UTM UNIVERSITI TEKNOLOGI MALAYSIA
INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING
ISSN 2180-4370
Journal Homepage : https://ijic.utm.my/

Evidence Collection and Handling Process Model in Mobile Forensic for Malaysian Law Enforcement Agencies

Munif Bafana[1] & Maheyzah Md Siraj[2]
Faculty of Computing
University Teknologi Malaysia
81310, UTM Johor Bahru, Johor, Malaysia
Email: munif95@graduate.utm.my[1]; maheyzah@utm.my[2]

Submitted: 21/7/2025. Revised edition: 10/11/2025. Accepted: 11/11/2025. Published online: 30/11/2025
DOI: https://doi.org/10.11113/ijic.v15n2.570

***Abstract*—The rapid adoption of mobile technology has revolutionized criminal investigations, with mobile devices becoming crucial sources of evidence. The current state of mobile forensics faces challenges from a growing backlog of devices to be analyzed. There have been many initiatives to improve the state of mobile digital forensics. However, most initiatives have focused on relieving the digital forensic analyst on pre-analysis tasks such as triage, extraction workflow and management of cases and evidence. There is still a bottleneck at the actual analysis stage that hampers swift legal resolution. The research objectives include identifying current challenges in mobile forensics, developing an alternative process mobile forensic process model, and evaluating the feasibility of the proposed model. The methodology used in this research is Design Science Research (DSR) as it seeks to enhance knowledge in technology and science through problem-solving and innovative solutions to real-world problems. Through this study, an alternative mobile forensics process model was developed involving a central pseudo air-gapped digital forensics extraction lab with analysis hubs in different locations connected over private networks. The model is validated through surveys with domain experts to offer promising efficiency improvements and feasiblity albeit with potential technical, operational, and security challenges. The significance of this research lies in enriching the knowledge base of digital forensics professionals and legal experts, offering valuable insights for real-world implementation to enhance the efficiency and timelines of mobile forensic analysis, and ultimately contributing to a more just legal system.**

***Keywords*—Mobile Forensics, Law Enforcement, Backlog, Data Network**

I. INTRODUCTION

An average mobile phone user touches his or her phone 2617 (Mobile Touches dscout's inaugural study on humans and their tech, 2016) times every day. Recent data adds that the average person spends 4 hours and 37 minutes on their phone every day with half of all screen time sessions beginning within 3 minutes of the last (Duarte, 2025). Such interaction frequency between users and their mobile devices naturally makes it a central source of evidence. A 2022 report has found that British police forces are overwhelmed when it comes to digital forensics – and there is a backlog of 25,000 devices waiting to be examined (His Majesty's Inspectorate of Constabulary and Fire & Rescue Services, 2022). The main essence of digital forensics lies in its timely and precise extraction, interpretation of digital data, and ensuring its admissibility in the court of law. Clearly, inefficiencies are a problem not only for the enforcement officers but also for the citizens at large, as the saying goes: justice delayed is justice denied.

The current state of digital forensics is described to be in shortage of trained personnel, having limited operational labs that cost a bomb to set up and maintain, and pressured with a growing backlog of devices (His Majesty's Inspectorate of Constabulary and Fire & Rescue Services, 2022). This poses a significant hurdle in the timely and effective pursuit of justice. There is an urgent need to address the current state of digital forensics, specifically mobile digital forensics. Previous attempts to address these issues were focused on relieving the digital forensics analyst from doing pre-analysis tasks such as management of cases and evidence (Evidence Management: The Importance Of Management In Evidence, 2023), triage (Hitchcock, 2016), and extraction workflow (R. I. de Braekt, 2016). However well these initiatives work, it is still insufficient to handle the exponential demand and growth of our dependence on mobile devices.

The structure of this study is organized as follows. Chapter Two presents the literature review to understand what mobile digital forensics and its current state is. This covers topics of digital forensics, evidence management, and networking concepts. It also covers previous work and proposals that investigate the issue of increasing forensics backlog cases. Chapter Three discusses the methodology taken to develop this alternative process model for law enforcement agencies to reduce backlog of mobile forensic cases. Chapter Four presents the discussions and alternative process model. Five presents the feasibility study and finally, Chapter 6 will conclude and provide future works that can be done to the model to further reduce mobile forensics backlog cases.

This research will propose an alternative process model to provide effective and sustainable mobile digital forensics services. This model involves designing a pseudo air gapped central digital forensics extraction lab with analysis hubs across different locations over a private network to address the backlog issue at the analysis stage.

II. LITERATURE REVIEWS

A. Basic Concepts in Mobile Device Forensics

Forensics involves the application of scientific knowledge and techniques to solve crimes. According to Dr. Edmond Locard (1877-1966), a forensic scientist, a fundamental principle asserts that whenever two objects come into contact, there is an inevitable exchange of material between them. When a perpetrator enters a crime scene, they introduce something into the environment and simultaneously carry something away. Both of which can serve as forensic evidence either supporting or implicating an individual. Mobile devices are no exception to the Locard's principle. As a user interacts with a mobile device, there are digital artifacts created in operating system logs, files, databases, metadata, and history that correlates to the user's actions on a device.

Generally, digital forensics follows a set of procedures or guidelines through proven methods accepted by the scientific community for examining digital evidence. There are multiple approaches to digital forensics, but commonly includes the following five phases: Preparation, Collection / Preservation, Examination / Analysis, Presentation / Reporting and Disseminating the Case (Selamat *et al*., 2008) or Closure.

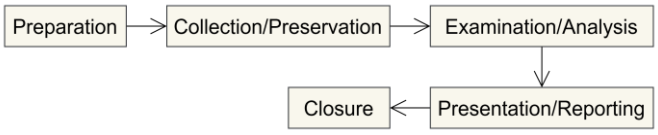

Fig. 1. Five Stages of Digital Forensic Investigation

B. Triage

Triage in digital forensics involves the classification and sorting of cases or scenes by first responders to ascertain whether specific devices require additional examination in a lab environment. Digital triage is an important phase of forensic analysis and comes in two forms: live and dead, each serving specific purposes. Live triage focuses on extracting volatile and logical data quickly from powered-on devices, providing rapid intelligence. Dead triage, conducted in the lab, involves working with physical image files, including tasks such as acquiring image file copies, indexing, searching, cracking, analyzing digital content, and presenting forensic reports.

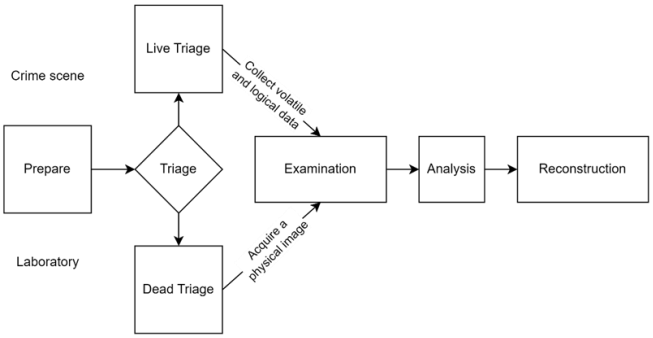

Fig. 2. General Forensic Triage (D. -Y. Kao, 2020)

C. Evidence Management

Proper evidence handling process involves the protection of evidence integrity, preservation of its nature, and the assurance that there are no doubts over tampering. The following is an example of evidence handling process practiced in Digital Forensics Department at MCMC, a Malaysian Law Enforcement Agency. The process below ensures proper chain of custody and integrity of evidence that was submitted to them from investigating officers for forensic cases. However, the evidence handling process has constraints at the analysis stage. Shall they receive more cases than what their digital analysts can handle per given time, there will be backlogs of cases sitting in their EPR (Evidence Preservation Room).

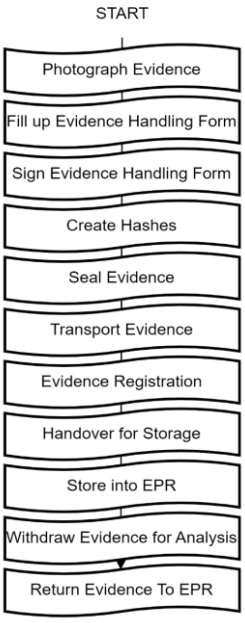

Fig. 3. Evidence Handling Process at DFD MCMC

D. Triage Triangle Strategy of Digital Forensic Components

Cybercrimes have placed Law Enforcement Agencies (LEAs) at a disadvantage. To address the backlog challenge, a triage triangle strategy was proposed by the Department of Criminal Investigation, Central Police University, Taiwan. The proposed strategy enhances the efficiency of digital forensics through guidelines encompassing principles, forensics, and governance (D. -Y. Kao, 2020).

E. Increasing Investigator Availability through Workflow Flow Management and Automation

Another proposed strategy to address the backlog issue is through automating tasks prior to the analysis and reporting stage to reduce the load on the forensic analysts from doing the more menial tasks and allowing him to have more time conducting the actual digital forensic investigation. The framework consists of three independent automation components (R. I. de Braekt, 2016): First it tries to automate existing forensic command line tools to perform the imaging by creating scripts in a configuration file requiring minimal user input and process knowledge other than choosing the right options for the nature of the case and the tool will then perform the necessary steps as per the configuration file and trigger the next step of the workflow according to the queue server that controls third party software. Lastly, backup and archiving are also taken cared of periodically by clean up servers. Each of these components help reduce wasted investigator effort and provides the investigator with significantly more time to conduct detailed investigation.

F. Tiered Forensic Methodology Model for Digital Field Triage by Non-Digital Evidence Specialists

To enhance investigational efficiency and reduce backlogs in Technological Crime Units (TCUs), Digital Field Triage (DFT) is designed to empower non-digital evidence specialists with the necessary knowledge, skills, and abilities to perform limited forensic activities. In practice, a DFT member's job is to identify and evaluate which digital evidence parts contain relevant artifacts. For instance, it would be sufficient for the DFT to consider as evidence for further analysis if illicit images were found on a computer in a child pornography inquiry. However, the DFT member's observations are limited, and they may not provide in-depth information, such as how the images were obtained or their specific location—details that only a trained forensic analyst could provide. Emphasizing the distinction each role play in the forensic process is as below.

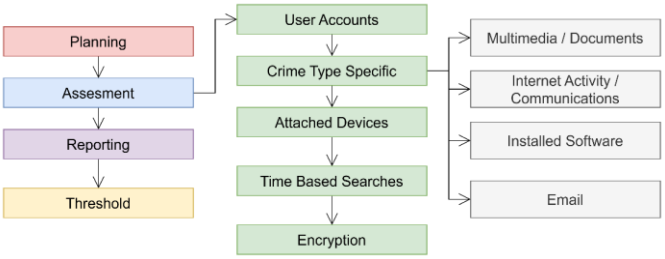

Fig. 4. Digital Field Triage model (Hitchcock, 2016)

G. ISO/IEC 17025 Testing and Calibration Laboratories

Commonly referred to as ISO 17025, this certification is relevant for any organization involved in testing, sampling, or calibration. Sectors ranging from forensics to asbestos testing, acoustics, chemicals, and more adopt ISO/IEC 17025 to signify the quality of their labs. The ISO/IEC 17025 standard comprises five key categories: Scope, Normative Resources, Terms and Definitions, Management Requirements, and Technical Requirements. It covers aspects such as testing and calibration standards, staff competence, equipment standards, and quality management. ISO 17025 accreditation aims to ensure the consistent production of valid results (How to Become a Digital Forensics Professional in 2023, 2023). While originally intended for testing and calibration laboratories, some argue it is the most suitable standard for Digital Forensic Laboratories due to the absence of another international standard for digital forensics.

H. ISO/IEC 27043:2015 Information technology — Security Techniques — Incident Investigation Principles And Processes

The standard provides guidelines for common incident investigation processes involving digital evidence from pre-incident preparation through investigation closure. It is broken up into a few big topics such as digital investigations, digital investigation processes, readiness processes, initialization processes, acquisitive processes, investigative processes, concurrent processes, and digital investigation process model schema. The processes and principles described are applicable to various kinds of investigations, including, but not limited to, unauthorized access, data corruption, system crashes, or corporate breaches of information security. The standard gives a broad overview of all incident investigation principles without dictating instructions and emphasizes the importance of reviewing the investigation process to identify areas for improvement and updating policies accordingly.

I. Enhancing Network Security

Two key strategies play pivotal roles in safeguarding sensitive information: Air Gapping and Virtual Private Networks (VPNs). Air Gapping involves physically isolating a computer or network from external connections, particularly the internet. This deliberate separation minimizes the risk of cyber-attacks by creating an "air gap" between the isolated system and potential sources of compromise. While air gapping has its security benefits, it may be inconvenient and prone to human-error to schedule the copying of data and carrying it to the physically isolated system. A data diode offers a more seamless alternative. It is a network device that is placed between two networks and acts as a one-way valve permitting the movement of data in only one direction while blocking all data in the opposite direction. This means that if you have requirements for physical separation, it can be fulfilled (in the reverse direction) by a data diode but at the same time enable a network connection in the forward direction. VPNs, on the other hand, address security concerns in a different manner. A VPN creates a secure and encrypted connection over the

internet, ensuring the confidentiality and integrity of data in transit. This is achieved by creating a virtual tunnel between the user's device and a VPN server. This encrypted tunnel protects the data from malicious actors trying to intercept sensitive information. VPNs serve various purposes, including anonymizing user identities by masking IP addresses, bypassing geographical restrictions to access region-locked content, and providing secure remote access to corporate networks. They are instrumental in enhancing online privacy and security.

III. IMPLEMENTATION DESIGN

A. Central Digital Forensics Extraction Lab

The alternative process model is to have an air-gapped central digital forensics extraction lab with analysis hubs across different locations accessible over a private network. The system architecture will be such that the existing digital forensics lab be maintained. A backup central repository of extracted evidence is created via a data diode link. This backup central repository is what's made available / accessible over a private network from remote workstations. Analysis can now be performed over the extracted evidence using normal workstations as only the extraction requires specialized hardware and software. More personnels can be trained to conduct analysis as the space constraint is lifted. Law enforcement agencies throughout the nation can perform the analysis at their home bases using workstations set for this purpose without having to wait in queue for their case to be analyzed by the digital forensics' analyst. Most importantly, there is no need to build and maintain a new fully functional digital forensics lab.

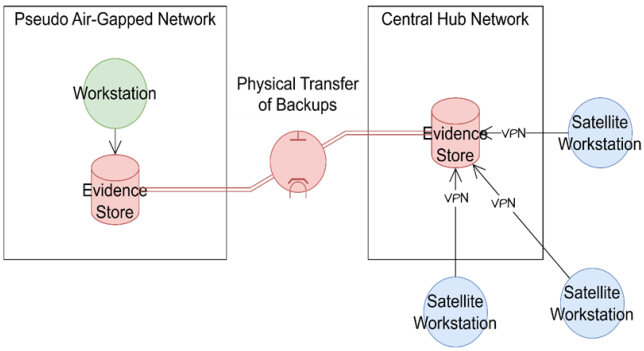

Fig. 5. System Architecture

B. New Evidence Collection and Process Model Flow

The evidence handling process outlined in this process model represents a new approach that has been developed by adapting and combining various sources from the literature reviews. The evidence handling process outlined in this model begins with the triage conducted by a Digital Field Triage (DFT) member. The DFT role implemented here is to identify and assess digital evidence items that contain sufficient artifacts relevant to the ongoing investigation. Next, documenting the initial state of the evidence. This is crucial for preserving the physical integrity of the evidence. Documentation typically involves capturing images that accurately depict the state of the evidence at the time of collection. Then the process moves to paperwork completion for administrative purposes. This involves filling out evidence handling paperwork, which is essential for maintaining a clear and organized record of the evidence submitted to the central mobile digital forensics lab. Maintaining the chain of custody is paramount in digital forensics. This is achieved through signatures during handovers of the evidence. Each transfer of custody is documented and signed off by authorized personnel to ensure accountability and integrity. To further ensure the integrity of the evidence, hashes are generated. These hashes serve as digital fingerprints that can be used to verify and compare the integrity of the evidence and detect any signs of tampering. Following hash creation, the evidence is sealed until it is handed over to the digital forensic analyst for extraction to ensure that the evidence remains secure and uncontaminated. The evidence then undergoes extraction using specialized tools. Backup copies are created using hardware and software forensic tools to ensure that the integrity of the original evidence is preserved during the extraction process. Prior to this step, a DFT member has been the one handling the evidence hence, freeing a lot of the digital forensic analyst resources. The extracted evidence is then stored in the Evidence Preservation Room (EPR). Analysis is conducted only on a working copy to avoid tampering with the original evidence. A working copy of the evidence is then sent to the pseudo air-gapped network for two purposes, as a controlled copy and analysis. Another copy is sent to the central hub network that is accessible to satellite workstations over a private network via the data diode link. This allows for onsite analysis if needed, while also providing access to remote personnel for analysis. Finally, upon completion of the extraction and backups, the requester is notified. They have the option to conduct analysis using their trained personnel on satellite workstations or opt for analysis by the central digital forensics lab. Subsequently, the reports are produced by the analyst who conducted the analysis. Presentation of findings are then typically done by the investigating officer. The analyst may be needed in the future to provide expert witness in court.

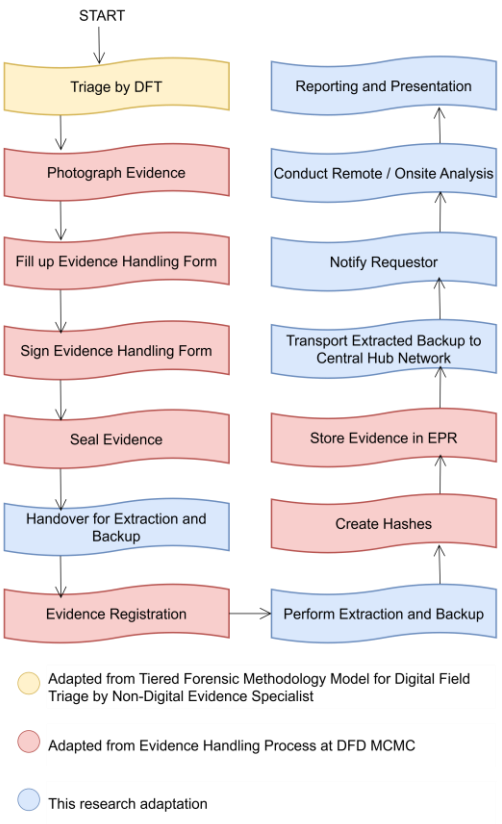

Fig. 6. Alternative Process Model Evidence Handling Flow

IV. FEASIBILITY DISCUSSION

This proposal offers a comprehensive solution to several challenges in the field of digital forensics and addresses a key bottleneck in the process. Importantly, previous initiatives and efforts made at the pre-analysis stage can still be integrated into this new process model. Additionally, this approach enables more personnel to be trained and stationed at their respective home base agencies, reducing the need for extensive infrastructure. Only a dedicated workstation with access to the central repository is required, facilitating remote analysis. Extending the existing digital forensics lab to be the central digital forensics extraction lab with analysis hubs distributed across different locations is much more feasible than setting up new and expensive labs. It allows for a more efficient utilization of resources, decentralizes the workload, and enables quicker response times. Implementing secure protocols and adequate bandwidth for transferring data between the pseudo air-gapped lab and the central repository is crucial to maintaining integrity and confidentiality. However, it is not impossible because many industries such as banking and finance also rely on large data transfers and rapidly accurate synchronization.

A. Technical Feasibility

The alternative model can address the shortage of trained personnel by enabling analysis to be performed on normal workstations, thereby reducing the dependency on specialized hardware as technical expertise can be trained. The use of Data Diodes and VPN in the architecture is a feasible secure solution as it is already being used by other industries. VPN uses AES encryption, according to Bruce Schneier's calculations in his book Applied Cryptography; he concluded that brute-force attacks against 256-bit keys will be infeasible unless computers are built from something other than matter and occupy something other than space (The Doghouse: Crypteto, 2009). Data diodes on the other hand are basically electrical diodes that allow electricity to flow in only one direction. It's hardware design makes it 100 percent impossible to allow data to flow in the opposite direction than intended. This means that the pseudo air-gap design can ensure data integrity is not corrupted at the central repository as it can only flow out and not flow in. Overall, the cost of a data diode is a fraction of setting up new digital forensics labs at various locations. Hence, this architecture is highly cost effective and secure.

B. Legal and ISO Feasibility

The alternative process model must align with existing legal frameworks and regulations governing digital forensics to ensure the admissibility of evidence in court. This includes compliance with chain of custody requirements, maintaining the integrity of evidence, adhering to standards for data handling and preservation, and respecting privacy and data protection laws. By maintaining existing digital forensics lab, a lot of the compliance are already in place. The additional part in the alternative model is the remote sites and electronic data transfers. ISO/IEC 17025-2017 in point 5.4 (ISO/IEC 17025) has made clear mention that laboratories carrying out activities should meet the requirement of the document regardless of location be it permanent facilities, at sites away from its permanent facilities, in associated temporary or mobile facilities or at a customer's facility. Hence, there are no compliance issues surrounding the existence of remote mobile forensics lab. It is of course crucial to ensure a chain of custody and evidence integrity is maintained when accessing evidence from remote analysis hubs. This can be done by implementing secure protocols for data transfer and access control, maintaining detailed audit logs, employing cryptographic techniques for tamper detection, and documenting all interactions with the remote evidence. All of which is well in compliance of ISO/IEC 27043-2015 in point 9.5 (ISO/IEC 27043:2015) which clearly states the transportation of digital evidence can be done physically or electronically. If the evidence is transported electronically, special precautions must be taken to preserve the integrity and chain of custody, such as encrypting and digitally signing data. A potential legal hurdle may come from jurisdictional issues and cross border data transfer regulations. Addressing these challenges may require legal expertise and close collaboration with relevant stakeholders to ensure admissibility of electronically stored information (ESI) in court.

C. Expert Opinion Feasibility

Domain experts from Digital Forensics Department MCMC participated in a survey to validate the feasibility of the

alternative model. Additionally, the survey was also posted on the largest global online community for Digital Forensics and Incident Response to get expert opinion. The survey began with background information of the respondents such as their position and number of years in that position to assess their credibility. The survey then followed suit with backlog assessment such as number of backlogs they currently hold in their digital forensics lab to validate the need of a new model. Finally, the survey proceeds to seek validation of the feasibility of the model from the technical, legal and regulatory standpoint. Based on the respondents' feedback, they all admit backlog issues in their digital forensics lab and are open to the idea of an alternative process model. The alternative process model is seen as somewhat feasible, but its success depends on overcoming several key challenges. One out of four respondent expressed low confidence in secure data transfer, while the rest was more optimistic concerning evidence integrity and data security in transit. A respondent added that the remote workstation reliability will require validation of the tools used to maintain court-acceptable evidence standards. The model may also require infrastructure upgrades such as high-speed networks to accommodate large data transfers. Other than that, the experts all agree that for a successful adoption of the alternative process model, there is a need for investment in technology, training and policy adjustments. The alternative process model offers promising efficiency improvements and is feasible albeit with potential technical, operational, and security challenges.

V. CONCLUSION

The alternative process model addresses three interconnected challenges faced by law enforcement agencies in mobile forensics: a shortage of trained personnel, limited and expensive operational digital forensics labs, and a growing backlog of devices. Key features of the alternative model are the evidence handling process and the use of secure networking concepts such as pseudo air-gapped networks and Virtual Private Networks (VPNs) in its architecture design to integrate with existing digital forensic labs complemented by analysis hubs distributed across different locations. In summary, this research contributes to advancing the field of mobile forensics by proposing a practical and innovative solution to alleviate backlog cases. Overall, the research questions were answered successfully through theoretical analysis and engaging the digital forensic community as is the scope and methodology chosen for this research.

VI. FUTURE WORKS

In the future, further refining and validating the feasibility of the alternative model can be done by looking into Y2Q, short for "Year to Quantum" and how it may affect the model. Y2Q refers to the potential date when quantum computers could break current public-key cryptography. This could lead to the decryption of sensitive data and a major disruption to various systems. It's a concern that has prompted many to consider migrating to quantum-safe cryptographic algorithms. Adjustments can be made to enhance the model's feasibility and potential impact on reducing backlogs in law enforcement agencies.

ACKNOWLEDGMENT

All praises and thanks to Allah for this opportunity. My sincere appreciation to my supervisor Dr. Maheyzah Md. Siraj for the guidance, advice, critics and understanding in this study.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest regarding the publication of this paper

REFERENCES

[1] A., H. (2024). *What is VPN*. Hostinger. https://www.hostinger.my/tutorials/what-is-vpn

[2] Casey, E. F. (2009). Investigation delayed is justice denied: Proposals for expediting forensic examinations of digital evidence. *Journal of Forensic Sciences, 54*, 1353–1364. https://doi.org/10.1111/j.1556-4029.2009.01150.x.

[3] Kao, D.-Y., & N.-C. (2020). A triage triangle strategy for law enforcement to reduce digital forensic backlogs. *22nd International Conference on Advanced Communication Technology (ICACT)* (pp. 1173–1179). https://doi.org/10.23919/ICACT48636.2020.9061240.

[4] Advenica. (n.d.). *Data diodes – An effective alternative to air gaps*. https://advenica.com/learning-center/blog/data-diodes-an-effective-alternative-to-airgaps.

[5] Crime Museum. (n.d.). *Edmond Locard*. https://www.crimemuseum.org/crime-library/forensic-investigation/edmond-locard/.

[6] Financial Crime Academy. (2023). *Evidence management: The importance of management in evidence*. https://financialcrimeacademy.org/evidence-management/.

[7] Gillis, A. S. (2022). *Air gapping*. TechTarget. https://www.techtarget.com/whatis/definition/air-gapping.

[8] Haluszka, E., & ——. (2023). *A comparative review of ISO standards for digital forensics laboratory accreditation*. https://doi.org/10.13140/RG.2.2.13619.40480.

[9] Hevner, A. (2007). *A three cycle view of design science research*. ResearchGate. https://www.researchgate.net/publication/254804390.

[10] His Majesty's Inspectorate of Constabulary and Fire & Rescue Services. (2022.). *An inspection into how well the police and other agencies use digital forensics in their investigations*. https://hmicfrs.justiceinspectorates.gov.uk/publication-html/how-well-the-police-and-other-agencies-use-digital-forensics-in-their-investigations/.

[11] Hitchcock, B., & L.-K. (2016). Tiered forensic methodology model for digital field triage by non-digital evidence specialists. *Digital Investigation, 16*, S75–S85. https://doi.org/10.1016/j.diin.2016.01.010.

[12] Hoare, A. (2023). *What is ISO 17025 and why is it important?* Ideagen. https://www.ideagen.com/thought-leadership/blog/what-is-iso-17025-and-why-is-it-important.

[13] Forensic Notes. (2023). *How to become a digital forensics professional in 2023*. https://www.forensicnotes.com/category/digital-forensics-dfir/.

[14] International Organization for Standardization. (2017). *ISO/IEC 17025:2017 testing and calibration laboratories*. https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html.

[15] ISO. (2022). *ISO/IEC 27001:2022—Information security management systems—Requirements*.

[16] ISO. (2012). *ISO/IEC 27037:2012—Guidelines for identification, collection, acquisition and preservation of digital evidence*.

[17] ISO. (2015). *ISO/IEC 27043:2015—Incident investigation principles and processes*. Geneva, Switzerland.

[18] Kelly, M. (2023). *Addressing Tennessee digital evidence backlog*. Yahoo News. https://news.yahoo.com/addressing-tennessee-digital-evidence-backlog-000000634.html.

[19] Koleoso, R. A. (2018). *A digital forensics investigation model with digital chain of custody for confidentiality integrity and authenticity*. Conimsconference.com.ng.

[20] Devries, M., & E., S. (2024). A survey on the quantum security of block. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3520364

[21] Mazumdar, K. (2024). State-of-the-art analysis of quantum cryptography: Applications and future prospects. *Frontiers*. (Authors: Swastik Kumar Sahu & Kaushik Mazumdar)

[22] dscout. (2016). *Mobile Touches: dscout's inaugural study on humans and their tech*.

[23] Montasari, R. (2016). *The comprehensive digital forensic investigation process*. University of Derby.

[24] Otterloo, S. van. (2017). *Information security and PDCA (Plan–Do–Check–Act)*. https://ictinstitute.nl/pdca-plan-do-check-act/.

[25] de Braekt, R. I., & N.-A.-K. (2016). Increasing digital investigator availability through efficient workflow management and automation. *4th International Symposium on Digital Forensic and Security (ISDFS)* (pp. 68–73). https://doi.org/10.1109/ISDFS.2016.7473520.

[26] Rosehaizad, A. F. (2022). *Improvement of information quality in digital forensic guideline*. Universiti Teknologi Malaysia.

[27] Rowlingson, R. (2004). A ten step process for forensic readiness. *International Journal of Digital Evidence, 2*(3).

[28] Sammons, J. (2015). *The basics of digital forensics* (2nd ed.). Elsevier.

[29] Sarah, K. T., Miratun, M. S., & Zabri, A. T. (2018). An analysis of digital forensic laboratory. *World Academy of Science, Engineering and Technology*.

[30] Scanlon, M. (2016). Battling the digital forensic backlog through data deduplication. *Sixth International Conference on Innovative Computing Technology (INTECH)* (pp. 10–14). https://doi.org/10.1109/INTECH.2016.7845139

[31] Department of Standards Malaysia. (n.d.). *Skim Akreditasi Makmal Malaysia (SAMM)*. https://jsm.gov.my/accreditation/resources-accreditation/general.

[32] Taylor, P. (2023). *Number of smartphone users worldwide*. Statista. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

[33] Schneier, B. (2009, September 30). *The Doghouse: Crypteto*. https://www.schneier.com/blog/archives/2009/09/the_doghouse_cr.html.

[34] The Stack. (2023, January 3). *Deloitte UK police digital forensics contract*. https://www.thestack.technology/deloitte-uk-police-digital-forensics-contract/

[35] Valjarevic, A., & ——. (2015). Comprehensive and harmonized digital forensic investigation process model. *Journal of Forensic Science, 60*, 1467–1483.

[36] Lavie, E., & Lim, C. C. (2022). Improved coherent one-way quantum key distribution for high loss channels. *Physical Review Applied, 18*(6), 064053. https://doi.org/10.1103/physrevapplied.18.064053

[37] Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevičius, R., et al. (2021). Post-quantum era privacy protection for intelligent infrastructures. *IEEE Access, 9*, 36038–36077. https://doi.org/10.1109/access.2021.3062201

[38] Duarte, F. (2025, June 5). *Time spent using smartphones (2025 statistics)*. Exploding Topics. https://explodingtopics.com/blog/smartphone-usage-stats.