International Journal of Engineering Sciences & Research Technology

(A Peer Reviewed Online Journal)
Impact Factor: 5.164

IJESRT

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

DATA EXTRACTION FROM PASSWORD PROTECTED MOBILE PHONE BY USING CHIP-OFF METHOD –A FORENSIC CASE STUDY

Akhlesh Kumar[*1], Bhushan Ghode[2] & Khevna Maniar3
[*1,2&3]Central Forensic Science Laboratory, DFSS, MHA, Govt. of India, Chandigarh-36

DOI: https://doi.org/10.29121/ijesrt.v10.i3.2021.5

ABSTRACT

The current digital era is full of digital devices and to ensure the safety of their data, users utilize the protective armor of passwords using the fingerprints lock, face lock, pin codes and password locks. The trial-and-error method possesses an infinite possibility of passwords in patterns/ pin locks for unlocking the devices. The levels of security ensure that only a limited number of trials are possible before any device blocks itself or makes unlocking harder. In these circumstances, especially when a victim is a deceased person (e. g. an abetment in suicide case), the password is practically impossible to attain through the authorities. However, the data can be retrieved with the unique and distinctive method of Chip-off analysis. In this study, a password protected mobile phone was retrieved from a deceased individual and only the analysis of his/her mobile could lead to investigative insights for catching the perpetrator. The Chip-off method has several difficulties and a password/ pin protected device increases the difficulties for analysis several folds. This study highlights the significance of chip-off analysis in achieving accurate importing and extraction of maximum data along with the use of the hardware/software, MSAB, XRY and other software.

KEYWORDS: Password protected mobile phones, Chip-off analysis facility, unsoldering, MSAB XRY, etc..

1. INTRODUCTION

Even as the commercial tools are improving and making innovations at an impressive rate, unfortunately, the devices continue to evolve posing challenges for the examiners. The chip-off technique is a promising alternative means for data recovery of mobile phones that are damaged, broken or locked due to which the standard procedures for extraction of data are not possible in such devices [1]. This technique when utilized with other software is capable of extracting dump which can then be decoded further [2].

XRY and JTAG methods are advanced levels of data acquisition methods involving connecting the device's Test Access Ports (TAPs) and processing the chip to gather the raw data from the chip. Thus, it enables the examiners to extract full physical image from the devices which are not supported by the standard forensic tools.

One of the other software that can help analyze the extracted data is Forensic Explorer. Forensic Explorer is an advanced sorting and filtering software which combined with its flexible graphic user interface enables the investigators to access available data, analyze a large volume of information from multiple sources, automate complex filtering tasks and produce detailed reports of the data extracted.[3]

Certain open source applications are also available to analyze the data significantly. During this study, we came across one such application and utilized it. WhatsApp Viewer is an open-source application that enables WhatsApp users to view their WhatsApp chat on their computers. This application makes it easier to copy the messages on the computer, even while reading older messages. The added advantage of this application is that it displays chats from the Android msgstore. db file and supports crypt5, crypt7, crypt8 and crypt12 versions of the database. The data can also be saved as txt, html and is on files for easy storage.[4]

The study is comprising of a case of abetment of suicide in which one male committed suicide under perilous circumstances. After his death, the family of the victim registered a police complaint under section of 306, Indian Penal Code (IPC). They mentioned in the complaint that their son was being mentally tortured as a classmate was generally picking fights with him and being abusive in the college. Moreover, their son was being blackmailed with threats to spread the news of an alleged affair with their upstairs neighbor's daughter-in-law. The constant harassment faced by the daughter-in-law led to her committing suicide to escape the daily upheaval. The case was then presented before the court. The accused(s) got the case dismissed under the pretext of being a victim themselves and being accused of the crime under false pretenses.

The perpetrator also continued his tortures with the victim. After more than one month had passed since the suicide, when tired of the constant suppression being faced by him, the victim decided to end his life. The entire incidents were occurring in person and hence, there was no proof of the matter except the victim's mobile device. The victim had left his written suicide note as well as a voice recording of the same in which he had named the perpetrator and his accomplices along with the incidences as they had happened. However, the mobile phone was found in a locked condition whose password was unknown to any relatives of the victim. Hence, the examiners were faced with a dilemma to solve this problem. Furthermore, the forensic tools like UFED, XRY, etc. in the laboratory were unable to by-pass the model of the mobile device (Samsung, Model: SM-G510F). Essentially, permission to conduct chip-off was required from the legal authorities. Thus, began the procedure for attempting to conduct chip-off method on the received device.

As mentioned above, the chip-off is an alternative method for data extraction when standard forensic methods become unfeasible or inoperative for the purpose. Here, the password protection of the device demanded that either the password or the permission to attempt chip-off be provided for examination purposes.

Chip-off forensics is a powerful technique that allows collecting a complete physical image/forensic dump of nearly any device using the retrieved NAND flash memory chip(s) from a device and then acquiring the raw data/image using a specialized forensic tool. Retrieving data from locked and unlocked phones is getting harder day-by-day as the complexity of the patterns and the number of digits in the pin-locks keep on expanding. Often, a digital forensic investigator uses the CHIP-OFF Forensic Technique to remove NAND flash memory where the data is stored. [5]

The chip-off analysis utilizes thermal/IR-based procedures to physically remove the NAND chip from the motherboard of the devices. The chip is then accessed using various forensic tools to acquire its physical image.

1.1 Performing Chip-off analysis:

1. The mobile device is opened using the heat and air combination to remove its back and front covers, battery screws, other connections, etc. to retrieve the motherboard from it.
2. The NAND flash memory is located on the retrieved motherboard/circuit board.
3. Using appropriate heat (disordering) and chemicals (adhesive removal), the memory chip is physically removed.
4. The removed chip is cleaned and/or reballed if necessary.
5. The forensic image/dump of the chip is then acquired by using any imaging software and an adapter connecting it to the PC.
6. Further analysis can be conducted with standard software available in the laboratory.

The chip-off method can be used to extract data from nearly any devices that utilises flash memory (NAND, NOR, One NAND and eMMC).[6] The main aim during the examination and analysis of the device is to retrieve the relevant data according to the query posed by the legal authorities/ inquirers. In this case, relevant data included the audio-video recordings, WhatsApp data and Images/ photographs from the device.

1.2 General difficulties/ obstacles faced during retrieval of the chip:

1. Locating NAND flash memory of the exhibit from its motherboard.
2. Setting optimum hot airgun temperature so that chip can be plucked easily.
3. Cleaning of the chip after successfully disordering it from its motherboard.
4. Locating pinpoints for reading the chip and choosing suitable adapters for it.

During this study, the chip-off technique was utilized at its most basic and adept conditions. Moreover, this method even as it posed difficulties, complications and being time-consuming, it was the most effective, secure and potent method for data retrieval from the locked mobile device.

2. MATERIALS AND METHODS

2.1 Step-wise procedures followed for the study:

Whenever any mobile phone is subjected to data extraction, standard laboratory procedures and standard hardware/software are utilized. For this study, freeware, as well as paid forensic software, are employed for extraction and analysis.

Case opening

The case was received by hand from a messenger in sealed condition. The parcel contained one mobile phone of Samsung, Model: SM- G531F. The phone was appropriately marked and kept for charging.

Device activation

Once the charging of the mobile was completed and the device activated, the mobile phone was immediately switched to Airplane Mode. When attempted to open the mobile phone it showed that the mobile phone was password protected (Fig. 1) and after several attempts of trial-and-error method, the device could not be unlocked. Thus, after getting permission from legal authorities to continue with the chip-off method, the procedure was started.

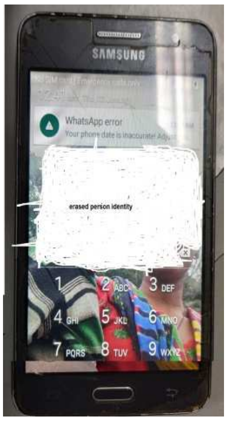


Fig. 1: Pin lock protected mobile device

Chip unsoldering

The device's back and front covers were first removed using a hot airgun (Fig. 2). The screws and other connectors were removed from the device. The NAND memory chip located and subsequent process for chip unsoldering was followed (Fig. 3).

Chip unsoldering was performed using a hot air gun (at 310°C) and a disordering machine. The airgun and disordering machine can be of the desired company based on the availability and efficiency of the product for the user.

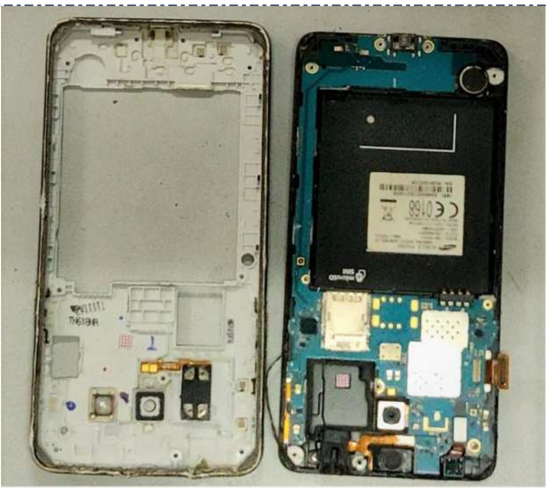


Fig.2: An opened device for circuit board

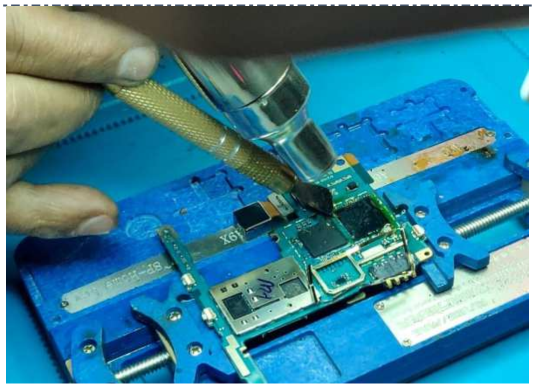


Fig.3: Unsoldering of the chip from a circuit board

Chip processing and cleaning

The unsoldered chip now must be cleaned (Fig. 4) and processed in such a manner that the adhesives applied to the chip are removed and the connectors of the chip can be easily detected by the chip reader.

The chip is treated with a soldering paste with intermittent heating using the soldering gun. This removes the glue and other metal impurities stuck to the chip. This is followed by further treatment of the chip with a glue cleaning chemical to substantially clean all the connector points on the chip (Fig. 5). This step ensures an adequate and clear connection of the chip with the eMMC adapters during extraction.

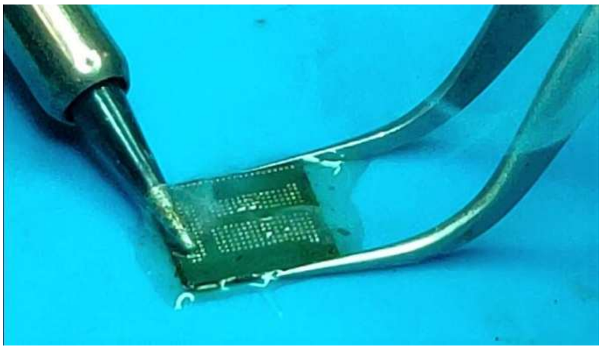


Fig.4: Cleaning of the unsoldered chip

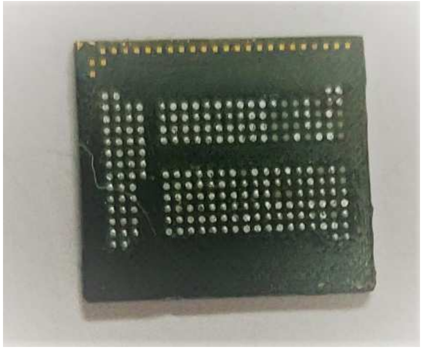
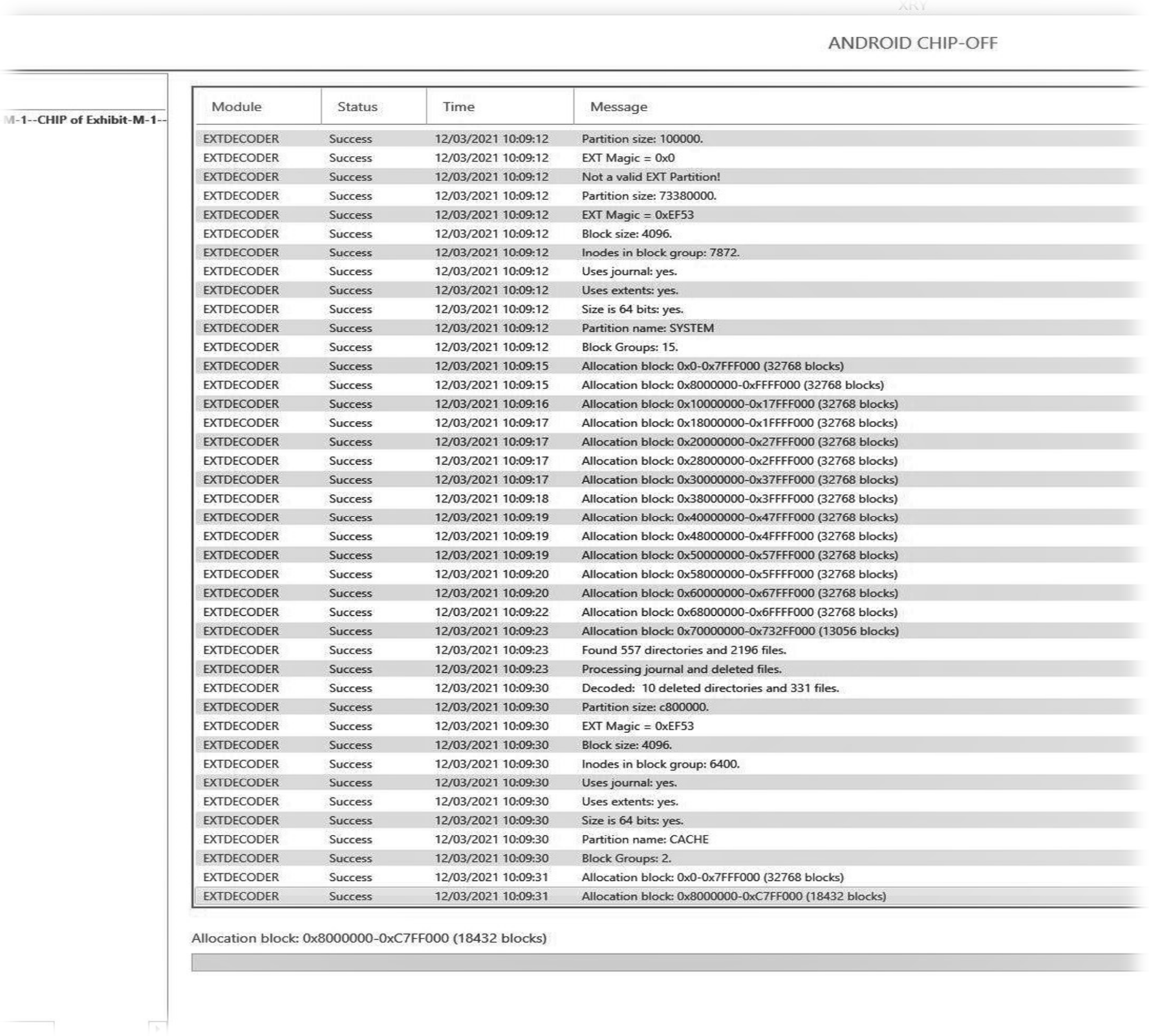


Fig.5: Chip ready for extraction

Data extraction and decoding

The retrieved chip was now utilized for data extraction and decoding using the following software:

a) MSAB XRY and XMAN with eMMC adapter.
b) Forensic Explorer.
c) WhatsApp Viewer.[7]



Module	Status	Time	Message
EXTDECODER	Success	12/03/2021 10:09:12	Partition size: 100000.
EXTDECODER	Success	12/03/2021 10:09:12	EXT Magic = 0x0
EXTDECODER	Success	12/03/2021 10:09:12	Not a valid EXT Partition!
EXTDECODER	Success	12/03/2021 10:09:12	Partition size: 73380000.
EXTDECODER	Success	12/03/2021 10:09:12	EXT Magic = 0xEF53
EXTDECODER	Success	12/03/2021 10:09:12	Block size: 4096.
EXTDECODER	Success	12/03/2021 10:09:12	Inodes in block group: 7872.
EXTDECODER	Success	12/03/2021 10:09:12	Uses journal: yes.
EXTDECODER	Success	12/03/2021 10:09:12	Uses extents: yes.
EXTDECODER	Success	12/03/2021 10:09:12	Size is 64 bits: yes.
EXTDECODER	Success	12/03/2021 10:09:12	Partition name: SYSTEM
EXTDECODER	Success	12/03/2021 10:09:12	Block Groups: 15.
EXTDECODER	Success	12/03/2021 10:09:15	Allocation block: 0x0-0x7FFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:15	Allocation block: 0x8000000-0xFFFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:16	Allocation block: 0x10000000-0x17FFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:17	Allocation block: 0x18000000-0x1FFFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:17	Allocation block: 0x20000000-0x27FFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:17	Allocation block: 0x28000000-0x2FFFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:17	Allocation block: 0x30000000-0x37FFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:18	Allocation block: 0x38000000-0x3FFFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:19	Allocation block: 0x40000000-0x47FFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:19	Allocation block: 0x48000000-0x4FFFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:19	Allocation block: 0x50000000-0x57FFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:20	Allocation block: 0x58000000-0x5FFFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:20	Allocation block: 0x60000000-0x67FFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:22	Allocation block: 0x68000000-0x6FFFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:23	Allocation block: 0x70000000-0x732FF000 (13056 blocks)
EXTDECODER	Success	12/03/2021 10:09:23	Found 557 directories and 2196 files.
EXTDECODER	Success	12/03/2021 10:09:23	Processing journal and deleted files.
EXTDECODER	Success	12/03/2021 10:09:30	Decoded: 10 deleted directories and 331 files.
EXTDECODER	Success	12/03/2021 10:09:30	Partition size: c800000.
EXTDECODER	Success	12/03/2021 10:09:30	EXT Magic = 0xEF53
EXTDECODER	Success	12/03/2021 10:09:30	Block size: 4096.
EXTDECODER	Success	12/03/2021 10:09:30	Inodes in block group: 6400.
EXTDECODER	Success	12/03/2021 10:09:30	Uses journal: yes.
EXTDECODER	Success	12/03/2021 10:09:30	Uses extents: yes.
EXTDECODER	Success	12/03/2021 10:09:30	Size is 64 bits: yes.
EXTDECODER	Success	12/03/2021 10:09:30	Partition name: CACHE
EXTDECODER	Success	12/03/2021 10:09:30	Block Groups: 2.
EXTDECODER	Success	12/03/2021 10:09:31	Allocation block: 0x0-0x7FFF000 (32768 blocks)
EXTDECODER	Success	12/03/2021 10:09:31	Allocation block: 0x8000000-0xC7FF000 (18432 blocks)

Allocation block: 0x8000000-0xC7FF000 (18432 blocks)

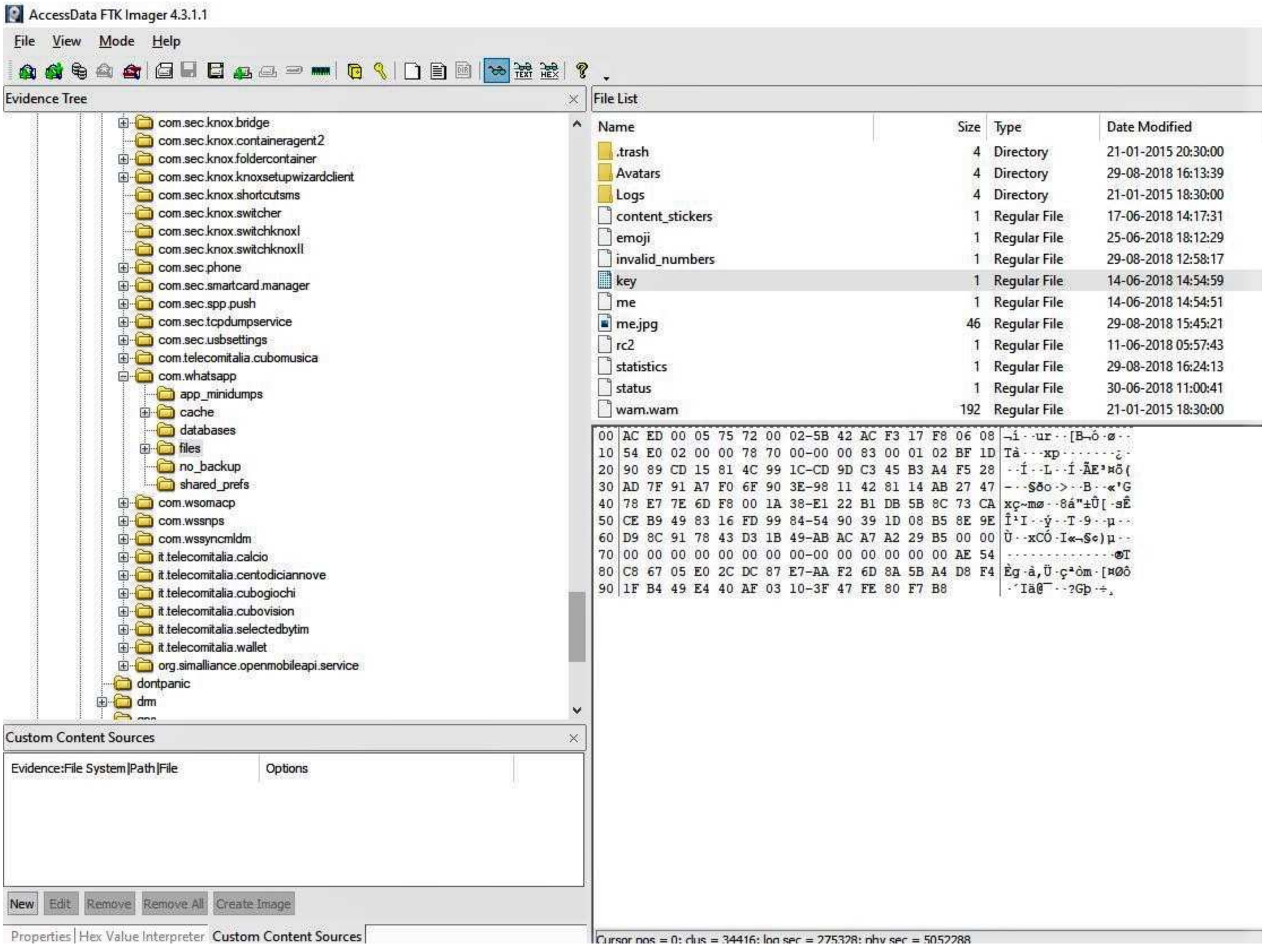
Fig.6: Extraction and decoding using XRY

Once the physical dump of the chip is extracted, the crucial task of decoding the dump begins. Dump decoding is a complex task that is generally performed by skilled examiners. The XRY software is one of the software which supports the decoding of the physical dump which has been extracted from the chip. Here, the same was utilized (Fig. 6).

3. RESULTS AND DISCUSSION

The retrieved chip when initially connected to XRY and chip reader for data extraction, partial data (audio, video, documents, etc.) was retrieved from the software.

Chips in mobile devices (eMMC) have an interface similar to SD cards [2] therefore, subsequently, the software FTK Imager, Version 4.1 was utilized for imaging the chip. The image was then analyzed using the software Forensic Tool Kit (FTK), Version 6.4. This led to successful retrieval of audio, video, pictures, documents, etc. However, WhatsApp chats and database retrieved were found to be encrypted. The software WhatsApp Viewer (Fig. 7) (open source) was downloaded (from https://whatsapp-database-viewer.software.informer.com/1.9/) and WhatsApp database was decrypted using the key file found in the root folder of the image of the chip (Fig.8). In this way, the WhatsApp chats were also retrieved successfully.



```
com.sec.knox.bridge
com.sec.knox.containeragent2
com.sec.knox.foldercontainer
com.sec.knox.knoxsetupwizardclient
com.sec.knox.shortcutsms
com.sec.knox.switcher
com.sec.knox.switchknoxI
com.sec.knox.switchknoxII
com.sec.phone
com.sec.smartcard.manager
com.sec.spp.push
com.sec.tcpdumpservice
com.sec.usbsettings
com.telecomitalia.cubomusica
com.whatsapp
    app_minidumps
    cache
    databases
    files
    no_backup
    shared_prefs
com.wsomacp
com.wssnps
com.wssyncmldm
it.telecomitalia.calcio
it.telecomitalia.centodiciannove
it.telecomitalia.cubogiochi
it.telecomitalia.cubovision
it.telecomitalia.selectedbytim
it.telecomitalia.wallet
org.simalliance.openmobileapi.service
dontpanic
drm
```

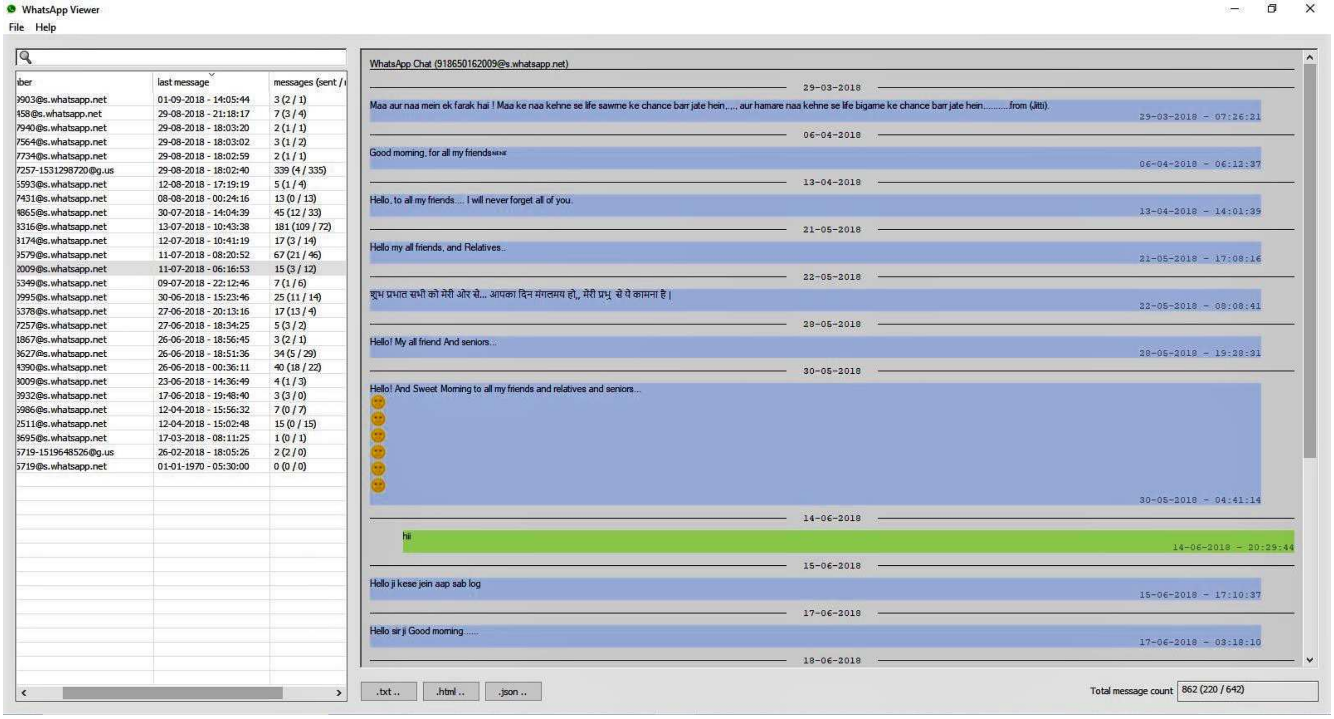
Name	Size	Type	Date Modified
.trash	4	Directory	21-01-2015 20:30:00
Avatars	4	Directory	29-08-2018 16:13:39
Logs	4	Directory	21-01-2015 18:30:00
content_stickers	1	Regular File	17-06-2018 14:17:31
emoji	1	Regular File	25-06-2018 18:12:29
invalid_numbers	1	Regular File	29-08-2018 12:58:17
key	1	Regular File	14-06-2018 14:54:59
me	1	Regular File	14-06-2018 14:54:51
me.jpg	46	Regular File	29-08-2018 15:45:21
rc2	1	Regular File	11-06-2018 05:57:43
statistics	1	Regular File	29-08-2018 16:24:13
status	1	Regular File	30-06-2018 11:00:41
wam.wam	192	Regular File	21-01-2015 18:30:00

```
00 AC ED 00 05 75 72 00 02-5B 42 AC F3 17 F8 06 08 ¬í··ur··[B¬ó·ø··
10 54 E0 02 00 00 78 70 00-00 00 83 00 01 02 BF 1D Tà···xp·······¿·
20 90 89 CD 15 81 4C 99 1C-CD 9D C3 45 B3 A4 F5 28 ··Í··L··Í·ÃE³¤õ(
30 AD 7F 91 A7 F0 6F 90 3E-98 11 42 81 14 AB 27 47 -··§ðo·>··B··«'G
40 78 E7 7E 6D F8 00 1A 38-E1 22 B1 DB 5B 8C 73 CA xç~mø··8á"±Û[·sÊ
50 CE B9 49 83 16 FD 99 84-54 90 39 1D 08 B5 8E 9E Î¹I··ý··T·9··µ··
60 D9 8C 91 78 43 D3 1B 49-AB AC A7 A2 29 B5 00 00 Ù··xCÓ·I«¬§¢)µ··
70 00 00 00 00 00 00 00 00-00 00 00 00 00 00 AE 54 ··············®T
80 C8 67 05 E0 2C DC 87 E7-AA F2 6D 8A 5B A4 D8 F4 Èg·à,Ü·çªòm·[¤Øô
90 1F B4 49 E4 40 AF 03 10-3F 47 FE 80 F7 B8       ·´Iä@¯··?Gþ·÷¸
```

Evidence:File System|Path|File	Options

Cursor pos = 0; clus = 34416; log sec = 275328; phy sec = 5052288

Fig.7: WhatsApp Key in the image of the chip



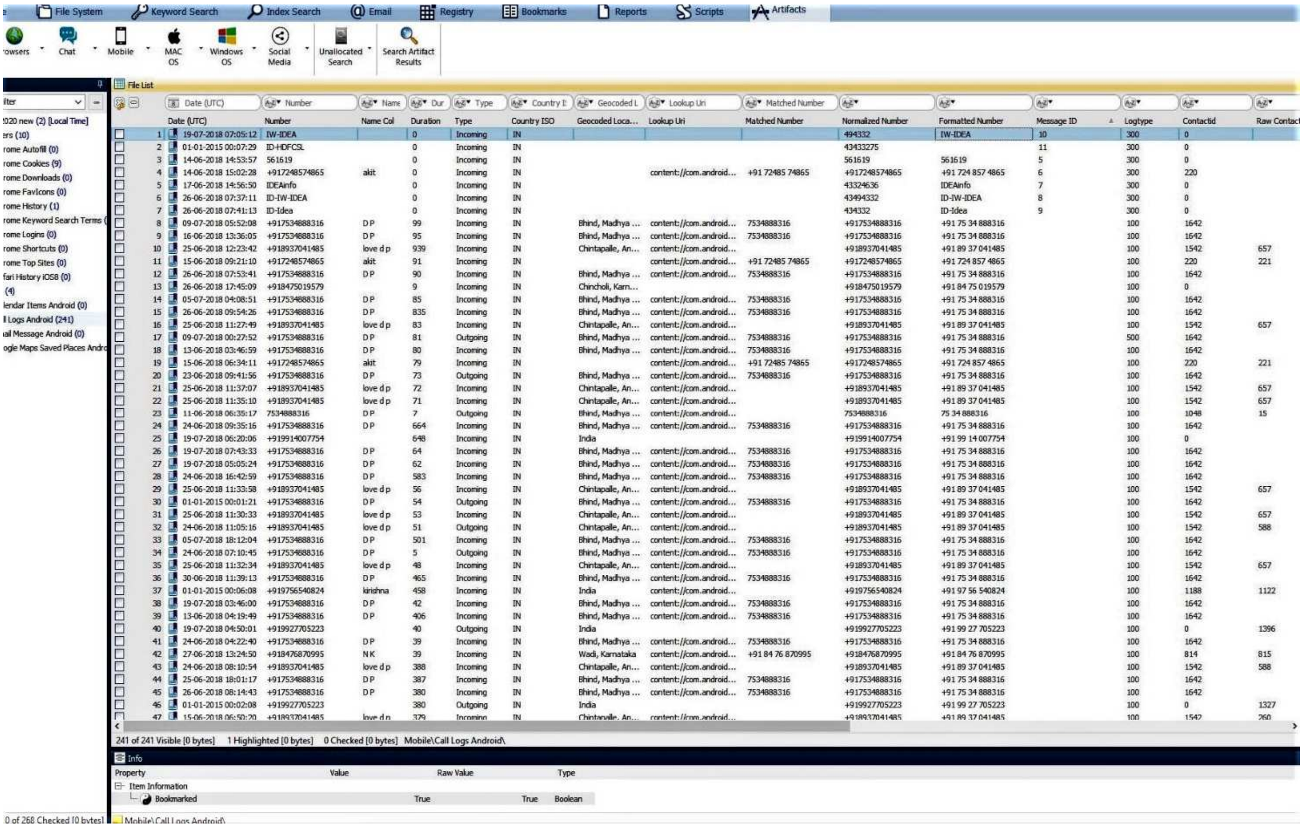
ıber	last message	messages (sent / ı
9903@s.whatsapp.net	01-09-2018 - 14:05:44	3 (2 / 1)
458@s.whatsapp.net	29-08-2018 - 21:18:17	7 (3 / 4)
7940@s.whatsapp.net	29-08-2018 - 18:03:20	2 (1 / 1)
7564@s.whatsapp.net	29-08-2018 - 18:03:02	3 (1 / 2)
7734@s.whatsapp.net	29-08-2018 - 18:02:59	2 (1 / 1)
7257-1531298720@g.us	29-08-2018 - 18:02:40	339 (4 / 335)
5593@s.whatsapp.net	12-08-2018 - 17:19:19	5 (1 / 4)
7431@s.whatsapp.net	08-08-2018 - 00:24:16	13 (0 / 13)
4865@s.whatsapp.net	30-07-2018 - 14:04:39	45 (12 / 33)
3316@s.whatsapp.net	13-07-2018 - 10:43:38	181 (109 / 72)
3174@s.whatsapp.net	12-07-2018 - 10:41:19	17 (3 / 14)
9579@s.whatsapp.net	11-07-2018 - 08:20:52	67 (21 / 46)
2009@s.whatsapp.net	11-07-2018 - 06:16:53	15 (3 / 12)
5349@s.whatsapp.net	09-07-2018 - 22:12:46	7 (1 / 6)
0995@s.whatsapp.net	30-06-2018 - 15:23:46	25 (11 / 14)
5378@s.whatsapp.net	27-06-2018 - 20:13:16	17 (13 / 4)
7257@s.whatsapp.net	27-06-2018 - 18:34:25	5 (3 / 2)
1867@s.whatsapp.net	26-06-2018 - 18:56:45	3 (2 / 1)
3627@s.whatsapp.net	26-06-2018 - 18:51:36	34 (5 / 29)
4390@s.whatsapp.net	26-06-2018 - 00:36:11	40 (18 / 22)
3009@s.whatsapp.net	23-06-2018 - 14:36:49	4 (1 / 3)
3932@s.whatsapp.net	17-06-2018 - 19:48:40	3 (3 / 0)
5986@s.whatsapp.net	12-04-2018 - 15:56:32	7 (0 / 7)
2511@s.whatsapp.net	12-04-2018 - 15:02:48	15 (0 / 15)
3695@s.whatsapp.net	17-03-2018 - 08:11:25	1 (0 / 1)
5719-1519648526@g.us	26-02-2018 - 18:05:26	2 (2 / 0)
5719@s.whatsapp.net	01-01-1970 - 05:30:00	0 (0 / 0)

```
WhatsApp Chat (918650162009@s.whatsapp.net)

29-03-2018
Maa aur naa mein ek farak hai ! Maa ke naa kehne se life sawme ke chance barr jate hein,.,., aur hamare naa kehne se life bigame ke chance barr jate hein..........from (Jitti).
29-03-2018 - 07:26:21

06-04-2018
Good morning, for all my friendsNENE
06-04-2018 - 06:12:37

13-04-2018
Hello, to all my friends.... I will never forget all of you.
13-04-2018 - 14:01:39

21-05-2018
Hello my all friends, and Relatives..
21-05-2018 - 17:08:16

22-05-2018
शुभ प्रभात सभी को मेरी ओर से... आपका दिन मंगलमय हो,, मेरी प्रभु से ये कामना है।
22-05-2018 - 08:08:41

28-05-2018
Hello! My all friend And seniors...
28-05-2018 - 19:28:31

30-05-2018
Hello! And Sweet Morning to all my friends and relatives and seniors...
☺
☺
☺
☺
☺
☺
30-05-2018 - 04:41:14

14-06-2018
hii
14-06-2018 - 20:29:44

15-06-2018
Hello ji kese jein aap sab log
15-06-2018 - 17:10:37

17-06-2018
Hello sir ji Good morning......
17-06-2018 - 03:18:10

18-06-2018
```

Total message count 862 (220 / 642)

Fig.8: WhatsApp chats extracted from the key

The image of the chip was further analyzed using the software Forensic Explorer (Fig. 9 and Fig. 10) through which contacts, call logs and SMS were exported.



ilter
2020 new (2) [Local Time]
ers (10)
rome Autofill (0)
rome Cookies (9)
rome Downloads (0)
rome FavIcons (0)
rome History (1)
rome Keyword Search Terms (
rome Logins (0)
rome Shortcuts (0)
rome Top Sites (0)
fari History iOS8 (0)
(4)
lendar Items Android (0)
l Logs Android (241)
ail Message Android (0)
ogle Maps Saved Places Andro

	Date (UTC)	Number	Name Col	Duration	Type	Country ISO	Geocoded Loca...	Lookup Uri	Matched Number	Normalized Number	Formatted Number	Message ID	Logtype	Contactid	Raw Contact
1	19-07-2018 07:05:12	IW-IDEA		0	Incoming	IN				494332	IW-IDEA	10	300	0	
2	01-01-2015 00:07:29	ID-HDFCSL		0	Incoming	IN				43433275		11	300	0	
3	14-06-2018 14:53:57	561619		0	Incoming	IN				561619	561619	5	300	0	
4	14-06-2018 15:02:28	+917248574865	akit	0	Incoming	IN		content://com.android...	+91 72485 74865	+917248574865	+91 724 857 4865	6	300	220	
5	17-06-2018 14:56:50	IDEAinfo		0	Incoming	IN				43324636	IDEAinfo	7	300	0	
6	26-06-2018 07:37:11	ID-IW-IDEA		0	Incoming	IN				43494332	ID-IW-IDEA	8	300	0	
7	26-06-2018 07:41:13	ID-Idea		0	Incoming	IN				434332	ID-Idea	9	300	0	
8	09-07-2018 05:52:08	+917534888316	D P	99	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
9	16-06-2018 13:36:05	+917534888316	D P	95	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
10	25-06-2018 12:23:42	+918937041485	love d p	939	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	657
11	15-06-2018 09:21:10	+917248574865	akit	91	Incoming	IN		content://com.android...	+91 72485 74865	+917248574865	+91 724 857 4865		100	220	221
12	26-06-2018 07:53:41	+917534888316	D P	90	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
13	26-06-2018 17:45:09	+918475019579		9	Incoming	IN	Chincholi, Karn...			+918475019579	+91 84 75 019579		100	0	
14	05-07-2018 04:08:51	+917534888316	D P	85	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
15	26-06-2018 09:54:26	+917534888316	D P	835	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
16	25-06-2018 11:27:49	+918937041485	love d p	83	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	657
17	09-07-2018 00:27:52	+917534888316	D P	81	Outgoing	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		500	1642	
18	13-06-2018 03:46:59	+917534888316	D P	80	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
19	15-06-2018 06:34:11	+917248574865	akit	79	Incoming	IN		content://com.android...	+91 72485 74865	+917248574865	+91 724 857 4865		100	220	221
20	23-06-2018 09:41:56	+917534888316	D P	73	Outgoing	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
21	25-06-2018 11:37:07	+918937041485	love d p	72	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	657
22	25-06-2018 11:35:10	+918937041485	love d p	71	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	657
23	11-06-2018 06:35:17	7534888316	D P	7	Outgoing	IN	Bhind, Madhya ...	content://com.android...		7534888316	75 34 888316		100	1048	15
24	24-06-2018 09:35:16	+917534888316	D P	664	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
25	19-07-2018 06:20:06	+919914007754		648	Incoming	IN	India			+919914007754	+91 99 14 007754		100	0	
26	19-07-2018 07:43:33	+917534888316	D P	64	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
27	19-07-2018 05:05:24	+917534888316	D P	62	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
28	24-06-2018 16:42:59	+917534888316	D P	583	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
29	25-06-2018 11:33:58	+918937041485	love d p	56	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	657
30	01-01-2015 00:01:21	+917534888316	D P	54	Outgoing	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
31	25-06-2018 11:30:33	+918937041485	love d p	53	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	657
32	24-06-2018 11:05:16	+918937041485	love d p	51	Outgoing	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	588
33	05-07-2018 18:12:04	+917534888316	D P	501	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
34	24-06-2018 07:10:45	+917534888316	D P	5	Outgoing	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
35	25-06-2018 11:32:34	+918937041485	love d p	48	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	657
36	30-06-2018 11:39:13	+917534888316	D P	465	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
37	01-01-2015 00:06:08	+919756540824	kirishna	458	Incoming	IN	India	content://com.android...		+919756540824	+91 97 56 540824		100	1188	1122
38	19-07-2018 03:46:00	+917534888316	D P	42	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
39	13-06-2018 04:19:49	+917534888316	D P	406	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
40	19-07-2018 04:50:01	+919927705223		40	Outgoing	IN	India			+919927705223	+91 99 27 705223		100	0	1396
41	24-06-2018 04:22:40	+917534888316	D P	39	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
42	27-06-2018 13:24:50	+918476870995	N K	39	Incoming	IN	Wadi, Karnataka	content://com.android...	+91 84 76 870995	+918476870995	+91 84 76 870995		100	814	815
43	24-06-2018 08:10:54	+918937041485	love d p	388	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	588
44	25-06-2018 18:01:17	+917534888316	D P	387	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
45	26-06-2018 08:14:43	+917534888316	D P	380	Incoming	IN	Bhind, Madhya ...	content://com.android...	7534888316	+917534888316	+91 75 34 888316		100	1642	
46	01-01-2015 00:02:08	+919927705223		380	Outgoing	IN	India			+919927705223	+91 99 27 705223		100	0	1327
47	15-06-2018 06:50:20	+918937041485	love d p	379	Incoming	IN	Chintapalle, An...	content://com.android...		+918937041485	+91 89 37 041485		100	1542	260

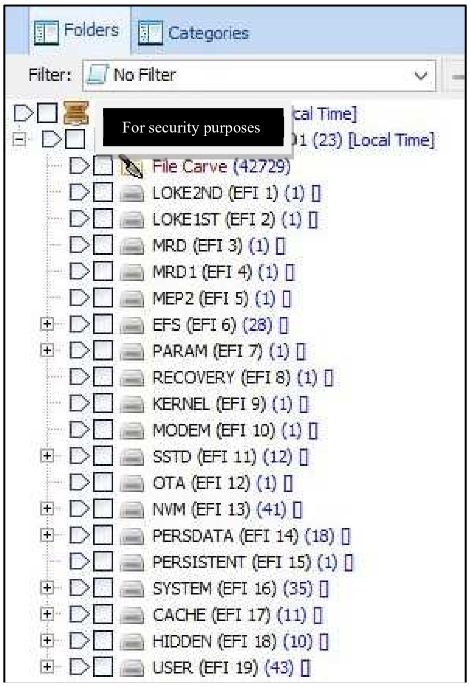
241 of 241 Visible [0 bytes]   1 Highlighted [0 bytes]   0 Checked [0 bytes]   Mobile\Call Logs Android\

Info

Property	Value	Raw Value	Type
Item Information			
Bookmarked	True	True	Boolean

0 of 268 Checked [0 bytes]   Mobile\Call Logs Android\

Fig.9: Data extracted from Forensic Explorer



For security purposes

cal Time]
1 (23) [Local Time]
File Carve (42729)
LOKE2ND (EFI 1) (1)
LOKE1ST (EFI 2) (1)
MRD (EFI 3) (1)
MRD1 (EFI 4) (1)
MEP2 (EFI 5) (1)
EFS (EFI 6) (28)
PARAM (EFI 7) (1)
RECOVERY (EFI 8) (1)
KERNEL (EFI 9) (1)
MODEM (EFI 10) (1)
SSTD (EFI 11) (12)
OTA (EFI 12) (1)
NVM (EFI 13) (41)
PERSDATA (EFI 14) (18)
PERSISTENT (EFI 15) (1)
SYSTEM (EFI 16) (35)
CACHE (EFI 17) (11)
HIDDEN (EFI 18) (10)
USER (EFI 19) (43)

Fig.10: Data type from Forensic Explorer

Every technique practiced are with its own challenges/ critical decisions. Similarly, there were several challenges faced as the examiner during the study. The primary challenge was the location and plucking of the chip from the mobile device. The mobile device was whole and intact when it was submitted in the laboratory due to which the optimum temperature and time for the back and front covers to detach was required to be regulated carefully. The optimum temperature was allocated at 310°C and the heating required to be intermittent in nature and a roving motion around the cover. Following that, the motherboard of the device was delicate and had to be skillfully removed from the connections. Later, the chip also had to be located and unsoldered with intermittent air heating from the socket of the motherboard.

Given the complicated extent of the chip-off method, no examiner should perform the technique on the intended device initially. The method must be duly practiced on demo devices before the actual procedure. Here, in the laboratory, before conducting the chip-off method on the submitted mobile device, practice for the same had been conducted on several demo devices of similar models. The practices are of utmost importance as they allow your hands to skillfully set for plucking the chip as well as in identifying and locating the chip in the device being examined.

4. CONCLUSION

The challenges of extracting data from mobile devices keep on evolving and surfacing steadily. In such scenarios, innovative ideas must be created and made functional to keep up with such challenges. As observed, the Chip-off method is one of the most innovative and distinctive methods to extract data from mobile devices when standard forensic tools are found inoperative. Several challenging circumstances are observed when mobile devices are received with password protection, especially when either the accused refuses to share the password or the victim is inaccessible (as seen here, in a suicide case). Moreover, this method is not only accessible for password locked phones but also for the devices that are damaged or in broken and non-working condition. However, the limitations of this method are observed when the mobile device received are of higher Android or IOS versions. The only data extracted from such mobile devices by chip-off method are found in an encrypted condition and methods of decryption are yet under development.

5. ACKNOWLEDGMENTS

The authors are thankful to Dr. S. K. Jain, Director & Chief-Forensic Scientist, DFSS, MHA, Govt. of India, Central Forensic Science Laboratory, Chandigarh for his valuable guidance and support throughout this research project.

REFERENCES

[1] C. Ence, J. R. Through and G. D. Cantrell, “Chip-off Success Rate Analysis comparing Temperature and Chip type,” The Journal of Digital Forensics, Security and Law, pp. 33-59, February 2019.

[2] S. O. Mikhaylov Igor, “Digital Forensic Corp in “CHIP-OFF TECHNIQUE IN MOBILE FORENSICS”,” 2016. [Online]. Available: https://www.digitalforensics.com/blog/chip-off-technique-in-mobile-forensics/.

[3] “https://www.teeltech.com/mobile-device-forensic-tools/forensic-explorer-2/#:~:text=Forensic%20Explorer%20is%20a%20tool,searching%2C%20previewing%20and%20scripting%20technology.,” [Online].

[4] S. O. Mikhaylov Igor, “]. Igor Mikhaylov, Oleg Skulkin, Digital Forensic Corp in “DECRYPTING ENCRYPTED WHATSAPP DATABASES WITHOUT THE KEY” via www.digitalforensics.com/blog/decrypting-encrypted-whatsapp-databases-without-the-key/,” 2018. [Online]. Available:]. Igor Mikhaylov, Oleg Skulkin, Digital Forensic Corp in “DECRYPTING ENCRYPTED WHATSAPP DATABASES WITHOUT THE KEY” via arwww.digitalforensics.com/blog/decrypting-encrypted-whatsapp-databases-without-the-key/.

[5] A. Fukami, S. Ghose, Y. Luo, Yu Cai and O. Mutlu, “Improving the reliability of chip-off forensic analysis of NAND flash memory devices,” Digital Investigation, pp. S1-S11, 2017.

[6] Y. Cai, "Error analysis and retention-aware management for NAND flash memory," Intel Technology, pp. 140-164, 2013.

[7] A. Jenenfey, "https://www.tenorshare.com/whatsapp-tips/how-to-read-encrypted-whatsapp-messages-on-andHow to Read Encrypted WhatsApp Messages on Android Without Keys". Via blog," [Online].