

Task 1 – Digital Forensics

Mathis FENOT – 17/04/2026

Table des matières

1.	Current State of Digital Forensics: Tools, Features, and Capabilities	2
2.	Intersection of Digital Forensics and Cybersecurity	3
3.	Emerging Trends in Digital Forensics	4
4.	Key Challenges in Digital Forensics	5
5.	National and International Job Market.....	6

1. Current State of Digital Forensics: Tools, Features, and Capabilities

Digital Forensics is a very recent field, that was created in 1983 after the first occurrences of computer crimes over the 70's and the 80's. During the forty years since its creation, it has matured from a simple investigative practice into a core component of modern cyber defence and legal systems. According to recent industry reports, the field is increasingly driven by rising cybercrime, regulatory compliance needs, and enterprise adoption across sectors such as finance, healthcare, and government.

The tools used are numerous and vary a lot, and as such they respond to various needs, such as the need to acquire data and image it while preserving its integrity, the need to retrieve deleted, hidden or corrupted files, which is also known as data recovery or carving.

There are the imaging tools, such as Autopsy, EnCase imager, FTK Imager. They allow to create copies of data which can be later used as evidences. There are also the memory capture tools, used to capture volatile data. Volatility, Magnet RAM Capture count as such tools. A third type of digital forensics tools is the network forensics tools. These ones are used on network packets and traffic analyses. Cisco Secure Network Analytics is an example of tools like that. All of the different digital forensics tools also support the digital forensics regulations, one of them being the chain of custody for example, in order to be able to present the acquired evidences in court without tempering with their integrity. There are others functions that they can do, such as memory , cloud and mobile forensics. Some of the recent advancements in the field integrate automation and Artificial Intelligence into these tools, which allow them to process more data faster than usual.

Sources

- [Reanin, Digital Forensics Market Size & Share Analysis - March 2026](#)
- [Cornell University, Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation - December 2022](#)
- [BlueVoyant, Digital Forensics: Get Started with These 9 Open Source Tools](#)
- [Forensics Colleges, A Guide to Digital Forensics and Cybersecurity Tools \(2026\) - January 21 2026](#)
- [Science Direct, Unveiling cybersecurity mysteries: A comprehensive survey on digital forensics trends, threats, and solutions in network security - November 2025](#)
- [Journal of Digital Forensics, Security and Law, Digital Forensic Readiness in Organizations: Issues and Challenges - December 2017](#)

2. Intersection of Digital Forensics and Cybersecurity

Digital forensics is a domain deeply connected with the one of cybersecurity. Because cybersecurity focuses on defence and cyber-attacks prevention, digital forensics focuses on investigating said attacks in response to them. There are different ways for the cybersecurity field and the digital forensics field to intersect. One of them is over compliance and governance. In order to meet regulatory requirements, like the GDPR for example, organizations have to use digital forensics into the cybersecurity frameworks.

Digital forensics is also used to recover lost data following a cyber-attack and also allow to provide evidences for courtrooms and other legal procedures. The use of digital forensics in complement to cybersecurity allows organisations to establish the root cause of the attacks, how they are carried and what can be done to counter them, thus helping the cybersecurity team to improve the organisation defences.

Sources :

- SISA, Digital Forensics in Cyber Security 101
- SpirelTES, Digital Forensics in 2025: Challenges, Trends and Toolkits
- MarketsandMarkets, Digital Forensics Market Emerging Trends to Watch in 2024
- World Economic Forum, Global Cybersecurity Outlook 2026 - January 2026

3. Emerging Trends in Digital Forensics

Nowadays, the digital forensics field is undergoing significant transformation due to technological innovation and new threat landscapes, especially with the arrival of Artificial Intelligence.

Artificial Intelligence is revolutionizing digital forensics by enabling the automation of evidence analysis, detecting anomalies and different patterns faster than the existing tools, and it also helps predict attacker behaviour to a certain degree. However, while AI significantly helps cybersecurity and digital forensics, it also empowers cybercriminals. A new trend that is emerging is the cloud computing. With more and more companies turning their gaze toward the cloud, it introduces new challenges related to multi-tenancy and jurisdiction. Internet of Things (IoT) is expanding the field of possible cyber-attacks as the number of connected devices increases. Some academic institutions state that investigating such connected devices is a lot more complicated than usual due to their heterogeneity and data fragmentation.

Quantum technology presents another new aspect to the field of digital forensics, for it allows cryptographic analysis to go past their current limits. There are other applications of quantum technology that are currently being studied.

Finally, there is a global effort of harmonising the legal framework of digital forensics.

Sources :

- NCC Group, Digital investigations: Opportunities and challenges - January 2025
- Computer Forensics Lab, Digital Forensic Trends 2025: AI, Cloud, and Risk - February 2026
- Salvation DATA, Cybersecurity and Digital Forensics-Their Critical Link - March 2025

4. Key Challenges in Digital Forensics

Despite the technological advancements, digital forensics still faces several challenges. The first one is about the data volume and the complexity of its investigation. Because of the growth of digital data, it is more and more challenging for an analysis to be performed on them without taking too much time

Another challenge that digital forensics faces is the end-to-end encryption and the privacy regulations. More and more applications like WhatsApp and Signal use end-to-end encryption, which complicates the access of the evidences if their integrity must remain intact.

Data destruction presents itself to be challenging for digital forensics, as there is a risk of losing the evidence or tampering with its integrity while recovering it.

The cloud, while being a new technology and bringing opportunities and advantages to the digital world, its distributed data storage may raises legal questions about the ownership or the access rights, and as such the admissibility in court of evidences acquired through it.

One of the final key challenges is that with the constant evolution of technologies, digital forensics analysts must constantly adapt their tools and their skills.

Sources :

- [Geeks for Geeks, Challenges in Digital Forensics - April 2026](#)

5. National and International Job Market

Nowadays, the global market for digital forensics professionals is growing rapidly because of technological innovations, an increasing number of cyber-crimes, digital transformation... Certain sectors such as law enforcement, governmental agencies, healthcare, technology are searching for an increased number of digital forensics professionals. And so the jobs of digital forensics analyst, malware analyst, cybercrime investigator are jobs that are highly demanded.

The demand for digital forensics professionals is concentrated in part of the world such as Europe, North America and Asia-Pacific. North America dominated the digital forensics market in 2025 with 37% of the market, while Asia-Pacific will have the fastest growth over the coming period according to the predictions.

Sources :

- [Linkedin, Digital Forensic Analyst](#)
- [LinkedIn, Digital Forensic Analyst at city of Clovi](#)
- [TechRadar, Why modern cyber conflict is partly a global skills challenge - April 2026](#)
- [Precedence Research, Digital Forensics Market Size, Share and Trends 2026 to 2035 - March 2026](#)