INTERNATIONAL JOURNAL OF LEGAL SCIENCE AND INNOVATION

[ISSN 2581-9453]

Volume 7 | Issue 5

2025

© 2025 International Journal of Legal Science and Innovation

Follow this and additional works at: https://www.ijlsi.com/

Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com)

This Article is brought to you for free and open access by the International Journal of Legal Science and Innovation at VidhiAagaz. It has been accepted for inclusion in International Journal of Legal Science and Innovation after due review.

In case of **any suggestion or complaint**, please contact **support@vidhiaagaz.com.**

To submit your Manuscript for Publication at **International Journal of Legal Science and Innovation**, kindly email your Manuscript at **editor.ijlsi@gmail.com.**

Digital Evidence and Cyber Forensics: Facing the Real-World Challenges of Law and Integrity

ANIRBAN DAM[1] AND NEELDIP SASMAL[2]

ABSTRACT

In today's digital age, electronic data has become a powerful tool in solving crimes and settling legal disputes. This kind of data, often called digital evidence, includes things like emails, social media posts, digital documents, and information from smartphones. Cyber forensics is the field that deals with collecting, examining, and keeping this evidence safe. But bringing digital evidence into a courtroom isn't always easy. Two major concerns are whether the evidence is admissible—meaning it can legally be used in court—and whether its integrity has been preserved, meaning it hasn't been changed or tampered with.

This paper looks into the common challenges in dealing with digital evidence. These include the risk of alteration, differences in legal rules across regions, and the importance of using proper methods to collect and store the data. A big part of the challenge is showing that the evidence is authentic and was gathered legally.

As technology advances, cybercrimes are becoming more sophisticated, and so is the way we need to handle digital evidence. By examining real cases and current practices, this paper offers insights and recommendations to help ensure digital evidence remains trustworthy and useful in legal settings.

Understanding these challenges is key to ensuring justice in our increasingly digital world.

Keywords: *Digital evidence, Cyber forensics, Admissibility, Integrity, Authentication, Legal challenges, Evidence collection, Data preservation, Digital crimes, Courtroom, Legal rules, Technology, Tampering, Real cases, Best practices, Trustworthiness, Legal disputes, Smartphones, Social media, Emails.*

I. INTRODUCTION

In today's world, technology is a part of almost everything we do. We use computers, smartphones, and the internet to talk to people, manage our money, shop, and even work. But as our digital lives grow, so do the risks. Cybercrimes like hacking, online scams, and data theft are becoming more common. To deal with these problems, we now rely on something called

[1] Author is a Student at Adamas University, Barasat, Kolkata, India.
[2] Author is a Student at Adamas University, Barasat, Kolkata, India.

© 2025. International Journal of Legal Science and Innovation [ISSN 2581-9453]

digital evidence and a process known as cyber forensics.

Digital evidence is any kind of information stored on a device that can help prove what happened during a crime. This could be emails, text messages, files, videos, or even social media posts. Just like fingerprints or DNA can be used in regular investigations, digital evidence can help show who did what, when, and how.

Cyber forensics is the process of investigating crimes that happen in the digital world. Experts in this field carefully collect and study digital evidence using special tools and follow legal rules to make sure everything is done the right way. Their work helps police and lawyers understand how a cybercrime happened and who is responsible.

These tools are more important than ever. With so much of our personal and business information online, a single data breach or cyberattack can cause serious damage. Cyber forensics helps protect people, businesses, and even governments from these threats by tracking down criminals and preventing future attacks.

II. LEGAL FRAMEWORK AND ADMISSIBILITY

Digital evidence has become a key part of many legal cases today. But it's not enough to just find digital data—it has to be collected, handled, and presented in a way that follows the law. To make sure this happens, there are rules and laws in place, both within countries and internationally.

Different countries have their own legal systems for managing digital evidence. In **India**, the **Information Technology (IT) Act, 2000** helps define how electronic records and digital signatures can be used in court. In the **United States**, the **Federal Rules of Evidence (FRE)** explain how evidence, including digital files, should be treated to make sure it's fair and reliable. In **Europe**, the **General Data Protection Regulation (GDPR)** focuses on protecting people's personal data. It ensures that any digital information is collected and handled with care, especially when it's used in legal matters.

For digital evidence to be accepted in court, it has to meet some important conditions:

1. **Relevance** – The evidence must be directly connected to the case and help prove something important.
2. **Authenticity** – It should be clear that the evidence is real and hasn't been faked or edited.
3. **Integrity** – The information must stay the same from the moment it's found until it's shown in court.

4. **Chain of custody** – There should be a clear record showing who collected the evidence, who handled it afterward, and where it was stored. This helps prove that the evidence wasn't changed or tampered with.

If any of these steps aren't followed properly, the evidence might not be allowed in court—even if it could have helped the case.

Technical Challenges

Even though digital evidence is a powerful tool for solving cybercrimes, it comes with some serious technical challenges. Finding and using this kind of evidence isn't always easy, and there are several reasons why.

One of the biggest problems is that digital evidence is **fragile**. It can be changed, deleted, or lost very quickly. For example, just turning off a computer or restarting a phone can make important data disappear. If someone knows they're being investigated, they might erase files within seconds. This means investigators have to act fast and be extremely careful when collecting digital data.

Another issue is **encryption** and **anonymization**. Encryption locks data so that only someone with the right password or key can open it. Anonymization hides a person's identity online. While these tools help protect privacy, they can also make it very difficult for investigators to access the information they need to solve a case.

There's also the challenge of **too much data** from too many places. Digital evidence can come from phones, laptops, cloud storage, smart watches, home devices, and more. This mix of devices and formats is known as **data volume and variety**. Investigators have to sort through huge amounts of information, often stored in different ways, which takes time and special skills.

Lastly, some criminals use **anti-forensics tools** to cover their tracks. These are programs or tricks designed to hide, delete, or change digital evidence. For example, they might use software that erases files automatically or makes it look like someone else used the device. This makes the job even harder for those trying to uncover the truth.

III. INTEGRITY AND CHAIN OF CUSTODY

When it comes to digital evidence, keeping it exactly the way it was found is incredibly important. From the moment it's collected to the time it's presented in court, it must not be changed, edited, or damaged in any way. This is what we mean by **maintaining the integrity** of the evidence. If there's even a small chance that the evidence was tampered with, it can lose

its value in court—and that could seriously affect the outcome of a case.

To protect digital evidence, investigators follow a process called the **chain of custody**. This is a clear and detailed record that shows every step the evidence went through—who collected it, when and where it was stored, and who handled it along the way. It's like a timeline that tracks the evidence from start to finish. The goal is to make sure there's no room for doubt about where the evidence came from or whether it was changed.

For example, if police take a phone from a suspect, the chain of custody would show who took the phone, what time they took it, where it was kept, and who accessed it later. If anything in that chain is missing or unclear, the evidence might be questioned or even rejected in court.

To take things a step further, investigators also use something called **hashing algorithms**. These are special tools that create a kind of digital fingerprint for a file. Two common ones are **MD5** and **SHA-256**. When a file—like a photo or document—is collected, its hash value is recorded. Later, that hash can be checked again. If the value hasn't changed, it proves that the file is exactly the same as it was when it was first found.

In simple terms, it's like sealing something in a tamper-proof bag and checking the seal before opening it. If the seal is unbroken, you know nothing inside has been touched.

IV. TOOLS AND TECHNIQUES USED IN CYBER FORENSICS

Solving cybercrimes isn't just about knowing where to look—it's also about having the right tools and techniques to find and understand digital evidence. In cyber forensics, experts use powerful software and smart methods to uncover the truth hidden inside computers, phones, networks, and other digital devices.

Some popular tools used in this field include **EnCase**, **FTK (Forensic Toolkit)**, **Autopsy**, **Wireshark**, **Volatility**, and **X-Ways Forensics**.

- **EnCase** helps investigators search and collect data from devices in a way that doesn't damage the original evidence.
- **FTK** is great for scanning large amounts of data quickly and recovering files that were deleted.
- **Autopsy** is a free, easy-to-use tool that helps find useful files and evidence on hard drives.
- **Wireshark** looks at network traffic—it can show what information was sent or received over the internet.

- **Volatility** is used to check what was happening in a computer's memory at a certain time, like what programs were running.
- **X-Ways Forensics** is a powerful tool for digging into hard drives and recovering hidden or damaged data.

Along with these tools, there are also key **techniques** that investigators use:

- **Data acquisition** is the safe copying of data from a device, making sure the original stays untouched.
- **Data carving** allows experts to recover files even if they've been deleted or the system is damaged.
- **Network forensics** focuses on tracking activity across a network, which can help identify hackers or suspicious behavior.
- **Memory analysis** looks at what was happening inside a computer's RAM, which can reveal hidden threats or malware.

V. ETHICAL AND PRIVACY CONCERNS

As helpful as digital forensics is in solving crimes, it also brings up serious questions about privacy and ethics. Investigators often need to dig into people's personal data to find the truth—but that doesn't mean they can ignore someone's right to privacy. Finding the right balance between solving a case and respecting personal boundaries is one of the biggest challenges in this field.

One major issue is **how to balance investigations with privacy rights**. Everyone has a right to keep their private messages, photos, and online activity safe from unwanted access. But what happens when that same data could be important in a crime? Investigators have to make tough choices. They must ask themselves: "Do we really need this information?" If it's not absolutely necessary, they shouldn't access it. Just because something *can* be seen doesn't always mean it *should* be.

Another concern is the **risk of surveillance abuse**. Forensic tools are powerful—they can unlock phones, track online activity, and recover deleted files. But in the wrong hands or without proper rules, these tools can be misused. For example, someone could secretly monitor another person without a valid reason. This kind of abuse not only invades privacy, it also damages public trust.

There are also **ethical problems when working across different countries**. What's allowed in one place may be illegal in another. One country might let investigators access cloud data

easily, while another has strict rules that protect user privacy. In these cases, investigators must be extra careful to follow international laws and respect people's rights, no matter where they live.

At the heart of all this is a simple idea: **just because technology allows something doesn't mean it's right**. Digital forensics isn't just about getting results—it's about doing the right thing, the right way. Investigators need to follow the law, respect personal boundaries, and think carefully before they act.

VI. JURISDICTIONAL AND CROSS-BORDER CHALLENGES

Cybercrime is tricky because it doesn't happen in just one place. Unlike a normal crime, which usually takes place somewhere specific, cybercrime can start in one country, use servers in another, and affect people all around the world. This makes it really hard for police and courts to figure out whose laws apply and who should be in charge of investigating and prosecuting the criminals.

One big problem is that the internet connects the whole world, but the law doesn't work that way. If a hacker in Country A attacks a company in Country B using a server in Country C, which country's police get to step in? Each country has different rules, and sometimes their laws don't match up at all. This can cause confusion and slow down efforts to catch cybercriminals.

Because cybercrime crosses borders so easily, countries need to **work together**. Nobody can fight this alone. That's why international agreements like the **Budapest Convention** are so important. This treaty is the first of its kind to help countries cooperate on cybercrime. It gives governments a way to share information, request help, and gather evidence across borders. This kind of teamwork makes it easier and faster to catch criminals who operate globally.

Even with agreements like this, sharing digital evidence between countries isn't simple. Different countries have different ideas about privacy and data protection. What's allowed in one place might be against the law somewhere else. Sometimes, getting access to important data from a company or server in another country takes a lot of time, or even hits a dead end if that country won't cooperate. Politics and trust also play a role—some countries hesitate to share information for fear of exposing secrets or losing control.

All of these things make it harder for investigators to do their job. If they can't get the evidence they need quickly, it's tough to prove who did what and hold them responsible. Investigations can stall or even fail because of these legal and practical hurdles.

VII. LANDMARK CASE LAWS

Digital forensics plays a huge role in solving cybercrimes, but the law also has a big say in how evidence is used and what investigators are allowed to do. Looking at some important court cases helps us understand how forensic work and legal challenges come together in real life.

Take the **WannaCry ransomware attack in 2017**, for example. This attack locked up computers in hundreds of countries and caused a lot of damage. Forensic experts worked hard to study the malware and trace where it came from. But it wasn't easy for prosecutors because the hackers used servers all over the world and encrypted their messages. Courts had to figure out how to handle evidence that was gathered from different countries, and whether it could be used in their own courts. This case really showed how complicated it is to deal with crimes that cross borders.

Another interesting case is about **insider threats**, called *United States v. Nosal*[3]. Here, an employee accessed company information he wasn't supposed to see. Digital forensics helped by looking at computer logs and emails to prove what happened. But the court also had to make sure that the way investigators collected the evidence didn't violate privacy rules or company policies. This case set some important limits on how much companies can watch their employees and how they must collect digital evidence carefully.

Financial fraud is another area where digital forensics is key. In the *SEC v. Rajaratnam* case[4], forensic experts looked through emails and phone records to uncover insider trading, where secret information was shared illegally to make money in the stock market. The court had to be sure that the evidence was real and hadn't been changed or tampered with. This case showed how important it is to protect the honesty of digital evidence.

VIII. METADATA AS EVIDENCE

When it comes to digital investigations, metadata is like the secret diary of a file. It's the hidden information attached to things like photos, documents, or videos that tells us important details—like when a file was created or changed, where it was made, and who worked on it. This "behind-the-scenes" data is super helpful for investigators trying to figure out what really happened.

One of the coolest things about metadata is that it helps verify if digital evidence is real or if someone has messed with it. For example, imagine you have a photo that's supposed to prove

[3] *United States v. Nosal*[3].
[4] *SEC v. Rajaratnam* case[4]

where and when something happened. The metadata inside that photo can confirm the exact time and place it was taken. If everything matches up, that makes the evidence stronger. But if the timestamps or locations don't make sense, it can be a big red flag that the file has been changed or faked.

Metadata also helps investigators piece together the story by showing timelines and hidden clues. By looking at the dates and times on a bunch of files, experts can build a clear timeline of events—what happened first, what came next, and so on. This is really useful in cases like hacking or fraud, where understanding the order of events is key. Metadata can even reveal strange patterns, like files being accessed from unusual places or repeated attempts to open certain documents, which might point to suspicious activity.

The tricky part is that metadata is often ignored or deliberately removed by criminals. People who want to cover their tracks sometimes strip metadata from files so it's harder to find out where the files came from or when they were made. Because of this, forensic investigators know it's super important to check metadata early on—before it disappears or gets deleted.

IX. COURTROOM PRESENTATION OF DIGITAL EVIDENCE

These days, digital evidence is a huge part of solving crimes. But one of the biggest challenges is making sure that judges and juries actually understand this kind of evidence. Often, digital evidence includes complicated technical stuff—like computer codes, hacking methods, or data logs—that can sound like a totally different language to most people. If it's not explained in a simple way, there's a real risk that the evidence might be confusing or even ignored.

Most judges and juries don't have a tech background, so when they hear about things like encryption or network traffic, it can feel overwhelming. This makes it tough for them to see how the evidence connects to what really happened. If the details are too hard to follow, the case can suffer because the people making decisions won't fully get why the digital clues matter.

That's why **expert witnesses** are so important in court. These are people who know the technical stuff inside and out but also know how to explain it in plain, everyday language. Their job is to take all that complicated information and break it down into simple stories or examples that everyone can understand. A great expert witness helps the judge and jury see why the evidence matters and how it proves what really happened.

To make things even clearer, experts use **visual aids** like charts, diagrams, or timelines. These visuals can show exactly when and how something happened, step by step. For instance, a timeline might show when a hacker broke in and what they did next. Experts also use

demonstration tools—like videos or live computer screens—to show the evidence in action. This helps turn confusing numbers and codes into something real and easier to grasp.

It's really important that the evidence is clear and easy to follow. If the court finds it confusing, they might just dismiss it, which could let a criminal walk free. Forensic teams know this, so they spend a lot of time preparing how to explain things simply and answering questions clearly.

X. CYBER TERRORISM AND NATIONAL SECURITY

Nowadays, terrorists aren't just using traditional weapons—they've taken their activities online. The internet has become a new way for them to cause harm. Terror groups use digital platforms to do things like raise money, spread their messages, and recruit new members. It's easier for them to reach people around the world through social media, websites, and even encrypted chats.

One of the biggest challenges is the **dark web**, a hidden part of the internet where criminals and terrorists can operate in secret. Because it's tough to find and monitor, national security teams have to work extra hard to keep an eye on what's going on there. Many countries have special groups—called national forensics units—that constantly watch online activity, trying to spot threats before they become real problems. These teams also try to decrypt secret messages so they can understand what terrorists are planning.

But it's not just about catching the bad guys—it's also about respecting people's privacy and following the law. Governments have to walk a fine line. On one hand, they need to watch suspicious online behaviour and stop attacks. On the other, they must respect legal rules that protect citizens' privacy. This creates a tricky situation: how much can the government monitor without crossing the line and invading people's rights?

This balance is a hot topic around the world. Different countries have different rules about surveillance and privacy, which makes it even harder to work together internationally. Still, experts agree that there need to be clear laws and open discussions to make sure surveillance is done fairly and responsibly.

To sum it up, cyber terrorism is a real threat because terrorists use the internet for funding, spreading dangerous ideas, and recruiting. National forensics teams play a key role in tracking down these threats, especially on secret parts of the web. But they must always work within the law, balancing safety with respect for privacy. Finding that balance is one of the toughest challenges in today's fight against cyber terrorism.

XI. AUTOMATION AND ARTIFICIAL INTELLIGENCE IN FORENSICS

In today's digital world, there's just so much data that trying to go through it all by hand is almost impossible. That's why automation and artificial intelligence, or AI, have become game changers in the field of digital forensics. These smart technologies help investigators sort through mountains of information quickly and spot what really matters.

AI and machine learning are basically computer programs that can learn from the data they see. They're great at finding patterns and picking out unusual things that might be signs of cybercrime. Instead of an investigator spending weeks digging through files and logs, AI tools can do the heavy lifting in just hours—or even minutes. This means investigators get answers faster and can spend more time focusing on solving the case.

One way AI helps is by automating log analysis. Logs are like digital footprints showing what's been happening on a computer or network. AI scans these logs super fast to catch anything suspicious, like a hacker sneaking in or unusual activity that doesn't belong. Doing this by hand would take forever and it's easy to miss something important.

AI is also amazing at detecting malware—bad software that hackers use to mess up computers or steal info. Traditional tools look for known malware by matching patterns they already know. But AI can spot new and sneaky malware by recognizing strange behaviours, even if it hasn't been seen before. This makes it much harder for cybercriminals to slip by unnoticed.

Another cool thing AI does is **anomaly spotting**. It learns what "normal" looks like for a system—like when people usually log in or how data usually moves around. When something odd happens, like a sudden burst of data or a login from a weird location, AI raises a red flag so investigators can check it out.

That said, AI isn't about replacing humans. It's a powerful tool that helps investigators by handling the boring and time-consuming parts. The real experts still need to look at the findings, use their experience, and make smart decisions.

XII. CONCLUSION

Digital evidence and cyber forensics have become really important in solving crimes today. Since so much of our lives happen online or on digital devices, criminals have moved their actions there too. This means that things like emails, messages, or digital files often hold the clues needed to catch them. But working with digital evidence isn't always easy—it brings some real challenges, especially when it comes to following the law and making sure the evidence is trustworthy.

© 2025. International Journal of Legal Science and Innovation [ISSN 2581-9453]

One big challenge is the legal side of things. Different countries have different rules about how digital evidence should be collected, stored, and used in court. If these rules aren't followed closely, there's a risk that important evidence could be rejected, and criminals might escape punishment. That's why knowing and respecting the law is just as important as understanding the technology behind digital forensics.

Another challenge is keeping digital evidence safe and unchanged. Unlike physical evidence, digital data can be easily changed or deleted—sometimes without anyone realizing it. Forensic experts have to be very careful and keep detailed records about every step they take with the evidence. This "chain of custody" helps prove that the evidence hasn't been tampered with from the moment it was collected until it's shown in court. Without this, the evidence might not be trusted.

There are also technical hurdles. Criminals use tools like encryption and other tricks to hide what they're doing online. Plus, there's a huge amount of data coming from phones, computers, cloud storage, and smart devices, making it a big job just to find what matters. While tools like artificial intelligence and automation can help speed things up, experts still need their skills and judgment to get things right.

Finally, investigators must balance catching criminals with respecting people's privacy. It's important to protect rights while keeping everyone safe. Also, since the internet connects the whole world, countries need to work together, but different laws can make that tough.

*****

© 2025. International Journal of Legal Science and Innovation [ISSN 2581-9453]