HSPI The Open Access Publisher

J F S R JOURNAL OF FORENSIC SCIENCE AND RESEARCH
ISSN 2575-0186

Prospective Study

Digital Forensics and Media Offences – Investigate Synergy in the Cyber Age

Gauri Goyal*

Amity University, India

Abstract

In the digital age, media offenses pose significant threats to privacy and reputation. Digital forensics plays a crucial role in combating these crimes by providing systematic methods and valuable knowledge. This work reviews how the field has proven effective in solving cases and preventing offenses, offering a solid career path for those interested in crime-solving and digital evidence collection.

More Information

***Address for correspondence:** Gauri Goyal, Amity University, India, Email: gaurigoyal803@gmail.com

Submitted: February 25, 2025
Approved: March 05, 2025
Published: March 06, 2025

How to cite this article: Goyal G. Digital Forensics and Media Offences – Investigate Synergy in the Cyber Age. J Forensic Sci Res. 2025; 9(1): 015-020. Available from: https://dx.doi.org/10.29328/journal.jfsr.1001074

Copyright license: © 2025 Goyal G. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Keywords: Media offenses; Privacy disruption; Digital forensics; Social media

Check for updates

OPEN ACCESS

Introduction

It has been reported that" digital forensics is the key to working cybercrimes and guarding digital data." In a day where digital geography functions as both a playground and a battlefield, the relationship between media offenses and digital forensics has surfaced as a pivotal concern for investigators worldwide. Technology has advanced at a rate that has not been seen before, and with it, so too have the ways thieves use to benefit from these advances. The number and complexity of media offenses have increased; they now include cyberbullying, online abuse, and sophisticated hacking as well as intellectual property theft. Because of this, learning about digital forensics has become more pivotal for tracking down digital substantiation, examining cybercrimes, and catching their malefactors. Since its inception, forensic science has advanced much beyond blood typing and fingerprint analysis. The recording of DNA in criminal investigations has played a very game-changing part in the investigation. It has made it easier for the experts to solve the crime and to know about the leads of the suspect. The experts now use many tools to know the crime's timeline. The experts use the help of digital forensics for solving the crime as it has mechanisms that can detect how the crime happened or what the sources included in the crime very easily. So the experts use evidence collection, an autopsy of the body, or any media offence that happened.

About digital forensics

“Digital forensics is a branch of forensic science that focuses on identifying, acquiring, processing, analysing, and reporting on data stored electronically. Electronic evidence is a component of almost all criminal activities, and digital forensics support is crucial for law enforcement investigations” [1]. Digital forensics can also be used in civil investigations. For example, law enforcement authorities might employ digital forensics to examine data from a murder suspect's devices, while cyber security experts might use it to find the cybercriminals responsible for a malware attack. Because it handles digital evidence like any other type of evidence, digital forensics has many uses. To prevent tampering, digital forensics investigators handle digital evidence according to a stringent forensics procedure, also called a chain of custody, just as authorities follow particular procedures to collect tangible evidence from a crime scene. It's common to refer to computer forensics and digital forensics interchangeably. In contrast to computer forensics, which focuses on obtaining evidence exclusively from computing devices including computers, tablets, smartphones, and other gadgets having a CPU, digital forensics technically collects data from any digital device. “Digital Forensics and Incident Response (DFIR) is an emerging cybersecurity discipline that integrates computer forensics and incident response activities to accelerate the remediation of cyber threats while ensuring that any related digital evidence is not compromised” [2]. Now a deeper analysis will be done as to why digital forensics is an important aspect.

In a world where technology is taking over, digital forensics has become an invaluable field in the current era, aiding in investigating and resolving crimes. The nature of crime has changed significantly due to the widespread use of digital devices and the internet, rendering conventional investigative techniques inadequate on their own. Justice can be served in

an increasingly complicated digital world thanks to the tools and procedures that digital forensics fills in to find, examine, and present digital evidence in a legally admissible way.

The use of digital forensics in cybercrime is one of the important factors that contribute to preventing cybercrime, such as online theft, hacking an account, phishing, and trolling, which has grown globally and emerged as a strong thing around the world, due to which many people are facing mental health problems. This crime is also impacting the government and many MNCs, which is very threatening. So to curb these crimes, digital forensics offers many new techniques and tools to solve these crimes, because it helps in detecting harmful software. Digital devices frequently contain crucial evidence that might prove motives, disprove alibis, or show intent. Text messages, emails, and exchanges on social media, for example, can reveal information about the ties and exchanges between victims and suspects. Reconstructing events and timelines are made easier by the ability to place people at certain locations at particular times using location data from mobile devices. Digital forensics can reveal intricate strategies in financial fraud cases by examining electronically stored financial data and transaction logs. Digital forensics includes criminal cases, which makes it easy to solve the cases because the stored data helps in the collection of evidence. In this subject case, there is a very well-known one known as the BTK killer [3], in which the killer killed ten people and was on the loose, and police were not able to find the killer. But once the killer had sent the cryptic note in a word, digital forensics were able to catch him through his floppy disk. Here, without the intention to be controversial, a case is presented in which digital forensics was used. The case was about Sunanda Pushkar [4], the wife of famous politician Shashi Tharoor. Sunanda, being murdered. Some say that she was murdered by his husband, but some suspect it was a suicide. Later, reports said the death was unnatural and might be due to a drug overdose. The later doctor who conducted the autopsy reported that it came out to be a fault, and the next autopsy said that it was due to poisoning. But in May 2018 Shashi Tharoor was charged with abetment, suicide of his wife, and marital cruelty. In August 2018, a special court in Delhi discharged Tharor from all the charges for Pushkar's death. Furthermore, discussing the significance of digital forensics and conducting further in-depth studies will allow all to apply their understanding to consider how these cases may have contributed to the resolution of other cases. The case was explained on many news where the experts have said that the death of Mrs. Tharor was an unnatural one. The autopsy showed that she had 15 bruises on her body.

Why is digital forensics important?

"Most people believe that digital forensics exclusively applies to digital and computing contexts. However, its impact on society is far more extensive. Due to the widespread use of computers and other electronic devices in daily life, digital evidence is now essential for resolving a wide range of criminal and court cases, both online and offline.

All linked devices generate massive volumes of data. Numerous gadgets record everything that their users do in addition to the autonomous tasks that they carry out, like network connections and data transfers. This covers a wide range of both public and private electronics, such as traffic lights, automobiles, cell phones, routers, and personal computers.

In an inquiry or legal procedure, digital evidence may be used to support the following claims:

Digital forensics is used in data theft and network breaches to identify the perpetrators and the circumstances surrounding the incident. It is used to analyse the effects of a breach on businesses and their clients, including identity theft and online fraud, and to gather digital evidence from smartphones, automobiles, and other devices near the scene of violent crimes like burglaries, assaults, and murders. It is also utilised to investigate and collect evidence related to white-collar crimes, such as corporate fraud, embezzlement, and extortion. It can be utilised within a company to locate and look into physical security incidents as well as cybersecurity incidents. The most frequently utilised in incident response procedures to help find and confirm breaches, pinpoint threat actors and their origins, neutralise threats, and supply proof to legal teams and law enforcement. It is possible to identify a crime's perpetrators using digital forensics. Finding the source of a leak, tracking down the origin of a cyberattack, and connecting a suspect to a crime scene are all made easier with its assistance. This aids in the investigations of law enforcement organisations and helps convicts face justice.

The example provided here is the Aarushi Talwar-Hemraj double murder case [5], where digital forensics helped in tracing the electronic evidence. The detectives were able to examine the interactions that happened between the victim and the possible suspects through mobile phones, computers, emails, and mobile phone records. The investigator was able to discover the footprint, which also provided information on the victim's activities and possible suspects. As one can also see in the example, digital forensics has played an important part in catching the possible suspect and it also helped in framing the timelines of the event in solving the crime cases in the case of the Bikni killer (Charles Sobhraj) [6] digital forensics has helped in solving the case by investigating the call records and tickets and tracing the evidence by doing forensics techniques on dead bodies. By looking into instances of copyright infringement, trade secret theft, and unlawful access to private information, digital forensics helps to defend intellectual property rights. Forensics experts can track out the source of information leaks, apprehend those responsible, and produce proof for court cases. This guarantees the protection of innovators' and creators' rights in the digital sphere.

Therefore, organizations must centrally manage logs and other digital evidence, ensure they keep it for a sufficient amount of time, and safeguard it against alteration, unauthorized access, or unintentional loss to enable digital forensics.

Branches of digital forensics

Computer forensics: The use of investigation and analytical methods to collect and preserve data from a specific computing device so that it can be presented in court is known as computer forensics. Computer forensics aims to precisely determine what occurred on a computer device and who was responsible for it by conducting a systematic investigation and keeping a recorded chain of evidence [7]. A crucial component of contemporary investigations may involve computer forensics. One of the more popular locations to search for hints after a crime is committed and an inquiry is launched is the suspect's computer or mobile phone. A specialist in computer forensics can help in this situation. For example, if the police want to trace the location of the burglar or any person who has committed the crime, the computer forensics specialist can help in tracing the location or last location of the SIM used by that person.

In essence, computer forensics—also known as cyber forensics, computer forensic science, or digital forensics—is data recovery combined with legal compliance rules to allow the material to be admitted in court. A mention is to be made of a very famous example in which computer forensics has been used for the detection of fraudulent practices. In the Nirav Modi case [8], the culprit was arrested in London, and his bail plea was refused. Computer forensics has helped in tracing the bank details and statements of Nirav Modi, from which they can know that he is doing a scam.

Mobile device forensics: A branch of digital forensics called mobile device forensics, or mobile forensics, focuses on forensically sound information extraction from mobile devices, like tablets and smartphones. Mobile device forensics can retrieve deleted files, call logs, text messages, application data, GPS data, pictures, and videos, among other types of data [9].

Similar to other forensics fields, evidence recovery for criminal investigations is a common use for mobile device forensics. Because of this, mobile device forensic investigators need to be careful to gather and examine information that is acceptable as evidence under the law.

Network forensics: A subset of digital forensics known as "network forensics" is primarily concerned with examining networks and the traffic that passes through them when it is suspected that the network is engaged in malicious activity. Examples of such networks include those that spread malware to steal credentials or analyze cyber-attacks. With the growth and popularity of network-based services like email and the World Wide Web, cybercrimes and their importance increased in tandem with the expansion of the Internet.

Forensic data analysis

To find evidence and insights relevant to legal or financial investigations, forensic data analysis, or FDA, is a methodical procedure that involves investigating, analyzing, and interpreting complicated data sets. Using sophisticated analytical tools and methodologies, this procedure looks for trends, abnormalities, and correlations in the data that can point to financial irregularities, fraudulent activity, or other unlawful actions. It focuses on the extraction, analysis, and presentation of evidence from phones, computers, and networks. The example presented here is about the Sushant Singh Rajput case [10]. Was it murder, or did he commit suicide? Forensic data analysis helped the branch trace the evidence; it also helped in tracing potential leads through call logs, chats, computers, and emails. Social media also helped in tracing the inside connection, intention, and motive of this act.

Database forensics

Examining database access and documenting modifications to the data are the tasks of database forensics. Database forensics is useful for several things. Database forensics, for instance, can be used to find database transactions that point to fraud. Databases are used to store vast amounts of important data in the current digital era, such as financial records, consumer information, intellectual property, and more. As a result, hackers frequently target these databases in an attempt to obtain unauthorized access, steal confidential data, or alter data for illegal ends. Here is the example of the case of the accused, Larry Thomas [11], who committed murder. His bracelet picture on Facebook helped in identifying that he was the killer, but later on, the picture was deleted on purpose a long time ago. In simple sentences, database forensics helps in keeping a record of the data of everything, and it also keeps sensitive information. It also keeps a record of who has access to that information, who can log in, and who cannot. The forensics experts use database forensics to know the motive and method of the crime. There was a case where the criminal came into custody due to the evidence collected through database forensics, in which the expert discovered in the suspect's computer the pill that he used to kill his wife.

About media offenses

Media offenses are focused on in this section, and later the detailed analysis of the relationship between digital forensics and media offenses is discussed with the help of case studies.

The term "media offenses" describes illicit and criminal behaviours that exploit the internet, communication technology, and digital media platforms. These offenses cover a broad spectrum of actions that involve the improper use of digital means to cause harm to people, groups, or society as a whole. The extent and impact of media offenses have

increased as technology has become more pervasive in daily life. For this reason, it is critical to comprehend the nature, ramifications, and strategies employed to prevent media offences. Our Indian Constitution contains a separate article, 19, to avoid these things from happening as previously noted. Protection of specific rights about freedom of speech, etc. Article 19(A) states that one has the right to freedom of speech and expression, but it does not give oneself the freedom to offend people or do actions that are against the law. When one commits crimes, one violates the privacy and dignity of others. As stated by Stephane Nappo, it takes 20 years to build. A reputation and a few minutes of cyber-incident to ruin it. These offenses include a wide range of actions, such as cyberbullying, defamation, obscenity, hate speech, copyright infringement, privacy violations, fraudulent advertising, and contempt of court. This thorough investigation will examine every kind of offense, consider its ramifications, and evaluate the legal systems that deal with it.

Types of media offences

Defamation: Disseminating false information that damages the reputation of a person or organization is known as defamation. It falls into two categories: slander (spoken) and defamation, and libel(written defamation). It can be seen that by making false statements about the person, publications such as newspapers, television, and social media may unintentionally or deliberately disseminate libelous content. In defamation lawsuits, it is frequently necessary to demonstrate that the remarks were untrue, harmful, and partially incorrect. Social media's explosive growth in defamation cases has made stronger legal frameworks necessary to shield people and organizations from damage to their reputations.

For example, people in the cinema can be made to make false comments about other actors, and for the protection of their reputation, the other person files a defamation lawsuit against that person. The most recent example is of Poonam Pandey, who pulled up a stunt of fake death in which one person filed a defamation claim because that person thought that she was making fun of that disease. When linking defamation and forensics, a discussion follows about how defamation cases can sometimes distract people by making false accusations against an innocent person, and then the main culprit can walk freely, but with the help of forensics, the main culprit can face repercussions. Forensics can help in analysing the crime scene, obtaining the DNA and footprints, and also verify the validity of the suspect. There was a series where this kind of case was shown. The series name was Criminal Justice: Adhura Sach in which the accused has to face many false accusations and manipulations because of the crime he has committed. The media has also defamed him, and the real culprit was not harmed in this, but later it was shown that forensics had helped in the crime scene and evidence collection when the case was reopened, and due to this, the false accused was announced as a free man and the real culprit was able to be found. Even this kind of thing can be used as a role reversal for revenge. The movie article 375 shows the power of this.

Hate speech

Hate speech means making public speech that can cause violence toward a person or a group of people including any kind of (race, caste, sect, gender). If talking about the relationship between hate speech and forensics, then a discussion follows on pattern recognition, which is connected to forensics. For example, if the crime was committed due to any kind of hate speech, then the investigator will be keen to find out about the criminal, so he/she will see the video and analyze the video, and then he/she will see if there is any exchange of numbers, passwords, or any words that motivated that person to do this crime. Additionally, any kind of illegal deal happened between them so the expert will analyze and do deep research on it. The prime case example is the 2017 murder of journalist Gauri Lankesh [12], where she was murdered due to her outspoken views, which the person had taken as hate speech, and the forensics examined her online activity case of her and also discovered the suspect's digital footprints, which has led them to solving the crime.

Obscenity

Obscenity means the character that is indecent, vulgar, or inappropriate as per society or any act which does not support the morality of the society present [13]. One interesting example is the song “Real Slim Shady” by Eminem, which faced a problem because, due to the broadcast rules, these songs contain some obscene lines and words that have to be banned, but they did not. So eventually, the FCC (Federal Communications Commission), dropped the fine. In the new order, issued on January 7th by David H. Solomon, Chief of the FCC’s Enforcement Bureau, the commission said that the edited version of the song still contained sexual references but that they were too oblique to fall under the FCC’s Indecency Policy guidelines. “We disagree with our initial analysis, and we now conclude that the material at issue was not patently offensive under contemporary community standards for the broadcast medium,” Solomon wrote. “Accordingly, we conclude that the licensee did not violate the applicable statute or our indecency rule and that no sanction is warranted.” When discussing obscenity in forensics, then it can start with the evidence collection. Supposedly, a crime happened because someone's picture or video went viral, which was obscene and didn't fall under the category of normal videos. So here, the forensics team will recover the mobile and check from where the video was sent, what was the IP address of the sender, and lastly, what was the motivation for this crime. After gathering the information, the video will be deleted from everywhere. A hypothetical example is of a victim who has shot an obscene video, and after seeing the video, the guy committed her murder, and he shot the video in an isolated location. No one

knows about the location, so the forensics team will trace the location and will be able to capture the criminal.

The interconnection between digital forensics and media offences

Digital forensics and media offences have a complex link that involves the use of forensic tools to look into and handle illicit behaviors in media material. Digital forensics is used in media offences. When it comes to gathering and maintaining evidence about media offences, digital forensics is essential. Forensic specialists, for example, can recover deleted messages, emails, social media posts, and other digital communications that are relevant to accusations of defamation or cyberbullying. Ensuring the genuineness and integrity of this evidence is essential for court cases. Evidence collection and preservation mostly help in criminal cases when the autopsy of the body happens, so it helps in detecting the bite marks and hair. This kind of evidence has been traced and preserved. So later on, it can be used as a main source of evidence.

As a branch of computer forensics, media forensics is concerned with confirming the legitimacy of multimedia files, including pictures, videos, and audio recordings. This is especially crucial when it comes to defamation, hate speech, and privacy concerns, as manipulated or fake media can be used to hurt or deceive people. The uniqueness and reliability of the media are established with the aid of methods like audio waveform analysis, pixel inspection, and metadata analysis.

Discovering the sources of media offences requires the application of digital forensics tools. For instance, forensic specialists can examine network logs, IP addresses, and digital fingerprints in copyright infringement cases to determine the origin of illicit distribution. Similar to this, forensic analysis can assist in identifying the networks and tracing the offenders in instances of hate speech or national security breaches. To combat media offences, law enforcement organizations and cybersecurity experts rely heavily on the assistance of digital forensics. Experts in digital evidence analysis and criminal behavior patterns help to prevent and lessen cybercrimes by evaluating digital evidence. This cooperative strategy improves the overall efficacy of cybersecurity and legal measures. Digital forensics can also help in tracking the media offence and spreading misinformation. These two can make a great team in curbing the crimes and offences that happen in the whole world. Digital forensics also helped in the protection of tampering of evidence, as they have tightened their security and passwords. The file where everything has been recorded including autopsy and legal data. With the help of interconnection, the expert can help in restructuring the timeline of the event in which a crime has taken place, as this will make it easier to solve the crime. At the time of legal proceedings, all the evidence that was collected by the forensics expert will be admissible in court. Sometimes forensics experts were used to call in court to provide their testimony as witnesses, and then they explained the techniques and everything about how they gathered the evidence.

Conclusion

In this online age or digital age, media offenses have become a very important issue that disrupts the privacy of the people and also takes advantage of the people's reputation and their character. So to prevent this from happening to a person digital forensics plays a crucial part in solving this. It offers a very wide and very systematic structure to prevent this crime and it also offers knowledge about digital technology. After reviewing so many examples and real-life case laws about how digital forensics has helped in solving cases and how it has helped in detecting media offences, experts have been instrumental in solving and applying the methods to solve the crime. From the author's perspective, this can be a very solid career one can pursue. If one has an interest in solving the murder case and one has to know about how digital forensics works and how the testing, evidence collection happen. It can also be seen after reading the chapter how much these two topics are connected and help each other in solving crimes such as the blue whale challenge, which let children and adults commit suicide. Here, what is seen is the connection between the two that has led to solving and banning the game by spreading awareness through the media, the game was a media offence too as it was forcing people to take their own lives by controlling their minds. This has also resulted in the establishment of stringent guidelines and policies regarding how individuals should use social media. Raising awareness of these issues has improved society.

References

1. Digital forensics [Internet]. Available from: https://www.interpol.int/en/How-we-work/Innovation/Digital-forensics
2. IBM, Badman A. Digital forensics [Internet]. Forrest A, editor. What is digital forensics? 2024. Available from: https://www.ibm.com/topics/digital-forensics
3. Computer disk may have cracked BTK case [Internet]. NBC News. 2005. Available from: https://www.nbcnews.com/id/wbna6988048
4. Khan A. Sunanda death case: Autopsy shows 15 bruises on her body. The Times of India [Internet]. 2019. Available from: https://timesofindia.indiatimes.com/city/delhi/sunanda-death-case-autopsy-shows-15-bruises-on-her-body/articleshow/70761854.cms
5. Seo. The Power of Mobile Device Forensics: Investigating Digital Footprints in 2024 [Internet]. Karnavati University. 2024. Available from: https://karnavatiuniversity.edu.in/the-power-of-mobile-device-forensics-investigating-digital-footprints-in-2024/
6. Hollingsworth J, Renton A. From diplomat to detective, this man helped bring Asia's notorious 'Serpent' killer to justice [Internet]. Cable News Network (CNN). 2021. Available from: https://edition.cnn.com/2021/03/13/asia/serpent-bikini-killer-sobhraj-intl-hnk-dst/index.html
7. Awati R, Lutkevich B. Computer forensics (cyber forensics) [Internet]. Search Security. 2024. Available from: https://www.techtarget.com/searchsecurity/definition/computer-forensics
8. The PNB Fraud Case Study: Forensic Accounting and Risk Management Perspective - Hunarho [Internet]. Hunarho. 2024. Available from: https://hunarho.com/blog/the-pnb-fraud-case-study/

9. Jayaraman N. Mobile device forensics in the evolving world of electronics [Internet]. Cybersecurity Exchange. 2023. Available from: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/mobile-device-forensics/

10. Ians. India TO. Sushant Singh Rajput case: Forensic re-examination hints at discrepancies. The Times of India [Internet]. 2020. Available from: https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/sushant-singh-%20%20rajput-case-forensic-re-examination-hints-at-discrepancies/articleshow/78173036.cms

11. EclipseForensics. 3 Famous cases solved through digital forensics - Eclipse Forensics [Internet]. Eclipse Forensics. 2024. Available from: https://eclipseforensics.com/3-famous-cases-solved-through-digital-forensics/

12. The killing of Gauri Lankesh [Internet]. Columbia Journalism Review. Available from: https://www.cjr.org/special_report/gauri-lankesh-killing.php

13. Media and Obscenity. Legal Service India - Law articles - Legal resources [Internet]. Available from: https://www.legalserviceindia.com/legal/article-7096-media-and-obscenity.html#google_vignette