



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	OAKMON-WS32 / Windows 10 Pro
Total points	115
Prepared	2026-09-28

For authorized training use only.

Scenario briefing

An engineer is suspected of copying proprietary designs to a personal USB drive before resigning.

Oakmont Energy has referred a matter to you for examination. Connor Aguilar, a Senior Design Engineer, gave notice on a Friday afternoon. Over the weekend, a manager noticed that several confidential design documents had been opened from the shared drive outside normal hours. Security believes Connor may have copied company property to a personal USB device before leaving.

You have received a forensic image and the extracted Windows artifacts from Connor's workstation, OAKMON-WS32. Determine whether a USB device was connected, what was copied, and when. Establish a defensible timeline.

Evidence inventory

Windows

File path	Description	Size	MD5 / SHA-256
C/Windows/System32/config/SYSTEM	SYSTEM registry hive	12.0 KB	MD5: 61f468ea48ed0dbae30aa1c7b504ede5 SHA-256: 33cc9a1d6bb69847d0e0ce5a4ab2353883f5dfc219e4879b7931571fc18038f2
C/Windows/System32/config/SOFTWARE	SOFTWARE registry hive	8.0 KB	MD5: 95f294af29f334b7861ec7380c3ed3c8 SHA-256: 842ef3406a675ee3e48febff91f283b1aa967327e012f445fd9cf428d8433dda
C/Users/caguilar/NTUSER.DAT	NTUSER.DAT for caguilar	8.0 KB	MD5: df6f0cb021453a21e0f8f464a1a4db19 SHA-256: f937db4c94095a6c318d4e15529e37b177e047f67154cb4171dc990467805fca
C/Windows/Prefetch/7ZFM.EXE-56DE4F9A.pf	Prefetch for 7ZFM.EXE	1.2 KB	MD5: 1adcf87b581f83c21875a1ab6e453be9 SHA-256: c1e1ba68a77b407c841d679c2fbc4d41e2a53553e92e0af17fb86cac86f796cb
C/Windows/Prefetch/SVCHOST.EXE-D02762BF.pf	Prefetch for SVCHOST.EXE	1.3 KB	MD5: 235801ef7807b561b3d86a722edad276 SHA-256: c64fd4db4e5bfd2cfa94bf8b110fd7d02711fa062a178bda2d089c463404adf
C/Windows/Prefetch/EXPLORER.EXE-D5E97654.pf	Prefetch for EXPLORER.EXE	1.3 KB	MD5: af3e292d0db4c17d97dd0cef39ed97cc SHA-256: ec14697015d9eae435af2f4e35c8636ae7d40be3e2e66d5242f528623835474f
C/Windows/Prefetch/CHROME.EXE-AED7BA3C.pf	Prefetch for CHROME.EXE	1.4 KB	MD5: 6bfff4a06e9fa956e021b5b24c0cd0940 SHA-256: 0f994b017a591f4ed14e7dd29e6327b220d7a58e3c24000195306f5e2b0819c7
C/Windows/Prefetch/NOTEPAD.EXE-C5670914.pf	Prefetch for NOTEPAD.EXE	1.3 KB	MD5: 0315853c9fab30bbc2da9c418b581c3b SHA-256: c306ac8b7e77d8c44836da74e5724064f76f4ca5823c95c85b4002ea7c394cc9
C/Windows/Prefetch/SEARCHPROTOCOLHOST.EXE-69C456C3.pf	Prefetch for SEARCHPROTOCOLHOST.EXE	1.3 KB	MD5: 48560278ee153ac980190895fe135fb4 SHA-256: 49a1a3e1d86de4c574b4eda6f10eddc7341dba89301abfbefad9db9465c6e2c
C/Windows/Prefetch/CONHOST.EXE-0C6456FB.pf	Prefetch for CONHOST.EXE	1.3 KB	MD5: d0eb1588842702ae8e5500e87a1a5926 SHA-256: e6d90c6e27d8ba45537957b9c655082537e0d31fd7941fd44d3352b2458f9a55
C/Windows/Prefetch/RUNDLL32.EXE-B0CF1E13.pf	Prefetch for RUNDLL32.EXE	1.3 KB	MD5: 4a455b3d7fb1e77c54fd57cd6defa0f9 SHA-256: 17ee9937c81154881e25f9acbad2e2fdc0216bcc464fdfea8ab786b81e3c9156
C/Windows/Prefetch/TASKHOSTW.EXE-2E5D4B75.pf	Prefetch for TASKHOSTW.EXE	1.3 KB	MD5: 78fe5462ab0847d1db386ddfa2a199c2 SHA-256: bf6a7bf9540fd68dbb47b31aca9a9e0ab887f4036f3b2360cf2cf23e6df986bb

File path	Description	Size	MD5 / SHA-256
C:/Users/caguilar/AppData/Roaming/Microsoft/Windows/Recent/project_files.7z.lnk	LNK shortcut to E:\project_files.7z	415 B	MD5: ed10185bf449c50747f7a6284fdd6cfb SHA-256: d0cedbf7acb3298f331564d3438ce75be3ad36c8b6f40c323dc4e682d6cbb784
C:/Users/caguilar/AppData/Roaming/Microsoft/Windows/Recent/Rotor Assembly Spec.docx.lnk	LNK shortcut to C:\Users\caguilar\Documents\Rotor Assembly Spec.docx	770 B	MD5: e09257f4f757dc1b76fa8938e3d41a1f SHA-256: aa189acda33c437b57ac441b06dd7ba76e00128c58298e2178174e10d3d25ca6
C:/Users/caguilar/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/f01b4d95cf55d32a.automaticDestinations-ms	Jump list (explorer)	3.0 KB	MD5: 2d047ab02ec99c8c059964150ed9d0c3 SHA-256: 2291cef97523ed329229a8a8e8e8d06bcb16105c78d8fca312606d21b10a7d8d
C:\\$MFT_timeline.csv	MFT-style filesystem timeline (CSV, MFTECmd layout)	3.1 KB	MD5: b088c651ccc518a219f901ec130dd70e SHA-256: b276f67c7b82167c3ea614951a72050f20eaa5245d07c992bc8d9d668858cad1

Eventlog

File path	Description	Size	MD5 / SHA-256
C:/Windows/System32/winevt/Logs/Security.evtx	Security event log (69 records)	68.0 KB	MD5: a579b609e40d76f95f0a720ec3e16936 SHA-256: 60c3e2e97fff52b0a37db8d360512b1d52fa36420f82a432f9a070823b84ba2c
C:/Windows/System32/winevt/Logs/System.evtx	System event log (13 records)	68.0 KB	MD5: 2edf5d5415c5377437c335a61feff4a4 SHA-256: 80239c4e6cfa5ad1ab842cad3de252bcc2f4028ab3bfc0b66d425ff5a0ecbf85

Disk

File path	Description	Size	MD5 / SHA-256
disk/evidence.dd	Raw FAT32 disk image (21 files, 64 MB)	64.0 MB	MD5: 8debcce6509ef69cc7fb53de59374cb5 SHA-256: 098627be77d1c6eba0492c06737177400f749892f8dbf9e81a3355b8790d73f3

Suggested tools

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

Questions

Q1. What is the username of the account under investigation?

5 pts | easy

Q2. What is the make and model (FriendlyName) of the USB device that was connected?

8 pts | easy

Q3. What is the serial number of the USB device?

10 pts | medium

Q4. When was the USB device first connected (UTC)?

10 pts | medium

Q5. When was the USB device last connected (UTC)?

10 pts | medium

Q6. What is the full path of the archive that was written to the removable drive (as recorded in the shortcut)?

10 pts | medium

Q7. Which archiving program was run according to UserAssist? Give the executable name.

12 pts | hard

Q8. How many times was the archiving tool executed according to Prefetch?

8 pts | medium

Q9. When was the archive created on the USB device (shortcut target creation, UTC)?

12 pts | hard

Q10. What is the SHA-256 of the staged archive found on the disk image?

15 pts | hard

Q11. At what time did the interactive logon occur (UTC)?

5 pts | easy

Q12. What is the SHA-256 of the confidential BOM spreadsheet on disk?

10 pts | hard

Submission checklist

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