Lex Scientia Law Review
Vol. 8 Issue 1 (2024) 355–384
DOI: https://doi.org/10.15294/lslr.v8i1.2952
Online since: September 22, 2024

LEX SCIENTIA LAW REVIEW
https://journal.unnes.ac.id/journals/lslr/index

The Legal Position of Digital Forensic Experts in the Settlement of Information Technology Crime Cases

Indriati Amarini [a]✉, Rizky Aulia Cahyadri [b], Maulida Ayu Fitriani [c], Noorfajri Ismail [d]

[a] Faculty of Law, Universitas Muhammadiyah Purwokerto, Indonesia
[b] District Court Sangatta, East Kalimantan, Indonesia
[c] Faculty of Engineering and Science, Universitas Muhammadiyah Purwokerto, Indonesia
[d] Faculty of Syariah and Law, Universitas Sains Islam Malaysia, Negeri Sembilan, Malaysia

✉ Corresponding email: indriatiamarini@ump.ac.id

Abstract

Digital forensic expert testimony is required by judges to resolve cases related to information technology. However, there are allegations of violations committed by certain parties on several servers such as illegal access, configuration changes, and shutdowns. This is increased by the destruction of crime scene and digital evidence. In some cases, analyzing the data collected can be time-consuming, and practical understanding is needed by judges to avoid irrelevant questions for digital forensic experts in court. Therefore, this research aims to determine and analyze forensic digital experts in court hearings, the duties and roles of judges in resolving information and technology cases as well as the position of

forensic experts in the judicial process. The doctrinal research is sourced from secondary data in the form of Electronic Information and Transaction laws, criminal procedure laws, research reports, books, and scientific journals. The results show that digital forensics expert testimony is needed to assist judges as gatekeepers in obtaining material truth. Practical digital forensic knowledge is used to increase the efficiency of case examination time by avoiding irrelevant questions. Best practices are used in the actions, procedures, handling, and analysis of electronic evidence as well as digital forensic expert testimony in judicial practice.

KEYWORDS *Digital forensic, Expert Witnesses, Court*

Introduction

The development of the use of information technology is very rapid. The widespread integration of computers across diverse aspects of human life increases the negative impacts, specifically the exploitation for illicit purposes. Technology crime, also known as cybercrime, encompasses a wide range of illegal activities conducted through the internet and other forms of digital communication. There are two main types of cybercrime that can be distinguished based on the method of attack. There are two main categories of cybercrime that organizations should be aware of in order to properly allocate resources and responsibilities. The first category is cyber-enabled crime, which involves traditional crimes that are magnified or extended through the use of digital technology. The second category is cyber-dependent crime, which involves offenses that require the use of digital technology and are typically targeted towards computers or systems that store valuable information. Understanding the distinctions between these two categories is crucial for organizations to effectively combat cyber threats.[1]

Here are some notable cases in the realm of technology crime: (1) The Yahoo Data Breach in 2013-2014. One of the largest data breaches in history, where hackers stole data associated with all 3 billion Yahoo user accounts. Personal information, including names, email addresses, telephone numbers, dates of birth, and security questions, was compromised (2) The Equifax Data Breach in 2017. A breach that exposed the personal information of 147 million

[1] Paul Reedy, *Strategic Leadership in Digital EvidenceWhat Executives Need to Know* (Academic Press, 2020), https://doi.org/https://doi.org/10.1016/C2018-0-05426-2.

people, including Social Security numbers, birth dates, and addresses. The breach highlighted vulnerabilities in the credit reporting industry and led to widespread concerns about identity theft (3) The WannaCry Ransomware Attack in 2017. A global ransomware attack that affected over 200,000 computers across 150 countries, encrypting files and demanding ransom payments in Bitcoin (4) The Ashley Madison Breach in 2015. Hackers released personal information of users of Ashley Madison, a website designed for extramarital affairs. The breach exposed the personal details of millions of users, leading to public embarrassment, personal fallout, and even reports of suicides linked to the breach. These cases highlight the diverse and evolving nature of cybercrime, demonstrating the need for robust cybersecurity measures and international cooperation to combat these threats effectively.

In recent years, the proliferation of technological advancements has become so commonplace that a remarkable 53.7% of Indonesia's citizens now regularly access the internet.[2] Technology crime, often referred to as cybercrime, has been a significant issue in Indonesia, mirroring global trends. These crimes encompass a wide range of illegal activities involving computers and networks. Here are some notable cases and trends in technology crime in Indonesia: (1) Phishing and Online Scams. Case of Fake E-commerce Websites: Numerous instances have been reported where criminals set up fake e-commerce websites to steal personal and financial information from unsuspecting shoppers. These websites often mimic legitimate businesses. (2) Investment Scams: Investment fraud, including Ponzi schemes and fake cryptocurrency investments, has been prevalent. Criminals use social media and fake endorsements to lure victims. (3) Hacking and Data Breaches. One of the largest data breaches in Indonesia involved Tokopedia, a major e-commerce platform. Hackers reportedly accessed data of over 91 million users, including email addresses and hashed passwords. Another significant breach affected Bukalapak, with the personal data of millions of users compromised. These breaches raise concerns about data security practices in Indonesian companies. (4) Corporate Attacks: Indonesian businesses across various sectors have faced ransomware attacks, leading to operational disruptions and financial losses. (5) Online Fraud and Identity Theft. ATM Skimming: Although not entirely a cybercrime, ATM skimming involves using technology to steal card information. Skimmers install hidden devices on ATMs to capture card details, which are then used for fraudulent transactions. (6) SIM Card Swaps: Criminals use social engineering to convince

[2] Ismail Hamzah et al., "Methods to Prevent Privacy Violations on the Internet on the Personal Level in Indonesia," *Procedia Computer Science* 216 (2022): 650–54, https://doi.org/https://doi.org/10.1016/j.procs.2022.12.180.

mobile operators to transfer a victim's phone number to a new SIM card, which is then used to gain access to the victim's online accounts. (7) Illegal Content and Cyber Defamation. Defamation and Hate Speech: With the rise of social media, cases of online defamation and hate speech have increased.

Technology crime in Indonesia reflects global trends, with significant challenges posed by data breaches, online fraud, and ransomware. Indonesian law enforcement actively monitors and prosecutes such offenses under the Information and Electronic Transactions Act (UU ITE) (1) Distribution of Illegal Content: Cases involving the distribution of pornography and other illegal content are also prosecuted under UU ITE. (2) Cryptojacking. Unauthorized Mining: There have been instances of cryptojacking, where attackers secretly use a victim's computing resources to mine cryptocurrencies. This can slow down systems and increase electricity costs. (3) Digital Payment Fraud. E-Wallet Frauds: As digital payment systems grow in popularity, so do fraud schemes targetting e-wallet users. Criminals exploit security loopholes or use phishing techniques to steal funds from users' accounts.

In this context, the assurance of the credibility and soundness of electronic evidence necessitates substantiation by professionals in digital forensics. The analysis of electronic evidence in guaranteeing reliability and validity serves as the main key in handling electronic evidence within judicial practice

The rapid advancements in technology necessitate that law enforcement agencies keep pace with the evolving landscape of digital forensics. As technology continues to permeate all aspects of society, traditional crime scenes have expanded to include a combination of physical and virtual elements, requiring law enforcement to adapt their investigative techniques. The use of smart homes, infrastructure, factories, and cities as sources of evidence has become common, leading to a shift in the way investigations are conducted. The field of digital forensics has seen significant growth within the criminal justice system, with a notable increase in both the quantity and complexity of forensic evidence.[3]

The justice system has witnessed a rapid increase in digital evidence since the introduction of forensic science, leading to a rise in the amount and complexity of forensic evidence.[4] The introduction of forensic science has led to a rapid growth in digital evidence within the justice system. Additionally,

---

[3] Johannes Fähndrich et al., "Digital Forensics and Strong AI: A Structured Literature Review," *Forensic Science International: Digital Investigation* 46 (2023), https://doi.org/https://doi.org/10.1016/j.fsidi.2023.301617.

[4] Paul Reedy, "Artificial Intelligence in Digital Forensics," *Encyclopedia of Forensic Sciences, Third Edition* 1 (2023): 170–92, https://doi.org/https://doi.org/10.1016/B978-0-12-823677-2.00236-1.

there has been a notable increase in the amount and complexity of forensic evidence. As outlined in Article 5 of Law Number 11 of 2008 concerning Electronic Information and Transactions, electronic information and documents are considered a form of legal evidence. This indicates that digital evidence presented in criminal court can be deemed admissible and valid.[5]

Digital forensic investigations play a crucial role in ensuring justice is achieved by providing reliable results. However, the trustworthiness of these investigations is often taken for granted and not thoroughly examined. Failure to accurately assess the trustworthiness of an investigation can lead to decreased reliability of results and erode trust from external parties. Instances of misconduct in investigations are not regularly detected, highlighting the susceptibility of digital forensic investigations to allegations of wrongdoing. In cases where expert witnesses breach their duties in court, they may face disciplinary action or even criminal charges for contempt of court. A recent legal case has established guidelines for sentencing experts found guilty of contempt, including the possibility of imprisonment.[6]

Digital Forensics has an important role in criminal investigations, and the process must be supported by a well-defined and strong methodology. A significant amount of research has defined and codified digital forensic investigation process and the stages. Even though current models of digital forensic investigation process offer a strong framework, prevailing efforts predominantly concentrate on the tangible tasks executed at each stage of the examination. However, the fundamental cognitive processes, discernments, and behaviors integral to proficient investigative practice are not often considered.[7] The widespread use of information and communication technology provides access to all activities, and users with malicious tendencies can also be attracted to commit old crimes. This has led to an increasing need for digital forensic results by case investigators, prosecutors, lawyers, and judges.[8]

---

[5] Bagus Pribadi, Sri Rosdiana, and Samsul Arifin, "Digital Forensics on Facebook Messenger Application in an Android Smartphone Based on NIST SP 800-101 R1 to Reveal Digital Crime Cases," *Procedia Computer Science* 216 (2023): 161–67, https://doi.org/10.1016/j.procs.2022.12.123.

[6] N V Todd, "Expert Witnesses, Contempt of Court and Custodial Sentencing," *The Bulletin of the Royal College of Surgeons of England* 102, no. 1 (December 31, 2019): 34–36, https://doi.org/10.1308/rcsbull.2020.34.

[7] Graeme Horsman and Nina Sunde, "Unboxing the Digital Forensic Investigation Process," *Science & Justice* 62, no. 2 (2022): 171–80, https://doi.org/https://doi.org/10.1016/j.scijus.2022.01.002.

[8] H M A van Beek et al., "Digital Forensics as a Service: Stepping up the Game," *Forensic Science International: Digital Investigation* 35 (2020): 301021, https://doi.org/https://doi.org/10.1016/j.fsidi.2020.301021.

The exponential expansion of the Internet and cyberspace has resulted in an increase in malicious behavior. In this regard, digital forensics plays a crucial role in uncovering the activities that occur on a compromised system. This process involves three key stages: acquisition, analysis, and presentation. However, there are significant challenges in digital forensic analysis, such as dealing with the vast amount of data collected and the absence of automated techniques. In some instances, it may take days or even weeks to analyze the data collected.[9] Given that the law is intricately linked to the evolving landscape of technology, legal professionals must stay abreast of the rapid advancements in information technology.[10]

Judges typically possess specialized knowledge within the respective fields rather than comprehensive expertise across all domains. Despite the proficiency, certain intricacies may not be fully understood due to the inherent limitations of individual understanding. Martiman Prodjohamidjojo states that a judge may not reject case even though the law or statute does not regulate the process as a principle in the judiciary. Therefore, the testimony of an expert is needed to gain in-depth knowledge about a matter since the judge is not considered to know everything. The principle of ius curia novit contains the spirit that must be possessed by a judge in line with the development of society.[11]

The rise in the use of digital devices, along with their varying types, has resulted in a surge in the amount of different types of data being used in criminal or civil investigations. This increase in large digital forensic data has required professionals to expand their efforts to collect a broader range of devices and gather larger amounts of data related to the case being examined. As a result, law enforcement agencies globally are facing a significant backlog of cases.[12]

This research focuses on normative legal research,[13] which is doctrinal research to find positive legal materials used to develop theories and solve

---

[9] Somayeh Soltani and Seyed Amin Hosseini Seno, "Detecting the Software Usage on a Compromised System: A Triage Solution for Digital Forensics," *Forensic Science International: Digital Investigation* 44 (2023): 301484, https://doi.org/https://doi.org/10.1016/j.fsidi.2022.301484.

[10] Amran Suadi, *Sosiologi Hukum: Penegakan, Realitas Dan Nilai Moralitas Hukum* (Jakarta: Prenada Media, 2018).

[11] Benget Hasudungan Simatupang, "Alat Bukti Keterangan Ahli Hukum Pidana Dalam Proses Pemeriksaan Perkara Pidana," *Ensiklopedia Sosial Review* 2, no. 3 (2020): 304–13, https://doi.org/https://doi.org/10.33559/esr.v2i3.637.

[12] Brandon L Garrett et al., "Judges and Forensic Science Education: A National Survey," *Forensic Science International* 321 (2021): 110714, https://doi.org/https://doi.org/10.1016/j.forsciint.2021.110714.

[13] Sholahuddin Al-Fatih and Ahmad Siboy, "Menulis Artikel Karya Ilmiah Hukum Di Jurnal Nasional Dan Internasional Bereputasi," *Inteligensia Media*, 2021.

existing problems. Legal principles, doctrines, and concepts as well as legislation relating to information and technology are evaluated as criminal procedure law. As an initial step, a review is conducted to identify regulations relating to digital forensic expert witnesses in court practice. This step is used to analyze the position of digital forensics in resolving information and technology cases.

Digital Forensic Expert in Court

A digital forensic expert is indispensable in the contemporary legal landscape, bridging the gap between complex technical data and legal standards. Their work ensures that digital evidence is properly handled and accurately interpreted, ultimately contributing to the administration of justice. A digital forensic expert plays a crucial role in the legal system, particularly in cases involving digital evidence. Their expertise ensures that electronic data is collected, preserved, analyzed, and presented in a manner that is legally sound and scientifically reliable.

As the field of digital forensics remains vital in criminal investigations, it is crucial for its investigative processes to be supported by clearly outlined and strong methodologies.[14] Here are the key responsibilities and functions of a digital forensic expert in court:

1. Evidence Collection and Preservation:
   a. Acquisition: The expert is responsible for acquiring data from various digital devices (computers, smartphones, servers, etc.) while ensuring the integrity of the data. This process often involves creating bit-by-bit copies of digital storage devices.
   b. Preservation: Ensuring that the evidence is preserved in its original state. This includes maintaining a proper chain of custody to avoid any allegations of tampering or contamination.
2. Analysis:
   a. Data Recovery: The expert uses specialized tools and techniques to recover deleted, hidden, or encrypted data that may be relevant to the case.
   b. Metadata Analysis: Analyzing metadata to determine the origin, authorship, and timeline of the digital documents or communications.
   c. Log Analysis: Reviewing system and application logs to understand the activities performed on a device.
3. Interpretation:
   a. Contextual Understanding: Interpreting the data in the context of the case. This might involve linking the digital evidence to the actions of the individuals involved.

[14] Horsman and Sunde, "Unboxing the Digital Forensic Investigation Process."

b. Reconstruction: Reconstructing digital events to provide a narrative that can be understood by the court. This might include timelines of events or detailed explanations of the digital interactions that took place.

4. Expert Testimony:
   a. Communication: Presenting complex technical findings in a clear and understandable manner to the court, often through both written reports and verbal testimony.
   b. Credibility: Providing an unbiased and objective interpretation of the digital evidence. The expert's credibility is paramount, as their testimony can significantly influence the outcome of the case.
5. Cross-Examination:
   a. Defense Scrutiny: The expert must be prepared to withstand cross-examination by the defense, addressing challenges to their methods, findings, and conclusions.
   b. Clarification: Clarifying any technical aspects that may be misunderstood or misrepresented during the cross-examination.
6. Legal Compliance and Ethics:
   a. Adherence to Standards: Ensuring that all forensic processes adhere to established legal and ethical standards, such as those set by organizations like the International Association of Computer Investigative Specialists (IACIS) or the National Institute of Standards and Technology (NIST).
   b. Continued Education: Staying updated with the latest developments in digital forensics to maintain competency and credibility in court.
7. Importance in Legal Proceedings
   The role of a digital forensic expert is critical in modern legal proceedings due to the increasing reliance on digital evidence in both criminal and civil cases. They provide the technical expertise needed to understand and validate digital evidence, thereby aiding the court in delivering a fair and informed judgment.
8. Validation of Evidence: Ensuring that digital evidence presented in court is reliable and has not been tampered with.
   a. Support for Prosecution or Defense: Providing crucial evidence that can support the arguments of either the prosecution or the defense.
   b. Educating the Court: Helping judges and juries understand the technical aspects of the evidence, which is essential for making informed decisions.

Digital forensics has gained significant importance in the fields of criminal justice and law enforcement due to its role as a crucial form of evidence. As technology, databases, and information systems continue to advance, digital forensics has become an indispensable tool in both investigative and legal procedures. The confidentiality of digital evidence is a nuanced and ever-

changing concept, often necessitating the expertise of professionals to understand its relevance in investigations.[15]

Digital forensics, a branch of science that deals with crimes involving computer technology, involves the use of specialized procedures and techniques in cybercrime investigations that must be admissible in court. The main goal of these procedures is to determine the source of an incident and ensure the integrity of evidence. Additionally, the process of tracing digital evidence has become crucial in mapping out the sequence of events from various sources to gather evidence for further analysis.[16]

In legal proceedings, expert testimony plays a crucial role in providing specialized information or clarification that may be beyond the judge's knowledge. This is necessary for delving into the intricate details of a case and ensuring a comprehensive analysis in court. At the same time, the constantly evolving landscape of information and communication technologies, along with the interconnected nature of cyberinfrastructure, present new obstacles for security experts and law enforcement agencies. The upcoming challenges and advancements in digital forensics are examined, with a focus on the measures needed to safeguard society and combat cybercrime effectively.[17]

Digital forensics involves using scientific tools and techniques to gather and examine data that can be used as evidence in legal cases. On a more technical level, it involves piecing together the events that led to the current state of an information technology system. As technology has become more prevalent, the need for digital forensics has increased due to the vast amount of data being generated.[18]

The fields of cybersecurity and digital forensics are intricately linked to the legal proceedings of today and tomorrow, as the use of digital evidence continues to grow in significance within criminal trials. Digital forensics is not only essential in cybersecurity, but also in various everyday criminal cases such as car theft, drug offenses, and traditional forms of organized crime. Moreover,

---

[15] John Kwaku Oppong, "Evidence Confidentiality and Digital Forensic Experts," *Research Nexus in IT, Law, Cyber Security & Forensics* 1, no. 1 (2022): 161–66, https://doi.org/https://dx.doi.org/10.22624/aims/crp-bk3-p26.

[16] Siti Rahayu Selamat et al., "Traceability in Digital Forensic Investigation Process," in *2011 IEEE Conference on Open Systems (ICOS2011)*, 2011, 101–6, https://doi.org/10.1109/ICOS.2011.6079259.

[17] Luca Caviglione, Steffen Wendzel, and Wojciech Mazurczyk, "The Future of Digital Forensics: Challenges and the Road Ahead," *IEEE Security & Privacy* 15, no. 6 (2017): 12–17, https://doi.org/10.1109/MSP.2017.4251117.

[18] Vassil Roussev, "Issues, Methods, and Challenges," in *Digital Forensic Science* (Springer Cham, 2017), https://doi.org/https://doi.org/10.1007/978-3-031-02351-4.

it plays a crucial role in aiding judicial decision-making by providing experts with valuable traces and data to support their arguments in court. Consequently, the presentation of digital data as evidence in criminal trials has become a routine and technically straightforward process.[19]

An Expert's responsibility is to provide technical information supporting the argument of the lawyer or prosecutor.[20] Impartiality means that the experts work under scientific principles and legal procedures in assisting the trier of fact. The concept of expert impartiality encompasses both individual and industry perspectives. Experts are expected to maintain high personal standards, such as avoiding irrelevant information, utilizing reliable methods, conducting thorough analysis, and presenting findings in a comprehensive manner. Additionally, adherence to forensic science standards regarding technical requirements, laboratory management, and professional conduct is essential. Failure to maintain impartiality can lead to biased expert witnesses, which can compromise the integrity of the legal process and impede the objectives of assisting the trier of fact.[21]

Expert testimony is needed to clarify a problem that cannot be answered by the judge. Considering the importance, the testimony must be provided freely and protected from all legal actions.[22] Experts have a special place in court, bringing knowledge and skills in the form of opinion evidence. This allows fact-finders to make more effective legal decisions and experts are often allowed to play a role in civil and criminal matters.[23]

The field of digital investigations must constantly evolve to combat information technology crimes and bring offenders to justice, all while working alongside international partners to share knowledge and strategies for prevention. The Cyber Forensics in Digital Ecosystem Model provides a

---

[19] Uwe Ewald, "Digital Forensics vs. Due Process: Conflicting Standards or Complementary Approaches?," in *CECC 2019: Proceedings of the Third Central European Cybersecurity Conference*, 2019, 1–2, https://doi.org/https://doi.org/10.1145/3360664.3362697.

[20] Oren Masory, "From Litigation Consulting to Research and Education," in *17 Th LACCEI International Multi-Conference for Engineering, Education, and Technology*, 2019, https://doi.org/https://doi.org/10.18687/laccei2019.1.1.250.

[21] Mingxiao Du, "Legal Control of Expert Witness Bias," *The International Journal of Evidence & Proof* 21, no. 1–2 (December 29, 2016): 69–78, https://doi.org/10.1177/1365712716674798.

[22] Indriati Amarini and Ratna Kartikawati, "Strengthening the Position of Expert Witness in Judicial Process," *Jurnal Media Hukum* 27, no. 1 (2020): 44–54, https://doi.org/https://doi.org/10.18196/jmh.20200141.

[23] Brad D Booth, Joel Watts, and Mathieu Dufour, "Lessons from Canadian Courts for All Expert Witnesses.," *The Journal of the American Academy of Psychiatry and the Law* 47, no. 3 (May 16, 2019): 278–85, https://doi.org/https://doi.org/10.29158/JAAPL.003838-19.

comprehensive framework for navigating the complexities of today's technology landscape. It is essential to stay up-to-date with advancements in forensic tools and techniques, as well as to collaborate with others in the global Digital Forensics community to effectively gather digital evidence, enforce cybersecurity policies, prevent security threats, counter anti-forensic practices, and prosecute cyber criminals. It is crucial to adapt and improve current practices in order to effectively combat cybercrime and stay ahead in the ever-changing technological landscape.[24] Moreover, there has been a significant increase in the amount of evidence gathered through digital forensic investigations in recent years. Experts in this field are forecasting a surge in ransomware attacks in the near future, which will require the legal community to be equipped to handle the growing volume and intricacy of these cases.[25]

Duties and Role of Judges in Resolving Information and Technology Cases

Judges play a critical role in resolving information and technology (IT) cases, which often involve complex technical issues and rapidly evolving legal landscapes. Judges in IT cases must combine a deep understanding of technical issues with strong legal acumen, balancing various interests to ensure fair and just outcomes while keeping pace with the rapidly evolving technological landscape. Their duties and roles can be broadly categorized as follows:

1. Understanding Technical Complexities
   Acquiring Technical Knowledge: Judges need to familiarize themselves with the technical aspects of the cases they preside over. This may involve understanding the nuances of software, hardware, data management, cybersecurity, and other IT-related fields.
   Expert Testimony: They must evaluate expert testimonies from IT professionals, assessing the credibility and relevance of the technical evidence presented.
2. Legal Interpretation and Application
   Interpreting Laws and Regulations: Judges interpret and apply existing laws and regulations to IT cases, including intellectual property law, data protection regulations, cybersecurity laws, and digital rights.

---

[24] Regner Sabillon et al., "Digital Forensic Analysis of Cybercrimes: Best Practices and Methodologies," *International Journal of Information Security and Privacy* 11, no. 2 (2017): 25–37, https://doi.org/https://doi.org/10.4018/IJISP.2017040103.

[25] Hans Henseler and Sophie van Loenhout, "Educating Judges, Prosecutors and Lawyers in the Use of Digital Forensic Experts," *Digital Investigation* 24 (2018): S76–82, https://doi.org/https://doi.org/10.1016/j.diin.2018.01.010.

Precedent and Case Law: They consider precedent and relevant case law, ensuring that their rulings align with established legal principles and contribute to the development of IT jurisprudence.

3. Balancing Interests
   Privacy vs. Security: Judges often have to balance the right to privacy with the need for security, particularly in cases involving data breaches or government surveillance.
   Innovation vs. Regulation: They must weigh the benefits of technological innovation against the need for regulatory oversight to protect consumers and ensure fair competition.
4. Ensuring Fair Process
   Due Process: Ensuring that all parties receive a fair hearing, with adequate opportunities to present their case and respond to opposing arguments.
   Impartiality and Objectivity: Judges must remain impartial and objective, making decisions based solely on the evidence and legal arguments presented.
5. Adjudicating on Specific Issues
   Intellectual Property Disputes: Resolving disputes related to patents, copyrights, trademarks, and trade secrets in the IT sector.
   Data Protection and Privacy: Adjudicating cases involving data breaches, misuse of personal data, and compliance with data protection laws such as GDPR or CCPA.
   Cybercrime: Addressing issues related to cybercrimes, such as hacking, identity theft, and online fraud.
   Contract Disputes: Settling conflicts arising from IT contracts, including software licensing agreements, service level agreements, and development contracts.
6. Staying Informed on Evolving Technologies
   Continuing Education: Judges often participate in continuing education programs to stay informed about the latest technological advancements and their legal implications.
   Collaboration with Technical Experts: They may collaborate with technical experts and legal scholars to better understand and address the challenges posed by new technologies.
7. Public Policy and Ethical Considerations
   Policy Implications: Judges consider the broader policy implications of their decisions, particularly how they might influence future technological development and regulation.
   Ethical Considerations: Addressing ethical issues related to technology, such as the impact of AI on employment, bias in algorithms, and the ethical use of data.

8. Crafting Appropriate Remedies

   Injunctions and Damages: Judges determine appropriate remedies, which may include injunctions to prevent further harm, monetary damages, or specific performance to fulfill contractual obligations.

   Enforcement: Ensuring that their rulings are effectively enforced, which may involve overseeing compliance with court orders.

Experts provide evidence outside court and enable specialized knowledge to be understood by the judge. The primary duty of providing opinions to court and not to the party. Experts may be held in contempt or face criminal sanctions when misleading court and these individuals should also declare no conflict of interest from the outset of case.[26] Experts in criminal, civil, and social cases have to present opinions in court and this aspect should not be viewed solely as a burden, despite occasional feelings of overwhelm experienced by the expert. The instances may arise when discussions reiterate articulated opinions or questions appear biased against the perspective. However, the expert is advised to appear calm and objective during questioning by the judge and the parties or participants, and should not be provoked by questions.[27]

The recent development of Information Communication Technology has made changes in every aspect of life. The positive influence of cyberspace on knowledge, trade, business, and communication is unquestionable. However, there is a dark side to cyberspace that undermines its peaceful use. Cybercrime is defined as any illegal activity conducted through cyberspace and the electronic environment. Unlike "traditional" crimes, it presents a real dilemma because the identity of the perpetrator can be hidden. The concept of digital forensics has been developed as an attempt to formulate possible ways for the investigation and analysis of cybercrime. The advancements in information technology have significantly increased the significance of digital evidence in both criminal and civil cases. In order for this evidence to be admissible in court, it must be accurate, reliable, and verifiable, which is why accreditation is crucial to ensuring its validity.[28]

---

[26] John Reynard, "Being an Expert Witness," in *Medicolegal Issues in Obstetrics and Gynaecology*, ed. Swati Jha and Emma Ferriman (Cham: Springer International Publishing, 2018), 51–54, https://doi.org/10.1007/978-3-319-78683-4_10.

[27] Marcus Schiltenwolf, Nickolas Beckmann, and Peter Gaidzik, "Erörterung Eines Sachverständigengutachtens Vor Gericht Und Die Haftung Des Sachverständigen [Expert Opinions in Court: Liability of the Expert]," *Z Orthop Unfall* 155, no. 6 (2017): 727–31, https://doi.org/10.1055/s-0043-116798.

[28] Schiltenwolf, Beckmann, and Gaidzik; Hong Guo and Junlei Hou, "Review of the Accreditation of Digital Forensics in China," *Forensic Sciences Research* 3, no. 3 (July 3, 2018): 194–201, https://doi.org/10.1080/20961790.2018.1503526.

A judge is required to hear and decide on a case even if the law is unclear or does not exist. Furthermore, judges are expected to be well-versed in the law in order to provide fair and just legal resolutions, adhering to principles such as propriety, legal certainty, and justice.[29] The law is also understood through the principle of curia novit, which describes the spirit of a judge willing to follow developments in the world of law and society. As technology advances at an increasing pace, society becomes connected with the use of information and communication technology. Therefore, courtroom settings experience an increase in the presentation of digital data, traces, and electronic evidence. Technological advancements pervade every sector and domain, with particular prominence in the international arena. Numerous Best Practices have been crafted and put into effect, governing actions, procedures, and the meticulous handling and analysis of electronic evidence provided by Digital Forensics Experts during trials.

With the spirit of ius curia novit, there is only one answer to the current conditions of society in digital world, where a judge must learn and follow developments in information technology. Current laws and regulations do not provide special prerequisites for someone to be considered an expert and able to provide information. The important thing for a judge to ask digital forensic expert is regarding the Code of Ethics for Digital Forensic Expert Witnesses. The code of ethics is understood as a "convention among professionals", which has the aim of protecting professionals from pressures and providing collective recognition of responsibilities.[30]

Different countries have varying legal frameworks that define the role and responsibilities of digital forensic experts. For example, in the U.S., the Federal Rules of Evidence provide guidelines for the admissibility of expert testimony. International Guidelines: International bodies such as the International Organization for Standardization (ISO) provide guidelines (e.g., ISO/IEC 27037) for the identification, collection, and preservation of digital evidence. Codes of Ethics are established by organizations or institutions that oversee a profession in providing accreditation or certification for a field of expertise. Therefore, in international practice, there are many Codes of Ethics for Digital Forensics Experts, depending on the organization overseeing the profession. A common thread can be identified as the basic idea of the Code of Ethics or

---

[29] Muhidin et al., "Implementation of The Ius Curia Novit Principle in Examining Case At The Constitutional Court of The Republic of Indonesia," *Baltic Journal of Law & Politics* 15, no. 1 (2022): 453–65, https://doi.org/10.2478/bjlp-2022-00030.

[30] Filipo Sharevski, "Rules of Professional Responsibility in Digital Forensics: A Comparative Analysis," *Journal of Digital Forensics, Security, and Law* 10, no. 2 (2015): 39–53, https://doi.org/https://doi.org/10.15394/jdfsl.2015.1201.

Conduct for Digital Forensics Experts. In essence, the purpose is the same in guaranteeing the implementation and provision of guidance.

Understanding the code of ethics serves the vital purpose of furnishing a foundational framework delineating the ethical standards that an Expert Witness must uphold while carrying out duties. For example, in a trial conducted by digital forensics expert, legal practitioner who is reliable should understand the limitations of the opinion provided. The foundational validation of the analytical methodology should be inquired when an expert exceeds these boundaries. The method lacking adequate explanation shows a potential impropriety or ethical violation, demanding a warning in case of the occurrence.

Electronic Information and Documents in legal system are an extension of valid Evidence as regulated in Article 5 paragraphs 1, 2, and 3 of Law Number 11 of 2008 concerning Electronic Information and Transactions. Article 5 of the Provision highlighted the valid evidence, such as:

1. Electronic Information and Documents are valid legal evidence.
2. Electronic Information and Electronic Documents in paragraph (1) are an extension of valid evidence under the Procedural Law in force.
3. Electronic Information and Documents are declared valid when the system is used in accordance with the provisions regulated in the Law

Electronic Information and Documents accepted as valid evidence must meet several requirements based on the nature, form, and content. The formal requirements in Article 5 paragraph (4) of Information and Information Technology Law regulate the invalidity of Electronic Information as valid evidence. According to the law, letters must be made in written form or as a notarial deed. Electronic evidence is unable to prove or cannot be valid evidence when a letter must be in written form or a notarial deed. Article 5 paragraph (4) regulates that the provisions regarding Electronic Information and Documents, as intended in paragraph (1), do not apply to letters that must be made in written form or notarial deed.

Material requirements or conditions relating to the contents of electronic evidence are contained in Article 6 where Electronic Information and Documents must be accessible to electronic evidence. To ensure the fulfillment of material requirements, Digital Forensics Expert is needed to provide information at trial regarding the electronic evidence. Electronic Information and Documents are considered valid in explaining a situation when there are provisions other than those regulated in Article 5 paragraph (4).

Electronic evidence is technological information system and legal view of the criminal procedural form, intended to optimize the processes of collection, registration, and preservation of criminal case material. The development is

aimed at outlining new approaches to organizing the work of investigative and judicial institutions, considering achievements in the field of information technology, and providing new techniques for collecting relevant criminal, procedural-criminological, and significant information. The proposed concept also improves interaction and communication in the service of preliminary investigative bodies with officials of information technology systems to collect evidentiary information.[31] Scientific novelty refers to a systematic change that is observed in the current information society, particularly in relation to the challenges faced in criminal evidentiary law, procedural practices in various sectors, and the utilization of advanced technological tools for information gathering. This new perspective involves the integration of digital technologies to enhance the scientific foundation of evidentiary procedures, with the ultimate goal of streamlining and improving the evidentiary process in criminal investigations.

The formulation of inquiries for digital Forensics Expert by the judge adheres to the stages delineated in Digital Forensics. This method was selected with the intention that the questions are coherent and possibly memorized easily as follows: [32]

(1) Digital Forensics Expert Formalities
The questions begin by first asking about the formalities to ensure that the expert presented is someone who has special expertise in the field of Information Technology. Information must first be requested regarding the formality requirements for an expert. To ensure that the expert presented is someone who has special expertise in the field of Information Technology.

(2) First Time Interacting with Electronic Evidence
The initial interaction with the electronic evidence should be inquired to ascertain the origin and maintain a comprehensive record regarding integrity from the moment of discovery. There are 2 terms in Digital Forensics related to personnel who handle electronic evidence, namely Digital Evidence First Responder (DEFR) and Digital Evidence Specialist (DES). DEFR is someone who is authorized, trained, and qualified to act first at the scene of an incident in collecting and acquiring digital evidence. Meanwhile, DES is someone who can carry out DEFR tasks and has

[31] Anna A Dmitrieva and Pavel S Pastukhov, "Concept of Electronic Evidence in Criminal Legal Procedure," *Journal of Digital Technologies and Law* 1, no. 1 (2023): 270–95, https://doi.org/https://doi.org/10.21202/jdtl.2023.11.

[32] Rizky Aulia Cahyadri, *Apa Yang Harus Ditanyakan Kepada Ahli Digital Forensic? Panduan Bagi Praktisi Hukum* (Yogyakarta: Deepublish, 2021).

special knowledge, skills, and abilities to handle various technical problems.

(3) Identification Stages

Further information regarding the identification stage of electronic devices has the potential to store electronic evidence identified and recorded, including indications that there are hidden or concealed devices. The identification stage includes the process of identifying and searching for digital devices with the possibility of storing electronic evidence. The initial stage obtains all digital devices with the potential to store electronic evidence because the storage can be very small or hidden.

(4) Collection Stages

The collection stage relates to the process of storing electronic evidence which depends on the condition of the device. The stage includes the process of collecting digital devices with the possibility of containing electronic evidence, such as the process of moving digital devices to a laboratory or controlled environment. The primary inquiry revolves around the state of digital device identified as potentially storing electronic evidence in an on or off-state.

(5) Acquisition Stages

The subsequent question relates to the acquisition stage, namely the process of making a copy of electronic evidence similar to the original because electronic evidence is volatile. For evidence analysis, a copy identical to the original is known as a disk or forensic image. The acquisition stage is the process of making a copy of electronic evidence identical to the original. Bringing an entire digital device to trial is impractical and redundant since the crucial focus lies in presenting the electronic evidence contained or stored within the device. Electronic evidence is vulnerable to changes, additions, reductions, or modifications. Therefore, analysis of electronic evidence can be carried out on a copy of the electronic evidence known as a disk or forensic image.

(6) Preservation Stages.

The preservation stage is related to securing electronic evidence and storage to avoid damage or changes.

(7) Analysis Stages.

The final question is related to the stages of analysis, which include the choice of location for analyzing electronic evidence, method used stages, conformity, and Expert's explanation. The stage includes actions carried out by Digital Forensics Experts to examine, research, analyze, and interpret electronic evidence. Questions to Digital Forensics Experts at the Analysis stage ensure that the results are accurate, reliable, and repeatable

or reproducible by other parties. There must be a standard in implementing analytical methods, but new methods can be used because of the very rapid development of Information Technology. In case of using a new method, digital Forensics Expert must be able to explain the relevance of using the method. The results provide insight into the need to facilitate the definition of correct requirements to properly support anticipated investigations.

This information aims to ensure the availability, accessibility, integrity, and accountability of the presented electronic evidence to elucidate a situation or event effectively. By posing pertinent inquiries during the trial, legal practitioners aim to leverage the expertise of an expert witness to show the intricacies of case effectively. After the questions in the analysis stage have been asked, digital forensics expert can be invited to explain the report on the results of examination before the police.[33]

The Position of Digital Forensic Experts in the Criminal Justice Process

Digital forensic experts play a crucial role in the criminal justice process, providing essential expertise in the collection, analysis, and interpretation of digital evidence. Their position and responsibilities span several stages of the criminal justice process.[34]

1. Investigation Stage

   Collection of Evidence: Digital forensic experts are involved in the identification, collection, and preservation of digital evidence from various electronic devices, such as computers, smartphones, and network systems. This includes ensuring that the evidence is collected in a manner that maintains its integrity and admissibility in court.

   Technical Expertise: They use specialized tools and techniques to recover deleted files, decrypt data, and extract information from damaged or encrypted devices. Their technical know-how is crucial for uncovering hidden or obscure evidence.

2. Analysis Stage

   a. Data Examination: Experts analyze the collected data to find relevant information. This includes examining file structures, metadata, logs, and other digital traces that can provide insights into criminal activities.

---

[33] Cahyadri.

[34] Indriati Amarini, *Saksi Ahli Dalam Praktik Peradilan* (Semarang: Saraswati Nitisara, 2019).

b. Pattern Recognition: They identify patterns, such as repeated behaviors or connections between different pieces of digital evidence, which can help build a case against suspects.
c. Reporting: Digital forensic experts compile detailed reports of their findings, which outline the methods used for data recovery and analysis, and present the evidence in a clear and comprehensible manner.

3. Prosecution Stage
   a. Expert Testimony: Digital forensic experts may be called upon to testify in court as expert witnesses. They explain the technical aspects of the evidence, how it was obtained, and its significance to the case. Their testimony can be pivotal in helping the court understand complex digital evidence.
   b. Validation of Evidence: They help validate the authenticity and reliability of digital evidence presented in court, countering claims of tampering or improper handling.
4. Defense Stage
   a. Independent Analysis: Defense attorneys may also employ digital forensic experts to conduct independent analyses of the digital evidence. This can involve verifying the prosecution's findings, uncovering exculpatory evidence, or identifying flaws in the collection and analysis processes.
   b. Challenging Evidence: Defense experts can challenge the methods used by prosecution experts, potentially discrediting improperly collected or analyzed evidence.
5. Judicial Decision-Making Stage
   a. Advising the Court: Judges may consult with digital forensic experts to gain a better understanding of the technical details of the evidence and its implications. This can assist judges in making informed decisions regarding the admissibility and weight of digital evidence.
   b. Key Considerations for Digital Forensic Experts
   c. Chain of Custody: Maintaining a clear and documented chain of custody is essential to ensure that digital evidence is not compromised.
   d. Legal and Ethical Standards: Digital forensic experts must adhere to legal and ethical standards, ensuring that their work complies with relevant laws and professional guidelines.
   e. Continual Education: Due to the rapidly evolving nature of technology, digital forensic experts must continually update their knowledge and skills to stay current with new tools, techniques, and legal precedents.

Digital forensic experts are integral to modern criminal investigations and prosecutions, providing the technical expertise necessary to handle digital evidence. Their role encompasses the meticulous collection and analysis of data,

the ability to communicate complex technical information to non-experts, and the maintenance of ethical standards throughout the judicial process. As digital technology continues to evolve, the importance and complexity of their work are likely to increase, underscoring the need for highly skilled and knowledgeable professionals in this field.

Digital era has revolutionized human life and work buttechnology is still challenged by many cyber crimes, endangering user privacy and data. The increasing prevalence of cybercrime has become a pressing issue for experts in the field, leading to the development of digital forensics as a valuable tool for investigating and combating these attacks.[35] Digital forensic experts are often called to serve as expert witnesses in court. Their role is to provide an independent and professional opinion based on their specialized knowledge and skills.

Digital forensics involves the application of scientific methods to legally extract information from various electronic devices, such as computers and smartphones. It encompasses a wide range of disciplines, including network, server, computer, internet, social media, memory, online games, data, and VR forensics. The process of investigating digital crimes involves several key steps, including identification, recovery, investigation, validation, and presentation of evidence. In light of the increasing prevalence of cyber threats and attacks, there is a growing need for forensic experts and scientists to navigate the complexities of the digital landscape. Due to the nature of data recovery and analysis involved in digital forensics, this field faces a variety of technical, legal, and resource-related challenges.[36]

Expert in the field of Digital Forensics or related to electronic evidence is regulated in:

1. Article 183 of the Criminal Procedure Code: A judge cannot deliver a sentence unless a criminal act transpired and the defendant is culpable for the commission.
2. Article 184 of the Criminal Procedure Code:
   (8) Valid evidence includes a. witness statements, b. expert information, c. letter, d. instruction, and e. defendant's statement.
   (9) Facts widely acknowledged do not necessitate explicit proof.

---

[35] Abhisek Kumar Pandey et al., "Current Challenges of Digital Forensics in Cyber Security," in *M. Husain & M. Khan (Eds.), Critical Concepts, Standards, and Techniques in Cyber Forensics* (IGI Global, 2020), 31–46, https://doi.org/https://doi.org/10.4018/978-1-7998-1558-7.ch003.

[36] Bhoopesh Kumar Sharma et al., "Emerging Trends in Digital Forensic and Cyber Security- An Overview," in *2019 Sixth HCT Information Technology Trends (ITT)*, 2019, 309–13, https://doi.org/10.1109/ITT48889.2019.9075101.

3. Article 186 of the Criminal Procedure Code: Expert testimony refers to the presentation of specialized knowledge or opinions by an expert witness in court proceeding.

The Criminal Procedure Code regulates the differences in understanding witness and expert testimonies.

1. Article 1 point 27 regulates the complete meaning of witness testimony as evidence in a criminal case in the form of a statement from witness regarding an incident heard, saw, and experienced.
2. Expert testimony is regulated in Article 1 number 28: Expert testimony is information given by a person with special expertise regarding matters needed to analyze criminal cases.

If a review is carried out on the origin of the word, the term Expert Statement consists of two basic words, namely the word information and expert. The term explanation refers to the person who provides a description to state an explanation. Meanwhile, an expert denotes an individual who possesses proficiency or deep understanding in a particular field or discipline. The term Expert Statement is formulated in Article 1 number 28 of the Criminal Procedure Code and this law does not explain the definition.

To be accepted as an expert witness, the forensic expert must demonstrate their qualifications, including education, training, and experience in the field of digital forensics. As expert witnesses, they must maintain impartiality and objectivity, providing testimony based on facts and their expert analysis rather than advocacy for either party. According to Tristram Hodkinson and Mark James, the definition of an expert includes two aspects, firstly, an individual who possesses experience and skills. Secondly, someone who is trained through practice, competent, skilled, and possesses specialized knowledge or abilities in a particular area. In the context of legal proceedings, an expert refers to an individual possessing specialized knowledge, skills, training, or experience adequate to provide information and opinions not readily accessible to the general public. From the definitions, the term signifies an individual with experience, expertise, and knowledge. Drawing from these attributes, an expert can furnish information, opinions, and explanations on matters unfamiliar to the general public, when queried before the trial.

The practice of proceedings has experienced development in the definition of Expert Statements regulated within the Procedure Guidelines of Legal Review Cases at the Constitutional Court. These rules are different from the scope of the General Court used as a theoretical comparison. Article 1 Number 13 of Constitutional Court Regulation Number: 06/PMK/2005 concerning Procedure Guidelines in Legal Review Cases regulates that an Expert Statement

is information provided by a person who has expertise or in-depth knowledge relating to technical or other special opinions.

The definition regarding the meaning of Expert Statement, between the Criminal Procedure Code and the Guidelines for Proceedings in the Constitutional Court, has shown a development in the definition. The Criminal Procedure Code only defines expert testimony as information provided by someone who has special expertise. Meanwhile, expert testimony provides a more detailed definition of providing the basis for expertise obtained from education and experience. The guidelines also provide an understanding of the opinions given by an expert at trial, namely scientific, technical, or other special opinions regarding evidence or facts required.

Provisions regarding the role of Experts are regulated in Article 43 of Law Number 11 of 2008 concerning Information and Electronic Transactions. According to Article 43, State Police Officers of the Republic of Indonesia and Civil Servant Officials within the Government are given special authority in the Law on Criminal Procedure Law to carry out investigations of criminal acts. In the explanation of Article 43 paragraph (5) letter h of Law Number 11 of 2008 concerning Information and Electronic Transactions, an expert is someone held accountable academically and practically regarding knowledge.

The demand for digital forensic investigations manifests in both civil and criminal proceedings as society becomes more digitalized and interconnected. Ensuring the use of scientifically proven or thoroughly validated methodologies is crucial. However, keeping pace with the rapid advancement of technology presents challenges in consistently achieving the standard. In addition, developing applications used to reconstruct, analyze, and categorize events is also important in the discipline.[37] Due to the extensive scope and intricate nature of digital forensic investigations, it is essential for professionals to carefully plan and execute their examination processes in order to ensure efficiency and effectiveness.[38]

The best way to serve the public and legal system is by providing access to unbiased and scientific expert witness testimony in both civil and criminal cases. As professionals and individuals, we have a moral duty to contribute to the justice system. This statement outlines suggestions for promoting advocacy,

---

[37] Victor R Kebande et al., "Mapping Digital Forensic Application Requirement Specification to an International Standard," *Forensic Science International: Reports* 2 (2020): 100137, https://doi.org/https://doi.org/10.1016/j.fsir.2020.100137.

[38] Graeme Horsman, "Digital Evidence Strategies for Digital Forensic Science Examinations," *Science & Justice* 63, no. 1 (2023): 116–26, https://doi.org/https://doi.org/10.1016/j.scijus.2022.11.004.

education, research, qualifications, standards, and ethical conduct in order to enhance the quality of expert testimony.[39]

The significant material and intellectual losses incurred due to technological and information crimes in recent years have shown the importance for relevant institutions and organizations to formulate a scientific and sustainable strategy for mitigating losses. In the last two decades, the discovery and investigation of crimes have become the main task of security agencies and the judiciary. The advantages conferred by computer forensics expertise extend beyond being an essential prerequisite for security and judicial institutions. Professional users and owners of computer systems, as well as networks, must possess a comprehensive awareness of legal and technical requisites associated with forensics.[40]

Digital forensic experts play a crucial role in investigating and analyzing digital evidence related to cybercrimes and other legal matters involving digital data. Their functions encompass a wide range of activities aimed at identifying, preserving, analyzing, and presenting digital evidence. Here are the key functions of digital forensic experts.[41]

1. Identification
   a. Recognizing Potential Evidence: Identifying relevant digital devices and storage media (e.g., computers, smartphones, tablets, servers, USB drives) that may contain evidence.
   b. Assessing Scope: Determining the type and extent of digital evidence required for the investigation.
2. Preservation
   a. Securing Evidence: Ensuring that digital evidence is preserved in its original state to prevent tampering or loss. This often involves creating bit-by-bit copies (forensic images) of storage media.
   b. Chain of Custody: Maintaining a documented history of the evidence to establish its integrity and authenticity from collection to presentation in court.

---

[39] Stephan R Paul et al., "Expert Witness Participation in Civil and Criminal Proceedings," *Pediatrics* 139, no. 3 (March 1, 2017): e20163862, https://doi.org/10.1542/peds.2016-3862.

[40] Seyyed Sajjad Kazemi and Sajjad Heidari, "Digital Forensics and It's Role in Promoting Criminal Prosecution," *Revista Eletrônica Em Gestão, Educação e Tecnologia Ambiental* 25, no. 0 SE-ENVIRONMENTAL THECNOLOGY (August 2, 2022): e5, https://doi.org/10.5902/2236117063798.

[41] Cahyadri, *Apa Yang Harus Ditanyakan Kepada Ahli Digital Forensic? Panduan Bagi Praktisi Hukum*.

3. Analysis
   a. Data Recovery: Retrieving data from damaged, deleted, or encrypted storage devices.
   b. Examination: Analyzing digital data to uncover relevant information, such as emails, documents, browser histories, chat logs, and metadata.
   c. Pattern Recognition: Identifying patterns, anomalies, or specific items of interest within the digital data.
   d. Timeline Reconstruction: Reconstructing events in a chronological order to understand the sequence of actions or events.
4. Interpretation
   a. Contextual Understanding: Providing context to the digital evidence, explaining its relevance and implications in relation to the case.
   b. Expert Opinions: Offering expert interpretations and insights based on the analysis of the digital evidence.
5. Reporting
   a. Documentation: Preparing detailed reports that outline the methods used, findings, and conclusions of the forensic analysis.
   b. Clear Communication: Ensuring that the reports are clear, accurate, and comprehensible to non-technical stakeholders, such as lawyers, judges, and juries.
6. Presentation
   a. Testimony: Serving as expert witnesses in court to present and explain the digital evidence and the results of the forensic analysis.
   b. Demonstrations: Providing visual aids or demonstrations to help illustrate complex technical concepts and findings to the court.
7. Security and Compliance
   a. Ensuring Legal and Ethical Standards: Adhering to legal, ethical, and professional standards throughout the forensic investigation process.
   b. Data Protection: Ensuring that sensitive data is handled securely and in compliance with relevant laws and regulations.
8. Consultation
   a. Advising Organizations: Providing advice to organizations on best practices for digital security, data protection, and incident response.
   b. Training: Educating law enforcement, legal professionals, and organizations on digital forensics and cybersecurity issues.
9. Research and Development
   a. Staying Updated: Keeping up-to-date with the latest developments in digital forensic tools, techniques, and trends.

b. Tool Development: Developing or improving forensic tools and methodologies to enhance the efficiency and accuracy of digital investigations.

10. Collaboration
    a. Working with Law Enforcement: Collaborating with law enforcement agencies during criminal investigations.
    b. Interdisciplinary Cooperation: Working alongside other forensic experts, such as those in physical forensics, to provide a comprehensive investigation.

Digital forensic experts play a vital role in modern investigations, leveraging their expertise to uncover and analyze digital evidence that can be crucial in solving crimes and resolving legal disputes.

Conclusion

The role and legal position of digital forensic experts in the settlement of information technology (IT) crime cases are crucial, given the increasing prevalence of cybercrime and the complexity of digital evidence. Digital forensic experts play a pivotal role in investigating, analyzing, and presenting digital evidence in legal proceedings. Their expertise is essential for understanding the intricacies of digital data and ensuring the integrity and reliability of evidence used in court. A judge was considered to know the law or *ius curia novit*, which was a judicial principle to describe the spirit of someone willing to follow developments in the world of law and society. Digital data, traces, and electronic evidence could be presented in courtrooms with the development of technology, where society was connected to the use of information and communication technology. Technological developments occurred in every line and sphere, specifically in the international sphere where many Best Practices were prepared and implemented relating to actions, procedures, handling, and analysis of electronic evidence and statements by Digital Forensics Experts at trials. In line with *ius curia novit*, there existed a singular solution to the contemporary challenges posed by digital landscape, where judges and legal practitioners must actively engage in learning.

References

Al-Fatih, Sholahuddin, and Ahmad Siboy. "Menulis Artikel Karya Ilmiah Hukum Di Jurnal Nasional Dan Internasional Bereputasi." *Inteligensia Media*, 2021.

Amarini, Indriati. *Saksi Ahli Dalam Praktik Peradilan*. Semarang: Saraswati

Nitisara, 2019.

Amarini, Indriati, and Ratna Kartikawati. "Strengthening the Position of Expert Witness in Judicial Process." *Jurnal Media Hukum* 27, no. 1 (2020): 44–54. https://doi.org/https://doi.org/10.18196/jmh.20200141.

Beek, H M A van, J van den Bos, A Boztas, E J van Eijk, R Schramp, and M Ugen. "Digital Forensics as a Service: Stepping up the Game." *Forensic Science International: Digital Investigation* 35 (2020): 301021. https://doi.org/https://doi.org/10.1016/j.fsidi.2020.301021.

Booth, Brad D, Joel Watts, and Mathieu Dufour. "Lessons from Canadian Courts for All Expert Witnesses." *The Journal of the American Academy of Psychiatry and the Law* 47, no. 3 (May 16, 2019): 278–85. https://doi.org/https://doi.org/10.29158/JAAPL.003838-19.

Cahyadri, Rizky Aulia. *Apa Yang Harus Ditanyakan Kepada Ahli Digital Forensic? Panduan Bagi Praktisi Hukum*. Yogyakarta: Deepublish, 2021.

Caviglione, Luca, Steffen Wendzel, and Wojciech Mazurczyk. "The Future of Digital Forensics: Challenges and the Road Ahead." *IEEE Security & Privacy* 15, no. 6 (2017): 12–17. https://doi.org/10.1109/MSP.2017.4251117.

Dmitrieva, Anna A, and Pavel S Pastukhov. "Concept of Electronic Evidence in Criminal Legal Procedure." *Journal of Digital Technologies and Law* 1, no. 1 (2023): 270–95. https://doi.org/https://doi.org/10.21202/jdtl.2023.11.

Du, Mingxiao. "Legal Control of Expert Witness Bias." *The International Journal of Evidence & Proof* 21, no. 1–2 (December 29, 2016): 69–78. https://doi.org/10.1177/1365712716674798.

Ewald, Uwe. "Digital Forensics vs. Due Process: Conflicting Standards or Complementary Approaches?" In *CECC 2019: Proceedings of the Third Central European Cybersecurity Conference*, 1–2, 2019. https://doi.org/https://doi.org/10.1145/3360664.3362697.

Fähndrich, Johannes, Wilfried Honekamp, Roman Povalej, Heiko Rittelmeier, Silvio Berner, and Dirk Labudde. "Digital Forensics and Strong AI: A Structured Literature Review." *Forensic Science International: Digital Investigation* 46 (2023). https://doi.org/https://doi.org/10.1016/j.fsidi.2023.301617.

Garrett, Brandon L, Brett O Gardner, Evan Murphy, and Patrick Grimes. "Judges and Forensic Science Education: A National Survey." *Forensic Science International* 321 (2021): 110714. https://doi.org/https://doi.org/10.1016/j.forsciint.2021.110714.

Guo, Hong, and Junlei Hou. "Review of the Accreditation of Digital Forensics in China." *Forensic Sciences Research* 3, no. 3 (July 3, 2018): 194–201.

https://doi.org/10.1080/20961790.2018.1503526.

Hamzah, Ismail, Finley Febiyanto, Kevin, and J V Moniaga. "Methods to Prevent Privacy Violations on the Internet on the Personal Level in Indonesia." *Procedia Computer Science* 216 (2022): 650–54. https://doi.org/https://doi.org/10.1016/j.procs.2022.12.180.

Henseler, Hans, and Sophie van Loenhout. "Educating Judges, Prosecutors and Lawyers in the Use of Digital Forensic Experts." *Digital Investigation* 24 (2018): S76–82. https://doi.org/https://doi.org/10.1016/j.diin.2018.01.010.

Horsman, Graeme. "Digital Evidence Strategies for Digital Forensic Science Examinations." *Science & Justice* 63, no. 1 (2023): 116–26. https://doi.org/https://doi.org/10.1016/j.scijus.2022.11.004.

Horsman, Graeme, and Nina Sunde. "Unboxing the Digital Forensic Investigation Process." *Science & Justice* 62, no. 2 (2022): 171–80. https://doi.org/https://doi.org/10.1016/j.scijus.2022.01.002.

Kazemi, Seyyed Sajjad, and Sajjad Heidari. "Digital Forensics and It's Role in Promoting Criminal Prosecution." *Revista Eletrônica Em Gestão, Educação e Tecnologia Ambiental* 25, no. 0 SE-ENVIRONMENTAL THECNOLOGY (August 2, 2022): e5. https://doi.org/10.5902/2236117063798.

Kebande, Victor R, Stacey Baror, Reza M Parizi, Kim-Kwang Raymond Choo, and H S Venter. "Mapping Digital Forensic Application Requirement Specification to an International Standard." *Forensic Science International: Reports* 2 (2020): 100137. https://doi.org/https://doi.org/10.1016/j.fsir.2020.100137.

Masory, Oren. "From Litigation Consulting to Research and Education." In *17 Th LACCEI International Multi-Conference for Engineering, Education, and Technology*, 2019. https://doi.org/https://doi.org/10.18687/laccei2019.1.1.250.

Muhidin, Eman Suparman, M Guntur Hamzah, and Indra Officer. "Implementation of The Ius Curia Novit Principle in Examining Case At The Constitutional Court of The Republic of Indonesia." *Baltic Journal of Law & Politics* 15, no. 1 (2022): 453–65. https://doi.org/10.2478/bjlp-2022-00030.

Oppong, John Kwaku. "Evidence Confidentiality and Digital Forensic Experts." *Research Nexus in IT, Law, Cyber Security & Forensics* 1, no. 1 (2022): 161–66. https://doi.org/https://dx.doi.org/10.22624/aims/crp-bk3-p26.

Pandey, Abhisek Kumar, Ashutosh Kumar Tripathi, Gayatri Kapil, Virendra Singh, Mohd. Waris Khan, Alka Agrawal, Rajeev Kumar, and Raees

Ahmad Khan. "Current Challenges of Digital Forensics in Cyber Security." In *M. Husain & M. Khan (Eds.), Critical Concepts, Standards, and Techniques in Cyber Forensics*, 31–46. IGI Global, 2020. https://doi.org/https://doi.org/10.4018/978-1-7998-1558-7.ch003.

Paul, Stephan R, Sandeep K Narang, William M McDonnell, Robin L Altman, Steven A Bondi, Jon Mark Fanaroff, Richard L Oken, et al. "Expert Witness Participation in Civil and Criminal Proceedings." *Pediatrics* 139, no. 3 (March 1, 2017): e20163862. https://doi.org/10.1542/peds.2016-3862.

Pribadi, Bagus, Sri Rosdiana, and Samsul Arifin. "Digital Forensics on Facebook Messenger Application in an Android Smartphone Based on NIST SP 800-101 R1 to Reveal Digital Crime Cases." *Procedia Computer Science* 216 (2023): 161–67. https://doi.org/10.1016/j.procs.2022.12.123.

Reedy, Paul. "Artificial Intelligence in Digital Forensics." *Encyclopedia of Forensic Sciences, Third Edition* 1 (2023): 170–92. https://doi.org/https://doi.org/10.1016/B978-0-12-823677-2.00236-1.

Reedy, Paul. *Strategic Leadership in Digital EvidenceWhat Executives Need to Know*. Academic Press, 2020. https://doi.org/https://doi.org/10.1016/C2018-0-05426-2.

Reynard, John. "Being an Expert Witness." In *Medicolegal Issues in Obstetrics and Gynaecology*, edited by Swati Jha and Emma Ferriman, 51–54. Cham: Springer International Publishing, 2018. https://doi.org/10.1007/978-3-319-78683-4_10.

Roussev, Vassil. "Issues, Methods, and Challenges." In *Digital Forensic Science*. Springer Cham, 2017. https://doi.org/https://doi.org/10.1007/978-3-031-02351-4.

Sabillon, Regner, Jordi Serra-Ruiz, Victor Cavaller, and Jeimy J Cano. "Digital Forensic Analysis of Cybercrimes: Best Practices and Methodologies." *International Journal of Information Security and Privacy* 11, no. 2 (2017): 25–37. https://doi.org/https://doi.org/10.4018/IJISP.2017040103.

Schiltenwolf, Marcus, Nickolas Beckmann, and Peter Gaidzik. "Erörterung Eines Sachverständigengutachtens Vor Gericht Und Die Haftung Des Sachverständigen [Expert Opinions in Court: Liability of the Expert]." *Z Orthop Unfall* 155, no. 6 (2017): 727–31. https://doi.org/10.1055/s-0043-116798.

Selamat, Siti Rahayu, Y Robiah, Shahrin Sahib, and Nor Hafeizah Hassan. "Traceability in Digital Forensic Investigation Process." In *2011 IEEE Conference on Open Systems (ICOS2011)*, 101–6, 2011. https://doi.org/10.1109/ICOS.2011.6079259.

Sharevski, Filipo. "Rules of Professional Responsibility in Digital Forensics: A

Comparative Analysis." *Journal of Digital Forensics, Security, and Law* 10, no. 2 (2015): 39–53. https://doi.org/https://doi.org/10.15394/jdfsl.2015.1201.

Sharma, Bhoopesh Kumar, Michelle Ann Joseph, Biju Jacob, and Bryan Miranda. "Emerging Trends in Digital Forensic and Cyber Security- An Overview." In *2019 Sixth HCT Information Technology Trends (ITT)*, 309–13, 2019. https://doi.org/10.1109/ITT48889.2019.9075101.

Simatupang, Benget Hasudungan. "Alat Bukti Keterangan Ahli Hukum Pidana Dalam Proses Pemeriksaan Perkara Pidana." *Ensiklopedia Sosial Review* 2, no. 3 (2020): 304–13. https://doi.org/https://doi.org/10.33559/esr.v2i3.637.

Soltani, Somayeh, and Seyed Amin Hosseini Seno. "Detecting the Software Usage on a Compromised System: A Triage Solution for Digital Forensics." *Forensic Science International: Digital Investigation* 44 (2023): 301484. https://doi.org/https://doi.org/10.1016/j.fsidi.2022.301484.

Suadi, Amran. *Sosiologi Hukum: Penegakan, Realitas Dan Nilai Moralitas Hukum*. Jakarta: Prenada Media, 2018.

Todd, N V. "Expert Witnesses, Contempt of Court and Custodial Sentencing." *The Bulletin of the Royal College of Surgeons of England* 102, no. 1 (December 31, 2019): 34–36. https://doi.org/10.1308/rcsbull.2020.34.

***

Acknowledgment
None

Funding Information
None

Conflicting Interest Statement
The authors state that there is no conflict of interest in the publication of this article.

History of Article
Submitted : March 28, 2024
Revised : May 20, 2024; September 7, 2024
Accepted : September 15, 2024
Published : September 22, 2024