2014

# Testing Framework for Mobile Device Forensics Tools

Maxwell Anobah
*Stockholm University*

Shahzad Saleem
*Stockholm University*

Oliver Popov
*Stockholm University*

# TESTING FRAMEWORK FOR MOBILE DEVICE FORENSICS TOOLS

Maxwell Anobah, Shahzad Saleem and Oliver Popov
Department of Computer and Systems Sciences
Stockholm University, Forum 100, Isafjordsgatan 39
SE- 16440 Kista, Sweden
{maxw-ano, shahzads, popov}@dsv.su.se

## ABSTRACT

The proliferation of mobile communication and computing devices, in particular smart mobile phones, is almost paralleled with the increasing number of mobile device forensics tools in the market. Each mobile forensics tool vendor, on one hand claims to have a tool that is best in terms of performance, while on the other hand each tool vendor seems to be using different standards for testing their tools and thereby defining what support means differently. To overcome this problem, a testing framework based on a series of tests ranging from basic forensics tasks such as file system reconstruction up to more complex ones countering anti-forensic techniques is proposed. The framework, which is an extension of an existing effort done in 2010, prescribes a method to clearly circumscribe the term support into precise levels. It also gives an idea of the standard to be developed and accepted by the forensic community that will make it easier for forensics investigators to quickly select the most appropriate tool for a particular mobile device.

**Keywords**: mobile device forensics, digital forensics, forensics tool testing, forensics tool evaluation, testing framework, support profiles

## 1. INTRODUCTION

The number of mobile devices (MD) is increasing (Baggili, Mislan, & Rogers, 2007), as well as the ways they are being used in our everyday professional and private activities. This is evidenced, for example, through the immense growth of cellular subscriptions (which is expected to reach almost seven billion by the end of 2014 (International Telecommunication Union (ITU), 2014) and the volume of SMS exchanged that was close to 6.1 trillion in 2010 (International Telecommunication Union (ITU), 2010). Butler also stated that, 41% of the population uses the embedded digital cameras in their mobile phones, while 13%, 10% and 21% use them for internet access, radio access and mini games respectively (Butler, 2010).

Modalities of how mobile devices are being used range from simple voice calls, audio/video conferencing, emails, short messages, social networking media, chatting, internet browsing, GPS navigation, pictures, videos, and standalone application. MDs are a very good source of information regarding various activities of their users and thus serve as some kind of digital behavioral archives (Gonzalez, Hung, & Friedberg, 2011). The artifacts thus produced potentially create a wealth of digital evidence possibly highly relevant to different law-enforcement organizations and legal institutions (such as criminal and civil court cases) (Butler, 2010).

Numerous criminal offenders have been convicted partly due to the evidence from either their mobile phones and/or those of their respective victims. In fact, more than 80% of court cases in US have some form of

digital evidence linked to them (Baggili et al., 2007; Butler, 2010). Consequently, the need and the demand for tools that are capable of extracting, archiving, reconstructing, analyzing and presenting digital evidence (termed as mobile device forensics tools or MDFT) is on the rise. Most often two or more tools are used to extract data from mobile devices (for instance smart phones) to validate the results and to ensure that not a single piece of information has been missed or lost (Armstrong, 2003; Butler, 2010).

That is why, (Jansen, Delaitre, & Moenner, 2008) assert that these tools should be reliable enough to provide valid results, which can be admissible in the court of law. In the course of this research, the term validity refers to the ability of the tool to identify, extract and reconstruct a digital object in the same state as the MD user was presented with. This includes the reconstruction of the binary content of the file (even if fragmented) and the ability to represent any file objects with the corresponding metadata via its 'natural' application.

In addition, (Ahmed & Dharaskar, 2008) elaborate that digital evidence is a necessity as users now use their mobile phones to store almost any kind of information about themselves, which underlines the requirements that MDFTs have to extract electronic evidence without altering any data (Al-Zarouni, 2006). This can be done only by tools that fully support a particular function in the extraction process, hence no mobile forensic tool can claim to fully support any particular phone (MSAB Blog, 2011). Their compatibility and abilities should be explicitly stated to help an investigator in the selection of an appropriate tool.

The engineering behind the commercial MDFTs is usually proprietary and not clear to the investigators. On the other side, the open source tools are not documented properly and they undergo constant changes with respect to their design and functionalities (Baggili et al., 2007). Since the role of MDFT in digital investigations is crucial and potentially definitive in deciding the outcome of legal cases, investigators need to be assured in the accuracy of the tools or their potential error rates, which qualifies the extent of support to mobile devices and eventually its quantification (Baggili et al., 2007; MSAB Blog, 2011).

Currently, the only framework available is from the National Institute of Standards and Technology (NIST) (Baggili et al., 2007; National Institute of Standards and Technology (NIST), 2010a, 2010b), which is being used as a set of recommendations rather than a standard for MDFT testing (Baggili et al., 2007). The framework was defined in 2010, and it is obvious that in the meantime mobile devices have evolved a lot so modification and extension to the specifications and associated test plans are truly needed.

The tools should produce valid results based on what is really needed in terms of data objects that are admissible in the court of law (Jansen et al., 2008). Most of the investigators face a great challenge of selecting the appropriate tool capable of producing a forensically sound evidence (Kubi, Saleem, & Popov, 2011; Saleem, Popov, & Baggili, 2014; Saleem, Popov, & Kubi, 2013; Saleem & Popov, 2013). Therefore, we need a standardized tool testing framework for MDFTs.

## 1.1 Research Problem

Due to the lack of any standards, each tool vendor defines the term 'support' differently. This creates enormous and challenging difficulties for an investigator to know and understand what each tool vendor means by the term 'supported'. Most of the forensic tool vendors claim to support the highest number of phones, which has become the central focus rather than the quality (for instance the capability and the accuracy) of the respective tool (Curran, Robinson, Peacocke, & Cassidy, 2010; MSAB Blog, 2011). These mobile forensic tools are important to law

enforcement agencies in solving criminal investigations. However, if the results produced by these tools are incorrect or the tool does not perform well for the important types of evidence in a specific case then the results might be deemed inadmissible in the court of law (Guo, Slay, & Beckett, 2009).

Once a tool vendor claims support for a phone, the term support should be qualified. Sometimes extraction of call logs and text messages alone is enough for an MD to be included into the list of supported MDs. This means that the term support is ambiguous and subjective as it does not reflect the real level of support a tool has for a specified MD. Hence, each tool has its own capabilities required to be bench marked (Ahmed & Dharaskar, 2008; MSAB Blog, 2011).

The evolution in MDs capabilities, ranging from battery life, memory, processing power, and the changes in the computing and communications paradigms through virtualization, cloud computing, distributed network storage, combined with useful spectrum of applications has transformed them into rather powerful computing and communications devices. The level of configuration and personalization in the MDs is also on the rise. Modern MDs are very flexible and provide interfaces for various tasks which have also opened possibilities to easily exploit anti-forensics techniques. The user of an older MD (for example Nokia 3310) cannot change for instance the default location settings of data objects generated as a consequence of the normal usage of the device. However with the new smartphones, the user can manipulate these default location settings or even install other third party applications to change the contents of the corresponding data objects.

Text messages can be a good example to understand the complexities being encountered by the forensics tools. These messages are now not only generated by the native application in SMS format but also by many third party apps (for example Handcent, Viber, Whatsapp, Twitter, Skype

and Hangout). Every application provides different levels of customization and operates on different standards and formats to work with the corresponding data objects. In order to answer these questions, a framework is proposed to check the quality of data extracted by a mobile forensic tool with emphasis on anti-forensic techniques and to quantify the term "supported" in the context of a MDFT.

## 1.2 Related Work

NIST has evaluated some MDFTs against their specifications and published the results (National Institute of Standards and Technology (NIST), 2013). NIST specifications (National Institute of Standards and Technology (NIST), 2010a) have six core and fifteen optional requirements. In addition, the work has proposed a tool testing plan (National Institute of Standards and Technology (NIST), 2010b) based on these specifications (National Institute of Standards and Technology (NIST), 2010a). The plan has thirty two (32) compulsory assertions and forty four (44) optional assertions. NIST has defined the following twenty (20) profiles by using different combinations of these seventy six (76) assertions.

1. Connectivity (between the tool and the MD)
2. Data Acquisition and Interpretation
   a. Presentation
   b. Subscriber and Equipment Related Data
   c. Personal Information Management (PIM) Data
   d. Call Logs
   e. Text Messages (SMS, EMS, MMS)
   f. Stand-alone Multi-media Data
   g. Application Data
   h. Internet Related Data
3. Location Related Data
4. Tool Acquisition Variations
5. Device Data Not Modified
6. Generated Reports / Preview-Pane
7. Case File/Data Protection

8. SIM PIN/PUK Authentication
9. Physical Acquisition
10. Non-ASCII Character Presentation
11. Stand-alone Acquisition
12. Hashing
13. GPS Reporting

Similarly some formal techniques were also presented (Kubi et al., 2011; Saleem et al., 2014, 2013; Saleem & Popov, 2013) to help select the most appropriate tool. All of them relied on the specifications by NIST that were defined in 2010. One of the obvious problems associated with NIST specification is that, MDs (since 2010) have gone through so many changes that a revision and enrichment to these specifications and corresponding test plans is required.

The remaining sections of this paper explain the terms being used in the introduction, the extension to the NIST testing plan and its evaluation using two MDFTs. Discussion on the standard used to quantify the term "support" for all the twenty profiles is followed by a concluding section that includes a discussion on the framework, its application, the test results and the direction of future research in this domain.

# 2. MOBILE DEVICE FORENSICS

Mobile Device Forensics (MoDeFo) is a branch of digital forensics where the main goal is the retrieval of data or evidence from MDs and similar devices (Bhadsavle & Wang, 2009). MoDeFo is based on proven scientific methodologies to collect facts regarding an object, an artifact, or an event in a specific time frame in order to determine if the object under consideration claims to be or is just alleges its existence (Casey, 2009).

As posited earlier, MDs have become dynamic mobile computing platforms due to the constant upgrades, changes and new additions. The lack of forensic tools that will be able to retrieve data and thereby be compatible with the continuous surge of new mobile device models is a problem being faced

by the experts in MoDeFo (Bhadsavle & Wang, 2009).

## 2.1 Sources of Evidence

Gonzalez et al. (2011) outlined major types of evidence that can be obtained from MDs. These include call logs, SMS, contacts, calendar, memos, multimedia items, notes, videos, maps, internet browsing history, screenshots, voicemails, wireless network data etc. They also explain some of the challenges that arise when it comes to MoDeFo and the potential outcomes from an investigation.

For instance, Curran et al. (2010) state that, the most viable evidence that gives a clear cut between traditional computers and mobile phones is the location data. The hint about the specific location of the person at the time of an incident is important for numerous investigations. This important piece of location data may be obtained from various sources of the MDs (Gonzalez et al., 2011).

## 2.2 Mobile Device Forensics Tools

MDFTs are the main tools aside synchronization software, which are used in the extraction of data from MDs (Jansen et al., 2008). In fact, they form an interface with which the examiner can connect to the MD to view, extract or examine its contents (Williamson & Apeldoorn, 2005). For extracted data to be admissible in the court of law, a forensic expert should be able to show that the data is forensically sound which means that it has not been tampered with during the entire investigation process (Casey, 2009). Two MDFTs were selected to test the proposed framework. Their names are kept confidential and hence are denoted by the variables "U" and "X".

## 2.3 Extraction Methods

Manual extraction, logical extraction and physical extraction are the three main methods used to extract data from MDs. We used logical and physical extraction and a

brief introduction of these methods is given below.

### 2.3.1 Manual Extraction

In this type of extraction the examiners go through the documentation of an MD and manually access and record information on the screen (Brothers, 2007; Casey, 2011). Documentation is done to preserve the chain of custody and to ensure that every detail is well captured/recorded. In this case, data which is accessible through the operating system is retrieved and captured either by photographing or videotaping (Casey, 2011). Physically damaged phone is a problem with this type of extraction such as the case when the keys fail to respond and the screen has cracks or it is damaged (Brothers, 2007).

### 2.3.2 Logical Extraction

In logical extraction, a connection is established between the mobile devices and the computer of the examiner via Bluetooth, cable or infra-red interface using protocols such as OBEX, BREW, AT commands and F-BUS. Only data which is accessible through the operating system is extracted and communication works only through a client/server mode (Brothers, 2007; Casey, 2011).

Disabled data port is a major problem with this type of extraction (Brothers, 2007). If a phone has a security code enabled and the modem mode disabled then the phone needs to be set to modem mode before logical extraction can proceed (due to the need for inter device communication). Moreover, if the phone is locked and the modem port is also disabled then it becomes difficult to do extraction and one may need to resort to a manual extraction.

### 2.3.3 Physical Extraction

Physical extraction deals with mining of the entire memory content through communication ports. It is accomplished by using a boot loader or an unsigned code which is pushed into the memory of the mobile

phone. The data that is pushed out through the communication conduit is stored in a raw HEX or binary format. The interpretation of the binary data is dependent on how the data is stored in the memory of the phone. An example of the interfaces used in this type of extraction is the JTAG interface. It allows a complete extraction of the memory. Many of the mobile forensic tool vendors have begun to support more phones in this type of extraction over the last couple of years. (Brothers, 2007; Casey, 2011)

This type of extraction is time consuming and the output is difficult to analyze. Dumped and decoded data cannot be easily compared to what is seen on the interface of the MD.

## 2.4 Anti Forensics

For long, criminals have used anti-forensics techniques to thwart evidence on weapons or other artifacts they have used in a crime scene and thus misleading investigators to make wrong conclusions (Ispirian, 2013). Wearing gloves to avoid finger prints on the weapons used in the crime was one of the simple yet effective techniques. In a similar way, the wrongdoers have implored the concept of anti-forensic techniques to cover their digital foot prints. The term "anti-forensics" therefore refer to a combination of software tools and techniques designed to impede the digital investigation and to make it difficult for a forensic examiner to find or locate data, or to make potential evidence inadmissible in the court of law (Ispirian, 2013).

### 2.4.1 Anti-Forensic Methods

There are four main methods to perform anti-forensics namely, data contraception, data hiding, data destruction and data misdirection (Bilby, 2006).

1. Data Contraception: prevents the potential evidence from existing somewhere on the phones memory where it can be analyzed. For example, using a memory only malware to force execution on just a

certain part of the phone's main memory.

2. Data Hiding: In this case, potential evidence data is put on the disk somewhere unlikely for the forensic tools to locate. For example, placing a picture in the root directory of a rooted/jail broken MD, as the forensic tools may go to the default picture related folders to extract them as evidence.

3. Data Destruction: involves destroying any evidence before a forensics activity (such as wiping the memory by a special application). It may be used to manipulate the potential data stored in the phone memory according to a set of user specified instructions, such as slowing down the connectivity to the forensic tool and then deleting potential evidence data before allowing the tool to start extraction.

4. Data Misdirection: provides the forensic tools with false data that is indistinguishable from the real thing. For example, changing a .pdf file to an .exe file and thus making it look like an executable.

It is really hard to extract any useful information after data destruction. In this case finding unique patterns in the memory or the artifacts related to a data destruction tool are usually enough to convict an individual for spoliation. Similarly, data contraception is related to physical memory or RAM analysis so out of the scope of this work and the proposed framework. Therefore, the remaining two methods (data hiding and data misdirection) were used in creating and testing the proposed framework.

# 3. MOS[1] TESTING FRAMEWORK FOR MOBILE DEVICE FORENSICS

The basic aim of the framework is the evaluation of MDFTs with emphasis on anti-

forensics and quantification of the term "support". In addition, it provides some level of quality assurance for the performance of the tool with respect to a specific profile. Quality assurance is defined as *"a planned and systematic pattern of all the actions which are necessary to provide adequate confidence that an item or a product conforms to established technical requirements."* (Radatz, Geraci, & Katki, 1990)

The framework is based on the Carrier's attribute list (Carrier, 2003). The list outlines the following major attributes that a digital forensic tool must possess:

1. Usability: is the ability of a tool to present evidence in accurate and unambiguous format so as to prevent misinterpretation.

2. Comprehensive: is the ability of a tool to present all the forms of extracted evidence inclusive of exculpatory and inculpatory evidence.

3. Accuracy: is the ability of a tool to present extracted evidence accurately with a known margin of error to ensure the correctness of the results.

4. Deterministic: is the ability of a tool to produce consistent results.

5. Verifiable: is the ability of a tool to ensure accuracy of the results either via using an independent tool or manual means.

MOS framework actually extends the test plan from NIST by including assertions and test actions to cover anti-forensics as well. The section below will only discuss the new profiles introduced by our framework. The ones not discussed must be treated in accordance to the original NIST test plan (National Institute of Standards and Technology (NIST), 2010b).

## 3.1 Personal Information Management (PIM)

Assertion MOS-AO-01: If a cellular forensic tool completes acquisition of the target device without error then address book entries shall be presented in a useable format even if some

---

[1] Maxwell, Oliver and Shahzad

fields are manipulated with data hiding or misdirecting intentions.

Assertion MOS-AO-02: If a cellular forensic tool completes acquisition of the target device without any error then datebook, calendar and note entries shall be presented in a useable format, even if the associated data is hidden or misdirected by setting wrong date and time stamps.

Test Action: Populate integer fields and leave character fields empty.

Test Action: Populate character fields and leave integer fields empty.

Test Action: Set calendar entries to "x" years later or earlier. Whereas x = 1,2,3...

Conformance Indicator: Acquired PIM data matches known PIM data for all test cases.

## 3.2 Call Logs

Assertion MOS-AO-03: If a cellular forensic tool completes acquisition of a target device without error then the corresponding date/timestamps and the duration of the call shall be presented in a useable format and it should be reported in UTC to counter any impact of the change in the time zone.

Test Action: Populate the internal memory with incoming calls

Test Action: Populate the internal memory with missed calls

Test Action: Populate the internal memory with outgoing calls

Conformance Indicator: Acquired call log data matches known call log data, acquired timestamp is reported in UTC for all calls and all the fields/attributes are duly reported.

## 3.3 Text Messages (EMS, SMS, MMS and Third Party Applications)

Class of text messages shall not be confined to the messages originating from the native applications in the form of EMS, SMS and MMS only, but artifacts associated with all

the sorts of text messaging applications should be included (for instance, Skype, Viber, Whatsapp, Twitter, Facebook). Hence all the instances of EMS, SMS and MMS in all the appropriate core and optional assertions must be replaced, tested and evaluated against this generic class of messages.

Assertion MOS-AO-04: If a cellular forensic tool completes acquisition of the target device without error then text messages not only from the default location but from any possible location shall be presented in a useable format to counter any data hiding attempts.

Assertion MOS-AO-05: If a cellular forensic tool completes acquisition of the target device without error then the corresponding date/time stamps for text messages shall be presented in useable format and reported in UTC to counter any impact of the change in time zone.

Assertion MOS-AO-06: If a cellular forensic tool completes acquisition of the target device without error then text messages even if locked shall be presented in a useable format to counter any data hiding attempts.

Test Action: If MD has the capability, then create a new folder and move messages to the newly created folder.

Test Action: Change the time zone of the device before beginning data population.

Test Action: If MD has lock feature, activate the lock on all the possible messages.

Conformance Indicator: Acquired text messages match known text messages, timestamps are reported in UTC/Device and all entries from all the locations and all the fields duly reported.

## 3.4 Stand-alone Multi-media Data (Audio, Video and Graphics)

Assertion MOS-AO-07: If a cellular forensic tool completes acquisition of the target device without error then stand-alone multi-media

files both from default and any other location shall be presented in a useable format.

Test Action: Populate data into the default folder.

Test Action: If the device has capability, create a new folder and move files into the newly created folder

Conformance Indicator: Acquired multi-media matches known multi-media data for both test cases.

Assertion MOS-AO-08: If a cellular forensic tool completes acquisition of the target device without error then stand-alone multi-media files with missing header/footer shall be presented in a useable format.

Test Action: Populate the MD with multi-media files having headers and or footers modified. Hex Editor by NEO was used to modify the headers and footers of different files.

Test Action: Relocate files to a non-default location.

Conformance Indicator: Acquired multi-media data matches the known multi-media data for both cases and the status of the data reported as tempered or corrupted[2].

Assertion MOS-AO-09: If a cellular forensic tool completes acquisition of the target device without error then stand-alone multi-media files with missing/modified extensions shall be presented in a useable format.

Test Action: Populate the device default location with files having file extensions modified.

Test Action: Relocate the files to non-default location.

Conformance Indicator: Acquired multi-media data matches the known multi-media data for both cases and the tool reports the exact file type.

Assertion MOS-AO-10: If a cellular forensic tool completes acquisition of the target device without error then stand-alone multi-media files which are corrupted shall be presented as corrupted.

Test Action: Populate the device default location with corrupted files.

Test Action: Relocate corrupted files to non-default locations.

Conformance Indicator: The acquired multi-media data matches the known multi-media data and the device also reports that the file has been tampered or corrupted.

Assertion MOS-AO-11: If a cellular forensic tool provides support for multi-media files of the target device then the tool shall successfully acquire large data from the target device without error.

Test Action: Populate device default location with large multi-media files.

Test Action: Relocate large multi-media files to non-default locations.

Conformance Indicator: Acquired multi-media data matches the known multi-media data and the extraction does not terminate prematurely.

## 3.5 Application Data

Application data means data in the form of text documents, spreadsheet, power-points, pdf and other document formats.

Assertion MOS-AO-12: If a cellular forensic tool completes acquisition of the target device without error then application data files both from default and any other location shall be presented in a useable format.

Test Action: Populate device data into the default folders.

Test Action: If the device has capability, create a new folder and move files into the newly created folder

---

[2] Corrupted in the sense of header/footer or extension(s)

Conformance Indicator: Acquired application data matches the known application data for both the test cases.

Assertion MOS-AO-13: If a cellular forensic tool completes the acquisition of the target device without error then application data files with missing header/footer shall be presented in a useable format.

Test Action: Populate the device default location with files having header and footer modified.

Test Action: Relocate files to non-default locations.

Conformance Indicator: Acquired application data matches the known application data for both the cases and the data are reported as tempered corrupted.

Assertion MOS-AO-14: If a cellular forensic tool completes the acquisition of the target device without error then application data files with missing/modified extensions shall be presented in a useable format.

Test Action: Populate device default location with files having file extensions modified.

Test Action: Relocate files to non-default location.

Conformance Indicator: Acquired application data matches the known application data for both cases.

Assertion MOS-AO-15: If a cellular forensic tool provides support for application data files of the target device then the tool shall successfully acquire large data files from the target device without any error.

Test Action: Populate device default locations with large files.

Test Action: Relocate these files to non-default locations.

Conformance Indicator: Acquired application data matches the known application data. Extraction does not terminate prematurely.

Assertion MOS-AO-16: If a cellular forensic tool completes the acquisition of the target device without an error then application data files which are corrupted shall be presented as corrupted.

Test Action: Populate device default locations with corrupted files.

Test Action: Relocate corrupted files to non-default locations.

Conformance Indicator: Acquired application data matches the known application data and the tool reports that the file has been tampered with or corrupted.

# 4. EVALUATING MOS TESTING FRAMEWORK

The framework was evaluated by testing the aforementioned tools via experimentation (Ayers, 2007). The results were documented and a method to quantify the level of the term "support" was also introduced.

Each tool was tested against all the test assertions including seventy six (76) from NIST test plan and sixteen (16) from MOS framework. For each assertion the tool was awarded a number from 0, 1 or 2 depending on the following criteria.

a) 2 – Obtained results conform to the expected results. It means that the data was found and duly reported

b) 1 – Obtained results were rather closer to the expected results, which mean that the assertion was on borderline (neither passed nor failed).

c) 0 – Obtained results did not conform to the expected results or not found.

Then the tool was assigned grades for each of the twenty profiles using equation (1) and equation (2). The grades can help quantify the term support for each profile. Grading was done for NIST assertions alone (Equation 1), MOS assertions alone (Equation 1) and the combination of NIST and MOS assertions (Equation 2). The framework increased the resolution of quantification levels for the term support to suit the requirements of an

investigator and give him an opportunity to select the appropriate tool for his/her needs.

Table 1 Grading Scale

| Support Level | Percentage Score |
|---|---|
| $A_1 - A_{10}$ | 91 -100 |
| $B_1 - B_{10}$ | 81 - 90 |
| $C_1 - C_{10}$ | 71-80 |
| $D_1 - D_{10}$ | 61-70 |
| $E_1 - E_{10}$ | 51-60 |
| F | score $\leq$ 50 |

$$\text{score} = (p \div n) \times 100 \qquad (1)$$

$$\text{score}_{\text{combined}} = (2 \times CA + AO) \div 3 \qquad (2)$$

Whereas, p = total points obtained for a specific profile and n = total number points for that specific profile. Each assertion can give a maximum of two (2) points and a tool can obtain any discrete point from zero (0) to two (2) depending on the test results. score$_{\text{combined}}$ represents the combined score of both compulsory assertions (CA) and optional assertions (AO) for a profile. CA were given double the importance than AO while calculating score$_{\text{combined}}$ (Equation 2). Grading is done following the scale in Table 1.

# 5. RESULTS AND DISCUSSION

Table 2 represents the evaluation results of our framework. Two tools "X" and "U" were tested for all the new sixteen assertions in MOS and seventy six assertions in NIST using two MDs (Samsung Galaxy S4 Gt-i9505 and iPhone 4 A1332). The results of all these assertions were used to get the grades for each profile. There are six grades (A to F) and each grade has then ten steps within (1 to 10) to increase the resolution. It has a potential to precisely quantify the level of support for each tool in a given profile.

Table 2 represents the evaluation results in three forms. It has the evaluation results against the new assertions introduced in MOS only (using Equation 1), assertions in NIST only (using Equation 1) and all the assertions in NIST and MOS combined (using Equation 2). It can help quantify the level of support for anti-forensics only, NIST only and combined depending on the requirements of the case being investigated. Table 2 shows that tool "X" scores better grades for most of the profiles in MOS only, NIST only and MOS+NIST.

Table 2 Evaluation Results

| | Support Level | MOS | | NIST | | MOS+NIST | |
|---|---|---|---|---|---|---|---|
| | | X | U | X | U | X | U |
| | Connectivity (between the tool and the MD) | | | $E_6$ | $D_7$ | $E_6$ | $D_7$ |
| Data Acquisition and Interpretation | --Presentation | | | $A_{10}$ | $A_{10}$ | $A_{10}$ | $A_{10}$ |
| | --Subscriber and Equipment Related Data | | | $A_{10}$ | $D_7$ | $A_{10}$ | $D_7$ |
| | --Personal Information Management (PIM) Data | $A_{10}$ | F | $C_5$ | $C_5$ | $C_8$ | $D_9$ |
| | --Call Logs | $A_{10}$ | $A_{10}$ | $A_{10}$ | $A_2$ | $A_{10}$ | $A_4$ |
| | --Text Messages | $A_{10}$ | $A_{10}$ | $A_4$ | $B_7$ | $A_6$ | $B_{10}$ |
| | --Stand-alone Multi-media Data | $C_{10}$ | F | $A_{10}$ | $A_{10}$ | $A_3$ | $C_{10}$ |
| | --Application Data | $D_3$ | F | F | $A_{10}$ | $E_4$ | $C_5$ |
| | --Internet Related Data | | | $A_{10}$ | $A_{10}$ | $A_{10}$ | $A_{10}$ |
| | Location Related Data | | | $A_{10}$ | $A_{10}$ | $A_{10}$ | $A_{10}$ |
| | Tool Acquisition Variations | | | $C_8$ | $C_8$ | $C_8$ | $C_8$ |
| | Device Data Not Modified | | | $A_{10}$ | $A_{10}$ | $A_{10}$ | $A_{10}$ |

| | | | | | | |
|---|---|---|---|---|---|---|
| Generated Reports / Preview-Pane | | | $A_{10}$ | $A_{10}$ | $A_{10}$ | $A_{10}$ |
| Case File/Data Protection | | | F | F | F | F |
| SIM PIN/PUK Authentication | | | $A_{10}$ | $D_7$ | $A_{10}$ | $D_7$ |
| Physical Acquisition | | | F | $D_7$ | F | $D_7$ |
| Non-ASCII Character Presentation | | | $A_{10}$ | F | $A_{10}$ | F |
| Stand-alone Acquisition | | | $A_{10}$ | $A_{10}$ | $A_{10}$ | $A_{10}$ |
| Hashing | | | F | F | F | F |
| GPS Reporting | | | $A_{10}$ | $A_{10}$ | $A_{10}$ | $A_{10}$ |

Table 3 Individual scores for each assertion in NIST and MOS

| Assertion | X | U | Assertion | X | U | Assertion | X | U |
|---|---|---|---|---|---|---|---|---|
| SPT-CA-01 | 2 | 2 | SPT-CA-32 | 2 | 2 | SPT-OA-31 | 2 | 2 |
| SPT-CA-02 | 0 | 0 | SPT-OA-01 | 2 | 2 | SPT-OA-32 | 1 | 2 |
| SPT-CA-03 | 1 | 2 | SPT-OA-02 | 0 | 0 | SPT-OA-33 | 0 | 1 |
| SPT-CA-04 | 2 | 2 | SPT-OA-03 | 2 | 2 | SPT-OA-34 | 1 | 1 |
| SPT-CA-05 | 2 | 0 | SPT-OA-04 | 2 | 2 | SPT-OA-35 | 1 | 1 |
| SPT-CA-06 | 2 | 2 | SPT-OA-05 | 2 | 2 | SPT-OA-36 | 1 | 1 |
| SPT-CA-07 | 2 | 1 | SPT-OA-06 | 2 | 2 | SPT-OA-37 | 1 | 1 |
| SPT-CA-08 | 2 | 2 | SPT-OA-07 | 2 | 2 | SPT-OA-38 | 1 | 2 |
| SPT-CA-09 | 2 | 1 | SPT-OA-08 | 2 | 2 | SPT-OA-39 | 1 | 1 |
| SPT-CA-10 | 0 | 0 | SPT-OA-09 | 2 | 2 | SPT-OA-40 | 2 | 1 |
| SPT-CA-11 | 0 | 2 | SPT-OA-10 | 2 | 1 | SPT-OA-41 | 2 | 1 |
| SPT-CA-12 | 2 | 2 | SPT-OA-11 | 0 | 0 | SPT-OA-42 | 2 | 2 |
| SPT-CA-13 | 2 | 2 | SPT-OA-12 | 2 | 2 | SPT-OA-43 | 0 | 0 |
| SPT-CA-14 | 2 | 2 | SPT-OA-13 | 2 | 1 | SPT-OA-44 | 2 | 2 |
| SPT-CA-15 | 2 | 2 | SPT-OA-14 | 2 | 2 | MOS-AO-01 | 2 | 1 |
| SPT-CA-16 | 2 | 2 | SPT-OA-15 | 2 | 2 | MOS-AO-02 | 2 | 1 |
| SPT-CA-17 | 2 | 2 | SPT-OA-16 | 2 | 1 | MOS-AO-03 | 2 | 2 |
| SPT-CA-18 | 2 | 2 | SPT-OA-17 | 2 | 2 | MOS-AO-04 | 2 | 2 |
| SPT-CA-19 | 2 | 2 | SPT-OA-18 | 2 | 2 | MOS-AO-05 | 2 | 2 |
| SPT-CA-20 | 2 | 1 | SPT-OA-19 | 0 | 0 | MOS-AO-06 | 2 | 2 |
| SPT-CA-21 | 2 | 2 | SPT-OA-20 | 2 | 2 | MOS-AO-07 | 2 | 2 |
| SPT-CA-22 | 2 | 2 | SPT-OA-21 | 2 | 2 | MOS-AO-08 | 2 | 2 |
| SPT-CA-23 | 2 | 2 | SPT-OA-22 | 2 | 2 | MOS-AO-09 | 2 | 0 |
| SPT-CA-24 | 2 | 2 | SPT-OA-23 | 0 | 0 | MOS-AO-10 | 0 | 0 |
| SPT-CA-25 | 2 | 2 | SPT-OA-24 | 0 | 0 | MOS-AO-11 | 2 | 0 |
| SPT-CA-26 | 2 | 2 | SPT-OA-25 | 2 | 2 | MOS-AO-12 | 2 | 2 |
| SPT-CA-27 | 1 | 2 | SPT-OA-26 | 2 | 2 | MOS-AO-13 | 1 | 2 |
| SPT-CA-28 | 2 | 2 | SPT-OA-27 | 0 | 0 | MOS-AO-14 | 2 | 0 |
| SPT-CA-29 | 2 | 2 | SPT-OA-28 | 2 | 2 | MOS-AO-15 | 2 | 0 |
| SPT-CA-30 | 2 | 2 | SPT-OA-29 | 2 | 1 | MOS-AO-16 | 0 | 0 |
| SPT-CA-31 | 2 | 2 | SPT-OA-30 | 2 | 1 | | | |

Table 3 carries the raw results in the form of assertions with their obtained marks for both "X" and "U" tools. These were used in equation (1), equation (2) to calculate the combined scores. Combined scores were used in the light of the scale (Table 1) to calculate the grades representing the level of support for each profile.

# 6. CONCLUSION

The increasing capabilities of the mobile devices, as well as the ongoing changes in the communication and computing paradigms, in addition to global wide-spread usage and many benefits in the professional and private activities to their users, has also opened up many opportunities for their abuse in unwanted deeds and actions including the use of anti-forensics techniques to avoid detection while being investigated. Moreover, the sophistication of the users and available applications makes it much easier to exploit various anti-forensics techniques in order to hinder prospective digital investigations. In order to address these challenges, it was required to extend the NIST smartphone test plan with an emphasis to counter any potential anti-forensics attempts. The novel testing framework, based on the existing NIST criteria and MOS extension can evaluate a MDFT while taking care of the use of potential anti-forensics techniques as well.

As of today, we have found that the term "supported" with respect to MDFT is also subjective. Quantification of the term "support" is another advantage of using the MOS framework, as an extension of the NIST one from 2010. The framework introduces a standard to define and then tag the term support to a MDFT.

The resolution of the level of support is also quite high; hence it can potentially quantify the level of support with fairly high precision. Consequently, it can help an investigator to select the tool with an unambiguously defined support level for a particular profile. A better choice of the tool

can result in saving time and effort required to perform a digital investigation.

To the best of our knowledge, this is an innovative way of looking into the problem of MDFT evaluation. Currently, we have only introduced sixteen new assertions in only five profiles. To make the framework more robust, encompassing, and to a certain degree more general, we will explore and extend more areas (profiles) where anti-forensics techniques can potentially be employed.

# REFERENCES

Ahmed, R., & Dharaskar, R. (2008). Mobile forensics: an overview, tools, future trends and challenges from law enforcement perspective. 6th International Conference on E-Governance, ICEG, Emerging Technologies in E-Government, M-Government, 312–323. Retrieved from http://www.academia.edu/download/304 22105/34_312-323.pdf

Al-Zarouni, M. (2006). Mobile handset forensic evidence: a challenge for law enforcement. 4th Australian Digital Forensics Conference. Perth. Retrieved from http://ro.ecu.edu.au/adf/24/

Armstrong, C. (2003). Developing a framework for evaluating computer forensic tools. Evaluation in Crime Trends and justice: Trends and Methods Conference in Conjunction with the Australian Bureau of Statistics, Canberra Australia, 24-25. Canberra. Retrieved from http://www.aic.gov.au/media_library/co nferences/evaluation/armstrong.pdf

Ayers, R. (2007). Cell phone forensic tools: an overview and analysis update. Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. Retrieved from http://csrc.nist.gov/publications/nistir/n istir-7387.pdf

Baggili, I., Mislan, R., & Rogers, M. (2007). Mobile Phone Forensics Tool Testing: A Database Driven Approach. *International Journal of Digital Evidence*, *6*(2). Retrieved from http://www.utica.edu/academic/institutes/ecii/publications/articles/1C33DF76-D8D3-EFF5-47AE3681FD948D68.pdf

Bhadsavle, N., & Wang, J. (2009). Validating tools for cell phone forensics. American Society for Engineering Education (ASEE) Southeastern Section Conference. Marietta. Retrieved from http://icee.usm.edu/ICEE/conferences/ASEE-SE-2010/Conference Files/ASEE2009/papers/PR2009088WAN.PDF

Bilby, D. (2006). Low down and dirty: Anti-forensic rootkits. Proceedings of Ruxcon. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Low+Down+and+Dirty:+Anti-Forensic+Rootkits#0

Brothers, S. (2007). IPhone Tool Classification. Retrieved on March 12, 2012 from http://www.sambrothers.com

Butler, J. (2010). Forensic Analysis of Mobile Phones. Retrieved May 10, 2014, from http://www.geodeforensics.com/Images/White paper.pdf

Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. *International Journal of Digital Evidence*, *1*(4), 1–12. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.14.9813&amp;rep=rep1&amp;type=pdf

Casey, E. (2009). Digital forensics: Coming of age. *Digital Investigation*, *6*(1-2), 1-2. doi:10.1016/j.diin.2009.08.001

Casey, E. (2011). Digital evidence and computer crime: forensic science, computers, and the Internet, 3rd ed.

Curran, K., Robinson, A., Peacocke, S., & Cassidy, S. (2010). Mobile phone forensic analysis. *International Journal of Digital Crime and Forensics* (IJDCF), *2*(3), 15-27.

Gonzalez, J., Hung, J., & Friedberg, S. (2011). Mobile Device Forensics : A Brave New World. Retrieved on April 04, 2012 from http://www.strozfriedberg.com/files/Publication/224ca0f8-5101-4e1b-938a-4d4b128ad5ed/Presentation/PublicationAttachment/ef4a28ad-ff7d-4014-aea8-80505789b86c/Mobile Device Forensics_A Brave New World.pdf

Guo, Y., Slay, J., & Beckett, J. (2009). Validation and verification of computer forensic software tools-Searching Function. *Digital Investigation*, 6, S12–S22. doi:10.1016/j.diin.2009.06.015

International Telecommunication Union (ITU). (2010). The World in 2010: ICT Facts and Figures. Retrieved on May 10, 2014 from http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf

International Telecommunication Union (ITU). (2014). The World in 2014: ICT Facts and Figures. Retrieved on May 10, 2014 from http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2014-e.pdf

Ispirian. (2013). The Dark Side of Forensics. Retrieved on January 01, 2013 from http://www.ispirian.com/Articles/TheDarkSideofForensics.pdf

Jansen, W., Delaitre, A., & Moenner, L. (2008). Overcoming impediments to cell phone orensics. Proceedings of the 41st Hawaii International Conference on System Sciences, 1-9. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4439183

Kubi, A., Saleem, S., & Popov, O. (2011). Evaluation of some tools for extracting e-evidence from mobile devices.

Application of Information and Communication Technologies, 603-608. Baku: IEEE. doi:10.1109/ICAICT.2011.6110999

MSAB Blog. (2011). Mobile Forensic Controversies. Retrieved on December 09, 2011 from http://www.msab.com/posts/blog

National Institute of Standards and Technology (NIST). (2010a). Smart Phone Tool Specification, Version 1.1. Retrieved from http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Specification.pdf

National Institute of Standards and Technology (NIST). (2010b). Smart Phone Tool Test Assertions and Test Plan, Version 1.1. Test. Retrieved from http://www.cftt.nist.gov/documents/Smart_Phone_Tool_Test_Assertions_and_Test_Plan.pdf

National Institute of Standards and Technology (NIST). (2013). Computer Forensics Tool Testing Program: Mobile Devices. Retrieved on May 05, 2014 from http://www.cftt.nist.gov/mobile_devices.htm

Radatz, J., Geraci, A., & Katki, F. (1990). IEEE standard glossary of software engineering terminology. IEEE Standards Board, New York, Standard IEEE Std. doi:10.1109/IEEESTD.1990.101064

Saleem, S., & Popov, O. (2013). Formal Approach for the Selection of a Right Tool for Mobile Device Forensics. 5th International Conference on Digital Forensics & Cyber Crime. Moscow.

Saleem, S., Popov, O., & Baggili, I. (2014). Right of a Fair Trial and Selection of the Right Tool for Mobile Device Forensics. *Journal of Digital Forensics, Security and Law* (Submitted) (Vol. 9).

Saleem, S., Popov, O., & Kubi, A. (2013). Evaluating and Comparing Tools for Mobile Device Forensics using Quantitative Analysis. Digital Forensics

and Cyber Crime: Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, 114, 264-282. doi:10.1007/978-3-642-39891-9_17

Williamson, B., & Apeldoorn, P. (2005). Forensic analysis of the contents of Nokia mobile phones. In *Advances in Digital Forensics*, 191-204. Springer. Retrieved from http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1035&context=adf