

DIGITAL FORENSICS ANALYSIS AND INVESTIGATION OF CORPORATE ESPIONAGE: A RESEARCH AND FORENSIC ASSESSMENT OF THE QUANTUM TECH AI PATENT THEFT CASE

Student Name	: MD Shibli Hossain
Student ID Number	: 2517990
Programme	: MSc Cybersecurity and Digital Forensics
Module	: Digital Forensics Analysis
Module Code	: ACCA7031
Lecturer	: Dr. Mohamed Ghanem
Internal Verifier	: Mr. Munyaradzi Murira
Assignment Title	: Research, Analyse and Investigate Cybersecurity incidents and perform digital forensic assessment

Submission Deadline : 17, August 2026

Table of Contents

Task 1: Research on Digital Forensics.....	4
Introduction.....	4
Current State of Digital Forensics.....	4
Digital Forensics and Cybersecurity.....	5
Emerging Trends and Challenges	5
National and International Job Market	6
Task 2: Digital Forensic Investigation Plan	7
Case Overview	7
Investigation Methodology	7
Evidence Identification	8
Evidence Preservation.....	Error! Bookmark not defined.
Forensic Evidence Acquisition	10
Digital Evidence Examination	12
Evidence Analysis and Correlation	14
Forensic Reporting.....	14
Evidence Acquisition Strategy.....	15
Chain of Custody Documentation.....	15
Evidence Labelling and Secure Packaging.....	Error! Bookmark not defined.
Evidence Transfer and Secure Storage	16
Hash Verification and Integrity Validation.....	16
Legal Admissibility and Documentation	Error! Bookmark not defined.
Planned Evidence Analysis	17

Digital Artefact Examination Strategy	17
Communication Analysis	17
Multimedia Analysis	19
Document Analysis	21
Metadata Analysis	22
USB and File System Examination.....	23
Timeline Reconstruction	23
Cross-device Correlation	24
Legal, Ethical and Reporting Considerations	24
Legal Admissibility	24
Ethical Responsibilities.....	25
Investigation Limitations	25
Recommendations	25
Expected Deliverables and Conclusion	26
References.....	26

Task 1: Research on Digital Forensics

Introduction

Digital forensics has emerged as a strategic resource that enables organisations to conduct investigations about cyber incidences in an orderly fashion by finding answers to cyber incidences by identifying, acquiring, preserving and analysing digital evidence. Besides aiding law enforcement, forensic investigations assist organisations in becoming resilient and allow them to justify their decision in responding to incidents and come up with reliable evidence that can be used in fighting insider threats, intellectual property theft and corporate espionage.

Digital forensics is also the key factor in preserving trust in organisations as it makes sure that digital investigations adhere to accepted legal and ethical processes. The field is concerned with the original evidence being preserved and not distorted by other individuals when doing acquisition and analysis. The modern forensic investigations have compelled the investigators to follow internationally recognized rules, maintain proper records and record all the work performed by the investigator. This methodological process will make evidence admissible in a court of law, reproducible, and reliable, and will justify an open-minded decision-making process in cases of responding to cybersecurity incidents.

Current State of Digital Forensics

Digital forensics is increasingly concentrated on an enterprise setting where investigation of cloud platforms, mobile devices and distributed networks are involved instead of isolated computers. Globally, cybercrime losses are estimated to be more than US 10 trillion annually, which explains the need to have scalable forensic capabilities (Casino et al., 2022). FTK Imager is another handy acquisition tool that can be employed in performing forensic imaging and hash checking, although the Cellebrite is oriented towards mobile extraction, and the Autopsy is oriented towards the examination of evidence. Such a combination of these tools will enhance the reliability of the evidence and efficiency of investigations in the complicated digital worlds.

The use of remote working, cloud storage, and mobile applications has greatly contributed to the increased diversity of digital evidence that can be used during investigations. The organisations should now scrutinize the information stored in various platforms, such as smartphones, cloud

services, external storage devices, and enterprise servers (Patel and Mann, 2025). Therefore, forensic investigators are becoming more dependent on the integrated toolsets as opposed to one application. Forensic imaging, file system examination and artefact examination should be integrated to ensure completeness of evidence with minimal probability of overlooking any important digital traces that could help in an investigation.

Digital Forensics and Cybersecurity

Digital forensics is applied to support cybersecurity to transform the alert notification into the evidence that could be presented in the court. Unlike in the case of cybersecurity where it is more focused on prevention and containment of threats, forensics identifies the origin of the attack, the motive and damage by correlating evidence and reconstructing the timeline (Kozlowski, 2025). This integration is especially useful when it comes to insider threat and corporate espionage investigations where the integrity of evidence has a direct impact on organisational responsibility and the resultant legal implementation.

In addition to the incident investigation, digital forensic evidence may be crucial in the organisational risk management by indicating the gaps in the security controls, system configurations and employee behaviours. The experience acquired in a forensic analysis can enable organisations to improve access controls further, improve employee awareness programmes, and improve incident response procedures to mitigate future security incidents (Tyagi et al., 2024). The collaboration between cybersecurity specialists and forensic investigators can enable them to detect threats more quickly and collect evidence and restore the incident reasonably. This integrated approach enhances organisational security position, enables informed decision making, and promotes stability in the long term through preventing similar cyberattacks and strengthening an overall cybersecurity governance.

Emerging Trends and Challenges

Forensic efficiency is being enhanced by artificial intelligence, which automates artefact classification and anomaly detection, and cloud, mobile and Internet of Things investigations are broadening the areas of forensics. Anti-forensic techniques and rapid multiplication of e-evidence are however, thwarting timely investigations using encrypted messages. Distributed cloud

infrastructures also have complexities with respect to jurisdiction and evidence collection. Later it is an important requirement to ensure the chain of custody and prove forensic integrity and make them legally admissible regardless of the level of technological advancement.

The other critical issue is the growing amount of digital evidence produced by contemporary organisations. The existence of terabytes of data within different devices, cloud-based systems, and network systems is one of the challenges that investigators are forced to cope with; these are time-consuming and resource-intensive to analyze manually. Automation, artificial intelligence, and machine learning are increasingly becoming more helpful to assist investigators prioritize relevant artefacts, detect anomalies, and discover suspicious patterns in a more efficient way (Singh and Mishra, 2023). However, it is still human professionalism to interpret forensic results, validation of automated results, accuracy in investigation, legal admissibility and objective conclusions that can not be challenged during investigations by the court and organisations.

National and International Job Market

The level of digital forensic specialists has continued to increase with the more sophisticated cyber threats that organisations are increasingly encountering. Digital Forensic Investigators and Cyber Incident Responders work in the law enforcement and government and DFIR Analysts and Mobile Forensic Examiners are employed in the private sector as a part of multinational investigations in the United Kingdom. The practical use of FTK Imager, EnCase, Cellebrite, Autopsy, chain-of-custody management and professional forensic reporting is starting to take precedence among employers as the growing strategic importance of evidence-based cyber investigations in all sectors worldwide.

The digital forensics profession has seen a rise in the importance of professional certifications and continuous training. Most employers would prefer applicants with familiar certifications, practical laboratory experience and a wealth of knowledge regarding forensic standards and investigative methods and legal procedures. Strong analytical thinking skills, technical problem-solving skills, report writing skills, and case presentation in a courtroom are also necessary as the investigators must be able to express complicated technical findings in an understandable manner to non-technical audiences, legal experts and organisational stakeholders (Sharma et al., 2022). As cybercrime is dynamic, maintaining their suitability and relevance to stay abreast with the

dynamism of digital forensic investigation will require life-long learning, professional certification and skill development.

Task 2: Digital Forensic Investigation Plan

Case Overview

Quantum Tech has received information that its AI chip design patent (QT-AI-2025) is illegally violated, which means that a corporate spy may have targeted it. Emma is a senior engineer, who is said to have passed on confidential intellectual property via Joe, an intermediary to Norman who is representing the purchasing organisation. The question will be to find out, can we have digital evidence on the mobile devices and on a USB drive that may objectively substantiate these allegations and yet retain the integrity of evidence and admissibility into the legal process during the forensic process.

The purported stealing of the QT-AI-2025 artificial intelligence chip patent needs to be investigated in a structured digital forensic manner to ascertain whether or not confidential information was accessed, copied, or exchanged, illegally using digital devices. FTK Imager has been chosen as the main tool of acquisition and examination in this investigation since it allows forensic investigators to obtain forensic images without damaging the integrity of the digital evidence. The software provides an analysis of file systems, application data, multimedia files and metadata within a read only environment without changing the original evidence.

The forensic investigation is aimed at finding evidence that can prove unauthorized communications or transfer of confidential information between Emma, Joe, and Norman. Relying on obtained evidence on the mobile devices, investigators will look into application directories, WhatsApp media folders, downloaded documents, pictures, voice recordings, and cache files among other user-generated content (Almuqren et al., 2024). Not just to ascertain the existence of possibly relevant files but also to find out whether the artefacts can be connected to the nature of activity related to the alleged disclosure of the QT-AI-2025 patent.

Artefacts of various Android phones, such as Huawei, Nokia, Samsung Galaxy A13 and Ulefone, can also be found in the available evidence. These devices provide different kinds of digital

evidence, such as multimedia files, downloaded documents, WhatsApp pictures, voice recordings, application cache files, and directories of Android systems (Patel and Mann, 2025).

The preservation of the integrity of digital evidence at all phases of the forensic process is also another significant part of this investigation. The tool that will help verify the forensic acquisition based on hash algorithms (MD5 and SHA-1) to confirm that the forensic image is identical to the source is FTK Imager.

Investigation Methodology

The application of the study will be in the systematic forensic process which involves identification, recovery, hash confirmation, preservation, examination and reporting of evidence to minimize the evidential pollution and offer consistency of the process. Initially, all digital devices will be uniquely identified, documented and secured using an authenticated chain of custody (Yaacoub et al., 2022). The scans of the removable media will be performed with a hardware write blocker in such a way that no evidence is altered. The FTK Imager will additionally obtain forensic images and simultaneously calculate MD5 and SHA-1 hash values to ensure integrity in the acquisition. The pre-imaging and post-imaging values of hashes are supposed to be the same, which will prove that there has not been a change that occurred during collection. The retained forensic images will be then analyzed with a meticulous examination and all investigative procedures are recorded to offer transparency, repeatability and legal defensibility.

Evidence Identification

The forensic examination started with listing and documenting all digital devices that were provided as evidence during the examination. It was found that four Android smartphones, i.e., Huawei POT-LX1 P Smart, Nokia C2 2nd Edition, Samsung Galaxy A13, and Ulefone Note 14 serve as the main sources of digital evidence. A different identifier of evidence was assigned to each device and a forensic investigation was started. Documenting evidence included the part of capturing the details of the recording device, including its manufacturer, model name, type of the extraction, and the date of acquisition (Sharma et al., 2022). Evidence folders produced in the course of the acquisition process were marked in a systematic manner so as not to be confused when analysing them. The process of acquisition was photographically documented and evidence directories were kept to help in maintaining the chain of custody. The device identifiers and reports

of extraction that were done in the acquisition process were stored so that each forensic image can be identified to a specific source in the investigation process.

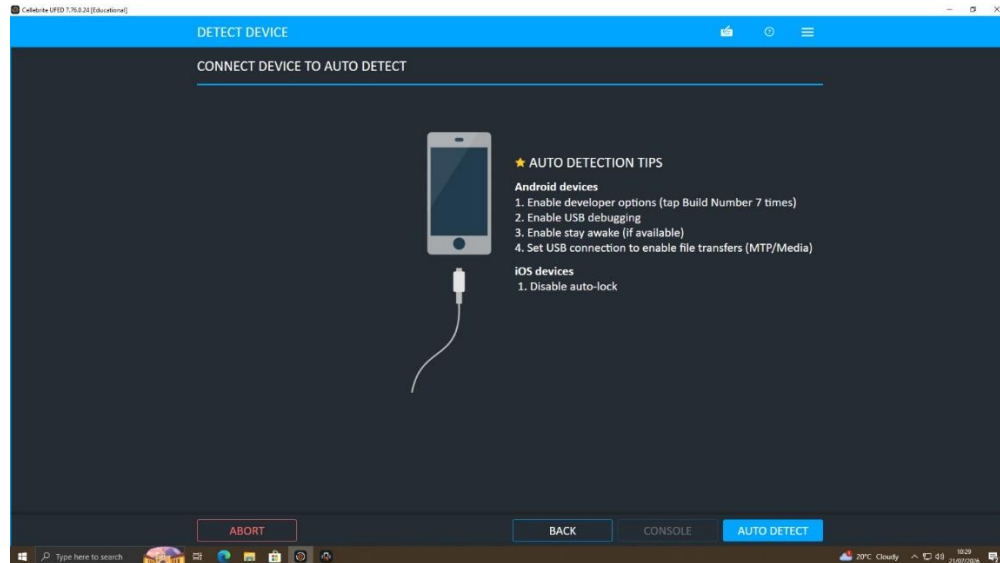


Figure 2.1: Mobile Device Identification

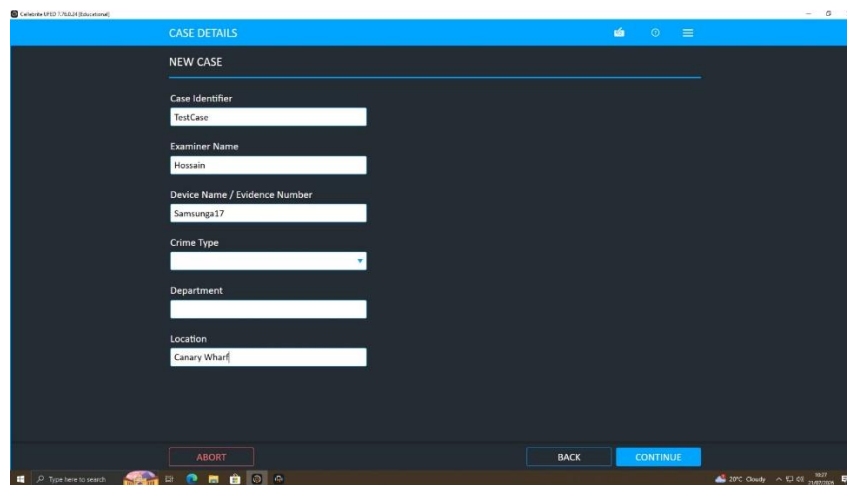


Figure 2.2: Forensic Case Details

Table 2.1: Mobile Device Identification

Evidence ID	Person	Device	Model
E-01	Emma	Huawei	Huawei POT-LX1 P Smart

E-02	Joe	Samsung	Samsung Galaxy A13
E-03	Norman	Nokia	Nokia C2 2nd Edition

Table 2.1 creates a correlation between each individual and the respective mobile device, which gives a clear foundation for further cross-device forensic analysis.

Forensic Evidence Acquisition

The evidence presented during a case was the forensic images which were already acquired and which had been utilized in the investigation. The mobile devices were acquired in the form of a file system acquisition technique, which enabled investigators to analyze user generated data, application folders, multimedia files, downloaded documents and Android system directories. The forensic evidence was loaded and analyzed in a structured and read-only setting using FTK imager. The MD5 and SHA-1 cryptographic hash values were obtained and compared to the stored acquisition hash in the process of acquisition verification (Bruno and Shivanthana, 2026).

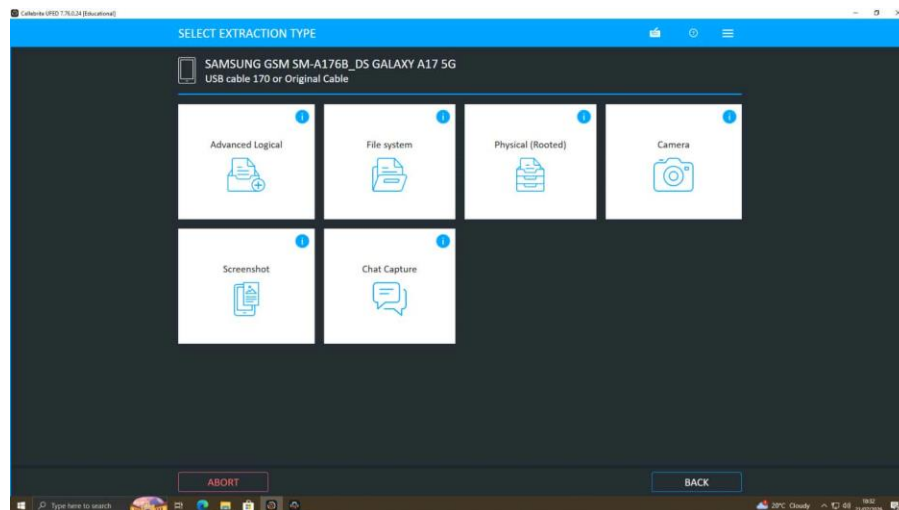


Figure 2.3: Cellebrite Extraction Options

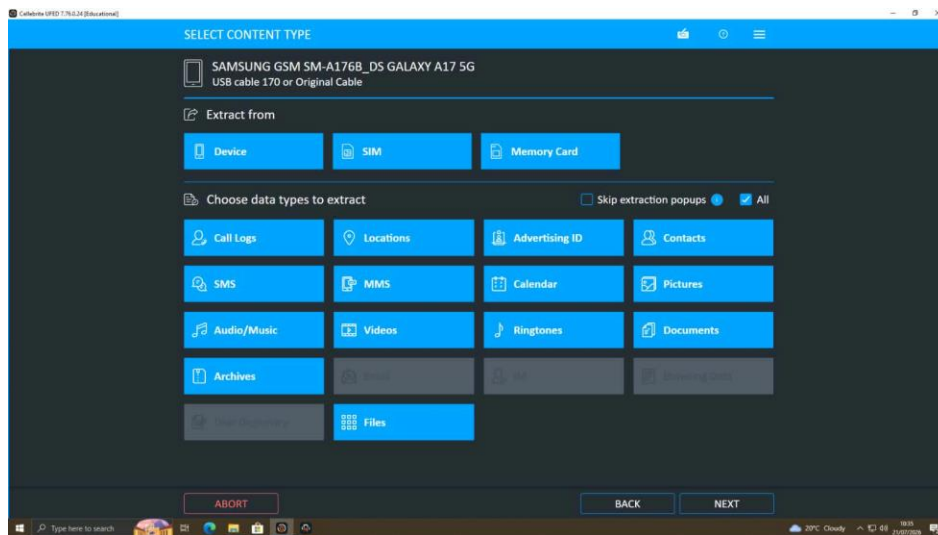


Figure 2.4: Mobile Data Selection

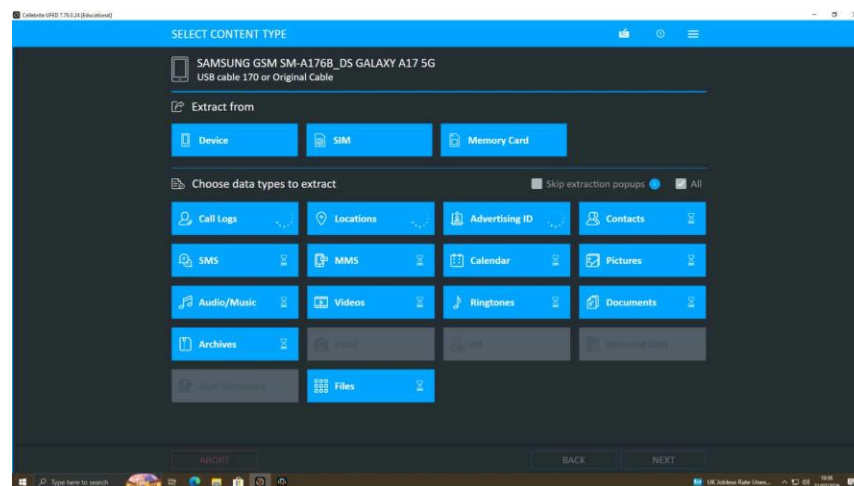


Figure 2.5: Cellebrite Data Extraction

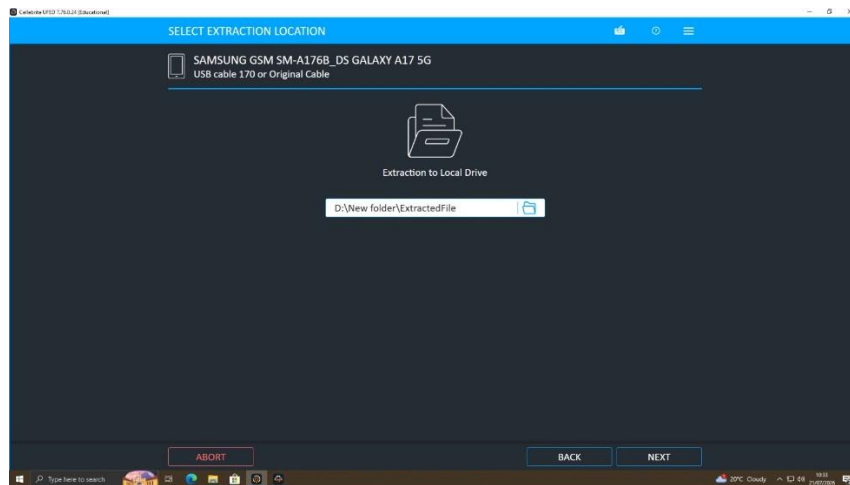


Figure 2.6: Evidence Extraction Location

Digital Evidence Examination

Digital evidence was analyzed using the FTK Imager, which involved loading the forensic images, and (step by step) browsing through the extracted Android file systems. The data under study were user-created artefacts including WhatsApp media folders, downloads, videos, images, audio records, video, applications cache directories and Android system files. Multimedia files, voice recordings, PDF files, and application data were reviewed to find information that might be of interest to the investigation (Alshammari, 2023). Where possible, metadata like file names, directory path names, timestamps, and file sizes were examined to determine the context of artefacts recovered. The analysis also took into account what is available in terms of timeline with the use of file timestamps and all the artefacts that could be accessed were recorded and stored to be further examined in forensic analysis without making any changes in the original evidence.

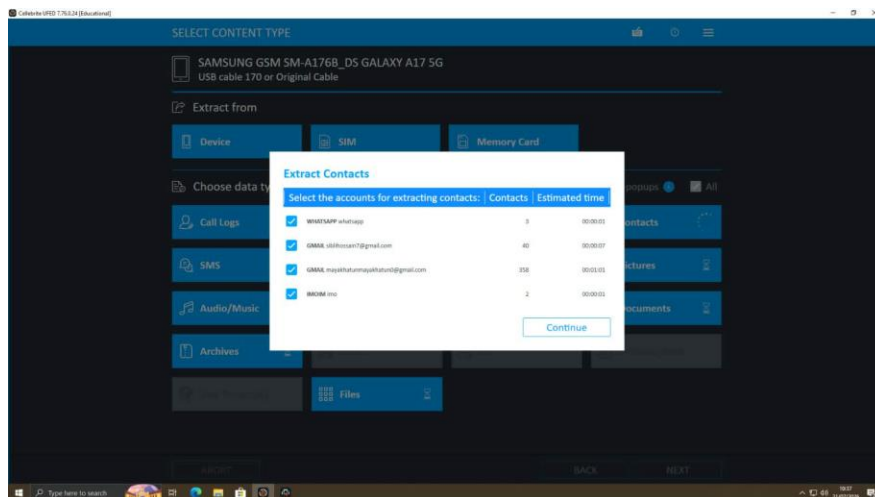


Figure 2.7: Application Contact Extraction

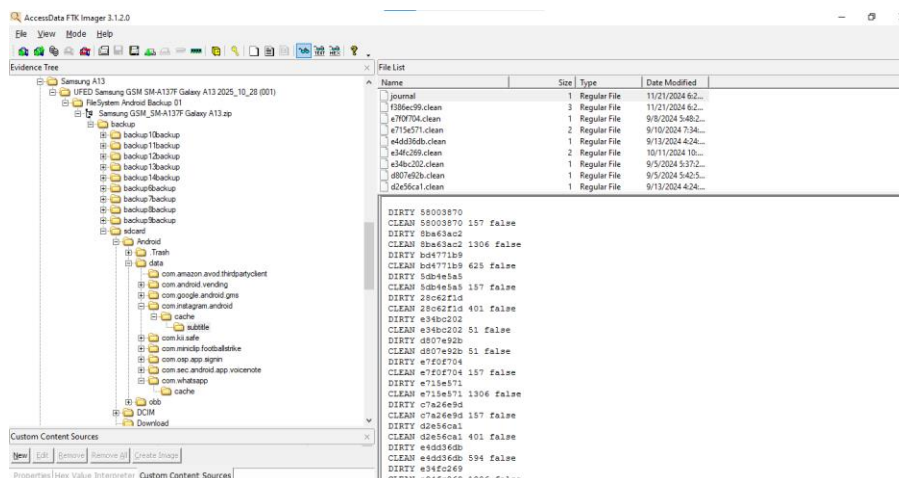


Figure 2.8: Samsung Evidence File System

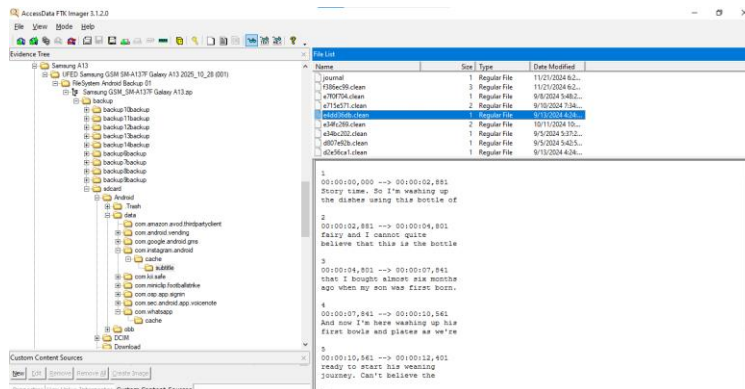


Figure 2.9: Recovered Text Evidence

(Source: FTK Imager)

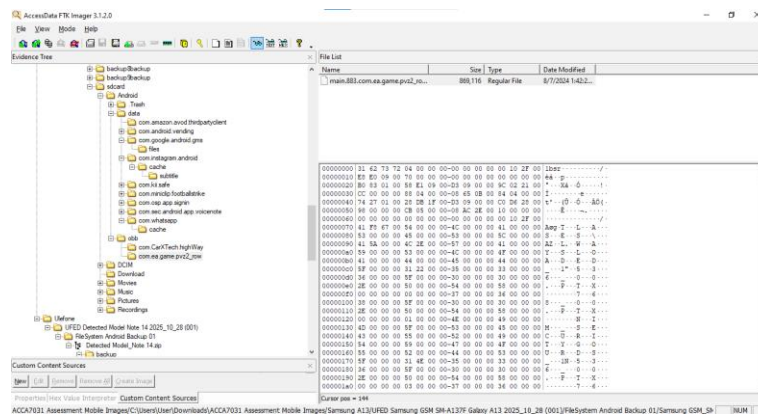


Figure 2.10: Application File Examination

Evidence Analysis and Correlation

The analysis step was followed by comparing the evidence on the Huawei of Emma, Samsung Galaxy A13 of Joe, and the Nokia and Ulefone of Norman to identify the possible relationships between the devices. Artefacts of communication (downloaded multimedia files, WhatsApp media folders, available application data) were analysed. Metadata and file timestamps were analyzed to help to reconstruct potential activity timelines and find any evidence of file sharing or communication between Emma, Joe, and Norman. A cross-device comparison was performed to find out the potential of shared artefacts or files to the accusations of an intellectual property theft of the QT-AI-2025 patent (Nath et al., 2024).

Forensic Reporting

The results that were acquired in the FTK Imager examination were recorded in a systematic manner to promote transparency, reproducibility, and legal admissibility. The operation of forensic examination, artefacts collected and evidence directory schemes were shown in screenshots taken during the investigation. The evidence inventory, the results of hash verification and the recovered file data were placed in the structured evidence tables (Loffi et al., 2025). A summary of all significant artefacts was made including their forensic value and metadata. Chain-of-custody records were kept during the investigation, allowing the preparation of an objective and forensic report of findings made on evidence-based conclusions, and professional interpretations in line with the accepted digital forensic investigation practices.

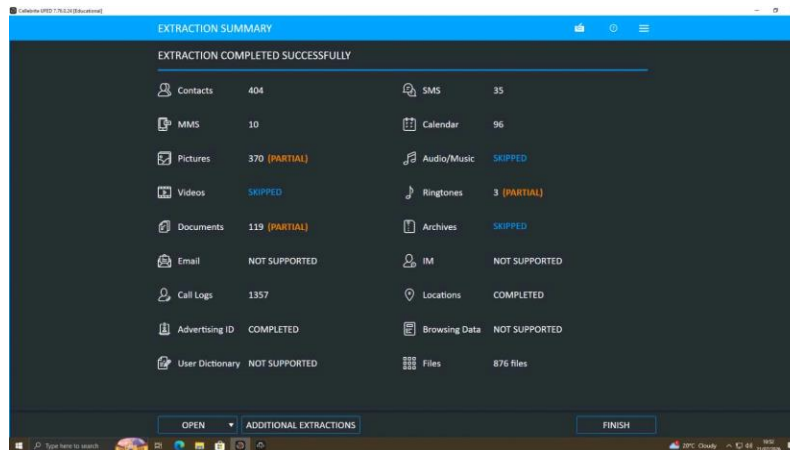


Figure 2.11: Extraction Results Summary

Evidence Acquisition Strategy

Forensic acquisition of the four Android smartphones and the corresponding USB flash drive found in Table 2.1 will be performed since they are the main sources of possible evidential artefacts. Prior to the acquisition of each mobile device, each will be linked with its known owner and given a special evidence identifier. When possible, a bit-to-bit forensic image will be created, and MD5 and SHA-1 hash values will be compared to ensure the integrity of each image using FTK Imager (GonzoArias et al., 2024). The process of acquisition will not incorporate any alteration of the original devices, and it is in line with the accepted forensic principles. A complete chain-of-custody will consist of an identification of the evidence, the name of the owner of the device, the date and time of acquisition, the name of the examiner, information on how the evidence was obtained and where it was safely stored.

Chain of Custody Documentation

To ensure authenticity, traceability and admissibility of digital evidence in the court of law, it is necessary to have an unbroken chain of custody. Immediately the devices were identified, evidence items were assigned a unique identifier of the evidence and added to the investigation record. The chain of custody document entailed details on the description of the evidence, date of its acquisition and time, who carried out the examination, how it was acquired, the location where it was kept and all the other transactions it had undergone since then with the evidence. The documentation of all handling activities was done to develop complete accountability in the investigation (Patil et

al., 2024). The integrity and ownership of any digital artefact might be established by the proper recording, not only during the process of the forensic examination, but also in case of any legal proceedings.

Evidence Transfer and Secure Storage

During the investigation, any evidence transfers were meticulously recorded so as to avoid continuity of evidence. Whenever digital evidence was transferred between the investigators or the examination location, the date and time of transfer, the sender, receiver and the purpose of the transfer was recorded in the chain of custody documentation. Forensic evidence was only accessible to authorised persons. Evidence storage in secure evidence storage facilities was done to minimize the possibility of accidental alteration, theft or loss of original devices and forensic images. FTK Imager was operated in a read-only setup during examination to make sure that no alterations were made to the original forensic evidence but still enable investigators to examine the recovered digital artefacts in a secure environment.

Hash Verification and Integrity Validation

The authenticity of all forensic images was proved with the help of the cryptographic hash verification using MD5 and SHA-1. Following the acquisition process, the FTK Imager hash values had been calculated on all the forensic images and a subsequent comparison of the acquired hash values to the acquired hash values. The successful comparison of MD5 and SHA-1 has made sure that there was no change in the process of evidence acquisition, storage, and examination (Pandey et al., 2024). The use of hash verification thus offered mathematical confirmations that the forensic evidence was the same as the original source during the investigation and therefore the reliability and authenticity of recovered digital artefacts.

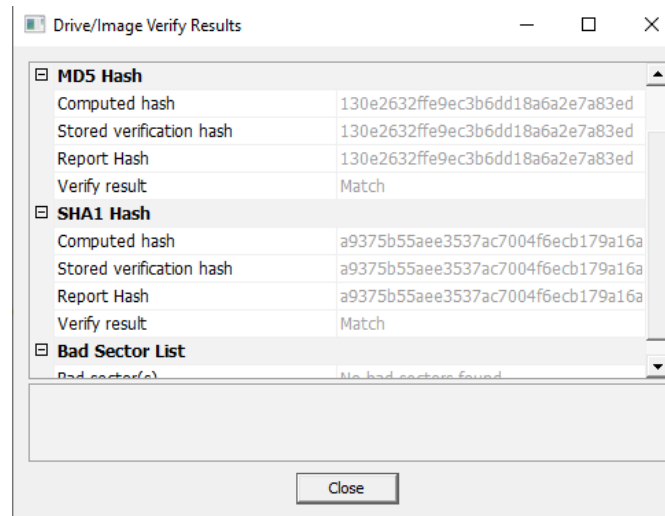


Figure 2.12: Hash Verification Results

Planned Evidence Analysis

The analysis of evidence will use correlation approach to enhance reliability of the results by analyzing correlation of various digital artefacts. Communication logs of WhatsApp, email, Instagram messages and call logs will be analyzed to locate communications of the illegal transfer of the QT-AI-2025 patent (NIST, 2026). The chronology of communications, file transfers and communication between Emma, Joe and Norman will be determined by recreation of the timeline. To determine the presence or absence of a copy and/or transfer of the proprietary information by Emma, the USB will be searched by searching and reviewing the patent documents, CAD files and metadata, such as file creation, modification and access date. The communication records will be matched with the records of the calls and file metadata to confirm the payment talks, appointment of meetings and file transfers.

Digital Artefact Examination Strategy

Communication Analysis

The communication analysis was intended at uncovering digital artefacts, which could provide insight into the communications between the alleged culprits of the alleged intellectual property theft. The Android application directories, and accessible folders were systematically searched in the FTK Imager examination to locate communication related artefacts. Special attention was paid



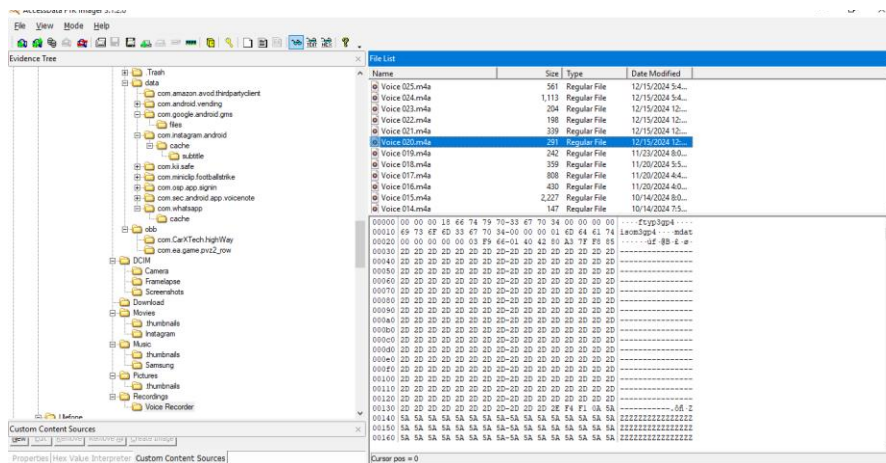


Figure 2.19: WhatsApp Voice Evidence

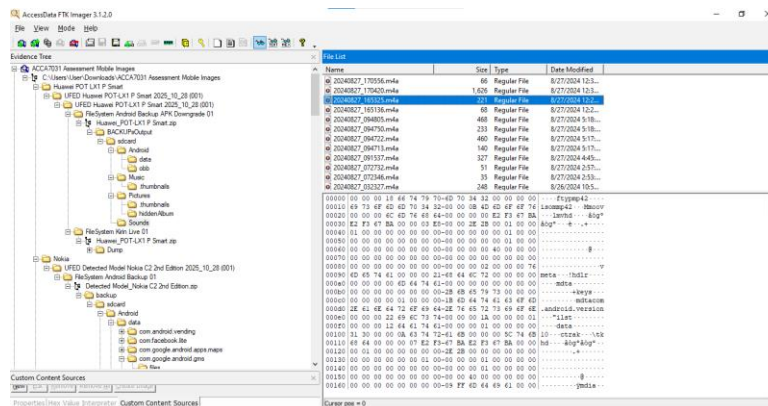


Figure 2.20: Huawei Audio Evidence

Document Analysis

Document analysis focused on files that had a potential of holding confidential organisational information or evidence in connection with the supposed theft of the QT-AI-2025 patent. Through FTK Imager Browsing of document directories, download folders and application storage location where user generated documents are typically stored was done through FTK Imager. This analysis was done on PDF files, ZIP files which were compressed, text files and other documents which were accessible to the user which had been acquired by the forensic images. Installing files and reports were looked at as they were downloaded to determine the potential evidential value of this information. Special focus was provided to finding documents in relation to engineering designs, patent information, confidential reports or intellectual property.

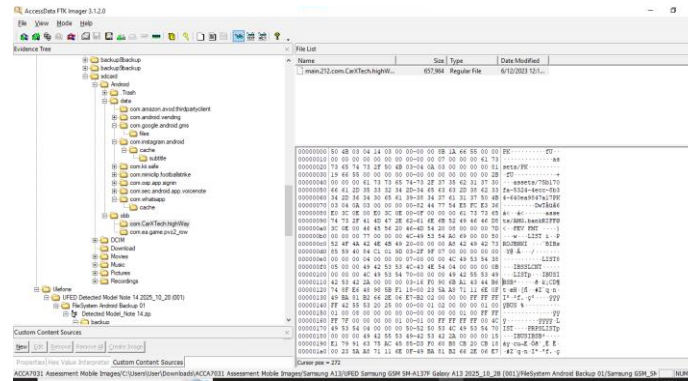


Figure 2.21: Archived File Examination

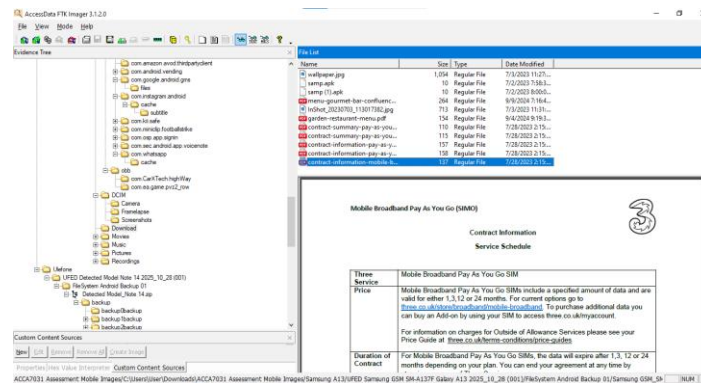


Figure 2.22: Recovered Document Evidence

Metadata Analysis

The analysis of metadata was conducted to give some contextual information about recovered digital artefacts. FTK Imager enabled the investigators to see the properties of the files like the directory structure, file names, file sizes, date of creation, date of modification and the timestamps of access where feasible. The order of user operations was formed through these metadata attributes, and the time of the creation or modification of particular artefacts (Mansoor et al., 2026). Information on file path was also helpful in determining which applications were used to create particular files. In places, metadata would be compared between various artefacts to discover links between evidence found and aid further forensic interpretation. This procedure helped to ensure consistency and traceability of digital evidence during the investigation.

USB and File System Examination

The forensic evidence available was mainly extracted Android file systems which were analyzed with FTK Imager. The search was conducted by conducting a systematic search of user directories, application folders, downloaded files, multimedia artefacts and available backup data. Another aspect that the researcher considered during the investigation was the presence of hidden directories of applications, compressed archives, and system-generated directories (Maurya and Mishra, 2025). Signatures of files and structure of the directory were checked to determine the nature and origin of recovered files. Integrity of evidence was ensured by making continuous hash verification with MD5 and SHA-1 values that were generated at the time of acquisition. This verification would be to show that the forensic pictures were not in any way distorted during the investigation and the evidence retrieved was authentic and reliable before the law.

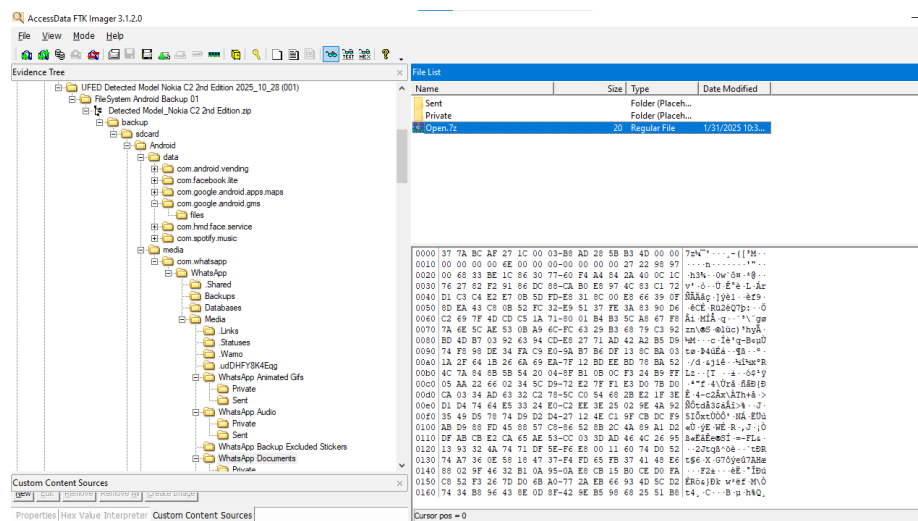


Figure 2.23: WhatsApp Archive Evidence

Timeline Reconstruction

The reconstruction of the timeline was also based on the devices that were investigated and available metadata and file timestamps. Creation dates, modification dates and directory information were verified so that in as far as possible the chronological order of user actions can be established. Even though no detailed communication logs were found in the evidence presented, the timestamps related to multimedia files, downloaded documents, and artefacts created by applications helped to recreate some of the user activity. Such time sequence enabled the

investigators to classify potential times the devices were used, documents were accessed and production of multimedia that could assist in comprehension of the general chronology of the events during the investigation.

Cross-device Correlation

In the cross-device correlation, artefacts obtained on Huawei POT-LX1 P Smart, Samsung Galaxy A13, Nokia C2 2 nd Edition and Ulefone Note 14 were compared to perform the cross-device correlation. The possible links between the analyzed devices were sought in the application directories of the same nature, WhatsApp media files, multimedia files, downloaded documents, and available metadata (Prabowo et al., 2025). A comparative analysis was done to determine whether there could be common artefacts, copied files or duplicated application data as a way of demonstrating interactions between Emma, Joe and Norman. Although no obvious evidence could be found to show beyond reasonable doubt that the devices in question were utilized to steal the QT-AI-2025 patent, the cross-device comparison offered a methodical means to align digital artefacts without infringing on forensic integrity and giving credence to objective investigation results.

Legal, Ethical and Reporting Considerations

Legal Admissibility

Digital evidence can be admissible, provided that it can be shown that the evidence has not been altered in any way during the forensic investigation. In this case, the forensic analysis that ensued was in line with accepted digital forensic practices so that all evidence that was retrieved could be in good condition. Identification, acquisition, examination, storage and transfer of every piece of evidence was documented in chain of custody, which gave full traceability to the evidence during the investigation. The FTK Imager was set to read-only mode to prevent changes to the original forensic images to analyze them. Moreover, MD5 and SHA-1 hash validation was conducted to validate that the forensic images were the same as the obtained evidence (Salah et al., 2025). The fact that the hash values matched, showed that the digital evidence was not tampered with by an unqualified person and could be regarded as valid and admissible in court.

Ethical Responsibilities

Digital forensic investigations are conducted in high ethical standards which are supposed to be maintained by the investigators throughout the investigation process. The investigators are not supposed to invade the privacy of the individuals as they can only search as far as the evidence is involved in the investigation and the investigators are not supposed to search unnecessary personal information and information that are not related to the investigation in the digital devices. Data obtained during the forensic examination but was confidential must be treated carefully and revealed to the people who have been mandated to take part in the investigation. The professional conduct demands that the investigators conduct examinations without bringing personal views and biases in the investigations. All the inferences made in the forensic report must be backed up with verifiable digital evidence instead of conjectures (Ismail and Akram Zainol Ariffin, 2025). This makes the information unbiased and confidential and enhances the credibility of the investigation and confidence in the forensic conclusions drawn.

Investigation Limitations

A full-fledged digital forensic investigation can be influenced by a number of practical limitations. Modern mobile systems tend to be encrypted to prevent unauthorised access to sensitive user data unless appropriate authentication credentials or specific forensic tools are used. Secondly, one cannot be certain that a deleted file and communication records can ever be recovered, particularly when the files are deleted through secure deletion mechanisms. The increasing application of cloud storage and cloud-based messaging services may also have the impact of having valuable evidence existing outside of the actual device being examined. Moreover, some applications create proprietary data formats or encrypted databases which cannot be completely read with FTK Imager alone.

Recommendations

Using the forensic analysis, there are a number of suggestions that can be made to enhance the organisational security and minimise risk of future intellectual property theft. Stronger access control measures should be adopted by organisations as a way of limiting access to sensitive research data based on the principle of least privilege. Data Loss Prevention (DLP) devices will be deployed to make sure that any unlawful transfer of sensitive information via the use of

removable devices or online communication technology is identified and prevented (Serttaş and Al-Turjman, 2025). The use of external storage devices in the corporate environment should be monitored by putting in place USB device monitoring policies to identify and regulate the use of external storage devices. As a routine cybersecurity awareness programme, employees should be trained on insider threats and on the information handling processes. Multi-factor authentication should be used to access the key organisational systems and continuous monitoring of the insider threats is necessary so as to identify the suspicious user behaviour before the significant security events.

Expected Deliverables and Conclusion

The finished investigation will yield forensic photos, chain-of-custody records, an evidence list, communication records, date analysis, metadata records, suspect profiling, and a legally sound decision and practical suggestions on the case to Quantum Tech and the police. All these deliverables will be capable of giving justifiable record of evidence which can be used as a reference during the court proceedings. The known best practices of digital forensic evidence manipulation will be applied to regulate evidence acquisition, preservation and analysis during the investigation to provide integrity, reproducibility, transparency and admissibility to the known best practices of the professional legal system. Digital forensic investigation is an approach to explore, identify, conserve, examine and report on digital evidence in a structured and scientifically validated way, to aid in organisational and legal inquiries. By using the established forensic procedures and making sure that the investigation is well documented, reliability, integrity and reproducibility of digital evidence can be demonstrated successfully. FTK Imager helped to systematically analyse the forensic images at hand and ensured the integrity of the evidence through read-only analysis and hash verification.

References

Almuqren, A., Alsuwaelim, H., Rahman, M.H. and Ibrahim, A.A., 2024. A systematic literature review on digital forensic investigation on Android devices. *Procedia Computer Science*, 235, pp.1332-1352.

Alshammari, A., 2023. Detection and investigation model for the hard disk drive attacks using FTK imager. *International Journal of Advanced Computer Science and Applications*, 14(7).

Bruno, A. and Shivanthana, S., 2026, April. Digital Evidence Extraction And Source Image in Disk Forensics Using Parallel Data Streams. In *2026 Third International Conference on Networking and Communications (ICNWC)* (pp. 1-7). IEEE.

Casino, F., Dasaklis, T.K., Spathoulas, G.P., Anagnostopoulos, M., Ghosal, A., Borocz, I., Solanas, A., Conti, M. and Patsakis, C., 2022. Research trends, challenges, and emerging topics in digital forensics: A review of reviews. *Ieee Access*, 10, pp.25464-25493.

González Arias, R., Bermejo Higuera, J., Rainer Granados, J.J., Bermejo Higuera, J.R. and Sicilia Montalvo, J.A., 2024. Systematic review: anti-forensic computer techniques. *Applied Sciences*, 14(12), p.5302.

Ismail, I. and Akram Zainol Ariffin, K., 2025. The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS One*, 20(9), p.e0331683.

Kozłowski, K., 2025. CORPORATE ESPIONAGE FROM AN INFORMATION SECURITY MANAGEMENT PERSPECTIVE: A CASE STUDY ANALYSIS. *Management & Quality/Zarządzanie i Jakość*, 7(1), p.200.

Loffi, L., Camillo, G.L., De Souza, C.A., Westphall, C.M. and Westphall, C.B., 2025. Management of the chain of custody of digital evidence using blockchain and self-sovereign identities: A systematic literature review. *IEEE Access*, 13, pp.77804-77832.

Mansoor, S.I.U., Shah, S.A. and Wani, S.A., 2026. Digital Forensics and Chain of Custody: Safeguarding the Integrity and Admissibility of Electronic Evidence in Legal Proceedings. In *Legal and Regulatory Perspectives on Electronic Records as Evidence* (pp. 191-218). IGI Global Scientific Publishing.

Maurya, M. and Mishra, S., 2025. Evidentiary Value and Admissibility of Forensic Evidence. *Issue 2 Int'l JL Mgmt. & Human.*, 8, p.4170.

Nath, S., Summers, K., Baek, J. and Ahn, G.J., 2024, October. Digital evidence chain of custody: Navigating new realities of digital forensics. In *2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)* (pp. 11-20). IEEE.

NIST, 2026. Computer Forensics Tool Testing Program (CFTT). available at: <https://www.nist.gov/itl/csd/secure-systems-and-applications/computer-forensics-tool-testing-program-cftt/cftt-7> [Accessed on: 06.08.2026]

Pandey, S., Alam, I., Rahman, R.U. and Patel, S.C., 2024, October. A Comprehensive Framework for Analyzing Metadata from Recovered Deleted WhatsApp Media on Windows. In *The International Conference on Advances in Emerging Trends and Technologies* (pp. 257-271). Cham: Springer Nature Switzerland.

Patel, B. and Mann, P.S., 2025. A survey on mobile digital forensic: Taxonomy, tools, and challenges. *Security and Privacy*, 8(2), p.e470.

Patel, B. and Mann, P.S., 2025. A survey on mobile digital forensic: Taxonomy, tools, and challenges. *Security and Privacy*, 8(2), p.e470.

Patil, R.Y., Patil, Y.H., Bannore, A. and Ranjanikar, M., 2024. Ensuring accountability in digital forensics with proxy re-encryption based chain of custody. *International Journal of Information Technology*, 16(3), pp.1841-1853.

Prabowo, W.A., Mohsen, F. and Selamat, S.R., 2025. WhatsApp mobile applications in the lens of digital forensics: Deciphering the Msgstore. db. crypt14 file. *Journal of Cyber Security and Mobility*, 14(4), pp.823-848.

Salah, S., Amro, B. and Moreb, M., 2025, July. WhatsApp Messenger Forensics: Extracting Insights for Enhanced Learning Analytics in Smart Education. In *2025 International Conference on Smart Learning Courses (SCME)* (pp. 106-112). IEEE.

Serttaş, Z. and Al-Turjman, F., 2025. Usability of cloud-based applications in digital forensics: an experimental study on image acquisition and digital evidence preservation processes. *NEU Journal for Artificial Intelligence and Internet of Things*, 4(2).

Sharma, Y.K., Noval, S.S., Jain, A., Sabitha, B. and Ramya, T., 2022, December. Forensics-as-a-service: A Review of Mobile Forensics. In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 486-491). IEEE.

Sharma, Y.K., Noval, S.S., Jain, A., Sabitha, B. and Ramya, T., 2022, December. Forensics-as-a-service: A Review of Mobile Forensics. In *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)* (pp. 486-491). IEEE.

Singh, S.K. and Mishra, A., 2023. Digital forensics and cybersecurity tools. In *Advancements in Cybercrime Investigation and Digital Forensics* (pp. 367-382). Apple Academic Press.

Tyagi, A.K., Kumari, S. and Richa, 2024. Artificial Intelligence-Based Cyber Security and Digital Forensics: A Review. *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing*, pp.391-419.

Yaacoub, J.P.A., Noura, H.N., Salman, O. and Chehab, A., 2022. Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations. *Internet of Things, 19*, p.100544.