

Digital Forensics Analysis

Task 1: Research Report

“The Evolving Landscape of Digital Forensics:
Tools, Cybersecurity Convergence, Emerging Trends, Challenges, and Labor Market Demand”

Task 2: Forensic Investigation Report

“Quantum Tech Digital Forensic Investigation Report”

Program: MSc Cybersecurity and Digital Forensics

Module: Digital Forensics Analysis (ACCA7031)

Lecturer: Dr. Mohamed Ghanem

Student Name: Md Obaydul Haque

Student ID: 2435442

University of Wales Trinity Saint David

Submission Date:

27 April 2026

Task 1:

Research Report

Table of Contents

1. Introduction	3
2. Current State of the Field and Tools	4
3. Intersection of Digital Forensics and Cybersecurity	5
4. Emerging Trends in Digital Forensics	6
5. Key Challenges and Professional Risks.....	7
6. National and International Labor Market Demand.....	8
7. Conclusion.....	9
8. References (IEEE Style)	9

1. Introduction

Digital forensics is a methodology that aims at identification, preservation, collection, examination, analysis and presenting of digital evidences such that the results can corroborate with the legal, organizational and initial investigative intentions. In 2026, this proposition is not restricted to restoration of files from confiscated desktop computers. Mobile phones, cloud accounts, social-media activity, collaboration platforms, enterprise logs, removable storage media such as USB drives and external hard disks, Internet-of-things devices (IoT), in-vehicle systems (IVS) and volatile memory are items regularly examined by investigators. The center stage of Cyber Resilience has been taken up by digital forensics, as this explains the what, how, and which data or systems were affected and what remediation is required. The National Institute of Standards and Technology (NIST) forensic incident-response guidance dedicates forensics as a capability of an organization to aid in both security incident investigation and operational troubleshooting [1]. The same can be said for the guidance around mobile forensics where it is determined that evidence must only be recovered under forensically sound conditions-i.e.94–45 methods which would be deemed acceptable [2]. That is, professional digital forensics exceeds technical tools usage. A Level 7 approach will need to perform an academic analysis of evidential integrity, repeatability, validation, proportionality and privacy (given that ex parte evidence can be particularly intrusive), who has legal authority for the actions performed and finally what responsibility does the examiner have to report the findings. It assesses the current state of the discipline, with common tools used; the intersection between data science and cybersecurity; emerging trends; key professional challenges and labor market demand in the UK and internationally.

2. Current State of the Field and Tools

Integrated, multi-source analysis is the hallmark of the state of digital forensics today. NIST SP 800-86 describes forensic techniques as method of investigation that process used for resolving isolated information security incident and aid in solving IT operational problems, where evidence could be found from files, operating system, network communication traffic and server applications respectively [1]. Considering that most cases are seldom reliant on one device or an artifact, this is particularly pertinent to contemporary investigations. A sample case could contain disk images, endpoint detection logs, Windows event records, registry keys, browser histories, email headers, cloud audit trails and memory captures. Thus, it is not just about finding a unique artifact, the evidential value comes from mapping them into a robust timeline that separates user action versus automated system activity versus potentially malicious conducts.

Smartphones integrate years of communication records, massive application databases, photos, location history and Internet of Things which can includes authentication tokens & cloud synchronization. NIST SP 800-101 Rev. 1 defines mobile device forensics as the recovery of digital evidence from a mobile device in a manner that preserves the integrity, validation, preservation, acquisition, examination, analysis and reporting [2]. This means in practice an examiner should note things as device state, extraction type, acquisition environment, tool version, known limitations time-zone handling (when applicable), hash values where appropriate and indicate if the result is logical, file-system based, physical backup-based or cloud / web artifact. A message, picture or location log may look different on a handset, in a back-up as well as inside a cloud account so corroboration is still absolutely crucial.

So, tool selection is strategic and not mechanical. For integrated investigations, Magnet AXIOM is valuable since it may compile computer, mobile, cloud, vehicle and acquired data in a single case file along with its AI-assisted analysis features Connections and Timeline [3]. Autopsy is an open-source digital forensics tool used for hard-drive investigation and offers functionality nearly identical to many commercial tools [4], which is very important at this point. If you are specifically interested in forensic imaging, FTK Imager is still helpful for hash value comparison for digital investigations, while solutions like Cellebrite and Magnet tools can still be used to extract mobile data and parse application artifacts. However, every forensic tool is not self-validated. E.g. as in the case of SWGDE [5], transparency or documentation is used to ensure that during live collection the integrity from acquisition phase is still maintainable, since it affects/change or creates evidence. More proprietary tools can speed processing but obscure parsing logic, while more open-source tools minimize transparency but require greater examiner skill. As such, strong practice includes cross-tool validation where appropriate, manual checking of key artifacts proportionally to risk, established known-dataset testing, engineered versions of tools, and a transparent audit trail.

3. Intersection of Digital Forensics and Cybersecurity

Digital forensics has become closely allied to cybersecurity, in particular incident response, threat detection, and cyber risk management/governance. When a cyber incident occurs, forensic evidence is key to answering the very questions that security leaders, regulators, insurers, and victims alike must understand: what was the initial access vector; which accounts were used; what privileges were gained; (if any) persistence mechanisms created; whether data was accessed or exfiltrated by the threat actor; and whether or not the threat actor still lingers. While a spike in security alerts may show that something happened, it is forensic analysis that builds up the timeline and attempts to invalidate conflicting narratives. It matches NIST's perception of forensics as embedded into the incident response process within the organization and not an isolated law-enforcement activity [1].

You can see the association in ransomware, business email compromise, insider threat, and cloud-compromise investigation findings. E.g. in a ransomware, memory may detail running processes, disk analysis will find dropped payloads, event logs of possible lateral movement through the network or mail for phishing and cloud audit logs to determine whether data was exfiltrated prior to encryption. Those results can then feed into better cybersecurity controls like endpoint detection and response rules, SIEM correlation, privileged-access management, network segmentation and phishing awareness and backup strategy. That makes digital forensics both historical and forward looking: it digs through the events of the past, while fortifying the defense in future.

This convergence also produces a kind of professional friction. Incident responders tend to focus on containment, business continuity and service restoration while forensic examiners typically prioritize the preservation of evidence, chain of custody and repeatability. Responses such as wiping systems, rotating logs, turning off volatile devices or modifying files and the lack of documentation of actions can lead to the destruction of important evidence. As a result, strong organizations develop forensic readiness in advance of a breach. Examples are logging policies, handling procedures of evidence and chain-of-custody forms, secure storage with defined legal authority, escalation routes to data-protection teams, plus playbooks explaining when volatile data should be collected before containment. The greatest investigations are not concocted following a breach; they come from readiness.

4. Emerging Trends in Digital Forensics

Multiple trends are changing the face of digital forensics. The cloud and SaaS forensics is the first one. Rather than a single seized device, evidence might be found in Microsoft 365, Google Workspace, iCloud, WhatsApp backups, or Teams messages—or on social-media platforms or remote servers. Guidance from SWGDE on cloud-service-provider imagery discusses acquisition, preservation and analysis of data held by such providers across a range of issues including the necessary authority, scope and provider processes for consummating jurisdictional requirements [6]. There are challenges with cloud evidence; for example, a local cached image may contain insufficient data, the provider-returned data may include metadata not visible on the device itself, and account data can exist in multiple places. This means that investigators have to distinguish between evidence which is local, synchronized and provider-held.

The second development is Artificial Intelligence and automation. By using AI triaging, image classification, entity extraction, chat clustering and anomaly detection it can help with huge data retention as well. And commercial tools are following suit: for instance, connections and timeline functions to identify important evidence faster with the promise of AI-powered analysis in Magnet AXIOM [3]. Workforce data also indicates AI and cloud security are some of the most crucial specialized skills in current cyber security, with ISC2 finding that there is widespread need for skills across the profession [10]. Nevertheless, AI should not be treated simply as a replacement for examiner judgment. AI-supported triage could cut backlog and assist prioritization of reviews but it can also create opacity, bias and reproducibility issues here. The presentation of AI-assisted results in a forensic report which is defensible should impart an understanding of how the results were produced, validated and corroborated; such explanations are dissimilar to relying upon unverifiable automated outputs.

Expansion of new sources of non-traditional evidence is the 3rd trend vehicle infotainment and telematic systems may contain caller logs, details of paired devices, journeys travelled, locations and media metadata that are therefore becoming more common in criminal, civil and corporate investigations [7]. Drones may log information about flights, control stations, geographic locations, payloads, and media files that can be important when reconstructing movements or attribution [8]. IoT devices, wearables, smart speakers and home network equipment is likewise capable of offering sensor occasions, connectivity statistics and user interplay information. They are alluring because such sources can situate a device, account or person in time and space, but only with careful interpretation. A device event does not automatically equal a human action; it can also be the result of automated processes running in the background, account syncing or another legitimate user.

5. Key Challenges and Professional Risks

Encryption continues to be one of the most lingering technical problems. Without an unlocked device, extraction in a lawful way, integrity of usable backup data, and/or endpoint artifact or knowledge about the return will be confiscated from the total device media and therefore blocked by full disk encryption, secure enclaves from biometric locks as one model or wealth ethics, e.g. end-to-end encrypted message (only success with consent driven acquisition) devices can determine access. That limitation is not merely a headache; it reveals real protections for security and privacy. Forensic practice, therefore, must work within legal powers and proportionally. Investigators may still examine the metadata, notifications, file names and timestamps, backups and logs for a Google account as well as the communication pattern but such unaccused content should clearly be defined in the report. The way data is acquired affects what can be recovered and how confidently it can be interpreted, therefore mobile evidence procedures need to follow validated, forensically sound methods [2].

A second challenge relates to the volume of data. A single case can have terabytes of disk images, hundreds of thousands of messages, years of cloud logs, and sometimes many devices belonging to the suspect or the corporation. Triage is inevitable, but bad triage can leave out important content. A defensible approach identifies the boundaries of what is included in, and excluded from the project including the timeframe within which you are searching; your search terms; categorization of evidence artifacts (including together with reference to media type); decisions made in prioritizing evidence activity and justification for any inclusions or escalations. For large cases, the documents and the integrity of evidence (SWGDE) are important when acquisition has to be selective, or there is a live collection update [5]. As such, corporate investigations must also balance the forensic need for information against employee privacy considerations (and the possibility of business disruption and data-minimization duties).

Attribution and reliability are further complicated by anti-forensics. Wipe tools, timestamp manipulation, log deletion, hidden activities in VBMS, and encrypted containers or applications that focus on privacy. Double absence: Examiners should make sure not to run into the overclaim case of absence of evidence is not evidence of absence. Establish the possibility of forensic activity with all supporting artifacts (prefetch files, shell bags, link files, registry keys, etc.) and correlate this to cloud logs, app databases, vnet recs. The report must separate observation, interpretation, and inference, including whether evidence appears to have been manipulated or destroyed.

Thirdly, legal and ethical issues, as well as jurisdictional issues, are also highly significant. Evidence may cross borders, retention policies of providers can differ, and datasets will inherently have third-party PI not related to the investigation. For further information, SWGDE's cloud guidance points to the need of addressing data held by provider and how to deal with a request on such [6]. As such, examiners are expected to use necessity, proportionality and authorization as well privacy controls. Another risk for the professional is tool validations. Acquisition settings, tool versions, hash values, time zones, well known tool limitations and independent validation of key findings should be documented by the examiner. The value of a technically correct discovery is diminished, if it cannot communicate, replicate and justify itself.

6. National and International Labor Market Demand

Even though employability has become a composite of broader cybersecurity competence, human- and machine-applicable evidence from the labor market is consistent with the existential importance individuals ought to place on digital forensic capability. The 2025 CYBER- SKILLS REPORT estimated about 143,000 in cyber-security roles throughout the UK economy and a workforce gap of around 3,800 professionals [9] according to the UK Government. Core cyber job postings in 2024 the number of all core cyber job postings was reported at 32,370 placements per year and median GBP 55,000 (higher than private sector wide IT labor market median) for community professionals [9]. The same report found that businesses have "strong" technical skills gap in advanced areas, such as forensic analysis, interpretation of malicious code and penetration testing [9]. Despite broader changes in the digital sector that have affected job postings, these numbers suggest sustained demand.

The hybrid profile of digital forensics graduates is the strongest internationally. Practitioners who can preserve evidence and write defensible reports are valued, but building pressure around employing them means employers want people with either an instinct for incident-response and cloud-platform awareness, identity and access management (both of themselves is the customer a lightweight user of Cloud Services? And the same goes for SIEM use, endpoint telemetry as well), scripting proficiency, malware-behavior knowledge, privacy judgment, stakeholders speaking to them. In their 2025 workforce study, ISC2 shows us organizations are focusing more on specialized skills such as AI and cloud security instead of just the number of people [10]. This is important for careers in forensic investigations, as a lot involves cloud logs, AI-assisted triage of relevant data, mobile artifacts and enterprise security telemetry.

Those graduates that incorporate legal defensibility with the cloud, mobile award and AI aware protocol communication are going to be far more competitive than applicants who know one tool. Development paths that are useful are vendor training in Cellebrite or Magnet, open-source practice with Autopsy and The Sleuth Kit, certifications like GCFE, GCFA, EnCE and CHFI.

7. Conclusion

Digital forensics has become a multidisciplinary, high-accountability discipline linking together evidence, cyber security, law, governance and organizational resilience. New types of information such as mobile devices, cloud services, enterprise telemetry, encrypted applications and vehicle systems; new classes of sources like IOT sources, volatile memory and even big data sets. Magnet AXIOM, Autopsy and FTK Imager are a few examples of tools that can speed up acquisition and analysis process in conjunction with examiner interpretation not instead of. Ideally all investigations are legal, commensurate, repeatable, verified and completely documented and the results independently substantiate with more than one artifact of evidence. Markets in emerging areas, such as AI-assisted triage, cloud forensics, vehicle data and drone forensics correspondingly offer both dangers and opportunities. Forensic skills are most useful when combined with a wider cybersecurity capability particularly in cloud, incident response, AI awareness and professional reporting according to labor-market evidence. Thus, future-ready digital forensic practitioners should be technically sound, ethical conscious and able to express complex evidence in a clear, impartial and defensible manner.

8. References

- [1] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," National Institute of Standards and Technology, NIST Special Publication 800-86, Gaithersburg, MD, USA, Aug. 2006.
- [2] R. Ayers, S. Brothers, and W. Jansen, "Guidelines on Mobile Device Forensics," National Institute of Standards and Technology, NIST Special Publication 800-101 Rev. 1, Gaithersburg, MD, USA, May 2014.
- [3] Magnet Forensics, "Magnet AXIOM | Digital forensic software," 2026.
- [4] Sleuth Kit Labs, "Autopsy - Digital Forensics," 2026.
- [5] Scientific Working Group on Digital Evidence, "Best Practices for Digital Evidence Collection," SWGDE 18-F-002-2.0, Jun. 30, 2025.
- [6] Scientific Working Group on Digital Evidence, "Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers," SWGDE 23-F-004-1.1, Jan. 13, 2025.
- [7] Scientific Working Group on Digital Evidence, "Best Practices for Vehicle Infotainment and Telematics Systems," SWGDE 12-F-004-3.2, 2024.
- [8] Scientific Working Group on Digital Evidence, "Best Practices for Drone Forensics," SWGDE 21-F-002, Jan. 13, 2022.
- [9] Department for Science, Innovation and Technology, "Cyber security skills in the UK labor market 2025," GOV.UK, 2025.
- [10] ISC2, "2025 ISC2 Cybersecurity Workforce Study," 2025.

Task 2:

Forensic Investigation Report

Case:

“Suspected theft and attempted external sale of the QT-AI-2025 proprietary AI chip design patent.”

Field	Submission Details
Examiner	Md Obaydul Haque
Reference Number	2435442
Tool used	Cellebrite Physical Analyzer 7.73.0.11
Device mapping used in this report	Emma = Huawei; Joe = Samsung/contact identified in Huawei communication; Norman = Nokia; Samsung GSM SM-G950U = additional source evidence as shown in the extraction material.

Forensic reporting declaration:

This report is prepared as an evidence-based digital forensic investigation report. It distinguishes between the artifacts themselves (what we observe) and interpretation, preserves verbatim wording when it is pertinent to doing so via screenshots of content, refrains from speculation that cannot be supported through the underlying evidence available, and notes caveats where limiting uncertainty with regard to a contested fact does not support unambiguous conclusions.

Table of Contents

Contents

1. Executive Summary	12
2. Case Background and Investigation Scope.....	12
3. Evidence Inventory and Continuity of Evidence	13
4. Acquisition and Examination Methodology	15
5. Forensic Images and Integrity Verification	17
6. Communication Analysis	17
7. File and Source Analysis	21
8. Timeline Reconstruction and Correlation	23
9. Suspect Role Analysis	24
9.1 Emma - primary insider suspect.....	24
9.2 Joe - suspected intermediary.....	25
9.3 Norman - suspected buyer	25
9.4 Vanessa / NexGen Circuits	25
10. Findings, Evidential Weight and Limitations.....	26
11. Conclusion	27
12. Recommendations.....	27
12.1 Further forensic work	27
12.2 Organizational recommendations for Quantum Tech	21
Appendix A. Figure Source Log.....	28
References	28

1. Executive Summary

This report describes an Inference-based digital forensic investigation into the alleged theft and attempted external sale of Quantum Tech's patented design for its proprietary AI chip, identified in this case material as QT-AI-2025. The analysis was carried out with Cellebrite Physical Analyzer v7.73.0.11 and is fourfold examining the mobile evidence, source information for Emma's Huawei phone, some communication artifacts related to Joe, items of evidentiary importance from Norman's Nokia device as well as data on Samsung GSM SM-G950U sources available here:

The only real evidence of communication comes from the Huawei WhatsApp/Genie message marked "Top-up" In the case of the conversation we reviewed, a DM to Joe asking for help with something private followed by an obvious message that says: I have info on some secret and valuable intel from ABC Technologies. It's linked to our new AI Neuro offering. I was going to sell it, or pass on for someone who may want one. The exact wording is retained as it came from the forensic tool (an artifact of sorts). This is particularly relevant within provided Quantum Tech case scenario because it indicates availability of sensitive corporate information and intention to market outside the group. This supports the allegations that (there was an attempt to) misuse of intellectual property.

Other WhatsApp/Genie artifacts revealed a more advanced stage of planning and pressure language ("Local part stays as planned", "We can push harder" & "I have others waiting"). The messages reflect coordination, onward recipients, and pressure to advance the activity. Yet, the report is still measured: It states evidence "strongly" supports attempted sale or externalization of valuable company information, but absent file-transfer artifacts (or other) supporting a transfer / actual completion-of-sale requisite for QT-AI-2025 should not even be claimed.

2. Case Background and Investigation Scope

Quantum Tech said it was informed of a possible theft during unauthorized access to documents relating its patented AI chip design patents The case material reflects Emma as a senior engineer who might have been privileged to sensitive and confidential patent related materials. Joe is also seen as possible go-between given evidence of communications from Huawei to Joe and back. For example, both Norman being a suspected buyer and Vanessa/NexGen Circuits are treated as relevant outside contact needing to seed corroboration.

This report is specific to the digital evidence provided in this case file; data examined with no other forensic tools besides those available within Cellebrite Physical Analyzer. The report covers factors on acquisition documentation, establishment of continuity and integrity, analysis of communication forensics across various platforms (DNS/odbc logs often seem missing), apparently a proper examination file/source review has not taken place including recording relevant timestamps to assist in timeline reconstruction; long the primary element placing big issues onto how suspects would be assessed as role players or users rather than originators position could become easily vitriolic if allegations were made against me pertaining calculable deficient evidential limitations especially because bifurcation seems recommended? It does not claim facts that are inconsistent with the forensic artifacts reviewed or scenario presented by evidence accompanying a case.

Investigation objective	How it is addressed in this report
Acquire and document evidence	In this blog post, we will show the examining workflow with Cellebrite source views and extraction viewpoints as well screenshots documentation.
Maintain integrity	Demonstrating repeatability and continuity is achieved through hash verification, along with screenshotted extraction/source metadata.
Analyse communications	A thorough review of artifacts from WhatsApp/Genie, and the contact email & call log are done looking for signs of planning, coordination or sales indicators
Analyze files/source evidence	Patent-file identifiers, file names, and paths are examined in document and filesystem views.
Reconstruct timeline	A timeline table contains correlated timestamps for communication, extraction, and source activity.
Assess roles	We instead assess evidence-strength categories the same as what is done in some data-based methods to include four different people: Emma, Joe, Norman, and Vanessa—using no assumptions.

3. Evidence Inventory and Continuity of Evidence

A comprehensive evidence inventory helps in linking each finding or observation to its corresponding source, which indicates continuity of proof. The table below documents the sources examined and respective roles, artifact types seen, and integrity/continuity position.

Exhibit	Source/item	Owner or role	Observed evidence type	Integrity and continuity note
E1	Huawei / Huawei_POT-LX1 P Smart	Emma - primary insider suspect	Device overview, WhatsApp / Genie Data sources, and Manifest contact & IM contacts for email/messaging call log message! Filesystem and App Category	Link to this exhibit as linked evidence of publicly available data for analysis by supporting documents summary and artifact category screenshots
E2	Samsung phone / Samsung or Note source	Joe - suspected intermediary	Artifacts of the: communication, filesystem, document, and location, depending on how the final device is linked	Use as source for only Joe where you could confirm over device mapping that it is ownership otherwise use visible artifacts.
E3	Nokia phone	Norman - suspected buyer	Nokia profile, text/log views timeline / location artifacts	Only usable for Norman findings where the content is visible and contextually relevant
E4	Samsung GSM SM-G950U source	Additional source/removable evidence as shown in the extraction material	Extraction successful, hash verification, discover category, source metadata	Hash/source metadata screenshots Integrity, use the same exact text in the description of the source type that is represented by Cellebrite.

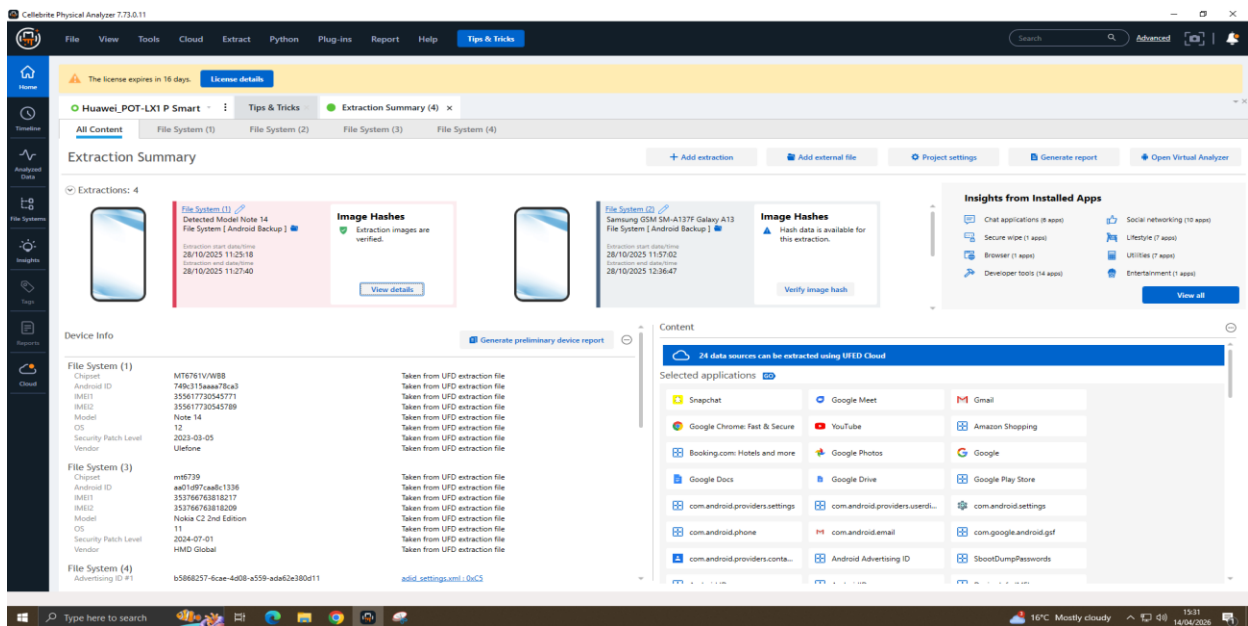


Figure 1: Cellebrite Physical Analyzer source overview showing the Huawei source and extracted artifact categories used to structure the investigation.

The importance of this artifact is that it makes the Huawei device a structured forensic informative source available in Cellebrite Physical Analyzer. The range of artifact types visible indicates that the analysis was not restricted to a single item it encompassed communications, files, logs and application data. This latter aspect of the findings supports reliability for follow-up analysis, in providing chronologies based on a recognized forensic workflow.

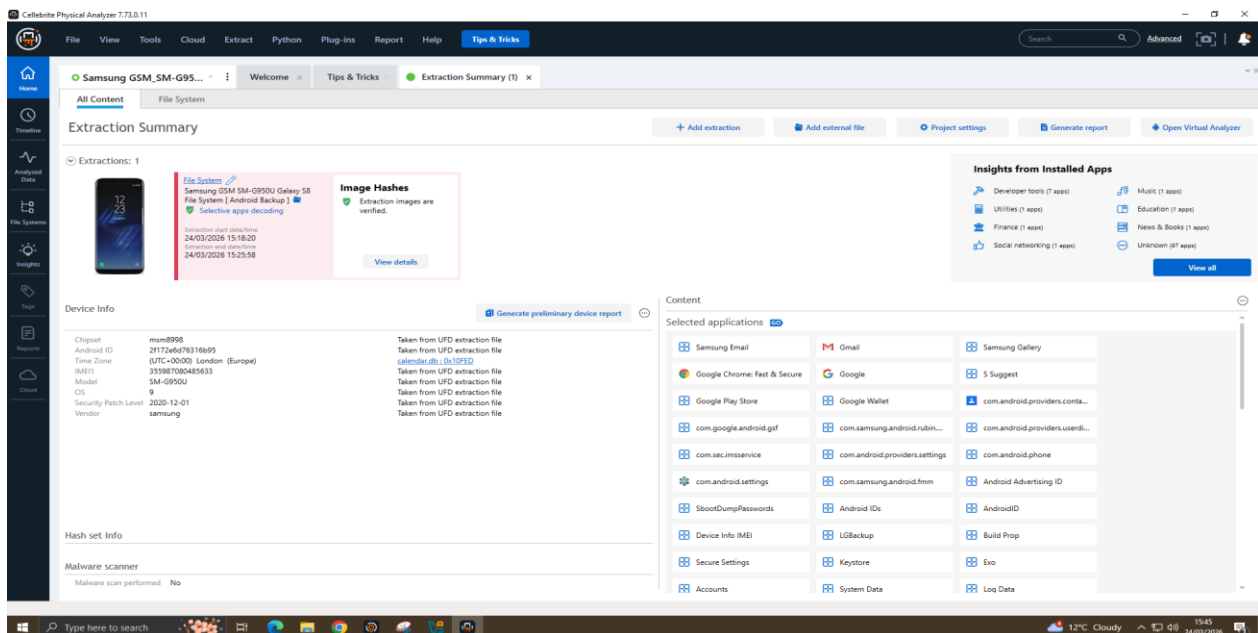


Figure 2: Hash and extraction-information view for Samsung GSM SM-G950U showing image-hash verification and source metadata.

This artifact is important because it attests to the evidence that has been extracted. This successful hash confirmation means that the data examined during processing was not lightly modified in other words, it remained static. This provides added evidential value to any files, documents or meta data subsequently reviewed from that same source.

4. Acquisition and Examination Methodology

At that time, the exam was done using Cellebrite Physical Analyzer 7.73.0.11. The workflow was preservation first: determine the source, load extraction, verify status and hash information (where available), category follow-up for artifacts reviewed, documentation of relevant screenshots, then correlation across sources.

The approach conforms to established digital-forensic principles: follow the chain of custody, document conditions under which evidence was acquired and examined, use hash values to check integrity where possible, avoid altering original data or media (the 'M' in our 4 M's), distinguish observations from interpretation and include caveats as required. In cases where it provided previously earned evidence rather than physical devices, the analysis is restricted to what can be seen in the extraction output and associated documented forensic artifacts.

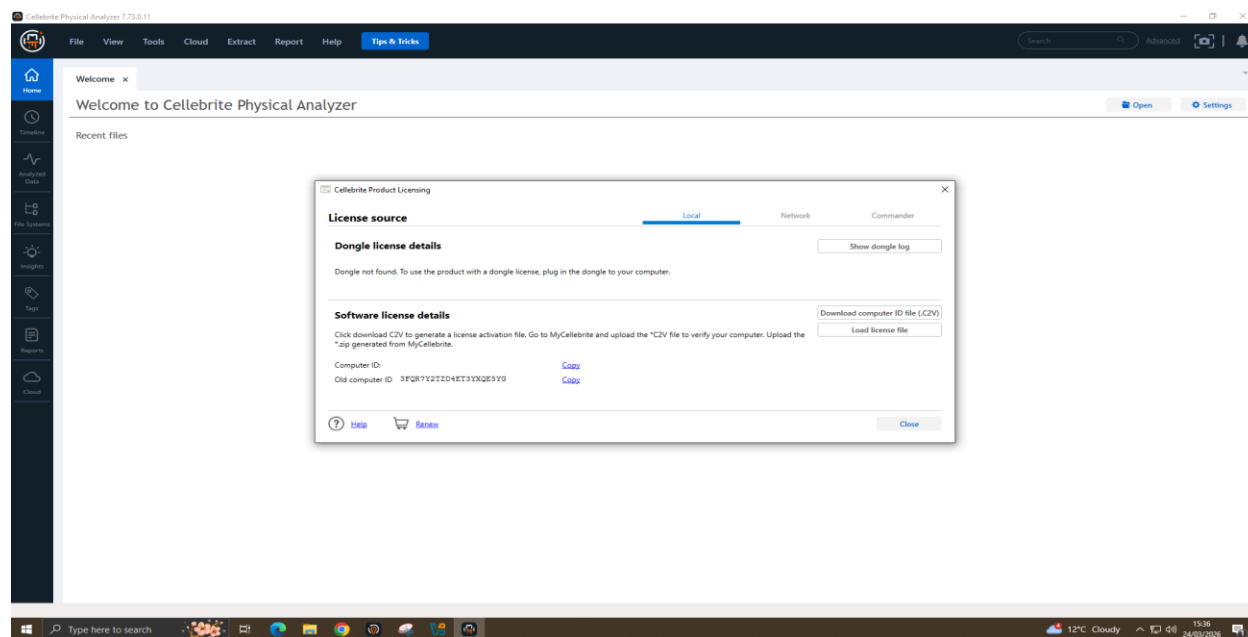


Figure 3: Cellebrite Physical Analyzer workspace showing the evidence sources available for examination.

This artifact is important in that it speaks to the forensic controlled environment where this investigation has taken place. Instead of having to manually go through evidence, the artifacts were loaded into Cellebrite Physical Analyzer, enabling an easy and repeatable review process. This adds to the method design professionalism and defensibility.

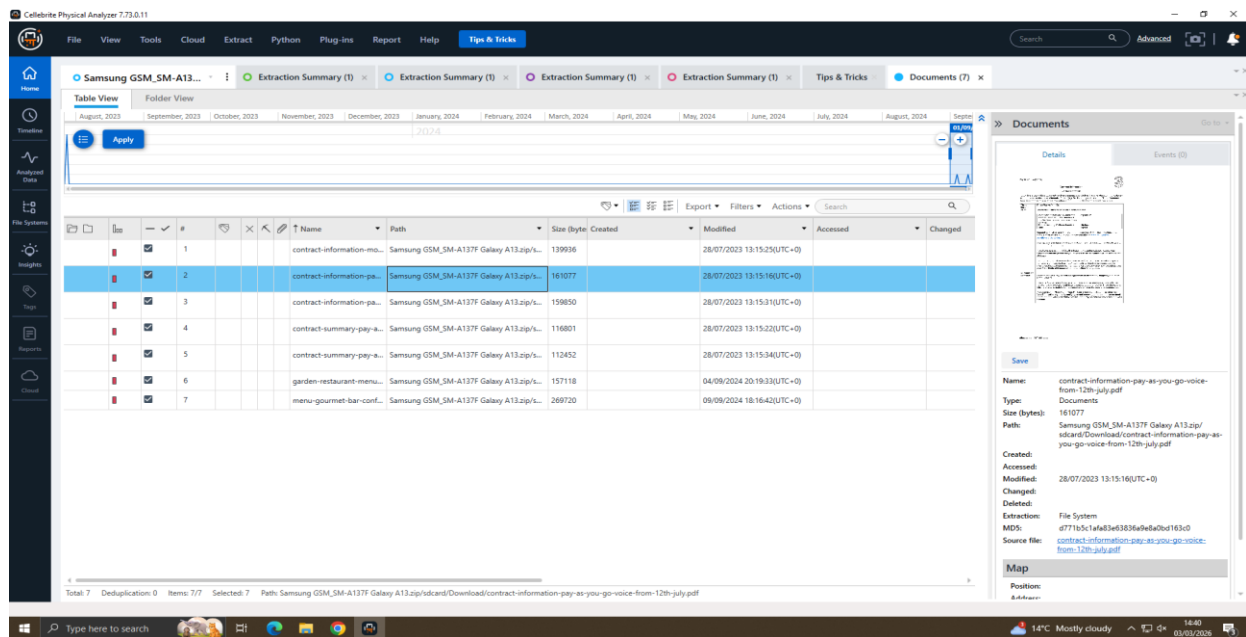


Figure 4: Extraction and processing confirmation view showing that the evidence source was processed before analysis.

This artifact is significant because it confirms that the extraction process was completed before detailed analysis began. A completed extraction reduces the risk of relying on partial or incomplete evidence. When combined with hash verification, it supports the reliability of the subsequent communication, file and timeline findings.

The examination steps applied were:

- Loaded the obtained source/extraction into Cellebrite Physical Analyzer and verified visibility of 3rd party sources.
- Checked available sources for extraction information and hash status
- Investigated artifact types that encompasses WhatsApp/Genie chats, contacts and emails along with call logs, filesystem/logs as well social media, images and timeline items.
- Evaluated each person of interest in isolation to ensure that the artifacts associated with one device are not incorrectly attributed to another without supporting information.

5. Forensic Images and Integrity Verification

The collection and integrity of evidence is relevant because it establishes that this was an item to allow tracking through a repeatable forensic workflow. Screenshots are not a full extraction report, but they can be useful supporting material when the image shows whether something was successfully extracted (and if so from where), metadata about source tracking information, hash values and artifact categories.

Integrity item	Observed/required evidence	Importance
Extraction status	The extraction/processing screenshot shows the source was processed in Cellebrite.	Indicates that the evidence source was analyzed based on a less treated extraction rather than an uncontrolled viewpoint.
Hash verification	Screenshot image-hash shows Samsung GSM SM-G950U.	Supports admissibility, repeatability, and chain-of-custody.
Source metadata	Display Model, OS version, Android ID (Android identifier), IMEI, and extraction times on Samsung GSM SM-G950U.	Associate the image with a valid source instead of just an unknown file.
Examiner documentation	Retain examining name, date, where it is kept and what the IDs are attached to investigation file.	Provides data for the maintenance of professional continuity records and auditability

6. Communication Analysis

WhatsApp/Genie messages, contact information emails, and call logs are categorized as Communication analysis. The goal was not one of measuring how many messages were exchanged but rather whether the communication artifacts support planning, coordination, a sale attempt being made an appointment scheduled either to make payment or send files and/or to conceal each party having actually engaged in such activity. Perhaps the strongest piece of evidence that communication took place is who spoke to Huawei for Top-up.

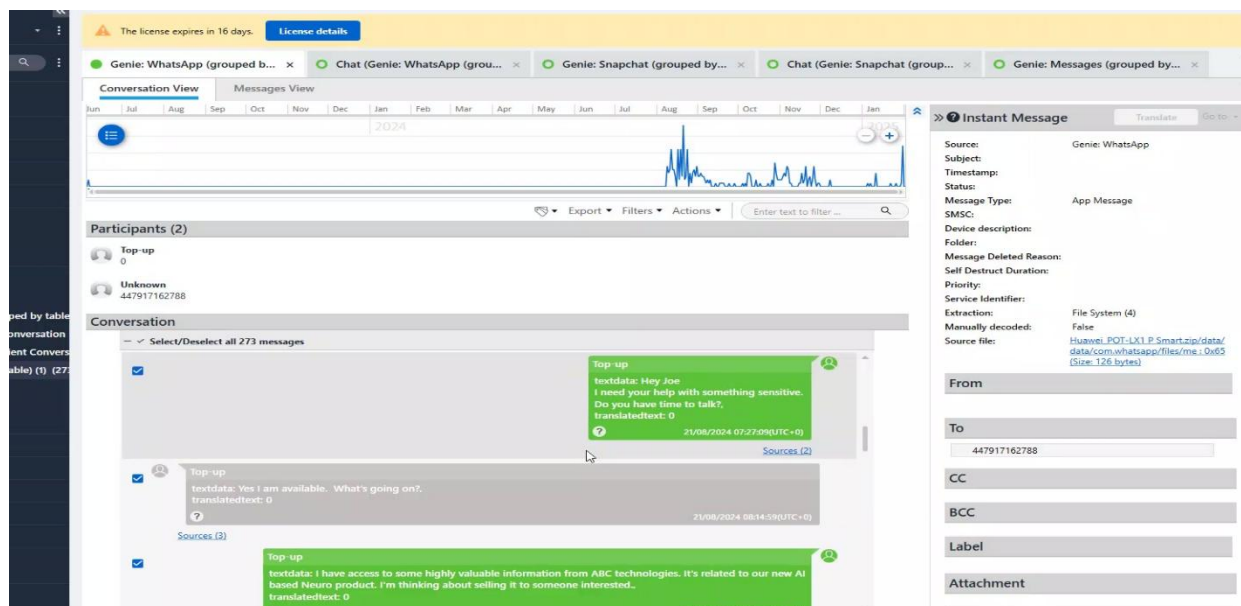


Figure 5: Huawei Top-up WhatsApp/Genie conversation showing a direct message to Joe and an intention to sell valuable company information.

Figure 5 is the strongest screenshot for communication. It shows direct contact with Joe, access to highly valuable company information, and consideration of selling it to an interested party. The wording is preserved exactly as visible in the artifact and should be interpreted within the supplied Quantum Tech scenario.

Visible timestamp/context	Observed message text	Forensic interpretation
21/08/2024 07:27:09 UTC+0	The following is the start of an email prompting Joe to help him with a sensitive issue. Do you have time to talk?"	A sign of direct contact with Joe, and bringing up a delicate subject. That is helping as Joe becomes more than just a passive contact.
21/08/2024 08:14:59 UTC+0	"Yes, I am available. What's going on?"	Mention of Joe indicating he is contactable and still in the conversation.
21/08/2024 09:58:21 UTC+0	This story includes the views of some core information I have gained from ABC Technologies. So it has to do with what we came up with in our Neuro product based on AI. That I am betting to sell it, if someone is interested in buying.	Highly encourages the purpose of monetizing or outsourcing some if not all its data. While very germane to the allegation, quoted organization/product specific phrasing should not be changed.

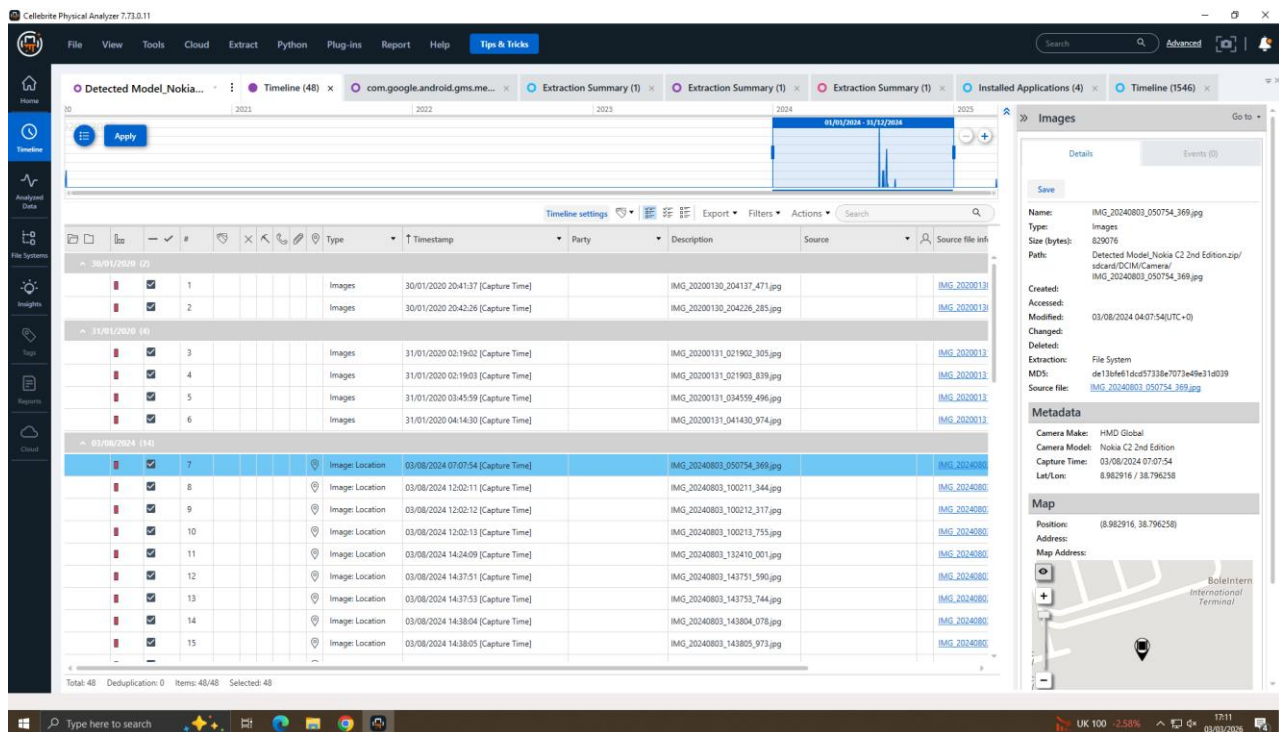


Figure 6: Existing screenshot of the Top-up WhatsApp/Genie conversation showing later planning and pressure language.

This shows later suspicious language in the same communication context. This screenshot supports an inference of continued planning, pressure, and onward party involvement.

Visible timestamp/context	Observed message text	Forensic interpretation
31/01/2025 10:23:38 UTC+0	“Local part stays as planned. He’s taking his sweet time. Not liking this.”	Indicates fixation on a potential arrangement and anger with how the third party is dragging things out. Local part: it could mean something coded or context-specific and needs to be correlated with your file activity.
31/01/2025 10:23:56 UTC+0	“It’s all about patience. We can push harder.”	Supports pressure / escalation in a managed activity.
31/01/2025 10:24:11 UTC+0	“Ok. Keep me posted. I have others waiting.”	Important because it suggests additional buyers or receivers. But it is in line with an intermediary/buyer model, and should be tied to the actual file or recipient indicating that evidence of delivery.
31/01/2025 11:28:14 UTC+0	“We’ll be watching...”	May continue to monitor or take action This should be treated with caution and in conjunction with other artifacts.

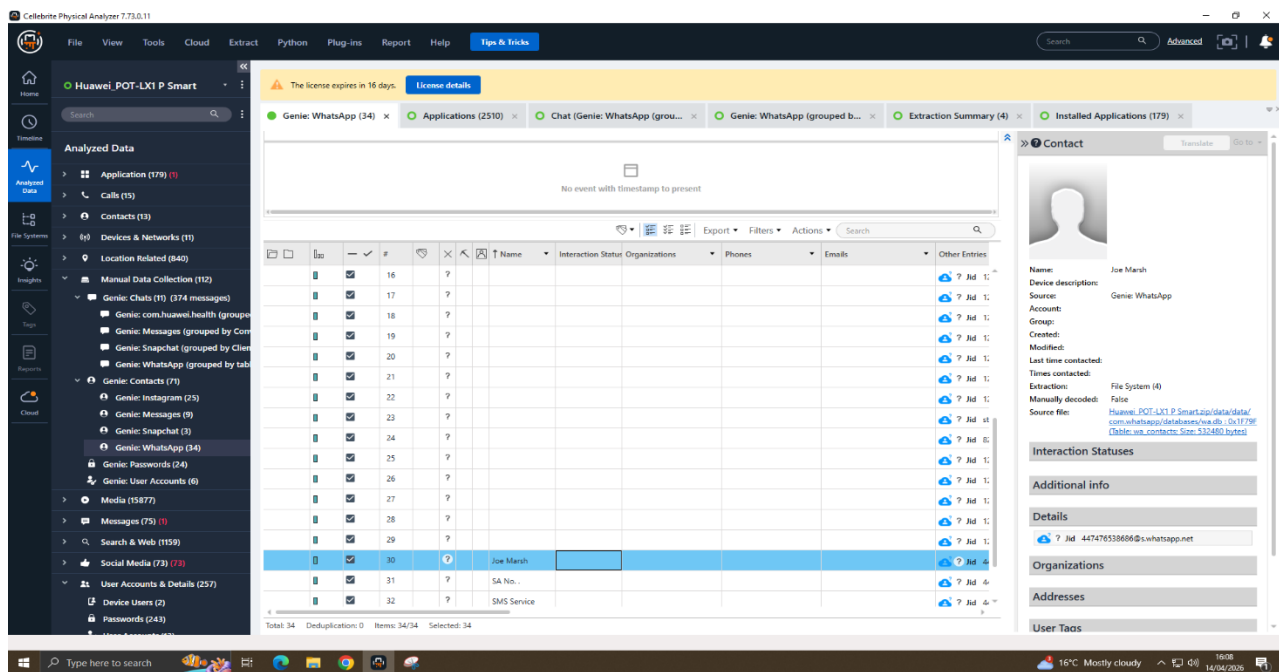


Figure 7: WhatsApp/Genie contact context showing Joe Marsh, supporting the identification of a relevant communication link.

This artifact is important both because the messages contain language to indicate co-ordination, delay pressure and potential onward recipients. Phrases like "Local part remains on course" and "I have others holding out here", etc. are not evidence for theft in themselves but suspicious when paired with file/timeline artifacts. Along with the documentary evidence, this allows for some supposition of a broader coordinated effort instead of typical incidental contact.

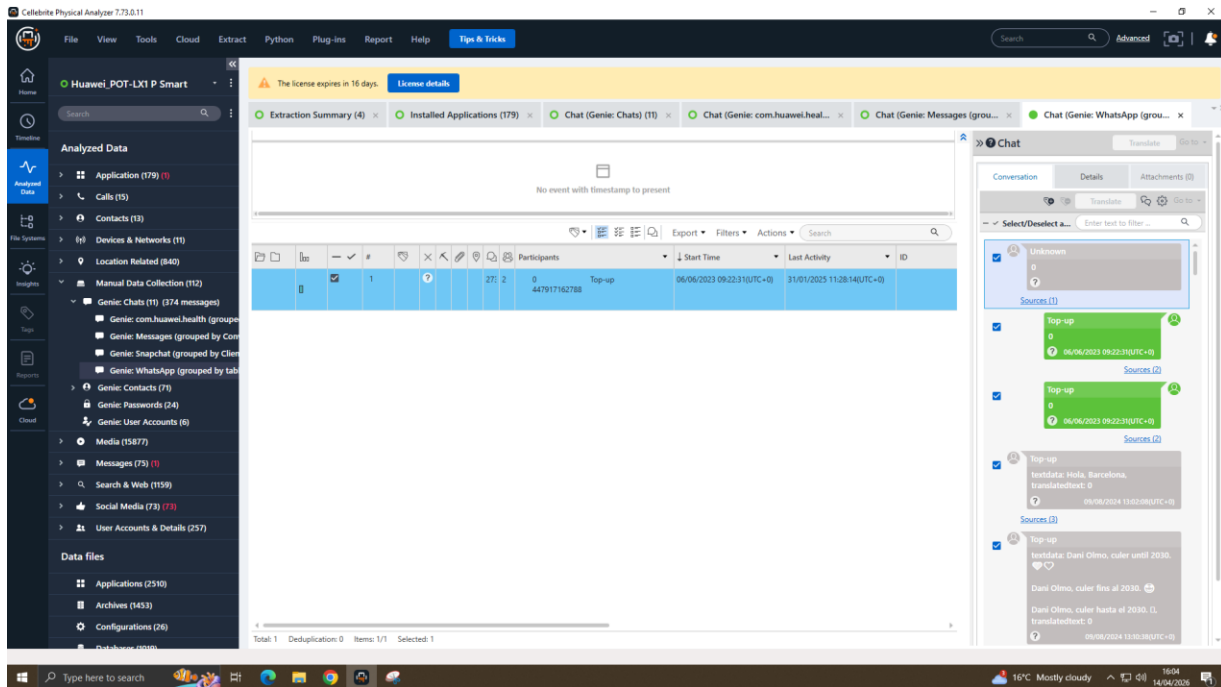


Figure 8: Huawei call log artifacts that can be cross referenced with message timestamps and file activity.

Call logs can provide supportive timeline evidence around key communications and therefore this artifact is significant. Call activity can help indicate contact behavior prior to or immediately after suspicious messaging/file actions, even when the content of calls is not in view. The call log helps in broader communication patterns when correlated with WhatsApp and document timestamps.

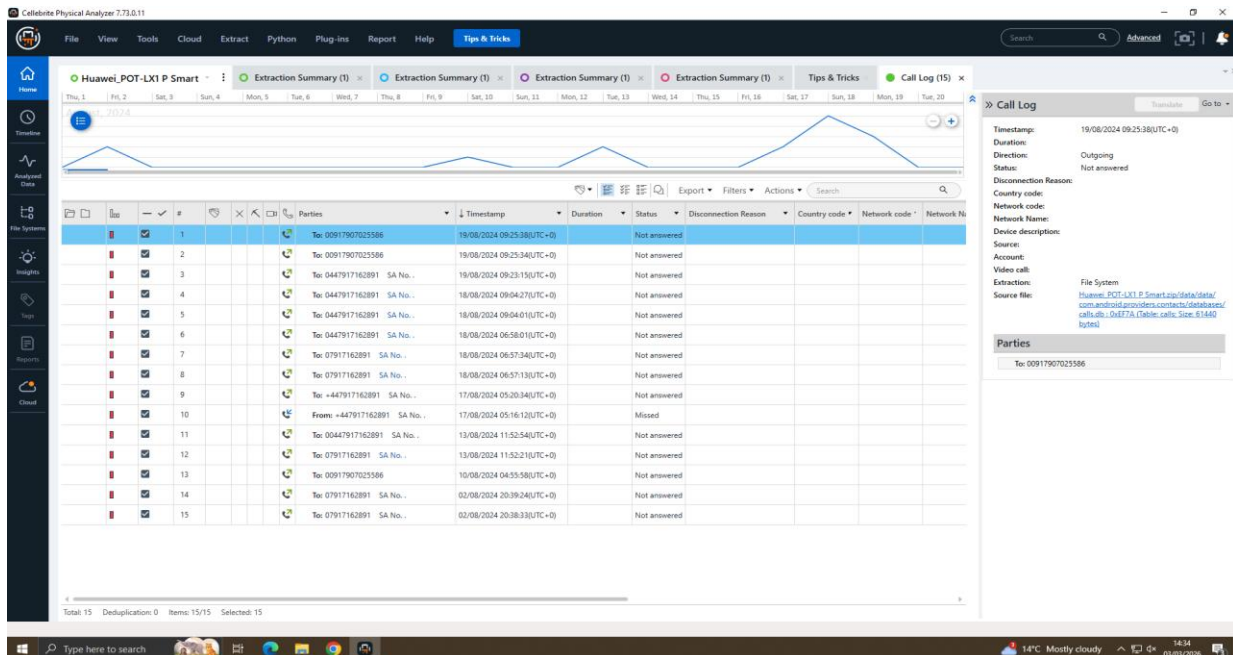


Figure 9: Email artifact view showing available email account and message list evidence reviewed in Cellebrite.

The importance of this artifact is that, it provides an insight into the consideration of email evidence as a part of broader communication scrutiny. Visible email artifacts may not in isolation prove an attempted sale or transfer occurred, but they do assist the fact that numerous communication channels were searched through. It enhances the completeness of analysis while reducing dependence on any one type of artifact.

7. File and Source Analysis

Purely file analysis is key to all of this due the nature of patent allegation. The screenshots readily displayed are of document and filesystem review although the visible documents do not in any manner prove that a QT-AI-2025 file is actually being copied, transmitted or sold. Consequently, a professional forensic report should refrain from declaring exfiltration as having occurred unless it can be evidenced by screenshot or export displaying file name(s), path, metadata related to the transfer route and/or confirmation of receipt.

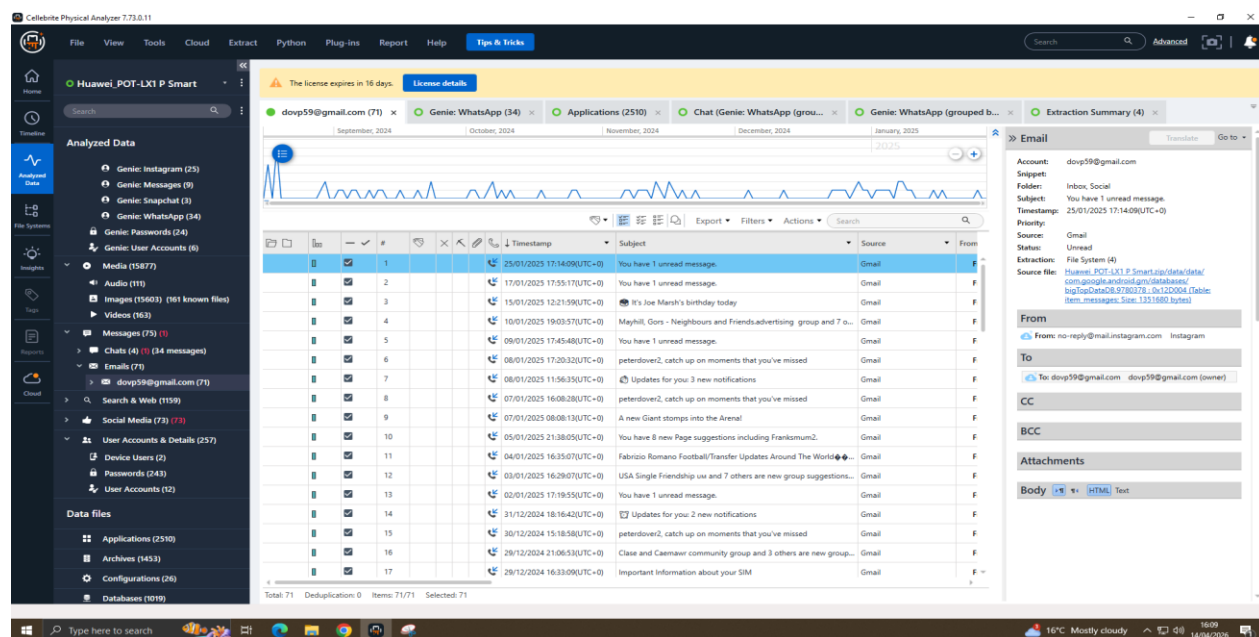


Figure 10: Document/file details view in Cellebrite showing how recovered document artifacts and metadata are inspected.

This artifact is particularly pertinent because the allegation involves dealing with non-public patent-related material, meaning document metadata playing a key role in this investigation. File names, file paths, file sizes and relative timestamps can help determine whether there was relevant material placed on or transferred from the device. Document evidence is crucial when assessing whether suspicious messages are indicative of a file actually being in use, if it can be linked back to communication artifacts.

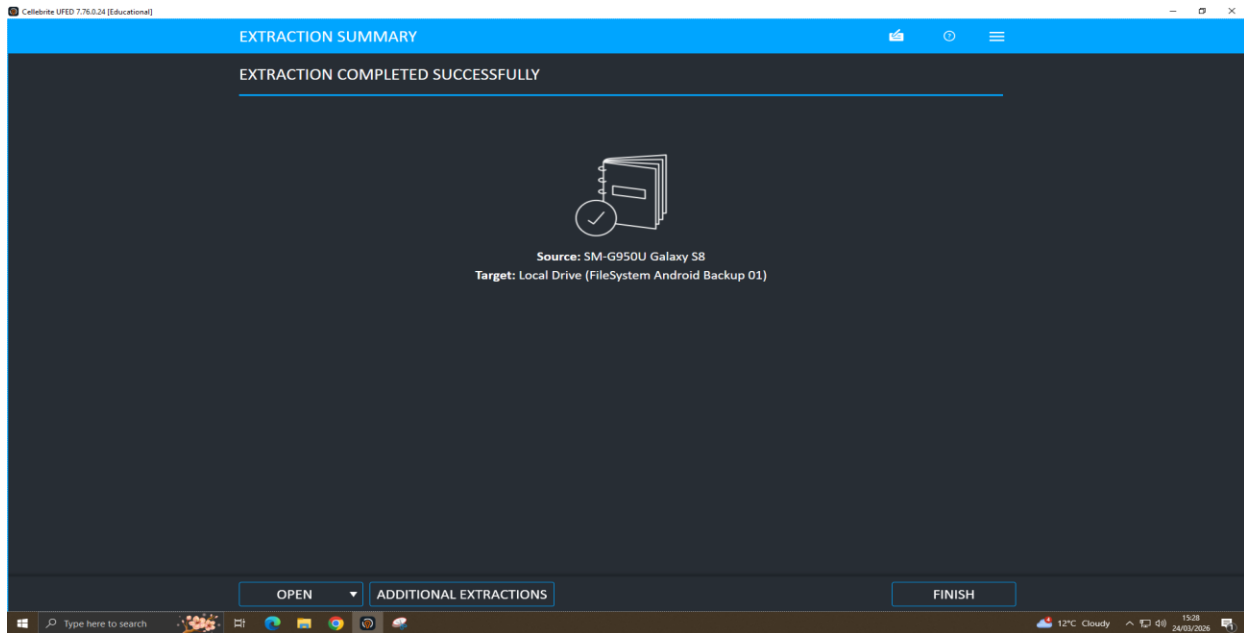


Figure 11: Samsung source document-category view showing recovered document artifacts available for file analysis.

The importance of this artifact is that it confirms which document categories were checked in the source from which they have been extracted. Document artifacts are evidence that patent material is in the source, and whether it was available to a suspect. The evidential weight of this is gauged by its correlation to the file names, metadata, and communication timeline.

File-analysis requirement	Evidence status in selected material	Forensic status
Patent-file name/path	It is not conclusively demonstrated with the selected screenshots that a QT-AI-2025 filename/path comes directly.	Otherwise, ownership or staging means nothing (unless proven with a supporting file-name/path/metadata artifact)
File metadata	Document/file views exist, but clearly visible non patent file examples.	Metadata findings should only be what is identifiable in the figure or the extraction report.
USB/removable/source evidence	The extraction material is treated as a reviewed source for the Samsung GSM SM-G950U.	Do not assume USB unless you can verify it describe the source as Cellebrite describes it.
Deleted/recovered files	None of the selected material displays a strong deleted-patent artifact.	Deleted/recovered outcomes need direct artifacts to be viewed as supported.

This means that the file evidence has a double barrier. The screenshots of the tool and document-category show that file artifacts were inspected in a forensic environment. Second, to take ownership by leading with timing (i.e. we were here first in the lab), all patent-specific file names with paths and hunks of hash values are required before possession, staging or transfer QT-AI-2025 material can be firmly secured as sufficiently supported. Derive any patent-specific artifact with reference to the WhatsApp timestamps along with communication between Joe/Norman and Vanessa.

8. Timeline Reconstruction and Correlation

A forensic timeline should support human-human testimony about when an event occurred (and thus a defense), but we only show screenshots of the artifacts? The table below distinguishes observed evidence from interpretation.

Date/time	Source	Observed event	Evidential significance
21/08/2024 07:27:09 UTC+0	Huawei WhatsApp/Genie / Top-up	Direct message to Joe: “I need your help with something sensitive.”	Add Joe a sensitive communication thread.
21/08/2024 08:14:59 UTC+0	Huawei WhatsApp/Genie / Top-up	Joe responds: “Yes, I am available. What’s going on?”	Indicates Joe is part of the Discussion
21/08/2024 09:58:21 UTC+0	Huawei WhatsApp/Genie / Top-up	Message states access to highly valuable company information and intention to sell it to an interested person.	Indications of attempts to externalize / monetizing sensitive information.
31/01/2025 10:23:38 UTC+0	Huawei WhatsApp/Genie / Top-up	“Local part stays as planned. He’s taking his sweet time. Not liking this.”	Shows further planning and postponement that waits for the third party
31/01/2025 10:23:56 UTC+0	Huawei WhatsApp/Genie / Top-up	“It’s all about patience. We can push harder.”	Supports pressure or escalation.
31/01/2025 10:24:11 UTC+0	Huawei WhatsApp/Genie / Top-up	“Ok. Keep me posted. I have others waiting.”	Refers potential recipients or interested parties further.
24/03/2026 15:18:20- 15:25:58	Samsung GSM SM-G950U extraction screenshot	Extraction timing and image-hash verification are visible.	Supports integrity and acquisition documentation.
Not established in visible screenshots	Patent-file metadata	No direct QT-AI-2025 created/modified/copied/exported timestamp is clearly visible.	Keeps an evidence limitation needing keyword and metadata review.
Not established in visible screenshots	Norman Nokia communication	No direct Norman request, receipt, negotiation, payment or acknowledgement is visible in the selected material.	Role of the buyer is speculative still in need of validation.

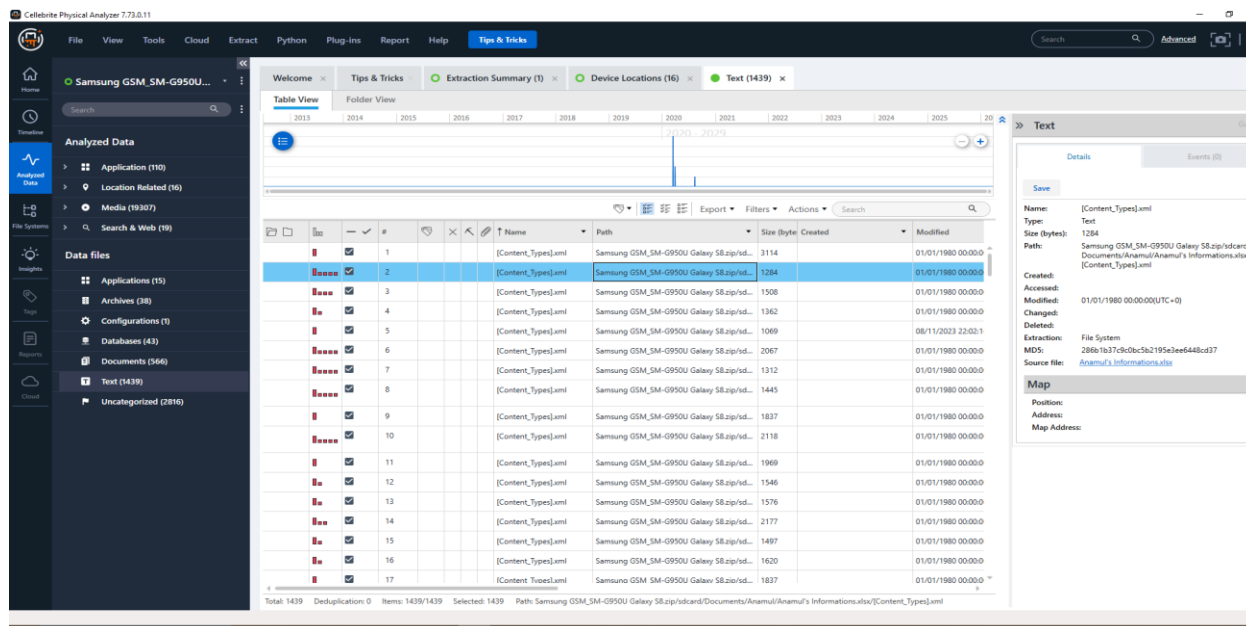


Figure 12: Nokia timeline view demonstrating how Norman/source activity can be placed into a chronological sequence.

The timeline evidence here is important because it gives chronological context to device activity history. While a timeline view alone might not establish buyer interest, it can back up or contradict the timing of communications meetings and file activity. It also helps in determining if Norman's activity fits within the suspected broader coordinated effort, when viewed alongside Huawei communications and document artifacts.

9. Suspect Role Analysis

The suspect role analysis employs three evidential classes: Supported, partially supported and requiring additional verification. This minimizes the risk of overstating but not so much that it prevents a determination on where you can reasonably see roles given by existing evidence.

9.1 Emma - primary insider suspect

Regarding the primary insider suspect, Emma is ranked by lowest score as per her assessment being comminated with those that allowed you access to confidential material and mapped source on Emma for Huawei. The Top-up messages are quite insightful as to Joe and have made it clear that they wish to sell company sensitive information. Emma has a secure position as an insider. Nonetheless, evidence of patent file metadata or transfer proof and acknowledgment from the recipient for a completed file transfer or sale is still necessary.

9.2 Joe - suspected intermediary

Although Joe performs the function, direct evidence of communication provides partial support for his role. The Top-up communication requests Joe for help regarding a delicate assignment, and Joe replies that he is free. This legitimizes Joe's associated function as a potential intermediary or communication bridge. The evidence would get stronger if payment, meeting/transfer arrangements were reflected in messages from the Samsung/Joe-source or communication relayed to Norman/Vanessa.

9.3 Norman - suspected buyer

Unless Nokia messages, emails or timeline events show demand, negotiation receipt by Norman and payment for proprietary material i.e. awareness of the following evidence makes Normans role less likely than his absence they must be assessing these influences as lesser in their triage model (ed). Nokia timeline snapshot may help chronology but not be considered buyer proof unless text material is irrefutably tied back to QT-AI-2025 or the sale context.

9.4 Vanessa / NexGen Circuits

Vanessa/NexGen Circuits should be considered with prudence. While my screenshots go beyond Vanessa meaning to other non vanessa direct communications, and the case material puts her in as a " Relevant External Contact" they are anyway chosen snaps do not show any real context of someone actually speaking directly with vanessa. Emails, WhatsApp and Instagram or call log artifacts that demonstrate contact with Vanessa linked to the proprietary material should be included under communication along with any related file activity. Vanessa still needed validation as an external contact with no direct artifacts.

Person	Likely role	Current support level	Corroborating evidence required
Emma	Insider / primary suspect	Huawei Top-up messages strongly supportive of attempted externalization intent; file transfer is still presumption based.	Screenshot of patent file possession/staging, file metadata and transfer or recipient acknowledgement.
Joe	Suspected intermediary / communication bridge	Partially supported by face-sensitive and availability response	Samsung/Joe messages or calls text message indicating a relay, call details about the reach of another user to your device; payment information and meeting times Scheduler that is considered by some as free content for fans relatively high in price.
Norman	Suspected buyer / external recipient	Requires corroboration.	Messages/emails from Nokia that show request, receipt, negotiation for payment or awareness.
Vanessa	Relevant NexGen contact	Requires corroboration.	Direct messaging or call/email/contact link tied to the proprietary content.

10. Findings, Evidential Weight and Limitations

The inquiry led to the following:

- Cellebrite Physical Analyzer usage and extraction/hash screenshots defend the forensics of it.
- The Cellebrite artifact-category views validate that prints of pertinent communications, contact info, call-logs and mail turned into evaluated in line with class (e-mail or social-media) as are files from the filesystem.
- Evidence is strongest in Huawei Top-up conversation: a forthright approach to Joe regarding sensitive business information, a message claiming access to valuable company property for sale to an interested person.
- Continuing planning at Top-up messages for pressure and onward-party involvement
- Joe is relevant as an intermediary since the communicative passage, at least for its visible part, speaks of and to him and notes his availability in this sensitive thread.
- Email and call-log artifacts give context but should not be regarded as direct evidence unless they contain patent, payment, NexGen Relation to Vanessa or sample/file transfer content.
- Document and file system screenshots document that property artifacts were searched, the uploaded evidence fails to demonstrate a QT-AI-2025 filename/path/transfer event or sale process executed.
- Norman and Vanessa are merely suspects or contacts to be pinned down by direct contact transfer evidence

The major constraint here is evidential visibility. Some artifacts show method and coverage by category rather than culpatory content. Evidence of communication strongly indicates attempted externalization or sale intent, however file transfer and completed sale are unproven unless supported through specific pairs both in the authors dominion over files to recipient artifacts Recording these limits enhances the credibility and legal defensibility of a report.

11. Conclusion

Further the obtainable use of Cellebrite is capable to support a well-founded, professional inquiry into possible abuse or misuse towards Quantum Tech proprietary material. We have the Huawei Top-up comms, which stands as strongest evidence and is captured in contact with Joe regarding a sensitive matter Statement visible on direct access to high-value company information Intention to sell externally This bolsters accusations of attempted externalization, or selling insider trade secrets.

The latter Top-up messages add to coordination and pressure, with mentions of a part local part, pushing harder push and others wait. When combined, the communication evidence is not inconsistent with an insider-driven effort to engage another individual and direct useful information away from insiders.

That said, the ending must be commensurate. The evidence cited does not even prove that QT-AI-2025 was directly copied, transferred to or received by and/or sold. To prove that finding would mean taking a straight screenshots of the patent file, metadata of files asked savings handwriting backdoor transfer logs records evidencing payment and note with receipt by Joe Norman Vanessa or any other third party external to Teradata. This in turn allows only the most defensible conclusion to be drawn, which is that all evidence strongly supports intent for attempted externalization/sale and coordination of activity but not yet confirmed exfiltration or sale completion.

12. Recommendations

12.1 Further forensic work

- Export the entire Cellebrite report per\source and keep acquisition/hash summaries.
- Keep a clean export copy of the Top-up communication artifact representing both the immediate Joe message and sale intent message.
- Search meta-keyword QT-AI-2025, QI-AI—2025 patent chip circuit CAD for design, schematic Neuro NexGen Vanessa payment sample meeting and handover sale and assignment.
- Maintain and audit all direct patent-file metadata such as name, path, size, created/modified/accessed times, and hash value if available.
- Emma, Joe, and Norman | Vanessa Now cross-reference by phone numbers Unique across 5 databases Cross reference contacts to establish links between people over time. Phone Socrates WhatsApp IDs Contacts Names Email Addresses
- Gain access to any available sanctioned cloud, email server, endpoint and enterprise logs; as mobile evidence alone may not record all file-transfer activity.
- Normalize all timestamps and document time zone handling before use of the final timeline

12.2 Organizational recommendations for Quantum Tech

- Enforce stronger removable-media controls and apply DLP policies to intellectual-property repositories such as patent or design-locked servers.
- Track access to sensitive patent folders, particularly downloads, exports, screenshots and archives as well as external sharing.
- Revisit insider-threat controls of new joiners and privileged engineering capabilities.
- Implement alerts for atypical access to critical intellectual property outside of regular hours.
- Enhance staff awareness of intellectual-property Anti-Terrorism related handling, confidentiality, and reporting suspicious contact.
- Immediately back up logs on VPN, endpoint, cloud, etc., for email and repository when the suspected theft is filed.

Appendix A. Figure Source Log

This log of figure sources records each major figure used in the report along with their evidential purpose. The material is added to ease the audit of this report against examined Cellebrite artifacts and exported screenshots.

Figure	Title / placement	Evidence source	Evidential purpose
Fig. 1	Cellebrite source overview showing Huawei and artifact categories	Cellebrite source overview / All Together view	Establishes the examination environment and relevant artifact categories.
Fig. 2	Hash and extraction-information view for Samsung GSM SM-G950U	Image-hash and source-metadata screenshot	Supports integrity, repeatability and source identification.
Fig. 3	Cellebrite workspace / evidence-source view	Cellebrite Analyzer workspace screenshot	Shows that evidence sources were loaded and reviewed in the forensic tool.
Fig. 4	Extraction and processing confirmation	Extraction/processing confirmation screenshot	Supports that the source was processed before analysis.
Fig. 5	Top-up conversation showing direct Joe message and intention to sell valuable information	Huawei WhatsApp/Genie artifact screenshot	Strongest communication evidence of sensitive information and sale intent.
Fig. 6	Later Top-up planning and pressure messages	Huawei WhatsApp/Genie artifact screenshot	Supports continued planning, pressure and onward-party involvement.
Fig. 7	Joe Marsh / Top-up contact context	Contact or group-context artifact screenshot	Links the Top-up communication context to Joe.
Fig. 8	Huawei call-log artifacts	Huawei call-log screenshot	Provides communication context and possible correlation points.
Fig. 9	Email artifact view	Email/account artifact screenshot	Provides background communication context where case-related content is visible.
Fig. 10	Document/file details view	Document details screenshot	Shows how recovered file artifacts and metadata were inspected.
Fig. 11	Samsung source document-category view	Samsung document-category screenshot	Shows that document artifacts were reviewed from the source material.
Fig. 12	Nokia timeline view	Nokia timeline screenshot	Supports chronology where the timeline event is case-relevant.

References

- [1] National Institute of Standards and Technology (NIST), *Special Publication 800-101 Revision 1: Guidelines on Mobile Device Forensics*, 2014.
- [2] ISO/IEC 27037:2012, *Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence*.
- [3] Association of Chief Police Officers (ACPO), *Good Practice Guide for Digital Evidence*, Version 5, 2012.