STUDENT WORKSHEET

Digital Forensics Laboratory Exercise

Insider Data Theft via USB

Document	STUDENT WORKSHEET
Case ID	RH-2026-7430-001
Scenario	Insider Data Theft via USB (difficulty: medium)
Student	Student 1 [student-001]
Host	Windows 10 Pro
Total points	197
Prepared	2026-11-12

For authorized training use only.

Scenario briefing

An engineer who has resigned is suspected of walking out with confidential files on a USB stick. Prove what was connected, what was copied, and when.

Oakmont Energy has referred this one to you. A Senior Design Engineer handed in notice on a Friday afternoon. Over the weekend a manager noticed confidential documents had been opened outside normal hours. Security thinks the engineer copied company files to a personal USB stick on the way out.

You have a forensic image and the extracted Windows artifacts from the engineer's workstation, OAKMON-WS32. Was a USB device connected? What was copied, and when? Build a timeline you could defend.

Evidence inventory

Eventlog

File path	Description	Size	MD5 / SHA-256
`C/Windows/System32/winevt/Logs/Security.evtx`	Security event log (EVTX)	132.0 KB	`MD5: ece343342b7afde4a1bc708282f1395d` `SHA-256: e75be8e312705284181bc7b5240c6e096feb255fae2a118bdeeb639ecc1db9a6`
`C/Windows/System32/winevt/Logs/System.evtx`	System event log (EVTX)	68.0 KB	`MD5: 526a9f846c4f6c90b1bfe0c5c52fe8e9` `SHA-256: d777e2653fde74fb273b53eecb188f16895eb50f049e350ecbd6844473eb9b93`

Windows

File path	Description	Size	MD5 / SHA-256
C/Windows/System32/config/SYSTEM	SYSTEM registry hive	24.0 KB	MD5: bd970d7fee76ee75a8b5ca9bb4ac0521 SHA-256: a0cba8684ef88f0b89c2fc654ef0b80acee4ca0e73b7df950298ca489efd7585
C/Windows/System32/config/SOFTWARE	SOFTWARE registry hive	12.0 KB	MD5: 767a5e836136b37287c3436c561282f1 SHA-256: fb66091f56e3ff98794f95a330eb47801f2a330ff5737e2aec7cf25a4a012cbd
C/Users/caguilar/NTUSER.DAT	NTUSER.DAT registry hive	24.0 KB	MD5: 8fa65ac35311c33ff5520ce89c396aee SHA-256: ab342fbb4b1cbdc7a6eb361356e97cbc3aef2f331107c10efd3398c83dd09dfe
C/Windows/Prefetch/7ZFM.EXE-56DE4F9A.pf	Prefetch file	4.3 KB	MD5: d7e819935e8e756c48035557d201232f SHA-256: c06105aed93d1bae1447d8b9520de0e72a78f0cd2a2af17f7f293ee9016099d1
C/Windows/Prefetch/SVCHOST.EXE-D02762BF.pf	Prefetch file	4.4 KB	MD5: 5238ba737e2237ccc58f90000f425e07 SHA-256: 21e02c0f49282afa63e9cda15e558b898119a9b45ab62e3884d19c79badf51e0
C/Windows/Prefetch/EXPLORER.EXE-D5E97654.pf	Prefetch file	4.1 KB	MD5: 7e063e3a5ae311479b37e69f3f1215c6 SHA-256: 76e750c8b2538eb3ac9d390f5703f7af3fa70e98576b2080fe039a28f38d3ab8
C/Windows/Prefetch/CHROME.EXE-AED7BA3C.pf	Prefetch file	4.7 KB	MD5: 8b1648f188eef0d59f3f12b936fcfa50 SHA-256: 123a071871286e13b6bdb578b92fda2d1643114970a9cec967a089e8fc3007cc
C/Windows/Prefetch/NOTEPAD.EXE-C5670914.pf	Prefetch file	4.6 KB	MD5: 563568a04c220594a23120ac408706e7 SHA-256: b5a69bfab9860bd3bf157898eb1793b9ef09ee9ce9c97e97067db46728522562
C/Windows/Prefetch/SEARCHPROTOCOLHOST.EXE-69C456C3.pf	Prefetch file	4.7 KB	MD5: 6efd5cae63e4957cdb8382c2c8747713 SHA-256: bccc69edd414f96169e9501436632e07c7f166c255ae90089de069f3b2b0fe9f
C/Windows/Prefetch/CONHOST.EXE-0C6456FB.pf	Prefetch file	4.6 KB	MD5: 131d5e9cc98ec545e4b8d58f61448801 SHA-256: f24a2f838f1eb75dc0e9b7362365d7624f4a3d4f812c299c866d402b850d726d
C/Windows/Prefetch/RUNDLL32.EXE-B0CF1E13.pf	Prefetch file	4.1 KB	MD5: 80a74486176e9b5c3a963eead4f08a12 SHA-256: 655ab5dcf5cf723777a509dbff044fa79fbb48fe917ca5f2229371fb0a17bbaa
C/Windows/Prefetch/TASKHOSTW.EXE-2E5D4B75.pf	Prefetch file	4.3 KB	MD5: 200dc71b19cf70b140d14a14b4774bcd SHA-256: e29ef13c7268481d807e336ec5c45084df2d2f77c5e9e06e65dccbd120c71f33
C/Users/caguilar/AppData/Roaming/Microsoft/Windows/Recent/project_files.7z.lnk	LNK shortcut (Recent Items)	415 B	MD5: 62558c571ecc35d869d380b59979b300 SHA-256: 1decdba9ecef46bf9045ccf8a969b73a201a6d3bdc2a976b5f23f494a9867bd0
C/Users/caguilar/AppData/Roaming/Microsoft/Windows/Recent/Rotor Assembly Spec.docx.lnk	LNK shortcut (Recent Items)	770 B	MD5: e4c2781e7c941fcac2be46970204fe93 SHA-256: 0d8873e14977356503a41048feff902c539163d721bb700578e1c371f789f74b
C/Users/caguilar/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/f01b4d95cf55d32a.automaticDestinations-ms	Jump list (AutomaticDestinations)	3.0 KB	MD5: 0168fadafb299f7b2ee72b2a28c01c9c SHA-256: 8850ac69757c48a44185a276e1a0a227772bd2a2883fe66789bc5762db4402b1
C/$MFT_timeline.csv	MFTECmd CSV of the file table (selected files)	38.7 KB	MD5: 7e5e66d121191a33e6a5e7e94fc01080 SHA-256: cb8d61d45866fab5d93b4900ddd25d2ab3a5b36ae75428535fd87000cbeb4da6

Disk

File path	Description	Size	MD5 / SHA-256
`disk/evidence.dd`	Raw disk image	64.0 MB	`MD5: fc60d17a006c57efd9fbd9e71e4bb9a0` `SHA-256: 715ccf6a8970d6c08d4d43dfd7f867edbbde515757fbea5b5f64da177646d2c3`

Suggested tools

- Autopsy
- Registry Explorer
- FTK Imager
- PECmd
- JLECmd
- LECmd
- EvtxECmd

Questions

Q1. What time zone is the workstation set to? Give the TimeZoneKeyName from the registry. **5 pts | easy**

Q2. What is the make and model (FriendlyName) of the USB device that was connected? **8 pts | easy**

Q3. When did the logon session during which the USB device was connected begin (UTC)? **5 pts | easy**

Q4. What is the serial number of the USB device? 10 pts | medium

Q5. When was the USB device first connected (UTC)? 10 pts | medium

Q6. When was the USB device last connected (UTC)? 10 pts | medium

Q7. What is the full path of the archive that was written to the removable drive (as recorded in the shortcut)? 10 pts | medium

Q8. How many times was the archiving tool executed according to Prefetch? 8 pts | medium

Q9. What is the true file type of the file with a .jpg extension that isn't an image? 8 pts | medium

Q10. What network share did the user type into Explorer's address bar? 10 pts | medium

Q11. When did the logon session during which the USB device was connected end (UTC)? 10 pts | medium

Q12. What spreadsheet appears in the user's RecentDocs? 10 pts | medium

Q13. What VID and PID does the registry record for the USB device? Answer as VID_xxxx&PID_xxxx. 8 pts | medium

Q14. What file size (bytes) does the shortcut record for the archive on the USB device? 12 pts | medium

Q15. What last-access time does the shortcut to the document in the user's Documents folder record for its target (UTC)? 12 pts | medium

Q16. When does UserAssist record the archiving program last being run (UTC)? 12 pts | hard

Q17. When was the USB device last removed (UTC)? 10 pts | hard

Q18. What is the SHA-256 of the staged archive found on the disk image? 15 pts | hard

Q19. What is the SHA-256 of the deleted document recoverable from the user's Temp folder? 12 pts | hard

Q20. What is the SHA-256 of the document carved from unallocated space? 12 pts | hard

Submission checklist

- ☐ Verify the MD5 / SHA-256 hash of every evidence file before analysis.
- ☐ Answer every question. Don't leave any blank.
- ☐ Cite the exact evidence location (file and record) for each answer.
- ☐ Export your findings and attach any supporting screenshots.