

The Art of Network File Sharing Forensics and Data Recovery

Author: Hussain Altayeb

Advisor: *Michael Long*

Accepted: *February 13th, 2024*

Abstract

Network file-sharing forensics is one of the challenging topics in Windows forensics as the user interacts with the file not located inside the Windows machine or server.

Network file sharing is utilized heavily in enterprise environments to read, write, save, and interact with other files. While logging the file activities for files inside the network share is possible, doing so is not practical and difficult to achieve because of the cost.

Most organizations cannot do so because of the number of transactions or logs per second. On the other hand, network forensics aid in resolving many cases and is widely used by most organizations nowadays for investigating a variety of cases. However, it requires saving a significant amount of data for a long time to analyze the files when needed, and most organizations need the luxury to do it. Additionally, most of the network traffic nowadays is encrypted. This research describes multiple practical methods to do network file sharing and data carving across network and host forensics using open-source free tools.

1. Introduction

1.1. SMB Background

Server Message Block (SMB) is a communication protocol initially created by IBM and used by Microsoft since the mid-1990s (Desktop Windows Version Market Share Worldwide | Statcounter Global Stats, n.d.). Several versions of the same protocols have been developed since then, and the latest Version is 3.1.1, introduced with Windows 10 and Windows Server 2016.

Network File Sharing is utilized heavily in enterprise environments to save, interact with, read, and write files. While logging the file activities for files inside the network file share is possible, doing so requires saving lots of events, indexing, and parsing for operational events which is a luxury for small to medium enterprises and requires big investments for large organizations. Most organizations cannot do so because of the number of transactions or logs per second. Many digital forensics analysts are using the network for Network File Share to gather the evidence. Again, doing that requires saving a significant amount of data captured for a long time to analyze when needed. Another concern is encrypted protocols like SMBv3, which gives little evidence and metadata as most of the traffic is encrypted.

1.2. Windows Operating Systems

Microsoft Windows has been the leading operating system for desktop computers for decades, with a market share of approximately 68.2% as of Nov 2023 (It is 2022. Why Do You Keep Using SMB?, 2023). Microsoft Windows is utilizing SMB heavily in its operating systems operations, therefore Microsoft SMB forensics has been selected for this research.

1.3. Research Goal

SMB creates lots of artifacts, and it is not quiet. The ever-evolving landscape of cyber threats and the way that enterprises and organizations are structuring their network introduced the need for quicker digital forensics investigation methods. This paper explores different quick forensics methods to analyze SMB file share activities for SMBv2 and SMBv3. It will also address the feasibility of recovering these files through a network or host. That can help the community find ways to see the file-sharing activities without spending lots of money on niche requirements.

2. Research Method

The research methods are divided into three main parts: the operating systems utilized, the tools used during the research, and the procedure used to create the results.

2.1. Environment Set Up.

A physical and virtual lab was set up that includes the specifications below.

- Windows 10 OS 22H1 (CIS image)
- Windows 10 OS 22H2 (CIS image)
- Windows 11 OS (CIS image)
- Two Windows Server 2019 (CIS image)
- Windows Server 2016 (CIS image)
- Network File Share. Windows server has been used as a file share.
- SOF-ELK distribution

Figure 1 below shows the network design.

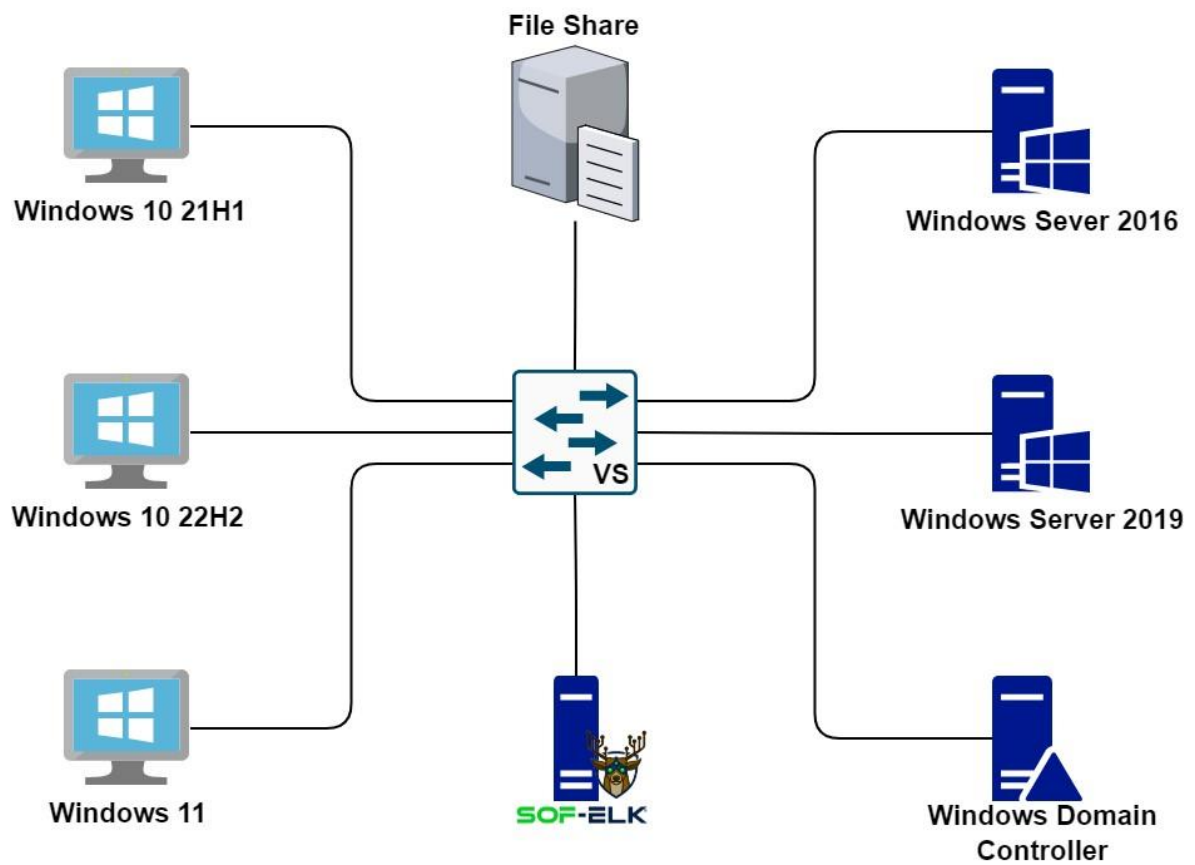


Figure 1. Lab Network Design

2.1.1. Windows Operating System Configurations

All these components have connected to one network to ease the testing. Host firewalls are turned off. The images are CIS-based images for Windows.

2.1.2. Domain Controller

While it is not necessary, installing a domain controller on the Windows server to ease the deployment of any changes and to unify the user accounts is part of the network design for this research. To mimic a real enterprise environment a domain controller is used to control all the server and workstations' policy objects.

2.2. Tools Used

2.2.1. Host Tools

- Process Monitor: Also called Procmon, it is an advanced monitoring tool for Windows that shows real-time file systems (including file creation, deletion, and renaming), registry changes, and other system interactions (2023). The tools are handy for live forensics investigation.
- Logs Parser: While commercial tool is used for ease of testing, but any tool can be used such as SOF-ELK.Loghrythm which has been used to parse the logs.
- Thumb cache viewer and Thumbs viewer
- Windows PowerShell
- Registry Explorer: a tool created by Eric Zimmerman for registry viewer with searching, multi-hive support and different plugins for easily reading registry keys (MDwiki, n.d.).
- PhotoRec

2.2.2. Network Tools

- Wireshark

SOF-ELK distribution: is a platform for digital forensics that is used by forensics examiners to analyze data consisting of Elasticsearch storage and search engine, logs

Hussain ALTayeb, hussain_altayeb@tatweerpetroleum.com

ingestion, and Kibana dashboard (Kim, 2023). It can be used for log parsing, and network analytics as well as data extraction.

2.3. Procedure for Testing

The procedure shows the steps that have been taken in the lab to create results.

1. Different file types have been created and interacted with (read, write, preview, download) at the network file share.
2. Observing all the activities at the Windows operating systems (Windows 10, 11 and Windows Server 2019)
3. Different tools have been used for recording host activities (Registry Explorer, Procmon, ThumbCache viewer, Thumbs viewer, logs, and Sysmon)
4. Observing and taking packet captures for analysis.
5. Different network tools have been used for network analysis (Network Miner, Kibana, Wireshark)
6. Using Recovery tools like PhotoRec for data recovery.
7. Some manual correlation between the host data and network data was used to validate the results.

Tests have been done for SMBv2 and SMBv3 with and without encryption.

3. Findings and Discussion

The first results aimed to gather Windows events and any data related to files being interacted with at the host level. SMBv2 and SMBv3 created the same results. Before exploring the results, it is good to understand the following features in Windows:

- Alternate Data Stream
- Windows Temp Folders
- Windows LNK files
- Windows Shell Bags

3.1. Windows Important Features

3.1.1. Alternate Data Stream

Windows operating system utilizes the NTFS file system, which includes support for alternate data streams. Alternate data streams allow files to contain one or more data streams, which means the file itself and another stream that contains further data or metadata about the file, e.g., where the files were downloaded from (Wilson, 2021). There are multiple data stream attributes in Windows; the most important two are: “\$Data” and “Zone.identifier.” \$Data is part of the file where the actual data resides. The Zone identifier was introduced in Windows XP as a security feature and determines if the file should be trusted. Nowadays, Microsoft applications, for example, use the Zone.id to identify where the files come from and do an action using a policy based on that (Wilson, 2021) (Windows :: DATA Alternate Data Stream | OWASP Foundation, n.d.).

3.1.2. Windows Temp Folders

A Temp folder in Windows can be accessible by the environment variable “%temp%” in the run window or by accessing “%UserProfile%\AppData\Local\Temp.” Windows creates temporary files which become useless once the tasks are completed. Also, sometimes Windows and other applications will have files saved in the temp folder for multiple reasons like saving a copy of a file, where the file is interacted with, or where, if the program crashes unexpectedly, the program will rely on the saved TMP file to recover itself (Bott & Stinson, 2021). As a result, it may contain valuable information worth investigating.

3.1.3. Windows LNK File

Windows creates LNK files when users open or interact with files, folders, and devices. LNK files contain information about an interaction that happened, timestamps of the file from where it is located, and volume data like drive letters (A. Hassan, 2019). LNK files are in “C:\%UserProfile%\AppData\Roaming\Microsoft\Office\Recent.” There

are multiple tools (open source and commercial) to interpret the LNK file; one is LEcmd, written by Eric Zimmerman (MDwiki, n.d.).

3.1.4. Windows Shell Bags

Microsoft Windows records the view preferences of folders and Desktop. Every time a user interacts with a folder or a directory, Windows will remember the location for better user experience so the user can refer to those locations faster. Microsoft Windows operating system saves those preferences in the Registry as a key known as Shell Bag (Lo, 2014).

3.2. Host Forensics Data for Microsoft Documents

The initial testing was done on all the flavors for Windows, including workstations and servers. The first section was about testing Windows Microsoft documents. Three file types were chosen: Microsoft Word, Excel, and PowerPoint 2019. File interactions included reading files, writing new files, previewing the files, and deleting the files. However, the primary focus will be on previewing or reading the files at the network share.

3.2.1. Registry Evidence

Windows Registry is where the system configuration resides. It contains valuable information and records almost every event the users or system takes. Two important registries should be considered for this research to confirm accessing a share and opening or reading a file. The first location is “Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2”, where it shows all the mounted shares (Figure 2) where it can be correlated with Shell Bags to see the interaction with the folders (Figure 3). The other registry location is “NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs,” where it contains the latest file opened along with a timestamp of accessing the file. Then, these events can be correlated and accessing a file share to interact with files in specific locations can be confirmed. to the method/process to locate these files on a Windows machine should also be considered.

Registry hives (1)		Available bookmarks (34/0)		
Enter text to search...		Find		
Key name	# values	# subkeys	Last	
ControlPanel	2	0	20	
Discardable	0	1	20	
ExtractionWizard	1	0	20	
FeatureUsage	1	5	20	
FileExts	0	232	20	
HideDesktopIcons	0	1	20	
LogonStats	2	0	20	
LowRegistry	0	0	20	
MenuOrder	0	1	20	
MMSStuckRects3	12	0	20	
Modules	0	3	20	
MountPoints2	0	14	20	
##NABnCSVM1#Data	1	0	20	
##NABnCSVM1#Transfer	1	0	20	
##nabncsvm1#users\$#AltayebH	1	0	20	

Figure 2. Mounted shares



Figure 3. Shell bag evidence for accessing a file on file share.

3.2.2. File System Artifacts

Windows creates artifacts when a user interacts with a file. The focus here is on the most critical elements of the research topic which are

- Copy of a file in some location in Windows.
- Registry modifications.
- Network Evidence.
- Thumbnails.
- Master File Table (MFT) Metadata changes.

LNK file creation.

Gathering Windows file system activities was done by using Procmon and experimentation. So, once a user reads or previews a Windows Microsoft Office document in a network file share, the Windows operating system caches a copy with a different name (Figure 4) of the file in %UserProfile%\Appdata\Local\Microsoft\Windows\INetCache\Content.MSO (Figure 5). This file will be deleted once the user stops previewing/reading the file.

Another artifact is that Windows will keep the same metadata of the original file, like when the file was modified, the classification of the file, the original author of the file, and other metadata, but the creation of the file will be the time the file was previewed or read (Figure 6) as Windows will consider the file as a copied file, and Windows considers a copied file as a new file creation as part of Windows time rules (Kim, 2024).

EXCEL.EXE	25980	CreateFile	C:\Users\altayebh707\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\793C1B94.xlsx
EXCEL.EXE	25980	CreateFile	C:\Users\altayebh707\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\793C1B94.xlsx
EXCEL.EXE	25980	CreateFile	C:\Users\altayebh707\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\793C1B94.xlsx
EXCEL.EXE	25980	CreateFile	C:\Users\altayebh707\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\793C1B94.xlsx
EXCEL.EXE	25980	CreateFile	C:\Users\altayebh707\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\793C1B94.xlsx

Users > altayebh707 > AppData > Local > Microsoft > Windows > INetCache > Content.MSO				
Name		Date modified	Type	Size
77C6B6FD.xlsx		03/12/2023 10:11 PM	Microsoft Excel W...	7 KB
99E52716.xlsx		30/11/2023 7:23 PM	Microsoft Excel W...	8 KB
793C1B94.xlsx		30/11/2023 7:01 PM	Microsoft Excel W...	9 KB

Figure 5. Copy of the file with a different name

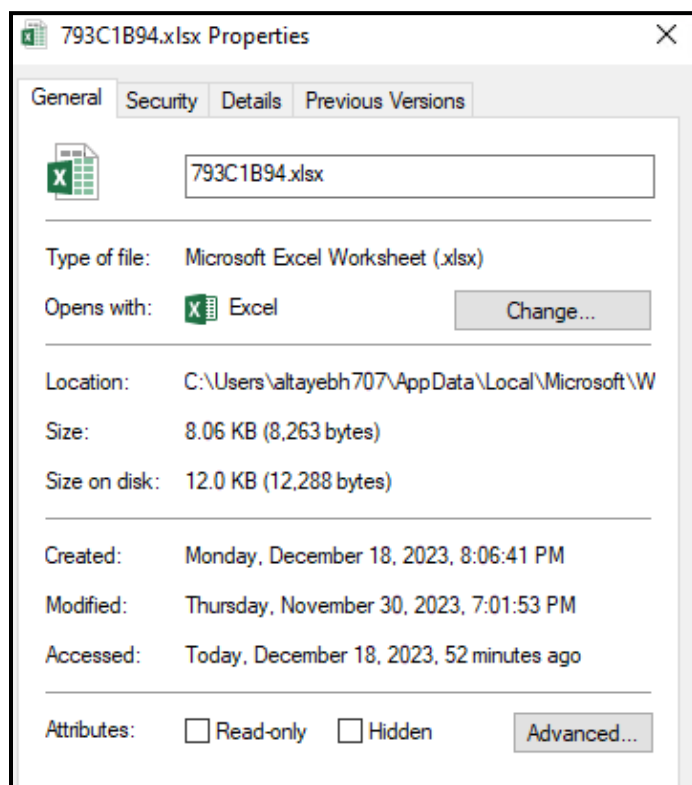


Figure 6. Metadata of the file

Microsoft will create an LNK file or amend an existing LNK file. Also, another file is created with the Alternate DataStream: Zone identifier, indicating that the file has been read, previewed, and copied- “Figure 7”. The Alternate Data Stream (ADS) is an attribute of the file that Windows uses to store data. Windows uses the Zone identifier to determine the file’s download location, e.g., Zone.ID = 3. Figure 8 identifies that the file has been downloaded from the internet, and the ADS can give more information, like the website from which the file was downloaded (Wilson, 2021).

CreateFile	C:\Program Files\Internet Explorer\iexplore.exe
CreateFile	C:\Windows\System32\mspaint.exe
CreateFile	C:\Windows\System32\notepad.exe
CreateFile	C:\Program Files (x86)\Common Files\Microsoft Shared\MSEnv\VSLauncher.exe
CreateFile	C:\Program Files (x86)\Windows Media Player\wmplayer.exe
CreateFile	C:\Program Files\Windows NT\Accessories\wordpad.exe
CreateFile	\\nabncsvm1\Transfer\#\MasterTest#\TestWord2.docx
CreateFile	\\nabncsvm1\Transfer\#\MasterTest#\TestWord2.docx:Zone.Identifier

Figure 7. the Alternate Data stream, Zone identifier

3.2.3. Key Windows Logs

```
PS>Get-Content -Path C:\temp\ColorSplash.themepack -Stream Zone.Identifier
[ZoneTransfer]
ZoneId=3
HostUrl=http://download.microsoft.com/download/F/B/D/FBD00A74-6A14-43AC-938D-E3283056023C/ColorSplash.themepack
PS>
```

Figure 8: Using PowerShell to identify the Host URL for a downloaded file

```
Share</Task><Opcode>Info</Opcode><Keywords>Audit Success</Keywords><TimeCreated
SystemTime='2023-12-03T19:31:02.609656400Z'/><EventRecordID>409302003</EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='39540'/><Channel>Security</Channel>
<Computer>nabwsiem1.bh1-og.com</Computer><Security/></System><EventData><Data
Name='SubjectUserSid'>BH1-OG\AltayebH707</Data><Data
Name='SubjectUserName'>AltayebH707</Data><Data Name='SubjectDomainName'>BH1-OG</Data><Data
Name='SubjectLogonId'>0x3d7f04b84</Data><Data Name='ObjectType'>File</Data><Data
Name='IpAddress'>10.221.143.30</Data><Data Name='IpPort'>65015</Data><Data
Name='ShareName'>\\*\Users</Data><Data Name='ShareLocalPath'>\\?.C:\Users</Data><Data
```

Figure 9. Event ID 5145 and Zone ID evidence along with the file name logs, so the focus is on Event ID 5154 (without the Object access security log, which creates lots of logs). Windows event 5145 tracks if a network file share was accessed (Windows Security Log Event ID 5145 - a Network Share Object Was Checked to See Whether Client Can Be Granted Desired Access, n.d.). However, it has a great artifact showing whether the file has been read or previewed (Figure 9). For some reason, Microsoft uses Zone ID along with the file name, and after some testing, it was concluded that whenever a user previews a file through network share, Zone ID will be associated with the file names that have been read or previewed.

3.3. Host Forensics Data for Non-Microsoft Documents

An enormous number of applications create files in Windows, so the focus here will be on PDF files and Wireshark PCAP files. Hundreds of millions worldwide use

PDF files, which may contain sensitive information, whereas digital forensics examiners use PCAP files, which can be used to construct files from Section 3.5 of this paper.

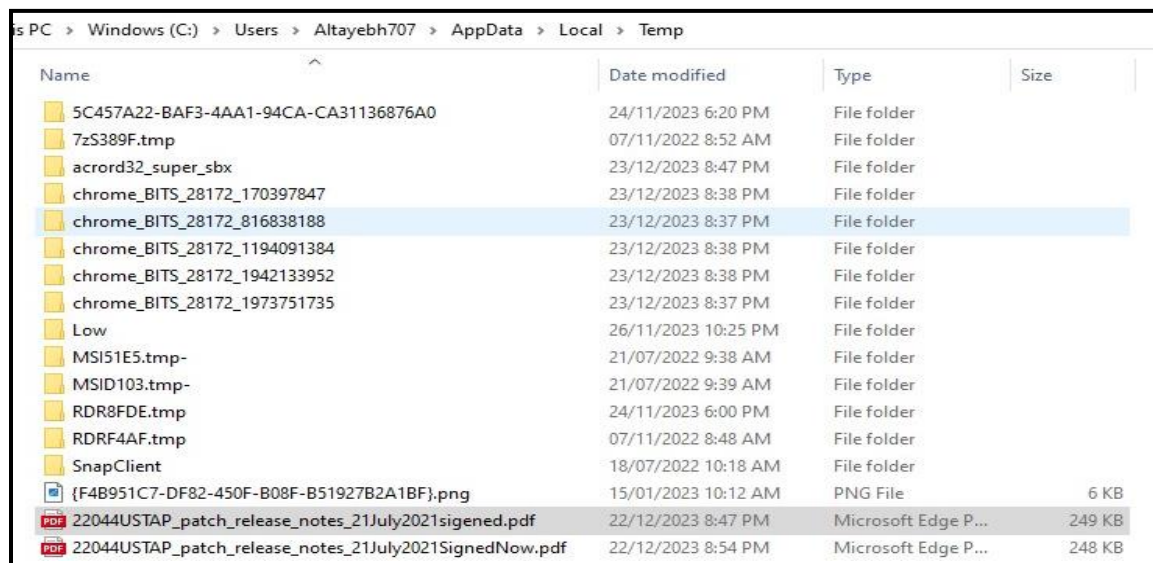
3.3.1. Windows 21H1 Artifacts for PDF Files

While Windows 21H1 is out of support, it still contains valuable information, and some enterprises may still use it. So, for the PDF files for 21H1, two applications are tested for reading pdf files: Adobe Acrobat Reader 11.0 and Foxit pdf Reader. Adobe for Windows 21H1 created an artifact in which some files, when they are opened in a file share, a copy of the file is kept in the Windows temp folder in “C:\%UserProfile%\AppData\Local\Temp” (Figure 10). The files constantly get amended with a number at the beginning, e.g., if the file name is “testmasters,” the new file name would be “123testmasters.”

Some metadata of the file changes like the modification of the file stays the same in Windows 10 (just like copying the file Windows rules), where the creation time would be the time of the file when it was opened or previewed, and the access time will be the same for the first time and will change depending on file access (Figure 11).

However, there is no consistency in determining when the temp folder will keep a copy of the file. Out of 31 samples, 21 samples of the files were created in the temp folder. The test has been done again, and the results are different. Out of 30 samples, 14 files were created. Nevertheless, it gives evidence where a digital forensic examiner might be looking for files that have never been saved on a desktop but in a mounted share. Additionally, attackers might leverage such location to search for sensitive files where the user would think it is safe in a shared file. These files stay for a long time in the file share, as shown in Figure 12, which might also help digital examiners recover old files.

Another important artifact is the creation of the file. The file is created by Windows “explorer.exe” and not the application itself, which Windows will do for a specific unknown reason, as a regular forensics examiner would expect from Microsoft (Figure 13).



Name	Date modified	Type	Size
5C457A22-BAF3-4AA1-94CA-CA31136876A0	24/11/2023 6:20 PM	File folder	
7zS389F.tmp	07/11/2022 8:52 AM	File folder	
acrord32_super_sbx	23/12/2023 8:47 PM	File folder	
chrome_BITS_28172_170397847	23/12/2023 8:38 PM	File folder	
chrome_BITS_28172_816838188	23/12/2023 8:37 PM	File folder	
chrome_BITS_28172_1194091384	23/12/2023 8:38 PM	File folder	
chrome_BITS_28172_1942133952	23/12/2023 8:38 PM	File folder	
chrome_BITS_28172_1973751735	23/12/2023 8:37 PM	File folder	
Low	26/11/2023 10:25 PM	File folder	
MSI51E5.tmp-	21/07/2022 9:38 AM	File folder	
MSID103.tmp-	21/07/2022 9:39 AM	File folder	
RDR8FDE.tmp	24/11/2023 6:00 PM	File folder	
RDRF4AF.tmp	07/11/2022 8:48 AM	File folder	
SnapClient	18/07/2022 10:18 AM	File folder	
{F4B951C7-DF82-450F-B08F-B51927B2A1BF}.png	15/01/2023 10:12 AM	PNG File	6 KB
22044USTAP_patch_release_notes_21July2021signed.pdf	22/12/2023 8:47 PM	Microsoft Edge P...	249 KB
22044USTAP_patch_release_notes_21July2021SignedNow.pdf	22/12/2023 8:54 PM	Microsoft Edge P...	248 KB

Figure 10. PDF files created in temp directory.

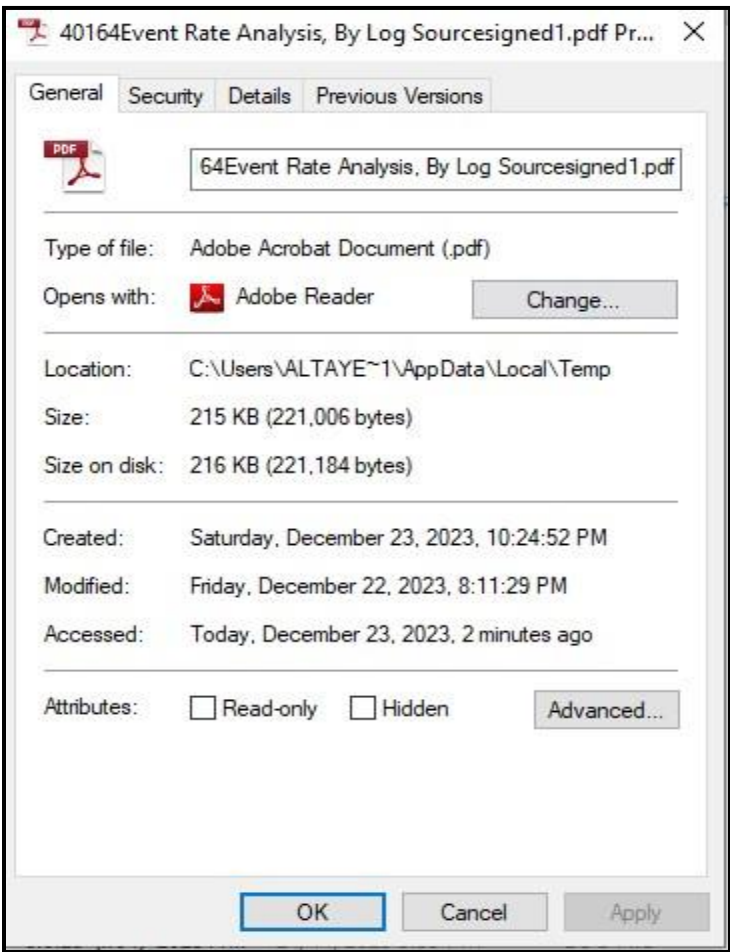


Figure 11. Metadata of file creation in temp folder

Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\acord32_super_sbx	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Windows Explorer				
Microsoft Corporation				
C:\WINDOWS\Explorer.EXE			C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	NAME NOT FOUND
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	SUCCESS
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	NAME INVALID
Explorer.EXE	36504	CreateFile	C:\Users\Altayebh\0\AppData\Local\Temp\40164Event Rate Analysis, By Log Sourcesigned1.pdf	IS DIRECTORY

Figure 12. Windows Procmon showing explorer.exe creating copy of the files in temp folder.

Figure 13. Temp files are kept for a long time.

Windows 22H2 did not have the same behavior for PDF files using Adobe, but using Foxit Reader, some fascinating artifacts have been found. While opening the file in a shared drive, it did not have evidence, and after some testing, both applications created the “.TMP” file in the Window Temp directory.

One more artifact is that these files were created differently; in the case of Adobe PDF reader, Explorer.exe will create the TMP file, whereas Foxit reader will create the TMP file by itself (Figure 18). This was investigated by using Microsoft Sysinternal procmon.exe.

52EB.tmp	30/12/2023 8:30 PM	TMP File	241 KB
BGInfo.bmp	30/12/2023 8:30 PM	BMP File	8.101 KB

Figure 14. Foxit reader creates a temp pdf file in temp directory

```
%PDF-1.6
%aãÏ0
1 0 obj
<</Pages 2 0 R/Type/Catalog>>
endobj
2 0 obj|
<</Count 0/Kids[]/Type/Pages>>
endobj
3 0 obj
<<>>
endobj
xref
0 4
0000000000 65535 f
0000000016 00000 n
0000000061 00000 n
0000000107 00000 n
trailer
<</Size 4/Root 1 0 R/Info 3 0 R/ID[<7A520DC3A47B3F40BE5363C573426A75><7A520DC3A47B3F40BE5363C573426A75>]>>
startxref
127
%%EOF
```

Figure 15. PDF file creating only new tmp file containing a signature

52EB.pdf - Foxit PDF Reader

LogRhythm
The Security Intelligence Company

SmartResponse Plugin Guide:
FortiGate

August 2, 2018 – Revision B

Introduction

This guide describes the FortiGate SmartResponse Plugin, the plugin's available actions, and how to configure the plugin. This plugin uses FortiGate's RESTful API to view group information and add IP addresses or domains to a group.

Prerequisites

- This SmartResponse Plugin is compatible with LogRhythm Enterprise 7.2.7 and later.
- To use this plugin, you must be running PowerShell v3.0 or later. To determine your PowerShell version, open PowerShell and enter **\$PSVersionTable.PSVersion** at the prompt. If necessary, download a new version from the Microsoft Download Center.

Digitally signed by AITayebH
DN: cn=AITayebH, o=AITayebH, ou=AITayebH, email=AITayebH@tateerpetroleum.com
Reason: I am the author of this document
Location: your signing location
Date: 2023.12.30 18:00:00+0000
Foxit PDF Reader Version: 11.1.8

Figure 16. Valid pdf file after changing .tmp to .pdf

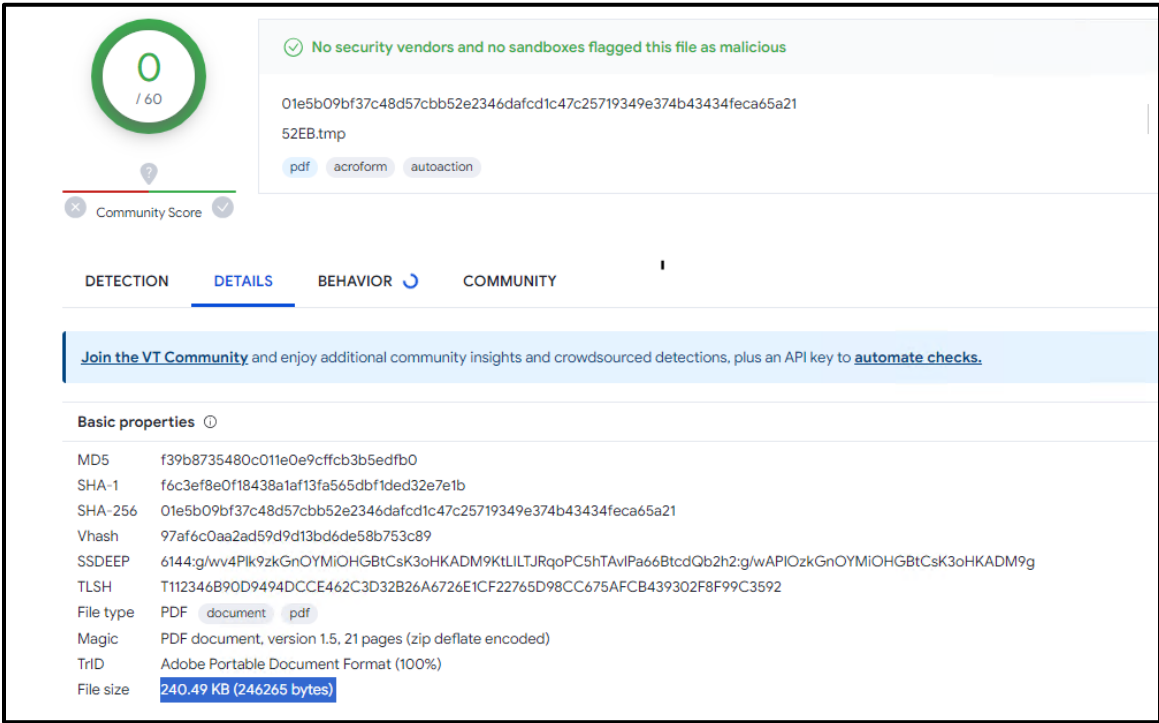


Figure 17. VirusTotal upload result of 52EB.tmp file

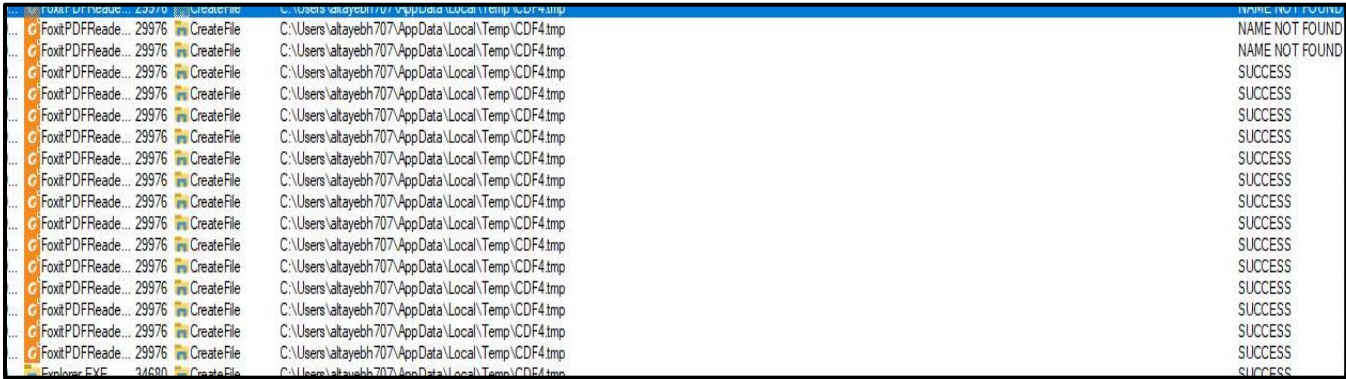


Figure 18. Creation of TMP files

3.3.3. Windows 10+ Artifacts for Wireshark

Wireshark is one application that creates a copy of a packet capture in the temp folder. Wireshark will create a copy in case the user has started a packet capture for some time and stopped it for analyzing the Wireshark sample (Figure 19).

Wireshark is important since it has some capabilities in constructing files. Alternatively, the examiner can even take the packet capture and use other network forensics tools like Zeek, Network Miner, and many others to carve the data out of packet captures, and SMB is no exception.

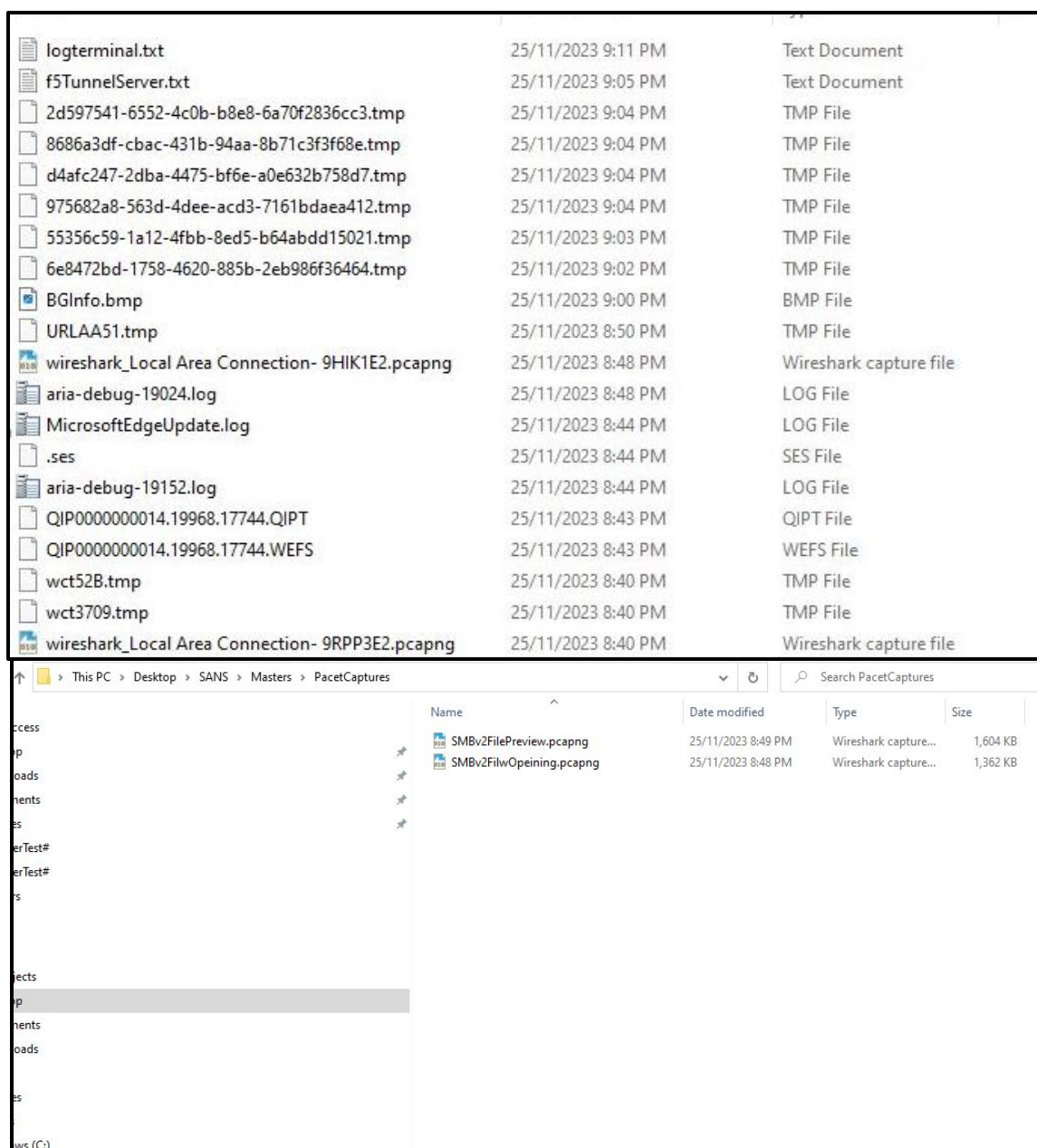


Figure 19. Wireshark packet capture creation in temp folder

3.3.4. Thumbnails Cache Might Help

A thumbnail is a small picture preview that the operating system creates for specific file types. The “Thumbs. dB” hidden system folder or the “thumb cache” database contains these thumbnails. To help with investigations or incident response, forensic analysts can use these thumbnails to learn more about the files viewed on a Windows system. During the experiment in the lab, a file was opened on a shared drive with the explorer set to a large icons layout, which generated an artifact on the local disk (thumbnail) that contains the first-page snapshot (Figure 20). Thumbnails or ThumbCache databases are stored in:

“%userprofile%\AppData\Local\Microsoft\Windows\Explorer.” the tool

“thumbcache_viewer” was used to read the database. This is important to recover a part of the opened documents through SMB.

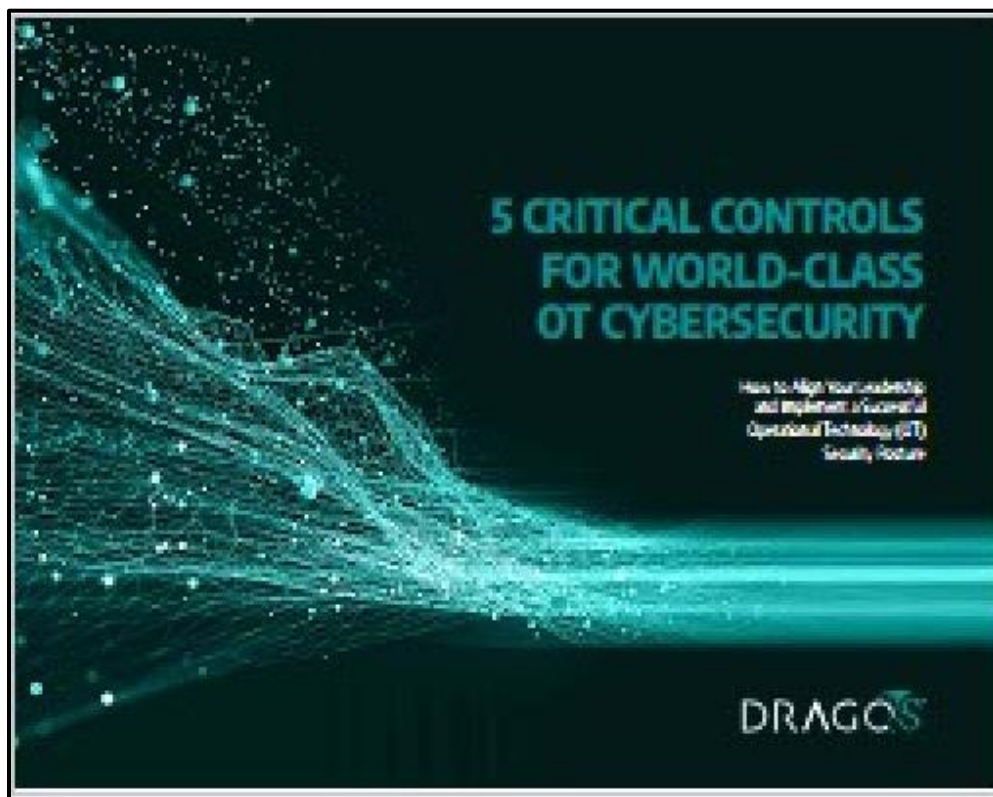


Figure 20. A thumbnail that was collected from one of the Thumb cache Databases

3.4. Files Recovery

As mentioned in the previous section, PDF file recovery is easier since retention depends on the tempt folder cleanup process. However, Microsoft Office documents will be deleted right after closing the document. In this case, experimenting with file recovery through unallocated space analysis is one solution to recover the file. Examining the areas of a storage device that are not currently assigned to any particular file is necessary for file recovery from unallocated space. Data from deleted files could linger in the unallocated space until they are replaced by new data (Bott & Stinson, 2021).

Forensic investigators can employ specialized tools to look for file signatures or structures in the unallocated space. Files deleted or fragmented can be recovered thanks to these programs that find patterns that correspond with popular file formats.

Unallocated space recovery success, however, depends on several variables, including the file system being used, the amount of time since deletion, and whether or not the space has been overwritten.

PhotoRec is a free and open-source file recovery software designed to recover lost files, including videos, documents, and archives from hard disks, CD-ROMs, and lost pictures from camera memory. It operates based on file carving, which means it does not rely on the file system but instead searches for known file headers and footers to identify and recover files (PhotoRec, 2023).

PhotoRec will recover files and give files different names (Figure 21). Nevertheless, the content would be the same for the files. PhotoRec effectively recovers photos as well. NIST Tested PhotoRec v7.0 in 2014, and it was most successful in recovering gif,bmp, png, jpg, and tiff files (Department of Homeland Security, 2014).

f295014320.jar	9/25/2023 1:02 PM	JAR File	178 KB
f297579816_Content_Types.zip	8/14/2012 4:55 PM	zip Archive	8 KB
f297936824.docx	12/14/2023 7:57 PM	Microsoft Word D...	19 KB
f297938544_Content_Types.zip	8/14/2012 4:54 PM	zip Archive	6 KB
f308508703_Content_Types.zip	12/31/2011 7:00 PM	zip Archive	3 KB
f308509312_Content_Types.zip	12/31/2011 7:00 PM	zip Archive	4 KB
f308509624_charts.zip	12/31/2011 7:00 PM	zip Archive	1 KB
f313959544_Content_Types.zip	7/11/2023 3:02 AM	zip Archive	19 KB
f313960808_Content_Types.zip	7/11/2023 3:02 AM	zip Archive	23 KB

Figure 21. File Carving Results using PhotoRec

3.5. Network Forensics Data for SMB

SMBv2 has been in the wild for some time now, and SMB3 is used a lot on newer Windows operating systems like Windows 10 and 11. There is a misconception about SMBv3 that it comes with encryption enabled by default, but SMBv3 does not. Nevertheless, SMB3 has lots of great features like multichannel support and end-to-end encryption (2023).

Using Network packet captures, SMB2 and SBM3 — using SMB3 default configuration without encryption” — will create the same evidence like file read, file creation, file deletion, and other file operations.

For the network forensics topic for this paper, the interaction is going to be with Microsoft Office documents and PDF files. Different interaction will be covered which are: file deletion, file creation, file read or preview and finally file copy.

SMB is very noisy when it creates lots of data once a folder is opened. Sometimes once a user interacts with a folder that has multiple Microsoft documents, SMB will have the actual data of the files inside the packets. This means that the examiner will have a chance to construct the files out of the packet capture. Nevertheless, one important header for SMB to look at is the Disposition.

3.5.1. File Read or Preview

Disposition has multiple options that indicate the interaction with the file. During the testing over Wireshark, Wireshark filters were used that to look for file interaction. For example, the filter “SMB.cmd == 5 “(Figure 22) the server response will indicate that the file has been read or previewed . Keeping in mind that the file’s actual data will be constructed – even though it has not been copied – and Wireshark can be used to export the objects out of the packet capture.

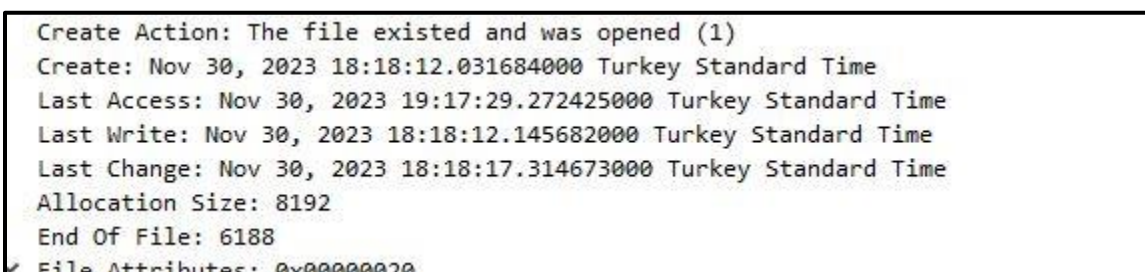


Figure 22. Using filter “SMB.cmd == 5“to see the file read under SMB application data in Wireshark

3.5.2. File Creation

Users can still interact with the file share and if they have the privilege to write objects or create files inside a specific file share, they can do so. Wireshark can interpret the data from the server regarding files creation. Figure 23 shows the create options under the disposition in SMB headers will show that a file was created.

3.5.3. File Deletion

Another piece of evidence is the file deletion. If a user deletes a file from a file share, then it is also recorded in the packet capture as shown in Figure 24.


```

Disposition: Create (if file exists fail, else create it) (2)
✓ Create Options: 0x00000064
....0 = Directory: File being created/opened must not be a directory
...0. = Write Through: Writes need not flush buffered data before completing
....1. = Sequential Only: The file will only be accessed sequentially
....0... = Intermediate Buffering: Intermediate buffering is allowed
...0.... = Sync I/O Alert: Operations NOT necessarily synchronous
....1.... = Sync I/O Nonalert: All operations SYNCHRONOUS, waits not subject to alert
....1.... = Non-Directory: File being created/opened must not be a directory
....0.... = Create Tree Connection: Create Tree Connections is NOT set
...0.... = Complete If Oplocked: Complete if oplocked is NOT set
...0.... = No EA Knowledge: The client understands extended attributes
....0... = 8.3 Only: The client understands long file names
....0... = Random Access: The file will not be accessed randomly
...0.... = Delete On Close: The file should not be deleted when it is closed
...0.... = Open By FileID: OpenByFileID is NOT set
....0... = Backup Intent: This is a normal create
....0... = No Compression: Compression is allowed for Open/Create
....0... = Reserve Opfilter: Reserve Opfilter is NOT set
...0.... = Open Reparse Point: Normal open
....0... = Open No Recall: Open no recall is NOT set
....0... = Open For Free Space query: This is NOT an open for free space query
✓ Filename: NABnCSVM1.bh1-og.com\Transfer\#Master#\New Microsoft Excel Worksheet.xlsx
  Blob Offset: 0x00000078

```

Figure 23. File creation evidence in Wireshark

```

....0 = Read: Object can NOT be shared for read
...0. = Write: Object can NOT be shared for write
....1. = Delete: Object can be shared for DELETE

```

Figure 24. File deletion evidence in Wireshark

3.5.4. File Rename

Wireshark can help in detecting file renames. The client might initiate a request for renaming a file as shown in (Figure 25) indicating a file rename operation.

The most important thing out of this operation that all interaction with these files will let Wireshark or Zeek to carve the data

```
224 SetInfo Request FILE_INFO/SMB2_FILE_RENAME_INFO File: NABnCSVM1.bh1-og.com\Transfer\#Master#\New Text Document.txt NewName:#Master#\TestCreation.txt
124 SetInfo Response
438 Create Request File: NABnCSVM1.bh1-og.com\Transfer\#Master#
378 Create Response File: NABnCSVM1.bh1-og.com\Transfer\#Master#
154 Notify Request File: NABnCSVM1.bh1-og.com\Transfer\#Master#
484 Create Request File: NABnCSVM1.bh1-og.com\Transfer\#Master#;Find Request SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *;Find Request SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern:
131 Notify Response, Error: STATUS_PENDING
242 Create Response File: NABnCSVM1.bh1-og.com\Transfer\#Master#
850 Find Response
131 Find Response, Error: STATUS_NO_MORE_FILES
146 Close Request File: NABnCSVM1.bh1-og.com\Transfer\#Master#
183 Close Response
```

Figure 25. File Rename evidence using Wireshark

3.5.5. SMBv3 and SOF-ELK

The most significant issues arise when enabling SMBv3 end-to-end encryption in which traffic cannot be seen, and apparently, the examiner will not be able to see any SMB data that can help them to see file flow.

Tools like SOF-ELK can help the examiner conduct analytics over the network traffic to see the bandwidth of SMB traffic and then confirm file read or file copy, but not much can be done. For this research, the lab utilized SOF-ELK to analyze SMBv3 traffic, but there was another issue that SMB3 imposes, which is SMB compression that Microsoft does to consume less network bandwidth (2023). In Figure 26, Windows shows a file that should be 19 MB (actual file size), while SOF-ELK shows 15MB, including the other packet headers. In a single session, the user can start reading the network events before deciding to go to the host and do further investigation. Another method could be decrypting the traffic for SMBv3 which requires the private key, and it would give the same results as SMBv2.

t	ApplicationPath	/ip/tcp/smb
t	ApplicationTags	file_mngt
Ⓜ	Captured	false
t	Channel	0
#	ChildFlowNumber	1
t	CommandString	smb2 negotiate, smb2 session setup
Ⓜ	ConnectionEstablished	false
#	CreditCharge	1
#	CreditsRequested	33
#	DestBytes	15MB
#	DestBytesDelta	15MB
Ⓜ	DestIP	10.221.16.134
t	DestMAC	00:09:0f:09:19:02
#	DestPort	445
#	Duration	0:05:07
#	FieldCount	51
t	Flags	25
Ⓜ	FlowClassified	true

Figure 26. SOF-ELK Metadata for SMBv3 traffic

4. Recommendations and Implications

4.1. Recommendations for Practice

Based on the analysis and experiments that have been done, there are many SMB artifacts. Digital forensic examiners can utilize a plethora of methods to analyze Windows files that have never been saved on disk.

Forensic examiners only have access to some of the information at once, and sometimes, they are left with only Windows machines to analyze, packet capture to parse, or just a few Windows event logs.

Identifying the different use cases can save time by adopting the different methods discussed in this research for analyzing Windows SMB traffic. Analyzing all packet captures does not help, but using tools like Zeek and SOF-ELK, the examiner can build the use cases based on the filters that can identify the file creation, modification, rewrite, or deletion. Using tools like Network Miner or even SOF-ELK to look for specific traffic and save exported objects compressed in storage for even a few days can save lots of time when the Security Operation Center works effectively.

On the side of analyzing Windows artifacts, there are many SIEM (free and commercial) tools on the market that log all registry modifications and Windows Logs or parse any data that the examiner would like to see easily on a dashboard. Nevertheless, the due diligence of doing Windows forensics depends on the cases being investigated. Different tools create different artifacts, so the examiner should test the tools being used on the environment to save time during forensics examinations, as can be seen in the section for PDF file creation in the Tmp folder, where two different tools created two different results over two different operating system versions.

It is recommended that forensics examiner should always have a lab that can mimic a natural environment. So, he can test the tools, verify what artifacts can be created, and build cheat sheets, saving him lots of time when an investigation occurs.

4.2. Implications for Future Research

This research represented many methods to analyze SMB traffic and recover deleted files or files that have never been saved on the disk. Attackers utilize SMB because it is relatively easy and challenging to detect lateral movement as they use the living off-the-land method to reach their goal.

One of the things that can be done is automating all events used in this research into a single tool to analyze the SMB events and traffic. Then, the tool can correlate the network and Windows events data and create an excellent report of specific file tracking.

Another tool that can be created is a tool that gathers the data from the Windows Process monitor and Windows registry to track any file creation in the TMP folder or content. MSO folder and saves the files in a different location before they are deleted. The tool can also highlight how the file has been created, which process created the file, which saved the metadata of the file, and the original location of the file.

5. Conclusion

Defenders should always test their tools and understand their environment. There are many capabilities and events that defenders and forensics examiners can come up with. These capabilities need to be documented in Microsoft documents or the tool being used. While the attacker does lots of testing before his next step, the defender should do the same. Defenders always run after commercial solutions that cost lots of money and sometimes do not meet their requirements. SMB creates multiple artifacts where defenders and examiners should consider the methods of this research to create their use cases inside their tools, whether it is SIEM or network analytics tools, without waiting for the investigation to commence. Instead, they should be proactive.

References

Desktop Windows Version Market Share Worldwide | Statcounter Global Stats. (n.d.).

StatCounter Global Stats, from <https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide>

It's 2022. Why do you keep using SMB? (2023, September 8), from

<https://www.ivanti.com/blog/it-s-2022-why-do-you-keep-using-smb>

M. (2023, March 9). Process Monitor - Sysinternals. Microsoft Learn, from

<https://learn.microsoft.com/en-us/sysinternals/downloads/procmon>

Kim, A. (2023, December 18). SOF-ELK | SANS Institute, from

<https://www.sans.org/tools/sof-elk/>

Wilson, C. (2021, October 8). Forensic Analysis of the Zone.Identifier Stream. Digital

Detective, from <https://www.digital-detective.net/forensic-analysis-of-zone-identifier-stream/>

Kim, A. (2024, January 29). Windows Forensic Analysis | SANS Poster.

<https://www.sans.org/posters/windows-forensic-analysis/>

Windows ::DATA Alternate Data Stream | OWASP Foundation. (n.d.), from

https://owasp.org/www-community/attacks/Windows_alternate_data_stream

Bott, & Stinson. (2021). Windows 10 Inside Out (4th Edition). Pearson Education, Inc.

A.Hassan. (2019). Digital forensics basics: A Practical Guide Using Windows OS (First).

Springer Science.

- Windows Security Log Event ID 5145 - A network share object was checked to see whether client can be granted desired access. (n.d.), from <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=5145>
- MDwiki. (n.d.), from <http://ericzimmerman.github.io>
- PhotoRec. (2023, July 11), from Softonic, from <https://photorec.en.softonic.com/>
- D. H. (2023, February 23). New SMB file server 3.0 features - Windows Server. Microsoft Learn, from <https://learn.microsoft.com/en-us/troubleshoot/windows-server/high-availability/smb-3-file-server-features>
- Department of Homeland Security . (2014, July). [Test Results for Graphic File Carving Tool], from <https://www.dhs.gov/>.
- N. (2023, May 18). SMB Compression, from Microsoft Learn. <https://learn.microsoft.com/en-us/windows-server/storage/file-server/smb-compression?tabs=powershell%2Crobocopy%2Cgroup-policy>
- Lo. (2014, March 24). Windows ShellBag Forensics in Depth. Giac.Org. Retrieved January 30, 2024, from <https://www.giac.org/paper/gcfa/9576/windows-shellbag-forensics-in-depth/128522>