HSPI Inc. The Open Access Publisher

J F S R JOURNAL OF FORENSIC SCIENCE AND RESEARCH
ISSN 2575-0186

Research Article

Comparative analysis of mobile forensic proprietary tools: an application in forensic investigation

Parth Chauhan[1]*, Tamanna Jaitly[2] and Animesh Kumar Agrawal[1]

[1]School of Digital Forensic Sciences, NICFS, NFSU (Delhi Campus), Ministry of Home Affairs, Govt. of India

[2]School of Forensic Sciences, NICFS, NFSU (Delhi campus), Ministry of Home Affairs, Govt. of India

More Information

***Address for Correspondence:** Parth Chauhan, School of Digital Forensic Sciences, NICFS, NFSU (Delhi Campus), Ministry of Home Affairs, Govt. of India
Email: jaipur.parth99@gmail.com

Submitted: November 15, 2022
Approved: November 21, 2022
Published: November 22, 2022

How to cite this article: Chauhan P, Jaitly T, Agrawal AK. Comparative analysis of mobile forensic proprietary tools: an application in forensic investigation. J Forensic Sci Res. 2022; 6: 077-082.

DOI: 10.29328/journal.jfsr.1001039

Keywords: Security breach; Mobile forensic; Acquisition; Cumulative evidence; Corroborative evidence and Data extraction

Abstract

The utilization of the Internet and wireless communication reaches its pinnacle from one side of the planet to the other. Marking the rise of criminal activity in recent years sees enormous growth in security breaches and data theft-related cases in mobile phones. To mitigate them, the implementation of security patches, safety fixes, and updates in mobile devices is of high priority for the organization. The need to foster techniques and procedures in the field to be able to extract and precisely dissect digital crime cases, providing valuable tactical data about the investigation. Mobile forensics is a developing branch assisting the investigator in criminal trials and investigations. Acquisition, Collection, and Analysis of mobile phones settle the purpose of recovering cumulative and corroborative evidence. Upgradation and innovation of mobile devices with time imposed a challenge to mobile forensic technology to extract information from such devices. The study aims at extracting comparative and statistical approaches in the analysis of Physical data acquisition utilizing significant versatile mobile criminological proprietary tools. The proposed study also introduces newly developed utility tools along with their characteristic features which help in successful data extraction from mobile devices.

Introduction

Considering the upward trajectory in urbanization results in a remarkable increase in world population crossing 7.91 billion with augmentation of cyberspace to approximately 4.95 billion as per Digital 2022 Global Overview Report. As the number of users increases day by day, the amount of data generated from mobile devices is at high-security risk. Internet activity focus contributes over 5.31 billion and estimates 67.1% of the total population employs smartphones till Jan 2022. Demographical data manifests 4.62 billion of the total population as dynamic web-based media clients which gauges 58.4% till Jan 2022 [1]. Moderation techniques and strides to these unavoidable dangers paves a way for steady data assurance. Certain Smartphone Industries are looking to mitigate these risks by implementing security patches and updates regularly

the Indian smartphone market is pacing upward and reaches 150 Million in 2020 and will increase to 11% with 167 - 168 Million in 2020 with a high prediction of 187 - 190 million market pace in 2022 [1]. This produces a challenge to the forensic investigator to extract useful data from the suspected user's mobile devices for criminal investigation and trial purposes. Another challenge [2] in mobile forensics is the Boot loop during data extraction which is the device freezing on the startup screen and does not start further, mostly when using a noncompatible mobile forensic tool or the operating system for extraction and acquisition [3]. The scientific process of acquisition, extraction, analysis, and presentation of mobile devices and related evidence in a forensically sound condition is known as Mobile forensics. Mainly [2] mobile forensic tools work on Logical, Physical, and File system acquisition. The application of these acquisition methods mainly depends on the operating system of Mobile devices and the functionality of the tools. The [2] investigator must have an idea about the make & model along with the operating system and its security patch level before choosing any tool for smooth evidence collection for the mobile device. Much research conducted on techniques of data extraction from different mobile devices using open-source and proprietary mobile forensic tools which are now conclusively implemented in forensic labs for extraction purposes. Rusydi Umar, et al. [3] conducted forensic analysis on the WhatsApp application database having

.crypt12 encryption using Belkasoft Evidence (Trial version) and WhatsApp Key/DB Extractor in which Whatsapp key/DB Extractor gave better results in extracting text messages while Belkasoft Evidence gave much better results in extracting the media & documents.

Oluwafemi Osho, et al. [4] conducted an evaluation of mobile forensic tools including AccessData FTK, EnCase, MOBILedit Forensic Express and Oxygen Forensic Suite on two mobile devices named HTC Desire 300 with android v4.1.2 and Samsung Galaxy GT-S5300 android v2.3.5 focusing on the recovery of deleted data. They concluded that FTK and EnCase are better in recovery than MOBILedit and Oxygen Forensic Suite. Not only WhatsApp applications, but a previous study [5] was also conducted on forensic analysis of fitness applications in mobile devices using Android Studio and DB browser by manual acquisition. The manual acquisition technique [2] is least considerable due to the fact that the artifact can tamper with while handling the mobile evidence directly. In place of Manual acquisition being considered first [2]. Logical and Physical acquisition is preferable by many forensic laboratories all over the world [6]. The reference study conducted forensic data extraction of five social networking apps using MAGNET AXIOM and MSAB-XRY in three conditions mainly before data deletion, some data deletion from the app, and after uninstallation of the app. The study used logical data acquisition techniques for investigation.

This paper discusses the [7] physical acquisition of an isolated sample mobile device using proprietary tools and the comparative analysis of the recovered artifacts. The study focuses on the practical performance of proprietary tools [8] by testing the artifacts recovery method and its overall features from the acquisition till report generation.

Methodology

The experiment was partitioned into stages: experimental setup of sample mobile device; acquisition of sample mobile device using three forensic proprietary tools for artifacts gathering and recovery and comparative result generation from the analysis of artifacts recovered from all three forensic tools. As per the current extraction types, generally, extraction is of three types Physical, Logical, and File system. On the other hand, cloud-based extractions can be performed on a separate basis as the data backup resides on cloud storage which has to be exported using token generation and session IDs Image 1.

The sample mobile device was procured (Table 1) and tested in front of laymen with his consent. Note that the SIM was not part of the experimental setup with the intention to narrow down the study. The physical dump is collected by the acquisition of internal and cloud storage only taking into account that SIM would not give much information as compared to the information stored in the social media database, internal storage media, and cloud.

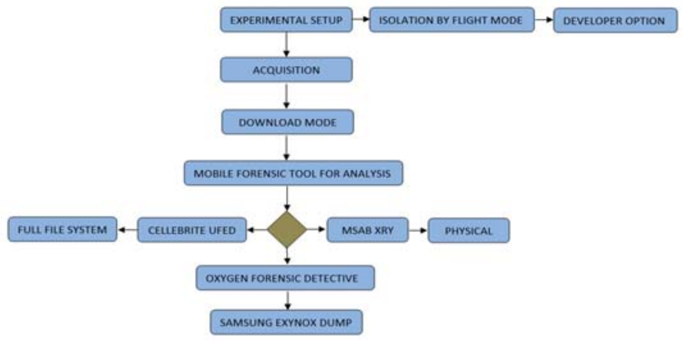


Image 1: Flow chart explains experimental sections and tools with their physical acquisition techniques.

Table 1: Equipment identification before the examination.

Device name	Model	Android vesion	security patch level
Samsung Galaxy M31	SM-M315F/DS	11	December 1st, 2021

Logical extraction may not require physically connecting the mobile device in order to extract the data. Such extraction works on the principle of injection of the third-party application which collects the on-device data. The injection of such third-party applications can either be by connecting the device with OTG or using wireless bandwidth. While in the case of iOS Technology, the older version can be partial jailbreak using the vulnerability engagement in the device.

The system and software information is rechecked online for custom ROM installation [9] by providing an IMEI number at https://www.imei.info/. The compatibility of the Sample mobile device is checked before the acquisition using the [10,11] in-built support of manuals of all three mobile forensic tools [2,12]. The mobile used for testing purposes is checked with the latest android version and security patch level to correctly examine the analytical performance of Forensic tools which helps forensic experts for further analysis in forensic laboratories.

Step one is to isolate the mobile device by enabling Flight mode or Airplane mode [13]. Along with this, enable the developer option and check the stay awake option to prevent the screen from locking [13].

The mobile forensic proprietary tools used for the experimental study are shown in Table 2.

Staging towards the acquisition part after completing the experimental setup of the sample device, the mobile device is now connected to the particular tool at a time for the data collection using physical acquisition [2,14]. To complete the step of acquisition, a mobile device is necessary to put in download mode (Image 2).

Table 2: Mobile forensic tools with their version used in an experimental study.

	Tool Used	Version
1	MSAB-XRY	10.0.0
2	Cellebrite UFED4PC	7.50.0.137
3	Oxygen Forensic Detective	13.6.0.47

https://doi.org/10.29328/journal.jfsr.1001039

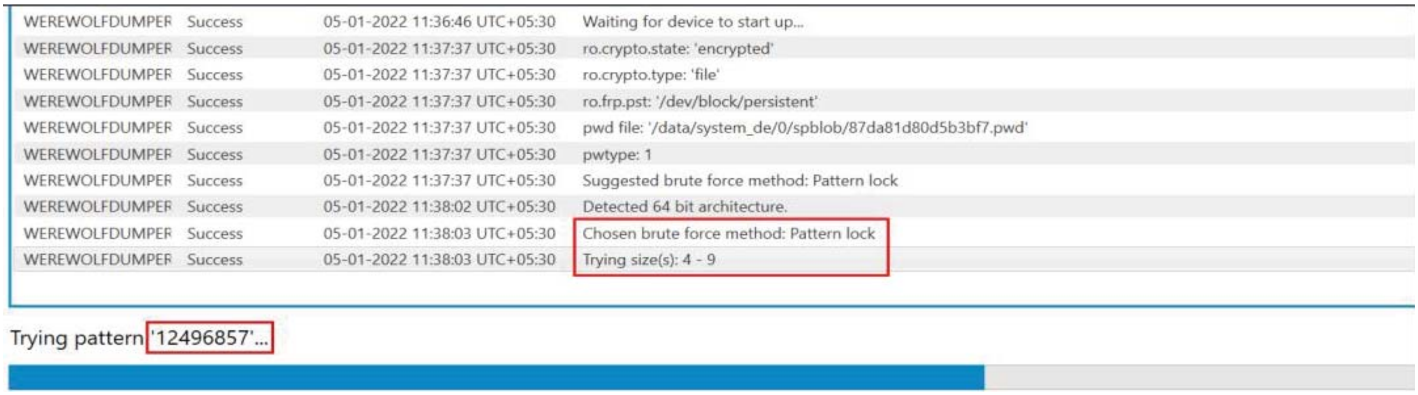
Image 2: Download mode enabled in Sample mobile device.

The mobile phone is made pattern locked with 8 keys in pattern as *"729513486"* So to check whether these tools were able to bypass or crack the pattern lock and the type of technique they adopt [13] Image 3.

A special booting mode specifically made by Samsung for certified repair technicians to get the root access privilege and debug the system easily for easy maintenance, software, and firmware updates along with recovery of data [13,15,16] Images 4-6.

Results and discussion

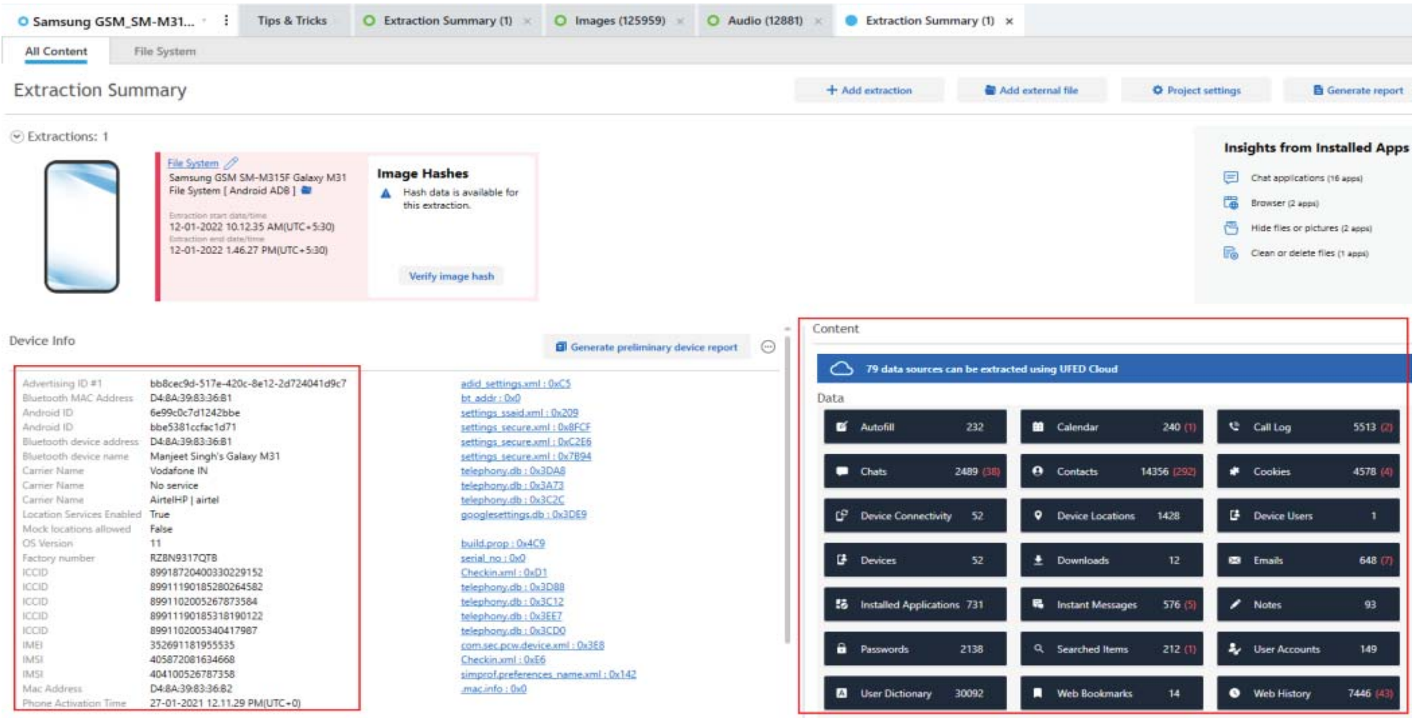
The objective of this study is fulfilled by examining the working performance of mobile forensic proprietary tools using Physical acquisition [17-20] with a major focus on the recovery of deleted artifacts. The artifacts collected from the examination using different tools are shown in Tables 3,4.



```
WEREWOLFDUMPER  Success  05-01-2022 11:36:46 UTC+05:30  Waiting for device to start up...
WEREWOLFDUMPER  Success  05-01-2022 11:37:37 UTC+05:30  ro.crypto.state: 'encrypted'
WEREWOLFDUMPER  Success  05-01-2022 11:37:37 UTC+05:30  ro.crypto.type: 'file'
WEREWOLFDUMPER  Success  05-01-2022 11:37:37 UTC+05:30  ro.frp.pst: '/dev/block/persistent'
WEREWOLFDUMPER  Success  05-01-2022 11:37:37 UTC+05:30  pwd file: '/data/system_de/0/spblob/87da81d80d5b3bf7.pwd'
WEREWOLFDUMPER  Success  05-01-2022 11:37:37 UTC+05:30  pwtype: 1
WEREWOLFDUMPER  Success  05-01-2022 11:37:37 UTC+05:30  Suggested brute force method: Pattern lock
WEREWOLFDUMPER  Success  05-01-2022 11:38:02 UTC+05:30  Detected 64 bit architecture.
WEREWOLFDUMPER  Success  05-01-2022 11:38:03 UTC+05:30  Chosen brute force method: Pattern lock
WEREWOLFDUMPER  Success  05-01-2022 11:38:03 UTC+05:30  Trying size(s): 4 - 9

Trying pattern '12496857'...
```

Image 3: Brute Forcing of pattern lock in Samsung M31 using MSAB-XRY.



Extraction Summary

Extractions: 1

File System
Samsung GSM SM-M315F Galaxy M31
File System [Android ADB]
Extraction start date/time
12-01-2022 10.12.35 AM(UTC+5:30)
Extraction end date/time
12-01-2022 1.46.27 PM(UTC+5:30)

Image Hashes
Hash data is available for this extraction.

Insights from Installed Apps
Chat applications (16 apps)
Browser (2 apps)
Hide files or pictures (2 apps)
Clean or delete files (1 apps)

Device Info

Advertising ID #1	bb8cec9d-517e-420c-8e12-2d724041d9c7	adid_settings.xml : 0xC5
Bluetooth MAC Address	D4:8A:39:83:36:B1	bt_addr : 0x0
Android ID	6e99c0c7d1242bbe	settings_ssaid.xml : 0x209
Android ID	bbe5381ccfac1d71	settings_secure.xml : 0x8FCF
Bluetooth device address	D4:8A:39:83:36:B1	settings_secure.xml : 0xC2E6
Bluetooth device name	Manjeet Singh's Galaxy M31	settings_secure.xml : 0x7B94
Carrier Name	Vodafone IN	telephony.db : 0x3DA8
Carrier Name	No service	telephony.db : 0x3A73
Carrier Name	AirtelHP | airtel	telephony.db : 0x3C2C
Location Services Enabled	True	googlesettings.db : 0x3DE9
Mock locations allowed	False	
OS Version	11	build.prop : 0x4C9
Factory number	RZ8N9317QTB	serial_no : 0x0
ICCID	89918720400330229152	Checkin.xml : 0xD1
ICCID	89911190185280264582	telephony.db : 0x3D88
ICCID	8991102005267873584	telephony.db : 0x3C12
ICCID	89911190185318190122	telephony.db : 0x3EE7
ICCID	8991102005340417987	telephony.db : 0x3CD0
IMEI	352691181955535	com.sec.pcw.device.xml : 0x3E8
IMSI	405872081634668	Checkin.xml : 0xE6
IMSI	404100526787358	simprof.preferences_name.xml : 0x142
Mac Address	D4:8A:39:83:36:B2	.mac.info : 0x0
Phone Activation Time	27-01-2021 12.11.29 PM(UTC+0)	

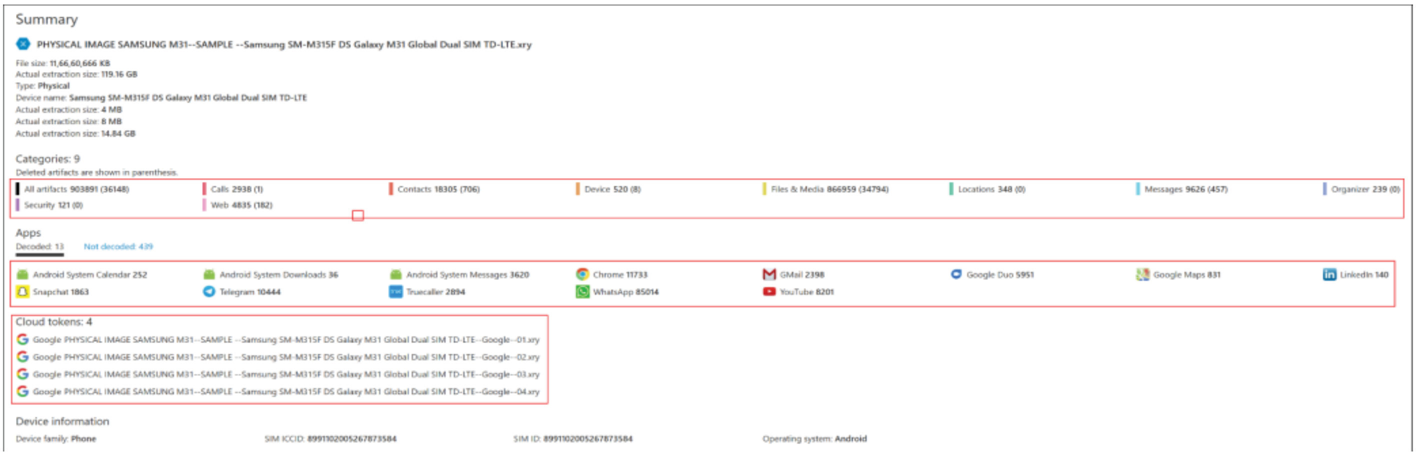
Content

79 data sources can be extracted using UFED Cloud

Data

Autofill 232	Calendar 240 (1)	Call Log 5513 (2)
Chats 2489 (38)	Contacts 14356 (292)	Cookies 4578 (4)
Device Connectivity 52	Device Locations 1428	Device Users 1
Devices 52	Downloads 12	Emails 648 (7)
Installed Applications 731	Instant Messages 576 (5)	Notes 93
Passwords 2138	Searched Items 212 (1)	User Accounts 149
User Dictionary 30092	Web Bookmarks 14	Web History 7446 (43)

Image 4: Cellebrite UFED interface after extraction.



Summary

PHYSICAL IMAGE SAMSUNG M31--SAMPLE --Samsung SM-M315F DS Galaxy M31 Global Dual SIM TD-LTE.xry

File size: 11,66,60,666 KB
Actual extraction size: 119.16 GB
Type: Physical
Device name: Samsung SM-M315F DS Galaxy M31 Global Dual SIM TD-LTE
Actual extraction size: 4 MB
Actual extraction size: 8 MB
Actual extraction size: 14.84 GB

Categories: 9
Deleted artifacts are shown in parenthesis.

All artifacts 903891 (36148)	Calls 2938 (1)	Contacts 18305 (706)	Device 520 (8)	Files & Media 866959 (34794)	Locations 348 (0)	Messages 9626 (457)	Organizer 239 (0)
Security 121 (0)	Web 4835 (182)						

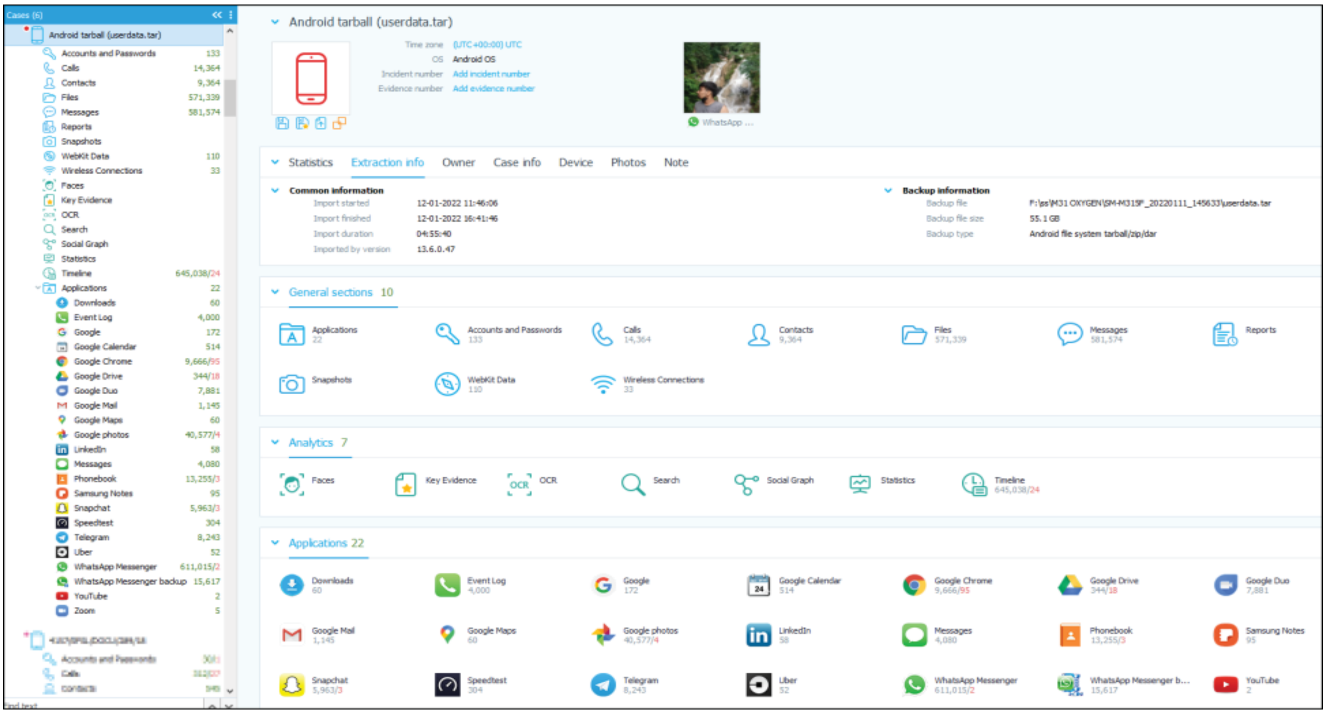
Apps
Decoded: 13   Not decoded: 439

Android System Calendar 252	Android System Downloads 36	Android System Messages 3620	Chrome 11733	GMail 2398	Google Duo 5951	Google Maps 831	LinkedIn 140
Snapchat 1863	Telegram 10444	Truecaller 2894	WhatsApp 85014	YouTube 8201			

Cloud tokens: 4
Google PHYSICAL IMAGE SAMSUNG M31--SAMPLE --Samsung SM-M315F DS Galaxy M31 Global Dual SIM TD-LTE--Google--01.xry
Google PHYSICAL IMAGE SAMSUNG M31--SAMPLE --Samsung SM-M315F DS Galaxy M31 Global Dual SIM TD-LTE--Google--02.xry
Google PHYSICAL IMAGE SAMSUNG M31--SAMPLE --Samsung SM-M315F DS Galaxy M31 Global Dual SIM TD-LTE--Google--03.xry
Google PHYSICAL IMAGE SAMSUNG M31--SAMPLE --Samsung SM-M315F DS Galaxy M31 Global Dual SIM TD-LTE--Google--04.xry

Device information
Device family: Phone   SIM ICCID: 8991102005267873584   SIM ID: 8991102005267873584   Operating system: Android

Image 5: MSAB XRY interface after extraction.



Cases (6)

Android tarball (userdata.tar)

Accounts and Passwords	133
Calls	14,364
Contacts	9,364
Files	571,339
Messages	581,574
Reports	
Snapshots	
WebKit Data	110
Wireless Connections	33
Faces	
Key Evidence	
OCR	
Search	
Social Graph	
Statistics	
Timeline	645,038/24
Applications	22
Downloads	60
Event Log	4,000
Google	172
Google Calendar	514
Google Chrome	9,666/95
Google Drive	344/18
Google Duo	7,881
Google Mail	1,145
Google Maps	60
Google photos	40,577/4
LinkedIn	58
Messages	4,080
Phonebook	13,255/3
Samsung Notes	95
Snapchat	5,963/3
Speedtest	304
Telegram	8,243
Uber	52
WhatsApp Messenger	611,015/2
WhatsApp Messenger backup	15,617
YouTube	2
Zoom	5

Find text

Android tarball (userdata.tar)

Time zone (UTC +00:00) UTC
OS Android OS
Incident number Add incident number
Evidence number Add evidence number

WhatsApp ...

Statistics | Extraction info | Owner | Case info | Device | Photos | Note

Common information
Import started 12-01-2022 11:46:06
Import finished 12-01-2022 16:41:46
Import duration 04:55:40
Imported by version 13.6.0.47

Backup information
Backup file F:\ss\M31 OXYGEN\SM-M315F_20220111_145633\userdata.tar
Backup file size 55.1 GB
Backup type Android file system tarball/zip/dar

General sections 10

Applications 22	Accounts and Passwords 133	Calls 14,364	Contacts 9,364	Files 571,339	Messages 581,574	Reports
Snapshots	WebKit Data 110	Wireless Connections 33				

Analytics 7

Faces	Key Evidence	OCR	Search	Social Graph	Statistics	Timeline 645,038/24

Applications 22

Downloads 60	Event Log 4,000	Google 172	Google Calendar 514	Google Chrome 9,666/95	Google Drive 344/18	Google Duo 7,881
Google Mail 1,145	Google Maps 60	Google photos 40,577/4	LinkedIn 58	Messages 4,080	Phonebook 13,255/3	Samsung Notes 95
Snapchat 5,963/3	Speedtest 304	Telegram 8,243	Uber 52	WhatsApp Messenger 611,015/2	WhatsApp Messenger b... 15,617	YouTube 2

Image 6: Oxygen Forensic Detective interface after extraction.

Table 3: Total artifacts retrieved from Samsung Galaxy M31 SM-M315F/DS.

Category	Tools used		
	Cellebrite UFED	MSAB-XRY	Oxygen Forensic Detective
Total artifacts	553455	940039	1176939

Table 4: Categorization of artifacts retrieved from Samsung Galaxy M31 SM-M315F/DS.

Data category	Tools used		
	cellebrite UFED	MSAB XRY	Oxygen Forensic Detective
call logs	5513(2)	2938(1)	14364
contacts	14356(292)	18305(706)	9364
device	731(0)	520(8)	Not Categorized
files&media	407551(12682)	866959(34794)	571339
locations	1428(0)	348(0)	Not Categorized
messages	3713(50)	9626(457)	581574
calender	240(1)	239(0)	514
user accounts	149	116	133
web data	7460(43)	4835(182)	2080

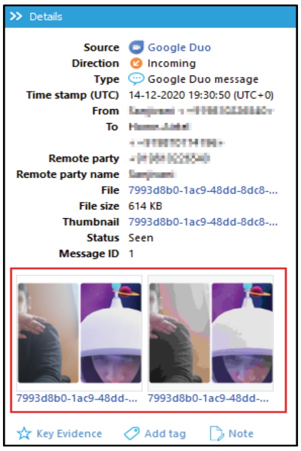
Note: Deleted Artificats are shows in parenthesis.

For dead devices, chipset-based extraction is performed in order to get the physical dump of data. Along with this method, the device was turned into suitable mode by pressing certain keys which make the tool perform the exploit. However, the chances of getting more amount of deleted data are higher in the case of extraction of the rooted device as compared to the non-rooted one. In order to get the deleted data by physical extraction, the device was made into flashed and made into partial root mode which is called download mode or Emergency Download mode (EDL).

The study highlighted the data extraction using Download mode [13,15,16] which is specifically built for technical support and maintenance in Samsung smartphones. Other factors were also considered for the proper analysis of tools as shown in Table 5.

Table 5: Comparison of tools.

Factors	Tools used		
	Cellebrite UFED	MSAB-XRY	Oxygen Forensic Detective
Interface usability	✓	✓	✓
Device compatibility	✓	✓	✓
Log Report generation	×	✓	×
Hashing of report	✓	✓	✓



Source Google Duo
Direction Incoming
Type Google Duo message
Time stamp (UTC) 14-12-2020 19:30:50 (UTC+0)
From [redacted]
To [redacted]
Remote party [redacted]
Remote party name [redacted]
File 7993d8b0-1ac9-48dd-8dc8-...
File size 614 KB
Thumbnail 7993d8b0-1ac9-48dd-8dc8-...
Status Seen
Message ID 1

7993d8b0-1ac9-48dd-... 7993d8b0-1ac9-48dd-...

Image 7: On-call snapshot retrieved by Oxygen Forensic Detective.

One of the reasons for considering MSAB XRY over other mobile forensic tools mentioned above is the generation of log reports to examine the errors while performing acquisition. On the other hand [11]. Oxygen forensic detective summarizes artifacts in a much better way than the above tools by filtering the data according to the type of file and application separately [10]. UFED and XRY are more efficient in data and meta-carving as compared to Oxygen Forensic Detective.

Analyzing social media artifacts, Oxygen Forensic Detective finds a vast range of artifacts especially for Whatsapp and Google Duo by extracting the on-call snapshots as compared to other tools as shown in Image 6. The above study was found to be helpful for forensic investigators in mitigating the challenge of unlocking Samsung smartphones, efficient analysis & report generation [8] Image 7.

Conclusion

Above mentioned tools, Cellebrite UFED, MSAB XRY and Oxygen Forensic Detective were found to give the best results in different domains of artifact retrieval. The functionality of these proprietary tools is much better in all aspects as compared with open-source tools. In the advancement of Mobile Forensics, the tools need to be updated with the latest Mobile device modules and technology to recover deleted artifacts. Extracting the artifacts from the latest android and security patch level will always be a challenge to forensic experts. The extraction of social messaging application data is a challenging task in view of the probability of finding critical evidence is more as compared to other artifacts. Capturing the token and in order to live capturing of cloud-based application data is another challenging task for law enforcement agencies as well as proprietary tool manufacturers. The research in the developing field of forensic science cannot be compromised by the upgradation of smartphones.

References

1. Simon K, Pte K. Ltd. https://datareportal.com/reports/digital-2022-global-overview-report

2. Lahesoo P, Mäses S. Forensic Traces of Messaging Applications on Android and iOS Mobile phones.

3. Umar R, Riadi I, Zamroni GM. Mobile forensic tools evaluation for digital crime investigation. Int J Adv Sci Eng Inf Technol. 2018; 8(3): 949.

4. Osho O, Ohida SO. Comparative evaluation of mobile forensic tools. IJ Inf. Technol. Comput. Sci. 2016; 1:74-83.

5. Sinha R, Sihag V, Choudhary G, Vardhan M, Singh P. Forensic Analysis of Fitness Applications on Android. In the International Symposium on Mobile Internet Security 2021; 222:235.

6. Aljahdali A, Alsaidi N, Alsafri M, Alsulami A, Almutairi, T. Mobile device forensics. Romanian Journal of Information Technology and Automatic Control. 2021; 31(3): 81-96.

7. Eriş FG, Akbal E. Forensic Analysis of Popular Social Media Applications on Android Smartphones. Balkan Journal of Electrical and Computer Engineering. 2021; 9(4):386-397.

8. Dasgupta RK. Mobile forensic: Investigation of dead or damaged smartphone-An overview, tools and technique challenges from law enforcement perspective. Research gate Journal. 2021. https://www.researchgate.net/profile/Rhythm-Dasgupta/publication/340939977_Mobile_Forensic_Investigation_of_Dead_or_Damage_Smart_Phone_-An_Overview_Tools_Technique_Challenges_from_Law_Enforcement_Perspective/links/5ea68b62299bf11256128683/Mobile-Forensic-Investigation-of-Dead-or-Damage-Smart-Phone-An-Overview-Tools-Technique-Challenges-from-Law-Enforcement-Perspective.pdf

9. Agrawal AK, Sharma A, Sinha SR, Khatri P. Forensic of an unrooted mobile device. International Journal of Electronic Security and Digital Forensics. 2020; 12(1):118-137.

10. Release notes (September 2019). UFED 4PC, UFED Touch 2, and UFED InField v7.23 https://cf-media.cellebrite.com/wp-content/uploads/2019/09/ReleaseNotes_7.23.pdf

11. Press Release (December 2021). Oxygen Forensics Closes the year with Major upgrades in extraction capabilities, VPN support, Data analysis, and more. https://www.oxygen-forensic.com/uploads/press_kit/OFDv142ReleaseNotes.pdf

12. Hazra S, Mateti P. Challenges in android forensics. In International Symposium on Security in Computing and Communication. 2017; 286-299. Springer, Singapore.

13. Joshua J, Zach Lanier D, Mulliner C, Fora O, Ridley SA, Android's GW. Hacker Handbook, John Wiley& Sons; https://books.google.co.in/books?id=2qo6AwAAQBAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false 2014.

14. Gaikar V. Article by Tricks Machine on How to root samsung galaxy S3. 2012. https://www.tricksmachine.com/2012/07/how-to-root-samsung-galaxy-s3.html

15. Kong J. Data extraction on mtk-based android mobile phone forensics. Journal of Digital Forensics, Security and Law2015; 10(4): 3.

16. Alendal G, Dyrkolbotn GO, Axelsson S. Forensics acquisition—Analysis and circumvention of samsung secure boot enforced common criteria mode. Digital Investigation. 2018; 24: S60-S67.

17. Tajuddin TB, Abd Manaf A. Forensic investigation and analysis on digital evidence discovery through physical acquisition on the

https://doi.org/10.29328/journal.jfsr.1001039

smartphone. In 2015 World Congress on Internet Security (WorldCIS). IEEE. 132-138.

18. Sathe SC, Dongre NM. Data acquisition techniques in mobile forensics. In 2018 2nd international conference on inventive systems and control (icisc). IEEE. 2018; 280-286.

19. Ayers R. Smart Phone Tool Specification, computer forensic tool testing. 2010. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=905497,www.cftt.nist.gov

20. Osho O, Ohida SO. Comparative evaluation of mobile forensic tools. IJ Inf. Technol. Comput. Sci, 2016; 1:74-83.

https://doi.org/10.29328/journal.jfsr.1001039