### CYBER FORENSICS

**Definition -**

* Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.
* It can be used in the detection and prevention of crime and in any dispute where evidence is stored digitally.
* Cyberforensics is also known as computer forensics.

**Techniques-**

* Cross-driven analysis

Correlates data from multiple hard drives

* Live analysis

Obtains data acquisitions before a PC is shut down .Traditionally, the computer forensic examiner would make a copy (or acquire) information from a device which is turned off. A write-blocker [[4]](https://forensiccontrol.com/resources/beginners-guide-computer-forensics/" \l "glossary) would be used to make an exact bit for bit copy [[5]](https://forensiccontrol.com/resources/beginners-guide-computer-forensics/" \l "glossary) of the original storage medium. The examiner would work from this copy, leaving the original demonstrably unchanged.[MAKING A COPY]

However, sometimes it is not possible or desirable to switch a computer off. It may not be possible if doing so would, for example, result in considerable financial or other loss for the owner. The examiner may also wish to avoid a situation whereby turning a device off may render valuable evidence to be permanently lost. In both these circumstances the computer forensic examiner would need to carry out a ‘live acquisition’ which would involve running a small program on the suspect computer in order to copy (or acquire) the data to the examiner’s hard drive.

By running such a program and attaching a destination drive to the suspect computer, the examiner will make changes and/or additions to the state of the computer which were not present before his actions. However, the evidence produced would still usually be considered admissible if the examiner was able to show why such actions were considered necessary, that they recorded those actions and that they are to explain to a court the consequences of those actions.

* Deleted file recovery

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 sytems do not always erase physical file data, allowing investigators to reconstruct it from the physical [disk sectors](https://en.wikipedia.org/wiki/Disk_sector). [File carving](https://en.wikipedia.org/wiki/File_carving) involves searching for known file headers within the disk image and reconstructing deleted materials.

**Stages of examination -**

The computer forensic examination process is divided into six stages, presented in their usual chronological order.

* Readiness

Forensic readiness is an important and occasionally overlooked stage in the examination process. In commercial computer forensics it can include educating clients about system preparedness; for example, forensic examinations will provide stronger evidence if a device’s auditing features have been activated prior to any incident occurring.

For the forensic examiner themself, readiness will include appropriate training, regular testing and verification of their software and equipment, familiarity with legislation, dealing with unexpected issues (e.g., what to do if indecent images of children are found present during a commercial job) and ensuring that the on-site acquisition (data extraction) kit is complete and in working order.

* Evaluation

The evaluation stage includes the receiving of instructions, the clarification of those instructions if unclear or ambiguous, risk analysis and the allocation of roles and resources. Risk analysis for law enforcement may include an assessment on the likelihood of physical threat on entering a suspect’s property and how best to counter it.

Commercial organisations also need to be aware of health and safety issues, conflict of interest issues and of possible risks – financial and to their reputation – on accepting a particular project.

* Collection

If acquisition is to be carried out on-site rather than in a computer forensic laboratory, then this stage would include identifying and securing devices which may store evidence and documenting the scene. Interviews or meetings with personnel who may hold information relevant to the examination (which could include the end users of the computer, and the manager and person responsible for providing computer services, such as an IT administrator) would usually be carried out at this stage.

The collection stage also involves the labelling and bagging of evidential items from the site, to be sealed in numbered tamper-evident bags. Consideration should be given to securely and safely transporting the material to the examiner’s laboratory.

* Analysis

Analysis depends on the specifics of each job. The examiner usually provides feedback to the client during analysis and from this dialogue the analysis may take a different path or be narrowed to specific areas. Analysis must be accurate, thorough, impartial, recorded, repeatable and completed within the time-scales available and resources allocated.

There are myriad tools available for computer forensics analysis. It is our opinion that the examiner should use any tool they feel comfortable with as long as they can justify their choice. The main requirements of a computer forensic tool is that it does what it is meant to do and the only way for examiners to be sure of this is for them to regularly test and calibrate the tools they rely on before analysis takes place.

Dual-tool verification can confirm result integrity during analysis (if with tool ‘A’ the examiner finds artefact ‘X’ at location ‘Y’, then tool ‘B’ should replicate these results).

* Presentation

This stage usually involves the examiner producing a structured report on their findings, addressing the points in the initial instructions along with any subsequent instructions. It would also cover any other information which the examiner deems relevant to the investigation.

The report must be written with the end reader in mind; in many cases the reader will be non-technical, and so reader-appropriate terminology should be used. The examiner should also be prepared to participate in meetings or telephone conferences to discuss and elaborate on the report.

* Review

As with the readiness stage, the review stage is often overlooked or disregarded. This may be due to the perceived costs of doing work that is not billable, or the need ‘to get on with the next job’.

However, a review stage incorporated into each examination can help save money and raise the level of quality by making future examinations more efficient and time effective.

A review of an examination can be simple, quick and can begin during any of the above stages. It may include a basic analysis of what went wrong, what went well, and how the learning from this can be incorporated into future examinations’. Feedback from the instructing party should also be sought.

Any lessons learnt from this stage should be applied to the next examination and fed into the readiness stage.

**Issues-**

The issues facing computer forensics examiners can be broken down into three broad categories: technical, legal and administrative.

* Technical issues

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 [[6]](https://forensiccontrol.com/resources/beginners-guide-computer-forensics/" \l "glossary)) which is usually lost on computer shut-down; another reason to consider using live acquisition techniques, as outlined above.

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.

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.

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.

* 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. Trojans have many uses, and include key-logging [[7]](https://forensiccontrol.com/resources/beginners-guide-computer-forensics/" \l "glossary)), uploading and downloading of files and installation of viruses. 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.

* Administrative issues

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.

**INSTITUTE:**

Resource Centre for Cyber Forensics (RCCF) is a pioneering institute, pursuing research activities in the area of Cyber Forensics. The centre was dedicated to the nation by the then Honorable union minister in August 2008.

**TOP 5 COMPANIES IN CYBER FORENSICS :**

 [ANA Cyber Forensic Pvt. Ltd.](https://www.siliconindia.com/cyber-forensic/ana-cyber-forensic-catid-61-cid-708.html)

 [A & R Info Security Solutions](https://www.siliconindia.com/cyber-forensic/A-and-R-info-security-solutions-catid-61-cid-703.html)

 [Forensics Guru](https://www.siliconindia.com/cyber-forensic/forensics-guru-catid-61-cid-707.html)

 [Secugenius](https://www.siliconindia.com/cyber-forensic/secugenius-catid-61-cid-704.html)

 [Synclature](https://www.siliconindia.com/cyber-forensic/synclature-catid-61-cid-709.html)

**Case:-**

[The Neglected Cyber Forensics Issues Of Aarushi Murder Case](http://perry4law.org/cfii/?p=55)

RESOURCES:

<http://www.cyberlawsindia.net/cases1.html>

<https://forensiccontrol.com/resources/beginners-guide-computer-forensics/>

<https://www.techopedia.com/definition/2388/cyberforensics>

<http://searchsecurity.techtarget.com/definition/computer-forensics>