3.4.1 Technical issues

a. Encryption – Encrypted data can be impossible to view without the correct key or password. Examiners should consider that the key or password may be stored elsewhere on the computer or on another computer which the suspect has had access to. It could also reside in the volatile memory of a computer (known as RAM) which is usually lost on computer shut-down; another reason to consider using live acquisition techniques, as outlined above.

b. Increasing storage space – Storage media hold ever greater amounts of data, which for the examiner means that their analysis computers need to have sufficient processing power and available storage capacity to efficiently deal with searching and analysing large amounts of data.

c. New technologies – Computing is a continually evolving field, with new hardware, software and operating systems emerging constantly. No single computer forensic examiner can be an expert on all areas, though they may frequently be expected to analyse something which they haven't previously encountered. In order to deal with this situation, the examiner should be prepared and able to test and experiment with the behaviour of new technologies. Networking and sharing knowledge with other computer forensic examiners is very useful in this respect as it's likely someone else has already come across the same issue.

d. Anti-forensics – Anti-forensics is the practice of attempting to thwart computer forensic analysis. This may include encryption, the over-writing of data to make it unrecoverable, the modification of files' metadata and file obfuscation (disguising files). As with encryption, the evidence that such methods have been used may be stored elsewhere on the computer or on another computer which the suspect has had access to. In our experience, it is very rare to see anti-forensics tools used correctly and frequently enough to totally obscure either their presence or the presence of the evidence that they were used to hide.

3.4.2 Legal issues

Legal issues may confuse or distract from a computer examiner's findings. An example here would be the 'Trojan Defence'. A Trojan is a piece of computer code disguised as something benign but which carries a hidden and malicious purpose. A lawyer may be able to argue that actions on a computer were not carried out by a user but were automated by a Trojan without the user's knowledge; such a Trojan Defence has been successfully used even when no trace of a Trojan or other malicious code was found on the suspect's computer. In such cases, a competent opposing lawyer, supplied with evidence from a competent computer forensic analyst, should be able to dismiss such an argument. A good examiner will have identified and addressed possible arguments from the "opposition" while carrying out the analysis and in writing their report.

3.4.3 Administrative issues

a. Accepted standards – There are a plethora of standards and guidelines in computer forensics, few of which appear to be universally accepted. The reasons for this include: standard-setting bodies being tied to particular legislations; standards being aimed either at law enforcement or commercial forensics but not at both; the authors of such standards not being accepted by their peers; or high joining fees for professional bodies dissuading practitioners from participating.

b. Fit to practice – In many jurisdictions there is no qualifying body to check the competence and integrity of computer forensics professionals. In such cases anyone may present themselves as a computer forensic expert, which may result in computer forensic examinations of questionable quality and a negative view of the profession as a whole.

3.4 TYPES OF INVESTIGATION

There are four main types of investigation performed by digital forensics specialists[17]. The first three are broadly similar in the activities they involve, but differ in terms of the legal restrictions and guidelines imposed as well as the type of digital evidence and form of report.

3.5.1 Criminal forensics

The largest form of digital forensics and falling under the remit of law enforcement (or private contractors working for them). Criminal forensics is usually part of a wider investigation conducted by law enforcement and other specialists with reports being intended to facilitate that investigation and, ultimately, to be entered as expert evidence before the court. Focus is on forensically sound data extraction and producing report/evidence in simple terms that a lay man will understand.

3.5.2 Intelligence gathering

This type of investigation is often associated with crime, but in relation to providing intelligence to help track, stop or identify criminal activity. Unless the evidence is later to be used in court forensic soundness is less of a concern in this form of investigation, instead speed can be a common requirement.

3.5.3 Electronic discovery (eDiscovery)

Similar to "criminal forensics" but in relation to civil law. Although functionally identical to its criminal counter part, eDiscovery has specific legal limitations and restrictions, usually in relation to the scope of any investigation. Privacy laws (for example, the right of employees not to have personal conversation intercepted) and human rights legislation often affect electronic discovery.

3.5.4 Intrusion investigation

The final form of investigation is different from the previous three. Intrusion investigation is instigated as a response to a network intrusion, for example a hacker trying to steal corporate secrets. The investigation focuses on identifying the entry point for such attacks, the scope of access and mitigating the hackers activities. Intrusion investigation often occurs "live" (i.e. in real time) and leans heavily on the discipline of network forensics.

3.5 TECHNIQUES OF DIGITAL FORENSICS

A number of techniques are used during computer forensics investigations and much has been written on the many techniques used by law enforcement in particular[1].

3.6.1 Cross-drive analysis

A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.

3.6.2 Live analysis

The examination of computers from within the operating system using custom forensics or existing *sysadmin* tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

3.6.2.1 Volatile data

Volatile data is a data that is lost if the power is switched off. Computer requires some memory space where it could store most frequently used data, intermediately results of an operation, etc. which could be access by the CPU of a computer at faster rate. Some of the examples of fast memory are CPU registers, Cache memory, Random Access Memory(RAM), etc. The access time to these memory devices is low but they are volatile in nature. RAM contains wealth of information like system registries, passwords, browsing history, information about open processes and ports, uses profile of the system i.e. who logged into the computer, what are the hardware attached to the system, remote login details, IP address, etc. which could be very useful for the forensics investigator.

As discussed earlier, there are many volatile memory units present in system like CPU registers, Cache memory, RAM, etc. with different order of volatility. Order of volatility specifies the how sensitive the memory is towards the loss of data. Higher is the order of volatility, higher are the chances of data being lost/changed/modified. Therefore, the forensics investigator must follow the order of volatility to capture data from different memory devices. The order of volatility of various digital storage devices or digital evidences is shown in *Figure 8*. The higher is the level of memory in the pyramid, higher is the order of volatility.

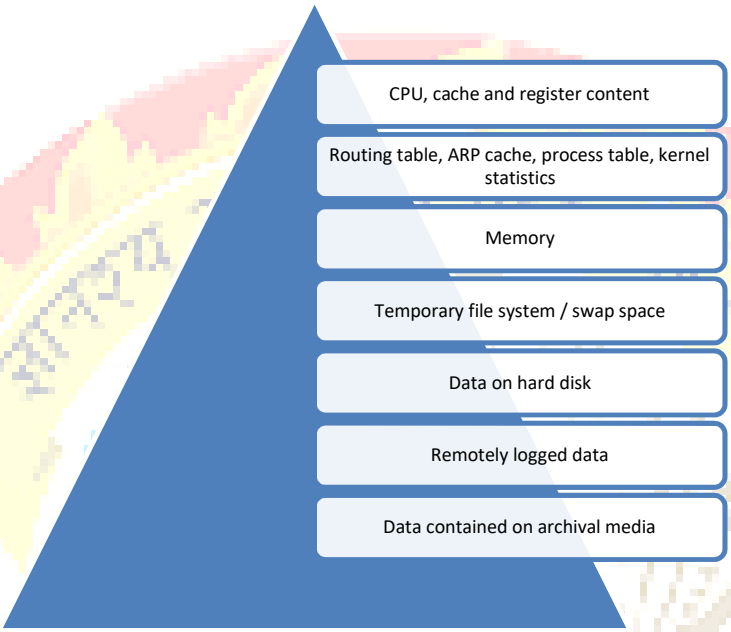

Figure 8: Order of volatility of digital evidences

3.6.3 Recovery of Deleted files

A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

3.6.4 Stochastic forensics

A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

3.6.5 Steganography

One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes. In Forensic examination, Steganalysis is used to get the details of Steganographic contents.