Research Paper Final

Charles Oddo

Kent State University

IT-36318-340: Survey of Information Security, Internet Fraud, and Computer Forensics

Shawn Golden, Ph.D.

7/8/2026

Abstract

Digital evidence has become an important part of today's criminal investigations. It has reshaped how suspects are identified, how events are reconstructed, and how information is presented in a court of law. This paper will examine the evolution, significance, and the application of digital evidence in a criminal investigative environment. Drawing on established literature and recent research, it will explore various types of digital evidence commonly encountered including computers, mobile or handheld devices, cloud data, and Internet of Things (IoT) sources. It will analyze both technical and procedural requirements for proper evidence collection, preservation, and authentication. This research paper will also evaluate legal and ethical challenges, including privacy concerns, court admissibility standards, and challenges presented by encryption and jurisdiction complexities. Additionally, it will highlight emerging investigative technologies and the ever-growing reliance on digital investigative tools by major law enforcement agencies. This paper demonstrates that digital evidence is indispensable to effective criminal investigations; however, the value of the evidence depends on the use of acceptable forensic methodology, adhering to legal standards, and adapting to rapidly changing technologies.

The Role of Digital Evidence in Criminal Investigations

According to Avala Chaitanya digital evidence, a foundational component in modern criminal investigations, is transforming how crimes are committed, detected, investigated, and prosecuted with the exponential growth of technology (Chaitanya, 2024). Its effectiveness greatly depends on proper collection, preservation, interpretation, and ethical use; thus, requiring investigators to balance technological capabilities with legal and procedural safeguards (Major Cities Cheifs Association, 2024). Eoghan Casey defines digital evidence as “any data stored or transmitted using a computer [or digital device] that support or refute a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi” (Casey, 2011, p. 7). Casey’s definition focused on computers, but modern investigations rely on a much broader range of digital devices.

The rapid expansion of digital devices—computers, smartphones, cloud platforms, surveillance cameras, and Internet of Things (IoT) devices—has reshaped investigative practices (Singla, 2025). Digital evidence is available in nearly every type of criminal case, from fraud and cybercrime to homicide and missing persons (Casey, 2011).

For example, the disappearance of Nancy Guthrie from her home in Tucson, Arizona, on January 31, 2026. The U.S. Federal Bureau of Investigation (FBI) was able to obtain video footage captured by a Google Nest doorbell camera that depicted an individual armed with a handgun wearing black gloves, ski mask, coat, and a backpack approached the door and attempted to block the camera’s view (Federal Bureau of Investigation, 2026). Despite the lack of subscription to retain the camera footage, small

portions of the footage were able to be recovered from the cloud servers (Federal Bureau of Investigation, 2026).

As digital systems have become embedded in nearly every aspect of daily life, the nature of criminal activity has evolved right alongside them. Traditional investigative methods—interviews, physical evidence, eyewitness statements—remain important; however, they often only provide minor details of the events (Casey, 2011). Digital evidence offers precise timestamps, geolocation data, communication records, and patterns that can reveal what happened (Casey, 2011). The volume of digital interactions generated daily provides investigators with important clues that can help to narrow down the scope of the investigation (Rakha, 2024). This shift has changed expectations for modern investigations, making forensic competence an essential skill for law enforcement (Major Cities Cheifs Association, 2024).

Digital forensics emerged in the later part of the 20th century as computers were increasingly being used for business and personal use (Pollitt, 2010). Mark Pollitt identifies the earliest investigations as “much of the focus was on recovering data from standalone computers. Data recovery was a major issue because storage was costly and users routinely deleted data and re-formatted media” (Pollitt, 2010, p. 6). Pollitt also explains that many of the early investigations were tools created or modified by the investigators “The tools used by the pioneering investigators included home-grown, command line tools and commercial products adapted to forensic use” (Pollitt, 2010, p. 7). Today, digital forensics encompasses a wide range of data sources and requires specialized tools and methodologies (Rakha, 2024).

The evolution of digital forensics accelerated in the early 2000s as cybercrime expanded and personal computers became more sophisticated (Pollitt, 2010). Law enforcement agencies began forming specialized digital forensic units and standardized investigative procedures (Pollitt, 2010). Marie-Helen Maras refers to the BTK killer case "The identity of the BTK killer (Dennis Rader) was also revealed by embedded metadata in a deleted Word document included on a floppy disk that the suspect had sent to a TV station. Specifically, this information enabled law enforcement agents to trace the document back to a church to which Dennis Rader belonged" (Maras, 2014, p. 200). This case highlights how digital artifacts can reveal critical information (Maras, 2014).

Digital evidence can originate from numerous sources, each of which provides unique insight and, in many cases, they may overlap, allowing an investigator to verify the information via multiple sources (Major Cities Cheifs Association, 2024). Computer artifacts can be system logs, registry entries, deleted files, browser history and application data (Jakobsen, 2024). Modern mobile devices or smartphones can produce much of the same along with call logs, text messages, GPS data, app usage, photos, and cloud backups (Jakobsen, 2024). Cloud data can include email, shared documents, account activity, and remote storage (Jakobsen, 2024). Network traffic includes IP logs, packet captures, firewall records, and intrusion detection alerts (Jakobsen, 2024). Social media could include posts, messages, metadata, geolocation tags, and account interactions (Jakobsen, 2024). IoT devices can include smart home sensors, doorbell or smart home cameras, vehicle telematics, and wearable devices (McClaran, 2021).

Nathan McClaran states that fitness trackers often record location data and can provide accurate time of death determinations (McClaran, 2021). A recent case on

February 22, 2024, in Athens, Georgia, Laken Riley went on a morning run through a wooded area when she was attacked and brutally murdered by being beaten in the head with a rock (Jones, 2024). The FBI was able to obtain GPS data from Laken's cell phone and data from a Garmin smartwatch she was wearing to pinpoint when she was attacked and subsequently murdered (Jones, 2024). The smartwatch was able to identify Laken's speed during the run, when she was stopped, and her heart rate before, during, and after the attack (Jones, 2024). The FBI was also able to obtain video footage from the surrounding areas and video Laken recorded on her smartphone of the suspect running behind her (Jones, 2024). FBI Special Agent James Burnie testified in court that the suspect, José Antonio Ibarra's cellphone data, put his location in the same area at the time of the attack (Jones, 2024). This case is a prime example showing how digital evidence including IoT device evidence can provide investigators with a precise timeline making them invaluable for reconstructing events and pinpointing locations (McClaran, 2021).

According to Naeem Allah Rakha proper collection and preservation of evidence is essential to maintaining the integrity and admissibility of digital evidence (Rakha, 2024). Mishandling the evidence could alter or destroy the data, compromising its value. It is essential to maintain clear documentation of everyone who has come into contact with the evidence from when the investigation begins until well after the court case has concluded (Rakha, 2024). This is the chain of custody where every contact with the evidence acts like a link in a chain. If one link is missing the chain is broken. Eoghan Casey stresses "without a solid chain of custody, it could be argued that the evidence

was handled improperly and may have been altered, replaced with incriminating evidence, or contaminated in some other fashion" (Casey, 2011, p. 22).

The defense in a court case will make every attempt to have incriminating evidence excluded from the hearing, while the evidence could clearly prove a defendant's guilt, if it is not properly collected, documented, and maintained it may not have any value in the case (Casey, 2011).

It is essential when working with digital evidence the investigator does not accidentally alter the evidence, altering the evidence could be as little as pressing a single key on the keyboard causing the computer to write information to the drive, altering data and potentially overwriting crucial evidence (Casey, 2011). Therefore, prior to performing any investigations on digital evidence, the investigator must create a forensic image of the device (Casey, 2011). A forensic image is a bit-by-bit copy that could include deleted information that has not been overwritten by the device (Jakobsen, 2024). Once the forensic image is created, the National Institute of Standards and Technology (NIST) indicates "It is best practice to hash digital images and other objects using a NIST approved hashing algorithm and the resulting hashes should be stored separately from the image or file in a secure location" (Guttman, White, & Walraven, 2022). NIST recommends using newer hashing algorithms with SHA-256 being the most commonly used; however, they state it is acceptable to use older hashing algorithms such as MD5 or SHA-1 if necessary (Guttman, White, & Walraven, 2022). They also recommend saving more than a single copy of the digital file (Guttman, White, & Walraven, 2022). Creating the forensic copy allows investigators

to analyze the data without risking contamination of the original evidence (Jakobsen, 2024).

Another important aspect of digital evidence that needs to be collected quickly is volatile data (Scientific Working Group on Digital Evidence, 2020). Volatile data is cleared away when a computer or device is turned off, as such it is imperative to collect this data from a running system (Scientific Working Group on Digital Evidence, 2020). Dr. Princy Singla states “Memory forensics is another critical method, enabling the retrieval of volatile data, such as encryption keys and running processes, from a system's RAM before it is lost upon shutdown” (Singla, 2025). Understanding what processes were running and access to potential encryption keys can give investigators a head start when investigating a drive.

According to Adam Tilmar Jakobsen, special considerations need to be given in order to preserve evidence when transporting and storing digital evidence as there are a number of elements that could damage, hinder or erase the evidence (Jakobsen, 2024). High temperature and humidity can decrease the lifespan of media, powerful magnets like those on the back of audio speakers could erase or damage magnetic media (Jakobsen, 2024). It is possible that radio signals or remote access to devices could allow evidence to be altered or a device to be factory reset (Maras, 2014). The Scientific Working Group on Digital Evidence recommends “Examiners should manually confirm network connectivity has been disabled or consider alternate means of isolation, including placing the device in an RF shielded enclosure, or utilizing a Cellular Network Isolation Card (CNIC) for GSM phones” (Scientific Working Group on Digital Evidence, 2020, p. 13). They mention historically the device was placed in “airplane mode”

however, modern devices may not disable Bluetooth and Wi-Fi allowing the device to be compromised (Scientific Working Group on Digital Evidence, 2020).

Digital investigations operate within a complex ethical and legal framework. Richard Spinello emphasizes that “The law is one of the most important forces that regulate behavior in cyberspace” (Spinello, 2021, p. 5). This underscores the need for investigators to balance investigative goals with the legal protections that safeguard civil liberties. The United States Fourth Amendment protects everyone in the United States from unreasonable searches and seizures performed by or on behalf of the government. Jacobus Gerhardus J. Nortje states “the more a search intrudes on the “inner sanctum” of persons, such as their homes, the more the search infringes on their rights and the investigators can intrude where the expectations of privacy are very high– this is specifically so with computers and mobile phones” (Nortje, 2023, p. 811). As such, searches of digital devices require search warrants specifying the scope of the search within which investigators must operate, if during the investigation, evidence is discovered of an additional crime, investigators will need to obtain a separate search warrant to expand the scope of the search to include the additional crime (Maras, 2014). Courts have ruled that digital searches must be narrowly tailored due to the vast amount of personal information stored on devices (Maras, 2014). The plain view doctrine allows investigators to seize evidence found in plain view during a lawful search however, courts have limited its application to digital evidence because opening files or applications may exceed the scope of the warrant (Maras, 2014).

Digital investigation tools must be authenticated and shown to be reliable to be accepted in court. Marie-Helen Maras notes that “The authenticity of electronic evidence

depends on the computer program that generated or processed the data in question" (Maras, 2014, p. 47). The Daubert standard requires the tools being used to investigate the evidence meet four criteria, whether theory or technique can be tested and has been tested (Maras, 2014). Whether there is a high known or potential rate of error, and the existence and maintenance of standards controlling the technique's operation (Maras, 2014). Whether the theory or technique has been subjected to peer review and publication (Maras, 2014). Whether the theory or technique enjoys "general acceptance" within the relevant scientific community (Maras, 2014). It is important that the tools used during the investigation are credible and acceptable (Maras, 2014).

Digital evidence presents several use cases depending on the crime committed. Avala Chaitanya claims "This evidence can provide crucial insights into a suspect's actions, motives, and movements" (Chaitanya, 2024, p. 1802). As mentioned at the beginning of this paper, digital evidence can assist investigators in reconstructing a timeline (Casey, 2011). This can help place a suspect at a location during the time of a crime or it could align a suspect with an alibi proving they were not at the scene of the crime (Casey, 2011). Additionally, digital evidence can help identify suspects and co-conspirators (Casey, 2011).

A recent event that was thwarted by law enforcement focused on multiple suspects from across the country who were planning a mass killing event in Washington D.C. during an event being held at the White House. The suspects used digital sources to communicate the plans where they would deploy drones with explosives to cause panic with event attendees causing them to evacuate the venue. The suspects then planned to be positioned to shoot the attendees while the fled the explosions. Law

enforcement was able to identify the suspects where 2 were from California, Ohio, Missouri, and Nebraska (U.S. Department of Justice, District of Nebraska, 2026). Dr. Princy Singla reinforces “enhancing the speed, accuracy, and credibility of investigations, these technologies address traditional limitations and adapt to the challenges posed by cybercrime and sophisticated criminal activities” (Singla, 2025, p. 1). The speed of the investigation prevented the potential mass casualty event from being planned and carried out (Singla, 2025).

Digital evidence plays a critical role in link analysis, the MCCA digital evidence working group describes “Link analysis creates visual representations of relationships between different entities, facilitating a deeper understanding of complex networks” (Major Cities Cheifs Association, 2024, p. 12). By examining call logs, messaging patterns, shared IP addresses, and social media interactions, investigators can map networks of co-conspirators and determine how the information flowed during the planning of the crime (Singla, 2025). Behavioral analysis tools can identify anomalies in search history, app usage, or financial transactions to identify premeditation (Singla, 2025). These methods allow investigators to move past isolated data points and gain a better understanding of criminal behavior (Singla, 2025).

Despite the value digital evidence provides, it also presents several challenges. Naeem Allah Rakha points out “Encryption, anonymity, and jurisdictional issues can make it difficult to access data on digital devices, identify suspects, and trace their online activities” (Rakha, 2024, p. 48). Strong encryption can prevent investigators from accessing data (Rakha, 2024). Even with warrants, some devices remain inaccessible without cooperation from device manufacturers (Maras, 2014). Many mobile devices

allow the device owner to configure a lock screen that requires a password to be entered to access the device, if the incorrect password is entered an excessive amount of times, the device will perform a factory reset clearing all of the data from the device (Maras, 2014).

An adjacent challenge that also needs to be considered is the budgetary strain presented while attempting to keep up with the quickly changing landscape of digital evidence. Captain Dana V. Ferreira mentioned “One of the most challenging aspects of deploying an effective digital forensics strategy is obtaining the necessary tools, equipment, and training to be successful. Implementing various solutions and technologies may require significant funds, to cover both initial outlays for equipment and recurring costs for services and software” (Major Cities Cheifs Association, 2024, p. 42). Law enforcement agencies across the country will need to stay current on hardware, software, and training. Cities, Counties, and States will need to work together to ensure they are properly equipped to handle these complex investigations.

Jurisdictional issues may also hinder an investigation by preventing law enforcement from acquiring the evidence that may be housed on a server located in a different state or even in another country that may not be willing to allow access to the digital evidence (Maras, 2014). Another complication could be the sheer amount of data that can be stored on devices (Beebe, 2009). It is not uncommon for devices to store hundreds of Gigabytes of data or even over a Terabyte and some cases a petabyte, this amount of data can slow an investigation down as it will take additional time to sift through this vast amount of data (Beebe, 2009).

Nathan McClaran points out the difficulty with obtaining evidence from IoT devices “Complexity of evidence, diversity in devices and a lack of techniques to address this, issues with correlating data to the case, volume of data, and difficulty in unified time lining of data gathered from devices” (McClaran, 2021, p. 10). When working with a number of IoT devices each may use a different technologies and may store data on different platforms (McClaran, 2021). For instance, an individual may have an Amazon Alexa device, Google Nest device, and more. These devices can store data on separate platforms and they can interact together. There are also ethical concerns where an investigator could misuse digital surveillance tools and unintentionally violate privacy rights or collect unnecessary data.

Digital evidence will continue to evolve as technology advances and the tools used to investigate and analyze data will improve with new technologies. Dr. Princy Singla lays out “The future of law enforcement will be heavily shaped by technological integration, with trends pointing toward broader adoption of AI, big data analytics, and real-time surveillance systems” (Singla, 2025, p. m658). Artificial Intelligence (AI) can automate evidence analysis by identifying patterns and flag anomalies (Singla, 2025). More and more devices are moving to storing data on the cloud (Beebe, 2009). Investigators will need to adapt and rely on cloud-native forensics tools capable of analyzing remote storage (Beebe, 2009). With advancing IoT devices including Automated License Plate Recognition cameras (ALPR), there will be an increasing amount of sensor data and environmental recordings that will assist investigators . There will be added potential using the vast amount of data to create prediction models that could help identify when and where potential crimes may occur (Singla, 2025).

Digital evidence is indispensable to modern criminal investigations and will continue to expand in both importance and quantity (Casey, 2011). It provides accurate, reliable information that helps investigators reconstruct events, identify suspects, and present compelling evidence in court (Casey, 2011). However, its value depends on proper collection, preservation, and adherence to legal and ethical standards (Maras, 2014). As technology continues to expand and evolve, investigators must adapt to new tools, new challenges, and new expectations (Major Cities Cheifs Association, 2024). The Guthrie case demonstrates how everyday devices can become critical sources of evidence, reinforcing the need for investigators to understand and leverage digital technologies effectively. Digital evidence will remain central to criminal investigations, shaping the future of law enforcement and public safety.

Bibliography

Beebe, N. (2009). Digital Forensic Research: The good, the bad and the unaddressed. In G. Peterson, & S. Shenoi, *Advances in Digital Forensics V* (pp. 17-36). Berlin: Springer.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic science, computers, and the internet.* (Third Edition ed.). Academic press.

Chaitanya, A. (2024). Forensic criminology and the analysis of digital evidence: A review. *International Journal of Innovative Research in Technology, 11*(5), 1801-1803. Retrieved from https://ijirt.org/publishedpaper/IJIRT168801_PAPER.pdf

Federal Bureau of Investigation. (2026, January 31). *Seaking Information: Nancy Guthrie video footage*. Retrieved June 28, 2026, from FBI: https://www.fbi.gov/video-repository/nancy-guthrie-home-footage-013126-01.mp4/view

Guttman, B., White, D. R., & Walraven, T. (2022). *Digital evidence preservation: Considerations for evidence handlers.* National Institute of Standards and Technology. doi:https://doi.org/10.6028/NIST.IR.8387

Jakobsen, A. T. (2024). *Practical Cyber Intelligence: A Hands-on Guide to Digital Forensics.* Hoboken: Wiley.

Jones, C. (2024, November 19). Inside final minutes of Laken Riley's life as smartwatch data captured desperate battle against suspect killer who 'slept like baby' after alleged murder. *The Mirror US*. Retrieved June 28, 2026, from https://www.themirror.com/news/us-news/laken-riley-murder-georgia-immigration-813416

Major Cities Cheifs Association. (2024). Digital evidence: Enhancing public safety using digital investigative technologies. Retrieved from https://majorcitieschiefs.com/wp-content/uploads/2024/10/MCCA-Digital-Evidence-White-Paper-_-Oct-2024.pdf

Maras, M.-H. (2014). *Computer Forensics: Cybercriminals, laws, and evidence* (2nd ed.). Jones & Bartlett Learning. Retrieved from https://yuzu.vitalsource.com/books/9781284066234

McClaran, N. (2021). *The Opportunities and Challenges of Internet of Things Evidence in Regard to Criminal Investigations.* Searcy: Harding University. Retrieved from https://scholarworks.harding.edu/cgi/viewcontent.cgi?article=1002&context=honors-theses

Nortje, J. G. (2023). Impediments during the execution of a search and seizure warrant for digital information by forensic investigators in South Africa. *Journal of Financial Crime, 31*(4), 810-822. doi:https://doi.org/10.1108/JFC-05-2023-0125

Peterson, G., Shenoi, S., & (Eds.). (2009). *Advances in Digital Forensics V.* Berlin: Springer.

Pollitt, M. (2010). A History of Digital Forensics. *6th IFIP WG 11.9 International Conference on Digital Forensics (DF).* Hong Kong, China: Springer. doi:10.1007/978-3-642-15506-2_1

Rakha, N. A. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. *Mexican Law Review (New Series), XVI*(2), 23-54. doi:10.22201/iij.24485306e.2024.2.18892

Scientific Working Group on Digital Evidence. (2020). *SWGDE Best Practices for Mobile Device Evidence Collection & Preservation: Handling and Acquisition (Version 1.2).* Scientific Working Group on Digital Evidence (SWGDE). Retrieved from https://drive.google.com/file/d/1sVko_Uo7o6iootWwn9IoLJ3mrMVXqTDg/view?usp=sharing

Singla, P. (2025). The impact of technology on criminal investigations and evidence. *International Journal of Creative Research Thoughts, 13*(3). Retrieved from https://ijcrt.org/papers/IJCRT25A3457.pdf

Spinello, R. A. (2021). *Cyberethics: Morality and Law in Cyberspace* (7th ed.). Jones & Bartlett Learning.

U.S. Department of Justice, District of Nebraska. (2026, June 17). *Five Men Arrested and Charged in Plot to Attack and Kill Government Officials and Others Attending the Ultimate Fighting Championship at White House*. Retrieved from Unites States Department of Justice:

https://www.justice.gov/usao-ne/pr/five-men-arrested-and-charged-plot-attack-and-kill-government-officials-and-others