Practical Windows Forensics

Experiments and Forensic Artifacts
Windows Registry, Event Logs Analysis
Email Forensics And Practical Examples

PREPARED BY: WALID HADDAD

Prepared by Walid Haddad

v1.0 May | 3 | 2021

Table of Contents

Windows Forensics

In this book, I will be taking a deep dive into some of the forensic artifacts I see in my information security investigations that I find the most useful and the most interesting. I will talk about the things left behind unintentionally that will help an investigator get to the bottom of an incident.
Here are just a few of the artifacts I'll be covering in this book:

Windows Registry keys
Windows Recycle Bin
Link Files
ThumbCache
Shell Bags
Prefetch Files
Amcache Artifacts
Internet Explorer Forensics
Event logs
Mounted USB Devices
Email Header Analysis
Other stuff

Windows Registry

Windows registry is a key component for Microsoft Windows, you can consider it as a database that contains all information that the Operating system and installed applications needs to operate. It contains all the configuration settings for the OS, applications, etc…
These registry artifacts that I will be detailing are not put there by Microsoft for forensic investigations but for different services like helping the applications run quickly, better user experience, storing settings and configurations, etc… Also these artifacts can change from windows to windows versions.

I will be highlighting some of the registry keys which can help investigating an incident and searching for artifacts.

The registry itself is found in (**Windows\system32\config**).

NB: you cannot copy, edit the registry files on a running windows unless you will be using a special tools like FTKImager since it is used by the system.

The Most important Registry Hives Locations:

HKLM (system Registry)
HKEY_LOCAL_MACHINE\SYSTEM >> **C:\Windows\system32\config\system**
HKEY_LOCAL_MACHINE\SAM >> **C:\Windows\system32\config\sam**
HKEY_LOCAL_MACHINE\SECURITY >> **C:\Windows\system32\config\security**
HKEY_LOCAL_MACHINE\SOFTWARE >> **C:\Windows\system32\config\software**

HKCU (User Registry)
HKEY_USERS\.DEFAULT >> **C:\Windows\system32\config\default**
HKEY_USERS\ >> **C:\Users\{UserName}\NTUSER.DAT**

Userclass.dat
C:\Users\{username}\AppData\Local\Microsoft\Windows

NB: There is an automatic back up of the registry and it is stored in (Windows\system32\config\RegBack).

NB: Every user has an NTUSER.DAT stored in (C:\Users\{Username}) which is a part of the registry related to this user. HKCU (current user registry) reads from NTUSER.DAT.

The Registry is structured as below :

Hives: Hives are the registry directories and contain the keys
Keys: keys can contain another keys and values
Subkeys: Subkeys are Childs of keys
Values: Values are the data stored in the keys

Registry Exploration Tool:

Registry Explorer and Windows Regedit (preferred tools)

Artifacts

MRUs or (Most Recently Used)

MRU Keys are stored in the NTUSER.DAT so they are user specific.

RunMRU

Registry key Location:
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer**RunMRU**

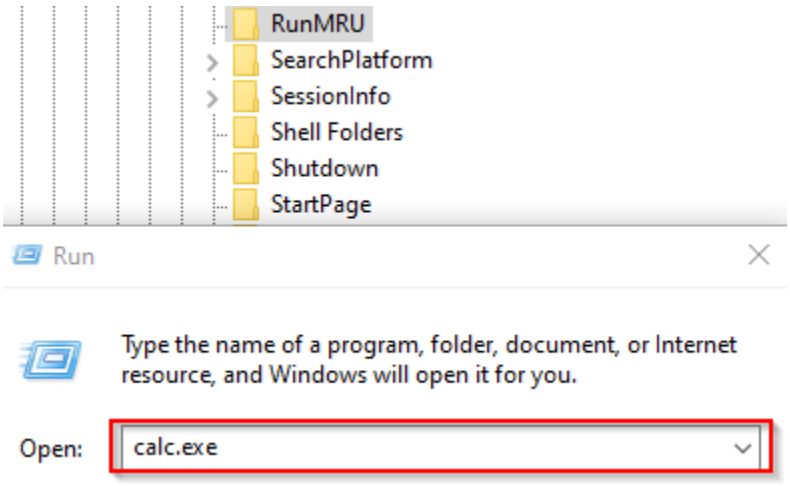
All programs lunched from run are stored in the RunMRU key. This artifact can be useful to understand what was executed recently on the device and detect any suspicious apps execution (eg Nmap).

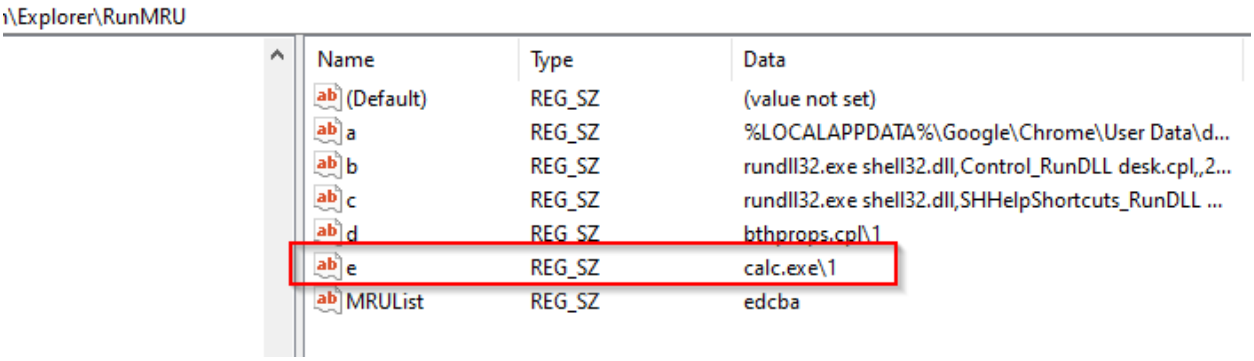
Experiment 1 - Running calc.exe from run window

For this test I will be launching calculator.exe from the run window and observe the artifacts in the RunMRU registry key. For this, i executed calc.exe as seen in the screenshot below

Results

When the application was run from the run windows, a new entry was created beneath '**RunMRU**'. Note that the order is specified in the MRUList key ebcda, means calc.exe (e) was run recently.





OpenSavePIDMRU

Registry key Location:
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32**OpenSavePIDMRU**

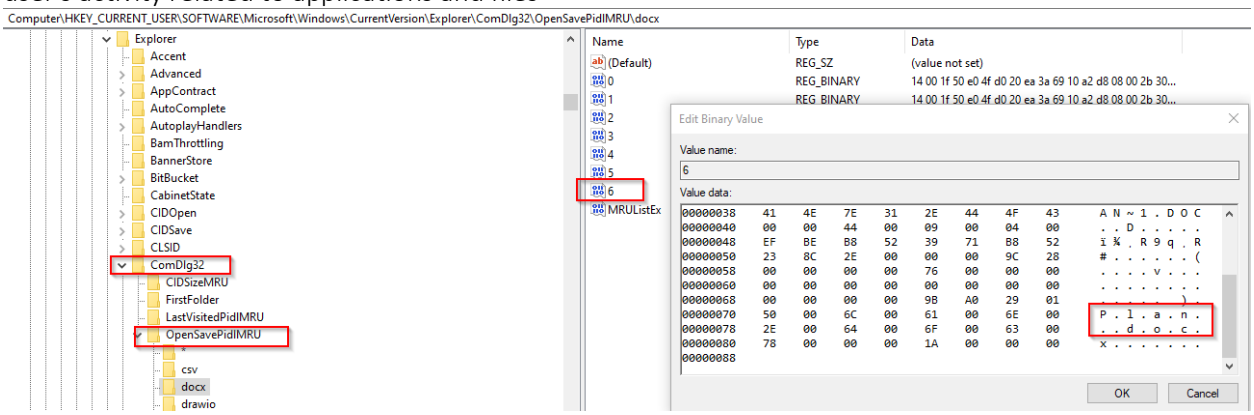
Experiment 1 – Executing a document file

For this test I will be opening a word document and observe the artifacts in the OpenSavePIDMRU sub-key.

Results

When the document was opened, a new entry was created beneath '**RunMRU**'. Note that the order is specified in the MRUList key ebcda, means calc.exe (e) was run recently.

user's activity related to applications and files



Last VisitedPIDMRU

Registry key Location:
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32**LastVisitedPidMRU**

This artifact can be used to understand which documents were viewed recently on the device.

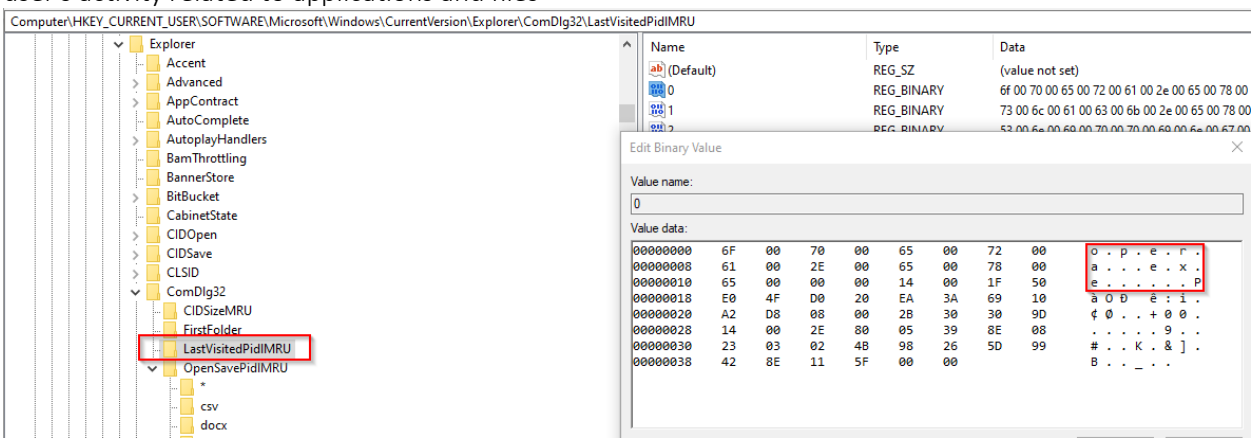
Experiment 1 – Executing an application

For this test I will be executing opera.exe and observe the artifacts in the **LastVisitedPidMRU** sub-key.

Results

When the the application was executed, a new entry was created beneath '**LastVisitedPidMRU**'.

user's activity related to applications and files



Typed Paths

Registry key Location:
Computer\HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer**TypedPaths**

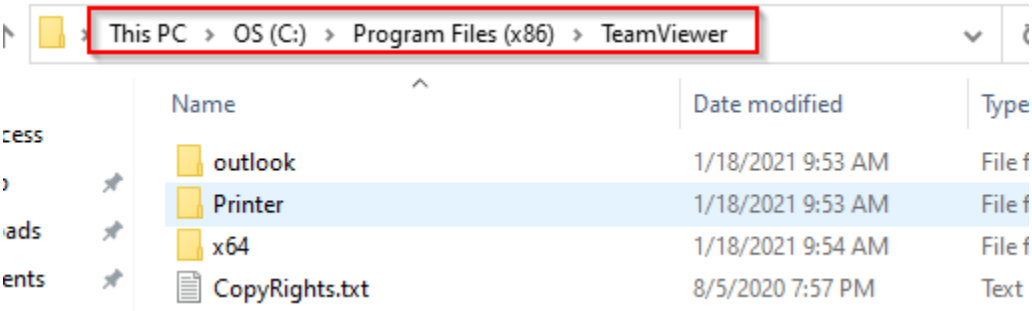
All path locations typed in windows explorer will be stored in TypedPaths key .As seen in the 2 screenshots below. This can be used to view what was been searched recently).

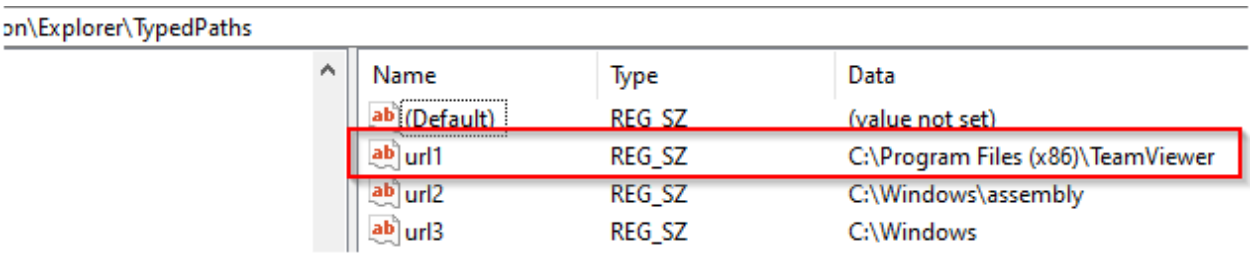
Experiment 1 – typing and navigating to path location in windows explorer

For this test I will be typing and navigating to a path and observe the artifacts in the **TypedPaths** sub-key.

Results

When the path typed in windows explored was executed, a new entry was created beneath '**TypedPaths**'. Note that url1 is the most recent. (if you are trying this by yourself don't forget to close the windows explorer after you browse the path, because it will not be shown in the Typedpaths key until it is closed).





OpenSaveMRU

Registry Key Location:

Computer\HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU

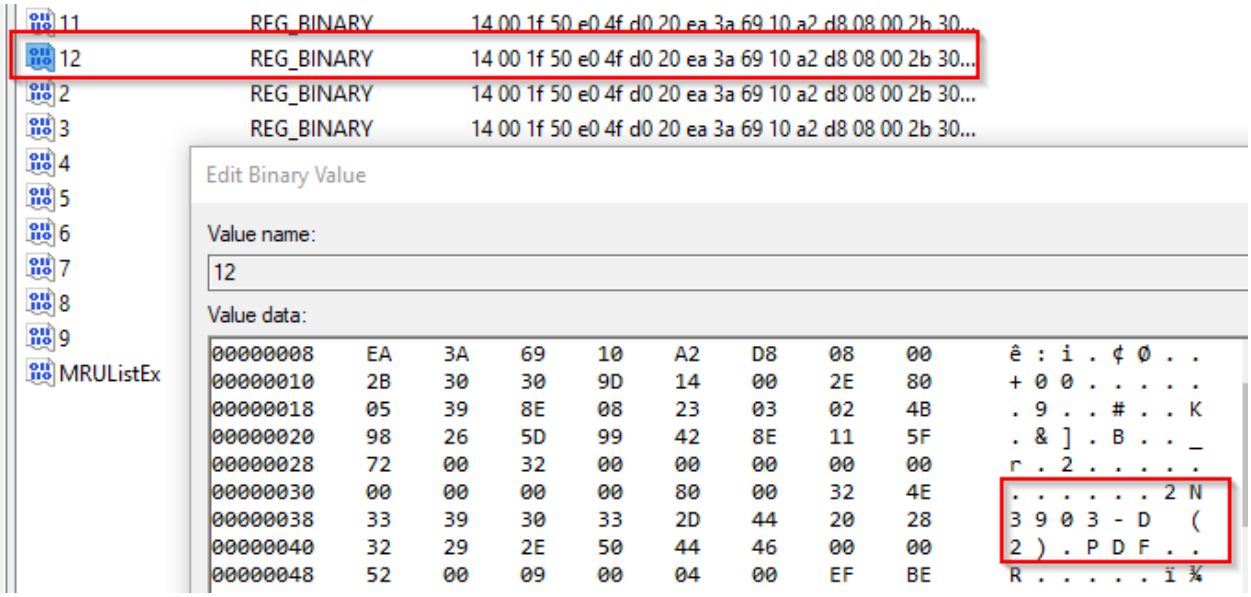
This key maintains a list of recently opened or saved files via Windows Explorer-style dialog boxes (Open/Save dialog box) (e.g. .txt, .pdf, htm, .jpg).

Experiment 1 – downloading a pdf file from a website

For this for demonstration I downloaded a pdf file from a website and saved it.

Results

Note that as seen in the screenshots below the highest number in the registry values (12) is the most recent. After double cliking on it you can see the file name in Hex and ASCII.

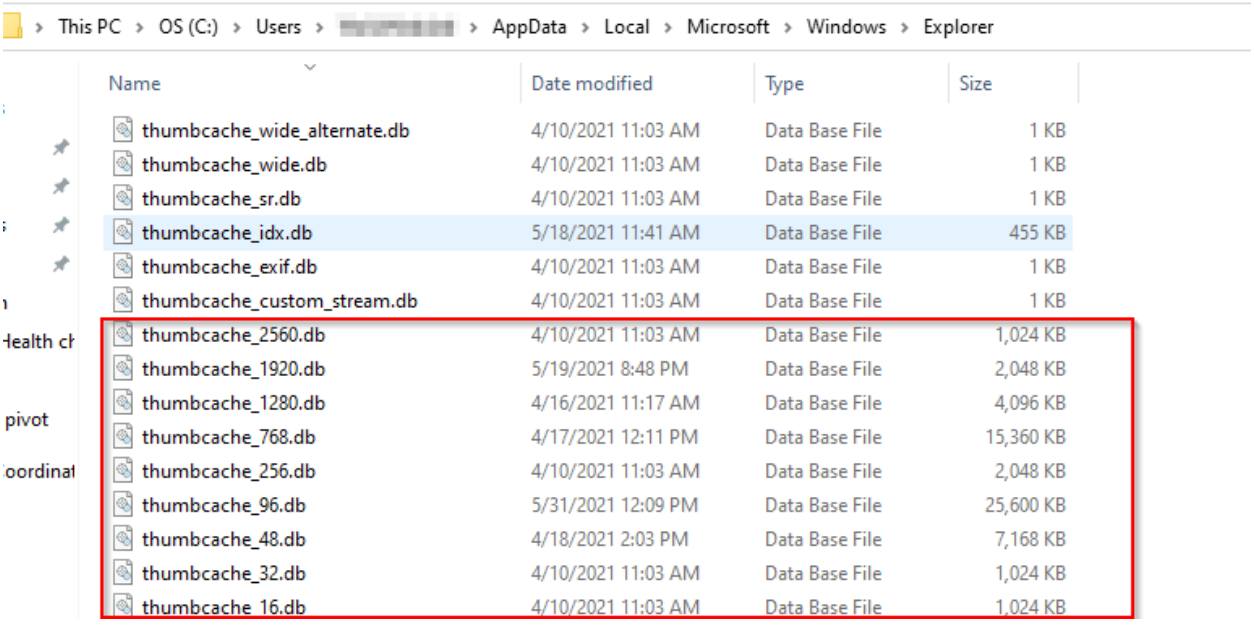


ThumbCache

When you are in a windows folder and you display the pictures in a directory using the Thumbnails views, a small thumbnail version is created. Thumbnail image analysis can help an investigator to get information about a picture on a storage or information about the original file used to create the thumbnail like the full path and the file name. ThumbCache can be used to recover deleted pictures, their file names and modification date.

Tools: Thumbcache Viewer (thumbs viewer)

Location: C:\Users\{username}\AppData\Local\Microsoft\Windows\Explorer\Thumbcache.db



UserAssist

Registry Key Location:

NTUSER.DAT HIVE:
NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\
{GUID}\Count

During a forensic analysis of a Windows system, it is often critical to understand when and how a particular process has been started. UserAssist shows evidence of application execution (what GUI-based programs were executed, how many times and last execution date and time).

NB: Registry values under these subkeys are encoded using ROT-13 algorithm.

following GUIDs key were observed beneath UserAssist key which are common across Windows 7 and higher versions:

1. {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA} - A list of applications, files, links, and other objects that have been accessed.

2. {F4E57C4B-2036-45F0-A9AB443BCFE33D9F} - Lists the shortcut links used to start programs.

Experiments

A number of experiments were formulated to as certain information required for the objective. These experiments were performed on both type of systems to validate the results highlighted in the subsequent section. Below are the research questions that need to answer through experiments and observations:

• What information is stored when host-based applications are executed? applications on UserAssist key?
• What information is stored when portable applications are run from drives and shared network?

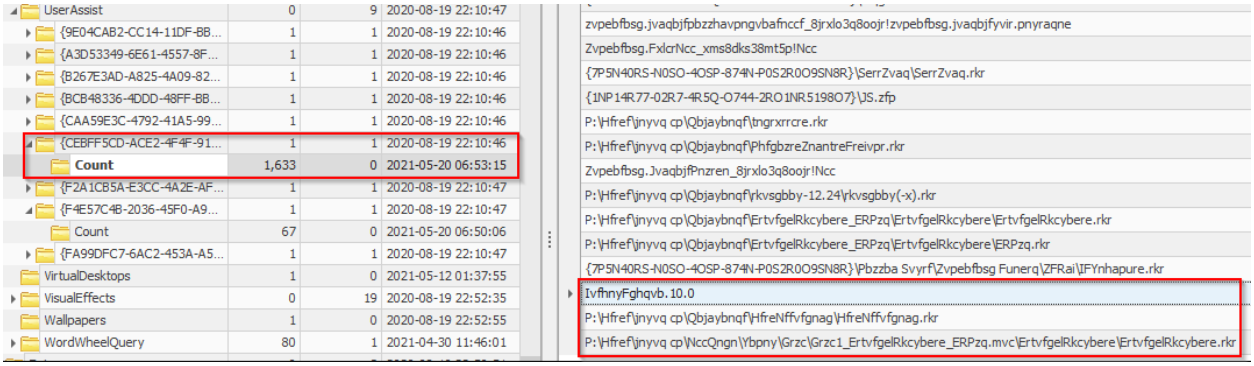
Experiment 1 - Running Host-based Applications

This experiment was performed to determine the effects on UserAssist key when host-based applications are run on a Windows system. For this, i executed different host-based applications, such as VisualStudio, Userassistant.exe, RegistryExplorer.exe. via all possible ways of launching. Note that these possible ways of launching a host-based application and its effects on UserAssist key are provided in subsection screenshot below.

Results

Execute application from their parent folder. When applications were run from their parent folder then

entries were created beneath 'Count' subkey of {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}.



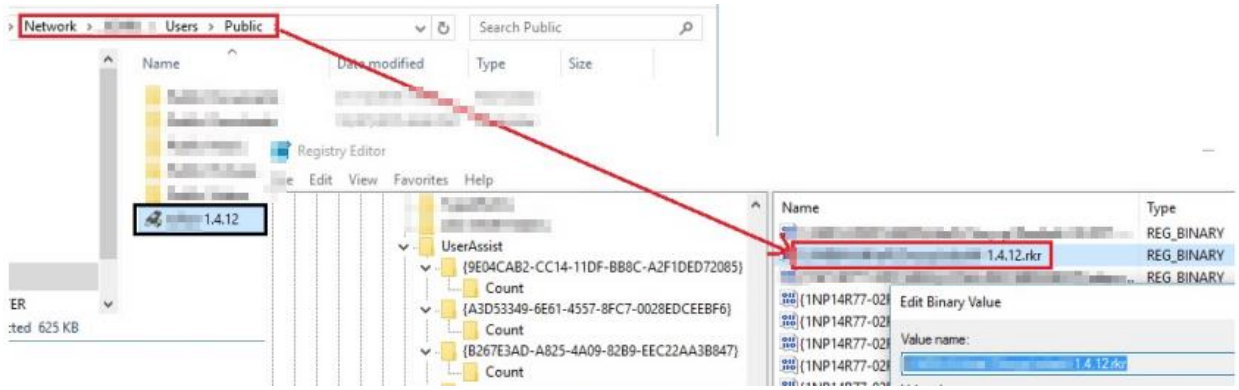
Use www.rot13.com to decode the rot13 registry values
IvfhnyFghqvb.10.0 **>> VisualStudio.10.0**

P:\Hfref\jnyvq cp\Qbjaybnqf\HfreNffvfgnag\HfreNffvfgnag.rkr **>>**
C:\Users\{user}\Downloads\UserAssistant\UserAssistant.exe

P:\Hfref\jnyvq
cp\NccQngn\Ybpny\Grzc\Grzc1_ErtvfgelRkcybere_ERPzq.mvc\ErtvfgelRkcybere\ErtvfgelRkcybere.rkr **>>**
C:\Users\walid
pc\AppData\Local\Temp\Temp1_RegistryExplorer_RECmd.zip\RegistryExplorer\RegistryExplorer.exe

Experiment 2 - program run from a shared network

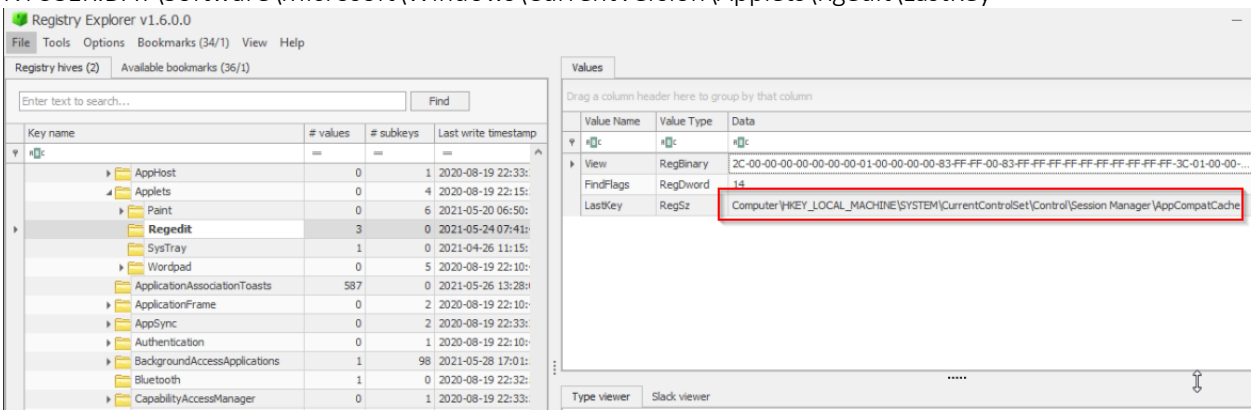
The decoded value names refer the complete file path from which the portable applications were executed including the computer-name of the shared computer over a network.



Last Registry Key Viewed

You can check the last registry key viewed by the user.

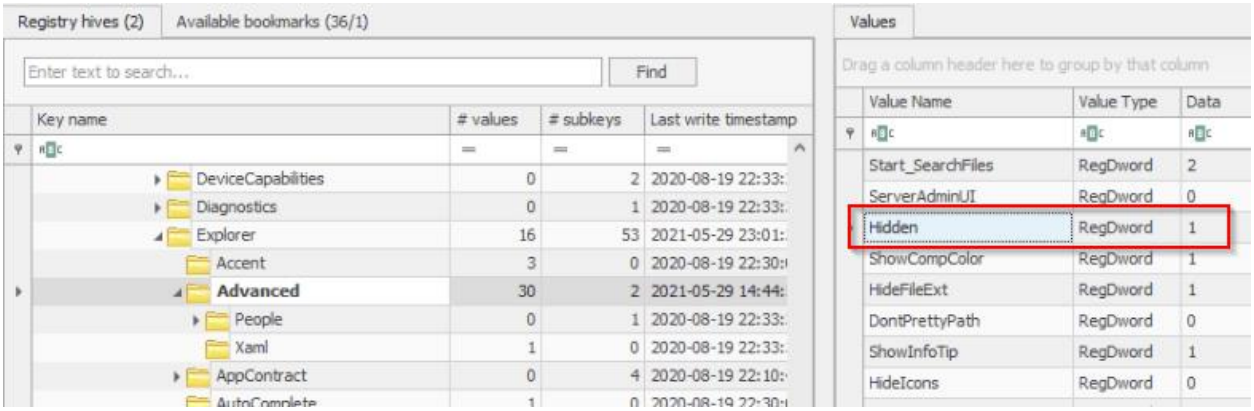
Registry Key Location:
NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Applets\Rgedit\LastKey



Hidden Files settings

Check the hidden files settings in the directories as it could be used for malicious activity.

Registry Key Location:
SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced



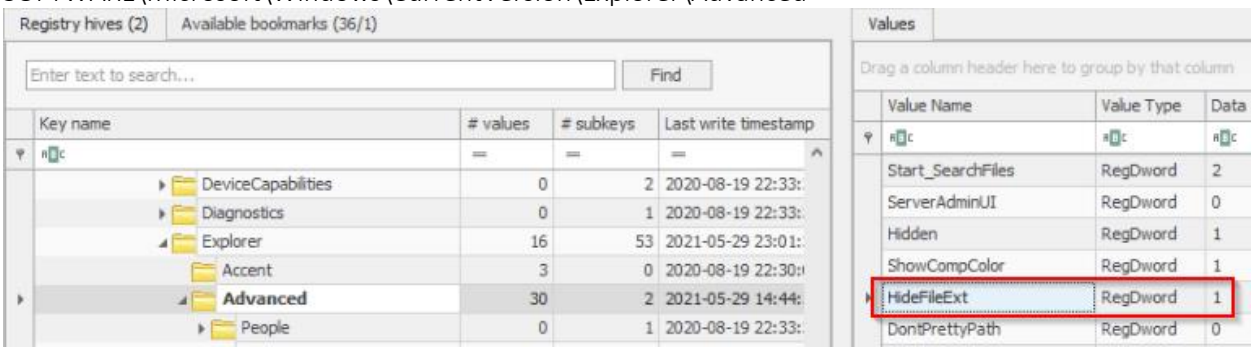
Hidden = 0 (means do not show hidden files)
Hidden = 1 (means show hidden files)

Files Extensions hiding settings

Check the hide file extensions settings in the directories as it could be used for malicious activity.

Registry Key Location:

SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced



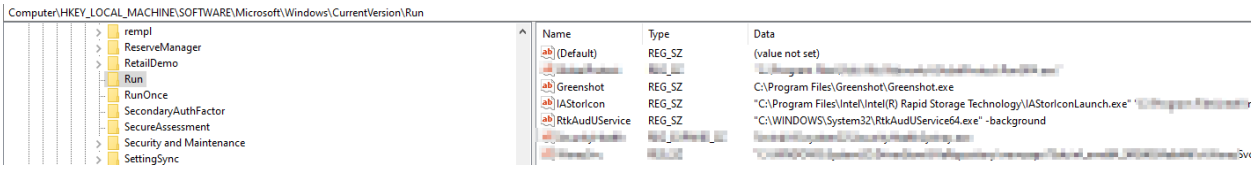
HideFileExt = 0 (means show the file extension)
HideFileExt = 1 (means do not show the file extension)

Auto-runKeys

This first Run key usually contains programs or components paths that are automatically run during system startup without requiring user interaction: malware usually leaves trace in this key to be persistent whenever system reboots.

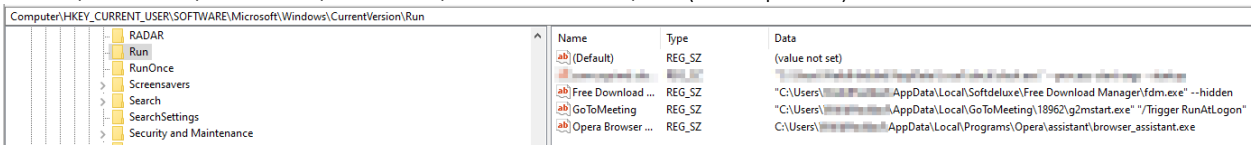
The RunOnce keys identifies programs that run only once, at startup and can be assigned to a specific user account or to the machine.

Registry Key Location:
HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
HKCU\Software\Microsoft\Windows\CurrentVersion\Runonce (user specific)
HKCU\Software\Microsoft\Windows\CurrentVersion\Run (user specific)
HKLM\System\CurrentControlSet\Services
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

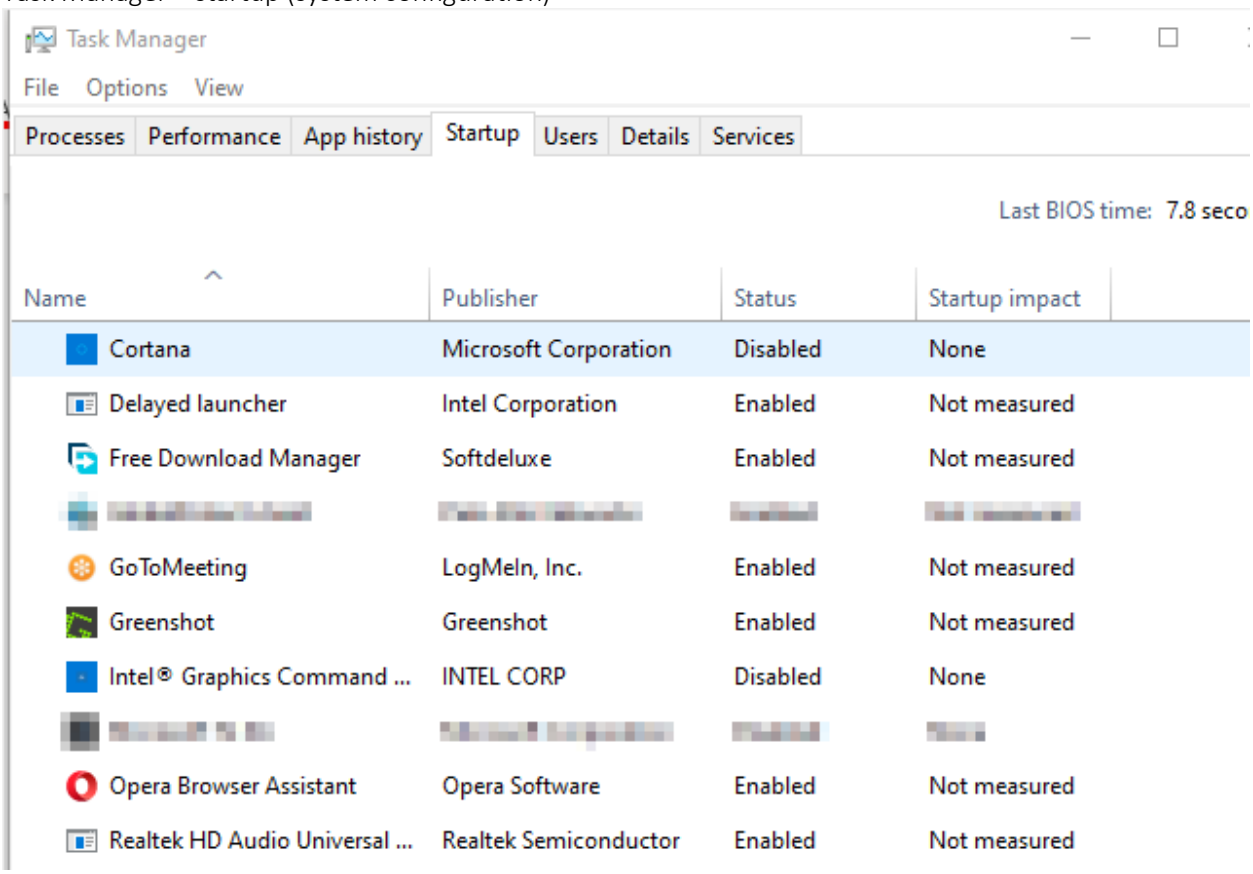


HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Run (user specific)



Task Manager > startup (system configuration)



NB: Another place to start application automatically is the Scheduled tasks .

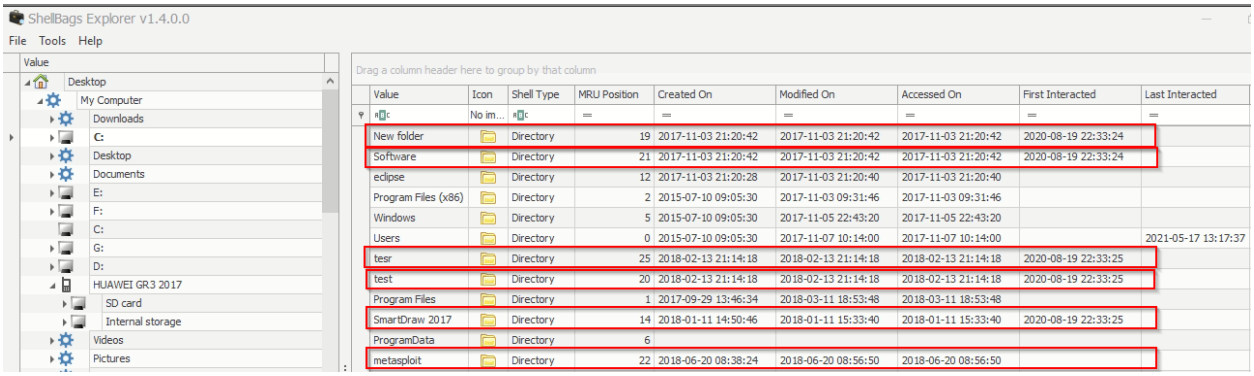
ShellBags

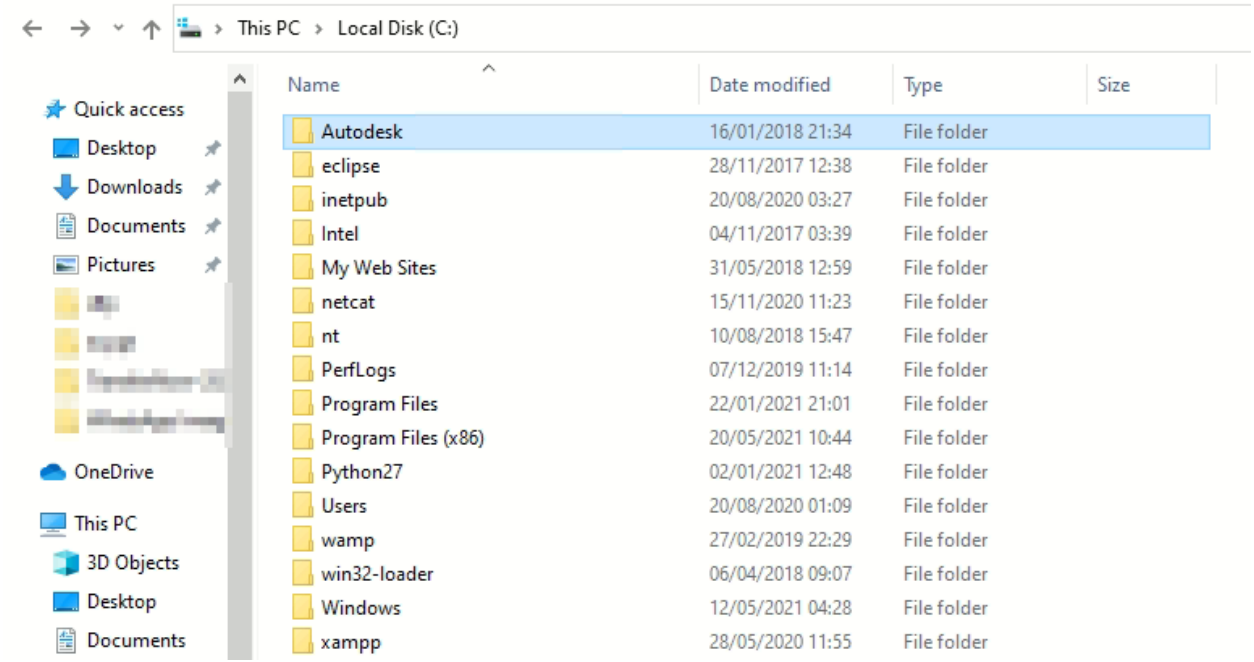
When you visit a folder Shellbags store the information like the icons customizations, the look and the feel of the folder, window position, size, sorting methods, etc..

Shellbags are extremely useful to find traces about folders that were on the system and were deleted since shellbags persist on the system even after deleting the folder.

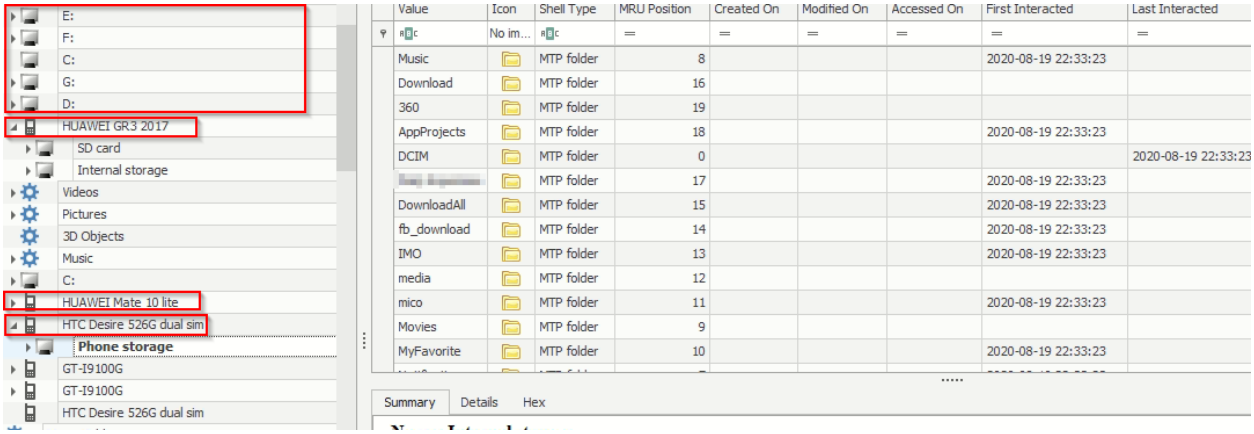
Registry Key Location: (NTuser.dat and usrclass.dat)
HKCU\SOFTWARE\Microsoft\Windows\Shell\BagMRU
HKCU\SOFTWARE\Microsoft\Windows\Shell\Bags

Tools: Shellbags Explorer
We can see directories that does not exist currently on the C: drive (deleted).
We can see also the last modification date on these folders.





Also we can see Drives like E:, F:, phones volumes. Those are networks paths or removable drives that once were mounted on the system. These are good evidences to proof that for example a USB flash drive was mounted to the system on a specific date and time and used to browse a particular folder on the drive or on the shared folder.



Mounted USB devices or Flash drives

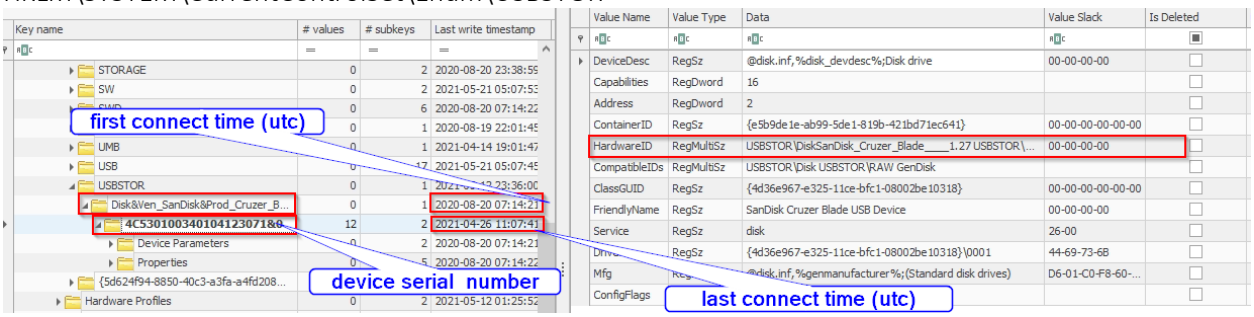
This experiment was performed to determine the effects on registry keys when plugging a new device via USB. For this, i connected a previously a storage device via USB to my PC. Its effects on Registry keys are provided in subsection screenshot below. These traces left are very useful to discover USB devices plugged to a system in any given time, what was accesses, who mounted them, etc.. even when the device is disconnected from the system.

Tool: USBDeview

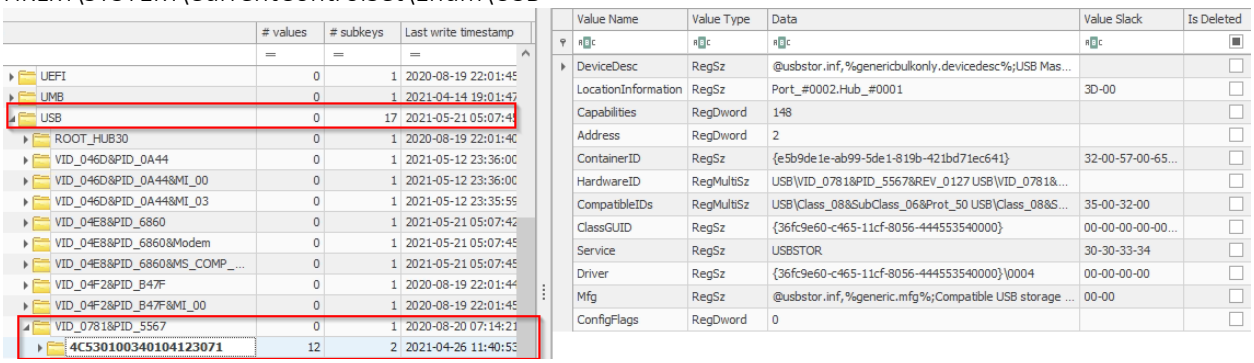
Registry Key Location:
HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR
HKLM\SYSTEM\CurrentControlSet\Enum\USB
HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices
HKLM\SYSTEM\MountedDevices
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\EMDMgmt (on if the device is not SSD)

NB: CurrentControlSet key can only be seen on a live system. If you are analysing a forensic image there will be no CurrentControlSet. There will be ControlSet001 or ControlSet002 or ControlSet004 or ControlSet00*.
(sometimes there is more then on ControlSet if the system had some problems during startup). To know which control set is last used on the system go to the registry key:
HKLM\SYSTEM\select and look at the “current” key value. If it’s “1” for example this will indicate that the current control set is 001.

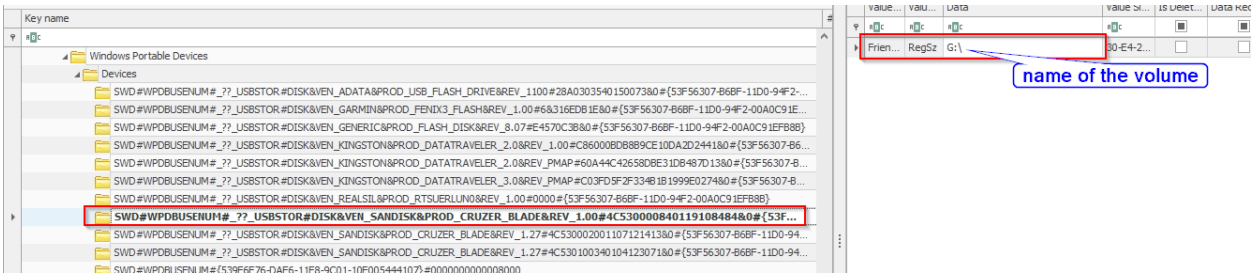
HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR



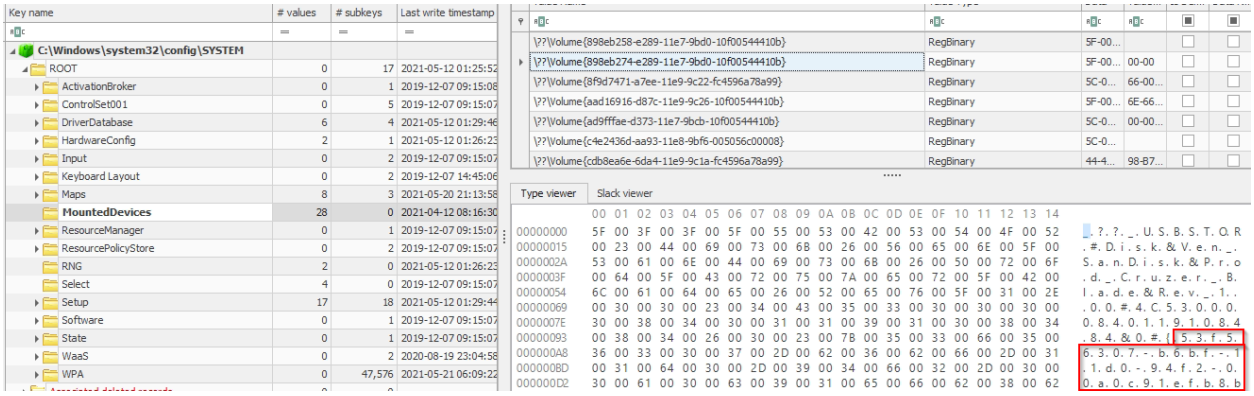
HKLM\SYSTEM\CurrentControlSet\Enum\USB



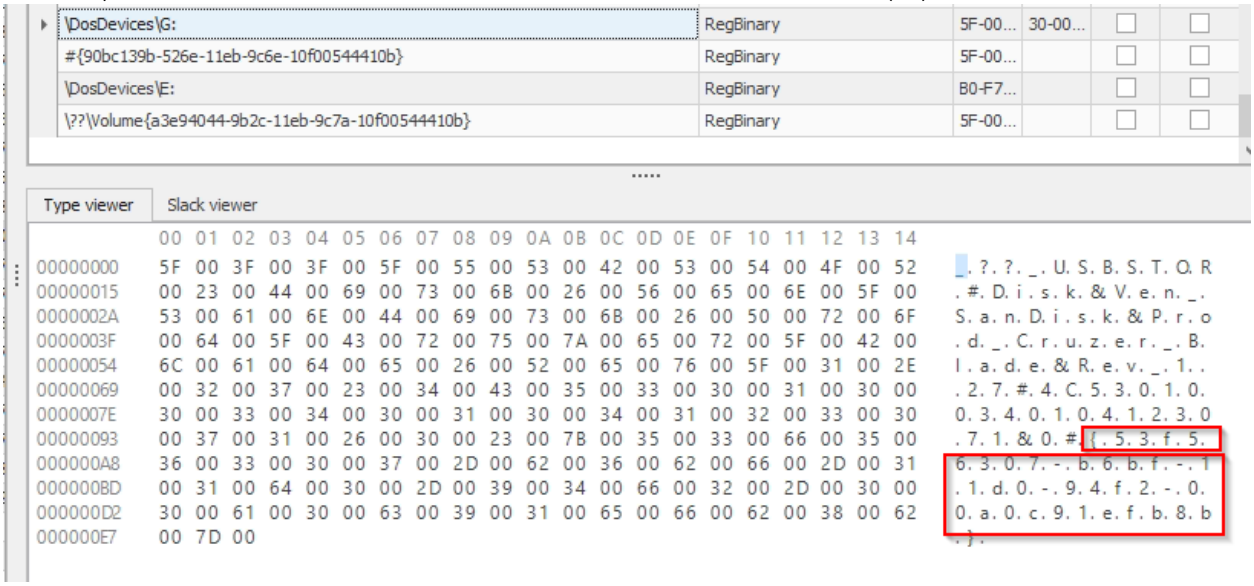
HKLM\SOFTWARE\Microsoft\Windows Portable Devices\Devices



HKLM\SYSTEM\MountedDevices (match up the serial number in order to find the GUID for this item on the system) Volume GUID: \??\Volume{898eb274-e289-11e7-9bd0-10f00544410b}

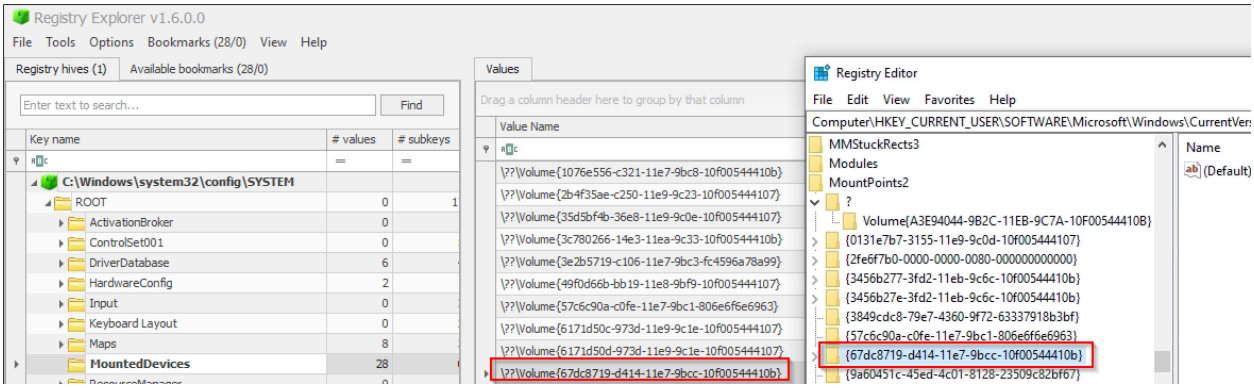


Match up serial number to obtain drives that were attached to that device (G:)



Now we know the make, model ,vendor, serial number, volume name, first and last time date mounted.

To find the user who mounted the USB device:
NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2
Since the volume is found in the
NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2 registry hive this means the actual user mounted the USB device



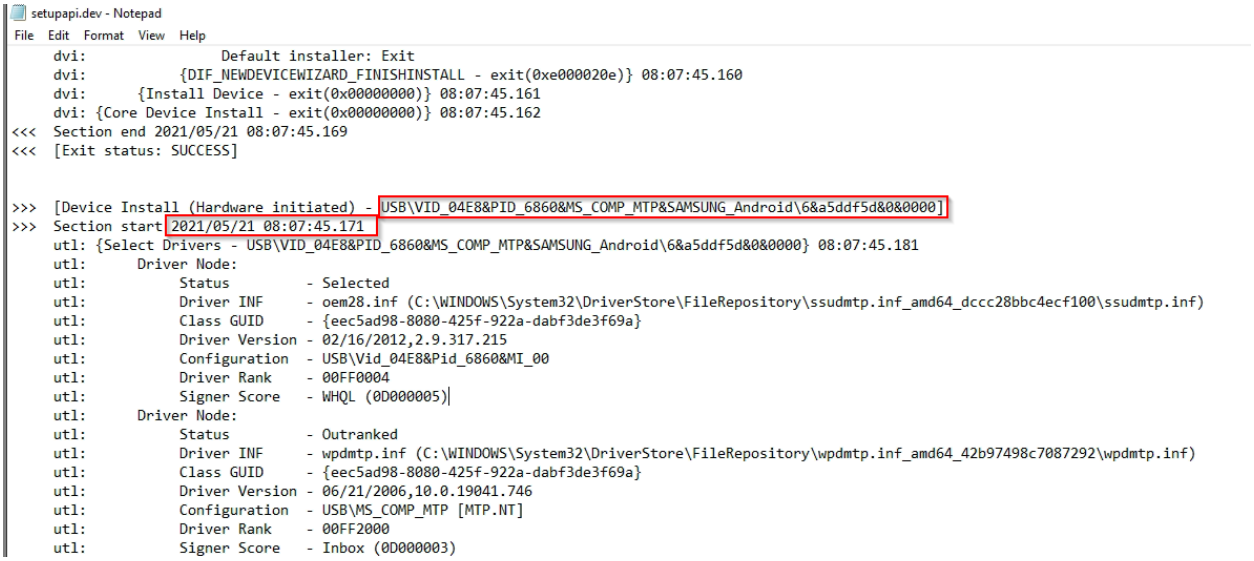
Setupapi.dev.log

Location: C:\windows\inf\setupapi.dev.log

Setupali.dev.log contain additional information about USB devices.

Setupapi logs after connecting a Samsung device via USB.

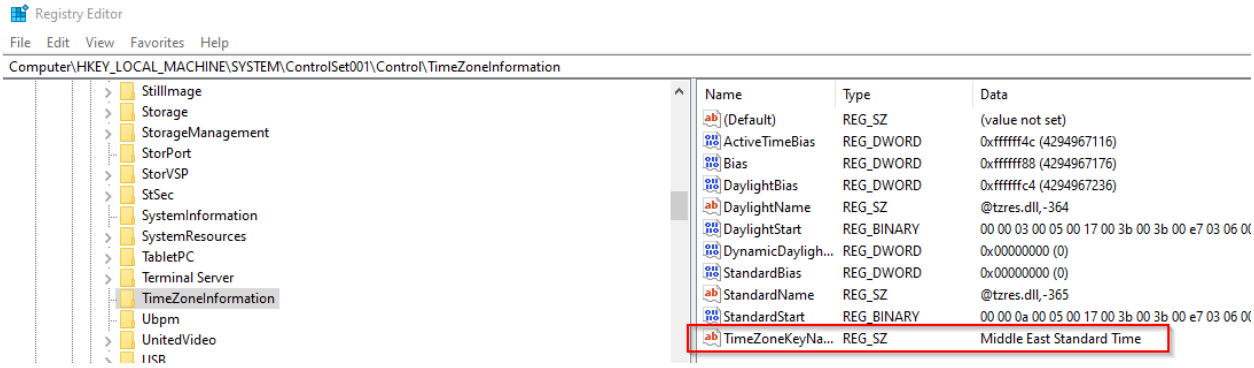
Log file showing device vendor, hardware installation time, etc…



Timezone Information

To view what time zone the computer is on.

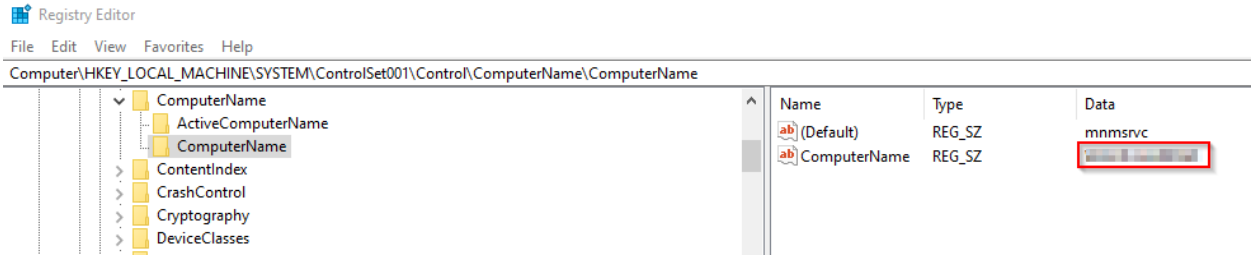
Registry Key Location:
SYSTEM\ControlSet001\Control\TimeZone\Information



Computer Name

To know what is the computer name of the offline image.

Registry Key Location:
SYSTEM\ControlSet001\Control\ComputerName\ComputerName



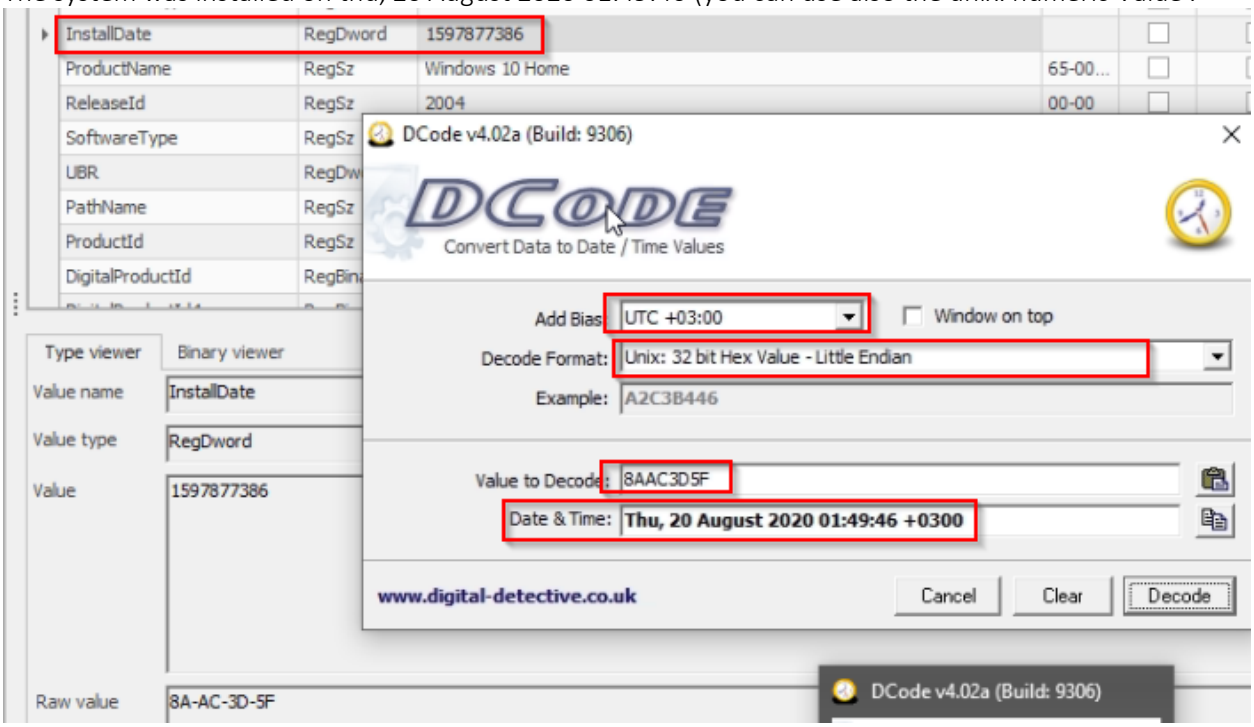
Windows information

To get some information about the system.

Registry Key Location:
SOFTWARE\Microsoft\WindowsNT\CurrentVersion

(Default)	REG_SZ	(value not set)
BaseBuildRevisi...	REG_DWORD	0x00000001 (1)
BuildBranch	REG_SZ	vb_release
BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffff
BuildLab	REG_SZ	19041.vb_release.191206-1406
BuildLabEx	REG_SZ	19041.1.amd64fre.vb_release.191206-1406
CompositionEdi...	REG_SZ	Enterprise
CurrentBuild	REG_SZ	19042
CurrentBuildNu...	REG_SZ	19042
CurrentMajorVer...	REG_DWORD	0x0000000a (10)
CurrentMinorVe...	REG_DWORD	0x00000000 (0)
CurrentType	REG_SZ	Multiprocessor Free
CurrentVersion	REG_SZ	6.3
DigitalProductId	REG_BINARY	a4 00 00 00 03 00 00 00 30 30 33 33 30 2d 35 31 39 3...
DigitalProductId4	REG_BINARY	f8 04 00 00 04 00 00 00 30 00 33 00 36 00 31 00 32 00...
DisplayVersion	REG_SZ	20H2
EditionID	REG_SZ	Professional
EditionSubMan...	REG_SZ	
EditionSubstring	REG_SZ	
EditionSubVersion	REG_SZ	
InstallationType	REG_SZ	Client
InstallDate	REG_DWORD	0x603d7a88 (1614641800)
InstallTime	REG_QWORD	0x1d70ef3bacd4d9e (132591154004577694)
PathName	REG_SZ	C:\Windows
PendingInstall	REG_DWORD	0x00000000 (0)
ProductId	REG_SZ	00330-51972-82358-AAOEM
ProductName	REG_SZ	Windows 10 Pro
ReleaseId	REG_SZ	2009
SoftwareType	REG_SZ	System
SystemRoot	REG_SZ	C:\WINDOWS
UBR	REG_DWORD	0x000003d9 (985)

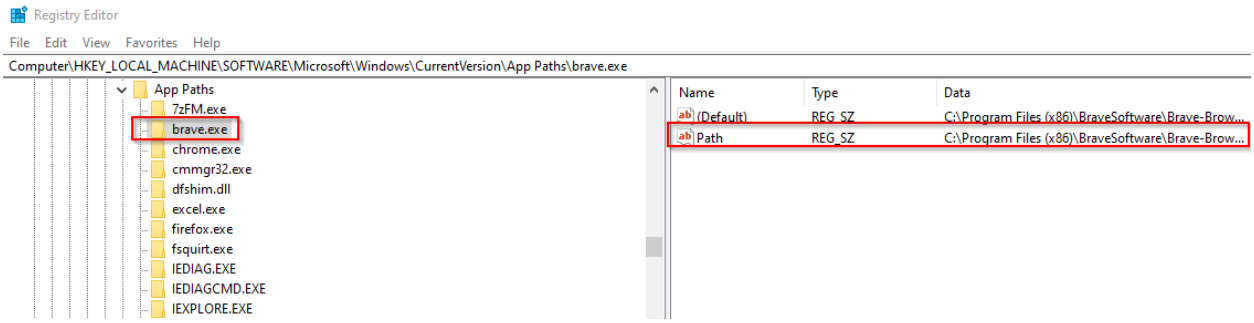
The system was installed on thu, 20 August 2020 01:49:46 (you can use also the unix: numeric Value .



Softwares Installed

To get a list of installed softwares on the system. Sometimes even the program were uninstalled the registry key is still in the registry. This will help us to identify also any removed application from the system.

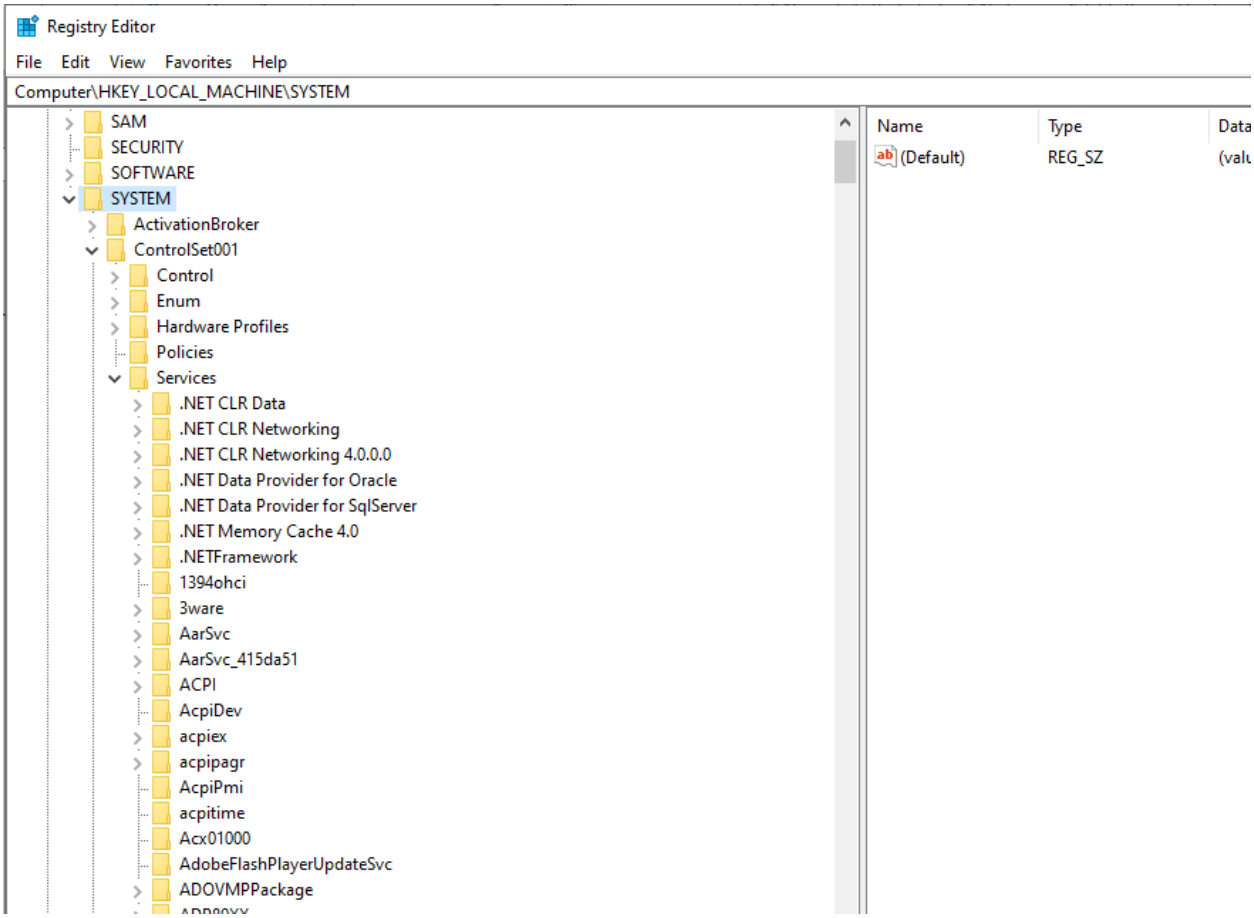
Registry Key Location:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\



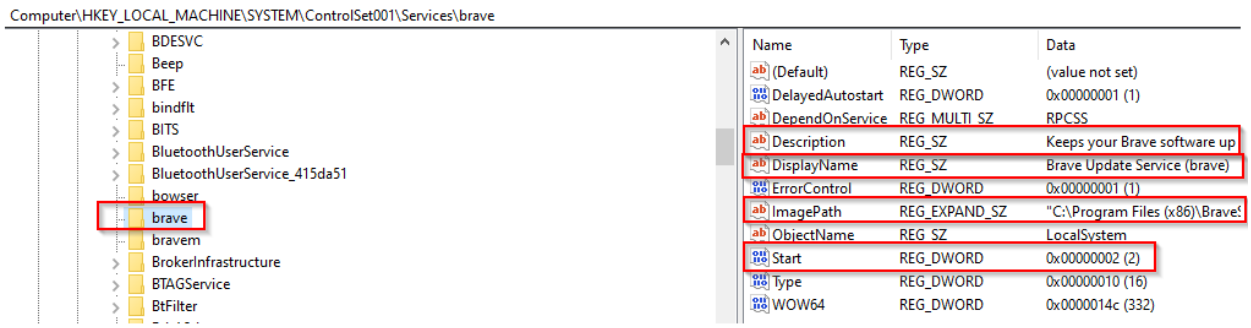
Windows Services

To check current windows services

Registry Key Location:
SYSTEM\ControlSet00%\Services\



To get more information about the service description, path, if it starts automatically on windows startup or no (start : 2 means automatic start , 3 means manual, 1 means system, 4 means disabled)



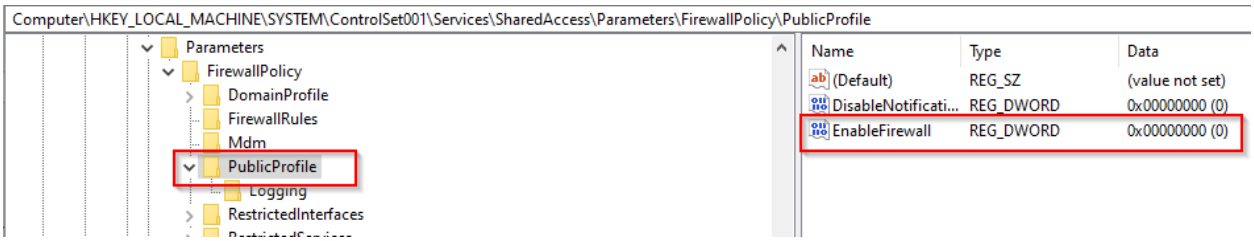
Windows Firewall

To check current Windows Firewall status on the system.

Registry Key Location:
Private profile:
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile

Public Profile:
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\PublicProfile

Domain Profile:
HKLM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfile



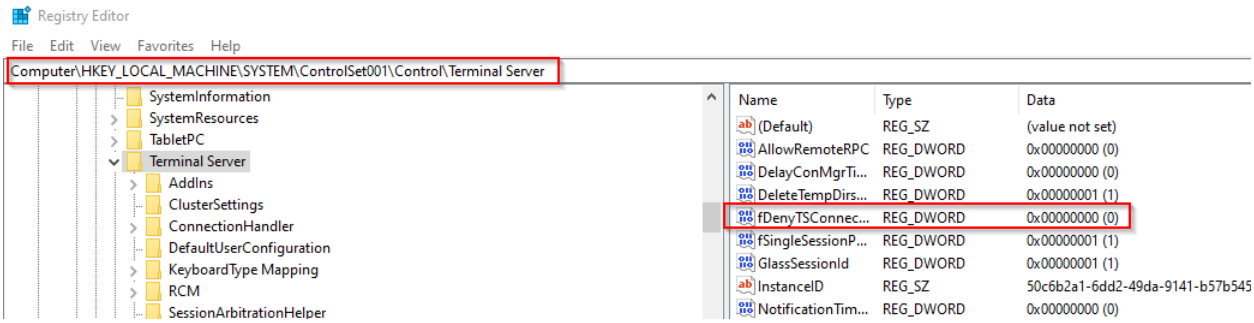
EnableFirewall =0 means the firewall is disabled
EnableFirewall=1 means the firewall is enabled

Remote Desktop

To check if Remote Desktop is enabled or not on the system.

Registry Key Location:
HKLM\SYSTEM\ControlSet001\Control\Terminal Server

0 means RDP is enabled
1 means RDP is disabled

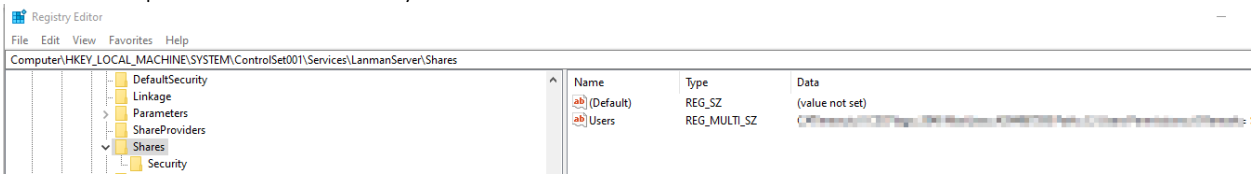


Shares

List shared folders configured on the system.

Registry Key Location:
SYSTEM\ControlSet001\Services\LanmanServer\Shares

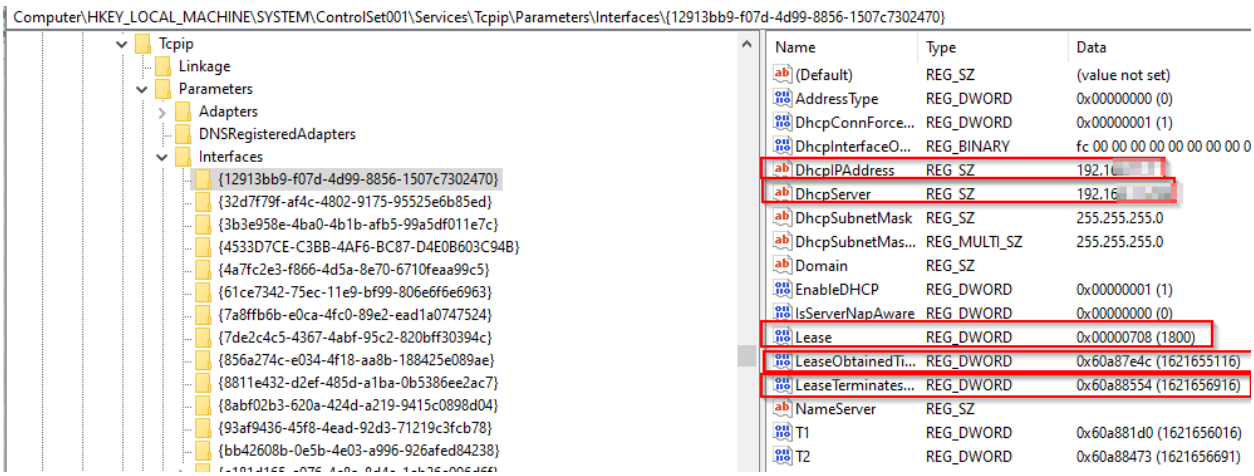
In this example no shares on the system



Network configuration

To see the network configuration of the offline image like DHCP IP address, DHCP server IP, Lease time, Lease obtained time…

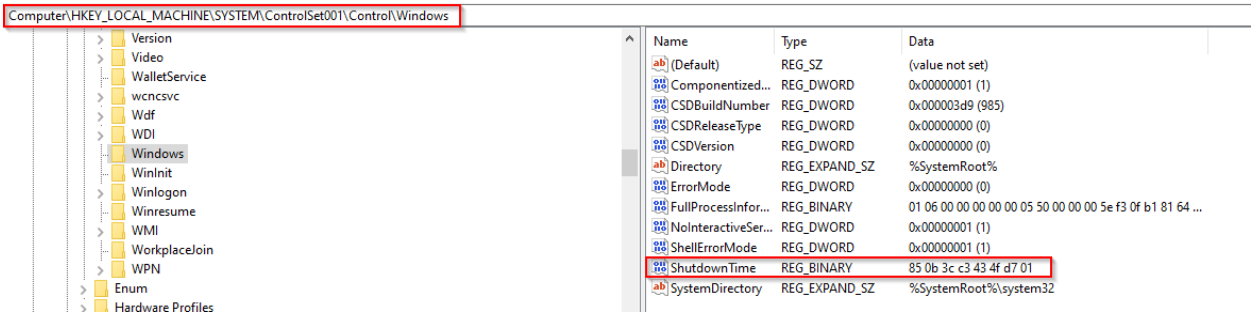
Registry Key Location:
SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces



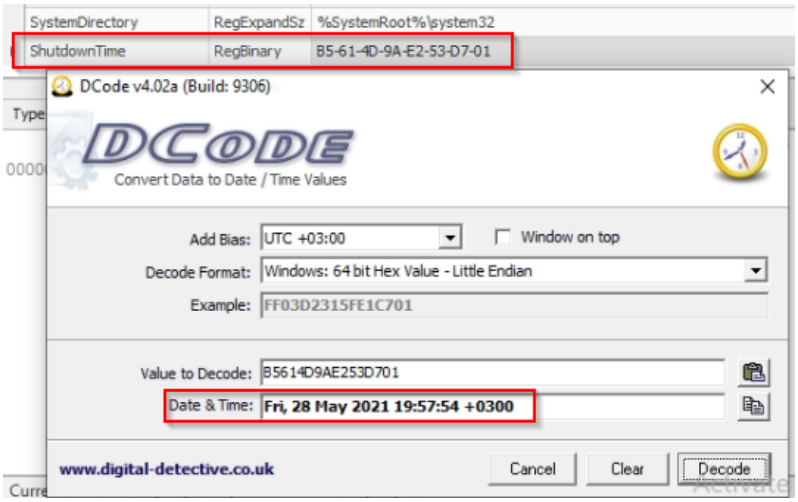
Last Shutdown

To determine the last Shutdown time.

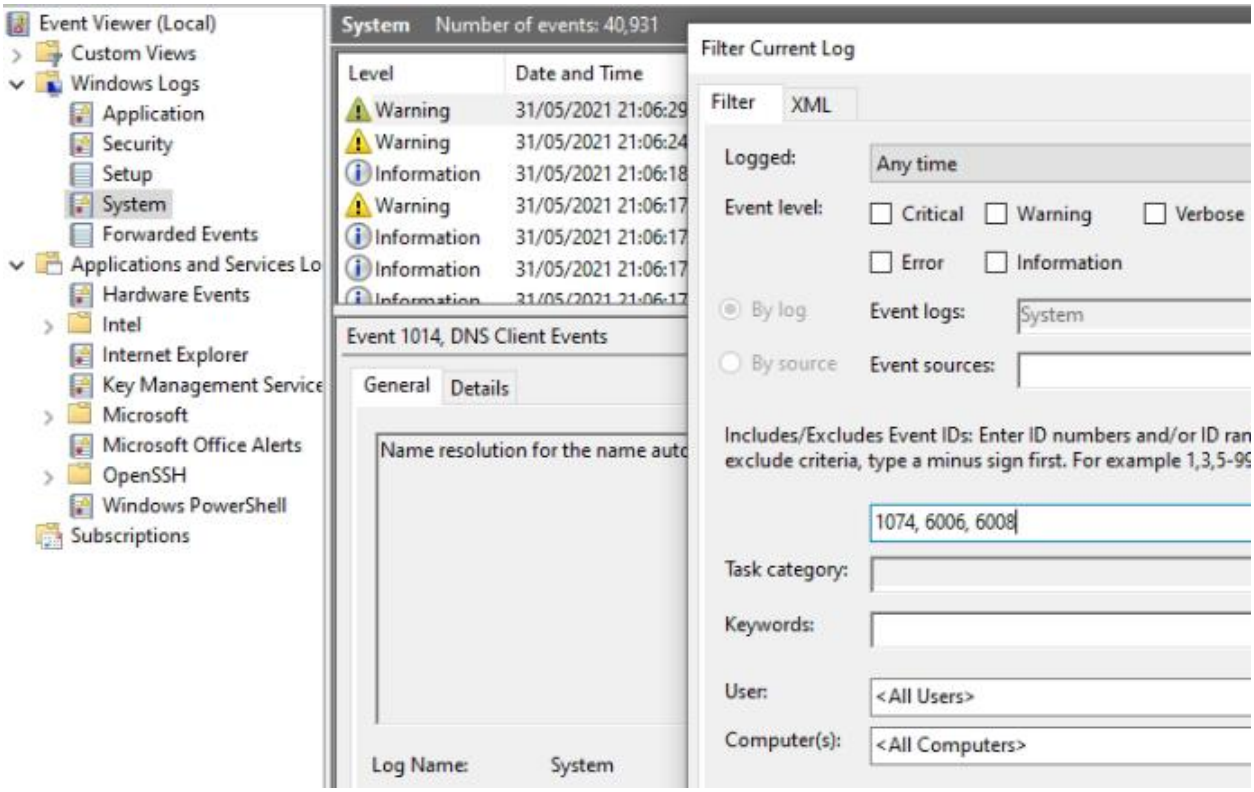
Registry Key Location:
HKLM \SYSTEM\ControlSet001\Control\Windows

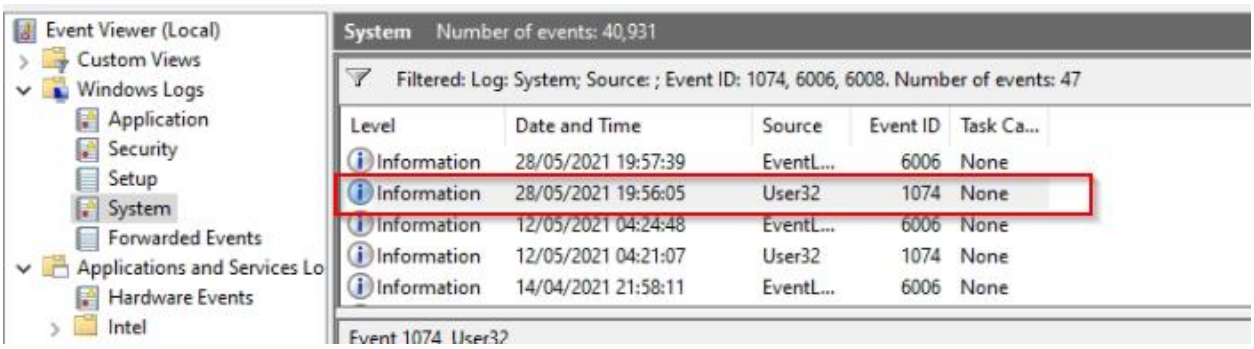


Last Shutdown time



To confirm with event logs (filtering shutdown event ID (related to the shutdown))



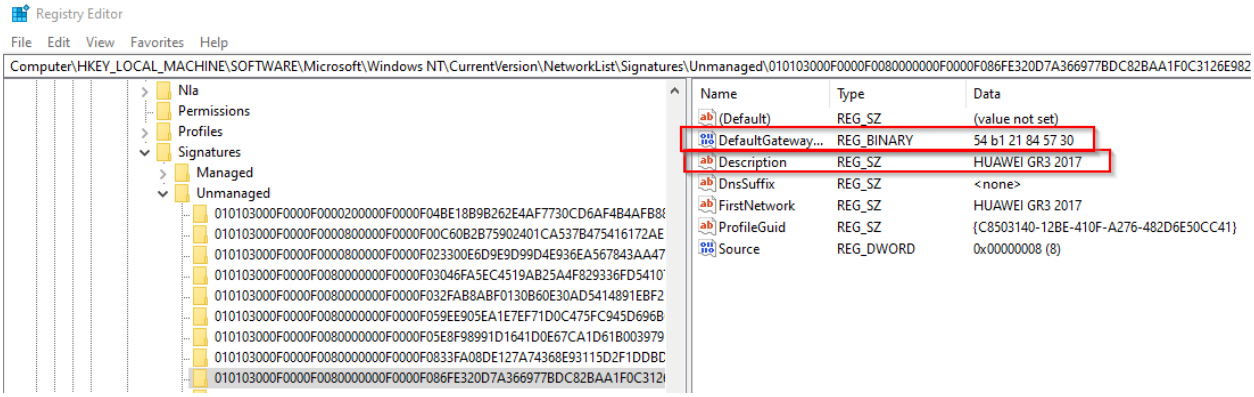


Network list

Determine the last time a pc connected to a particular network

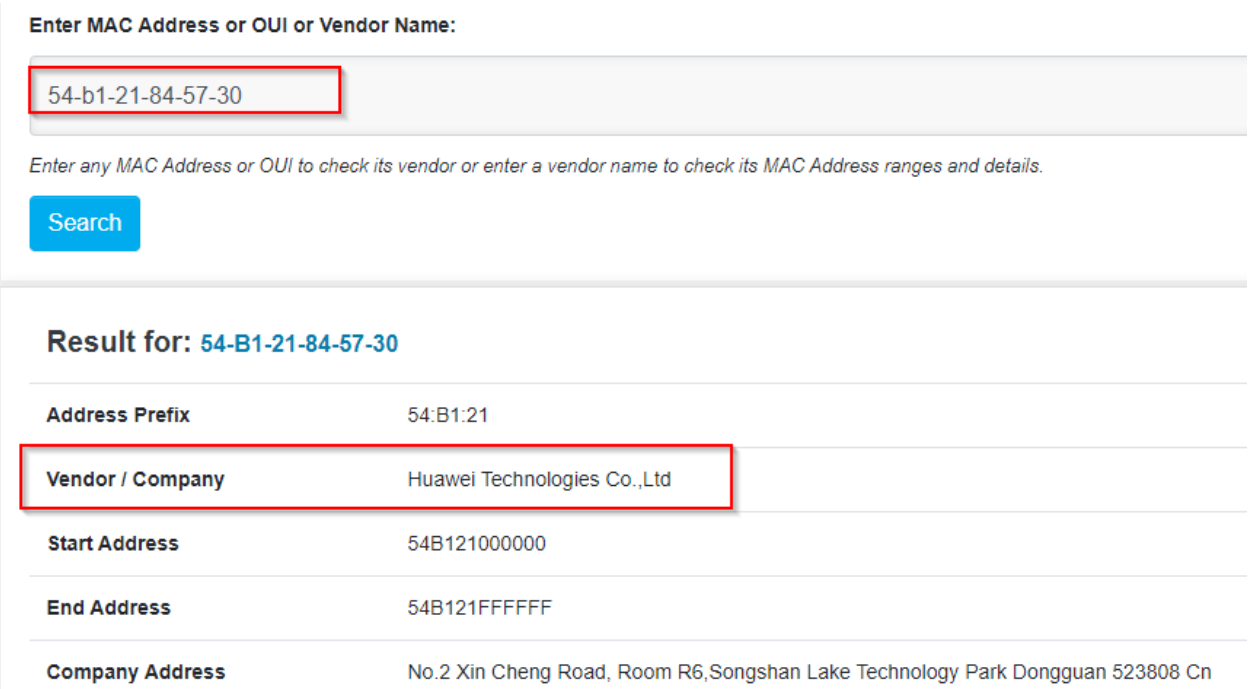
Registry Key Location:
HKLM\Software\Micrososft\Windows NT\CurrentVersion\NetworkList

For this test I have recently connected my pc to my phone hotspot



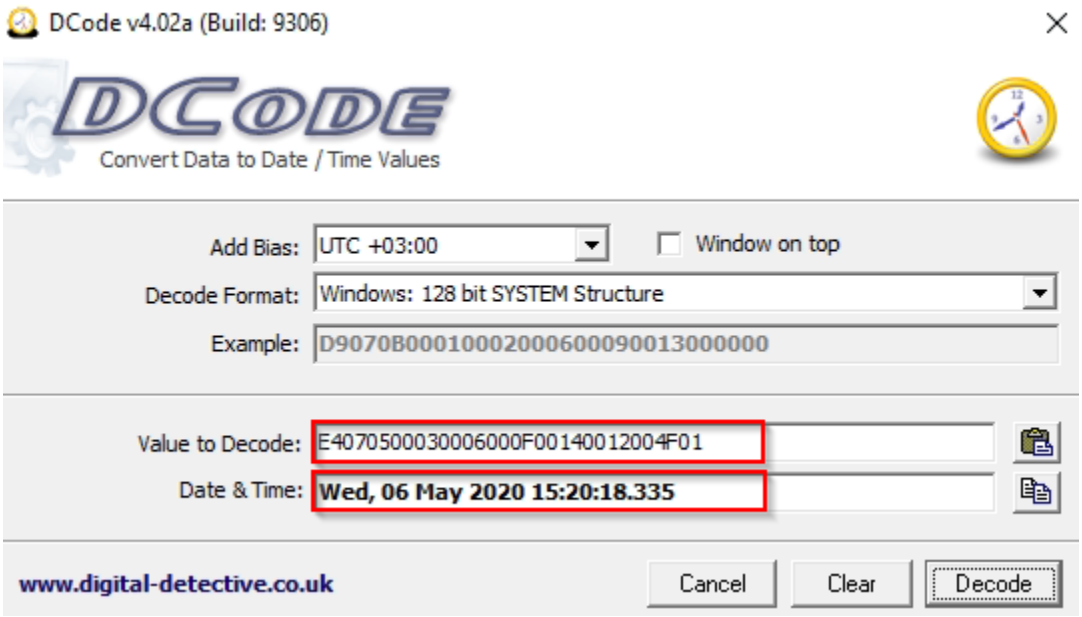
You can also perform a MAC address lookup

In order to determine the type of connection the device was connected to (wired or wireless network) note the profileGUID in the previous screenshot . Search in the profiles key for the same profileGUID. Look in the NameType value .(6 indicates that the device was connected to a wired network, 71 and 47 indicates that the device was connected to a wireless network and 17 means the device was connected to a broadband network.) In this case it is 71 (wireless network).
The date Created (128 windows system time structure UTC) and Date last connected indicates

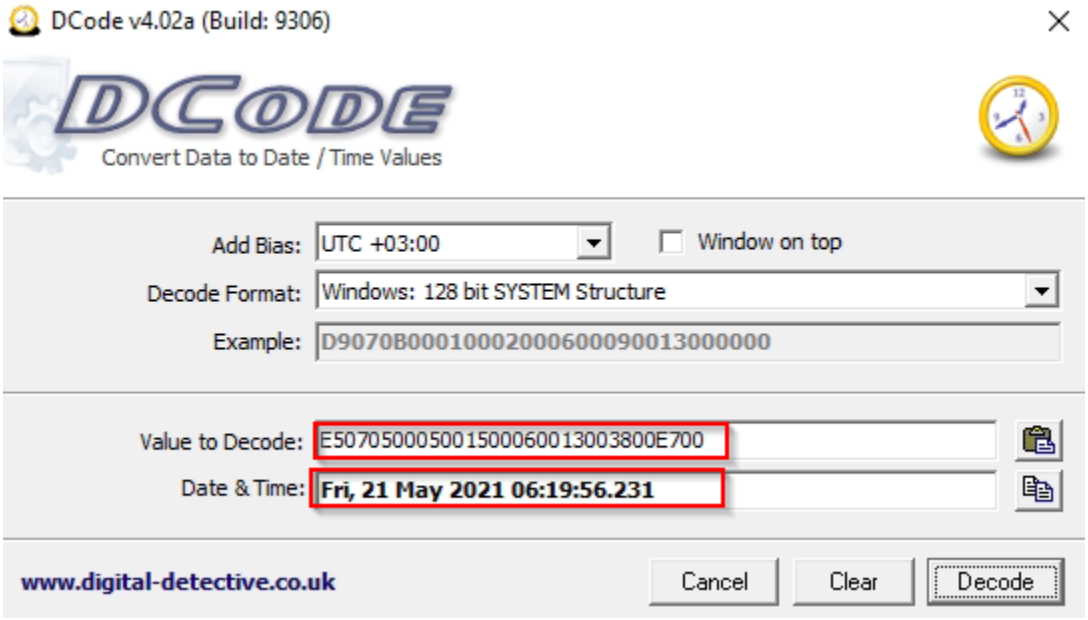


respectively the first time the device was connected and the last time the device was connected. (use Dcode to convert the time values).

First connect time



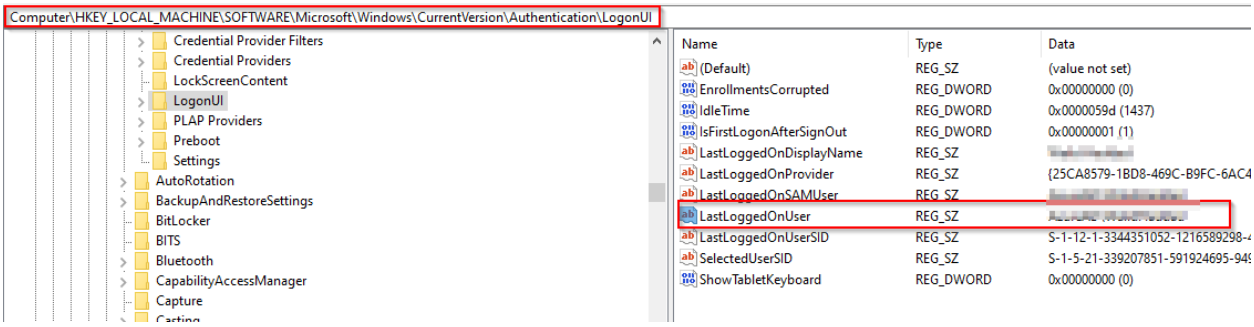
Last connect time



Last User Logged In

To determine when was the last time the user logged in to the system.

Registry Key Location:
HKLM\Software\Micrososft\Windows\CurrentVersion\Authentication\LogonUI\LastLoggedOnUser

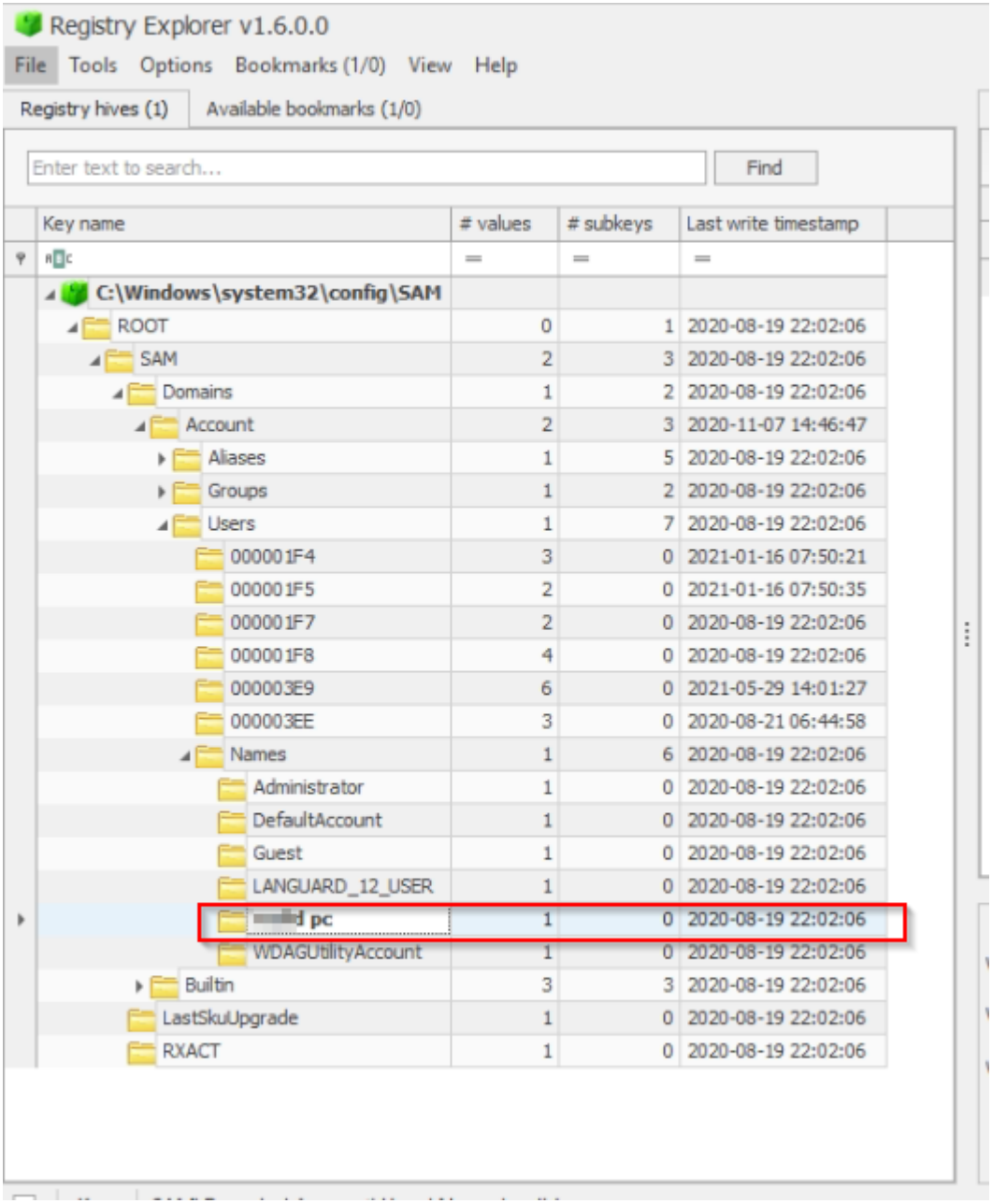


SAM Users

To determine all the users in the SAM file.

Registry Key Location:
SAM\Domains\Account\Users\Names\WDAGUtilityAccount

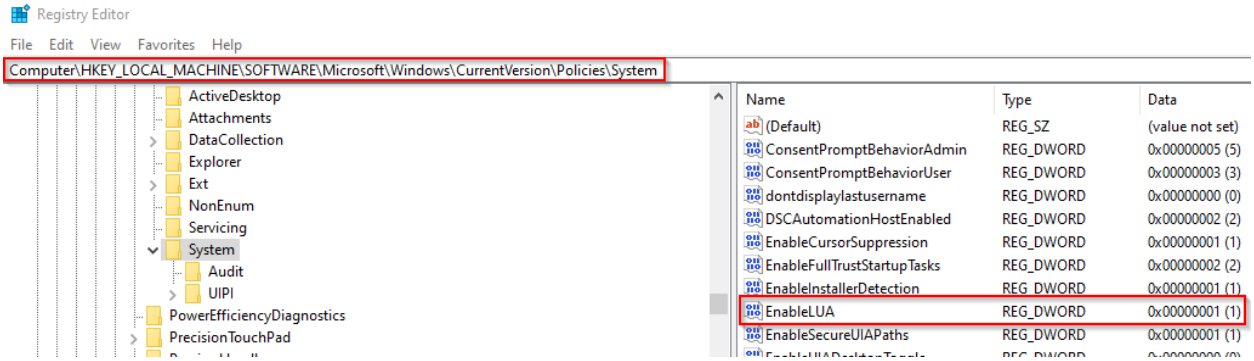
NB: You cannot access the SAM file on a live system using the regedit.exe. You can use Registry explorer.



User Account Control (UAC)

UAC allows normal users to perform administrative tasks without switching to the administrator account. This security feature can be turned OFF from Control Panel.

Registry Key Location:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System



EnableLUA=0 (UAC disabled)
EnableLUA=1(UAC enabled)

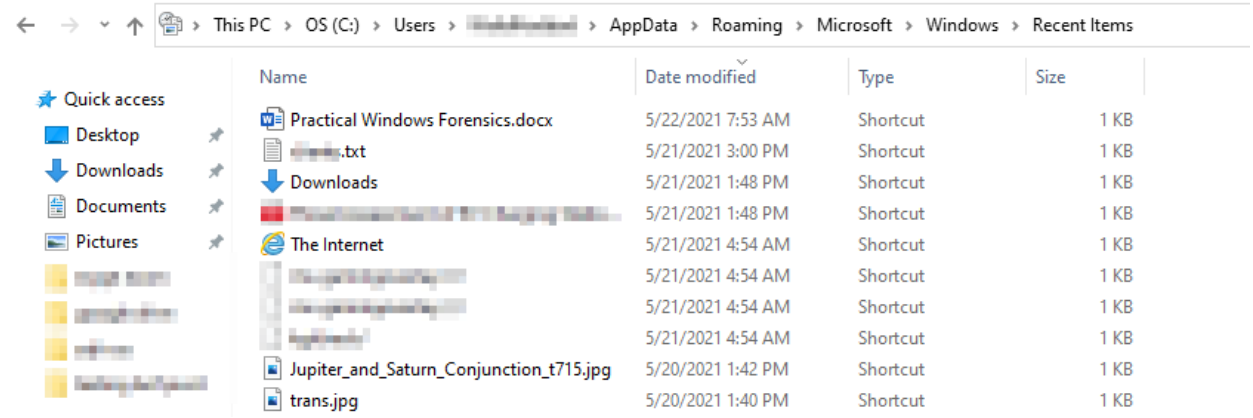
LNK files

A lnk file is an object that contains information that can be used to access another data object (Shortcuts).
Windows automatically create LNK (.lnk) files for a number of different actions that you perform on the system. LNK files contains a lot of data useful for investigation MAC times, original path of the file, size, serial number of volume, network volume share, mac address of host computer, etc…
Tool: Exiftool

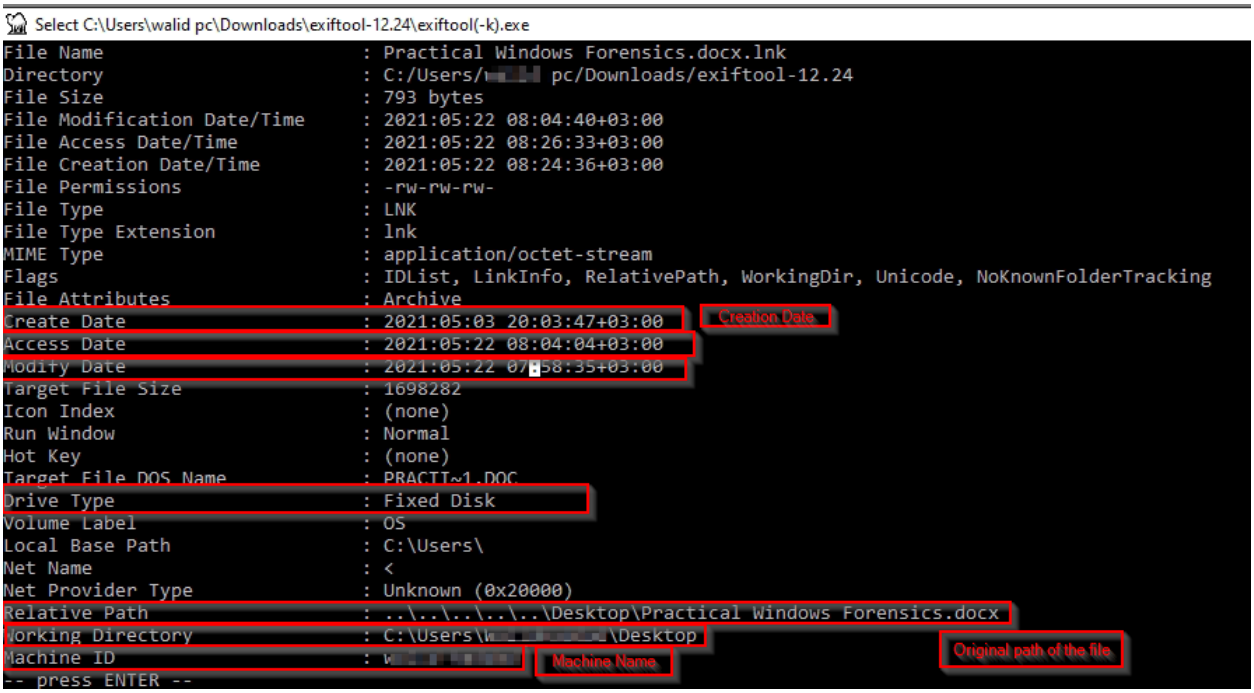
LNK files Location:
C:\{username}\AppData\Roaming\Microsoft\Windows\Recent items
C:\{username}\AppData\Roaming\Microsoft\Office\Recent

Registry Location: (ntuser.dat)
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

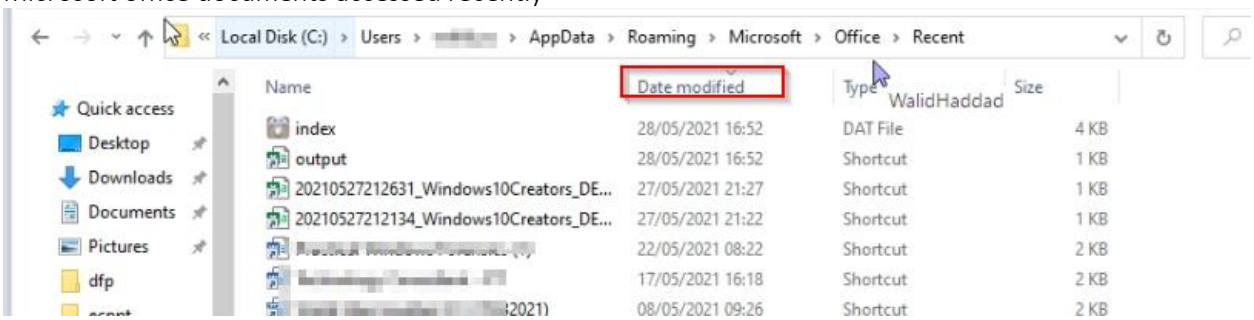
You can see the files accessed



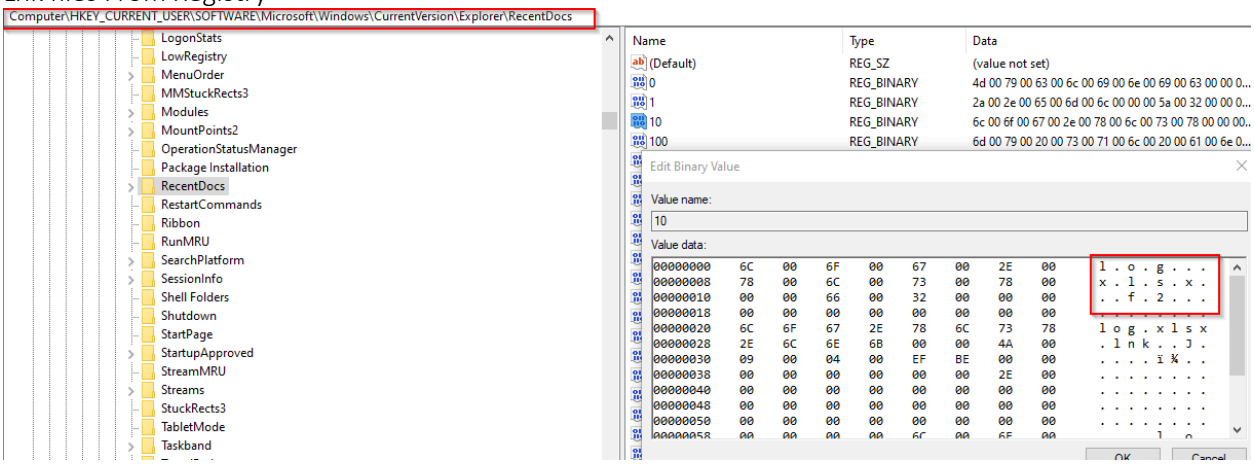
Let's feed the last file to exiftool (tool to analyse file metadata) to get more data about the file observed.



Microsoft office documents accessed recently

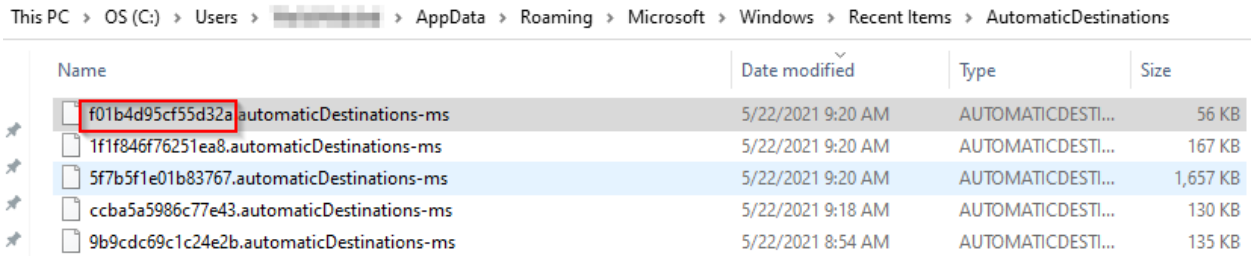


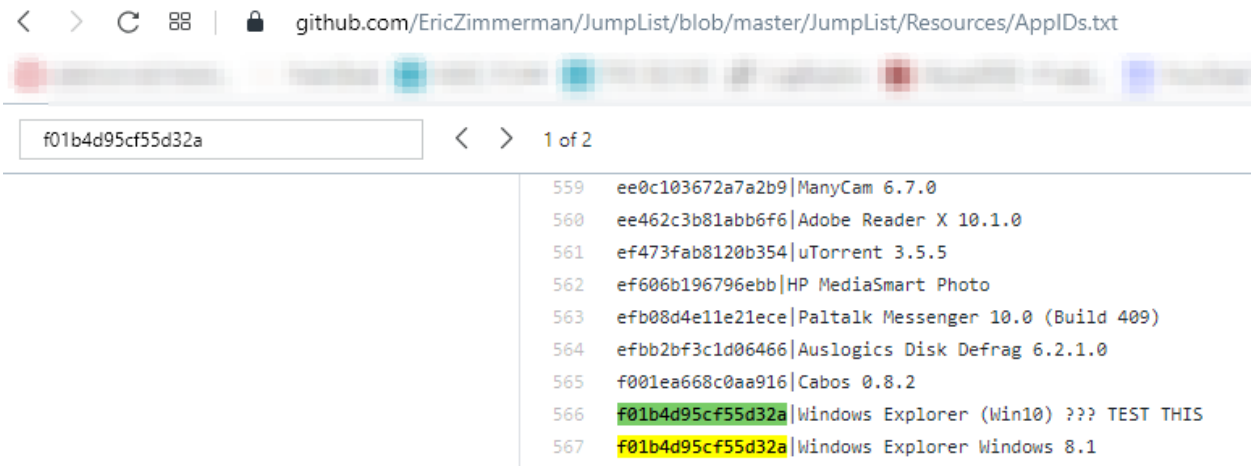
Lnk files From Registry



Jump lists

Jump lists, list files that have been previously accessed by an application.
From jump lists you could obtain tasks, links to recent files, frequently used files, links to pinned files, etc..





Prefetcher and Superfetch

Prefetcher and superfetche improves user experience by caching data that is frequently used and accessed on the system to make it faster for the user. As forensics investigators we can leverage these artifacts to show application execution (run from GUI based or command line interface). Prefetch files has the .pf extension and stores information such as executable file name, absolute path of the executable, number of times the program was run, the last time the application was run, list of DLLs used by the program.

NB:Note that prefetcher and superfetcher are not tied to a specific user
NB: if the same executable ran from different paths you will find two different prefetch files.
NB: Prefetch is sometimes disabled on servers and on SSD drives

Prefetch Location:
C:\Windows\Prefetch

Tool: WinPrefetchView

The items listed are the name of the executable followed by a dash and 8 random characters (hash of the file path on the system)

```
C:\Windows\Prefetch>dir
 Volume in drive C is OS
 Volume Serial Number is 9ECF-B7C0

 Directory of C:\Windows\Prefetch

05/24/2021  09:15 AM    <DIR>          .
05/24/2021  09:15 AM    <DIR>          ..
04/21/2021  12:06 PM            11,518 [redacted]
04/21/2021  12:11 PM             7,831 [redacted]
03/02/2021  01:55 AM           334,168 [redacted]
04/21/2021  11:42 AM           123,902 [redacted]
05/22/2021  12:53 PM           487,567 [redacted]
05/22/2021  12:53 PM         1,579,137 [redacted]
05/22/2021  12:53 PM         6,175,492 [redacted]
05/24/2021  09:06 AM           151,687 [redacted]
05/24/2021  09:06 AM         2,961,418 [redacted]
05/22/2021  12:53 PM           558,896 [redacted]
05/21/2021  09:22 AM            31,877 ANYDESK (2).EXE-F3059DE6.pf
05/22/2021  02:29 PM            29,776 ANYDESK.EXE-ED5DFCA7.pf
05/23/2021  12:52 PM            17,446 APPLICATIONFRAMEHOST.EXE-8CE9A1EE.pf
05/13/2021  12:24 AM            19,390 BACKGROUNDTASKHOST.EXE-7EF448C4.pf
05/24/2021  09:14 AM            18,827 BACKGROUNDTASKHOST.EXE-AD9A3486.pf
05/24/2021  04:56 AM            15,444 BRAVEUPDATE.EXE-71F336A7.pf
04/25/2021  01:18 PM            46,737 BURPSUITECOMMUNITY.EXE-1B1A271B.pf
05/23/2021  12:54 PM            10,060 cadrespri.7db
04/19/2021  09:24 PM            47,886 CALCULATOR.EXE-548AA30F.pf
05/24/2021  09:15 AM            17,960 CMD.EXE-0BD30981.pf
```

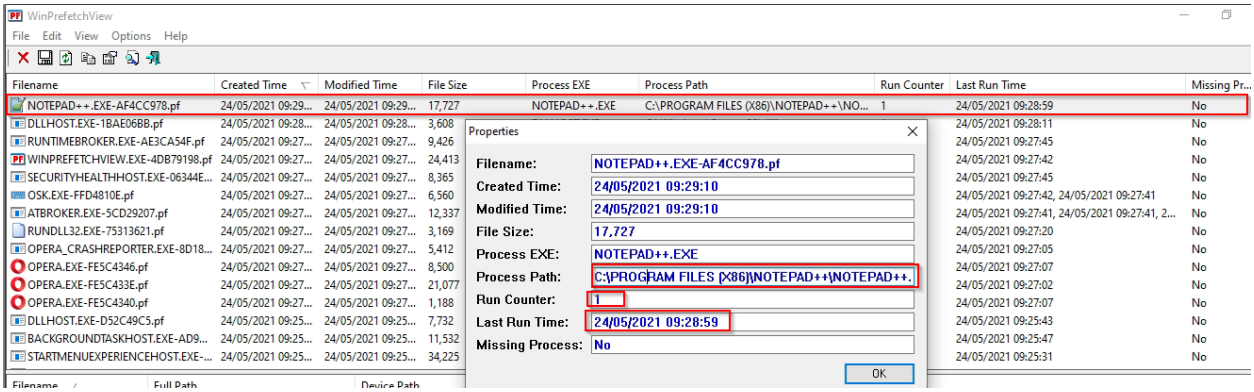
NB: observing multiple executables with different paths could be suspicious (for example cmd.exe with different paths)

Experiment 1 - Running NOTEPAD++

This experiment was performed to determine the effects on Prefetch when host-based applications are run on a Windows system. For this, i executed NOTEPAD.exe.

Results

When NOTEPAD++ was run, new entry was created beneath Prefetch folder “NOTEPAD++.EXE-AF4CC978.pf”



NB:The file create date indicate when the first time the application ran
NB:The last modified date indicate the last time the application ran

Windows Application Compatibility cache (Shimcache)

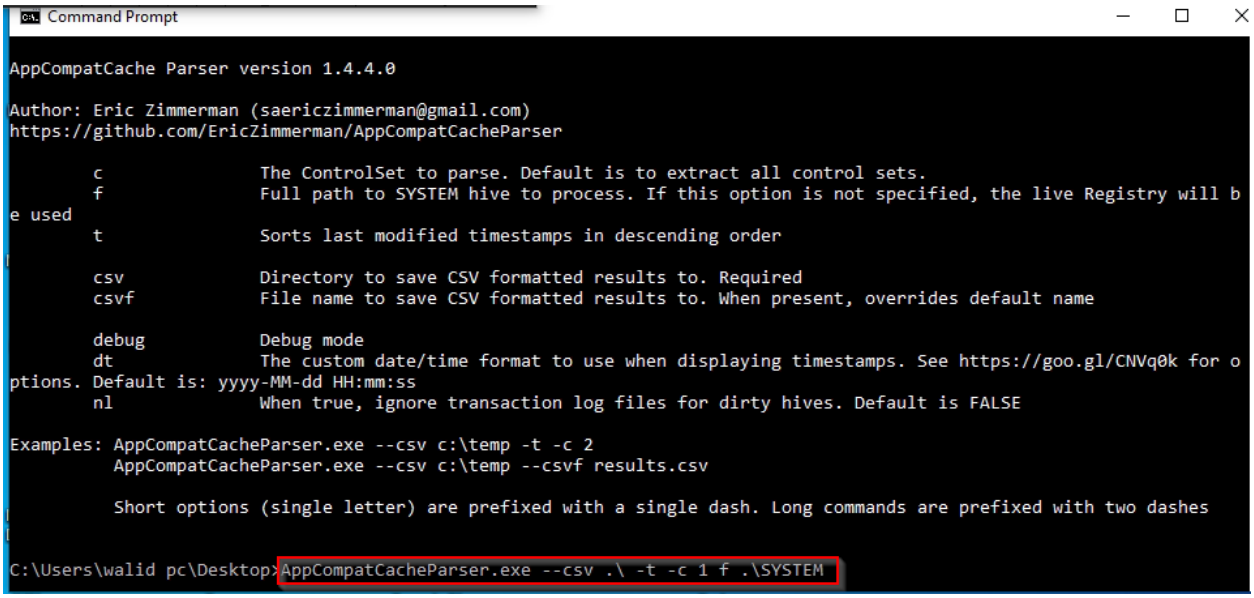
Windows Application Compatibility cache (Shimcache) can be used to determine execution of application execution on a windows system. It allows windows to execute the applications that has compatibility issues.Shicahce allow us to identify the excutable or scipt name and full path, last modification date, size,

Prefetch Location:
C:\Windows\AppCompat\Programs\Amcache.hve

Registry Key Location:
HKLM\System\CurrentControlSet\Control\Session Manager\AppCompatCache

NB: shimcache is only written to registry upon system shutdown. When condicting a Live Response You can use volatility plugin to read the shimcache from memory.

Tool: AppCompatCache Parser

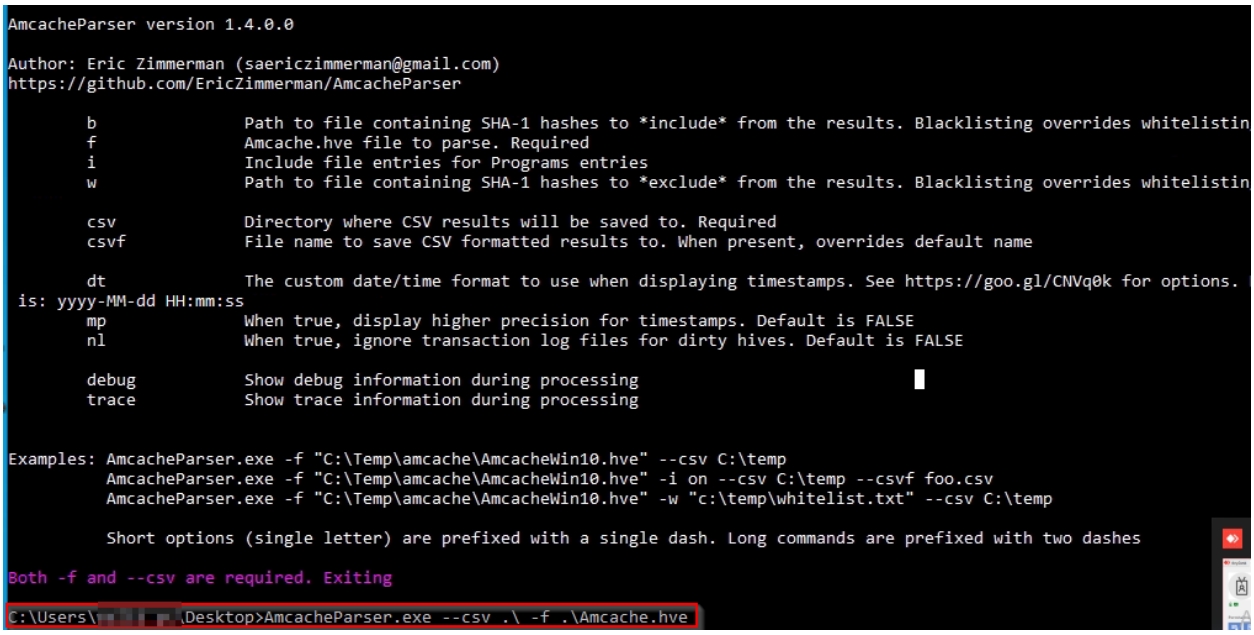


Output

1	Control	CacheE	Path	LastModifiedTi	Execute	Duplica	Source
932	1	52	C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.2104.10-0\MsMpEng.exe	5/9/2021 19:17	NA	FALSE	Live Registry
933	1	43	C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.339.303.0.exe	5/10/2021 1:51	NA	FALSE	Live Registry
934	1	35	C:\Users\WALIDP~1\AppData\Local\Temp\.opera\EED89729A050				lProgramsOpera\10428_	5/10/2021 15:36	NA	FALSE	Live Registry
935	1	36	C:\Users\walid pc\AppData\Local\Temp\.opera\EED89729A050\				ppDataLocalProgramsOpera\10428_2	5/10/2021 15:36	NA	FALSE	Live Registry
936	1	33	C:\Users\WALIDP~1\AppData\Local\Temp\.opera\EED89729A05				AppDataLocalProgramsOpera\10428_	5/10/2021 15:38	NA	FALSE	Live Registry
937	1	34	C:\Users\walid pc\AppData\Local\Temp\.opera\EED89729A050\				ppDataLocalProgramsOpera\10428_5	5/10/2021 15:38	NA	FALSE	Live Registry
938	1	26	C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.339.323.0.exe	5/10/2021 19:30	NA	FALSE	Live Registry
939	1	13	C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.339.373.0.exe	5/11/2021 19:34	NA	FALSE	Live Registry
940	1	12	C:\Program Files (x86)\Google\Update\Install\{20AFBA10-629F-4272-9533-92DD8A0A7EA9}\90.0.4430.212_90.0.4430.9	5/11/2021 22:59	NA	FALSE	Live Registry
941	1	10	C:\Program Files (x86)\Google\Update\Install\{20AFBA10-629F-4272-9533-92DD8A0A7EA9}\CR_C4A7B.tmp\setup.exe	5/11/2021 22:59	NA	FALSE	Live Registry
942	1	6	C:\WINDOWS\SoftwareDistribution\Download\Install\AM_Delta_Patch_1.339.443.0.exe	5/11/2021 23:32	NA	FALSE	Live Registry
943	1	5	C:\WINDOWS\SoftwareDistribution\Download\Install\Windows-KB890830-x64-V5.89.exe	5/11/2021 23:38	NA	FALSE	Live Registry
944	1	4	C:\WINDOWS\system32\MRT.exe	5/11/2021 23:38	NA	FALSE	Live Registry

AMcache

Tool: Amcache Parser



System Resource Utilization Monitor

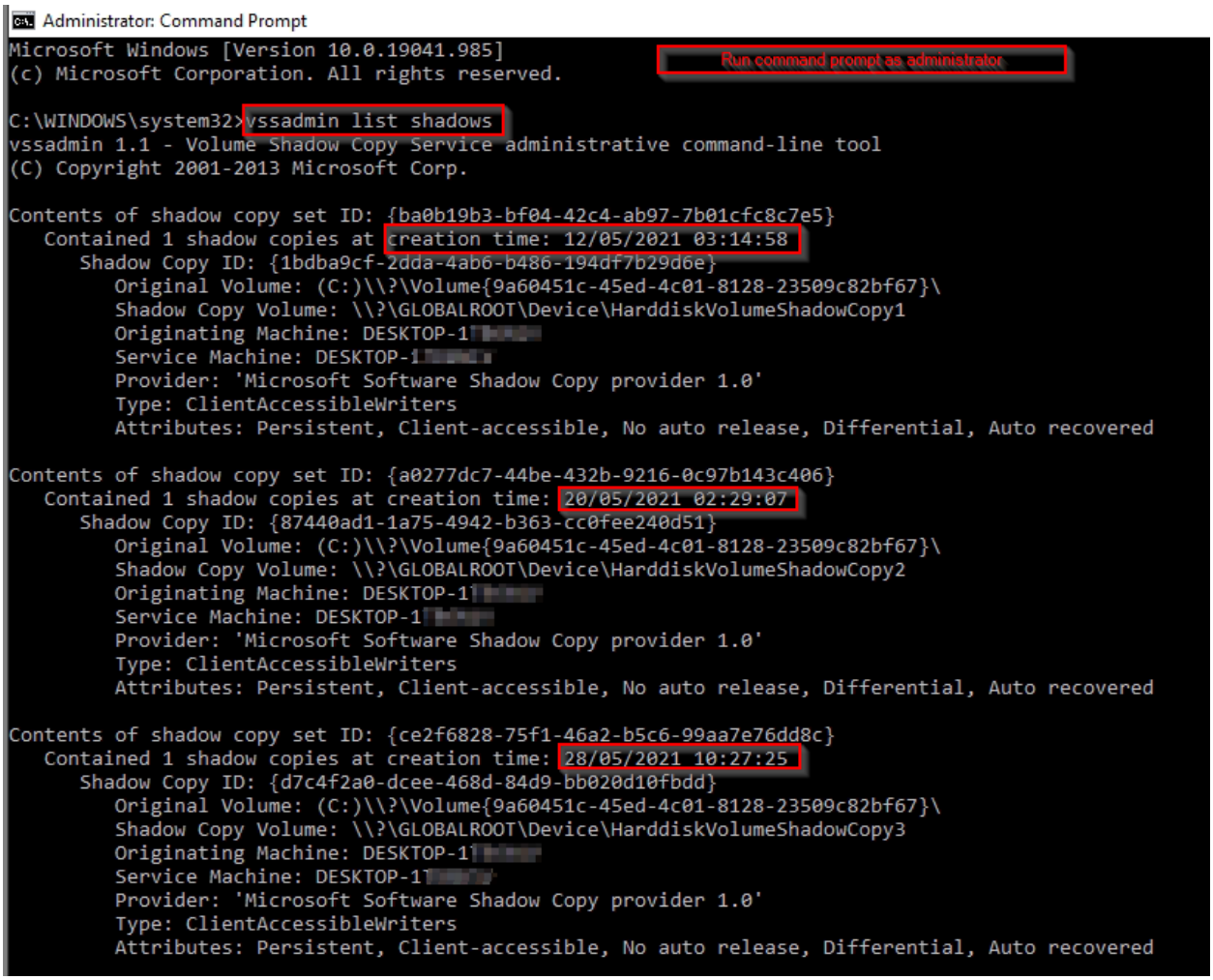
The Windows System Resource Usage Monitor (aka SRUM) contains a wealth of information about all the activities that occur on your machine. It keeps the names and paths of every application that executes on your system even the ones the attackers deleted. It was designed to track windows resource utilization.

Location: %systemroot%\Windows\System32\sru\srudb.dat
Tool: SRUM-dump.exe

NB: the srub.dat is locked by the system and it cannot be copied from a live system .It can be done with FTKimager or via vssadmin.

NB: data are written to srub.dat on system shutdown.

Get srudb.dat via vssadmin



Create a symbolic link

```
C:\Users\[redacted]>cd Desktop

C:\Users\[redacted]\Desktop>mklink /d output \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\
symbolic link created for output <<===>> \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\

C:\Users\[redacted]\Desktop>
C:\Users\[redacted]\Desktop>cd output

C:\Users\[redacted]\Desktop\output>dir
 Volume in drive C has no label.
 Volume Serial Number is E88E-CD3E

 Directory of C:\Users\[redacted]\Desktop\output

16/01/2018  22:34    <DIR>          Autodesk
28/11/2017  13:38    <DIR>          eclipse
16/04/2017  10:27           183,992 g2ldr
16/04/2017  10:27             8,192 g2ldr.mbr
20/08/2020  03:27    <DIR>          inetpub
04/11/2017  04:39    <DIR>          Intel
31/05/2018  12:59    <DIR>          My Web Sites
15/11/2020  12:23    <DIR>          netcat
10/08/2018  15:47    <DIR>          nt
07/12/2019  12:14    <DIR>          PerfLogs
22/01/2021  22:01    <DIR>          Program Files
19/01/2021  19:34    <DIR>          Program Files (x86)
02/01/2021  13:48    <DIR>          Python27
14/02/2019  16:57               445 sql.txt
20/08/2020  01:09    <DIR>          Users
27/02/2019  23:29    <DIR>          wamp
06/04/2018  09:07    <DIR>          win32-loader
12/05/2021  02:15    <DIR>          Windows
28/05/2020  11:55    <DIR>          xampp
               3 File(s)        192,629 bytes
              16 Dir(s)   6,631,534,592 bytes free
```

copy the SRUDB.dat

```
 Directory of C:\Users\[redacted]\Desktop\output\Windows\System32\sru

12/05/2021  03:11    <DIR>          .
12/05/2021  03:11    <DIR>          ..
12/05/2021  03:13             8,192 SRU.chk
12/05/2021  03:13            65,536 SRU.log
12/05/2021  03:11            65,536 SRU13764.log
12/05/2021  03:11            65,536 SRU13765.log
12/05/2021  03:11            65,536 SRU13766.log
12/05/2021  03:11            65,536 SRU13767.log
12/05/2021  03:11            65,536 SRU13768.log
12/05/2021  03:11            65,536 SRU13769.log
12/05/2021  03:11            65,536 SRU1376A.log
12/05/2021  03:13       136,134,656 SRUDB.dat
12/05/2021  03:13            32,768 SRUDB.jfm
15/01/2021  12:32            65,536 SRUres00001.jrs
15/01/2021  12:34            65,536 SRUres00002.jrs
12/05/2021  03:11            65,536 SRUtmp.log
              14 File(s)    136,896,512 bytes
               2 Dir(s)   6,631,534,592 bytes free

C:\Users\[redacted]\Desktop\output\Windows\System32\sru>copy SRUDB.dat \users\[redacted]\Desktop\SRUDB.dat
The syntax of the command is incorrect.

C:\Users\[redacted]\Desktop\output\Windows\System32\sru>copy SRUDB.dat "\users\[redacted]\Desktop\SRUDB.dat"
        1 file(s) copied.
```

Load SRUDB.dat using SRUM-dump.exe

```
C:\Users\[redacted]\Desktop\srum-dump-master\srum-dump-master>srum_dump2.exe -i ..\..\SRUDB.dat -o output.xlsx -t SRUM_TEMPLATE2.xlsx
Processing 574418 records across 11 tables

Now dumping table ruDbCheckpoint containing 0 rows
While you wait, did you know ...
 Did you know SANS Automating Infosec with Python SEC573 teaches you to develop Forensics and Incident Response tools?

|XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX| 100.00% FINISHED

Now dumping table Energy Estimation Provider containing 90293 rows
While you wait, did you know ...
 To learn how SRUM and other artifacts can enhance your forensics investigations check out SANS Windows Forensic Analysis FOR500.
```

Output: Network Data Usage. you can see the last application executions on the system with the user SID associated, in addition to other details like data sent and received.

	A	B	C	D
1	SRUM EN	SRUM ENTRY CREATION	Application	User SID
2	176647	2021-05-12 0:10:00	\device\harddiskvolume3\users\walid pc\appdata\local\programs\opera\75.0.3969.218\opera.exe	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
3	176648	2021-05-12 0:10:00	Dnscache	S-1-5-20 (NT Authority)
4	176649	2021-05-12 0:10:00	\device\harddiskvolume3\program files (x86)\microsoft\edge\application\msedge.exe	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
5	176650	2021-05-12 0:10:00	\device\harddiskvolume3\program files (x86)\google\chrome\application\chrome.exe	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
6	176651	2021-05-12 0:10:00	\device\harddiskvolume3\program files (x86)\winscp\winscp.exe	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
7	176652	2021-05-12 0:10:00		
8	176653	2021-05-12 0:10:00	DiagTrack	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
9	176654	2021-05-12 0:10:00	System	S-1-5-18 (Local System)
10	176655	2021-05-12 0:10:00	\device\harddiskvolume3\users\walid pc\appdata\local\microsoft\onedrive\21.062.0328.0001\file	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
11	176656	2021-05-12 0:10:00	WpnService	S-1-5-18 (Local System)
12	176657	2021-05-12 0:10:00	\device\harddiskvolume3\windows\system32\speech_onecore\common\speechmodeldownload.	S-1-5-20 (NT Authority)
13	176658	2021-05-12 0:10:00	microsoft.windowscommunicationsapps_16005.13426.20920.0_x64__8wekyb3d8bbwe	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
14	176659	2021-05-12 0:10:00	wuauserv	S-1-5-18 (Local System)
15	176660	2021-05-12 0:10:00	wuauserv	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
16	176661	2021-05-12 0:10:00	\device\harddiskvolume3\program files (x86)\microsoft office\root\office16\sdxhelper.exe	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
17	176662	2021-05-12 0:10:00	DoSvc	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
18	176663	2021-05-12 0:10:00	SSDPSRV	S-1-5-19 (NT Authority)
19	176664	2021-05-12 0:10:00	BITS	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
20	176665	2021-05-12 0:10:00	BITS	S-1-5-18 (Local System)
21	176666	2021-05-12 0:10:00	CryptSvc	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)
22	176667	2021-05-12 0:10:00	\device\harddiskvolume3\program files (x86)\microsoft office\root\office16\excel.exe	S-1-5-21-3026893380-3979506429-968727220-1001 (unknown)

To convert the SID to the actual user

```
C:\Users\w      :\Desktop\srum-dump-master\srum-dump-master>wmic useraccount get name,sid
Name                SID
Administrator       S-1-5-21-3026893380-3979506429-968727220-500
DefaultAccount      S-1-5-21-3026893380-3979506429-968727220-503
Guest               S-1-5-21-3026893380-3979506429-968727220-501
LANGUARD_12_USER    S-1-5-21-3026893380-3979506429-968727220-1006
                    S-1-5-21-3026893380-3979506429-968727220-1001
WDAGUtilityAccount  S-1-5-21-3026893380-3979506429-968727220-504
```

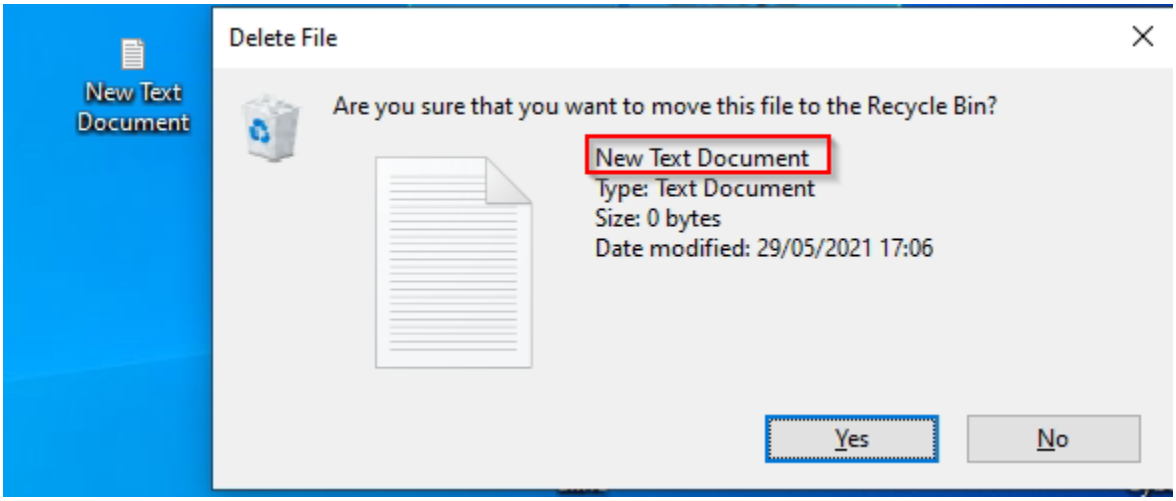
Recycle Bin

The recycle bin is located in the root of the OS drive. Called $Recycle.bin (hidden).
Each deleted file will result in 2 files placed within the $Recycle.bin. Both files are renamed with random characters value starting with $I and $R.

$Ixxxxxx contain meta data specific to that file (file name, PATH prior to deletion, size, time deleted.
$Rxxxxxx contain actual file contents .

Tool: $I Parse

Experiment 1 – Deleting a file from desktop



$Recycle.Bin location

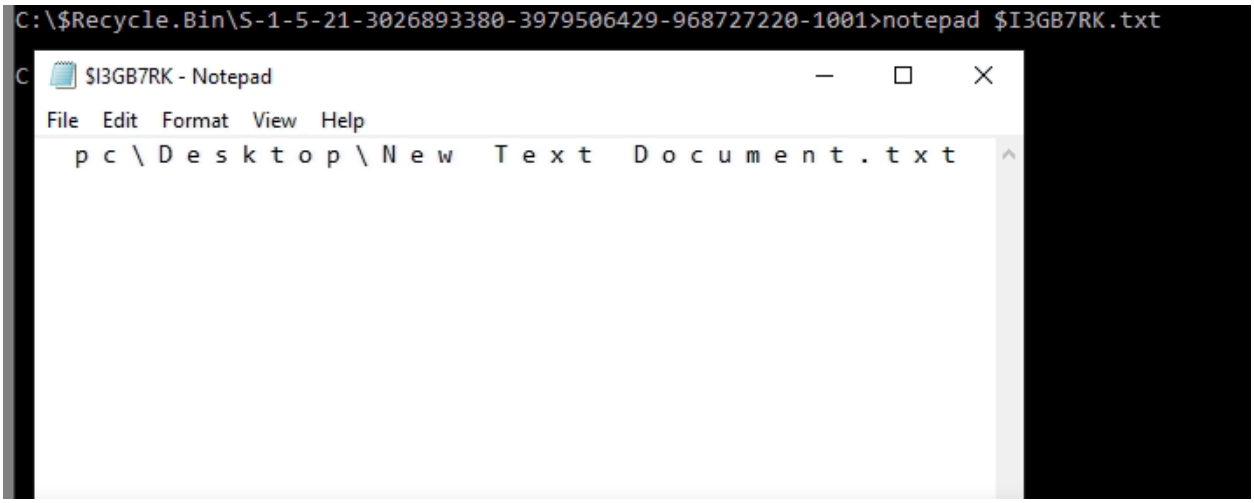
```
C:\>dir a
 Volume in drive C has no label.
 Volume Serial Number is E88E-CD3E

 Directory of C:\

File Not Found

C:\>dir /a
 Volume in drive C has no label.
 Volume Serial Number is E88E-CD3E

 Directory of C:\

08/06/2018  13:47    <DIR>          $AV_ASW
08/11/2017  17:32    <DIR>          $Recycle.Bin
30/07/2020  03:02    <DIR>          $WinREAgent
```

Results

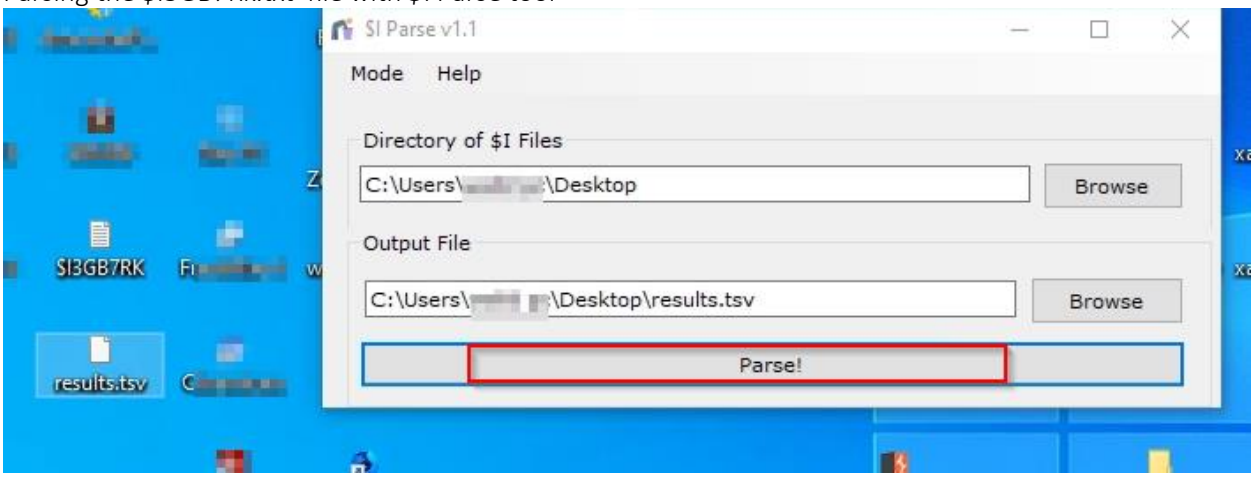
2 new files were created in the $Recycle.Bin folder

```
C:\$Recycle.Bin\S-1-5-21-3026893380-3979506429-968727220-1001>dir
 Volume in drive C has no label.
 Volume Serial Number is E88E-CD3E

 Directory of C:\$Recycle.Bin\S-1-5-21-3026893380-3979506429-968727220-1001

27/05/2021  21:26               216 $I36EVG2.csv
29/05/2021  17:10               124 $I3GB7RK.txt
08/05/2021  12:09               178 $I40SXHE.pdf
20/05/2021  09:40               112 $I5CUX6J
29/05/2021  17:06               124 $I7B8JUU.txt
29/04/2021  18:52               116 $I7RO4K8.rar
19/05/2021  20:23               150 $IDELXHL.zip
20/05/2021  09:34               120 $IGHNDQE
28/04/2021  20:38               112 $IKB4N9D.pdf
27/05/2021  21:22               216 $IKJT4UH.csv
13/06/2018  21:19               104 $IKQ3LDD
28/04/2021  20:38               140 $INAXX30.ics
20/05/2021  09:40               120 $IOS0H0H.zip
28/04/2021  20:38               132 $IQLX073.ics
11/05/2021  07:05               166 $IRR8L4Z.pdf
27/05/2021  21:38               216 $IT8A03E.csv
20/05/2021  09:34               128 $IVRGALG.zip
28/05/2021  17:33               110 $IZ53D4K.PNG
27/05/2021  21:22           132,601 $R36EVG2.csv
```

Opening the $I3GB7Rk.txt we can see the original path and file name of the file deleted



Parsing the $I3GB7Rk.txt file with $I Parse tool



Results

	A	B	C	D
1	Deleted Date	File Name	File Size (I	Version
2	05/29/2021 14:10:25 UTC	C:\Users\ \Desktop\New Text Document.txt	0	Windows 10
3				
4				

RDP Cache

When you use the mstsc RDP client on your windows the cache is stored in a specific folder “RDP Cache”. The purpose of this cache is to improve performance by caching sections of the screen .

RDP Cache Location: C:\Users\{username}\AppData\Local\Microsoft\Terminal Server Client\Cache

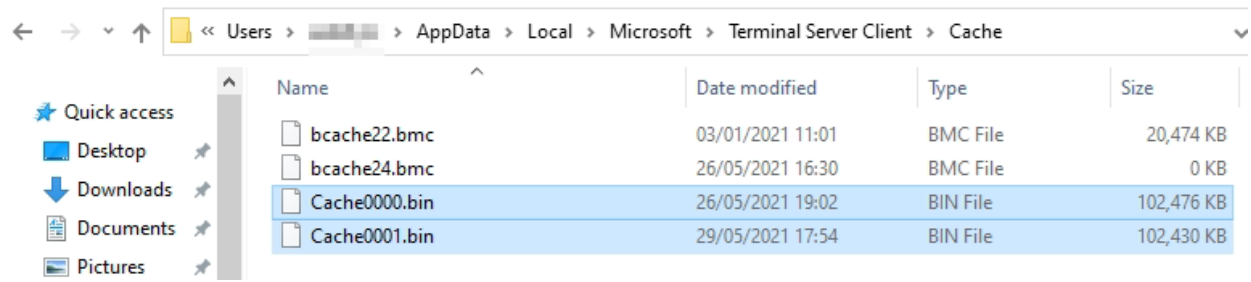
Tool:bmc-tools

Experiment 1 – Accessing another device using RDP

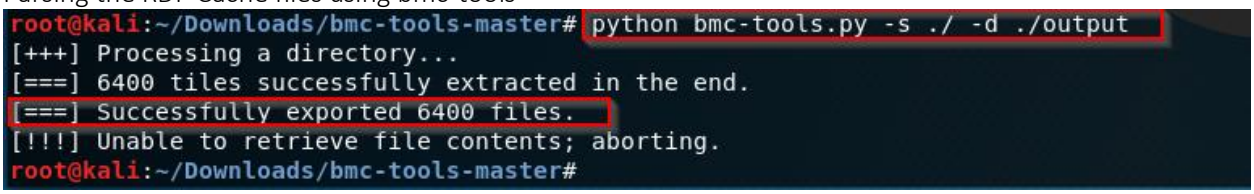
In order to perform this test, I have accessed another pc on the network using RDP. After that I copied the Cache0000.bin and Cache0001.bin to my Kali linux and used the bmc-tools RDP Cache parser to extract the data from the RDP Cache

Results

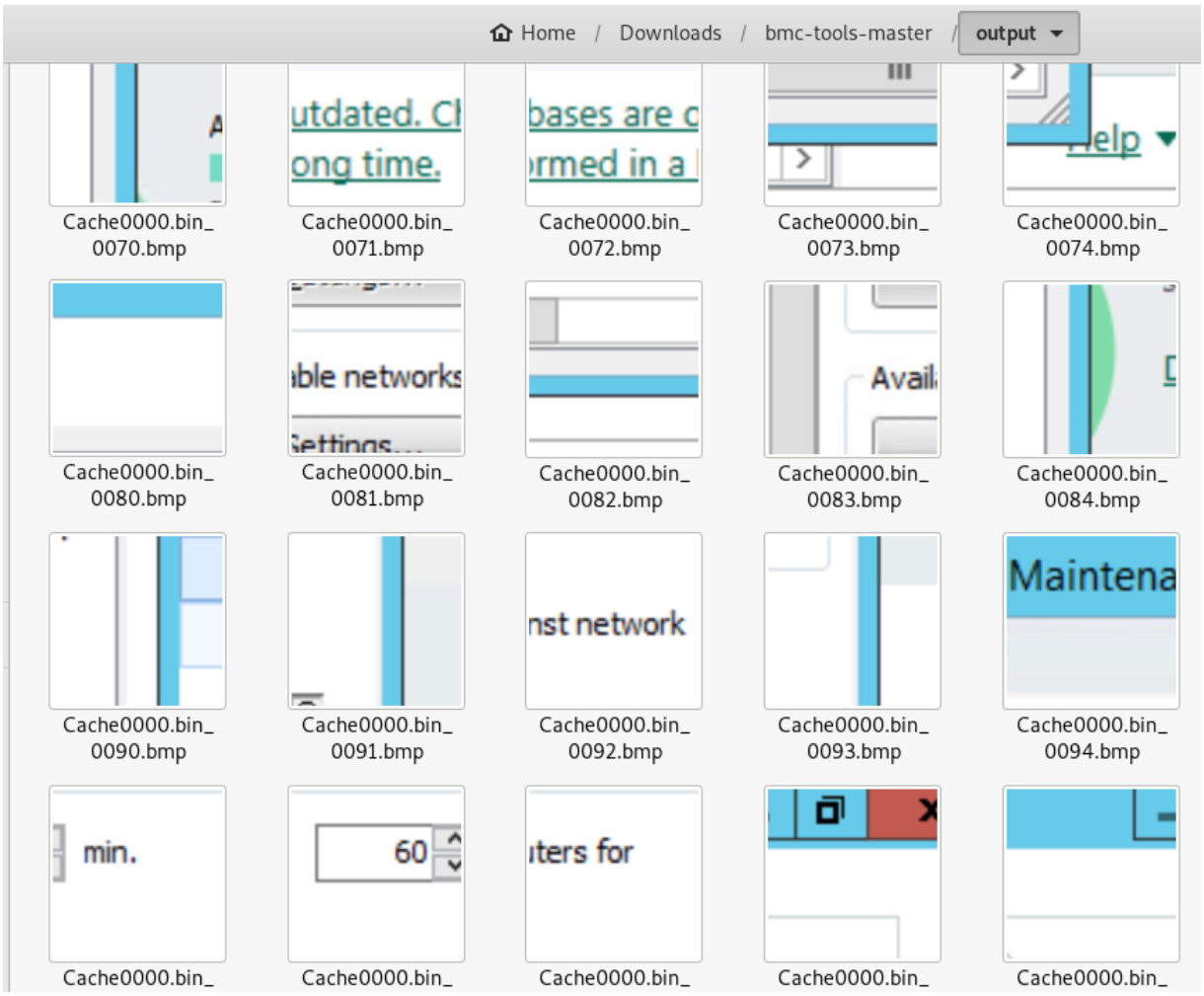
RDP Cache location



Parsing the RDP Cache files using bmc-tools



Photos resulted from the parsing of the RDP Cache using bmc-tools



Volume ShadowCopy Service (VSS)

Volume ShadowCopy Service (VSS) is a windows feature used to allow volume backup during the running of the system.
This windows feature allows users to roll back to a previous windows state. This will be useful to find information that was written in the past.
Snapshots can be created automatically when windows updates are installed, driver/software installation, or via a scheduled task.
Using the VSS we can recover files, registry keys, etc..

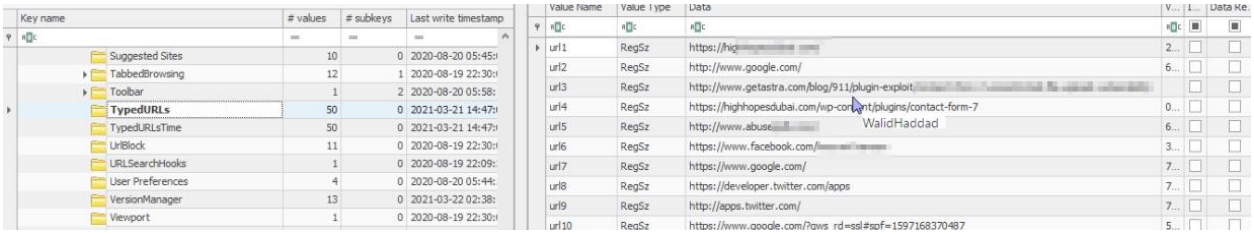
Tools: VSSAdmin and Mklink

To list the shadows copies on a system ; command: **vssadmin list shadows /for=c:**

IE typed URLs

All typed URLs by the user are stored in a particular registry key. This information can be used to investigate what URLs and websites were visited by the user.

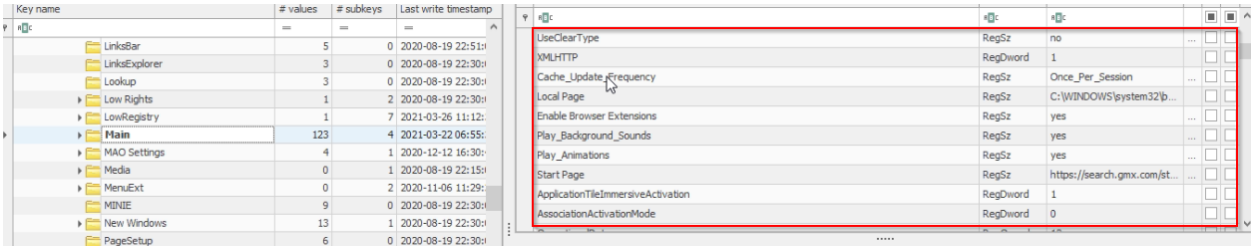
Registry Key Location:
NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLs
NTUSER.DAT\Software\Microsoft\Internet Explorer\TypedURLsTime



IE Browser Settings

To check Internet explorer settings.

Registry Key Location:
NTUSER.DAT\Software\Microsoft\Internet Explorer\Main



Logs Analysis

Windows Events logs Analysis

After a compromise, the first thing investigators will do is review the log files. Windows events logs contains a lot of information about system and users activities. Event logs can provide a lot of information for investigators like login attempts ,system restart and other system events.

Windows Events Logs Location : \%SystemRoot%\System32\winevt\Logs*.evtx

Main Event Logs

System Log

The System Log records events that are logged by the Operating System (eg. data about hardware changes, device drivers, system changes, and all activities related to the machine).

Security Log

The Security Log contains Logon/Logoff activity and other activities related to windows security. (useful to detect and investigate attempted and/or successful unauthorized activity).

Application Log

The Application Log records application related events. It records the errors that occur in an application, informational events, and warnings from the software applications. (Useful to troubleshoot any software problem that prevents it from either logging in or functioning properly).

Useful events for forensics analysis

Event ID (Vista/7/8/2008/2012)	Description	Log Name
4624	Successful Logon	Security
4625	Failed Login	Security
4648	A logon was attempted using explicit credentials	
4776	Successful /Failed Account Authentication	Security
4720	A user account was created	Security
4723	An user attempted to change an account's password	
4732	A member was added to a security-enabled local group	Security
4728	A member was added to a security-enabled global group	Security
4769	A service ticket was requested by a user account for a specified resource	
4771	Depending on the reason for a failed Kerberos logon, either Event ID 4768 or Event ID 4771 will be created	
4776	While less common in a domain environment, NTLM may still be used for Authentication	
5140	A network share object was accessed	
7030	Service Creation Errors	System
7040	The start type of the IPSEC Services service was changed from disabled to auto start.	System
7045	A service was installed in the system	
106	Scheduled Task Created	
4698	A scheduled task was created.	
6006	The event log service was stopped	
5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network	
5152	The Windows Filtering Platform blocked a packet	
5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections	
5156	The Windows Filtering Platform has allowed a connection	
5157	The Windows Filtering Platform has blocked a connection	
5158	The Windows Filtering Platform has permitted a bind to a local port	
5159	The Windows Filtering Platform has blocked a bind to a local port	
1102	Clear Event log	
2003	Disable firewall	

Logon Type Codes

One of the useful information that Successful/Failed Logon event provide is how the user/process tried to logon (Logon Type) . Windows display this information as a number. The list below explain the logon type and their codes:

Logon type	Logon title	Description
2	Interactive	A user logged on to this computer.
3	Network	A user or computer logged on to this computer from the network.
4	Batch	Batch logon type is used by batch servers, where processes may be executing on behalf of a user without their direct intervention.
5	Service	A service was started by the Service Control Manager.
7	Unlock	This workstation was unlocked.
8	NetworkCleartext	A user logged on to this computer from the network. The user's password was passed to the authentication package in its unhashed form. The built-in authentication packages all hash credentials before sending them across the network. The credentials do not traverse the network in plaintext (also called cleartext).

Useful tools:

Log Parser

Tool that provides universal query access to text-based data such as log files, XML files and CSV files, as well as key data sources on the Windows operating system such as the Event Log, the Registry, the file system, and Active Directory.
https://www.microsoft.com/en-us/download/details.aspx?id=24659

python-evtx

Python parser for recent Windows Event Log files (.evtx).

EvtxParser

A parser framework for Microsoft Windows Vista event log files in their native binary (.evtx) format.

Interesting logs to looks at:

- Event Log start/stop. Event ID's 6005 and 6006 represent the Event Log service starting and stopping, respectively. Individuals looking to hide their actions may stop the Event Log service, but the most likely cause of these events is a system shutdown.

- System shutdown/restart. Event ID 6008 indicates an unexpected shutdown, and 6009 the associated restart. Event ID 6009 is generally preceded by a 6006 event to stop the Event Log service. 1074 is used to show the process which initiated a shutdown, and 1076 (on Windows 2003) shows the reason provided for the shutdown.

- Event ID 26 in the system log may indicate a successful buffer overflow attempt. Event ID 1001 indicates a memory dump was performed and will list the location of the dump file.

- Service Pack update/installation. Showing a particular patch was installed at a particular time can be useful in refuting claims of infection or exploit by malware. Event ID 19 shows successful installation of an automated patch. Event ID 4377 shows specific package hotfix installations. The initial Windows installation with build number should be one of the first listed events (assuming log recycling has not occurred) with an event ID 60054.

- Event ID 100 indicates a failure to authenticate against a known account, and a series of these events may indicate password guessing or a brute force tool use. Failures to log on are one of the best indicators of password guessing or bruteforce attacks on a system. Failed attempts are logged based on the reason for failure: wrong password or user name (Event ID 529; may be a hacking attempt), account is disabled or expired or locked (Event IDs 531 and 532 and 539, respectively; could be password sharing or disgruntled former employees), or the user tries to log in to a resource to which he or she is not permitted access (Event ID 533; possible unauthorized access).

- Unfortunately, failed log-ons also occur in large numbers for legitimate reasons. Users forget passwords, automated tools are misconfigured, and Caps Lock keys are accidentally depressed, making it difficult to separate out malicious log-on failures. In generally, malicious failures will be more numerous in nature, will be closer together (if an automated tool is used), and may show failures to multiple account names (from the same source machine).

- Alteration of machine information. Event ID 6011 denotes a system name change. Investigations into a particular machine name that does not match with existing information should look for this ID to indicate a potential change of name after an event occurred.

- Successful Log-on/Log-off Events. Successful log-on events are used to show who performed a particular action. Interactive log-on events are characterized by Event ID 528, with a subcategory defining the log-on type.

- Remote Desktop Connection .Remote Desktop Connection events can be bounded by connection types other than log-offs as well. Disconnects leave the user logged in but detach the actual terminal machine from the server. Reconnects re-attach and are accompanied by log-on events.

The disconnection is an Event ID of 683 and the subsequent reconnection a 682.

- Changing of the audit policy .Changing of the audit policy (specifically removing the auditing of certain events) is indicative of a hacking attempt or root kit installation. Event ID 612 is a change of audit policy. Any change from prior 612 Event ID entries that show a removal (minus sign) of policy that was previously present (plus sign) should be questioned.

- Successful or Failed Object Access. Auditing for specific NTFS files and folders can be turned on using the Advanced button on the Security tab within the particular object's properties. Enabling auditing on an object can log anything from attempted reads of that object to successful deletion of that object. If this level of auditing is enabled, it can show when a given entity was accessed and by whom and when a file or folder was changed or deleted, or highlight unauthorized access attempts on key objects.

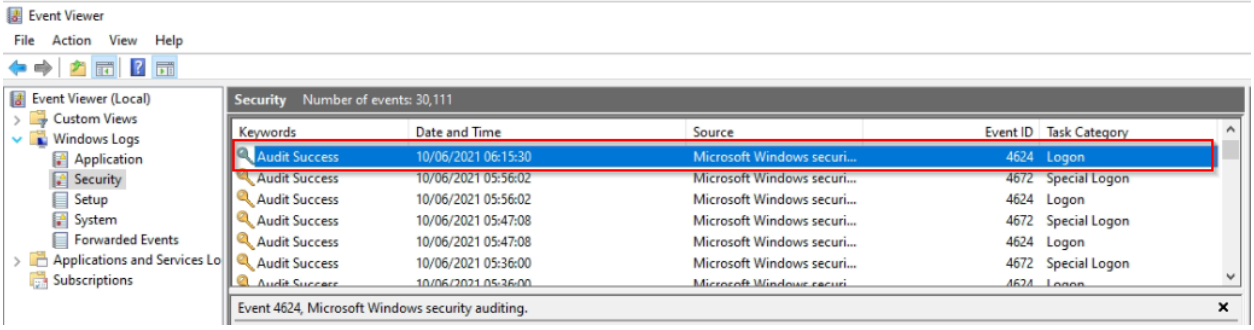
- Account Change. Changes to an individuals account settings may be the result of malicious activity. Event ID 642 indicates an account settings change. Event ID 628, the most common follow-up event, indicates that the password and a particular account were changed.

- Log Clearing. An Event ID of 517 indicates the security event log was cleared. There is no corresponding event for clearing the application or system logs. Clearing the security log is almost never done without saving the old log to a file for legitimate reasons, but may indicate an intruder covering his or her tracks. A search for EVT files or a text search for common Event ID wording on the drive may turn up old Event Viewer details if the log was saved before deletion

Investigating an unplanned system restart

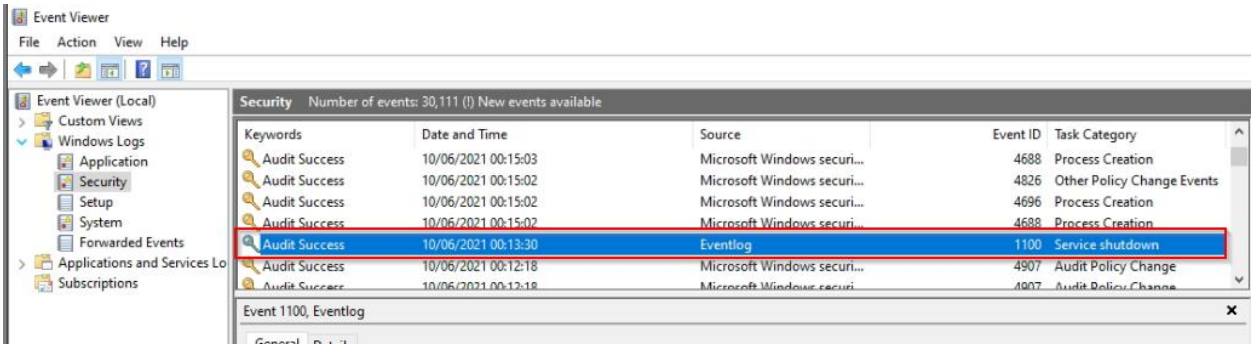
In this case scenario I will investigate an unplanned restart for an unknown reason to understand the reason behind the restart. The screenshots below shows the steps performed to investigate this incident.

At 6:15:30 AM we logged in to my device that was restarted for an unknown reason.

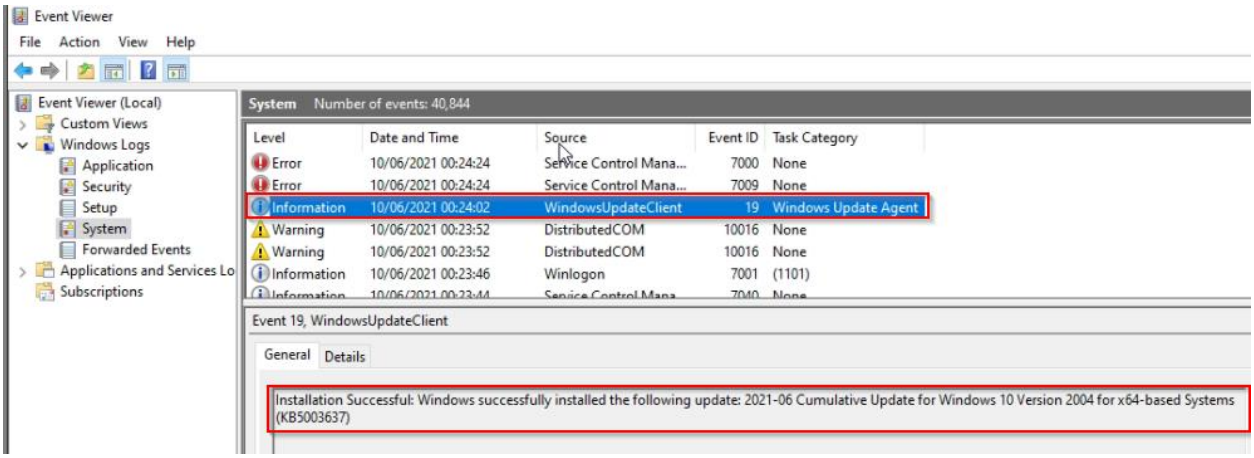


Now we know that we should be looking in the logs from 10/6/2021 06:15:30 backwards to the previous day.
Went back in the time line , still in the security logs to find more information and found the "The event

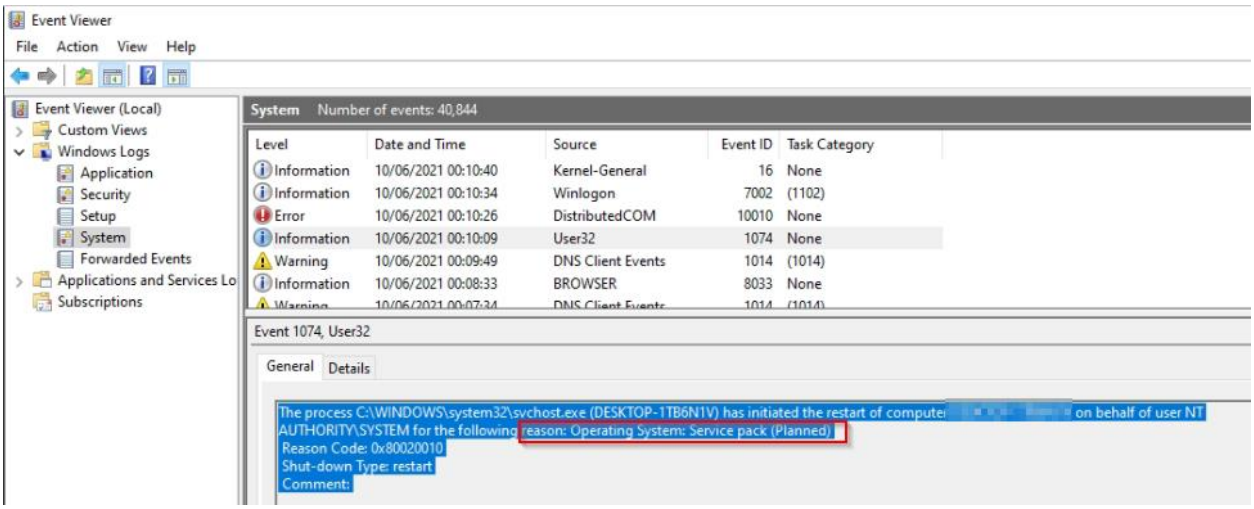
logging service has shut down" event. This could indicate the system restarting and killing services (or could indicate an attacker is stopping the logging). Now we have an idea on when the system could be restarted.



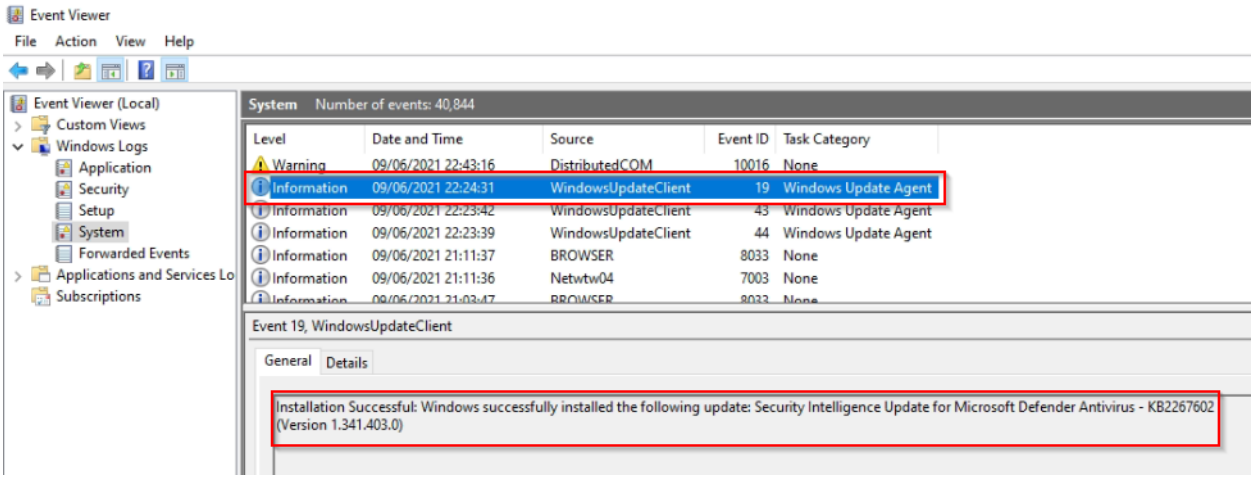
Switching the system events. While going back to the time of shutdown (10/06/2021 00:13:30) we found this event which indicate a successful installation of a system update.(we still need to understand what triggered the system restart at 06:15:30).



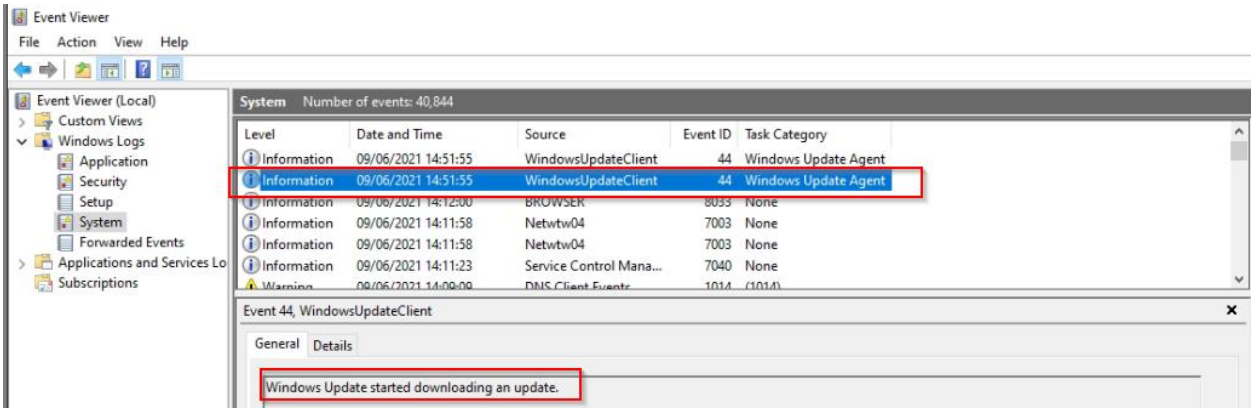
Minutes before the restart we found this event which indicated without any doubt the reason behind the system restart.



System update was running since 09/06/2021 22:24:31 Additional updates were been installed post system restart.



Windows update started downloading the files on 09/06/2021 14:51:55



Investigating RDP connection Event Logs (Lateral movement)

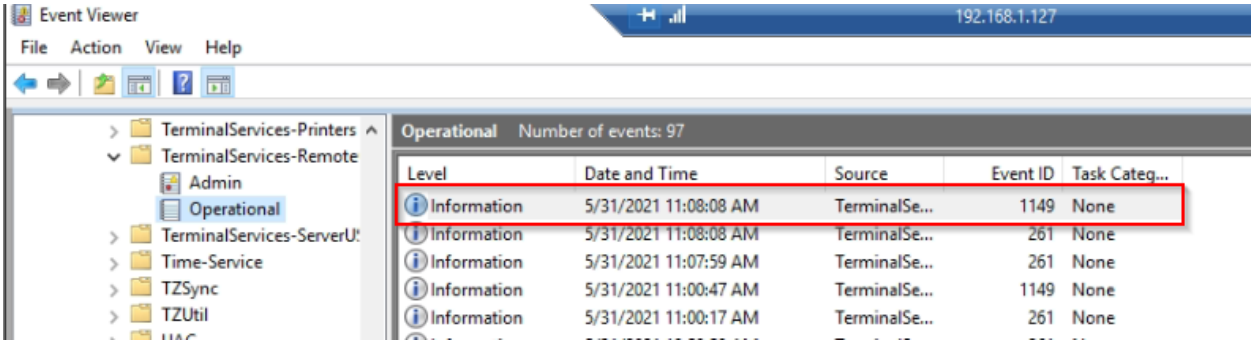
When a user remotely connects to the Remote desktop, a whole number of events appear in the Windows Event Viewer. There are several different logs where you can find the information about Remote Desktop Connections. We'll look at the logs and events on the main stages of an RDP connection that may be of interest (Network Connection, Authentication, logon, Session Disconnect/Reconnect, Logoff).

Experiment 1 – Accessing another pc on the network using RDP and logging on

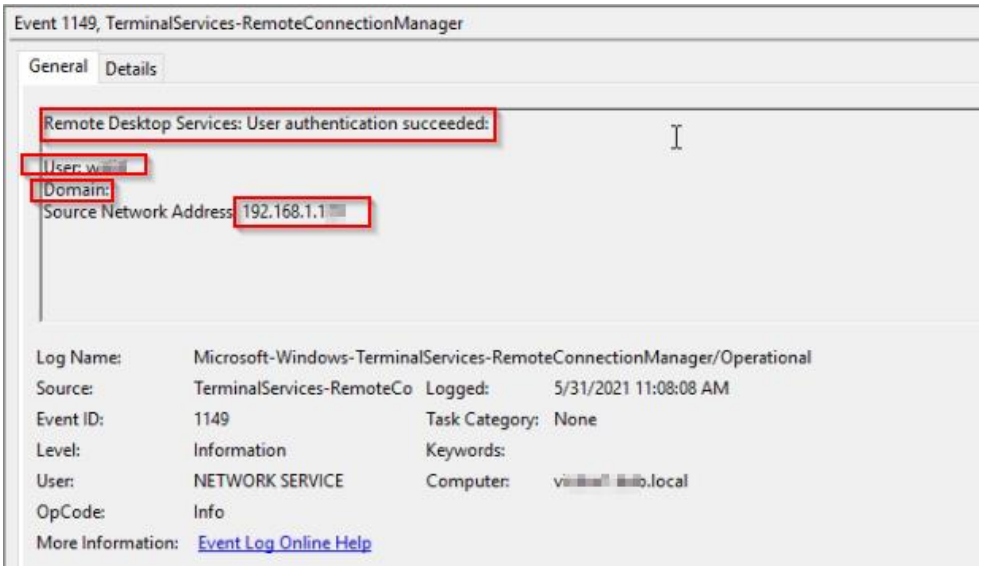
After a successful established connection to the remote server using RDP, The below logs were observed .

NB: If you are performing an investigation on a pc and you want to check all remote connections that were made to this device using RDP you can apply a filer with event ID 1149.

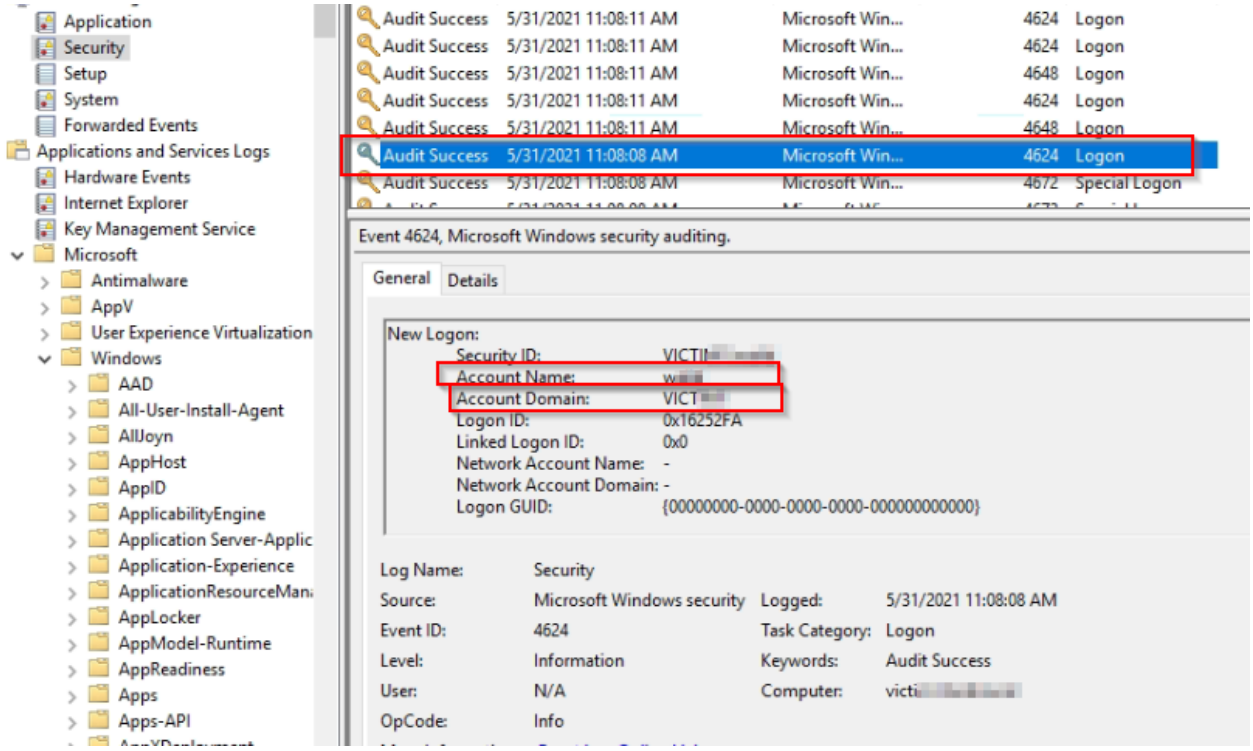
NETWORK Connection Event Viewer > Applications and Services Logs > Microsoft > Windows > TerminalServices-RemoteConnectionManager. Event ID 1149 (Remote Desktop Services: User authentication succeeded)



The logs details provide username, domain, and the source IP

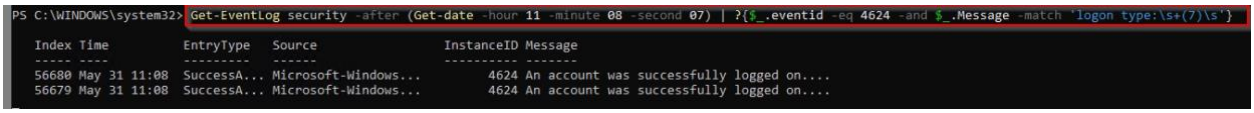


Authentication The authentication log shows whether the RDP user has been successfully authenticated on the server or not. The log is located in **Windows > Security.** If the authentication was successful you would see EventID 4624, if the authentication failed you would see EventID 4625. Also pay attention to the LogonType value. If the RDP service has been used to create a new session during logon, LogonType=10. If the LogonType=7, it means that a user has reconnected to the existing RDP session.

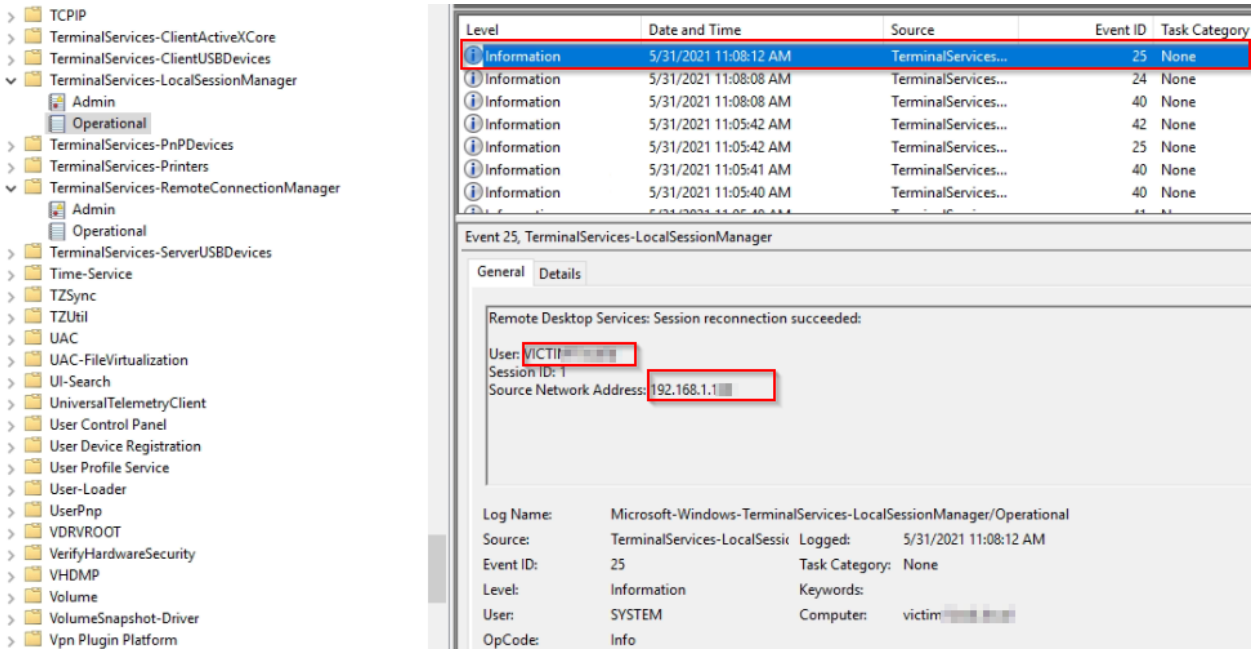


You can find the user name in the event description in the Account Name field, a computer name – in Workstation Name, and an IP address – in Source Network Address, , Logon type, etc...

This can be done also using PowerShell
Command: Get-EventLog security -after (Get-date -hour 11 -minute 08 -second 07) | ?{$_.eventid -eq 4624 -and $_.Message -match 'logon type:\s+(10)\s'} | Out-GridView



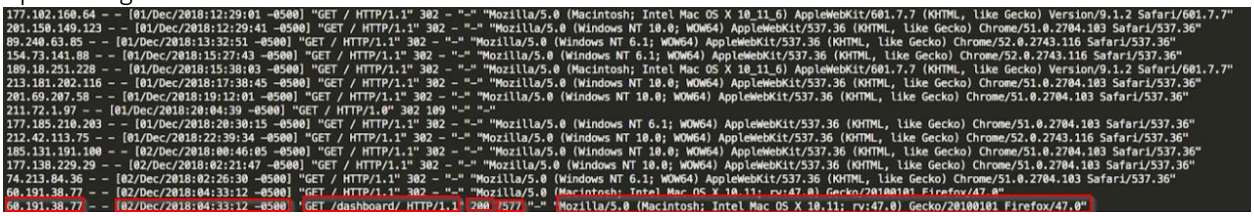
Logon refers to an RDP logon to the system, an event that appears after a user has been successfully authenticated. It is an event with the EventID 21 (Session logon succeeded), 24 (Session has been disconnected), 25, 39, 40 (Remote Desktop Services: Session logon succeeded). This events are located in the "Applications and Services Logs > Microsoft > Windows > TerminalServices-LocalSessionManager > Operational". As you can see, here you can find the ID of a user RDP session — Session ID.



Apache logs Analysis

Location: /var/www/apache2/logs/access logs

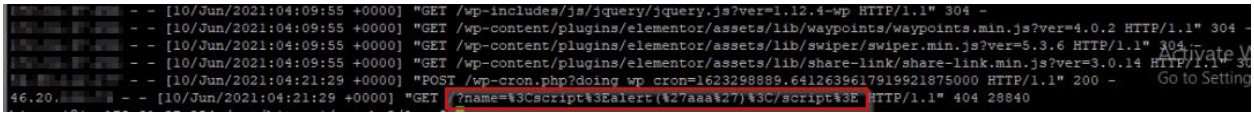
Apache logs screenshot



Searching for web attacks payloads

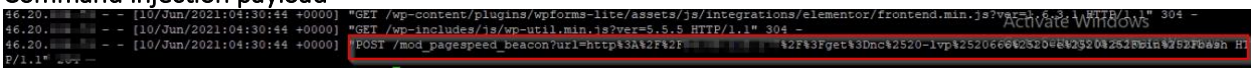
The logs start with the source IP that initiated the request , then the date and time, status code, request size, User agent.
If we want to manually inspect the logs for web attacks we can use the “grep” tool (on linux) to search for malicious payloads like XSS, SQLI, command injection, directory traversal attempts.

XSS payload



SQLI payload

Command Injection payload



Email Forensics

When you look at an email in outlook, gmail, or any other email client, you only see a fraction of the data that the email contains. Emails contains subject line, date, sending address and message body. However by looking at the email header you get all the information needed to perform a forensic analysis about the email, like the route taken by the email to reach it's destination and the results of authentication testing. Examination of these headers can help to detect phishing emails.

Three potential signs of a phishing email:

- Mismatches in the sender's address
- Suspicious path between sender and recipient
- Use of an unusual email client

Mismatched sender addresses

The display name in an email is easily faked. Comparing the various email headers associated with the sender's address can be helpful in identifying emails spoof. In the sample header below the email is received from Amazon's audiobook company. You can see that all header values in this email are the same except for the **From:** one, which is what would be displayed to the email's recipient. Comparing these headers can help identifying a phishing email, in this case the email is legitimate.

Sample email header

```
smtp.mailfrom=20200426102150b3db05ce8b564d7fb0b92eb4bbe0p0na-C139VA4WBJQ38E@bounces.audible.com;
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=audible.com
Return-Path: <20200426102150b3db05ce8b564d7fb0b92eb4bbe0p0na-C139VA4WBJQ38E@bounces.audible.com>
Received: from a15-239.smtp-out.amazonses.com (a15-239.smtp-out.amazonses.com. [54.240.15.239])
        by mx.google.com with ESMTPS id c55si6308910qtb.303.2020.04.26.03.21.50
        for <        @gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-SHA bits=128/128);
        Sun, 26 Apr 2020 03:21:51 -0700 (PDT)
Received-SPF: pass (google.com: domain of 20200426102150b3db05ce8b564d7fb0b92eb4bbe0p0na-
c139va4wbjq38e@bounces.audible.com designates 54.240.15.239 as permitted sender) client-ip=54.240.15.239;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@audible.com header.s=ojj34j72ahle3pv2wtzo647qowfxsajr header.b=R2cSrJKP;
       dkim=pass header.i=@amazonses.com header.s=224i4yxa5dv7c2xz3womw6peuasteono header.b=YaiuadYH;
       spf=pass (google.com: domain of 20200426102150b3db05ce8b564d7fb0b92eb4bbe0p0na-
c139va4wbjq38e@bounces.audible.com designates 54.240.15.239 as permitted sender)
smtp.mailfrom=20200426102150b3db05ce8b564d7fb0b92eb4bbe0p0na-C139VA4WBJQ38E@bounces.audible.com;
       dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=audible.com
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=ojj34j72ahle3pv2wtzo647qowfxsajr;
d=audible.com; t=1587896510; h=From:To:Message-ID:Subject:MIME-Version:Content-Type:Date;
bh=HhN8WE1G8zk3msaBQGn7hSq4PXUzqxRS8gW4OJ74v6s=;
b=R2cSrJKPOjCt1+QqjhpKAbF5ICk8MBE6pmR2X5XT4v2E/KnJ+zB53IXyRWx+RWzI
UNN7eQOXspK6XudzLYRDE2lPfJtygVyeoCbqOrMZk8aQGcTzCFaHZBgNmfvjhgGtt98 PHe4Ms2PjKntdisPJRpwP8v24VqBMaBl2k/J7ZGA=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=224i4yxa5dv7c2xz3womw6peuasteono;
d=amazonses.com; t=1587896510; h=From:To:Message-ID:Subject:MIME-Version:Content-Type:Date:Feedback-ID;
bh=HhN8WE1G8zk3msaBQGn7hSq4PXUzqxRS8gW4OJ74v6s=;
b=YaiuadYHWl9C0bXecUa37uGbwpX9x6pUhtQ+2n9+VjcidfkoQpATiO5KUi0LHOHp
FQlfwDZAZrKmDCvAtW8KiIdmuXrSE+dXVOCnbO6uEVc454TAAGDEUYRdeD3gE2Fqw2e qjXkbJnDAYQ6JhB2E/Vn71uXgOEKvcgBNvPT9UG8=
From: Audible <newsletters@audible.com>
To:          @gmail.com
Message-ID: <01000171b601e7b5-836f8d05-144e-4166-b628-a12782e62f6e-000000@email.amazonses.com>
Subject: Today's Daily Deal
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="----=_Part_2590386_1075090975.1587896510379"
X-AMAZON-MAIL-RELAY-TYPE: notification
Bounces-to: 20200426102150b3db05ce8b564d7fb0b92eb4bbe0p0na-C139VA4WBJQ38E@bounces.audible.com
```

Email Travel path

Between the sender and the destination, an email moves through multiple email servers. The number of servers depends on the email, but it should always have at least two: the sending and receiving server. This email originated from a yahoo.com address, so it makes sense that its sending server would be a yahoo.com server.

```
Received: from [redacted] ([redacted].yahoo.com. [77.238.176.206])
        by mx.google.com with ESMTPS id [redacted]
        for [redacted]
        (version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 31 Mar 2020 10:07:27 -0700 (PDT)
```

Examining these email servers can help to identify inconsistencies regarding an email's supposed origins. For example, an email claiming to originate from the USA may have an initial server in China or UK, which would be suspicious. Keep in mind that at each stage of the journey, an email server has the ability to modify email headers. If DKIM and SPF are enabled, this should result in a failed verification. However, the original sender of the email may have spoofed the headers to try to hide that they are the original sender of the message.

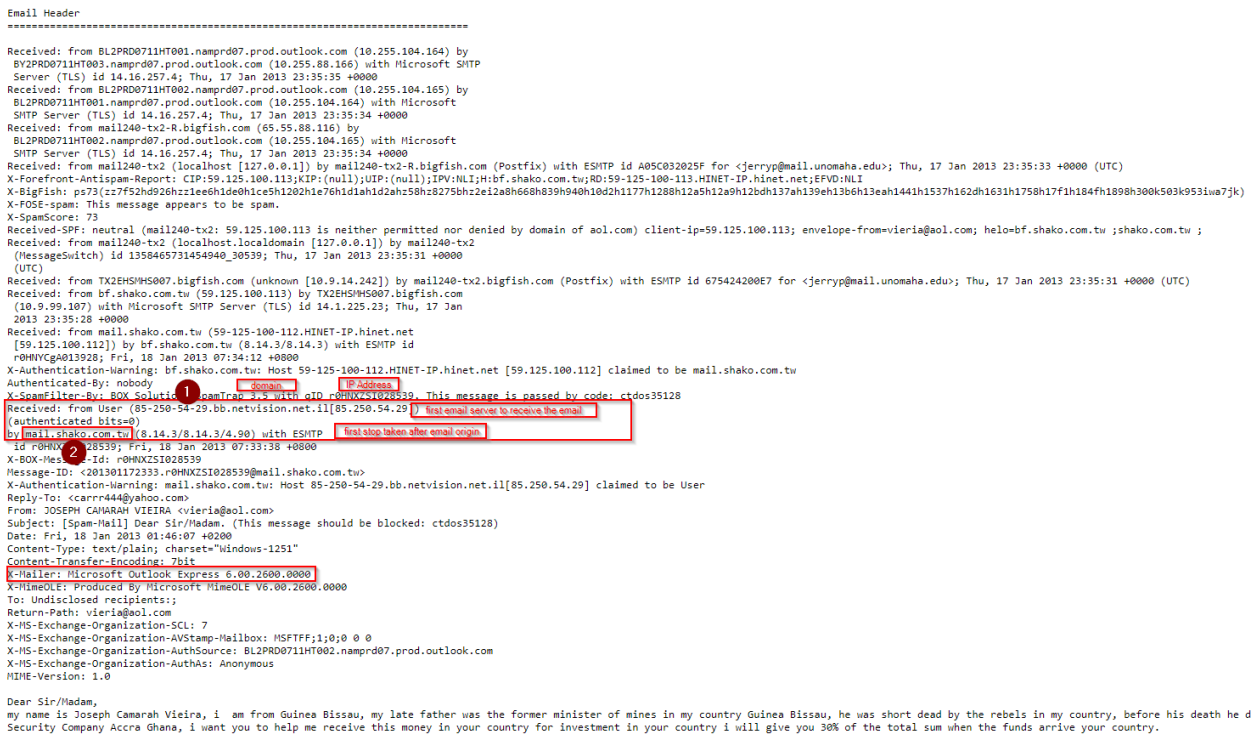
Email Client

When sending an email, most people do not connect directly to the email server and type in an email in the command line. Instead, they use an email client, like Outlook or Gmail. The mail client used by an email's sender is included in an email's headers. If this header looks unusual in any way, it could be a reason for suspicion.

```
X-Mailer: WebService/1.1.15555 YMailNorrin Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/79.0.3945.88 Safari/537.36
```

Sample Email header Analysis

if you observe the email header below there seems to be a lot of Received: entries in there. As an email travels from the source to its destination, each server adds its header entries to the top of the email body. So if we want to trace the email origin, this will be the very first Received: entry encountered from the bottom of the raw email. If you see something like Received-SPF:, ignore it.




```
Email Header
================================================================================

Received: from BL2PRD0711HT001.namprd07.prod.outlook.com (10.255.104.164) by
 BY2PRD0711HT003.namprd07.prod.outlook.com (10.255.88.166) with Microsoft SMTP
 Server (TLS) id 14.16.257.4; Thu, 17 Jan 2013 23:35:35 +0000
Received: from BL2PRD0711HT002.namprd07.prod.outlook.com (10.255.104.165) by
 BL2PRD0711HT001.namprd07.prod.outlook.com (10.255.104.164) with Microsoft
 SMTP Server (TLS) id 14.16.257.4; Thu, 17 Jan 2013 23:35:34 +0000
Received: from mail240-tx2-R.bigfish.com (65.55.88.116) by
 BL2PRD0711HT002.namprd07.prod.outlook.com (10.255.104.165) with Microsoft
 SMTP Server (TLS) id 14.16.257.4; Thu, 17 Jan 2013 23:35:34 +0000
Received: from mail240-tx2 (localhost [127.0.0.1]) by mail240-tx2-R.bigfish.com (Postfix) with ESMTP id A05C032025F for <jerryp@mail.unomaha.edu>; Thu, 17 Jan 2013 23:35:33 +0000 (UTC)
X-Forefront-Antispam-Report: CIP:59.125.100.113;KIP:(null);UIP:(null);IPV:NLI;H:bf.shako.com.tw;RD:59-125-100-113.HINET-IP.hinet.net;EFVD:NLI
X-BigFish: ps73(zz7f52hd926hzz1ee6h1de0h1ce5h1202h1e76h1d1ah1d2ahz58hz8275bhz2ei2a8h668h839h940h10d2h1177h1288h12a5h12a9h12bdh137ah139eh13b6h13eah1441h1537h162dh1631h1758h17f1h184fh1898h300k503k953iwa7jk)
X-FOSE-spam: This message appears to be spam.
X-SpamScore: 73
Received-SPF: neutral (mail240-tx2: 59.125.100.113 is neither permitted nor denied by domain of aol.com) client-ip=59.125.100.113; envelope-from=vieria@aol.com; helo=bf.shako.com.tw ;shako.com.tw ;
Received: from mail240-tx2 (localhost.localdomain [127.0.0.1]) by mail240-tx2
 (MessageSwitch) id 1358465731454940_30539; Thu, 17 Jan 2013 23:35:31 +0000
 (UTC)
Received: from TX2EHSMHS007.bigfish.com (unknown [10.9.14.242]) by mail240-tx2.bigfish.com (Postfix) with ESMTP id 675424200E7 for <jerryp@mail.unomaha.edu>; Thu, 17 Jan 2013 23:35:31 +0000 (UTC)
Received: from bf.shako.com.tw (59.125.100.113) by TX2EHSMHS007.bigfish.com
 (10.9.99.107) with Microsoft SMTP Server (TLS) id 14.1.225.23; Thu, 17 Jan
 2013 23:35:28 +0000
Received: from mail.shako.com.tw (59-125-100-112.HINET-IP.hinet.net
 [59.125.100.112]) by bf.shako.com.tw (8.14.3/8.14.3) with ESMTP id
 r0HNYCgA013928; Fri, 18 Jan 2013 07:34:12 +0800
X-Authentication-Warning: bf.shako.com.tw: Host 59-125-100-112.HINET-IP.hinet.net [59.125.100.112] claimed to be mail.shako.com.tw
Authenticated-By: nobody
X-SpamFilter-By: BOX Solution SpamTrap 3.5 with qID r0HNYZSI028539, This message is passed by code: ctdos35128
Received: from User (85-250-54-29.bb.netvision.net.il[85.250.54.29])
(authenticated bits=0)
by mail.shako.com.tw (8.14.3/8.14.3/4.90) with ESMTP
 id r0HNXZSI028539; Fri, 18 Jan 2013 07:33:38 +0800
X-BOX-MessageID: r0HNXZSI028539
Message-ID: <201301172333.r0HNXZSI028539@mail.shako.com.tw>
X-Authentication-Warning: mail.shako.com.tw: Host 85-250-54-29.bb.netvision.net.il[85.250.54.29] claimed to be User
Reply-To: <carrr444@yahoo.com>
From: JOSEPH CAMARAH VIEIRA <vieria@aol.com>
Subject: [Spam-Mail] Dear Sir/Madam. (This message should be blocked: ctdos35128)
Date: Fri, 18 Jan 2013 01:46:07 +0200
Content-Type: text/plain; charset="Windows-1251"
Content-Transfer-Encoding: 7bit
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
To: Undisclosed recipients:;
Return-Path: vieria@aol.com
X-MS-Exchange-Organization-SCL: 7
X-MS-Exchange-Organization-AVStamp-Mailbox: MSFTFF;1;0;0 0 0
X-MS-Exchange-Organization-AuthSource: BL2PRD0711HT002.namprd07.prod.outlook.com
X-MS-Exchange-Organization-AuthAs: Anonymous
MIME-Version: 1.0

Dear Sir/Madam,
my name is Joseph Camarah Vieira, i  am from Guinea Bissau, my late father was the former minister of mines in my country Guinea Bissau, he was short dead by the rebels in my country, before his death he d
Security Company Accra Ghana, i want you to help me receive this money in your country for investment in your country i will give you 30% of the total sum when the funds arrive your country.
```

start scanning from the bottom of the header towards the top and examine the very first Received: entry. It looks like this:

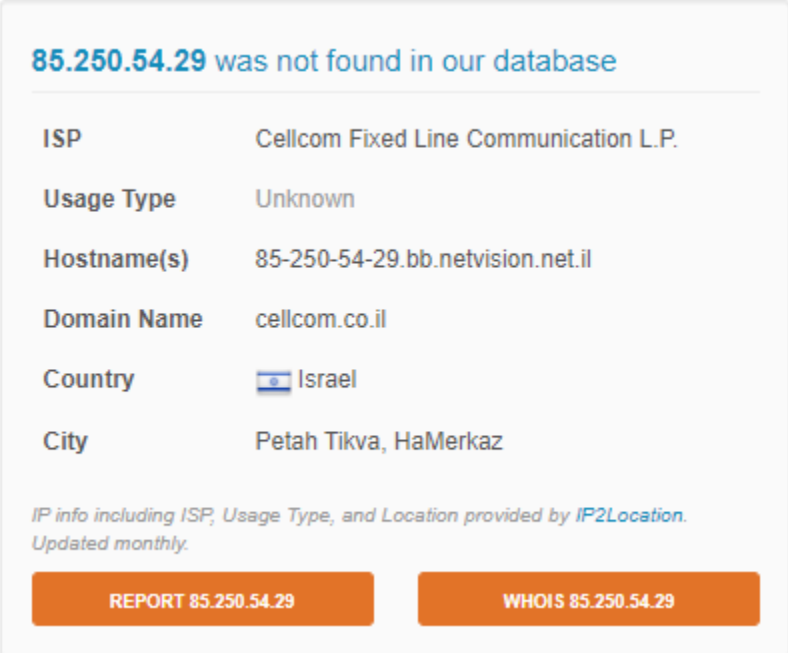
```
Received: from User (85-250-54-29.bb.netvision.net.il[85.250.54.29])
(authenticated bits=0)
by mail.shako.com.tw (8.14.3/8.14.3/4.90) with ESMTP
 id r0HNXZSI028539; Fri, 18 Jan 2013 07:33:38 +0800
```

The first email server to receive the email from the sender's computer creates this entry. If the email client is web-based then this entry will include details about the server hosting the email web application.

Let's further break down this entry. The from part of this entry indicates source of the email for this leg of the travel: User (85-250-54-29.bb.netvision.net.il[85.250.54.29]). You can pick out a Domain Name (85-250-54-29.bb.netvision.net.il) and an IP address (85.250.54.29) here.

The by part indicates the first stop taken after email origin:
mail.shako.com.tw (8.14.3/8.14.3/4.90). You can pick out a Domain Name here: mail.shako.com.tw.

The first encountered email server adds this header entry and every other entry below it. There is a high chance that a malicious sender has full control of this email-server. So do not trust this information. Regardless, we now have some information to do further investigation. Let's try to figure out where the geographic location of the email-server.



The searches reveal that a computer in Israel used an email server in Taiwan as the first stop on its way to the U.S., while the actual body of the email claims the sender is from Guinea Bissau. Something is not right!

There are few other fields that you should investigate in the email header.

Return-Path: See if the email address in this entry matches the email address in the From: entry. They typically will not match for mass emailers like advertisers or spammers. The Return-Path: email address is used when an email cannot be delivered to its recipients, and it "bounces back". Spammers don't want all the undelivered email to end up in their inboxes!

Reply-To: See if the email address in this entry matches the email address in the From: entry. When you hit reply to an email, the Reply-To entry is used to populate the recipients' email. If it is different, you may accidentally send your reply to someone else.

X-Distribution: if this field's value is bulk. This indicates bulk/spam email.

X-Mailer: field indicates the email client. If it includes weird names, be suspicious.

Bcc: or X-UIDL: entries exist. This is a sign of poorly crafted header. They are never in normal emails!

X-Spam score, X-Spam flag and X-Spam status entries help determine “spamminess”. But the scores are not standardized across servers so these have to examine on a case by case basis.