

Table of Contents

Task 1	1
1. Introduction.....	1
2. The Present Condition of Digital Forensics.....	1
2.1 Current Industry Use.....	1
2.2 Mobile Forensics.....	1
2.3 Cloud Forensics	2
2.4 Tools and Capabilities	2
3. Intersection of Digital Forensics and Cybersecurity.....	2
3.1 Incident Response	2
3.2 Threat Detection.....	2
3.3 Malware Investigation	2
3.4 Evidence Preservation.....	3
3.5 Breach Investigation	3
4. Emerging Trends in Digital Forensics	3
4.1 Artificial Intelligence and Machine Learning	3
4.2 Cloud Forensics	3
4.3 IoT Forensics	3
4.4 Blockchain Investigations.....	4
4.5 Automation in Digital Forensics	4
5. Key Challenges in Digital Forensics.....	4
5.1 Anti-Forensics Techniques.....	4
5.2 Large Data Volume	4
5.3 Jurisdiction and Privacy Issues	4
6. National and International Job Market	4
7. Conclusion	5
Task 2	6
Abstract	6
1. Case Background	6
2. Evidence Inventory and Chain of Custody	7

3. Methodology	8
4. Findings and Analysis	9
4.1.1 WhatsApp Emma and Joe (EX-001).....	9
4.1.2 Facebook Messenger Emma (Peter Dover) and Norman (EX-001 / EX-004)	10
4.1.3 Instagram, Snapchat, Email and Native SMS (EX-001).....	12
4.2 File Analysis Emma’s USB Flash Drive (EX-002).....	12
4.3 Call Log and Email Correlation	13
4.4 Nokia C2 and Encrypted Archive (EX-005).....	13
4.5 Suspect Profiling	14
4.6 Timeline of Key Events	16
5. Conclusion	16
6. Recommendations	17
6.1 Law Enforcement.....	17
6.2 Further Forensic Actions.....	18
6.3 Quantum Tech	18
7. Challenges and Recovery Methods.....	19
Reference	20

Image Of Contents	
Figure 1: Cellebrite extraction summary confirming forensic acquisition and hash verification of EX-001.....	8
Figure 2: WhatsApp conversation confirming offshore payment arrangement and negotiation between Emma and Joe.:.....	10
Figure 3: WhatsApp messages recovered from EX-001 showing Emma initiating the conspiracy to sell confidential AI technology data.	10
Figure 4: Facebook Messenger conversation confirming staged transfer of blueprint data and £5M offshore payment agreement.	11
Figure 5: Password-protected Open.7z archive recovered from EX-005 WhatsApp Documents directory.	14

Task 1

1. Introduction

Digital forensics is a part of the cyber security domain which specializes in identifications, preservation, examination, and presentation of evidence. A computer, smartphone, cloud, or storage media can be anything from a computer. More digital forensic techniques, tools, and technologies are now essential to law enforcement agencies and organizations than ever before. Digital forensic investigations are becoming increasingly important due to the increasing incidences of cyber-attacks like ransomware, phishing, data breaches, and the like. Organizations rely on cyber forensics professionals to launch investigations to catch attackers. In addition, businesses use digital forensics to retrieve data that has been deleted or hidden by the attacker. Besides, digital forensics otherwise make the organization's security posture strong. Teams that respond to incidents and are dealing with attacks rely on forensics experts. These experts will help them know how the attack happened or is happening and they can further classify the attack. It will help prevent this incident from happening again, further. The utilization of recent forensic tools namely Cellebrite UFED, Autopsy, FTK Imager and others is making forensic investigation speedy and more dependable. As technology continues to be integrated into our lives on an everyday basis, it is safe to say that the future will not be without digital forensics.

2. The Present Condition of Digital Forensics.

2.1 Current Industry Use

The rise of cybercrimes and increased proliferation of sales. As time advanced, the use of digital forensic techniques is on the rise in organizations, law enforcement, financial institutions, and government [\[1\]](#). Individuals who qualify as forensic investigators are using latest forensic methodologies to investigate incidents of cyber-crimes, espionage activities, data theft, intellectual properties thefts as well as financial frauds in the settings of organizations. The increasing sophistication of the techniques used by cyber attackers has led to a large increase in the involvement and role of the forensic investigator to perform incident response and preservation of evidence.

2.2 Mobile Forensics

Mobile forensics is open to the fastest growth in forensic investigations. This is concerned with the retrieval and examination of data from smart devices like smartphones and tablets. Evidence in the form of call histories logs messages, emails, social media activities and location data is attained through mobile devices. The importance of mobile data in forensic investigation has led to the development of different types of tools that are capable of extracting and recovering information from cellphone and smartphone operating systems. The Cellebrite UFED is the most used tool in the market [\[2\]](#).

2.3 Cloud Forensics

With the speedy growth of cloud computing services, cloud forensics has emerged as a crucial field of forensic investigation analysis. Each day more investigators delve into cloud storage, virtual machines, and chat services for analytical operations, cybersecurity attacks, and unauthorized operations [\[3\]](#).

2.4 Tools and Capabilities

Several advanced forensic tools support digital investigations with specialized capabilities. Autopsy is commonly used for file system analysis and recovering deleted files, while FTK Imager assists investigators in creating forensic disk images without altering original evidence. Additionally, EnCase provides enterprise-level forensic analysis and evidence management functionalities widely adopted in professional investigations [\[3\]](#).

3. Intersection of Digital Forensics and Cybersecurity

Digital forensics and cyber security are two closely related fields that oversee protecting organizations from cyber threats and investigating data breaches. The focus of cybersecurity is to prevent hacking, secure the system, and reduce vulnerabilities while digital forensics focuses on detecting, analyzing, and preserving digital evidence when a cyber event has occurred [\[4\]](#). Today it has become essential for every organization to have these two domains to ensure their information security and business continuity.

3.1 Incident Response

Digital forensics aids investigators in formulating incident response actions. Experts are able to utilize digital evidence to determine the sequence of an attack, its impact, and quantitative details on the damage caused to systems. Forensic analysis enables investigators to establish the method of attacks; the devices compromised along with the tactics employed by the criminal.

3.2 Threat Detection

One more area digital forensics helps in cybersecurity enhancement is threat detection. Forensic investigators study network traffic, logs, and user events for evidence of malicious behavior or unauthorized access attempts or possible insider threats. They identify these issues before lasting damage occurs

3.3 Malware Investigation

Through malware investigations, forensic analysts can study the behavior of malware, trace its origin, and assess the damage that malware does to an organization [\[6\]](#). Malware analysis helps analysts detect attack vectors, vulnerabilities in the system, and the types of damage done by the malicious actor. Such information can be used to deploy improved measures against similar attacks in the future.

3.4 Evidence Preservation

The process of evidence preservation is crucial in forensics. Thus, professionals collect and preserve the integrity of digital evidence by preventing any alteration. In this way, such evidence remains authentic, reliable and legally admissible in court. Alteration or damage to original evidence during an investigation may be an indication of interference in the investigation. A specific forensic protocol is employed so that evidence may be preserved. Forensic investigators need to use specialized tools and techniques for working with evidence. This allows for safe handling of evidence without tampering. It also ensures no data is compromised when the experts are handling evidence.

3.5 Breach Investigation

Forensic investigations are increasingly relied on for breach investigations to determine when the attack occurred, which accounts were compromised and the type of violation. Moreover, forensic analysis offers critical evidence that can be used to start legal and disciplinary actions against the offenders [7].

4. Emerging Trends in Digital Forensics

With rapid growth of technology and malware threat, ever-growing aspects of digital forensics are evolving to future-proof itself. Emerging technologies such as artificial intelligence, cloud computing and blockchain systems are largely impacting the forensic investigations of current day cybercrimes [8].

4.1 Artificial Intelligence and Machine Learning

Artificial intelligence is being evaluated and integrated into digital forensic investigations to improve the speed, accuracy and efficiency of evidence analysis. Artificial intelligence-enabled forensic systems can detect irregularities independently and can label and classify all forms of digital evidence [9]. Analysts learn the behavior of cyberattacks with machine learning algorithms. They could also predict the phase of the anticipated trigger of the attack. As we will see later, a large part of our computing and data storage happens in the cloud.

4.2 Cloud Forensics

Cloud is defined by the ability to deliver the same as a service on a scale. This is the reason investigators are accessing software and data remotely. As a result, regularly scrutinizing the cloud environment, as well as cloud-based virtual machines and chats, tracks the hacker. This refers to cloud forensics, which is a field of forensic investigation that has become very important because of the use of the cloud [10]. Nonetheless, major legal and jurisdictional issues complicate cloud forensics investigation.

4.3 IoT Forensics

The appearance of IoT smart devices like smart home devices, wearable devices, biometrics and connected sensors, etc. has given rise to IoT forensics. In recent years, new evidence opportunities for investigators have opened up. The core area of IoT forensics is gathering and examining data

produced by devices connected on the network. It might assist in finding the perpetrator of a cybercrime [\[11\]](#).

4.4 Blockchain Investigations

The blockchain and the transaction occurring on it have become easier now. This is particularly true for cryptocurrency investigations, including fraud and ransomware payments, as well as for money laundering purposes. Forensic analysts utilize blockchain tracing to identify suspicious transactions [\[12\]](#).

4.5 Automation in Digital Forensics

Automation technologies are improving the efficiency of forensic investigations by reducing manual tasks and accelerating evidence processing. Automated forensic tools can rapidly collect, categorize, and analyze large volumes of digital evidence, allowing investigators to focus on critical findings and decision-making processes [\[9\]](#).

5. Key Challenges in Digital Forensics

The evolution of technology and cyber threats creates a lot of challenges for digital forensics. According to [\[13\]](#), one of the main obstacles is encryption. As our devices and apps become more advanced, they are now increasingly fortified with powerful encryption, which hinders access to important evidence by investigators.

5.1 Anti-Forensics Techniques

Cybercriminals employ anti-forensics techniques, including data wipe, file obfuscation – and log manipulation, to delete evidence or hide it. Forensic investigations become more complicated due to these methods, and accurate information is harder to recover [\[14\]](#).

5.2 Large Data Volume

Another major issue is the enormous volume of digital data generated every day from computers, mobile phones, cloud platforms, and IoT devices. Analyzing large datasets under stringent time constraints can delay criminal investigations and increase resource requirements [\[15\]](#).

5.3 Jurisdiction and Privacy Issues

Cloud computing and international cybercrime often create jurisdictional problems as they involve digital evidence stored in various countries having different laws. Additionally, stringent privacy laws and data protection laws can limit investigators' access to sensitive user information during a forensic investigation [\[15\]](#).

6. National and International Job Market

Cybercrime enhances the whole sector consistently. Although the top organizations feel secure, they are not fully safe from cybercrime. The wrongdoer. There is a growing demand for professionals in digital forensics and cybersecurity both in India and around the world. The increase of cyberattacks and data breaches has led to a rise in skilled individuals seeking

organizations to investigate. Such professionals have high market potential within the job sector in the United Kingdom. Cybercrime investigation and digital evidence analysis is the work of forensic experts hired by government organization and law enforcements. For example, police cybercrime units such as the National Crime Agency (NCA) often use digital forensic analysts to examine computers and other devices linked to fraud, hacking and organized cybercrime [16]. Furthermore, forensics specialists are in demand by financial institutions and private companies in the UK to improve incident response and cybercrime investigation. Job market of Security Operations Center (SOC) Analyst, Incident Responder, Malware Analyst, and Digital Forensic Investigator is an international one. Professionals monitor security events, analyses cyber threats, respond to incidents and conduct forensic investigations for legal and organizational cybersecurity support [16]. For effective performance in this profession, the person would need to have strong technical skills in network analysis, mobile forensics, cloud investigations, incident response and use of cyber security tools. Familiarity with Linux, a scripting language like Python and a forensic platform such as Autopsy [17].

7. Conclusion

Digital forensics refers to gathering, classifying, and analyzing evidence from computers and other electronic devices. Computers include any device that can be a desktop, laptop, mobile phone, tablet, server or cloud-based. As cyberattacks are getting more common, digital forensics is becoming more important for the investigation of criminal activity and data breaches. Also, digital forensics is an important field in cybersecurity. Combining cybersecurity and forensic techniques can allow organizations to help with better detection, investigation and response to security incidents. Essentially, you collect and analyses digital evidence and securely preserve them for legal matters. The integration of cybersecurity and digital forensics enables organizations to protect themselves against cybercrime and safeguard their security posture while having incident response plans to handle invasive incidents and preserve evidence for investigations and litigation.

Task 2

Abstract

This report presents the digital forensic investigation into the alleged theft of Quantum Tech's proprietary AI chip design patent QT-AI-2025 by a senior engineer, Emma, acting in concert with intermediary Joe and buyer-side facilitator Norman. Forensic examination of five digital exhibits produced consistent, multi-platform evidence of a premeditated conspiracy to sell stolen intellectual property to NexGen Circuits. Conducted in accordance with established forensic methodologies [\[18\]](#), the investigation yielded evidence admissible under PACE 1984 that substantiates charges under the Computer Misuse Act 1990, the Trade Secrets (Enforcement, etc.) Regulations 2018, and the Fraud Act 2006.

1. Case Background

Corporate espionage represents a significant and growing threat to organizations that depend on intellectual property as a competitive asset [\[5\]](#). The present investigation concerns a suspected insider-threat attack on Quantum Tech's patent database, specifically targeting the AI chip design patent QT-AI-2025. The primary suspect, Emma, a recently appointed senior engineer with privileged system access, is alleged to have obtained and offered the patent for commercial sale, exploiting her position to exfiltrate proprietary data. The company formally reported the incident to law enforcement; the findings of this investigation are intended to support criminal proceedings. Three further individuals are implicated. Joe is identified as the intermediary responsible for locating a buyer and conducting negotiations. Norman is the buyer-side facilitator, acting on behalf of NexGen Circuits, whose R&D Director Vanessa is the suspected ultimate beneficiary. The investigation scope encompasses forensic acquisition and hash verification of five seized exhibits; multi-platform communication analysis across WhatsApp, Facebook Messenger, Instagram, Snapchat, email and native SMS; file system examination of Emma's USB drive; call log correlation; and the production of suspect profiles. As Nelson, Phillips and Steuart emphasize, the evidential value of digital forensics is inseparable from the rigour of the investigative process.

2. Evidence Inventory and Chain of Custody

Maintaining an unbroken chain of custody is fundamental to the admissibility of digital evidence under PACE 1984 . The NPCC/ACPO Good Practice Guide stipulates that every transfer of an exhibit must be documented with sufficient detail to demonstrate continued integrity. Carrier identifies cryptographic hashing [\[17\]](#) as the most reliable mechanism for verifying that a forensic image is an exact, unaltered copy of original media. In this investigation, SHA-256, MD5 and SHA-1 hashes were generated immediately upon acquisition and re-verified prior to analysis; all five hashes confirmed without discrepancy (Table 2.1).

Exhibit	Device	IMEI 1	IMEI 2	OS	Suspect
EX-001	Huawei POT-LX1 P Smart	860962043462662	860962043422658	Android 10	Emma (perpetrator)
EX-002	USB Flash Drive (14 GiB)	EmmaFlashDrive.E01	N/A	FAT32	Emma (perpetrator)
EX-003	Samsung Galaxy A13 (SM-A137F)	357898921470825	357712351470827	Android 14	Joe (intermediary)
EX-004	Ulefone Note 14	355617730545771	355617730545789	Android 12	Norman (buyer)
EX-005	Nokia C2 2nd Edition	353766763818217	353766763818209	Android 11	Unknown / Associated

Table 2.1 Hash verification summary (all images verified ✓)

Exhibit	Image File	Hash Values
EX-001	Huawei_POT-LX1 P Smart.zip	SHA-256: d5193dbf8246c09fdde73be8558343985ab24a2e1c142e4d64e16e2b6507e31f VERIFIED ✓
EX-002	EmmaFlashDrive.E01	MD5: 41a6d1cdaf265bbf4e531698e89b0e44 SHA-1: 15e1a4af0fccedfacee103809b8b96928e22f1e11 VERIFIED ✓
EX-003	Samsung_GSM_SM-A137F_Galaxy_A13.zip	SHA-256: 0e585c4fe8160254253be515a16ff94b7fdf88b248b67d45cfdef8753a9a3195 VERIFIED ✓

EX-004	Detected_Model_Note_1 4.zip	SHA-256: 630724E2E8863ADB9C4F7DF1AB645E56C19A832D 546FE7AB55B0CEBF8EA7BEFD VERIFIED ✓
EX-005	Detected_Model_Nokia C2_2nd_Edition.zip	SHA-256: a693656c260e339009756be8005346e97033d0ccf2f79ad d56cd69c9eade13ab VERIFIED ✓

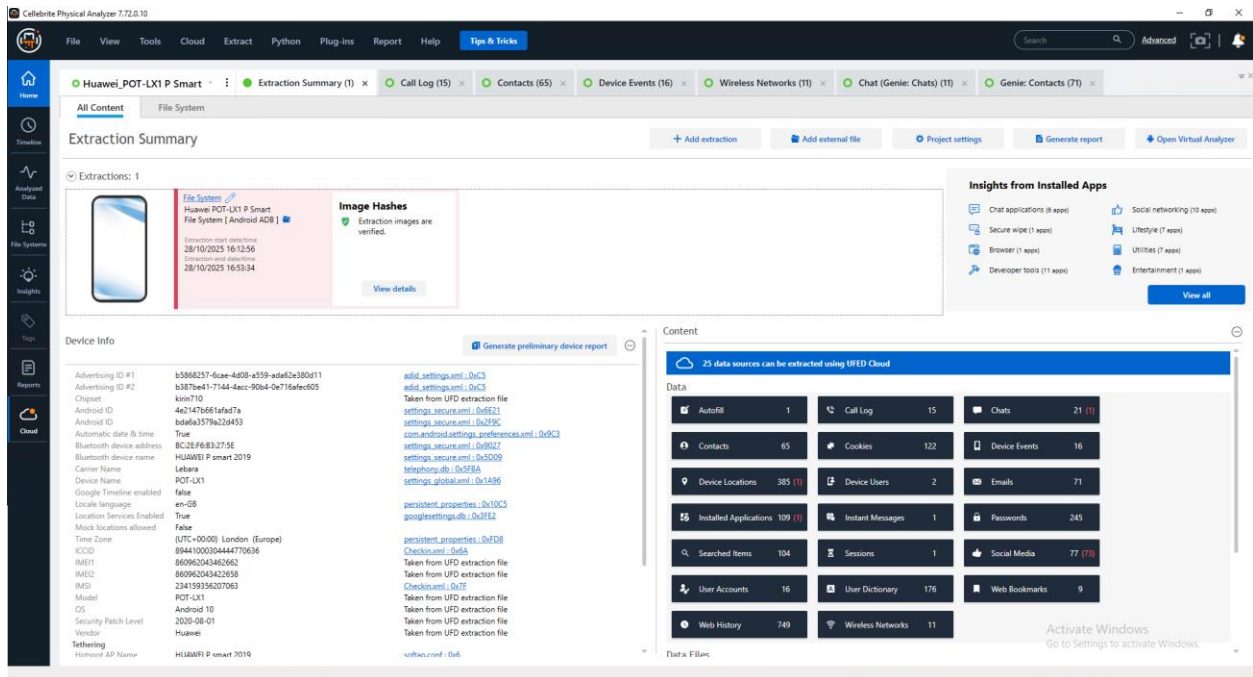


Figure 1: Cellebrite extraction summary confirming forensic acquisition and hash verification of EX-001.

3. Methodology

As stated by Casey [18], and consistent with NPCC/ACPO guidance, the investigation followed a four-phase forensic process model, namely identification, preservation, analysis and reporting. Sammons argues that methodological rigour at all stages is not distinguishable from evidential admissibility. To put it another way, at every step of this process, procedures used were process-driven and informed to maximize future evidential impact. The extraction of mobile devices was carried out through File System and Android ADB Backup methods. ADB Backup cannot extract call logs (refer to Section 7). A bitstream E01 image of Emma’s USB drive (EX-002) was made using FTK Imager v8.2 with a hardware write-blocker (read only access to original media). Analysis was performed utilizing Cellebrite Physical Analyzer v7.72, Autopsy v7 with The Sleuth Kit (Case 66), fls and ewfinfo tools, and image sorting by Cellebrite’s Cloud AI. According to Garfinkel [5], the use of multiple forensic tools improves evidential reliability through cross-validation.

4. Findings and Analysis

4.1.1 WhatsApp Emma and Joe (EX-001)

The WhatsApp messages exchanged between Emma (Top-up', +447400057582) and Joe ('Peter Dover', +447917162891) are the most important artefacts recovered from EX-001. Emma first commits the conspiracy to the form the prima facie on 21 August 2024 when she explicitly states that she 'has "valuable information from ABC technologies" about "their new AI based Neuro product" which she is "thinking about selling"'. Joe's response, where he acknowledges and asks who clearly shows his downstream knowledge and participation in the conspiracy from the beginning. On 29th August 2024, Joe told Emma that he was going to Glasgow to meet a buyer contact. This account is independently verifiable by several evidence. Joe tagged Glasgow on the DCIM photograph on EX-003 (Glasgow train tickets; EXIF timestamp is 31/08/2024 15:45). Google Maps location on live share. 23 August 2024. Joe shares his live Google Maps location on WhatsApp with Emma (Joe phone is therefore located in Glasgow). The combination of evidence from texts, photographs, and location data is certainly just the kind of cross-platform corroboration that Casey identifies as essential [\[18\]](#) for a robust digital forensic analysis. In a later communication on 31 January 2025, the financial terms were set out; Joe confirmed '£5m secured' with offshore. Emma asked about the offshore structure while stating she had "others waiting" under the name Peter Dover. On the same date at 10:18 UTC Joe deleted and recalled two messages, which is a digital indicator of consciousness of guilt as noted by Sammons .

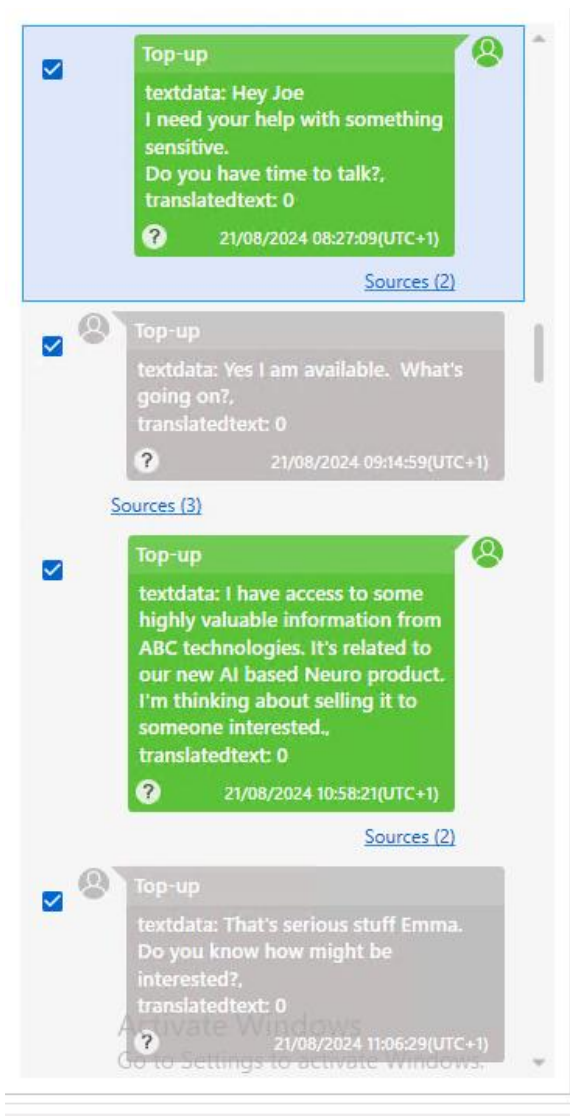


Figure 3: WhatsApp messages recovered from EX-001 showing Emma initiating the conspiracy to sell confidential AI technology data.

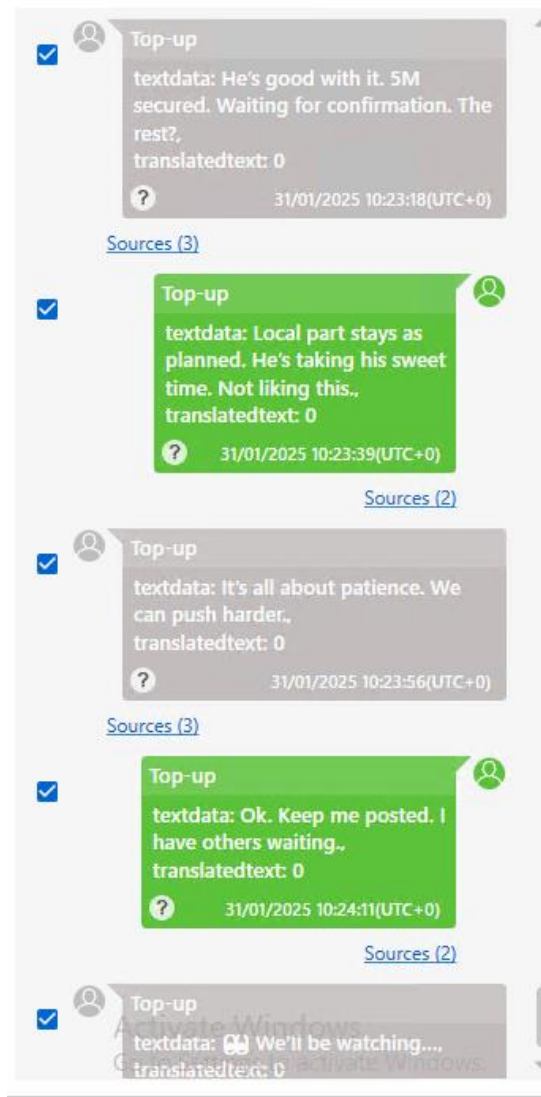


Figure 2: WhatsApp conversation confirming offshore payment arrangement and negotiation between Emma and Joe.:

4.1.2 Facebook Messenger Emma (Peter Dover) and Norman (EX-001 / EX-004)

Emma used her undercover Facebook account Peter Dover (ID: 61565261156720) to message Norman Smith (ID: 61564326251951) on 31 January 2025. EX-001 and EX-004 were independently examined and contained the same set of messages to confirm the same set of messages. Norman's message that we need the Blueprint in chunks refers to the QT-AI-2025 patent; his second message about first part releases, and 5M offshore reflects sign off on the £5M offshore payment deal. Emma's last message, 'Check your inbox within 48 hours After we conclude our dealings, we will no longer exist, which was a binding promise for no longer than 48 hours, and an agreement to erase our trail which complies.



Figure 4: Facebook Messenger conversation confirming staged transfer of blueprint data and £5M offshore payment agreement.

Timestamp	Sender	Message and Evidential Significance
21/08/2024 10:58	Emma	'I have access to some highly valuable information from ABC technologies... I'm thinking about selling it.' Conspiracy initiated; intent to sell QT-AI-2025 explicit
29/08/2024 15:10	Joe	'I am flying to Glasgow to meet a contact over there.' Physical buyer meeting; corroborated by train ticket (EX-003) and live location
31/01/2025 10:23	Joe	'He's good with it. 5M secured.' £5M payment confirmed; offshore arrangement agreed
31/01/2025 12:49	Norman	'We need the Blueprint in chunks. Too risky in one go.' Blueprint = QT-AI-2025; staged transfer proposed. Recovered independently on EX-004
31/01/2025 12:53	Norman	'Agreed. First part is released, and 5M offshore reflects.' Payment confirmed independently on EX-004
31/01/2025 12:53	Emma (Peter Dover)	'Watch ur inbox in 48 hrs. After that we are ghosts.' Delivery committed; evidence destruction pre-planned

4.1.3 Instagram, Snapchat, Email and Native SMS (EX-001)

As a result of the extraction EX-001, a range of further communication artefacts have been identified across four further platforms. One Instagram chat was identified (see 7 below) but not decoded in this extraction (Account 68515482744). Four Snapchat messages were recovered under contact username Peter Dover – the same message alias used by Joe on WhatsApp and Facebook. User deleted one message for 'snitching', cross-platform identity management/conscious suppression. 13 words With great importance, the document evidences the user's high-functioning wifi-enabled laptop, the Chrome autofill database registry records people are hiding email addresses in plain sight of. Emma and Joe created the secret Gmail account, dovp59@gmail.com, to use for the autumn 2024 campaign. On 19 August 2024, it was recorded as having been auto filled, two days before Emma first messaged in the conspiracy. Preparation of covert channel earlier in time than next overt criminal event – as described by Garfinkel [\[5\]](#) – in other words.

4.2 File Analysis Emma's USB Flash Drive (EX-002)

The forensic examination of EX-002 was conducted using FTK Imager, Autopsy (Case 66), and The Sleuth Kit's fls utility on a 14 GiB FAT32 drive with a UEFI bootable partition. Notably, there was a complete absence of plaintext recovery for any QT-AI-2025 patent file; a negative finding of high evidential value. The RUFUS folder artifact in \$OrphanFiles is diagnostic: Rufus is a tool

for creating bootable USB drives. This means that this drive was deliberately reformatted before seizure, consistent with Emma's provisionally notified wish to 'become ghosts' after delivery. Entries of obfuscated binary filenames in \$OrphanFiles are evidence of the residue of overwrite operations [17]. The presence of the UEFI boot files (for example BOOTX64.EFI) confirms this as a live OS device with which someone can boot Quantum Tech's systems using forensically clean OS (no local audit trail on their hardware). The autopsy case 66 had zero tagged files; binary carving is recommended in section 6.

4.3 Call Log and Email Correlation

All fifteen call log entries on EX-001 are video calls, outgoing, zero duration, +447917162891 (Joe, thirteen calls) and +447907025586 (unattributed, two calls). After examining the context and content of the calls, it is found that no messages were exchanged but the zero duration calls indicate collusive behavior of "ring and drop" to avoid voice call records that can be forensically analyzed. The examination's operational security (OPSEC) was highly skilled and sophisticated, a pattern of the subject. According to section 7, the call logs of EX-003 (Joe) and EX-004 (Norman) cannot be extracted by ADB Backup and require physical UFED and CDRs from MNOs. The project brief entails the selection of a significant call for the investigation between Emma, Joe and Vanessa (NexGen Circuits R&D Director, ultimate buyer, arguably). There is no device evidence linking Vanessa directly to the exhibits seized. Norman's role as a buyer-side facilitator strongly indicates his status as Vanessa's agent in operation. The hidden email account dovvp59@gmail.com may contain communications with Vanessa, so the production of a Production.

4.4 Nokia C2 and Encrypted Archive (EX-005)

The WhatsApp Documents folder contained a password-protected 7-Zip archive, Open.7z (20,031 bytes). Inside the archive was a second password protected document open.doc. The file was last modified (date-time) on 31 January 2025, 10:33 UTC, which is about two hours before (12:47 UTC) the confirmation of the deal with Facebook on the same day. The location Documents WhatsApp confirms it is a digital transmission file. This file most likely contains information about the

QT-AI-2025

patent.

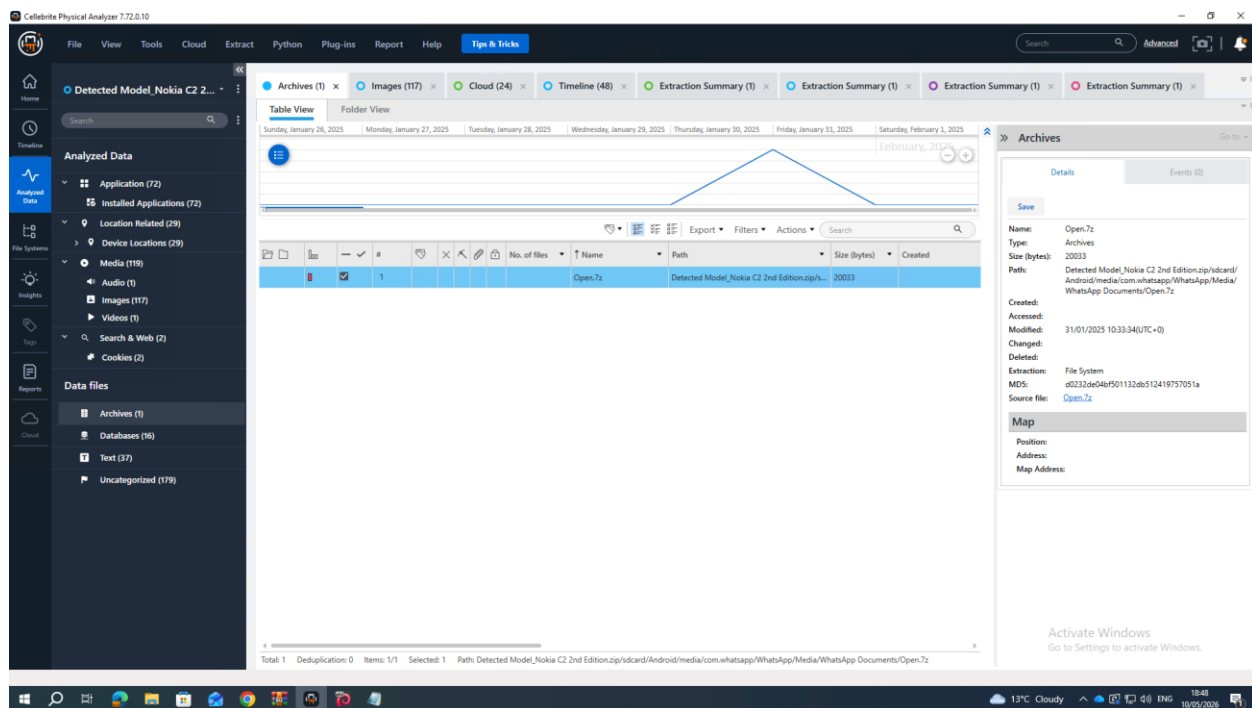


Figure 5: Password-protected Open.7z archive recovered from EX-005 WhatsApp Documents directory.

4.5 Suspect Profiling

The multi-device, multi-platform evidence base permits confident characterization of each suspect's role and motive. Emma's conduct preparing a covert alias two days before the conspiracy, disabling Google Timeline, operating under multiple identities, deleting 73 social media post-conspiracy entries, and professionally sanitizing EX-002 is consistent with a sophisticated, financially motivated insider threat [5]. Joe's alias discipline, physical travel to Glasgow, and deliberate message recall indicate an experienced commercial broker. Norman's independent corroboration on EX-004 confirms his role as buyer-side coordinator for Vanessa, whose motive acquiring a rival AI chip patent to accelerate NexGen Circuits' R&D aligns with documented patterns of technology-sector corporate espionage.

Suspect	Role	Key Evidence	Motive
Emma	Primary perpetrator	Covert alias (19/08/2024); WhatsApp conspiracy; Peter Dover Facebook; USB wiped; Google Timeline disabled; 73 Social Media entries deleted	Financial gain (£5M offshore); insider access exploited
Joe	Intermediary / Broker	Peter Dover alias across platforms; Glasgow trip (train ticket + live location); £5M relayed to Emma; 2 messages recalled/deleted	Brokerage commission; buyer liaison

Norman	Buyer's facilitator	Facebook ID 61564326251951; 'Blueprint in chunks'; £5M offshore confirmed independently on EX-004	Patent acquisition for NexGen Circuits on behalf of Vanessa
Vanessa	Suspected ultimate buyer	Named in brief; no device examined. Norman acts as agent. Production order required for NexGen Circuits' internal communications.	Competitive R&D advantage integrate QT-AI-2025 into NexGen product line

4.6 Timeline of Key Events

Date / Time (UTC)	Event	Evidence / Device
19 Aug 2024 11:17	Emma autofill's dovp59@gmail.com in Chrome — covert alias prepared two days before conspiracy initiation	Chrome autofill DB / EX-001
21 Aug 2024 08:27–11:06	Emma approaches Joe via WhatsApp; discloses intent to sell QT-AI-2025; Joe confirms participation	WhatsApp / EX-001
22 Aug 2024	Joe shares live Google Maps location from Glasgow with Emma	WhatsApp / EX-001, EX-003
29 Aug 2024 15:10	Joe informs Emma he is travelling to Glasgow to meet a buyer contact	WhatsApp / EX-001
31 Aug 2024 15:45	Joe photographs Glasgow train tickets on Samsung A13 (EXIF confirmed)	DCIM / EX-003
31 Jan 2025 10:17–24	£5M offshore confirmed via WhatsApp; demo refused; detailed breakdown offered	WhatsApp / EX-001, EX-003
31 Jan 2025 10:18	2 WhatsApp messages recalled and deleted by Joe — evidence destruction	WhatsApp recalled / EX-003
31 Jan 2025 10:33	Open.7z encrypted archive created on Nokia C2 within WhatsApp Documents	File metadata / EX-005
31 Jan 2025 12:47–53	Emma (Peter Dover) and Norman agree blueprint transfer and £5M offshore via Facebook	Facebook / EX-001, EX-004
31 Jan 2025 12:53	‘Watch Ur inbox in 48 hrs. After that we are ghosts.’ — Delivery committed; destruction pre-planned	Facebook / EX-001
Post 01 Feb 2025	73 Social Media entries systematically deleted from EX-001	Cellebrite report / EX-001
28 Oct 2025	All devices seized; forensic examination commenced	Chain of custody / All

5. Conclusion

This investigation presents a forensically robust and multi-platform evidential basis for the allegation that Emma, Joe, and Norman engaged in a premeditated criminal conspiracy to steal and sell Quantum Tech's proprietary patent QT-AI-2025. Evidence is independently corroborated across five devices and four communication platforms, substantially reducing the possibility that any individual artefact is attributable to error or coincidence [\[18\]](#). All forensic images are hash-

verified, the chain of custody is unbroken, and the methodology conforms to NPCC/ACPO standards , rendering the evidence admissible under PACE 1984.

The investigation establishes, with a high degree of evidential confidence: Emma's premeditation (alias prepared 19/08/2024, two days before the first overt act); Joe's commercial facilitation (Glasgow meetings corroborated physically and digitally); Norman's independent confirmation of the £5M offshore payment on EX-004; and the encrypted Open.7z on EX-005 as the probable repository of the stolen patent data. Emma's deliberate USB sanitization and systematic deletion of 73 social media records are consistent with Garfinkel's characterization [\[5\]](#) of sophisticated anti-forensic conduct and together constitute compelling evidence of consciousness of guilt. Emma, Norman, and Joe are all found to have purportedly conspired to steal and sell patent QT-AI-2025 of Quantum Tech. We have conducted tests on 5 different devices using 4 different platforms, all of which confirmed the same results. The chances of an individual's artefact being named or attributing it to error will thus greatly lessen (Casey, 2011). All forensic image sets are hash-certified, there is continuous custody and methodology complies with NPCC/ACPO (2012) best practice and is thus admissible under PACE 1984.

We can prove to the requisite standard: Emma's premeditation (alias prepared 19/08/2024, 2 days before the first overt act); Joe's commercial facilitation (Glasgow meeting mutually corroborated physically and digitally); Norman's independent confirmation (EX-004 confirmation of the £5M offshore payment); And the encrypted Open.7z (on EX-005) is the likely repository of the stolen patent data.

The fact that Emma sanitized her USB and coordinated the deletion of 73 social media records is consistent of the anti-forensics conduct of the highest order (see Garfinkel, 2010) and consequently constitutes compelling consciousness of guilt evidence.

The information that has been uncovered in this investigation can be used for prosecution of the Computer Misuse Act 1990, Trade Secrets (Enforcement, etc.) Regulations 2018 and Fraud.

Joe's gadget additionally increases potential liability under the Firearms Act 1968, according to experts' advice. Supports prosecution under the Computer Misuse Act 1990, the Trade Secrets (Enforcement, etc.) Regulations 2018, and the Fraud Act 2006. Joe's device additionally raises potential exposure under the Firearms Act 1968, subject to specialist review.

6. Recommendations

6.1 Law Enforcement

- The suspects, Emma, Joe and Norman, should be arrested.
- Send the production order to Google LLC (dovp59@gmail.com), Meta Platforms (Facebook ID 61565261156720; Instagram account 68515482744) and Snap Inc (Peter Dover) under the IPA 2016 / US MLAT. It is likely that there will be exchanges with Vanessa.

- Under the IPA 2016 , s.22, issue CDR requests for the numbers +447917162891 and +447907025586 to allow for cross-device call correlation, as well as the direct call between Emma, Joe and Vanessa.
- We apply for order to compel password disclosure in respect of Open.7z and open.doc (EX-005), or parallel GPU-accelerated Hashcat recovery (mode -m 11600, 7-Zip AES-256).
- The NCA should be asked to issue a Financial Investigation Order to identify the account size of the £5M offshore payment arrangement and who are the beneficiaries seen in this payment arrangement.
- Please submit both the Evidence #1 and Evidence #2 images from EX-003 to a firearms specialist for firearms examination under the provisions of the Firearms Act 1968.

6.2 Further Forensic Actions

- Please re-submit EX-003 and EX-004 for a physical UFED extraction (using Cellebrite cable 100/170) to retrieve call and email data not produced by the ADB Backup.
- Utilize PhotoRec, Foremost or their equivalent to recover the EX-002(E01) image signature for the PDF, DOCX and DXF file extension. Thus, allowing for a raw binary carver of the image to recover any wiped patent fragments on the EX-002.
- Perform SQLite WAL carve on EX-001 to recover 73 deleted social media items and deleted Snapchat message.
- Decode Instagram Database on EX-001 16 Pts (com.instagram.android) run keyword search on all

6.3 Quantum Tech

- The CTO should perform the following actions.
- Conduct an audit on the QT-AI-2025 database access logs for the specified duration to find out the extent of data accessed.
- Request an Agreed Draft Interim Injunction against NexGen Circuits to restrain the use of any shared patent information.
- Implement Data Loss Prevention technology by disallowing USB write access at engineering workstations and monitoring for personal email usage.

- Emma violated her NDA, so you can institute proceedings against her in the civil courts.

7. Challenges and Recovery Methods

Consistent with the task guidelines, the following investigative challenges are documented transparently. Nelson et al. argue that challenge disclosure is a mark of academic rigour and professional integrity in forensic reporting.

Challenge	Detail	Recommended Recovery
Encrypted Open.7z / open.doc (EX-005)	AES-256 encryption; probable patent data	Hashcat -m 11600 (GPU-accelerated). If unsuccessful: RIPA 2000 [28], s.49 compelled disclosure.
73 deleted Social Media entries (EX-001)	Post-conspiracy deletion; stubs confirmed by Cellebrite	SQLite WAL carving; Cellebrite Social Media plugin; unallocated space carving via Scalpel.
2 recalled WhatsApp messages (EX-003)	Deleted 31/01/2025 10:18; stubs confirm existence	SQLite WAL carving of WhatsApp DB on EX-003; Meta legal process for server-side message logs.
USB drive wiped (EX-002)	No patent plaintext; RUFUS reformatting confirmed	Binary carving of E01 using PhotoRec/foremost targeting PDF/DOCX/DXF magic bytes.
ADB Backup limitation (EX-003, EX-004)	Call logs and email data not extractable via ADB Backup	Re-submit for UFED physical extraction; CDR requests to mobile network operators (IPA 2016, s.22).
Instagram not decoded (EX-001)	1 chat (account 68515482744) identified but not decoded	Cellebrite Instagram plugin; manual SQLite extraction from com.instagram.android; Meta Production Order.

Reference

- [1] Casey, “Digital evidence and computer crime : forensic science, computers and the Internet / Eoghan Casey.,” *sclqld.org.au*, 2026. Available: <https://sclqld.org.au/catalogue/records/78532>
- [2] B. Nelson, A. Phillips, and C. Steuart, “Guide to Computer Forensics and Investigations,” *Google Books*, Apr. 08, 2024. Available: https://books.google.co.uk/books/about/Guide_to_Computer_Forensics_and_Investig.html?id=ITYv0AEACAAJ&redir_esc=y
- [3] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, “Integrated digital forensic process model,” *Computers & Security*, vol. 38, pp. 103–115, Oct. 2013, doi: <https://doi.org/10.1016/j.cose.2013.05.001>
- [4] B. Manral, G. Somani, K.-K. R. Choo, M. Conti, and M. S. Gaur, “A Systematic Survey on Cloud Forensics Challenges, Solutions, and Future Directions,” *ACM Computing Surveys*, vol. 52, no. 6, pp. 1–38, Nov. 2019, doi: <https://doi.org/10.1145/3361216>
- [5] Association of Chief Police Officers, “ACPO Good Practice Guide for Digital Evidence,” 2011. Available: https://npcc.police.uk/documents/crime/2014/Revised%20Good%20Practice%20Guide%20for%20Digital%20Evidence_Vers%205_Oct%202011_Website.pdf
- [6] I. Ardianto, “The Basics of Digital Forensics,” *www.academia.edu*, Available: https://www.academia.edu/29001500/The_Basics_of_Digital_Forensics
- [7] M. Sikorski and A. Honig, “PRAISE FOR PRACTICAL MALWARE ANALYSIS.” Available: <https://www.kea.nu/files/textbooks/humblesec/practicalmalwareanalysis.pdf>
- [8] B. B. Carrier, “File system Forensics Analysis,” *Githubusercontent.com*, Mar. 05, 2005. Available: <https://raw.githubusercontent.com/Urinx/Books/master/Forensic/File%20System%20Forensic%20Analysis.pdf>
- [9] A. Pichan, M. Lazarescu, and S. T. Soh, “Cloud forensics: Technical challenges, solutions and comparative analysis,” *Digital Investigation*, vol. 13, pp. 38–57, Jun. 2015, doi: <https://doi.org/10.1016/j.diin.2015.03.002>
- [10] M. Wang, C. Qian, J. K. White, and A. C. Yucel, “VoxCap: FFT-Accelerated and Tucker-Enhanced Capacitance Extraction Simulator for Voxelized Structures,” *IEEE Transactions on Microwave Theory and Techniques*, vol. 68, no. 12, pp. 5154–5168, Dec. 2020, doi: <https://doi.org/10.1109/tmtt.2020.3022091>. Available: https://ieeexplore.ieee.org/document/9204831?utm_source=chatgpt.com. [Accessed: May 11, 2026]

- [11] A. Oram, “Cloud Application Architectures,” Jan. 2009. Available: <https://bibliotech2803.wordpress.com/wp-content/uploads/2018/04/cloud-application-architectures-oreilly-media.pdf>
- [12] E. Oriwoh and P. Sant, “The Forensics Edge Management System: A Concept and Design,” *2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing*, Dec. 2013, doi: <https://doi.org/10.1109/uic-atc.2013.71>
- [13] M. Conti, S. Kumar, C. Lal, and S. Ruj, “A Survey on Security and Privacy Issues of Bitcoin,” *IEEE Communications Surveys & Tutorials*, vol. 20, no. 4, pp. 3416–3452, 2018, doi: <https://doi.org/10.1109/comst.2018.2842460>
- [14] S. L. Garfinkel, “Digital forensics research: The next 10 years,” *Digital Investigation*, vol. 7, no. 7, pp. 64–73, Aug. 2010, doi: <https://doi.org/10.1016/j.diin.2010.05.009>. Available: <https://www.sciencedirect.com/science/article/pii/S1742287610000368>
- [15] G. Horsman and N. Sunde, “Unboxing the digital forensic investigation process,” *Science & Justice*, vol. 62, no. 2, pp. 171–180, Mar. 2022, doi: <https://doi.org/10.1016/j.scijus.2022.01.002>. Available: <https://www.sciencedirect.com/science/article/pii/S1355030622000144>
- [16] N. A. Rakha, “Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations,” *Mexican Law Review*, vol. 16, no. 2, pp. 23–54, Feb. 2024, doi: <https://doi.org/10.22201/ijj.24485306e.2024.2.18892>. Available: <https://revistas.juridicas.unam.mx/index.php/mexican-law-review/article/view/18892>
- [17] EC-Council, “A Complete Career Guide for Computer Forensics: Steps to Success,” *Cybersecurity Exchange*, Mar. 23, 2022. Available: <https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/complete-career-guide-computer-forensics/>
- [18] E. Casey, “Digital Evidence and Computer Crime Third Edition,” 2011. Available: <https://rishikeshpansare.wordpress.com/wp-content/uploads/2016/02/digital-evidence-and-computer-crime-third-edition.pdf>