Bridging the Digital Divide: The Imperative for Cyber Expertise Among Nepal's Justices/Judges, Litigators, and Investigators

Former Judge Dr. Shree Krishna Bhattarai
PhD. in Cyber Law
PG (USA, Australia, and Nepal), Diploma (India)
Emali:bhattaraisk@yahoo.com

Article History : *2025 Septermber 3*

Abstract:

Digital evidence is becoming a common component of litigation across Nepal's legal spectrum, including civil disputes, criminal trials, constitutional writs, and administrative reviews. It is no longer limited to cybercrime cases and may be found in everything from WhatsApp conversations and emails to cloud records and GPS logs. Nevertheless, the revelation of this evidence has glaringly revealed a structural problem with Nepal's legal system. This article makes the case that Nepalese cyber jurisprudence has developed slowly and is now in a primitive state due to a lack of a strong legal framework, including a specific Digital/Electronic Evidence Act, Data Protection Act, Cybercrime Act, Social Media Act, and updated forensics legislation, as well as a serious lack of cyber literacy among judges, attorneys, investigators, and prosecutors. This article demonstrates how the absence of ISO-accredited Digital Forensics Labs, cyber-expert staff, and fundamental digital knowledge compromises fair trials, impedes justice, and compromises the integrity of the legal system by looking at the real-world difficulties encountered in routine cases. It concludes by making a compelling case for comprehensive capacity building among law enforcement officials, including judges, legal reform, the hiring of cyber-savvy judges, and the necessary integration of cyber competence at all levels of the legal profession in order to bridge the widening gap between technology and justice in Nepal.

Key words: *Admissibility, Authentication, Best Evidence Rule, Chain of Custody, Cloud Forensics, Cryptocurrency Transactions, Cyber Jurisprudence, Data Protection, Digital Evidence, Digital Forensics, Encrypted Communications, Evidence Act 2031, Forensic Imaging, Forensic Integrity, Hash Value (MD5/SHA-256), ISO/IEC 17025 Accreditation, Judicial Capacity Building, Metadata, Electronic Transactions Act 2063.*

1. Introduction: The Digitalization of Every Case File

In the digital age, jurisprudence is undergoing a significant and systemic shift that goes beyond simple technological innovation to radically change the essence of legal evidence. A ubiquitous "digital footprint," an indisputable record of our everyday online interactions, has unquestionably replaced the classic "paper trail," which was formerly the gold standard of documentary proof[380]. This paradigm change affects not only well-known cybercrime cases but also every possible field of law, ranging from simple civil disputes to intricate constitutional issues. The admissibility and evidentiary value of electronic communication—such as a GPS log that locates a suspect at a crime scene, a WhatsApp message that confirms a contract, or a cloud-stored financial record that demonstrates embezzlement—are therefore now crucial to legal practice. This tendency extends into specialized domains including property partition (`ANSHABANDA`) processes, where digital papers frequently specify historical borders or agreements; tenant (`MOHI`) concerns; and land disputes, where electronic land records and communications are becoming more and more relevant. Furthermore, social media activity and electronic correspondence are commonly used as decisive evidence in private international law matters including marriage, divorce, and alimony. Complex digital transaction flows demonstrate that issues pertaining to contracts, corporations, and tax liabilities are now mostly resolved by forensic investigation of digital transactions in the larger international legal and trade arenas. From the Supreme Court reviewing a writ petition on a citizen's fundamental right to data privacy to a family court deciding a divorce based on electronic communications, the change is so fundamental that it impacts every level of the legal system. This illustrates how the distinction between "cyber" and "non-cyber" cases has become obsolete due to the digital revolution, making digital evidence a ubiquitous element of contemporary litigation.

This global reality clashes with a harsh local setting in Nepal. The endowment, procedures, and mentality of the country's judicial system, which includes judges, prosecutors, defense lawyers, and investigators, are still largely analog. Even while people are embracing digital technologies at a rapid pace, the legal system that is supposed to resolve their conflicts is stuck in a pre-digital age[381]. The current legal framework is a patchwork of ambiguous laws that is completely insufficient to handle the intricacies of digital evidence. It was based upon the Evidence Act of 2031 (1974) and only slightly revised by the Electronic Transactions Act, 2063 (2008). The lack of mandatory cyber training for judges and attorneys, the absence of specialized cyber benches in the majority of courts, and a severe lack of investigators and forensic analysts who are knowledgeable about the fundamentals of preserving and analyzing digital evidence all contribute to this legislative vacuum.

The essential tenets of justice are seriously threatened by Nepalese jurisprudence's rudimentary approach to digital evidence, which is the result of widespread systematic failure.

---

380 David Cole, Technology & Crime: How Digital Evidence Is Changing Criminal Trials, David Cole Lawyer (July 3, 2022), https://www.davidcolelawyer.com.au/technology-and-crime-digital-evidence-changing-criminal-trials.html.

381 World Bank, Five ways digital technologies are transforming courts and access to justice (Mar. 19, 2025), https://blogs.worldbank.org/en/governance/five-ways-digital-technologies-are-transforming-courts-and-acces.

Consensus on the evidentiary authentication of everyday digital artifacts is often and critically lacking in legal proceedings[382]. It is frequently contested whether a WhatsApp screenshot, scanned document, or email log is admissible, leading to inquiries about whether the best evidence rule has been followed or whether it is hearsay evidence. Raw CCTV footage, audio-visual recordings from spy cameras, and voice recordings are frequently contested for their legality based on the chain of custody's validity rather than their content. The present law enforcement system mainly lacks the techno-legal ability to appropriately seize and secure the original digital device from which the evidence was initially obtained. Legal suspicion is raised by future digital forensic imaging and analysis if this important step is skipped. Additionally, the proliferation of AI-powered evidence and the pervasiveness of the IoT[383] and IoE[384] have created a new level of complexity that is almost impossible for judges, prosecutors, and investigators to handle without highly specialized knowledge. This structural absence of basic "cyber savviness" jeopardizes the effectiveness, reliability, and fairness that are the foundations of justice. It runs the risk of making important evidence inadmissible, dragging out court cases, and finally producing unfair results[385]. In order to create a legal profession that can administer justice in the twenty-first century, this analysis will identify the institutional and legal gaps, navigate the pervasiveness of digital evidence in all case types, and provide a concrete path ahead[386].

2. The Pervasiveness of Digital Evidence: From Contract Law to Constitutional Law

It is a perilous misunderstanding to believe that digital evidence is exclusively useful in "cybercrime" situations. It can be found in almost every area of the practice of law.

A. Civil Litigation

The legal validity of electronic records is a well-established notion under prominent international legal frameworks, such as Singapore's Electronic Transactions Act[387] and the United States' Uniform Electronic Transactions Act (UETA)[388]. According to these frameworks, the mere fact that an electronic signature or record—such as an email or a

---

[382] Policy Paper on Advocating Chain of Custody and Governance of Digital Evidence in Nepal, Human Rights Journal of Nepal (2025), https://hrjc.org.np/wp-content/uploads/2025/01/report-advocating-chain-of-custody-and-governance-of-digital-evidence-in-nepal.pdf.

[383] Internet of Things

[384] Internet of Everything

[385] International Standards for Forensic Digital Evidence, Case Western Reserve University School of Law War Crimes Research Office (2025), https://scholarlycommons. law.case.edu/cgi/ viewcontent. cgi?article =1281&context=war_crimes_memos.

[386] Dr. Shree Krishna Bhattarai, Cybercrime in Nepal, Nagarik News (Sept. 2, 2025), https://nagariknews.nagariknetwork.com/opinion/135387-1514262180.html.

[387] Electronic Transactions Act (Cap. 88) (Singapore), https://www.jonesday.com/en/insights/2021/02/singapores-electronic-transactions-act-expanded (last visited Sept. 1, 2025).

[388] Uniform Electronic Transactions Act § 47-10-101 et seq. (Tenn.), https://www.ctas.tennessee.edu/eli/uniform-electronic-transactions-act (last visited Sept. 1, 2025).

clickwrap agreement—is in electronic form does not negate its legal force. The evidentiary authenticity of emails, e-signatures, and messaging app exchanges is therefore a matter of settled law in contractual disputes. The integrity and dependability of the digital record—making sure it accurately and fully reflects the parties' intent and agreement—are the court's primary concerns, not the medium.

i) Family Law:

Digital evidence has become crucial in family law and divorce proceedings. For example, social media posts have the potential to provide evidence of inappropriate behavior, which could be important in cases involving adultery or judicial separation. Digital forensic analysis of bank statements and mobile banking apps or payment gateway (eSewa, Connect IPS, IME Pay, Khalti) is frequently utilized for the financial disclosure phase in order to track down hidden assets for asset distribution and alimony. WhatsApp conversations and other electronic communications must be authenticated in child custody disputes in order to demonstrate a parent's suitability or unsuitability, which will have a direct impact on the court's assessment of the kid's best interests.

ii) Property and Debt Recovery:

Prima facie evidence in modern property and debt-related lawsuits is becoming more and more computerized. Digital title deeds are accepted as legally binding documents by the legal systems of developed countries. A scanned contract's evidentiary weight is based on its verified data integrity and non-repudiation, which guarantees the document hasn't been altered, rather than its actual absence. As trace evidence in asset recovery and debt collection proceedings, forensic acquisition of electronic bank statements and mobile payment records has become commonplace. The speedy and fair settlement of disputes depends heavily on the appropriate management of e-evidence, from its secure collection to its presentation in court.

B. Criminal Trials

i) Cybercrimes:

Digital evidence is essential to the prosecution of cybercrimes such identity theft, hacking, and online fraud. Digital transaction trails, IP addresses[389], and server logs must be forensically obtained and authenticated in order to support the prosecution's case. In order to prove non-repudiation and guarantee that the evidence is admissible in a court of law, it is crucial to maintain an uncorrupted chain of custody. Without this, it would be simple to contest and reject the prosecution's case.

ii) Conventional Crimes:

These days, the criminal investigation process is entirely computerized. To determine a person's position, forensic examination of GPS metadata and CDRs[390]

[389] Devices on a network, including the Internet, that communicate over the Internet Protocol are assigned a numerical designation called an IP address. Its main responsibilities include network interface identification (the device) and location addressing, which allow data to be sent to and from the right place.

[390] Call Detail Records

is a common practice. Building a case requires both the forensic analysis of CCTV material and the recovery of deleted text messages. Furthermore, social media forensics, which offers trace evidence of communication patterns and methods of operation, has emerged as a crucial weapon in human trafficking and other crimes.

iii) Financial and Organized Crime:

Digital forensics is now essential to the detection of complex frauds and money laundering activities. Digital banking systems, encrypted messaging apps like Telegram[391], and cryptocurrency exchanges are common places to find evidence. It takes specific knowledge of blockchain research and the capacity to decipher intricate digital transaction traces to track down illegal cash transactions. Prosecutors cannot build a convincing financial evidence trail to hold offenders accountable without this knowledge.

C. Constitutional Writs & Administrative Law

i) Right to Privacy:

In the Internet age, writ petitions and constitutional cases are increasingly at the center of the discussion over fundamental rights. The judiciary is directly challenged by issues pertaining to the right to digital privacy and the protection of personal data kept in government databases. These disputes frequently center on whether data breaches or state-sponsored monitoring violate people's constitutional rights. Using techno-legal concepts to determine the extent of a citizen's protected digital existence, the legal determination necessitates a careful balance between national security and the privacy of personal data.

ii) Freedom of Expression:

Courts are increasingly faced with the difficult issue of striking a balance between a citizen's fundamental right to freedom of expression and legal and societal norms as the digital public sphere takes over as the major communication medium. A sophisticated legal strategy is needed in cases involving alleged internet hate speech, defamation, contempt of court, or incitement to violence. An individual's posts' contextual digital trace, their channels of distribution, and their potential for harm must all be carefully examined by the judiciary. A thorough grasp of online platforms and the legal rules controlling them is necessary to make the legal assessment of whether an act of digital expression is a criminal violation or a valid exercise of a fundamental right.

iii) Right to Information:

Since citizens now exercise their right to information by requesting access to government-held material in digital formats, the development of e-governance has stretched the bounds of administrative law. Public institutions must adapt to this change by developing strong digital record management procedures and moving beyond conventional paper-based systems. The interoperability, data integrity, and

[391] Since most chats do not automatically use end-to-end encryption, Telegram's "top secrecy" feature is rather deceptive. Standard "Cloud Chats" are client-server encrypted, which may allow access by the business or outside parties, whereas "Secret Chats" provide secure E2EE and self-destructing messages.

accessibility of government databases are frequently at the center of legal disputes. Courts must decide on issues pertaining to a government's obligation to deliver information in a timely and safe manner, while also taking into account concerns about the security of critical digital assets and the protection of personal data, as citizens demand transparency.

D. Other Areas

i) Labor Law:

The digital record is now essential to proving facts in contemporary labor conflicts. Digital forensics is necessary to confirm the validity and integrity of email correspondence, which is crucial for establishing the chronology and character of events in wrongful termination instances. Similar to this, data generated by electronic attendance systems can be used as unquestionable proof of an employee's presence or absence, and metadata analysis can reveal important details about how the data was created and altered. Such evidence must be properly authenticated and a clear chain of custody established in order to be admitted.

ii) Intellectual Property:

Digital evidence is becoming essential in intellectual property infringement prosecutions. Digital forensics, which frequently involves the examination of IP addresses and web server logs, is used to identify the origin of copyright violations on peer-to-peer networks and websites. The use of WHOIS information[392] and other metadata to demonstrate the chain of ownership and intent is also necessary due to the prevalence of online trademark violations and domain name squatting. Due to this change, a key component of intellectual property litigation is now cyber-surveillance and the safe gathering of digital evidence.

iii) Foreign Employment:

Nowadays, digital evidence is the only basis for prosecuting dishonest employment agencies. These schemes, which are frequently a type of cyber-enabled fraud, trick job searchers by using social media accounts and complex websites. Careful digital forensics is necessary for the legal process in order to protect and examine a digital record of their online activity. To demonstrate dishonest intent, this includes social media accounts, website source code, and web server logs. The correct chain of custody of these digital artifacts is an unavoidable prerequisite for efficient law enforcement and judicial action since the admissibility of such evidence is crucial for conviction.

A judge or lawyer who is not conversant with digital evidence is practically unprepared to handle the great majority of modern cases due to its widespread use[393].

---

[392] WHOIS information is the publicly accessible data, such as contact details, registration and expiration dates, and name servers used, that is kept in a global database on registered internet domain names and their owners.

[393] Dr. Shree Krishna Bhattarai, Cybersecurity and Band on Tiktok, Desh Sanchar (Apr. 7, 2024), https://deshsanchar.com/2024/04/07/905717/.

3. The Legal Vacuum: Navigating Without a Compass

The handling of digital evidence in Nepal is complicated by a lack of a thorough legal framework, disagreements over procedures, and a severe skills deficit among important stakeholders. Although the ETA gives electronic records legal standing, it does not provide comprehensive instructions for managing digital artifacts. There are often disagreements regarding admissibility and chain of custody because traditional evidence concepts are not appropriate for the digital sphere. The situation is made more difficult by the absence of institutional capability and training, which leaves digital evidence cases in a vulnerable and archaic setting.

A. The Inadequacy of Existing Laws

i) Evidence Act, 2031 (1974):

When the Evidence Act was passed fifty-one years ago, the existence of virtual evidence seemed unimaginable. Physical evidence is rendered obsolete by the relatively recent innovation of the digital world. This legal gap is primarily caused by obsolete status. Although the second amendment[394], which added terminology like "electronic" and "digital," attempts to recognize modernity, the act is still essentially a set of guidelines created for physical, paper-based archives. For the complex lifetime of digital evidence, it offers no conceptual foundation. Provisions for the appropriate verification of email logs, social media communications, and digital data are absent from the Act. The use of hash values to confirm data integrity and guarantee non-repudiation, the admission of forensic photos as evidence, and the crucial processes for digital forensic photography are all left out. As a result, courts and attorneys are left without clear standards and are compelled to apply analog evidence procedures to problems that are fundamentally digital. Judges are forced to establish ad hoc precedents as a result, "fitting square digital pegs into round analog holes," a risky legal practice that compromises the justice and integrity of the legal system.

ii) Electronic Transactions Act, 2063 (2006):

In Nepal's cyber jurisprudence, the ETA is a fundamentally limited yet essential regulation. Although its original purpose was to validate transactional and commercial data, it has been expanded to become the principal legal basis for all electronic evidence. The ETA has a serious procedural flaw, even though Section 4 is an important first step because it gives electronic records legal legitimacy[395]. It does not offer a methodical approach to the forensic collection, preservation, and verification of digital evidence in criminal and civil cases. The essential concepts of chain of custody, forensic imaging, and expert testimony standards—all essential components of contemporary digital evidence—are noticeably absent from the Act. Judges are forced to use their own judgment in the absence of clear legal direction,

---

[394] Evidence (Second Amendment) Act, 2077 BS (Nepal), https://hrjc.org.np/wp-content/uploads/2025/01/report-advocating-chain-of-custody-and-governance-of-digital-evidence-in-nepal.pdf (last visited Sept. 1, 2025).

[395] Electronic Transactions Act, 2063 (Nepal) § 4, https://lawcommission.gov.np/content/13397/electronic--electronic--traded-international-act--2063/ (last visited Sept. 1, 2025).

which results in an unpredictable and inconsistent legal environment that compromises the justice system's impartiality and integrity.

iii) Criminal Procedure Code, 2074 (2017):

A really strong legal foundation for the digital age is still lacking, notwithstanding the introduction of a few progressive rules. A step in the right direction toward e-justice is the Criminal Procedure Code's support of electronic media for summons and warrants (Sections 62 and 64) and video conferencing (Sections 109 and 115). These clauses do, however, provide difficult techno-legal issues. Regarding how to guarantee the evidentiary integrity of evidence given through video, verify the identity of the individual on screen, and stop witness coaching, the law remains silent. Similar to this, serving a legal notice via email or other digital means introduces a serious procedural flaw pertaining to non-repudiation and proof of service. These well-intended digital technologies have the potential to undermine the due process they are intended to support by generating more legal disputes than they settle in the absence of clear legal procedures on how to authenticate receipt and the integrity of the document.

iv) Civil Procedure Code, 2074 (2017):

Despite its efforts to modernize the legal system, the Civil Procedure Code of 2074 reflects these difficulties. The provisions pertaining to electronic summons and notice service and video conferencing for case hearings and witness examination (Section 182) are praiseworthy. One step in the right direction toward transparency is Section 198, which allows court rulings to be uploaded to a website. However, these laws present a severe procedural flaw, just as their criminal counterpart. The code doesn't include specific procedures for confirming the evidentiary integrity of the remote testimony itself or for technically authenticating a participant's identification during a video hearing. Additionally, the law does not specify a precise standard for proof of service, such as whether a straightforward read receipt or a more sophisticated, cryptographically-signed electronic return is necessary, even if e-service provides a significant efficiency improvement. In addition to creating legal doubt and shifting the burden of proof to the sender, this ambiguity may result in procedural conflicts that undermine the very efficiency the code was designed to achieve.

B. The Missing Frameworks

There is no specialist legislation to bridge the vast gaps between these laws:

i) Absence of Digital/Electronic Evidence Act:

The lack of a specific Digital Evidence Act is Nepal's main legal shortcoming. A comprehensive, stand-alone statute is essential for offering a precise conceptual structure. A law of this kind would give a legal definition of digital evidence, create clear authentication standards for different types of electronic data, outline rules for the chain of custody, and make it clearer how the best evidence rule and hearsay exclusions apply to digital artifacts. Procedural integrity is jeopardized by this legal gap.

ii) Lack of Data Protection Act:

A significant legal gap regarding the handling of personal data in court proceedings is created by the lack of a comprehensive Data Protection Act. Uniform governance mechanisms for the gathering, handling, and storage of the enormous amounts of personally identifiable information (PII) utilized as evidence are lacking in the absence of a specific statute. In addition to compromising individual digital privacy, this raises legal questions about how to properly handle and sanitize sensitive data along the course of the legal system.

iii) Nonexistence of Digital Forensics Act:

Furthermore, the entire field is uncontrolled due to the absence of a specific Cyber Forensics Act. The integrity and dependability of all forensic evidence offered in court are jeopardized in the absence of laws mandating expert accreditation, forensic equipment validation, or the development of precise scientific standards for forensic labs. This regulatory gap undermines the fairness of court procedures by fostering an atmosphere in which the reliability of important digital evidence is constantly questioned.

C. Judicial Interpretation in a Void

The judiciary lacks the specific cyber skills needed for modern cases because it is made up of generalist judges. They frequently hesitate to fully engage in the field of digital forensics because of this knowledge gap. Judges are forced to become amateur technologists in this legislative vacuum. Without clear criteria, decisions on whether to admit digital evidence become haphazard and inconsistent. For example, based on a witness's statement, one judge might allow a Facebook screenshot, but another might deny it since the platform provider hasn't authenticated it. Since both judges and attorneys are frequently uninformed in this specialized sector, this lack of uniformity threatens the predictability and fairness of the legal system, which are fundamental components of the rule of law.

4. The Institutional Desert: The Crisis of Forensic Infrastructure

Nepal's institutional and physical infrastructure for digital forensics is woefully inadequate.

i) **National Forensic Science Laboratory (NFSL)[396]:** The NFSL is the renowned forensic laboratory of Nepal. It has seven distinct units, such as Toxicology, Narcotics, Chemistry, DNA, Serology, Wildlife, and Questioned Documents. However, it does not provide cyber forensic services. As a result, there is no cyber forensic division even though it is under the Ministry of Education, Science, and Technology.

ii) **Nepal Police Central Forensic Science Laboratory (NPCFSL)[397]:** The NPCFSL has 11 units: Biology/Serology, DNA, Chemistry/Narcotics, Explosives, Toxicology, Fingerprints, AFIS, Questioned Documents, Ballistics, Physics, IT, and Photography. However, it lacks dedicated cyber forensics units, missing critical digital evidence examination.

---

[396] National Forensic Science Laboratory, https://forensic.gov.np (last visited Aug. 15, 2025).

[397] Nepal Police Central Forensic Science Laboratory, https://forensic.nepalpolice.gov.np/about-us/introduction/ (last visited Aug. 15, 2025).

iii) **The Criminal Investigation Department (CID) Digital Forensic Lab (DFL):** Nepal does not yet have an independent DFL. Nonetheless, the CID's Cyber Crime Investigation Unit asserts that it possesses the DFL. "Cyber Crime Investigation Unit Annual Progress Report 2080[398]" states that the lab investigates cybercrimes (dark web activity, online fraud), does computer and mobile forensics, and more. However, it lacks advanced memory forensics (Volatility) skills, ISO 17025 accreditation, and blockchain analysis tools for locating bitcoin. Basic social media and cloud forensics are taken care of, but more complex cases require assistance from private organizations like Interpol. These differences show that in order to handle the growing issues related to cybercrime, updated systems and standardized practices are required.

The absence of essential ISO/IEC 17025 in Nepal's cyber forensics compromises the validity of the evidence and its admissibility in court. The DFL is becoming increasingly concerned about the lack of established forensic protocols and independent, standardized validation techniques. Additionally, access to sophisticated capabilities like blockchain analytics and cloud forensics is limited due to the lack of an independent lab. Unaccredited procedures continue to employ manual evaluation methods, and emerging threats (such bitcoin laundering and encrypted communications) are outpacing investigative capabilities.

A. Capacity Gaps in Existing Labs

The Digital Forensics Lab struggles because of its antiquated resources, despite its admirable job. Using outdated, frequently out-of-date software impairs their capacity to carry out their responsibilities. The lab utilized outdated software versions, including Atola Technology's Insight Forensic 5.6.9102.18310 and Magnet AXIOM v8.8.042722, the latter of which expired in April 2022, as was made public in the Sunil Rai case[399]. Their capacity to stay up with current encryption and developing forensic procedures is seriously hampered by such outdated equipment, which are not acceptable in court:

i) **Technological Lag:** They frequently lack sophisticated capabilities for deciphering data from the newest smartphones and apps, bitcoin transactions, and encrypted chats.

ii) **Skill Gaps:** Analysts with extensive training in fields like memory analysis, network forensics, and cloud forensics (data from Google Drive, iCloud) are in limited supply.

iii) **Case Overload:** These few labs are overloaded as digital evidence becomes commonplace in even small cases, resulting in enormous case backlogs and delays in the administration of justice.

B. The Conflict of Interest

Keeping the analyst and investigator apart to maintain objectivity is a cornerstone of forensic science. The Nepal Police, which also conducts criminal investigations, is in

---

398 Cyber Crime Investigation Unit, Annual Factsheet on Suicide & Cyber Crime: Fiscal Year 2080/81 (2024), Nepal Police Headquarters, Crime Investigation Department, https://www.nepalpolice. gov.np/media/filer_ public/fd/ 3e/fd3e1c95-aaa1-41bd-815e-0221254141d4/fy_2080-81_suicide__cyber_crime_-_en.pdf, at 12–15 (last visited Aug. 16, 2025).

399 Dr. Shree Krishna Bhattarai, defense attorney in Government of Nepal v. Sunil Rai, Case No. 081-C1-0786 (sub judice), based on personal forensic analysis performed on the digital media submitted by Digital Forensics Examiners, identifying use of outdated forensic software versions including Atola Technology's Insight Forensic v5.6.9102.18310 and Magnet AXIOM v8.8.042722 (expired April 2022).

charge of managing the country's digital forensic labs. A perceived, if not real, conflict of interest results from this. It would be simple for the defense to claim that the forensic analysis favors the prosecution's theory. Maintaining the integrity of the process requires an impartial national digital forensics body that serves all facets of the legal system.

5. Human Resource Dearth: A System-Wide Cyber Illiteracy

In Nepal's legal system, managing digital or electronic evidence is a multi-phase procedure that involves certain roles and legal requirements. The first person in charge of the initial diagnosis, preservation, and gathering of digital evidence is the SOCO[400]. Securing and maintaining the integrity of the evidence on-site is the main responsibility of the SOCO Officer.

Following preservation, the evidence is sent for forensic analysis, and the investigating officer receives the resulting Forensic Examination Report. The forensic results must be integrated into the larger criminal inquiry by this officer. From the first gathering until the analysis, every step of the procedure needs to be painstakingly recorded before being presented to the Public Prosecutor for further instruction.

Using all of the digital forensic reports as essential evidence, the public prosecutor creates and submits the charge-sheet. The Presiding Judge oversees the court's proceedings after the case comes under its jurisdiction, which includes directing the prosecution to provide evidence against the accused in line with Section 25 of the Evidence Act, 2031 procedure[401]. As required by Section 18 of the Due Process of Law, expert witness testimony—including cross-examination—is an essential part of this procedure[402].

A. The Investigators

For investigators and first responders, managing digital evidence is essential, but errors can have serious techno-legal repercussions. Critical metadata, such as timestamps and "last accessed" information, might be altered by errors, jeopardizing the integrity of the evidence. Furthermore, they frequently overlook the technical and legal requirements of a rigorous chain of custody, which might result in defense arguments that result in the dismissal of a case. The absence of a write-blocker, which keeps data from being sent to the source device and maintains its pristine condition, is another crucial mistake. In the absence of these protocols, evidence can be declared inadmissible under the "best evidence rule," rendering its integrity and authenticity hard to verify. Important evidence may be rendered inadmissible in court due to early mismanagement.

B. The Prosecutors & Defense Attorneys

The difficulties in managing digital evidence often arise in the courtroom, where attorneys usually lack the specific expertise needed to handle these cases. Many lawyers find it difficult to pose the right queries to a digital forensics expert. In an attempt to prove the

---

[400] Scene of Crime Officer

[401] Evidence Act, 2031, §§ 18, 25, Nepal Law Commission, https://lawcommission.gov.np/path-to-act (last visited Sept. 2, 2025).

[402] Criminal Procedure Code, 2074, §§ 6, 7, 8, 10, 18, 19, 21, 23, 26, 31, 32, 38, 99, 102, Nepal Law Comm'n, https://lawcommission.gov.np/content/13458/civil-criminal-procedure-code-2074/ (last visited Sept. 2, 2025).

integrity and legitimacy of the evidence, a prosecutor may unlawfully lead it. A defense attorney who is unable to understand the subtleties may fail to appropriately cross-examine the expert or challenge the methods used to collect evidence. This leads to cases in which the judge, who decides the facts, is not provided with the comprehensive analysis of the evidence required for a fair trial.

C. The Judges

The court is the ultimate arbiter of evidence. Nonetheless, many judges acknowledge that they feel unprepared to deal with digital evidence. The fundamental idea of digital evidence may be unfamiliar to a court used to physical evidence, which could overwhelm them and make them want to return to more conventional approaches. It's obvious that the incorrect individual is in the appropriate position in this instance. A judge overseeing a delicate case needs to be knowledgeable about the field of digital forensics. If not, they ought to step aside. How, for instance, can a judge decide on a Daubert-style[403] challenge to the validity of a forensic tool in the absence of training? How can they assess the significance of a hash value discrepancy? Two unfavorable consequences may result from this discomfort: either the unquestioning acceptance of whatever evidence that the police or prosecution present, or the overly cautious rejection of credible evidence because of ignorance. Either way, justice has not been served[404].

D. The Result

A justice system that is inefficient, unreliable, and unfair is the result of systemic illiteracy in the legal profession. This lack of cyber-savvy damages public trust and leads to drawn-out legal disputes. Digital evidence that is misunderstood or handled incorrectly might result in the innocent being wrongfully condemned and the guilty avoiding conviction. This disregard for the technical details of contemporary evidence compromises the legal system as a whole and emphasizes the necessity of thorough digital literacy in the courts and law enforcement[405].

Key Stages of Digital Evidence Handling: A Technical and Legal Overview

Stage	Purpose	Key Technical Actions	Critical Legal Considerations
1. Identification	To recognize potential digital evidence and determine its location and type.	Identify digital devices (laptops, phones), cloud storage, and accounts that may contain relevant data.	Legal authority (warrant or consent) is required to access data.

[403] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993), https://www.law.cornell.edu/supct/html/92-102.ZS.html (last visited Aug. 15, 2025).

[404] Dr. Shree Krishna Bhattarai, Interview by Dr. Vijay Mishra, DC Nepal (Feb. 2024), https://www.dcnepal.com/2024/02/548718/.

[405] Dr. Shree Krishna Bhattarai, Cyberlaw and Internet Crimes, Nepalese Legal Frameworks and Judicial Practices, (Communication Registrar's Office, Ministry of Internal Affairs and Law, Bagmati Province Government, July 2024).

2. Preservation	To secure the original evidence without alteration or contamination.	Isolate the device from networks (airplane mode, Faraday bag). Create a **forensic image** (exact bit-by-bit copy) of the data.	The Hash value must be calculated and documented before and after imaging to prove the copy is identical to the original.
3. Collection	To physically and logically acquire the evidence while maintaining its integrity.	Transport the device in a secure, static-free bag. Document every person who handles the evidence.	**Chain of Custody** is meticulously logged to prove the evidence has not been tampered with.
4. Forensic Examination	To analyze the digital evidence and extract relevant information.	Use specialized forensic software to search for and recover deleted files, chat logs, browser history, and metadata.	The examination must be repeatable and follow accepted scientific methods.
5. Reporting	To document the findings of the forensic examination in a clear, concise, and objective manner.	Write a comprehensive report detailing the steps taken, tools used, and all relevant findings. Use clear language and avoid jargon.	The report must be truthful, impartial, and signed by a qualified expert.
6. Witness Testimony	To present the findings in court and explain the technical and legal significance of the evidence.	The forensic examiner is called to testify as an **Expert Witness**. They must explain the entire process from collection to analysis.	The witness must be qualified to testify, and their testimony must be based on reliable scientific methods. The defense attorney will cross-examine the witness on the reliability of the tools and methods used.

Source: *@ Author*[406]

[406] Dr. Shree Krishna Bhattarai, Key Stages of Digital Evidence Handling: A Technical and Legal Overview (generated by Google Gemini, https://gemini.google.com/app/eb85ec06ab4863eb, Sept. 2, 2025) (on file with author).

6. The Path Forward: Building a Cyber-Proficient Legal Ecosystem

Building a cyber-efficient legal ecosystem requires a holistic approach. To regain integrity and public confidence in the legal system, this entails educating all parties involved, purchasing cutting-edge digital forensic equipment, and amending legislation to address cybercrime and digital evidence.

A. Legislative Reform

Adopting a comprehensive Digital Evidence Act is the first and most important step. This action needs to:

- Give precise definitions of digital and electronic evidence.
- Set up legal protocols for its identification, preservation, gathering, collection, storage, and display.
- Explain the best evidence rule, hearsay, and authentication regulations in the context of digital media.
- Require forensic labs to be accredited in accordance with ISO 17025.

A strong Data Protection Act must be passed quickly to go along with this. This act is crucial for safeguarding individual privacy, regulating data collection and use, and holding entities accountable for breaches.

B. Institutional Reform

An independent National Digital Forensics Laboratory that satisfies ISO 17025 requirements must be established by the government. To maintain its impartiality and meet the interests of all parties involved—prosecution, defense, and civil litigation—this lab need to be under the jurisdiction of the judiciary or another neutral organization rather than the police.

C. Human Resource Development: Mandatory Cyber Proficiency

The most important long-term investment is this one.

i) **For Judges:** Even while hearing matters other than those classified as cybercrime, all judges, from the District Court to the Supreme Court, must be cyber experts. As a fundamental human right, the litigant must have the right to have a highly qualified and experienced judge decide their case. Cyber specialist judges should be hired from the legal field if there aren't enough expert judges available. The National Judicial Academy (NJA) and other national and international training providers should mandate that all judges attend ongoing, mandatory training sessions on digital evidence if these measures prove insufficient. Technical foundations, legal admissibility principles, and hands-on experience assessing digital evidence should all be covered in this curriculum. Additionally, each court has to appoint judges with cyber knowledge and establish dedicated cyber benches.

ii) **For Lawyers:** For license renewal, the Nepal Bar Council must require continuous legal education (CLE) on digital evidence. Regular workshops and seminars on this subject should be held by bar associations, such as the Kathmandu District Court Bar Association.

iii) **For Investigators:** hrough demanding training and certification programs, the Nepal Police and other investigating agencies must cultivate a cadre of cyber-specialist investigators. All police training programs must include instruction on how to preserve digital evidence.

7. Conclusion: A Mandate for Modernization

Nepal's legal and judicial system has to be fundamentally reevaluated in light of the widespread incorporation of digital evidence into every aspect of contemporary litigation. As this article has shown, a systemic lack of cyber-literacy among important stakeholders—from judges to first responders and litigators—endangers the integrity of the evidence, compromises due process, and eventually erodes public confidence in the legal system. Legal ambiguity and unfair results result from the current legal system's reliance on antiquated laws like the Electronic Transactions Act, 2063, which is unable to handle the complexity of a digitally first society.

A thorough and multidimensional approach is necessary to close this crucial digital divide. The underlying legal procedures for a cyber-aware justice must be provided by legislative change, starting with the passage of a strong Data Protection Act and a specific Digital Evidence Act. At the same time, it is imperative to make a significant investment in human resource development, which includes hiring judges with cyber-savvy skills and requiring ongoing training for all legal professionals. The accreditation of digital forensic labs and the creation of dedicated cyber benches would strengthen the legal system's ability to handle matters involving complicated technology. Nepal can preserve its constitutional commitment to a just and equitable society and guarantee that the search for justice and the truth always comes first by proactively creating a cyber-proficient legal ecosystem.

References:

David Cole, Technology & Crime: How Digital Evidence Is Changing Criminal Trials, David Cole Lawyer (July 3, 2022), https://www.davidcolelawyer.com.au/technology-and-crime-digital-evidence-changing-criminal-trials.html.

Electronic Transactions Act (Cap. 88) (Singapore), https://www.jonesday.com/en/insights/2021/02/singapores-electronic-transactions-act-expanded (last visited Sept. 1, 2025).

Uniform Electronic Transactions Act § 47-10-101 et seq. (Tenn.), https://www.ctas.tennessee.edu/eli/uniform-electronic-transactions-act (last visited Sept. 1, 2025).

Evidence (Second Amendment) Act, 2077 BS (Nepal), https://hrjc.org.np/wp-content/uploads/2025/01/report-advocating-chain-of-custody-and-governance-of-digital-evidence-in-nepal.pdf (last visited Sept. 1, 2025).

Electronic Transactions Act, 2063 (Nepal) § 4, https://lawcommission.gov.np/content/13397/electronic--electronic--traded-international-act--2063/ (last visited Sept. 1, 2025).

National Forensic Science Laboratory, https://forensic.gov.np (last visited Aug. 15, 2025).

Nepal Police Central Forensic Science Laboratory, https://forensic.nepalpolice.gov.np/about-us/introduction/ (last visited Aug. 15, 2025).

Cyber Crime Investigation Unit, Annual Factsheet on Suicide & Cyber Crime: Fiscal Year 2080/81 (2024), Nepal Police Headquarters, Crime Investigation Department, https://www.nepalpolice.gov.np/media/filer_public/fd/3e/fd3e1c95-aaa1-41bd-815e-0221254141d4/fy_2080-81_suicide__cyber_crime_-_en.pdf (last visited Aug. 16, 2025).

Dr. Shree Krishna Bhattarai, defense attorney in Government of Nepal v. Sunil Rai, Case No. 081-C1-0786 (sub judice), based on personal forensic analysis performed on the digital media submitted by Digital Forensics Examiners, identifying use of outdated forensic software versions including Atola Technology's Insight Forensic v5.6.9102.18310 and Magnet AXIOM v8.8.042722 (expired April 2022).

Evidence Act, 2031, §§ 18, 25, Nepal Law Commission, https://lawcommission.gov.np/path-to-act (last visited Sept. 2, 2025).

Criminal Procedure Code, 2074, §§ 6, 7, 8, 10, 18, 19, 21, 23, 26, 31, 32, 38, 99, 102, Nepal Law Comm'n, https://lawcommission.gov.np/content/13458/civil-criminal-procedure-code-2074/ (last visited Sept. 2, 2025).

Dr. Shree Krishna Bhattarai, Key Stages of Digital Evidence Handling: A Technical and Legal Overview (generated by Google Gemini, https://gemini.google.com/app/eb85ec06ab4863eb, Sept. 2, 2025) (on file with author).