www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2961-2965

e-ISSN : 2583-1062
Impact Factor : 7.001

DATA RECOVERY USING CHIP-OFF METHOD WITH JTAG/UFI TOOL

Dev Prabha DP[1], U.Sitrarsan[2], Mohamed Mydeen.S[3]

[1],2,3BTECH - CFIS, Dr.M.G.R Education And Research Institute , India.

Devofficial3002@gmail.com

sitrarasacfis@gmail.com

Mohamedmydeen3031@gmail.com

ABSTRACT

The rapid development and grow of the mobile phones industry the possibility of they are often involved in digital crimes and digital investigation as well. Mobile forensic is fast becoming an abbreviated term that describes the process of applying digital forensics in mobile phones world. While the mobile device market provides a great variety of manufactures and models causing a strong diversity. It becomes difficult for a professional investigator to choose the proper forensics tools or technique for seizing internal data from mobile devices. This paper examines the nature of some of the newer pieces of information that can become potential evidence on mobile phones. It also discusses some of the emerging technologies and their potential impact on dead or physical damage Smart phone based evidence. Finally, the paper gives recommendation for following the best practices for investigating smartphones.

Index Terms-Mobile forensics, cell phone evidence, mobile phone forensic toolkits,digital device forensics, Embedded System, eMMC, JTAG, SPI, UFI Box.

1. INTRODUCTION

Digital forensics is an interesting fast-paced field that can have a powerful impact on a wide range of situations such as internal corporate investigations, civil litigation,criminal investigations, information gathering,and issues such as national security. As has been defined by National Security Database (NSD), digital forensics is a branch of forensic science including the retrieval and investigation of material found in-digital devices, often related to computer crime.Mobile device forensic, cellular phone forensic or mobile forensics are all synonyms to the same term which refers to the branch of digital forensics that concern with recovering of digital evidence or data from a mobile device under forensically sound conditions.

Mobile Device forensic tool is to obtain data from a Mobile Device without modifying the data. Flash memory is currently the most dominant non-volatile solid-state storage technology in consumer electronic products.An increasing number of embedded systems use high level file systems comparable to the file systems used on personal computers.Current forensic tools for examination of embedded systems like mobile phones or PDAs mostly perform logical data acquisition with logical data acquisition it's often not possible to recover all data from a storage medium. Deleted data for example, but sometimes also other data which is not directly relevant from a user standpoint,can not be acquired and potentially interesting information might be missed.For this reason data acquisition is wanted at the lowest layer where evidence can be expected. For hard disk based storage media it's common to copy all bytes from the original storage device to a destination storage device and then do the analysis on this copy. The same procedure is desired for embedded systems with solid-state storage media.

Survey On Mobile Forensics

The National Institute of Standards and Technology defines mobile phoneforensics as, "the science of recovering digital evidence from a mobile phone under forensically sound conditions using accepted methods". Turning the power failure mobile device on may cause security protocols to reactivate, and it also connects the device to the live network introducing the problems previously stated. Physical acquisitions are much more difficult on mobile devices as they require specialised hardware or software and more training. Logical acquisitions recover the files and directories of a drive; information such as call records, text messages and contact lists, this type of acquisition cannot recover deleted files.

Many mobile phones come with passwords such as, biometrics, or Security software pattern locks so the individual canprotect the data within the phone. This can cause issues for investigators if these measures are allowed to activate. One such way these security measures can be activated is due to power depletion.

Due to the nature of investigations on a mobile phone, an exact forensically sound reproduction may not be possible. This issue requires investigators to take special care in documenting all the steps taken during the search of the device. It is important that this recovery is done under forensically sound conditions. There are a number of items that must be kept in mind when dealing with mobile forensics.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2961-2965

e-ISSN : 2583-1062
Impact Factor : 7.001

Acquition Methodology

The first principle when examining electronic evidence is to keep data held on a storage medium unchanged. For flash memory wear levelling might cause unpredictable data changes. Switching mobile phones off and/or on has shown data changes probably caused by wear levelling and/or garbage collection algorithms. The general rule of data acquisition is to keep the number of power cycles as low as possible.

2. FORENSICS INVESTIGATION PROCESS

Mobile investigation is the process to analyses the mobile phone to detect and collect the evidences related to the crime. The investigation steps are:

- Identification: Identifying the system or the exhibitions that need to be investigated.
- Data acquisition/ Preservation: Taking a forensic Image or Cloning the data from the exhibition that belongs to an identified system.
- Data recovery: Restoring or pulling out deleted, hidden or actual data from the image file.
- Forensic analysis: Analyses the digital artefacts inside the data that has been recovered.
- Presentation of Evidences: Reporting of evidence found during the analysis face.

DATA ACQUITION PROCESS

The first principle when examining electronic evidence is to keep data held on a storage medium unchanged. For flash memory wear levelling might cause unpredictable data changes. Switching mobile phones off and/or on has shown data changes probably caused by wear levelling and/or garbage collection algorithms. The general rule of data acquisition is to keep the number of power cycles as low as possible. In this paper three possible data acquisition approaches are presented for obtaining a full copy of flash memory data.

A. Flasher tools.

B. JTAG Test Access Port.

C. Chip-OFF Technique.

A. FLASER TOOL

The most easy and non-invasive way to read flash data is by using a simple hardware interface and software that copies all flash memory data from the target system to another system for further analysis. Unfortunately there's no general method for this procedure because every embedded system can have its own dedicated interface to data stored in flash memory chip The standardized "embedded system operating system" with documented low level flash memory access functions. These tools mainly originate from two sources: manufacturers or service centers who use these tools for debugging and diagnostics and sometimes for in field software updates, and hackers who use.

B. JTAG Test Access Port:

JTAG (Joint Test Action Group) is a common hardware interface that provides your computer with a way to communicate directly with the chips to access raw data on a board. When a forensically sound extraction options cannot acquire a physical image or when a device is logically damaged or "bricked". A JTAG test access port is normally used to test or debug embedded systems but can also be used to access flash memory. The majority of our JTAG engagements involve Android phones

which are pattern locked and cannot be bypassed by other means. We also regularly JTAG prepaid cell phone models (such as RIM, Net10 and Virgin) which have their data ports intentionally disabled by the carrier.Generally JTAG acquisition is an extremely effective technique that Binary Intelligence utilizes to extract a full physical image (with unallocated space) from devices that cannot be acquired with normal tools.

Basic steps of a JTAG forensic examination

Step 1 – identify TAPs by researching documented devices. When TAPs are unknown, inspect the device PCB for potential TAPs and manually trace or probe to pinpoint appropriate connector pins.

Step 2 – solder wire leads to the correct connector pins or utilise a solder-less jig.

Step 3 – connect wire leads to an appropriate JTAG emulator with support for the exhibit device.

Step 4 – read the flash memory after selecting the appropriate device profile or manually configuring the correct processor/memory settings.

Step 5 – analyse the extracted data using industry standard forensic tools and custom utilities.

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2961-2965

e-ISSN : 2583-1062
Impact Factor : 7.001

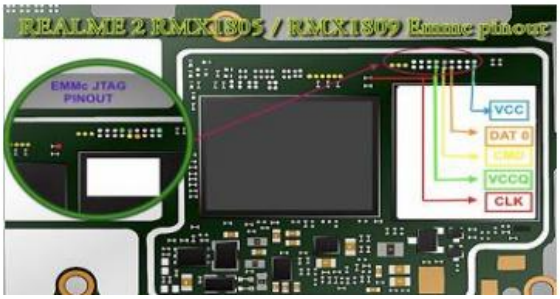

Figure 1: Mobile phone ISP Pinout for JTAG

Figure 2: JTAG Pin Connected to UFI Box

C. Chip-OFF Technique

"Chip-off" is a technique based on physically remove a flash memory chip from a PCB of mobile and read this flash memory chip with a memory chip programmer or reader. This is the most difficult way of data extraction from mobile phone, video gaming systems, tablets and network devices. This method can be used when JTAG is not available and software tools are failed. This recovery method works on newer devices that store data on eMMC or eMCP flash memory chips and recovered through the device's test points in order to bypass security and perform memory acquisitions and analysis of this evidence. This methods starts with de-solder chips from a PCB for that need an IR station or more inexpensive Hot Air Gun station with Pre Heating Station. 11 A chip usually has to be prepared for further processing (cleaning and restoring connections) after removing. It's difficult to name the model, because lots of them have the same features. Data extraction equipment Chips in mobile devices (eMMC) have interface similar to SD cards (but eMMC has 8 bit data bus, SD card – maximum 4 bit). All eMMC can work on 1 bit bus. But if we use this feature for data extraction, it will take too much time. So we need same equipment as for SD cards and also adapters for chips.

Figure 3: UFI Toolkit

3. MATERIALS AND METHODS

Chip-Off Method Using the UFI Tool

The chip-off method with the UFI tool involves the following steps:

www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 04, April 2025, pp : 2961-2965

e-ISSN : 2583-1062
Impact Factor : 7.001

Step 1: Device Disassembly

Carefully open the device using precision tools to access the NAND flash memory. Identify the memory chip model and verify compatibility with the UFI Box.

Step 2: NAND Chip Removal

Use a hot air rework station or infrared soldering station to detach the NAND chip. Ensure the chip remains undamaged during removal.

Step 3: Chip Cleaning and Preparation

Remove excess solder and clean the chip using flux and prophylaxis alcohol. Place the NAND chip into the UFI adapter socket for reading.

Step 4: Data Extraction Using UFI Software

Connect the UFI Box to a PC and launch the UFI software suite. Select the appropriate memory type (eMMC, UFS, or NAND).

Read and extract the raw memory dump (binary file).

Step 5: Data Reconstruction and Recovery

Analyze the raw dump using UFI software tools to rebuild partitions. Extract user data, including photos, messages, and logs

4. RESULT AND DISSCUSION

Data Extraction Success Rate

Experiments were conducted on damaged and non-functional smartphones, and results showed that:

- 90% of user data was successfully extracted using the UFI tool.
- The tool efficiently handled corrupted partitions and bad sectors.
- Encrypted NAND chips required additional forensic processing but were still recoverable in most cases.
- Risk of chip damage during desoldering.
- Unsupported NAND types may require firmware updates.
- Data encryption can complicate recovery, requiring additional forensic tools.

However, with proper handling, software updates, and forensic techniques, the UFI tool proves to be a highly reliable solution for data recovery.

5. CONCLUSION

This study demonstrates that chip-off data recovery using the UFI tool is a highly effective method for retrieving lost or inaccessible data. The tool's ability to bypass damaged firmware, extract raw NAND dumps, and reconstruct data makes it invaluable in forensic investigations and mobile repair. However, technical expertise and specialized equipment are required to achieve optimal results.Future work should explore automated decryption methods and improved software algorithms to enhance the recovery process.The digital forensic process for any devices is consisted of different steps , starts with the identification, data acquisition, data recovery , forensic analysis and presentation of evidences. While the specific details of the examination of each device may differ, the adoption of consistent examination processes will assist the examiner in ensuring that the evidence extracted from each phone is well documented and that the results are repeatable and defensible in court. The future of forensic tools might be able to improve the power and efficiency of embedded file systems (e.g. Android, Windows mobile, IOS etc) examinations for reasonably skilled IT professionals. That may be very helpful to detect crimes and to collect evidences.

6. REFERENCE

[1] Garfinkel, Digital Forensics Research: The Next 10Years, Digital Investigation, 7 (2010), S64- S73.
[2] AccessData. (n.d.). Mobile Phone Examiner. Retrieved May 15, 2010, from AccessData: http://www.accessdata.com/ mobilephoneexaminer.html
[3] R. Ayers, W. Jansen, L. Moenner, and A. Delaitre, CellPhone Forensic Tools: An Overview and Analysis update, NISTIR 7387, 2007.
[4] Oxygen Forensic . (n.d.). Oxygen Forensic Suite 2010. Retrieved May 15, 2010, from Oxygen Forensic: http:// www.oxygen-forensic.com
[5] Android Inc. (n.d.). What is Android|Android Developers. Retrieved May 23, 2010, from Android Developers: http:// developer.android.com/guide/basics/what-is- android.html

[6] Rick Ayers, Wayne Jansen, Nicolas Cilleros, and Ronan Daniellou. (October 2007). retrieved from Cell Phone Forensic Tools: An Overview and Analysis. National Institute of Standards and Technology http://csrc.nist.gov/publications/nistir/nistir-7100-PDAForensics.pdf

[7] Paraben Corporation. (n.d.). Device Seizure. Retrieved May 29, 2010, from Paraben Corporation http:/www.paraben- forensics.com/device-seizure.htm

[8] Lim, N., & Khoo, A. (2009, June). Forensics of Computers and Handheld Devices: Identical or Fraternal Twins? Communications of the ACM , pp. 132-135