

Assignment 2

Sanjay Kumar s1504445



November 10, 2022

Melbourne Polytechnic

.

Contents

[Part A (700 words) (10 Marks – 1 Mark/per Question) 2](#_Toc119649391)

[Convert your student number to MD5 hash. 2](#_Toc119649392)

[Save hash in a notepad file. 3](#_Toc119649393)

[Record the hash of the file. 3](#_Toc119649394)

[Does either of the following change the hash? Why/Why not. 4](#_Toc119649395)

[Change Attributes (Read-Only/Hidden) 4](#_Toc119649396)

[Change Permissions (Full Control/Modify/Read/Write) 5](#_Toc119649397)

[Change extensions (e.g. \*.txt to \*.exe) 5](#_Toc119649398)

[email to yourself and download it. 5](#_Toc119649399)

[Append the file with spaces 5](#_Toc119649400)

[Remove the spaces (in (v)) 6](#_Toc119649401)

[In a Linux System 9](#_Toc119649402)

[In Wireshark what was the sender and destination IP? 9](#_Toc119649403)

[What is the hash of the packet? 9](#_Toc119649404)

[What is the hash of the content 9](#_Toc119649405)

[Did the destination reply? 9](#_Toc119649406)

[Does either of the following change the hash? Why/Why not. 10](#_Toc119649407)

[Send the file 10 times 10](#_Toc119649408)

[Does the hash of the packet change? 10](#_Toc119649409)

[Does the hash of the content change? 10](#_Toc119649410)

[Import the notepad file as a Hash Import to a Forensic Software. Search for all occurrences of the hash. Does it search for the file or content of a file? Explain. 11](#_Toc119649411)

[Open the content of the packet use a Reverse MD5 hash. What was the end value? 11](#_Toc119649412)

[View and explain the history of your network traffic with Wireshark 12](#_Toc119649413)

[Part B 10 Marks 14](#_Toc119649414)

[Learn a new tool – that we have not used in class. Explain how to use it, what you do with it and the demonstrate it working. 14](#_Toc119649415)

[Conclusion: 15](#_Toc119649416)

[Video Link 15](#_Toc119649417)

# Part A (700 words) (10 Marks – 1 Mark/per Question)

## Convert your student number to MD5 hash.

After converting my student number into MD% hash file

Graphical user interface, text, application, email

Description automatically generated

The result I got is 1d8639ec14bde38e79539c19ce5a33f1

The result I got online for this is also the same

## Save hash in a notepad file.

Graphical user interface, text, application

Description automatically generated

## Record the hash of the file.

The hash of the file is 1d8639ec14bde38e79539c19ce5a33f1

## Does either of the following change the hash? Why/Why not.

### Change Attributes (Read-Only/Hidden)

After changing the attributes of the file to hidden only there will be no change in the hash because there is no modification in the content of the file.

Graphical user interface, text, application, email

Description automatically generated

### Change Permissions (Full Control/Modify/Read/Write)

There will be no change in the hash of the file because changing the permission is not creating any modification in the content of the file.

Graphical user interface, text

Description automatically generated

### Change extensions (e.g. \*.txt to \*.exe)

After changing the file type from txt to .exe will still keep the hash same because there are no modifications in the text of the file.

### email to yourself and download it.

Here is the screenshot of me Emailing it to myself.

As we can see Email also doesn’t affect the hash value because there were no modifications in the content of the file.

Graphical user interface, text, application, chat or text message

Description automatically generated

### Append the file with spaces

Adding empty spaces in the file will create content modification of the file so we will see that the hash value of the file has been changed

Graphical user interface, text, application

Description automatically generated

The changed hash of the file is 9849a510990e66651947e30f4ff8cf13

Graphical user interface, text, application, email

Description automatically generated

### Remove the spaces (in (v))

After Removing the spaces from the modified content file, we can see the hash value of the file becomes the same one which it was before.

Graphical user interface, text, application, email

Description automatically generated

1. Delete the file and recover it with forensics software (e.g. Autopsy)

First I will delete the file

Chart, scatter chart

Description automatically generated

Now I will open Autospy and from the case which I opened already I will extract the file from the option of deleted files.

Graphical user interface, text

Description automatically generated

1. Delete the file and recover it with backup software (e.g. photorec)

Open Photorec in the desktop

Text

Description automatically generated

Text

Description automatically generated

After that we will be going to the directory of the file and then scan the deleted files with photorec

## In a Linux System

sudo tcpdump -vX -I lo port 514

echo “hello” | nc -4u -q1 127.0.0.1 514

Complete the following:

### In Wireshark what was the sender and destination IP?

It will be executed with the help of ubuntu virtual machine with Wireshark downloaded into it.

Since it is a loop back address, so the sender and destination IP are the same as 127.0.0.1.

### What is the hash of the packet?

### What is the hash of the content

### Did the destination reply?

The destination reply is hello

## Does either of the following change the hash? Why/Why not.

### Send the file 10 times

No, the hash value will remain the same after sending the hash file 10 times because the content of the file has not been modified.

### Does the hash of the packet change?

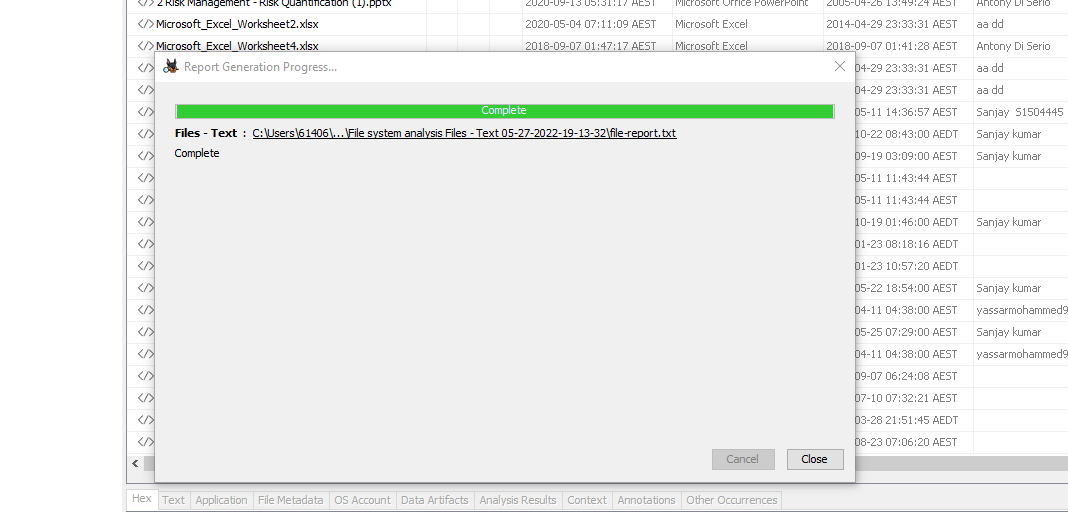
The content of the file is same so the hash of the all the different packets generated will stay same since the content is not modified in the hash file.

### Does the hash of the content change?

The content of the file does not change with sending the file to different locations so the hash of the content will not change.

## Import the notepad file as a Hash Import to a Forensic Software. Search for all occurrences of the hash. Does it search for the file or content of a file? Explain.

After importing a notepad file as a hash import it search for the content of a file and convert it into hash value. We can obtain hash set files



## Open the content of the packet use a Reverse MD5 hash. What was the end value?

An MD5 is 128 bits long. That means there are 2^128 possible hashes. That is a reasonably very large number. Moreover, MD5 hash is an irreversible algorithm because it is a cryptographic hashing algorithm which means it is only computed in one direction and can not go back to its original form.

## View and explain the history of your network traffic with Wireshark

To view the history of network traffic with Wireshark I will put the filter of HTTP. Host and currently I am using the wireless internet on my device so I will select that interface and start capturing the packets on that.

To check the history after beginning of packet capturing, I will go to statistics where I will select the load distribution in HTTP option and download the file. In the file I can see the network traffic history of my device which will be saving all the files I will be visiting.

Graphical user interface, text, application

Description automatically generated

Below the screenshot attached of my latest stats of network traffic from Wireshark

Table

Description automatically generated

# Part B 10 Marks

## Learn a new tool – that we have not used in class. Explain how to use it, what you do with it and the demonstrate it working.

For this part I have installed and demonstrated CAINE in my operating system

CAINE stands for Computer Aided Investigative Environment.

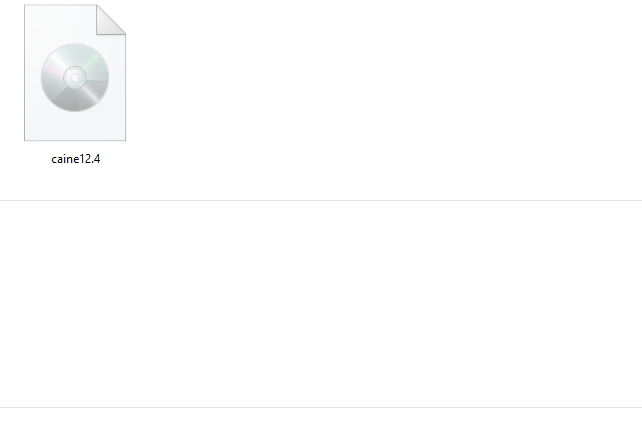
#### Purpose:

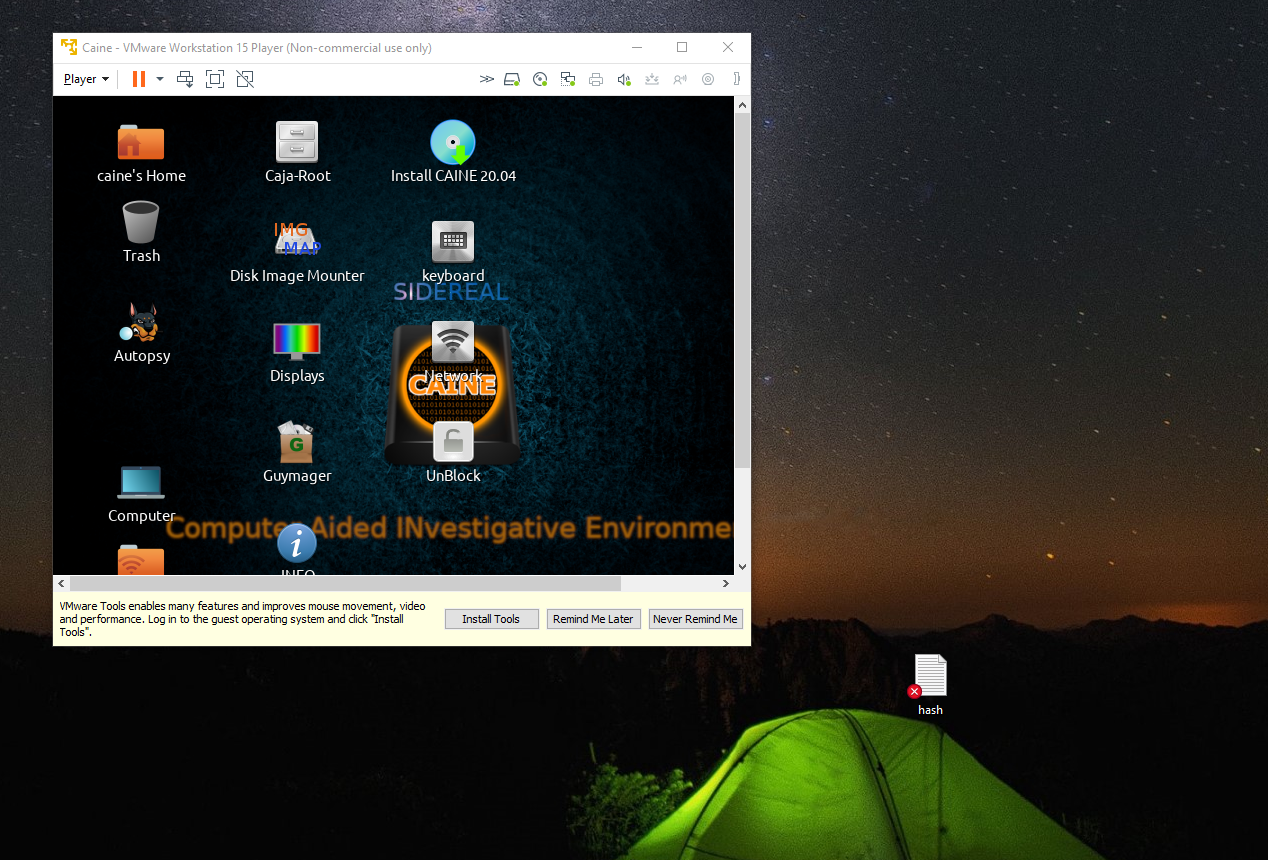
CAINE is a professional open-source forensic platform that integrates software tools as modules along with powerful scripts in a graphical interface environment. Its operational environment was designed with the intent to provide the forensic professional all the tools required to perform the digital forensic investigate process (preservation, collection, examination and analysis). CAINE is a live Linux distribution so it can be booted from removable media (flash drive) or from an optical disk and run in memory. It can also be installed onto a physical or virtual system. In Live mode, CAINE can operate on data storage objects without having to boot up a supporting operating system. The latest version can boot on UEFI/UEFI+Secure and Legacy BIOS allowing CAINE to be used on information systems that boot older operating systems (e.g. Windows NT) and newer platforms like Linux, Windows 10.

#### Installation: -

CAINE is based on Ubuntu 18.04 64-bit, using Linux kernel 5.0.0-32.[[6]](https://en.wikipedia.org/wiki/CAINE_Linux#cite_note-6) CAINE system requirements to run as a live disc are similar to Ubuntu 18.04. It can run on a physical system or in a virtual machine environment such as VMware Workstation.

For this device ISO file was downloaded first, and it was run in a VMware Workstation as shown below.





#### Tools: -

CAINE provides software tools that support database, memory, forensic and network analysis. File system image analysis of NTFS, FAT/ExFAT, Ext2, Ext3, HFS and ISO 9660 is possible via command line and through the graphic desktop.

For this report I have studied CAINE interface and some of its tool and demonstrated it in the video assignment.

## Conclusion:

Caine is a very powerful and useful forensic analysis platform which gives user wide variety of tools and features to use for doing investigation.

## Video Link

<https://youtu.be/UsRJV5wU3gU>