2022

WINDOWS FORENSICS

BY : ABDULLAH ALI ALHAKAMI | ABDULAZIZ HASSAN ALZAHRANI

CYBER SECURITY DEPARTMENT | UNIVERSITY OF JEDDAH | JEDDAH | KINGDOM OF SAUDI ARABIA

Table of Contents

1.INTRODUCTION

The branches of digital forensics are divided based on the type of digital devices. There are computer forensics, network forensics, USB forensics, mobile forensics, and a lot more.

The importance of digital forensics to resolve cybercrime and identify a fingerprint on devices to catch the criminal and many more. Investigations in digital forensics might use a variety of techniques depending on these factors. This research report paper will explain the methodology and strategy for the personal computer (windows 10 OS).

1.1 Computer Digital forensics

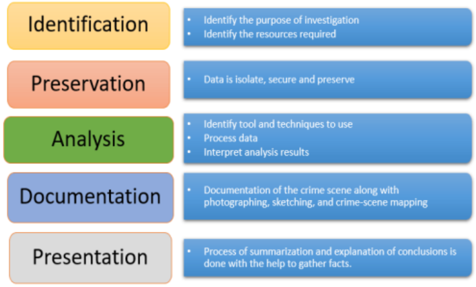
Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. Computer forensics aims to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.[1]

1.2 Windows Digital forensics

While we will investigate on windows 10 OS we can take advantage of the new features in Windows 10 like notification center, Cortana, Microsoft edge, multi-tasking, Xbox, universal apps, and windows store to help us in our investigation. Other sources for evidence location and forensic analysis the random access memory (RAM), which will help us to investigate a lot of artifacts such as windows registry hives, web browsers, email, and social networking applications installed on the system and the running process which will help us to detect the malware behavior and other things.

1.3 Digital forensics life cycle [Fig.1]

- Identification: It is the initial phase in the forensic investigation. The identification process primarily entails determining what evidence is there, where it is held, and, finally, how it is stored (in which format).
- Preservation: Data is isolated, secured, and kept throughout this period. Preventing someone from utilizing the digital device ensures that digital evidence is not tampered with.
- Analysis: In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.[2]
- Documentation: In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping. [2]
- Presentation: In this last step, the process of summarization and explanation of conclusions is done.[2]



Identification
- Identify the purpose of investigation
- Identify the resources required

Preservation
- Data is isolate, secure and preserve

Analysis
- Identify tool and techniques to use
- Process data
- Interpret analysis results

Documentation
- Documentation of the crime scene along with photographing, sketching, and crime-scene mapping

Presentation
- Process of summarization and explanation of conclusions is done with the help to gather facts.

Fig.1 Digital forensics life cycle [2]

2. Artifacts in windows 10

Digital forensics on windows divide into two sections system and user artifacts. System artifacts are data that can be acquired about system activity in reaction to stimulation. The term "user artifacts" refers to artifacts discovered in connection with user activity and/or files utilized by the user.

2.1 Jump Lists

Jump list files will show us the recently visited [Fig.3] and frequently files and it also links to pinned files. Notice that each application has there own jump list file.

2.2 Thumbnails

When the user selects the Windows folder viewing option's Thumbnails or Filmstrip views, a tiny Thumbnails version of the photographs is generated and saved in a single file. it is impossible to get back the pictures if the user deletes the thumbnail files but it hasn't deleted it recovery will be possible.

2.3 Windows Search History

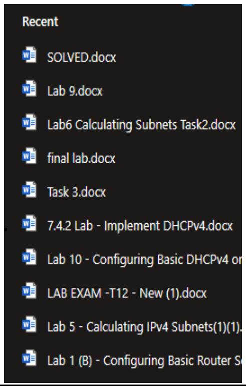
This feature has been introduced since windows 8.1 it allows the user to search for anything on his machine. The forensics value of this feature is that we can know the first date and time the user search for a specific word.

2.3 Prefetch Files

This prefetch file is created when the user executes any Portable Executable to make the windows performance more efficient to perform fast loading the next time executing the same portable executable. The benefit we can take from the prefetch file we can know how many times the executable ran and when is the last time.

2.4 shortcut (.lnk) files

Shortcut files according to Microsoft its object contain data about another object(The real file). Notice shortcut files contain metadata that will help windows performance and also help us as digital forensics investigators. these file has their own MAC timestamps.



Recent

SOLVED.docx

Lab 9.docx

Lab6 Calculating Subnets Task2.docx

final lab.docx

Task 3.docx

7.4.2 Lab - Implement DHCPv4.docx

Lab 10 - Configuring Basic DHCPv4 or

LAB EXAM -T12 - New (1).docx

Lab 5 - Calculating IPv4 Subnets(1)(1).

Lab 1 (B) - Configuring Basic Router S

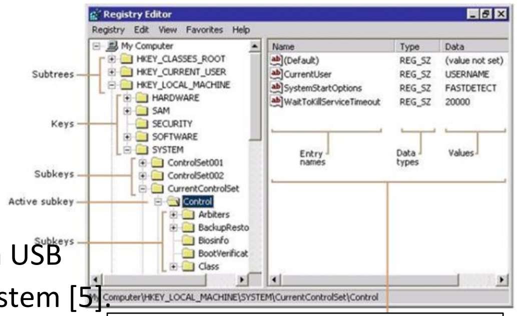
Fig.3 recently visited in MS word[2]

2.5 Windows Registry

The registry is like the configuration for the windows operation system [Fig.4]. We can find a lot of artifacts if we knew how to investigate them. The windows registry is divided into two parts, the System registry, and the User Registry. Investigating these registry files is very simple if we knew where to look. Common locations [4].

2.6 USB

Every day, USB devices are utilized for a variety of purposes. In some cases, the problem was caused because the attacker did only attach a USB device [Fig.5]. Even if the USB is removed the details are still in the system [5].



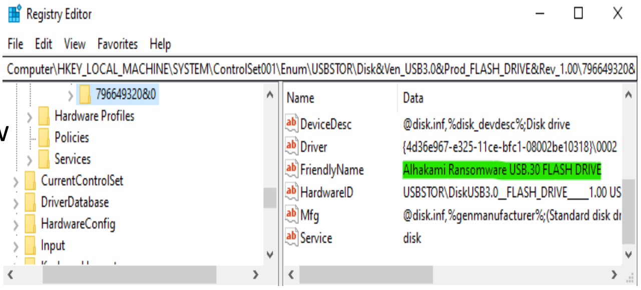
Name	Type	Data
(Default)	REG_SZ	(value not set)
CurrentUser	REG_SZ	USERNAME
SystemStartOptions	REG_SZ	FASTDETECT
WaitToKillServiceTimeout	REG_SZ	20000

My Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control

Fig.4 Windows Registry structure [3]

2.7 ShellBags

When the users using Windows Explorer all the data save on NTUser.dat and USRClass.dat registry. it's Containing the view , icon, position, and size of folders. As a digital investigator you can find multiple timestamps and other pieces of information that refer to evidence that was present at one time. Even after the original folders, files, and physical devices have been removed from the system, information remains.



Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_USB3.0&Prod_FLASH_DRIVE&Rev_1.00\796649320&

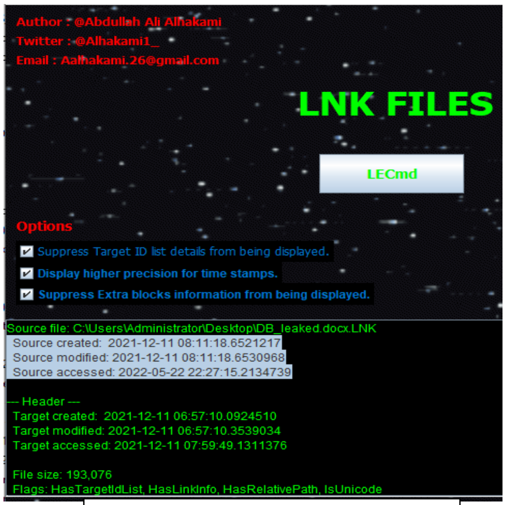
Name	Data
DeviceDesc	@disk.inf,%disk_devdesc%;Disk drive
Driver	{4d36e967-e325-11ce-bfc1-08002be10318}\0002
FriendlyName	Alhakami Ransomware USB.30 FLASH DRIVE
HardwareID	USBSTOR\DiskUSB3.0_FLASH_DRIVE____1.00 US
Mfg	@disk.inf,%genmanufacturer%;(Standard disk dr
Service	disk

Fig.5 Details of USB devices stored in the registry

2.8 Browser

Web browsers are currently the most common computer application. Artifacts created by nearly all web browsers are divided into three sections.

- History: time and date for the website user visited.
- Cache: Store local copies of data that is retrieved.
- Cookies: Small bits of info. that a site may instruct a browser to store such as site preference and maintain session information.


Author : @Abdullah Ali Alhakami
Twitter : @Alhakami1_
Email : Aalhakami.26@gmail.com

☑ Suppress Target ID list details from being displayed.
☑ Display higher precision for time stamps.
☑ Suppress Extra blocks information from being displayed.

```
Source file: C:\Users\Administrator\Desktop\DB_leaked.docx.LNK
 Source created:  2021-12-11 08:11:18.6521217
 Source modified: 2021-12-11 08:11:18.6530968
 Source accessed: 2022-05-22 22:27:15.2134739

--- Header ---
 Target created:  2021-12-11 06:57:10.0924510
 Target modified: 2021-12-11 06:57:10.3539034
 Target accessed: 2021-12-11 07:59:49.1311376

 File size: 193,076
 Flags: HasTargetIdList, HasLinkInfo, HasRelativePath, IsUnicode
```

Fig.6 shortcut file MAC timestamp

2.8.1 Internet Explorer

It is pre-installed on the Windows operating system and is the most widely used browser in major corporations. autocomplete, typed URLs, and Preferences are all stored in the Windows Registry. All of the cache, bookmarks, and cookies are saved in the File System.

Artifact location [6] :

• Cache :

- \%USERPROFILE%\AppData\Local\Microsoft\Windows\Temporary Internet Files\

• Bookmarks :

- \%USERPROFILE%\Favorites

• Cookies :

- \%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies
- \%USERPROFILE%\AppData\Roaming\Microsoft\Windows\Cookies\Low

2.9 Random Access Memory (RAM)

Investigation of the random access memory is a very important step because it may have a very important artifact. It will also help us to be able to identify the process that was running in the device, In case the device is infected by malware, we can analyze the behavior of malware.

2.10 Volume ShadowCopy Service (VSS)

VSS (Volume Shadow Copy Service) is a collection of Microsoft Windows Component Object Model (COM) interfaces that provide the framework for doing volume backups and producing reliable, point-in-time copies of data (known as shadow copies). VSS produces consistent shadow copies by coordinating business applications, backup programs, fast-recovery solutions, file system services, and storage hardware. In addition provides find them named as restore points. snapshots sometimes find them named as restore points.

3.Conclusion

The Windows operating system is the most widely used in businesses and organizations. They believe that by just removing traces of their errors, all would be resolved. What they don't realize is that we can recover the data utilizing the correct digital forensics approach and tools. That artifacts shows the Windows digital forensics Investigation specially Windows 10 OS, and what are the evidences for digital forensics investigator that should looking for to use it. An investigator is required to have a strong knowledge of the underlying technology as well as the ability to use tools of Digital Forensics to support him in his investigation.

References

[1] What is Computer Forensics (Cyber Forensics)? (techtarget.com)

[2] What is Digital Forensics? History, Process, Types, Challenges (guru99.com)

[3] Windows Architecture - Registry 101 - Microsoft Tech Community

[4] Forensic Analysis of the Windows Registry - Forensic Focus

[5] USB Forensics: Find the History of Every Connected USB Device on Your Computer | Cybrary

[6] Windows Forensic Analysis | SANS Poster