

LAB **** – System Navigation & System Auditing Basics

Learning Outcomes :

- Navigating in a Drive, Searching for Files, Establish Files and Folders Properties
- System Auditing Basics

Instructions:

The lab notes provided are designed just to provide instruction on some of the activities which you are expected to be familiar with. They do NOT provide a comprehensive set of notes on the activities you will undertake in the lab as not all the required information is provided in these notes. It is important that YOU make YOUR OWN NOTES which you can later refer to for studying purposes.

Warning:

Students are reminded of the module Code of Conduct & Ethics and must ensure they have permission from the proper individuals before using any of the techniques described within, and respect all the relevant laws surrounding computer usage and data protection.

Introduction:

Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law to resolve litigations and cases. It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. The report, or findings are then presented on a Court of Law for the purpose of delivering Justice.

Let's have a preliminary play and basic understanding using windows system, and use some of the utilities and features provided by the Microsoft Windows Systems to see what lies beneath and will be helpful in an investigation. Although these activities and utilities may seem simple, it is important to have a clear understanding of the basic concepts so as to ensure you'll be able to complete further investigations using these basics as a reference.

Learning Outcome 1 : Navigating in a Drive, Searching for Files, Establish Files and Folders Properties

The tasks outlined above could be done in a GUI interface as well as Command interface. Since we will be using a Windows system as informed earlier we will primarily focus on GUI interface, some of the command functions will also be explained, however we will not deep dive into the command

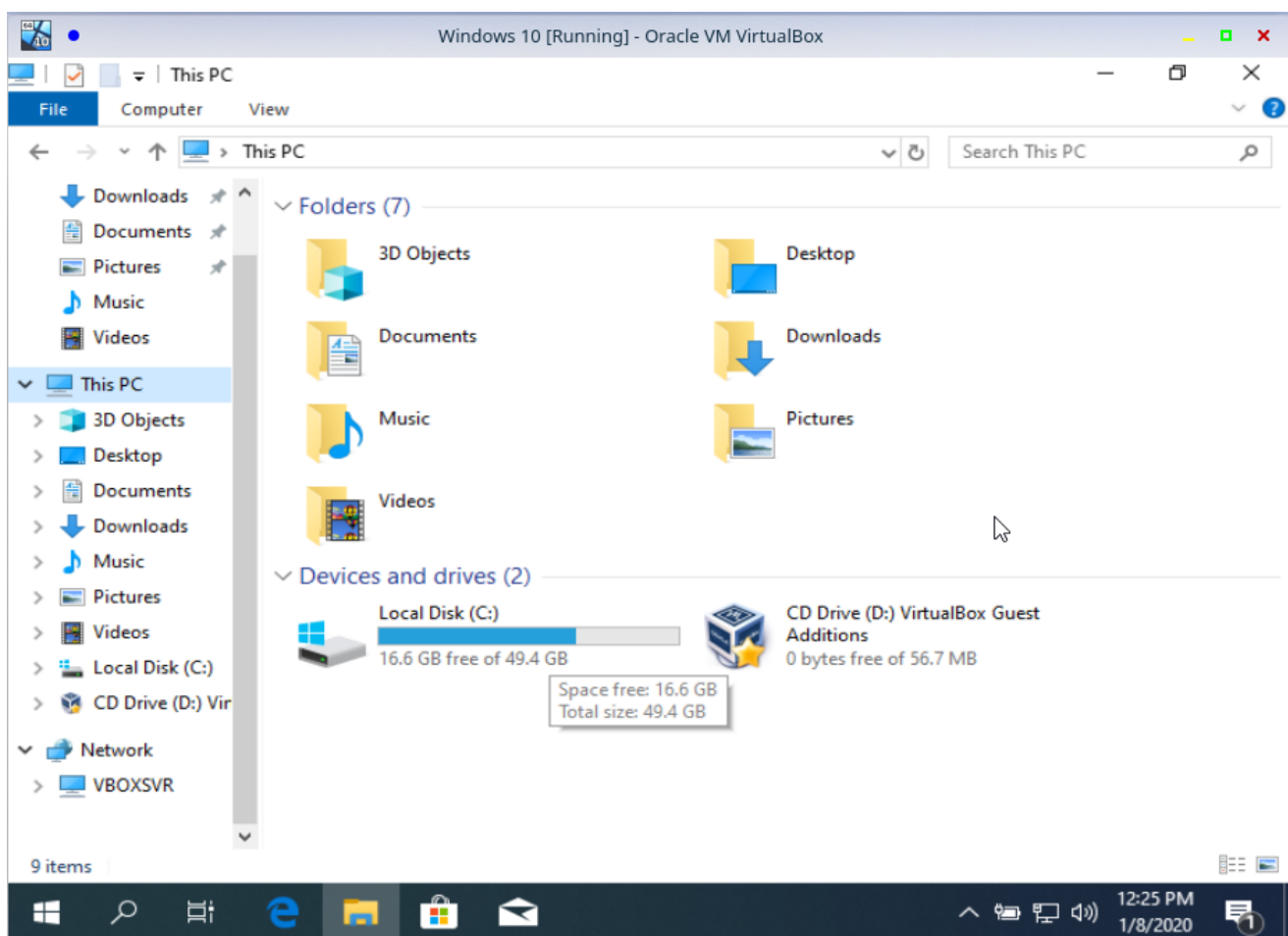
interface and expect you all to do the research regarding the tasks performed and their alternative command lines.

Windows Explorer allows the user to navigate and browse the files and folders on your Windows computer. Any time you open a folder on your Windows computer, you're using Windows Explorer.

Lets dive into the Windows Explorer for the purpose.

Task 1 : Navigating in a Drive

- **Click the Start button.** This button can be found in the lower-left corner of the screen, and may just be a Windows logo.
- **Click the Computer or File Explorer button.** In Windows 10, this looks like a folder and can be found on the left side of the menu, or in your Windows task bar at the bottom of the screen.
- **Click This PC in the left sidebar (Window 10).** This will display the drives connected to your computer.

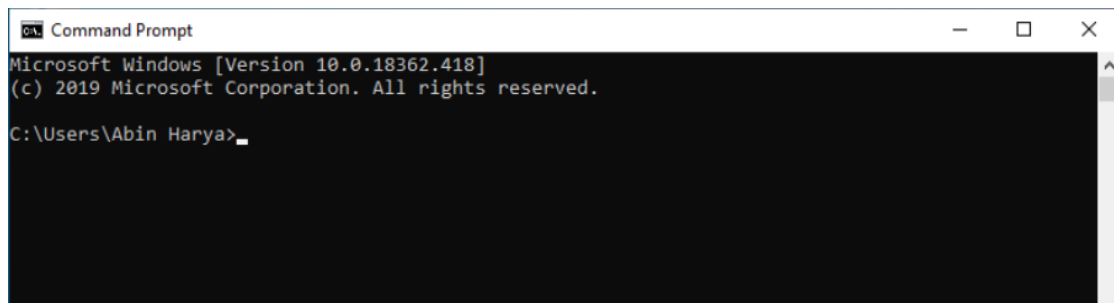


- To see what's on your hard drive, under Devices and Drives, double-click the drive you want to see. To find a file or folder on a floppy disk, CD-ROM, or other media, under Devices with Removable Storage, double-click the item you want to see. Alternatively to find a file in a folder, under Folders, double-click a folder.

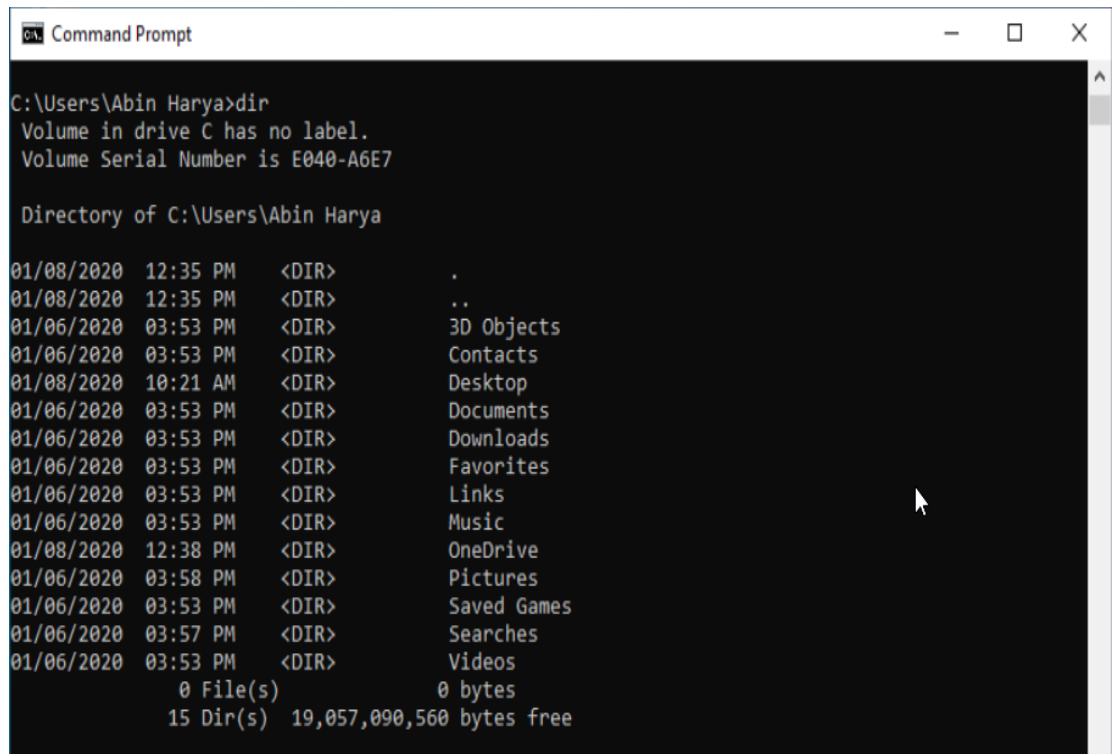
- **Using Command Prompt**

To establish the similar information (it does not always appear the same way) you can use the command prompt as well.

- Open the run box Windows + R shortcut, alternatively click the Start button, select the Run and type 'cmd' for the command window.



- **Note your current folder.** When you start the Command Prompt, you'll start in your User folder (Abin Harya as shown in screenshot)
- **Type `dir` and press enter.** This will display the contents of the current directory. The screen will stop scrolling whenever the screen has filled, and you can press any key to keep scrolling.
 - `<DIR>` entries are folders inside of your current directory.
 - The size of each file will be displayed in bytes before the file name.



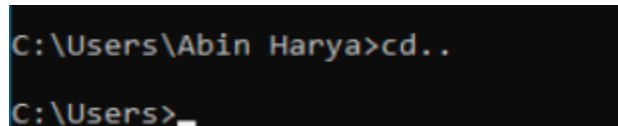
```
Command Prompt

C:\Users\Abin Harya>dir
Volume in drive C has no label.
Volume Serial Number is E040-A6E7

Directory of C:\Users\Abin Harya

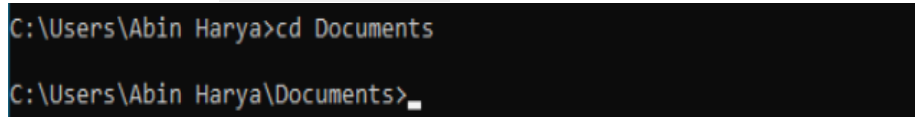
01/08/2020  12:35 PM  <DIR>          .
01/08/2020  12:35 PM  <DIR>          ..
01/06/2020  03:53 PM  <DIR>          3D Objects
01/06/2020  03:53 PM  <DIR>          Contacts
01/08/2020  10:21 AM  <DIR>          Desktop
01/06/2020  03:53 PM  <DIR>          Documents
01/06/2020  03:53 PM  <DIR>          Downloads
01/06/2020  03:53 PM  <DIR>          Favorites
01/06/2020  03:53 PM  <DIR>          Links
01/06/2020  03:53 PM  <DIR>          Music
01/08/2020  12:38 PM  <DIR>          OneDrive
01/06/2020  03:58 PM  <DIR>          Pictures
01/06/2020  03:53 PM  <DIR>          Saved Games
01/06/2020  03:57 PM  <DIR>          Searches
01/06/2020  03:53 PM  <DIR>          Videos
               0 File(s)              0 bytes
              15 Dir(s) 19,057,090,560 bytes free
```

- Type **cd ..** and press enter. This will take you up one directory level.



```
C:\Users\Abin Harya>cd ..
C:\Users>_
```

- Type **cd *folderName*** to open a folder in your directory. For example, in your User folder you can type **cd documents** and press enter to open your Documents folder.



```
C:\Users\Abin Harya>cd Documents
C:\Users\Abin Harya\Documents>_
```

- Type **cd *path*** to go to a specific directory. For example, to move directly to the Microsoft Office 15 directory in Program Files, you would type **cd C:\Program Files\Microsoft Office 15**

```
C:\Program Files>cd C:/Program Files/"Microsoft Office 15"

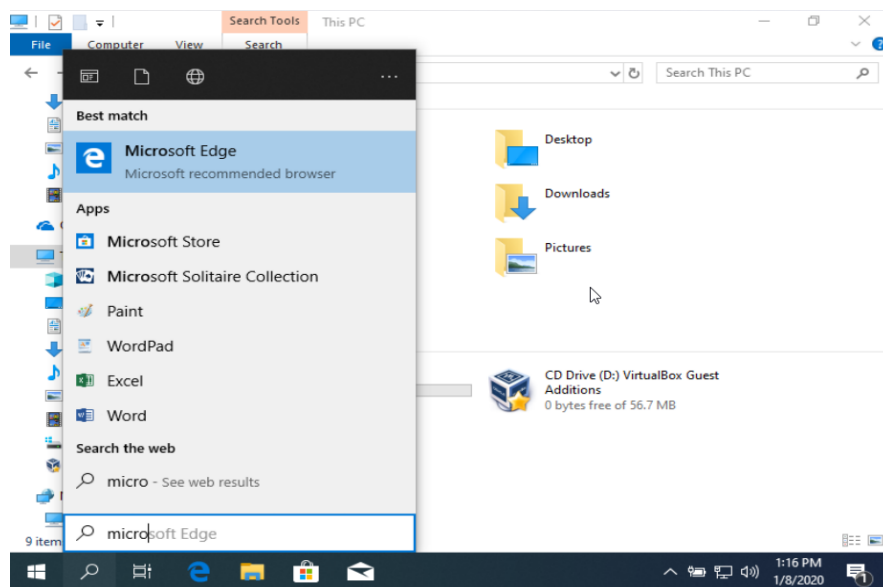
C:\Program Files\Microsoft Office 15>dir
Volume in drive C has no label.
Volume Serial Number is E040-A6E7

Directory of C:\Program Files\Microsoft Office 15

10/14/2019  01:09 PM    <DIR>          .
10/14/2019  01:09 PM    <DIR>          ..
10/14/2019  01:09 PM    <DIR>          ClientX64
               0 File(s)                0 bytes
               3 Dir(s)  19,057,541,120 bytes free
```

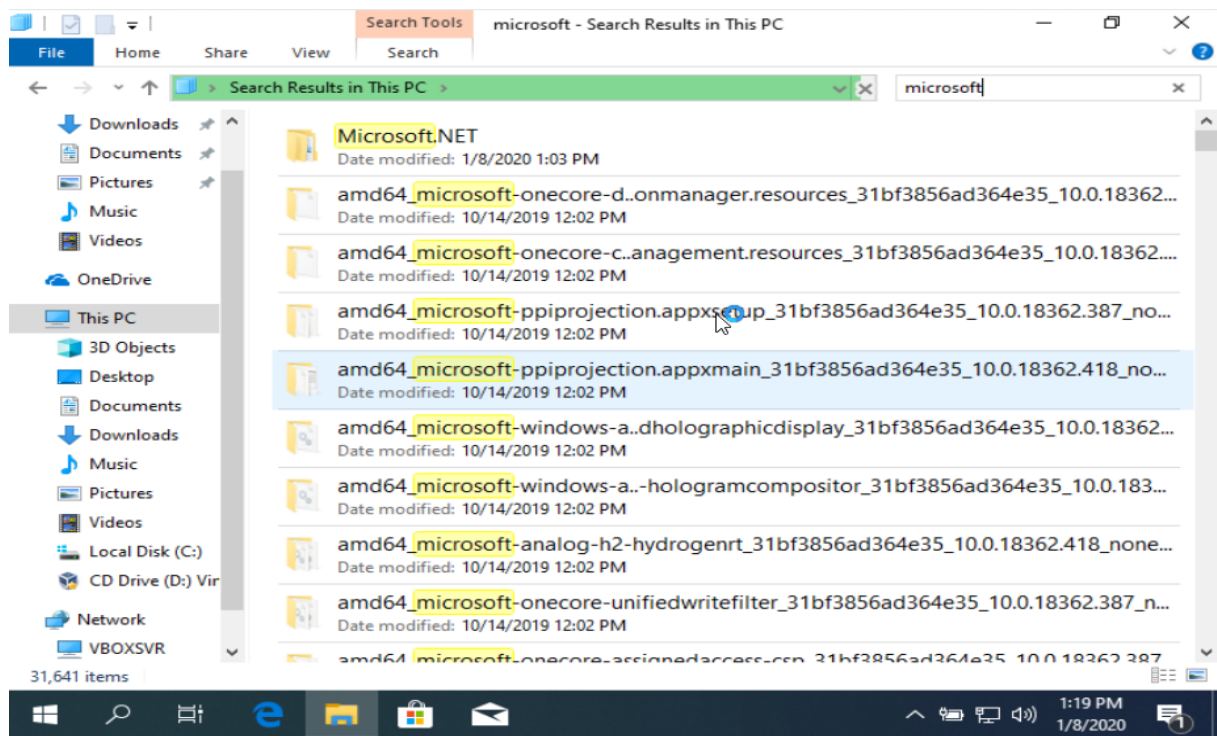
TASK 2 : Searching for a File

- **Search from the taskbar:** Type the name of a document (or a keyword from it) into the search box on the taskbar. You'll see results for documents across your PC and OneDrive under Best match.



- **Search File**

Explorer: Open **File Explorer** from the taskbar or right-click on the **Start** menu, and choose **File Explorer**, then select a location from the left pane to search or browse. For example, select **This PC** to look in all devices and drives on your computer, or select **Documents** to look only for files stored there.



➤ Using Command Prompt

- Open the run box Windows + R shortcut, alternatively click the Start button, select the Run and type 'cmd' for the command window.
- Type **cd /** This command propels you to the root directory (folder) on the main hard drive, or you may navigate to the directory by specifying a path of your choice as explained earlier in Task 1.
- Type **dir FILENAME.EXT /s** For example, if you're looking for the file hello.txt, type **hello.txt**. You can type upper- or lowercase letters. The **/s** option directs a search of all folders on the hard drive

```
CA Command Prompt
Microsoft Windows [Version 10.0.18362.418]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Abin Harya>cd /

C:\>dir hello.txt /s
Volume in drive C has no label.
Volume Serial Number is E040-A6E7

Directory of C:\Program Files\Hello

01/08/2020  01:25 PM                0 hello.txt
                        1 File(s)                0 bytes

Total Files Listed:
                1 File(s)                0 bytes
                0 Dir(s) 19,054,161,920 bytes free

C:\>
```

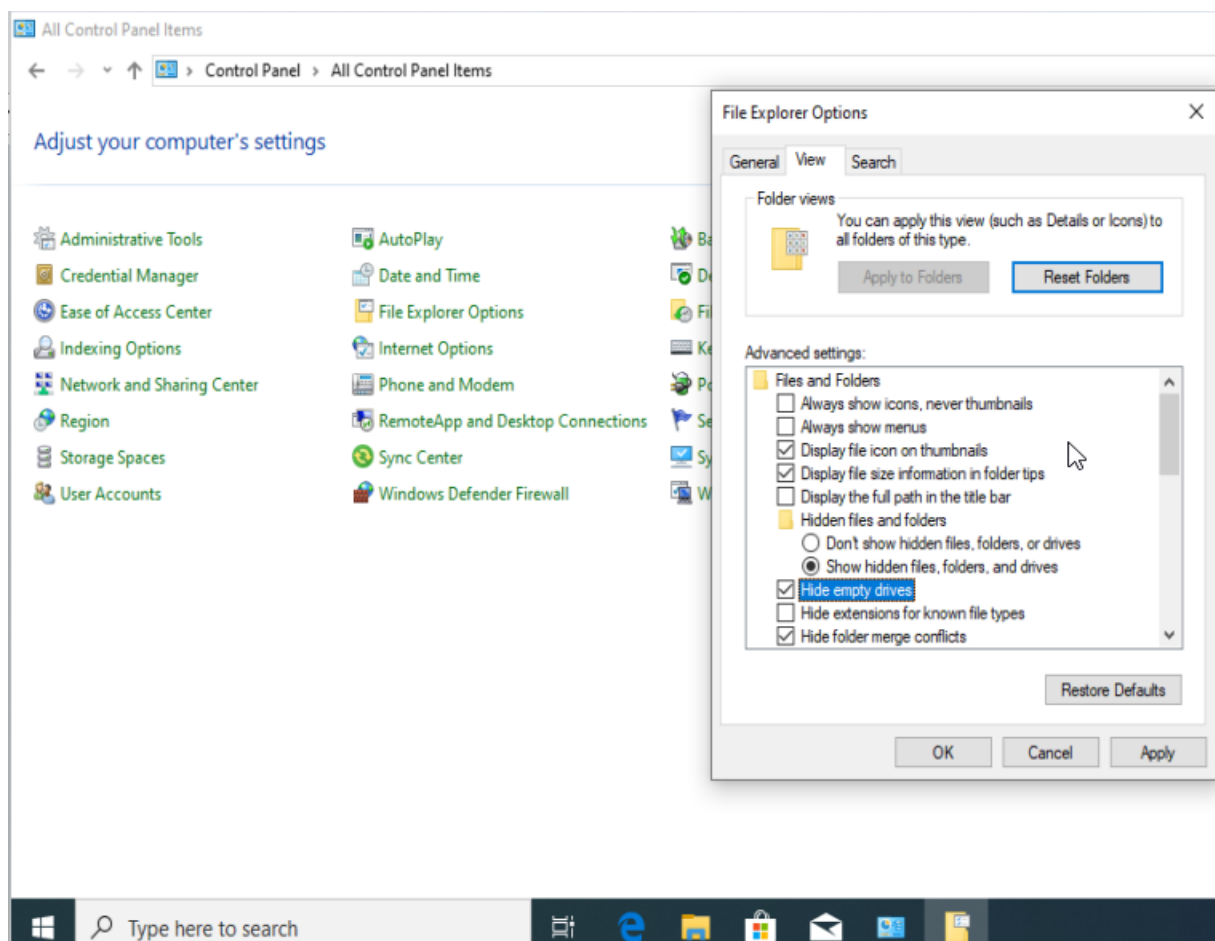
TASK 3 : Establish File and Folder Properties

File attributes are metadata associated with computer files. These are settings associated with computer files that grant or deny certain rights to how a user or the operating system can access that file as well keeps track of date a file was created and last modified, as well as the file's size and extension.

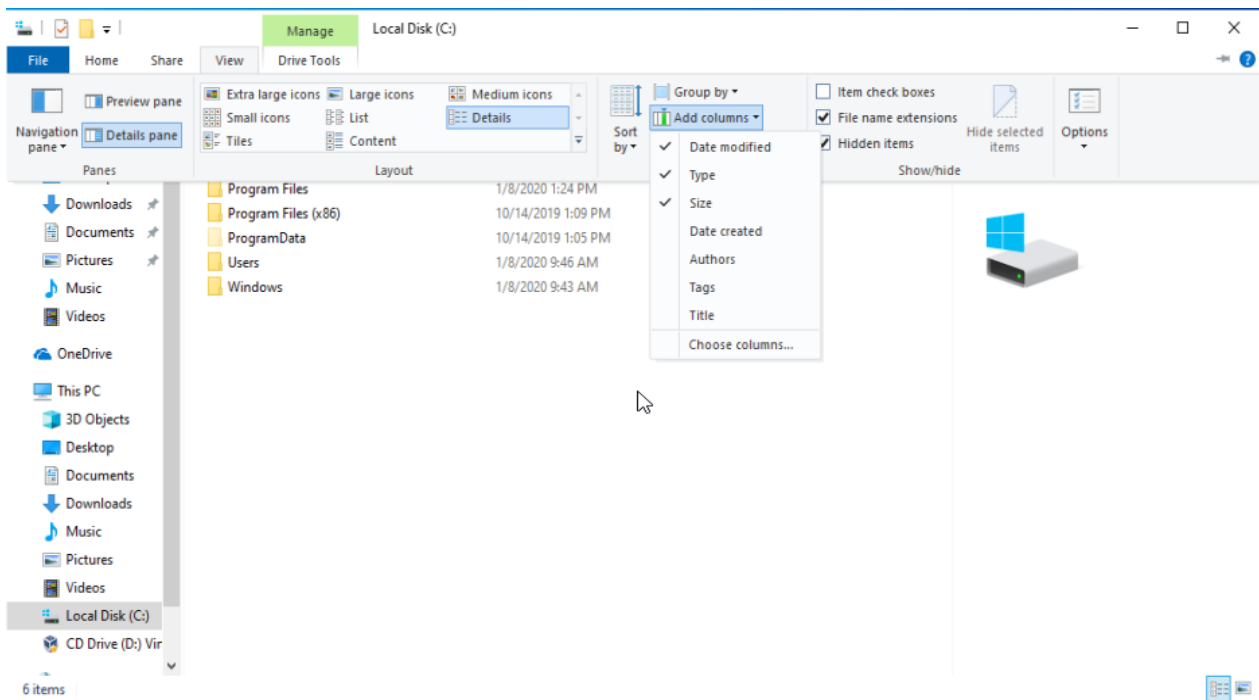
A **hidden directory** or **hidden file** is a folder or file that is not shown in a normal listing of the files contained in a directory by default. Files are hidden to protect them from change or deletion. Hidden directories are most often used to hide important operating system-related files and user preferences. Unfortunately, this functionality can also be used by malicious programs to hide their presence from unaware users. On the Apple Macintosh, hidden files are also called invisible files. By default, Windows is designed to hide hidden files, but from a forensics perspective it is important to be able to view these files.

To view more details about folders and file in Windows explorer a few setting have to be altered.

- Select **Control Panel | Appearance and Personalisation | File Explorer Options. . .** , then on the **View** tab select, under the Files and Folders section, **check** the radio button **Show hidden files and folders** and **uncheck** the button for **Hide extensions for known file types**.



- Navigate to a folder and, with a folder displayed, select **View | Details | Add Columns** and then add a few more attributes to the list. You should now get an updated display detailing more information about the files.



- You should now get a detailed view of Folders and Files.

Learning Outcome : System Auditing

System Information for Windows (SIW.EXE)

It is an advanced System Information for Windows tool that gathers detailed information about your system properties and settings and displays it in an extremely comprehensible manner. SIW is a standalone utility that does not require installation (Portable Freeware) that you can run directly from an USB flash drive, from a floppy, from a network drive or from a domain login script.

The system information that is discovered can be divided into the categories:

- **Software Inventory** (Operating System, Installed Software and Hotfixes, Processes, Services, Users, Open Files, System Uptime, Software Licenses, Secrets)
- **Hardware Inventory** (Motherboard, Sensors, BIOS, CPU, chipset, PCI/AGP, USB and ISA/PnP Devices, Memory, Video Card, etc.)
- **Network Information** (Network Cards, Network Shares, currently active Network Connections, Open Ports)
- **Network Tools** (MAC Address Changer, Neighborhood Scan, Ping, Trace, Statistics)
- **Real-time monitors** (CPU, Memory, Page File usage and Network Traffic)

Auditing the System Properties

- Download SIW (free demo online).
- If you run the SIW.exe you will find it provides a very comprehensive audit of a computer's hardware and software resources.
- If you click on the Licence tab you will discover the program installed and their associated licence keys(not for the free demo).

The screenshot shows the SIW 2019 64-bit application window. The title bar reads "SIW 2019 64-bit (Licensed To Gabriel Topala) - running on \\BOOK2-GABI". The menu bar includes File, Edit, View, Software, Hardware, Network, Tools, and Help. The left sidebar shows a tree view of system categories, with "Operating System" selected. The main pane displays the "Property" and "Value" table for the selected "Operating System" category.

Property	Value
Operating System	Windows 10
Name	Windows 10 Pro x64, version 1903 (May 2019 Update)
Version	1903 (OS Build 18362.175)
Product Name	Windows 10 Pro
Code Name	19H1
Features	64 Bit Edition, Terminal Services in Remote Admin Mode, Ta
Edition Type	Professional
Edition ID	[TH]X19-99497
Key Type	OEM:DM
EULA	OEM
SKU	0x30 Windows 10 Pro
Computer Name	BOOK2-GABI
Computer Description	Gabriel's laptop
Windows Insider Program	Disabled
Windows Sandbox	No
Language	English
Safe Mode	No
Activation Status	Activated
License Status	Licensed [Windows(R) Operating System, OEM_DM channel
Genuine	Yes
Checked Build	No
UAC Enabled	Yes
OS Root	C:\Windows\

Windows File Analyzer

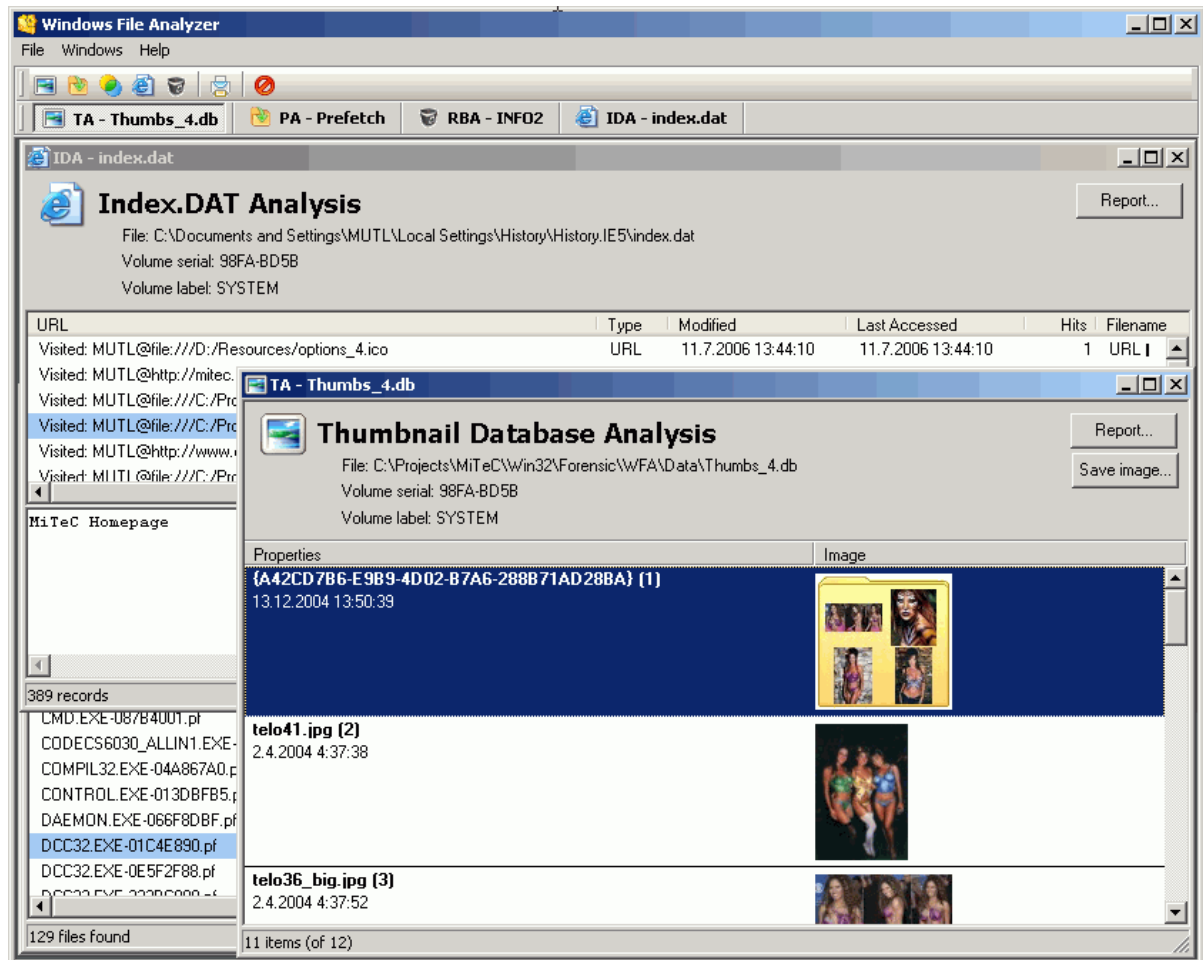
Windows File Analyzer is a tool to decode and analyze some special files used by Windows Operating System. In these files user will find some interesting information related to forensic analysis and Incident response. Every analysis results can be printed in user-friendly form.

The list of analyzer include the following analyzers:

- **Windows XP Thumbnail Database Analyzer**
This analyzer reads Thumbs.db file and displays its content with stored data include image preview.
- **ACDSee Thumbnail Database Analyzer**
This analyzer reads ACDSee *.fpt file and displays its content with stored data include image preview.
- **Google Picasa Thumbnail Database Analyzer**
This analyzer reads Picasa *.db file and displays its content with stored data include image preview.
- **FastStone Viewer Thumbnail Database Analyzer**
This analyzer reads fsviewer.db file and displays its content with stored data include image preview.
- **HP Digital Imaging Thumbnail Database Analyzer**
This analyzer reads *.db or *.dat file and displays its content with stored data include image preview.
- **Prefetch Analyzer**
It reads files stored usually in Prefetch folder and diggs out stored informaton.
- **Shortcut Analyzer**
This tool reads all shortcut files in specified folder and displays data stored in them.

- **Index.DAT Analyzer**

This analyzer reads specified Index.Dat file and displays its content. Index.Dat files store usually data of Internet Explorer cookies, temporary files or history.



- **Recycle Bin Analyzer**

This analyzer decodes and displays Info2 files that hold WinXP recycle bin content information or \$I files holding Vista and above recycle bin information.

- 1) **Thumbnail** : These are reduced-size versions of pictures or videos, used to help in recognizing and organizing them, serving the same role for images as a normal text index does for words.

The two main points of value often raised by the presence of Windows thumbnail databases are:

- A large proportion of computer users have no knowledge of the presence of Windows thumbnail databases so that whilst they might delete incriminating pictures the evidence of their illicit activity often remains in the thumbnail databases.
- The presence of pictures in a Windows thumbnail database is taken as an indicator of guilty knowledge; for the pictures to exist in the thumbnail database the folder containing the pictures must have been opened in Windows Explorer in a thumbnail view thus implying that the user must have knowledge of them.

Analysing Thumbnails

A thumbs.db file in a folder may contain information about files that are no longer present in that folder. Sometimes the program gives anomalous results – pictures not necessarily matching up to the file name. You then have to decide what has happened – has the database within thumbs.db been corrupted, or is the program not as good as you had hoped

- 1) Download the thumbs.db file on Moodle (associated to week 1 – .db file corresponds to Windows XP).
- 2) Using Windows File Analyzer analyse the file

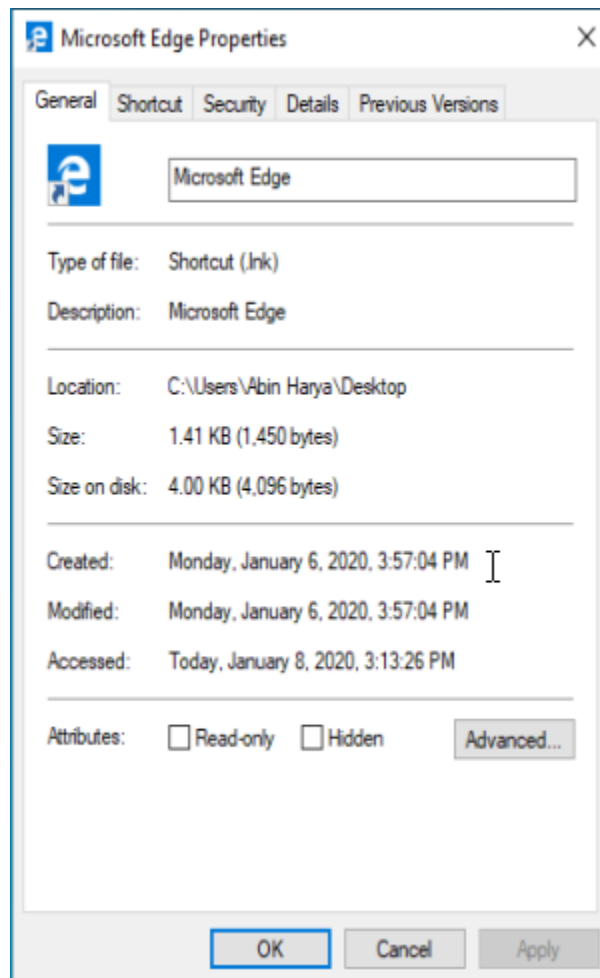
2) Windows Shortcut or Link Files :

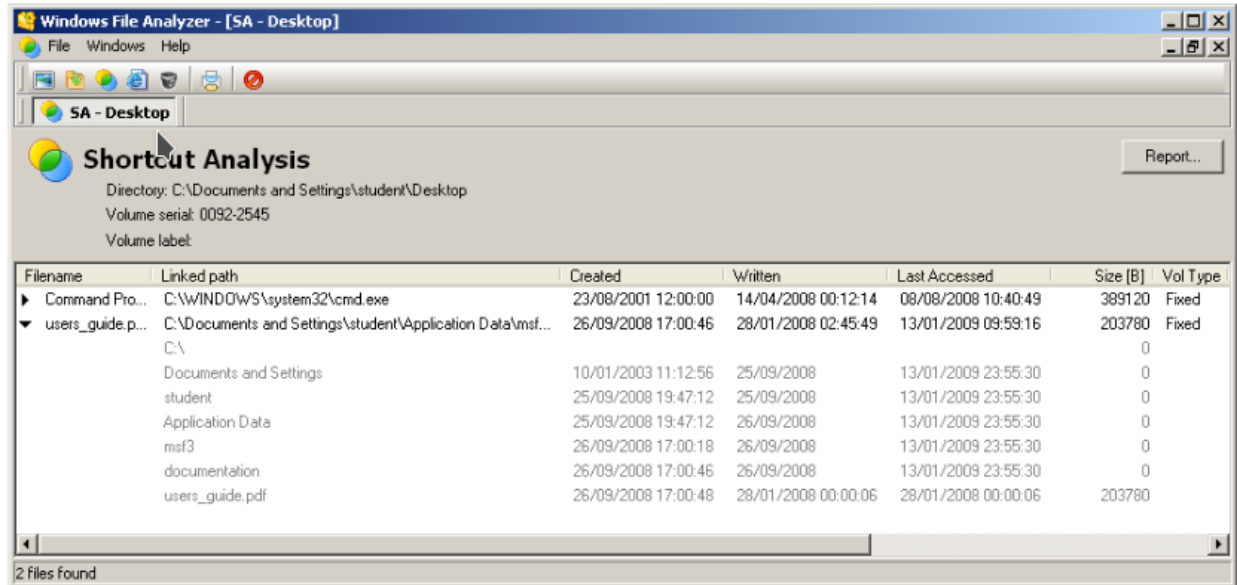
A **shortcut** is a link that points to a program on the computer. Shortcuts allow you to create links to programs in any folder, Start bar, Taskbar, desktop or other locations on the computer. A shortcut in Windows has a small arrow in the bottom left corner of the icon. Shortcut files end with a file extension of **.lnk**.

Each link file has its own Created, Modified and Accessed dates and within each link file there are Created, Modified and Accessed dates which belong to the target file. In addition, if the target file still exists on the media, that file has its own three dates.

Many individual applications also provide a list of files recently opened by that application.

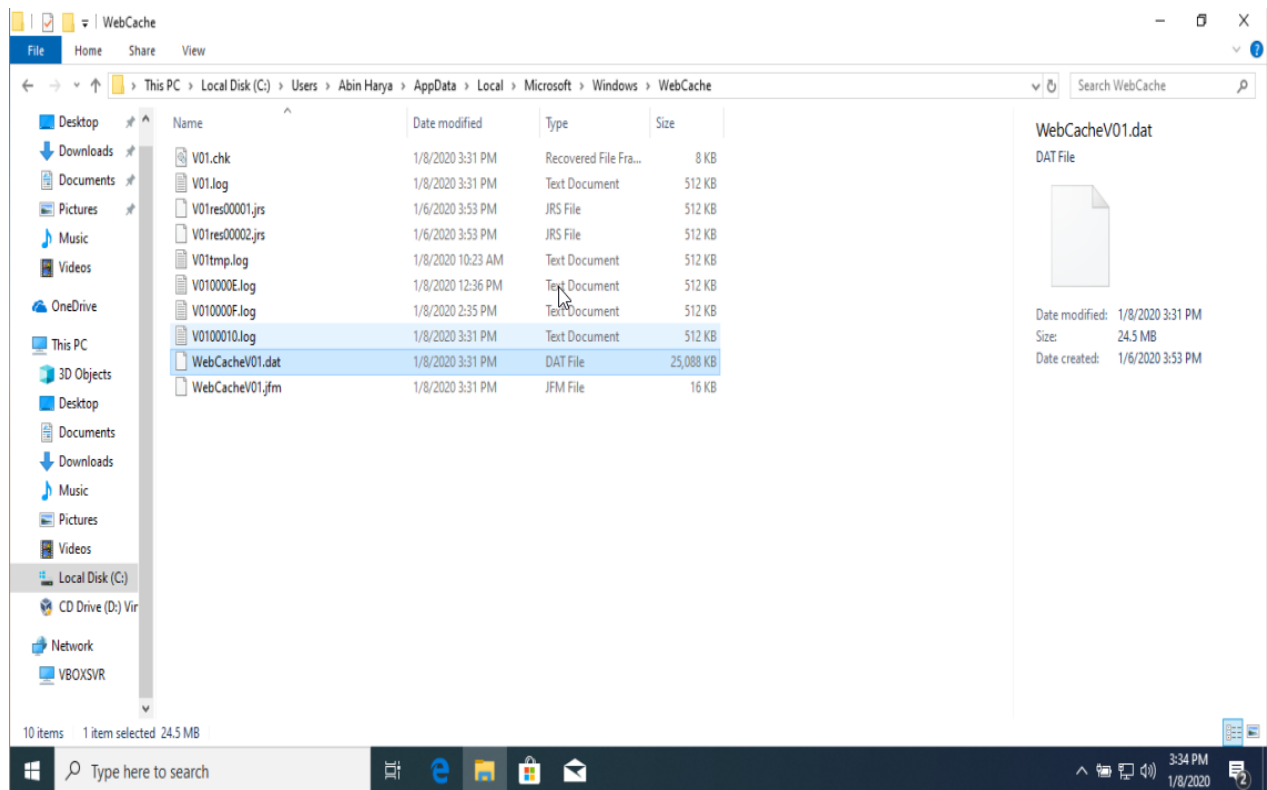
- For a desktop icon you can right-click the lnk file and view its properties. The same can be done for lnk files in other folders.
- You can also try and open an lnk file in notepad but you'll find much of it is unreadable.





- Open the WFA's Shortcut Analyser. To investigate this option select the Analyze Shortcuts option and browse to a folder in which you can expect to find a lot of lnk files.

3) **Webcache Files** : When you surf the Internet using a browser, nearly all the web pages visited are copied to and then stored on your computer, so that if you revisit a website the pages can be retrieved from your hard disk as opposed to the browser re-requesting the pages across the Internet. The location where the pages are stored is called a cache and in a Windows system they are held in a group of folders called Temporary Internet Files. The pages are not kept indefinitely but are deleted after a given time period (depends on what browser you use and any alterations made to the default settings). The browser needs to know what files it has already stored and the 'management' file is called WebcacheV01.dat.



Analysing Webcache V01.dat

- Go to the location: C:\users\username\AppData\Local\Microsoft\ Windows\WebCache\ WebcacheV01.dat and make sure you have such a file there by using Internet Explorer for a few queries.
- Download NirSoft and see what information you can retract from the .dat file

4) Recycle Bin

Recycle Bin represents a directory in which deleted files are temporarily stored. This enables you to retrieve files that you may have accidentally deleted. From time to time, you'll want to *purge* the recycle bin to free up space on your hard disk.

From the forensic point of view, the recycle bin is a gold mine for gathering evidence, clues, etc. By analyzing the recycle bin, we can recover useful data. In order for this facility to operate there is a hidden file called INFO, and this option allows you to look at the contents of the INFO file (one for each Windows disk partition) without having to start the undelete process.

Analysing Recycle Bin :

Run the Analyze Recycle Bin tool and make a note of the kinds of files you are able to find. (It may be advisable to run the tool on a variety of computers to which you have easy access to get a full understanding to the capabilities of the tool).

Summary :

In this first lab you carried out an examination of many of the artefacts found on your computer although in a relatively unprincipled and non-forensic way! Hopefully this week will have given you a flavour of the kinds of things a forensic investigator might look at, but you should be aware that a proper forensic investigation has quite a few more requirements. In the next few weeks we will be examining these requirements in more detail and looking at how they have evolved to keep pace with technological developments