

Common Windows Artifacts

Dr. Darryl J D'Souza
Mob No: 9986382162





Task 1 -Continuation to Windows Forensics

Windows maintains a list of recently opened files for each user. As we might have seen when using Windows Explorer, it shows us a list of recently used files. This information is stored in the NTUSER hive and can be found on the following location:

Recent Files

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs

Registry hives (7)Available bookmarks (108/0)

Enter text to search...Find

Key name

RecentDocs

Ribbon

RunMRU

SearchPlatform

Shell Folders

Shutdown

StartPage

Streams

StuckRects3

TabletMode

Taskband

TypedPaths

User Shell Folders

UserAssist

VirtualDesktops

VisualEffects

Wallpapers

ValuesRecent documents

Drag a column header here to group by that column

Extension	Value Name	Target Name	Lnk Name	Mru Position	Opened On	Extension Last Opened
c	c	c	c	=	=	=
RecentDocs	7	EZtools	EZtools.lnk	0	2021-12-01 13:00:34	
RecentDocs	6	Settings	Settings.lnk	1		2021-11-30 10:56:23
RecentDocs	5	WallpaperSettings.xml	WallpaperSettings.lnk	2		2021-11-30 10:56:21
RecentDocs	4	System and Security	System and Security.lnk	3		
RecentDocs	3	::{BB06C0E4-D293-4F75-8A90-CB05B6477E-EE}	System.lnk	4		
RecentDocs	1	KAPE	KAPE.lnk	5		
RecentDocs	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	6		2021-11-24 18:18:48
RecentDocs	2	ChangeLog.txt	ChangeLog.lnk	7		2021-11-24 18:18:48
Folder	2	Settings	Settings.lnk	0	2021-11-30 10:56:23	
Folder	1	System and Security	System and Security.lnk	1		
Folder	0	KAPE	KAPE.lnk	2		
.xml	0	WallpaperSettings.xml	WallpaperSettings.lnk	0	2021-11-30 10:56:21	
.txt	0	ChangeLog.txt	ChangeLog.lnk	0	2021-11-24 18:18:48	
.ps1	0	Get-KAPEUpdate.ps1	Get-KAPEUpdate.lnk	0	2021-11-24 18:18:48	

Screen Shot 1 – Recent files

Registry Explorer allows us to sort data contained in registry keys quickly. For example, the Recent documents tab arranges the Most Recently Used (MRU) file at the top of the list. Registry Explorer also arranges them so that the Most Recently Used (MRU) file is shown at the top of the list and the older ones later.

Sort data

Another interesting piece of information in this registry key is that there are different keys with file extensions, such as .pdf, .jpg, .docx etc. These keys provide us with information about the last used files of a specific file extension. So if we are looking specifically for the last used PDF files, we can look at the following registry key:

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs\.pdf

Office Recent Files

Similar to the Recent Docs maintained by Windows Explorer, Microsoft Office also maintains a list of recently opened documents. This list is also located in the NTUSER hive. It can be found in the following location:

NTUSER.DAT\Software\Microsoft\Office\VERSION

The version number for each Microsoft Office release is different. An example registry key will look like this:

NTUSER.DAT\Software\Microsoft\Office\15.0\Word

Here, the 15.0 refers to Office 2013. A list of different Office releases and their version numbers can be found on this link.

Starting from Office 365, Microsoft now ties the location to the user's live ID. In such a scenario, the recent files can be found at the following location.

NTUSER.DAT\Software\Microsoft\Office\VERSION\UserMRU\LiveID_####\FileMRU

In such a scenario, the recent files can be found at the following location. This location also saves the complete path of the most recently used files.

Open/Save and Last Visited Dialog MRUs

When we open or save a file, a dialog box appears asking us where to save or open that file from. It might be noticed that once we open/save a file at a specific location, Windows remembers that location. This implies that we can find out recently used files if we get our hands on this information. We can do so by examining the following registry keys

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

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



Drag a column header here to group by that column				
Value Name	Mru Position	Executable	Absolute Path	Opened On
0		notepad.exe	My Computer\C:\Program Files\Amazon\Ec2ConfigService\Settings	2021-11-30 10:56:19

Activity - Open up notepad. Type some random data and save it anywhere on the computer. (This will be helpful in the later exercise)

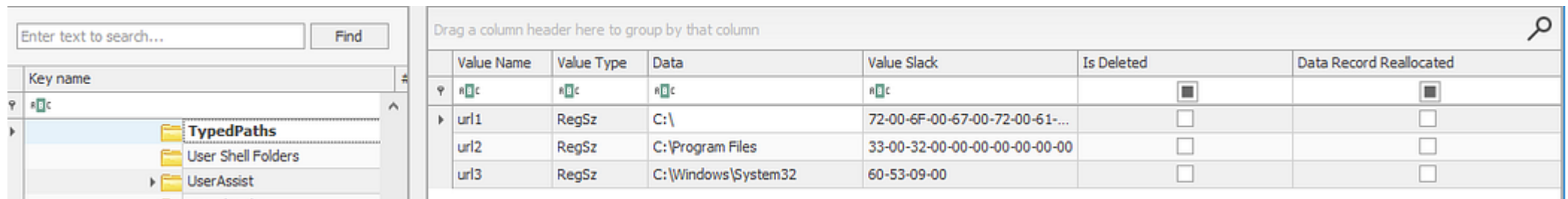
Windows Explorer Address/Search Bars

Another way to identify a user's recent activity is by looking at the paths typed in the Windows Explorer address bar or searches performed using the following registry keys, respectively.

NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\TypedPaths

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

Here is how the TypedPaths key looks like in Registry Explorer:



Drag a column header here to group by that column						
Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated	
url1	RegSz	C:\	72-00-6F-00-67-00-72-00-61-...	<input type="checkbox"/>	<input type="checkbox"/>	
url2	RegSz	C:\Program Files	33-00-32-00-00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>	
url3	RegSz	C:\Windows\System32	60-53-09-00	<input type="checkbox"/>	<input type="checkbox"/>	

UserAssist

Windows keeps track of applications launched by the user using Windows Explorer for statistical purposes in the User Assist registry keys. These keys contain information about the programs launched, the time of their launch, and the number of times they were executed. However, programs that were run using the command line can't be found in the User Assist keys. The User Assist key is present in the NTUSER hive, mapped to each user's GUID. We can find it at the following location:

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

Registry hives (1)		Available bookmarks (31/0)		Values		UserAssist	
Enter text to search...		Find		Drag a column header here to group by that column			
Key name				Program Name	Run Counter	Focus Count	Last Executed
HKEY_CURRENT_USER				UEME_CTLCUACount:ctor	0	0	0d, 0h, 00m, 00s
{F4E57C4B-2036-4...				{Common Programs}\Accessories\Snipping Tool.lnk	9	0	2021-11-25 03:14:34
{FA990FC7-6AC2-...				UEME_CTLSESSION	54	0	0d, 0h, 00m, 00s
VirtualDesktops				{Common Programs}\Accessories\Paint.lnk	7	0	2021-11-25 03:14:34
VisualEffects				{Programs}\Accessories\Notepad.lnk	6	0	2021-11-25 03:14:34
Wallpapers				{User Pinned}\TaskBar\File Explorer.lnk	26	0	2021-12-01 13:02:43
WordWheelQuery				{Programs}\Windows PowerShell\Windows PowerShell.lnk	1	0	2021-11-25 03:37:24
Ext				{User Pinned}\TaskBar\Firefox.lnk	2	0	2021-12-01 12:32:34
Feeds				{Common Programs}\Accessories\Remote Desktop Connection.lnk	1	0	2021-11-25 03:59:55
FileAssociations				{User Pinned}\TaskBar\Opera Browser.lnk	1	0	2021-11-25 04:10:02
FileHistory				{Common Programs}\Accessories\Notepad.lnk	1	0	2021-11-30 10:55:21
GameDVR							
Group Policy							
Holographic							

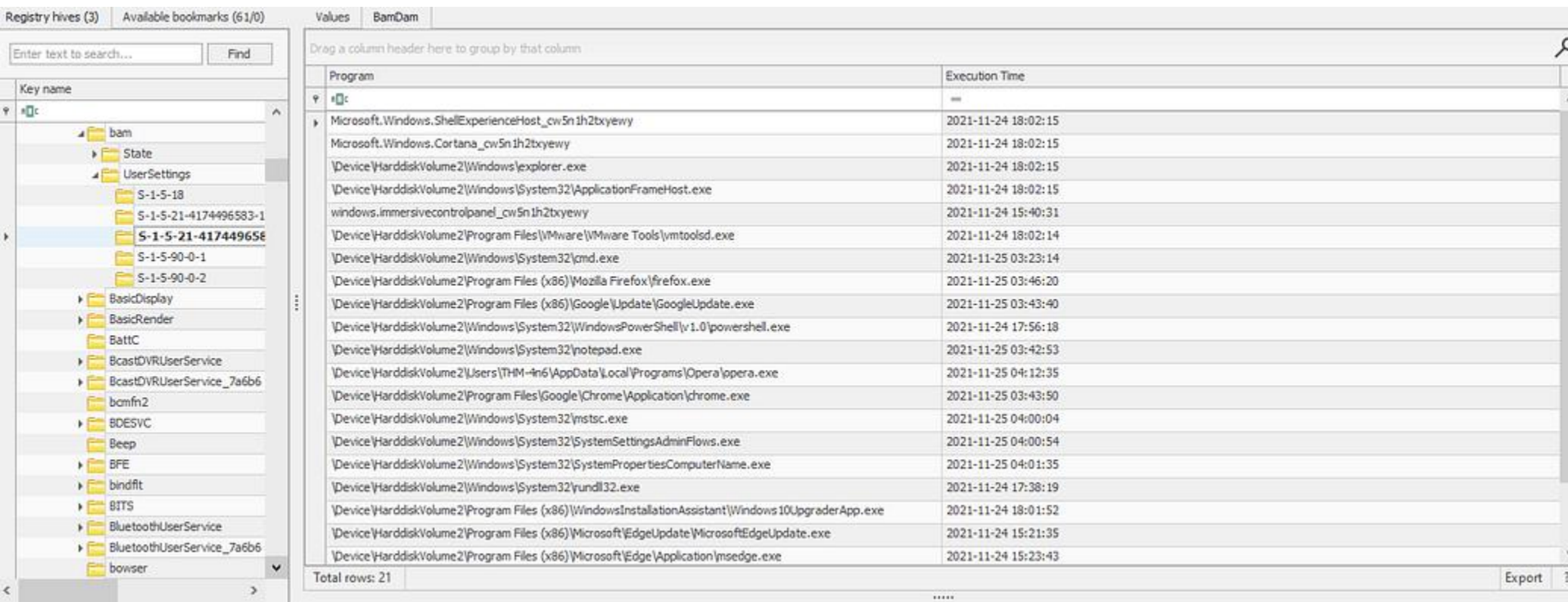
Background Activity Monitor or BAM keeps a tab on the activity of background applications. Similar Desktop Activity Moderator or DAM is a part of Microsoft Windows that optimizes the power consumption of the device. Both of these are a part of the Modern Standby system in Microsoft Windows.

BAM/DAM

In the Windows registry, the following locations contain information related to BAM and DAM. This location contains information about last run programs, their full paths, and last execution time.

SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}

SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}



Registry hives (3) Available bookmarks (61/0)

Enter text to search... Find

Key name

Values BamDam


Drag a column header here to group by that column

Program	Execution Time
Microsoft.Windows.ShellExperienceHost_cw5n1h2txyewy	2021-11-24 18:02:15
Microsoft.Windows.Cortana_cw5n1h2txyewy	2021-11-24 18:02:15
\Device\HarddiskVolume2\Windows\explorer.exe	2021-11-24 18:02:15
\Device\HarddiskVolume2\Windows\System32\ApplicationFrameHost.exe	2021-11-24 18:02:15
windows.immersivecontrolpanel_cw5n1h2txyewy	2021-11-24 15:40:31
\Device\HarddiskVolume2\Program Files\VMware Tools\vmtoolsd.exe	2021-11-24 18:02:14
\Device\HarddiskVolume2\Windows\System32\cmd.exe	2021-11-25 03:23:14
\Device\HarddiskVolume2\Program Files (x86)\Mozilla Firefox\firefox.exe	2021-11-25 03:46:20
\Device\HarddiskVolume2\Program Files (x86)\Google\Update\GoogleUpdate.exe	2021-11-25 03:43:40
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	2021-11-24 17:56:18
\Device\HarddiskVolume2\Windows\System32\notepad.exe	2021-11-25 03:42:53
\Device\HarddiskVolume2\Users\THM-4n6\AppData\Local\Programs\Opera\opera.exe	2021-11-25 04:12:35
\Device\HarddiskVolume2\Program Files\Google\Chrome\Application\chrome.exe	2021-11-25 03:43:50
\Device\HarddiskVolume2\Windows\System32\mstsc.exe	2021-11-25 04:00:04
\Device\HarddiskVolume2\Windows\System32\SystemSettingsAdminFlows.exe	2021-11-25 04:00:54
\Device\HarddiskVolume2\Windows\System32\SystemPropertiesComputerName.exe	2021-11-25 04:01:35
\Device\HarddiskVolume2\Windows\System32\rundll32.exe	2021-11-24 17:38:19
\Device\HarddiskVolume2\Program Files (x86)\WindowsInstallationAssistant\Windows10UpgraderApp.exe	2021-11-24 18:01:52
\Device\HarddiskVolume2\Program Files (x86)\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe	2021-11-24 15:21:35
\Device\HarddiskVolume2\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	2021-11-24 15:23:43

Total rows: 21 Export ?



Task 2 -External Devices/USB device forensics



When performing forensics on a machine, often the need arises to identify if any USB or removable drives were attached to the machine. If so, any information related to those devices is important for a forensic investigator. In this task, we will go through the different ways to find information on connected devices and the drives on a system using the registry.

The following locations keep track of USB keys plugged into a system. These locations store the vendor id, product id, and version of the USB device plugged in and can be used to identify unique devices. These locations also store the time the devices were plugged into the system.

Device Identification:

SYSTEM\CurrentControlSet\Enum\USBSTOR

SYSTEM\CurrentControlSet\Enum\USB

Registry hives (3)

Available bookmarks (61/0)

Enter text to search...

Find

Key name

C:

USB

USBSTOR

XENBUS

XENVIF

Values

USBSTOR

Drag a column header here to group by that column

Timestamp

Manufacturer

Title

Version

Disk Id

Serial Number

Device Name

Installed

First Installed

Last Connected

Last Removed

2021-11-24 18:25...

Ven_Kingston

Prod_DataTraveler_2.0

Rev_PMAP

{e251921f-4da2-11ec-a783-001a7dda7110}

1C6F654E59A380C179D366AE80

Kingston DataTraveler 2.0 USB Device

2021-11-24 18:25...

2021-11-24 18:25...

2021-11-24 18:40...

2021-11-24 18:27...

Ven_USB3.0

Prod_External_Device

Rev_SDM1

{f529a9d6-4d9e-11ec-a782-001a7dda7110}

0123456789ABCDE80

USB3.0 External Device USB Device

2021-11-24 18:27...

2021-11-24 18:27...

2021-11-24 18:27...

Similarly, the following registry key tracks the first time the device was connected, the last time it was connected and the last time the device was removed from the system.

SYSTEM\CurrentControlSet\Enum\USBSTOR\Ven_Prod_Version\USBSerial#\Properties\{83da6326-97a6-4088-9453-a19231573b29}\####

In this key, the #### sign can be replaced by the following digits to get the required information:

ValueInformation0064First Connection time0066Last Connection time0067Last removal time

Although we can check this value manually, as we have seen above, Registry Explorer already parses this data and shows us if we select the USBSTOR key.

The device name of the connected drive can be found at the following location:

USB device
Volume Name:

SOFTWARE\Microsoft\Windows Portable Devices\Devices

We can compare the GUID we see here in this registry key and compare it with the Disk ID we see on keys mentioned in device identification to correlate the names with unique devices. Take a look at these two screenshots and answer Question # 3.

Combining all of this information, we can create a fair picture of any USB devices that were connected to the machine we’re investigating.

Timestamp	Device	Serial Number	Guid	Friendly Name
2021-11-25 07:16:54			{E251921F-4DA2-11EC-A783-001A7DDA7110}	USB
2021-11-25 07:16:54			{F529A9D6-4D9E-11EC-A782-001A7DDA7110}	New Volume

Web Browsers



Web browsers are used globally for accessing websites. In the context of digital forensics, web browsers can provide a wealth of information about a user's browsing history, cookies, downloaded files, saved passwords, and much more. This information can be used to determine what a user might have been up to, and identify any potentially suspicious activity.

There are numerous browsers available online, but we'll just be exploring the two most commonly used browsers, Firefox and Chrome.

Firefox

Firefox stores its data that can be valuable during a digital forensics investigation under the directory `C:\Users\%USERNAME%\AppData\Roaming\Mozilla\Firefox\Profiles`. This includes cookies, saved logins, browsing history, bookmarks, and some other useful information stored in .json files.

Web Browsers

Firefox saved Logins

Firefox encrypts the saved logins using a master key in the file key4.db located in the profile's directory. To extract usernames and passwords, we can use a tool called firefox_decrypt that can be downloaded from

https://github.com/unode/firefox_decrypt.

For You to try:

Clone the GitHub repo - https://github.com/unode/firefox_decrypt.

Firefox Decrypt is a tool to extract passwords from profiles of Mozilla (Fire/Water)fox™, Thunderbird®, SeaMonkey® and derivatives.

It can be used to recover passwords from a profile protected by a Master Password as long as the latter is known. If a profile is not protected by a Master Password, passwords are displayed without prompt.

This tool does not try to crack or brute-force the Master Password in any way. If the Master Password is not known it will simply fail to recover any data.

Process of extracting saved passwords from Chrome - **For you to try**

Chrome



Chrome stores its data including saved passwords, cookies, and other useful information under the directory

`C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default.`

This data is encrypted by default, but the key can be found in the directory

`C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Local State.`

Event logs provides records of important system, security, and application events. These logs are automatically generated by Windows, and can provide valuable information during a digital forensics investigation.

Event Logs

The event logs are stored in C:\Windows\System32\winevt\Logs and can be viewed and analyzed using the Event Viewer, a built-in tool in Windows.

Out of the three types of event logs i.e., system, security, and application logs, only the security logs will be of interest to us. The log files that may contain security related events include:

- Security.evtx
- Microsoft-Windows-Windows Defender%4Operational.evtx
- Microsoft-Windows-Windows Firewall With Advanced Security%4Firewall.evtx
- Microsoft-Windows-PowerShell%4Operational.evtx

NOTE: that these are not the only files that may be useful during a digital forensics investigation, but for this lab, we are interested in these files only.

Event Logs

Each of the events have a specific id associated with them, which can be used to identify and filter specific events of interest. For example, the event ID for a user logging in would be 4624, while the event ID for a user logging out would be 4634. The following table lists some common security-related event IDs and provides a brief summary of the information that can be gathered from each event:

Microsoft-Windows-Windows Defender%4OperationalNumber of events: 904

Level	Date and Time	Source	Event ID	Task Category
Information	21/01/2023 6:47:02 pm	Windows Defender	2010	None
Information	21/01/2023 6:46:28 pm	Windows Defender	1117	None
Warning	21/01/2023 6:46:27 pm	Windows Defender	1116	None
Information	21/01/2023 6:46:27 pm	Windows Defender	1117	None
Warning	21/01/2023 6:46:17 pm	Windows Defender	1116	None
Warning	21/01/2023 6:45:51 pm	Windows Defender	1116	None
Information	21/01/2023 6:45:49 pm	Windows Defender	2010	None
Information	21/01/2023 6:45:48 pm	Windows Defender	2010	None
Information	21/01/2023 6:41:10 pm	Windows Defender	2000	None
Information	21/01/2023 6:41:10 pm	Windows Defender	2000	None

Event 1117, Windows Defender

GeneralDetails

Microsoft Defender Antivirus has taken action to protect this machine from malware or other potentially unwanted software. For more information please see the following:
<https://go.microsoft.com/fwlink/?linkid=37020&name=Trojan:Win32/Wacatac.B!ml&threatid=2147735505&enterprise=0>

Name: Trojan:Win32/Wacatac.B!ml
ID: 2147735505
Severity: Severe
Category: Trojan
Path: file: C:\Users\saad\Downloads\Debugg-V2.exe
Detection Origin: Local machine
Detection Type: FastPath
Detection Source: Real-Time Protection
User: NT AUTHORITY\SYSTEM
Process Name: C:\Windows\explorer.exe
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x00000000
Error description: The operation completed successfully.
Security Intelligence Version: AV: 1.381.2505.0, AS: 1.381.2505.0, NIS: 1.381.2505.0
Engine Version: AH: 1.1.19900.2, NIS: 1.1.19900.2

Log Name:Microsoft-Windows-Windows Defender/Operational

Source:Windows Defender

Logged:21/01/2023 6:46:28 pm

Event ID:1117

Task Category:None

Level:Information

Keywords:

User:SYSTEM


Computer:DESKTOP-HOLTRRS

OpCode:Info

More Information:[Event Log Online Help](#)

Event ID	Event Summary
1006	The antimalware engine found malware or other potentially unwanted software.
1007	The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.
1015	The antimalware platform detected suspicious behavior.
1116	The antimalware platform detected malware or other potentially unwanted software.
1117	The antimalware platform performed an action to protect your system from malware or other potentially unwanted software.
1100	The event logging service has shut down.
1102	The audit log was cleared.
4624	An account was successfully logged on.
4625	An account failed to log on.
4634	An account was logged off.
4648	A logon was attempted using explicit credentials.
4720	A user account was created.
4722	A user account was enabled.
4723	An attempt was made to change an account's password.
4724	An attempt was made to reset an account's password.

Lab Questions

1. When was EZtools opened ? (Refer Screenshot)
 2. At what time was My Computer last interacted with?
 3. What is the Absolute Path of the file opened using notepad.exe?
 4. When was this file opened?
 5. How many times was the File Explorer launched?
 6. Which of the artifacts saves the full path of the executed programs?
- 

For complete information

<https://tryhackme.com/r/room/windowsforensics1>



Lab Questions

1. What is the serial number of the device from the manufacturer 'Kingston'?
2. What is the name of this device?
3. What is the friendly name of the device from the manufacturer 'Kingston'?

Refer The ppts above for answers



Lab Questions

1. Given the Firefox profile of a suspect, answer the following:

- I. What's the username and password stored in the saved logins?
- II. What's the most frequently visited website?
- III. What's the name of the file downloaded by the suspect?



Lab Questions

2. Given the PowerShell Event logs of a compromised system, answer the following:
- I. What's the command executed by the attacker to download a file on the system?
 - II. Can you analyze the downloaded file and understand what's the purpose of that file?
- 