International Journal of Safety and Security Engineering
Vol. 15, No. 4, April, 2025, pp. 757-766

Journal homepage: http://iieta.org/journals/ijsse

Investigating PTTPoC Communication Equipment and Smart Device Apps: A Digital Forensic Approach

Kritarth Y. Jhala*, Nilay R. Mistry, Naveen Kumar Chaudhry

National Forensic Sciences University, Gandhinagar 382007, India

Corresponding Author Email: kritarth.jhala@nfsu.ac.in

https://doi.org/10.18280/ijsse.150412

Received: 27 January 2025
Revised: 11 April 2025
Accepted: 17 April 2025
Available online: 30 April 2025

Keywords:
mobile communication technology, mobile forensics, radio communication equipment, digital forensics, push-to-talk, PTTPoC, smartphone integration, digital artifacts

ABSTRACT

Today's radio communication equipment is used for more than simply analog two-way communication; newer technology includes text messaging, GPS tracking, private calls, smartphone integration, and other features. In addition, a lot of these gadgets are smartphone-integrated allowing users to connect two-way radios and smartphones via Push-To-Talk providers. The adaptability of such gadgets is increasing in the global market. However, minimal study has been conducted on the digital footprints found in modern radio communications equipment. In this study, we examine several radio communication devices and related services that digital forensic practitioners and law enforcement organizations could encounter at a crime scene or during an investigation. It focuses on the process of acquiring and analyzing digital artifacts and validating techniques through tests with sample devices and related services.

1. INTRODUCTION

Since Guglielmo Marconi's 1895 radio connection there has been a significant shift in propertied radio equipment from analog to digital. Digital radio equipment are two-way radios having features like address books, short message services, call logs, GPS, and telemetry. These days, telemetry applications include detecting and sending data from sensors in cars, smart meters, power supplies, Internet of Things wildlife, robotics, and many other areas. Push-to-talk over Cellular has revolutionized far-flung conversation by delivering swift talk across cellular towers, doing away with the need for individual radios [1]. Ever since its beginning in 1987 with Nextel's iDEN system, PoC has undergone considerable advancement, exploiting 3G and LTE innovations to craft a broadly extended worldwide radio infrastructure. PoC now empowers individuals across industries, whether coordinating emergency responses or collaborating on energy line installations, uniting dispersed teammates through pocket-sized devices connected to the mobile network [2].

Push-to-Talk Over Cellular (PoC) integrates smartphone technology and the fundamental PTT idea into one unit. To get beyond traditional PTT's limited coverage, users can use PoC to take advantage of the half-duplex communication mode for 2-way connectivity via 3G, 4G, or WiFi networks. PoC technology improves communication efficiency by leveraging cellular networks, offering a broader and more reliable reach compared to traditional radio-based systems. The global push-to-talk over cellular market, valued at 5.1 billion USD in 2023 is predicted to grow to 10.6 billion USD by 2032, at an 8.2% CAGR. Factors driving this growth include remote working adoption, emergencies, and cross-platform compatibility [3, 4].

Key benefits

- Provides real-time communication for quick response times and efficient team coordination.
- Incorporates end-to-end encryption for privacy and security in workplaces.
- Enables sharing of location and media files for precise information and visuals.

With a number of benefits this technology is also posing a threat to compromise the cause of compromising this technology owing to the vulnerabilities present in the communication ecosystem the descriptions of various vulnerabilities in PTTPoC system are:

A) Weak Authentication and Authorization

The initial layers of protection against unwanted access are authorization and authentication of the stored as well as in transit data sets. Insufficient authentication techniques including weak passwords or no multi-factor authentication (MFA) techniques expose the system to fraudsters who can pretend as authorized users. In such cases, attackers/fraudsters/hackers may gain confidential messages, personal information, or create system disruptions if sufficient authorization checks are not in place.

B) Insecure APIs

APIs enable PTTPoC systems to communicate with backend servers and internal storage repository of the devices. If these APIs are vulnerable, attackers can use this vulnerable APIs to gain unwanted access of device data and services.

C) Lack of End-to-End Encryption (E2EE)

End-to-end encryption ensures that messages are only readable by the intended receiver and prevents interception or tampering. If PTTPoC interactions are only encrypted during transmission rather than end-to-end, attackers with network access may be able to intercept the discussions.

D) Man-in-the-Middle (MITM) Attack

A Man-in-the-Middle (MITM) attack is the type of attack in which an attacker intercepts and modifies communication between two parties (sender & receiver). This may occur if communication certificates of the devices are not checked or messages are not adequately secured which allows a hacker to intercept or insert harmful content into discussions.

E) Vulnerabilities in the Underlying Network Infrastructure

PTTPoC services are dependent on cellular networks and related infrastructure. The weaknesses/loopholes in the cellular network such as SIM Swapping, SIM card cloning or vulnerabilities in mobile communication netwok could allow attackers to intercept the PTTPoC connection or reroute connections to take over the ongoing cellular sessions.

F) Denial of Service (DoS) & Distributed Denial of Service (DDoS) Attacks

DoS & DDoS attack attempts to disrupt the available PTTPoC services by flooding it with false traffic or requests. A successful DoS & DDoS attack on PTTPoC systems would prevent users from utilizing the service which impact the operations and communication of the service provider.

G) Vulnerabilities in the PTTPoC Client App

The PTTPoC communication mobile applications build for various mobile OS i.e Android, iOS, Symbian etc. can potentially have security weaknesses which expose it to intrusions. With the usage of such vulnerabilities can permit the attacker for unauthorized access to the functionality of the application installed within the mobile OS.

H) Lack of Patch Management

In order to achieve smooth channel communications and interconnectivities, PTTPoC systems are dependent on external software or libraries. The attackers might exploit known vulnerabilities if particular components from this software and libraries are not patched and updated regularly. If patch management is overlooked, the old software may vulnerable to attack the system.

When it comes to radio technology, such as software-defined radio (SDR), packet radio, digital mobile radio, HF, VHF, and UHF transceivers, law enforcement agencies have limited investigative experience. Since radio equipment had minimal forensic value in the past this did not usually pose an issue. On the other hand, modern systems use a range of digital technologies, including GPS, computing & programming, digital speech and data channels, and more. Email, chat, location monitoring, and telemetry are examples of data communication methods that are feasible and have demonstrated potential for use in vehicle communication for some time. Furthermore, telecom operators and radio equipment rental companies across the globe provide PTT services. Radio communication equipment is transitioning from analog to digital devices, with features like call logs and GPS. This shift is gaining popularity in telemetry applications and for controlling data. However, there is limited literature on digital radio communication equipment. Law enforcement faces challenges in keeping up with new technologies and digital evidence backlogs, but there is limited research on digital forensic traces in radio communication devices, both in literature and practice. Due to lack of investigation into digital radio communication equipment can lead to the neglect of valuable evidence, requiring further research to understand current knowledge levels, evidence sources, and methods [5].

This paper discusses forensic acquisition and analysis of radio communication equipment as well as radio communication based smart mobile OS applications evaluating popular tools for artefact acquisition, and proposing a workflow for investigation.

2. BACKGROUND

Push-to-Talk Over Cellular (PTToC) is a technology that allows users to connect instantly over a cellular network, eliminating the need for dialing or waiting for calls. It functions like walkie-talkies, allowing real-time voice messages and utilizing existing cellular network infrastructure for widespread coverage.

2.1 Classification of push to talk over cellular (PoC)

There are three varieties of PTToC: two for commercial products and one for open standards.

a) Carrier-based PTToC (C-PTToC)
Carrier-based PTToC: Mobile network operators like AT&T, Kodiak, Verizon, Vodafone, Airtel, Sprint etc offer services that are closely integrated with their networks [6, 7].

b) Over-the-Top PTToC (OTT-PTToC)
Over-the-Top PTToC: As shown in Figure 1, products like Talker, Zello, Voxer, Two-Way, and Slide2Talk run as mission-critical applications over a network, independent of any carrier network [6, 7]

c) Mission-Critical PTT (M-PTToC)
Mission-Critical PTT : The 3GPP initiative, based on Open Mobile Alliance's OMA-POC technology, aims to establish a mission-critical open standard for PTT over LTE [6, 7]

Carrier-based PTToC is being adopted by non-mission-critical users and public safety agencies as an alternative to LMR due to its fast, standard call types, and ability to handle saturated networks. However, integration is challenging both technically and commercially due to engineering reasons and technical incompatibility between carriers. Commercial barriers also exist, as companies may restrict the use of PTToC to a limited range of smartphones, which may not be suitable for mission-critical users who need cross-network PTT with better service than standard commercial networks [6-8].

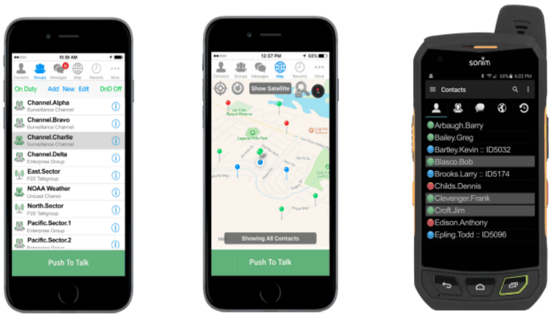


Figure 1. Examples of Push-to-Talk (PTT) applications and devices (iOS, Android)

As shown in Figure 2, Ott PTToC is a carrier-agnostic application that allows for flexible use across networks with various devices and broadband access technologies. However, it locks users into a proprietary ecosystem, limiting interoperability between vendors. OTT apps also lack Direct Mode communications, making them incompatible with carrier-based systems. Bridging or console patching may work, but the proprietary nature of OTT applications remains a significant issue [6-8].

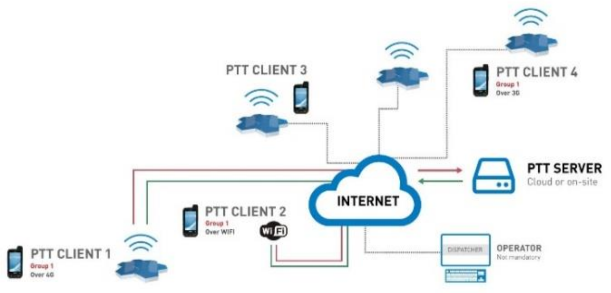


Figure 2. Push-to-Talk (PTT) system architecture: clients connect with a PTT server (cloud or on-site) over 3G, 4G, or WiFi networks with an optional dispatcher

3GPP has developed MCPTT, an open standard PTT over LTE specification that meets mission-critical requirements identified by the National Public Safety Telecommunications Council (NPSTC). Both carrier-based and OTT PTToC vendors have announced plans to modify or upgrade their offerings to the MCPTT standard. Deployments of MCPTT to public safety have begun, but the issue of whether PTToC is mission-critical remains unresolved. Most devices available for MCPTT are standard consumer products, and the reliability and availability of communication will still not meet public safety expectations. Interoperability between LTE networks and legacy LMR systems is also a point of ongoing discussion. Direct Mode for LTE remains a challenge [6-8].

Walkie-talkie solutions use mobile terminals with talk buttons and networks for push to talk calls. Push to Talk over Cellular (PoC) is a real-time voice-over-IP service that uses a GSM, GPRS or LTE networks for direct voice communication. Users must define settings like access point, PTT, SIP, XDM, and presence. PTT is used for testing IP multimedia Service services due to its delay tolerance and is designed for interoperability between different operators on cellular mobile networks. PTT uses SIP for signaling and control sessions, while RTP/RTCP is used for voice traffic transmission. Clients send packets to the server, distributing them to other session members [9].

a) Push to Talk over Cellular (PoC) Client

This entity is a User Equipment functional entity that registers on the IMS network, initiates, modifies, terminates PTT sessions, generates, sends, receives, processes talk bursts, and supports Talk Burst Control Protocol procedures.

b) Push to Talk over Cellular (PoC) Server

The PTT service, which supports call control functions, handles SIP sessions and talk bursts, providing a comprehensive solution for AS.

2.2 Accessories for radio communication equipment

Digital radio communication equipment and software are manufactured by many brands like Vertex, Kenwood, LHR, Motorola, etc. These manufacturers also provide portable and mobile two-way radios, repeaters, and accessories such as headsets and remote speaker mics. Micro-SD cards are also compatible with these devices.

2.3 Software defined radio (SDR)

The most recent SDR version may serve as both a server and a console, whereas the earlier models needed radio components in a hardware box. FlexRadio1 offers hardware and software for communication with SDR, while RTL-SDR2 is a cheap device for receiving and decoding radio signals. Digital Speech Decoder (DSD)3 decodes digital speech formats using the mbelib library, but does not decode encrypted communications.

2.4 Push to talk over cellular (PoC) applications

PTT (Phone-to-Telephone) has been utilized by cellular providers for years, providing real-time communication and filling unused airspace. Nokia phones with Symbian s40 and s60 systems support PTT functions, even without a specific button, using the free Nokia Team Suite application for PTT entry and call-to-call [9].

Smartphones have led to the development of various PTTPoC applications such as Motorola's WAVE, Cisco Instant Connect, Zello, Voxer, iTeamTalk, Side2Talk, Two-Way etc. In order to provide a private and secure environment, several PTT applications can also interact via WiFi and/or Bluetooth. Fantom Dynamics' DXBm 5 is a modular solution that allows users to convert their smartphones and tablets into their own off-grid peer-to-peer network. Additional modules that come with encryption include DMR, P25, MDC-1200, UHF, Dual band, 800 MHz, and RoIP modules.

3. METHODOLOGY

Radio communication equipment, such as HF transceivers, linked devices, and computer programs, can include important digital forensic traces. Radio repeaters are primarily receivers that transmit the received payload on another frequency. Portable and mobile two-way radios can contain configuration data, call logs, and message logs, which can be analyzed using the customer program software (CPS) application. Accessories like remote speakers/microphones or Bluetooth devices can also contain valuable digital traces. An involvement in a crime scene may be revealed by remote PTT buttons that pair with a smartphone or two-way radio via Bluetooth.

Mobile device and application forensics are a mature research area, but challenges persist due to rapid advancements and the wide range of mobile devices. Data acquisition from mobile devices remains a key operational and research challenge, especially when data-at-rest and data-in-transit encryption solutions are not supported by existing commercial tools [10].

3.1 Forensic investigation acquisition & analysis process

The Lowrance LHR 80I is a portable radio VHF/GPS with both analogue and digital radio capabilities. It was tested using the Customer Programming Software (CPS) version V7.06.02.006 on a clean virtual Windows machine. This cutting-edge software is intended to improve the communication experience by allowing easy programming and customization on Motorola devices. The radio's antenna was removed to prevent remote disabling and the transceiver was active on channel RPTR-1_TG9.2 in zone RePeaTeR-1. The code plug file, Lowrance LHR 80I.rcdx, was read-only and saved. It was possible to retrieve the radio's unique components, including its make and model, serial number, frequency range that has been used, radio alias, and Radio ID. The analysis report revealed the anonymous Radio-ID and Radio-Alias [10, 11].

In Figure 3, the procedure for acquiring and extracting processes pertaining to the radiomodules is illustrated. The diagram encompasses the entire forensic process lifecycle beginning from acquisition to the subsequent analysis. beginning from acquisition to the subsequent analysis.

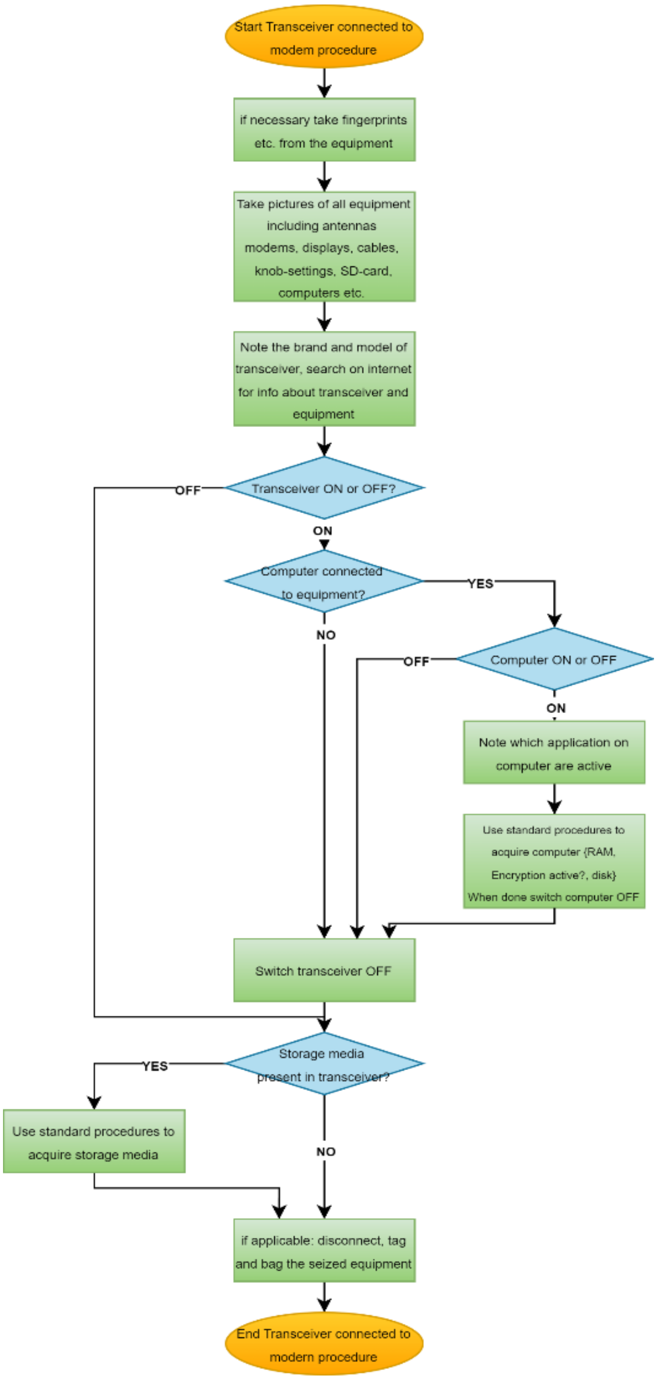

Start Transceiver connected to modem procedure
if necessary take fingerprints etc. from the equipment
Take pictures of all equipment including antennas modems, displays, cables, knob-settings, SD-card, computers etc.
Note the brand and model of transceiver, search on internet for info about transceiver and equipment
Transceiver ON or OFF?
OFF
ON
Computer connected to equipment?
YES
NO
Computer ON or OFF
OFF
ON
Note which application on computer are active
Use standard procedures to acquire computer {RAM, Encryption active?, disk}
When done switch computer OFF
Switch transceiver OFF
Storage media present in transceiver?
YES
NO
Use standard procedures to acquire storage media
if applicable: disconnect, tag and bag the seized equipment
End Transceiver connected to modem procedure

Figure 3. Flowchart data acquisition of Radio Modules

3.2 Smartphone push-to-talk application

Data acquisition involves cloning and copying digital data from mobile devices. Traditional methods, such as manual extraction, logical acquisition, physical acquisition, and chip-off, are considered insufficient due to the security revolution in mobile devices. Logical acquisition is a method that extracts bit-by-bit copies of logical storage objects from their allocated space but it cannot access slack spaces. It works best on unrooted & jail broken mobile phones. Physical acquisition involves creating bit-by-bit copies of physical storage. Professional forensic examiners can use hardware-based data acquisition methods like JTAG and CHIP-Off, which can result in damaged chips [11]. Software-based acquisition doesn't cause physical harm to the device, but requires file system privilege to access the data sets.

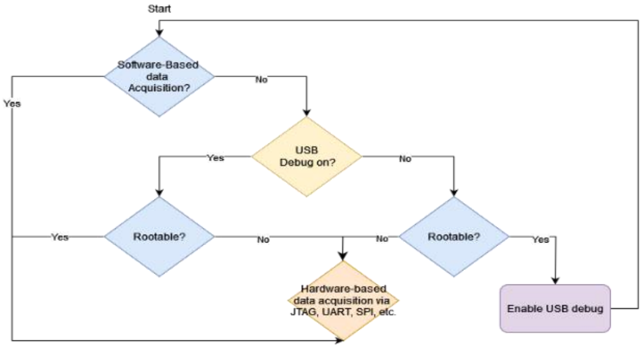

Start
Software-Based data Acquisition?
No
Yes
USB Debug on?
Yes
No
Rootable?
Yes
No
No
Rootable?
Yes
Hardware-based data acquisition via JTAG, UART, SPI, etc.
Enable USB debug

Figure 4. Flowchart for 3rd party data acquisition in mobile forensics

3.3 Other possible traces

Investigating radio communication devices may require additional sources beyond the scope of this paper. Provider agencies may keep records of frequency users, real-time radio signals, and dispatch equipment, which may include call logs, text messages, GPS data, or recorded voice as shown in Figure 4. These additional sources can provide valuable insights into potential users and their activities. Recorded voice and data from mobile radio networks can be valuable for investigation, but may have a short retention time. Many countries use a one-week retention time, while service provider system has log files on the Central Message Servers (CMS). PTT applications like zello, voxer etc can also provide valuable logs. Digital radio devices use Radio-IDs for communication, and Ham-radio amateurs connect their repeaters to Ham DMR networks. These networks offer useful information and last-heard connections.

3.4 Analysis process

A forensic investigator examines a forensic image by searching for the app's folder name, which must be identical to its package name. If the folder exists, the investigator can examine the files in the app's folder, which typically includes sub-folders like shared_prefs, cache, files, databases, and lib. However, folders do not necessarily store a single type of evidence. Automated forensic knowledge-sharing platforms like Cellebrite UFED, Oxygen Forensic Suite, Magnet Axiom and MSAB XRY can help extract forensic artifacts from mobile devices. File formats in these folders are a better indication of potential evidence, such as XML files, web cache data, SQLite files, and standalone media files. Integrating these steps and processes is not straightforward, resulting in multiple re-iterations of the discovery process [11]. Figure 5 presents a flowchart depicting the steps involved in third-party data acquisition for mobile forensic investigations.

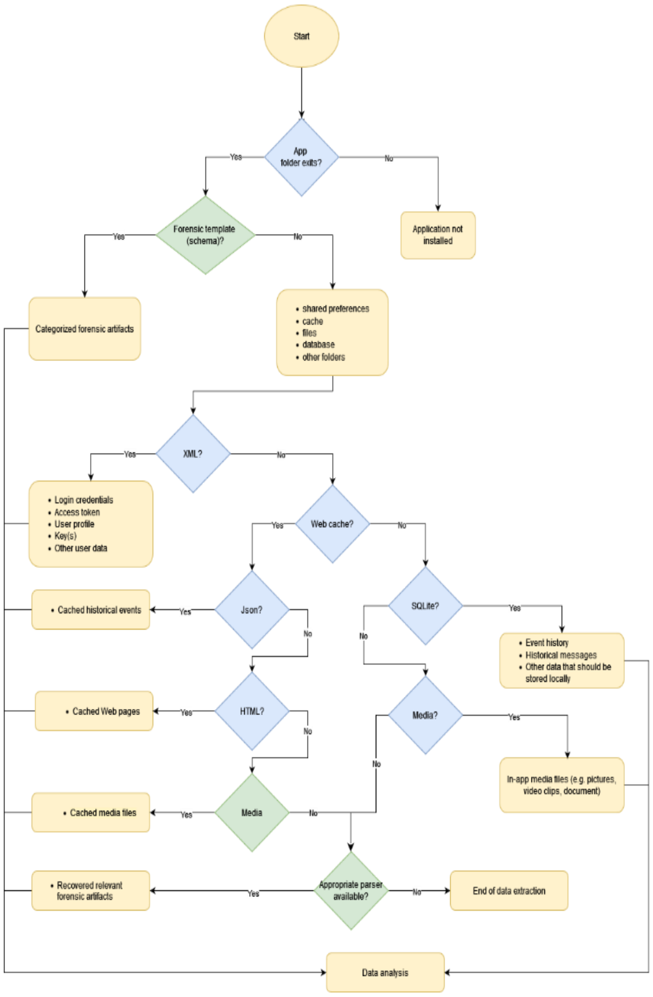


Figure 5. Flowchart for 3rd party data acquisition in mobile forensics

4. EXPERIMENTAL SETUP

Popular mobile-focused digital forensic tools include Cellebrite's UFED4PC & Physical Analyzer, Oxygen Forensic Suite, MSAB's XRY, and Data Pilot. However, they do not support two-way radio devices. CPS can read two-way radios using vendor-specific cables i.e. HKKLN4027A Cable and recent two-way radios have a micro-USB connection. CPS software installed in a clean virtual machine can provide configuration settings. In cases where mobile devices are not supported by forensic software or data loss is possible, manual extraction using photography-based device investigation software like the Cellebrite UFED camera is recommended. This will generate a digital or paper-based report with corresponding hash values, documenting the investigative process [12].

For the collecting and analysis of PTTPOC-related artifacts, two scenarios were investigated to get the needed data sets. In the first scenario, the Hytera PD785G Portable radio set is designed to detect and verify probable artifacts caused by the radio sets. Another use case is divided into two categories: the first is related to the PTTPoC applications in smart devices that are configured on an Android and iOS platforms, and the second is related to Symbian, as the S40 and S60 variants of Symbian OS include PTT applications by default. The research will focus on the digital traces that these applications left behind through the setup of test beds.

4.1 Use case 1: The hytera PD785G portable radio set

The Lowrance LHR 80I is a portable radio with both analog and digital radio capabilities using the DMR protocol, which is used to detect PTT-related forensic artifacts on devices. a freshly configured virtual Windows workstation running Customer Programming Software (CPS) version V7.06.02.006. RMS Express, an email application by Winlink, was investigated using a workflow to identify a radio transceiver connected to a modem. The transceiver was a dual-band VHF or UHF transceiver receiving on 144.850 MHz. Tigertronics Signalink-USB Soundlink modem, Diamond X-30 in-house antenna, and Kenwood TH-F7E portable transceiver were among the equipment relied on. A Signalink soundmodem and a Windows 11 based system running RMS Express were linked by a HKKLN4027A USB cable. The PC displayed two programs and the FTK imager was utilized to generate a forensic image of the data that the device could access [13].

4.2 Use case 2: Push-to-talk application for android application (take 5 applications tests with both and do comparison analysis)

A) Devices Used

- iPhone 15 Pro with iOS version 17.5.1
- OnePlus Nord with Android 13
- Samsung Galaxy J7 Prime with Android 11
- Samsung SM-A715F/DS with Android 12
- Iphone XS-A2097 with iOS version 18.0

B) Tools Used

- Cellebrite UFED for extraction
- Cellebrite Physical Analyzer for analysis
- Oxygen Forensic Suite
- MSAB XRY
- Magnet Axiom

C) Data Extraction Procedure

- Filesystem Extraction: Conducted using Cellebrite UFED4PC, Magnet Axiom, Oxygen Forensic Suite, MSAB XRY to minimize data loss.

D) Application Details

- Zello:
    - Package Name: com.loudtalk
- Voxer:
    - Package Name: com.rebelvox.voxer
- Slide2Talk:
    - Package Name: com.slide2talk.android.app
- Talker
    - Package Name: network.talker.app

E) Analysis Tools

- Cellebrite Physical Analyzer: Used to locate and analyze data within the mobile directory.
- Oxygen Forensic Suite: Used for supplemental analysis to verify findings.
- MSAB XRY: Used to locate and analyze data within the mobile directory.

- Magnet Axiom: Used for supplemental analysis to verify findings.

F) Findings

- Zello: Multimedia files (photos, audio, GIFs) were consistently accessible in plain view across all devices.

I). iPhone 15 Pro (iOS 17.5.1) (see Table 1)

Table 1. Application comparison analysis on iOS 17.5.1

Application	Data Type	Data Location	Visibility	Description and Notes
Zello	Multimedia (Photos, Audio, GIFs)	/var/mobile/Applications/Zello	Visible	Multimedia files were found in their respective directories.
Voxer	Text Messages	/var/mobile/Applications/Voxer	Plain Text	Text messages were stored in plain text format.
Slide2talk	Voice Messages	/var/mobile/Applications/Slide2talk	Encrypted	Voice messages were encrypted and require decryption.
talker	Group Chats	/var/mobile/Applications/talker	Visible	Group chat data was visible in the application directory.

II). OnePlus Nord (Android 13) (see Table 2)

Table 2. Application comparision analysis on Android 13

Application	Data Type	Data Location	Visibility	Description and Notes
Zello	Multimedia (Photos, Audio, GIFs)	/data/data/com.loudtalks	Visible	Multimedia files were found in their respective directories.
Voxer	Text Messages	/data/misc/profiles/ref/com.rebelvox.voxer	Plain Text	Text messages were stored in plain text format.
Slide2talk	Voice Messages	/Root/data/com.slide2talk.android.app	Encrypted	Voice messages were encrypted and require decryption.
talker	Group Chats	/Root/data/network.talker.app	Visible	Group chat data was visible in the application directory.

III). Samsung Galaxy J7 Prime (Android 11) (see Table 3)

Table 3. Application comparision analysis on Android 11

Application	Data Type	Data Location	Visibility	Description and Notes
Zello	Multimedia (Photos, Audio, GIFs)	/data/data/com.loudtalks	Visible	Multimedia files were found in their respective directories.
Voxer	Text Messages	/data/misc/profiles/ref/com.rebelvox.voxer	Plain Text	Text messages were stored in plain text format.
Slide2talk	Voice Messages	/Root/data/com.slide2talk.android.app	Encrypted	Voice messages were encrypted and require decryption.
Talker	Group Chats	/Root/data/network.talker.app	Visible	Group chat data was visible in the application directory.

IV). Samsung SM-A715F/DS (Android 12) (see Table 4)

Table 4. Application comparision analysis on Android 12

Application	Data Type	Data Location	Visibility	Description and Notes
Zello	Multimedia (Photos, Audio, GIFs)	/data/data/com.loudtalks	Visible	Multimedia files were found in their respective directories.
Voxer	Text Messages	/data/misc/profiles/ref/com.rebelvox.voxer	Plain Text	Text messages were stored in plain text format.
Slide2talk	Voice Messages	/Root/data/com.slide2talk.android.app	Encrypted	Voice messages were encrypted and require decryption.
talker	Group Chats	/Root/data/network.talker.app	Visible	Group chat data was visible in the application directory.

V). Iphone XS-A2097 (iOS 18.0) (see Table 5)

Table 5. Application comparision analysis on iOS 18.0

Application	Data Type	Data Location	Visibility	Description and Notes

Zello	Multimedia (Photos, Audio, GIFs)	/var/mobile/Applications/Zello	Visible	Multimedia files were found in their respective directories.
Voxer	Text Messages	/var/mobile/Applications/Voxer	Plain Text	Text messages were stored in plain text format.
Slide2talk	Voice Messages	/var/mobile/Applications/Slide2talk	Encrypted	Voice messages were encrypted and require decryption.
talker	Group Chats	/var/mobile/Applications/talker	Visible	Group chat data was visible in the application directory.

- Voxer: Text messages were consistently stored in plain text format across all devices [14].
- Slide2talk: Voice messages were encrypted on all devices, requiring decryption to access their contents. Decrypting encrypted voice messages audio files from Slide2Talk involves having access to the decryption key which can be stored on the device or communicated over a secure channel. Forensic tools will try to recover these keys but this will depend on the encryption algorithm and the presence of the key. In the absence of the decryption key forensic analysis will be restricted to metadata or plaintext content [15].
- Talker: Group chat data was visible without encryption in the application directories on all devices.This table summarizes the types of data extracted from each application on all tested devices. It shows the consistency and variability in data accessibility across different platforms and applications during the forensic analysis [16].

4.3 Nokia PTT services

Push-to-Talk (PTT) features by default are available on Nokia Symbian handsets enabling users to converse via voice calls instantly, much like with a typical walkie-talkie. Databases on these devices hold frequencies associated with PTT services provided by service providers. Figure 6 describes the step-by-step procedure to extract this default PTT datasets from the Symbian device [17, 18].

Analysts must generate a backup file from Symbian cellphones in order to access these datasets. Once the backup is in NBF format, it is converted to ZIP format. This method allows analysts to thoroughly study and extract data from each folder within the backup files which allows complete access and investigation of recorded PTT-related frequencies and associated data sets [19-21].

Figure 7 indicates that while converting a.nbf file into a.zip file, a list of numerous databases can be extracted. One of which is frequency-db.db as shown in Figure 8, which is responsible for the data saved pertaining to PTT conversation.

Opening the frequency-db.db sqlite database file with the required software such as SQLite DB viewer or SQLite manager, allows us to extract detailed frequency-based information about the PTT service in plain text. This extracted sqlite database file contains a structured collection of frequencies used in PTT talks, modulation types, and channel allocations which helps analysts understand Symbian smartphone communication patterns and aids in forensic investigations [22-24].

Based on the experiment performed for the data extraction and analysis of various mobile devices and mobile operating systems the in-depth observations using various forensic tools and techniques are as shown in Table 6:

- Y – 'Yes' indicates that the data was retrieved.
- N – 'No' signifies that no data was recovered during this process.
- N(Enc.) – 'N(Enc.)' indicates that the data was retrieved but in encrypted format.
- A – 'A' indicates the results of Image & Video files extracted from the PTTPoC applications.
- B – 'B' indicates the results of Audio files extracted from the PTTPoC applications.
- C – 'C' indicates the results of Contact Details extracted from the PTTPoC applications.
- D – 'D' indicates the results of Communication Frequencies extracted from the PTTPoC applications.
- E – 'E' indicates the results of Call Log History extracted from the PTTPoC applications.

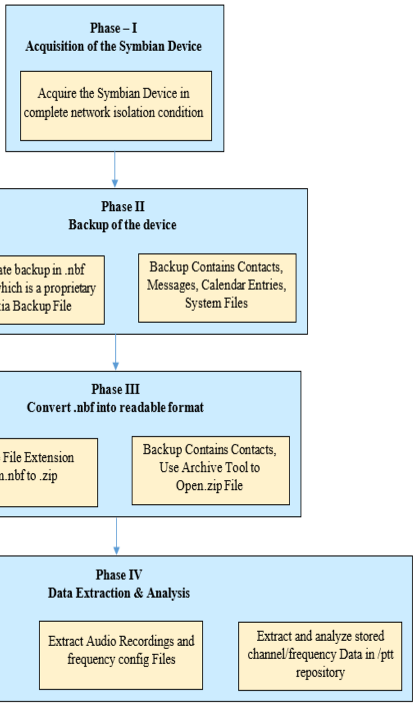
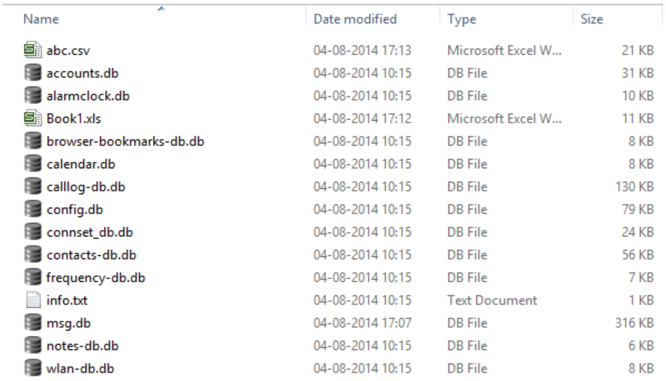

Phase – I
Acquisition of the Symbian Device
Acquire the Symbian Device in complete network isolation condition
Phase II
Backup of the device
Generate backup in .nbf format which is a proprietary Nokia Backup File
Backup Contains Contacts, Messages, Calendar Entries, System Files
Phase III
Convert .nbf into readable format
Change File Extension from.nbf to .zip
Backup Contains Contacts, Use Archive Tool to Open.zip File
Phase IV
Data Extraction & Analysis
Extract Contents with emphasis on PTT Data
Extract Audio Recordings and frequency config Files
Extract and analyze stored channel/frequency Data in /ptt repository

Figure 6. Step-by-step approach for extracting the default PTT database from Symbian based devices



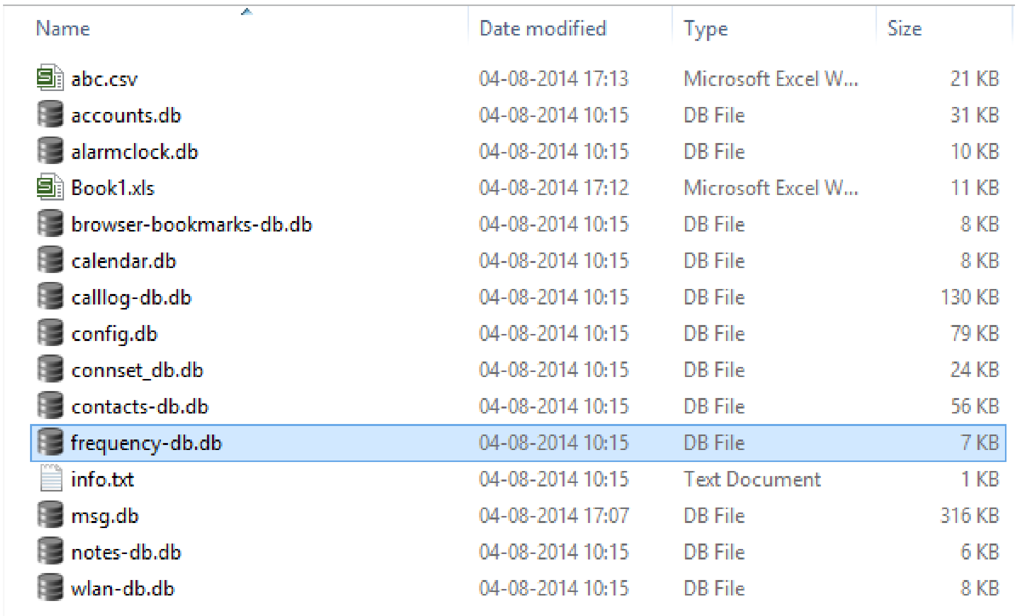
Name	Date modified	Type	Size
abc.csv	04-08-2014 17:13	Microsoft Excel W...	21 KB
accounts.db	04-08-2014 10:15	DB File	31 KB
alarmclock.db	04-08-2014 10:15	DB File	10 KB
Book1.xls	04-08-2014 17:12	Microsoft Excel W...	11 KB
browser-bookmarks-db.db	04-08-2014 10:15	DB File	8 KB
calendar.db	04-08-2014 10:15	DB File	8 KB
calllog-db.db	04-08-2014 10:15	DB File	130 KB
config.db	04-08-2014 10:15	DB File	79 KB
connset_db.db	04-08-2014 10:15	DB File	24 KB
contacts-db.db	04-08-2014 10:15	DB File	56 KB
frequency-db.db	04-08-2014 10:15	DB File	7 KB
info.txt	04-08-2014 10:15	Text Document	1 KB
msg.db	04-08-2014 17:07	DB File	316 KB
notes-db.db	04-08-2014 10:15	DB File	6 KB
wlan-db.db	04-08-2014 10:15	DB File	8 KB

Figure 7. DB file extraction from Symbian devices

Table 6. Comparative analysis of different forensic techniques and technologies based on the extracted data sets

Device	Application	Forensic Tool	A	B	C	D	E
iPhone 15 Pro (iOS 17.5.1)	Zello	Cellebrite UFED4PC	Y	Y	Y	Y	N
		Magnet AXIOM	Y	Y	Y	Y	N
		Oxygen Forensic Suite	Y	Y	Y	Y	N
		MSAB XRY	Y	Y	Y	Y	N
	Voxer	Cellebrite UFED4PC	N	N	Y	Y	N
		Magnet AXIOM	N	N	Y	Y	N
		Oxygen Forensic Suite	N	N	Y	Y	N
		MSAB XRY	N	N	Y	Y	N
	Side2 Talk	Cellebrite UFED4PC	N	N (Enc)	Y	N	N
		Magnet AXIOM	N	N (Enc)	Y	N	N
		Oxygen Forensic Suite	N	N (Enc)	Y	N	N
		MSAB XRY	N	N (Enc)	Y	N	N
	Talker	Cellebrite UFED4PC	N	Y	Y	Y	N
		Magnet AXIOM	N	Y	Y	Y	N
		Oxygen Forensic Suite	N	Y	Y	Y	N
		MSAB XRY	N	Y	Y	Y	N
OnePlus Nord (Android 13)	Zello	Cellebrite UFED4PC	Y	Y	Y	Y	N
		Magnet AXIOM	Y	Y	Y	Y	N
		Oxygen Forensic Suite	Y	Y	Y	Y	N
		MSAB XRY	Y	Y	Y	Y	N
	Voxer	Cellebrite UFED4PC	N	N	Y	Y	N
		Magnet AXIOM	N	N	Y	Y	N
		Oxygen Forensic Suite	N	N	Y	Y	N
		MSAB XRY	N	N	Y	Y	N
	Side2 Talk	Cellebrite UFED4PC	N	N (Enc)	Y	N	N
		Magnet AXIOM	N	N (Enc)	Y	N	N
		Oxygen Forensic Suite	N	N (Enc)	Y	N	N
		MSAB XRY	N	N (Enc)	Y	N	N
	Talker	Cellebrite UFED4PC	N	Y	Y	Y	N
		Magnet AXIOM	N	Y	Y	Y	N
		Oxygen Forensic Suite	N	Y	Y	Y	N
		MSAB XRY	N	Y	Y	Y	N
Samsung Galaxy J7 (Android 11)	Zello	Cellebrite UFED4PC	Y	Y	Y	Y	N
		Magnet AXIOM	Y	Y	Y	Y	N
		Oxygen Forensic Suite	Y	Y	Y	Y	N
		MSAB XRY	Y	Y	Y	Y	N
	Voxer	Cellebrite UFED4PC	N	N	Y	Y	N
		Magnet AXIOM	N	N	Y	Y	N
		Oxygen Forensic Suite	N	N	Y	Y	N
		MSAB XRY	N	N	Y	Y	N
	Side2 Talk	Cellebrite UFED4PC	N	N (Enc)	Y	N	N
		Magnet AXIOM	N	N (Enc)	Y	N	N
		Oxygen Forensic Suite	N	N (Enc)	Y	N	N
		MSAB XRY	N	N (Enc)	Y	N	N
	Talker	Cellebrite UFED4PC	N	Y	Y	Y	N
		Magnet AXIOM	N	Y	Y	Y	N
		Oxygen Forensic Suite	N	Y	Y	Y	N
		MSAB XRY	N	Y	Y	Y	N
Samsung SM-A715F/DS (Android 12)	Zello	Cellebrite UFED4PC	Y	Y	Y	Y	N
		Magnet AXIOM	Y	Y	Y	Y	N
		Oxygen Forensic Suite	Y	Y	Y	Y	N
		MSAB XRY	Y	Y	Y	Y	N
	Voxer	Cellebrite UFED4PC	N	N	Y	Y	N
		Magnet AXIOM	N	N	Y	Y	N
		Oxygen Forensic Suite	N	N	Y	Y	N
		MSAB XRY	N	N	Y	Y	N
	Side2 Talk	Cellebrite UFED4PC	N	N (Enc)	Y	N	N
		Magnet AXIOM	N	N (Enc)	Y	N	N
		Oxygen Forensic Suite	N	N (Enc)	Y	N	N
		MSAB XRY	N	N (Enc)	Y	N	N
	Talker	Cellebrite UFED4PC	N	Y	Y	Y	N
		Magnet AXIOM	N	Y	Y	Y	N

Device	Application	Forensic Tool	A	B	C	D	E
		Oxygen Forensic Suite	N	Y	Y	Y	N
		MSAB XRY	N	Y	Y	Y	N
Iphone XS-A2097 (iOS 18.0)	Zello	Cellebrite UFED4PC	Y	Y	Y	Y	N
		Magnet AXIOM	Y	Y	Y	Y	N
		Oxygen Forensic Suite	Y	Y	Y	Y	N
		MSAB XRY	Y	Y	Y	Y	N
	Voxer	Cellebrite UFED4PC	N	N	Y	Y	N
		Magnet AXIOM	N	N	Y	Y	N
		Oxygen Forensic Suite	N	N	Y	Y	N
		MSAB XRY	N	N	Y	Y	N
	Side2 Talk	Cellebrite UFED4PC	N	N (Enc)	Y	N	N
		Magnet AXIOM	N	N (Enc)	Y	N	N
		Oxygen Forensic Suite	N	N (Enc)	Y	N	N
		MSAB XRY	N	N (Enc)	Y	N	N
	Talker	Cellebrite UFED4PC	N	Y	Y	Y	N
		Magnet AXIOM	N	Y	Y	Y	N
		Oxygen Forensic Suite	N	Y	Y	Y	N
		MSAB XRY	N	Y	Y	Y	N
Symbian Device	Push to Talk Service	Manual Extraction Technique	Y	Y	Y	Y	Y



Name	Date modified	Type	Size
abc.csv	04-08-2014 17:13	Microsoft Excel W...	21 KB
accounts.db	04-08-2014 10:15	DB File	31 KB
alarmclock.db	04-08-2014 10:15	DB File	10 KB
Book1.xls	04-08-2014 17:12	Microsoft Excel W...	11 KB
browser-bookmarks-db.db	04-08-2014 10:15	DB File	8 KB
calendar.db	04-08-2014 10:15	DB File	8 KB
calllog-db.db	04-08-2014 10:15	DB File	130 KB
config.db	04-08-2014 10:15	DB File	79 KB
connset_db.db	04-08-2014 10:15	DB File	24 KB
contacts-db.db	04-08-2014 10:15	DB File	56 KB
frequency-db.db	04-08-2014 10:15	DB File	7 KB
info.txt	04-08-2014 10:15	Text Document	1 KB
msg.db	04-08-2014 17:07	DB File	316 KB
notes-db.db	04-08-2014 10:15	DB File	6 KB
wlan-db.db	04-08-2014 10:15	DB File	8 KB

Figure 8. PTT Artefact frequncy.db file from Symbian devices

5. CONCLUSIONS

The current research in cyber forensic for the digital traces in radio communication equipment and services emphasizes the significance of understanding digital radio technology, standards, products, and user behaviour. However, there is a significant knowledge gap when it comes to extracting data from digital two-way radios using standard mobile forensic tools such as Cellebrite UFED, MSAB XRY, Oxygen Forensic Suite and Magnet Axiom as mentioned in this paper. Despite these constraints procedural flowcharts have been created to assist in the manual gathering of data from transceivers and other radio components resulting in successful data extraction from radio communication equipment. These procedures necessitate manual intervention and have scope for improvement in efficiency and automation. Radio communication devices and their infrastructure, including digital trails, settings, frequencies, and connections, are potential sources of forensic evidence that digital investigators need to search for. Advanced data access methods like APIs, JTAG, and chip-offs are necessary for modern digital radios because of their IP capabilities and proprietary restrictions.

Furthermore, in the era of smart devices, many Push-to-Talk over Cellular (PTTPoC) applications are widely used. This research paper discusses the forensic analysis of these applications, demonstrating that ample information can be extracted through traditional mobile forensics approaches using available commercial and open-source toolsets. Consequently, law enforcement digital experts must adapt to the evolving landscape of digital communication tools and continue to refine and expand their forensic techniques to effectively gather evidence from both digital two-way radios and modern PTTPoC applications.

ACKNOWLEDGMENT

The authors would like to express their gratitude to the Centre of Excellence in Digital Forensics at National Forensic Sciences University India for providing the technical conditions and machines utilized to create and test the solution.

REFERENCES

[1] Anderson, A., Wang, X., Baker, K.R., Grunwald, D. (2015). Systems for spectrum forensics. In Proceedings of the 2nd International Workshop on Hot Topics in Wireless, pp. 26-30. https://doi.org/10.1145/2799650.2799657

[2] Baldini, G., Karanasios, S., Allen, D., Vergari, F. (2013). Survey of wireless communication technologies for public safety. IEEE Communications Surveys & Tutorials, 16(2): 619-641. https://doi.org/10.1109/SURV.2013.082713.00034

[3] IMARC Group. (2023). Push-to-talk over cellular (PoC) market: Global industry trends, share, size, growth, opportunity and forecast 2023-2028. https://www.imarcgroup.com/push-to-talk-over-cellular-market https://www.imarcgroup.com/push-to-talk-over-cellular-market.

[4] Custom Market Insights. (2023). Global Remote Workplace Services Market Size, Share 2032. https://www.custommarketinsights.com/report/remote-workplace-services-market/.

[5] Hitchcock, B., Le-Khac, N.A., Scanlon, M. (2016). Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. Digital Investigation, 16: S75-S85. https://doi.org/10.1016/j.diin.2016.01.010

[6] Forester, E. (2019). Is commercial PTToC mission critical? Tait Radio Academy. Tait Radio Academy | Free Educational Content About Critical Communications. https://www.taitradioacademy.com/topic/is-commercial-pttoc-mission-critical/.

[7] Armoogum, S., Khonje, P., Li, X. (2021). Digital forensics of cyber physical systems and the Internet of Things. In Crime Science and Digital Forensics, CRC Press, pp. 117-148. https://doi.org/10.1201/9780429322877-9

[8] Chen, W.P., Licking, S., Ohno, T., Okuyama, S., Hamada, T. (2007). Performance measurement, evaluation and analysis of Push-to-Talk in 3G networks. In 2007 IEEE International Conference on Communications, Glasgow, UK, pp. 1893-1898. https://doi.org/10.1109/ICC.2007.315

[9] Estes, T. (2021). The push-to-talk ecosystem: Cellular, Wi-Fi, and unified platforms. Security Magazine. https://www.securitymagazine.com/articles/94433-the-push-to-talk-ecosystem-cellular-wi-fi-and-unified-platforms, accessed on Jan. 27, 2021.

[10] de Braekt, R.I., Le-Khac, N.A., Farina, J., Scanlon, M., Kechadi, T. (2016). Increasing digital investigator availability through efficient workflow management and automation. In 2016 4th International Symposium on Digital Forensic and Security (ISDFS), Little Rock, AR, USA, pp. 68-73. https://doi.org/10.1109/ISDFS.2016.7473520

[11] Kouwen, A., Scanlon, M., Choo, K.K.R., Le-Khac, N.A. (2018). Digital forensic investigation of two-way radio communication equipment and services. Digital Investigation, 26: S77-S86. https://doi.org/10.1016/j.diin.2018.04.007

[12] Lillis, D., Becker, B., O'Sullivan, T., Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. arXiv Preprint, arXiv: 1604.03850. https://doi.org/10.48550/arXiv.1604.03850

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

[14] Al-Dhaqm, A., Abd Razak, S., Ikuesan, R.A., Kebande, V.R., Siddique, K. (2020). A review of mobile forensic investigation process models. IEEE Access, 8: 173359-173375. https://doi.org/10.1109/ACCESS.2020.3014615

[15] Cuomo, R., D'Agostino, D., Ianulardo, M. (2022). Mobile forensics: Repeatable and Non-Repeatable technical assessments. Sensors, 22(18): 7096. https://doi.org/10.3390/s22187096

[16] Grover, J. (2013). Android forensics: Automated data collection and reporting from a mobile device. Digital Investigation, 10: S12-S20. https://doi.org/10.1016/j.diin.2013.06.002

[17] Murias, J.G., Levick, D., McKeown, S. (2023). A forensic analysis of streaming platforms on Android OS. Forensic Science International: Digital Investigation, 44: 301485. https://doi.org/10.1016/j.fsidi.2022.301485

[18] Horsman, G. (2018). A forensic examination of the technical and legal challenges surrounding the investigation of child abuse on live streaming platforms: A case study on Periscope. Journal of Information Security and Applications, 42: 107-117. https://doi.org/10.1016/j.jisa.2018.07.009

[19] Immanuel, F., Martini, B., Choo, K.K.R. (2015). Android cache taxonomy and forensic process. In 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, pp. 1094-1101. https://doi.org/10.1109/Trustcom.2015.488

[20] Apple Inc. (2011). iPhone and iOS forensics. In Elsevier eBooks. Elsevier. https://doi.org/10.1016/c2010-0-68895-x

[21] Wu, M., Chang, T., Li, M.Y. (2021). Digital forensics security analysis on IOS devices. Journal of Web Engineering. https://doi.org/10.13052/jwe1540-9589.20310.

[22] Zhang, X., Liu, C.Z., Choo, K.K.R., Alvarado, J.A. (2021). A design science approach to developing an integrated mobile app forensic framework. Computers & Security, 105: 102226. https://doi.org/10.1016/j.cose.2021.102226

[23] Yasar, K. (2024). Proof of concept (PoC) exploit. SearchSecurity. https://www.techtarget.com/searchsecurity/definition/proof-of-concept-PoC-exploit.

[24] Carstens, R. (2024). What is push to talk over cellular (PoC)? Radiocoms. https://www.radiocoms.co.uk/push-to-talk-over-cellular/.