 seconds -----
----- Processed .\artefacts\prefetch\WIDGETS.
EXE-AF9DC2D4.pf in 0.02197290 seconds -----
----- Processed .\artefacts\prefetch\WIDGETS.
EXE-E998E6EC.pf in 0.02243110 seconds -----
----- Processed .\artefacts\prefetch\WIDGETSE
RVICE.EXE-03CC7297.pf in 0.02008800 seconds -----
-----
----- Processed .\artefacts\prefetch\WIDGETSE
RVICE.EXE-C21EFD8F.pf in 0.01860310 seconds -----
-----
----- Processed .\artefacts\prefetch\WINDOWS-

```

```

KB890830-X64-V5.142.E-92039E5E.pf in 0.01602450 se
conds -----
----- Processed .\artefacts\prefetch\WINDOWSP
ACKAGEMANAGERSERVER.E-AFF4EFA9.pf in 0.04643860 se
conds -----
----- Processed .\artefacts\prefetch\WINDOWST
ERMINAL.EXE-0DDF887E.pf in 0.02120960 seconds ----
-----
----- Processed .\artefacts\prefetch\WINDOWST
ERMINAL.EXE-3DD18850.pf in 0.02039040 seconds ----
-----
----- Processed .\artefacts\prefetch\WINLOGO
N.EXE-DEDDC9B6.pf in 0.01669410 seconds -----
----- Processed .\artefacts\prefetch\WINRAR-X
64-723.EXE-FDDE966E.pf in 0.02151860 seconds -----
-----
----- Processed .\artefacts\prefetch\WINSAT.E
XE-C345C80B.pf in 0.02116730 seconds -----
----- Processed .\artefacts\prefetch\WINSTOR
E.APP.EXE-D3CC3D1B.pf in 0.02034100 seconds -----
-----
----- Processed .\artefacts\prefetch\WLRMDR.E
XE-A7C36FDD.pf in 0.02171100 seconds -----
----- Processed .\artefacts\prefetch\WMIADAP.
EXE-BB21CD77.pf in 0.01979540 seconds -----
----- Processed .\artefacts\prefetch\WMIAPSR
V.EXE-FC8436DD.pf in 0.02106080 seconds -----
----- Processed .\artefacts\prefetch\WMIPRVS
E.EXE-E8B8DD29.pf in 0.02038630 seconds -----
----- Processed .\artefacts\prefetch\WSCRIPT.
EXE-3FF4D889.pf in 0.02571210 seconds -----
----- Processed .\artefacts\prefetch\WUAUCLTC
ORE.EXE-07BDE0CF.pf in 0.01548390 seconds -----
--
----- Processed .\artefacts\prefetch\WUAUCLTC
ORE.EXE-84257BB2.pf in 0.02103660 seconds -----
--
----- Processed .\artefacts\prefetch\WWAHOST.

```

```

EXE-55C529F0.pf in 0.02403860 seconds -----
----- Processed .\artefacts\prefetch\ZOOM.EXE
-953DDC7B.pf in 0.02204500 seconds -----
----- Processed .\artefacts\prefetch\ZOOMINST
ALLERFULL.EXE-3C7F6855.pf in 0.01436900 seconds --
-----

```

Processed 413 out of 413 files in 8.3320 seconds

CSV output will be saved to .\analysis\prefetch\20260823154251_PECmd_Output.csv

CSV time line output will be saved to .\analysis\prefetch\20260823154251_PECmd_Output_Timeline.csv

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1>

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1> D:\UOW\SEM3\Tools\ZimmermanTools\net9\PECmd.exe -d .\artefacts\prefetch --csv .\analysis\prefetch -q
PECmd version 2026.5.0

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

Command line: -d .\artefacts\prefetch --csv .\analysis\prefetch -q

Warning: Administrator privileges not found!

Keywords: temp, tmp

Looking for prefetch files in .\artefacts\prefetch

Found 413 Prefetch files

----- Processed .\artefacts\prefetch\151.0.7922.138_CHROME_INSTALL-FFDC6407.pf in 0.03313970 seconds -----
----- Processed .\artefacts\prefetch\ACROBAT.EXE-F94F9B29.pf in 0.02532590 seconds -----
----- Processed .\artefacts\prefetch\ACROBAT.EXE-F94F9B2A.pf in 0.02216370 seconds -----
----- Processed .\artefacts\prefetch\ACROBAT.EXE-F94F9B30.pf in 0.01425850 seconds -----
----- Processed .\artefacts\prefetch\ADNOTIFICATIONMANAGER.EXE-E7F9E8B8.pf in 0.02075990 seconds -----
----- Processed .\artefacts\prefetch\ADOBESLIM.EXE-F9223367.pf in 0.01705310 seconds -----
----- Processed .\artefacts\prefetch\ADOBESLIMHELPER.EXE-E37F7F0C.pf in 0.00750680 seconds -----
----- Processed .\artefacts\prefetch\ADOBESLIMHELPER.EXE-FAB8E1EF.pf in 0.01305850 seconds -----
----- Processed .\artefacts\prefetch\ADOBESLIM.UCB.EXE-C04E772A.pf in 0.00704780 seconds -----
----- Processed .\artefacts\prefetch\ADOBECOLLABS.VNC.EXE-A30339B6.pf in 0.00669110 seconds -----
----- Processed .\artefacts\prefetch\AM_BASE.EXE-3F70DC96.pf in 0.00656360 seconds -----
----- Processed .\artefacts\prefetch\AM_BASE_PATCH1.EXE-B2AC3990.pf in 0.00533920 seconds -----
----- Processed .\artefacts\prefetch\AM_DELTA.EXE-78CA83B0.pf in 0.00619020 seconds -----
----- Processed .\artefacts\prefetch\AM_ENGINE.EXE-F1C956E4.pf in 0.00661250 seconds -----
----- Processed .\artefacts\prefetch\AM_ENGINE_PATCH1.1.26060.300-49F3FAFB.pf in 0.00537560 seconds -----
----- Processed .\artefacts\prefetch\APPRACTIONS.EXE-D77D7F4C.pf in 0.00659740 seconds -----
----- Processed .\artefacts\prefetch\APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf in 0.00700040 seconds -----
----- Processed .\artefacts\prefetch\ARMSVC.EXE-A68AEEA4.pf in 0.00829600 seconds -----
----- Processed .\artefacts\prefetch\AUDIODOG.EXE-AB22E9A6.pf in 0.00671630 seconds -----
----- Processed .\artefacts\prefetch\AUDITPOL.EXE-2D4A3037.pf in 0.00576920 seconds -----
----- Processed .\artefacts\prefetch\BACKGROUNDTASKHOST.EXE-4589797A.pf in 0.00682690 seconds -----
----- Processed .\artefacts\prefetch\BACKGROUNDTASKHOST.EXE-51333CCD.pf in 0.00586080 seconds -----

```

```

Processed \artefacts\prefetch\WERFAULT.EXE-8EE1E6D7.pf in 0.02578530 seconds
Processed \artefacts\prefetch\WERMGR.EXE-BE3A7985.pf in 0.02161270 seconds
Processed \artefacts\prefetch\WERMGR.EXE-F439C551.pf in 0.01372730 seconds
Processed \artefacts\prefetch\WEVTUTIL.EXE-1E154F39.pf in 0.01288410 seconds
Processed \artefacts\prefetch\WHOAMI.EXE-9D378AFE.pf in 0.01606670 seconds
Processed \artefacts\prefetch\WIDGETS.EXE-93188904.pf in 0.01494400 seconds
Processed \artefacts\prefetch\WIDGETS.EXE-AF9DC2D4.pf in 0.02197290 seconds
Processed \artefacts\prefetch\WIDGETS.EXE-E998E6EC.pf in 0.02243110 seconds
Processed \artefacts\prefetch\WIDGETSERVICE.EXE-03CC7297.pf in 0.02008800 seconds
Processed \artefacts\prefetch\WIDGETSERVICE.EXE-C21EFD8F.pf in 0.01860310 seconds
Processed \artefacts\prefetch\WINDOWS-KB890830-X64-V5.142.E-92039E5E.pf in 0.01602450 seconds
Processed \artefacts\prefetch\WINDOWSPACKAGEMANAGERSERVER.E-AFF4EFA9.pf in 0.04643860 seconds
Processed \artefacts\prefetch\WINDOWSTERMINAL.EXE-0DDF887E.pf in 0.02120960 seconds
Processed \artefacts\prefetch\WINDOWSTERMINAL.EXE-3DD18850.pf in 0.02039040 seconds
Processed \artefacts\prefetch\WINLOGON.EXE-DEDDC9B6.pf in 0.01669410 seconds
Processed \artefacts\prefetch\WINRAR-X64-723.EXE-FDDE966E.pf in 0.02151860 seconds
Processed \artefacts\prefetch\WINSAT.EXE-C345C80B.pf in 0.02116730 seconds
Processed \artefacts\prefetch\WINSTORE.APP.EXE-D3CC3D1B.pf in 0.02034100 seconds
Processed \artefacts\prefetch\WLMRDR.EXE-A7C36FDD.pf in 0.02171100 seconds
Processed \artefacts\prefetch\WMIADAP.EXE-BB21CD77.pf in 0.01979540 seconds
Processed \artefacts\prefetch\WMIAPSRV.EXE-FC8436DD.pf in 0.02106080 seconds
Processed \artefacts\prefetch\WMIPIRVSE.EXE-E888DD29.pf in 0.02038630 seconds
Processed \artefacts\prefetch\WSCRIPT.EXE-3FF4D889.pf in 0.02571210 seconds
Processed \artefacts\prefetch\WUAUCLTCORE.EXE-07BDE0CF.pf in 0.01548390 seconds
Processed \artefacts\prefetch\WUAUCLTCORE.EXE-84257BB2.pf in 0.02103660 seconds
Processed \artefacts\prefetch\WMAHOST.EXE-55C529F0.pf in 0.02403860 seconds
Processed \artefacts\prefetch\ZOOM.EXE-953DDC7B.pf in 0.02204500 seconds
Processed \artefacts\prefetch\ZOOMINSTALLERFULL.EXE-3C7F6855.pf in 0.01436900 seconds

Processed 413 out of 413 files in 8.3320 seconds

CSV output will be saved to .\analysis\prefetch\20260823154251_PECmd_Output.csv
CSV time line output will be saved to .\analysis\prefetch\20260823154251_PECmd_Output_Timeline.csv
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1>

```

- Parse Event Logs with EvtxECmd

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1> mkdir .\analysis\event_logs -Force | Out-Null

```

```

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1> D:\UOW\SEM3\Tools\ZimmermanTools\net9\EvtxECmd\EvtxECmd.exe -d .\artefacts\event_logs --csv .\analysis\event_logs
EvtxECmd version 2026.5.0

```

Author: Eric Zimmerman (saericzimmerman@gmail.com)
<https://github.com/EricZimmerman/evttx>

Command line: -d .\artefacts\event_logs --csv .\analysis\event_logs

Warning: Administrator privileges not found!

CSV output will be saved to .\analysis\event_logs\20260823155321_EvtxECmd_Output.csv

Maps loaded: 383

Looking for event log files in .\artefacts\event_logs

Processing .\artefacts\event_logs\Application.evt
X...

Chunk count: 23, Iterating records...

Record #: 13 (timestamp: 2026-07-14 08:07:31.5270557): Warning! Time just went backwards! Last seen time before change: 2026-07-14 16:07:30.0696560

Record #: 793 (timestamp: 2026-07-14 12:12:07.2253414): Warning! Time just went backwards! Last seen time before change: 2026-07-16 07:46:41.3247835

Event log details

Flags: None

Chunk count: 23

Stored/Calculated CRC: 19AE6BFF/19AE6BFF

Earliest timestamp: 2026-07-14 08:07:31.5270557

Latest timestamp: 2026-08-16 09:27:37.3411204

Total event log records found: 1,222

Records included: 1,222 Errors: 0 Events dropped: 0

Metrics (including dropped events)

Event ID	Count
0	28
1	13
5	2
11	1
15	54
16	1
23	10
24	10
63	14
86	28
102	4
105	12
108	8
256	9

258	16
259	3
260	8
264	2
271	7
272	8
300	3
301	5
302	3
325	1
326	3
781	8
900	20
902	12
903	11
1001	102
1003	53
1004	26
1005	2
1008	1
1010	1
1013	1
1016	2
1022	2
1025	19
1029	1
1033	15
1034	144
1035	2
1036	2
1038	3
1040	9
1042	9
1066	12
1130	4
1531	14
1532	12
2562	157

4097	16
4108	1
4109	1
4111	3
4112	1
4113	1
4202	8
4625	1
5611	2
5615	14
5617	14
6000	35
6003	13
6004	1
8197	1
8198	13
8200	1
8208	1
8224	10
8230	4
10000	7
10001	7
10005	1
10010	3
11707	7
11728	1
11729	1
12288	18
12289	1
16384	63
16388	4
16394	67
20481	1
20482	1
20488	1
20489	1

Processing .\artefacts\event_logs\Microsoft-Window

s-DriverFrameworks-UserMode%40operational.evtx...
Chunk count: 1, Iterating records...

Event log details

Flags: None

Chunk count: 1

Stored/Calculated CRC: 917FDF0E/917FDF0E

Earliest timestamp: 2026-07-17 13:46:06.9141820

Latest timestamp: 2026-08-16 07:24:07.7874701

Total event log records found: 3

Records included: 3 Errors: 0 Events dropped: 0

Metrics (including dropped events)

Event ID	Count
1000	3

Processing .\artefacts\event_logs\Microsoft-Windows-Partition%4Diagnostic.evtx...

Chunk count: 1, Iterating records...

Record #: 5 (timestamp: 2026-07-14 08:10:22.1603994): Warning! Time just went backwards! Last seen time before change: 2026-07-14 16:07:18.4403733

Event log details

Flags: None

Chunk count: 1

Stored/Calculated CRC: C7D3DA4/C7D3DA4

Earliest timestamp: 2026-07-14 08:10:22.1603994

Latest timestamp: 2026-08-16 07:24:03.0945935

Total event log records found: 19

Records included: 19 Errors: 0 Events dropped: 0

Metrics (including dropped events)

Event ID	Count
1006	19

Processing .\artefacts\event_logs\Security.evtx...
Chunk count: 412, Iterating records...

Record # 26244 (Event Record Id: 26244): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string

Record # 26571 (Event Record Id: 26571): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string

Record #: 26873 (timestamp: 2026-07-14 12:12:06.6613870): Warning! Time just went backwards! Last seen time before change: 2026-07-16 07:46:46.9061620

Record # 28083 (Event Record Id: 28083): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string

Record # 29618 (Event Record Id: 29618): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string

Record # 31449 (Event Record Id: 31449): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string

Record # 34286 (Event Record Id: 34286): In map for event 1100, Property /Event/UserData[@Name="ServiceShutdown"] not found! Replacing with empty string

Event log details

Flags: None

Chunk count: 412

Stored/Calculated CRC: 16312577/16312577

Earliest timestamp: 2026-07-14 10:45:06.5454767

Latest timestamp: 2026-08-16 09:27:37.4016520

Total event log records found: 28,454

Records included: 28,454 Errors: 0 Events dropped:
0

Metrics (including dropped events)

Event ID	Count
1100	6
4608	6
4616	6
4624	654
4625	4
4634	10
4647	6
4648	28
4663	47
4672	626
4688	2,876
4689	2,712
4696	7
4719	5
4797	8
4798	98
4799	174
4800	3
4801	3
4826	6
4902	6
4907	20,301
5024	6
5033	6
5058	14
5059	11
5061	16
5379	771
5381	1
5382	20
6416	11
6417	6

```
Processing .\artefacts\event_logs\System.evtx...
Chunk count: 19, Iterating records...
Record #: 4 (timestamp: 2026-07-14 16:04:38.586329
3): Warning! Time just went backwards! Last seen t
ime before change: 2026-07-14 16:05:12.3882416
Record #: 192 (timestamp: 2026-07-14 16:07:04.4124
060): Warning! Time just went backwards! Last seen
time before change: 2026-07-14 16:07:29.4185786
Record # 194 (Event Record Id: 194): In map for ev
ent 13, Property /Event/EventData/Data[@Name="Boot
Mode"] not found! Replacing with empty string
Record #: 267 (timestamp: 2026-07-14 08:07:31.1709
170): Warning! Time just went backwards! Last seen
time before change: 2026-07-14 16:07:30.5841731
Record #: 322 (timestamp: 2026-07-14 08:10:10.6061
905): Warning! Time just went backwards! Last seen
time before change: 2026-07-14 08:10:26.5382742
Record # 324 (Event Record Id: 324): In map for ev
ent 13, Property /Event/EventData/Data[@Name="Boot
Mode"] not found! Replacing with empty string
Record #: 434 (timestamp: 2026-07-14 08:11:33.8877
616): Warning! Time just went backwards! Last seen
time before change: 2026-07-14 08:11:54.2802032
Record # 438 (Event Record Id: 438): In map for ev
ent 13, Property /Event/EventData/Data[@Name="Boot
Mode"] not found! Replacing with empty string
Record #: 551 (timestamp: 2026-07-14 08:25:14.9607
924): Warning! Time just went backwards! Last seen
time before change: 2026-07-14 08:25:32.9596247
Record # 553 (Event Record Id: 553): In map for ev
ent 13, Property /Event/EventData/Data[@Name="Boot
Mode"] not found! Replacing with empty string
Record #: 637 (timestamp: 2026-07-14 09:49:55.6788
044): Warning! Time just went backwards! Last seen
time before change: 2026-07-14 09:50:05.4442185
Record #: 833 (timestamp: 2026-07-14 09:58:08.5401
211): Warning! Time just went backwards! Last seen
time before change: 2026-07-14 09:58:16.4450483
```

Record #: 945 (timestamp: 2026-07-14 10:01:23.8054506): Warning! Time just went backwards! Last seen time before change: 2026-07-14 10:01:38.2514389

Record # 947 (Event Record Id: 947): In map for event 13, Property /Event/EventData/Data[@Name="Boot Mode"] not found! Replacing with empty string

Record #: 1337 (timestamp: 2026-07-14 11:28:28.3341302): Warning! Time just went backwards! Last seen time before change: 2026-07-14 11:28:45.9445730

Record # 1339 (Event Record Id: 1339): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string

Record #: 1482 (timestamp: 2026-07-14 11:30:12.3994888): Warning! Time just went backwards! Last seen time before change: 2026-07-14 11:30:27.6771167

Record # 1484 (Event Record Id: 1484): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string

Record #: 1587 (timestamp: 2026-07-14 11:37:41.3354294): Warning! Time just went backwards! Last seen time before change: 2026-07-14 11:38:00.8339177

Record # 1589 (Event Record Id: 1589): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string

Record #: 1682 (timestamp: 2026-07-14 12:11:53.2845826): Warning! Time just went backwards! Last seen time before change: 2026-07-16 07:46:33.9507927

Record #: 1688 (timestamp: 2026-07-14 12:12:06.6562667): Warning! Time just went backwards! Last seen time before change: 2026-07-16 07:46:37.1268039

Record #: 1714 (timestamp: 2026-07-14 12:36:05.1666129): Warning! Time just went backwards! Last seen time before change: 2026-07-16 08:18:49.5599141

Record #: 1745 (timestamp: 2026-07-16 10:48:16.8272673): Warning! Time just went backwards! Last seen time before change: 2026-07-17 13:26:32.8502364

Record #: 1780 (timestamp: 2026-07-17 13:41:19.1300010): Warning! Time just went backwards! Last seen

n time before change: 2026-07-17 13:46:08.3332977
Record # 1782 (Event Record Id: 1782): In map for
event 13, Property /Event/EventData/Data[@Name="Bo
otMode"] not found! Replacing with empty string
Record #: 1890 (timestamp: 2026-07-17 19:30:23.946
9510): Warning! Time just went backwards! Last see
n time before change: 2026-08-06 09:55:57.3289877
Record # 1892 (Event Record Id: 1892): In map for
event 13, Property /Event/EventData/Data[@Name="Bo
otMode"] not found! Replacing with empty string
Record #: 2037 (timestamp: 2026-08-06 10:18:52.049
5184): Warning! Time just went backwards! Last see
n time before change: 2026-08-12 09:15:49.6456902
Record #: 2058 (timestamp: 2026-08-12 09:16:50.341
5917): Warning! Time just went backwards! Last see
n time before change: 2026-08-16 07:24:08.6393717
Record # 2060 (Event Record Id: 2060): In map for
event 13, Property /Event/EventData/Data[@Name="Bo
otMode"] not found! Replacing with empty string

Event log details

Flags: None

Chunk count: 19

Stored/Calculated CRC: 9C8D9DE0/9C8D9DE0

Earliest timestamp: 2026-07-14 08:07:31.1709170

Latest timestamp: 2026-08-16 09:27:37.3741844

Total event log records found: 2,358

Records included: 2,358 Errors: 0 Events dropped:
0

Metrics (including dropped events)

Event ID	Count
1	31
3	15
4	2
6	213
11	1

12	34
13	11
14	14
15	13
16	392
18	27
19	123
20	33
22	4
23	14
24	32
25	42
26	1
27	18
30	1
32	33
34	1
35	2
37	10
41	2
42	1
43	104
44	194
52	1
55	56
98	29
100	2
107	1
109	11
112	242
129	1
134	1
153	14
172	14
238	14
247	14
519	1
566	10

577	11
1025	14
1027	1
1038	6
1039	8
1041	14
1074	12
1282	14
1500	1
1501	2
1796	6
2004	1
2005	1
3261	1
4107	4
4500	1
4501	1
6005	14
6006	12
6008	2
6009	14
6011	3
6013	18
6156	14
7001	13
7002	11
7023	1
7026	14
7030	1
7040	104
7045	28
10005	1
10010	2
10016	34
15007	9
15008	10
16962	14
16977	15

16983	14
20003	5
50036	28
50037	12
50103	14
50104	12
50105	12
50106	12
51046	14
51047	12
51057	12

Processed 5 files in 9.2672 seconds

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario
io_1>

```
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1> mkdir .\analysis\event_logs -Force | Out-Null
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1> D:\UOW\SEM3\Tools\ZimmermanTools\net9\EvtxECmd\EvtxECmd.exe -d .\artefacts\event_logs --csv .\analysis\event_logs
EvtxECmd version 2026.5.0
Author: Eric Zimmerman (sericzimmerman@gmail.com)
https://github.com/EricZimmerman/evt
Command line: -d .\artefacts\event_logs --csv .\analysis\event_logs
Warning: Administrator privileges not found!
CSV output will be saved to .\analysis\event_logs\20260823155321_EvtxECmd_Output.csv
Maps loaded: 383
Looking for event log files in .\artefacts\event_logs
Processing .\artefacts\event_logs\Application.evtx...
Chunk count: 21; Iterating records...
Record #: 13 (timestamp: 2026-07-14 08:07:31.5278557): Warning! Time just went backwards! Last seen time before change: 2026-07-14 16:07:30.0696560
Record #: 793 (timestamp: 2026-07-14 12:12:07.2253416): Warning! Time just went backwards! Last seen time before change: 2026-07-16 07:46:41.3247835
Event log details
Flags: None
Chunk count: 22
Stored/Calculated CRC: 19AE68FF/19AE68FF
Earliest timestamp: 2026-07-14 08:07:31.5278557
Latest timestamp: 2026-08-16 09:27:37.3411204
Total event log records found: 1,222
Records included: 1,222 Errors: 0 Events dropped: 0
Metrics (including dropped events)
Event ID      Count
-----
1              25
2              13
3               2
11             1
13             50
15             1
```

15008	10
16962	14
16977	15
16983	14
20003	5
50036	28
50037	12
50103	14
50104	12
50105	12
50106	12
51046	14
51047	12
51057	12

Processed 5 files in 9.2672 seconds

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1>

DF Analyst

▼ Scenario 1

| Parsing

- parsing prefetch with PECmd

```
& "D:\UOW\SEM3\Tools\ZimmermanTools\net9\PECmd.exe" `
    -d "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\prefetch" `
    --csv "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\prefetch" `
    --csvf "scenario_1_prefetch.csv"
```

```
Executable name: ZOOMINSTALLERFULL.EXE
Hash: 3C7F6855
File size (bytes): 258,884
Version: Windows 11

Run count: 1
Last run: 2026-08-16 09:17:46

Volume information:
# #: Name: \VOLUME{01dd13b23dcb8909-043dd6e4} Serial: 43DD6E4 Created: 2026-07-14 17:00:15 Directories: 6 File references: 30

Directories referenced: 6
00: \VOLUME{01dd13b23dcb8909-043dd6e4}\USERS
01: \VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST
02: \VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS
03: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS
04: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\APPPATCH
05: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32

Files referenced: 24
00: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\WTDLL.DLL
01: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\C_1252.NLS
02: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\C_437.NLS
03: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\INTL.NLS
04: \VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\ZOOMINSTALLERFULL.EXE (Executable: True)
05: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\KERNEL32.DLL
06: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\KERNELBASE.DLL
07: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\LOCALE.NLS
08: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\APPHelp.DLL
09: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\APPPATCH\01dd20589FDEDE4F.SYSMAIN.SDB
10: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\USER32.DLL
11: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\WIN32U.DLL
12: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\GDI32.DLL
13: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\GDI32FULL.DLL
14: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\MSVCP_WIN.DLL
15: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\UCRTBASE.DLL
16: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\SHELL32.DLL
17: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\OLEAUT32.DLL
18: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\COMBASE.DLL
19: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\RPCRT4.DLL
20: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\TIM32.DLL
21: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\OLE32.DLL
22: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\KERNEL_APPCORE.DLL
23: \VOLUME{01dd13b23dcb8909-043dd6e4}\WINDOWS\SYSTEM32\MSVCRT.DLL

----- Processed D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\prefetch\ZOOMINSTALLERFULL.EXE-3C7F6855.pf in 0.02468910 seconds -----
Processed 413 out of 413 files in 20.4131 seconds

CSV output will be saved to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\prefetch\scenario_1_prefetch.csv
CSV time line output will be saved to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\prefetch\scenario_1_prefetch_Timeline.csv
PS C:\WINDOWS\system32>
```

- sanity check

```
PS C:\WINDOWS\system32> $pf = Import-Csv "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\prefetch\scenario_1_prefetch.csv"
```

```
is\prefetch\scenario_1_prefetch_Timeline.csv"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> $pf |
>> Where-Object { $_.ExecutableName -match 'CHRO
MESETUP|WINRAR-X64|VLC-3|READER_EN|ZOOMINSTALLERFU
LL|NPP\.8\.9\.6' } |
>> Sort-Object RunTime |
>> Format-Table RunTime, ExecutableName -AutoSiz
e
```

RunTime	ExecutableName
-----	-----
2026-08-16 09:08:00	\VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\CHROMESETUP.EXE
2026-08-16 09:08:02	\VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\CHROMESETUP.EXE
2026-08-16 09:09:48	\VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\WINRAR-X64-723.EXE
2026-08-16 09:10:31	\VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\VLC-3.0.23-WIN32.EXE
2026-08-16 09:11:36	READER_EN_R9BVLF8K_INSTALL.EX
2026-08-16 09:11:38	READER_EN_R9BVLF8K_INSTALL.EX
2026-08-16 09:17:46	\VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\ZOOMINSTALLERFULL.EXE
2026-08-16 09:18:51	\VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\NPP.8.9.6.2.INSTALLER.X64.EXE

```
PS C:\WINDOWS\system32>
```

```

PS C:\WINDOWS\system32> $pf = Import-Csv "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\prefetch\scenario_1_prefetch_Timeline.csv"
PS C:\WINDOWS\system32> $pf |
PS C:\WINDOWS\system32> $pf |
>> Where-Object { $_.ExecutableName -match 'CHROMESETUP|WINRAR-X64|VLC-3|READER_EN|ZOOMINSTALLERFULL|NPP\.\9\6' } |
>> Sort-Object RunTime |
>> Format-Table RunTime, ExecutableName -AutoSize

RunTime          ExecutableName
-----
2026-08-16 09:08:00 VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\CHROMESETUP.EXE
2026-08-16 09:08:02 VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\CHROMESETUP.EXE
2026-08-16 09:09:48 VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\WINRAR-X64-723.EXE
2026-08-16 09:10:31 VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\VLC-3.0.23-WIN32.EXE
2026-08-16 09:11:36 READER_EN_R9BVLFBK_INSTALL.EX
2026-08-16 09:11:38 READER_EN_R9BVLFBK_INSTALL.EX
2026-08-16 09:17:46 VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\ZOOMINSTALLERFULL.EXE
2026-08-16 09:18:51 VOLUME{01dd13b23dcb8909-043dd6e4}\USERS\DFANALYST\DOWNLOADS\NPP.8.9.6.2.INSTALLER.X64.EXE

PS C:\WINDOWS\system32>

```

- parsing event logs with EvtxECmd

```

& "D:\UOW\SEM3\Tools\ZimmermanTools\net9\EvtxCmd\Evt
xECmd.exe" `
    -d "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scen
ario_1\artefacts\event_logs" `
    --csv "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\s
cenario_1\analysis\event_logs"

```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> & "D:\UOW\SEM3\Tools\ZimmermanTools\net9\EvtxCmd\EvtxECmd.exe" `
>> -d "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\event_logs" `
>> --csv "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\event_logs"
EvtxECmd version 2026.5.0

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

Command line: -d D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\event_logs --csv D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\event_logs

CSV output will be saved to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\event_logs\20260824210813_EvtxECmd_Output.csv

Maps loaded: 383
Looking for event log files in D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\event_logs

Processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\event_logs\Application.evt...
Chunk count: 23, Iterating records...
Record #: 13 (timestamp: 2026-07-14 08:07:31.5278557): Warning! Time just went backwards! Last seen time before change: 2026-07-14 16:07:30.0696560
Record #: 795 (timestamp: 2026-07-14 12:12:07.2253414): Warning! Time just went backwards! Last seen time before change: 2026-07-16 07:46:41.5247835

Event log details
Flags: None
Chunk count: 23
Stored/Calculated CRC: 19AE6BFF/19AE6BFF
Earliest timestamp: 2026-07-14 08:07:31.5278557
Latest timestamp: 2026-08-16 09:27:37.3411204
Total event log records found: 1,222

Records included: 1,222 Errors: 0 Events dropped: 0

```

```
Processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\event_logs\System.evtx...
Chunk count: 19, Iterating records...
Record # 4 (timestamp: 2026-07-14 16:04:38.5863295): Warning! Time just went backwards! Last seen time before change: 2026-07-14 16:05:12.3882416
Record # 192 (timestamp: 2026-07-14 16:07:04.4124068): Warning! Time just went backwards! Last seen time before change: 2026-07-14 16:07:29.4185786
Record # 194 (Event Record Id: 194): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 267 (timestamp: 2026-07-14 08:07:31.1709170): Warning! Time just went backwards! Last seen time before change: 2026-07-14 16:07:30.5841731
Record # 322 (timestamp: 2026-07-14 08:10:10.0061905): Warning! Time just went backwards! Last seen time before change: 2026-07-14 08:10:26.5382742
Record # 324 (Event Record Id: 324): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 430 (timestamp: 2026-07-14 08:11:33.0877610): Warning! Time just went backwards! Last seen time before change: 2026-07-14 08:11:54.2303032
Record # 438 (Event Record Id: 438): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 551 (timestamp: 2026-07-14 08:25:14.9687924): Warning! Time just went backwards! Last seen time before change: 2026-07-14 08:25:32.9596247
Record # 553 (Event Record Id: 553): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 637 (timestamp: 2026-07-14 09:49:55.6788044): Warning! Time just went backwards! Last seen time before change: 2026-07-14 09:50:05.4442185
Record # 833 (timestamp: 2026-07-14 09:58:08.5401211): Warning! Time just went backwards! Last seen time before change: 2026-07-14 09:58:16.4450483
Record # 945 (timestamp: 2026-07-14 10:01:23.8054506): Warning! Time just went backwards! Last seen time before change: 2026-07-14 10:01:38.2514389
Record # 947 (Event Record Id: 947): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 1337 (timestamp: 2026-07-14 11:28:28.9341302): Warning! Time just went backwards! Last seen time before change: 2026-07-14 11:28:45.3445739
Record # 1339 (Event Record Id: 1339): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 1482 (timestamp: 2026-07-14 11:30:12.3994888): Warning! Time just went backwards! Last seen time before change: 2026-07-14 11:30:27.6771167
Record # 1484 (Event Record Id: 1484): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 1587 (timestamp: 2026-07-14 11:37:41.3354294): Warning! Time just went backwards! Last seen time before change: 2026-07-14 11:38:00.8339177
Record # 1589 (Event Record Id: 1589): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 1682 (timestamp: 2026-07-14 12:11:53.2845826): Warning! Time just went backwards! Last seen time before change: 2026-07-16 07:46:33.9507927
Record # 1688 (timestamp: 2026-07-14 12:12:06.6562667): Warning! Time just went backwards! Last seen time before change: 2026-07-16 07:46:37.1268039
Record # 1716 (timestamp: 2026-07-14 12:36:05.1669129): Warning! Time just went backwards! Last seen time before change: 2026-07-16 08:10:49.5399141
Record # 1745 (timestamp: 2026-07-16 10:48:16.8272573): Warning! Time just went backwards! Last seen time before change: 2026-07-17 13:26:32.8502364
Record # 1780 (timestamp: 2026-07-17 13:41:19.1300010): Warning! Time just went backwards! Last seen time before change: 2026-07-17 13:46:06.3332977
Record # 1782 (Event Record Id: 1782): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 1890 (timestamp: 2026-07-17 19:30:23.9469510): Warning! Time just went backwards! Last seen time before change: 2026-08-06 09:55:57.3289877
Record # 1892 (Event Record Id: 1892): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string
Record # 2037 (timestamp: 2026-08-06 10:18:52.0495184): Warning! Time just went backwards! Last seen time before change: 2026-08-12 09:15:49.6456902
Record # 2058 (timestamp: 2026-08-12 09:16:50.3415917): Warning! Time just went backwards! Last seen time before change: 2026-08-16 07:24:08.6393717
Record # 2060 (Event Record Id: 2060): In map for event 13, Property /Event/EventData/Data[@Name="BootMode"] not found! Replacing with empty string

Event log details
Flags: None
Chunk count: 19
Stored/Calculated CRC: 9C8D9DE0/9C8D9DE0
Earliest timestamp: 2026-07-14 08:07:31.1709170
Latest timestamp: 2026-08-16 09:27:37.3741844
Total event log records found: 2,358

Records included: 2,358 Errors: 0 Events dropped: 0

Metrics (including dropped events)
Event ID      Count
1             31
3             15
```

- sanity check

```
Get-ChildItem "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\event_logs"
```

```
PS C:\WINDOWS\system32> Get-ChildItem "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\event_logs"

Directory: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\event_logs

Mode                LastWriteTime         Length Name
----                -
-a----             8/24/2026  10:08 PM       34916513 20260824210813_EvtxECD_Output.csv

PS C:\WINDOWS\system32>
```

- parsing shellbags with SBECmd

```
$sb = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags"
```

```
# Clean the folder from the previous half-completed attempt
```

```
Remove-Item "$sb\*" -Force -ErrorAction SilentlyContinue
```

```
# Pre-create dummies (SBECmd lock-check workaround)
```

```
New-Item -ItemType File -Path "$sb\UsrClass.csv" -For
```

```

ce | Out-Null
New-Item -ItemType File -Path "$sb\NTUSER.csv" -For
ce | Out-Null

# Parse
& "D:\UOW\SEM3\Tools\ZimmermanTools\net9\SBECmd.exe"
`

    -d "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scen
ario_1\artefacts\shellbags" `
    --csv $sb `
    --nl

# Cleanup: delete dummies FIRST, then rename the real
0_-prefixed outputs
Remove-Item "$sb\NTUSER.csv", "$sb\UsrClass.csv" -Forc
e
Rename-Item "$sb\0_NTUSER.csv" "NTUSER.csv"
Rename-Item "$sb\0_UsrClass.csv" "UsrClass.csv"

# Verify
Get-ChildItem $sb

```

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Parse
PS C:\WINDOWS\system32> & "D:\UOW\SEM3\Tools\ZimmermanTools\net9\SBECmd.exe" `
>> -d "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags" `
>> --csv $sb
>> --nl
SBECmd version 2026.5.0

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

Command line: -d D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags --csv D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags --nl

Directory to process: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags
Deduplication: False
All messages will be saved to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\SBECmd_Messages.txt
Processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags\NTUSER.DAT
Setting output path to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\0_NTUSER.csv due to existing file D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scen
ario_1\analysis\shellbags\NTUSER.csv
Parse time: 0.11 seconds

Total ShellBags found: 0

Totals by bag type

Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags\NTUSER.DAT
Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\0_NTUSER.csv

-----
Processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags\UsrClass.dat
Setting output path to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\0_UsrClass.csv due to existing file D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scen
ario_1\analysis\shellbags\UsrClass.csv
Parse time: 0.13 seconds

Total ShellBags found: 12

Totals by bag type

Root folder: GUID: 4
Directory: 7
Drive letter: 1

Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags\UsrClass.dat
Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\0_UsrClass.csv

```

```

-----
Processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags\UsrClass.dat
Setting output path to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\0_UsrClass.csv due to existing file D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\UsrClass.csv
Parse time: 0.13 seconds

Total ShellBags found: 12

Totals by bag type
Root folder: GUID: 4
Directory: 7
Drive letter: 1

Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\artefacts\shellbags\UsrClass.dat
Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\0_UsrClass.csv
-----

Processing complete!
Processed 2 files in 0.24 seconds!
Total ShellBags found: 12

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Cleanup: delete dummies FIRST, then rename the real 0_-prefixed outputs
PS C:\WINDOWS\system32> Remove-Item "$sb\NTUSER.csv", "$sb\UsrClass.csv" -Force
PS C:\WINDOWS\system32> Rename-Item "$sb\0_NTUSER.csv" "NTUSER.csv"
PS C:\WINDOWS\system32> Rename-Item "$sb\0_UsrClass.csv" "UsrClass.csv"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Verify
PS C:\WINDOWS\system32> Get-ChildItem $sb

Directory: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags

Mode                LastWriteTime         Length Name
----                -
-a----           8/24/2026 10:15 PM         2493 !SBECmd_Messages.txt
-a----           8/24/2026 10:15 PM          227 NTUSER.csv
-a----           8/24/2026 10:15 PM         2288 UsrClass.csv

PS C:\WINDOWS\system32>

```

- sanity check

```

PS C:\WINDOWS\system32> Import-Csv "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\UsrClass.csv" |
>> Sort-Object LastInteracted |
>> Format-Table AbsolutePath, ShellType, FirstInteracted, LastInteracted, LastWriteTime -AutoSize -Wrap

```

AbsolutePath

ShellType	FirstInteracted	LastInteracted
-----------	-----------------	----------------

ed	LastWriteTime
----	---------------

Desktop\This PC\C:\Users
Directory

2026-08-16 09:22:56

Desktop\This PC\C:\Temp

Directory 2026-07-14 09:58:45

2026-08-16 09:22:56

Desktop\This PC\C:\DISS_Config

Directory 2026-07-14 10:11:28

```

2026-08-16 09:22:56
Desktop\Downloads
Root folder: GUID 2026-07-14 10:39:56
2026-08-16 09:26:38
Desktop\Desktop
Root folder: GUID 2026-07-14 10:39:54
2026-08-16 09:26:38
Desktop\Win11 21H2
Root folder: GUID 2026-07-14 09:52:42
2026-08-16 09:26:38
Desktop\This PC\C:
Drive letter                                2026-07-14 0
9:53:05 2026-07-14 09:53:05
Desktop\This PC\C:\Users\dfanalyst
Directory                                2026-07-14 09:53:09 2026-07-14 0
9:53:09 2026-07-14 09:53:09
Desktop\This PC\C:\DISS_TESTDATA\PILOT
Directory                                2026-07-17 1
9:29:12 2026-07-17 19:29:12
Desktop\This PC\C:\DISS_TESTDATA
Directory                                2026-08-16 0
9:22:56 2026-08-16 09:22:56
Desktop\This PC\C:\DISS_TESTDATA\PILOT\P00R01_BROW
SED_A7K9 Directory                        2026-08-16 09:23:06 202
6-08-16 09:23:06 2026-08-16 09:23:06
Desktop\This PC
Root folder: GUID                        2026-08-16 0
9:26:38 2026-08-16 09:26:38

```

```

PS C:\WINDOWS\system32>

```

```
PS C:\WINDOWS\system32> Import-Csv "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_1\analysis\shellbags\UsrClass.csv" |
>> Sort-Object LastInteracted |
>> Format-Table AbsolutePath, ShellType, FirstInteracted, LastInteracted, LastWriteTime -AutoSize -Wrap

AbsolutePath                               ShellType      FirstInteracted   LastInteracted    LastWriteTime
-----
Desktop\This PC\C:\Users                  Directory      2026-07-14 09:58:45 2026-08-16 09:22:56
Desktop\This PC\C:\Temp                  Directory      2026-07-14 10:11:28 2026-08-16 09:22:56
Desktop\This PC\C:\DISS_Config            Directory      2026-07-14 10:39:56 2026-08-16 09:22:56
Desktop\Downloads                        Root folder: GUID 2026-07-14 10:39:54 2026-08-16 09:26:38
Desktop\Desktop                          Root folder: GUID 2026-07-14 10:39:54 2026-08-16 09:26:38
Desktop\Win11 21H2                       Root folder: GUID 2026-07-14 09:52:42 2026-08-16 09:26:38
Desktop\This PC\C:                        Drive letter   2026-07-14 09:53:05 2026-07-14 09:53:05
Desktop\This PC\C:\Users\dfanalyst        Directory      2026-07-14 09:53:09 2026-07-14 09:53:09
Desktop\This PC\C:\DISS_TESTDATA\PILOT    Directory      2026-07-17 19:29:12 2026-07-17 19:29:12
Desktop\This PC\C:\DISS_TESTDATA          Directory      2026-08-16 09:22:56 2026-08-16 09:22:56
Desktop\This PC\C:\DISS_TESTDATA\PILOT\P00R01_BROWSED_A7K9 Directory      2026-08-16 09:23:06 2026-08-16 09:23:06
Desktop\This PC                           Root folder: GUID 2026-08-16 09:26:38 2026-08-16 09:26:38

PS C:\WINDOWS\system32>
```

▼ Scenario 4

▼ Run 1

| Parsing All 3 artifacts

```
$run = 1 # change to 2 then 3 for the next runs

$src = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\artefacts"
$dst = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis"
$tool = "D:\UOW\SEM3\Tools\ZimmermanTools\net9"

# Fresh analysis folder
Remove-Item -Path $dst -Recurse -Force -ErrorAction SilentlyContinue
New-Item -ItemType Directory -Path "$dst\prefetch" -Force | Out-Null
New-Item -ItemType Directory -Path "$dst\event_logs" -Force | Out-Null
New-Item -ItemType Directory -Path "$dst\shellbags" -Force | Out-Null

# 1. Prefetch
& "$tool\PECmd.exe" `
    -d "$src\prefetch" `
    --csv "$dst\prefetch" `
    --csvf "scenario_4_run$($run)_prefetch.csv"
```

```
# 2. Event logs (no --csvf, EvtxECmd quirk)
& "$tool\EvtxCmd\EvtxECmd.exe" `
    -d "$src\event_logs" `
    --csv "$dst\event_logs"

# 3. ShellBags (SBECmd dummy-file workaround)
New-Item -ItemType File -Path "$dst\shellbags\UsrClass.csv" -Force | Out-Null
New-Item -ItemType File -Path "$dst\shellbags\NTUSER.csv" -Force | Out-Null

& "$tool\SBECmd.exe" `
    -d "$src\shellbags" `
    --csv "$dst\shellbags" `
    --nl

Remove-Item "$dst\shellbags\NTUSER.csv", "$dst\shellbags\UsrClass.csv" -Force
Rename-Item "$dst\shellbags\0_NTUSER.csv" "NTUSER.csv"
Rename-Item "$dst\shellbags\0_UsrClass.csv" "UsrClass.csv"

# Verify
Write-Host "`n=== Run $run analysis folder ==="
Get-ChildItem $dst -Recurse -File | Select-Object FullName, Length | Format-Table -AutoSize
```

```
total ShellBags found: 15

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Remove-Item "$dst\shellbags\NTUSER.csv", "$dst\shellbags\UsrClass.csv" -Force
PS C:\WINDOWS\system32> Rename-Item "$dst\shellbags\0_NTUSER.csv" "NTUSER.csv"
PS C:\WINDOWS\system32> Rename-Item "$dst\shellbags\0_UsrClass.csv" "UsrClass.csv"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Verify
PS C:\WINDOWS\system32> Write-Host "`n=== Run $run analysis folder ==="
=== Run 1 analysis folder ===
PS C:\WINDOWS\system32> Get-ChildItem $dst -Recurse -File | Select-Object FullName, Length | Format-Table -AutoSize

FullName                                                                 Length
-----
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\analysis\event_logs\20260824214719_EvtxECmd_Output.csv 33163069
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\analysis\prefetch\scenario_4_run1_prefetch.csv      3314742
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\analysis\prefetch\scenario_4_run1_prefetch_Timeline.csv 124550
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\analysis\shellbags\SBECmd_Messages.txt           2634
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\analysis\shellbags\NTUSER.csv                  227
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\analysis\shellbags\UsrClass.csv                 2618

PS C:\WINDOWS\system32>
```

▼ Run 2

| Parsing All 3 artifacts

```
$run = 2

$src = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\artefacts"
$dst = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis"
$tool = "D:\UOW\SEM3\Tools\ZimmermanTools\net9"

# Fresh analysis folder
Remove-Item -Path $dst -Recurse -Force -ErrorAction SilentlyContinue
New-Item -ItemType Directory -Path "$dst\prefetch" -Force | Out-Null
New-Item -ItemType Directory -Path "$dst\event_logs" -Force | Out-Null
New-Item -ItemType Directory -Path "$dst\shellbags" -Force | Out-Null

# 1. Prefetch
& "$tool\PECmd.exe" `
    -d "$src\prefetch" `
    --csv "$dst\prefetch" `
    --csvf "scenario_4_run$($run)_prefetch.csv"

# 2. Event logs (no --csvf)
& "$tool\EvtxCmd\EvtxECmd.exe" `
    -d "$src\event_logs" `
    --csv "$dst\event_logs"

# 3. ShellBags (dummy-file workaround)
New-Item -ItemType File -Path "$dst\shellbags\UsrClass.csv" -Force | Out-Null
New-Item -ItemType File -Path "$dst\shellbags\NTUSER.csv" -Force | Out-Null
```

```
& "$tool\SBECmd.exe" `
    -d "$src\shellbags" `
    --csv "$dst\shellbags" `
    --nl

Remove-Item "$dst\shellbags\NTUSER.csv", "$dst\shellbags\
UsrClass.csv" -Force
Rename-Item "$dst\shellbags\0_NTUSER.csv" "NTUSER.csv"
Rename-Item "$dst\shellbags\0_UsrClass.csv" "UsrClass.csv"

# Verify
Write-Host "`n=== Run $run analysis folder ==="
Get-ChildItem $dst -Recurse -File | Select-Object Full
Name, Length | Format-Table -AutoSize
```

```
Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\artefacts\shellbags\NTUSER.DAT
Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\analysis\shellbags\0_NTUSER.csv

-----

Processing complete!

Processed 2 files in 0.24 seconds!
Total ShellBags found: 13

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> Remove-Item "$dst\shellbags\NTUSER.csv", "$dst\shellbags\UsrClass.csv" -Force
PS C:\WINDOWS\system32> Rename-Item "$dst\shellbags\0_NTUSER.csv" "NTUSER.csv"
PS C:\WINDOWS\system32> Rename-Item "$dst\shellbags\0_UsrClass.csv" "UsrClass.csv"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Verify
PS C:\WINDOWS\system32> Write-Host "`n=== Run $run analysis folder ==="

=== Run 2 analysis folder ===
PS C:\WINDOWS\system32> Get-ChildItem $dst -Recurse -File | Select-Object FullName, Length | Format-Table -AutoSize

FullName                                                                 Length
-----
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\analysis\event_logs\20260824221204_EvtxECmd_Output.csv 32743484
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\analysis\prefetch\scenario_4_run2_prefetch.csv 3258565
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\analysis\prefetch\scenario_4_run2_prefetch_Timeline.csv 122599
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\analysis\shellbags\SBECmd_Messages.txt 2634
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\analysis\shellbags\NTUSER.csv 227
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\analysis\shellbags\UsrClass.csv 2351

PS C:\WINDOWS\system32>
```

▼ Run 3

| Parsing All 3 artifacts

```

$run = 3

$src = "D:\U0W\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\artefacts"
$dst = "D:\U0W\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis"
$tool = "D:\U0W\SEM3\Tools\ZimmermanTools\net9"

# Fresh analysis folder
Remove-Item -Path $dst -Recurse -Force -ErrorAction SilentlyContinue
New-Item -ItemType Directory -Path "$dst\prefetch" -Force | Out-Null
New-Item -ItemType Directory -Path "$dst\event_logs" -Force | Out-Null
New-Item -ItemType Directory -Path "$dst\shellbags" -Force | Out-Null

# 1. Prefetch
& "$tool\PECmd.exe" `
    -d "$src\prefetch" `
    --csv "$dst\prefetch" `
    --csvf "scenario_4_run$($run)_prefetch.csv"

# 2. Event logs (no --csvf)
& "$tool\EvtxCmd\EvtxECmd.exe" `
    -d "$src\event_logs" `
    --csv "$dst\event_logs"

# 3. ShellBags (dummy-file workaround)
New-Item -ItemType File -Path "$dst\shellbags\UsrClass.csv" -Force | Out-Null
New-Item -ItemType File -Path "$dst\shellbags\NTUSER.csv" -Force | Out-Null

& "$tool\SBECmd.exe" `
    -d "$src\shellbags" `
    --csv "$dst\shellbags" `

```

```
--nl
```

```
Remove-Item "$dst\shellbags\NTUSER.csv", "$dst\shellbags\UsrClass.csv" -Force
```

```
Rename-Item "$dst\shellbags\0_NTUSER.csv" "NTUSER.csv"
```

```
Rename-Item "$dst\shellbags\0_UsrClass.csv" "UsrClass.csv"
```

```
# Verify
```

```
Write-Host "`n=== Run $run analysis folder ==="
```

```
Get-ChildItem $dst -Recurse -File | Select-Object FullName, Length | Format-Table -AutoSize
```

```
Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\shellbags\NTUSER.DAT
Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\analysis\shellbags\0_NTUSER.csv
-----
Processing complete!
Processed 2 files in 0.44 seconds!
Total ShellBags found: 13

PS C:\WINDOWS\system32> Remove-Item "$dst\shellbags\NTUSER.csv", "$dst\shellbags\UsrClass.csv" -Force
PS C:\WINDOWS\system32> Rename-Item "$dst\shellbags\0_NTUSER.csv" "NTUSER.csv"
PS C:\WINDOWS\system32> Rename-Item "$dst\shellbags\0_UsrClass.csv" "UsrClass.csv"
PS C:\WINDOWS\system32> # Verify
PS C:\WINDOWS\system32> Write-Host "`n=== Run $run analysis folder ==="

=== Run 3 analysis folder ===
PS C:\WINDOWS\system32> Get-ChildItem $dst -Recurse -File | Select-Object FullName, Length | Format-Table -AutoSize

FullName                                                                                                     Length
-----
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\analysis\event_logs\20260824221421_EvtxECmd_Output.csv 32556025
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\analysis\prefetch\scenario_4_run3_prefetch.csv      3155288
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\analysis\prefetch\scenario_4_run3_prefetch_Timeline.csv 121004
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\analysis\shellbags\!SBECmd_Messages.txt           2634
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\analysis\shellbags\NTUSER.csv                    227
D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\analysis\shellbags\UsrClass.csv                  2351

PS C:\WINDOWS\system32>
```

- Prefetch Sanity Check

```
PS C:\WINDOWS\system32> 1..3 | ForEach-Object {
>>     $run = $_
>>     $csv = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis\prefetch\scenario_4_run$($run)_prefetch.csv"
>>     Write-Host "`n=== Run $run HELLOWORLD.EXE ==="
>>     Import-Csv $csv |
>>     Where-Object { $_.ExecutableName -match 'HEL
```

```

LOWORLD' } |
>>      Select-Object SourceFilename, ExecutableName,
RunCount, LastRun, Volume0Name, Volume0Serial |
>>      Format-List
>> }

```

```

PS C:\WINDOWS\system32> 1..3 | ForEach-Object {
>>     $run = $_
>>     $csv = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis\prefetch\scenario_4_run$(($run)_prefetch.csv"
>>     Write-Host "`n=== Run $run HELLOWORLD.EXE ==="
>>     Import-Csv $csv |
>>     Where-Object { $_.ExecutableName -match 'HELLOWORLD' } |
>>     Select-Object SourceFilename, ExecutableName, RunCount, LastRun, Volume0Name, Volume0Serial |
>>     Format-List
>> }

=== Run 1 HELLOWORLD.EXE ===

SourceFilename : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_1\artefacts\prefetch\HELLOWORLD.EXE-36846810.pf
ExecutableName : HELLOWORLD.EXE
RunCount       : 1
LastRun        : 2026-08-22 11:49:06
Volume0Name    : \VOLUME{01dd13b23dcb8909-043dd6e4}
Volume0Serial  : 43DD6E4

=== Run 2 HELLOWORLD.EXE ===

SourceFilename : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_2\artefacts\prefetch\HELLOWORLD.EXE-5EC49DAB.pf
ExecutableName : HELLOWORLD.EXE
RunCount       : 1
LastRun        : 2026-08-22 20:35:47
Volume0Name    : \VOLUME{01dd13b23dcb8909-043dd6e4}
Volume0Serial  : 43DD6E4

=== Run 3 HELLOWORLD.EXE ===

SourceFilename : D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_3\artefacts\prefetch\HELLOWORLD.EXE-5EC49DAB.pf
ExecutableName : HELLOWORLD.EXE
RunCount       : 1
LastRun        : 2026-08-22 21:02:44
Volume0Name    : \VOLUME{01dd13b23dcb8909-043dd6e4}
Volume0Serial  : 43DD6E4

```

- ShellBags Sanity Check

```

PS C:\WINDOWS\system32> 1..3 | ForEach-Object {
>>     $run = $_
>>     $csv = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis\shellbags\UsrClass.csv"
>>     Write-Host "`n=== Run $run ALL shellbags with any 2026-08 timestamp ==="
>>     Import-Csv $csv |
>>     Where-Object {
>>         $_.FirstInteracted -match '^2026-08' -or
>>         $_.LastInteracted  -match '^2026-08' -or
>>         $_.LastWriteTime    -match '^2026-08'
>>     } |

```

```
>> Format-Table AbsolutePath, ShellType, FirstI
nteracted, LastInteracted, LastWriteTime -AutoSize
>> }
```

```
PS C:\WINDOWS\system32> 1..3 | ForEach-Object {
>> $run = $_
>> $csv = "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis\shellbags\UsrClass.csv"
>> Write-Host "`n=== Run $run ALL shellbags with any 2026-08 timestamp ==="
>> Import-Csv $csv |
>> Where-Object {
>>     $_.FirstInteracted -match '^2026-08' -or
>>     $_.LastInteracted -match '^2026-08' -or
>>     $_.LastWriteTime -match '^2026-08'
>> } |
>> Format-Table AbsolutePath, ShellType, FirstInteracted, LastInteracted, LastWriteTime -AutoSize
>> }

=== Run 1 ALL shellbags with any 2026-08 timestamp ===

AbsolutePath          ShellType              FirstInteracted        LastInteracted         LastWriteTime
-----
Desktop\Win11 21H2    Root folder: GUID      2026-07-14 09:52:42    2026-08-22 11:50:14    2026-08-22 11:50:14
Desktop\This PC       Root folder: GUID      2026-07-14 10:39:54    2026-08-22 11:50:14    2026-08-22 11:50:14
Desktop\Desktop       Root folder: GUID      2026-07-14 10:39:56    2026-08-22 11:50:14    2026-08-22 11:50:14
Desktop\Downloads     Root folder: GUID      2026-07-14 10:39:56    2026-08-22 11:50:14    2026-08-22 11:50:14
Desktop\CLSID_ThisPCDocumentsRegFolder Root folder: GUID      2026-08-22 11:46:48    2026-08-22 11:50:14    2026-08-22 11:50:14
Desktop\E:\           Users property view: Drive letter
Desktop\This PC\C:    Drive letter           2026-08-22 11:46:35    2026-08-22 11:46:35    2026-08-22 11:46:35
Desktop\This PC\E:    Drive letter           2026-08-22 11:48:05    2026-08-22 11:48:05    2026-08-22 11:48:05
Desktop\E:\\PORTABLE Directory              2026-08-22 11:48:05    2026-08-22 11:48:05    2026-08-22 11:48:05

=== Run 2 ALL shellbags with any 2026-08 timestamp ===

AbsolutePath          ShellType              FirstInteracted        LastInteracted         LastWriteTime
-----
Desktop\Win11 21H2    Root folder: GUID      2026-07-14 09:52:42    2026-08-22 20:36:21    2026-08-22 20:36:21
Desktop\This PC       Root folder: GUID      2026-07-14 10:39:54    2026-08-22 20:36:21    2026-08-22 20:36:21
Desktop\Desktop       Root folder: GUID      2026-07-14 10:39:56    2026-08-22 20:36:21    2026-08-22 20:36:21
Desktop\Downloads     Root folder: GUID      2026-07-14 10:39:56    2026-08-22 20:36:21    2026-08-22 20:36:21
Desktop\E:\           Users property view: Drive letter
Desktop\E:\\PORTABLE Directory              2026-08-22 20:35:24    2026-08-22 20:35:24    2026-08-22 20:35:24

=== Run 3 ALL shellbags with any 2026-08 timestamp ===

AbsolutePath          ShellType              FirstInteracted        LastInteracted         LastWriteTime
-----
Desktop\Win11 21H2    Root folder: GUID      2026-07-14 09:52:42    2026-08-22 21:03:13    2026-08-22 21:03:13
Desktop\This PC       Root folder: GUID      2026-07-14 10:39:54    2026-08-22 21:03:13    2026-08-22 21:03:13
Desktop\Desktop       Root folder: GUID      2026-07-14 10:39:56    2026-08-22 21:03:13    2026-08-22 21:03:13
Desktop\Downloads     Root folder: GUID      2026-07-14 10:39:56    2026-08-22 21:03:13    2026-08-22 21:03:13
Desktop\E:\           Users property view: Drive letter
Desktop\E:\\PORTABLE Directory              2026-08-22 21:01:54    2026-08-22 21:01:54    2026-08-22 21:01:54

PS C:\WINDOWS\system32>
```

- Event Logs Sanity Check

```
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> 1..3 | ForEach-Object {
>> $run = $_
>> $csv = Get-ChildItem "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis\event_logs\*_EvtxECmd_Output.csv" |
>> Select-Object -First 1
>> Write-Host "`n=== Run $run Partition/Diagnostic event 1006 on 2026-08-22 ==="
>> Import-Csv $csv.FullName |
>> Where-Object { $_.Channel -match 'Partition' -and $_.EventId -eq '1006' -and $_.TimeCreated -match '^2026-08-22' } |
```

```
>>      Select-Object TimeCreated, EventId, MapDescription, PayloadData1, PayloadData2, PayloadData3, PayloadData4 |
>>      Format-List
>> }
```

=== Run 1 Partition/Diagnostic event 1006 on 2026-08-22 ===

```
TimeCreated      : 2026-08-22 11:31:57.1441402
EventId          : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: VMware Virtual NVMe Disk
PayloadData2     : Capacity: 85899345920
PayloadData3     : Manufacturer: NULL
PayloadData4     : SCSI SerialNumber: CE0B_26C0_97DC_756F_000C_296D_C3AD_654B.
```

```
TimeCreated      : 2026-08-22 11:44:32.8116085
EventId          : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: UDisk
PayloadData2     : Capacity: 4026531840
PayloadData3     : Manufacturer: General
PayloadData4     : SCSI SerialNumber:
```

```
TimeCreated      : 2026-08-22 11:44:45.8523249
EventId          : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: UDisk
PayloadData2     : Capacity: 0
PayloadData3     : Manufacturer: General
PayloadData4     : SCSI SerialNumber:
```

```
TimeCreated      : 2026-08-22 11:45:40.6515730
EventId          : 1006
MapDescription    : USB Insertion/Removal
```

PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 4026531840
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

TimeCreated : 2026-08-22 11:50:19.1059755
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 0
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

TimeCreated : 2026-08-22 11:51:07.8478373
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 0
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

=== Run 2 Partition/Diagnostic event 1006 on 2026-08-22 ===

TimeCreated : 2026-08-22 20:29:22.7392422
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: VMware Virtual NVMe Disk
PayloadData2 : Capacity: 85899345920
PayloadData3 : Manufacturer: NULL
PayloadData4 : SCSI SerialNumber: CE0B_26C0_97DC_756F_000C_296D_C3AD_654B.

TimeCreated : 2026-08-22 20:33:49.5505399

EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 4026531840
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

TimeCreated : 2026-08-22 20:36:25.9126024
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 0
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

TimeCreated : 2026-08-22 20:36:53.7013273
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 0
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

=== Run 3 Partition/Diagnostic event 1006 on 2026-08-22 ===

TimeCreated : 2026-08-22 20:57:00.6445254
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: VMware Virtual NVMe Disk
PayloadData2 : Capacity: 85899345920
PayloadData3 : Manufacturer: NULL
PayloadData4 : SCSI SerialNumber: CE0B_26C0_97DC_756F_000C_296D_C3AD_654B.

TimeCreated : 2026-08-22 21:00:28.2104334
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 4026531840
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

TimeCreated : 2026-08-22 21:03:17.7301332
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 0
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

TimeCreated : 2026-08-22 21:03:47.5917954
EventId : 1006
MapDescription : USB Insertion/Removal
PayloadData1 : Model: UDisk
PayloadData2 : Capacity: 0
PayloadData3 : Manufacturer: General
PayloadData4 : SCSI SerialNumber:

```

PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> 1..3 | ForEach-Object {
>>     $run = $_
>>     $csv = Get-ChildItem "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis\event_logs\*_EvtxECmd_Output.csv" |
>>     Select-Object -First 1
>>     Write-Host "`n=== Run $run Partition/Diagnostic event 1006 on 2026-08-22 ==="
>>     Import-Csv $csv.FullName |
>>     Where-Object { $_.Channel -match 'Partition' -and $_.EventId -eq '1006' -and $_.TimeCreated -match '^2026-08-22' } |
>>     Select-Object TimeCreated, EventId, MapDescription, PayloadData1, PayloadData2, PayloadData3, PayloadData4 |
>>     Format-List
>> }

=== Run 1 Partition/Diagnostic event 1006 on 2026-08-22 ===

TimeCreated      : 2026-08-22 11:31:57.1441402
EventId           : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: VMware Virtual NVMe Disk
PayloadData2     : Capacity: 85899345920
PayloadData3     : Manufacturer: NULL
PayloadData4     : SCSI SerialNumber: CE0B_26C0_97DC_756F_000C_296D_C3AD_654B.

TimeCreated      : 2026-08-22 11:44:32.8116085
EventId           : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: UDisk
PayloadData2     : Capacity: 4026531840
PayloadData3     : Manufacturer: General
PayloadData4     : SCSI SerialNumber:

TimeCreated      : 2026-08-22 11:44:45.8523249
EventId           : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: UDisk
PayloadData2     : Capacity: 0
PayloadData3     : Manufacturer: General
PayloadData4     : SCSI SerialNumber:

TimeCreated      : 2026-08-22 11:45:40.6515730
EventId           : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: UDisk
PayloadData2     : Capacity: 4026531840
PayloadData3     : Manufacturer: General
PayloadData4     : SCSI SerialNumber:

```

```

=== Run 3 Partition/Diagnostic event 1006 on 2026-08-22 ===

TimeCreated      : 2026-08-22 20:57:00.6445254
EventId           : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: VMware Virtual NVMe Disk
PayloadData2     : Capacity: 85899345920
PayloadData3     : Manufacturer: NULL
PayloadData4     : SCSI SerialNumber: CE0B_26C0_97DC_756F_000C_296D_C3AD_654B.

TimeCreated      : 2026-08-22 21:00:28.2104334
EventId           : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: UDisk
PayloadData2     : Capacity: 4026531840
PayloadData3     : Manufacturer: General
PayloadData4     : SCSI SerialNumber:

TimeCreated      : 2026-08-22 21:03:17.7301332
EventId           : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: UDisk
PayloadData2     : Capacity: 0
PayloadData3     : Manufacturer: General
PayloadData4     : SCSI SerialNumber:

TimeCreated      : 2026-08-22 21:03:47.5917954
EventId           : 1006
MapDescription    : USB Insertion/Removal
PayloadData1     : Model: UDisk
PayloadData2     : Capacity: 0
PayloadData3     : Manufacturer: General
PayloadData4     : SCSI SerialNumber:

```

```

PS C:\WINDOWS\system32> 1..3 | ForEach-Object {
>>     $run = $_
>>     $csv = Get-ChildItem "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis\event_logs\*_EvtxECmd_Output.csv" |
>>     Select-Object -First 1

```

```
>> Write-Host "`n=== Run $run Security 4688 HELLO
WORLD ==="
>> $hits = Import-Csv $csv.FullName |
>> Where-Object { $_.EventId -eq '4688' -and
($_.PayloadData1 -match 'HELLOWORLD' -or $_.PayloadDa
ta2 -match 'HELLOWORLD' -or $_.PayloadData3 -match 'H
ELLOWORLD' -or $_.PayloadData4 -match 'HELLOWORLD')}
>> if ($hits) {
>>     $hits | Select-Object TimeCreated, EventI
d, PayloadData1, PayloadData2, PayloadData3, PayloadD
ata4 | Format-List
>> } else {
>>     Write-Host "No 4688 rows for HELLOWORLD –
process auditing likely disabled or event pruned."
>> }
>> }
```

=== Run 1 Security 4688 HELLOWORLD ===

```
TimeCreated : 2026-08-22 11:49:06.9627639
EventId      : 4688
PayloadData1 : Parent process: \Device\HarddiskVolume
6\PORTABLE\HelloWorld.exe
PayloadData2 : PID: 0x1840
PayloadData3 : Parent PID: 0x2174
PayloadData4 : Mandatory label: SECURITY_MANDATORY_ME
DIUM_RID
```

=== Run 2 Security 4688 HELLOWORLD ===

```
TimeCreated : 2026-08-22 20:35:47.2472828
EventId      : 4688
PayloadData1 : Parent process: \Device\HarddiskVolume
```

```
5\PORTABLE\HelloWorld.exe
PayloadData2 : PID: 0x1554
PayloadData3 : Parent PID: 0x2034
PayloadData4 : Mandatory label: SECURITY_MANDATORY_ME
DIUM_RID
```

```
=== Run 3 Security 4688 HELLOWORLD ===
```

```
TimeCreated   : 2026-08-22 21:02:44.3060453
EventId       : 4688
PayloadData1  : Parent process: \Device\HarddiskVolume
5\PORTABLE\HelloWorld.exe
PayloadData2  : PID: 0x2D14
PayloadData3  : Parent PID: 0x2C8C
PayloadData4  : Mandatory label: SECURITY_MANDATORY_ME
DIUM_RID
```

```
PS C:\WINDOWS\system32>
```

```

PS C:\WINDOWS\system32> 1..3 | ForEach-Object {
>> $run = $_
>> $csv = Get-Childitem "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_4\run_$run\analysis\event_logs\EvtxCmd_Output.csv" |
>> Select-Object -First 1
>> Write-Host "=== Run $run Security 4688 HELLOWORLD ==="
>> $hits = Import-csv $csv.FullName |
>> Where-Object { $_.EventId -eq 4688 } -and ($_.PayloadData1 -match 'HELLOWORLD' -or $_.PayloadData2 -match 'HELLOWORLD' -or $_.PayloadData3 -match 'HELLOWORLD' -or $_.PayloadData4 -match
'HELLOWORLD')
>> if ($hits) {
>> $hits | Select-Object TimeCreated, EventId, PayloadData1, PayloadData2, PayloadData3, PayloadData4 | Format-List
>> } else {
>> Write-Host "No 4688 rows for HELLOWORLD - process auditing likely disabled or event pruned."
>> }
>> }

=== Run 1 Security 4688 HELLOWORLD ===

TimeCreated : 2026-08-22 11:49:06.9627639
EventId      : 4688
PayloadData1 : Parent process: \Device\HarddiskVolume6\PORTABLE\Helloworld.exe
PayloadData2 : PID: 0x1840
PayloadData3 : Parent PID: 0x2174
PayloadData4 : Mandatory label: SECURITY_MANDATORY_MEDIUM_RID

=== Run 2 Security 4688 HELLOWORLD ===

TimeCreated : 2026-08-22 20:35:47.2472828
EventId      : 4688
PayloadData1 : Parent process: \Device\HarddiskVolume5\PORTABLE\Helloworld.exe
PayloadData2 : PID: 0x1554
PayloadData3 : Parent PID: 0x2034
PayloadData4 : Mandatory label: SECURITY_MANDATORY_MEDIUM_RID

=== Run 3 Security 4688 HELLOWORLD ===

TimeCreated : 2026-08-22 21:02:44.3060453
EventId      : 4688
PayloadData1 : Parent process: \Device\HarddiskVolume5\PORTABLE\Helloworld.exe
PayloadData2 : PID: 0x2014
PayloadData3 : Parent PID: 0x2C9C
PayloadData4 : Mandatory label: SECURITY_MANDATORY_MEDIUM_RID

PS C:\WINDOWS\system32>

```

▼ Scenario 7

▼ Run 1

| Parsing all artefacts

Scenario 7 - Run 1

\$T = "D:\UOW\SEM3\Tools\ZimmermanTools\net9"

Set-Location "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2"

New-Item -ItemType Directory -Path .\analysis\prefetch, .\analysis\event_logs, .\analysis\shellbags -Force | Out-Null

& "\$T\PECmd.exe" -d .\artefacts\prefetch --csv .\analysis\prefetch --csvf scenario_7_run1_prefetch.csv -q

& "\$T\EvtxCmd\EvtxECmd.exe" -d .\artefacts\event_logs --csv .\analysis\event_logs

New-Item -ItemType File -Path .\analysis\shellbags\UsrClass.csv, .\analysis\shellbags\NTUSER.csv -Force | Out-Null

& "\$T\SBECmd.exe" -d .\artefacts\shellbags --csv .\analysis\shellbags --nl

```

Remove-Item .\analysis\shellbags\UsrClass.csv, .\analysis\shellbags\NTUSER.csv
Rename-Item .\analysis\shellbags\0_UsrClass.csv UsrClass.csv
Rename-Item .\analysis\shellbags\0_NTUSER.csv NTUSER.csv

```

```

Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\artefacts\shellbags\NTUSER.DAT
Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\analysis\shellbags\0_NTUSER.csv
-----
Processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\artefacts\shellbags\UsrClass.dat
Setting output path to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\analysis\shellbags\0_UsrClass.csv due to existing file D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\analysis\shellbags\UsrClass.csv
Parse time: 0.17 seconds
Total ShellBags found: 15
Totals by bag type
Root folder: GUID: 5
Directory: 9
Drive letter: 1
Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\artefacts\shellbags\UsrClass.dat
Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1\analysis\shellbags\0_UsrClass.csv
-----
Processing complete!
Processed 2 files in 0.49 seconds!
Total ShellBags found: 15

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1> Remove-Item .\analysis\shellbags\UsrClass.csv, .\analysis\shellbags\NTUSER.csv
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1> Rename-Item .\analysis\shellbags\0_UsrClass.csv UsrClass.csv
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1> Rename-Item .\analysis\shellbags\0_NTUSER.csv NTUSER.csv
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1>
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_1>

```

▼ Run 2

| Parsing all artifacts

```

# Scenario 7 - Run 2
$T = "D:\UOW\SEM3\Tools\ZimmermanTools\net9"
Set-Location "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2"
New-Item -ItemType Directory -Path .\analysis\prefetch, .\analysis\event_logs, .\analysis\shellbags -Force | Out-Null
& "$T\PECmd.exe" -d .\artefacts\prefetch --csv .\analysis\prefetch --csvf scenario_7_run2_prefetch.csv -q
& "$T\EvtxCmd\EvtxECmd.exe" -d .\artefacts\event_logs --csv .\analysis\event_logs
New-Item -ItemType File -Path .\analysis\shellbags\Usr

```

```

Class.csv, .\analysis\shellbags\NTUSER.csv -Force | Out-Null
& "$T\SBECmd.exe" -d .\artefacts\shellbags --csv .\analysis\shellbags --nl
Remove-Item .\analysis\shellbags\UsrClass.csv, .\analysis\shellbags\NTUSER.csv
Rename-Item .\analysis\shellbags\0_UsrClass.csv UsrClass.csv
Rename-Item .\analysis\shellbags\0_NTUSER.csv NTUSER.csv

```

```

-----
Processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\shellbags\UsrClass.dat
Setting output path to D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\analysis\shellbags\0_UsrClass.csv due to existing file D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\analysis\shellbags\UsrClass.csv
Parse time: 0.14 seconds

Total ShellBags found: 15

Totals by bag type
Root folder: GUID: 5
Directory: 9
Drive letter: 1

Finished processing D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\artefacts\shellbags\UsrClass.dat
Exported to: D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2\analysis\shellbags\0_UsrClass.csv
-----

Processing complete!
Processed 2 files in 0.39 seconds!
Total ShellBags found: 15

PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2> Remove-Item .\analysis\shellbags\UsrClass.csv, .\analysis\shellbags\NTUSER.csv
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2> Rename-Item .\analysis\shellbags\0_UsrClass.csv UsrClass.csv
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2> Rename-Item .\analysis\shellbags\0_NTUSER.csv NTUSER.csv
PS D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_2> ..

```

▼ Run 3

| parsing all artifacts

```

# Scenario 7 - Run 3
$T = "D:\UOW\SEM3\Tools\ZimmermanTools\net9"
Set-Location "D:\UOW\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3"
New-Item -ItemType Directory -Path .\analysis\prefetch, .\analysis\event_logs, .\analysis\shellbags -Force | Out-Null
& "$T\PECmd.exe" -d .\artefacts\prefetch --csv .\analysis\prefetch --csvf scenario_7_run3_prefetch.csv -q
& "$T\EvtxCmd\EvtxECmd.exe" -d .\artefacts\event_logs --csv .\analysis\event_logs

```

```

New-Item -ItemType File -Path .\analysis\shellbags\Usr
Class.csv, .\analysis\shellbags\NTUSER.csv -Force | Ou
t-Null
& "$T\SBECmd.exe" -d .\artefacts\shellbags --c
sv .\analysis\shellbags --nl
Remove-Item .\analysis\shellbags\UsrClass.csv, .\analy
sis\shellbags\NTUSER.csv
Rename-Item .\analysis\shellbags\0_UsrClass.csv UsrCla
ss.csv
Rename-Item .\analysis\shellbags\0_NTUSER.csv NTUSER.c
sv

```

```

Totals by bag type

Finished processing D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\artefacts\shellbags\NTUSER.DAT
Exported to: D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\analysis\shellbags\0_NTUSER.csv
-----
Processing D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\artefacts\shellbags\UsrClass.dat
Setting output path to D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\analysis\shellbags\0_UsrClass.csv due to existing file D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenari
o_7\run_3\analysis\shellbags\UsrClass.csv
Parse time: 0.20 seconds
Total ShellBags found: 15

Totals by bag type
Root folder: GUID: 5
Directory: 9
Drive letter: 1

Finished processing D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\artefacts\shellbags\UsrClass.dat
Exported to: D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3\analysis\shellbags\0_UsrClass.csv
-----
Processing complete!
Processed 2 files in 0.39 seconds!
Total ShellBags found: 15

PS D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3> Remove-Item .\analysis\shellbags\UsrClass.csv, .\analysis\shellbags\NTUSER.csv
PS D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3> Rename-Item .\analysis\shellbags\0_UsrClass.csv UsrClass.csv
PS D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3> Rename-Item .\analysis\shellbags\0_NTUSER.csv NTUSER.csv
PS D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3>
PS D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3>
PS D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3>
PS D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3>
PS D:\UQM\SEM3\msc-diss-7csef001w\scenarios\scenario_7\run_3>

```

- sanity check