Trends & issues in crime and criminal justice

No. 460 August 2013

Australian Government
Australian Institute of Criminology

Mobile device forensics: A snapshot

Christopher Tassone, Ben Martini, Kim-Kwang Raymond Choo and Jill Slay

Foreword | *In the increasingly dynamic environment of mobile forensics, this paper provides an overview of the capabilities of three popular mobile forensic tools on three mobile phones based on Apple's iOS, Google's Android and RIM's BlackBerry operating systems. The paper identifies where each specific tool is best applied and also describes the limitations of each in accessing contacts, call history, message data (SMS, MMS and emails), media files and other data. New releases of forensic tools and mobile operating systems may change the way the data are acquired and preserved in the future. It is therefore hoped that future research will continue to provide the digital forensics community with the most up-to-date overview of mobile forensics capabilities.*

Adam Tomison
Director

Mobile devices are fast becoming ubiquitous in populations worldwide. For example, the 2012 IBM Tech Trends Report (based on a survey of more than 1,200 professionals who make technology decisions for their organisations in 16 different industries and 13 countries, as well as more than 250 academics and 450 students across these same countries) predicted that

> [b]y the end of 2012, mobile devices are expected to outnumber people. Sources of analytical insight continue to multiply, with the world generating 15 petabytes of new data every day—that's roughly eight times the information housed in all the academic libraries in the United States (Lo, Wyble & Hupfer 2012: 2).

The Australian Communications and Media Authority also demonstrated the growth and ubiquity of Australian mobile devices in their recent report Communications Report 2011–12, which noted

> [t]he total number of mobile services in operation increased by three per cent to reach 30.2 million, approximately four mobile services to every three people in Australia (ACMA 2013a: 3).

With the increasing prevalence of mobile devices, forensic evidence extracted from mobile (as well as other electronic) devices can be an invaluable source of evidence for investigators in both civil and criminal prosecution (Adams, Whitledge & Shenoi 2008). Mobile device data can be extracted and then used to generate reports on a range of data including an individual's communication and travel habits. For example, in a criminal investigation, the data including transaction information such as call history, message data (SMS/MMS/emails), calendar events, photos and emails, are often able to be supplied to the investigating officer in a report format (Androulidakis 2012). For the evidence to be admissible in a court of law, appropriate forensic procedures must be followed (McKemmish 2008).

NDLERF National Drug Law Enforcement Research Fund

While these forensic procedures are often organisation specific, a number of frameworks exist to provide guidance for the conduct of digital forensics that form that basis of these procedures. These frameworks have been published (Kent et al. 2006; McKemmish 1999; Martini & Choo 2012), as have mobile forensic procedures and tools (Me & Rossi 2008; Owen & Thomas 2011; Savoldi & Gubian 2008). This has allowed practitioners to make sound decisions in the development of high-level forensic procedures and in specific cases using specific tools (Guo, Slay & Beckett 2009).

One of the key strategic challenges presented to digital forensic practitioners, particularly those in law enforcement, is maintaining capability in an environment of rapid development of information and communications technologies, and its ready adoption by the public and offenders (Adams 2008; Choo 2011). Smart mobile devices, for example, are much more complex than traditional mobile phones and with a range of personal data management facilities, these mobile devices more resemble personal computers than they do phones (Lim & Khoo 2009; Quick & Choo forthcoming). This makes them particularly interesting candidates for analysis as they hold a significant amount of data that could be of interest to a forensic investigator. However, the method of collecting evidence is quite different when compared with traditional forensic computer hard disk (Jansen, Delaitre & Moenner 2008).

While there is a large range of smart mobile devices, three main operating systems dominate the market, namely Apple iOS, Google Android and RIM Blackberry (see Table 1; ACMA 2013). These are the three operating systems that the analysis focuses on in this paper. To analyse the capabilities available to forensic practitioners in the area of mobile forensics, three of the most popular mobile forensic collection and analysis tools were used. The three tools selected were Tool 1, Tool 2 and Tool 3 (these software tools have been anonymised to avoid being seen as promoting commercial interests, however information can be provided upon request). These tools are currently popular with forensic practitioners both locally and globally, and as such, this typifies the range of capabilities available to forensic practitioners in the area of mobile forensics. This paper describes the role of mobile forensic collection and analysis tools. The term extraction is used to refer to the process of collecting and extracting of data from mobile devices using the mobile forensic tools.

Table 1 Top six smartphone operating systems (%)[a]

Mobile device operating system	Q2 2012 US market share	Q2 2012 AUS market share	Q2 2012 EU market share	Q2 2012 average
Android	41.9	58.0	61.0	53.4
iOS	53.3	35.9	25.3	38.2
Blackberry OS	1.4	0.3	4.4	2.0
Symbian	0.2	1.0	2.6	1.3
Windows Phone 7	2.7	4.2	4.7	3.9
Other	0.6	0.7	2.0	1.1

a: Percentages may not total 100 due to rounding

Source: Adapted from ACMA 2013b

Table 2 Specifications of mobile devices

Mobile device	iPhone 4 16GB Black GSM (A1332)	HTC Sensation XE Beats Audio Z715a	BlackBerry Bold 9700
Manufacturer	Apple	HTC	RIM
Operating system	5.1	Android 4.0.3 (Ice Cream Sandwich)	Blackberry OS v5.0
RAM	16GB	4GB (1GB user available)	256MB
Internal memory	512 MB	768MB	256MB
External memory card	none	microSD (8GB)	microSD (2GB)
Chipset	Apple A4	Qualcomm MSM8260 Snapdragon	Marvell PXA930
CPU	1 GHz Cortex-A8	Dual-core 1.5 GHz Scorpion	624 MHz

Study setup

Smart mobile devices

The following three phones were selected for this study, based upon the popularity of their operating systems—Apple iPhone 4 16GB, HTC Sensation XE with beats Audio Z715a and BlackBerry Bold 9700 (see Table 2). Although these phones were not running the very latest versions of their operating systems at the time of the study, this was intentional. Digital forensic tools can take some time to be certified as capable of analysing newer versions of operating systems and therefore, it was considered prudent to use supported operating systems with the mobile forensics tools wherever possible.

To ensure that the study results were valid and as close as possible to real world practice, the three phones selected were used extensively by real users before being used in this study. This proved invaluable compared with only seeding the phones with a minimum of data as it allowed detection of anomalies within high volumes and a range of data that would otherwise not have been detected (this is discussed further in the *Findings and Implications for Digital Forensic Practitioners* section).

Personal computer environment

All of the forensic tools used required a computer for analysis or viewing of reports. To ensure that there were no conflicts between the tools, all three tools were installed on three separate personal

Table 3 iPhone logical extraction results

Data type	Tool 1	Tool 2	Tool 3
Contacts	0[a]	0[a]	0[a]
Call history	100	100	100
SMS	41,181 **(1,485)**	29,798	41,181
MMS	205	202	202
Email	Unsupported[b]	Unsupported	Unsupported
Calendar entries	1	Unsupported	1
Bookmarks	22	Unsupported	22
Web history	15	Unsupported	15
Images	870	418	1,412
Video	23	23	23
Audio	0[c]	0[c]	0[c]

a: The device did not have any undeleted contact data at the time of extraction

b: Tool 1 documentation notes that iPhones must be jailbroken (a process that bypasses software protections to allow privileged code to execute on the mobile device without manufacturer approval) to extract emails in logical mode. Other tools may have similar limitations

c: The device did not have any undeleted audio files stored at the time of extraction

Table 4 Android logical extraction results

Data type	Tool 1	Tool 2	Tool 3
Contacts	156	399	430
Call history	323	323	323
SMS	3,027	3,027	3,027
MMS	46	46	46
Email	Unsupported	Unsupported	Unsupported
Calendar entries	89	89	89
Bookmarks	12	Unsupported	12
Web history	245	Unsupported	245
Images	2,691	2,170	78
Video	11	8	0
Audio	200	31	0

computers of identical specifications. As one of the tools only supported a 32bit operating system, to maintain an identical environment all the tools were restricted to a 32bit operating system with 3.16GB of usable random-access memory (RAM). RAM is a form of temporary computer data storage. The specifications of the PCs used in this study are as follows:

CPU: Intel® Core™ i5-2410M 2.3GHz

RAM: 4GB (3.16GB usable)

OS: Windows 7 Professional SP1 32bit

GPU: NVIDIA GeForce GT 540M 1GB

HDD: 750GB @ 5400rpm

Mobile forensics tools

Three popular mobile device forensic tools were used in this study.

Tool 1 and Tool 2 both have supported phone guides that list the phones that have been certified by the vendor as working with their product and the capabilities for forensic extraction their product supports for a given phone. Tool 3 lists the operating systems that are supported for extraction.

Both logical and physical extractions using all three tools were attempted. Logical extraction refers to the ability to copy the logical storage objects of the mobile device (eg directories and files; Grispos, Storer & Glisson 2011). All of the tools selected have the ability to perform a logical extraction; it is understood that this extraction acquires the data from the mobile device using the vendor's interface, which is most commonly used for synchronising the handset with a computer. This extraction method does not usually recover any deleted information due to the data being transferred file by file rather than bit for bit.

Physical extraction refers to the ability to perform a bit-for-bit copy of the entire physical storage, which allows the forensic tools to acquire remnants of deleted data (Grispos, Storer & Glisson 2011). However, this process requires direct access to the file system of the mobile device. This is necessary to be able to recover deleted data from the disk using methods such as carving, where particular file headers are searched for to recover target file types. Carving is a commonly used technique in digital forensics to extract a collection of data from a larger data set (see DFRWS 2006).

Study results format

Prior to undertaking the study, it is necessary to define the types of data that needed to be collected from physical and logical extractions. Each of the output data types available from the forensic tools was reviewed and it was found that while they shared a subset of common data types (eg contact data, call history, SMS, MMS, images, audio, video), they also had a number of less common data types that were not supported across all three tools. The study results focus on the data types that were best represented across all three of the forensic tools. As such, only the results on the following data types—contacts, call history, SMS, MMS, email, calendar entries, bookmarks, web history, images, video and audio—are reported. These data types were extracted and the total number of items tallied (both current and deleted). Where a difference was noted, further investigation was conducted to determine what data was different and if possible, why the difference occurred between the forensic tools.

Findings and implications for digital forensic practitioners

Tables 3 to 8 show the number of items extracted by the forensic tools across the three mobile devices (inclusive of deleted items). The figures in bold parentheses represent the number of deleted items.

Table 5 Blackberry logical extraction results

Data type	Tool 1	Tool 2	Tool 3
Contacts	76	75	75[a]
Call history	53	53	53
SMS	245	245	245
MMS	4	4	4
Email	117	Unsupported	117
Calendar entries	19	11	11
Bookmarks	2	Unsupported	2
Web history	1	Unsupported	1[b]
Images	46	46	46
Video	3	3	3
Audio	22	22	22

a: Tool 3 reported 89 contact entries, however 14 were found to be duplicates

b: Tool 3 extracted 6 additional cache entries not included in this total

Table 6 iPhone physical extraction results

Data type	Tool 1	Tool 2	Tool 3
Contacts	0[a]	0[a]	
Call history	100 (6)	101 (1)	
SMS	41,182 (1,496)	41,388 (228)	
MMS	205	202	
Email	50	50 (38)	
Calendar entries	1	1	Unsupported
Bookmarks	22	22	
Web history	40	15	
Images	883	961 (4)	
Video	23	23	
Audio	0[b]	0[b]	

a: The device did not have any undeleted contact data at the time of extraction

b: The device did not have any undeleted audio files stored at the time of extraction

Contacts

The contact data extracted from the Android device demonstrated the complexities in collecting contact data stored on a device that correlates data from multiple sources (see Tables 4 and 7). The iPhone did not have contact data stored and as such, could not be assessed under this category. The Blackberry results were very similar across all three forensic tools; Tool 3 produced a number of duplicate entries, however, once these duplicate entries were removed, Tool 3 extracted a similar sum to the other two tools (see Table 5).

The large variances in the Android results appear to relate to the multiple data sources for contacts on the device. Contact data sources on the device included local records, Google accounts, a Facebook account and a LinkedIn account. The forensic tools handled these different data sources in different ways—some accounts were merged by some tools, other accounts could not be extracted at all by some tools. Tool 3 was the most comprehensive of the tools in collecting contact data, however, it is difficult to determine exactly which contacts were extracted from which source using the tools.

Call history

All three forensic tools successfully extracted call history records across the three mobile devices as part of the logical extraction process (see Tables 3–5). The data extracted was similar in all cases but Tool 1 found six deleted call history records. This was unable to be proven as the call history was not pre-populated onto the mobile device. Physical extraction produced similar results for those tools that supported the mobile devices (see Tables 6–8).

SMS/MMS

SMS and MMS messaging demonstrated the utility of using devices with 'real world' usage. While the Android and Blackberry SMS/MMS messaging data was logically extracted successfully, the iPhone showed a number of anomalies. This was likely due to the large volume and types of messages on the device. All three tools extracted significantly different numbers of SMS messages from the iPhone and as such, the remainder of this section describes the iPhone results.

Tool 1 was unexpectedly able to recover approximately 1,485 deleted messages from the iPhone during the logical extraction. It is considered that it was able to recover the messages from the SQLITE database (which stores the messages), as the sms.db file keeps deleted records until a garbage collection operation is run. Garbage collection is a clean-up operation, which is normally run on demand or when a database is idle for performance reasons.

Tool 2 was only able to extract a maximum of 30,000 SMS messages (after several attempts) before reporting a memory limitation issue for the Tool (see Figure 1). This study also appeared to demonstrate that a maximum of 30,000 non-file records (eg contacts, call log, SMS etc) can be extracted by Tool 2 from an iPhone in logical mode.

Once deleted messages had been removed, Tool 1 and Tool 3 differed by only one SMS message. Further investigation determined that this was due to data inconsistency (an invalid SMS) and this invalid SMS was removed from the Tool 1 total, therefore

making the total number of undeleted SMS extracted by Tool 1 and Tool 3 equal. Tool 1 was able to extract three more MMS messages than Tool 2 and Tool 3, this appears to relate to how the forensic tools handle messages that are blank or contain unprintable characters.

Email

Email was generally not well supported by the forensic tools on any of the devices tested. For the logical extraction, emails from the Blackberry were only successfully extracted using Tool 1 and Tool 3. All other logical combinations could not proceed. This was often due to the need to jailbreak or root the device. A jailbreak (a process that bypasses software protections to allow privileged code to execute on the mobile device without manufacturer approval; Obaidli, Iqbal & Iqbal 2012) was not used and neither was a root (a process that permits loaded software to bypass standard software restrictions and gain 'root' super-user privileges; Christin, Vidas & Zhang 2011) on any devices as part of this study. In the case of the Android device, the only viable method of rooting required unlocking the boot loader, which (using the vendor's application) would securely erase the phone's contents.

Physical extractions fared slightly better. Tool 2 was able to collect more emails from the Blackberry device in physical extraction mode than the other two tools were able to in logical mode (as well as some deleted emails). iPhone email was also extracted as part of the physical extraction and both Tool 2 and Tool 1 were able to extract 50 emails, with Tool 2 able to locate 38 deleted emails on the iPhone device.

Calendar entries

Calendar entries were extracted and reported on by the tools that supported calendar data. Support did vary somewhat between the tools. For example, with the Blackberry logical extraction, Facebook calendar data (birthdays) (included under 'Calendar entries'—see Table 5) were extracted by Tool 1 but not by the other two tools. This implies that all Facebook calendar entries would not have been included in the extraction reports of the other tools. Tool 2 was able to recover five deleted calendar entries from the Blackberry as part of its physical extraction.

Bookmarks

Bookmark collection was mostly identical across the tools that supported their extraction from a mobile device. Both physical and logical extractions produced the same number of bookmark entries for each tool, per device.

Web history

Web history collection produced similar results across logical extractions from tools that supported history extraction. The format in which this data is displayed varied between the tools, as did what each tool considered a web history record. Tool 1, for example, was able to include history records from the YouTube application on the iPhone device as part of web history, which the other two tools did not. Equally, Tool 3 presented 'cache' information (which is considered part of web history) and the other two tools did not.

Physical extraction presented quite different results from the logical extraction, with many more entries found by supported tools. It is presumed that the methods used by the tools for collecting web history vary significantly between logical and physical extractions. This is by contrast with other item collections where the similarities in numbers of items extracted would suggest that the same or very similar methods are being used to collect data from physical and logical extractions (eg parsing a database file).

Media files

Media files including images, videos and audio were extracted in similar numbers across those tools that supported these items. Where logical tools required physical

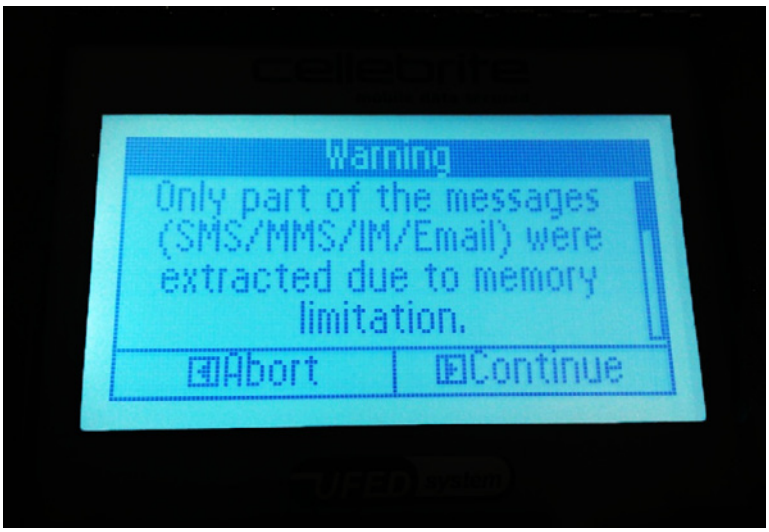
Table 7 Android physical extraction results

Data type	Tool 1	Tool 2	Tool 3
Contacts		133 (26)	
Call history		0	
SMS		3,207 (181)	
MMS		45 (1)	
Email		31 (3)	
Calendar entries	Unsupported	89	Unsupported
Bookmarks		12	
Web history		263 (15)	
Images		10,985 (1,502)	
Video		18 (22)	
Audio		76	

Table 8 Blackberry physical extraction results

Data type	Tool 1	Tool 2	Tool 3
Contacts		113 (38)	
Call history		52	
SMS		269 (24)	
MMS	Unsupported	0	
Email		124 (4)	
Calendar entries		27 (5)	Unsupported
Bookmarks		0	
Web history		92	
Images	58	136	
Video	5	4	
Audio	27	0	

Figure 1 Tool 2 Memory limitations



access to the SD memory card (ie removal from the device and insertion into a card reader) from the device to collect media items, the study did not proceed as it was considered to be part of a physical extraction.

One interesting difference was the increased number of image and video files detected by Tool 1 as part of the logical Android extraction. Tool 1 was able to detect the extra files as it appeared to use file signature analysis to detect these file types rather than simply relying on file extensions. Most of the media files located via this process were standard files (eg mp3 and mp4) used in installed applications with modified extensions.

Physical extraction

Support for extraction did not appear to be strong across all three devices and three tools tested. A number of device/tool combinations were unsupported for physical extraction and even when supported, the results were mixed. The physical extraction methods had to be repeated several times before a successful result could be declared. Physical extraction is an area for potential improvement with all of the forensic tools used in this study.

Conclusion

The aim of this study was to gain a better understanding of the practical capabilities of three popular mobile forensics tools in collecting and analysing three popular mobile devices. These mobile devices represent the three most popular operating systems (iOS, Android and Blackberry) for smart mobile devices worldwide. Findings were mixed and it was concluded that no single tool can be solely relied upon to collect and present every item of potential evidence from a smart mobile device.

During this study, both innovative features and limitations were found. Some of the more innovative features some tools presented included recovering deleted messages from a logical extraction, file signature analysis on mobile devices to detect files with non-standard extensions, extraction of data (eg contacts, calendar) from multiple original sources and comprehensive collection of web records beyond the default browser. Limitations found included the requirement to 'root' a phone, which would result in the destruction of the data stored on the device, hard limits for the collection of text data from a mobile device and incoherent display of data making comparison of data such as contacts and messaging difficult, if not impossible. These limitations are not insurmountable as it is assumed that given time, many of them will be overcome as the mobile forensics tools are updated and upgraded. Due to the sheer number of different handsets entering the world market, it is very unlikely that every tool will have the ability to support all phones as demonstrated in this study.

It should be noted that results may vary when analysing mobile devices that use operating systems designed for use by many different manufacturers (eg Android). Manufacturers will often customise their implementation of the operating system, which can result in data being stored in different locations to the standard operating system conventions (eg HTC Sense and Samsung TouchWiz).

To successfully collect the maximum amount of data from a mobile device, investigators and practitioners need to be aware of the key features and limitations of the tools they use. This will allow them to make informed selections in an environment where timeliness is often critical and workloads are high. However, forensic tools are constantly updated to provide support for new devices and expand support for existing devices.

Disclaimer

At the time of this research, findings are accurate to the best of the authors' knowledge. However, new releases of forensic tools and mobile operating systems may change the way the data are acquired and preserved in the future.

References

All URLs correct at May 2013

Adams CW 2008. Legal issues pertaining to the development of digital forensic tools, in *Proceedings of the SADFE Third International Workshop on Systematic Approaches to Digital Forensic Engineering*: 22 May 2008: 123–132

Adams C, Whitledge A & Shenoi S 2008. Legal issues pertaining to the use of cell phone data. *Advances in Digital Forensics IV* 285: 231–243

Androulidakis I 2012. *Mobile phone security and forensics: A practical approach*. Springer, NY: Briefs in Electrical and Computer Engineering

Australian Communications and Media Authority (ACMA) 2013a. *Communications report 2011–12*. http://www.acma.gov.au/webwr/_assets/main/lib550049/comms_report_2011-12.pdf

Australian Communications and Media Authority (ACMA) 2013b. *Communications report 2011–12 series Report 3 Smartphones and tablets: Take-up and use in Australia*. http://www.acma.gov.au/webwr/_assets/main/lib310665/report-3-smartphones-tablets-comms_report_11-12_series.pdf

The authors are with the Information Assurance Research Lab, University of South Australia.
This research is funded by NDLERF 2009/10-237: Exploitation of electronic evidence from mobile phone mediated drug crime.

General editor, *Trends & issues in crime and criminal justice* series:
Dr Adam M Tomison, Director,
Australian Institute of Criminology

Note: *Trends & issues in crime and criminal justice* papers are peer reviewed

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

ISSN 0817-8542 (Print)
1836-2206 (Online)

GPO Box 2944
Canberra ACT 2601, Australia
Tel: 02 6260 9200
Fax: 02 6260 9299

Choo K-KR 2011. Harnessing information and communications technologies in community policing, in Putt J (ed), Community policing in Australia. *Research and public policy series* no. 111. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/rpp/100-120/rpp111.aspx

Christin N, Vidas T & Zhang C 2011. Toward a general collection methodology for android devices. *Digital Investigation* 8(Supplement): S14–S24

DFRWS 2006. *DFRWS 2006 forensics challenge overview*. http://www.dfrws.org/2006/challenge/

Grispos G, Storer T & Glisson W 2011. A comparison of forensic evidence recovery techniques for a windows mobile smart phone. *Digital Investigation* 8(1): 23–36

Guo YH, Slay J & Beckett J 2009. Validation and verification of computer forensic software tools-Searching Function. *Digital Investigation* 6(3–4): 12–22

Jansen WA, Delaitre A & Moenner L 2008. Overcoming impediments to cell phone forensics, in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*: 7–10 January 2008: 483–483

Kent K, Chevalier S, Grance T & Dang H 2006. *Guide to integrating forensic techniques into incident response*. SP800-86. Gaithersburg, MD: US Department of Commerce

Lim N & Khoo A 2009. Forensics of computers and handheld devices identical or fraternal twins? *Communications of the ACM* 52(6): 132–135

Lo J, Wyble C & Hupfer S 2012. *Fast track to the future: The 2012 IBM Tech Trends Report*. Armonk, NY: IBM Corporation

Martini B & Choo K-KR 2012. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation* 9(2): 71–80

McKemmish R 2008. When is digital evidence forensically sound. *Advances in Digital Forensics* IV(285): 3–15

McKemmish R 1999. What is forensic computing? *Trends & Issues in Crime and Criminal Justice* no. 118. Canberra: Australian Institute of Criminology. http://www.aic.gov.au/publications/current%20series/tandi/101-120/tandi118.html

Me G & Rossi M 2008. Internal forensic acquisition for mobile equipments, in *Proceedings of IEEE International Symposium on Parallel and Distributed Processing*: 14–18 April 2008: 1–7

Obaidli HA, Iqbal A & Iqbal B 2012. A novel method of iDevice (iPhone, iPad, iPod) forensics without jailbreaking, in *Proceedings of 2012 International Conference on Innovations in Information Technology* (IIT): 18–20 March 2012: 238–243

Owen P & Thomas P 2011. An analysis of digital forensic examinations: Mobile devices versus hard disk drives utilising ACPO & NIST guidelines. *Digital Investigation* 8(2): 135–140

Quick D & Choo KKR 2013. Digital droplets: Microsoft SkyDrive forensic data remnants. *Future Generation Computer Systems* 29(6): 1378–1394. http://www.sciencedirect.com/science/article/pii/S0167739X13000265

Quick D & Choo K-KR forthcoming. *Dropbox analysis: Data remnants on user machines*. Digital Investigation

Savoldi A & Gubian P 2008. Data recovery from Windows CE based handheld devices. *Advances in Digital Forensics* IV(285): 219–230