

**Forensics Open Book Exam**

**BSc in Computer Science**

School of Computer Science

TU Dublin – City Campus

**Wednesday 12th May 2021**

**Exam Duration: 2pm – 5pm**

# Question 1

*1(a) Answer:*

*[Max Word Count: 350 words]*

***A digital investigator may triage computers and other digital media at the start of the  
investigation. What is the main focus of the triage and what role would the investigators play in this process?***

The term triage may refer to first determining what the priorities are, such as preserving the crime scene to obtaining all the evidence possible before it is tampered with or about to be destroyed, or going after the culprit who’s on the run. As well trying to make a call, by law enforcements if identifying the culprit could result in a financial loss.

Extreme example: arsonist escaping crime scene, do you help fight the fire they caused to save people/property or chase the suspect?

These are decisions investigators and law enforcement have to make. The role of investigators when securing digital media as evidence such as a computer at the start of an investigation is to assess all potential risks that can happen, and try to mitigate or nullify all possible risks, such as any damage to computers, securing any volatile data or be wary of any harmful malware within the system could all be seen as risks, or simply tampering with the evidence, possibly affecting it’s soundness.

*1(b) Answer:*

*[Max Word Count: 500 words]*

***Compare and contrast the main issues and differences in operation with hardware write blockers and software write blockers. How can these issues and differences relate to the results of a digital forensic analysis of a drive?***

Write blockers can be used to permit read only access, making it impossible to edit or delete content, keeping the integrity of the data intact. This is so the original data is not altered by much, damaging the soundness of the evidence, however it is to note that even write blockers will alter the state of the hard drive to a certain extent

Write blockers can be used when creating a memory capture and copying data, protecting the state as to not change the contents of the drive.

An example of a write blocker that is software based would be the Windows Registry, this involves editing one of the hives stored changing the variables in the Windows registry. However, one of the main issues with using this method is that messing with the registry tool could end up making the entire system unstable and would require a back-up registry to resolve.

Hardware writes blockers such as Tableau for example, performs identical operation to a software write blocker, which is to permit read-only access in a device, preserving it’s data integrity.

Issues with hardware write blockers is that they perform the same operation as software, though require a separate device with its own configuration. As well as that, hardware write blockers have software within them as well, so there really isn’t much difference besides having another separate device, and could potentially cost more than a standard software write blocker.

*1(c) Answer:*

*[Max Word Count: 800 words]*

***“In the world of digital forensics, metadata is the data and information that is part of  
or attached to some other more obvious piece of data”. Explain in detail three forms  
of metadata that can be useful to an investigator, and how they are used to identify  
useful information as part of a forensic investigation.***

3 types of metadata that can be examined are file system metadata, substantive metadata, and embedded metadata

File system metadata tells the file system how to find the file by providing the location of that file. Investigators can find this information extremely useful. When inspecting a system, the file system metadata can help investigators how to track down certain files that seem suspicious. If searching for specific files, the file system metadata can allow the investigator to easily locate it, instead of spending a lot of time searching the directories. In short, file system metadata can make the investigator’s life much easier when it comes to searching the file system for any potential suspicious files.

File system metadata also provides identification information for each file. As it is possible to have the same file name in a computer, by having the same-named file in 2 different directories, it is not possible to have 2 of the same file name in the same directory. If the investigator locates a suspicious file X, there may be multiple traces of the file X in several directories, so by using the file system metadata, every instance of file X can be discovered as well as their individual locations

Certain applications provide security for managing permissions. Investigators can investigate these to understand the permissions that are going on the system. As well as that file system metadata contains MAC data. MAC data provides dates and times of when a file is modified, accessed or created. These are of course very useful to the investigator when the want to document and understand the time frame of a file’s modification as a date and time of a crime is always useful to an investigation.

It is to be noted that the date of creation is not when the file was created. If copied the creation date is updated as well as certain utilities to modify the file’s create date exist. This makes the create date a bit more unreliable and inaccurate.

The modified date gets changed, once the file is changed in any form. Any action against a file such as simply opening it will modify the file’s access date.

Other 2 types of metadata are embedded metadata and substantive metadata, which contain different MAC data than the one generated by the system.

Embedded metadata contains information about the file that isn’t always available to the user. An example could be a formulas written by the user used to calculate in a spreadsheet. It provides extra information about a file such as calculating a formula. It’s data associated with the application unseen by the user. This can be used by investigators to see what user inputs were in a particular file or application, which can provide some insight into their intent, such as what have they been calculating in an excel, and try figure out why.

Substantive metadata contains data which reflect the changes to a document, such as any notes added to a file made by the user.

It is important to note, applications allow custom metadata as well as changes to metadata such as author, title or organizations in a pdf file. All these can be examined and should be looked at carefully to give more insight into the investigators and allow them to gather more evidence. Any changes to metadate will be contained within the Substantive metadata, in which investigators can get an idea of modifications made to a file, in which they can take note of when examining and might discover something interesting.

# Question 2

*2(a) Answer:*

*[Max Word Count: 350 words]*

Text, letter

Description automatically generated

Criminal Justice Act 2017 stated

A person who without lawful authority or reasonable excuse, intentionally access an information system by infringing a security measure shall be guilty of an offence.

Before Cyber crimes were never an issue in around the 1990s, thus there was never really an real legislation against cybercrimes and computer related crimes. For example, The criminal damage act of 1991 to deal with unlawful entry or unauthorised access stated that unauthorised access without actual damage such as hacking was not an offence, but merely a breach of confidentiality, and was only punishable with a measly fine of 500 pounds. Cybercrimes were not stated in legislation and punishment was not severe enough to make people stop committing it.

As well as that information theft in the criminal Justice Act of 2001 stated a person is guilt of theft is he dishonestly appropriate property without consent of its owner and with the intention of depriving its owner of it.

Unlike the 2017 act, it stated property, the 2001 act could be interpreting property as physical property only such as jewellery or money, not information from a computer. It wasn’t well defined there for someone could commit information theft yet still argue the case that theft of “property “ was not committed, however, 2017 clearly states and specifies access of an information system by bypassing the security is an offence. With the growth of new technology, the laws need to be updated as well to address new issues and crimes that can arise, hence the need of the 2017 act that clearly specifies cybercrimes and doesn’t leave anything to interpretation.

*2(b) Answer:*

*[Max Word Count: 500 words]*

Text

Description automatically generated

File carving is a technique that is used in cyber forensics, to discover where a file ‘s hex code has been altered and corrupted as well as locate missing or deleted files. File carving recreates a file from its raw data, by identifying it’s associated data, and creating a new file from this data.

First step in the file carving process is to identify the header and footer, which is where the file signature begins an end. Note that different file types have different headers and footers (types like JPEG will be different from PNG files)

Using a hex editor such as HxD, it can bring up the hex code of the file. Inspect usually either the header or footer has been altered, an investigator can check if the hex code is in place (so for example for a JPG file, a JPG signature would be FF D8 FF for it’s header, if the first 6 characters of the hex code is for example FF D5 FF then it has been altered and corrupted). Changing the signature back to how it’s supposed to be (so FF D8 FF) can create a new file with the original contents of the missing JPG file.

This is how file carving can be used to recover files, as well as that, if files have had their signature altered, it would give further evidence of tampering and intent, as the suspect who altered this file did so knowingly.

As well as that, this technique can simply extract any hidden files without it being corrupted but are simply in unallocated space by using the hex editor to extract all the bits from the header to the footer of a specific file type and using that to recreate the file.

*2(c) Answer:*

*[Max Word Count: 800 words]*



When managing a case, it can be divided into 3 separate stages which are preparation, investigation and presentation.

The first stage of a forensics case is called preparation. As it implies this is the preparation phase and would normally be done before the forensic investigation actually begins. To prepare, it’s important to actually set up the forensic team, by selecting who will be the investigators of the case, as well as other members of staff and make sure everyone in the department who will be involved in the investigation is assigned a role. As well that, it is important that all members of the investigation team is well aware and up to date of all the policies and procedures, to make sure nobody accidently or unknowingly act unaccordingly and breaks protocols

The next and main part of the case is the investigation. A number of events happen, such as triage (explain in Q1), first response and crime scene management. First response is a set of protocols, whoever arrives at the scene has to make a call of how the evidence will be gathered, of course to the best of their ability in a forensically sound manner so that no evidence becomes unreliable. If necessary a live-response could be performed.

The crime scene has to be preserved, meaning it should look as it was when the investigators and law enforcement first arrived to it. This is so that evidence gathered are more natural and becomes easier to reconstruct the crime if nothing has been tampered with. Once arrived at the scene, as well as preserving it, the scene should be surveyed looking for any locations and items that might be of some interest and searched for any possible evidence. Everything should be documented, as well as the scene itself, so investigators should take a loslackt of photo and videos of the scene.

Once evidence has been gathered, the investigators would normally return to the labs and prepare a repository in their machines with taking to account enough storage and security (though forensic workstations should be in nature strong with regards to memory and security). All tools for analysis should be ready such as write blockers, capture tools and ensure that their personnel are ready to receive any evidence from them.

It is important to note when handling evidence, prevent the environment from contaminating the evidence, such as power outage onsite destroying any volatile data or if the room itself is set to a condition that won’t damage or overheat any device. Another example would be to block electromagnetic transmission that could potentially affect any devices. When transporting devices, use faraday bags if handling mobile devices to block telecommunications, and as well as that, all devices should have sources of power to be kept on, as so not to delete volatile data in RAM for example. Key thing is to document all evidence handling, meaning keep excellent record of the chain of custody, any evidence handed to someone else must always be documented.

When examining evidence, you the right tool for the right job, use memory capture tools to capture RAM, use browser analysis on browsers, use a windows write blocker on a windows machine. Never work on the original, always work on copies or else the soundness of the evidence will be ruined, and finally investigators must always document everything they do when examining the evidence.

Final stage of the case is the presentation stage, which brings all the results in. results should be based on fact and knowledge, not interpretation or theories. The evidence will be incriminating to the defendant or help his case, no evidence should be concealed, and all statements or findings must be backed up in a document or report.

The report will consist of the case summary, all warrants, subpoenas and authorizations used for searches, all notes, videos and photographs and contain a conclusion.

The case summary will include details of who requested the investigation, what were the principles, when and where was the incident happening, where was the reports filed and a brief summary of the details of the case itself and what had allegedly happened.

The report will also consist of an inventory of items examined, all the tools used to examine these items, a timeline of events and the procedures and actions that have been performed along with who was involved., and All findings and exactly how they were obtained are documented as well, what tools were used on what piece of evidence etc.

Finally the report conclusion which ties the report together and presents the evidence, again either supporting or going against the defendant.

# Question 3

*3(a) Answer:*

*[Max Word Count: 350 words]*



Certain hard disks are divided into several clusters, containing of up to 32KB of memory space. If a file does not use up all the space within a cluster, the remaining space that is left over on the hard disks are referred to as local space. As well as that slack space also exist between partitions on a hard disk.

Slack space can be used as a whole separate file system and can be a place to hide files. Tools such as Slacker can be used to manage all the slack space into it’s own file system. So investigators need to be aware of slack space being a potential hiding place for files.

Data can be recovered using tools such as Slacker. Since slack spaces are generally undetectable by some file browsing utilities, it requires a executable to launch an interface or shell to manage the file system.

The registry hives can be used on a windows system to check for recently run programs. This can be used to detect the potential program such as Slacker that manages the slack space file system, and use it to recover the files

*3(b) Answer:*

*[Max Word Count: 500 words]*

Text, letter

Description automatically generated

Steganography is similar to cryptography, except hiding messages, in which it’s secret is known to the receiver. Steganography is instead using certain utilities such as files in order to hide information. Anti-forensic techniques are all about different techniques to hide information to so that the investigator cannot find it. As mentioned, Steganography is an anti-forensic technique of hiding data within files or images. Files can be hidden within other files, as well as that compression algorithms can be used so that covert data can be piggypacked onto another file

Certain data and files can be hidden within images as well. Using a tool such as Steghide, it is possible to hide a file, such as a PDF document within the contents of a simple PNG or JPG file if it is large enough. It is as simple as 1 command steghide embed -cf imagename -ef documentname. And with that an Image acts as a cover, hiding a document in which an investigator might overlook. Other tools such as OpenStego can allow for data hiding and using cover images to hide important data

OpenStego can also be used to retrieve data and extract them from cover files. One of the techniques that be used to find cover files, is for an investigator need to keep an eye out to the size of the file. If a JPG file is suddenly a certain amount of bytes larger than usual, then it may warrant more investigating as it may be a cover image containing a hidden document. Another method is to examine the MIME type of the file. This can be used to discover cover files. As well as that the pixels within cover images may be off about the picture that could indicate something may be hidden.

A variety of commercial tools as well exists in discover and extract data hiding within cover files used by steganography.

*3(c) Answer:*

*[Max Word Count: 800 words]*

Text, letter

Description automatically generated

A ram capture is a snapshot of the RAM on a user’s computer. Examining a user’s RAM can provide a lot of information that would otherwise be lost when the user shuts down their machine. A variety of tools can be used to perform a memory capture such as FTK Imager, DD and Memoryze.

It is good practice to use a write blocker when performing the capture in order to preserve the integrity.

The general procedure of Memory capture is to document all the processes involved. After that to run a batch file that will collect data such as any date and time, all open files as well as important network connections. A memory dump can be collected as well as copy the paging and any hibernation files

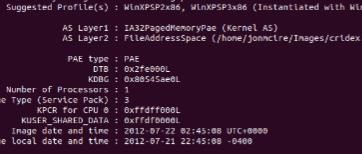
To perform a RAM capture using a tool such as FTK Imager, open the tool and simply select the type (such as physical drive / USB), Select the image destination and type and finally select the folder needed, and this will create the image file

Once captured, a memory analysis tool such as Volatility can be used to examine the capture. Volatility provides a number of plugins that can be used to examine the RAM which can provide a lot of information to the investigator.

In order to examine a RAM capture, first access the capture itself and find the profile for the Capture in order to use all the other plugins to obtain information. To identify the image, use the command.

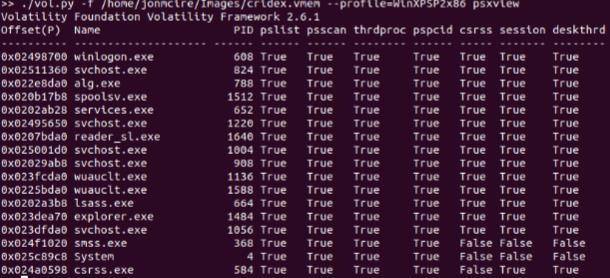


From this, we can understand basic information of the image such as the machine type and operating system used., the example shown below in the image shows that this capture came from a Windows XPmachine

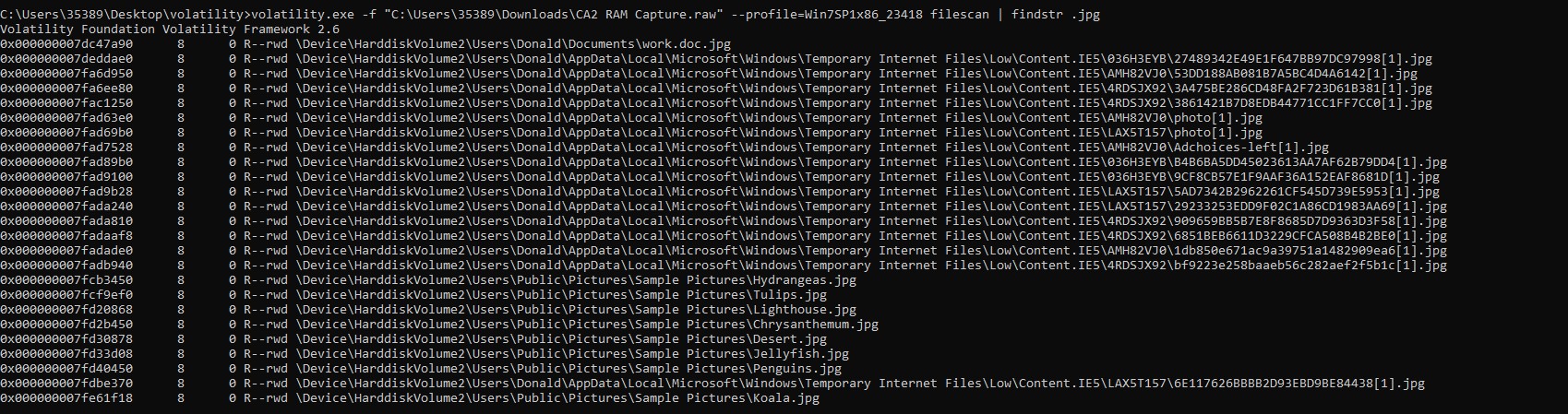


Once this information is gathered, a number of different plugins can be used to obtain information. One such plugin is pslist, which will show all the current running processes in the form of a list, along with its process ID, name and what time it was run.

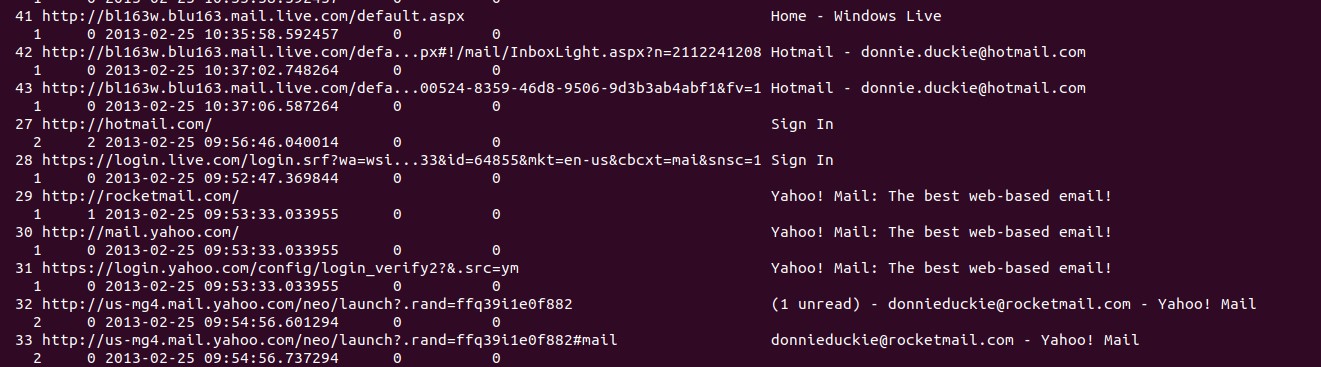
Another plugin is the psxview, which will show every single process that is hidden. A hidden process will give a False value in the pslist column, otherwise the process isn’t considered hidden. Any hidden process may intrigue the investigator to investigate deeper into the hidden process



Filescan is a plugin that will show every single currently open file at the time, as well as the directory they are stored in. the use of GREP (or strings in Windows) can be used to search for specific files if needed, or file types. This can be useful to the investigator as they can now locate files of interest, as well as their locations as well, such as which directory a certain file is located in.



Chromehistory is a plugin that needs to be downloaded externally as it doesn’t come within Volatility. It will provide all searches in chrome, and the response given. This can be used to determine which websites were visited in the chrome browser, as well as the date it was visited in.



The investigator can know where the suspect browsed, when and what searches were entered. From this as well, any potential files downloaded can be found from the actual site as well as the browser used, with a timestamp on it.

There are plugins such as connscan and netscan which retrieve network artificats which show the network connections, such as IP addresses. This was one of the processes needed to follow when performing a memory capture.

The plugin of cmdline / cmdscan, allows to show which were the last commands were run.

And finally, a memory dump could also be performed to extract files that warrant suspicion. These are all potential evidence that be used for the investigation, all obtained from analysing a captured RAM image.