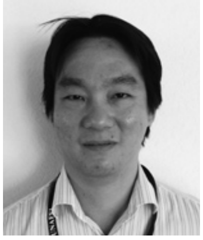
CONTEMPORARY DIGITAL FORENSIC INVESTIGATIONS

*Dr. Kim-Kwang Raymond Choo**



I. DIGITAL FORENSIC INVESTIGATIONS

Information and communications technologies (ICT) are fundamental to modern society and open the door to increased productivity, faster communication capabilities, and immeasurable convenience. However, the era of ICT-enhanced globalisation has also been accompanied by an increase in the sophistication and volume of malicious cyber-activities. Malicious cyber-activities are a rapidly expanding form of criminality that knows no borders, and such activities can have serious effects on the present and/or future of defensive or offensive effectiveness of a country's national and cybersecurity. The consequences can impact a vast array of sectors, including fixed and mobile telecommunications, traffic control systems, water treatment facilities, health and emergency services, defence and other government systems and much more (see Choo 2010b).

Given the increase in ICT (e.g. cloud services, mobile devices and Internet-of-Things) in everyday life, digital evidence is becoming more commonplace. However, attempting to gather digital evidence from a range of systems and devices, particularly across borders, resulted in new challenges for government and law enforcement agencies. The former South Australian Director of Public Prosecutions explained that "[f]or the prosecutor, the challenge is to have the data translated into a form that is acceptable as evidence to the courts ... Assuming that the fragile and elusive evidence can be gathered together, the prosecutor must keep in mind that he or she will one day need to be able to prove the chain of evidence. All processes will need to be appropriately documented in a way that can be understood by the layman, and the prosecutor must be prepared if necessary to demonstrate that the 'original' digital material has not been changed or tampered with in any way" (Pallaras 2011: 80). Such a process is known as digital forensics, and is increasingly being used in the courts in Australia and overseas. It is, therefore, important to have a rigorous methodology and set of procedures for conducting digital forensic investigation as well as incident response.

Digital forensics, a relatively new sub-discipline of forensic science when compared to other common forensic science disciplines, is the process of gathering evidence of some type of an incident or crime that has involved computer systems and their associated networks (see McKemmish 1999; Martini and Choo 2012; Quick, Martini and Choo 2014). In such circumstances, the expectation is that there has been some accumulation or retention of data by the various components of a system which will need to be identified, preserved and analysed. This process can be documented and defined, and be used to obtain information or evidence pertaining to a crime or malicious cyber-incident. For example, when the systems belonging to a cloud service provider are compromised, digital forensics can be used to facilitate the collection of evidence from compromised cloud servers and client devices for analysis. This would allow subsequent reconstructing of the incident and establish facts such as

- Where did the attack come from?;
- What vulnerability(ies) was/were exploited?; and
- What data / which systems was/were compromised? (Ab Rahman and Choo 2015).

*Fulbright Scholar and Senior Researcher, University of South Australia, Australia.
Email: raymond.choo@unisa.edu.au. This paper is compiled from the author's previously published materials, including those co-authored with Nurul Hidayah Ab Rahman, Abdullah Afzar, Andrew Butler, Quang Do, Jody Farnden, Lin Liu, Ben Martini and Darren Quick.

The evidence collected can be used to inform risk mitigation strategy as well as be used in the prosecution of the offender in a court of law. To ensure the admissibility of evidence in a court of law, it is necessary to identify and examine the many influences, impacts upon and contributions to the presentation of evidence by an expert witness. Suffice to note that for an expert witness to provide their opinion there must be forensic evidence that requires interpretation and presentation, and for forensic evidence to exist, an investigative process would need to have been undertaken in response to an incident, criminal or civil (Butler and Choo 2015).

McKemmish (1999, p. 1) provided one of the first definitions of digital forensics, defining it as: "the process of identifying, preserving, analysing and presenting digital evidence in a manner that is legally acceptable". There are four key elements in McKemmish's digital forensics framework — namely, the identification, preservation, analysis and presentation of digital evidence.

1. Identification of digital evidence defines the requirement for evidence management, knowing it is present, its location and its type and format.

2. Preservation is concerned with ensuring evidential data remains unchanged or changed as little as possible. For example, if a forensic investigator needs to recover data from a device, it is important that the data is recovered using methods that are forensically sound (e.g. they do not write to the original data source as information such as 'file last accessed times' on key system files could be changed if a seized computer is improperly booted before a disk image capture is undertaken).

3. Analysis transforms the bit level data collected in the earlier two phases into evidence presentable to a court of law.

4. Finally, the presentation element is concerned with presenting evidence to the courts in terms of providing expert testimony on the analysis of the evidence.

As noted by Martini and Choo (2012), another widely used digital forensics framework is that of the National Institute of Standards and Technology (NIST) (Kent et al. 2006). The four phases and definitions in NIST's framework share some similarities with the framework of McKemmish (1999):

1. Collection discusses identifying relevant data, preserving its integrity and acquiring the data;

2. Examination uses automated and manual tools to extract data of interest while ensuring preservation;

3. Analysis is concerned with deriving useful information from the results of the examination; and

4. Reporting is concerned with the preparation and presentation of the forensic analysis (Kent et al. 2006, p. ES-1).

II. CLOUD AND MOBILE FORENSICS

Due to the increasing popularity of consumer devices such as mobile devices and technologies such as cloud computing, existing forensic frameworks may not be fit-for-purpose. For example, existing digital forensic techniques are designed to collect evidential data from devices where we have physical access or from typical mobile device users (e.g. where advanced security features and anti-forensic techniques are rarely exploited to their full extent). In contrast, serious and organised criminals often make use of devices specifically designed to evade legal interception and forensic collection attempts. In the case of cloud forensics, Bagby and Schwerha (2013) also raised a number of legal questions, such as the physical location of records. As noted by the authors, "subpoenas used by investigators as well as the document production demands made in civil litigation generally require accurate physical location data for targeted files, backups, responsible custodians (humans), and knowledgeable supervisors" (Bagby and Schwerha 2013, p. 13).

Therefore, the digital forensic "space" can be seen as a race, not only to keep up with device (i.e.

hardware) and software releases by providers (e.g. cloud service provider and mobile app designers), but also from software and hardware modifications made by end users, particularly serious and organised criminals, to complicate or prevent the collection and analysis of digital evidence.

A. Cloud Forensics

The growth in the use of cloud computing has resulted in a growing need for forensic investigations involving cloud technologies and, consequently, spawned the growth of research in cloud forensics (Martini and Choo 2014). The lack of physical access to digital artefacts over the servers spanning across multiple jurisdictional areas as well as integrity of data artefacts (e.g. log files) provided by the Cloud Service Providers (CSP) (Chung et al 2012; Grispos, Storer, and Glisson 2013; Hooper, Martini, and Choo 2013; Martini and Choo 2014a) complicate digital investigations. Even if the evidence could be identified, it could be illegal to access the raw log data that contains records of multiple users in a multi-tenancy cloud environment (ENISA, 2012). The wide range of mobile devices (Zatyko and Bay 2011; Tassone et al. 2013) and the use of encryption by CSPs or individuals (Grispos, Storer, and Glisson 2012) further complicate cloud forensic investigations.

In recent years, researchers have attempted to extract evidential data from data remnants on client devices when a cloud storage service has been accessed on these devices. For example, Chung et al. (2012) analyzed Amazon S3, Google Docs and Evernote and, based on the findings, presented a plan to collect data from personal computers and mobile devices. Hale (2013) studied Amazon cloud drive on Windows XP and Windows 7 computers.

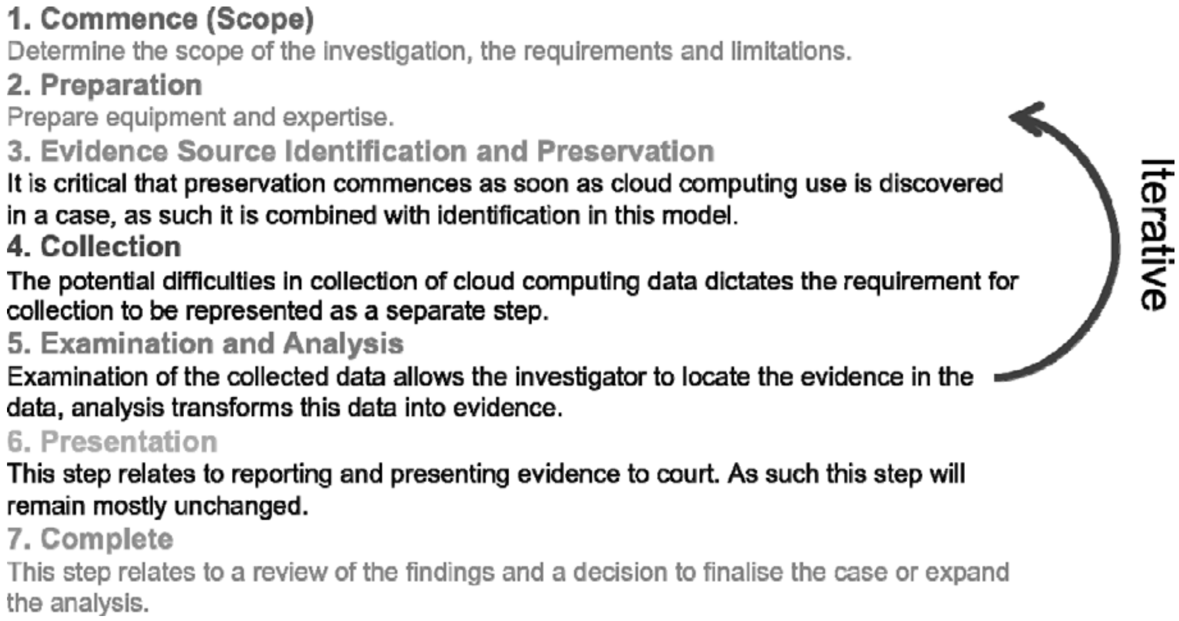
The first digital forensic framework designed for both client and server investigations of cloud services is presented by Martini and Choo (2012). The framework, based on McKemmish (1999) and NIST (Kent et al. 2006), has been validated by the authors using ownCloud (Martini & Choo 2013), XtreemFS (a distributed filesystem) (Martini & Choo 2014b), and vCloud (Martini & Choo 2014c), as well as by Thethi and Keane (2014) using EC2 cloud. There are four stages in this framework, namely: evidence source identification and preservation, collection, examination and analysis, and reporting and presentation for collecting digital evidence from the cloud environment — see Table 1.

1. Evidence Source Identification and Preservation. In this phase, potential sources of relevant data are identified. Any device capable of connecting to the cloud services, either via a browser or a client application, is considered a potential source of evidence. In this phase, the investigator should also ensure that ACPO principles are adhered to, wherever possible.

2. Collection. During collection of evidence from storage media, particularly media belonging to external parties, the investigator should also ensure that relevant laws and regulations are followed (Kent et al. 2006).

3. Examination and Analysis. Information from acquired data is extracted in this phase. Methods to circumvent or bypass protection mechanisms on the devices may be used to examine and analyze information collected and preserved from the previous phase (e.g. use of tools to brute-force password-protected data). During this phase, findings should also be reviewed with information or intelligence drawn from other sources and investigations before a conclusion is drawn.

4. Presentation. In the last phase, findings are documented for presentation in a court of law.



1. Commence (Scope)
Determine the scope of the investigation, the requirements and limitations.

2. Preparation
Prepare equipment and expertise.

3. Evidence Source Identification and Preservation
It is critical that preservation commences as soon as cloud computing use is discovered in a case, as such it is combined with identification in this model.

4. Collection
The potential difficulties in collection of cloud computing data dictates the requirement for collection to be represented as a separate step.

5. Examination and Analysis
Examination of the collected data allows the investigator to locate the evidence in the data, analysis transforms this data into evidence.

6. Presentation
This step relates to reporting and presenting evidence to court. As such this step will remain mostly unchanged.

7. Complete
This step relates to a review of the findings and a decision to finalise the case or expand the analysis.

Figure 1: Integrated cloud forensic framework of Quick, Martini and Choo (2014)

Another cloud forensic framework was proposed a year later by Quick and Choo (2013a) and validated using Dropbox (Quick and Choo 2013b), SkyDrive (Quick and Choo 2013a) and Google Drive Quick and Choo (2014). These two frameworks were subsequently merged into one (Quick, Martini, Choo 2014) — see Figure 1.

In the integrated framework, the process is iterative as it is common that during an investigation a forensic practitioner may need to return to a previous phase. For example, during the examination and analysis phase, a practitioner may uncover information relating to data stored with a particular CSP. The practitioner may start a new iteration of the framework and undertake enquiries to locate, identify, and collect the newly identified data using legal processes. At the same time, the forensic analysis of other data already collected would continue. Once the CSP has been identified, the investigator or the practitioner will commence preservation and collection of the data.

Table 1: Summary of cloud forensic challenges (Ab Rahman and Choo 2015)

Cloud	Challenges	Service(s) affected	Potential mitigation strategies	References
Multi-tenancy (Virtualised environment)	Confidentiality and privacy issue of data belonging to or about cloud service users (CSUs) residing on the same physical machine but are not part of the law enforcement investigation or court orders	SaaS , PaaS, IaaS (slightly)	Virtual machine (VM) snapshots can serve as the acquisition image; traditional forensic acquisition may need to be adapted; digital forensics readiness; standard event information format; Information disclosure policy Potential research topic: Remote cloud forensics	(Grobauer & Schreck 2010); (Monfared & Jaatun 2012); (Zimmerman & Glavach 2011)
	Cloud service provider (CSP) may have difficulties in specifically referring to the malicious or compromised VM, due to resource pooling	IaaS		
	Different log formats due to different hardware used, and challenges in segregating log files of CSUs not under investigation	SaaS, PaaS, IaaS		
Multi-location (i.e. data location)	Complications due to time synchronisation as data is likely to reside on multiple physical machines in multiple geographical regions with different time zones	SaaS, PaaS, IaaS	Harmonised regulation and compliance; improving log generation technique to allow successful analysis and correlation of information from varying sources; improving live analysis techniques; international protocol to achieve time synchronisation (e.g. RFC 5095); digital forensics readiness	(Grobauer & Schreck 2010); (Zimmerman & Glavach 2011); (Martini & Choo 2012)
	Data mirroring over multiple machines in different jurisdictions, lack of transparency, and non-uniform privacy and related laws	SaaS, PaaS, IaaS		
	CSP may not be able to provide a precise physical location of the data location	SaaS, PaaS, IaaS		
Scope of user control (and cloud actors participation)	Logging and log details are heavily dependent on CSP: CSU has no or limited access to event sources and vulnerability information generated by infrastructure components under the control of CSP	SaaS, PaaS	● Granular configuration of functionality and access rights; and must be clarified in SLA ● Client-side incident response and forensic investigation can be conducted for IaaS and PaaS ● CSP should provide a set of security APIs (e.g. event monitoring, forensic services, IDS/IPS, policy-based autonomic management system) as add-on services, or implementing middleware tool ● CSP can implement software agent on CSU's site to facilitate a cross-layer security solution; therefore neither CSU nor CSP need to know each other's architecture. ● Incident detection and reporting obligations (e.g. Amazon Vulnerability Report, ENISA Cloud Incident Reporting Framework), and must be set out in SLA ● More attention to mutual auditability ● Dedicated monitoring tool and policy of cloud insider incident.	(Grobauer & Schreck 2010); (Monfared & Jaatun 2012); (Kozlovszky et al. 2013); (Sarkar et al. 2011); (Li et al. 2012); (Dekker, Liveri & Lakka 2013)
	Inability to add security-specific event sources (e.g. web application firewall)	SaaS, PaaS		
	No or limited knowledge about architecture	SaaS (mostly), PaaS		
	Unclear incident handling responsibilities among cloud stakeholders	SaaS, PaaS, IaaS		
	Data ownership — deleted data, terminated contract, CSP shuts down business.	SaaS, PaaS, IaaS		
	Participation of a few number of CSPs, e.g. a CSP that provides an email application (SaaS) may depend on a third-party provider to host log files (PaaS)	SaaS (mostly), PaaS, IaaS		
	Requires a specific strategy for incident handling	SaaS (mostly), PaaS, IaaS (slightly)		
	CSP's employee (insider) may compromise security and privacy of CSU	SaaS (mostly), PaaS, IaaS (slightly)		
	Lack of coordination or interruption of activities correlation (dependency chain) across cloud stakeholders	SaaS (mostly), PaaS, IaaS		
	Misdirection of incident reporting (to whom should reports be directed?)	SaaS, PaaS, IaaS		

B. Mobile Forensics

Evidential information that can be potentially extracted from a mobile device includes SMS messages, phone call logs, photos and location data. While extraction of these types of data has been commonplace for some time, more recently a focus has been placed upon collecting data from third-party apps that users install on their mobile devices. In a recent work, for example, Azfar, Choo and Liu (2015) examine 40 popular Android mobile health apps. Based on their findings, a taxonomy incorporating artefacts of forensic interest to facilitate the timely collection and analysis of evidentiary materials is proposed — see Table 1.

App Name	Version	App Category				Artefact Category						
		Patient care and monitoring	Health apps for the layperson	Communication, education, and research	Physician or student reference	Databases	User credentials and pins	Personal details of users	User activities	User location	Activity timestamps	Images
MyFitnessPal	3.6.1	P	F	P	N	F	P	F	F	N	F	F
RunKeeper - GPS	5.4	N	F	N	N	F	N	N	F	F	F	N
Period Calendar	1.51	P	F	N	N	F	F	F	F	N	P	N
WebMD	3.5	N	F	F	P	P	N	N	P	N	N	N
Blood Pressure (BP) Watch	3.0.11	P	F	N	N	F	N	P	F	N	F	N
Calorie Counter by FatSecret	-	P	F	P	N	F	N	N	F	N	P	N
Google Fit	1.51.07	N	F	N	N	P	N	N	P	N	F	N
MyNetDiary Calorie Counter PRO	2.2.0	P	F	P	N	N	N	N	N	N	N	F
Drugs.com Medication Guide	1.23	N	F	F	P	F	N	F	N	N	P	N
My Diet Diary Calorie Counter	1.9.11	P	F	P	N	F	N	P	F	N	F	N
Calories! Basic – cal counter	1.1.7	P	F	P	N	F	N	N	P	N	F	N
Period Tracker	2.0.6.4	P	F	N	N	F	N	N	F	N	P	N
Calorie Counter	4.2.5	P	F	P	N	F	N	F	F	N	F	N
My Pregnancy Today	1.14.0	P	F	N	N	N	P	N	N	N	N	F
Water Your Body	3.062	N	F	N	N	F	N	N	F	N	N	N
Instant Heart Rate	-	P	F	N	N	F	N	N	N	N	N	N
Calm – Meditate, Sleep, Relax	1.9.4	N	P	N	N	F	N	F	N	N	F	N
Runtastic Pedometer	1.5.1	N	F	N	N	F	N	N	F	N	F	N
Smiling Mind	2.0.3	N	F	N	N	F	N	F	N	N	F	N
Pedometer	5.10	N	F	N	N	P	N	N	F	N	F	N
Quit Now: My QuitBuddy	2.1	P	F	N	N	N	N	N	N	N	N	F

App Name	Version	App Category				Artefact Category						
		Patient care and monitoring	Health apps for the layperson	Communication, education, and research	Physician or student reference	Databases	User credentials and pins	Personal details of users	User activities	User location	Activity timestamps	Images
Mindbody Connect	2.8.3	N	P	N	N	F	N	N	P	P	N	N
My Baby Today	-	N	F	N	N	F	N	F	N	N	P	N
Lifesum- Calorie Counter	-	P	F	P	N	F	N	P	F	N	F	F
Quit Smoking – QuitNow!	-	N	F	N	N	N	N	N	N	N	N	N
Strava Running and Cycling GPS	4.3.1	N	F	N	N	F	N	F	F	F	F	N
Lorna Jane	1.2	N	F	N	N	F	N	N	P	F	F	F
Walk with Map My Walk	3.5.1	N	F	N	N	F	N	F	F	F	F	P
FitNotes – gym Workout Log	1.12.0	P	F	N	N	F	N	N	F	N	P	N
Nike+ Running	1.5.2	N	F	N	N	F	N	F	F	N	F	F
30 day Ab Challenge	2.0	N	P	N	N	N	N	N	N	N	N	N
Genesis YNB	1.0.2	N	F	N	N	N	N	F	N	P	N	F
BMI Calculator	-	N	P	N	N	N	N	N	N	N	N	N
Endomondo Running Cycling Walking	10.6.3	N	F	N	N	F	N	N	F	F	F	F
Fitness Buddy: 300+ Exercises	3.10	N	F	N	N	F	N	N	F	N	F	N
My Tracks	2.0.9	N	F	N	N	F	N	N	F	F	F	N
Under Armour Record	2.1.1	N	F	N	N	F	N	F	F	N	F	F
Noom Walk Pedometer: Fitness	1.1.0	N	P	N	N	F	N	N	F	N	F	F
Bleep Fitness Test	1.8	N	P	N	N	F	N	F	F	N	P	N
BodySpace- Social Fitness	1.3.9	N	F	N	N	F	N	F	F	N	P	F

Notes: "F" - detailed information was recovered; "P" - only partial information was recovered (e.g. artefacts from some apps provided partial timestamp such as only the date of the activity rather than the time in hours, minutes and seconds); and "N" - unsupported category.

Table 1: Mobile health app forensic taxonomy (Azfar, Choo and Liu 2015)

However, there has not been a commensurate level of research conducted on the most effective method of collecting and analyzing evidence from mobile apps. Much of the research (Barmpatsalou et al. 2013) which has been conducted in this area has also aged, as mobile devices and apps continue to advance and change with new mobile devices and apps being released on a regular basis.

Current digital forensics techniques for extracting data from a mobile device can be categorized into live analysis where the forensic information is taken directly from the device, and offline analysis where a copy of the device's data is analyzed (Martini, Do and Choo 2015a). However, existing research does not generally use a forensic framework as the basis of their evidence collection and/or analysis techniques.

Therefore, to contribute towards filling the literature gap, Martini, Do and Choo (2015a) present an evidence collection and analysis methodology for Android devices, which is designed to comply with forensic soundness principles, particularly in terms of data handling, and that the process is device agnostic as far as practical. The utility of the methodology is then demonstrated using seven popular Android cloud-based apps (Martini, Do and Choo 2015b) and nine popular Android mobile dating apps (Farnden, Martini and Choo 2015). Dating apps are a previously understudied app category that makes significant use of a user's location when the user checks-in, such as with Facebook and Foursquare, or uses a more active proximity system, where a user's location is continuously broadcast to find nearby users or locations.

Dating apps have come into public focus as popular dating sites, such as Plenty of Fish, are now reporting that 70% of usage takes place via a mobile phone. A study of the homosexual community found that many gay men surveyed had used mobile phones and a GeoSocial app (Phillips et al., 2014) to facilitate casual meetings. This is not surprising when Grindr, a popular gay dating GSN, has millions of users and continues to grow daily (Grov et al., 2014).

Despite all the hype and attention to dating apps, these services remain relatively understudied in traditional academic research, mainly being studied and analyzed only by enthusiasts. There is also limited support by professional forensic tools used by law enforcement and government agencies (e.g. EnCase, XRY, LANTERN, Paraben device seizure and ACESO), with most tools focusing on the more traditional address book and call log data. This inhibits the process of evidence collection, which is undertaken when a crime involving one or more of these apps is reported.

In the study of Farnden, Martini and Choo (2015), they determined that "[d]ating apps store messages or location readings on the device that can be used to reconstruct events or prove an alibi, which may aid in the prosecution of crimes involving these apps. In many cases, activities performed on the dating app could expose other members of the community, such as in the Grindr database, where there is a collection of all profiles the user has seen nearby, and the Skout app, which collected Facebook data from non-Skout users. In two cases (i.e. the FullCircle and MiuMeet apps), private images were viewable, which could be exploited by a malicious actor and this is a clear violation of user privacy".

III. THE WAY FORWARD

Contemporary digital forensics, particularly extracting data from remote cloud systems and devices that provide advanced security not only for data at rest (which has now become commonplace across all smart mobile devices) but also advanced encryption capabilities for data in transit (such as instant messages and emails being transmitted and received from a mobile device management (MDM) server), is an under-researched topic.

Current forensic techniques make use of vendor data communication facilities built into the mobile devices (e.g. iTunes backups for iOS devices) for the purpose of forensic extraction. Often this limits the potential for data extraction, for example, current tools would not be able to collect evidence from devices that are encrypted using strong passwords. A mobile computing device, such as a BlackBerry, which has been configured securely is almost impossible to analyze using current prevalent forensic techniques. Challenges faced by the digital forensic community are compounded when anti-forensic techniques are added to a device via software/hardware manufacturers or individual device users.

Therefore, it is important that research efforts be focused on contributing to filling the knowledge gap between existing scholarship and challenges faced by digital forensic practitioners and researchers (including those in governments) in this rapidly changing environment by addressing the following research questions:

1. How ICT are used in the commission and execution of serious and organized crimes, and how suspects are using advanced security features on systems and devices as well as anti-forensic techniques to evade legal forensic collection attempts?

2. What types of evidential data (e.g. data-at-rest and data-in-transit) are available, considering the

advanced security features and anti-forensic techniques that could be utilised by serious and organised criminals?

3. What techniques can government and law enforcement agencies use to legally gain access to the identified evidential data by circumventing advanced security features (e.g. developing low-level exploits and undertaking physical hardware analysis), without compromising the evidence's integrity?

To keep pace with the growth and changing face of criminal activity, particularly to ensure that evidential data can be forensically recovered, a number of governments have undertaken measures to enhance their technical capability (and in some instances, seeking to circumvent or weaken existing security measures) and introduce legislation that allows national security and law enforcement agencies to conduct online surveillance. For example, in September 2014, Australian government agencies have successfully lobbied for new legal powers to put Internet users under surveillance (see National Security Legislation Amendment Bill (No. 1) 2014).

Legitimate surveillance by government agencies (e.g. law enforcement, criminal intelligence and national security agencies) can be an effective crime deterrence measure, gather evidence, monitor the behaviour of known offenders and reduce the fear of crime. For example, analysis of intelligence gathered from different or disparate data sets (including data from the cloud and big data applications) may facilitate the prediction of major impending events and identify connections between individuals of interest.

Due to the advancement of ICT and interconnectedness of our society, however, the scope and reach of online surveillance by governments is constantly being expanded and sometimes to the detriment of individual privacy. For example, when we upload to or store our data (e.g. photos, videos and documents) in one of the cloud services, do we know the path of the transmitted data (i.e. through which countries or internet service providers our data will be routed) or whether anyone is collecting and analysing our transmitted or stored data?

While there is a legitimate need for cooperation between cloud service providers and governments, there are also concerns about cloud service providers being compelled to scan or search data of interest to 'national security' and to report on, or monitor, particular types of transactional data (Choo 2010a). Concerns about wide-scale government surveillance targeting cyberspace and invasion of individual user data privacy are not restricted to authoritarian societies but also liberal democracies, particularly post-11 September 2001. In 2013, for example, leaked US National Security Agency (NSA) documents by Edward Snowden, a former NSA contractor, indicated that the agency allegedly undertook broad online surveillance activities. The latter includes intercepting and collecting information from non-US citizens (as well as US citizens if they are conversing with a foreign target) and targeting organizations such as major US cloud computing service providers (Gellman and Lindeman 2014; Greenwald 2014).

In response to the NSA surveillance revelations, the European Parliament conducted an inquiry on the impact of the surveillance programme on European Union (EU) citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. It was determined that these programmes allowed for the mass surveillance of internet users "through direct access to the central servers of leading US internet companies (PRISM programme), the analysis of content and metadata (Xkeyscore programme), the circumvention of online encryption (BULLRUN), access to computer and telephone networks, and access to location data, as well as to systems of the UK intelligence agency GCHQ such as the upstream surveillance activity (Tempora programme), the decryption programme (Edgehill), the targeted 'man-in-the-middle attacks' on information systems (Quantumtheory and Foxacid programmes) and the collection and retention of 200 million text messages per day (Dishfire programme)" (European Parliament 2014, p. 20).

The concern is generally not about the privacy rights of criminals or terrorist suspects, but the unintended collateral damage where the privacy of innocent individuals and ordinary citizens may be comprised in such surveillance programmes (e.g. finer granulated aspects of an individual's life are derived or inferred from the intelligence collection and analysis).

There is, therefore, a need to ensure that we balance the need for a secure cyberspace and the rights of individuals to privacy against the need to protect the community from serious and organized crimes and cybersecurity interests. This is an issue that has serious implications on the ability of governments to protect their citizens against serious and organized crimes. However, this remains an under-researched area perhaps due to the interdisciplinary challenges specific to this topic. Therefore, to develop theoretical clarity with real world applicability, it is important to bring together approaches from social science and computing to address the major contemporary forensic challenges associated with the use of securely configured ICT in serious and organised crimes.

References

N. H. Ab Rahman, and K.-K. R. Choo 2015. A survey of information security incident handling in the cloud. *Computers & Security*, vol. 49, pp. 45–69.

A. Azfar, K.-K. R. Choo, and L. Liu 2015. Forensic taxonomy of popular Android mHealth apps. In Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015), 13–15 August 2015, Puerto Rico [In press].

J. W. Bagby, and J. J. Schwerha 2013. Migrating digital forensics and electronic discovery into the cloud: An injustice risk analysis. <http://faculty.ist.psu.edu/bagby/Pubs/ALSB2013_0103_paper.pdf> [Last accessed 5 May 2015].

K. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos 2013. A critical review of 7 years of mobile device forensics. *Digital Investigation*, vol. 10, no. 4, pp. 323–349.

A. Butler, and K.-K. R. Choo 2015. IT standards and guides do not adequately prepare IT practitioners to appear as expert witnesses: An Australian perspective. *Security Journal* [In press, DOI: <http://dx.doi.org/10.1057/sj.2013.29>].

K.-K. R. Choo 2010a. Cloud computing: Challenges and future directions. *Trends & Issues in Crime and Criminal Justice*, vol. 400, pp. 1–6. <http://www.aic.gov.au/media_library/publications/tandi_pdf/tandi400.pdf> (Accessed October 2014).

K.-K. R. Choo 2010b. High tech criminal threats to the national information infrastructure. *Information Security Technical Report*, vol. 15, no. 3, pp. 104–111.

H. Chung, J. Park, S. Lee, and C. Kang 2012. Digital forensic investigation of cloud storage services. *Digital Investigation*, vol. 9, no. 2, pp. 81–95.

M. Dekker, D. Liveri, and M. Lakka 2013. *Cloud security incident reporting framework for reporting about major cloud security incidents*. Heraklion, Greece: European Network and Information Security Agency.

European Network and Information Security Agency (ENISA) 2012. *Procure secure: a guide to monitoring of security service levels in cloud contracts*. Heraklion, Greece: European Network and Information Security Agency.

European Parliament 2014. Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs. <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//EN> [Last accessed 5 May 2015].

J. Farnden, B. Martini, and K.-K. R. Choo 2015. Privacy risks in mobile dating apps. In Proceedings of 21st Americas Conference on Information Systems (AMCIS 2015), 13–15 August 2015, Puerto Rico [In press].

B. Gellman, and T. Lindeman. Inner workings of a top-secret spy program. *NYTimes* (29 June 2014). <http://apps.washingtonpost.com/g/page/national/inner-workings-of-a-top-secret-spy-program/282/> [Last accessed 5 May 2015].

G. Greenwald 2014. XKeyscore: NSA tool collects 'nearly everything a user does on the internet'. *The Guardian* (31 July 2013). <http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data> [Last accessed 5 May 2015].

C. Grobauer, and T. Schreck 2010. Towards incident handling in the cloud. In Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop (CCSW 2010), 8 October 2010, Chicago, IL, USA, pp. 77–85.

C. Grov, A. S. Breslow, M. E. Newcomb, J. G. Rosenberger, and J. A. Bauermeister 2014. Gay and bisexual men's use of the internet: Research from the 1990s through 2013. *The Journal of Sex Research*, vol. 51, no. 4, pp. 390–409.

G. Grispos, T. Storer, and W. Glisson 2012. Calm before the storm: the challenges of cloud computing in digital forensics. *International Journal of Digital Crime and Forensics*, vol. 4, no. 2, pp. 28–48.

J. S. Hale 2013. Amazon cloud drive forensic analysis. *Digital Investigation*, vol. 10, no. 3, pp. 259–265.

C. Hooper, B. Martini, and K.-K. R. Choo 2013. Cloud computing and its implications for cybercrime investigations in Australia. *Computer Law & Security Review*, vol. 29, no. 2, pp.152–163.

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

M. Kozlovszky, L. Kovacs, M. Torocsik, G. Windisch, S. Acs, D. Prem, G. Eigner, P. Sas, T. Schubert, and V. Póserné 2013. Cloud security monitoring and vulnerability management. In Proceedings of the 17th IEEE International Conference on Intelligent Engineering Systems (INES 2013), 19–21 June 2013, San Jose, Costa Rica, pp. 265–269.

H. Li, X. Tian, W. Wei, and C. Sun 2012. A deep understanding of cloud computing security security issues in cloud computing. *Communications in Computer and Information Science*, vol. 345, pp 98–105.

R. McKemmish 1999. What is forensic computing? *Trends and Issues in Crime and Criminal Justice*, vol. 118, pp. 1–6.

B. Martini, and K.-K. R. Choo 2012. Cloud forensic technical challenges and solutions: A snapshot. *IEEE Cloud Computing*, vol. 1, no. 4, pp. 20–25.

B. Martini, and K.-K. R. Choo 2014a. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, vol. 9, no. 2, pp. 71–80.

B. Martini, and K.-K. R. Choo 2014b. Distributed filesystem forensics: XtreemFS as a case study. *Digital Investigation*, pp.1–19.

B. Martini, and K.-K. R. Choo 2014c. Remote programmatic vCloud Forensics: A six-step collection process and a proof of concept. In Proceedings of the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2014), 24–26 September 2014, Beijing, China, pp. 935–942.

B. Martini, Q. Do, and K.-K. R. Choo 2015a. Conceptual evidence collection and analysis methodology for Android devices. In R. Ko and K.-K. R. Choo, editors, Cloud Security Ecosystem, Syngress, an Imprint of Elsevier [In press].

B. Martini, Q. Do, and K.-K. R. Choo 2015b. Mobile cloud forensics: An analysis of seven popular Android apps. In R. Ko and K.-K. R. Choo, editors, Cloud Security Ecosystem, Syngress, an Imprint of Elsevier [In press].

A. Monfared, and M. G. Jaatun 2012. Handling compromised components in an IaaS cloud installation.

Journal of Cloud Computing: Advances, Systems and Applications, vol. 1, no. 1, pp. 1–21.

S. Pallaras 2011. New technology: opportunities and challenges for prosecutors. *Crime, Law and Social Change*, vol. 56, no. 1, pp. 71–89.

G. Phillips, M. Magnus, I. Kuo, A. Rawls, J. Peterson, Y. Jia, J. Opoku, and A. E. Greenberg 2014. Use of geosocial networking (GSN) mobile phone applications to find men for sex by men who have sex with men (MSM) in Washington, DC. *AIDS and Behavior*, vol. 18, no. 9, pp. 1630–1637.

D. Quick, B. Martini and K.-K. R. Choo 2014. *Cloud storage forensics*. Syngress, an Imprint of Elsevier.

D. Quick, and K.-K. R. Choo 2013a. Digital droplets: Microsoft SkyDrive forensic data remnants. *Future Generation Computer Systems*, vol. 29, no. 6, pp. 1378–1394.

D. Quick, and K.-K. R. Choo 2013b. Dropbox analysis: Data remnants on user machines. *Digital Investigation*, vol. 10, no. 1, pp. 3–18.

D. Quick, and K.-K. R. Choo 2013c. Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata? *Digital Investigation*, vol. 10, no. 3, pp. 266–277.

Quick, D., & Choo, K.-K. R. (2014). Google Drive: Forensic analysis of data remnants. *Journal of Network and Computer Applications*, vol. 40, pp. 179–193.

C. Tassone, B. Martini, K.-K. R. Choo, and J. Slay 2013. Mobile device forensics: A snapshot. *Trends & Issues in Crime and Criminal Justice*, vol. 460, pp. 1–7.

N. Thethi, and A. Keane 2014. Digital forensics investigations in the cloud. In Proceedings of the 2014 IEEE International Advance Computing Conference (IACC 2014), 21–22 February 2014, Gurgaon, India, pp. 1475–1480.

K. Zatyko, and J. Bay 2011. The digital forensics cyber exchange principle. *Forensic Magazine*. <http://www.forensicmag.com/articles/2011/12/digital-forensics-cyber-exchange-principle> [last accessed 4 May 2015].

S. Zimmerman, and D. Glavach 2011. Cyber forensics in the cloud. *IAnewsletter*, vol. 14, no. 1, pp. 4–7.