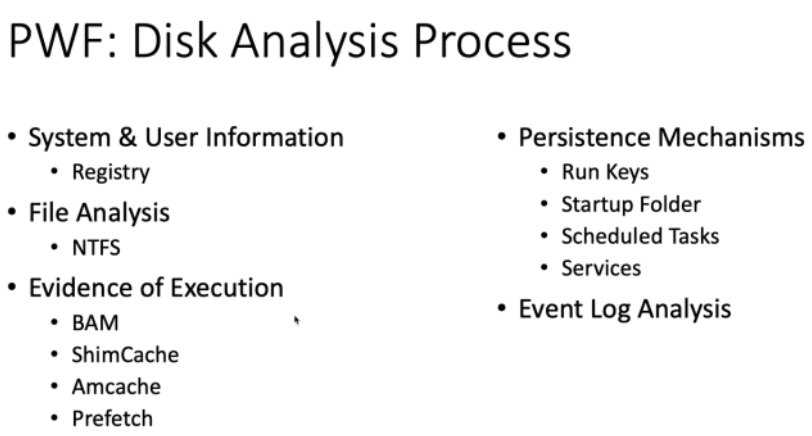
Artifacts Cheat Sheet - By Roey Bartov

Friday, January 12, 2024 8:56 PM



Path 1: System & User Information

First, we will look into some of the system and user information to learn more about what system version and what we find out about it in order to understand what can we even be looking for.
That kind of information is mostly stored in the Regsitry.

- The Windows Registry is a hierarchical database that stores configuration settings and options for the operating system, hardware devices, installed software, and user preferences.

A list of the registry keys which related to system information:

- **Computer name:** HKLM\System\CurrentControlSet\Control\Computername\ComputerName
- **Windows Version:** HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
- **Time Zone:** HKLM\System\CurrentControlSet\Control\TimeZoneInformation
- **Network Information:** HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces{interface-name}
- **Shutdown Time:** HKLM\System\ControlSet001\Control\Windows\ShutdownTime
- **Defender Settings:** HKLM\SOFTWARE\Microsoft\Windows Defender
- **Network Shares:** SYSTEM\CurrentControlSet\services\LanmanServer\Shares
- **USB Connections:** HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
  HKLM\SYSTEM\CurrentControlSet\Enum\USB
- **Mount Devices:** HKLM\System\MountedDevices

A list of registry keys which related to user information:

- **Users, Groups, Login Information and Password Policies:** SAM\Domains\Account\Users
- **Users Profiles (Only Exist For Users Who Logged in Interactively):** SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

User Behavior Analysis:

- **UsserAssist (Applications Opened, Only From GUI):**
  NTUSER\Software\Microsoft\Windows\CurrectVersion\Explorer\UserAssist

- Subkey: **A List Of Applications, Files, Links That Have Been Accessed** - {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
- Subkey: **Lists The Shortcut Links Used To Start Programs -** {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}

✓ UserAssist is a key in a part of the Registry that contains a record of programs frequently executed by a user.

- **RecentDocs (Recently Used Applications):**
  NTUSER.DAT\Software\Microsoft\Windows\CurrectVersion\Explorer\RecentDocs

- Physically: "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent"

- **JumpLists (Historic Activity):**

- **Automatic destinations:**
  C:\%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations

- **Custom Destinations:**
  C:\%UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations

✓ Jumplists feature is designed to provide the user with quick access to recently accessed application files and common tasks.

- **Shellbags (Locations Browsed By The User, Don't Get Confused With Shell Referring To CLI)**

- **NTUSER.DAT:**
  HKCU\Software\Microsoft\Windows\Shell\BagMRU
  HKCU\Software\Microsoft\Windows\Shell\Bags

- **USRCLASS.DAT:**
  Local Settings\Software\Microsoft\Windows\Shell\BagMRU
  \Software\Classes\Local Settings\Software\Microsoft\Windows\Shell\Bags

✓ Shellbags are artifacts that are created when a user interacts with the shell.

- **Dialogue Boxes MRU (Most Recently Used Dialog Boxes):**

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU

✓ This artifact records the paths and files that have been accessed or selected through common dialog boxes

- Physically: "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Recent\ComDlg32"

- **MUICache (Multilingual User Interface Cache):**
  NTUSER.DAT\Software\Microsoft\Windows\ShellNoRoam\MUICache

✓ This artifact stores information about the applications that have been run on the system, including the executable paths and localized names.

- **Windows TypedPaths (Paths Manually Entered):**
  NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

✓ TypedPaths records the paths that a user has manually typed into the Windows Explorer address bar.

- **Search Keywords (Search Terms Entered):**
  NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\WordWheelQuery

✓ Search Keywords stores the search terms entered by the user in the Windows search box.

- **Remote Desktop Connection Artifacts (Connections):**
  NTUSER.DAT\Software\Microsoft\Terminal Server Client

- **PowerShell History (CLI History):**
  C:\Users\%USER%\AppData\Microsoft\Windows\PowerShell\PSReadLine

- **Browsing History (Chrome/Edge,etc):**
  C:\Users\%USER%\AppData\Local\Roamning\Google\Chrome\User Data\Default\History

- **Cookies (These gives us information about the past web sessions, domain names, etc):**
  C:\Users\%USER%\AppData\Local\Google\Chrome\User Data\Default\Network\Cookies

- **Favicons (The Domain Name Of The Website Is Recorded Also If The History Deleted):**
  C:\Users\%USER%\AppData\Local\Google\Chrome\User Data\Default\Favicons

- **Form History (Can Provide Information About The Text That a User Has Entered Web Forms.):**
  C:\Users\%USER%\AppData\Local\Google\Chrome\User Data\Default\Web Data

- **Extensions (Extensions Can Be Malicious Either From a Shady Third-Party Vendor):**
  C:\Users\%USER%\AppData\Local\Google\Chrome\User Data\Default\Extensions\{randomfoldername}*

- **Outlook Mailbox (OST File To See The User Inbox):**
  C:\Users\%USER%\Desktop\wb-ws-01\C\Users\ash.williams\AppData\Local\Microsoft\Outlook

Path 2: File Analysis (NTFS)

- **Master File Table ($MFT):**

The Master File Table (MFT) is the most important file for a forensic investigator, because any file that is being created, written, stored, modified, or deleted on the file system
All information about a file, including its size, time and date stamps, permissions, and data content, is stored either in MFT entries.
MFT also stores the metadata even if the file itself has been deleted.

- MFT can also be a good source for finding malicious URLs/domains that the files were downloaded from.
  It stores information known as **Zone.Identifier** stream which contains the URL that the files were downloaded from

- A file is smaller in size, like lower than 1kb in size, **it will be stored inside the MFT itself meaning we can get contents of that file from MFT.**
  These are called MFT resident files.

- **USN Journal ($J):**

USN Journal is feature of the Windows NT file system (NTFS) which maintains a record of changes made to the volume.
It basically keeps track of all the operations (like renaming, unarchive, deletion, creation, move etc.) that occur to files on the file system.
This file allows us to see the original file name and the renamed file name and timestamps to when a specific change was made to a file.

- **Windows Notification DB**

The feature provides real-time notifications of a variety of events such as email alerts, applications' updates, security alerts, reminders, and other application specific notifications.
Investigators can retrieve valuable details such as the text or content of the notification that was displayed to the user, the date and time when the notification was received, notification expiration date, and other details.
This feature enables investigators to track and recover events on the user device even if the source has been deleted.

- **Path:** C:\Users\%USER%\AppData\Local\Microsoft\Windows\Notifications\wpndatabase.db

- **SRUM Database**

SRUM tracks 30 to 60 days of system resource usage, particularly application's resource usage, energy usage, Windows push notifications and network connectivity, and data usage.
This artifact tracks and records program executions, power consumption, network activities, and much more information that can be retrieved even if the source has been deleted.

- **Path:** C:\Windows\System32\SRU\SRUDB.dat

- **Recycle Bin Artifacts**

Recycle bin artifacts retain valuable information related to the deleted item such as the name of the deleted item, the original location of the item before deletion, the size of the deleted item and the date and time when the item was deleted.

- **Path:** C:\$Recycle.Bin\{SID}\$I######

- **Search Index**

Windows Search service acts as an internal dictionary running in the background, collecting and indexing the content of the system.
The database contains a large amount of data related to the files, images, videos, directories and other file types found on Windows systems.
In addition, Windows Search database may also collect and index data from other sources such as Microsoft Outlook.
We can get partial contents of different file types like docx, pdf, txt etc, browser history even if the history was deleted from the browser.

- **Path**: C:\%USERPROFILE%\ProgramData\Microsoft\Search\Data\Applications\Windows\Windows.edb

- **Tool:** https://github.com/strozfriedberg/sidr

- **RDP Cache**

When a user connects to another system using RDP, small size (bitmap) images are stored in their RDP profile files, so that once the same image is to be used in the session it can be fetched/pulled quicker.
This artifact can help us sometimes in identifying what the user was seeing in their RDP sessions.

- **Path:** C:\Users\<username>\AppData\Local\Microsoft\Terminal Server Client\Cache\
- **Tool:** https://github.com/BSI-Bund/RdpCacheStitcher.

- **Thumbnail Cache**

When you open Windows Explorer in thumbnail view, the files within the folder are displayed as small images that represent the contents of the files.
Microsoft Windows stores thumbnails of many file types, some of which include JPEG, BMP, GIF, PNG, TIFF, AVI, PDF, PPTX, DOCX, HTML, MP4 etc.
When a user deletes a file, its thumbnail remains in the cached file

- **Path:** C:\Users\[Username]\AppData\Local\Microsoft\Windows\Explorer
- **Tool:** https://thumbcacheviewer.github.io/

Path 3: Evidence Of Execution

- **Background Activity Moderator (BAM)**

BAM is system component that monitors and manages background activities or processes on a computer system.
BAM provides the full path of the executable files that were run on the system as well as the last execution date and time of these files.

- **Path:** HKLM\SYSTEM\ControlSet00X\Services\bam\State\UserSettings\SID\

- **ShimCache (Application Compatibility Cache)**

Provide a record of information about executable files that have been running on the system, it usually keeps information like the name and the path of the file, the timestamp when it is run, and other metadata.
ShimCache can be used by forensic investigators to determine what programs have been running on a system, the exact timestamps of their execution, existence of executables even though they are not executed.

⇒ **Evidence of executable executions**
⇒ **Evidence of executable existence (If viewed from GUI. Listing the file names from CLI will not be populated in this registry key.)**

It is important to note that ShimCache can be modified or deleted by an attacker, so it is important to preserve the integrity of the evidence when examining shimcache.

⇒ **Path:** SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache

- **Amache**

The Amache hive is an artifact found on Windows systems that contains information about the applications and programs that are executed on the system.
From a forensics point of view, **it can be used to determine the programs running on a system and their exact times that they are run.**
It can also be used to identify when software was installed on a system, as well as the location of the installation files.

Amcache hive also stores executed applications data from external devices/sources like network shares, USB devices etc.

- Path: C:\Windows\AppCompat\Programs\Amcache.hve

- **Prefetch**

The purpose of the Prefetch file is to increase the performance of the computer by pre-loading code pages.
Forensic artifact that records information about applications and programs that have been executed on the system.
Windows stores a prefetch file for every single application that executed within the Windows Prefetch folder.

- **Path:** C:\Windows\Prefetch

Path 4: Persistence Mechanisms

- **Windows Run-Keys**

Autorun keys are registry entries in Windows that specify which programs should be automatically started when the system boots up or when a user logs in.
This is the first place to look into as a forensic analyst to see whether an attacker or malicious script might have tried to maintain persistence by adding something into these run keys.

❋ There is user specific run keys, that means only if the user logs into the system Windows would actually run those applications within those run keys.
❋ There is the software run keys, so no matter which user is going to log in, Windows is going to run those applications in any case.

- **Paths:**
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce

- **Startup Folder**

There is a way to place applications or binaries into specific folders, and Windows will automatically execute them during system startup or user logon.
There are two different startup paths, the first one is starts with "Username" and the second one has a similar path but it start with "ProgramData".
That means there are 2 different places, one for the user and one for the system.

- **Paths:**
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

- **Windows Services**

A service in Windows is a type of application that runs in the background and performs essential tasks without requiring user interaction.
By creating or modifying services, they can ensure their malicious code is executed automatically when the system starts or when specific conditions are met.

- **Path:** HKLM\SYSTEM\CurrentControlSet\Services

- **Scheduled Tasks**

A scheduled task in Windows is a task that is set to run automatically at specified times or in response to specific events.
By creating or modifying scheduled tasks, they can ensure their malicious code is executed automatically based on specific triggers, such as system startup, user logon, or at regular intervals.

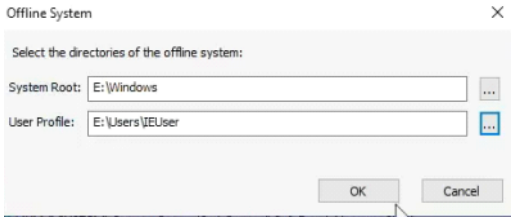
- **Path:**

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks

- **Physically**:
  C:\Windows\System32\Tasks

- **Bonus: Persistence Mechanisms Analysis with Autoruns**

- We can use the section “Offline System” and choose the User & the drive



Path 5: Windows Event Logs

Windows Event Logs are a critical component of the Microsoft Windows operating system that record various system, security, and application events that occur on a computer or server. They offer detailed insights into system activities, user behaviors, errors, warnings, and other significant events that can indicate security incidents.

- **Path:** C:\Windows\System32\winevt\logs

Security Events

Event ID	Event Name	Description
4624	Successful Logon	Indicates that a user has successfully logged on to the system.
4625	Failed Logon	Indicates a failed logon attempt.
4648	A Logon Was Attempted Using Explicit Credentials	Indicates that a user has attempted to log on using another user's credentials.
4672	Special Privileges Assigned To New Logon	Indicates that a session with administrative privileges has been opened.
4720	A User Account Was Created	Indicates a new user account has been created.
4728	A Member Was Added to a Security-Enabled Global Group	Indicates that a user has been added to a high-level security group.
4732	A Member Was Added to a Security-Enabled Local Group	Indicates a user has been added to a local group.
4756	A Member Was Added to a Security-Enabled Universal Group	Indicates that a user has been added to a global group in Active Directory.
1102	The Audit Log Was Cleared	Indicates that security logs have been cleared.
4771	Kerberos Pre-Authentication Failed	Indicates a Kerberos authentication attempt has failed.

System Events

Event ID	Event Name	Description
6008	The previous system shutdown was unexpected	Indicates an unexpected system shutdown.
1074	User-initiated shutdown	Indicates a user-initiated shutdown.
7000	The Service Control Manager encountered an error	Indicates a service could not start.
7001	Service Start Failure	Indicates the system failed to start a service due to a constraint.
7022	Service Hang Report	Indicates that a service is stuck at startup.
7023	Service Control Manager tried to take a corrective action	Indicates that a service is not working as expected and is being fixed.
7026	Boot Start or System Start Driver failed to load	Indicates that a driver failed to load at startup.
7036	Service State Change	Indicates a service state change (start, stop).
7040	Service Start Type Change	Indicates that the startup type of a service changed.
7045	A service was installed in the system	Indicates that a new service has been installed on the system.

Application Events

Event ID	Event Name	Description
1000	Application Error	Indicates that an application has unexpectedly crashed.
1001	Fault Bucket, type 0	Indicates that an error report was generated after an application crashed.
1002	Application Hang	Indicates that an application is unresponsive.
1026	.NET Runtime	Displays critical errors in .NET applications.
1030	Group Policy Error	Indicates errors encountered while applying Group Policy.
11707	Installation Succeeded	Indicates that an application was successfully installed.
11708	Installation Failed	Indicates that an application failed to install.
11724	Product Removal Failed	Indicates that an application failed to uninstall.
1042	Ending a Windows Installer Transaction	Indicates that the Windows Installer process has been terminated.

PowerShell Events

Event ID	Event Name	Description
400	Engine Lifecycle Start	Indicates that the PowerShell engine is running.
403	Engine Lifecycle Stopped	Indicates that the PowerShell engine is stopped.
600	Provider Lifecycle Start	Indicates that a PowerShell provider is in the startup phase.
800	PowerShell Remoting Session Connected	Indicates that a remote PowerShell session is started.
4103	Module Logging	Displays logs of PowerShell module loads and commands.
4104	Script Block Logging	Displays details about the script blocks that were executed. This is critical for the detection of malicious scripts.
4105	Script Block Invocation Start	Indicates the beginning of a script block call.
4106	Script Block Invocation Completed	Displays the completion of a script block call.

Other Essential Log Categories

- **Microsoft-Windows-Sysmon/Operational:**
  Sysmon (System Monitor) provides a detailed record of system activity, including network connections, file creation, and process startup/shutdown.
  It is vital for the detection of malicious activity and stealth attack techniques.

  Microsoft-Windows-WMI-Activity/Operational:
  Windows Management Instrumentation (WMI) activity is utilized to manage and modify configurations.
  Malware and cyber attacks often prefer WMI, so these logs are essential to detect malicious WMI use.

  Microsoft-Windows-TerminalServices-LocalSessionManager/Operational:
  Provides information about remote desktops connected and sessions running.
  It is used to detect unauthorized access attempts or remote logon events.

  Microsoft-Windows-TaskScheduler/Operational:
  Displays Task Scheduler activity, malware and attack tools often utilize Task Scheduler to create malicious tasks.
  These logs can help you detect suspicious tasks and scripts that run automatically.

  Microsoft-Windows-SMBServer/Operational:
  Displays incoming SMB requests and server responses to those requests when the Windows operating system is configured as an SMB server.
  It is critical for detecting potential security threats, such as attempted unauthorized file access, file sharing security breaches, and anomalous network traffic.