Journal of Advances in Science and Technology
Vol. 16, Issue No. 1, March-2019, ISSN 2230-9659

Joint Test Action Group and In-System Programming Techniques for Forensic Procedures

Dr. Sridevi*

Department of Computer Science, Karnatak University, Dharwad, India

Abstract – This paper focuses on physical acquisition strategies for the Joint Test Action Group (JTAG) and In-System Programming (ISP). These methods were developed by producers to monitor PCBs and fix products but are used as a forensic tool to gather data from a computer. The aim is to provide a forensic analysis of these methods, and in addition to some other studies it will attempt to show that they are forensically similar to some other process.

Keywords: Android, Forensic, JTAG, ISP, eMMC, Acquisition,…etc.

----------X----------

1. INTRODUCTION

Smartphones have been an important part of everyday life for people, with mobile subscribers at 2.9 billion in 2018, up 3.2 billion in 2019 and 3.5 billion by 2020, and is estimated to grow to 3.8 billion in the world by 2021[1]. Smartphones are pocket computers through which users can access the Internet, talk, e-mail, build and read documents and books, navigate by GPS, keep notes and much more. Combined with the reality that citizens prefer to transport their telephones around, these useful features render smartphones a blend of facts in court trials. Smartphones have generated a need for research that seeks primarily to look at these gadgets for facts and record them later on in court, and so electronic forensics, a sub-branch of the principal science of digital forensics, arose. Mobile forensics is comparatively recent, but develops exponentially as forensic examiners work with mobile devices more often than ever.

Mobile forensics is the discipline for the study of mobile devices. The forensic method includes gathering information, acquiring data and examining the data and disclosing the evidence. Data acquisition and processing may take one or two phases depending on the process and methodology used in mobile forensics. The data collection approaches may be classified into three types: mathematical, file system and physical acquisition. A logical acquisition is a "bit-by-bit" copy of logical storage items (e.g., files) residing on the logical storage, and a bit-by-bit copy of physical storage as stated in Wikipedia [2]. File system acquisition may include details for lost but not overwritten files when file system access is allowed by the software. Of method of acquisition has a range of data acquisition strategies, such as "android" backup (for Android devices alone) and "logical acquisition," for logical acquisition utilising "UFED Touch" and JTAG, ISP, chip-off and dd commands. The examiner must determine which approach is used according to the requirements of the case.

2. ANDROID FILE SYSTEM AND PARTITION LAYOUT

Android is the leading OS4 on the demand for smartphones, as calculated during the third quarter of 2017, with a global share of 86.8%[3]. Android uses a variety of file systems, the only valuable forensic partition that stores user data, uses EXT, FAT32, and YAFFS25[4]. Proprietary file systems such as Samsung's RFS file system can be identified. Digital file systems, which are not written to physical devices, also exist in Android, such as "proc" (kernel information, process parameters and settings) and "rootfs" (where kernel mount root file system at start-up). In the "/proc/filesystem" file you will find details on Linux-supported filesystems and Android extensions. The partition layout differs between different Android devices; however, some configurations are common in all devices.

3. DIGITAL FORENSIC

Science consists of many divisions, one of which is digital forensics, whose key goal is to retrieve and examine the content contained in digital evidence [5]. Further separates digital forensics in sub-branches such as forensic data processing, device, web forensics and network. From the seizure of a

show exhibit to the production of a study, this phase is called the "digital forensics process" [6]. The phases in this phase are:

- Seizure: Automated technical technicians gather the crime scene exhibits.
- Acquisition: for review, an accurate sector or forensic media duplication is made. The research must never be conducted on the initial computer only if the crime scene is studied live.
- Analysis: Automated forensic investigator conducts exhibit analysis to collect information utilising multiple techniques and equipment.
- Report: report of research conclusions.

The staff responsible for this phase, digital forensic technicians and digital forensic examiners, may be divided narrowly into two levels [5]. Technicians are liable for gathering or analysing information in the scene of crime and also for conducting a "live analysis" of evidence. Technicians should be educated in the correct management of exhibits. Examiners are trained in only one region, however.

3.1 Data Acquisition

Data acquisition is split into various levels/types of mobile forensics. According to the SWGDE Cell Phone Forensic best practises [7], these standards are:

1. Manual: Use the computer itself to manually check for facts.
2. Logical: Retrieval of portion of the file system.
3. File System: Allows file system control.
4. Physical (non-invasive): physical collection of mobile data without handset disassembly.
5. Physical (invasive): physical acquisition of telephone data involving system disassembly PCB (JTAG/ISP) access.
6. Chip-off: Chip removal for review from the PCB.
7. Micro Read: a high-power microscope is used to display the electronic circuitry visually Memory.

Logical acquisition the logical acquisition of logical database artefacts that exist in logical storage, i.e. the evidence that is assigned, is a bit-by-bit picture acquisition. This form of purchase is carried out by the usage of a specified API [8]. In this paragraph, certain conceptual acquisition methods are clarified. Notice that only Android devices have these two strategies.

ADB Pull ADB6 is an Android SDK command line tool that lets users connect with an Android device [4]. ADB has several commands [9] but the most useful command is the pull command from the forensic point of view, since it is used to retrieve data from the attached computer. The requirement of using this command and every other ADB command is that the developer's mode and USB debugging option are allowed. If the device has no root access, the device's ADB daemon operates with shell-related rights, close to those of non-root control on Linux terminals. Unencrypted applications, "tmpfs" file structure, which can contain user details and other accessible folders, are an example of valuable files that can be pulled. If the computer is rooted or has a custom ROM, it is easy to take it all out.

3.2 Backup Analysis

The backup analysis methodology is focused on the user's backup analysis [4]. In the early years of its use, Android had no backup system for user data that led Android users to back up their data utilising third-party software. Typically, the backup was saved in SD cards or the server. This backup typically includes the user files such as photos, videos and notes, although some programmes will also back up data from the application for rooted users. Rooted consumers now have a more efficient technology to back up their data called "android." Android backup can be accessed in two ways. By booting the system, you need to configure the recovery in recovery mode using the two most widely recognised and used CWM7 and TWRP8, or by using an application like "Online Android Backup" you need root [10]. Android backup generates a picture that often involves user data and device files.

3.3 Physical Acquisition

A physical acquisition is a bit-by-bit replica of a physical storage which may, utilising the 'dd' button, be intrusive, JTAG, ISP or Chip-off. From the investigative viewpoint, the distinction in physical and conceptual acquisition is that missing files can be restored through physical acquisition and the slack space can be checked.

The TAP standard test access and boundary-scan architecture for JTAG IEEE 1149.1 [11] is recognised as the JTAG boundary scan research architecture. JTAG was developed for research purposes, but recently began to be used by mobile forensics to obtain the flash memory at low raw quality. JTAG is a non-destructive intrusive procedure that ensures the system must be disassembled (invasive) but may be used again after the acquisition (non-destructive). The JTAG method demands that a hardware, flash box is

connected via solder, Molex or jig and a machine to the device's PCB test access points [12]. The best established JTAG flash box is the Riff box, other boxes include ATF10 and Z3X. JTAG is a method that uses the memory acquisition processor. This method involves, first and foremost, attaching JTAG system TAPs to the flash box, the machine box and then the programme flash box configuration. When this is attached and the software is fully set-up, the flash box would instruct the processor to retrieve the raw data contained on the chip via the test access points. The JTAG procurement process comprises:

1. Disassembly of the system
2. Find the PCB TAPs
3. Link to the corresponding TAP on the PCB the JTAG box attached to the device
4. Buy a chip picture using JTAG Box programme
5. Switch off the JTAG and assemble the system

3.4 ISP

The key distinction is that ISP attaches directly to an eMMC and/or eMCP flash memory and bypasses the processor. It is an acquisition strategy close to JTAG. In ISP, as in JTAG, the investigator wants to recognise the TAPs leading to the flash box and the memory. First, the procedure involves attaching eMMC TAPs to a flash box facilitating eMMC read/write operations, connecting the flash box to a device and setting up the programme for the flash box. If all is connected, the device is set up properly and the memory material can be read from the link between the flash box and eMMC.

If you do not have the programme of the flash box, then the internet and the forums are open. If neither of these works can be found manually by checking each TAP on PCB then it is understood that all the correct TAPs are required and that an ATF box and an amplifier is necessary for this method and a second instrument similar to the first for testing purposes. Finally, details on the TAPs of the eMMC is accessible on the schemes of the unit. Because the link to the memory chip in the ISP acquisition is faster than JTAG. It may even be used if a system is not JTAG-able.

3.5 Chip-off

Chip-off is an advanced data extraction technique which involves the first removal of the chip from the computer and then the installation of the chip and the development of an image of raw data [15]. Chip-off is not confined to cell phones only, but can even be seen on other gadgets that utilise flash memory, such as GPS and car parts. The method of chip-off consists of four steps:

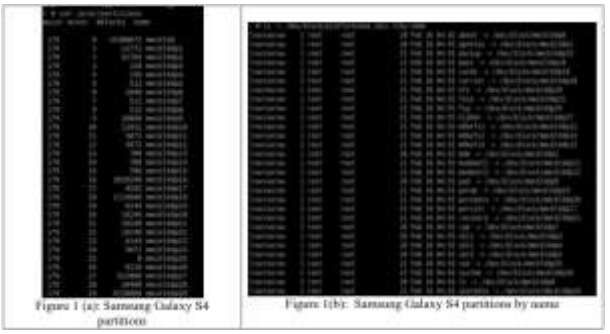
1. Delete the system chip.
2. Clean the chip and patch it.
3. Acquisition of photographs using advanced tools
4. Photo processing using traditional forensic equipment.

Only if there is no other option can this approach be used. Chip-off needs not only pricey machinery but also an expert and trained examiner. Beside the costly equipment process, there is another way to interpret the mind, but it is not suggested. This approach is also an ISP acquisition, but the flash box attaches directly to the TAPs on the chip instead of attaching to system TAPs. As the device may be killed by experts during the chip-off phase.

3.6 dd command

The "dd" command method is an intrusive technique of physical acquisition which uses the "dd' command" for Linux. This command is used to copy and convert files but it is used to build bit-by-bit images on the drives by forensic examiners [16]. As Android is built on Linux, when the system fulfils those criteria this command may be used for obtaining a partition or full disc image, the requirements are to root the device with the mounted BusyBox and the "USB debugging developer mode" option must be allowed.

The rooting process of a computer differs among devices. When this is met, an examiner must boot the system and link the device to a monitor, so the ADB tool can start looking again for the partition he needs to obtain, by checking the "/proc/partitions" file for partition details on the device, for Samsung Galaxy S4 partitions see in Figure1(a), Figure1(b).



4. CELLEBRITE UFED TOUCH

Cellebrite is a pioneer in mobile data technology, one of the resources they have developed is the UFED Touch. Their new innovation is UFED Touch 2, a handheld forensic analytical system for mobile

and GPS applications. UFED Touch embraces all three forms of computational, file system and physical data acquisition [8]. UFED Touch loads the required API into the system for logical acquisition, then allows read-only requests for data such as text messages and images. The quickest method of acquisition is rational, but the time differs due to the files on the computer.

4.1 ATF software setup

The new ATF edition supports Qualcomm, Exynos Marvell PXA, Broadcom and Spreadtrum CPUs. The following steps would demonstrate how the TP recognition programme is prepared.

Step 1: Link ATF 4in1 to the ATF flash box, USB2.0 port ATF box and run ATF programme.

Step 2: From the "Nokia Service" category, select "ATF Plus" as telephone generation then select "Find TP eMMC."

Step 3: Setup eMMC Test Point Finder. The settings used for Nokia Lumia 635 are seen in Figure 19.

- Kind of Processor: The sort of CPU the computer has.
- Objective: the test points to be established. Often start with CLK and CMD, then VCC and last data if appropriate.
- VCCIO: the supply voltage of the unit. Qualcomm-based systems do not require this since the power supply uses a USB cord. Devices centred on Spreadtrum need 3.3V.
- Repeat: This sets the amount of times the machine loops the exam. Set often to a huge amount.
- Delay: duration in seconds between attempts to classify the TP. This provides the time required to transfer the research sample to another test stage.

Step 4: Click on "Find Test Point for eMMC" and continue to check for test points.

The following figure 2 demonstrates the ATF test point recognition programme setup for eMMC

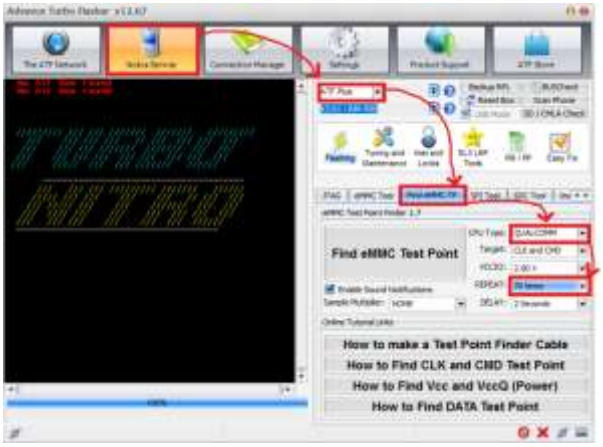


Figure 2: ATF software setup for eMMC Test Point Identificaiton

4.2 ISP Acquisition

The acquisition phase will start when the examiner recognises the test points and everything is related. A jig may be used with certain connection items; jigs are tiny PCBs which can be attached to the device's eMMC TAPs without any soldering. Each jig is built for just one computer, so various devices have different test points and not all devices have jigs. The acquisition method is very quick and fast, as long as the welding is performed correctly.

Step 1: Select “eMMC Tool” tab under Nokia Service - ATF Plus on ATF software.

Step 2: To choose the form of CPU, pick "Nokia Lumia – Snapdragon 2,3,4" and press "Scan eMMC." If the ties are strong and the connection to the eMMC-chip is created, the same information is seen on the screen as in Figure 3, and the next move is to reach the "User Area Size".

Figure 3: Nokia Lumia 635 eMMC information

Step 3: Pick the dumping partition and the height of the partition. The user region of phase 2 referring to 8GB of data was 7818182656 bytes. Pick 8GB for "Size," and the software fills the "End Block" in Figure 4 automatically.

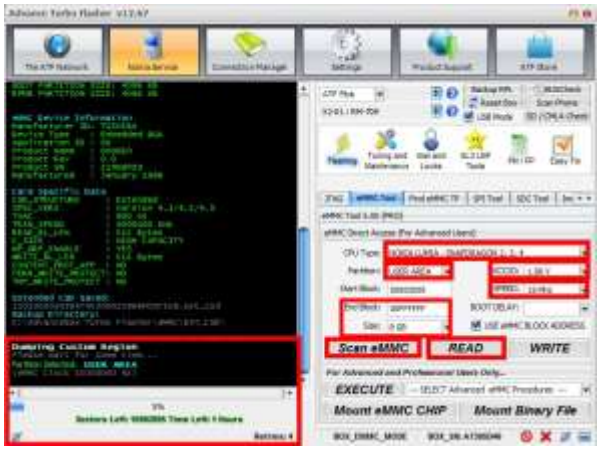


Figure 4: ISP Acquisition settings

Step 4 Build the VCCIO, set the VccQ value. If unknown, begin with 1.8V and, if necessary, switch to 3.3V. It was meaningless for this device since the device was operated by a USB cord.

Step 5 Set eMMC clock speed 15 MHz; try other values if it does not operate. A look at the chip's data sheet will provide details on clock speed, but different values are simpler to attempt.

Step 6 Click on "READ," assign the disc image output name and wait. On the screen the software displays which partition was chosen to interpret, the remaining sectors and the period left for the acquisition, Figure 4.

Figure 4 indicates the number of "Retries" in the lower right-hand side of the wide red box on the left; this number demonstrates how much contact with the eMMC chip the ATF box has been missing. Weak link indicates poor soldering; the wires can then be cautiously re-soldered. Bad links also provide a sluggish acquisition and will not be able to finish in certain situations. The instruments used in this study were inadequate (thick soldering tip and no microscope), resulting in weak connection. The link was lost at 49 percent of the acquisition before the software froze and the acquisition completely stopped; 4GB of memory were then copied. It wasn't necessary after several failed attempts to solder the wires again.

4.3 JTAG Acquisition

The acquisition of JTAG is identical to ISP but uses multiple reference points. Samsung Galaxy S4 I9505 was used for the acquisition of JTAG. The following resources are required for the acquisition of JTAG:

- Software Flash Box
- Iron soldering
- Wire 0.04mm or 0.02mm soldering wire
- A numerical microscope
- Power source for DC (not mandatory but useful)

5. JTAG TEST ACCESS POINTS

For this part the JTAG pinout interface is supposed to be identified, the source to check for JTAG pinouts as the Google, forums apps, manually by inspecting tips and the schemes of the system. For certain tablets, such as the one used for this test, JTAG jigs are available. Follow the steps to locate approved Riff box devices and the JTAG interface pinout:

Step 1: From “Box service” select “Check for Updates”.

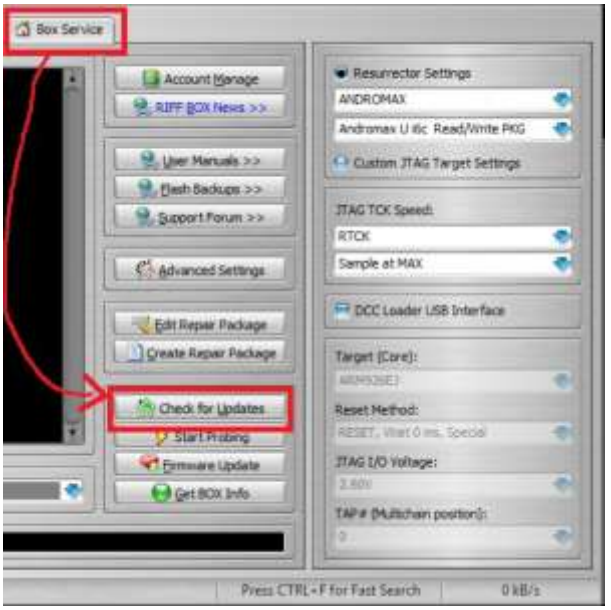


Figure 5: Riff Box “Check for Updates”

Step 2: Select "Resurrections" on the "Riff Updates Manager" window under "JTAG Manager Root." Choose the producer and check for the device. Download the file when the computer is located. If the installation is complete, the riff box downloads the files and the applications Begin Restart.

Step 3: In the "Resurrection" category, click "Interface Pinout" to see this device's JTAG pinout. This choice is not accessible on every unit. Under any scenario, the inspector himself can locate the JTAG pinout. Figure 32 indicates the system pin-out configuration used in this text.

Step 4: Solder the wire on the PCB of your phone as seen in Figure 6 or use a jig when convenient. With the package of Riff. Figure 33 demonstrates how the JTAG soldering cable feels and Figure 7 shows the JTAG cable.

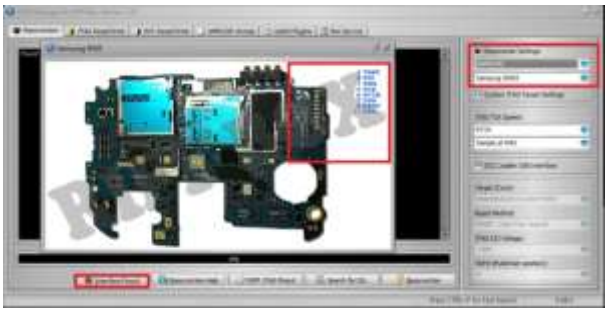


Figure 6: Resurrector Settings and JTAG Interface Pinout

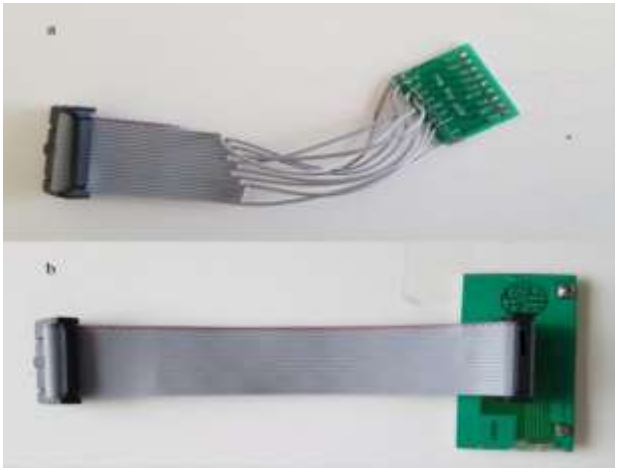


Figure 7: Riff Box JTAG connection

5.1 JTAG Acquisition Process

When the system is linked with the Riff package, it is time for the acquisition and as with ISP the procedure is reasonably easy. Below figure 8 shows Samsung Galaxy S4 I9505 connected to Riff Box via jig

Figure 8: Samsung Galaxy S4 I9505 connected to Riff Box via jig

Step 1: Open the tab "JTAG Read/Write."

Step 2: Pick the maker and model of the unit on "Resurector settings." This choice will only display the versions you have previously downloaded, as mentioned in the previous paragraph. If the system is not supported, then step 3 could otherwise be preceded by step 4.

Step 3: If the system from the riff box doesn't help, pick "Custom JTAG Target Settings."

- Begin with maximum 'JTAG TCK Rpm' and start lowering every time.
- "Target Core" selects a CPU unit, choosing a comparable one if not sponsored.
- Any unverified examination should be conducted first in a system similar to the original.
- JTAG I/O begins with 1.8V and if appropriate switches to higher values.

Step 4: Only the last four choices are clickable at the beginning. Tap on 'Link & Get ID' to display a notice that a 'dead body' has been found and all choices are now clickable, figure 9.

Step 5: Press the "Read Memory" button and wait for the software to end. You can have to test a couple times before it functions, Figure 35.

Step 6: Disk picture processing using some forensic instrument.

For this method DC power was required and the power supply supplied a large volume of current during the set-up due to a misconfiguration or system malfunction, which weakened the unit unrecoverably, with current equipment and time. Due to this case, a JTAG acquisition was not necessary. This tragic incident can be a warning of how cautious an examiner is to operate on original instruments in actual cases.

Figure 9: Riff Box JTAG Read/Write Tab

6. LIMITATION

The drawback of this analysis is the number of measuring instruments and access to suitable equipment. Two cameras, the Samsung Galaxy S4 I9505 with Android 5.1 and the Nokia Lumia 635 will be used for this paper. The Nokia system will be used to recognise the eMMC TAP and the ISP, while the Samsung device is used to measure the acquisition of JTAG, to evaluate various acquisition

methods and to examine the disc image of an encrypted device.

7. CONCLUSION

Data acquisition may be divided into logical, file system and physical, and more than one methodology might be applicable within each type. Any of the data acquisitions are as straightforward as attaching the computer to a different device, for example. Cellebrite UFED Contact conceptual acquisition when others are more sophisticated and can affect the computer, for example. Acquisition of JTAG and ISP. This article focuses on providing a rundown of JTAG and ISP sales as well as details on the numerous forms of acquisitions as well as encrypted computer instances.

REFERENCES

[1] "Smartphone users worldwide 2014-2020,". [Online]. Available: https://www.statista.com/statistics/330695/number-of-smartphone-usersworldwide/.

[2] "Mobile device forensics," [Online]. Available:https://en.wikipedia.org/wiki/Mobile_device_forensics.

[3] "IDC: Smartphone OS Market Share". [Online]. Available: http://www.idc.com/promo/smartphone marketshare/os;jsessionid=9331D99BA89FE54BBA 1A553649669DF7.

[4] A. Hoog, Android Forensics: Investigation, Analysis and Mobile Security for Google Android, 1 ed., Syngress, 2011.

[5] "Digital forensics," [Online]. Available: https://en.wikipedia.org/wiki/Digital_forensics .

[6] "Digital Forensic Process," [Online]. https://en.wikipedia.org/wiki/Digital_forensic_process.

[7] SWGDE, SWGDE Best Practices for Mobile Phone Forensics, 2.0 ed., 2013.

[8] "Cellebrite - Explaining Cellebrite UFED Data Extraction Processes," [Online]. Available: http://www.cellebrite.com/pages/explaining-cellebrite-ufed-dataextraction-processes.

[9] "Android Debug Bridge | Android Studio," [Online]. https://developer.android.com/studio/command-line/adb.html.

[10] D. Stieben, "What Is A Nandroid Backup and How Exactly Does It Work?," [Online]. Available: http://www.makeuseof.com/tag/what-is-a-nandroidbackup-and-how-exactly-does-it-work/.

[11] J. T. A. G. (JTAG), "IEEE Standard 1149.1 (JTAG) in the SX/RTSX/SXA/eX/RT54SX-S".Patent 1149.1, 05 2012.

[12] "JTAG, Chip-off & ISP Training and Equipment Guide," [Online]. Available: http://www.teeltech.com/mobile-device-forensics-training/equipment-guide/.

[13] J. Reyes-Rodriguez, JTAG Tool Testing, 2016.

[14] SWGDE, Best Practices for Examining Mobile Phones Using JTAG, 1.0 ed., 2015.

[15] J. Swauger, "Chip-Off Forensics," Extracting a full bit-stream image from devices containing embedded flash memory, pp. 52-56, 2012.

[16] D. Tindall and R. Tamma, Learning Android Forensics, 2015.

[17] V. Djagilev, "Android Chat Application Forensic Process Improvement & XRY Support," Tartu University, Tallinn, 2017.

Corresponding Author

Dr. Sridevi*

Department of Computer Science, Karnatak University, Dharwad, India