Analysis of Dependencies & Legal Barriers on Digital Forensic Investigations in Sri Lanka

P Perera[1#], P Mahanamahewa[2]
[1]*Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), Sri Lanka.*
[2]*Faculty of Law, University of Colombo, Sri Lanka.*
[#]For correspondence; priyankara@cert.gov.lk

Abstract— The objective of this research is to investigate dependencies and legal barriers arises when conducting digital forensic investigation in Sri Lankan context. Since the Sri Lankan legislations on computer crimes are now outdated and were written before the era of computer forensics, computer forensics experts face major problems during computer forensic investigations. Due to this issues, lot of court cases were delayed for over years and still open for interpretation. To firmly analyse this prevailing issue, Evidence (Special Provisions), Electronic Transactions Act, Payment Device Fraud Act, Computer Crime Act and Mutual Assistance in Criminal Matters Act were analysed against the basic digital forensic process (acquisition, preservation, analysis and presentation). Empirical evidences form digital forensic engineers were also gathered using questionnaires. Seven issues were recognized during this research and they are, Cross Jurisdictional Conflicts, Cloud Computing Challenges, Need of National Certification Authority, Need of Legally Accepted Forensic Software Tools, Stored Communication, Anonymization and Technical Competencies of digital forensic experts. These issues were discussed in detailed with the appropriate recommendations and suggestions to improvements. New domains of forensics analysis which need to be included in the current legislative system were also discussed during this research. By referring this research, computer forensics experts would be able to identify techniques to produce legally admissible evidences to the courts.

Keywords— **Digital Forensic Dependencies, Legal Barriers on Digital Forensic, Sri Lankan Legislations on Digital Forensic Investigations**

I. INTRODUCTION

Information and communication technologies (ICTs) are changing societies around the world improving productivity in traditional industries, revolutionizing labor processes and remodeling the speed and flow of capital (UN, 2005). This change also reflected in Sri Lanka during the past two decades and at the same time adoption of the ICT has shown a rapid growth. Failure to safeguard electronic data in motion, in processing and in stored has arisen considerable amount of computer related crimes in Sri Lanka. This includes, but not limited to fraud, hacktivism, identity theft and unauthorized access. However, when conducting a digital forensics investigation on such computer based criminal activities, computer forensics experts face many forensics dependencies and legal barriers due to ambiguities exists in current Sri Lankan legislative system. In order to preserve, collect, recover, analyze and present digital evidence to courts, computer forensics experts need to follow proper legal procedures enforced by the legislative system, however current Sri Lankan legislative system does not provide necessary legislative powers and technical frameworks required by computer forensics experts to continue with their investigations. This research is based on finding out such legal barriers and forensic dependencies and to discuss the areas which need to be revised in the current legislative system.

A. Research Problem

Digital forensic experts face numerous dependencies and legal barriers when producing and presenting legally acceptable evidences to the courts due to the poor support and provisions provided by the current Sri Lankan legislative system. As a result, a number of court cases were delayed over several years, remained as un justified and still open for interpretation.

B. Research Objectives

The main research objective is to identify dependencies and legal barriers on digital forensic investigations in Sri Lanka.

This research contains following sub objectives as well.

1) To identify the areas which are not covered by the Sri Lankan legislations on digital forensic analysis.
2) To discuss the ways which Sri Lanka can obtain international support and assistance to collect evidences located in foreign countries.
3) To examine areas which need to be introduced to address current requirements in digital forensics analysis.
4) To provide suggestions and recommendations on the main research objective.

C. Literature Review

As defined by McKemmish (McKemmish, 1999) Digital Forensics is the process of identifying, preserving, analyzing and presenting digital evidence in a manner that

is legally acceptable. Definition given by the McKemmish is further strengthened by Farmer & Venema (Farmer & Venema, 2001) by explaining digital forensic as Gathering and analyzing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system.

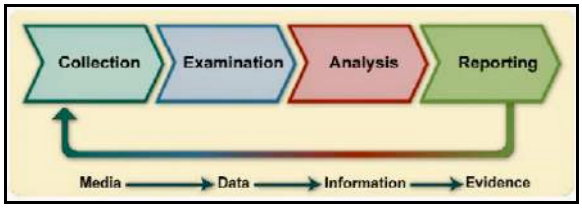

Figure 1: Digital Forensic Investigation Process

According to the description given by the United States Computer Emergency Readiness Team (US-CERT, 2008) Digital Forensic Investigation is the 'The discipline that combines elements of law and computer science to collect and analyze data from computer systems, networks, wireless communications, and storage devices in a way that is admissible as evidence in a court of law'. As explained by the McKemmish, Identification, Preservation, Analysis and Presentation are the four major steps involved in Digital Forensic Investigation as illustrated in figure 1. In Sri Lankan context, mainly necessary powers and grants to conduct digital forensic investigations is provided from the Evidence (Special Provisions) Act (No. 14 of 1995) and from the Computer Crime Act (No. 24 of 2007) of Sri Lanka. The Evidence Act provides necessary procedures to obtain legally admissible evidences during a digital forensic investigation.

II. METHODOLOGY

Collecting secondary data was the first step of this research. The Researcher has gone through all applicable legislations on this research topic to build up a proper understanding of applicable laws and regulations on Sri Lankan context. Several international conventions on cybercrime along with their publications and policy documents were also referred. Meanwhile similar research and publications done in the similar domain were used to find out the current research gap between Sri Lankan legislative system and legislations used by other nations. To collect the primary data mainly questionnaires were used. This is because, The Researcher has understood that, to gain further understanding of the research problem, it is mandatory to identify the dependencies and barriers faced by the digital forensics experts and legal personal (Ex. Lawyers, Judiciaries). To collect personal opinions and personal experience on the research question, The Researcher has interviewed several information security experts to collect qualitative data. Digital forensics experts and judicial officials were selected as the target population for collecting primary data.

A. Data Analysis Methodology

First of all, The Researcher has gone through the collected secondary data to identify key areas that causes forensic dependencies and legal barriers. Then Researcher has interviewed the Principal Information Security Engineer at Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT), Eng. Roshan Chandraguptha (Chandraguptha, 2017) to acquire additional impression on prevailing issues on the research problem. Feedbacks from the questionnaire were analyzed to confirm that issues identified by the Researcher is also exists with the digital forensic experts. Furthermore, from the explanation provided by digital forensic experts during the questionnaire, The Researcher has found additional areas on the research problem.

III. RESULTS

By analyzing responses for the questionnaire from 10 digital forensic experts, following dependencies and legal barriers were recognized.

1. More than 90% digital forensic experts answered that they are facing issues when obtaining an information relevant to forensics investigation from foreign nations.
2. More than 75% of experts highlighted that they are experiencing Cross border legal conflicts (between other nations).
3. More than 90% of digital forensic experts highlighted that there is a need of National Certification Authority (NCA) for Sri Lankan context.
4. 50% of security professionals uses an open source digital forensic investigation software and reaming security professionals use both commercial and open source software.
5. More than 50% digital forensic experts emphasized that 'Preservation' of the data is the most difficult phase in computer forensic investigation.

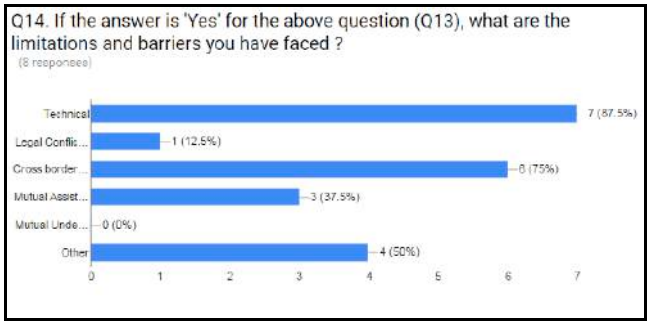

Figure 2: Survey Response for obtaining an information relevant to forensics investigation from foreign nations

Based on the interview had with Eng. Roshan Chandraguptha (Chandraguptha, 2017), following issues were also recognized.

1. Timely access to the service records, logs and stored communication owned by the service providers.
2. Anonymized communication.
3. Lack of technical competencies of digital forensic experts.

IV. DISCUSSION

This section elaborates identified dependencies & Legal Barriers on Digital Forensic Investigations with relevant recommendations.

A. Mutual Assistance with Foreign Nations

The Researcher understood that without having a proper diplomatic and cooperative arrangements with peer nations, when conducting a forensic investigation, it impossible to obtain all necessary and required information. Different legislative systems available in peer nations would act as a legal barrier which will hinder the continuation of a forensics investigation. The section 35 (1) of the Computer Crime Act of Sri Lanka, provide guidance to adhere with the 'Mutual Assistance in Criminal Matters Act of Sri Lanka', when seeking an assistance to obtain information relevant to a particular forensics investigation. The method of getting assistance relating to the taking of evidence, statements, the serving of process and the conduct of searches are mentioned under the section 35 (2) and (3) of the Computer Crime Act. According to the section 4 of the Mutual Assistance in Criminal Matters Act of Sri Lanka, the secretary to the ministry of the minister in charge of the subject of justice shall be the Central Authority. According to the section 8 of the same act, The Central Authority has given with the permission to seek the assistance required on identifying and locating evidences and suspects located in foreign nations. However, when dealing with other nations the powers granted to the Central Authority is not sufficient to conduct forensic investigations due to the cross-jurisdictional conflicts. Cybercrime cases that demand cooperative mechanisms that are not provided for within existing legal instruments create significant difficulties for police and prosecuting agencies (ITU, 2012).

In order to collect electronic evidences from the sources which are located outside of Sri Lankan geography, it is an essential to have a strong collaboration among international law enforcement entities. To establish such strong collaboration among such entities like Interpol, Europol, Council of Europe (CoE), European Union (EU), United Nations (UN) and Budapest Convention, the Sri Lankan legislative system need to be timely updated. This international level collaboration need to be establish at the diplomatic level with mutual understanding with the other nations. This collaboration should not be limited to gather evidences, but this should also need to be support to find, trace down and prosecute suspects who resides in a foreign nation. The Researcher has observed that recently, Government of Sri Lanka has become a fully-fledged member of the Budapest Convention on Cybercrime. This action will help to overcome cross-jurisdictional conflicts for upcoming legal cases. The Budapest Convention is the first international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations (Chandrasekara, 2015).

B. Need of National Certification Authority (NCA)

According to the section 7 and 8 of Electronic Transactions Act, No. 19 of 2006, there is a legal recognition for electronic signatures as well as Use of electronic records and electronic signatures in Government institutions and statutory bodies. Unlike signatures used in physical document to verify the authenticity, digital document needs to be digitally signed to verify the authenticity. Once the electronic document is digitally signed, the signee cannot be denying that he/she haven't signed that electronic document. As per the section 7 and 8 of the act, electronic documents which are digitally signed authenticated traded as legally admissible evidence(s). As per the section 8 (2) (C) all digital signatures used to sign the electronic documents need to be issued by a Certification Authority (CA) or Certification Service Provider. The task of a certification authority is to issues and maintain the lifecycle of a digital certificates which can be used to sign the electronic documents and verify the authenticity of a person or an entity.

Currently, there is no national level certification authority to issue and maintain digital certificates on behalf of Government of Sri Lanka (GOSL). Therefore, individuals and commercial organizations practices digital certificates issued by the 3rd party CAs which are situated outside the Sri Lanka. VeriSign (VeriSign, 2017), Thawte (Thawte, 2017) and Comodo (Comodo Group, 2017) are most common 3rd party certification authorities used in Sri Lanka. The problem arises when the authenticity of a Sri Lankan entity is being verified by a 3rd party Certification Authority which is belongs and located in a foreign country. As an example, to verify the authenticity of the website of the Parliament of Sri Lanka, it uses digital certificate issued by a 3rd party certification authority called Digicert (DigiCert, 2017) as illustrated in the figure 3. In such scenario, the validity of the digital certificates and digital signatures are highly questionable.

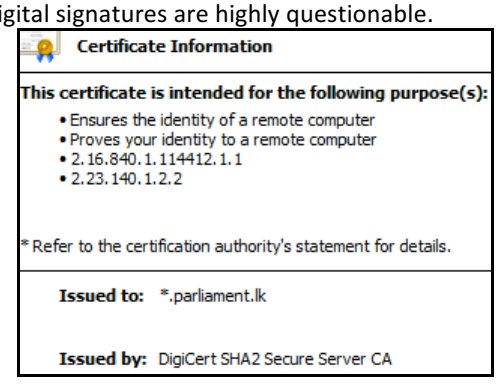

Figure 3: Digital Certificate issued to Parliament of Sri Lanka by digicert CA

The Electronic Transactions Act, No. 19 of 2006 does not have any clause to verify the authenticity of the digital certificates used by the non Sri Lankan certification authorities. Even though the section 18, 19 and 20 of Electronic Transactions Act clearly defines the requirements, establishment process and powers of a Certification Authority, currently there is an absence of national level root certification authority. This absence becomes a huge barrier to verify the authenticity of an electronic document, data message or an electronic record in order to provide legally admissible evidences to the courts.

As a solution, Information and Communication Technology Agency (ICTA) of Sri Lanka is currently in the process of implementing National Certification Authority. The Electronic Transaction Act, No. 19 of 2006 has given the provisions of setting up a Certification Authority, which will act as the National Certification Authority (Root CA) of Sri Lanka and hence accreditate and regulate the certification service providers (certificate service providers/issuing CAs) addressing the requirement of the country. Information and Communication Technology Agency (ICTA) of Sri Lanka has been designated as the Certification Authority for the purposes of the above act by the gazette notification on 24th September 2013.

C. Challenges with Could Computing

Researcher understood that more and more organizations and individuals are relying on cloud computing services to host their services, application and data. This proliferation of cloud computing has brought many challenges to forensic investigators as they rarely have physical access to the underlying infrastructure (Lopez, et al., 2016). Even though the Sri Lankan entities including government organizations are now stores their data in cloud storages and cloud services, the judicial system is unprepared to prosecute and investigate cloud based crimes. The key legal issue with the cloud computing is the ownership of the data stored in the cloud. Even though the ownership of the data belongs to Sri Lankan an entity, the data is physically stored in someone else's datacenter. Unlike traditional digital forensics methods, cloud forensics presents a unique challenge due to the omnipresent nature of 'the cloud'. The National Institute of Standards and Technology (NIST) defines Cloud Computing Forensic Science as "application of scientific principles, technological practices and derived and proven methods to reconstruct past cloud computing events through identification, collection, preservation, examination, interpretation and reporting of digital evidence" (NIST, 2014). The amount of data these cloud providers have from their clients is a very desirable objective for criminals. Additionally, hacktivists can use cloud computing as a platform to distribute malware, conduct scams and perform other criminal activity. Thus, investigating cloud related crimes is an arduous but essential task in order to bring criminals to justice (Lopez, et al., 2016).

As most of the cloud service providers store their data in different data centers across the globe, the key challenge is to find 'in what datacenter does your data lives?' The headquarters of the cloud service provider may be in a one country and its data centers may be located in different countries. Therefore, the question 'when your data is truly scattered across numerous servers, how do you determine which jurisdiction applies? (Ex. which state court do you rely on to issue subpoenas, file a civil suit, etc.)' (Willson, 2013) need to be properly answered. When it is required to obtain data from a cloud service provider, the data must be preserved until it can be lawfully acquired. Preservation is an essential tool in electronic discovery, particularly with highly volatile and elastic data (Dykstra, 2013). The discovery of electronic evidences during forensics investigation can be cumbersome, however with the support of the legal system we can make the preservation and extraction lot easier.

As a solution, Government of Sri Lanka can impose regulation on government entities and Sri Lankan citizens for store their organizational and confidential data on Lanka Government Cloud (LGC). LGC is fully owned by the Government of Sri Lanka and operations and governance is done by the Information and Communication Technology Agency (ICTA) of Sri Lanka. Since LGC is within the Sri Lankan geography, by nature, it will adopt all applicable legislations and therefore it is possible to conduct any type of computer forensic without any legal and technical barriers.

D. Legally Accepted Forensic Tools & Software

Forensics software and tools being used to automate the forensic analysis process and to extract data quickly than traditional methods. The science of digital forensics is founded on the principles of repeatable processes and quality evidence (Brunty, 2011). Therefore, Forensic software and tools must provide its results without modifying or altering existing data on the data sources. Modification done to the original sources of data will results integrity issues which leads to invalidate the output of such software. According to the definition provided by the NIST, 'digital forensics test results are repeatable when the same results are obtained using the same methods in the same testing environment' and 'digital forensics test results are reproducible when the same test results are obtained using the same method in a different testing environment' (Brunty, 2011). Moreover, such tool would be able to gather, authenticate and verify the

evidences in a sound manner while assuring that the original media is not altered. It should also need to maintain the chain of custody by maintaining the media, documents, and evidence related to a forensic case under the custody of the authoritative personal.

Forensic Toolkit (FTK) (AccessData, 2017), EnCase Forensic (Guidance Software, 2017) and Helix Enterprise (e-fense, 2017) can be named as the major commercial forensic analysis software used in the Sri Lankan context. Apart from commercial software, there are open source software as well. Autopsy® (Carrier, 2017), SANS Investigative Forensic Toolkit (SIFT) (SANS, 2017) and Computer Aided Investigative Environment (CAINE) (CAINE, 2017) are the most commonly used open source alternatives.

However, current Sri Lankan legislative system does not define what are the software tools which need to be used to produce legally admissible evidences to the courts. In some countries, legislations accept only the reports and evidences produced using commercial forensic software and does not admit the reports and evidences produced using open source forensics software. However, some countries accept reports and evidences from either commercial, open source or custom software designed by the forensics expert as long as the expert can justify the validity of the evidences to the courts. The Researcher recommends that to use commercially available and internationally recognized software and tools like Forensic Toolkit (FTK), EnCase Forensic and Helix Enterprise, because evidences and reports generated from commercial software are accepted in most other nations. Furthermore, it will help to avoid cross jurisdictional conflicts when conducting international level digital forensic investigations since most of the foreign law enforcement authorities accepts evidences from commercial forensic software.

D. Stored Communication

Preservation of data is the most important thing in stored communication. The preservation period of the information will differ from service provider to a service provider. Since most of the service providers do not have huge infrastructure to save all the communication details, most of the times they only keep stored communication data for several days. Preservation of stored communication is an essential part to protect the integrity and accuracy of evidences. Since the amount of days which service providers need to keep their communication information is not defined by the current legislation, most of the times when a investigation is carried out, relevant information might not be exists. This became a huge barrier to obtain relevant even after a few weeks from the date which the incident has occurred.

The Researcher, highly recommends that, for regarding IP addresses, SMS transactions, call logs and VPN tunnels, service providers need to retain information which can contains the user information for a considerable amount of time. The Researcher suggests that, such data need to be retained for at least period of 6 months, since normal court case would take about 6 months to resolve. However, as per the Australian Attorney General's department, Australian service providers need to retain their subscriber data along with their transactions for a minimum of 2 years (Government, July 2015). according to Eng. Roshan Chandraguptha (Chandraguptha, 2017), retaining data for 2 years is fairly expensive for a country like Sri Lanka. Therefore, his recommendation was to have a retention period of 3 months.

D. Anonymization

Anonymization is a technique used by the cyber criminals to hide their identity and cover their tracks. They are well aware about the normal situation, therefore they use sophisticated steps to hide their individuality. Anonymization techniques are specially crafted to conceal a user's identity when navigating the Internet or sending communications (Morris, 2004). Cybercrime offenders also exploit proxy servers to conceal online activity (Spence, 2003). Proxy services enable users to establish a connection to a network via an intermediary server. Common proxy servers can be configured for access control, caching services, and enhanced information security (Brown, n.d.). Furthermore, Virtual Private Networking (VPN) is another source for anonymization. VPN traffic is always encrypted and would not be able to intercept by other parties. Even for a digital forensic investigation, this traffic cannot be decrypted without having the required private or public Keys.

It is technically impossible to find out the content of anonymized traffic flow. Therefore, digital forensic experts would not be able to extract evidence out from anonymized traffic. The only possible answer is to filter out all the data traffic which comes in and out to Sri Lanka. However, such mechanism is costly and hard to implement. Therefore, this issue is beyond the control of legislations of Sri Lanka. The only step that legislation can perform is, block the access to the internet and VPN services. As an example, the authorities in China have intensified their crackdown on VPNs, internet connections that bypass the country's firewalls and online censorship (Jing, 2016).

E. Skills & Technical Competencies of a Digital Forensic Experts

Due to the growth of technology, the current measures used for finding cyber criminals and collect digital evidences are not sufficient. Therefore, digital forensic experts need to update their technical competencies more often. Methodologies which have been used to prosecute

cyber criminals before 5 years are not applicable now and many cybercrimes are now sophisticated and well-conceived, requiring police to apply technological expertise and deductive reasoning to unravel complex 'modus operandi' and substantiate elements of an offence (Bromby, March-July 2006).

In most of the cases digital forensic experts will be the first responders to a computer crime incident. Therefore, they need to possess with good technical skills and good leadership skills to obtain digital evidences at the crime scene. Seasoned leadership is required to effectively direct investigations and supervise the provision of forensic support (Horswell, 2004). However, competencies and skills required by first responders are not specifically mentioned in current Sri Lankan legislative system. According to the section 17 of the Computer Crime Act, 'any public officer having the required qualification and experience in electronic engineering or software technology' is defined as a forensic expert. Researcher strongly believes that the same set of skills needs to be acquired by Sri Lankan digital forensic expert to be an expertise in digital forensic domain. According to Brown (Brown , 2015), following set of hard and soft skills (illustrated in table1) need to be possessed by a digital forensic expert. The Researcher strongly believes that the same set of skills needs to be adopted by first responders and forensic experts.

Table 1: Soft Digital Forensics Investigative Skill Sets

Hard Skill	**Soft Skills**
Research	Communicative
Awareness	Rational
Evidence Continuity	Collaborative
Forensic Imaging	Intuitive
Networking Architecture	Coherent
Hardware	Resilient
File Systems	Punctual
Structured Data Analysis	Fastidious
Unstructured Data Analysis	Disciplined

V. CONCLUSIONS AND RECOMMENDATIONS

The Researcher has understood that it is too difficult to make modifications to the current legislative system and the changes should come from the top level governors of Sri Lanka. The Researcher recommends following high level modifications for the current legislative system.

1. Mutual Assistance in Criminal Matters Act (No. 25 of 2002) need to be updated to get assistance in obtaining digital evidences from a sources located in foreign nations. This should need to include assistance on preservation of data and obtain the preserved data.
2. Evidence (Special Provisions) Act (No. 14 of 1995) need to be modified to cater to the modern requirements of collecting digital evidences. Further, it need to be revised to support to collect evidence for foreign nations as well.
3. Government of Sri Lanka need to focus on establishing the National Certification Authority (NCA). This is to provide digital identity to Sri Lankan citizen where they can use their digital identity on the day to day electronic transactions and to sign digital documents. This will provide better traceability on evidences and offenders.
4. Government of Sri Lanka needs to focus on establishing a National Security Operations Center (NSOC) where security related incidents can be monitored real time. This will allow digital forensic experts to obtain necessary source and destination IP data along with data traffic information.
5. Act on real-time monitoring and interception of data traffic which empower police and security agencies to obtain court orders to intercept communications between computers in urgent and exceptional cases.
6. Act to access encrypted data which is in stored or in motion. This is to extract evidences from a sources where data are archived or stored with strong encryption.
7. Set of rules and regulations to keep the chain of custody during digital forensic investigation. This need to be included with instructions on digital crime scene processing and digital forensic services.
8. Need to define what are the competencies and skills need to be acquired by digital forensic experts and what are the legally acceptable digital forensic analysis software and tools.
9. Proper definition of who is a 'digital forensic expert' (this is because, Computer Crime Act defines Forensics Analyst form a government university as an 'expert', where Payment Devices Fraud Act defines Forensics Analyst from Sri Lanka CERT|CC as an 'expert). Furthermore, role of digital forensic experts need to be introduced to Government Analyst's Department.
10. Being a Commonwealth country, Sri Lanka needs to enter into the convention of 'Commonwealth Model Law on Computer and Computer Related Crime' in order to get the mutual and legal assistance to gather digital evidences during a forensic investigation as well as to prosecute cyber criminals.

ACKNOWLEDGMENT

Authors would like to express their sincere gratitude to Eng. Roshan Chandraguptha for his insightful comments and Eng. (Miss.) Vishakha Leelarathne for proofreading the entire research paper.

REFERENCES

AccessData, 2017. *Forensic Toolkit (FTK).* [Online]
Available at: http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
[Accessed 05 February 2017].

Adams, D., 2003. *Police prove a match for electronic foe.* [Online]
Available at: http://www.smh.com.au/articles/2003/12/15/1071336882279.html?from=storyrhs
[Accessed 10 February 2017].

Bromby, M. C., March-July 2006. Security Against Crime: Technologies for Detecting and Preventing Crime. *International Reviewof Law Computers & Technology,* Volume 20, pp. 1-5 .

Brown , C., 2015. Cyber-Attacks, Retaliation and Risk: Legal and Technical Implications for Nation-States and Private Entities. In: *Cybersecurity Policies and Strategies for Cyberwarfare Prevention.* s.l.:s.n., pp. 166-203.

Brunty, J., 2011. *Validation of Forensic Tools and Software: A Quick Guide for the Digital Forensic Examiner.* [Online]
Available at: http://www.forensicmag.com/article/2011/03/validation-forensic-tools-and-software-quick-guide-digital-forensic-examiner
[Accessed 05 February 2017].

CAINE, 2017. *CAINE 8.0.* [Online]
Available at: http://www.caine-live.net/
[Accessed 05 February 2017].

Carrier, B., 2017. *Autopsy Digital Forensics Platform.* [Online]
Available at: https://www.sleuthkit.org/autopsy/
[Accessed 05 February 2017].

Chandraguptha, R., 2017. *Principal Information Security Engineer, Sri Lanka CERT* [Interview] (January 2017).

Chandrasekara, G., 2015. *Sri Lanka joins Budapest Convention on Cybercrime.* [Online]
Available at: http://www.lankabusinessonline.com/sri-lanka-joins-budapest-convention-on-cybercrime/
[Accessed 14 February 2017].

Comodo Group, I., 2017. *SSL Certificates and Certificate Management.* [Online]
Available at: https://www.comodo.com/#sslcertificationcta
[Accessed 05 February 2017].

DigiCert, I., 2017. *SSL Certificates.* [Online]
Available at: https://www.digicert.com/ssl-certificate.htm
[Accessed 05 February 2017].

Dykstra, J., 2013. Seizing Electronic Evidence from Cloud Computing Environments. In: *Cybercrime and Cloud Forensics: Applications for Investigation Processes.* s.l.:O'Reilly Media, Inc. , pp. 156-172.

e-fense, 2017. *Helix3 Enterprise.* [Online]
Available at: https://www.e-fense.com/h3-enterprise.php
[Accessed 05 February 2017].

Farmer, D. & Venema, W., 2001. *Improving the Security of Your Site by Breaking Into it.* [Online]
Available at: http://www.fish.com/security/admin-guide-to-cracking.html
[Accessed 2 February 2017].

Government, A., July 2015. *DATA RETENTION - Frequently Asked Questions for Industry,* s.l.: Office of the Communications Access Co-ordinator, Australia.

Guidance Software, I., 2017. *EnCase Forensic.* [Online]
Available at: https://www.guidancesoftware.com/encase-forensic
[Accessed 05 February 2017].

Horswell, J., 2004. Chapter4: Crime scene investigation and third party quality systems accreditation. In: *The Practice Of Crime Scene Investigation.* s.l.:CRC Press, pp. 67-84.

ITU, 2012. *Understanding cybercrime: Phenomena, challenges and legal response,* s.l.: International Telecommunication Union.

Jing, L., 2016. *China blocks VPN services that let users get round its 'Great Firewall'.* [Online]
Available at: http://www.scmp.com/news/china/policies-politics/article/1922677/china-blocks-vpn-services-let-users-get-round-its-great
[Accessed 11 February 2017].

Lopez, E. M., Moon, S. Y. & Park, J. H., 2016. *Scenario-Based Digital Forensics Challenges in Cloud Computing.* s.l., s.n.

McKemmish, R., 1999. *What Is Forensic Computing?,* Canberra, Australia: Australian Institute of Criminology.

Mell, P. & Grance, T., 2011. *The NIST Definition of Cloud,* s.l.: National Institute of Standards and Technology.
Morris, S., 2004. *The future of netcrime now: Part 1 – threats and challenge,* United Kingdom : Home Office.

NIST, 2014. *NIST Cloud Computing Forensic Science Challenges,* s.l.: National Institute of Standards and Technology.
S., B. C., n.d. Cyber-Attacks, Retaliation and Risk: Legal and Technical Implications for Nation-States and Private Entities. *Cybersecurity Policies and Strategies for Cyberwarfare Prevention,* pp. 166-203.

SANS, 2017. *SANS Investigative Forensic Toolkit (SIFT) Workstation Version 3.* [Online]
Available at: https://digital-forensics.sans.org/community/downloads
[Accessed 05 February 2017].

Spence, E. E., 2003. Stalking and Technology: The Double-Edged Sword. *Journal of Technology in Human Services,* pp. 22(1), 5-18.

Thawte, 2017. *SSL Certificates.* [Online]
Available at: https://www.thawte.com/ssl/
[Accessed 05 February 2017].

UN, 2005. United Nations Office on Drugs and Crime. *The Eleventh United Nations Congress on Crime Prevention adn Criminal Justice,* p. 1.

US-CERT, 2008. *Computer Forensics ,* US-CERT: s.n.
VeriSign, I., 2017. *Everything You Need to Know About SSL Certificates.* [Online]
Available at: https://www.verisign.com/en_US/website-presence/website-optimization/ssl-certificates/index.xhtml
[Accessed 05 February 2017].

Willson, D., 2013. *Legal Issues of Cloud Forensics.* [Online]
Available at:
http://blog.globalknowledge.com/2013/03/20/legal-issues-of-cloud-forensics-part-2/
[Accessed 04 February 2017].

Author 1 : W.S.V. P Perara

Mr. W.S.V. P Perara obtained his B.Sc. Sp. (Honors) (First class) Degree in Information Technology from Sri Lanka Institute of Information Technology and his Post Graduate Diploma in Cyber Security from Curtin University of Technology, Western Australia. In addition, he has obtained his M.Sc. in Information Technology (Specialized in Cyber Security) from Sri Lanka Institute of Information Technology and his Master's in Business Studies from University of Colombo. Currently employed as an Information Security Engineer at Sri Lanka CERT|CC.

Author 2: Dr. P. Mahanamahewa

Dr. P. Mahanamahewa obtained his LL.B (Honours) (Second Class) from University of Colombo and his LL.M (Honours) in Commercial Law from University of Melbourne, Australia. In addition, he has obtained his Ph.D. in Law from University of Queensland, Australia. Currently working as a senior lecturer at the Faculty of Law, University of Colombo.