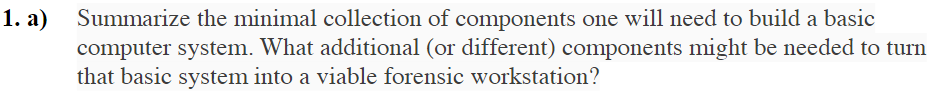
**Forensics**

**Exam Paper Revision**

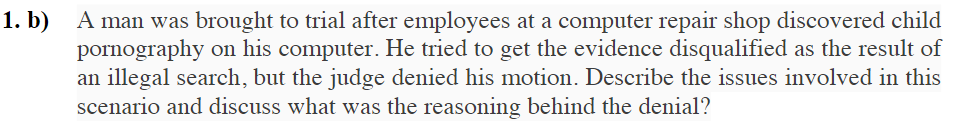
**2020 Summer SAMPLE Exam Paper**

Question 1:

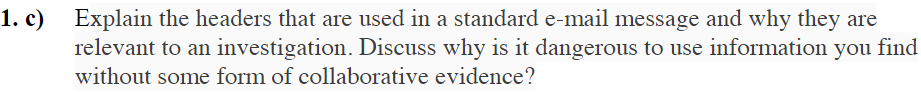


The minimal collection of components one will need to build a basic computer system is **Hard drives**, **keyboards**, and **monitors** such as **laptops**, **desktops**, and **servers** that obey standards. At the heart, a forensics workstation is just a more “*powerful computer*” Additional components needed to turn that basic system into viable forensic workstation is **Power**, **Security** and the **accessibility and authenticity of data**. It is not just the hardware that

dictates how well these factors will address either *\*More info at slides 423 to 425*



Uhhh



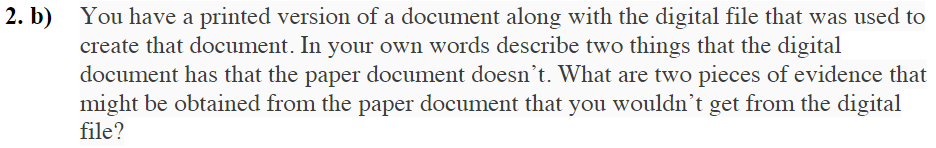
Email headers contain information about the path that email followed. One of the first things to look out for is “From: [markus.mccarthy@tudublinie](mailto:markus.mccarthy@tudublinie), Return: [markus.mccarthy@tudublinie](mailto:markus.mccarthy@tudublinie)”. If these do NOT match, we may have a spoofed email. Both paths (Return - Path) can be spoofed. It is verified by the Sender Policy Framework (SPF). The received header is the most important part of the email header and is usually the most reliable. They offer a list of all the servers the message visited as it was routed from source to destination. The top-most received header is closest to the destination, the bottom-most received header is closest to the source. This means the last received is where the mail originated from. Using the “dig” command the IP can be checked to see if this matches the domain name in the sender’s email address. (We check by comparing value from the final bottom-most received header against the value of DNS entry of the domain).

Collaborative Evidence – Is essentially the verification of data from multiple sources confirming that the evidence gathered is authentic.

Question 2:



A “*footprint*” in memory refers to the amount of main memory that a program uses or references while running. When an investigator is capturing live memory that are only catching a snapshot of a continually changing system. The actual content of memory changes as the snapshot is being made. This is known as a “*Smear Image*”. Under current technology it is impossible to get an instant capture of memory, even if you are investigating the system. All manufacturer of forensic software used to capture memory claim to have “*small footprints*”.



Certain printers mark every page with a pattern that can be uniquely associated with the device

\*Slide 34 for more information\*



Three forms of metadata 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 to spending a lot of time searching through directories. In short, the file system metadata can make the investigator’s life easier when it comes to searching the file system for any potential suspicious files. It also provides identification information for each file. Since it is possible to have the same file name in a computer, by having the same file in different directories, but not the same file in the same directory. If the investigator locates a suspicious file, there may be multiple traces of the file in several directories. By using the File System Metadata every instance of the file can be discovered as well as their location.

Certain applications that 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.

\*NOTE\* 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 unreliable as evidence

**Substantive Metadata** – Contains data which reflect the changes to a document, such as any notes added to a file made by the user. For example, it may include the text of actual changes to a document.

**Embedded Metadata** – Holds information about the file that is not always available to the user. It is a digital file that exists alongside the content (usually binary data) within the file, making the digital file self-describing

Question 3:

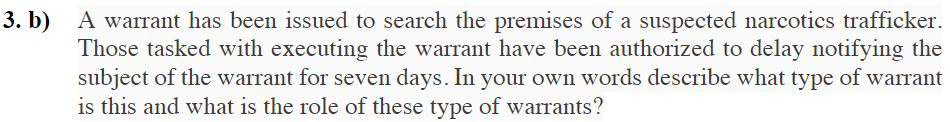


Temporary Files may still exist or be recoverable. Copies of documents are created by applications during creation or editing. The improper shutdown does not delete temporary files. Earlier versions of the files may still exist as either autosave or backup files

Reda’s Answer:

What are temporary files? Temporary files are used by your system to store data while running programs or creating permanent files, such as Word documents or Excel spreadsheets. If information is lost, your system can use temporary files to recover data.

Temporary files are a great asset in file recovery, to find files as if a machine is powered down or a file is deleted or wiped out, they still may leave behind artefacts. So even if a file is removed there is a chance that the temporary files may still exist within the system or may be recoverable, hence retrieving the contents of the removed file.



Reda’s Answer:

A warrant is a document issued by a legal or government official authorizing the police or another body to make an arrest, search premises, or carry out some other action relating to the administration of justice. Law enforcement must obtain a warrant issued by a judge or magistrate before a search or arrest can be carried out. Most searches require a warrant, and a warrant requires that the requesting agency provide reasonable cause. A warrant where a subject is not notified immediately is known as a Sneak and Peek Warrant. Other warrants require that the subject of the search be notified, however a sneak and peak warrant allows the subject of the search to be notified at least 90 days. There are many reasons for a sneak and peak such as endangering life of safety of an individual, any suspect or individual fleeing from prosecution, the destruction or tampering of evidence, or intimidation of any potential witnesses or otherwise seriously jeopardizing the investigation or unduly delaying a trial.

A sneak and peek search warrant (officially called a Delayed Notice Warrant and also called a covert entry search warrant or a surreptitious entry search warrant) is a search warrant authorizing the law enforcement officers executing it to effect physical entry into private premises without the owner's or the occupant's permission or knowledge and to clandestinely search the premises; usually, such entry requires a stealthy breaking and entering.

