Lecture 5- Operating System Forensics

Dr. Zunera Jalil

Email: zunera.jalil@au.edu.pk

18th March 2025

Data Analysis for OS Forensics

- Forensic examiners perform data analysis to examine artifacts left by perpetrators, hackers, viruses, and spyware.
- They scan deleted entries, swap or page files, spool files, and RAM during this process.
- These collected artifacts can provide a wealth of information with regard to *how malicious actors tried to cover their tracks and what they were doing to a system*.

What is Operating System Forensics?

- The process of retrieving useful information from the Operating System (OS) of the computer or mobile device in question.
- The aim is to acquire empirical evidence against the perpetrator.
  - The understanding of an OS and its file system is necessary to recover data for computer investigations.
  - The file system provides an operating system with a roadmap to data on the hard disk & also identifies how hard drive stores data.
  - There are many file systems introduced for different operating systems.
    - **FAT, exFAT,** and **NTFS** **for Windows OSs**
    - **Ext2fs,** or **Ext3fs** **for Linux OSs.**

What is Operating System Forensics?

- Data and file recovery techniques for these file systems include data carving, slack space, and data hiding
- Another important aspect of OS forensics is memory forensics, which incorporates virtual memory, Windows memory, Linux memory, Mac OS memory, memory extraction, and swap spaces.
- OS forensics also involves web browsing artifacts, such as messaging and email artifacts.
- Common Operating Systems are **Windows, Linux, Mac, iOS, and Android.**

Windows Forensics

- Investigators can search out evidence by analyzing the following important locations of the Windows:

1. **Recycle Bin:** This holds files that have been discarded by the user. When a user deletes files, a copy of them is stored in recycle bin. This process is called "Soft Deletion". Recovering files from recycle bin can be a good source of evidence.
2. **Thumbs.db Files:** These have images' thumbnails that can provide relevant information.
3. **Browser History:** Web Browser generates history files that contain significant information. Microsoft Windows Explorer is the default web browser for Windows OSs.
    1. Other supported browsers are Opera, Mozilla Firefox, Google Chrome, and Apple Safari.

4. Print Spooling:

- This process occurs when a computer prints files in a Windows environment. When a user sends a print command from a computer to the printer, the print spooling process creates a **“print job”** to some files that **remain in the queue** unless the print operation is completed successfully.
- Printer configuration is required to be set in either EMF mode or RAW mode.

- In a **RAW mode**, the print job merely provides a straight graphic dump of itself.
- In an **EMF mode**, the graphics are converted into the EMF image format (Microsoft Enhanced Metafile).
  - These EMF files can be indispensable and can provide an empirical evidence for forensic purposes.

Windows Forensics

- The path to EMF files is:

  For Windows NT and 2000:

  Winnt\system32\spool\printers

  For Windows XP/2003/Vista/2008/7/8/10:

  Windows\system32\spool\printers

- OS forensic tools can automatically detect the path; there is no need to define it

Registry Forensics

5. **Registry:** Windows Registry holds a database of values and keys that give useful pieces of information to forensic analysts.

- Windows Registry keeps most of the information pertaining policies, status etc. in form of keys, sub keys and values.
- Windows registry can be worked upon by administrator through application like **‘regedit’.**
- Windows can also be supplied with a command like tool like ’reg’ to help users work on registry.
- Registry contains **hives** under which sub keys are present. These hives play important role in the overall functioning of the system.

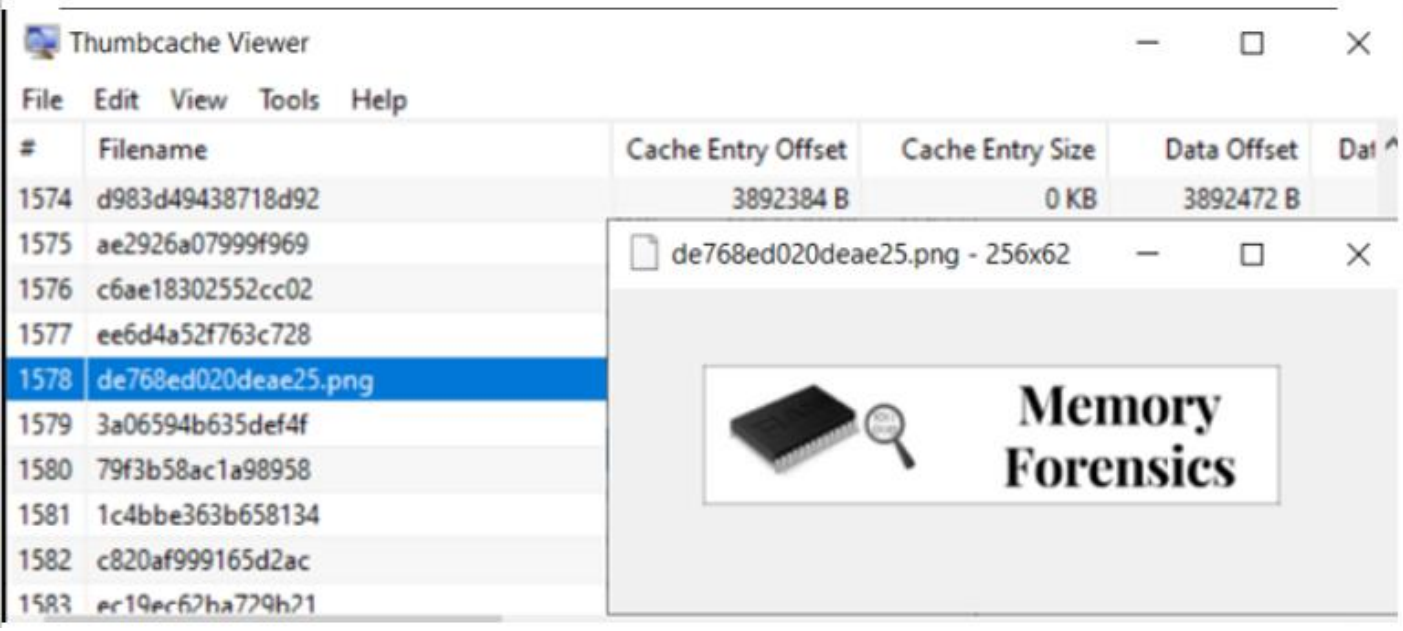
Windows Artifacts

Artifact	Artifact	Artifact
Thumbcache	Alternate Data Streams (ADS)	SYSTEM
Jump Lists	Link File – Shortcut (.lnk)	Windows Error Reporting (WER)
Recycle Bin	RDP Bitmap Cache (BMC)	EventTranscript.db
Prefetch Files	UserAssist	Volume Shadow Copy Service (VSS)
ShimCache	WordWheelQuery	User Access Logging (UAL)
Amcache	NTUSER.DAT	PowerShell
System Resource Usage Monitor (SRUM)	ShellBags	lsass.exe
Master File Table ($MFT)	Background Activity Moderator (BAM) / (DAM)	Windows.edb
Windows 10 Timeline (ActivitiesCache)	Security Account Manager (SAM)	sysmain.sdb
$J	SECURITY	Windows Registry Hive
$LogFile	SOFTWARE	Forensically interesting spots in Windows Registry

Thumbcache

What is it?

When the user views from the Windows folder viewing options, a small thumbnail version of the pictures will be created and stored in a single file. This file stores a thumbnail version of the existing and deleted pictures.



Forensic Value:

1. Evidences of deleted pictures
2. Recover deleted pictures
3. Good clue about the pictures contents that used

Location:

%USERPROFILE%\AppData\Local\Microsoft\Windows\Explorer

Tool:

thumbcache_viewer.exe , thumbs_viewer.exe

Jump lists

What is it?

Provides the user with a graphical interface associated with each installed application which lists files that have been previously accessed by that application.

A	B	C	D	
SourceCreated	SourceModified	AppId	AppIdDescription	TargetIDAbsolutePath
2/9/2021 20:29	9/28/2021 21:35	7e4dca80246863e3	Control Panel - Settings	Control Panel\System and Security\System
2/9/2021 20:29	9/28/2021 21:35	7e4dca80246863e3	Control Panel - Settings	All Tasks\Uninstall a program
2/9/2021 20:29	9/28/2021 21:35	7e4dca80246863e3	Control Panel - Settings	Control Panel\Network and Internet\Network and Sharing Center
2/9/2021 20:29	9/28/2021 21:35	7e4dca80246863e3	Control Panel - Settings	Control Panel\Programs\Programs and Features
2/9/2021 20:29	9/28/2021 21:35	7e4dca80246863e3	Control Panel - Settings	Control Panel\Hardware and Sound\Power Options

A	B	C	D	E
TargetAccesse	AppIdDescription	LocalPath	TargetIDAbsolutePath	Arguments
2/21/2021 21:11	Remote Desktop Connection 6.1.7600 (Win7)	C:\Windows\System32\mstsc.exe	My Computer\C:\Windows\System32\mstsc.exe	/v:"172.16.151.50"
5/5/2021 3:53	Remote Desktop Connection 6.1.7600 (Win7)	C:\Windows\System32\mstsc.exe	My Computer\C:\Windows\System32\mstsc.exe	/v:"172.16.151.150"
5/19/2021 23:51	Remote Desktop Connection 6.1.7600 (Win7)	C:\Windows\System32\mstsc.exe	My Computer\C:\Windows\System32\mstsc.exe	/v:"172.16.85.104:65520"

Forensic Value:

1. User activity who have interactively on system
2. Recover user's traces of recently accessed directories from the Windows Explorer jump list
3. History of attempted lateral movement by checking Remote Desktop jump lists, as they provide a list of recent connections
4. Destination IPs and ports via RDP

Location:

%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

%USERPROFILE%\AppData\Microsoft\Windows\Recent\CustomDestinations (via Taskbar)

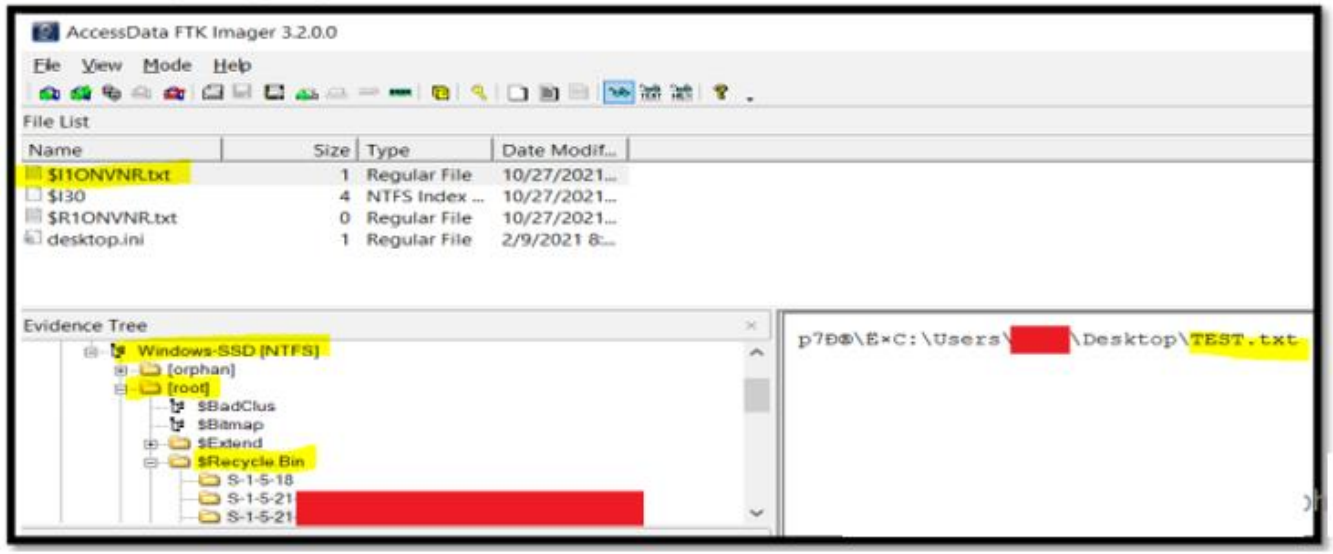
Tool:

JLECmd.exe

Recycle Bin

What is it?

When the user deletes a file, the file is moved into a temporary storage location for deleted files named Recycle Bin. Windows creates two files each time a file is placed in the Recycle Bin **$I** and **$R** with string six character identifier generated for each file. **$R file is a renamed copy of the "deleted"** file. While the **$I file replaces the usage INFO2 file as the source of accompanying metadata**.



Forensic Value:

1. The original file name and path
2. The deleted file size
3. The date and time of deletion

Location:

$Recycle.Bin

Tool:

RBCmd.exe , Rifiuti2, Recbin.exe, EnCase, FTK, Autopsy, RecycleDump.py , $I_Parse.exe

Prefetch files

What is it?

They are a performance optimization mechanism to reduce boot and application loading times. The cache manager can use these prefetch files like a " cheat sheet " to speed up the loading process. Prefetch is not enabled by default on Windows servers.

Forensic Value:

1. The executable's name
2. The absolute Path to the executable
3. The number of times that the program ran within the system
4. The last time the application ran
5. A list of DLLs used by the program

Location:

%SystemRoot%\prefetch

Tool:

PECmd.exe , WinPrefetchView.exe

	A	B
1	RunTime	ExecutableName
2	10/30/2021 20:21	\VOLUME{01d4207de1e70a8f-58e49381}\USERS\[redacted]\DFIR\PREFETCH\PECMD.EXE
3	10/30/2021 20:21	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\CMD.EXE
4	10/30/2021 20:21	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\CONHOST.EXE
5	10/30/2021 20:21	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\NOTEPAD.EXE
6	10/30/2021 20:20	\VOLUME{01d4207de1e70a8f-58e49381}\USERS\[redacted]\APPDATA\LOCAL\MICROSOFT\ONEDRIVE\21.196.0921.0007\FILECOAUTH.EXE
7	10/30/2021 20:20	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\SVCHOST.EXE
8	10/30/2021 20:20	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\SVCHOST.EXE
9	10/30/2021 20:20	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\SVCHOST.EXE
10	10/30/2021 20:20	\VOLUME{01d4207de1e70a8f-58e49381}\PROGRAM FILES\MICROSOFT OFFICE\ROOT\OFFICE16\EXCEL.EXE
11	10/30/2021 20:20	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE
12	10/30/2021 20:19	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE
13	10/30/2021 20:19	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE
14	10/30/2021 20:15	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\SNIPPINGTOOL.EXE
15	10/30/2021 20:14	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\BACKGROUNDTASKHOST.EXE
16	10/30/2021 20:14	\VOLUME{01d4207de1e70a8f-58e49381}\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE

	A	B	C	D	E	F	G	H	I	J	K	
	ExecutableName	Size	RunCount	LastRun	PreviousRun0	PreviousRun1	PreviousRun2	PreviousRun3	PreviousRun4	PreviousRun5	PreviousRun6	Directories
	ZOOM.EXE	492350	54	8/26/2021 17:48	8/25/2021 9:56	8/25/2021 9:51	8/25/2021 9:34	8/25/2021 9:31	8/17/2021 9:22	8/17/2021 9:19	8/17/2021 9:17	\VOLUME{01

ShimCache

What is it?

Allows Windows to track executable files and scripts that may require special compatibility settings to properly run. It is maintained within kernel memory and serialized to the registry **upon system shutdown or restart.**

Forensic Value:

1. The executable or script file names and full paths
2. The standard information last modified date
3. The size of the binary
4. Finally, whether the file actually ran on the system (just browsed through explorer.exe)

Location:

HKLM\SYSTEM\CurrentControlSet\Control\SessionManager\AppCompatCache\AppCompatCache

Tool:

AppCompatCacheParser.exe

	A	B	C	D	E	F	G
	ControlSet	CacheEntryPosition	Path	LastModifiedTimeUTC	Executed	Duplicate	SourceFile
2	1	898	C:\Program Files\Wireshark\extcap\USBPcapCMD.exe	5/22/2020 9:01	NA	FALSE	Live Registry
3	1	637	C:\Users[redacted]\Desktop\HxDSetup.exe	2/28/2020 11:32	NA	FALSE	Live Registry
4	1	634	C:\Program Files\HxD\HxD.exe	2/28/2020 9:25	NA	FALSE	Live Registry
5	1	142	C:\Users[redacted]\DFIR\$J & $LogFile\sqlite3.exe	1/1/2020 23:59	NA	FALSE	Live Registry
6	1	143	C:\Users[redacted]\DFIR\$J & $LogFile\LogFileParser.exe	1/1/2020 23:59	NA	FALSE	Live Registry
7	1	157	C:\Users[redacted]sqlite3.exe	1/1/2020 23:59	NA	FALSE	Live Registry
8	1	160	C:\Users[redacted]LogFileParser.exe	1/1/2020 23:59	NA	FALSE	Live Registry

AmCache

What is it?

The Amcache.hve is a registry hive file stores information related to execution of programs when a user performs certain actions such as running host-based applications, installation of new applications, or running portable applications from external devices.

	A	B	C	D	E	
	ApplicationName	FileKeyLastWriteTim	SHA1	FullPath	Name	ProductName
46	E0469640.LenovoUtility	10/3/2021 2:02	bf4a6a148bc020ababa121c0ead6b139fbfcbc6f	c:\program files\windowsapps\e0469640.lenovo	LenovoUtilityUI.exe	lenovo hotkeys
47	E0469640.LenovoUtility	10/3/2021 2:02	b638cf6f42ee38c8fbad13eece36190ce2748ecb	c:\program files\windowsapps\e0469640.lenovo	utility.exe	lenovo hotkeys
48	E046963F.LenovoCompanion	8/29/2021 13:15	9891831aab7f629fc09232d0551b5fbbf6283f8a	c:\program files\windowsapps\e046963f.lenovo	DeployAssistant.exe	deployassistant
49	E046963F.LenovoCompanion	8/29/2021 13:15	6dc45ea51d7c66599500081ed35c82b999ddc884	c:\program files\windowsapps\e046963f.lenovo	LenovoVantage.exe	lenovovantageuwp
50	DolbyLaboratories.DolbyAudio	2/14/2021 18:52	d5ea2346a435b19b1e04098fc86a1f7589053341	c:\program files\windowsapps\dolbylaboratories.	DAXUIDolbyAudio.exe	daxuidolbyaudio
51	Directory Snoop 5.11 (Trial Version)	8/20/2021 18:40	f4b830bd4c0430b05ea9479b25c32b2968eca470	c:\program files (x86)\briggs softworks\directory	DS_FAT.exe	
52	Directory Snoop 5.11 (Trial Version)	8/20/2021 18:40	93e80a42873a173ba22f944577bea4c3c46eacd8	c:\program files (x86)\briggs softworks\directory	DS_NTFS.exe	
53	Directory Snoop 5.11 (Trial Version)	8/20/2021 18:40	bb7cb0c41f726fccb418ff95fc5a07823d28b6c4	c:\program files (x86)\briggs softworks\directory	elrawdsk32.sys	rawdisk
54	Directory Snoop 5.11 (Trial Version)	8/20/2021 18:40	d2c4fa05eb56d98acf5e08f0b2cbbcddeaf1c401	c:\program files (x86)\briggs softworks\directory	elrawdsk64.sys	rawdisk
55	Directory Snoop 5.11 (Trial Version)	8/20/2021 18:40	08efa016657536d20844c550773b7b1a8568d1ad	c:\program files (x86)\briggs softworks\directory	elrawdski64.sys	rawdisk
56	Directory Snoop 5.11 (Trial Version)	8/20/2021 18:40	e78b47322c26265de7206d2f23c07dd97c989c2f	c:\program files (x86)\briggs softworks\directory	unins000.exe	
57	Digital Detective DCode v5.5	10/11/2021 15:02	32b7326cf6d99f15823dd86289a26076b0f7182f	c:\program files (x86)\digital detective\dcode v5\	unins000.exe	dcode
58	Digital Detective DCode v5.5	10/11/2021 15:02	a2a8758a196722c15d8beff7ec73d72944bcf959	c:\program files (x86)\digital detective\dcode v5\	DCode.exe	dcode
59	Autopsy	10/6/2021 7:34	afb7f7d1c52d3cc5a222d9b2e388c6bf4ef5c11a	c:\program files\autopsy-4.6.0\harness\launchers	app.exe	
60	Autopsy	10/6/2021 7:34	62b10c0f74461cc77addf13064b8fddf0b85902c	c:\program files\autopsy-4.6.0\harness\launchers	app64.exe	
61	Autopsy	10/6/2021 7:34	e1363c24efc0a3ef242ae7e47cfc37c559ef9cdf	c:\program files\autopsy-4.6.0\autopsy\photorec	fidentify_win.exe	
62	Autopsy	10/6/2021 7:34	c5e13c67ed1f65b8329b570dfd390f78837fcad6	c:\program files\autopsy-4.6.0\gstreamer\bin\gst	gst-inspect.exe	
63	Autopsy	10/6/2021 7:34	a1489868b5a35ba18940b91b54a29e1a2259bdb9	c:\program files\autopsy-4.6.0\gstreamer\bin\gst	gst-launch.exe	
64	Autopsy	10/6/2021 7:34	7995c588f4985c5602db6d676e0ad4d80adddc7f	c:\program files\autopsy-4.6.0\gstreamer\bin\gst	gst-player.exe	
65	AccessData FTK Imager	8/29/2021 13:15	436a1d28aa0fd5a23d8a955d6c9eecf6c6d3e5fe	c:\program files (x86)\accessdata\ftk imager\ade	adencrypt_gui.exe	adencrypt exe

Forensic Value:

1. The executable names and full paths
2. Last executed time
3. The size of the binary and its version
4. The executable hash (SHA1)

Location:

C:\Windows\appcompat\Programs\Amcache.hve

Tool:

AmcacheParser.exe , RegRipper (rr.exe)

```
Hive (Amcache.hve) is dirty.
If you need to process hive transasction logs, please consider using yarp + registryFlush.py
(Maxim Suhanov) or rla.exe (Eric Zimmerman).

amcache v.20200515
(amcache) Parse AmCache.hve file

***InventoryApplicationFile***

c:\users[redacted]\amcacheparser.exe  LastWrite: 2021-09-25 01:11:11Z
```

System Resource Usage Monitor (SRUM)

What is it?

SRUM is considered a gold mine of forensic information, as it contains all the activities that occur on a particular Windows system. SRUM tracks and records program executions, power consumption, network activities, and much more information that can be retrieved even if the source has been deleted.

Forensic Value:

1. Program executions
2. Power consumption
3. Network activities
4. Bytes Received & Sent

Location:

C:\Windows\System32\sru\SRUDB.dat

Tool:

SrumECmd.exe

	A	B	C	D
	Timestamp	ExeInfo	BytesReceiv	BytesSen
3	10/5/2021 1:16	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	1765826	528180
5	10/5/2021 0:13	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	41117327	1029971
3	10/2/2021 7:22	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	1717790	437444
4	10/2/2021 5:59	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	10948	9960
5	10/2/2021 5:36	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	3744	3648
9	10/2/2021 5:32	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	25092	5728
6	10/2/2021 5:27	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	267854	16224
3	10/2/2021 5:26	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	1007792	97860
3	9/27/2021 1:27	\device\harddiskvolume3\users\[redacted]\appdata\local\whatsapp\app-2.2134.10\whatsapp.exe	892605	42818

MFT

What is it?

A master file table is a database in which information about every file and directory on an NT File System (NTFS) volume is kept. An MFT will have a minimum one record for every file and directory on the NTFS logical volume. Moreover, each record contains attributes that tell the operating system how to handle the file or directory associated with the record.

Forensic Value:

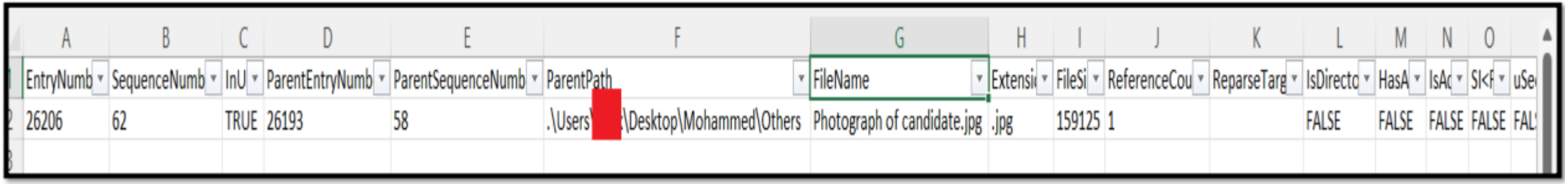
1. Timeline Analysis
2. Information about a file or directory
3. File Type, Size
4. Date/Time when created, modified and accessed

Location:

NTFS/root/$MFT (Extracted from FTK)

Tool:

MFTECmd.exe , MFTExplorer.exe



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
1	EntryNumb	SequenceNumb	InU	ParentEntryNumb	ParentSequenceNumb	ParentPath	FileName	Extensi	FileSi	ReferenceCou	ReparseTarg	IsDirecto	HasA	IsAc	SI<F	uSe
2	26206	62	TRUE	26193	58	.\Users[redacted]\Desktop\Mohammed\Others	Photograph of candidate.jpg	.jpg	159125	1		FALSE	FALSE	FALSE	FALSE	FAL
3																

Windows 10 Timeline

What is it?

Windows 10 Timeline info covering user activities is stored in the 'ActivitiesCache.db' file with the following path. The 'ActivitiesCache.db' file is an SQLite database. **StartTime** means the moment when an application was launched. **EndTime** means the moment when an application ceases to be used. **ExpirationTime** means the moment when the storage duration for a record covering a user activity expires in the database. **LastModifiedTime** means the moment when a record covering a PC user activity has been last modified (if such an activity has been repeated several times.

Forensic Value:

1. Timeline Analysis
2. Information about an application and file
3. Date/Time when started, created, modified and accessed

Location:

%USERPROFILE%\AppData\Local\ConnectedDevicesPlatform\<Profile ID>\ActivitiesCache.db

Tool:

WxTCmd.exe

	A	B	C	D	E	F	G	H
1	Executable	DisplayText	StartTime	LastModifiedTin	LastModifiedTimeOnClie	CreatedTime	ExpirationTime	OperationExpirationTim
2	System32\notepad.exe	File Carving_FROM_DISK.txt (Notepad)	9/29/2021 20:40	9/29/2021 20:40	10/16/2021 1:57	9/29/2021 20:40	11/15/2021 1:57	11/15/2021 1:57
3	Program Files x86\AccessData\FTK Imager\FTK Imager.exe	FTK Imager	10/2/2021 23:11	10/2/2021 23:11	10/27/2021 18:01	10/2/2021 23:11	11/26/2021 18:01	11/26/2021 18:01
4	System32\notepad.exe	test.txt (Notepad)	10/2/2021 23:32	10/2/2021 23:32	10/18/2021 14:10	10/2/2021 23:32	11/17/2021 14:10	11/17/2021 14:10
5	Program Files X64\Autopsy-4.6.0\bin\autopsy64.exe	Autopsy 4.6.0	10/5/2021 7:31	10/5/2021 7:31	10/27/2021 17:59	10/5/2021 7:31	11/26/2021 17:59	11/26/2021 17:59

$ J

What is it?

The $J data stream contains the contents of the change journal and includes information such as the date and time of the change, the reason for the change, the MFT entry, the MFT parent entry and others. This information can be useful for an investigation, for example, in a scenario where the attacker is deleting files and directories while he moves inside an organization in order to hide his tracks.

Forensic Value:

1. Timeline Analysis
2. File Activity Analysis (Open, Close and Update)
3. Evidence of renamed and deleted files

Location:

NTFS/root/$Extend/$RmMetadata/$UsnJrnl/$J
(Extracted from FTK)

Tool:

MFTECmd.exe

Name	Extension	EntryNumber	SequenceNumber	ParentEntryNumber	ParentSequenceNumber	UpdateSequenceNumber	UpdateTimestamp	UpdateReasons	FileAttributes	OffsetToData	SourceFile
ALHUMAID_TEST.txt	.txt	15321	214	21249	17	12297437784	10/27/2021 19:55:05.2	RenameNewName	Archive	3707503192	$J
ALHUMAID_TEST.txt	.txt	15321	214	21249	17	12297437880	10/27/2021 19:55:05.2	RenameNewName|Close	Archive	3707503288	$J
ALHUMAID_TEST.txt	.txt	15321	214	21249	17	12297438264	10/27/2021 19:55:05.3	ObjectIdChange	Archive	3707503672	$J
ALHUMAID_TEST.txt	.txt	15321	214	21249	17	12297438360	10/27/2021 19:55:05.3	ObjectIdChange|Close	Archive	3707503768	$J
ALHUMAID_TEST.txt	.txt	15321	214	21249	17	12297441088	10/27/2021 19:55:08.8	DataExtend	Archive	3707506496	$J
ALHUMAID_TEST.txt	.txt	15321	214	21249	17	12297441184	10/27/2021 19:55:08.8	DataExtend|Close	Archive	3707506592	$J
ALHUMAID_TEST.txt	.txt	15321	214	21249	17	12297442816	10/27/2021 19:56:19.3	RenameOldName	Archive	3707508224	$J
ALHUMAID_CHANGE.txt	.txt	15321	214	21249	17	12297442912	10/27/2021 19:56:19.3	RenameNewName	Archive	3707508320	$J
ALHUMAID_CHANGE.txt	.txt	15321	214	21249	17	12297443008	10/27/2021 19:56:19.3	RenameNewName|Close	Archive	3707508416	$J
ALHUMAID_CHANGE.txt	.txt	15321	214	21249	17	12297443944	10/27/2021 19:56:22.6	RenameOldName	Archive	3707509352	$J

$ Log file

What is it?

This file is stored in the MFT entry number 2 and every time there is a change in the NTFS Metadata, there is a transaction recorded in the $LogFile. These transactions are recorded to be possible to redo or undo file system operations. Why would $LogFile be important for investigation? Because the $LogFile keeps record of all operations that occurred in the NTFS volume such as file creation, deletion, renaming, copy.

Forensic Value:

1. Timeline Analysis
2. File Activity Analysis (Open, Close and Update)
3. Evidence of renamed and deleted files

Location:

NTFS/root/$LogFile (Extracted from FTK)

Tool:

NTFS_Log_Tracker.exe , LogFileParser.exe

LSN	EventTime(UTC+3)	Event	Detail	File/Directory Name	Redo	Target VCN	Cluster Index
58571421012	12/23/2021 03:12:18.0	Renaming File	New Text Document.txt -> Alhumaid_Test.txt	Alhumaid_Test.txt	Create Attribute	0x3B3E	4
58571423061	12/23/2021 03:12:18.0	File Creation		Alhumaid_Test.txt.lnk	Initialize File Record Segment	0x640	0
58571423281		Writing Content of Resident File	Writing Size : 584	Alhumaid_Test.txt.lnk	Update Resident Value	0x640	0
58571430272	12/23/2021 03:12:36.0	Renaming File	Alhumaid_Test.txt -> Alhumaid_Renamed.txt	Alhumaid_Renamed.txt	Create Attribute	0x3B3E	4
58571432968	12/23/2021 03:12:38.0	File Creation		Alhumaid_Renamed.txt.lnk	Initialize File Record Segment	0x39A9	0
58571433257		Writing Content of Non-Resident File	Data Runs(in Volume) : 10769738(1)	Alhumaid_Renamed.txt.lnk	Update Mapping Pairs	0x39A9	0
58571438672		Move(Before)		Alhumaid_Renamed.txt	Delete Attribute	0x3B3E	4

Link file-Shortcut (.lnk)

What is it?

A shortcut file is a small file which has information used to access or point to another file. Windows operating system automatically creates LNK files when a user opens a non-executable file or document. Windows creates these LNK files on a frequent basis and their creation is performed in the background without the explicit knowledge of the user. Shortcut files are most often referred to Link files by forensic analysts based on their .lnk file extension.

Forensic Value:

1. The path and size of target file
2. Timestamps for both the target file and LNK file
3. The attributes associated with the target file (i.e. read-only, hidden, archive, etc.)
4. The system name, volume name, volume serial number, and sometimes the MAC address of the system where the target is stored
5. Files opened from a specific removable USB device
6. Identification of files which no longer exist on a local machine

Location:

%USERPROFILE%\Recent

%USERPROFILE%\Application Data\Microsoft\Office\Recent

Tool:

LECmd.exe

User Assist

What is it?

UserAssist tracks every **GUI-based** programs launched are recorded in this registry key. This key contains two GUID subkeys (**CEBFF5CD** Executable File Execution, **F4E57C4B** Shortcut File Execution), each subkey maintains a list of system objects such as program, shortcut, and control panel applets that a user has accessed. Registry values under these subkeys are weakly encrypted using **ROT-13** algorithm which basically substitutes a character with another character 13 position away from it in the ASCII table.

Forensic Value:

1. The executed GUI program name
2. The executed GUI program path
3. Last executed time
4. Run count

Location:

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count

Tool:

RegRipper (rr.exe) , RegistryExplorer.exe

```
----------------------------------------
UserAssist
Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist
LastWrite Time 2021-02-09 20:21:57Z

2022-01-01 00:18:10Z
  {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\notepad.exe (180)
2022-01-01 00:09:14Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\AccessData\FTK Imager\FTK Imager.exe (11)
2021-12-31 23:56:11Z
  {6D809377-6AF0-444B-8957-A3773F02200E}\Adobe\Acrobat DC\Acrobat\Acrobat.exe (15)
2021-12-30 01:50:23Z
  C:\Users\Desktop\testdisk-7.2-WIP\photorec_win.exe (1)
```

Values | UserAssist

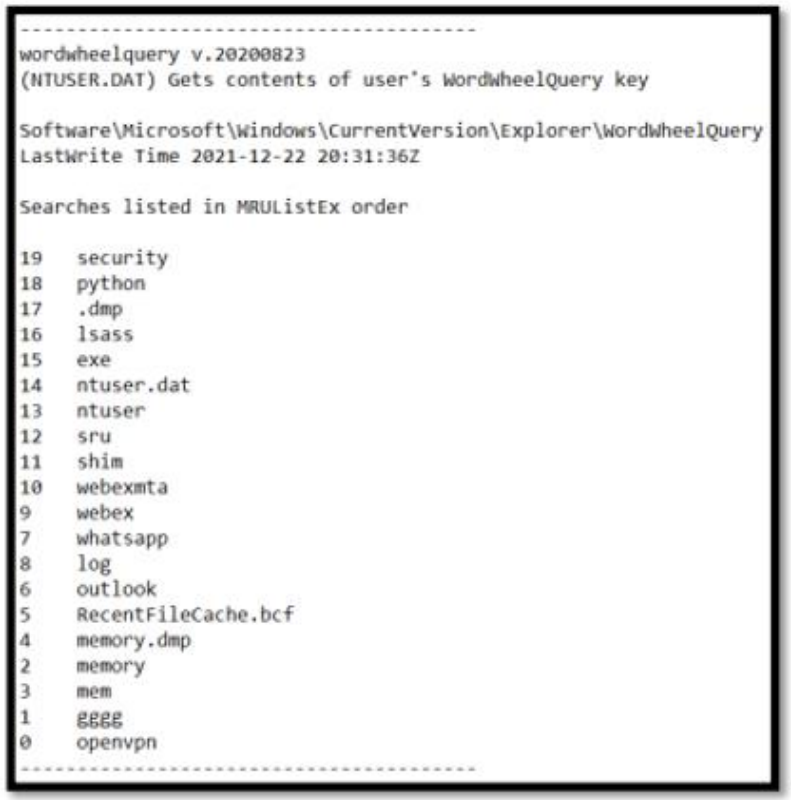
Drag a column header here to group by that column | system32 | Find

Program Name	Run Counter	Focus Count	Focus Time	Last Executed
{System32}\notepad.exe	180	391	0d, 2h, 19m, 10s	2022-01-01 00:18:10
{System32}\WindowsPowerShell\v1.0\powershell.exe	25	157	0d, 1h, 05m, 02s	2021-12-30 00:51:32
{System32}\cmd.exe	19	209	0d, 1h, 33m, 04s	2021-12-29 22:59:40
{System32}\SnippingTool.exe	16	55	0d, 0h, 14m, 40s	2021-12-30 01:03:28
{System32}\mspaint.exe	12	21	0d, 0h, 14m, 47s	2021-12-30 01:03:41
{System32}\mmc.exe	4	0	0d, 0h, 00m, 00s	2021-12-14 21:54:54
{System32}\eventvwr.exe	2	0	0d, 0h, 00m, 00s	2021-12-14 20:51:24
{System32}\Fondue.exe	0	2	0d, 0h, 00m, 15s	

Word Wheel Query

What is it?

WordWheelQuery is a registry key that stores keywords searched from the folder search menu bar. Keywords are added in Unicode and listed in temporal order in an MRUlist.



```
----------------------------------------
wordwheelquery v.20200823
(NTUSER.DAT) Gets contents of user's WordWheelQuery key

Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery
LastWrite Time 2021-12-22 20:31:36Z

Searches listed in MRUListEx order

19   security
18   python
17   .dmp
16   lsass
15   exe
14   ntuser.dat
13   ntuser
12   sru
11   shim
10   webexmta
9    webex
7    whatsapp
8    log
6    outlook
5    RecentFileCache.bcf
4    memory.dmp
2    memory
3    mem
1    gggg
0    openvpn
----------------------------------------
```

Forensic Value:

1. User Activity
2. Last folder search conducted (Last Write Time)
3. Keywords searched

Location:

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

=

NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

Tool:

RegRipper (rr.exe) , RegistryExplorer.exe

NTUSER.DAT

What is it?

It's hidden file in every user profile and contains the settings and preferences for each user. Windows accomplishes this by first storing that information to the Registry in the **HKEY_CURRENT_USER** hive. Then when user sign out or shut down, Windows saves that information to the **NTUSER.DAT** file. The next time user sign in, Windows will load NTUSER.DAT to memory, and all preferences load to the Registry again.

Forensic Value:

1. Collecting registry hive (HKEY_CURRENT_USER) through its supporting file (NTUSER.DAT)
2. Forensicate user activity, setting via registry hive
3. Forensic artifacts (Recent Docs, Typed URLs, UserAssist, Recent Apps, Run and Run Once, ComDig32 Subkey, Typed Paths Subkey, Microsoft Office applications and the MRU subkey, RunMRU, Windows search function and the WordWheelQuery)

Location:

C:\Users\<username>\NTUSER.DAT

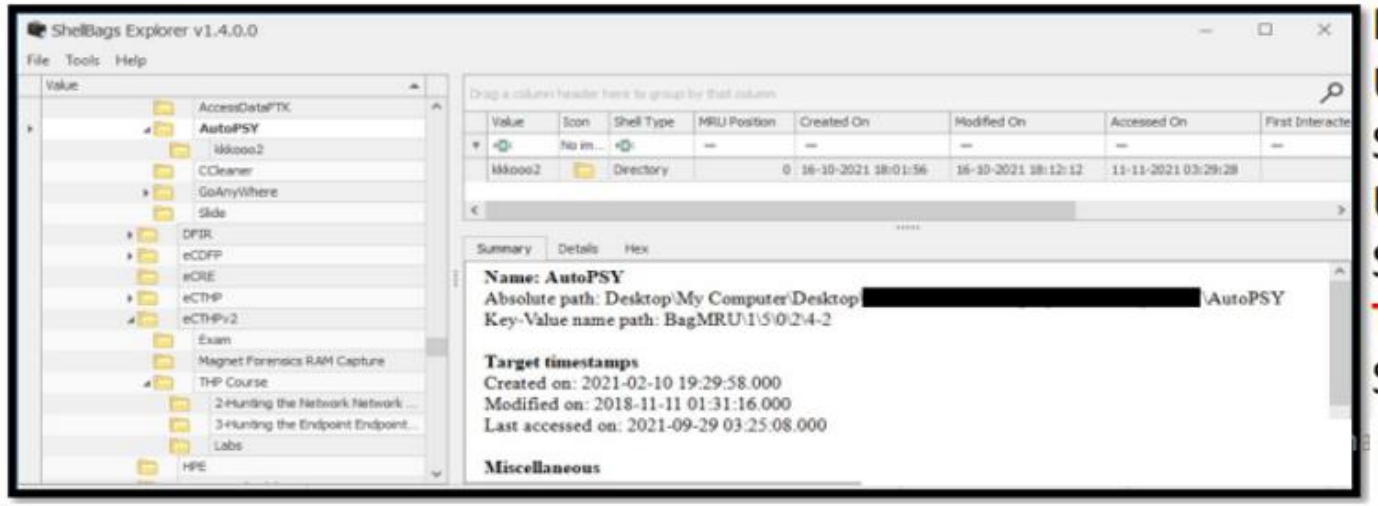
Tool:

RegRipper (rr.exe) , RECmd.exe , RegistryExplorer.exe

ShellBags

What is it?

Windows tracks and records user's view settings and preferences while exploring folders. These view settings (size, view mode, position) of a folder window are stored in ShellBags registry keys. ShellBags keep track of the view settings of a folder window once the folder has been viewed through Windows Explorer. ShellBags does not only track the view settings of a folder on the local machine, but also on removable devices and network folders.



Forensic Value:

1. User's navigation activity on the system
2. Timestamps analysis
3. Deleted folders
4. Folders accessed within local machine
5. Folders accessed from removable devices
6. Folders accessed from network folders

Location:

NTUSER.DAT\Software\Microsoft\Windows\Shell\BagMRU

NTUSER.DAT\Software\Microsoft\Windows\Shell\Bags

USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags

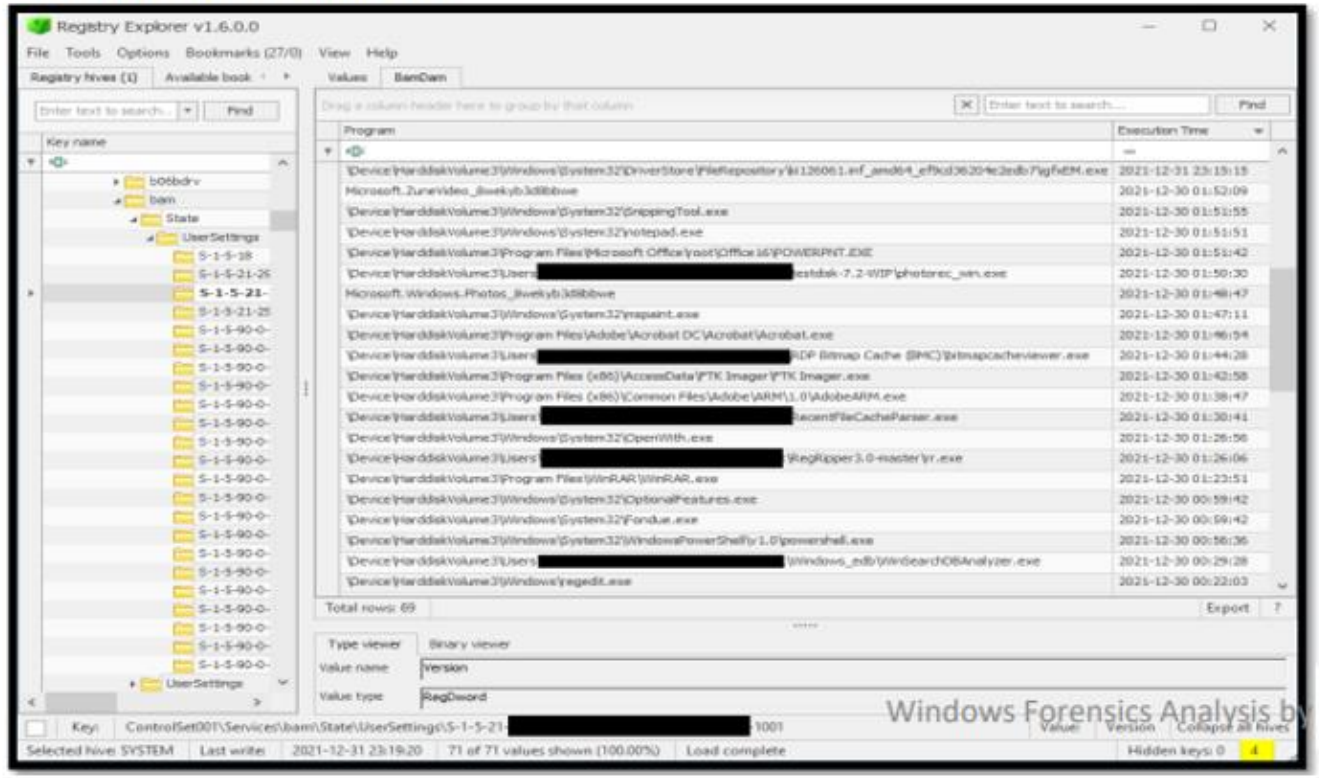
Tool:

SBECmd.exe , ShellBagsExplorer.exe , sbag64.exe

Background Activity Monitor (BAM)/DAM

What is it?

BAM is a Windows service that controls activity of background applications. The BAM entries are updated when **Windows boots**. Also, there is dam\UserSettings Desktop Activity Monitor (DAM) and stores similar information to BAM.



Forensic Value:

1. Evidence of execution
2. The executable's name
3. The absolute path to the executable
4. The last time the application ran

Location:

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet*\Service
bam\State\UserSettings\<SID>

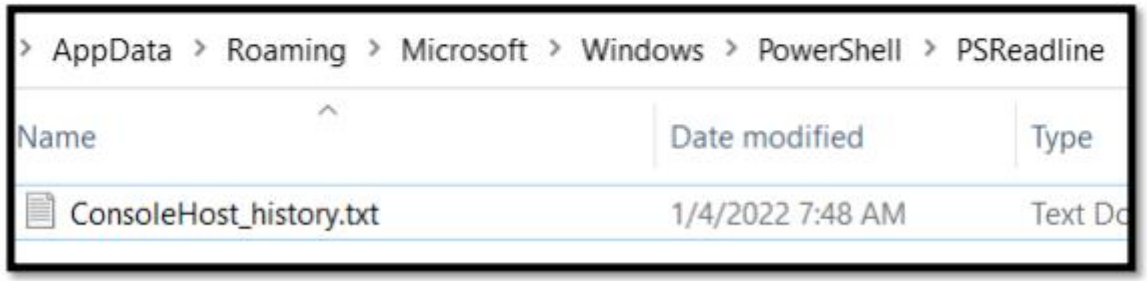
Tool:

RegistryExplorer.exe , BamParser.py

Power shell

What is it?

PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell in Windows 10 saves the last 4096 commands that are stored in a plain text file located in the profile of each user.



Forensic Value:

1. Evidence of PowerShell commands executed by the user

Location:

C:\Users\<username>\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt

Tool:

notepad.exe

WINDOWS Password Storage

- User and passwords in a window system are stored in either of two places:
  1. SAM (Security Account Manager)
  2. AD (Activity directory) SAM

1. **Security Account Manager (SAM)** is a database file in Windows XP, Windows Vista and Windows 7 that stores users' passwords. It can be used to authenticate local and remote users.

2. **Active Directory** is used to authenticate remote users. SAM uses cryptographic measures to prevent forbidden users to gain access to the system.

- The user passwords are stored in a hashed format in a registry hive. This file can be found in **%SystemRoot%/system32/config/SAM**

FIND it now?

Applications Password Cracking

- **Password cracker** is a program that can assist users to obtain unauthorized access to an application or resources.

- Can also help users to retrieve lost or forgotten passwords of any application.

- **Password cracking methods**
  - Brute force method
  - Dictionary searches
  - Rule based attack
  - Password guessing
  - Rainbow attack

Applications Password Cracking

- **Brute force attack**
  - Works by calculating every possible combination that could make up a password and testing it to see if it is the correct password.
  - As the password's length increases, the amount of time, on average, to find the correct password increases exponentially.
  - Short passwords can usually be discovered quite quickly, but longer passwords may take decades.
- **Dictionary attack**
  - a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary.
  - is based on trying all the strings in a pre-arranged listing, typically derived from a list of words such as in a dictionary (hence the phrase dictionary attack).
- **Rule based attack**
  - The attackers has many/ some preoccupied information using which the set of rules can be formed and then the possible searches can be narrowed down to a great extent. This type of attack is the most powerful one.

Applications Password Cracking

- **Hybrid attack and password guessing**
  - It is also based on dictionary attack. In this if the old password is known than concatenating it with other symbols can yield the right password. In case of guessing the common passwords that are mostly used by novice users are used to crack codes.
- **Rainbow attack**
  - Any computer system that requires password authentication must contain a database of passwords, either hashed or in plaintext, and various methods of password storage exist. Tables are vulnerable to theft, storing the plaintext password is dangerous. Most databases store cryptographic hash of a user's password in the database.
  - Rainbow tables are one tool is a Precomputed table for reversing cryptographic hash functions , usually for cracking password hashes.
  - Tables are usually used in recovering a Password (or credit card numbers, etc.) up to a certain length consisting of a limited set of characters.

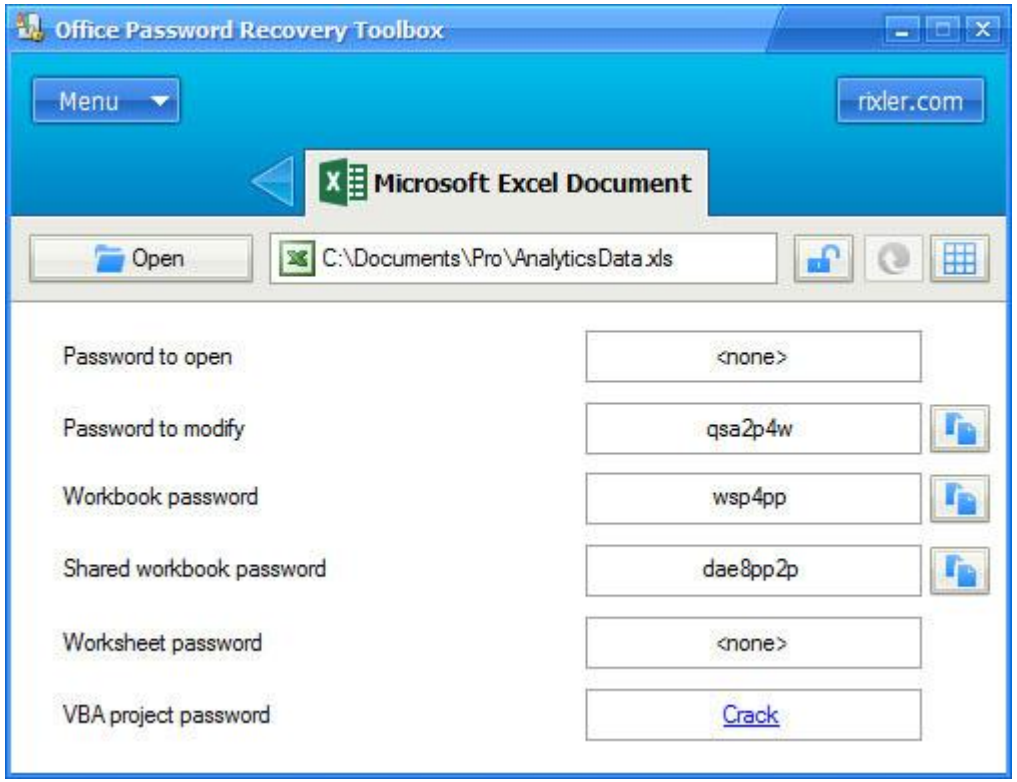
Applications Password Cracking

Brute-force attacks and dictionary attacks are the simplest methods available;

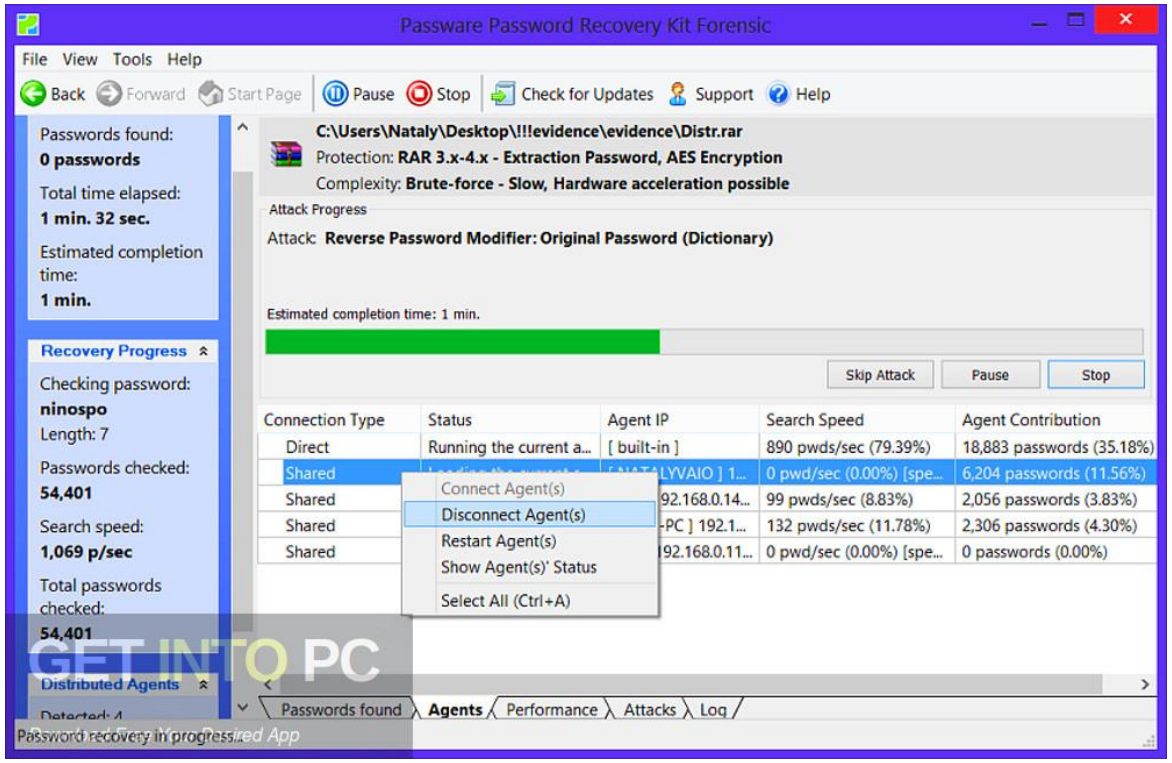
however these are not adequate for systems that use large passwords.

Password Recovery Tools

Office Password Recovery Toolbox is software which recovers lost password to any Microsoft Office document effectively.



Passware Kit Enterprise and Forensics can recover the password of up to 150 different file types.



Others OSs Forensics

Linux Forensics

- Linux is an open source, Unix-like, and elegantly designed operating system that is compatible with personal computers, supercomputers, servers, mobile devices, netbooks, and laptops.
- Unlike other OSs, Linux holds many file systems of the ext family, including ext2, ext3, and ext4.
- Linux can provide an empirical evidence if the Linux-embedded machine is recovered from a crime scene.
- Following folders and directories will be of interest for investigators:
  - **/etc [%SystemRoot%/System32/config]:** This contains system configurations directory that holds separate configuration files for each application.
  - **/var/log:** This directory contains application logs and security logs. They are kept for 4-5 weeks.
  - **/home/$USER:** This directory holds user data and configuration information.
  - **/etc/passwd:** This directory has user account information.

Linux Forensics

- Forensic specialists use a forensic toolkit to collect evidence from a Linux Operating System.
- The toolkit comprises many tools such as Dmesg, Insmod, NetstatArproute, Hunter.O, DateCat, P-cat, and NC

Command	Description
/mnt/cdrom/cat /proc/version	Operating system version
/mnt/cdrom/cat /proc/sys/kernel/name	Host name
/mnt/cdrom/cat /proc/sys/kernel/domainame	Domain name
/mnt/cdrom/cat /proc/cpuinfo	Information about hardware
/mnt/cdrom/cat /proc/swaps	All swap partitions
mnt/cdrom/cat /proc/partitions	All local file systems
/mnt/cdrom/cat /proc/self/mounts	Mounted file systems
mnt/cdrom/cat /proc/uptime	Uptime

Table 1 - An investigator can use these commands to collect information

Linux Forensics

- Helix is the distributor of the **Knoppix Live Linux CD**. It provides access to a Linux kernel, hardware detections, and many other applications.

Mac OS X Forensics

- Mac OS X is the **UNIX-based** operating system that contains a Mach 3 microkernel and a FreeBSD-based subsystem.
- Its user interface is Apple-like, whereas the underlying architecture is UNIX-like.
- Mac OS X offers a novel technique to create a forensic duplicate.
- To do so, the perpetrator's computer should be placed into a "Target Disk Mode".
- Using this mode, the forensic examiner creates a forensic duplicate of perpetrator's hard disk with the help of a Firewire cable connection between the two PCs.

Apple iOS Forensics

- Apple iOS is the UNIX-based operating system first released in 2007.
- It is a universal OS for all of Apple's mobile devices, such as iPhone, iPod Touch, and iPad.
- An iOS embedded device retrieved from a crime scene can be a rich source of empirical evidence.

Android Forensics

- Android is a **Google's open-source platform** designed for mobile devices.
- Widely used as the mobile operating system in the handsets industry.
- Android OS runs on a Linux-based kernel which supports core functions, such as power management, network infrastructure, and device drivers.
- **Android's Software Development Kit (SDK)** contains a very significant tool for generic and forensic purposes, namely Android Debug Bridge (ADB).
- ADB employs a USB connection between a computer and a mobile device.

Assignment 2

Explore the assigned topic in detail, 2) Perform hands-on activities as briefed in this lecture (Keep screenshots), and 3) Prepare a short report explaining the topic and results of your activities/findings i.e. screenshots (15-20 pages) and submit on GCR by 27th March, 2025.

- Group A--Apple iOS Forensics-
- Group B--Linux Kali Forensics
- Group C--Unix Forensics
- Group D--Mac OS X Forensics
- Group E--Android Forensics
- Group F—Windows Server
- Group G--Embedded and IoT OS
- Group H– Linux Ubuntu Forensics

Quiz Announcements

Quiz 2

25th March 2025

Lecture 4 and 5

Quiz 3

8th April (After Eid Holidays)

EC Council Modules 1, 2 3 and 4

Home Tasks/ References

- Chapter 5, Textbook

- Complete this course from Coursera: Windows OS Forensics

  https://www.coursera.org/learn/windows-os-forensics

- https://www.geeksforgeeks.org/windows-forensic-analysis/

- https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-operating-system-forensics/

- https://www.linkedin.com/learning/operating-system-forensics-24652677/operating-system-forensics

ANY QUESTIONS