

Digital Forensics analysis report

Task 1:

Digital Forensics analysis reportTask 1:	1
Introduction :	1
Scope of digital forensics :	1
Application of digital forensics :	2
Current industry trends :	2
Challenges in digital forensics :	3
Conclusion :	3

Introduction :

Digital forensics is a branch of forensics sciences that focuses on investigating digital evidence. In simple words: On a crime scene, every digital device found that is suspected to be related to the crime must be analyzed by digital forensic experts in order to find evidence, information that could help to identify the criminal or could help to understand the circumstances of the crime committed. Digital forensics is used in cybercrime investigations, criminal cases and civil cases. Tasks related to digital forensics includes: identification, preservation, analysis and presentation of evidence. In the past few years according to the “National Digital Forensic Science Strategy” published in 2020 by the National Police Chiefs' Council (NPCC), over 90% of crimes involve a digital element (UK Digital Forensic Strategy [3]) . Digital devices can store more than 50 000, messages, thousand of images an video to analyze, this huge amount of data to analyze has led to the creation of the digital forensics field. (Digital forensics definition – IBM [1])

Scope of digital forensics :

Digital forensics includes many different domains:

- Computer forensics: aims to analyze computer and storage devices, recover and analyze deleted files on those devices. Computers can contain a lot of threats and are most used by hackers: that's the main kind of device used for cybercriminals attacks.
- Mobile forensics is one of the most important field of digital forensics: smartphone dominate usage of digital devices, in fact, it consist mainly of extracting from phones messages GPS data, app data, sims data.
- Network forensics consist in analyzing networks to detect and analyze cyberattacks.
- Cloud forensics: over the past 15 years, the cloud has grown up, servers became more and more used by cybercriminals. Analyzing data and evidence on servers is becoming complex to investigate since this massive increase in digital data.
- IoT forensics: since smart devices are getting small and smaller devices are becoming more and more powerful over different format, IoT forensics is a very important domains that mainly consist in securing and analyzing devices on the field, for example with the use of faraday pouches, mobile analyzing platforms that can be brought on the field when the situation needs it.

Digital forensics has multiple scope: it must adapt to every situation, always prioritizing protection and integrity of evidence, and can be able to analyze many different format of device: from mobile phone and computers to networks and cloud based infrastructures. (Mobile device forensics overview [9])

Application of digital forensics :

Digital forensics is used to cover many different crime scenarios:

- Cybercrime: hacking, ransomware, phishing To identify attacker and trace origin of attacks.
- Fraud investigation: analyze financial transactions, detect fraud patterns, trace illegal money flows over the internet.
- Intellectual property thefts: identifying data theft, unauthorized access, mostly used for companies.
- Counterterrorism: analyse suspected devices to detect and prevent potential terrorist attacks, reconstruct actions (cctvs, videos, etc...)
- Cryptocurrency crimes: analyze blockchain to track illegal transaction, identify illegal funds (for example useful to detect drug and weapons sales)

Forensics experts helps to reconstruct digital footprints to solve cases. (Digital forensics investigations overview [2])

Current industry trends :

The digital industry is constantly growing and evolving new technologies and more powerful devices are released every day, allowing malicious people to imagine and setup new anti-forensics technics. Digital forensics experts are now using AI and machine learning process to automate analysis, detect threat and evidence patterns and process larger datasets. When today the cloud based industry is being prevalent on the business with larger datasets, newer cloud based forensics infrastructure are created: Digital forensics as a service (DFaaS) represent the development and distribution of cloud based forensics tools that delegate the computing power to servers to break password, analyze huge amount of data.

Those newer technologies shows that digital forensics expert must adapt continuously to newer technologies to handle the massive increase of cloud data, internet traffic and massive use of digital devices. (Future of digital forensics technologies [4]) (Digital forensics market growth [5])

Challenges in digital forensics :

Based on the recent explosion of cloud infrastructure, massive use and accessibility to the internet, digital forensics experts are encountering many different challenges:

- Data volume: huge amount of data to analyze require stronger infrastructure and more human resources to investigate,
- Encryption: algorithms are becoming more complex and require more computing power: especially with the future quantum computing based encryption that still represent a serious threat to millions of companies who still uses weak algorithm that can be broke easily with quantum computers.
- Cloud complexity: each country has its own laws regarding cloud data, which are spread across multiple platforms and different countries. That can make investigations way harder regarding the amount of different jurisdictions.
- Different formats: evidences are spread among a lot of different devices: smartphones, computers, iot and smart home devices, that get investigations a lot harder.

- Evidence integrity: regarding the laws, a device modified between a crime scene and the court law can bring an evidence legally unusable. Setting up a proper chain of custody is a primary task in digital forensic.

In short: Investigators are facing must always ensure evidence are always reliable and admissible in court, and must handle various of data format. (Challenges and trends in digital forensics [6]) (Digital evidence standards and practices [7]) (Mobile forensics trends [8])

Conclusion :

Digital forensics is essential in modern investigations, mostly used in law enforcement and cybersecurity. Since digital devices have become over the past twenty years the most used source of data, communications, and cybercrime. It must constantly adapt to newer technologies and newer anti-forensics technics including artificial intelligence, massive use of cloud technologies, and quantum computing. The future of digital forensics mostly depends on technological improvements and legal frameworks.

References :

Web sources:

[1]

IBM (n.d.) *What is digital forensics?* Available at:

<https://www.ibm.com/think/topics/digital-forensics> (Accessed: 28 April 2026).

[2]

Cognyte (n.d.) *Digital forensics investigations: An overview.* Available at:

<https://www.cognyte.com/blog/digital-forensics-investigations/> (Accessed: 28 April 2026).

[3]

NPCC (2020) *National Digital Forensic Science Strategy.* Available at:

<https://www.npcc.police.uk/SysSiteAssets/media/downloads/publications/publications-log/2020/national-digital-forensic-science-strategy.pdf> (Accessed: 28 April 2026).

[4]

TechUK (n.d.) *The future of digital forensics: how technology is transforming investigations.* Available at: <https://www.techuk.org/resource/the-future-of-digital-forensics-how-technology-is-transforming-investigations.html> (Accessed: 28 April 2026).

[5]

Grand View Research (n.d.) *Digital forensics market size report.* Available at:

<https://www.grandviewresearch.com/industry-analysis/digital-forensics-market> (Accessed: 28 April 2026).

[6]

IMedPub (n.d.) *Advances in digital forensics: addressing challenges and emerging trends.* Available at: <https://www.imedpub.com/articles/advances-in-digital-forensics-addressing-challenges-and-emerging-trends.php?aid=50873> (Accessed: 28 April 2026).

[7]

NIST (n.d.) *Digital evidence*. Available at: <https://www.nist.gov/digital-evidence> (Accessed: 28 April 2026).

[8]

Control Risks (n.d.) *Key trends for digital forensics on mobile devices*. Available at: <https://www.controlrisks.com/our-thinking/insights/key-trends-for-digital-forensics-on-mobile-devices> (Accessed: 28 April 2026).

[9]

Wikipedia (n.d.) *Mobile device forensics*. Available at: https://en.wikipedia.org/wiki/Mobile_device_forensics (Accessed: 28 April 2026).

Length: 1139 words



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David