



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

ACFA7004 - Research Methods and Professional Development

Student Name:

SMIT BRIJESHKUMAR PATEL

Student ID:

2506590

Programme:

MSc Cybersecurity and Digital Forensics

Research Topic:

Mobile Device Forensics on Encrypted Applications

Submission Date:

Friday, 1st May 2026

Contents

1. Introduction	2
1.1 Context and Background	2
1.2 Research Problem.....	2
1.3 Research Aim and Objectives	3
1.4 Significance of the Research	4
2. Literature Review	4
2.1 Introduction to the Literature Review	4
2.2 Theme 1: Evolution of Mobile Device Forensics	5
2.3 Theme 2: End-to-End Encryption in Mobile Messaging Applications	5
2.4 Theme 3: Forensic Tool Capabilities – Cellebrite UFED and UFED Physical Analyzer	6
2.5 Theme 4: Legal and Ethical Frameworks	6
2.6 Literature Summary and Research Positioning	6
3. Research Design and Methodology	7
3.1 Research Design	7
3.2 Research Methods	7
3.3 Research Materials	8
4. Expected Outcomes.....	9
4.1 Anticipated Results.....	9
4.2 Implications	9
4.3 Limitations	9
5. Project Timeline	9
6. References	11

1. Introduction

1.1 Context and Background

Mobile device forensics has become one of the most important areas of digital forensics over the past decade or so. At its core, it deals with how investigators acquire, preserve, examine, and present digital evidence drawn from smartphones, tablets, and similar handheld devices. The reason is simple: smartphones are everywhere. By 2024, there were over 6.8 billion active smartphone users worldwide [\[1\]](#), and for most people, their phone is where they live their digital life - call logs, messages, location histories, photos, financial records, and a whole range of communications through third-party apps are all stored there [\[2\]](#). That makes mobile devices a near-certain source of evidence in criminal, corporate, and civil investigations.

Two technological trends have come together to make this field both more important and considerably more complicated. The first is the widespread adoption of end-to-end encrypted messaging applications. Platforms like WhatsApp, Signal, Telegram, and Apple iMessage now serve well over four billion monthly active users between them [\[9\]](#). What these applications have in common is that they use cryptographic protocols most prominently the Signal Protocol which are designed so that message content is mathematically accessible only to the people actually communicating. Not the platform provider, not a government, and not a forensic investigator [\[5\]](#). The second trend is the hardening of device hardware itself. Both Apple and Google have built serious security architecture into their devices - Apple through the Secure Enclave Processor (SEP) on iOS, and Android through the Trusted Execution Environment (TEE) and these features substantially limit what any software-based extraction tool can actually get to [\[7\]\[8\]](#).

Into this environment steps Cellebrite UFED, paired with its companion analysis platform UFED Physical Analyzer. These tools represent the go-to tools for mobile forensic acquisition, used by law enforcement and investigative agencies worldwide. Cellebrite UFED covers over 36,000 device profiles and supports multiple extraction methods ranging from logical acquisition through to physical extraction and chip-off forensics [\[18\]](#). UFED Physical Analyzer sits on top of that, providing automated database decoding, application artefact parsing, timeline reconstruction, and report generation [\[3\]](#). Together

they form the toolkit most practitioners rely on but whether they can reliably get through today's encrypted applications is what this research sets out to test.

1.2 Research Problem

The core problem I am addressing in this study is the growing gap between what commercial forensic tools can technically acquire and what evidence is actually accessible when communications are protected by end-to-end encryption on modern mobile devices. Despite how widely Cellebrite UFED and UFED Physical Analyzer are used by law enforcement across the UK and internationally, there is a real shortage of current, peer-reviewed empirical evidence that systematically compares their performance across multiple E2EE platforms on both Android and iOS at the same time [9][4].

Three related challenges make this worse. First, application-layer encryption on platforms like Signal stores messages in locally encrypted SQLite databases, where the decryption keys are secured within the device's hardware security module - not somewhere a tool can easily reach [5]. WhatsApp has moved progressively from unencrypted local storage to AES-256 encrypted databases in its current versions [19][21], which has made forensic access harder. Second, application and OS updates happen constantly, and a forensic procedure that worked against one version may simply fail against the next release [9]. Third, the legal picture in the UK spanning the Investigatory Powers Act 2016, the Computer Misuse Act 1990, and UK GDPR is genuinely complex, and there are real ambiguities about how these frameworks apply to E2EE platforms where even the service provider cannot decrypt messages [6][16].

The upshot is that practitioners are often working without clear, current guidance on what their tools can and cannot do. This study tries to provide that.

1.3 Research Aim and Objectives

Research Aim: To critically evaluate the capability of Cellebrite UFED and UFED Physical Analyzer in acquiring and analysing digital evidence from end-to-end encrypted mobile messaging applications specifically WhatsApp, Signal, Telegram, and iMessage across Android (versions 14 and 15) and iOS (versions 17 and 18), and to develop practical recommendations for forensic practitioners grounded in the test results [9].

Research Objectives:

O1: To conduct a systematic review of existing literature on mobile device forensics, E2EE application architectures, and commercial forensic tool capabilities (2019–2025), mapping what is currently known and identifying the gaps this study addresses [4].

O2: To analyse the encryption architectures and local data storage mechanisms of WhatsApp, Signal, Telegram, and iMessage on Android 14/15 and iOS 17/18, identifying forensic acquisition points, encryption barriers, and potential artefact recovery opportunities [5].

O3: To conduct controlled laboratory experiments using Cellebrite UFED and UFED Physical Analyzer to assess the volume, completeness, accuracy, and integrity of data recovered from each target application under standardised acquisition conditions [18].

O4: To evaluate and compare tool performance across Android and iOS platforms using a defined evaluation rubric encompassing recovery rate, data integrity via hash verification, artefact completeness, and acquisition time [15].

O5: To examine the ethical, legal, and procedural considerations governing the forensic examination of encrypted mobile applications in the United Kingdom, with specific reference to the Investigatory Powers Act 2016, UK GDPR, and relevant case law [6].

O6: To synthesise the experimental and analytical findings into a practical framework and concrete recommendations that forensic practitioners and stakeholders can use [14].

1.4 Significance of the Research

This research matters on several fronts. For practitioners, digital forensic investigators in UK law enforcement, the National Crime Agency, and corporate forensic units need up-to-date, tested guidance on what Cellebrite UFED and UFED Physical Analyzer can and cannot do when they encounter E2EE application data [18]. Without that, there is real uncertainty and that uncertainty creates risks for both the admissibility of evidence in court and the investigation of serious crime [9].

Academically, this research provides a reproducible experimental methodology and a current empirical benchmark that fills a gap in the literature specifically, no one has done

an integrated assessment of encrypted mobile forensics in the UK context that combines all of these elements [9][4]. Rather than looking at one application or one platform in isolation, this study compares four applications across two major operating systems side by side.

Societally, the work feeds into a debate that is not going away anytime soon: the tension between individual privacy rights protected under Article 8 of the European Convention on Human Rights and the UK GDPR [16] [17] and the legitimate investigative needs of law enforcement. This research does not pretend to resolve that tension, but it does offer some evidence-grounded input to it.

2. Literature Review

2.1 Introduction to the Literature Review

This literature review surveys the existing body of scholarship on mobile device forensics [4], end-to-end encryption in consumer messaging applications [5], the capabilities and limitations of commercial forensic tools [9], and the legal and ethical frameworks that govern forensic access to encrypted data [6]. The review is structured thematically and draws primarily on peer-reviewed journal articles, conference proceedings, technical reports, and authoritative practitioner documentation published between 2019 and 2025, though certain foundational works published earlier are included where they remain the authoritative reference in their area [11]. The databases searched include IEEE Xplore, ACM Digital Library, Scopus, and Google Scholar. The aim is to identify key trends, significant contributions, methodological limitations, and the gaps this research sets out to address.

2.2 Theme 1: Evolution of Mobile Device Forensics

Mobile device forensics has changed enormously over the last two decades. The early conceptual groundwork was laid by Jansen and Ayers [11][13], whose procedural guidelines covering evidence preservation, acquisition method hierarchy, and chain-of-custody requirements remain foundational references even today. As devices evolved from basic feature phones to fully connected smartphones, the forensic surface area grew

quickly. Modern devices now simultaneously store application data, cloud-synchronised content, biometric credentials, and encrypted communications, opening up new evidential opportunities but also making investigations harder [4].

Barmpatsalou et al. [4] provide what I found to be one of the most useful contemporary surveys of the field, arguing convincingly that mobile forensics has shifted from a largely tool-driven practice to something requiring genuine technical depth specifically, a working understanding of operating system internals, application architectures, and cryptographic implementations. Grispos et al. [12] highlight the persistent difficulties created by the sheer diversity of mobile platforms and extraction methods. Hoog's [20] work on Android forensics remains a widely cited reference, though the introduction of hardware-backed keystore from Android 9 onwards [8] means several of the techniques it describes no longer work on current devices.

2.3 Theme 2: End-to-End Encryption in Mobile Messaging Applications

The Signal Protocol, developed by Open Whisper Systems and subsequently adopted by WhatsApp, Signal, and Google Messages, combines the Extended Triple Diffie-Hellman (X3DH) key agreement protocol with the Double Ratchet Algorithm to achieve both forward secrecy and future secrecy [5]. Forward secrecy means that compromise of a long-term private key does not expose previously exchanged messages; the Double Ratchet mechanism goes further by generating a fresh symmetric key for every individual message.

WhatsApp's implementation [21] layers the Signal Protocol for message encryption with AES-256 for local database encryption on Android. Signal's local storage is notably more resistant: it uses a SQLCipher-encrypted database with a key derived from the user's PIN and protected by secure hardware [5], which makes the forensic acquisition window much smaller. Telegram takes a different approach its Secret Chat feature provides E2EE, but standard cloud chats remain server-accessible [9], which is an important forensic distinction. Apple iMessage uses per-device keys protected by the Secure Enclave Processor, with additional iOS application-layer protections [23] that make things harder still for third-party forensic tools [7].

What I found particularly striking in reviewing this literature is that each of these applications has a meaningfully different encryption posture and yet most forensic studies

treat them as a single category. This research tries to fix that by looking at each platform on its own terms.

2.4 Theme 3: Forensic Tool Capabilities - Cellebrite UFED and UFED Physical Analyzer

Cellebrite UFED is the most widely deployed commercial mobile forensic acquisition solution, and UFED Physical Analyzer provides the analytical layer that practitioners rely on to decode and present extracted data [18][3]. Physical extraction, which produces a bit-for-bit image of device storage, was for many years the gold-standard acquisition method but its reliability has been progressively eroded by full-disk encryption, which has been enabled by default on Android since version 7.0 and on all iOS devices since iOS 8 [7][8].

Al-Azawi et al. [19] demonstrated that under certain configurations, WhatsApp's encryption key material could be recovered from Android devices via ADB-based extraction a meaningful result at the time, but one that has since been rendered largely ineffective by subsequent application updates. Anglano et al. [10] observed significant variation in the types of artefacts recoverable depending on which acquisition method was used, a finding that underlines the importance of acquisition method selection in any comparative study.

The gap I see in this literature is that nobody has done a systematic, ground-truth-validated comparison of Cellebrite UFED and UFED Physical Analyzer performance across all four target applications simultaneously, on current versions of both Android and iOS [9][4]. The majority of published studies focus on a single application or a single platform, or depend on methodologies that are no longer applicable to current software versions [10][19]. This research is designed to fill that gap directly.

2.5 Theme 4: Legal and Ethical Frameworks

In the United Kingdom, the Investigatory Powers Act 2016 (IPA 2016) is the primary statutory framework governing investigatory powers. Among other things, it provides powers to issue Technical Capability Notices requiring telecommunications operators to deliver communications data in an intelligible form [6]. However, the application of these provisions to E2EE platforms where the service provider genuinely does not hold the

decryption keys remains legally ambiguous in a way that has not been clearly resolved by the courts or by Parliament.

UK GDPR and the Data Protection Act 2018 impose additional constraints on the processing and retention of personal data obtained through forensic investigations [16]. The European Court of Human Rights, in *Big Brother Watch and Others v. the United Kingdom* [17], affirmed that surveillance measures must be both proportionate and subject to robust independent oversight a principle that has direct relevance to the forensic practices this study examines.

2.6 Literature Summary and Research Positioning

Four main points come out of this review. Mobile device forensics is facing an accelerating technical challenge from both hardware-level encryption and E2EE application architectures [4]. The Signal Protocol in particular is a very strong cryptographic barrier, and there are few realistic ways around it for forensic tools [5]. Cellebrite UFED and UFED Physical Analyzer are the most widely used tools among practitioners, but how well they perform against current encrypted apps is not well tested in the academic literature [9]. And the UK legal framework contains genuine ambiguities around what forensic access to E2EE communications is lawfully permissible and under what conditions [6].

This study goes after the most obvious of these gaps: no one has done a current, experimentally rigorous, cross-platform evaluation of Cellebrite UFED and UFED Physical Analyzer against all four target applications on contemporary Android and iOS devices [9][18].

3. Research Design and Methodology

3.1 Research Design

This study adopts an experimental research design within a pragmatist epistemological framework. I have chosen an experimental design because the primary research objectives genuinely require controlled, reproducible empirical testing under known conditions, with measurable outputs that can be quantitatively compared [15]. Pragmatism as an

epistemological position supports a mixed-methods design that selects methods based on their fitness for purpose rather than any ideological commitment to a single paradigm.

The overall research design follows a Design Science Research (DSR) approach: the study identifies a real problem that forensic practitioners face day-to-day, evaluates existing artefacts namely Cellebrite UFED and UFED Physical Analyzer through rigorous empirical testing, and contributes a best-practice framework as something practitioners can actually put to work [14].

3.2 Research Methods

3.2.1 Overview and Justification

A mixed-methods design is used throughout, combining quantitative experimental methodology with qualitative document and thematic analysis [15]. The quantitative component generates objective, reproducible performance data on tool efficacy [22] the qualitative component situates those findings within the legal, ethical, and practitioner landscape in a way that raw numbers alone cannot [9].

3.2.2 Research Strategy: Controlled Laboratory Experiment

The core investigative strategy is a controlled laboratory experiment. Rather than using physical smartphones, virtual device images for Android 14 and 15 and iOS 17 and 18 will be sourced from publicly available online repositories and configured as the experimental subjects. This approach removes device procurement costs, ensures a consistent and fully documented test environment, and allows the experimental setup to be precisely reproduced by future researchers. The experimental design follows established methodological precedents for Android data collection set out by Vidas et al. [22].

Known datasets of communications will be generated through each target application WhatsApp, Signal, Telegram, and iMessage creating a documented ground-truth dataset against which recovery results can be precisely validated [22]. Each device-application combination will be subjected to the full suite of acquisition methods available within Cellebrite UFED [18]. All experiments will be conducted in a Faraday-shielded, network-isolated environment to prevent any contamination of the test devices [13].

3.2.3 Evaluation Rubric and Data Analysis

Performance will be evaluated against a standardised rubric built around four metrics: Recovery Rate, defined as the percentage of known ground-truth artefacts successfully recovered [22] Data Integrity, verified through SHA-256 hash comparison [13] Artefact Completeness, meaning the proportion of message metadata correctly decoded by UFED Physical Analyzer [3] and Acquisition Time. Descriptive statistics will be used to characterise and compare tool performance across all application and platform combinations [15].

3.3 Research Materials

3.3.1 Data Sources and Collection

All primary research data will be generated by me using virtual device images under controlled laboratory conditions [22]. No real criminal data, personal communications, or third-party data of any kind will be used at any stage [16]. The ground-truth dataset will consist of a minimum of 200 text messages per application per device pair; 20 image files and 10 audio/video files per application; a minimum of 10 call or voice message records where the application supports them; and all associated metadata [22]. All acquisition images will be stored on encrypted, access-controlled storage media, with SHA-256 hash values recorded at the point of acquisition [13].

3.3.2 Software Tools

The primary forensic tools are Cellebrite UFED for hardware extraction and UFED Physical Analyzer for analysis [3][18]. Supporting tools include SQLite Browser for database inspection; Python 3.x with the pandas and hashlib libraries for hash verification and quantitative analysis; and NVivo for qualitative thematic coding.

3.3.3 Hardware Requirements

The hardware setup requires virtual device images for Android 14 and 15 and iOS 17 and 18, sourced from publicly available online repositories at no cost [8][7] a Cellebrite UFED Touch2 or UFED Premium unit, to be accessed through the University's Digital Forensics Laboratory [18] a dedicated Windows 10/11 workstation running UFED Physical Analyzer [3] encrypted external storage of at least 1TB personally funded by the lead researcher; and a Faraday cage for device isolation during acquisition [13].

3.3.4 Ethical Considerations

This research will be submitted for review and approval by the UWTSD Research Ethics Committee before any empirical work begins. The key ethical considerations are: the exclusive use of researcher-generated synthetic data throughout [22] secure storage and strictly controlled access to all acquisition images [13] responsible handling of any vulnerability knowledge that might emerge from the research [9] and the presentation of findings in a balanced and impartial manner. Given that no human participants are involved and no real personal data is processed at any point, this research presents a low ethical risk [16].

4. Expected Outcomes

4.1 Anticipated Results

Drawing on the existing literature and my own preliminary technical analysis, I anticipate several findings. First, Cellebrite UFED is likely to demonstrate higher recovery rates for WhatsApp and Telegram artefacts on Android compared to Signal and iMessage, which is consistent with what the documented storage and encryption characteristics of those applications would lead one to expect [5][7] Second, iOS virtual device images are likely to produce consistently lower recovery rates across all applications compared to Android, because Apple locks down data access more tightly [7] . It should be noted that because this research uses virtual device images rather than physical hardware, results relating to hardware-level security features such as the Secure Enclave Processor and Trusted Execution Environment may not fully represent real-world physical device behaviour. Third, UFED Physical Analyzer's automated decoding is expected to correctly parse a higher proportion of WhatsApp and Telegram artefacts than it

does Signal or iMessage records. Fourth, and perhaps most useful to practitioners, recovery rates are expected to vary between Android 14 and Android 15, and between iOS 17 and iOS 18 which shows how even minor platform updates can break forensic tool performance.

4.2 Implications

For forensic practitioners, the findings will give a current, tested account of what can and cannot be recovered from each target application something that is missing from the existing literature [9][18]. For legal professionals, the findings will inform both the drafting and the challenging of digital evidence submissions in proceedings where mobile messaging data is in question [17]. For policy makers, the research will contribute evidence relevant to the ongoing review of the Investigatory Powers Act 2016 [6], which could help inform a more proportionate regulatory response to encrypted communications [16].

4.3 Limitations

Several limitations are worth acknowledging upfront. The results will reflect specific tool and application versions at a particular point in time, and the frequency of updates to both means that findings may have a limited shelf life [9]. The use of synthetic data, whilst ethically necessary and methodologically sound, may not fully replicate the complexity of real evidential datasets encountered in practice [22]. Additionally, the use of virtual device images rather than physical smartphones means that hardware-level security features such as Apple's Secure Enclave Processor and Android's Trusted Execution Environment may not be fully replicated, which could affect the accuracy of results relating to physical extraction methods [7][8]. Access to the full capabilities of Cellebrite UFED Premium may be subject to licensing constraints depending on what the University laboratory can provide [18]. And the legal analysis is bounded by the UK jurisdiction, which limits its direct applicability to international forensic practice [6].

5. Project Timeline

The timeline below sets out the key phases, activities, milestones, and deliverables for this research project across a period of ten weeks (approximately 2.5 months). The condensed timeline reflects the focused scope of the experimental study and the availability of laboratory resources at the University of Wales Trinity Saint David.

Phase	Key Activities	Milestone/Deliverable	Weeks
Phase 1: Literature Review	Systematic database searches (IEEE Xplore, ACM, Scopus); critical review of E2EE architectures, Cellebrite tool capabilities, and UK legal frameworks; gap analysis	Annotated bibliography; literature review draft; identified research gaps.	Week 1–3
Phase 2: Lab Setup & Ethics	Source and configure virtual device images (Android 14/15, iOS 17/18) from publicly available online repositories; install WhatsApp, Signal, Telegram, iMessage; generate ground-truth dataset; obtain UWTSD ethics approval	Validated test environment; ground-truth dataset documented; ethics - approval granted.	Week 2-4
Phase 3: Data Collection	Cellebrite UFED acquisitions across all 16 device-application combinations (logical, file-system, physical modes); UFED Physical Analyzer decoding and report generation.	Complete acquisition dataset; UFED Physical Analyzer reports for all 16 combinations.	Week 4-7
Phase 4: Data Analysis	Quantitative analysis of recovery rate, SHA-256 hash integrity, artefact	Comparative performance tables;	Week 7-8

	completeness, and acquisition time; cross-platform statistical comparison.	statistical analysis report; visualisations.	
Phase 5: Legal & Ethical	Document analysis of IPA 2016, UK GDPR, ECtHR case law (Big Brother Watch v UK); thematic coding using NVivo; synthesis with experimental findings.	Legal-ethical framework analysis; integrated discussion of findings.	Week 8-9
Phase 6: Write up & Submission	Full thesis drafting; supervisor review and revisions; best-practice recommendations framework; final submission via Turnitin.	Complete thesis draft; final submission; practitioner recommendations report.	Week 9-10

Table 1: Research Project Timeline (10 Weeks)

Phase	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10
Ph1. Literature Review										
Ph.2 Lab Setup & Ethics										
Ph. 3 Data Collection										
Ph. 4 Data Analysis										
Ph.5 Legal & Ethics										
Ph.6 Write-up										

Figure 1: Gantt Chart – 10-week Project Schedule

6. References

[1] GSMA Intelligence, 'The Mobile Economy 2024,' GSMA, London, UK, Tech. Rep., 2024.

[2] Statista, 'Number of smartphone users worldwide 2014–2029,' Statista, 2024. [Online]. Available: <https://www.statista.com>

[3] Cellebrite Ltd., 'UFED Physical Analyzer: Technical Overview and User Guide,' Cellebrite Ltd., Tech. Rep., 2024.

[4] K. Barmpatsalou, T. Cruz, E. Monteiro, and P. Simoes, 'Current and future trends in mobile device forensics: A survey,' ACM Comput. Surv., vol. 51, no. 3, 2018.

[5] M. Marlinspike and T. Perrin, 'The Double Ratchet Algorithm,' Signal Foundation, Tech. Rep., 2016.

[6] UK Government, Investigatory Powers Act 2016, HMSO, London, UK, 2016.

[7] Apple Inc., 'iOS Security Guide,' Apple Inc., Tech. Rep., 2024.

[8] Google LLC, 'Android Security Bulletins,' Google LLC, 2024.

[9] N. Mee and J. Nurse, 'Understanding the challenges of mobile device forensics with encrypted applications,' Comput. Secur., vol. 111, 2021.

[10] A. Anglano, M. Canonico, and M. Guazzone, 'Forensic analysis of WhatsApp Messenger on Android smartphones,' Digit. Investig., vol. 11, no. 3, 2014.

[11] W. Jansen and R. Ayers, 'Guidelines on Cell Phone Forensics,' NIST, Spec. Publ. 800-101, 2014.

[12] G. Grispos, T. Storer, and W. B. Glisson, 'A comparison of forensic evidence recovery techniques for a windows mobile smart phone,' Digit. Investig., vol. 8, no. 1, 2011.

[13] R. Ayers, S. Brothers, and W. Jansen, 'Guidelines on Mobile Device Forensics,' NIST, Spec. Publ. 800-101 Rev. 1, 2014.

[14] A. R. Hevner, S. T. March, J. Park, and S. Ram, 'Design Science in Information Systems Research,' *MIS Quarterly*, vol. 28, no. 1, pp. 75–105, 2004.

[15] B. Carrier and E. Spafford, 'Getting physical with the digital investigation process,' *Int. J. Digit. Evid.*, vol. 2, no. 2, 2003.

[16] UK Information Commissioner's Office, 'Guide to the UK General Data Protection Regulation (UK GDPR),' ICO, 2023.

[17] European Court of Human Rights, 'Big Brother Watch and Others v. the United Kingdom,' App. Nos. 58170/13, 62322/14, 24960/15, 2021.

[18] Cellebrite Ltd., 'Cellebrite UFED: The Industry Standard for Mobile Forensics,' Product Brief, 2024.

[19] N. Al-Azawi, M. Sadiq, and S. Batten, 'Forensic acquisition of encrypted WhatsApp databases on Android devices,' in *Proc. ICITEE*, 2017, pp. 1–6.

[20] A. Hoog, *Android Forensics: Investigation, Analysis and Mobile Security for Google Android*, Elsevier, 2011.

[21] WhatsApp Inc., 'WhatsApp Encryption Overview,' Tech. White Paper, 2023.

[22] T. Vidas, C. Zhang, and N. Christin, 'Toward a general collection methodology for Android devices,' *Digit. Investig.*, vol. 8, pp. S14–S24, 2011.

[23] J. Zdziarski, *Hacking and Securing iOS Applications*, O'Reilly Media, 2012.