Data Extraction on Damaged Mobile Device: A Forensic Case Study

Surajit Paul[1], Binoy Das[2], Debaraj Rana[3]

[1] Department of EC, NIELIT Agartala, Tripura, India,
surajit@nielit.gov.in

[2] Department of CSE, NIELIT Agartala, Tripura, India,
erbinoy@nielit.gov.in

[3] Department of EC NIT Meghalaya, Shillong
p21ec007@nitm.ac.in

***Abstract*:**
Data extraction from damaged mobile phones is essential in digital forensics and recovery. Mobile phones have become essential to modern life and contain a wealth of personal, financial, and confidential information. However, accidents, hardware failures, and other mishaps can damage our phones and make it difficult to access the stored data. Forensic laboratories are regularly faced with mobile phones being exposed to damage that can be the outcome of purposeful attempts to abolish device data permanently. This article will cover an essential case study of a mobile device seized in a damaged or broken condition whose analysis of the circuit board and consequent actions led to getting vital evidence from it. This article examines the various processes of data extraction from nonworking mobile phones that could become vital evidence on that mobile device. Also, this discussion will highlight emerging technologies and their impact on dead or damaged phones based on the extracted evidence.

***Keywords*: Mobile forensics, JTAG, Chip off, JTAG, Chip-Off, data extraction, data description.**

(Article history: Received: Oct 31,2023 and accepted Jan, 31,2024)

I. INTRODUCTION

Mobile phones have become one of the essential devices in today's date, which contain a wealth of personal, confidential, and potentially damning information. However, these devices are not immune to accident, damage, or intentional destruction that may prevent access to your data. Criminals may damage mobile phones to destroy evidence. They could also break cell phones, shoot, hide, and cook. [1]. Forensic analysis of broken or damaged mobile phones plays a key role in extracting, preserving, and interpreting evidence from these devices, supporting investigations in various legal, criminal, and civil situations. These artilleries are frequently collected as digital evidence in the investigations of cybercrimes. Criminals may intentionally damage cell phones or computers to destroy evidence.

The paper additionally delves into the felony and moral concerns surrounding information extraction from broken cell telephones. It highlights the significance of adhering to privacy rules and acquiring the proper consent while accomplishing information healing procedures. Furthermore, case research is provided to demonstrate real-international situations in which information extraction from broken cell telephones performed a vital function in investigations, crook proceedings, and catastrophe healing efforts. These instances underscore the importance of well-timed and correct information retrieval from broken devices [2].

In conclusion, information extraction from broken cell telephones is a complicated and evolving discipline with implications for virtual forensics, regulation enforcement, catastrophe response, and private information healing. This paper serves as a complete manual for researchers, practitioners, and policymakers, imparting insights into the methodologies, challenges, and moral concerns related to this critical process. As generation continues to advance, the strategies and gear for information extraction from broken cell telephones will likely retain to evolve, necessitating ongoing studies and innovation in this place.

II. Memory And Storage Of The Mobile Phone

Mobile phones have non-volatile internal memory, which is used to store the phone's operating system. There are types of non-volatile memory named NANO and NOR are used in the mobile phone. The memory density of NANO flash is higher than the NOR flash memory; typically, the capacity ranges from 1 GB to 16 GB. The cell size of NANO flash is much smaller and has faster data transfer speeds than NOR flash memory [3]. The drawbacks of NANO flash are lower read speed and random access of memory is not allowed. Execution of data in NANO code is done by content hiding on RAM.

Most modern mobile phones are equipped with Embedded Multi Media Card (eMMC). The architecture of eMMC consists of memory and its controller on a common silicon chip. Therefore, the interface design becomes less complex. Apart from internal and external storage, it required a Subscriber Identity Module (SIM) card from the respective service provider. SIM cards also have a small storage capacity, which is very important from the cyber forensic point of view. The primary use of a SIM card is actually to communicate with the nearest mobile network. Usually, the SIM cards have a storage capacity of 32 to 128 KB. However, according to current market trends, the storage capacity of SIM cards is between 512MB and 1GB.

III. Mobile Phone Data Extraction Process

Extraction of data from phones is highly dependent on brand, model, and operating system. Many researchers have developed many frameworks and processes to restructure the mobile forensics process. But practically, these frameworks or methodologies are not fixed for any particular case. In mobile forensics, data acquisition requires logical and physical extraction of the mobile handset. Data can be extracted from working mobile by Logical extraction, which is reliable and fast. However, it cannot extract all data and can be manipulated during the extraction process. Deleted files cannot be retrieved in this process. The mobile data extraction process can be categorized into five different types, as shown in Table 1.

Table 1: Forensics Data Acquisition Methods [4]

Process	Method	Advantages	Disadvantages
I	Manual Extraction	• Doesn't require much specialized knowledge. • Less complex. • Less cost • Works with all brands and models of mobile phones.	• data manipulation threats • Deleted files cannot be retrieved. • If the equipment is damaged, it cannot be used.
II	Logical Extraction	• Low technical expertise is required. • Software-generated reports in standard formats.	• Data tampering threats • Threats in data Accessibility.
III	Joint Test Action Group (JTAG) process	• Less damaged mobile data can be extracted. • Bit-to-bit data extraction, including deleted data.	• Data decryption complexity. • We do not guarantee access to all storage areas.
VI	Chip-off	• Bit-to-bit data extraction	• Risk of chip damage • More Technical skill is required. • Report Format is not standard.
V	Micro read	• Destructive methods. • Very expensive. challenging. • Difficult to interpret and translate.	• Risk of permanent damage • sophisticated. • There is no standard report format.

IV. Mobile Phone Data Extraction Process

Mobile forensic detection techniques are very complicated compared to any other cyber forensic method. By Logical extraction methods, data extraction is possible for working mobile devices. But if the mobile device is damaged or not working in this scenario, physical extraction is essential to retrieve the data from the phone.

In this study, we will observe whether the manual or physical collection techniques are appropriate for data extraction from damaged mobile phones. This article introduces three possible data collection approaches to extract bit-to-bit data from a damaged mobile phone.

i. ISP and Flashing device.
ii. Chip-OFF Method.
iii. JTAG principle

A. ISP and Flashing device.

It is the easiest and most convenient way to extract mobile flash data using a small hardware interface. Simple software is used to extract all data from the target mobile. However, there is no particular approach to collecting data from any mobile phone, as each embedded system may have proprietary hardware to store data on the mobile memory chips. Most of the time, this method is used for bypassing mobile passwords and getting memory access. It consists of hardware devices, software, and drivers that execute low-level data capture of mobile data stored in the phone's memory. This method is not very popular in the digital forensics community as it has fooling drawbacks.

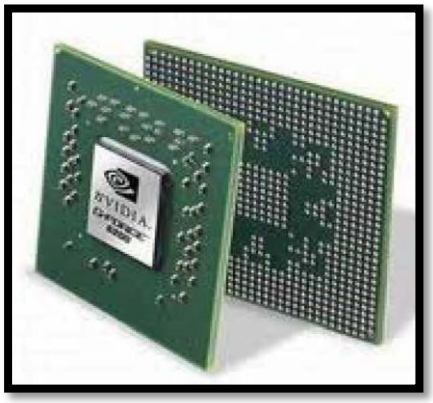
- Risk of data manipulation
- Dependent on hardware architecture.
- Less data security.

B. Chip-OFF Process:

Chip-off technology is an advanced data extraction and analysis technique that uses specialized equipment to remove chips from a specific device and collect data. Chip-off technology can be used in smartphones and other digital devices that use flash memory technology to store data (Digital Forensic Corp, 2018). Chip-off systems have had some success with devices that are physically damaged and inoperable. Chip-off is an invasive forensic collection tool that requires specialized technical tools and experts to reliably remove the chip, create a forensic image of its contents, and convert its contents into coherent data. Removing the chip from the machine requires precise skill. Even a small mistake will result in permanent loss of all your data. After removing the chip, connection to the system is carried out using a smartphone adapter [6].

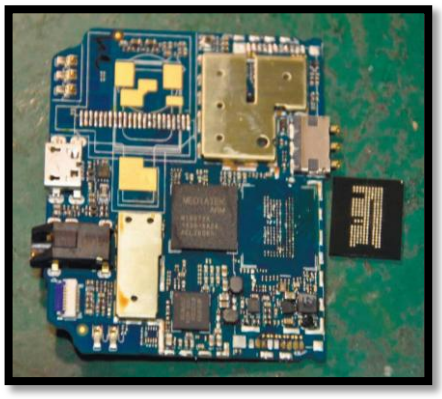
Desoldering the chip is the most important part of the chip-off process. Make sure the chip does not overheat. If it does not overheat, all data will be deleted. We recommend using converted stations. Even the best retrofitting stations with automatic temperature controllers can safely desolder chips. To remove the chip, we recommend heating it to 240 degrees Celsius and then using a blade to remove it from the smartphone board [7]. The removed circuit board contains non-volatile NAND memory, and the microchip is physically removed using appropriate heat and chemicals. The physically removed chip is cleaned and then forensically performed on the chip using various imaging software such as Oxygen Forensics, XRY, Belkasoft, Magne Forensics, Autopsy, and the desired smartphone kit adapter connected to the PC. An image/dump will be captured. Using available software, detailed analysis is performed, and valuable artifacts are retrieved from the chip [8].

a. Difficulties in using chip-off technology [9].
b. Specific micromemory circuits require their own expertise.
c. Once the memory chip is soldered, it cannot be returned to its original position.
d. If the circuit board overheats while soldering the memory chips during power-up, there is a risk that the device's circuit board will disintegrate and become completely inoperable.
e. Chip-off programmers are expensive, and not all specialized departments can afford programmers that work with all types of memory chips.



BGA

Desoldering Kit



Chip De-solder

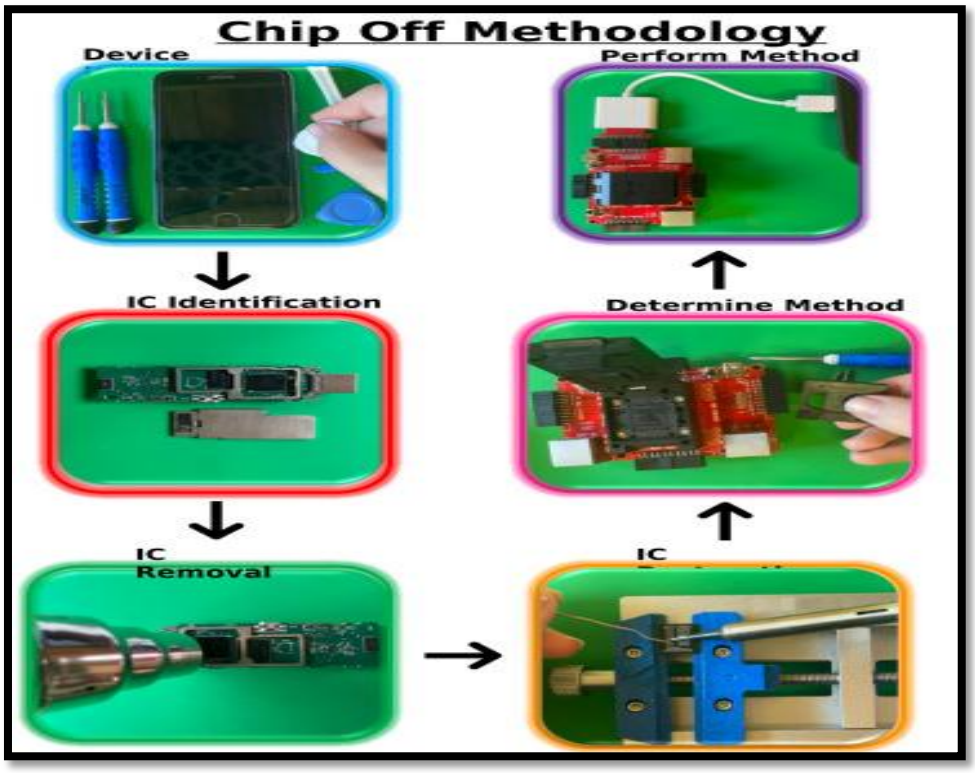


Fig. 1. The chip-off process

C. JTAG Test Access Port Process:

JTAG is a bodily information acquisition approach that connects to TAPs (Standard check get entry to ports) on a tool to switch the uncooked information to the related hardware immediately from the reminiscence chips [11].

Advantages:

- Bit-to-bit data extraction
- Compared to the Chip - off method, it is a non-destructive process.
- Not require any PIN codes or passwords for data access.
- Extraction from broken or damaged mobile
    - Liquid
    - Thermal
    - Structural

1) Extraction Process steps:

Four steps to data extraction from a damaged mobile device with the JTAG process are:

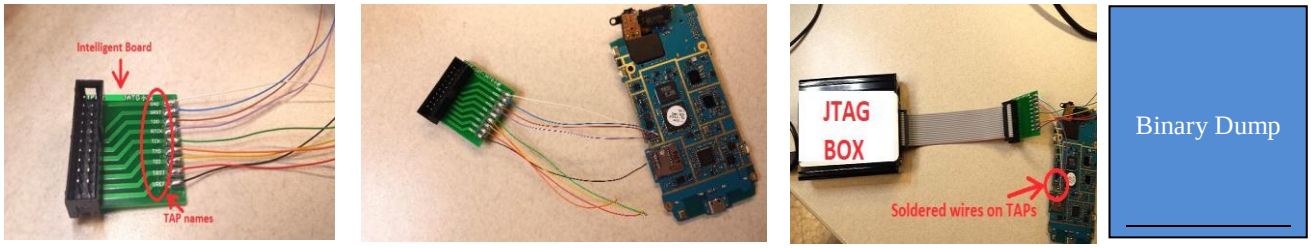


Fig. 2. Extraction Process steps

a) Step-1: JTAG connection pins identification:

Identification of JTAG pin to interface signal can be very sophisticated and complex. Because the hardware manufacturer can sometimes hide or disable the JTAG interface. Therefore before starting any research in this area, First ensure the JTAG pin and interface through which the communication will be performed. Sometimes JTAG pins are hidden by a capacitor or Battery. There are different standard JTAG connectors like 2x10, 2x8, 2x7, 2x5, etc are available. So before starting the process, first download the ta datasheet to find out JTAG pins and check the connection using a Digital multimeter, CRO, and Logical analyzer. Commonly used tools for JTAG are Devices such as the Easy JTAG Box, Medusa Pro, etc.

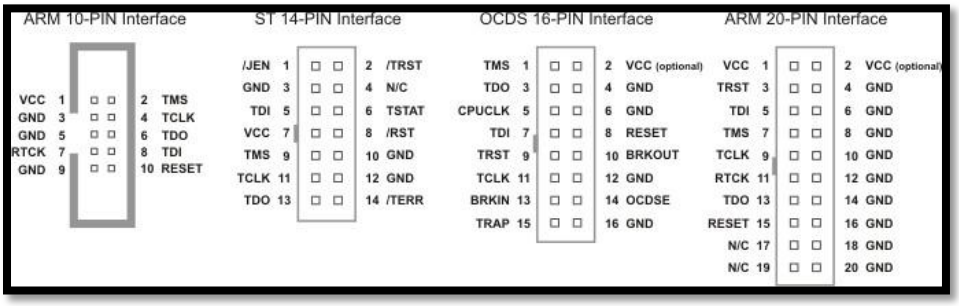
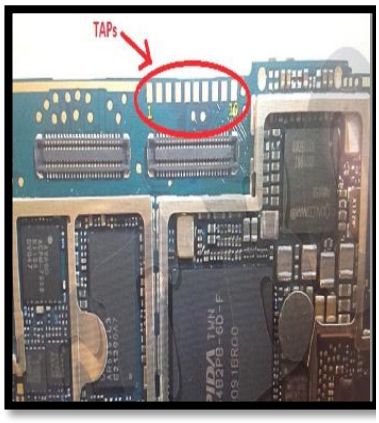
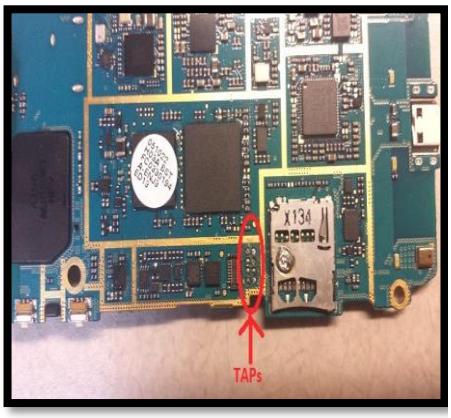


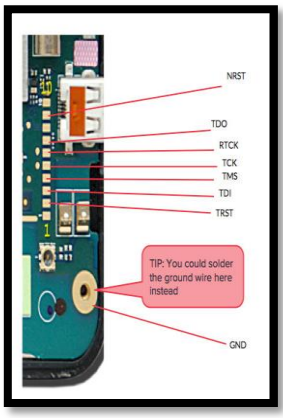
Fig.3. Pinout of different interface [14]



JTAG TAPs



JTAG TAPs



JTAG IDs

Fig. 4. Pins identification

b) Step 2: Verify communication with the JTAG interface.

After identification of JTAG pins, one can begin communication with the help of the JTAG interface. This process required two elements:

1. Software for JTAG communication
2. JTAG Converter/Adapter.

JTAG converter is used for physical connection between the JTAG interface and PC via USB interface. Communication software is used for data transmission between JTAG interface via JTAG Adapter [14].

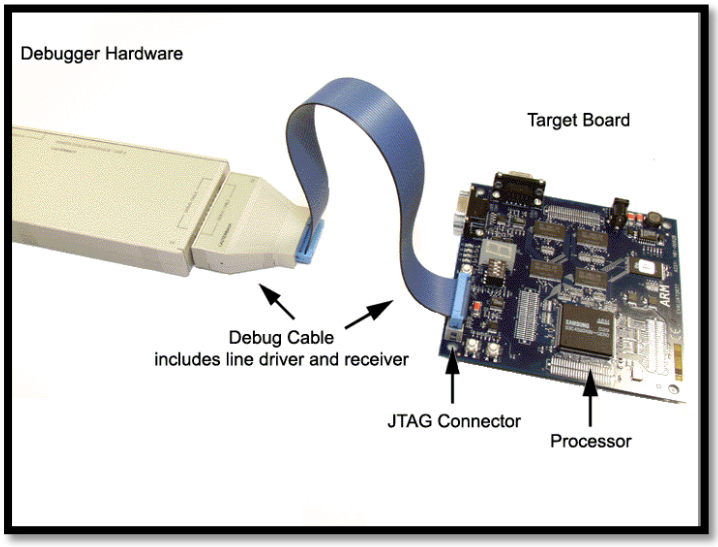


Fig. 5. JTAG interface

c) Step 3: Identify the chip's memory allocation.

After verifying the communication with the JTAG adapter, the succeeding step is to identify the chip's memory starting address and the capacity of the memory. Visually, one can observe the location of the Memory chip. It is helpful to search the Internet for information about hardware infrastructure and also the documentation for the memory chip. By the common line terminal of the device, one can check the boot loader for information about the flash memory model and address space.

d) Step 4: Extract firmware.

For extracting the firmware, one must use JTAG communication software to access the memory, which is identified in step 3. This process may take several minutes to save the data in a specific location based on the size of the flash memory and the data transfer speed of the JTAG interface.

V. ANALYSIS

JTAG allows control of firmware execution, including stopping execution, checking memory, configuring breakpoints, and stepping through code. One can also view the status of the processor. It is also possible to check the status of its registers, read and write memory, and access the other interfaces connected to the processor. It also allows access to all pins on the memory chip through the boundary scan feature. It provides accessibility to read and write each pin individually, allowing it to manipulate peripherals (GPIO, memory, flash, etc.) connected to the processor/microcontroller [16].

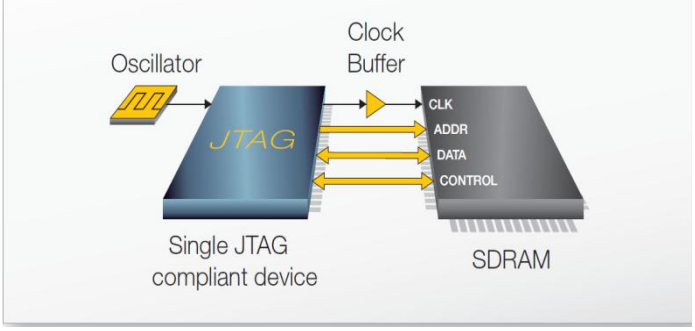


Fig. 6. JTAG interface

JTAG (Joint Test Action Group) is a standard for testing and debugging electronic devices, including mobile devices. In the context of mobile forensics, JTAG can be used as a method to perform physical extraction and analysis of data from a mobile device. In this process, the Debug and Test Access Block (DTAB) can be implemented on the target device as a "Passive" device that will never transfer data without permission. DTAB consists of the following pins:

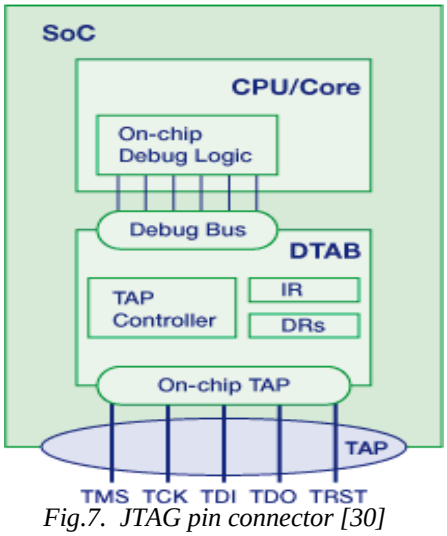


Fig.7. JTAG pin connector [30]

Following TAP signals are defined by IEEE standard which driving the TAP controller by serial communication.

Table 2 Test pins

TDI	*Test Data In*	*serial data from debugger to target*
TDO	*Test Data Out*	*serial data from target to debugger*
TCK	*Test Clock*	
TMS	*Test Mode Select*	*controls the TAP controller state transitions*
TRST	*Test Reset*	*optional, resets the TAP controller*

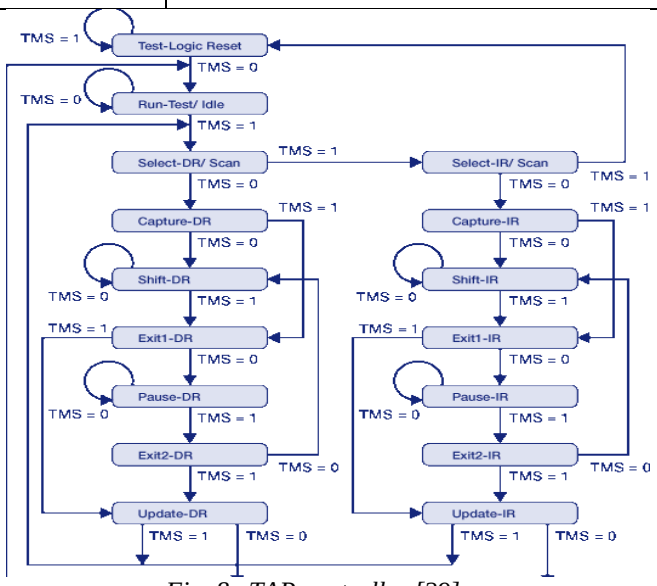


Fig. 8. TAP controller [29]

Figure 9 shows how Tri Core processor (IR: 8 bits, IDCODE DR: 32 bits) read the chip ID code from JTAG controller.

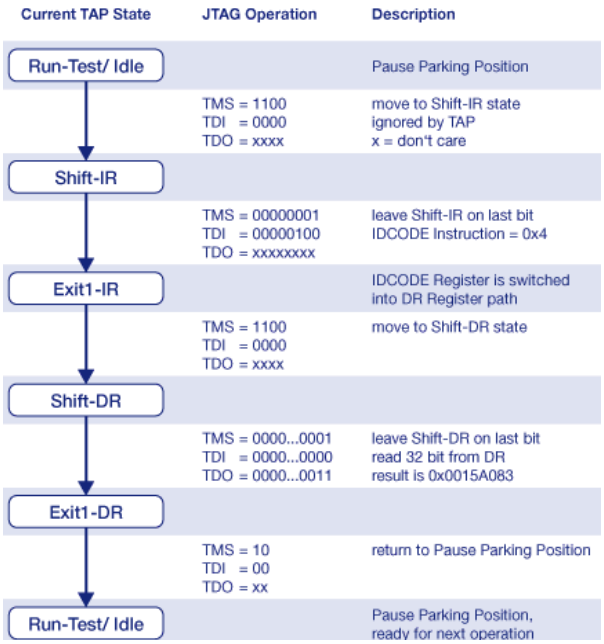


Fig. 9. Reference chip ID code [29]

The Phone Data, which is collected by the process of chip-off and JTAG Extraction, is in encrypted form and needs to be decrypted by forensically approved analyzing tools. After decryption, the investigator will be able to retrieve and analyze mobile data [27].

Popular Mobile data analysis tools are –

- Autopsy
- FTK Access Data,
- Oxygen Forensic,
- MOBILedit,
- UFED Celebrity etc.

VI. Results And Discussion

In this paper, the decryption of data from Samsung SM -A31 and Samsung SM-M30 is done using Celebrity UFED physical analyzer tools, and the original data is retrieved. The internal memory contents for Chip-Off binary images were decoded and analyzed with Cellebrite Physical Analyser 7.48.1.3.

Table 2 Numeric Data

Cellebrite Physical Analyser 7.48.1.3					
Mobile Device Binary Images: Chip-Off					
Mobile Used	**Methods**	**Efficiency %**	**Risk %**	**Data Loss %**	**Recovery Time (ms)/MB**
Samsung SM -A31	ISP and Flashing Devices	92.5	10.12	8.18	300
	Chip-off Data Extraction:	73.24	70.77	20.45	100
	JTAG (Joint Test Action Group)	80.40	20.22	10.33	200
Samsung SM-M30	ISP and Flashing Devices	95.00	11.00	9.10	350
	Chip-off Data Extraction:	75.32	72.22	23.33	120
	JTAG (Joint Test Action Group)	82.00	23.00	11.50	140

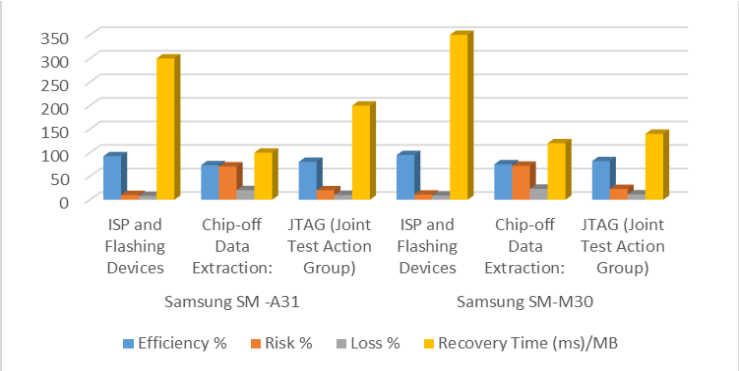


Fig. 11. Chart Table

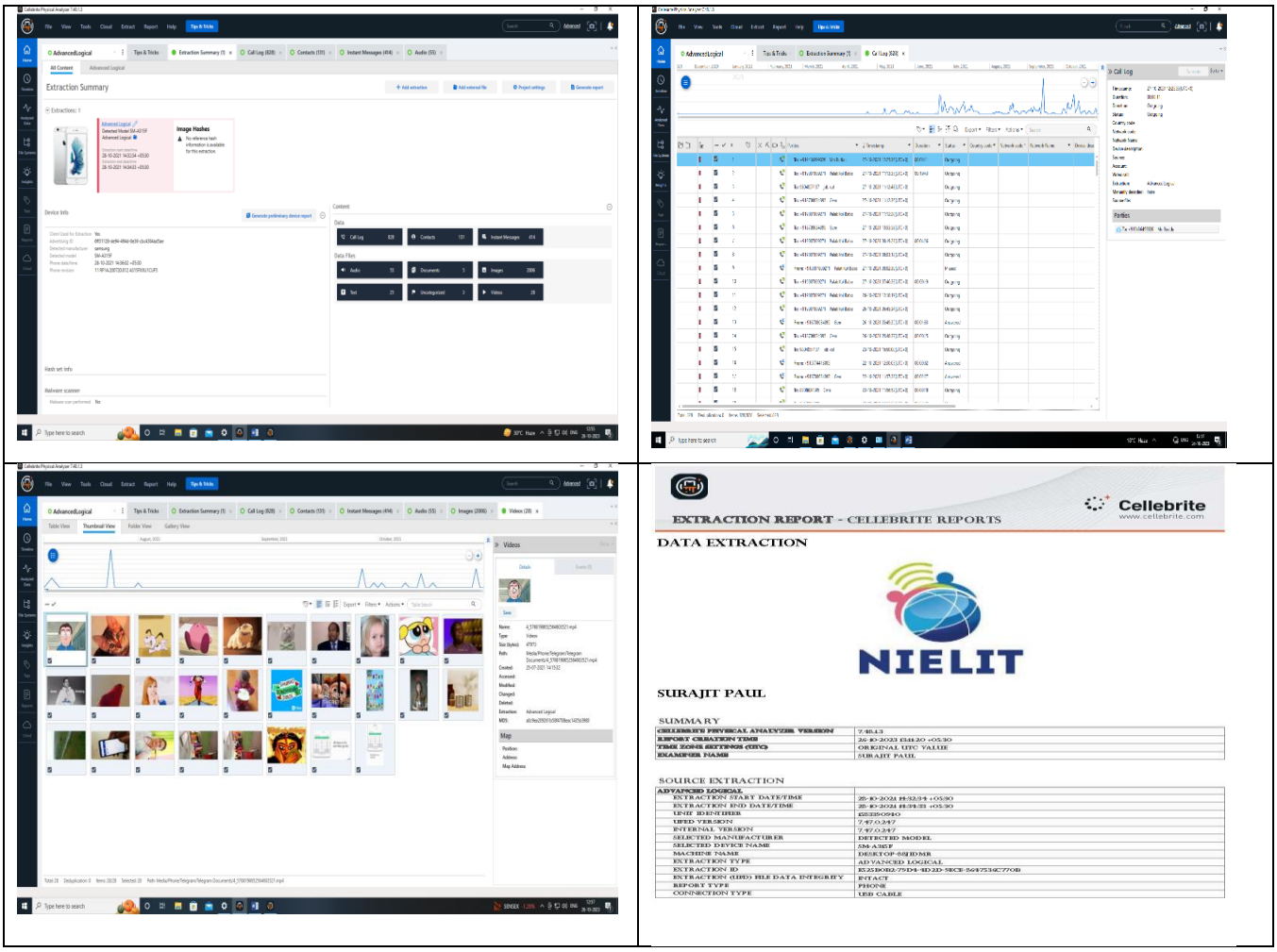


Fig. 12. Data Extraction snap shot

Table 3 Comparison of data Extraction Process

Items	**Extraction Process**		
	ISP & Flashing tools	**Chip-OFF Process**	**JTAG principle**
Implementation on	Working Mobile phone	Damage Mobile phone	Damage Mobile phone
Rooting	Required	Not required	Not required
USBDebugging	Essential	Not applicable	Not applicable
Risk Factor	Less	High	Moderate

Expertise	Not required	Moderately required	Highly required
Execution	Easy	Difficult	Difficult
OSdependence	Yes	No	No
Execution speed	Slow	Fast	Moderate
Cost	Less	Moderate	Expensive
Durability	Less	More	More
Reliability	Chance of data manipulation	Less data may be destroyed permanently	High, Very little chance of data loss
Complexity	Less	Moderate	High

It has been observed from the table that data extraction from the damaged mobile is not possible from ISP and flashing tool technique. The chipoff process experiences high-risk factors as compared to the JTAG process. The chip-off Process and JTAG principle are both OS-independent; therefore, there is no question of creaking passwords, which decreases the time to extract data from the phone. In the above case study, it is observed that the JATG process is more reliable than the Chipoff method [33].

Choosing between Chip-off and JTAG:

- Nature of the Case: If the device is physically damaged or has a damaged connector, Chip-off might be the only option.
- Device Compatibility: Some devices may have JTAG ports while others may not, and some may have more secure JTAG protection.
- Skill and Equipment Availability: Both methods require specialized skills and equipment. The forensic examiner's expertise and the availability of suitable tools play a crucial role.
- Legal and Ethical Considerations: Due to concerns about evidence preservation, destructive methods like Chip-off may not be preferred in some cases [35].

Ultimately, the choice between Chip-off and JTAG depends on the specific circumstances of the case, the type of device involved, and the available resources and expertise of the forensic examiner. In many cases, a combination of various forensic techniques may be employed to maximize the chances of successful data extraction [44].

VII. Conclusion and Future Scope

This research paper has explored and compared three data extraction processes from damaged mobile devices: the flash tool method, the chip-off method, and the JTAG method. These methods are crucial in digital forensics and data recovery, especially when dealing with devices that have physical damage or software issues. The choice of data extraction method for a damaged mobile phone should depend on the specific circumstances of the case. The flash tool method is a good starting point for devices with minor issues and non-functional screens. If the damage is severe, the chip-off and JTAG methods become necessary, but they come with increased risks and complexities. The growth of IoT (Internet of Things) and embedded systems may create new opportunities for chip-off and JTAG methods in extracting data from various types of devices and sensors. These methods may find applications in the cybersecurity domain, particularly in reverse engineering and vulnerability assessment. Ethical hackers and security professionals might use chip-off and JTAG to identify and fix security vulnerabilities in embedded systems. After an in-depth investigation, it is evident that each method has its advantages and limitations. Data extraction from damaged phones is critical to digital forensics, enabling investigators to retrieve valuable information in legal and investigative contexts. While challenges exist, advancements in technology and evolving techniques provide hope for improved success rates in the future.

Acknowledgment

The Authors would like to express sincere gratitude to Shri Niladri Das, Scientist E at NIELIT Agartala, for his invaluable guidance and support throughout the course of this research. His expertise and insights have significantly contributed to the development and success of this work.His unwavering dedication, constructive feedback, and collaborative spirit have been instrumental in shaping the outcomes of our research.

REFERENCES

[1] https://www.nist.gov/news-events/news/2020/01/nist-tests-forensic-methods-getting-data-damaged-mobile-phones
[2] https://www.dhs.gov/science-and-technology/forensics.
[3] F. Thomas-Brans, T. Heckmann1,3, K. Markantonakis, And D. Sauveron, New Diagnostic Forensic Protocol For Damaged Secure Digital Memory Cards, Digital Object Identifier 10.1109/Access.2022.3158958
[4] Dasgupta, Rhythm Kr. "Mobile forensic: Investigation of dead or damaged smartphone—An overview, tools and technique challenges from law enforcement perspective.". Accessed 3 (2021).
[5] Mobile forensic: Investigation of dead or damaged smartphone—An overview, tools and technique challenges from law enforcement perspective RK Dasgupta - … Journal. https://www. researchgate. net/publication …, 2021 - researchgate.net.
[6] K. Jonkers, "The forensic use of mobile phone flasher boxes," Digital Investigation, vol. 6, no. 3-4, pp. 168-178, May 2010.] [M. AI-Zarouni, "Introduction to Mobile Phone Flasher Devices and Considerations tor their Use in Mobile Phone Forensics," in 5th Australian Digital Forensics Can[, Perth, Western Australia, 2007, pp. 143-153.
[7] V.Venkateswara Rao and Dr.A.S.N Chakravarthy:" Forensic Analysis of Android Mobile Devices", IEEE International Conference on Recent Advances and Innovations in Engineering, December 23-25,2016, Jaipur,India.
[8] Khawla Abdulla Alghafli,Andrew Jones and Thomas Anthony Martin: "Forensics Data Acquisition Methods for Mobile Phones ", The 7th International Conference for Internet Technology and Secured Transactions(ICITST-2012).
[9] Aleksei N. Yakovlev1,2, Anna S. Danilova2, JTAG and Chip-Off Technologies in Computer Forensics, Author: Url: https://doi.org/10.30764/1819-2785-2018-13-3-109-115].
[10] Martien de Jongh, Coert Klaver, Ronald van der Knijtl and Mark Roeloffs Marcel Breeuwsma, "Forensic Data Recovery from Flash Memory," Small Scale Digital Device Forensics Journal, vol. 1, no. 1, pp. 1-17, June 2007.
[11] Author: Khawla Abdulla Alghafli, Andrew J ones, lThomas Anthony Martin Khalifa "Forensics Data Acquisition Methods for Mobile Phones", University of S cience, Technology and Research, UAE 2Edith Cowan University, Australia, Conference Paper · January 2012, url: https://www.researchgate.net/publication/261465980.
[12] S. Skorobogatov and C. Woods, "Breakthrough silicon scanning discovers backdoor in military chip," in Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst., 2012, pp. 23–40.
[13] I. M. F. Breeuwsma, "Forensic imaging of embedded systems using JTAG (boundary-scan)," Digit. Invest., vol. 3, no. 1, pp. 32–42, 2006.
[14] 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/
[15] B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in Proc. Int. Test Conf., 2004, pp. 339–344.
[16] CFTT– JTAG, Chip-Off NIST 2019https://www.nist.gov/system/files/documents/2020/08/21/CFTT%20%20JTAG%20and%20Chip-Off%202019.pdf
[17] Aya Fukami , Radina Stoykova and Zeno Geradts , A new model for forensic data extraction from encrypted mobile devices, Forensic Science International: Digital Investigation 38 (2021) 301169.
[18] Silveira, C., de Sousa Junior, R., Albuquerque, R., Amvame Nze, G., Júnior, G., Sandoval Orozco, A., García Villalba, L., 2020. Methodology for forensics data reconstruction on mobile devices with android operating system applying insystem programming and combination firmware. Appl. Sci. 10, 4231. https://doi.org/10.3390/app10124231.
[19] Walden, I., 2018. 'the sky is falling!' e responses to the 'going dark' problem. Comput. Law Secur. Rep. 34, 901e907. https://doi.org/10.1016/j.clsr.2018.05.013. URL: http://www.sciencedirect.com/science/article/pii/S0267364918301973. Willassen, S., 2005. Forensic analysis of mobile phone internal memory. In: Pollitt, M., Shenoi, S. (Eds.), Advances in Digital Forensics. Springer US, Boston, MA, pp. 191e204.
[20] https://semiengineering.com/security-for-android-based-ecosystem-with-mobile-storage-ip/
[21] https://www.riverloopsecurity.com/blog/2020/03/hw-101-emmc/
[22] https://www.nist.gov/news-events/news/2020/01/nist-tests-forensic-methods-getting-data-damaged-mobile-phones]
[23] S. Skorobogatov and C. Woods, "Breakthrough silicon scanning dis- covers backdoor in military chip," in Proc. Int. Workshop Cryptograph. Hardw. Embedded Syst., 2012, pp. 23–40.
[24] I. M. F. Breeuwsma, "Forensic imaging of embedded systems using JTAG (boundary-scan)," Digit. Invest., vol. 3, no. 1, pp. 32–42, 2006.
[25] F. Domke, "Blackbox JTAG reverse engineering," in Proc. Chaos Commun. Congr., 2009, pp. 1–5.
[26] I. Slochinsky, "Introduction to embedded reverse engineering for PC reversers," in Proc. REcon Conf., 2010.
[27] Cellebrite UFED Physical Pro Cell Phone Extraction Guide By Colby Lahaie, Patrick Leahy Center for Digital Investigation Champlain College.
[28] Cellebrite Reports – 2021 Quick Start User Guide, www.elabforensics.cominfor@elabforensics.com.
[29] https://www2.lauterbach.com/pdf/training_jtag.pdf
[30] https://www.corelis.com/education/tutorials/jtag-tutorial/jtag-test-overview/
[31] Dasgupta, Rhythm Kr. 2020. Mobile forensic: Investigation of dead or damaged smart phone—An overview, tools and technique challenges from law enforcement perspective..
[32] Fukami, Aya, and Kazuhiro Nishimura. 2019. Forensic analysis of water damaged mobile devices. In Proceedings of the nineteenth annual DFRWS USA. Digital Investigation 29: S71–S79.
[33] Hadgkiss, M., S. Morris, and S. Paget. 2019. Sifting through the ashes: Amazon Fire TV stick acquisition and analysis. Digital Investigation 28: 112–118. https://doi.org/10.1016/j.diin.2019.01.003.
[34] Jo, Wooyeon, et al. 2019. Digital forensic practices and methodologies for AI speaker ecosystems. Digital Investigation 29: S80–S93. https://doi.org/10.1016/j.diin.2019.04.013.
[35] Jones, G. Maria, and S. Godfrey Winster. 2017. Forensics analysis on smart phones using mobile forensics tools. International Journal of Computational Intelligence Research 13 (8): 1859–1869.
[36] Krishnan, S., B. Zhou, and M.K. An. 2019. Smartphone forensic challenges. International Journal of Computer Science and Security 13 (5): 183–200.
[37] Odom, N.R., J.M. Lindmar, J. Hirt, and J. Brunty. 2019. Forensic inspection of sensitive user data and artifacts from smart watch wearable devices. Journal of Forensic Sciences 64: 1673–1686. https://doi.org/10.1111/1556-4029.14109.
[38] Ramírez, Sanabria Perla Rocío. 2020. Digital forensics—Guidelines and tools for a digital evidence investigation process: A case study for a business data leak, 14–15. Thesis for Bachelor of Engineering, Information and Communications Technology, Turku University of Applied Sciences.
[39] Ryser, E., H. Spichiger, and E. Casey. 2020. Structured decision making in investigations involving digital and multimedia evidence. Forensic Science International: Digital Investigation 34: 301015. https://doi.org/10.1016/j.fsidi.2020.301015.
[40] Silveira, C.M., et al. 2020. Methodology for forensics data reconstruction on mobile devices with Android operating system applying in-system programming and combination firmware. Applied Sciences 10 (12): 4231. https://doi.org/10.3390/app10124231.