OPCODE 2019 comae tech-nologies

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

WhatsApp Digger Forensics Tool

Prepared by:
Deemah A Alotaibi, Lamyaa S Alsleem, Malak F Aldakheel, and Sarah A Alqahtani

Supervised by:
Norah Almubairik, and Dr.Khalid Alisa

In cooperation with the client
Eng, Mubarak Alshahrani
Digital investigator at Digital Evidence Center in Eastren Province, Saudi Arabia

جامعة الإمام عبدالرحمن بن فيصل
IMAM ABDULRAHMAN BIN FAISAL UNIVERSITY

Sarah Alqahtani

Deemah Alotaibi

Malak Aldakheel

Lamyaa Alsleem

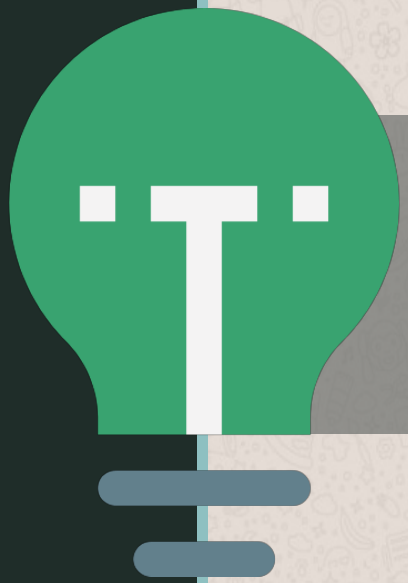
Cybersecurity and Digital Forensics senior students

Agenda

1. Introduction
2. WhatsApp Digger Model
3. Are There Similar Tools ?
4. What Makes WhatsApp Digger Special ?
5. Challenges
6. What Next?
7. Conclusion

1

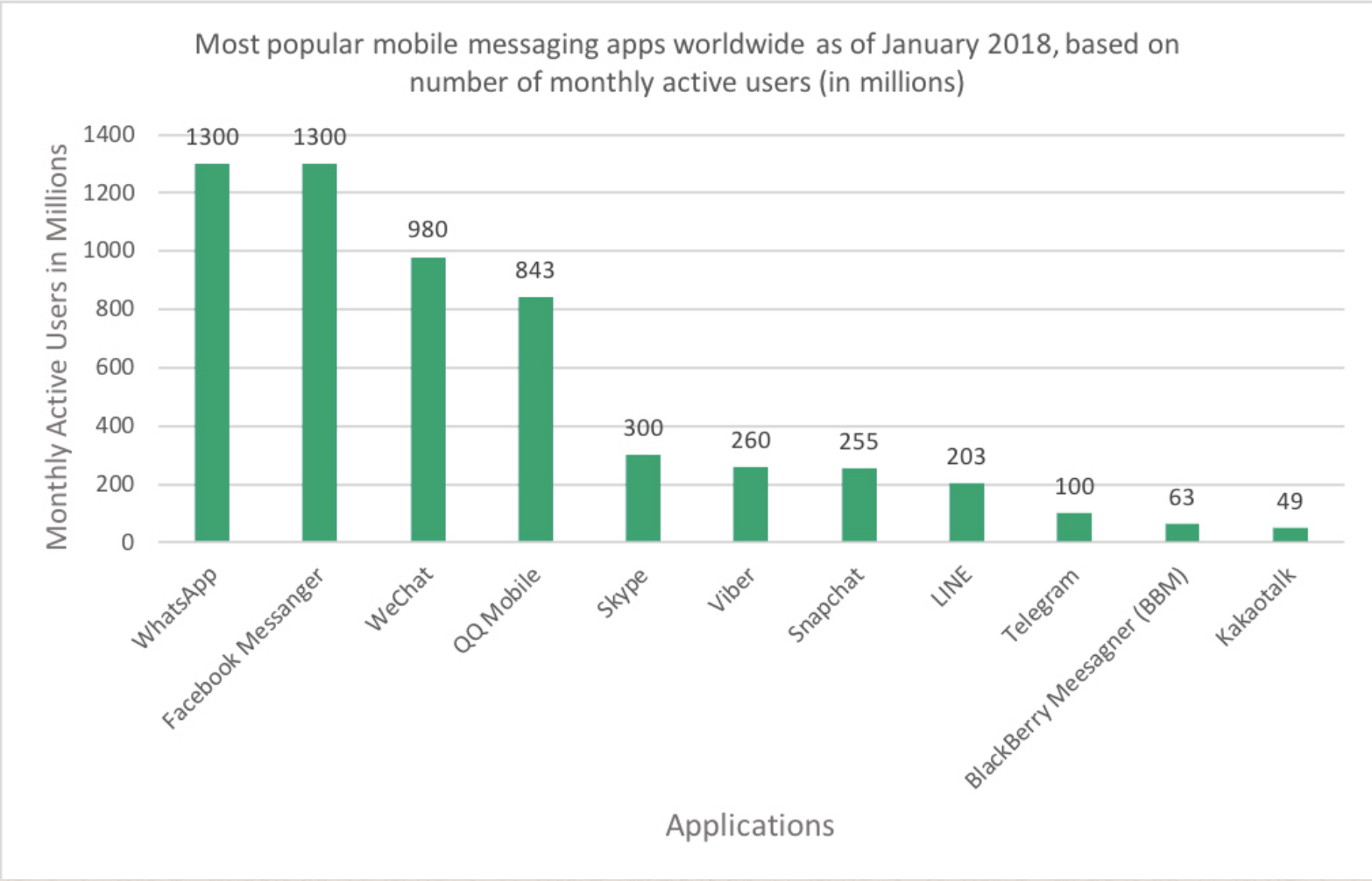
Introduction



Finding an Idea

Motivation

> 80% of digital investigation cases in Saudi Arabi involved **WhatsApp**



Acquisition types

1. **Physical acquisition**

Is the process of recovering the binary representation, which allows the recovery of all files, including deleted files.

Acquisition types

2. Logical acquisition

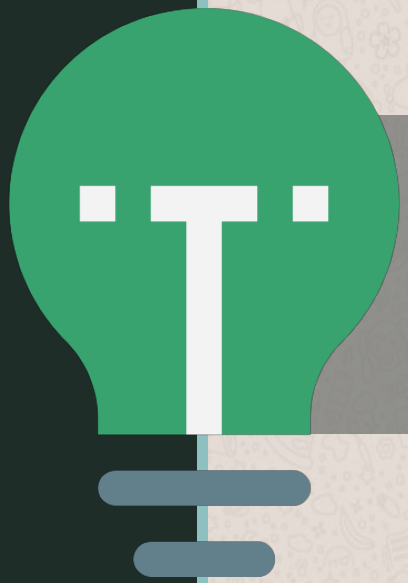
Concerns with retrieving data of interest, such SMS, pictures and text.

a. **Sparse acquisition**: Which is the same as the logical acquisition but with an additional capability of retrieving fragments of deleted data.

Acquisition types

3. Manual acquisition

Is the process of viewing the mobile device content (Manually) and document it by taking pictures.



Point of departure

Acquisition Tools

Acquire WhatsApp Files

Lack Some Analysis Features

Acquire Full Image of The Mobile Content

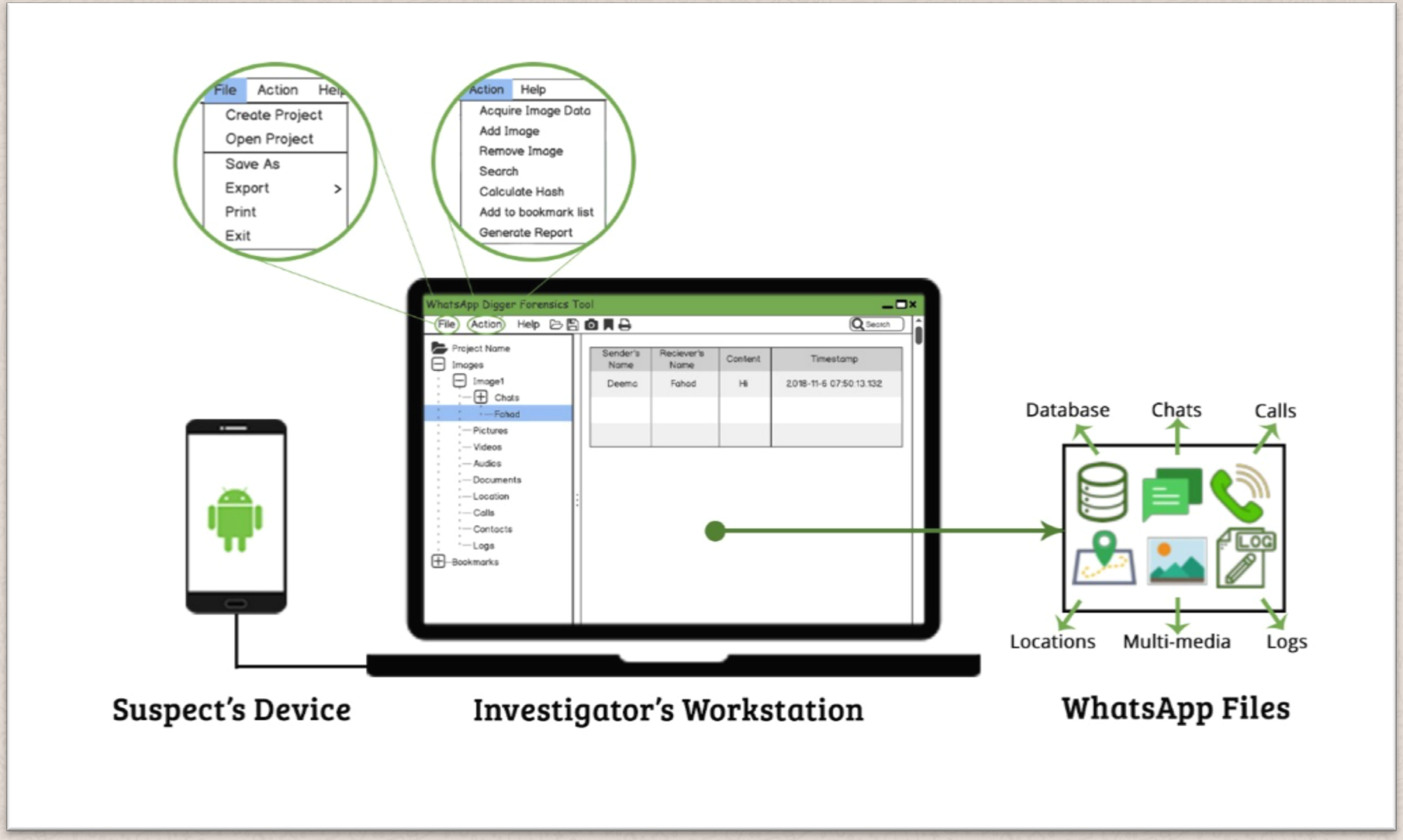
Search For WhatsApp Files

Analysis

2

WhatsApp Digger Model

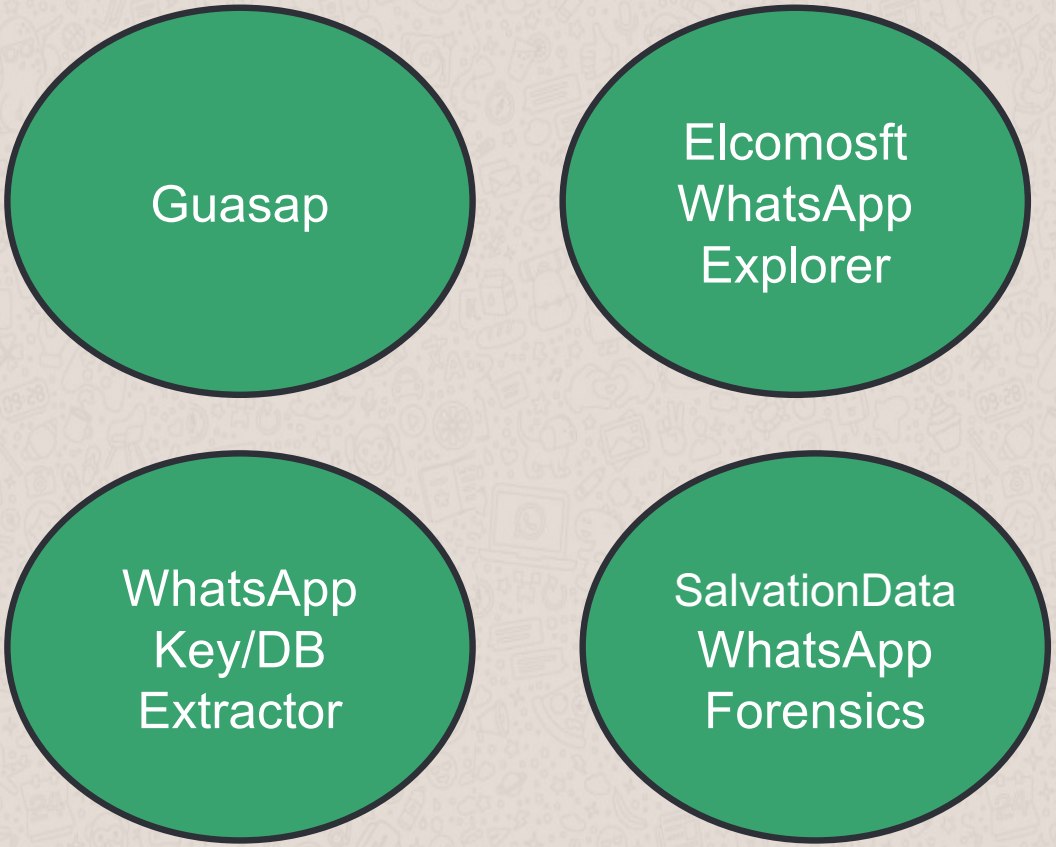
WhatsApp Digger Model



3

Are there similar tools ?

Are there similar tools?



Comparison Aspects

1

NIST Mobile Device Tool Test Assertions and Test Plan

Aims to evaluate the tool's ability to accurately acquire data objects from mobile devices

NIST Core Test Assertions

MDT-CA-01

If a mobile device forensics tool provides the user with an "**Acquire All**" data objects acquisition option, then the tool shall complete the logical/file system acquisition of all data objects without error.

NIST Core Test Assertions

MDT-CA-02

If a mobile device forensics tool provides the user with a "**Select All**" individual data objects, then the tool shall complete the logical/file system acquisition of all individually selected data objects without error.

NIST Core Test Assertions

MDT-CA-03

If the tool provides logical acquisition of "**selected**" objects then it should complete the acquisition process without an error.

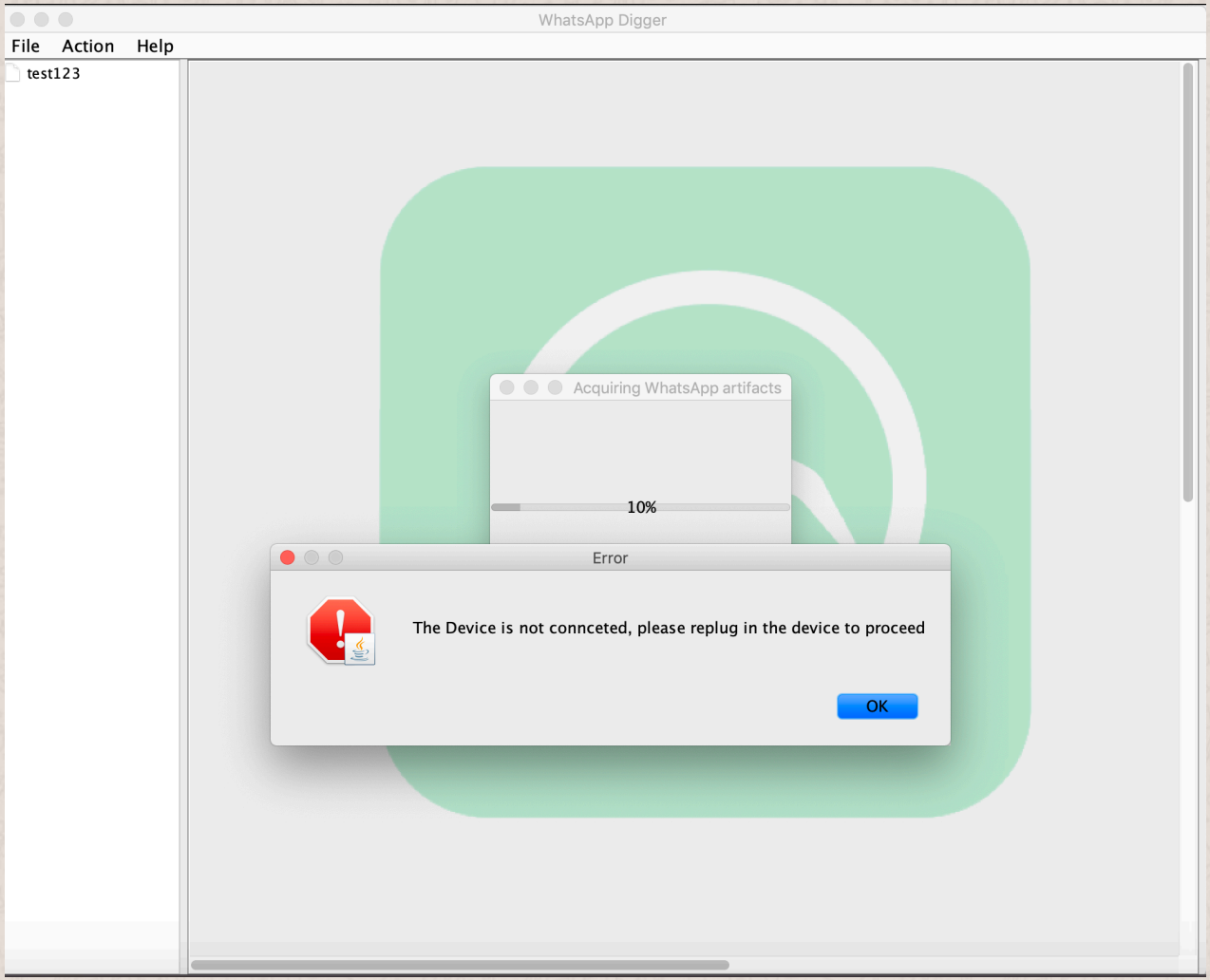
NIST Core Test Assertions

MDT-CA-04

If an interruption occurs during the acquisition process due to connectivity error, then the tool should notify the user with this error.

NIST Core Test Assertions

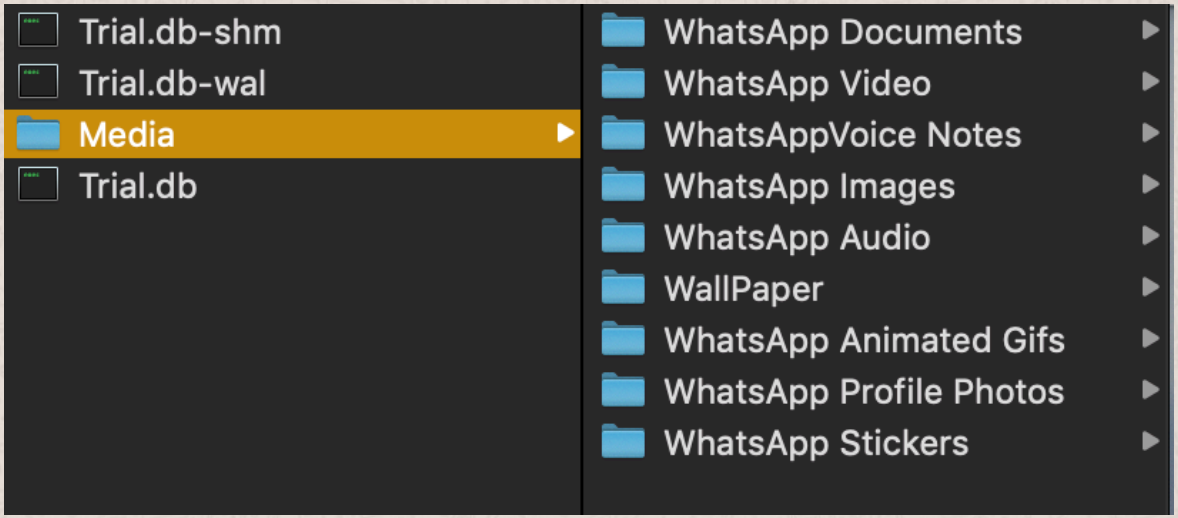
MDT-CA-04



NIST Core Test Assertions

MDT-CA-05

The tool should present the acquired data in a usable format via either preview-pane or generated report.



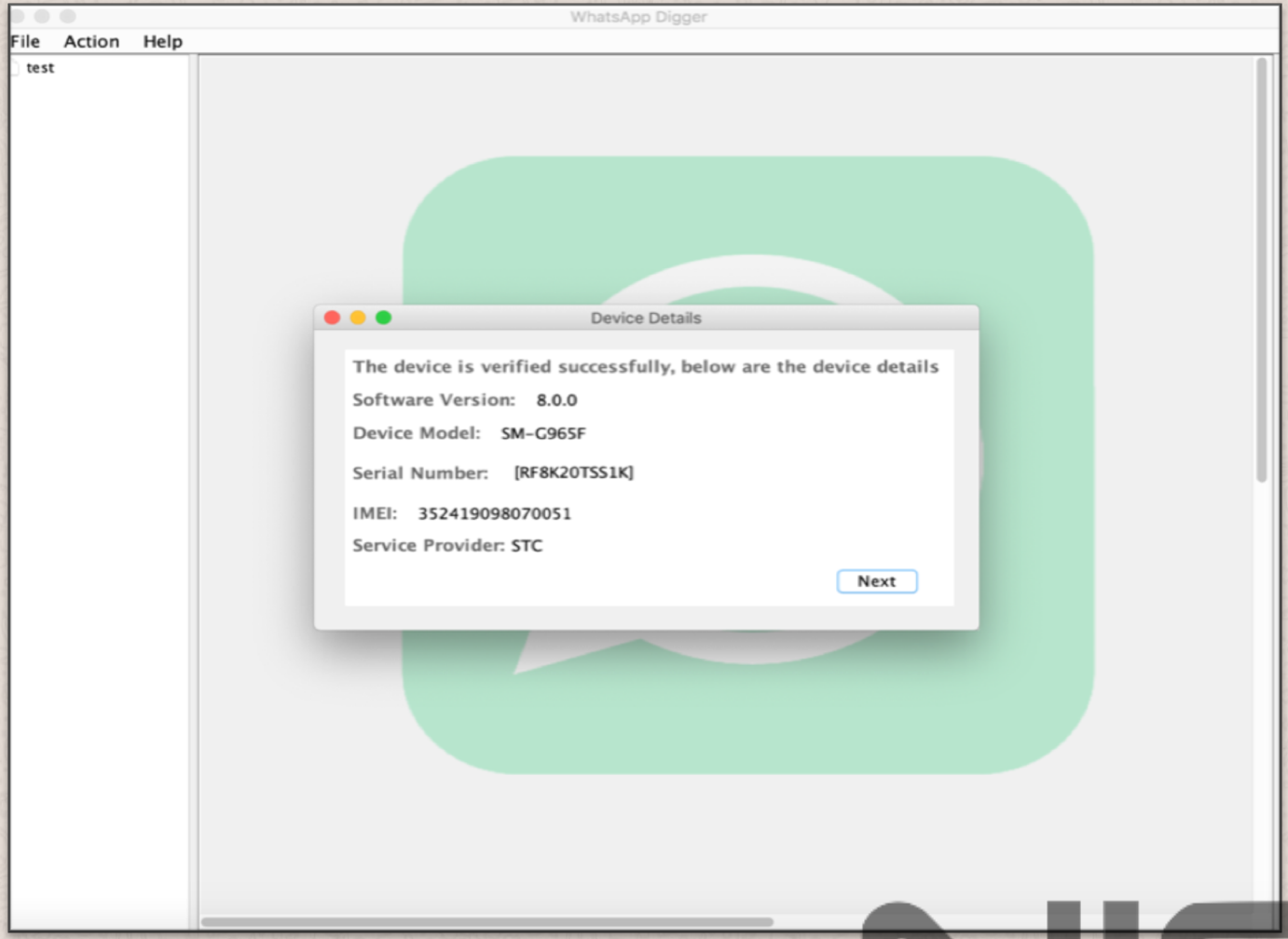
NIST Core Test Assertions

MDT-CA-06

The tool should present information about the target device, like IMEI.

NIST Core Test Assertions

MDT-CA-06



NIST Core Test Assertions

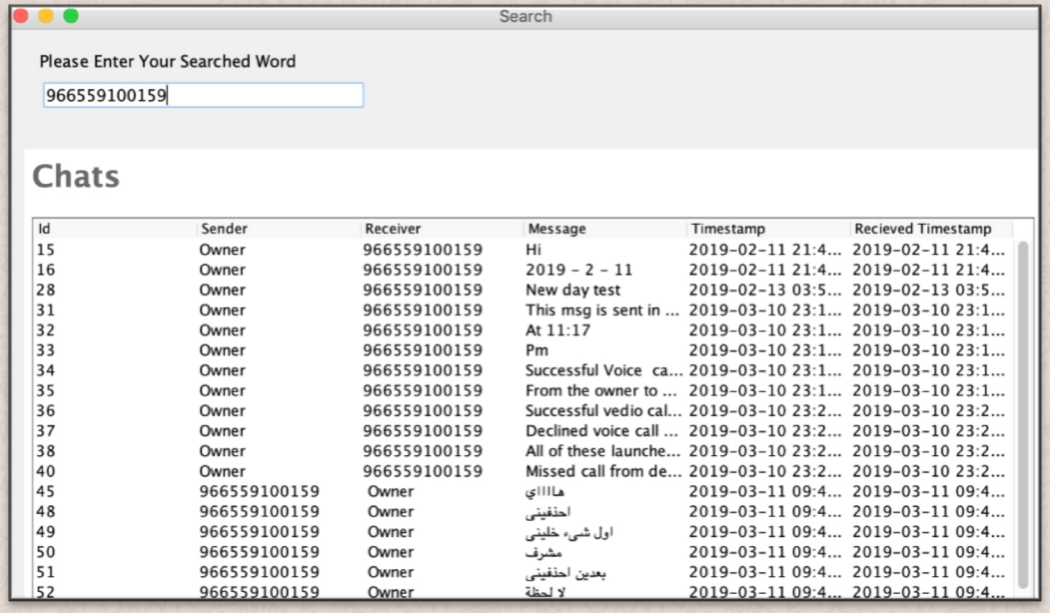
MDT-CA-07

If the tested tool completes the acquisition successfully, then all acquired data such as: Audios, pictures, videos, etc. must be presented in useful format.

NIST Core Test Assertions

MDT-CA-08

If the acquisition is done successfully, then non-Latin character shall be represented in their native format.

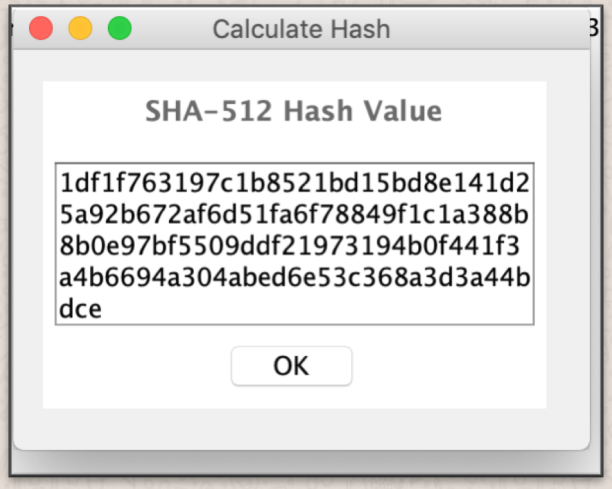


Id	Sender	Receiver	Message	Timestamp	Recieved Timestamp
15	Owner	966559100159	Hi	2019-02-11 21:4...	2019-02-11 21:4...
16	Owner	966559100159	2019 - 2 - 11	2019-02-11 21:4...	2019-02-11 21:4...
28	Owner	966559100159	New day test	2019-02-13 03:5...	2019-02-13 03:5...
31	Owner	966559100159	This msg is sent in ...	2019-03-10 23:1...	2019-03-10 23:1...
32	Owner	966559100159	At 11:17	2019-03-10 23:1...	2019-03-10 23:1...
33	Owner	966559100159	Pm	2019-03-10 23:1...	2019-03-10 23:1...
34	Owner	966559100159	Successful Voice ca...	2019-03-10 23:1...	2019-03-10 23:1...
35	Owner	966559100159	From the owner to ...	2019-03-10 23:1...	2019-03-10 23:1...
36	Owner	966559100159	Successful vedio cal...	2019-03-10 23:2...	2019-03-10 23:2...
37	Owner	966559100159	Declined voice call ...	2019-03-10 23:2...	2019-03-10 23:2...
38	Owner	966559100159	All of these launche...	2019-03-10 23:2...	2019-03-10 23:2...
40	Owner	966559100159	Missed call from de...	2019-03-10 23:2...	2019-03-10 23:2...
45	966559100159	Owner	هاااي	2019-03-11 09:4...	2019-03-11 09:4...
48	966559100159	Owner	احنفيني	2019-03-11 09:4...	2019-03-11 09:4...
49	966559100159	Owner	اول شيء خليني	2019-03-11 09:4...	2019-03-11 09:4...
50	966559100159	Owner	مشرف	2019-03-11 09:4...	2019-03-11 09:4...
51	966559100159	Owner	بعدين احنفيني	2019-03-11 09:4...	2019-03-11 09:4...
52	966559100159	Owner	لا لحظة	2019-03-11 09:4...	2019-03-11 09:4...

NIST Core Test Assertions

MDT-CA-09

If the tested tool acquired data successfully, it must report the hash value of the acquired data objects or overall case file.



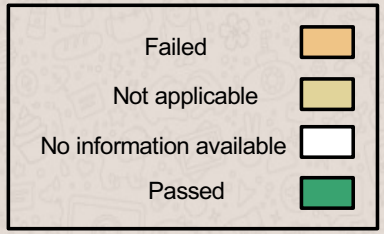
NIST Core Test Assertions

MDT-CA-10

If the generated case file or data objects from the tested tool, are modified by third party tool, the tested tool should report the modification.

NIST Core Test Assertions

NIST Test Assertions		WhatsApp Forensics tools				
		Guasap	Elcomosft WhatsApp Explorer	WhatsApp Key/DB Extractor	SalvationData WhatsApp Forensics	WhatsApp Digger
Core Test Assertions	MDT-CA-01					
	MDT-CA-02					
	MDT-CA-03					
	MDT-CA-04					
	MDT-CA-05					
	MDT-CA-06					
	MDT-CA-07					
	MDT-CA-08					
	MDT-CA-09					
	MDT-CA-10					



2

Researchers' Criteria

Selected based on conducted analysis to evaluate the tools' inclusiveness, compatibility scope and effectiveness

WhatsApp Artifacts

- Artifacts stored in SQLite database.
- SQLite database is encrypted.
- The encryption key is not accessible

Key access methods

Rooting

- Android constitutes of six partitions which are system, user data, cache, boot, and recovery.
  - System partition contains the original operating system that android boots from
  - Recovery partition contains the flashed custom operating system (Third party system), which allows the investigator to boot Android device from the recovery partition instead of the system partition and get root access
- Device dependent process
- New SAMSUNG GALAXY S9 comes with locked bootloader and another restriction which is 7 days jail which prevents flashing custom ROM
- Affect the evidence integrity while wiping the mobile data

Key access methods

Downgrading

- The process of reverting the current version of WhatsApp to an older version, specifically version 2.11.431
- Version 2.11.431 is the last version that allows Android Debugging Bridge (ADB) backup
- No longer supported for the newer versions of WhatsApp since current WhatsApp version enforces its users to upgrade the application to the latest version

Researchers' Criteria

Comparative Features	WhatsApp Forensics tools				
	Guasap	Elcomosft WhatsApp Explorer	WhatsApp Key/DB Extractor	SalvationData WhatsApp Forensics	WhatsApp Digger
Works on Windows Platform	■	■	■	■	■
Works on Linux Platform	■		■		■
Works on Mac Platform			■		■
Support Android Version 8	■				■
Does not use rooting			■	■	■
Does not use downgrading WhatsApp	■				■
Extracts msgstore.db	■	■	■	■	■
Extracts Media folder	◢	■			■
Parses and presents text		■			■
Parses and presents pictures		■			■
Parses and presents videos		■			■
Parses and presents calls		■			■
Parses and presents locations					■
Parses and presents documents					■
Parses and presents audios		■			■
Parses and presents voice notes		■			■
Supports Analysis		◢			■
Logical Acquisition	■	■	■	■	■
Supports Acquisition of Arabic Characters	■	■	■	■	■
Hashing	■				■
Project Arrangement Option					■

Not supported

No information available

Supported

Partially supported

4

What makes WhatsApp Digger Special?

What makes WhatsApp Digger Special?

1. **Key Access method**

   We came up with our own work around method to get the decryption key.

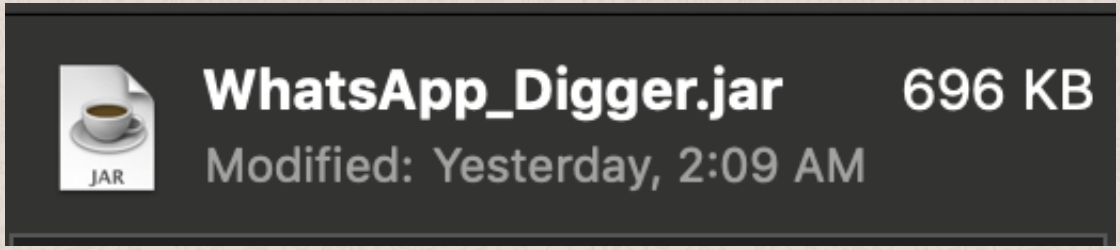
What makes WhatsApp Digger Special?

2. Efficiency

a. Short response time

	WhatsApp Digger
Device Connectivity	15 seconds
Acquisition	40 seconds

b. Minimal use of resources



What makes WhatsApp Digger Special?

3. Data Integrity

The hash value of the acquired data matches the resident data hash value.

4. Reliability

	WhatsApp Digger
Device Connectivity Interruption	7 seconds
Acquisition Interruption	5 seconds

5. Ease of use

Consistent with well-known investigation tools

6. Maintainability

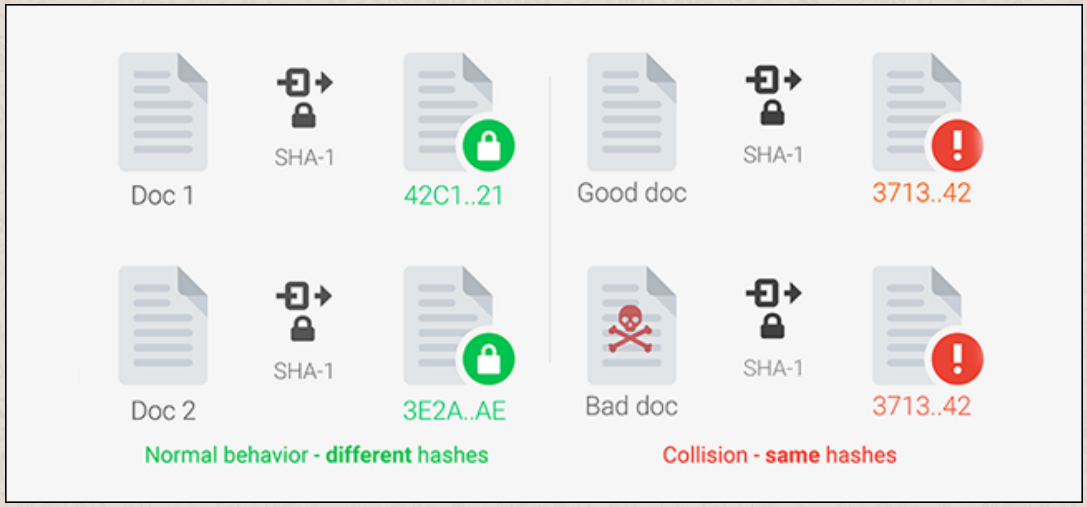
WhatsApp Digger is up to date with current mobile forensics tools.

Secure Hashing Algorithm (SHA-512)

Collision Attack

Collision attack in hash algorithms context means that two different messages or files have the same hash value . The longer the hash output the lower the possibility for the collision attack to happen, since it depends on the number of generated samples based on Birthday Paradox theory.

So, for SHA-512 to have a collision, there should be 2^{256} generated hashes.



Secure Hashing Algorithm (SHA-512)

Collision Attack

To generate this number of hash samples, provided that the attacker has the ability to calculate 300 quadrillion SHA-512 per seconds, then the required number of years to find 2256 samples can be calculated as:

$$\frac{2^{256}}{300 \times 10^{15} \times 3600 \times 365 \times 24} = 1.22 \times 10^{52} \text{ years}$$

This means that with a huge number of files, the possibility that two files have the same hashes is too low and infeasible to be found, which indicates that SHA-512 is highly secure in comparison to the hashes with shorter output.

5

Challenges

Challenges

Challenge:

- SQLite database structure: WhatsApp SQLite column names are

Vague and doesn't reflect what it stored.

Solution:

- We conducted small experiments by changing one thing at a time and then acquire the database, after that we compared the databases with each other to notice the differences.

Challenges

Challenge:

- Parse database data: Some media files have no names.

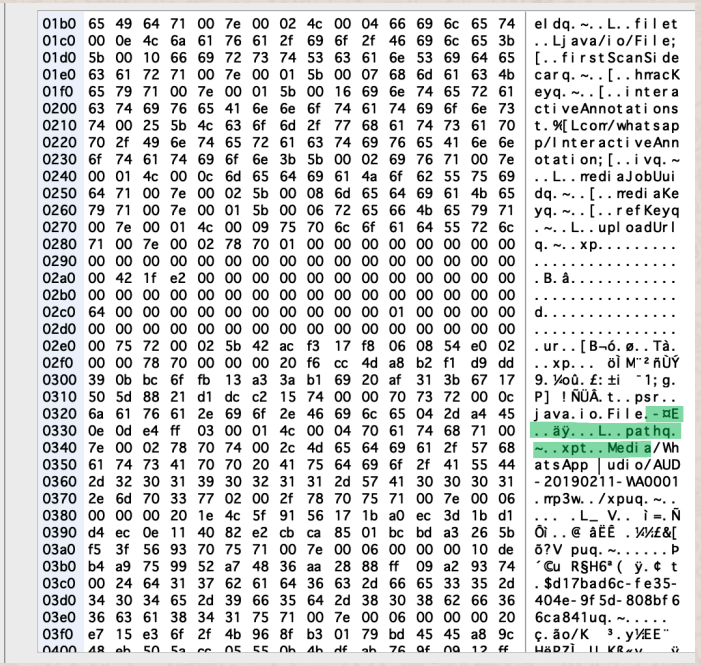
	data	timestamp	media_url	media_mime_type	media_wa_type	media_size	media_name
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
5	Ola	1548581744899	NULL	NULL	0	0	NULL
6	NULL	1548581749891	https://mmg-fn...	NULL	1	42738	aaeee741-d656...
7	NULL	1548581760284	https://mmg-fn...	video/mp4	3	704240	VID-20190127-...
8	NULL	1548581774898	NULL	NULL	15	0	2F60E81A9ECC...
9	NULL	1548581781477	https://mmg.w...	audio/ogg; cod...	2	8163	f5082c408a2f4...
10	27 Jan 2019 - ...	1548581918423	NULL	NULL	0	0	NULL
11	NULL	1548581924078	NULL	NULL	15	0	94BFF1A1E2F2...
12	NULL	1549910713817	NULL	NULL	0	19	NULL
13	Hey	1549910713814	NULL	NULL	0	0	NULL
14	NULL	1549910725810	https://mmg.w...	audio/ogg; cod...	2	5095	dfba052c7d4a4...
15	Hi	1549910726000	NULL	NULL	0	0	NULL
16	2019 - 2 - 11	1549910741000	NULL	NULL	0	0	NULL
17	NULL	1549910753000	https://mmg.w...	audio/mpeg	2	4333538	NULL
18	NULL	1549910796000	https://mmg-fn...	application/vnd....	9	2473649	Chapter2.docx
19	NULL	1549910834000	https://mmg-fn...	application/pdf	9	2262045	(IT_Support)_Fi...
20	NULL	1549910837000	https://mmg-fn...	image/png	9	28710	Drawing1
21	NULL	1549910889000	https://mmg-fn...	application/vnd....	9	11765	DeemaSarah.docx
22	NULL	1549910903000	https://mmg.w...	audio/ogg; cod...	2	8065	NULL
23	NULL	1549910928000	https://mmg-fn...	image/jpeg	1	69156	NULL

Challenges

Solution:

- Searching the string representation of the binary data.

	dia_hash	media_duration	origin	latitude	longitude	thumb_image	remote_resource	eceived_timestamp
		Filter	Filter	Filter	Filter	Filter	Filter	Filter
5		0	0	0.0	0.0	NULL	NULL	1548581744933
6	JzDVMbo...	0	0	0.0	0.0	BLOB	NULL	1548581749899
7	6eXfruzfd...	3	0	0.0	0.0	BLOB	NULL	1548581760315
8		0	0	0.0	0.0	NULL	NULL	0
9	vtC2uMyn...	3	1	0.0	0.0	BLOB	NULL	1548581783292
10		0	0	0.0	0.0	NULL	NULL	1548581918459
11		0	0	0.0	0.0	NULL	NULL	0
12		0	0	0.0	0.0	NULL	NULL	1549910713822
13		0	0	0.0	0.0	NULL	NULL	1549910713848
14	8ZBV7+f...	2	1	0.0	0.0	BLOB	NULL	1549910726217
15		0	0	0.0	0.0	NULL		1549910727376
16		0	0	0.0	0.0	NULL		1549910741928
17	VYjEns1Q...	270	0	0.0	0.0	BLOB		1549910754006
18	Z1UD06s...	0	0	0.0	0.0	BLOB		1549910797618
19	czFwKm...	33	0	0.0	0.0	BLOB		1549910834949
20	rHSWCCA...	0	0	0.0	0.0	BLOB		1549910838577
21	O7GrKUze...	0	0	0.0	0.0	BLOB		1549910890188
22	MrzfbrZfB...	4	1	0.0	0.0	BLOB		1549910908151
23	rEUXcU4d...	0	0	0.0	0.0	BLOB		1549910934763



Challenges

Challenge:

- The laptop was formatted: Using commands to communicate with the mobile device yields in formatting the laptop for no obvious reason! WhatsApp Digger codes were erased and many important files.

Solution:

- We do a daily backup, and we had to just rewrite the codes that has been deleted in this day. And most of the files in the laptop were stored in online drive.

Challenges

Challenge:

- Saving project data in a propriety format was not that easy, since there are a lot of options and it needs a careful study to serialize objects then un-serialize them.

Solution:

- We saved project objects in XML files.

6 What Next?

What Next?

- Creating our own propriety format
- Including IOS devices
- Retrieving deleted messages and log files

7

Conclusion

Conclusion

- **Findings and contribution**

There is a shortage in the current tools in both acquisition and analysis.

- **Limitations**

Due to time constraint, deleted messages were not in the scope and neither the log files.

- **Technology impact**

WhatsApp Digger is of a great value to the mobile investigation field, specifically, Department of Criminal Evidences.

- **Lessons Learned**

“Two is one, one is none”, always backup your data

References

statista, "Most popular mobile messaging apps worldwide," statista, January 2018. [Online]. Available: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/. [Accessed 4 October 2018].

N. Bill, P. Amelia and S. Christopher, Guide to Computer Forensics and Investigations: Processing Digital Evidence, Boston: Cengag Learning , 2015 .

J. K. a. Y. Lindell, Introduction to Modern Cryptography, CRC PRESS, 2007.

National Institute of Standards and Technology , "Mobile Device Tool Test Assertions and Test Plan," 1 Febrauray 2016. [Online]. Available: https://www.nist.gov/sites/default/files/documents/2017/05/09/mobile_device_tool_test_assertions_and_test_plan_v2.0.pdf. [Accessed 1 October 2018].

a. M. H. Lutta Pantaleon, "An Investigation into the Impact of Rooting Android Device on User Data Integrity," in 7th IEEE International Conference on Emerging Security Technologies, 2017.

J. Levin, Android Internals A Confectioner's Cookbook, Cambridge, MA: Technologeeks, 2015.

C. Z. N. C. Timothy Vidas a, "Toward a general collection methodology for Android devices," Elsevier , pp. S14-S24, 2011.

A. Oleg, "Extracting WhatsApp Conversations from Android Smartphones," 2 February 2017. [Online]. Available: https://blog.elcomsoft.com/2017/02/extracting-whatsapp-conversations-from-android-smartphones/. [Accessed 14 October 2018].

Android, " Android Debug Bridge (adb)," Android, 24 September 2018. [Online]. Available: https://developer.android.com/studio/command-line/adb.

SalvationDATA, "WhatsApp Forensics: Decryption of Encrypted Databases and Extraction of Deleted Messages on Non-Rooted Android Devices," 8 February 2018. [Online]. Available: https://blog.salvationdata.com/2018/02/08/whatsapp-forensics-decryption-of-encrypted-databases-and-extraction-of-deleted-messages-on-non-rooted-android-devices/. [Accessed 1 October 2018].

Thanks!

ANY QUESTIONS?