International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2173156

Forensic Analysis of Broken and Damaged Mobile Phone – A Crime Case Study

Akhlesh Kumar[1], Bhushan Ghode[2], Khevna Maniar[2], Dr. S. K. Jain[3]

[1]Assistant Director & Scientist - 'C', Central Forensic Science Laboratory, DFSS, MHA, Govt. of India, Chandigarh, India

[2]Forensic Professional, Central Forensic Science Laboratory, DFSS, MHA, Govt. of India, Chandigarh, India

[3]Director-cum-Chief Forensic Scientist, Central Forensic Science Laboratory, DFSS, MHA, Govt. of India, Chandigarh, India

Article Info
Volume 7, Issue 3
Page Number: 481-487

Publication Issue :
May-June-2021

Article History
Accepted : 12 June 2021
Published : 20 June 2021

ABSTRACT

Forensic laboratories are frequently subjected to mobile devices that are assailed by shock or forced damage which might be the result of intentional efforts to destroy proof from the devices or accidental exposure. Chip-off technique is an effective method for data retrieval from such kind of exhibits. However, nowadays all mobiles phones are securely encrypted with full disk encryption (FDE) or file-based encryption (FBE) which makes chip-off forensics an improbable process to successfully retrieve data. In many of these cases, the encryption is on the hardware and hence, the device could be successfully decrypted by bringing it in its original condition. Thus, the original user data can be obtained for investigative purposes. This process can be enabled by replacement of electronic parts of the original device which contains user data and decryption keys i.e. PCB to the new host. This research paper covers a case study of a mobile phone obtained in broken and shattered condition whose diagnosis of PCB and subsequent actions led to data recovery.

Keywords : Full Disk Encryption, File Based Encryption, Decryption, PCB, broken & damaged mobile phone, UFED Touch 2 and Physical Analyzer, forensic repair toolkit.

I. INTRODUCTION

Today's world is an era of accelerated technological progress characterized by new innovations whose rapid application and diffusion typically cause an abrupt change in society. The evolution of computer, mobile, networks, the devices that run on them and their everyday services occur at an amazing rate. It is unthinkable to consider our lives without mobile phones. Mobile phones have been one of the most successful technologies ever invented and adopted in the ever-developing world. Apart from making everyday life easy, mobile phones, computers and internet are most common weapons used by criminals to commit heinous crimes (McSweeney, 2020). These weapons are commonly collected evidences in cybercrimes that are examined by investigators. Sometimes criminals intentionally damage their mobile phones and computers to destroy the evidence. Therefore, it's becoming more challenging for an investigator/ examiner to extract data from the evidences (Dongan & Akbal, 2017).

Moreover, as the technology is rapidly increasing, mobile devices are also advancing daily making the data more secure as the operating system gets an upgrade (OS or MAC software upgrade) or a new security patch update. Full-Disk Encryption and File-Based Encryption makes mobile devices stronger against extraction of data via Chip-off and JTAG. Hence, examination of such evidences is required to be done using hardware and software tools to directly access the memory of device. The purpose of this study is to understand the encryption types and process a method for achieving data extraction from encrypted devices.

Disk encryption is a technology that protects information by converting it into an unreadable code that is challenging for unauthorized access to decipher. Disk encryption takes every bit of data stored on a disc or disc volume and converts it in an encrypted format using software or hardware-based disk encryption. This prevents unauthorized people from accessing data storage. The term Full disk Encryption is self-explanatory in stating that the whole disk is encrypted. The entire disk along with its user data and files as the main data gets stored in user data partition using an encrypted key on any Android device (Android, 2021). Once a device is encrypted, all user-created data is automatically encrypted before committing it to disk. Although, all the data is read in an automatically decrypted way before returning it to the calling process, since the device/ disk is encrypted, entire data is gathered in an encrypted format.

Several devices possessing Android 7.0 and higher support file-based encryption (FBE). File-based encryption allows different files to be encrypted with different keys that can be unlocked independently rather than encrypting the entire disk with one singular key. Users need to provide credentials before any data can be accessed, preventing the phone from performing all but the most basic of operations. For example, if the device was supporting file-based encryption, user credentials would be required to access simple tasks of alarms or receiving phones. If the user credentials are not entered, alarms would not operate, accessibility services would be unavailable, and calls could not be received except for the basic emergency dialer operations (Android, 2021).

The hardware of the mobile device is intricately formed and several components make it into a functional device. If any of these components were damaged, the mobile device would fail to function. An electrical failure due to a short circuit in the motherboard can shut the device abruptly. A short circuit is an abnormal connection between two nodes of an electric circuit intended to be at different voltages. This results in an electric current limited only by the therein equivalent resistance of the rest of the network which can cause circuit damage, overheating, fire or explosion (Wordpress, 2020). It might be due to touching of two nodes or a resistance created between connected nodes. This leads to a circuit failure that can be seen in PCB short-circuiting.

The investigating officers had seized 4150 grams of smuggled gold from an Innova car occupied by three people. The said three people were arrested. During investigation, two more people were arrested. The five people had voluntarily surrendered their mobile phones for investigation purposes. During interrogation, before the mobile could be analyzed (Samsung Galaxy Note 10 plus), the owner of the mobile threw the device at wall to break it in a planned attempt to destroy evidence. The directorate collected the broken pieces safely and sent it to the laboratory for forensic examination of the device to try for an alternative method for data retrieval.

The Forensic Science Laboratory in Chandigarh received one broken and damaged mobile phone (Samsung, Model: SM-N975F/DS) with chipset-Exynos 9825 (Fig.1), forwarded by investigation authority in a condition where it was unable to boot or be charged. The chip-off technique was not suitable to retrieve the data of the exhibit due to the higher Android version, which might extract the data in an encrypted form. When a closer look was taken at the motherboard, it was found that the motherboard was in good condition as all its parts were appropriately located (Fig.2). The device was reassembled and kept for charging. However, no sign or indication of charging was observed. The device was disassembled and a closer look was taken at the PCB. The preliminary examination of the PCB board showed a short circuit in its internal side.

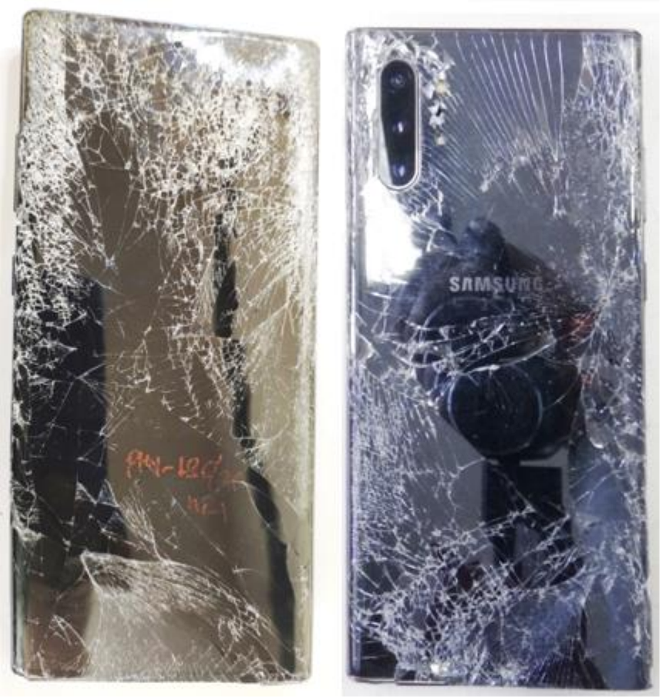


Fig. 1: Damaged Samsung Mobile Phone as delivered to the laboratory

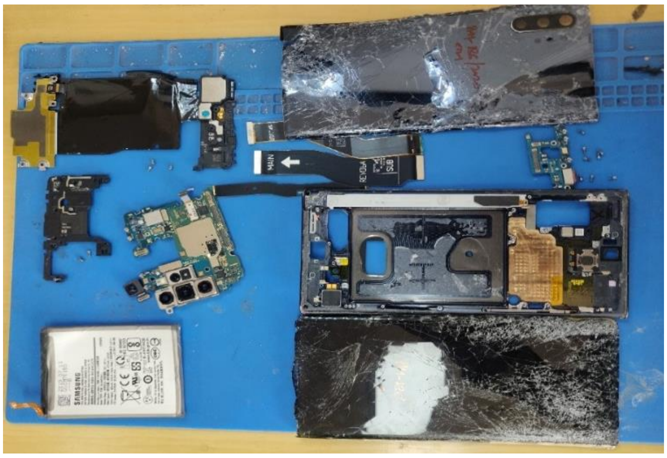


Fig. 2: Parts of the Damaged Mobile Phone after Disassembling the Device

The mobile phone (Fig.3) (Wiens & 19 other contributors)Samsung, Model: SM-N975F/DS, had two layered motherboard, like a silicon sandwich (Fig.4) (Wiens & 19 other contributors). This mobile device was then repaired using the forensic repair tool kit that restored the device in its working condition and data extraction became possible

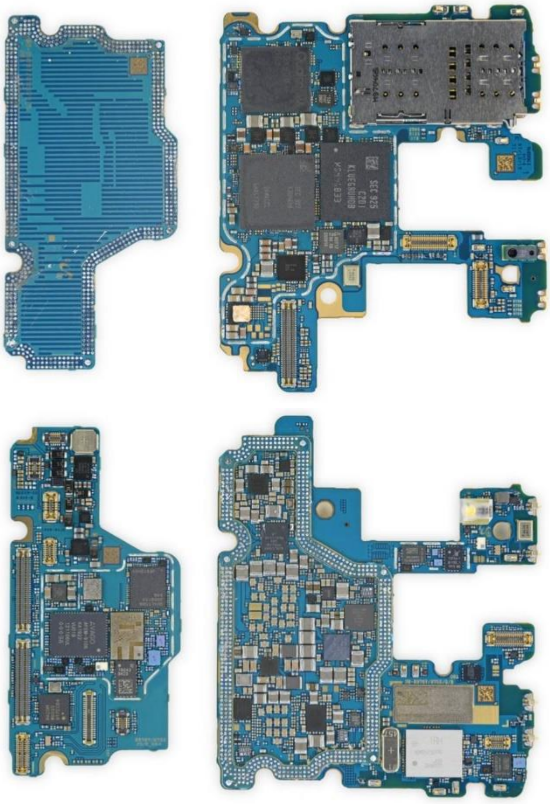


Fig. 3: Structure of a PCB

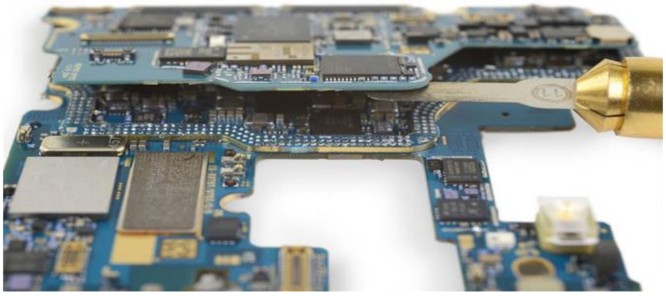


Fig.4: Silicon- Sandwich look of PCB Internally

II. METHODS AND MATERIAL

The materials employed for repairing of the device are readily available in a forensic repair tool kit including the screws, screw removers, forceps, brushes, cleaners, etc.

1. Step wise procedure followed by the study:

Whenever any mobile phone is subjected to data extraction, standard laboratory procedures and standard hardware/software are utilized. For this study, we have used forensic repairing Tool Kit and Universal Forensic Extraction Device by Cellebrite.

1.1 Case opening:

The case was received from a messenger in sealed condition. The parcel was appropriately marked. The parcel contained one mobile phone of Samsung, Model: N975F/DS (in Broken and Damaged condition). The mobile phone was appropriately marked/ tagged for identification.

1.2 Manual/ Physical Examination:

As the device was found in damaged condition, the device was physically examined with the help of a microscope after examining through naked eyes. The device was taken apart, into pieces by unscrewing it. Except motherboard every part of the device was damaged i.e. the screen, back panel, screen parts, etc. were all broken. Data extraction was possible for this mobile device by repairing it. Hence, materials for repairing were required. New screen combo was purchased for the device and all the parts of the exhibit were transplanted and installed with the new screen combo. The mobile phone was kept for charging but it showed no indication for the process. Hence, a look at PCB was taken as the theory pointed towards a possible PCB short-circuiting.

1.3 Diagnosis of short circuiting:

For detection of short circuiting a digital or analog multi-meter is needed as DC power supply cannot detect the small shorts from the PCB. (Wordpress, 2020)

Step one: Set multimeter on CONTINUITY buzzer for an analog multimeter which is set on x1 Ω (ohm).

Step two: Connect the Red probe to Circuit's battery connector plus (+) and Black probe to minus (-) meter. Check the reading. It should show no reading.

Step three: Check the opposite Connection- the Red probe to battery connector minus (-) and Black probe to plus (+) connector. Check the reading again. The multimeter shows some reading.

Usually, Digital Multimeter shows a reading between 300- 600. If the multimeter shows reading on both sides on the battery connector of the phone board PCB, it means the circuit has shorted.

For this device, the multimeter showed a reading for both the connecting sides. Once the motherboard was discovered in a short condition, detection of the location of short-circuit was essential. Soldering paste's/ chemical's liquid fumes were blown to surround the PCB in a layer and current was passed through the formed layer. As the current passed, one area was blackened. Thus, the area of the short-circuit was located on the PCB. Although, as the device had a silicon sandwich structure, the heavy pressure had sandwiched the parts and were found touching at a point.

Removing Shorting:

The silicon sandwich with the help of a hot air gun and glue cleaner was opened. Then, the touching part of the sandwiched silicon structure was covered with an insulating material and repacked.

1.4 Transplantation of motherboard and other parts:

New screen combo of the device had been purchased and all the parts of the exhibit were transplanted and installed into the new screen combo (Aya Fukami, 2019). Now, as the device was connected to a charger, the charging indication was observed. Later, when the device was fully charged, the device was rebooted and it was found to be pattern locked. The password was provided by forwarding authority and finally, the mobile device was accessible. The device was working correctly with all the sensors.

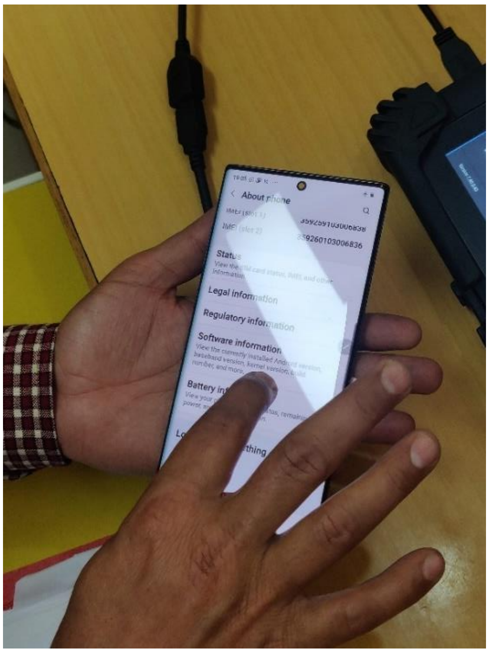


Fig. 5. Device rebooted and working fine

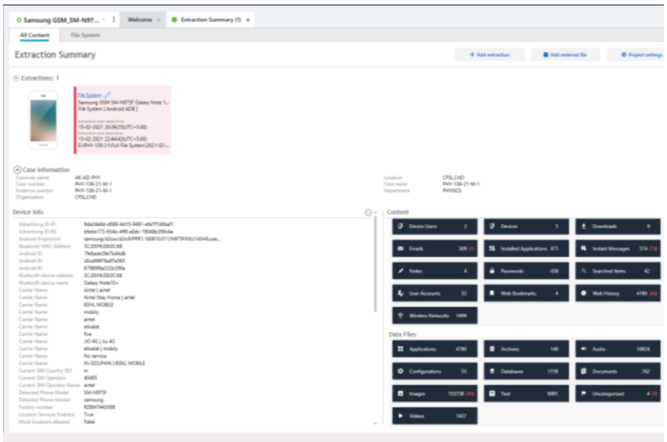
1.5 Extraction of data:

The device once opened with the pattern provided by the forwarding authority, it was immediately kept on airplane mode. Furthermore, USB debugging was enabled and other necessary settings to enter the extraction mode were followed. Using the Universal Forensic Extraction Device Touch-2 (UFED-2, Version-7.42) (Cellebrite), the device was kept for data extraction. The UFED Touch-2 extracted data was then further kept for analysis using the software Physical Analyzer, Version-7.42.

Fig. 6. Mobile Device analyzed using the UFED Touch-2-7.42

III. RESULTS AND DISCUSSION

The extracted data comprised of contacts, call logs, messages, multimedia artifacts (images, videos, documents, etc.), internet browsing history and application data of social media accounts including WhatsApp, Facebook, Telegram, etc. (Fig. 7). This entire data was provided to the case forwarding authority along with a hard-copy report.



Extraction Summary

Extractions: 1

File System
Samsung GSM SM-N975F Galaxy Note 1...
File System [Android ADB]
Extraction start date/time
15-02-2021 20:39:25(UTC+5:30)
Extraction end date/time
15-02-2021 22:44:42(UTC+5:30)
E:\PHY-136-21\Full File System\2021-02-...

Case Information

Examiner name	AK-AD-PHY	Location	CFSL CHD
Case number	PHY-136-21-M-1	Case name	PHY-136-21-M-1
Evidence number	PHY-136-21-M-1	Department	PHYSICS
Organization	CFSL CHD		

Device Info

Advertising ID #1	9da24a8d-d088-4d15-9481-efa7f7d0baf1
Advertising ID #2	b4ebb173-654b-4f48-a0dc-19048b390c4a
Android fingerprint	samsung/d2xxx/d2s:9/PPR1.180610.011/N975FXXU1ASH6:use...
Bluetooth MAC Address	3C:20:F6:D8:0C:68
Android ID	7fe8ade28e7b44d8
Android ID	c8ca89978a07e565
Android ID	6798f98a532b399e
Bluetooth device address	3C:20:F6:D8:0C:68
Bluetooth device name	Galaxy Note10+
Carrier Name	Airtel | airtel
Carrier Name	Airtel Stay Home | airtel
Carrier Name	BSNL MOBILE
Carrier Name	mobily
Carrier Name	airtel
Carrier Name	etisalat
Carrier Name	five
Carrier Name	JIO 4G | Jio 4G
Carrier Name	etisalat | mobily
Carrier Name	No service
Carrier Name	IN-DOLPHIN | BSNL MOBILE
Current SIM Country ISO	in
Current SIM Operator	40485
Current SIM Operator Name	airtel
Detected Phone Model	SM-N975F
Detected Phone Vendor	samsung
Factory number	RZ8M7443X8E
Location Services Enabled	True
Mock locations allowed	False

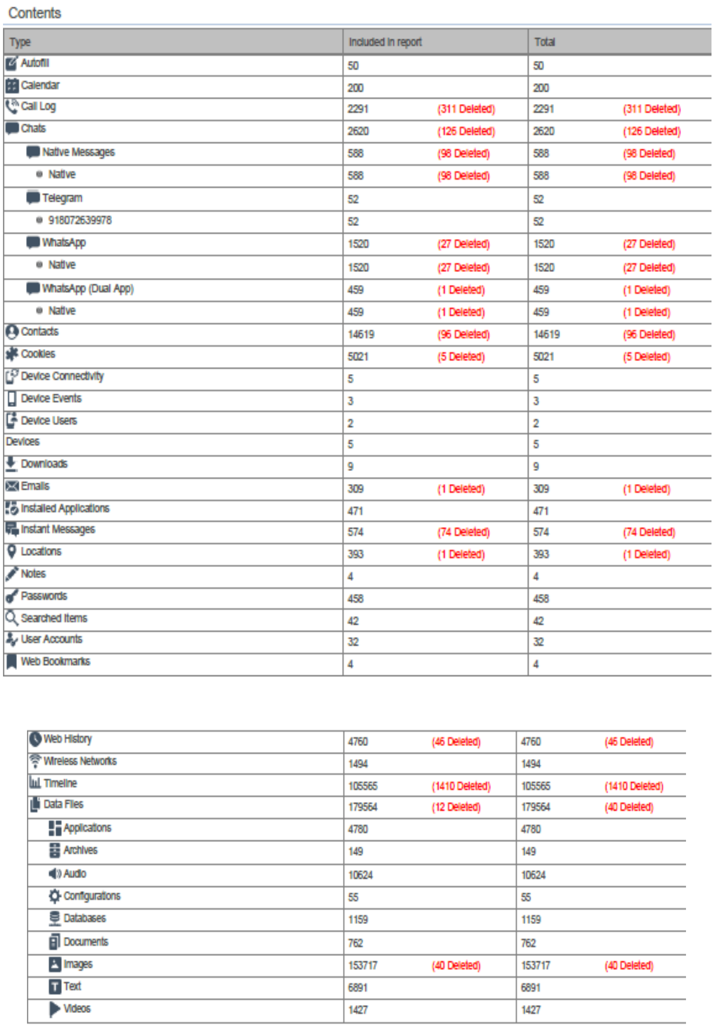
Content

Device Users	2	Devices	5	Downloads	9
Emails	309 (1)	Installed Applications	471	Instant Messages	574 (74)
Notes	4	Passwords	458	Searched Items	42
User Accounts	32	Web Bookmarks	4	Web History	4780 (48)
Wireless Networks	1494				

Data Files

Applications	4780	Archives	149	Audio	10624
Configurations	55	Databases	1159	Documents	762
Images	153738 (40)	Text	6001	Uncategorized	4 (4)
Videos	1427				

Fig. 7: Extraction Summary of the Mobile Device from UFED, Touch-2



Contents

Type	Included in report		Total	
Autofill	50		50	
Calendar	200		200	
Call Log	2291	(311 Deleted)	2291	(311 Deleted)
Chats	2620	(126 Deleted)	2620	(126 Deleted)
Native Messages	588	(98 Deleted)	588	(98 Deleted)
Native	588	(98 Deleted)	588	(98 Deleted)
Telegram	52		52	
918072639978	52		52	
WhatsApp	1520	(27 Deleted)	1520	(27 Deleted)
Native	1520	(27 Deleted)	1520	(27 Deleted)
WhatsApp (Dual App)	459	(1 Deleted)	459	(1 Deleted)
Native	459	(1 Deleted)	459	(1 Deleted)
Contacts	14619	(96 Deleted)	14619	(96 Deleted)
Cookies	5021	(5 Deleted)	5021	(5 Deleted)
Device Connectivity	5		5	
Device Events	3		3	
Device Users	2		2	
Devices	5		5	
Downloads	9		9	
Emails	309	(1 Deleted)	309	(1 Deleted)
Installed Applications	471		471	
Instant Messages	574	(74 Deleted)	574	(74 Deleted)
Locations	393	(1 Deleted)	393	(1 Deleted)
Notes	4		4	
Passwords	458		458	
Searched Items	42		42	
User Accounts	32		32	
Web Bookmarks	4		4	
Web History	4760	(46 Deleted)	4760	(46 Deleted)
Wireless Networks	1494		1494	
Timeline	105565	(1410 Deleted)	105565	(1410 Deleted)
Data Files	179564	(12 Deleted)	179564	(40 Deleted)
Applications	4780		4780	
Archives	149		149	
Audio	10624		10624	
Configurations	55		55	
Databases	1159		1159	
Documents	762		762	
Images	153717	(40 Deleted)	153717	(40 Deleted)
Text	6891		6891	
Videos	1427		1427	

Fig.8: Contents of the Mobile Device in Report from Physical Analyzer.

A comprehensive amount of relevant information consisting of call logs, contacts, WhatsApp chats, SMSs and location was collected from the mobile device and provided to the authority (Fig. 8). The locations from the mobile device enabled the authorities to track the movement of the smugglers from Abu Dhabi, Saudi Arabia to New Delhi, India on the same date and time as the smuggling plans (Fig. 9). This increased the evidence against the suspects regarding their devised plans including their movement, location and path taken.

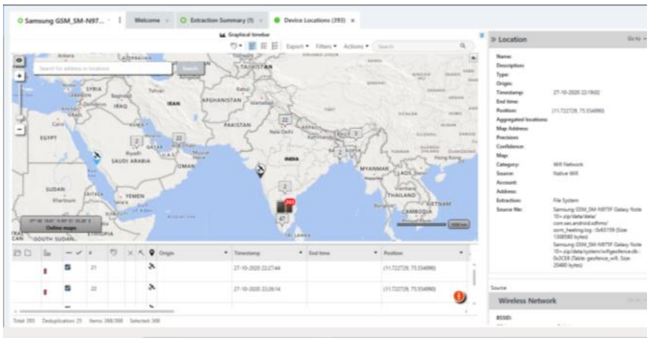


Fig.9: Location trace from Abu Dhabi to New Delhi with time and date

The ultimate obstacle in the cases of damaged and broken mobile devices is to efficiently locate the damage and the reason for the non- working condition of the device. A thorough knowledge of the working of the mobile devices is essential to gather such information. The following challenge is observed when the damaged devices need to be repaired intricately. However, in this case, the replacement of the screen combo parts and transplantation of the PCB board led to the successful restoration of the device and complete data extraction in a forensically sound manner.

IV. CONCLUSION

In the beginning of the case, the forwarding authorities were stumped by the ingenious planning of the smugglers who had left no clues behind that could directly connect them to the crime. The suspects had already managed to destroy any implicating evidence of the crime and had even tried to destroy their mobile devices. However, the innovative and industrious efforts of the scientific officers of the case enabled a complete restoration of the mobile device. The forwarding authority's invaluable support by providing the password and an intricate work in repairing the device by the scientific officer led to the successful solution of the case. This helped the authorities to convict the suspects and provided corroborative evidence of the crime.

V. ACKNOWLEDGMENTS

The authors are immensely grateful to Sh. Vinay Kumar Sahu, Surbhi Telecom, Sector-22, Chandigarh for sharing his knowledge, experience and providing technical support during course of the investigation.

VI. REFERENCES

[1]. Android. (2021, 04 27). Android Open Source. Retrieved from source.android.com: https://source.android.com/security/encryption/full-disk

[2]. Android. (2021, 05 20). Android Open Source. Retrieved from source.android.com: https://source.android.com/security/encryption/file-based

[3]. Aya Fukami, K. N. (2019, July). Forensic Analysis of Water Damaged Mobile Devices. Digital Investigation, Volume 29, S71-S79. Retrieved from https://www.sciencedirect.com/science/article/pii/S1742287619301586

[4]. Cellebrite. (n.d.). Retrieved from https://www.cellebrite.com/en/home/?utm_campaign=sf258976&utm_medium=Paid-Search&utm_source=adwords&utm_content=Homepage&gclid=Cj0KCQjw5auGBhDEARIsAFyNm9G1yI9GYpflulSqzAQI2hIVG4_lQjNFCXPc8ENgWuJ4Rwrc6osrEYUaApNwEALw_wcB

[5]. Dongan, S., & Akbal, E. (2017, July 13). Analysis of mobile phones in digital forensics. Retrieved from ieeexplore.ieee.org: https://ieeexplore.ieee.org/document/7973613

[6]. McSweeney, K. (2020, January 31). Burn, drown, or smash your phone: Forensics can extract data anyway. Retrieved from www.zdnet.com: https://www.zdnet.com/article/burn-drown-or-smash-your-phone-forensics-can-extract-data-anyway/

[7]. Wiens, K., & 19 other contributors. (n.d.). IFIXIT. Retrieved from www.ifixit.com: https://www.ifixit.com/Teardown/Samsung+Galaxy+Note10++5G+Teardown/125590

[8]. Wordpress. (2020, March 28). Phone Repairing Solutions. Retrieved from phonerepairingsolutions.com: https://phonerepairingsolutions.com/phone-board-pcb-short-circuit-repair/

Cite this article as :

Akhlesh Kumar, Bhushan Ghode, Khevna Maniar, Dr. S. K. Jain, "Forensic Analysis of Broken and Damaged Mobile Phone - A Crime Case Study", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 3, pp. 481-487, May-June 2021. Available at doi : https://doi.org/10.32628/CSEIT2173156
Journal URL : https://ijsrcseit.com/CSEIT2173156