The role of mobile forensics in terrorism investigations involving the use of cloud apps

Niken Dwi Wahyu Cahyani[a,b]
[a]University of South Australia
Adelaide, Australia 5095
+61883023807
[b]Telkom University, Bandung, Indonesia
niken.cahyani@mymail.unisa.edu.au

Nurul Hidayah Ab Rahman[a,c]
[a]University of South Australia
Adelaide, Australia 5095
+61883023807
[c]Universiti Tun Hussein Onn Malaysia, Johor, Malaysia
nurul_hidayah.ab_rahman@mymail.unisa.edu.au

Zheng Xu
Third Research Institute of the Ministry of Public Security
Shanghai, China
+8613817917970
xuzheng@shu.edu.cn

William Bradley Glisson
School of Computing
University of South Alabama
Alabama, USA
+12514607634
bglisson@southalabama.edu

Kim-Kwang Raymond Choo
University of South Australia
Adelaide, Australia 5095
+61883025876
raymond.choo@fulbrightmail.org

ABSTRACT
Mobile technologies can be, and have been, exploited in terrorist activities. In this paper, we highlight the importance of mobile forensics in the investigation of such activities. Specifically, using a series of controlled experiments on Android and Windows devices, we demonstrate how mobile forensic techniques can be used to recover evidentiary artefacts from client devices when popular cloud apps – Google Drive, Dropbox, and OneDrive – were used on the devices.

CCS Concepts
• Applied computing~Investigation techniques • Applied computing~Evidence collection, storage and analysis

Keywords
Android forensic; Mobile forensic; Terrorist investigations; Windows Phone forensic.

1. INTRODUCTION
Smart mobile devices are increasingly popular with both individuals and businesses. For example, Gartner reported that the worldwide sales, of smart mobile devices, were more than 300 million units in 2015, which is a 15.5 percent increase over the same period in 2014 [1]. However, mobile devices can also be criminally exploited by terrorists to facilitate terrorist activities, including the financing of terrorism [2], [3] .

Terrorism can be defined as "the use of violence by groups or individuals pursuing political objectives. Terrorists are frequently indiscriminate in their attacks and can deliberately target civilians and non-combatants, often seeking to inflict mass casualties" [4]. In the recent terrorist attack on December 2015 at San Bernardino, 14 civilians were reportedly killed and 22 were wounded. Subsequently, Apple Inc. refused to assist the Federal Bureau of Investigation's request to unlock an encrypted iPhone 5C allegedly belonging to one of the key suspects, as the suspect disabled iCloud backups several weeks prior to the incident [5]. This particular incident generated significant media attention, as well as debates among researchers and policymakers. This incident also demonstrated the potential role of mobile forensics in recovering evidential data from smart mobile devices due to the use of devices and apps during the planning, execution, etc., of terrorism (and other criminal) activities. For example, cloud storage apps may be used to store incriminating evidence, and communication apps used to exchange voice and video messages. Using forensic techniques, one could potentially recover information such as chat logs, multimedia files, contact lists, and geo-tagged data, which can then be used to determine the chain of events, and identify their associates.

The role of mobile forensics in terrorism investigations is, thus, the focus of this study. We demonstrate how our previously published integrated incident handling and digital forensics model [6] can be used to guide a mobile forensic investigation.

2. BACKGROUND
2.1 Terrorism
Terrorist-related activities can be broadly classified into (1) information propagation, (2) information concealment, (3) fund raising, and (4) recruitment and training [7]–[9].

Information propagation concerns the creation and dissemination of politically- or ideologically-motivated propaganda (e.g. video and text) with the aims of influencing a particular segment of the community, radicalising potential supporters, and inciting "naïve"

MOBIMEDIA 2016, June 18-19, Xi'an, People's Republic of China
Copyright © 2016 EAI
DOI 10.4108/eai.18-6-2016.2264416

individuals to conduct terrorist and other criminal activities [8]–[10].

Information concealment involves the misuse of (secure) communication platform to disseminate information to circumvent law enforcement scrutiny and existing surveillance tools [11]. Methods that can be used to conceal messages include steganography, encryption, IP-based cloaking, and anonymising.

Fundraising refers to the collection of funding to support terrorism and related operations. Source of funding includes donations from supporters, diverting funds raised by legitimate means (charity donations), and proceeds of crime [8], [12], [13].

Recruitment, of terrorist members, includes reaching out, communicating, influencing and radicalizing like-minded individuals on social networking sites and other informational communication technologies (ICT) [7]. The ease in disseminating and hosting training materials (e.g. how to build a dirty bomb guide) on publicly accessible websites result from the Internet being a virtual training ground.

In the context of this paper, examples of how mobile technologies can be used to facilitate or enable terrorism activities include using banking apps to raise funds, compromising mobile devices (e.g. malware) to steal sensitive information, acquiring funds (e.g. from compromised accounts), and using mobile steganography apps to conceal information. It is, therefore, imperative for investigators to have an up-to-date understanding of mobile forensic techniques [14]–[16].

2.2 Mobile forensics

As defined by the National Institute of Standards and Technology (NIST), "[m]obile device forensic is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods" [17]. Digital evidence acquisition in mobile forensic activities involves physical, logical, and manual methods. Physical acquisition refers to recovering binary representations of the internal memory of mobile devices and dumping them into files, while logical acquisition interacts with a mobile device's operating system to recover the logical objects stored in the file system [18]. Manual acquisition involves viewing the data content stored on a mobile device that requires manual manipulation of the buttons, keyboard or touchscreen and may be recorded using an external digital camera [17]. Existing mobile forensic research can be broadly classified into: (1) examining the capabilities of acquisition methods, (2) undertaking detailed forensic procedures, and (3) conducting in-depth forensic analysis of mobile apps or mobile operating systems.

Tassone et al. [19] demonstrated that mobile forensic tools have different capabilities in recovering artefacts from different mobile Operating Systems (OS). The author indicates that the amount of artefacts recovered varies for different OSs and that specific tool support for physical acquisitions of certain phone models is not always present. This is consistent with Glisson et al.'s [20] study, which concluded that there is a considerable variation in recovery results between recovery methods and between toolkits performance. They acknowledge that this variance can be caused by vendors having different designs, overall software engineering requirements, and practical implementation decisions. The authors go on to highlight the fact that this variance makes it, potentially, difficult to validate artefacts recovered by different toolkits. Focusing on Windows Mobile data recovery, Grispos et al. [18] conducted all three acquisition methods to a pre-defined dataset that contains various data formats such as documents, audio, video, and text messaging. The study showed that it is possible to recover files and artefacts from memory images of Windows Mobile devices using a combination of file carvers and string extraction software.

Specific procedures and techniques of a digital forensic investigation are required to ensure evidence can be acquired in a forensically sound methodology. Using several cloud storage services such as Amazon S3, Dropbox, Evernote, and Google Docs as case studies, Chung et al. [21] proposed to utilise iPhone backup files and rooting Android devices to collect evidence of interest. Based on McKemmish's framework [22], Martini et al. [23] proposed an evidence collection and analysis methodology for Android devices with detailed processes in the collection phase. Ariffin et al. [24] presented an operational technique to recover deleted image files by referring to an iOS journaling file system. Leom et al. [25] demonstrated forensic collection and analysis of thumbnails in Android that would be significant for investigating steganography image.

Recent research by Berman et al. [26] and McMillan et al. [27] indicate that GPS and mobile device artefact evidence is escalating in court case impact. Hence, locating specific evidentiary value, to be used in a court of law, requires an in-depth forensic analysis of extracted artefacts. An analysis of mobile cloud apps by Martini et al. [23] on Android; and Grispos et al.'s [28] analysis on both iOS and Android identified types of evidence artefacts along with their location on the devices' file system. Al Mutawa et al.'s [29] research showed different extraction results from social networking apps such as Facebook, Twitter, and MySpace found on Blackberry, Android, and iPhone. The authors observed no traces of social networking activities could be recovered from Blackberry devices. Whereas, iPhone and Android phones stored significant amounts of evidentiary data. Farhood et al. [30] examined social network app artefacts left on Android internal memory and iOS internal storage that produced evidence of interest which include login, username, password, name, contact information, profile picture, work and education, location, friend list, posts, messages, comments, and IP addresses.

The literature clearly presents the extent to which acquired artefacts depend on acquisition techniques, types of mobile operating systems, and support features of forensic tools. Current research indicates that file system architectures require particular techniques that pose challenges in mobile forensic investigations. Recent research also indicates that validation of extracted artifacts is not a trivial undertaking. Therefore, an in-depth understanding of acquisition techniques, file systems architecture, forensic tools features, artefacts taxonomy, and users' activities that triggered cybersecurity incidents are key points to provide effective investigation practices along with constructing event scenarios.

3. EXPERIMENTAL SETUP

Mobile devices were used to act as a sender (S) and a receiver (R) for both Android and Windows Phone platforms. Details of the used hardware and software are as follows.

- Sender devices — Samsung GT-i9300 Galaxy SIII; Nokia Lumia 625
- Receiver devices — Samsung GT-P3100 Galaxy Tab 2 7.0; Nokia Lumia 735
- Cloud storage apps — Dropbox (Android: v3.0.6.0.2; Windows Phone: v1.2.0.0), GoogleDrive (Android: v2.3.474.23.24) and OneDrive (Android: v3.6; Windows Phone: v3.6.3.0 for Nokia Lumia 625 and v4.15.0.0 for Nokia Lumia 735)
- Mobile forensic — XRY v6.15

- Mobile steganography apps — Stegais (Android: v1.2.2; Windows Phone: v1.2.0.0)

Our experiments simulate two scenarios of common terrorism activities: (1) information propagation activities that use public cloud storage services, and (2) information concealment activities that are associated with steganography apps. Figure 1 presents the acquisition procedures of our experiments. Initial inspection refers to early examination of device condition by collecting information such as manufacturer of device, model name, and IMEI number. The power status of devices will determine acquisition techniques. Logical acquisition is conducted if the power device is on and begins with the identification of missed calls, unread messages and time/date through the device's screen examination.

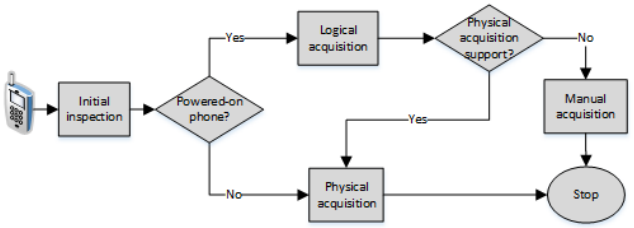

Figure 1. Data acquisition procedure

Physical acquisition is conducted if the devices' power is off while manual acquisition is optional if results from logical acquisition are limited and/or physical acquisition is not supported.

4. FINDINGS

4.1 Information Propagation

A pre-defined dataset was prepared that comprises 37 files made up of document, audio, picture, video and executable files. A description of the successful actions of upload, read and download files are presented in Figure 2. The actions were executed using both mobile client apps and mobile web browsers. Observation for Google Drive on mobile web browsers is discarded as the interface does not display properly in both Android and Windows Phones. Additionally, a mobile client app of Google Drive is not available in the Microsoft Apps store.

In Android devices, all file types and formats can be uploaded using both mobile client apps and a mobile web browser, while read and download actions present dissimilarity results. The mobile client apps of Dropbox, Google Drive, and OneDrive allow R to read files without downloading for all file types and formats. It should be noted that opening files in `.docx` and `.pdf` format from OneDrive required the Microsoft Office Mobile app.

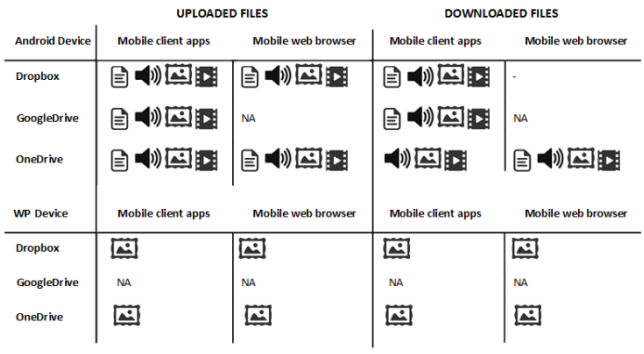

Figure 2. Uploaded and downloaded files

Using a mobile web browser for Dropbox, read actions cannot be undertaken without download, but OneDrive interface allows the actions for all file types and formats (without required Microsoft Office Mobile).

In Windows devices, on the other hand, it was identified that only image files were successfully uploaded. This was due to a limitation of the attachment menu to other types of files. Read and download actions therefore were undertaken for image files. It was observed that 7 out of 13 image files could be downloaded using a mobile web browser for Dropbox.

4.1.1 Artefacts on Android Devices

Artefacts on Android devices were collected using a combination of physical, logical and manual acquisition methods. A physical acquisition was undertaken on the sender's device whereas logical and manual acquisitions were undertaken on the receiver's device. It should be noted that XRY did not support physical acquisition of the receiver's device. Therefore, the dataset artefacts on the receiver's device were analyzed from a logical acquisition perspective. While the receiver's account information was mainly analyzed using manual acquisition techniques after we rooted the device. A rooting approach is applied to show that the receiver's account information is available and that there is a need for a proper method to acquire this information in a forensically sound manner. We are, however, aware that data alteration issues might occur when rooting a device.

A. Sender – Receiver Account

The cloud storage service account ID that connected devices is key information for further investigations. `Launcher.db` gives information about the execution of the Dropbox, GoogleDrive and OneDrive that can be used to confirm that the apps have been executed on the device. `Account.db` is a local SQLite database that contains account ID metadata for its associated component apps and encrypted passwords (see Table 1). We noted only Dropbox does not keep users' passwords in the table.

Table 1. Sender – receiver account artefacts in Android devices

id	**Name - Sender**	**type**	**password**
1	iar…@…l.com	Dropbox	-
2	iar…@…l.com	GoogleDrive	oauth2rt …
3	iar…@…l.com	SkysDrive	MCTlvExq…
id	**Name - Receiver**	**type**	**Password**
1	vic…@…l.com	Dropbox	oauth2rt…
2	vic…@…l.com	GoogleDrive	
3	vic…@…l.com	SkysDrive	MCX5!538…

Each cloud storage services has its own local SQLite database to keep account information. The information for Dropbox is stored in `prefs.db`; GoogleDrive's information can be found in `Doclist.db` in table `Account149`; and OneDrive keeps the information in `metadata.db` that can be located from table `item`.

B. Upload/Sharing – Access/Download Activities

We compared the acquired metadata between sender's device and receiver's device to map the Upload/Sharing – Access/Download activities. For Dropbox, useful information can be found from a database called `db.db` and a table called `upload_log`. Meanwhile, both GoogleDrive and OneDrive do not have a specific upload log table but upload information can be located from their key tables: `Entry149` and `item`, respectively. All activities' timestamp are presented in Epoch format. One example of OneDrive's log is shown in Table 2.

Table 2. OneDrive's log examples of uploaded and downloaded files

Side	Owner (id)	Create (date)	Shared (date)	Owner (Name)	Account
S	3E2…6	144…7	144…1	iar…@...l.com	iar…@…l.com
R	3E2…6	144…7	144…1	OneDrive user	vic…@…l.com

Cloud storage applications store cache file artefacts in a specific cache folder path. Cache files refer to files that have been accessed without being downloaded. Dropbox keeps the viewed files metadata in the path:

`/USERDATA/media/Android/data/com.dropbox.android/cache/thumbs/<foldername>/<filename>/.`

The cache folders of Google Drive can be located in the path:

`/USERDATA/data/com.google.android.apps.docs/cache/diskCache/fetching/accountCache_2/.`

The location of cache folders for OneDrive is:

`/USERDATA/data/com.microsoft.skydrive/no_backup/stream_cache/victimiarg@gmail.com/202/streams/.`

C. Clearing Traces

We simulated clearing trace activities of a sender by uninstalling the cloud storage apps and clearing browsing data. Data acquisition procedures were repeated and we observed the same evidence locations. The system's database of cloud apps are still in the device's internal memory but do not contain data in specific tables.

However, username ID for both Dropbox and Google Drive accounts, and the encrypted password of Google Drive still exist in `accounts.db` (see Table 3).

Table 3. Clearing trace artefacts for cloud storage services

id	name	Type	password
1	iar…@…l.com	Dropbox	-
2	iar…@…l.com	GoogleDrive	oauth2rt_1 ……

There is minimal data that mobile forensic investigations could acquire from cloud apps in this scenario. It is most likely that other types of forensic investigations would support evidence correlation such as data that is gathered from examining network logs.

D. Event Reconstruction

An example of event reconstructions for information propagation activity using Android devices is illustrated in Figure 3. We present the upload details of an executable file from the sender's side and report all artefacts on the receiver's side.

4.1.2 Artefacts on Windows Phone Devices

A. Sender – Receiver Account

It should be noted that XRY version 6.15 did not support physical acquisition of Windows Phone devices when this study was conducted. Logical acquisition obtained general information from sender and receiver devices such as device name, device manufacturer and model name.

B. Upload/Share – Read/Download Activities

Logical acquisition is conducted on both sender and receiver devices to collect the artefacts of upload/share – read/download activities. Media files such as documents, pictures, audios, videos, and archive files that were intact in the phone's internal memory and memory card were primarily acquired.

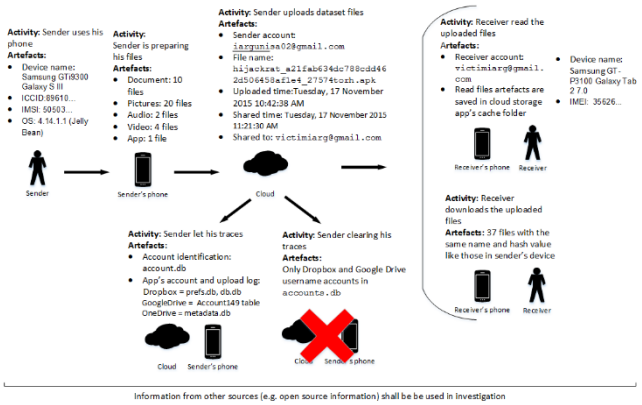

Figure 3. Information propagation on Android devices

Artefacts from cloud storage accounts, cache files, and xml documents (related with installation and apps' usage) were not found. Manual acquisition was conducted to identify any evidence of interest for cloud storage apps. Both of the sender and receiver phones were not protected with screen password, thus a complete list of installed apps, including cloud storage apps, were obtained. Examinations of archive folders (e.g. downloads) is recommended as the Windows Phone operating system allows users to side load an application. The archive folder is used to store `.xap` files of side load apps that might be useful in identify current or attempted installations of apps. A file's metadata such as name, type, size, created time and hash value were examined to reconstruct information propagation activities. Comparison of a file's metadata from sender and receiver suggested that the integrity for both of the uploaded files to and downloaded files from cloud storage is maintained (i.e. same file names and hash values).

C. Clearing Traces

We noted that there is no difference in logical acquisition results between, before and after uninstallation of cloud storage apps. There is also no difference in clearing browsing data activities extraction results.

D. Event Reconstruction

Event reconstruction for information propagation activities on Windows Phone devices is shown in Figure 4. From our findings, only image files were successfully uploaded and no artefacts were found even if the user viewed the files.

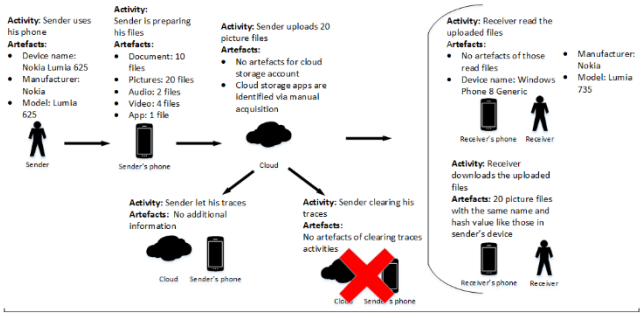

Figure 4. Information propagation on Windows Phone devices

4.2 Information Concealment

4.2.1 Artefacts on Android Devices

A. Sender – Receiver Account

OneDrive and Gmail were used to illustrate sending and receiving activities along with facilitating communication.

B. Hide/Send – Receive/Unhide Activities

Installation artefacts from the Stegais apps were collected from the path that has been created by the Android operating system: `/USERDATA/data/com.romancinkais.stegais/files/`. The generated steganography images can be located in: `/storage/sdcard0/stegais/`.

Similar with findings in Section 4.1.1, artefacts of shared steganography images on OneDrive are identified in `metadata.db` in table `item`. No artefacts are found for activities using Gmail. Moreover, no artefact was found if the sender did not store the steganography image to the device's internal memory before sending it.

We found traces of downloading from OneDrive and Gmail at `/storage/sdcard0/Download` path on the receiver's device.

C. Files Integrity

File integrity is maintained during transmission activities via OneDrive and Gmail services as evidenced by the same file name and hash values.

D. Event Reconstruction

An example of an event reconstruction for information concealment activities on Android devices is shown in Figure 5. We identify that OneDrive and Gmail did not change the integrity of the sent files.

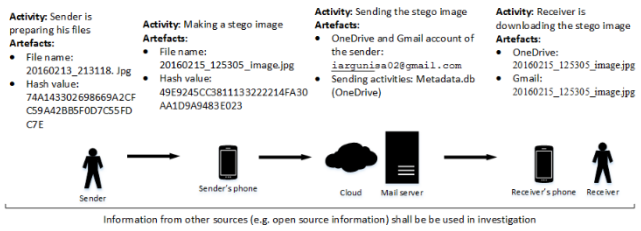

Figure 5. Information concealment on Android devices

4.2.2 Artefacts on Windows Phone Devices

A. Sender – Receiver Account

Logical acquisition results did not provide sufficient data to identify sender and receiver accounts for OneDrive and email.

B. Hide/Send – Receive/Unhide Activities

Steganography images can be prepared by taking pictures using the phone's camera and will be saved in the Camera Roll folder in the phone's memory. As expected, the logical acquisition successfully extracted an image from the Camera Roll folder.

The use of the Stegais app was identified from artefacts in documents and unrecognised files that were extracted from the sender's phones. `README_FIRST.txt` is an example of a Stegais app installation artefact that was extracted from `Lumia 625/SDcard/WPSystem/Apps/{D414A421-403A-4FCC-9069-7583604390BD}/Install`, where `{D414A4 21-403A-4FCC-9069-7583604390BD}` is a code for Stegais app in Windows Store. Another indication that Stegais was installed on the device was found in a collection of unrecognized files; `Steganography.ni.exe` was extracted from: `Lumia 625/SDcard/WPSystem/AppRepository/29636 DharmendraMauryaRajp.Steganography_1.0.0.0_neutral__d0xnxt1pzcw50/NI`.

Although the example files showed that a sender concealed information and delivered it, there is no artefact recovered from the hidden information that indicates the receivers' identity. Furthermore, the logical acquisition could only extract steganography images if the sender saves the images before sending them to the receiver. Manual acquisition was undertaken to identify the Stegais installation on the receiver's device; however, no documents nor unrecognized files were identified.

C. Files Integrity

We observed that cloud storage and email services do not modify the content of the sent steganography file. Uploaded and downloaded files have an identical hash value, but they have different file names.

D. Event Reconstruction

Figure 6 presents an event reconstruction of information concealment activity on Windows Phone devices. The findings are similar to the findings generated in the Android scenario.

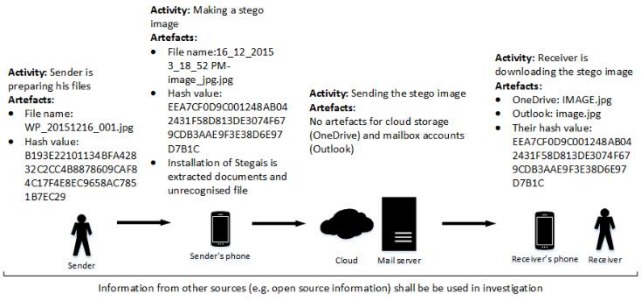

Figure 6. Information concealment on Windows Phone devices

5. CONCLUDING REMARKS

In this paper, we demonstrated the intricacies associated with investigating terrorist activities on mobile devices that interact with cloud environments. This research highlights the importance of mobile device forensics in these environments along with the necessity and potential utility of integrated incident handling and digital forensic models to investigate and reconstruct terrorist incidents. In our study, we also identified limitations of existing forensic tools in acquiring data from the wide range of mobile devices. Future research will extend this study to other apps and mobile devices through the implementation of practices proposed by Rahman and Choo [6].

REFERENCES

[1] Gartner. 2015. *Gartner Says Emerging Markets Drove Worldwide Smartphone Sales to 15.5 Percent Growth in Third Quarter of 2015*. [Online]. Available: http://www.gartner.com/newsroom/id/3169417 [Accessed: 28-Feb-2016].

[2] Choo, K.-K.R. 2013. New payment methods: A review of 2010–2012 FATF mutual evaluation reports. *Comput. Secur.* 36 (Jul. 2013), 12-26. DOI=http://dx.doi.org/10.1016/j.cose.2013.01.009.

[3] Choo, K.-K.R. 2014. Designated non-financial businesses and professionals: A review and analysis of recent financial action

task force on money laundering mutual evaluation reports. *Secur. J.* 27, 1, 1-26. DOI=http://dx.doi.org/10.1057/sj.2012.9.

[4] Australian Government. 2010. *Securing Australia: Protecting Our Community*. [Online]. Available: https://www.asio.gov.au/img/files/counter-terrorism_white_paper.pdf. [Accessed: 28-Feb-2016].

[5] Federal Bureau of Investigation. 2016. *Statement to Address Misleading Reports that the County Of San Bernardino Reset Terror Suspect's Iphone without Consent of the FBI*. [Online]. Available: https://assets.documentcloud.org/documents/2716811/Statement-from-the-FBI-Feb-20-2016.pdf. [Accessed: 28-Feb-2016].

[6] Ab Rahman, N. and Choo, K.-K.R. 2015. Integrating digital forensic practices in cloud incident handling: A conceptual cloud incident handling model. In *Cloud Security Ecosystem*, R. Ko and K.-K. R. Choo, Eds. Waltham, MA: Syngress, an Imprint of Elsevier, 383–400. DOI=http://dx.doi.org/10.1016/B978-0-12-801595-7.00017-3.

[7] Amble, J.C. 2012. Combating terrorism in the new media environment. *Stud. Confl. Terror.* 35, 5, 339-353. DOI=10.1080/1057610X.2012.666819.

[8] UNODC. 2012. *The Use of the Internet for Terrorist Purposes*. [Online]. Available: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf. [Accessed: 28-Feb-2016].

[9] Ogun, M.N. 2012. Terrorist use of internet: possible suggestions to prevent the usage for terrorist purposes. *J. Appl. Secur. Res.* 7, 2, 203-217.

[10] Choo, K.-K.R. 2008. Organised crime groups in cyberspace: A typology. *Trends Organ. Crime.* 11, 3 (Sep. 2008), 270-295. DOI=http://doi.org/10.1007/s12117-008-9038-9.

[11] Choo, K.-K.R., Smith, R.G., and McCusker, R. 2007. *Future directions in technology-enabled crime : 2007-2009*. Research and public policy No 78, Canberra: Australian Institute of Criminology.

[12] Choo K-KR, Smith RG, Walters J and Bricknell S. 2013. *Perceptions of money laundering and financing of terrorism in the Australian legal profession*. Research and Public Policy No 122(1), Canberra, ACT: Australian Institute of Criminology.

[13] Walters, J., Budd, C., Smith, R.G., Choo, K.-K.R., Mccusker, R., and Rees, D. 2012. Anti-money laundering and counter-terrorism financing across the globe: A comparative study of regulatory action. Research and public policy No 113, Canberra, ACT: Australian Institute of Criminology.

[14] Yang, T.Y., Dehghantanha, A., Choo, K.-K.R., and Muda, Z. 2016. Windows instant messaging app forensics: facebook and skype as case studies. *PloS One*. 11, 3 (Mar. 2016), e0150300. DOI= http://dx.doi.org/10.1371/journal.pone.0150300.

[15] Quick, D., Martini, B., and Choo, R. 2014. *Cloud Storage Forensics*. Waltham, MA: Syngress, an Imprint of Elsevier.

[16] Shariati, M., Dehghantanha, A., and Choo, K.-K.R. 2016. SugarSync forensic analysis. *Aust. J. Forensic Sci*. 48, 1, 95-117. DOI=10.1080/00450618.2015.1021379.

[17] Ayers, R., Brothers, S., and Jansen, W. 2014. Guidelines on mobile device forensics. *NIST Special Publication 800*, 101 Revision 1.

[18] Grispos, G., Storer, T., and Glisson, W.B. 2011. A comparison of forensic evidence recovery techniques for a windows mobile smart phone. *Digit. Investig.* 8, 1 (Jul. 2011), 23-36. DOI= 10.1016/j.diin.2011.05.016.

[19] Tassone, C., Martini, B., Choo, K.-K.R., and Slay, J. 2013. Mobile device forensics: A snapshot. *Trends Issues Crime Crim. Justice no. 460: 1–7*, Australian Institute of Criminology, Canberra.

[20] Glisson, W.B., Storer, T., and Buchanan-Wollaston, J. 2013. An empirical comparison of data recovered from mobile forensic toolkits. *Digit. Investig.* 10, 1 (Jun. 2013), 44-55. DOI= 10.1016/j.diin.2013.03.004.

[21] Chung, H., Park, J., Lee, S., and Kang, C. 2012. Digital forensic investigation of cloud storage services. *Digit. Investig.* 9, 2 (Nov 2012), 81-95. DOI= 10.1016/j.diin.2012.05.015.

[22] McKemmish, R. 1999. What is forensic computing? *Trends Issues Crime Crim. Justice no. 118:1-6*, Australian Institute of Criminology, Canberra.

[23] Martini, B., Do, Q., and Choo, K.-K.R. 2015. Mobile cloud forensics: An analysis of seven popular Android apps. in *Cloud Security Ecosystem*, R. Ko and K.-K. R. Choo, Eds Waltham, MA: Syngress, an Imprint of Elsevier, 309–345. DOI= 10.1016/B978-0-12-801595-7.00015-X.

[24] Ariffin, A., D'orazio, C., Choo, K.-K.R., and Slay, J. 2013. iOS Forensics: How can we recover deleted image files with timestamp in a forensically sound manner? In *Proceedings of the 8th International Conference on Availability, Reliability and Security (*Regensburg, Germany, Sept 2-6, 2013). IEEE, 375–382. DOI= 10.1109/ARES.2013.50.

[25] Leom, M.D., Dorazio, C.J., Deegan, G., and Choo, K.-K.R. 2015. Forensic collection and analysis of thumbnails in android. In *Proceedings of the 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communication (*Helsinki, Finland, Aug 20-22, 2015). IEEE, 1059–1066. DOI= 10.1109/Trustcom.2015.483.

[26] Berman, K.J., Glisson, W.B., and Glisson, L.M., 2015. Investigating the Impact of Global Positioning System Evidence. In *Hawaii International Conference on System Sciences* (Kauai, Hawaii, Jan 5-8, 2015). IEEE, 5234-5243. DOI= 10.1109/HICSS.2015.618.

[27] Mcmillan, J.E.R., Glisson, W.B., and Bromby, M. 2013. Investigating the increase in mobile phone evidence in criminal activities. In *Hawaii International Conference on System Sciences* (Wailea, Hawaii, Jan 7-10, 2013). IEEE, 4900-4909. DOI= 10.1109/HICSS.2013.366.

[28] Grispos, G., Glisson, W.B., and Storer, T., 2015. Recovering residual forensic data from smartphone interactions with cloud storage providers. In *Cloud Security Ecosystem*, R. Ko and K.-K. R. Choo, Eds. Waltham, MA: Syngress, an Imprint of Elsevier, 347–382. DOI= 10.1016/B978-0-12-801595-7.00016-1.

[29] Al Mutawa, N., Baggili, I., and Marrington, A. 2012. Forensic analysis of social networking applications on mobile devices. *Digit. Investig.* 9 (Aug. 2012), S24-S33. DOI= 10.1016/j.diin.2012.05.007.

[30] Farhood, N.D., Dehghantanha, A., Eterovic-Soric, B., and Choo, K.-K.R. 2015. Investigating social networking applications on smartphones detecting Facebook, Twitter, LinkedIn and Google+ artefacts on Android and iOS platforms. *Aust. J. Forensic Sci.* 1-20. DOI= http://dx.doi.org/10.1080/00450618.2015.1066854.