



Five Windows Forensic Artifacts for Every Incident Response

Jake Williams (@MalwareJake)

\$whoami

- Currently an independent security researcher
- IANS Faculty, former SANS Instructor
- Former NSA Hacker, endorsed by Shadow Brokers – aka Russian Intelligence
- “Digital terrorist,” breaker of software, responder of incidents, reverser of malware, injector of code, spaces > tabs
- **Dislikes:** those who call themselves “thought leaders,” “crypto bros,” and anyone who **needlessly adds blockchain** to a software solution

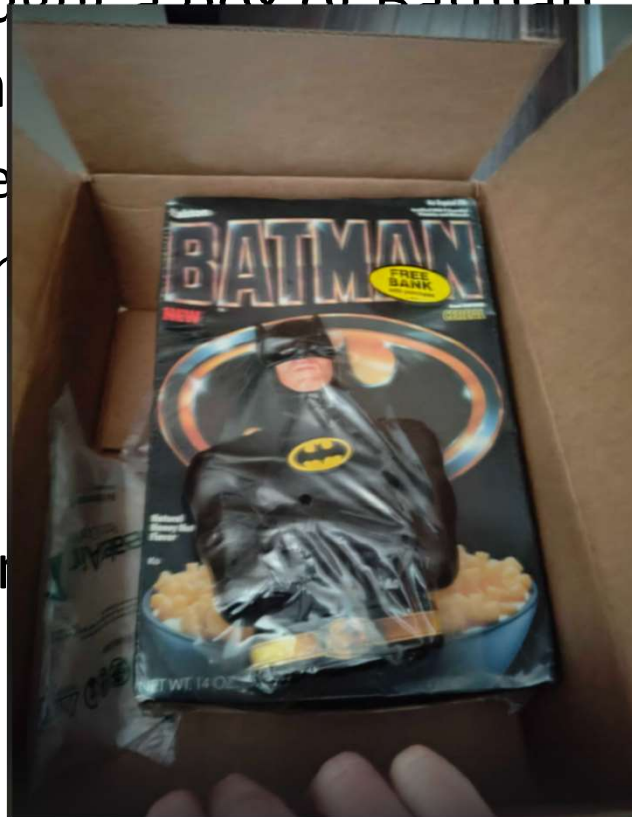
A Word On Scope

- We've got an hour to cover a few artifacts
 - I might not cover your favorite
 - In fact, it's statistically likely that I won't
- Even then, the depth we can cover is low in this format
- To learn more about artifacts generally, come take the class!
 - <https://www.antisiphontraining.com/advanced-endpoint-investigations/>
- If you want to debate artifact selection or coverage in this webcast, let's do it in Deadwood

Speaking of Deadwood...

- Grifter brought a box of Batman cereal from 1989
– It was awesome
– JK, it was horrible

- Mr. Strand



Agenda

- Why Five?
- Incident Responder Artifacts
 1. Filesystem Analysis
 2. USN Journal Analysis
 3. Prefetch Analysis
 4. Event Log Analysis
 5. Registry Analysis
- Closing Thoughts



Why Five Artifacts?

- It seems like every month, someone in forensics makes a discovery about a new artifact they've discovered
- Yay! We have more data points to analyze and contextualize a given investigation



Why Five Artifacts? (Cont.)

- As artifact density increases, forensic analysts are forced to triage and prioritize the data that will provide the best outcomes for their investigation
 - To the extent that digital forensics was ever about “answering everything” or “analyzing all artifacts” it isn’t anymore
- We must consider the purpose of performing forensics as providing decision support to stakeholders
 - As such, the types of decisions they need to make should inform the selection of artifacts analyzed

Artifact #1: Filesystem Analysis

- Filesystem analysis allows analysts to understand timestamps and reconstruct patterns of activity
- Each filesystem has its own nuance for how it handles timestamps and updates to those timestamps
- On Windows, the primary filesystem is NTFS and has additional files for analysis of timestamps, including:
 - \$LogFile
 - USN Journal
 - \$I30 (directory) files

MACB Timestamps

- The standard for filesystem timeline analysis is to create MACB timestamp output files
- For NTFS, the following rules apply
 - M. Content Modification
 - A. File Access Time
 - C. Metadata Change Time (e.g. file rename, permissions, etc.)
 - B. Birth Time (file creation time)
- Many filesystems lack the B time to show when a file was created (born)

NTFS \$STANDARD_INFORMATION and \$FILE_NAME

- Each file record on an NTFS volume has multiple copies of the MACB timestamps
 - \$STANDARD_INFORMATION timestamps are the ones you see in Explorer (aka “the normal timestamps”)
 - \$FILE_NAME timestamps are populated when the file is created and almost never modified
 - **Bonus:** most files have two \$FILE_NAME records, one for the regular file name and one for the 8.3 representation
- Because Windows APIs don't touch \$FILE_NAME timestamps, they can be useful in detecting timestamp manipulation

Filesystem Analysis: MFTECmd

- The tool MFTECmd (by Eric Zimmerman) parses the NTFS central database, the \$MFT
 - MFT is the Master File Table
- The MFT is typically parsed into a CSV that is then loaded into another tool, such as Excel or Timeline Explorer

```
C:\_tools>MFTECmd.exe -f C:\evidence\%MFT --csv=C:\evidence --csvf=mft.csv
MFTECmd version 1.2.1.0

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

Command line: -f C:\evidence\%MFT --csv=C:\evidence --csvf=mft.csv

Warning: Administrator privileges not found!

File type: Mft

Processed C:\evidence\%MFT in 4.6090 seconds

C:\evidence\%MFT: FILE records found: 143,670 (Free records: 13,099) File size: 153.2MB
CSV output will be saved to C:\evidence\mft.csv
```

Filesystem Analysis: Timeline Explorer

- The Timeline Explorer tool (by Eric Zimmerman) displays timeline CSV files in a more convenient format than Excel (and many other tools)

Timeline Explorer v1.3.0.0							
File Tools Tabs View Help							
mft.csv							
Drag a column header here to group by that column							
	Line	Tag	In Use	Parent Path	File Name	Created0x10	Created0x30
Y	=	<input type="checkbox"/>	<input checked="" type="checkbox"/>	#c 7-zip	#c	=	=
	102874	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\ProgramData\Microsoft\Windows\Start Menu\Progr...	7-Zip Help.lnk	2023-02-15 14:08:07	
	102865	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\ProgramData\Microsoft\Windows\Start Menu\Progr...	7-Zip File Manager.lnk	2023-02-15 14:08:07	
	102184	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\Program Files\7-Zip	Lang	2023-02-15 14:08:06	
	102182	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\Program Files\7-Zip	7-zip.chm	2022-07-16 02:00:00	2023-02-15 14:08:06
	102171	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\Program Files\7-Zip	readme.txt	2022-07-16 01:59:22	2023-02-15 14:08:06
	102162	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\Program Files\7-Zip	History.txt	2022-07-16 01:59:18	2023-02-15 14:08:06
	102154	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\Program Files\7-Zip	7zCon.sfx	2022-07-16 00:00:00	2023-02-15 14:08:06
	102151	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\Program Files\7-Zip	7z.sfx	2022-07-16 00:00:00	2023-02-15 14:08:06
	102148	<input type="checkbox"/>	<input checked="" type="checkbox"/>	.\Program Files\7-Zip	7z.exe	2022-07-16 00:00:00	2023-02-15 14:08:06

Artifact #2: USN Journal Analysis

- While the MFT does track last access timestamps, as we noted, these are disabled by many operating systems
 - The USN (Update Sequence Number) Journal provides data showing the operations performed on files
- This provides more than a simple timestamp when the last operation of a given type (create, access, modify, change metadata) was performed
 - The USN Journal also captures significantly more operation types than just MACB
 - USN journal data may include references to operations on deleted files

Why Process USN Journal?

- Some use cases for USN Journal analysis:
 - Knowledge that a file existed on the system
 - Knowledge of file deletion (and when)
 - Identifying that Prefetch files have been deleted (and which ones)
 - Seeing when a user has overwritten a file prior to deletion (often used in secure delete and anti-forensics)
 - Locating a staging directory where files were collected prior to being archived, exfiltrated, and deleted
 - Identifying when malware has marked files with the hidden or system attribute to limit visibility in Explorer (and unfortunately, other tools)

Processing the USN Journal

- The MFTECmd application from Eric Zimmerman used for MFT processing also processes data from the USN journal
 - The file name you need to acquire is \$Extend\\$\\$UsnJrnl
 - The data is in a special stream named \$J
- Point to the \$J file with the -f parameter, just like when using the tool to parse an MFT

```
Command line: -f C:\evidence\$$J -m C:\evidence\$$MFT --csv=C:\evidence --csvf=usn.csv
Warning: Administrator privileges not found!
File type: UsnJournal
Processed C:\evidence\$$MFT in 3.4267 seconds
C:\evidence\$$MFT: FILE records found: 143,670 (Free records: 13,099) File size: 153.2MB
      CSV output will be saved to C:\evidence\usn.csv

Processed C:\evidence\$$J in 1.0312 seconds
Usn entries found in C:\evidence\$$J: 267,085
      CSV output will be saved to C:\evidence\usn.csv
```

USN Journal Shows Interesting Deleted Files

- The USN Journal shows the existence of a now deleted file name exfil.7z (and a directory of the same name)

Line	Tag	Update Timestamp	Parent Path	Name	Update Reasons	Extension
=	<input checked="" type="checkbox"/>	=	Ⓜc	Ⓜc exfil	Ⓜc	Ⓜc
266459	<input type="checkbox"/>	2023-02-15 14:26:27	.\Users\booper\Desktop	exfil	RenameNewName	
266460	<input type="checkbox"/>	2023-02-15 14:26:27	.\Users\booper\Desktop	exfil	RenameNewName Close	
266461	<input type="checkbox"/>	2023-02-15 14:26:27	.\Users\booper\Desktop	exfil	ObjectIdChange	
266462	<input type="checkbox"/>	2023-02-15 14:26:27	.\Users\booper\Desktop	exfil	ObjectIdChange Close	
266466	<input type="checkbox"/>	2023-02-15 14:26:27	.\Users\booper\AppData\Roamin...	exfil.lnk	FileCreate	.lnk
266467	<input type="checkbox"/>	2023-02-15 14:26:27	.\Users\booper\AppData\Roamin...	exfil.lnk	DataExtend FileCreate	.lnk
266468	<input type="checkbox"/>	2023-02-15 14:26:27	.\Users\booper\AppData\Roamin...	exfil.lnk	DataExtend FileCreate Close	.lnk
266690	<input type="checkbox"/>	2023-02-15 14:28:13	.\Users\booper\Desktop	exfil.7z	FileCreate	.7z
266691	<input type="checkbox"/>	2023-02-15 14:28:13	.\Users\booper\Desktop	exfil.7z	DataExtend FileCreate	.7z
266692	<input type="checkbox"/>	2023-02-15 14:28:14	.\Users\booper\Desktop	exfil.7z	DataOverwrite DataExtend FileCreate	.7z
266693	<input type="checkbox"/>	2023-02-15 14:28:14	.\Users\booper\Desktop	exfil.7z	DataOverwrite DataExtend FileCreate Close	.7z
266703	<input type="checkbox"/>	2023-02-15 14:28:21	.\Users\booper\Desktop	exfil	RenameOldName	
266771	<input type="checkbox"/>	2023-02-15 14:28:53	.\Users\booper\Desktop	exfil.7z	RenameOldName	.7z

Artifact #3: Prefetch Analysis

- Some Windows systems log prefetch files, intended to aid in optimally moving drive heads to read files
 - The principle is that files needed early in execution by an application won't change substantially in future executions
- Prefetch files are not enabled on Windows servers and often are not enabled on workstations when Windows detects an SSD during installation
 - Subsequent change to an SSD doesn't disable Prefetch
- Prefetch files are located in C:\windows\Prefetch and have a .PF extension
 - One file is created per {appName, path, command line} tuple

Analyzing Prefetch Files

- The peCmd tool from Eric Zimmerman is a tool that can parse all known versions of prefetch files
 - Many prefetch parsers cannot handle compressed prefetch files (Win8+)
- Unlike many other prefetch parsers, peCmd can process an entire directory of prefetch files simultaneously
 - Most standalone parsers operate on a single file at a time
- The peCmd tool can also generate a timeline of Prefetch activity
 - This is useful in understanding the larger context of an investigation, especially when combined with filesystem timeline data


peCmd Output - Multiple Executions


Executable name: WINWORD.EXE


Hash: AB6EC2FA

File size (bytes): 324,782

Version: Windows 10

Run count: 3 

Last run: 2022-01-28 01:10:51 

Other run times: 2022-01-28 01:10:42, 2022-01-28 00:55:10 

Volume information:

#0: Name: Serial: 0 Created: 1601-01-01 00:00:00 Directories: 0 File references: 0

peCmd Output – File and Directory Hints

```
222: \VOLUME{01d80daa30bcd941-3830dc48}\WINDOWS\SYSTEM32\NORMNFKC.NLS
223: \VOLUME{01d80daa30bcd941-3830dc48}\WINDOWS\SYSTEM32\VRTDISK.DLL
224: \VOLUME{01d80daa30bcd941-3830dc48}\WINDOWS\SYSTEM32\FLTLib.DLL
225: \VOLUME{0000000000000000-e9be9148}\PRODUCT - OVERVIEW.DOCX
226: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\6A91873C.PNG
227: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\9A21C60D.PNG
228: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\9FE53CAA.PNG
229: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\6169D0A3.PNG
230: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\7B6B8A48.PNG
231: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\9E96B5A9.PNG
232: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\D7898F96.PNG
233: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\C6D80E9F.PNG
234: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\9C531814.PNG
235: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\65C43105.PNG
236: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\1FFB7B42.PNG
237: \VOLUME{01d80daa30bcd941-3830dc48}\USERS\LADYJESSICA\APPDATA\LOCAL\MICROSOFT\WINDOWS\INETCACHE\CONTENT.MSO\DC538E5B.PNG
```

Artifact #4: Event Log Analysis

- Entire presentations have been done on event log analysis
 - Due to the laws of space and time, we can't repeat all that content now
- I gave that presentation at Wild West Hackin' Fest Reno and looked for the recording but can't seem to find it
 - Maybe that will be a future webcast?
 - Or perhaps I'll update the presentation for Deadwood this year?

Event Logs Analysis

- There are no shortage of tools to process .evtx logs
 - Including the native Windows Event Viewer
- The data you see in the Event Viewer is a combination of the data stored in the event logs and maps to label the data
- When analyzing event logs on different systems from where they were generated, you may need to build your own maps to translate data elements appropriately

Event Logs Analysis: EvtxECmd

- The EvtxECmd (by Eric Zimmerman) can extract Event Logs to be analyzed in a CSV
- EvtxECmd features:
 - Include or exclude specific event IDs
 - Provide custom mappings for event logs
 - Only extract data from specific date and time ranges
 - Deduplicate entries from Volume Shadow Copies
 - Build a histogram of event IDs (EvtxECmd calls this “metrics”)

Event Logs Analysis: EvtxECmd (Cont.)

- EvtxECmd parsing the security event log

```
C:\_tools\EvtxECmd>EvtxECmd.exe -f C:\evidence\Security.evtx --csv=c:\evidence --csvf=security.csv
EvtxECmd version 1.0.0.0

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

Command line: -f C:\evidence\Security.evtx --csv=c:\evidence --csvf=security.csv

Warning: Administrator privileges not found!

CSV output will be saved to c:\evidence\security.csv

Maps loaded: 383

Processing C:\evidence\Security.evtx...
Chunk count: 218, Iterating records...
Record #: 3 (timestamp: 2023-02-14 02:09:22.5265005): Warning! Time just went backwards! Last seen time before change: 2023-02-14 02:09:36.66
15658
Record #: 27 (timestamp: 2023-02-14 02:09:25.8941493): Warning! Time just went backwards! Last seen time before change: 2023-02-14 02:09:36.6
615658
Record # 80 (Event Record Id: 80): In map for event 4718, Property /Event/EventData/Data[@Name="ProcessName"] not found! Replacing with empty
string
```

Artifact #5: Registry Analysis

- Registry analysis can provide multiple types of useful evidence for investigations, including:
 - Malware persistence
 - Evidence of file knowledge
 - Mounted drives
 - Services created
 - Software installed (and often uninstalled)
 - Files viewed in Explorer (USRCLASS.DAT)
 - Evidence of execution
 - SO... MUCH... MOAR!

Registry Analysis – Where to Start?

- The registry is an amazing (and often confusing) place to perform analysis
 - The vast majority of registry entries are uninteresting in any forensics investigation (many aren't even documented)
- The challenge is knowing where to apply your limited time
 - The plugins list from Zimmerman's RECcmd is a good place to start if you don't have any other leads
 - <https://github.com/EricZimmerman/RegistryPlugins>
 - Alternatively, consider the RegRipper Plugin list
 - <https://github.com/keydet89/RegRipper3.0/tree/master/plugins>

Registry Tools: RECcmd

- The RECcmd tool (from Eric Zimmerman) can be used to process registry files from the command line

```
C:\_tools\RECcmd>RECcmd.exe -f C:\evidence\config\SOFTWARE --nl --bn=BatchExamples\SoftwareASEPs.reb --csv=C:\evidence --csvf=software-asep.csv
RECcmd version 2.0.0.0

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

Note: Enclose all strings containing spaces (and all RegEx) with double quotes

Command line: -f C:\evidence\config\SOFTWARE --nl --bn=BatchExamples\SoftwareASEPs.reb --csv=C:\evidence --csvf=software-asep.csv

Processing hive C:\evidence\config\SOFTWARE
Registry hive is dirty and transaction logs were found in the same directory, but --nl was provided. Data may be missing! Continuing anyways.
..
Sequence numbers do not match! Hive is dirty and the transaction logs should be reviewed for relevant data!

Found key Clients\StartMenuInternet\IEXPLORE.EXE\shell\open\command and value (default)!
Found key Clients\StartMenuInternet\Microsoft Edge\shell\open\command and value (default)!
Found key Clients\StartMenuInternet\VMWAREHOSTOPEN.EXE\shell\open\command and value (default)!
```


Registry Tools: RECcmd

- Parsed SOFTWARE ASEP data in Timeline Explorer

Last Write Timestamp	Key Path	Value Name	Value Data
=	HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{00000000-0000-0000-0000-000000000000}		
2023-02-14 02:08:35	ROOT\Clients\StartMenuInternet\IEXPLORE.EXE\shell\op...	(default)	C:\Program Files\Internet Explorer\iexplore.exe
2023-02-14 02:10:00	ROOT\Clients\StartMenuInternet\Microsoft Edge\shell\...	(default)	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"
2023-02-14 14:28:09	ROOT\Clients\StartMenuInternet\VMWAREHOSTOPEN.EXE\sh...	(default)	"C:\Program Files\VMware\VMware Tools\VMwareHostOpen.exe" --default http
2022-05-07 07:39:22	ROOT\Microsoft\Active Setup\Installed Components\>{2...	(default)	Microsoft Windows Media Player
2022-05-07 07:39:22	ROOT\Microsoft\Active Setup\Installed Components\{22...	(default)	Microsoft Windows Media Player 12.0
2022-05-07 05:25:25	ROOT\Microsoft\Active Setup\Installed Components\{2C...	(default)	Themes Setup
2023-02-14 14:53:56	ROOT\Microsoft\Active Setup\Installed Components\{3a...	(default)	Offline Browsing Pack
2022-05-07 05:25:25	ROOT\Microsoft\Active Setup\Installed Components\{44...	(default)	DirectDrawEx
2023-02-14 14:53:56	ROOT\Microsoft\Active Setup\Installed Components\{45...	(default)	Internet Explorer Help
2022-05-07 05:25:25	ROOT\Microsoft\Active Setup\Installed Components\{4f...	(default)	Microsoft Windows Script 5.6
2023-02-14 14:53:56	ROOT\Microsoft\Active Setup\Installed Components\{5f...	(default)	Internet Explorer Setup Tools
2023-02-14 14:53:56	ROOT\Microsoft\Active Setup\Installed Components\{63...	(default)	Browsing Enhancements
2022-05-07 07:39:22	ROOT\Microsoft\Active Setup\Installed Components\{6B...	(default)	Microsoft Windows Media Player
2022-05-07 05:25:25	ROOT\Microsoft\Active Setup\Installed Components\{6f...	(default)	MSN Site Access
2022-05-07 05:25:25	ROOT\Microsoft\Active Setup\Installed Components\{77...	(default)	Address Book 7
2022-05-07 05:25:25	ROOT\Microsoft\Active Setup\Installed Components\{89...	(default)	Windows Desktop Update
2023-02-14 14:53:56	ROOT\Microsoft\Active Setup\Installed Components\{89...	(default)	Web Platform Customizations

Closing Thoughts

- Forensics is about analysis, **not** tools
 - Tools process the data
 - Analysts make sense of the output
- We've been pretty tool heavy today, but have also shown some types of questions you can answer with analysis
- We cover significantly more analysis considerations in the course
 - <https://www.antispyphontraining.com/advanced-endpoint-investigations/>