Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 9 (2014) pp. 019-026
© MIR Labs, www.mirlabs.net/jias/index.html

Validation of Digital Forensics Tools for Android Tablet

Razana Md Salleh[1], Masnizah Mohd[2] and Kamarul Baharin Khalid[3]

[1] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,
Selangor, 43600 Bangi, Malaysia
razanasalleh@yahoo.com

[2] Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia,
Selangor, 43600 Bangi, Malaysia
mas@ftsm.ukm.my

[3] Security Assurance Department, CyberSecurity Malaysia,
Selangor, 43300 Seri Kembangan, Malaysia
bahar@cybersecurity.my

***Abstract*: With the continued growth of the Android mobile device market, the possibility of their use in unlawful and unethical activities will only continue to increase. While vendors and developers of a variety digital forensics tools, both commercial and open-source ones, make various assertions about the capabilities and the performance of their tools, the evaluation of digital forensics tools has been recognized as a challenging, and insufficiently examined research topic in the field of digital forensics. This paper discusses the experiment conducted to acquire data on an Android tablet using four popular digital forensics tools, namely EnCase, Mobile Phone Examiner Plus, Oxygen Forensic Suite and MOBILedit Forensic. The results of the experiment provide an understanding of the capabilities and limitations of each tool and offer an inside view for investigators to choose the appropriate digital forensics tools for acquiring internal data from an Android device.**

Keywords: Forensics, Android, tablet, acquisition, extraction, validation**.**

I. Introduction

Digital forensics is a rapidly growing discipline of the field of forensic science. Since the birth of digital forensics in 1980s [1], investigators from both private and public sectors are relying on a range of digital forensics tools to acquire and analyze digital evidence as electronic crimes continue to pose a significant problem and cause huge financial losses.

Digital forensics community is facing utmost challenges in digital forensics investigations, especially in the process of data acquisition [2]. Although investigations on personal computers (PC) can be argued to be matured, investigation that involves data acquisition and analysis on mobile devices continues to be a challenge to digital forensics investigators. One of the challenges is that commercial forensics tools require a mobile device to be switched on during data acquisition process, thus allowing it to constantly update data and receive incoming calls, text messages and emails. Second, the operating systems (OS) of mobile devices are generally closed source, with the exception of Linux-based devices, which makes creating custom tools to retrieve evidence a difficult task [3]. With the release of OS updates very often, it is hard for forensics investigators to keep up with methods and tools required to forensically examine each release. In addition to that, most devices are set to have restricted filesystems and made it difficult for forensics investigators to access evidence in the devices. The variety of proprietary hardware of mobile devices is another issue faced by forensic investigators [4]. Proprietary hardware does not provide interfaces that are accessible through a computer and are not supported by most commercial forensics tools. Finally, different type of mobile devices requires different cables and chargers, which make identifying the right cable and charger for each mobile device is cumbersome for forensics investigators.

A tablet is a mobile device that falls in between a PC and a smart phone [5]. Tablets running on Android operating system are becoming one of the most used mobile devices in the market [6]. A tablet has a high forensics value for investigators because a tablet can store data much like a PC and function like a smart phone. Evidentiary data extracted from a tablet such as e-mail, picture, browsing activity, GPS and social network data can assist investigators in solving a crime. However, research on the extraction of evidentiary data from mobile devices that focused on tablets is minimal compared to similar research on smart phones.

In addition to that, digital forensics software developed for mobile devices focused more on the capability to extract data from smart phones rather than tablets. Most forensics investigations on tablets use commercial digital forensics software developed for mobile phone forensics investigations such as Forensic Toolkit (FTK), Mobile Phone Examiner Plus (MPE+), Oxygen Forensic Suite and MOBILedit Forensic (ME). Therefore, it is important to validate whether digital forensics tools used for data extraction from Android tablets function as the makers claimed and should be able to be verified as such.

This paper focuses on evaluation of digital forensics tools in performing logical acquisition from an Android tablet and is organized as follows. The introductory section describes the challenges faced by digital forensics investigators in investigating mobile devices. The second section discusses the nature of digital evidence and the importance and the salient requirements and features of evaluating digital forensics tools, as well as the major components that must be considered and evaluated. The paper continues with the third section, which is the actual process of evaluation of the tools: EnCase, Forensic Toolkit (FTK), Mobile Phone Examiner Plus (MPE+), Oxygen Forensic Suite and MOBILedit Forensic (ME). The tools are used to perform logical acquisition on the Motorola Xoom MZ601 tablet. It starts with the methodology, and then gives the results of the experiment against data identified in the test cases. Finally, the last section discusses the results of the evaluation and the comparative analysis and outlines possible research endeavor on mobile forensics.

II. Related Works

A. Digital evidence

Digital evidence is fragile in nature and can easily be modified, duplicated or damaged and digital evidence collected using an untested method may not withstand scrutiny in the court of law [7], [8]. This concern has led working groups and associations such as the Computer Analysis and Response Team (CART), the Scientific Working Group on Digital Evidence (SWGDE), the Technical Working Group on Digital Evidence (TWGDE), and the National Institute of Justice (NIJ) to establish general guidelines and standardize definitions, terminologies and techniques to mitigate inconsistencies in the area of digital forensics. Although it is quite a challenge to define a general method in digital forensics investigations as each investigation may have unique characteristics, the phases of investigations normally follows below [2]:

(1) Identification: The phase involves identifying digital and non digital items such as mobile phone, laptop, sticky notes and thumb drive that may contain potential evidences.
(2) Preservation: The phase involves putting adequate measures such as the secure storage for digital devices and enforcement of chain of custody to ensure the integrity of digital evidences.
(3) Collection: The phase involves seizing and collecting the identified items to the lab for further analysis and investigation.
(4) Acquisition: The phase involves extracting data from digital devices using forensically sound tools and methods.
(5) Analysis: The phase involves activities such as keyword searching, recovering deleted data and data carving to uncover digital evidences from the digital devices.
(6) Presentation: The phase involves presenting in various forms such as written or oral of the investigations conducted on the digital devices.

Although the same phases of investigations are applicable to both computers and mobile devices, the latter involves additional constrains and challenges. Data that resides in a mobile device such as smart phone and tablet is constantly changing and therefore it is impossible to preserve the current state of data. Therefore, the hash value of evidentiary data is unique and only valid at the time evidentiary data is extracted from a mobile device.

B. Digital forensics tools

Digital forensics discipline uses various digital forensics tools such as disk imager, registry viewer and malware analyzer to assist investigators in investigating a case. Since common operating system of a PC is running on Windows, most forensics investigations that involve a PC can be successfully acquired and analyzed. However, the operating systems for mobile devices are more diverse. There are IOS, Android, Java ME, Symbian, BlackBerry, Windows, Kindle and other proprietary operating systems. Similar to a smart phone investigation, extracting evidentiary data from a tablet is challenging for forensics investigators. There are various types of device with different brands and models, which requires different methods to extract data [9]. There are also many different cables, firmware and multiple power states instead of simply off or on [10]. Since most forensics tools require devices to be switched on during acquisition, evidentiary data may be overwritten or deleted. If the device is switched off or put into sleep mode, the device may activate its security mechanism such as lock code, which may restrain access to the device [11].

Currently, the technique used by most investigators to conduct investigations on a tablet is the same way as investigating a smart phone not supported by digital forensics tools [5]. Investigators usually manually thumb through a tablet to look for evidences, which can result in accidental alteration of data and loss of potential evidence due to lack of familiarity with the way the device works or stores data. Besides manually thumb through the tablet, digital forensics tools are used widely in investigating the device.

Although vendors and developers of commercial digital forensics tools make various claims about the capabilities of their tools to acquire data on mobile devices, the tools should function as advertised and should be able to be verified as such. However, the progress of the validation of such techniques and methods is limited and it is a challenge for forensics investigators to assure that evidentiary data extracted by the digital forensic tools is reliable [12]. Testing is one of the ways to verify and validate digital forensics tools used in forensics investigation. A validation framework for digital forensics tools that was established for laboratory testing and accreditation is the ISO 17025 standard. The standard is widely adopted by forensics laboratories to ensure procedures and tools used in the labs are verified and validated [13].

III. Validation Method

The evaluation of digital forensics tools was conducted in a forensically sound method. This is achieved by preventing changes on the data populated onto the tablet to ensure the integrity of original data was preserved. The evaluation method consists of four phases. Phase 2, Phase 3 and Phase 4 were adopted from the evaluation guideline developed by National Institute of Standards and Technology (NIST) to ensure that the evaluation process produced quality and trusted findings [14]. The evaluation method can be seen in Fig. 1.

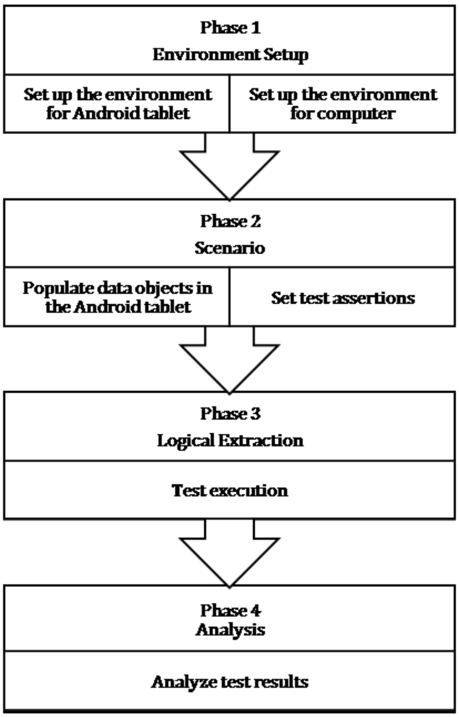


Figure 1. Validation method

NIST also provides a guideline that defined a list of data objects populated onto a smart phone that should be able to be extracted by digital forensics tools [15]. The guideline also defined test assertions which are general statements of conditions that can be checked after a test is executed. We adopted one of the core test assertions to validate whether the digital forensics tools tested able to acquire all data objects populated onto the internal memory of an Android tablet.

Kubi et al. [16] validated XRY and UFED Physical Pro capability to extract data objects populated onto two smart phones with Symbian and Windows Mobile operating systems. The research showed that XRY performed better than UFED Physical Pro. Similar research was conducted by Harshbarger [17], but the research focused on measuring the error rate of the tools while extracting data objects populated onto an Android tablet. Tolman [5] developed an extraction and analysis method for Android tablet. The research used some data objects listed by NIST to be populated onto the tablet. However, only AccessData Mobile Phone Examiner Plus software was used in the research to extract the data objects, therefore there was no comparison on the capabilityof software was made.

For this experiment, we compared the data objects listed in NIST publication against data objects used in previous research works. We adopted data objects used by Tolman as his research focused on evaluating the capabilities of digital forensics tools used to extract data objects populated onto the internal storage of a Motorola Xoom tablet, which is similar to our research. We added another data object that is the Device information as shown in Table 1 (data object numbered c). Device information is one of important evidences in an investigation that allows investigators identify International Mobile Equipment Identity (IMEI) that is the unique serial number of a tablet device.

Table 1. Data objects used for validation of digital forensics tools.

Data Object	Storage	NIST	Kubi et al.	Harshbarger	Tolman	Researchers
a. Contact	Internal and SIM card	√	√	×	×	×
b. Calendar	Internal	√	×	×	×	×
c. Device information • IMEI	Internal	√	×	×	×	√
d. Network information • IMSI	SIM card	√	×	×	×	×
e. Application file such as PDF and JPEG	Internal	√	√	√	√	√
f. Internet history such as bookmark, last visited page dan cache	Internal	√	√	×	√	√

g. Call log	Internal	√	√	×	×	×
h. Last dialed number	SIM card	√	√	×	×	×
i. Text message	Internal and SIM card	√	√	×	×	×
j. Multimedia message	Internal	√	√	×	×	×
k. Single file such as picture taken using device's camera	Internal	√	√	√	√	√
l. E-mail	Internal	√	√	×	√	√
m. GPS data	Internal	√	√	×	×	×
n. Wi-Fi setting	Internal	×	×	×	√	√
o. Application	Internal	×	×	×	√	√

A. *Environment setup*

1) *Android tablet*

The Motorola Xoom MZ601 tablet was reset to factory setting before the evaluation was conducted. The environment setting of the tablet is shown in Table 2.

Table 2. Motorola Xoom MZ601 setting.

Features	Description
Operating System	Android 4.0.4 "Ice Cream Sandwich"
Kernel	2.6.39.4
Build Number	1.7.1-45
Rooted	No
Wi-Fi	Activated
3G/4G	Not activated
USB Debugging	Activated

2) *Computer*

A laptop used for the evaluation was setup as depicted in Table 3.

Table 3. Laptop setting.

Features	Description
Operating System	Windows 7 Home Basic
Processor	Intel Core i3 2.4 GHz
Memory	6 GB
System	64-bit

All digital forensics tools evaluated were installed on the computer. Android SDK was also installed on the workstation with the latest Java updates. One of the tools extensively used to communicate with the Android device is the Android Debug Bridge (ADB) and this tool was included in the Android SDK. The environment setup is as depicted in Fig. 2.

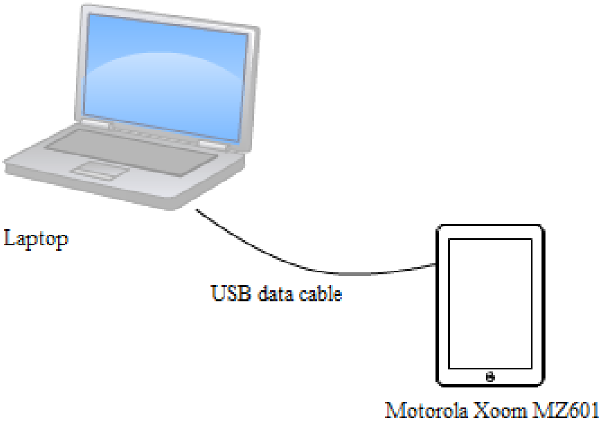


Figure 2. Environment setup

The software and hardware used for the evaluation are listed below:

- EnCase version 7.0
- Mobile Phone Examiner Plus (MPE+) version 4.0
- Oxygen Forensic Suite version 5.1 (trial)
- MOBILedit Forensic version 6.9 (trial)
- Android Software Development Kit (SDK) version 16.0
- USB data cable

EnCase and MPE+ were chosen because both software are widely used digital forensics tools in the world [18]. Although we used the trial version of Oxygen Forensic Suite and MOBILedit Forensic, the limitations set in the trial version did not affect the extraction function tested in this research.

B. *Scenario*

1) Population of data objects

A common scenario of tablet usage is created to allow the Motorola Xoom tablet to contain information. Data on the device is manually populated using the interface of the tablet by incorporating the following steps:

(1) A factory default Motorola Xoom MZ601 tablet running on Android operating system version 4.0.4 (Ice Cream Sandwich) was set up.

(2) A Wi-Fi network is connected to and saved.

(3) While the tablet was connected to a Wi-Fi network, the following steps were taken:

(a) Two websites were opened with the default browser (Google) and one of the websites was bookmarked.

(b) A search on Google website was performed and two document files (pdf format) and two picture files (jpeg format) were downloaded.

(c) Three email accounts were created. The first account (adam.andrd@gmail.com) was set as the default email account of the tablet. The second account (eve.andrd@gmail.com) was accessed using a laptop. A third account (latipah_cun@yahoo.com) was created and accessed using a laptop.

(d) Two emails were sent from the first account to the first and third accounts via the device with one of the emails contain picture attachment.

(e) An email is received from the second account and the email was opened using the device via the Gmail account.

(f) A Twitter application were downloaded at Google Play Store and installed on the device.

(g) A Twitter account was set up and two tweets were posted and one of the tweets contain picture. Two tweet accounts were followed.

(4) Five pictures were taken using the camera on the device. Two of the pictures were deleted.

Each data object populated onto the internal storage of the Motorola Xoom MZ601 was listed by manually examine the tablet and a benchmark was established for each data object found. The evaluation for each digital forensics tool was performed and the capability of each tool was determined based on the benchmark.

1) Test assertions setup

Since the Motorola Xoom MZ601 features are similar to a smart phone, the test assertions are adopted from the NIST Smart Phone Tool Specification [15]. The evaluation was performed based on the selections of requirements for core features of digital forensics tools as depicted in Table 4.

Table 4. Requirements for Core Features.

Features	Description
SPT-CR-05 (Data extraction)	Forensic tool shall have the ability to logically acquire all application supported data objects present in internal memory.

C. *Logical extraction*

There are four tools used for the acquisition that comprises of one computer forensics tool and three mobile phone forensics tools. The tools are described in Table 5.

Table 5. Digital Forensics Tools for Acquisition.

Digital Forensics Tools	Version	Description
EnCase	7.05	Software owned by Guidance Software. It is commonly used for computer forensics investigation.
Mobile Phone Examiner Plus (MPE+)	5.2	Software owned by AccessData Group developed for mobile phone forensics investigation.
Oxygen Forensic Suite (Oxygen)	5.1 (Trial)	Software owned by Oxygen Software Co. Ltd developed for mobile phone forensics investigation. The trial has some limitations, such as viewing timeline and performing search, but it does not affect the experiment conducted.
MOBILedit Forensic (ME)	6.9 (LITE)	Software owned by COMPELSON Labs developed for mobile phone forensics investigation. The trial version (LITE) has limitations, such as extracted data cannot be saved and export feature is disabled, but it does not affect the experiment conducted.

A logical acquisition was performed on the physical Motorola Xoom MZ601 tablet. The following steps were taken:

(1) Using each digital forensics tools, a logical image of the active files in the internal solid state drive was acquired by following instructions provided by each tool.

(2) The step of acquiring the logical image of the device was repeated two more times to ensure consistency and accuracy of data acquired.

D. *Analysis*

The test results were analyzed based on the requirements identified in test assertion setup depicted in Table 4. The formula used to measure the capability of each tool in extracting populated data objects is:

$$\frac{Data\ \ objects\ \ extracted}{Data\ \ objects\ \ populated} \times 100\%$$

IV. Results and findings

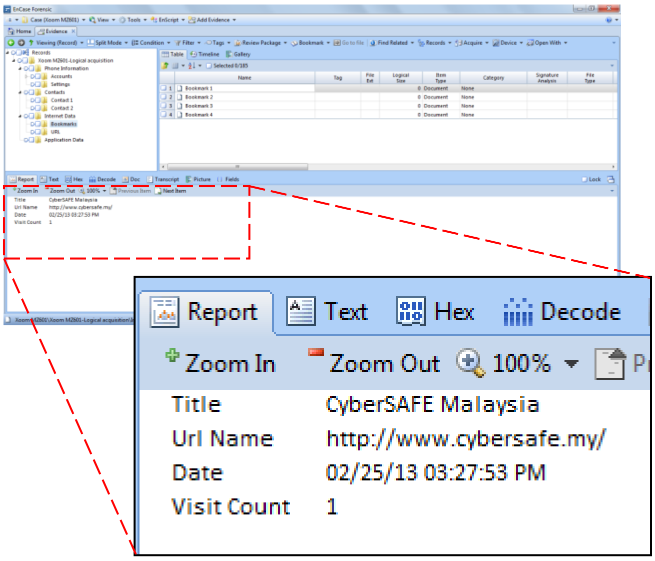
A comparison of data objects extracted by each digital forensics tool evaluated is tabulated in Table 6.

Table 6. Capabilities of tools to extract data objects

Data Object	No. of data objects	Data objects extracted			
		EnCase	MPE+	Oxygen	ME
Device information	3	3	3	3	3
E-mail	3	0	0	0	0
Wi-Fi setting	1	0	0	0	0
Internet history	3	3	0	0	0
Single file	5	0	5	5	5
Application file	4	0	4	4	4
Application	1	1	1	1	1

Based on the experiment conducted, the capability of EnCase in extracting data objects populated is 35% (7/20) and MPE+, Oxygen and ME are 65% (13/20). We found that EnCase, MPE+, Oxygen and ME were not able to extract E-mail and Wi-Fi setting data objects populated onto the Motorola Xoom MZ601 tablet.

We found that logical acquisition used in this experiment did not support the extraction of E-mail and Wi-Fi setting. The experiment result showed that EnCase is the only software capable to extract Internet history data object as Fig. 3. However, it failed to extract Single file and Application file data objects.

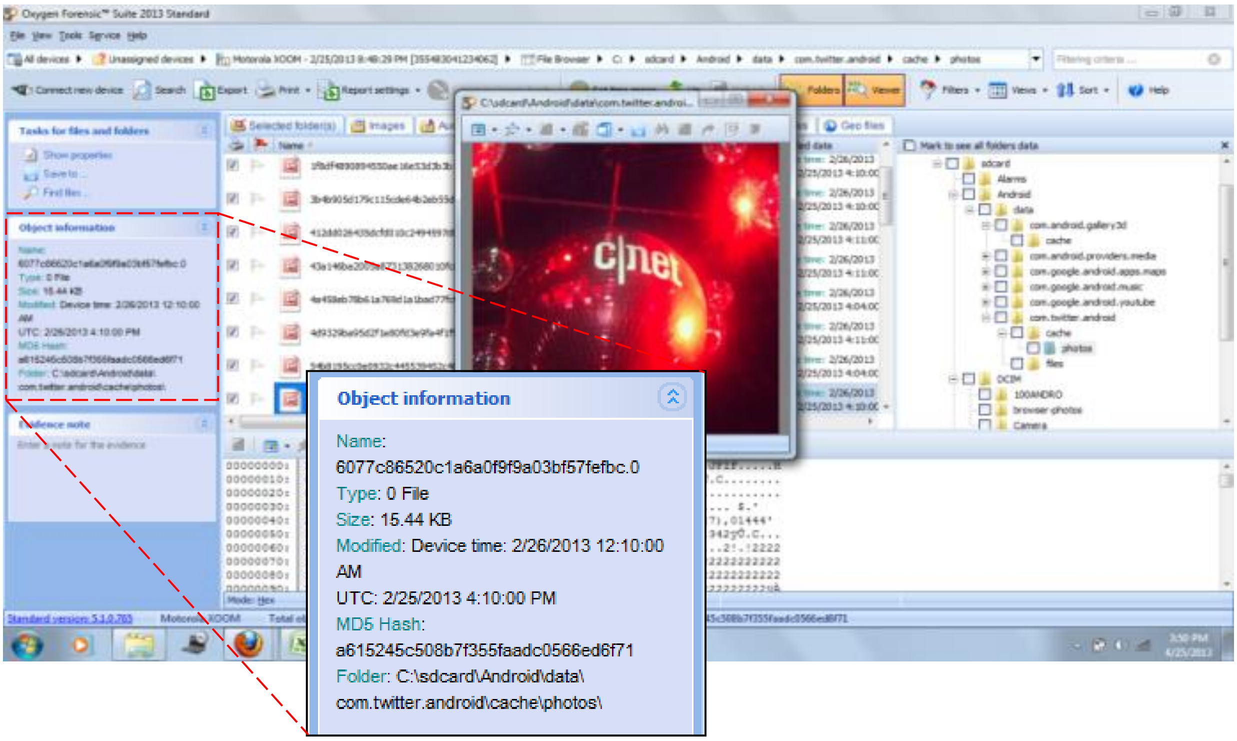


Title CyberSAFE Malaysia
Url Name http://www.cybersafe.my/
Date 02/25/13 03:27:53 PM
Visit Count 1

Figure 3. Internet history data object extracted by EnCase

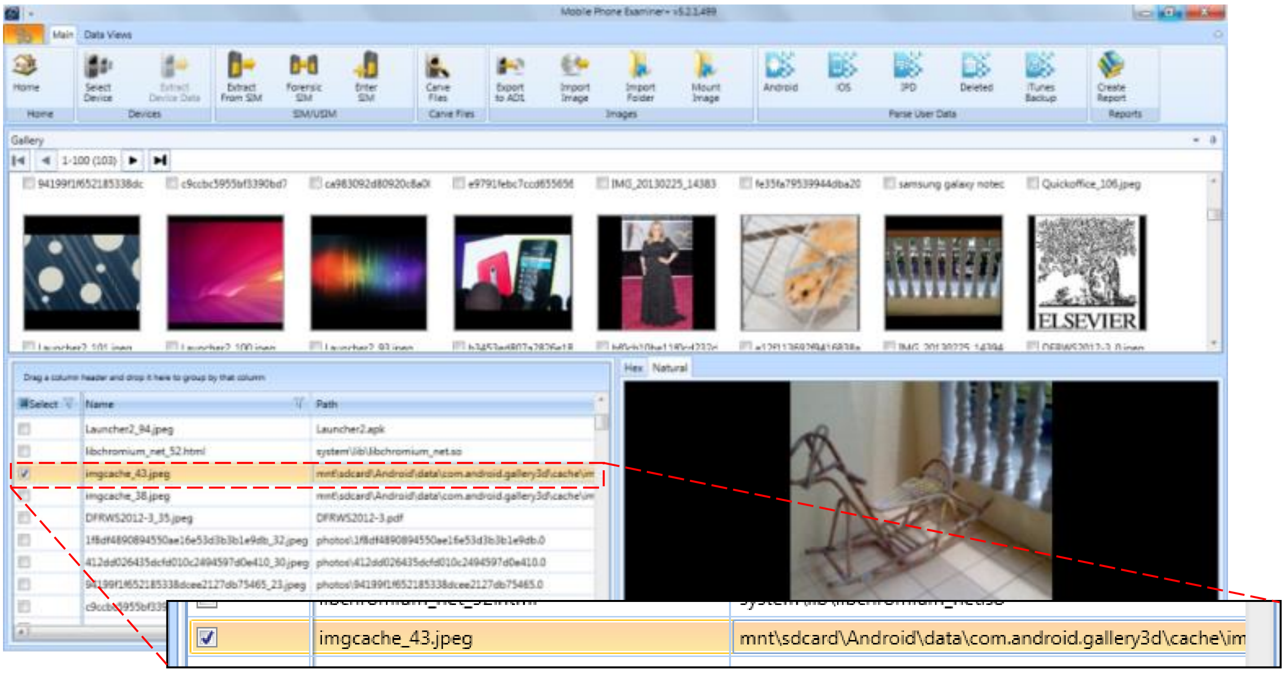
The experiment result showed that Oxygen software produced hash value of pictures downloaded while Application data object was populated onto the tablet. Oxygen software also generated the last modification date and time of each picture extracted as depicted in Fig. 4.

We found that MPE+, Oxygen and ME recovered deleted files populated as Single file data object. However, MPE+ software displayed the deleted data in a readable format as in Fig. 5.



Name:
6077c86520c1a6a0f9f9a03bf57fefbc.0
Type: 0 File
Size: 15.44 KB
Modified: Device time: 2/26/2013 12:10:00 AM
UTC: 2/25/2013 4:10:00 PM
MD5 Hash:
a615245c508b7f355faadc0566ed6f71
Folder: C:\sdcard\Android\data\com.twitter.android\cache\photos\

Figure 4. Oxygen produced hash value for extracted picture



Select	Name	Path
□	Launcher2_94.jpeg	Launcher2.apk
□	libchromium_net_52.html	system\lib\libchromium_net.so
☑	imgcache_43.jpeg	mnt\sdcard\Android\data\com.android.gallery3d\cache\im
□	imgcache_38.jpeg	mnt\sdcard\Android\data\com.android.gallery3d\cache\im
□	DFRWS2012-3_35.jpeg	DFRWS2012-3.pdf
□	1f8df4890894550ae16e53d3b3b1e9db_32.jpeg	photos\1f8df4890894550ae16e53d3b3b1e9db.0
□	412dd026435dcfd010c2494597d0e410_30.jpeg	photos\412dd026435dcfd010c2494597d0e410.0
□	94199f1f652185338dcee2127db75465_23.jpeg	photos\94199f1f652185338dcee2127db75465.0

Figure 5. MPE+ displayed deleted picture in a readable format

V. Conclusion

The experiment result showed different measurement of capabilities for each digital forensics tools in extracting data objects populated onto the Motorola Xoom MZ601 tablet. A forensically sound method of acquisition and analysis is possible on the Motorola Xoom MZ601 tablet, but with limitations. The experiment result showed that there is no one tool that can extract all data from the device. The results of the validation experiment can be used by digital forensics investigators in determining the appropriate tool to be used in an investigation. Based on the experiment result, EnCase software is suitable to be used in investigations that require evidentiary data involving Internet usage. Meanwhile, Oxygen software is suitable to be used in investigations that involve circulation of pornographic files as the hash value of files extracted from the device can be used to compare with the hash value of suspected files. MPE+ is suitable for investigations that involve extracting deleted evidentiary data as it automatically display recoverable deleted files in a readable format. Finally, the experiment results also demonstrate the importance of validation test to measure the capabilities of digital forensics tools as the strengths and weaknesses of each tool can be properly identified.

References

[1] M. Meyers, M. Rogers. “Computer forensics: The need for standardization and certification”, *International Journal of Digital Evidence*, 3 (2), pp. 1-11, 2004.

[2] M. Reith, C. Carr, G. Gunsch. “An examination of digital forensic models”, *International Journal of Digital Evidence*, 1 (3), pp. 1-12, 2002.

[3] N. Al Mutawa, I. Baggili, A. Marrington. “Forensic analysis of social networking applications on mobile devices”, *Digital Investigation*, 9, pp. S24-S33, 2012.

[4] A. Marwan. “Mobile handset forensic evidence: a challenge for law enforcement”. In *Proceedings of the 4th Australian Digital Forensics Conference*, 2006.

[5] J. Tolman. “Developing a forensic method of acquisition and analysis of the Motorola Xoom tablet”. *Masters Thesis*, Purdue University, College of Technology, Indiana, 2012.

[6] B. Reed. Android activations hit 1.3 million per day. http://bgr.com/2012/09/05/android-activations-1-3-million-daily-google-ceo-schmidt/, 2012.

[7] J. Wiles, A. Reyes. “Acquiring Data, Duplicating Data, and Recovering Deleted Files”, in *The best damn cybercrime and digital forensics book period*, Syngress, Burlington, 2007.

[8] A. Scholtz, A. Narayanan. “Towards an Automated Digital Data Forensic Model with specific reference to Investigation Processes”. In *Proceedings of the 8th Australian Digital Forensics Conference*, pp. 142, 2010.

[9] P. McCarthy. “Forensic analysis of mobile phones”. *BS CIS Thesis*, University of South Australia, School of Computer and Information Science, Mawson Lakes, 2005.

[10] P. Owen, P. Thomas. “An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines”, *Digital Investigation*, 8 (2), pp. 135-140, 2011.

[11] I. Sporea, B. Aziz, Z. McIntyre. “On the availability of anti-forensic tools for smartphones”, *International Journal of Security*, 6 (4), pp. 58-64, 2012.

[12] J. Liang. “Evaluating a selection of tools for extraction of forensic data: disk imaging”. *Masters Thesis*, Auckland University of Technology, Auckland, 2010.

[13] J.J. Barbara. “Digital Evidence Accreditation: Compliance with Select ASCLD/LAB Standards and Criteria, Part II”, *Forensic Magazine*, 2 (1), pp. 8-11, 2005.

[14] NIST. “General Test Methodology for Computer Forensic Tools”. National Institute of Standards and Technology, Washington, 2001.

[15] NIST. “Smart Phone Tool Specification”. National Institute of Standards and Technology, Washington, 2010.

[16] A.K. Kubi, S. Saleem, O. Popov. “Evaluation of some tools for extracting E-evidence from mobile devices”. In *Proceedings of the IEEE 5th International Conference on Application of Information and Communication Technologies*, pp. 1-6, 2011.

[17] W.G. Harshbarger. “Android tablet forensic logical image tool testing”. *Masters Thesis*, Purdue University, College of Technology, Indiana, 2012.

[18] Y. Guo, J. Slay, J. Beckett. “Validation and verification of computer forensic software tools—Searching Function”, *Digital Investigation*, 6, pp. S12-S22, 2009.

Author Biographies

Razana Md Salleh is a M.S. degree student (information technology) at the Universiti Kebangsaan Malaysia. The current working title of her thesis is validation of digital forensics tools for android tablet. She received her degree in information technology from the Universiti Utara Malaysia in 2001.

Masnizah Mohd received her PhD in computer and information sciences from the University of Strathclyde, UK in 2010. Her PhD thesis was titled design and evaluation of an interactive topic detection and tracking interface. She holds M.IT (2002) and B.IT (1999) degrees in Information Science from the Universiti Kebangsaan Malaysia. Her main research interests are in the areas of Information Retrieval, Topic Detection and Tracking and Natural Language Processing; with particular focus on aspects such as user interaction, user interface, named entity recognition, user tasks and evaluation

Kamarul Baharin Khalid obtained his degree in computer engineering from Cleveland State University, US in 1992. His main fields of interest include digital forensics, information security and software testing and verification. He received Certified Ethical Hacker (CEH) and EC-Council Certified Encryption Specialist certifications from EC-Council in 2013.