**Challenges in Digital Forensics**

Digital forensics has been defined as the use of scientifically derived and proven methods towards the identification, collection, preservation, validation, analysis, interpretation, and presentation of digital evidence derivative from digital sources to facilitate the reconstruction of events found to be criminal.[[1]](https://legaldesire.com/challenges-faced-by-digital-forensics/" \l "_ftn1) But these digital forensics investigation methods face some major challenges at the time of practical implementation. Digital forensic challenges are categorized into three major heads as per Fahdi, Clark, and Furnell (2013) these are:-

1. **Technical challenges**
2. **Legal challenges**
3. **Resource Challenges**
4. **Technical Challenges**

As technology develops crimes and criminals are also developed with it. Digital forensic experts use forensic tools for collecting shreds of evidence against criminals and criminals use such tools for hiding, altering or removing the traces of their crime, in digital forensic this process is called Anti- forensics technique which is considered as a major challenge in digital forensics world. ***Anti-forensics techniques******[[6]](https://legaldesire.com/challenges-faced-by-digital-forensics/" \l "_ftn6)*** are categorized into the following types:-

|  |  |  |
| --- | --- | --- |
| **S. No.** | **Type** | **Description** |
| **1** | Encryption | It is legitimately used for ensuring the privacy of information by keeping it hidden from an unauthorized user/person. Unfortunately, it can also be used by criminals to hide their crimes. |
| **2** | Data hiding in storage space | Criminals usually hide chunks of data inside the storage medium in invisible form by using system commands, and programs. |
| **3** | Covert Channel | A covert channel is a communication protocol which allows an attacker to bypass intrusion detection technique and hide data over the network. The attacker used it for hiding the connection between him and the compromised system. |

**Other Technical challenges are**:

* Operating in the cloud
* Time to archive data
* Skill gap
* Steganography

1. **Legal Challenges**

The presentation of digital evidence is more difficult than its collection because there are many instances where the legal framework acquires a soft approach and does not recognize every aspect of cyber forensics, as in ***Jagdeo Singh V. The State and Ors***, case Hon’ble High Court of Delhi held that *“while dealing with the admissibility of an intercepted telephone call in a CD and CDR which was without a certificate under Sec. 65B of the Indian Evidence Act, 1872 the court observed that the secondary electronic evidence without certificate u/s. 65B of Indian Evidence Act, 1872 is not admissible and cannot be looked into by the court for any purpose whatsoever.”* This happens in most of the cases as the cyber police lack the necessary qualification and ability to identify a possible source of evidence and prove it. Besides, most of the time electronic evidence is challenged in the court due to its integrity. In the absence of proper guidelines and the nonexistence of proper explanation of the collection, and acquisition of electronic evidence gets dismissed in itself.

|  |  |  |  |
| --- | --- | --- | --- |
| **Legal Challenges** | | | |
| **S. no** | **Type** | **Description** | |
| **1** | Absence of guidelines and standards | In India, there are no proper guidelines for the collection and acquisition of digital evidence. The investigating agencies and forensic laboratories are working on the guidelines of their own. Due to this, the potential of digital evidence has been destroyed. | |
| **2** | Limitation of the Indian Evidence Act, 1872 | The Indian Evidence Act, 1872 have limited approach, it is not able to evolve with the time and address the E-evidence are more susceptible to tampering, alteration, transposition, etc. the Act is silent on the method of collection of e-evidence it only focuses on the presentation of electronic evidence in the court by accompanying a certificate as per subsection 4 of Sec. 65B[[12]](https://legaldesire.com/challenges-faced-by-digital-forensics/" \l "_ftn12). This means no matter what procedure is followed it must be proved with the help of a certificate. |

**Other Legal Challenges**

* Privacy Issues
* Admissibility in Courts
* Preservation of electronic evidence
* Power for gathering digital evidence
* Analyzing a running computer

1. **Resource Challenges**

As the rate of crime increases the number of data increases and the burden to analyze such huge data is also increases on a digital forensic expert because digital evidence is more sensitive as compared to physical evidence it can easily disappear. For making the investigation process fast and useful forensic experts use various tools to check the authenticity of the data but dealing with these tools is also a challenge in itself.

**Types of Resource Challenges are:-**

* Change in technology

Due to rapid change in technology like operating systems, application software and hardware, reading of digital evidence becoming more difficult because new version software’s are not supported to an older version and the software developing companies did provide any backward compatible’s which also affects legally.

* Volume and replication

The confidentiality, availability, and integrity of electronic documents are easily get manipulated.  The combination of wide-area networks and the internet form a big network that allows flowing data beyond the physical boundaries. Such easiness of communication and availability of electronic document increases the volume of data which also create difficulty in the identification of original and relevant data.