Lab 2 — Common Windows Artifacts

The windows operating system is composed of a large number of artifacts, including files, directories, logs, registries, browser history, user accounts and other important data which are essential for it to function properly.

In this lab, we'll explore some such artifacts which are useful while conducting a forensics investigation, we'll learn where such artifacts are placed, and how we can extract valuable information out of them.

Windows Registry

The Windows Registry is a hierarchical database that stores configurations for users, applications, and hardware devices. Here's how Microsoft describes it:

> The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents that each can create, property sheet settings for folders and application icons, what hardware exists on the system, and the ports that are being used.

The Windows Registry is composed of five main root keys, also known as hives, under the root key `Computer`, these are:

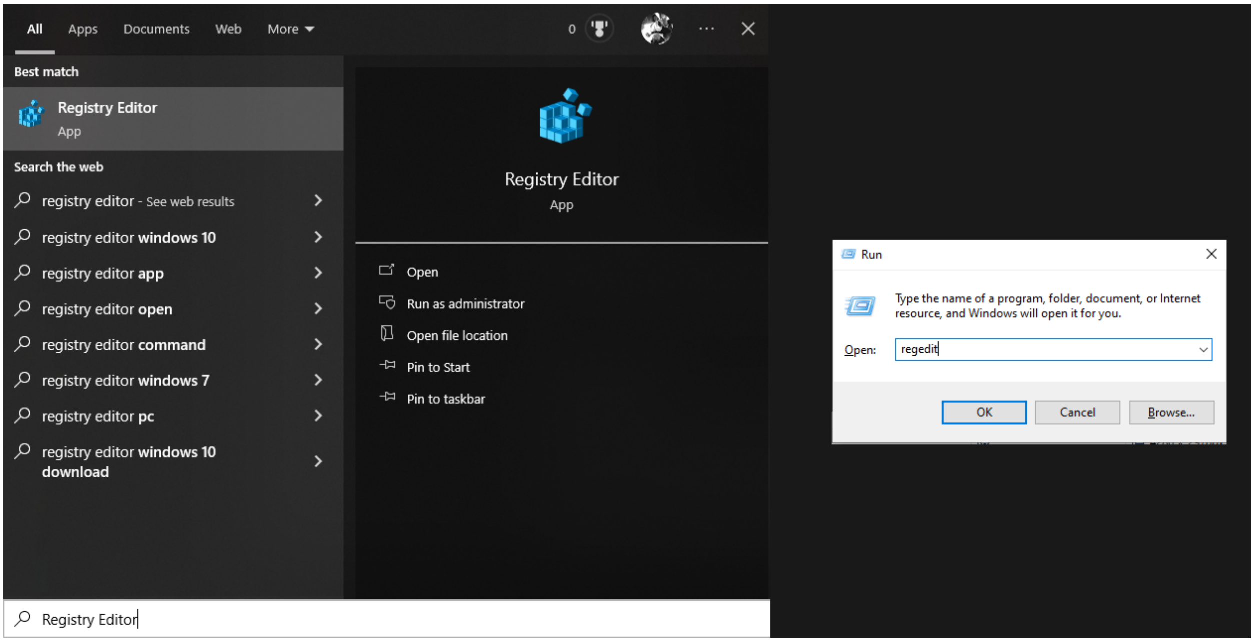
- `HKEY_CURRENT_USER (HKCU)` — contains information about the logged in user, including screen colors, and control panel settings.
- `HKEY_USERS (HKU)` — contains information about actively loaded user profiles on the system, including profiles and settings.

- `HKEY_LOCAL_MACHINE (HKLM)` — contains information about the system configuration (for any user).
- `HKEY_CLASSES_ROOT (HKCR)` — contains information about file types and their associated programs.
- `HKEY_CURRENT_CONFIG (HKCC)` — contains information about the hardware profile of the system.

Each of these keys contains a hierarchy of subkeys and values that store specific information about the system and its configuration. For example, the configuration for the mouse, such as sensitivity, and double click speed are stored in `Computer\HKEY_CURRENT_USER\Control Panel\Mouse`. We can also visualize it as a tree where each branch represents a subkey:

```
Computer
|__ HKEY_CURRENT_USER
  |__ Control Panel
    |__ Mouse
```

Registry keys can be viewed and modified by using the built-in Registry Editor. Following are two ways to open it, through the Search bar or by using the Run command (Win + R).

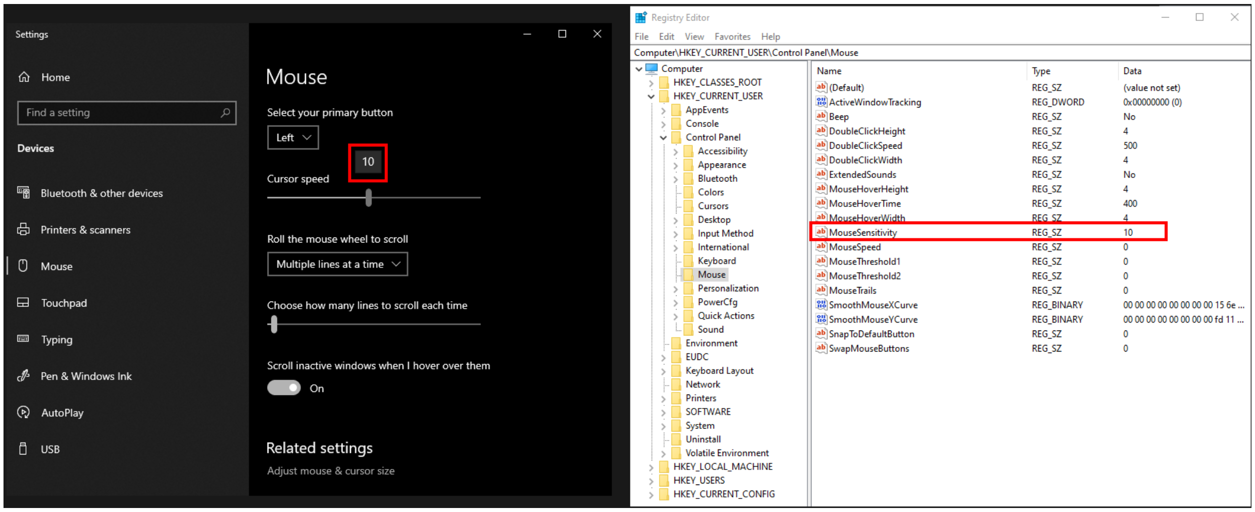


Registry Editor

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: regedit

To test it out, we can modify the mouse sensitivity in settings and see the changes reflected in registry keys.



Mouse

Select your primary button: Left

Cursor speed: 10

Roll the mouse wheel to scroll: Multiple lines at a time

Choose how many lines to scroll each time

Scroll inactive windows when I hover over them: On

Related settings

Adjust mouse & cursor size

Computer\HKEY_CURRENT_USER\Control Panel\Mouse

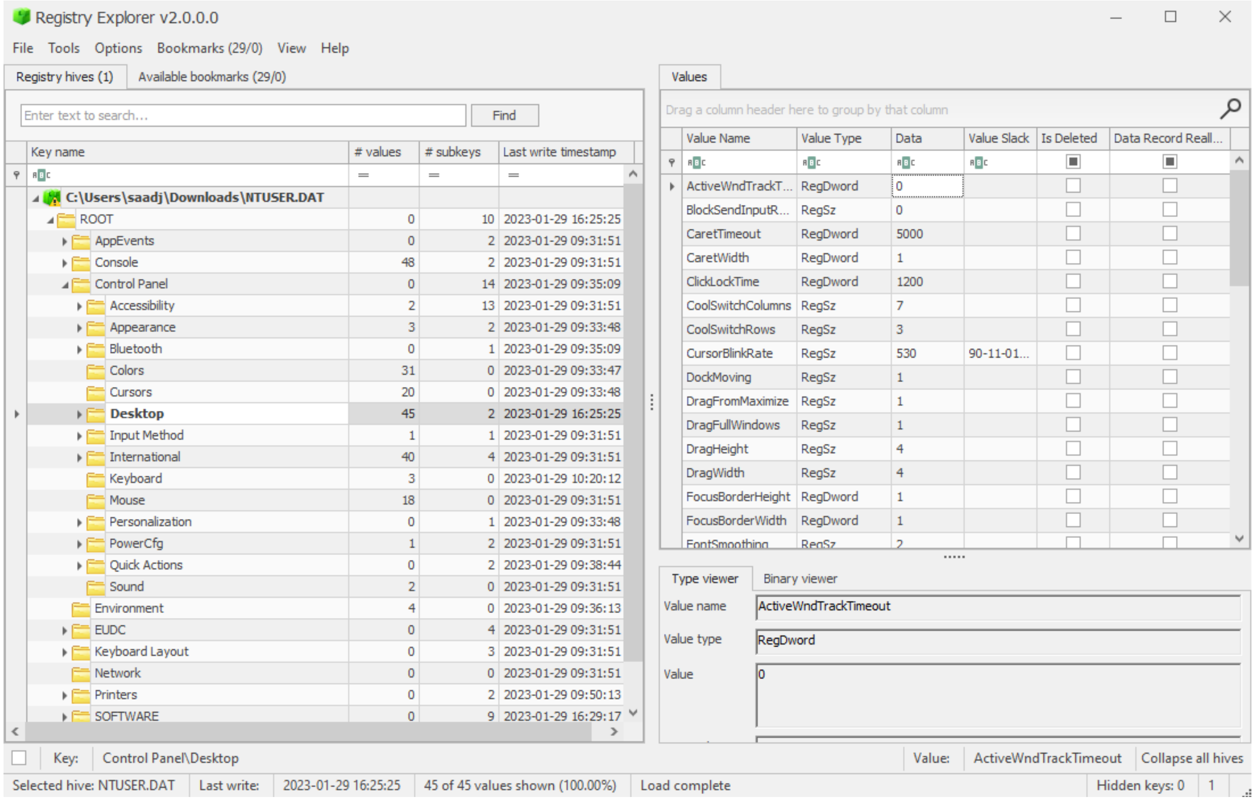
Name	Type	Data
(Default)	REG_SZ	(value not set)
ActiveWindowTracking	REG_DWORD	0x00000000 (0)
Beep	REG_SZ	No
DoubleClickHeight	REG_SZ	4
DoubleClickSpeed	REG_SZ	500
DoubleClickWidth	REG_SZ	4
ExtendedSounds	REG_SZ	No
MouseHoverHeight	REG_SZ	4
MouseHoverTime	REG_SZ	400
MouseHoverWidth	REG_SZ	4
MouseSensitivity	REG_SZ	10
MouseSpeed	REG_SZ	0
MouseThreshold1	REG_SZ	0
MouseThreshold2	REG_SZ	0
MouseTrails	REG_SZ	0
SmoothMouseXCurve	REG_BINARY	00 00 00 00 00 00 00 00 15 6e ...
SmoothMouseYCurve	REG_BINARY	00 00 00 00 00 00 00 00 fd 11 ...
SnapToDefaultButton	REG_SZ	0
SwapMouseButtons	REG_SZ	0

An alternative approach is to do it the other way around by first modifying the registry keys, and then seeing the changes after rebooting the computer or signing out and signing back in.

NTUSER.DAT

The `NTUSER.DAT` file is a user profile hive that is part of the registry. The per user configurations are stored in `C:\Users\%USERNAME%\NTUSER.DAT`.

The contents of the `NTUSER.DAT` file can be accessed using Registry Explorer by Eric Zimmerman as shown in the image below.



Key name	# values	# subkeys	Last write timestamp
C:\Users\saadj\Downloads\NTUSER.DAT			
ROOT	0	10	2023-01-29 16:25:25
AppEvents	0	2	2023-01-29 09:31:51
Console	48	2	2023-01-29 09:31:51
Control Panel	0	14	2023-01-29 09:35:09
Accessibility	2	13	2023-01-29 09:31:51
Appearance	3	2	2023-01-29 09:33:48
Bluetooth	0	1	2023-01-29 09:35:09
Colors	31	0	2023-01-29 09:33:47
Cursors	20	0	2023-01-29 09:33:48
Desktop	45	2	2023-01-29 16:25:25
Input Method	1	1	2023-01-29 09:31:51
International	40	4	2023-01-29 09:31:51
Keyboard	3	0	2023-01-29 10:20:12
Mouse	18	0	2023-01-29 09:31:51
Personalization	0	1	2023-01-29 09:33:48
PowerCfg	1	2	2023-01-29 09:31:51
Quick Actions	0	2	2023-01-29 09:38:44
Sound	2	0	2023-01-29 09:31:51
Environment	4	0	2023-01-29 09:36:13
EUDC	0	4	2023-01-29 09:31:51
Keyboard Layout	0	3	2023-01-29 09:31:51
Network	0	0	2023-01-29 09:31:51
Printers	0	2	2023-01-29 09:50:13
SOFTWARE	0	9	2023-01-29 16:29:17

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reall...
ActiveWndTrackT...	RegDword	0		□	□
BlockSendInputR...	RegSz	0		□	□
CaretTimeout	RegDword	5000		□	□
CaretWidth	RegDword	1		□	□
ClickLockTime	RegDword	1200		□	□
CoolSwitchColumns	RegSz	7		□	□
CoolSwitchRows	RegSz	3		□	□
CursorBlinkRate	RegSz	530	90-11-01...	□	□
DockMoving	RegSz	1		□	□
DragFromMaximize	RegSz	1		□	□
DragFullWindows	RegSz	1		□	□
DragHeight	RegSz	4		□	□
DragWidth	RegSz	4		□	□
FocusBorderHeight	RegDword	1		□	□
FocusBorderWidth	RegDword	1		□	□
FontSmoothing	RegSz	2		□	□

Value name: ActiveWndTrackTimeout

Value type: RegDword

Value: 0

□ Key: Control Panel\Desktop | Value: ActiveWndTrackTimeout

Selected hive: NTUSER.DAT | Last write: 2023-01-29 16:25:25 | 45 of 45 values shown (100.00%) | Load complete | Hidden keys: 0 | 1

The tool can be downloaded from https://f001.backblazeb2.com/file/EricZimmermanTools/net6/RegistryExplorer.zip.

LNK Files

LNK files are the shortcut files that serve as a quick access to frequently used files, folders, or programs on the system. These files typically have a `.lnk` file extension and can be found in locations such as the desktop, start menu, and recent documents folder.

Whenever a file is accessed for the first time, a `.lnk` file gets created in the Recents folder. This information is particularly useful in identifying when a file was first accessed.

These files are usually found in:

- `C:\Users\%USERNAME%\Recent`
- `C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Windows\Recent`
- `C:\Users\%USERNAME%\AppData\Roaming\Microsoft\Office\Recent`
- `C:\Users\%USERNAME%\Desktop`

One way to explore LNK files and extract useful information from them is by using a tool called LECmd. We can use it to extract original full path of the file, the date and time the file was created, last modified, last accessed, the desktop name, and the MAC address of the system where the file was created.

The tool can be downloaded from https://github.com/EricZimmerman/LECmd and here's how you can use it to extract useful information from a `.lnk` file:

```
PS C:\Tools\LECmd> LECmd.exe -f passwd.lnk
LECmd version 1.5.0.0

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

Command line: -f .\passwd.lnk

Warning: Administrator privileges not found!


Processing C:\Tools\LECmd\passwd.lnk

Source file: C:\Tools\LECmd\passwd.lnk
  Source created:  2021-03-15 08:25:27
  Source modified: 2021-03-15 10:36:47
  Source accessed: 2023-01-28 16:24:36

--- Header ---
  Target created:  2021-03-15 08:25:07
  Target modified: 2021-03-15 08:26:59
  Target accessed: 2021-03-15 08:27:07

  File size: 13
  Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, HasWorkingDir, IsUnicode, DisableK
nownFolderTracking
  File attributes: FileAttributeArchive
  Icon index: 0
  Show window: SwNormal (Activates and displays the window. The window is restored to its
 original size and position if the window is minimized or maximized.)

Relative Path: ..\..\..\..\..\Desktop\passwd.txt
Working Directory: C:\Users\Challenger\Desktop

--- Link information ---
Flags: VolumeIdAndLocalBasePath

>> Volume information
  Drive type: Fixed storage media (Hard drive)
  Serial number: 02916957
  Label: (No label)
  Local path: C:\Users\Challenger\Desktop\passwd.txt

--- Target ID information (Format: Type ==> Value) ---

  Absolute path:

  -File ==> (None)
    Short name: passwd.txt
    Modified:    2021-03-15 08:27:00
    Extension block count: 1

<SNIP>

--- End Target ID information ---

--- Extra blocks information ---

>> Tracker database block
   Machine ID:  desktop-rsrl4hd
   MAC Address: 08:00:27:2a:dc:e0
   MAC Vendor:  PCS SYSTEMTECHNIK
   Creation:    2021-03-11 06:29:01

   Volume Droid:       c2c1754c-762e-4361-8c04-e690782765de
   Volume Droid Birth: c2c1754c-762e-4361-8c04-e690782765de
   File Droid:         119740ae-8233-11eb-9779-0800272adce0
   File Droid birth:   119740ae-8233-11eb-9779-0800272adce0

<SNIP>

---------- Processed C:\Tools\LECmd\passwd.lnk in 0.25970300 seconds ----------
```

Web Browsers

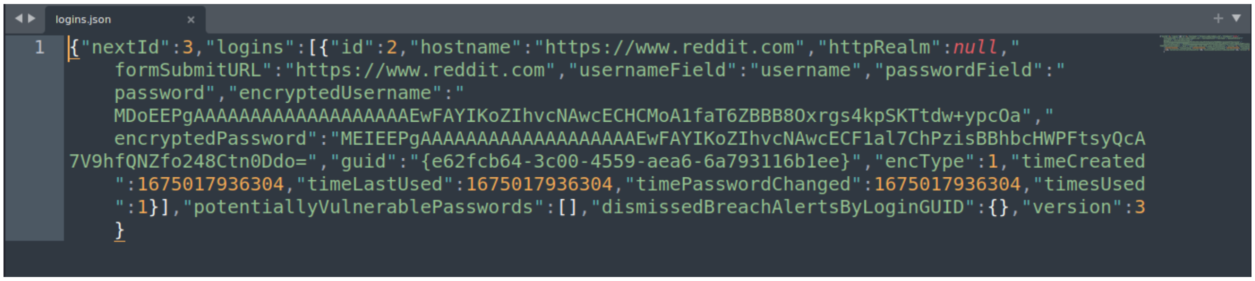
Web browsers are used globally for accessing websites. In the context of digital forensics, web browsers can provide a wealth of information about a user's browsing history, cookies, downloaded files, saved passwords, and much more. This information can be used to determine what a user might have been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

To view `.json` files, we can use any text editor as shown in the image below.



```
{"nextId":3,"logins":[{"id":2,"hostname":"https://www.reddit.com","httpRealm":null,"
    formSubmitURL":"https://www.reddit.com","usernameField":"username","passwordField":"
    password","encryptedUsername":"
    MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECHCMoA1faT6ZBBB8Oxrgs4kpSKTtdw+ypcOa","
    encryptedPassword":"MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECF1al7ChPzisBBhbcHWPFtsyQcA
7V9hfQNZfo248Ctn0Ddo=","guid":"{e62fcb64-3c00-4559-aea6-6a793116b1ee}","encType":1,"timeCreated
    ":1675017936304,"timeLastUsed":1675017936304,"timePasswordChanged":1675017936304,"timesUsed
    ":1}],"potentiallyVulnerablePasswords":[],"dismissedBreachAlertsByLoginGUID":{},"version":3
    }
```

However, the `.sqlite` files require a DB Browser such as `sqlitebrowser` that comes built-in with Kali Linux. Here's how we can use `sqlitebrowser` to view `.sqlite` files:

```
$ sqlitebrowser places.sqlite
```

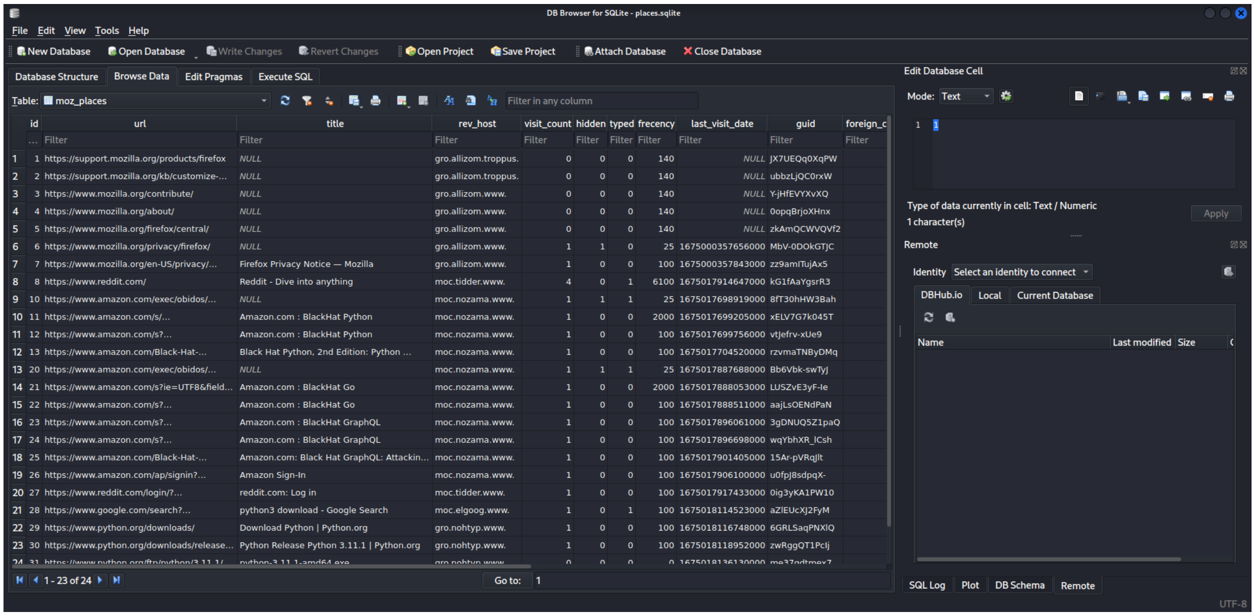


Table: moz_places

	id	url	title	rev_host	visit_count	hidden	typed	frecency	last_visit_date	guid	foreign_c
	...	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	1	https://support.mozilla.org/products/firefox	NULL	gro.allizom.troppus.	0	0	0	140	NULL	JX7UEQq0XqPW	
2	2	https://support.mozilla.org/kb/customize-...	NULL	gro.allizom.troppus.	0	0	0	140	NULL	ubbzLjQC0rxW	
3	3	https://www.mozilla.org/contribute/	NULL	gro.allizom.www.	0	0	0	140	NULL	Y-jHfEVYXvXQ	
4	4	https://www.mozilla.org/about/	NULL	gro.allizom.www.	0	0	0	140	NULL	0opqBrjoXHnx	
5	5	https://www.mozilla.org/firefox/central/	NULL	gro.allizom.www.	0	0	0	140	NULL	zkAmQCWVQVf2	
6	6	https://www.mozilla.org/privacy/firefox/	NULL	gro.allizom.www.	1	1	0	25	1675000357656000	MbV-0DOkGTJC	
7	7	https://www.mozilla.org/en-US/privacy/...	Firefox Privacy Notice — Mozilla	gro.allizom.www.	1	0	0	100	1675000357843000	zz9amITujAx5	
8	8	https://www.reddit.com/	Reddit - Dive into anything	moc.tidder.www.	4	0	1	6100	1675017914647000	kG1fAaYgsrR3	
9	10	https://www.amazon.com/exec/obidos/...	NULL	moc.nozama.www.	1	1	1	25	1675017698919000	8fT30hHW3Bah	
10	11	https://www.amazon.com/s/...	Amazon.com : BlackHat Python	moc.nozama.www.	1	0	0	2000	1675017699205000	xELV7G7k045T	
11	12	https://www.amazon.com/s?...	Amazon.com : BlackHat Python	moc.nozama.www.	1	0	0	100	1675017699756000	vtJefrv-xUe9	
12	13	https://www.amazon.com/Black-Hat-...	Black Hat Python, 2nd Edition: Python ...	moc.nozama.www.	1	0	0	100	1675017704520000	rzvmaTNByDMq	
13	20	https://www.amazon.com/exec/obidos/...	NULL	moc.nozama.www.	1	1	1	25	1675017887688000	Bb6Vbk-swTyJ	
14	21	https://www.amazon.com/s?ie=UTF8&field...	Amazon.com : BlackHat Go	moc.nozama.www.	1	0	0	2000	1675017888053000	LUSZvE3yF-Ie	
15	22	https://www.amazon.com/s?...	Amazon.com : BlackHat Go	moc.nozama.www.	1	0	0	100	1675017888511000	aajLsOENdPaN	
16	23	https://www.amazon.com/s?...	Amazon.com : BlackHat GraphQL	moc.nozama.www.	1	0	0	100	1675017896061000	3gDNUQ5Z1paQ	
17	24	https://www.amazon.com/s?...	Amazon.com : BlackHat GraphQL	moc.nozama.www.	1	0	0	100	1675017896698000	wqYbhXR_lCsh	
18	25	https://www.amazon.com/Black-Hat-...	Amazon.com: Black Hat GraphQL: Attackin...	moc.nozama.www.	1	0	0	100	1675017901405000	15Ar-pVRqJlt	
19	26	https://www.amazon.com/ap/signin?...	Amazon Sign-In	moc.nozama.www.	1	0	0	100	1675017906100000	u0fpJ8sdpqX-	
20	27	https://www.reddit.com/login/?...	reddit.com: Log in	moc.tidder.www.	1	0	0	100	1675017917433000	0ig3yKA1PW10	
21	28	https://www.google.com/search?...	python3 download - Google Search	moc.elgoog.www.	1	0	1	100	1675018114523000	aZlEUcXJ2FyM	
22	29	https://www.python.org/downloads/	Download Python | Python.org	gro.nohtyp.www.	1	0	0	100	1675018116748000	6GRLSaqPNXlQ	
23	30	https://www.python.org/downloads/release...	Python Release Python 3.11.1 | Python.org	gro.nohtyp.www.	1	0	0	100	1675018118952000	zwRggQT1PcIj	
24	31	https://www.python.org/ftp/python/3.11.1/	python-3.11.1-amd64.exe	gro.nohtyp.www.	0	0	0	0	1675018136130000	me37qdtmex7	

1 - 23 of 24

Go to: 1

Mode: Text

1

Type of data currently in cell: Text / Numeric
1 character(s)

Identity: Select an identity to connect

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.

The following commands demonstrate how to download and use this tool.

```
$ git clone https://github.com/unode/firefox_decrypt
Cloning into 'firefox_decrypt'...
remote: Enumerating objects: 1163, done.
remote: Counting objects: 100% (275/275), done.
remote: Compressing objects: 100% (40/40), done.
remote: Total 1163 (delta 250), reused 238 (delta 233), pack-reused 888
Receiving objects: 100% (1163/1163), 414.55 KiB | 1.14 MiB/s, done.
Resolving deltas: 100% (732/732), done.
```

```
$ python3 firefox_decrypt.py hxdvwqnb.default-release

Website:   https://www.facebook.com
Username: 'john.doe@example.com'
Password: 'my_password123'

Website:   https://twitter.com
Username: 'john_doe'
Password: 'my_twitter_password123'

Website:   https://google.com
```

```
Username: 'john.doe@gmail.com'
Password: 'some_random_p4ssw0rd'
```

Chrome

While we covered in detail how to extract saved passwords from Firefox using the `firefox_decrypt` tool, we will not be diving into the process of extracting saved passwords from Chrome. However, It’s worth noting that 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

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.

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`

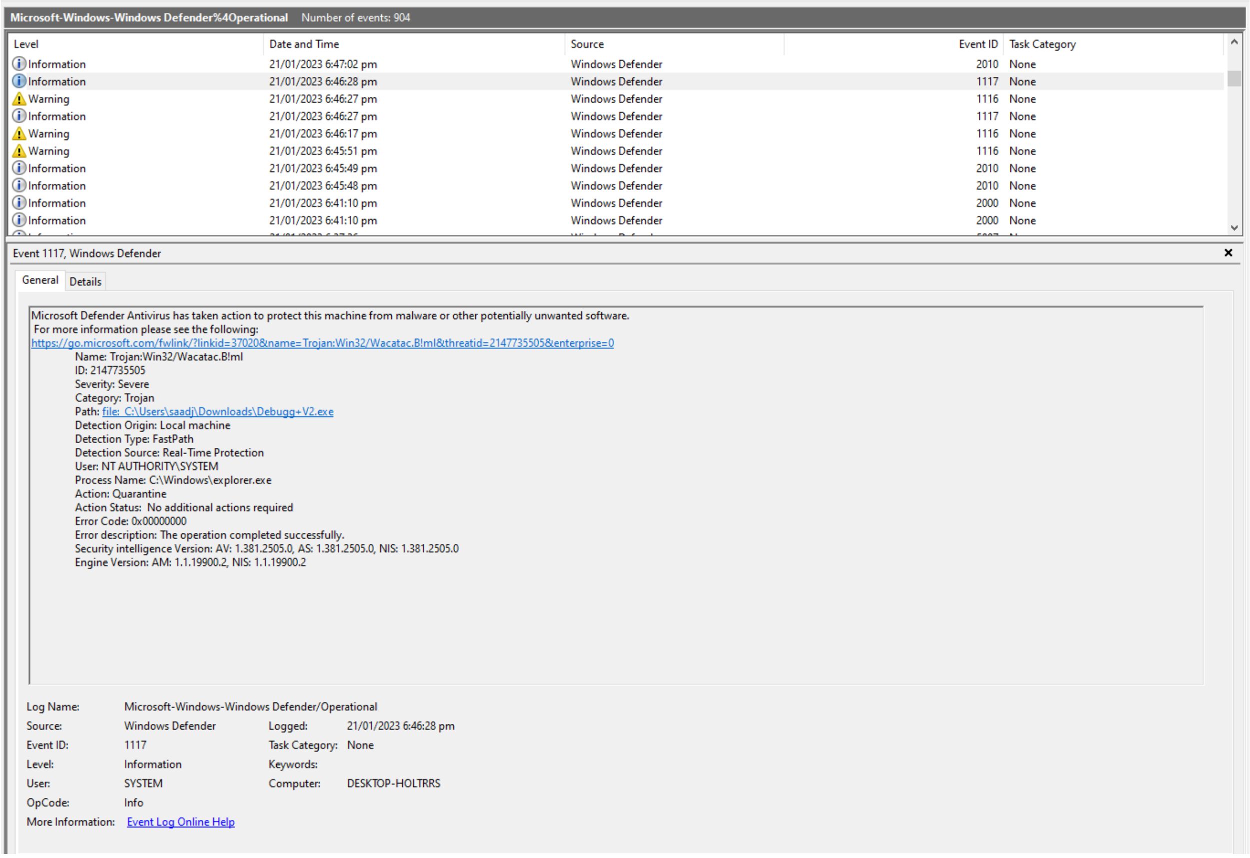
However, it's worth noting that these are not the only files that may be useful during a digital forensics investigation, but for this lab, we are interested in these files only.

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:

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.

Here’s an example of event ID `1117` in the file `Microsoft-Windows-Windows Defender%4Operational.evtx`, viewed using the built-in Event Viewer.



Microsoft-Windows-Windows Defender%4Operational   Number 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

```
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\saadj\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: AM: 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		

Exercises

1. Given the registry file of a system that was compromised, answer the following:
    a. What’s the mouse double-click speed?
    b. What’s the most recent typed path accessed as recorded in the registry?
    c. What’s the new value added to the registry by the malware in order to establish persistence over the system?

    The registry file can be downloaded from https://github.com/vonderchild/digital-forensics-lab/blob/main/Lab 2/files/NTUSER.DAT

2. Given the Firefox profile of a suspect, answer the following:
    a. What’s the username and password stored in the saved logins?
    b. What’s the most frequently visited website?
    c. What’s the name of the file downloaded by the suspect?

    The Firefox profile can be downloaded from https://github.com/vonderchild/digital-forensics-lab/blob/main/Lab 2/files/Firefox.zip

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

    The event logs file can be downloaded from https://github.com/vonderchild/digital-forensics-lab/blob/main/Lab 2/files/Microsoft-Windows-PowerShell%254Operational.evtx