International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 4, Jul-Aug 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Digital Forensics for Law Enforcement

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Digital forensics is a branch of investigative work that primarily focuses on recovering and analyzing materials from digital devices. At its core, digital forensics entails the meticulous extraction, preservation, and interpretation of digital evidence to shed light on unlawful activities. Digital forensics plays an important role in numerous law enforcement settings. One of the reasons the digital forensics field has seen such growth is that the world is increasingly connected; new devices have become commonplace, providing numerous avenues for cybercriminals and leading to crimes such as hacking, identity theft, and data breaches. Digital forensics professionals are trained in collecting digital evidence that can aid law enforcement professionals in bringing cybercriminals to justice. Cybercriminals are developing new ways to thwart digital forensic investigators.. Digital forensics provides law enforcement agencies with the tools and techniques necessary to collect, analyze, and preserve this evidence, helping to build stronger cases and bring criminals to justice. This paper provides an introduction to digital forensics in law enforcement.

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Digital Forensics for Law Enforcement" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-4, August 2025, pp.717-727, URL: www.ijtsrd.com/papers/ijtsrd97329.pdf

IJTSRD97329

INTRODUCTION

It is difficult to imagine life today without digital devices. Digital devices such as cell phones, tablets, gaming consoles, laptops, and desktop computers have become an indispensable part of modern society. With the proliferation of these devices in our everyday lives, there is a tendency to use information derived from them for criminal activities. As technologies develop, crimes and criminals are also evolving with them. Crimes such as fraud, drug trafficking, homicide, hacking, forgery, and terrorism often involve computers. Crimes committed within electronic or digital domains, particularly within cyberspace, have become common. The best way to improve computer security is to arm crime investigation with the most effective tools, techniques, and knowledge possible [1].

Criminals are using technology to commit offenses and create new challenges for law enforcement agents, attorneys, judges, military, and security professionals. This development has led to the rise of digital forensics, which is essentially the uncovering and examination of evidence located on all things electronic with digital storage, including computers, cell phones, and networks. Digital forensics has become an important instrument in identifying and solving computer-based and computer-assisted crimes.

WHAT IS DIGITAL FORENSICS?

To fight computer crimes, digital forensics (DF) (also known as digital forensic science) originated in law enforcement, computer security, and national defense. Forensics is the application of science to the legal process. It involves the application of the natural, physical, and social sciences to law matters. As shown in Figure 1, digital forensics is a multidisciplinary discipline involving computer science, engineering, information science, and criminal justice**.** It is the smart technology for collecting evidence in crime used by forensics professionals and law enforcement to be represented in the court of law to convict the individuals or groups who committed the crime. Digital forensics is the application of analysis techniques to the reliable and unbiased collection, analysis, interpretation, and presentation of digital evidence. It is commonly used in both criminal law and private investigations. It

serves as supporting proof or corroborating evidence often made by prosecutors and defendants. The term digital forensics was originally used as a synonym for computer forensics because only computers were included. Over the last four decades or so, as computers have become connected to several computer networks, the term computer forensics has become too limited to encompass the entire field. The field of digital forensics has expanded to cover the investigation of all devices capable of storing digital data. As illustrated in Figure 2, digital forensics can be split up into five branches [2-4]:

- *Computer Forensics:* This provides the collection, identification, preservation, and analysis of data from personal computers, laptops, and storage computing devices.
- *Network Forensics:* This branch monitors, registers, and analyzes any network activity. The network can be LAN, MAN, or WAN/Internet.
- *Mobile Device Forensic:* This is a branch of digital forensics relating to the recovery of digital evidence or data from mobile devices such as smartphones, SIM cards, mobile phones, GPS devices, tablets, PDAs, and game consoles.
- *Database Forensics:* This investigates any access to a database and reports any changes made in the database and their metadata.
- *Forensic Data Analysis:* This branch of forensics analyzes structured data with the aim of discovering and analyzing patterns of fraudulent activities resulting from crime.

Each branch of digital forensics has its guidelines on how to conduct investigations and handle data. Mobile device forensics is a newly evolving branch of digital forensics related to recovering digital evidence from a mobile device. The digital medium has become the key area for email hacking. Other forms of digital forensics include malware forensics, email forensics, memory forensics, wireless forensics, live forensics, cloud forensics, IoT forensics, and disk forensics.

CHARACTERISTICS OF DIGITAL FORENSICS

Digital forensics is used to help investigate cybercrime or identify direct evidence of a computer-assisted crime. The concept of digital forensics dates back to the late 1990s and early 2000s when it was considered as computer forensics. The legal profession, law enforcement, policymakers, the business community, education, and government all have a vested interest in DF. Digital forensics has been traditionally associated with criminal law. It requires rigorous standards to stand up to–cross-examination in court.

For digital evidence to be accepted in a court of law, it must be appropriately handled to avoid tampering. As illustrated in Figure 3, the key processes in digital forensics include the following [5,6]:

- *Identification:* This finds the evidence, noting where it is stored.
- *Preservation:* This preserves the data and prevents people from tampering with the evidence.
- *Collection:* This involves acquiring digital evidence, usually by seizing physical assets, such as computers, hard drives, or phones.
- *Examination:* This involves identifying and extracting data.
- *Analysis:* This analyzes data and concludes whether to prove or disprove a case based on the evidence found.
- *Interpretation*: This involves interpreting the result and making sense of it.
- *Documentation:* This creates a record of all the data to recreate the crime scene.
- *Presentation*: This summarizes and draws a conclusion.

Digital forensics is usually associated with the detection and prevention of cybercrime.

It is related to digital security in that both are focused on digital incidents. While digital security focuses on preventative measures, digital forensics focuses on reactive measures. Peer-to-peer file sharing is the soft area targeted by criminals.

Forensics tools are used by forensics experts to analyze Internet activity, e-mails, and other collected pieces of evidence from the system or the scene. The Forensics tools made the job of forensics professionals manageable in addition to obtaining more accurate results [7]. Some of the tools are displayed in Figure 4 [7].

BRIEF HISTORY

Digital forensics is a couple of decades old, beginning in the late 1970s as a response to a demand for service from the law enforcement community. In the 1980s, the field was known as computer forensics; in the 1990s, it became known as digital forensics. The first digital investigators worked for law enforcement agencies. Canada was the first country to pass legislation on forensics in 1983, with the United States following in 1986, Australia in 1989, and Britain's Computer Misuse Act in 1990. The history of digital forensics is summarized as follows [4]:

- Most of the first criminal cases that involved computers were for financial fraud. Other early computer crimes occurred in 1969 and 1970 when student protesters burned computers at various universities.
- In the 1970s, the United States introduced the 1978 Florida Computer Crimes Act, which was based on legislation against unauthorized alteration or deletion data in a computer system;
- In the 1980s, digital forensics training courses were developed by several organizations. The field of digital forensics grew rapidly in the late 1980-90s;
- Specialized computer forensic groups such as the FBI's Computer Analysis and Response team were established in the mid-1980s;
- In 1983, Canada was the first nation to pass legislation in the field of cybercrimes and computer forensics;
- In 1985, Britain created a computer crime department;
- In 1989, cybercrimes were added to the official list of crimes in Australia;
- The 1990 Britain's Computer Misuse Act made digital forensics well-recognized all over the world;
- In 1992, Collier and Spaul first used the term "computer forensics" in an academic paper;
- In 1993, the first International Conference on Computer Evidence was held in the United States;
- In 1995, International Organization on Computer Evidence (IOCE) was formed;
- In 2001, Britain created the National Hi-Tech Crime Unit;
- In 2004, 43 countries signed The Convention of Cybercrime;
- 2005 was marked by the appearance of an ISO standard for digital forensics.
- The years 1999–2007 were a kind of "golden age" for digital forensics.

DIGITAL FORENSIC SOFTWARE

Law enforcement agencies utilize a variety of digital forensics tools to investigate crimes. Digital forensics software is a specialized suite of tools designed to extract, analyze, and preserve digital evidence from various electronic devices and platforms. Used predominantly by law enforcement, cybersecurity professionals, and corporate investigators, this software aids in investigating incidents ranging from data breaches to cybercrimes. Digital forensics software for law enforcement helps investigators analyze digital evidence from computers, mobile devices, and other sources to uncover crucial information for criminal investigations. Navigating the world of digital forensics software can be a complex task, given the numerous choices and varied functionalities each tool offers. Popular options digital forensics software options include the following [8-10]:

- *Autopsy:* A popular, open-source digital forensics platform that provides a graphical interface for analyzing various data sources, including disk images, logical files, and unallocated space. Forensic investigators utilize Autopsy to decipher what transpired on a computer or phone. Its goal is to provide an intuitive, modular, end-to-end solution.
- *The Sleuth Kit:* A collection of command-line tools that can be used independently or integrated with Autopsy for forensic analysis. Used in conjunction with Autopsy, The Sleuth Kit is a collection of command-line tools for analyzing disk images and file systems.
- *FTK Forensic Toolkit:* Forensic Toolkit (FTK) is a digital forensics software that excels in the acquisition, analysis, and reporting of digital evidence stored in computers and mobile devices. It is a leading solution designed for comprehensive digital forensic investigations. With its specialized tools, it aids investigators in recovering, reviewing, and analyzing digital evidence from a myriad of digital devices.
- *OpenText Forensic:* Best for comprehensive digital investigations. This is a long-standing commercial tool used by law enforcement and government agencies to find and analyze digital evidence. OpenText Forensic is a renowned tool that empowers professionals to undertake extensive digital investigations, delving into hard drives, smartphones, and a plethora of other devices.
- *Belkasoft:* It offers software for acquiring, extracting, and analyzing data from various sources, including mobile devices and cloud storage.
- *Magnet AXIOM:* This is best for mobile and cloud evidence recovery. Magnet AXIOM is a comprehensive commercial tool designed to aid computer forensic examiners in retrieving evidence from a variety of digital platforms, particularly mobile phones and cloud environments. It supports investigation and

analysis of computer, mobile, cloud, and vehicle data.

- *Cyber Triage:* This focuses on providing efficient tools for incident response by diving deep into memory analysis and integrating threat intelligence.
- *MailXaminer:* Best for email analysis and recovery. MailXaminer is a dedicated tool designed to unlock the complexities of email data for forensic investigators. It is tailored to specialize in the extraction, research, and recovery of email content.
- *ExtraHop*: Best for real-time network activity insights. ExtraHop is a distinguished tool offering in-depth monitoring and insights into real-time network activities. With its advanced graphical interface, it simplifies the complex task of tracking network anomalies, proving it is exceptionally suited for providing real-time network activity insights.
- *Detego Global:* Best for unified digital forensics operations. Detego Global is at the forefront of streamlining digital forensics, offering tools and functionalities that unify operations from endpoint to endpoint. It boasts a wide range of features tailored for forensic professionals, from handling volatility in digital evidence to efficient endpoint analysis.
- *Cellebrite:* A tool used for mobile device forensics, including data extraction and analysis. It provides digital forensics solutions for data extraction and analysis, particularly for mobile devices, and is used by law enforcement, intelligence, and security agencies. Cellebrite is the go-to tool provider for mobile forensics, offering broad support of mobile devices.
- *Velociraptor:* This is an open source tool designed for internal security teams to gather evidence across all endpoints. It can rapidly gather and store event logs from an organization's endpoints so security teams can examine them for suspicious activity.
- *Wireshark:* This is an open source tool for network analysis that has been in use for more than 20 years. It can show every network packet sent from and received by a device, enabling an investigator to break down the type of traffic, as well as its source and destination. It suits analyzing a potential data breach to see where the attacker is sending compromised data.
- *Volatility:* This is an advanced memory forensics framework designed for the analysis of volatile memory (RAM) from computers during digital investigations. It aids in the recovery of digital artifacts from memory dumps, providing insights into the runtime state of the system, which is crucial for understanding the actions and intentions of potential attackers.

Free tools like Autopsy and Sleuth Kit are excellent for basic investigations, while commercial suites offer more advanced features and support, but at a higher cost. When diving into the world of forensic and cybersecurity software, choosing the right tool can be daunting. The market is flooded with a plethora of options, each claiming superiority. These tools help investigators uncover digital evidence from computers, smartphones, and other devices to support investigations and legal proceedings.

DIGITAL FORENSICS FOR LAW ENFORCEMENT

With the advancement of technology and the Internet of things (IoT), billions of people are more connected now than ever. This interconnectedness is enabling criminals to use technology to commit crimes. Digital forensics professionals with a digital forensics background can assist law enforcement agencies and the private sector in tracking down these criminals. They are instrumental in addressing fraud and identity theft. One of their primary responsibilities is to communicate findings to prosecutors and other law enforcement professionals.

Criminals are using technology to commit their offenses and create new challenges for law enforcement agents, attorneys, judges, military, and security professionals. This development has led to the rise of digital forensics, which is essentially the uncovering and examination of evidence located on all things electronic with digital storage, including computers, cell phones, and networks. Digital forensics has become an important instrument in identifying and solving computer-based and computer-assisted crime. By leveraging digital forensics, the FBI successfully dismantled a ransomware network that targeted critical establishments, notably hospitals. The operation culminated in both apprehensions and the retrieval of hefty ransom sums, fortifying defenses against subsequent threats. Figure 5 shows an FBI's investigation [11].

APPLICATION OF DIGITAL FORENSICS FOR LAW ENFORCEMENT

Digital forensics plays an important role in numerous law enforcement settings. Common applications of digital forensics in law enforcement include the following [11,12]:

- *Criminal Investigations:* Cybercrime can have a devastating impact on organizations in the private and public sectors. Digital forensics professionals are trained in collecting digital evidence that can aid law enforcement professionals in bringing cybercriminals to justice. Digital forensics is commonly used in both criminal law and private investigation. Digital forensics becomes a crucial aspect of law enforcement agencies and businesses. Depending on the type of case, a digital investigator may or may be involved. Digital investigators are expected to be a Jack of all trades since they are held responsible for their entire investigation environment (storage, network, software, security, etc.). Evidence can be used as evidence in investigation and legal proceedings for data theft and network breaches. Computer crimes such as fraud, forgery or identity theft leave a trail of evidence that forensic investigation can uncover. Digital forensics investigation is not restricted to retrieve data merely from the computer, as laws are breached by the criminals. A digital forensic investigation commonly consists of 3 stages: acquisition or imaging of exhibits, analysis, and reporting. During the analysis phase, an investigator recovers evidence material using a number of different methodologies and tools. Figure 6 shows a criminal arrest [13].
- *Digital Evidence:* This features in just about every part of our personal and business lives. Digital evidence is any sort of data stored and collected from any electronic storage device. Digital evidence exploitation is a relatively new tool for law enforcement investigations. It is increasingly being used in legal proceedings due to the increase of IT based systems and IT supported processes. It can be retrieved from wireless networks and random-access memory. It is commonly associated with electronic crime, or e-crime, such as child pornography or credit card fraud. However, digital evidence is now used to prosecute all types of crimes, not just e-crime. Laws dealing with digital evidence are concerned with two issues: integrity and authenticity. Digital evidence should be acquired in a forensically sound manner.
- *Fraud and Identity Theft*: Digital forensics professionals are instrumental in addressing fraud and identity theft. They can recover deleted files stored on computers or digital devices that law enforcement agencies have seized. They can also obtain encrypted or hidden data. This ability makes digital forensics professionals adept in tracking the digital trail of suspected identity theft criminals and providing justice for the victims.
- *Terrorism:* Digital forensics plays a unique role in the fight against terrorism. Military professionals can use computer forensics to evaluate vulnerable systems and network infrastructure that terrorists may exploit. Digital forensics can also be used to locate vulnerabilities in computer networks and systems to prevent future cyberterrorist attacks.

BENEFITS

Computers are used for committing crime, and law enforcement also uses computers to fight crime. Digital forensics offers numerous benefits for law enforcement by providing powerful tools to investigate crimes, gather evidence, and ultimately solve cases more effectively. Law enforcement agencies, financial institutions, and investment firms are incorporating digital forensics into their infrastructure. Other benefits of digital forensics include the following [14,15]:

- *Tracking Cybercrimes:* It helps uncover how crimes like identity theft, fraud, or any other attack have occurred by tracing the evidence and identifying the attackers. Cybercriminals accidentally leave traces, like email records and computer files, that can be tracked. Digital forensics helps identify criminals by analyzing these traces.
- *Speed and Efficiency*: Digital forensics analysis provides faster results than traditional methods, which helps solve cases more quickly. Speed is especially important in cybercrime cases where time is critical.
- *Helping with Legal Cases*: It ensures that evidence is collected properly and is ready for use in court. Well-preserved digital evidence strengthens legal cases and supports law enforcement efforts.
- *Enhanced Crime Investigation:* Digital forensics helps uncover the methods and identify perpetrators of cybercrimes like fraud, identity theft, and hacking by analyzing digital traces left behind. Digital devices often hold crucial information about a crime, including communications, location data, and financial transactions, which can be used to link suspects to a crime scene or establish motive.
- *Building Stronger Cases:* Digital forensics ensures that evidence is collected, preserved, and analyzed according to legal standards, making it admissible in court. Well-preserved and analyzed digital evidence can significantly strengthen legal

cases and support law enforcement efforts in prosecutions.

- *Protecting Organizations and Individuals*: Digital forensics helps companies understand how data breaches occurred, allowing them to implement better security measures and prevent future incidents. By demonstrating a commitment to digital security, law enforcement and organizations can build trust with the public.
- *Leveraging Technology:* Artificial intelligence and machine learning tools are increasingly used to analyze large datasets, identify patterns, and speed up investigations. AI-powered tools can help visualize connections between individuals and their movements, aiding in the identification of suspects and dismantling criminal networks.

CHALLENGES

Compared with traditional forensic science, digital forensics poses significant challenges. Analyzing evidence stored on a digital computer is one of the greatest forensic challenges facing law enforcement. A personal right to privacy is one area of digital forensics which is still largely undecided by courts. There is a need for training professionals in forensics, and some companies have started to offer certification programs. Law enforcement agencies are compelled to train officers to collect digital evidence and keep up with rapidly evolving technologies. Other challenges facing digital forensic include the following [14,16]:

- *Ethical Challenges:* As with any field rooted in technology, there are several ethical challenges in image forensic investigations. Ethical challenges are complex and multifaceted, often requiring professionals to make difficult decisions. These challenges revolve around privacy, accuracy, misuse of evidence, and the potential for bias in interpreting results. Understanding the ethical dilemmas inherent in image forensics is essential for ensuring the field's integrity and maintaining trust in its findings. One of the most pressing ethical issues in image forensics is the invasion of privacy. Ensuring that forensic professionals are well-trained in ethical decision-making is essential for maintaining the integrity of the field.
- *Data Privacy*: Digital forensics carries inherent challenges tied to privacy and civil rights. Experts must respect privacy laws to avoid violating people's rights. They must ensure that personal information is handled properly and complies with legal rules. Misusing personal data can lead to serious legal problems and hurt the investigation.
- *Data Security*: Handling digital evidence in image forensics demands strict adherence to data security protocols. Any alteration or tampering with the data can compromise the investigation's credibility. Ethical investigators must follow chain-of-custody procedures to protect the integrity of digital images, ensuring that evidence remains untampered and can be verified at every stage.
- *Accuracy of Image Analysis*: Inaccuracies in image forensic investigations can lead to wrongful accusations and misinterpretations. Ethical challenges arise when the technology used to analyze images is not foolproof, leading to potential errors in determining the authenticity of images. Figure 7 shows a case where the accuracy of an image is being examined [16].
- *Bias in Interpretation:* Human bias in the interpretation of forensic images is a concern that can lead to skewed results. It can influence the interpretation of forensic evidence. Whether conscious or unconscious, biases related to race, gender, or social status can affect how forensic experts view and present their findings. Ethical image forensics requires a commitment to neutrality, where the evidence speaks for itself without the influence of personal prejudices. It is crucial for forensic professionals to maintain their independence and present evidence without bias, even if it contradicts the narrative of the side that hired them. This accountability ensures the integrity of the legal process.
- *Confidentiality in Investigations:* Digital forensic experts often work with sensitive, confidential information that can impact legal cases or personal lives. Maintaining confidentiality is essential, and breaches can lead to significant ethical violations. Forensic professionals and law enforcement agencies must ensure that their work is conducted discreetly, with careful attention to protecting the information they handle.
- *Too Much Data:* A lot of data is created and stored daily, making it hard to analyze. Experts have to review different types of data (files, photos, messages) from many devices, which takes time and effort.
- *Hiding Evidence:* Encryption protects data, but it makes it hard for experts to access important information without the right keys. Some people also use tools to hide or change evidence, making it harder to find the truth.
- *New Technologies:* As technology advances quickly, experts must stay updated with new tools

like AI, machine learning, blockchain, and improved encryption to tackle new forensic challenges.

- *Cross-Border Issues*: In a globalized world, image forensic investigations often involve cross-border elements, where laws regarding privacy, data protection, and evidence collection may vary. When digital evidence comes from different countries, determining which country's laws should apply can be challenging. This makes international investigations more complicated. Laws like the National Computer Crime Law, or similar international frameworks, help streamline these cases by setting legal standards for cooperation between countries, ensuring that digital evidence collected abroad complies with domestic legal procedures.

CONCLUSION

Digital forensics is the process of identifying, preserving, analyzing, and presenting digital pieces of evidence. It is a multidisciplinary and interdisciplinary field encompassing diverse disciplines such as criminology, law, ethics, computer engineering, information, and communication technology (ICT), computer science, and forensic science [19]. As technology advances exponentially, digital forensics professionals can use their expertise to help law enforcement agencies and prosecutors collect the necessary evidence to prosecute criminals.

As cybercrime evolves and digital devices become increasingly central to our lives, the role of digital forensics has grown exponentially. As law enforcement leaders continue to modernize their agencies, departments of all sizes are now regularly purchasing and using a wide variety of technology to assist them with solving crimes and keeping their communities safe. While specific requirements may vary by law enforcement organization, digital-forensics professionals should generally have at least a bachelor's degree in computer science, computer engineering, cybersecurity or a related field. More information about digital forensics for law enforcement can be found in the books in [17-32] and the following related journals:

- Digital Investigation
- Journal of Digital Forensics, Security and Law
- Journal of Digital Investigation
- Journal of Digital Forensic Practice
- Small Scale Digital Device Forensic Journal
- International Journal of Digital Evidence
- International Journal of Forensic Computer Science
- International Journal of Digital Evidence
- International Journal of Digital Crime and Forensics
- Forensic Science International: Digital Investigation

REFERENCES

[1] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Digital forensics," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 7, no. 4, April 2017, pp. 274-276.

[2] "Digital forensics," https://www.niiconsulting.com/services/breach-response/digital-forensics.php

[3] N. Kumari and A. K. Mohapatra, "An insight into digital forensics branches and tools," *Proceedings of the International Conference on Computational Techniques in Information and Communication Technologies*, 2016.

[4] "Digital forensics: What is it in 2021—2022?" January 2021, https://recfaces.com/articles/digital-forensics

[5] "Digital forensics overview in a nutshell!" Unknown Source.

[6] "How well do you know digital forensics?" https://www.eccouncil.org/what-is-digital-forensics/

[7] K. Khalil, "Digital forensic tools," https://www.linkedin.com/pulse/digital-forensic-tools-kareem-khalil

[8] P. G. Miguel, "Top 24 digital forensics software of 2025," March 2025, https://thectoclub.com/tools/best-digital-forensics-software/

[9] S. Lee, "Digital forensics in law enforcement," https://www.numberanalytics.com/blog/digital-forensics-in-law-enforcement

[10] R. Shapland, "5 digital forensics tools experts use in 2023," August 2023, https://www.techtarget.com/searchsecurity/tip/Digital-forensics-tools-experts-use

[11] "Digital forensics: Salary & career outlook," https://www.ucf.edu/online/criminal-justice/news/digital-forensics-salary/

[12] M. N. O. Sadiku, S. R. Nelatury, and S. M. Musa, "Digital evidence," *Journal of Scientific and Engineering Research*, vol. 7, no. 4, 2020, pp. 160-164.

[13] S. L. Garfinkel, "Digital forensics," https://www.americanscientist.org/article/digital-forensics

[14] P. Pavithran, "Digital forensics explained: Investigate & prevent cyber threats," January

2025, https://fidelissecurity.com/cybersecurity-101/learn/digital-forensics/

[15] I. Resendez, P. Martinez, and J. Abraham, "An introduction to digital forensics," June 2014, https://www.researchgate.net/publication/228864187_An_Introduction_to_Digital_Forensics

[16] "Ethical challenges in image forensic investigations," October 2024, https://eclipseforensics.com/ethical-challenges-in-image-forensic-investigations/

[17] M. N. O. Sadiku, S. M. Musa, and O. D. Olaleye, *Digital Everything: A Primer – Volume 2.* Moldova, Europe: Lambert Academic Publishing, Chapter 2, 2023.

[18] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. San Diego, CA: Academic Press, 3rd edition, 2011, chapter 1.

[19] G. Johansen, *Digital Forensics and Incident Response: A Practical Guide to Deploying Digital Forensic Techniques in Response to Cyber Security Incidents.* Packt Publishing, 2nd edition, 2020.

[20] E. Casey, *Handbook of Digital Forensics and Investigation*. Academic Press, 2009.

[21] N. A. Hassan, *Digital Forensics Basics: A Practical Guide Using Windows OS.* Springer 2019.

[22] L. K. Tsado and R. Osgodo, *Exploring Careers in Cybersecurity and Digital Forensics.* Rowman & Littlefield Publishers, 2022.

[23] J. Kavrestad, *Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications.* Springer International Publishing, 2020.

[24] K. P. Chow and S. Shenoi (eds.), *Advances in Digital Forensics VI.* Berlin: Springer, 2010.

[25] J. A. Lewis, *Computer and Digital Forensics Corporate and Law Enforcement Training System, Text Manual.* Cyber Defense Training Systems, LLC, 5th Edition, 2011.

[26] J. Brunty and K. Helenek, *Social Media Investigation for Law Enforcement.* Taylor & Francis, 2014.

[27] J. T. Luttgens and M. Pepe, *Incident Response & Computer Forensics.* New York: McGraw Hill Education, 3rd edition, 2014.

[28] C. Altheide and H. Carvey, *Digital Forensics With Open Source Tools*. Elsevier, 2011.

[29] A. Årnes (ed.), *Digital Forensics.* John Wiley & Sons, 2017.

[30] J. Sammons, *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics*. Elsevier, 2012.

[31] G. Gogolin (ed.), *Digital Forensics Explained.* Boca Raton, FL: CRC Press, 2nd edition, 2021.

[32] L. Daniel and L. Daniel, *Digital Forensics for Legal Professionals: Understanding Digital Evidence from the Warrant to the Courtroom.* Syngress, 2011.

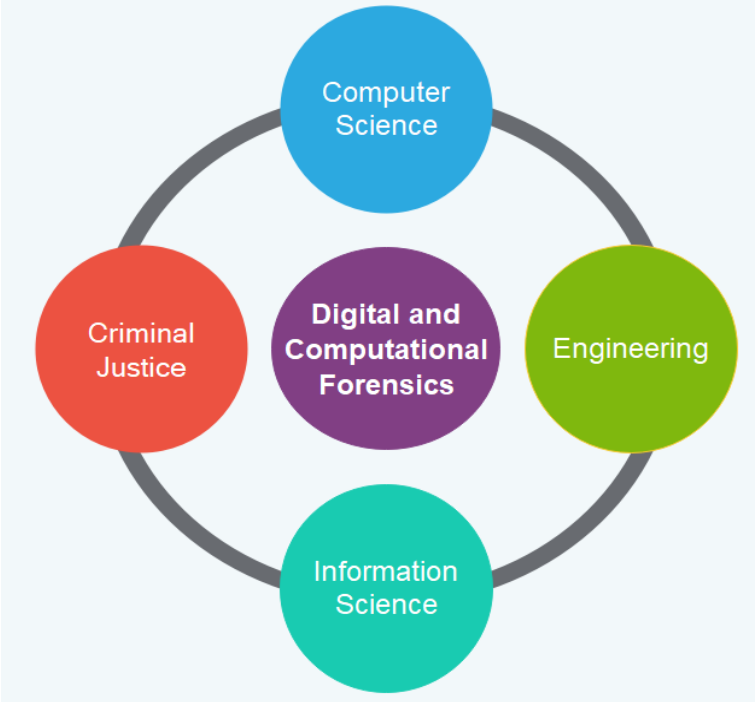

Figure 1 Multiple domains of digital forensics.

Figure 2 Branches of digital forensics.

Figure 3 The key processes in digital forensics.

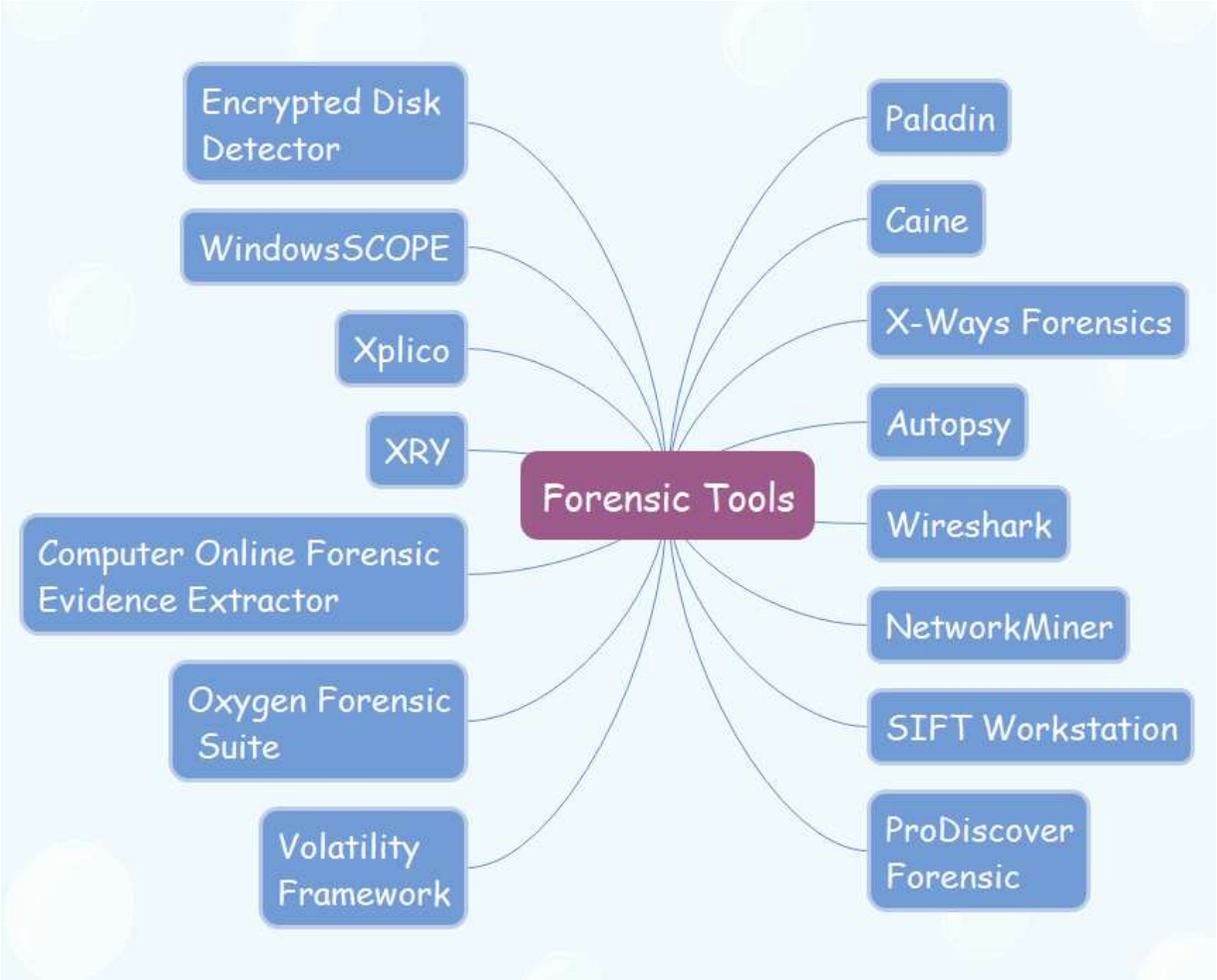

Figure 4 Some forensics tools.

Figure 5 FBI's investigation [11].

Figure 6 A criminal arrest [13].

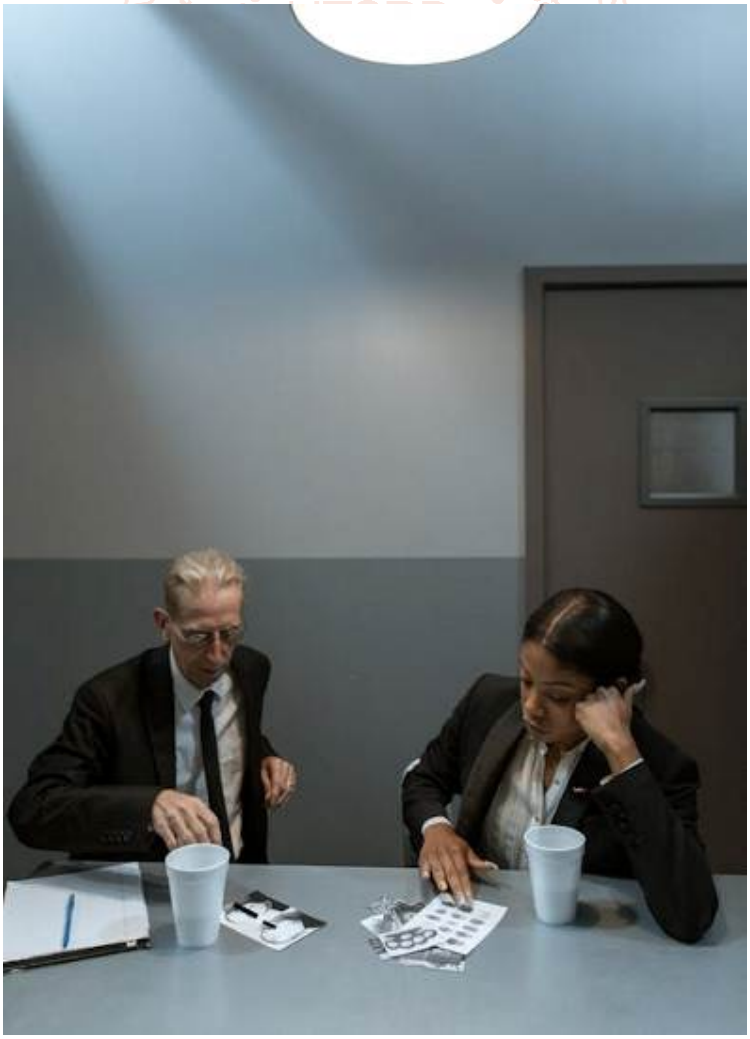

Figure 7 The accuracy of an image is being examined [16].