<table>
<thead>
<tr>
<th><strong>Title</strong></th>
<th>Digital Forensic Investigations in the Cloud: A Proposed Approach for Irish Law Enforcement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Authors(s)</strong></td>
<td>Plunkett, James; Le-Khac, Nhien-An; Kechadi, Tahar</td>
</tr>
<tr>
<td><strong>Publication date</strong></td>
<td>2015-01-28</td>
</tr>
<tr>
<td><strong>Conference details</strong></td>
<td>11th Annual IFIP WG 11.9 International Conference on Digital Forensics (IFIP119 2015), Orlando, Florida, United States, 26 - 28 January 2015</td>
</tr>
<tr>
<td><strong>Link to online version</strong></td>
<td><a href="http://www.ifip119.org/Conferences/">http://www.ifip119.org/Conferences/</a></td>
</tr>
<tr>
<td><strong>Item record/more information</strong></td>
<td><a href="http://hdl.handle.net/10197/7389">http://hdl.handle.net/10197/7389</a></td>
</tr>
</tbody>
</table>
Digital Forensic Investigations in the Cloud
A Proposed Approach for Irish Law Enforcement

James Plunkett, Nhien-An Le-Khac, and M-Tahar Kechadi
University College Dublin, Ireland
Email: jamesplunkett@gmail.com, {an.lekhac,tahar.kechadi}@ucd.ie
Abstract

Cloud computing offers utility oriented Information and Communications Technology (ICT) services to users all over the world. The evolution of Cloud computing is driving the design of data centres by architecting them as networks of virtual services; this enables users to access and run applications from anywhere in the world. Cloud computing offers significant advantages to organisations through the provision of fast and flexible ICT hardware and software infrastructures, thus enabling organisations to focus on creating innovative business values for the services they provide.

As the prevalence and usage of networked Cloud computer systems increases, logically the likelihood of these systems being used for criminal behaviour also increases. Thus, this new computing evolution has a direct effect on, and creates challenges for, digital forensic practitioners working in Irish law enforcement.

The field of digital forensics has grown rapidly over the last decade due to the rise of the internet and associated crimes; however while the theory is well established, the practical application of the discipline is still new and developing. Law enforcement agencies can no longer rely on traditional digital forensic methods of data acquisition through device seizure to gather relevant evidence pertaining to an investigation. Using traditional digital forensic methods will lead to the loss of valuable evidential material if employed during investigations which involve Cloud based infrastructures.

Cloud computing and its impact on digital forensics will continue to grow. This paper analyses traditional digital forensics methods and explains why these are inadequate for Cloud forensic investigations with particular focus on Irish law enforcement agencies. In this paper, we do a survey on approaches to digital forensics of Irish Law Enforcement Agencies for cloud based investigations and we propose a digital forensic framework approach to acquiring data from Cloud environments. This proposed approach aims to overcome the limitations of traditional digital forensics and the challenges Cloud computing presents for digital forensic practitioners working in Irish law enforcement.

**Keywords:** Cloud forensics, Irish Law Enforcement Agencies, Composite Approach, Digital Forensics, Cloud computing
1. Introduction

Cloud computing [1] is a new approach to delivering Information Communications Technology (“ICT”) to organisations. Cloud computing is built on the premise that organisations do not need to invest in buying hardware, software and network infrastructures to support business critical applications. Utilising a Cloud based infrastructure, organisations can increase ICT capacity or add additional ICT capabilities without investing in new infrastructure, training new personnel, or licensing new software. Cloud computing encompasses any subscription-based or pay-per-use service that, in real time over the Internet, extends an organisations existing ICT capabilities. The advent of Cloud computing is forcing a change from traditional software and hardware models to ICT being delivered over the internet or through private networks located in shared data centres (Public Cloud) or within private data centres (Private Cloud). As global markets change, organisations must also change to meet consumer demands. Organisations require flexible structures and to complement this flexibility they require the ability to quickly provide new applications, hardware and network infrastructures to support the changing market environments enabling the organisation to sustain a competitive advantage. Information weekly has conducted a survey annually illustrating that organisations are increasingly implementing Cloud based solutions and these adoption rates have risen from 16% in 2008 to 33% in 2012 [2].

On the other hand, the increased adoption rates of Cloud computing solutions are also an opportunity for criminals to store information within Cloud based environments. Criminals are aggressively expanding the use of digital technology for illegal activities. Crimes committed in cyberspace such as Data theft, Internet fraud, business espionage, pornography, on-line child exploitation, cyber terrorism are on the rise. In 2012 Trend Micro reported a 27% quarter on quarter increase in internet related criminal activity [3]. In addition, a study conducted by Deloitte shows that one in three financial companies in Ireland have been
affected by some form of computer related crime in 2012 and that computer related crime is on the rise as criminals seek to exploit new opportunities [4].

Law enforcement agencies are increasingly faced with Cloud computing solutions being used by companies and individuals who engage in illegally activity. Over the past 20 years digital forensic techniques have become a vital tool employed by Irish law enforcement agencies (“ILEAs”) in combating criminal activity. The evolution of computer forensics has advanced at a rapid pace due to the rise in computer related crime. Computer forensics, which is a branch of digital forensics, is the science of acquiring, retrieving, preserving and presenting data that has been processed electronically and stored on computer media [5].

The rise of Cloud computing not only exacerbates the problem of scale for digital forensic practitioners, but also creates a brand new forum for cybercrime with associated challenges [6]. ILEAs can no longer rely on traditional digital forensics techniques employed during investigations which involve Cloud computing platforms. The discovery and acquisition of digital evidence from remote, elastic, provider-controlled Cloud platforms differs considerably from the discovery and acquisition of digital evidence from local suspect devices such as Laptops, PCs and Servers. Acquiring data from Cloud based environments requires different tools, techniques and approaches. It is necessary to develop new processes and techniques to retrieve evidence from Cloud based environments [7]. As organisations exploit the benefits of the Cloud, ILEAs need to adapt their traditional approaches to digital forensics.

In this paper, we evaluate the above statement and will present a Composite Approach to digital forensics within Cloud based environments. This approach will draw on various aspects of digital forensics such analysis and acquisition methods. To support this approach a digital forensic framework model will be developed to support this Composite Approach during live investigations. This new approach will focus on the identification and the
acquisition of data within Cloud based environments during the execution of search warrants by ILEAs. The object of this approach is to meet the many challenges of conducting investigations in which evidential material is located within the Cloud. The rest of this paper is organised as follows: Section 2 deals with background research in the area. Section 3 presents our survey on approaches to digital forensics of ILEAs for cloud based investigation. We propose a digital forensic framework approach to acquiring data from Cloud environments for Irish Law Enforcement in Section 4. Finally, we conclude in Section 5.

2. Related work

With increasing adoption rates and access to a wide variety of Cloud solutions, Cloud computing is impacting greatly in the way digital forensic investigations are conducted in the future [6]. [6] recognises that Cloud computing operates in a computing environment which is different from traditional on-site client application environments. The additional complexity for digital forensic investigations within Cloud based environments arise from the various types of Cloud models. The increased adoption of Cloud computing technologies will impact on how ILEAs conduct investigations involving Cloud based environments. The majority of research concerning Cloud computing is focused on defining the challenges of performing digital forensic investigations within physical Cloud based environments [6][8][9]. These challenges can be listed as the evidence identification, legal, data acquisition and the suitability of traditional digital forensic tools to acquire data within Cloud based environments. These challenges not only exacerbate the problems of digital forensics within Cloud based environments but create a brand new front for digital forensic investigations.

[10] also highlights the important issue of data identification with Cloud based environments. Besides, according to [11] there is no foolproof, universal method of extracting evidence in an admissible fashion from within the Cloud, and in some cases, very little evidence is available to extract. As such, Cloud computing represents just one of the
fast-paced technological developments that is presenting an ongoing challenge to legislators, law enforcement officials, and computer forensic analysts.

The ACPO (Association of Chief Police Officers) search and seizure guidelines are particularly relevant when considering Cloud computing as these are the most difficult to satisfy due to the remoteness of Cloud data centres. Reilly states that certain aspects of computer forensic processes can be applied to Cloud computing, but the main stumbling block is the fact that it may be impractical or legally impossible for the digital forensic investigators to seize physical devices likely to contain digital evidence [9]. Dykstra and Sherman in 2012 state that discovery and acquisition of evidence in remote, elastic, provider controlled Cloud computing platforms differs from that in traditional digital forensics and examiners lack the proper tools to conduct these tasks [12]. Moreover, several researchers have pointed out that evidence acquisition is a forefront issue with Cloud forensics [6][12][13]. Indeed, [8] states that technical challenges of forensics investigations in Cloud computing environments focuses in on the various types of Cloud computing environments and how to conduct investigations within these environments. [14] suggests that “Cloud computing in particular may make it impossible to perform basic forensic steps of data preservation and isolation on systems of forensic interest”. However there are other considerations for Irish law enforcement officers to contemplate when conducting Cloud based investigations, such as time dependent issues, extracting large volumes of data, lack of access to data due to the absence of passwords or a lack of expertise, procedures and appropriate tools during the execution of search warrants. These issues have not been considered fully by previous research. Many users will have access to a particular Cloud. How does law enforcement seize only that portion of the media where the evidence may exist? How will they know if they have gotten everything that they will need during the analysis, interpretation, documentation and presentation phases [15]. According to the results
of a survey conducted by [6], the need for digital investigations in Cloud environments will increase as the adoption rates of Cloud services continues to grow. These increased adoption rates will compel law enforcement agencies to adapt their digital forensic procedures when conducting investigations within Cloud based environments. The extent to which law enforcement agencies have changed from traditional digital forensics processes to meet the challenges posed by Cloud forensics could not be established through this research. Besides, the challenges in relation to Cloud based forensics are not only technical, there are many legal challenges associated with data recording, privacy and access issues [16]. In addition, the manner in which the access is provided to the digital forensic practitioner and the process to acquire evidential material also pose legal concerns. These concerns are extremely important, especially in relation to Cloud environments being ubiquitous, multinational and widely distributed. However, these issues do not fully address the intricacies which Irish law enforcement investigators are faced with when executing search warrants within Cloud based environments.

While legal complications are introduced by [6][8][9], including Cloud-based evidence admissibility, no solutions are presented. [17] identified some research challenges, including “discovery of computation structure,” “attribution of data,” “stability of evidence,” and “presentation and visualisation of evidence”. Multi-jurisdictional law is escalating the challenge of Cloud forensics. The very nature of Cloud computing is that it is distributed worldwide. However data protection laws and legal frameworks are not the same throughout the world. Cross-border legislation issues have been identified by a number of researches such as [12]. These authors illustrate the challenges of evidence collection located within multi-jurisdictional computing environment but no specifics can be applied in the Irish legal context. As a conclusion, a number of authors have identified some critical points regarding Cloud forensics and the issues that law enforcement agencies will face. The lack of a digital
forensic framework model applicable to Cloud based forensics is required. In addition many researchers have stated that the current set of digital forensic tools cannot be fully applied to acquisitions in Cloud based environments.

3. Irish Law Enforcement Agencies approach to digital forensics for cloud based investigations

The foundation of our Composite Approach was developed by ascertaining and analysing the current approaches applied to Cloud based digital forensic investigations conducted by ILEAs and the associated challenges which they face. This information was acquired through a combination of interviews with, and questionnaires to, ILEAs.

3.1. Survey Questions

Eventually, our survey questions are designed based on: (i) Drawing from the research on Cloud forensics presented in Section 2; (ii) Analysing the results of a questionnaire posed by [6]; (iii) Circulating a draft questionnaire to colleagues in European Law enforcement agencies for input to ensure the main technical points of the research where addressed. These questionnaires were used either as the basis for an interview with, or responded to in writing by, a representative from the ILEAs\(^1\) surveyed. This research established:

- The depth of knowledge of Cloud computing among ILEAs.
- Digital forensic approaches used by ILEAs in investigations that involve Cloud based computing.
- How Cloud computing is affecting the investigations of ILEAs; specifically, do ILEAs need to adapt their traditional digital forensics methods to acquire data from Cloud based environments.

\(^1\) Name of ILEAs surveyed cannot be disclosed because of confidential agreement of the survey
ILEAs views on moving away from the traditional approach; specifically (i) What is the current digital forensic expertise within the agency and what approaches are used when faced with investigations in Cloud based environments? (ii) What Digital Forensic tools used by ILEAs? (iii) How Cloud computing is affecting their investigations? (iv) What are Irish law enforcement views on moving away from the traditional approach to digital forensics?

Due to the varying nature of the work of these agencies and the experience of their digital forensic practitioners, questions asked varied to a certain extent; for example questions posed to some ILEAs focused on their understanding of Cloud forensics and their experience to date, while questions posed to other ILEAs where more in-depth and questioned how the advent of Cloud computing affected their work during the execution of search warrants. A number of questionnaires were issued to the Crime Unit of an ILEA in order to obtain the views of a number of staff. The questionnaire allowed the answers to be written in a space below each question. Interviews took 40-60 minutes; interviews were based on questionnaire but also allowed for deeper exploration and discussion of answers.

3.2. Survey Analysis

This sub-section presents the results and analysis of our survey.

3.2.1 Depth of knowledge among Irish law enforcement agencies of Cloud computing

Most of the ILEAs have a thorough knowledge of Cloud computing and its principles and structures. In addition each agency has a strong understanding of Cloud computing security, its growth in Ireland and how it would affect their investigations. Some agencies have a high level of practical experience in dealing with investigations within the Cloud, while one agency has not conducted investigations within Cloud based environments but feel the advent of Cloud computing it is a pressing issue for them when conducting investigations.
3.2.2 What is the current digital forensic expertise within the agency and what approaches are used when faced with investigations in Cloud based environments?

Two ILEAs have extensive expertise in digital forensics. They have fully trained staffs which employ digital forensic best practice procedures to their investigations. Investigations by these agencies are predominantly supported by Encase Forensic and Access data digital forensic tools. Each agency utilises an internal digital forensic framework procedure tailored on the DFRWS framework model. They work within an entirely closed IP network and as such digital forensic investigations are primarily focused in internal investigations and network security. Three other ILEAs have dedicated personal providing digital forensic support. All agencies have encountered Cloud environments during investigations. They have also seen an increase in these investigations involving Cloud based environments.

3.2.3 What are the main Digital Forensic tools used by Irish Law Enforcement Agencies?

All agencies have licensed copies of Guidance Software’s Encase Forensic software and Access Data’s Forensic Tool kit and these tools are primary tools used during investigations. Some agencies use different varieties of these applications for instance, one ILEA utilises Guidance Software Encase Portable and Access Data’s Forensic imager to conduct target specific acquisitions they also utilise hardware and software write blockers when required. The Crime Unit of other ILEA utilises Guidance Software’s Encase Forensic Enterprise edition, and also Access Data’s Forensic imager and in some instances utilises Linux based forensics tools running on live CDs.

3.2.4 How Cloud computing is affecting their investigations?

Some ILEAs have encountered Cloud based environments and their experiences differ. For instance the Computer Crime unit of an ILEA has predominately had to deal with suspects who utilised the Cloud storage service Drop box. This Unit was able to acquire the
information under the Theft and Fraud offences Act 2001 using Access Data’s Forensic Imager. Other ILEA has encountered cases where suspects stored data within Google Apps. Both agencies stated that Cloud computing was changing the way the organisations conducted digital forensic investigations as traditional approaches and guidelines such as the ACPO guidelines did not fully meet their requirements. Each agency expressed that access to passwords to gain access to Cloud environments was vital to acquire data with these environments. The lack of passwords particularly during the execution of search warrants has hindered investigations.

3.2.5 Irish law enforcement agencies views on moving away from the traditional approach

Most ILEAs all agreed that traditional approaches to digital forensics - whereby suspect devices are powered off and seized - were not able to meet their needs when conducting investigations within the Cloud. All agencies felt that they needed to move away from purely traditional approaches to digital forensics due to the technical architecture of Cloud based solutions.

3.2.6 What scenarios as the agency been faced with when acquiring data from Cloud based environments?

The most prevalent Cloud based services found by ILEAs during the execution of search warrants are Drop Box, Google Apps for Business and Salesforce. The other agencies mentioned above have not had direct experience with Cloud-based services. Two ILEAs have encountered numerous Cloud based instances during the execution of search warrants.

3.2.7 Analysis

ILEAs have acknowledged the challenge they are faced with when encountering investigations within Cloud based environments. In addition the growth of social media is adding to the challenges faced by ILEAs when conducting Cloud based investigations.
Traditional approaches to digital forensics employed by ILEAs involve a computer forensic practitioner pulling the plug/power on a suspect system and seizing the device. This approach enables the computer forensic practitioner to create an acquisition image of the suspect device which can be reviewed for evidential purposes post seizure. This approach will hinder computer forensic practitioner in identifying and acquiring data within the Cloud during the execution of a search warrant. Computer forensic practitioners may only establish that a Cloud based solution was used by a suspect during the review of the seized evidence. This can lead to the destruction of evidence within the Cloud by a suspect. Using traditional approaches to digital forensics may ultimately lead to the loss of evidential material if employed during the execution of search warrants. Due to the limitations of traditional forensics, an alternative digital forensic process is required supported by a Digital framework to identify and extract data from within Cloud based environments. Based on this research and analysis, we identify, qualify and propose a Composite Approach to digital forensics in Cloud based investigations described in the next section. The interviewees contributed greatly to the research; their views are incorporated into the proposed Composite Approach.

4. Proposed composite approach

In this section, we describe a solution which can be used by ILEAs to identify and extract evidential material located within Cloud based environments.

4.1 Objectives

The primary objective of the Composite Approach is the identification and extraction of digital forensic evidence that exists within Cloud based environments. When applying the Composite Approach it is imperative that digital forensics practitioners be familiar with the various Cloud-based models. They should also have tested a number of approaches to acquire data from various Cloud based models that exist prior to the execution of a search warrant. This Composite Approach derives from two principles:
• **The Irish law enforcement digital forensic framework model**: This framework enables a digital forensic practitioner to identify and extract specific data relating to the investigation in the most efficient manner.

• **The Irish law enforcement digital forensic tool box**: The Irish law enforcement digital forensics tool box consists of a number of digital forensics tools which support the extraction of evidential material either within a Cloud based environment or within the local environment. These tools have been fully accepted by the Irish courts and are mentioned further in this section.

Research conducted for this paper has indicated that ILEAs need to be specific about the data volumes they identify and acquire. This applies to an organisation or individual which may be under investigation. It is not practical for ILEAs to seize entire virtual machines running within Cloud based environments, nor is it practical to seize entire physical servers within data centres supporting Cloud based environments. The Composite Approach has been developed by taking cognisance of the factors mentioned above while also ensuring that the following considerations are addressed:

• **Time on Site**: When Irish law enforcement officers conduct a search of a suspect location under a search warrant the time spent on site is a critical factor. ILEAs need to identify, document and acquire evidential material in a reasonable timeframe which does not impact greatly on the suspect organisation or individual.

• **Large data extraction**: During the execution of search warrant, ILEAs can be faced with very large volumes of electronic data. Extracting all electronic data during the execution of a search warrant can cause a number of issues.

### 4.2 Model
This is a digital forensic framework model for ILEAs to assist them during the execution of search warrants. It is an approach designed to be a step-by-step guide and consists of three main components coupled with the use of dedicated software and hardware outlined as (i) Pre-search preparation; (ii) Search; (iii) Post-search investigation. Each of the above components has a number of tasks that must be completed prior to the next component being utilised. A diagram illustrating these steps is provided in Figure 1 below.

4.2.1 Pre-search tasks

The Pre-search stage has five tasks which must be completed prior to the execution of search: (1) Identifying and gathering intelligence on suspect targets; (2) Digital forensic tool testing; (3) Preparation of storage media preparation; (4) Development of an on-site infrastructural questionnaire; (5) Briefing search teams prior to the execution of a search warrant.

4.2.2 Search Stage

The Search Stage is focused on the execution of the search warrant and the identification and acquisition of electronic evidence. The stage comprises of four phases. (1) Secure the scene; (2) Identify IT personnel and complete the on-site infrastructural questionnaire; (3) Prioritisation of targets and devices; (4) RAM & Internet acquisition – Review – Identified Cloud and local acquisition.

Phase One: Secure the scene

Objective: Secure scene, identification of target individuals and obtaining access passwords.

Each search team member will have been briefed and trained on how to secure the scene/search site prior to the execution of the search warrant. In addition, each team member will be assigned a high priority target identified in Pre-Search Task One. The main objective of this stage is to ensure that no suspect personnel delete any electronic data.
It is also vital at this stage that each team member acquire the username and passwords in order to maintain access the computing devices associated with individual targets. During the execution of the search warrant, Irish law enforcement officers have the right to request all passwords to access any systems which they believe may contain evidential material. Failure to do so can be viewed as an obstruction. The Criminal Justice Bill, 2011 and the Competition Act, 2002 have provisions and associated sanctions for non-cooperation.

Phase Two: Identify IT personnel and complete the On-Site

Objective. To gain an understanding of the ICT infrastructure in order to facilitate the acquisition of specific target data and the prioritisation of target individuals who utilise Cloud based systems.

When using the Composite Approach it is the responsibility of the lead digital forensics investigator is to identify the individual responsible for the maintenance of the ICT environment during the execution of the search warrant. If the ICT is managed externally the next step is to request the external ICT support organisation to assist the lead digital forensics investigator in establishing the ICT environment of the suspect organisation. If no assistance can be given to the lead digital forensic practitioner the warrant holder will be informed as the prioritisation of targets and data may change due to the lack of access or knowledge of the ICT infrastructure in question. Once completed, the ICT infrastructure questionnaire will provide the digital forensic practitioner a detailed view as to how the ICT infrastructure of the target location is constructed.

Phase Three: Prioritisation of Targets and Devices

The infrastructure questionnaire is focused on identifying if any Cloud based systems are being utilised by the organisation or individual. Once the questionnaire is completed the
digital forensics investigator will communicate with the warrant holder to establish if any further targets have been identified. The warrant holder will also communicate any additional passwords identified by the other team members during phase one. If no additional targets have been identified the lead digital forensic practitioner will begin the process of prioritising the target individuals and will acquire the specific electronic evidence. The acquisition of electronic data will be prioritised based on those targets that access Cloud based systems.

**Phase Four: RAM & Internet acquisition – Identified Cloud and local acquisition**

This stage has a number of predefined steps which must be carried out in order. These steps ensure that the most effective approach is applied to acquire electronic evidence either within the Cloud or stored on a local device.

4.2.3 **Post-search investigation**

The post-search investigation stage focuses on the acquisition of the evidence seized and analysis of this evidence. This stage is comprised of three phases.

**Phase 1: Acquisition**

All evidence seized from the suspect organisation or individual will be acquired from the sterile media as discussed in the pre-search stage. Best practice techniques state that a digital forensic practitioner should never work on original evidence therefore all evidence seized from the organisation will be copied to a digital forensic workstation [18]. A digital forensic workstation will be used to acquire and conduct analysis of all data acquired during an investigation. The forensic workstation will also utilise sterile discs and will not be connected to any networked environments. This is to ensure the integrity of the evidence being
analysed. Once the data is acquired it is verified against the original evidence. The original evidence is then given to the case exhibits officer to ensure the continuity of this evidence.

Phase 2: Analysis

Once all of the evidential material is acquired to the forensic workstation, the analysis of the evidential material can begin. An important aspect of this analysis is to ensure that all of the data seized from the target organisation or individual is made available to the case team. The pertinent evidence is identified by the case team and communicated to the digital forensic practitioner. The digital forensic practitioner will identify the evidence from the original acquisition images and will attempt to establish through document metadata, the report and intelligence gathered through the onsite infrastructural questionnaire who was the creator and editor of the identified evidential files.

Phase 3: Reporting

A digital forensic report will be created by the digital forensic practitioner. The on-site infrastructural questionnaire is a key component the generation of the digital forensic report as it forms the initial foundations of how and why evidence was identified and acquired. The onsite infrastructural questionnaire will also detail who had access to Cloud based systems, how they were used and what files were acquired from within the Cloud based environment. This information, coupled with the registry analysis and the report will try and link suspect individuals to vital pieces of evidence. The report will consist of an overview of the case and a summary, where the evidence was found, the forensic analysis which was conducted and the findings based on the evidential material.

5. Conclusion and Future work
In this paper, the challenges of Cloud forensics have been analysed. The utilisation of digital forensic tools that have the ability to systematically search digital devices whether in the Cloud or locally stored is critical to conducting effective digital investigations. Current research efforts suggest that Cloud forensics is still in its infancy. There are numerous challenges which have been identified and incorporated into the proposed Composite Approach put forward in this paper. Research for this paper has analysed the current methods of digital forensic acquisitions and supporting frameworks and identified shortfalls when being applied to Cloud based environments. A new approach to digital forensic investigations has been identified and tested in a live investigation. The proposed Composite Approach successfully identified and extracted data from within a Cloud based environment. The proposed Composite Approach attempts to improve upon existing digital frameworks through the amalgamation of standard techniques while also introducing supporting documentation and tools to assist Irish law enforcement officers identifying and extracting vital evidential material during the execution of search warrants. The proposed Composite Approach advocates a step by step approach supported by digital forensic tools which reduce the risks associated with the acquisition of digital evidence. A fundamental principle of digital forensics is to ensure that the acquired electronic evidence remains original. The Composite Approach abides by this principle while also providing support for the acquisition of data residing within Cloud based environments. Investigations within Cloud based environments bring new challenges from a legal stand point and have opened a new research area for the legal industry. Irish and European legislators understand the challenges faced by law enforcement officers when conducting investigations which involve digital devices. Enacted Irish and European legislation to date is assisting law enforcement agencies to combat criminal behaviour within the digital sphere. However, strong legislation and European cooperation is required especially involving investigations which cross multiple jurisdictions.
Mutual Assistance Conventions and Production Orders are helping to alleviate some of these difficulties but further international cooperation is required to ensure swift access to electronic data during criminal investigations. Besides, the growth of smart mobile devices and their integration with Cloud based systems is a new area and requires further research. Computing devices such as laptops and PC’s will soon be overtaken by smart mobile devices. This area opens a new set of challenges for Cloud forensics and will require fundamentally different tools and supporting frameworks.

References


