**3906ICT/7906ICT Digital Forensics**

**Tutorial 1.2 – Windows Forensic Artifacts**

The aim of this tutorial is to give you some experience with identifying and examining Windows based forensic artefacts. We will cover some of the topics raised in the Lecture, but there are many more Windows based forensic artefacts that you are open to explore. Please note that this tutorial is not a step-by-step guide. The expectations are that if you are not sure of how to do something, you should find out via internet search or by asking your tutor.

# Preliminaries

There are two options for doing the practical component of this tutorial. You can do this tutorial by logging into the Griffith Cyber Range which is an Internet isolated set of virtual machines that has been set up on the Griffith network. The other is to download and install the software on your local PC.

## Set Up Option 1 – Griffith Cyber Range

If you are not on a Griffith University campus need to VPN into the Griffith Network. Details of how to VPN into the Griffith Network can be found here: https://intranet.secure.griffith.edu.au/computing/remote-access/virtual-private-network. Go to the bottom of the page and find the instructions for your device.

Once you have set up your VPN to the Griffith network, you can use your browser to go to the following page: https://cyber.ict.griffith.edu.au/

The credentials for the Griffith Cyber Range Server are:

**Username: sXXXXXXX**

**Password: changeme**

sXXXXXXX is your Griffith username. When you log in for the first time change your password (which you will need to remember). To do this go to your username menu on the top right corner of the web page and select the Settings item. The Settings page will allow you to reset your password. Once you have reset the password, use your new password for subsequent logins. For this tutorial we will be using a Windows 7 virtual machine. Click on the Windows 7 link and you will be connected to a virtual machine running the Windows 7 virtual machine.

When you have finished your tutorial simply close the browser tab with the connection to the virtual machine. Or press Shift-Ctrl-Alt to access the web menu and disconnect from the Griffith Cyber Range.

## Set Up Option 2 – Install on your local PC

The other option is to install the SIFT workstation on your local PC. Links to the virtual machine OVA file for download are found on the Learning@Griffith web site. **Note:** The Windows 7 virtual machine is a 15GB download. You will need to install VirtualBox and select File->Import Appliance to install the Windows 7 Virtual machine. Start the Virtual Machine and log in.

The login credentials for the Windows 7 Virtual Machine are:

**Username: Local User Password: password**

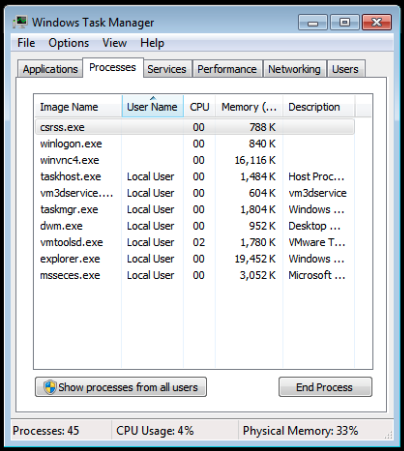
# Windows Processes

Start the Task Manager and examine the running processes.

1. Which running process uses the most memory? How accurate is this?
2. What is the difference between a running process and a service?

**Answer:**

|  |
| --- |
| Most memory is used by explorer.exe followed by winvnc4.exe, msseces.exe,taskmgr.exe…etc |



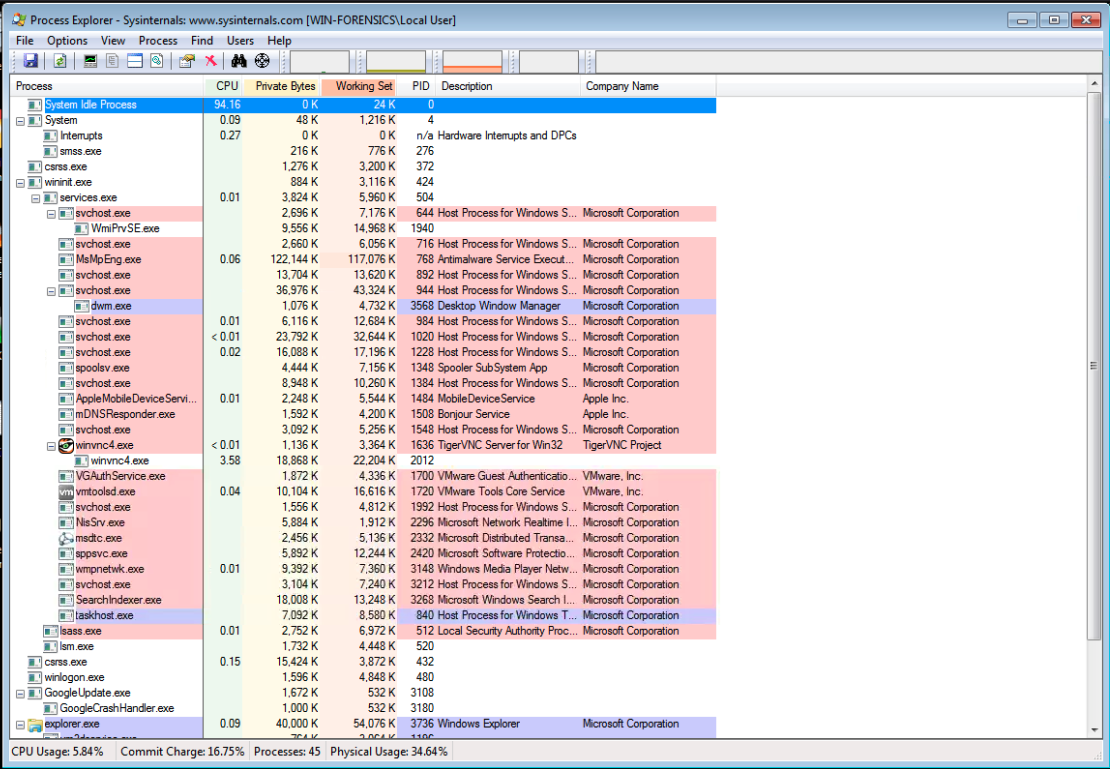
|  |
| --- |
| Install Process Explorer (found in the Documents folder) and use it to view the running processes.  The information shown is not accurate as there are more background services and processes running apart from the ones listed. The ones listed are accurate enough for themselves. |

Process vs Service

|  |
| --- |
| Services have no user interface, the run in the background and are all part of the windows system, eg, webserver, dhcp client.  Processes can also run in the background, they can have no interface or a limited interface that is hard to interact with. They generally allow interaction with the user.  “A process is an instance of a particular executable (.exe program file) running. A service is a process which runs in the background and does not interact with the desktop” – social.technet.microsoft.com |

1. Does the Process Explorer have any advantage over the Task Manager?

**Answer:**

****

Pink – service

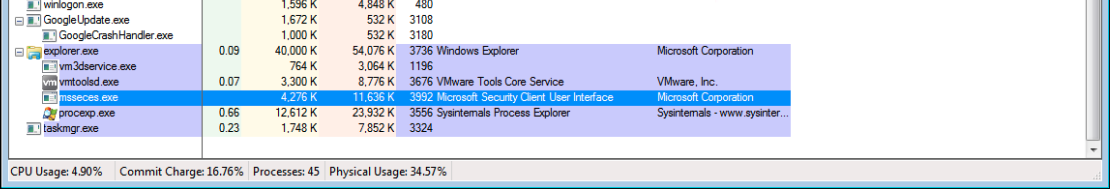
Purple – own process

|  |
| --- |
| Yes it does, it provides additional information such as the link between processes. They show executables that launch other executables.  Task manager is sufficient for basic troubleshooting, process explorer provides more information to investigate things. |

1. What is the process ID? What is the process ID of Microsoft Security Essentials?

**Answer:**

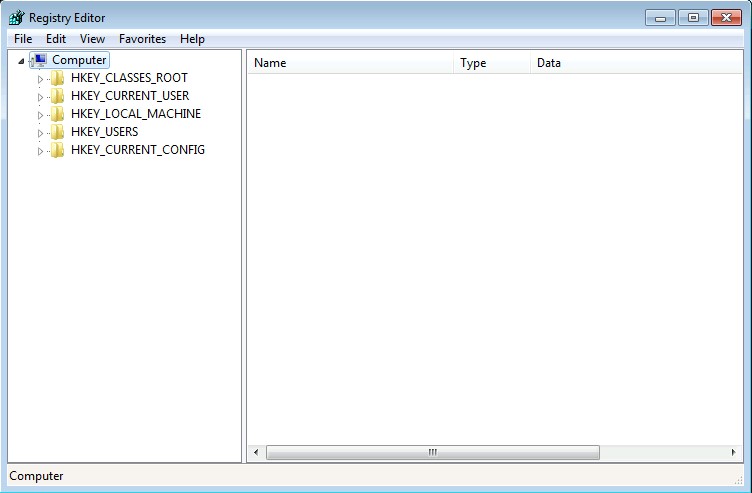
|  |
| --- |
| PID is the label that identifies the processes. |

****

|  |
| --- |
| PID for Microsoft security essentials is 3992 |

# Registry

Start the regedit.exe system tool and use it to find the answers to the following questions.

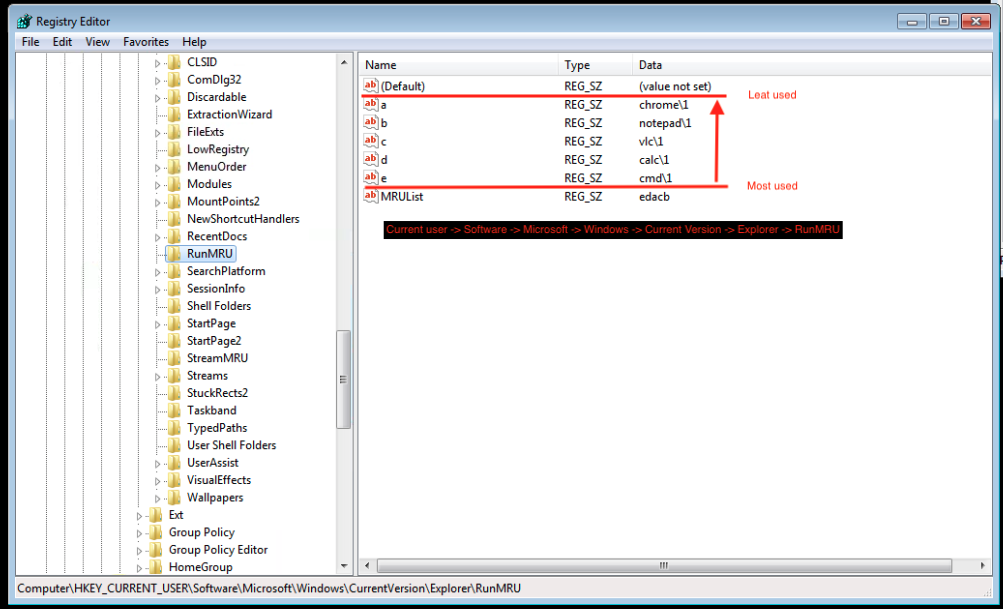


|  |
| --- |
| START -> regedit |

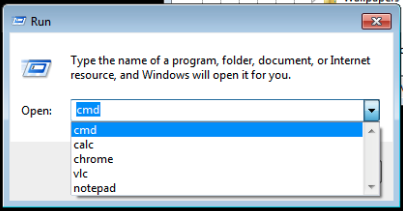
1. What are the most recently run 5 applications from the Start->Run menu? In what order did they get used?

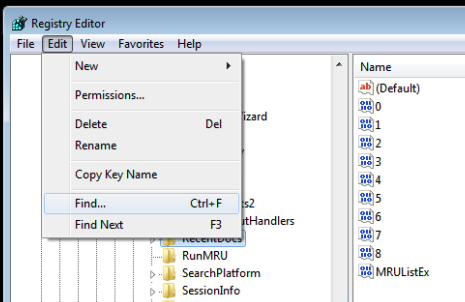
**Answer:**

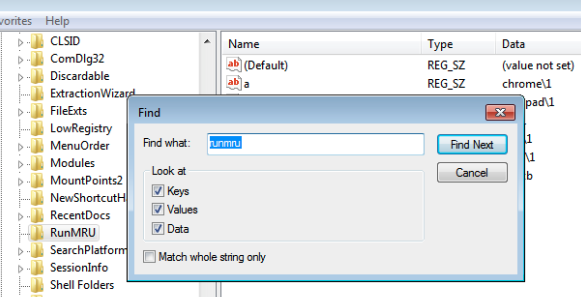
Current user -> Software -> Microsoft -> Windows -> Current Version -> Explorer -> RunMRU



\*Most recent order





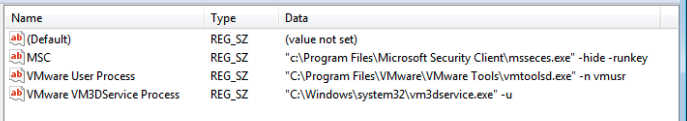


1. Are there any applications that are started on boot up?

**Answer:**

Google - run at boot registry

|  |
| --- |
| HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run |





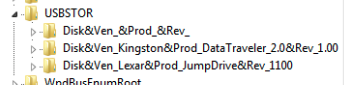
Quiz Tip – start from HKEY… not computer

1. What are the USB devices that have been connected to this system?

**Answer:**

Google - usb devices registry editor



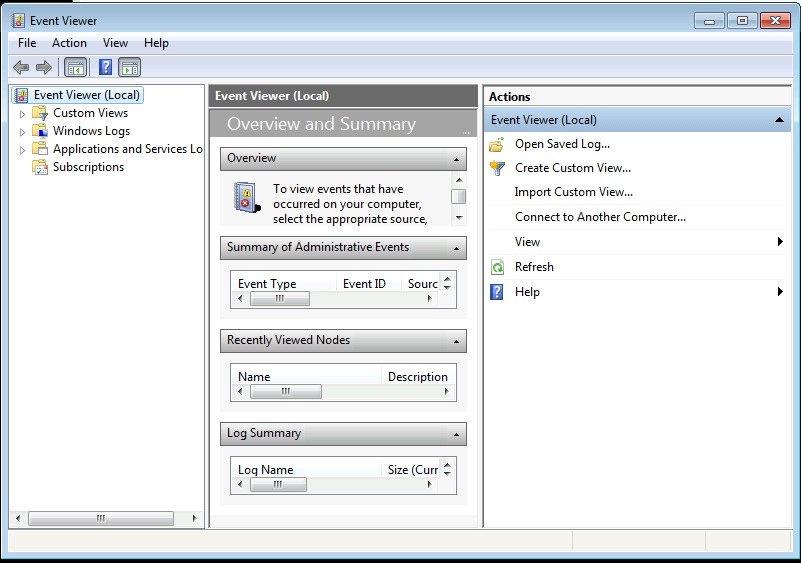


The first USB device has no name.

Look at the PID and the “FriendlyName” to identify the device

# Event Logs

Start the Event Viewer system tool and use it to find the answers to the following questions.



|  |
| --- |
| START -> Search[Event Viewer] |

Google – “windows 7 event id installation”

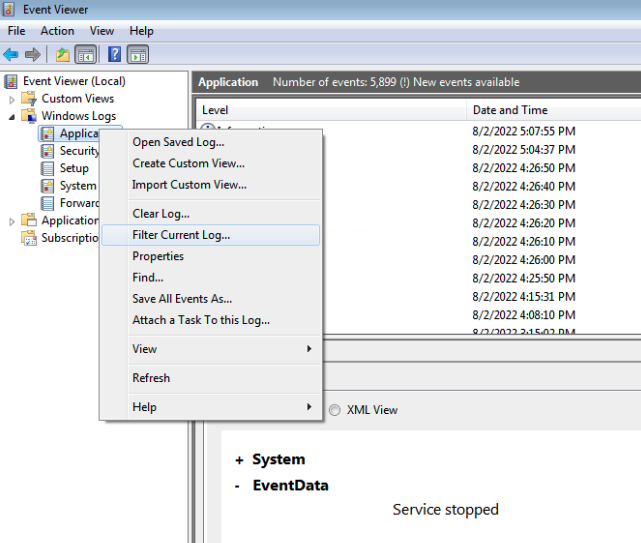
Result - https://docs.microsoft.com/en-us/windows/win32/msi/event-logging

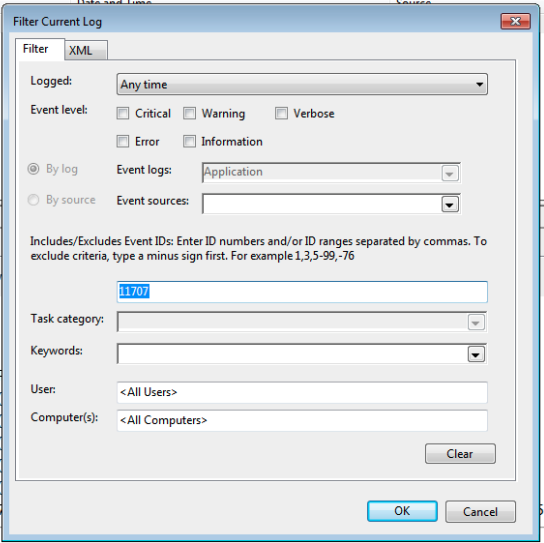
1. What order were the non-system applications installed?

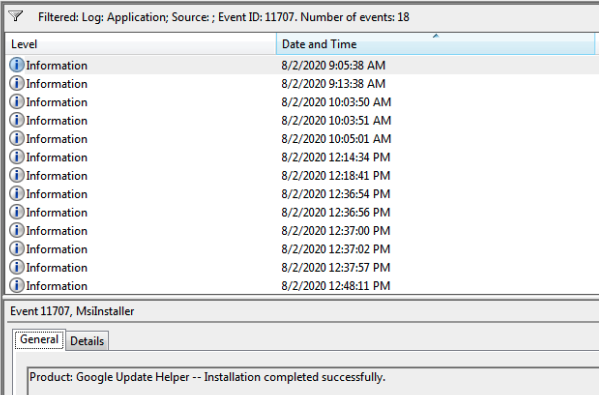
**Answer:**

Google – “windows 7 event id installation”

Result - <https://docs.microsoft.com/en-us/windows/win32/msi/event-logging>

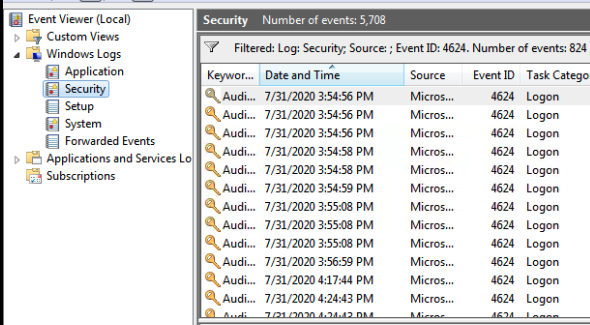






1. When was the first 4624?

**Answer:**



# Prefetch Files

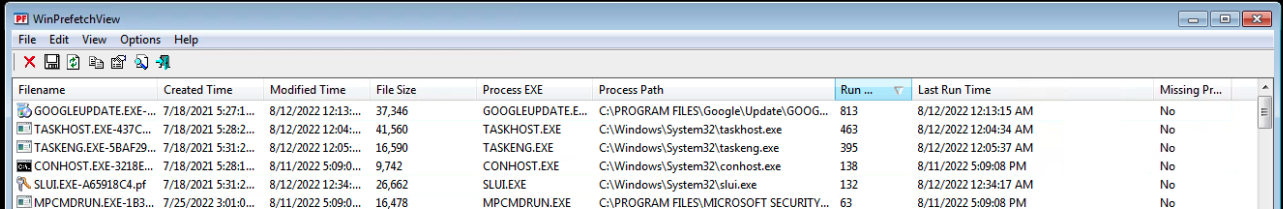
Install WinPrefetchView (also found in the Documents folder, unzip and run the executable file) and use it to find the answers to the following questions.

1. Which application is run the most and how often?

**Answer:**

Prefetch file location:





1. What information is provided with prefetch files that is not found in the Windows Registry?

**Answer:**

The last time it was run “Last Run Time”

Very useful for malware that was run (imagine a suspect claiming they were hacked)

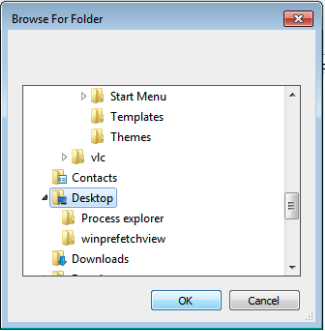
# Shortcut Files

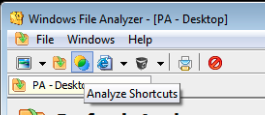
Install the Windows File Analyser (Run as Administrator) to examine shortcut files

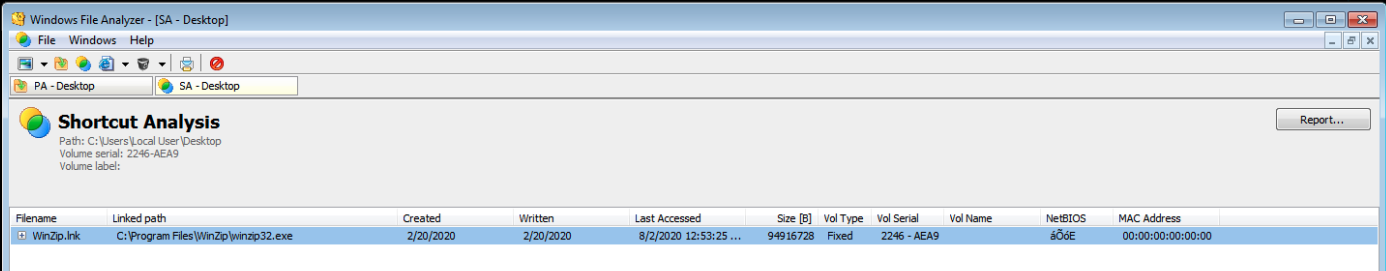
1. Is there evidence that an application has been deleted? Where was the application installed?

**Answer:**

We know it was deleted as we can see the path and the last accessed time, and we see the file is no longer in its original loation.

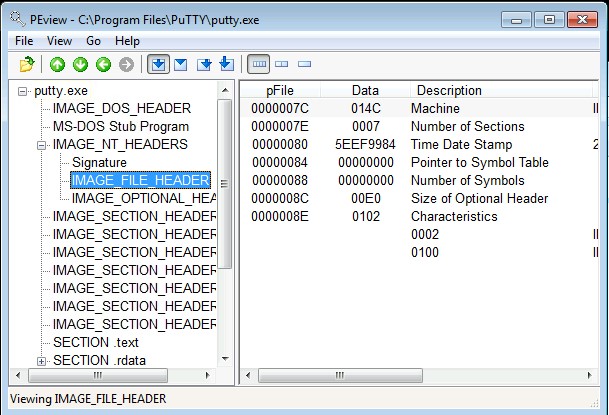






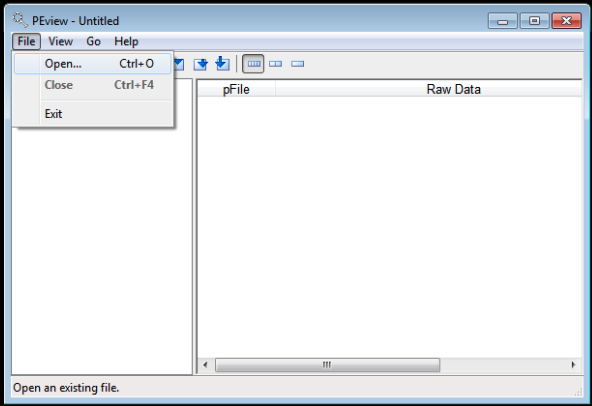
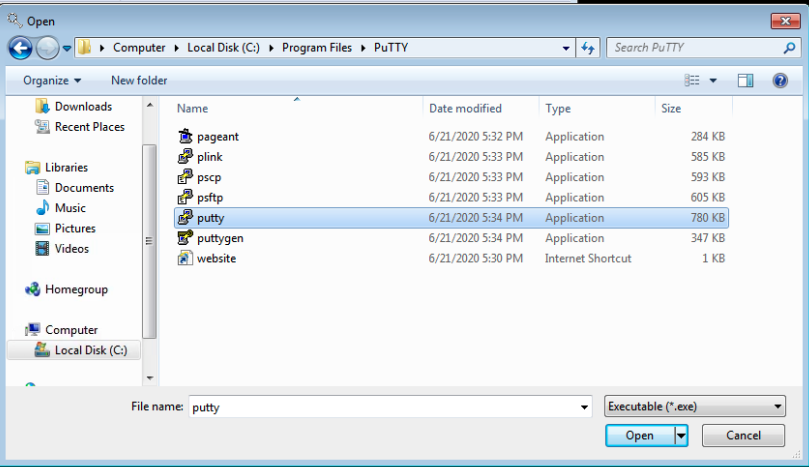
# Windows Executables

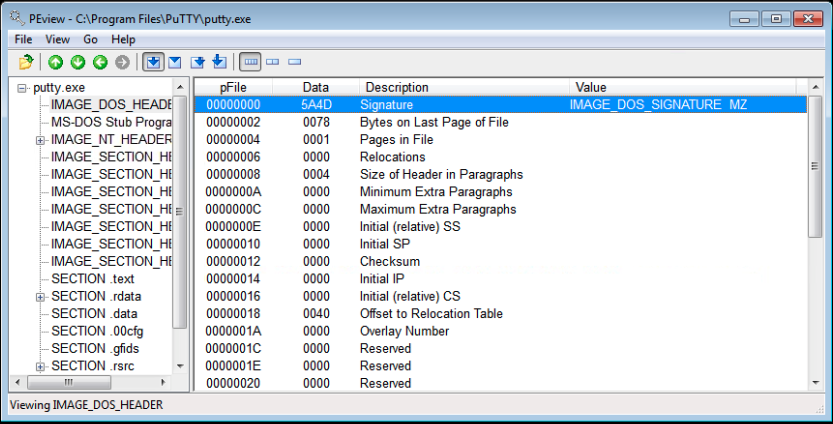
Install PE View or Resource Hacker (found in the Documents folder). Find the Putty application.

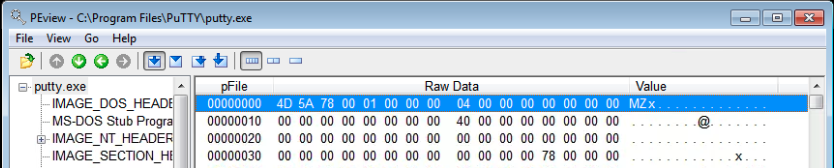


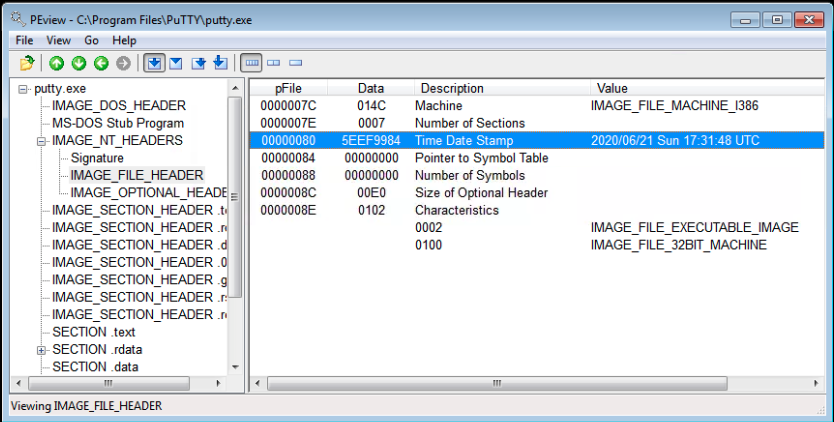
1. Use PE View or Resource Hacker to find out when was this application compiled? Look for the IMAGE\_FILE\_HEADER for the Time Date Stamp.

**Answer:**

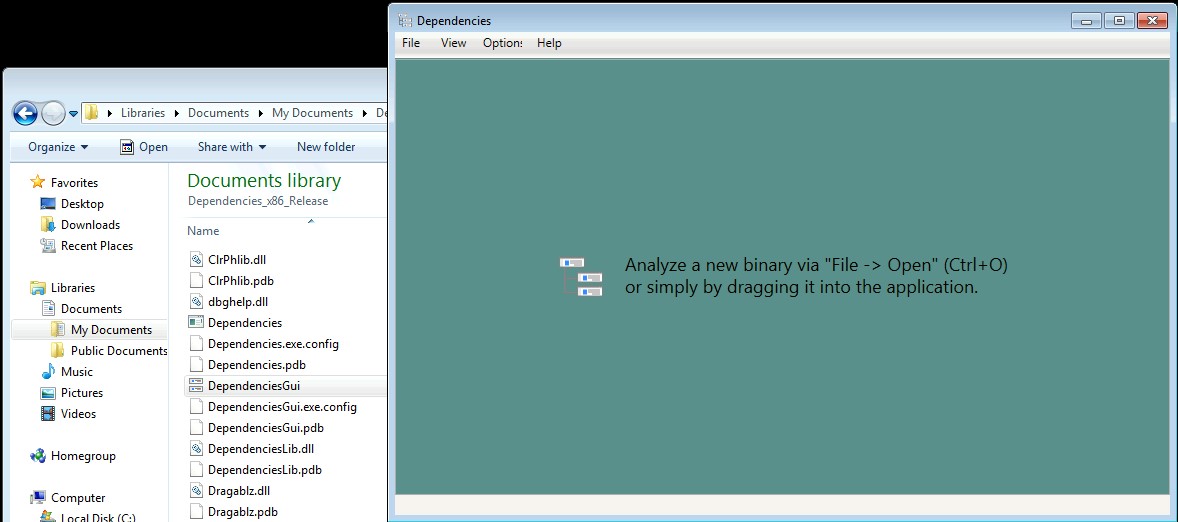








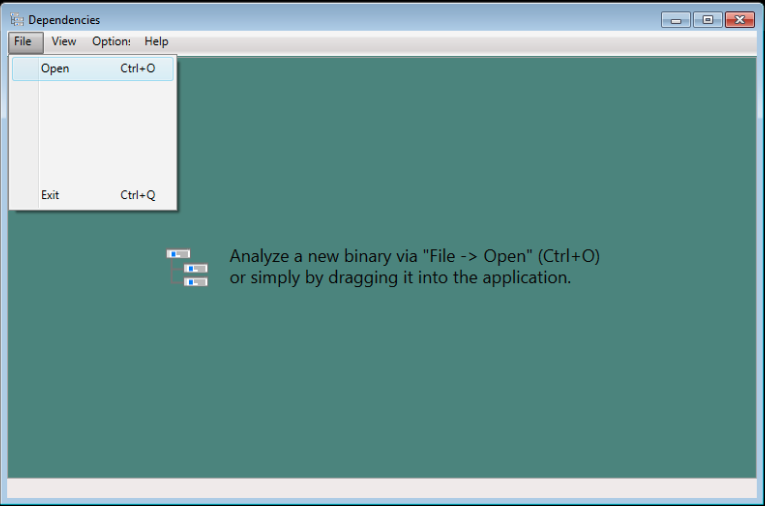
Unzip the Dependencies application (found in the Documents folder). Run the DependanciesGui application to start it.

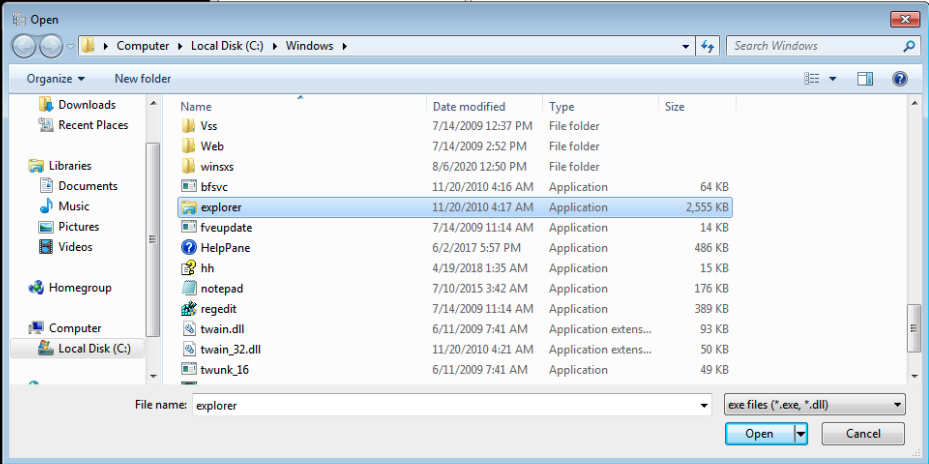


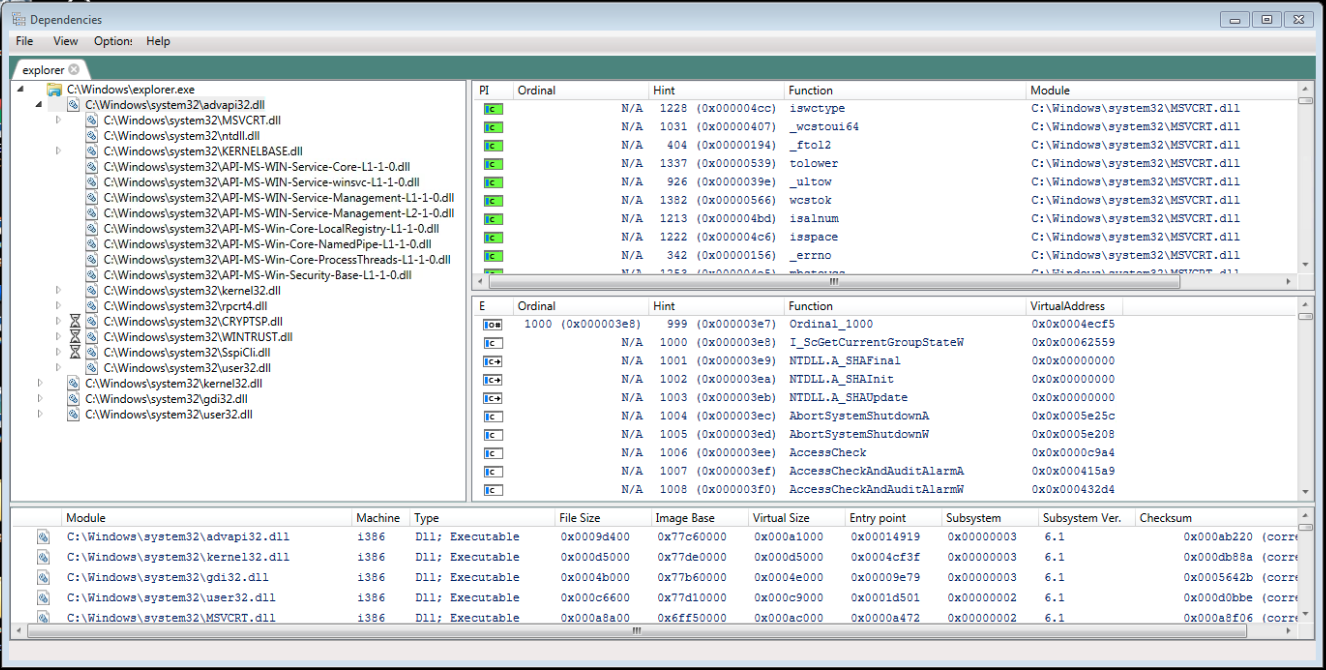
1. What is the DLL that has the most functions imported by Windows Explorer?

Examination of Windows forensic artefacts will allow the investigator to develop a narrative of what has happened on the system. Sometimes multiple artefacts will corroborate other evidence.

**Answer:**

****

****

****

1. In this week’s tutorial have there been examples of tools and artefacts that provide evidence of the same events occurring? Why is this good?

**Answer:**

Sometimes tools fail, its good to collaborate evidence having multiple tools for verification is useful to build confidence in the results.

# Tutorial Quiz

You have now completed the exercises for this tutorial. You can now attempt the quiz for this tutorial.

Software U

