Digital forensics and evolving cyber law: case of BIMSTEC countries

Sisira Dharmasri Jayasekara
Financial Intelligence Unit, Central Bank of Sri Lanka, Colombo, Sri Lanka, and
Iroshini Abeysekara
National Dengue Control Unit, Colombo, Sri Lanka

Abstract

Purpose – The purpose of this paper is to discuss the role of digital forensics in an evolving environment of cyber laws giving attention to Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) countries, comprising Bangladesh, India, Myanmar, Sri Lanka, Thailand, Nepal and Bhutan, in a dynamic global context.

Design/methodology/approach – This study uses a case study approach to discuss the digital forensics and cyber laws of BIMSTEC countries. The objective of the study was expected to be achieved by referring to decided cases in different jurisdictions. Cyber laws of BIMSTEC countries were studied for the purpose of this study.

Findings – The analysis revealed that BIMSTEC countries are required to amend legislation to support the growth of information technology. Most of the legislation are 10-15 years old and have not been amended to resolve issues on cyber jurisdictions.

Research limitations/implications – This study was limited to the members of the BIMSTEC.

Originality/value – This paper is an original work done by the authors who have discussed the issues of conducting investigations with respect to digital crimes in a rapidly changing environment of information technology and deficient legal frameworks.

Keywords Financial crime, Information technology, Banking, Digital forensics, Prosecution, Cyberlaw

Paper type Case study

1. Introduction

Financial crimes are becoming a global threat today because money is the main motive of most criminals. Globalization of financial markets and rapid development of information technology motivate the banking industry to rely on the digital files and digital data to sophisticate banking operations. This practice has led the criminals to breach or hack the banking systems frequently. In contrast to other institutions, the systems of financial institutions are exposed to customers where criminals extract this opportunity to hack the systems. Statista (2018) states that the number of data breaches in the USA increased from 157 million in 2005 to 781 million in 2015, while the number of exposed records jumped from around 67 million to 169 million during the same time frame. However, the recovery of data breaches is time-consuming and the losses are accrued continuously until recovery. For example, the largest data breach of all time, as of September 2016, was an allegedly state-sponsored hack of Yahoo, which dates to late 2014, but it was only uncovered in 2016 (Statista, 2018). Further, they state that

Journal of Money Laundering Control
Vol. 22 No. 4, 2019
pp. 744-752

1368-5201
DOI 10.1108/JMLC-02-2019-0019

financial access data theft is the second most common type of data breach which accounts for 22 per cent of all data breaches, and the costs of cybercrimes are rather high for the financial services sector. Global cybercrimes caused, on average, annual loss of US$13.5m for the financial services industry, the highest average among all industries. Lewis (2018) estimates that that cybercrimes may cost the world about US $600bn or 0.8 per cent of the global GDP in 2018. Gorman (2013) highlights that the cost of cyber espionage and cybercrime to the USA is as much as US$100bn each year and estimates the figure around 1 per cent of the US gross domestic product.

Crimes which involve a computer and a network are generally known as digital crime, computer crime or cybercrime. In such a crime, a computer may have been used in the commission of the crime or it may be the target of the crime where such a crime may threaten a person or a nation's security and financial system stability of a country. Lewis (2018) states that cybercrime ranks third in the order in dollar value as a global scourge which indicates the gravity of cybercrimes in the global context. According to McGinn (2018), the average cost of cybercrime for financial services companies globally has increased by more than 40 per cent over the past three years, from US$12.97m per firm in 2014 to US$18.28m in 2017, significantly higher than the average cost of US$11.7m per firm across all industries. This background shows the load of work that investigators and prosecutors have to perform with respect to financial crimes. Investigation and prosecution for cybercrimes are becoming more challenging owing to limitations of the legal framework of jurisdictions and the continuous growth of information technology. These difficulties have led to developing new areas of investigations and new disciplines under forensic science. Some of the subareas before evolving digital forensics are disk forensics, database forensics, network forensics, scanner forensics, printer forensics, mobile forensics and so on. We can define digital forensics as a branch of forensic science which focuses on the recovery and investigation of material found in digital devices in relation to digital crimes. The term digital forensics was originally used as a synonym for computer forensics and later expanded to cover investigation of all devices capable of storing digital data. The main objective of the digital forensics is to find any evidence and preserve it in its most original form while performing a structured investigation for the purpose of reconstructing past events. In the early days of digital evidence, the focus was predominantly on computer crime. However, today nearly every crime has some digital artefact that might be useful for an investigation. Since 2011, the number of start-ups in fintech (technology-based companies that often compete against traditional financial-services) has risen more than 50 per cent (Hugener *et al.*, 2017). This development expands the work of investigators and prosecutors. In this background, the objective of this paper is to discuss the role of cyber forensics giving particular attention to BIMSTEC countries in the dynamic global context of which legal frameworks are not much comprehensive. The remainder of this paper is structured as follows. Section 2 provides a critical overview of the role of cyber forensics. Section 3 discusses global issues of cyber laws. Section 4 discusses the development of cyber laws in BIMSTEC countries, and Section 5 concludes.

2. Role of digital forensics

Digital forensics is a discipline that combines elements of the law, computer science and information technology to collect and analyse data from computer systems, networks, wireless communication and storage devices in a way that is admissible as evidence in a court of law (US-CERT, 2018). Digital evidence is any information of probative value that is either stored or transmitted in a binary form (Quizlet, 2018). Such evidence is invisible, volatile, dynamic and highly fragile in nature. These characteristics make investigations

more difficult. Often digital evidence provided leads to other evidence and collaborate with them in defending a lawsuit. However, constant changes in information and communication technology force policymakers and law enforcement agencies to draft up-to-date policies and standard operating procedures to strengthen the legal framework of a jurisdiction.

The main goal of the digital forensics is gathering evidence of cyber or digital crime. Investigators and forensic specialists use different forensic tools such as time-stamped hashed records, repeatable and reproducible for a chain of custody to stand as evidence in courts of law. Sometimes law enforcement agencies have to deal with unique challenges when trying to examine the devices related to suspects of terrorism. Forensic accountants play a key role in conducting forensic investigations whether it is a cybercrime or any other crime. Frequently, there is a need for collaboration between digital forensics experts and forensic accountants in cases which relate to embezzlement and accounting improprieties. Traditionally, digital forensics has taken a post-mortem or reactive approach. However, today it has evolved to be a preventive strategy of cybercrimes.

2.1 Reactive approach

The reactive approach is a kind of post-mortem to a crime where forensic investigators collect evidence, preserve, analyse and report to law enforcement authorities or courts. For example, in the case of Bangladesh cyber-heist of which cyber hackers transferred money from a central bank account of Bangladesh to some other jurisdictions. Under the reactive approach, Bangladesh authorities had to collect information from various sources and preserve them for analysis. Evidence has to be reported to the court or law enforcement authorities based on the results of the analysis to take action (Figure 1).

2.2 Proactive approach

In contrast to the reactive approach, proactive approach functions as a preventive measure of controlling exposed risks. This allows designing, developing and deploying a set of digital forensic capabilities that facilitates digital forensic tasks for discovering indicators of malicious behaviour. This approach contributes to forming an effective response to computer security incidents in the shortest possible time and with reduced cost. The proactive approach is suitable for financial institutions to monitor transactions using artificial intelligence or predetermined parameters. For example, banks can develop transactions monitoring systems with predefined parameters to identify suspicious transactions which are required to be reported to the financial intelligence units. The monitoring system will generate alerts based on the predetermined criteria and banks are required to monitor and analyse the transactions. They have to predict the consequences of transactions if they are serious. Suspicious transaction reports have to be reported as a preventive measure where there is suspicion over the observed transactions Figure 2.

The comprehensive legal framework of a country which collaborates with other counterparts on cybercrimes is a prerequisite to get the maximum use of cyber forensics. The Convention on Cyber Crimes of 2001 is the main international treaty that allows a country to have jurisdiction if a cybercrime is committed by a country's national in its territory, on board a ship displaying the flag of the country or on board an aircraft registered

Source: Compiled by the authors

Figure 1.
Reactive approach of digital forensics

under the laws of the country, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. However, the treaty has not been changed with the rapid development of information technology and the continuous growth of global cybercrimes.

3. Global issues of cyber laws

The process of Investigation and Prosecution against cybercrimes is complex because often crimes occur across many jurisdictions. Therefore, a breach of cyber security is not limited to one jurisdiction. The cost involves with respect to victims as well as the investigators is enormous in many crimes. For example, Conger (2018) states that "Uber" would have to pay US$148m to settle a nationwide investigation into a 2016 data breach, in which a hacker managed to gain access to information belonging to 57 million riders and drivers. Considering the magnitude of cybercrimes, jurisdictions have to develop a strong legal framework to combat cybercrimes. However, cyberlaws have not been developed in line with the rapid growth in information and communication technology.

Most of the laws are based on the Budapest Convention which was introduced in 2001. Because information and communication technology has caused to transform societies worldwide. The cyber industry has evolved from computer servers to cloud servers and to blockchain technology. The Budapest Convention has limited itself to a certain class sect of cybercrime regulations. It is a criminal justice treaty which aids states by criminalizing a list of attacks against and by means of computers; implementing procedural law tools to make the investigation of cybercrime and securing of electronic evidence in relation to any crime more effective and subject to rule of law safeguards; and encouraging international police and judicial cooperation on cybercrime and electronic evidence (Council of Europe, 2018). The Treaty is open for signature by the member states and non-member states that have participated in its elaboration and for accession by other non-member states. By December 2018, after 16 years of the Convention, only 61 jurisdictions had ratified the Convention including 47 members of the Council of Europe (2018). Table I shows the top ten countries of most cybercrimes and their status with the Budapest Convention. Still, China and Brazil have not been signatories to the Convention despite their higher vulnerabilities to cybercrimes.

This evidence requires countries to strengthen cyber sovereignty under cyberlaw by broadening the definition. Germany has created separate cyber squads as a new strategy. Federal services will create a new cyber response force across German law enforcement agencies. Pfaffenbach (2018) states that the project, would cost around €400m ($435.32m) and is expected to be ready by 2022. The cost of the investment shows the importance of preventive measures of cyber crimes. Cybersecurity law is emerging as a key discipline of cyberlaw. Case law provides some rich insights into jurisdictional issues on cybercrimes.

Yahoo! Inc. v. *La Ligue Contre Le Racisme et l'antisémitisme* (LICRA) (2000) was an eyeopener on jurisdictional issues of cybercrimes. This raised concerns over the legal precedent regarding the right of one country to reach across borders and impose its own laws on online material that is stored in other regions. Internet experts testified that it was possible to keep some French Web servers from seeing the sites hindering internet freedom.

Source: Compiled by the authors

Figure 2.
Proactive approach of digital forensics

Table I.
Top 10 countries of most cybercrimes and status with the Budapest Convention

Rank	Country	Signatures and ratifications of Treaty		
		Signed on	Ratified on	Entry into force
1	USA	23.11.2001	29.09.2006	01.01.2007
2	China	–	–	–
3	Germany	23.11.2001	09.03.2009	01.07.2009
4	UK	23.11.2001	25.05.2011	01.09.2011
5	Brazil	–	–	–
6	Spain	23.11.2001	03.06.2010	01.10.2010
7	Italy	23.11.2001	05.06.2008	01.10.2008
8	France	23.11.2001	10.01.2006	01.05.2006
9	Turkey	10.11.2010	29.09.2014	01.01.2015
10	Poland	23.11.2001	20.02.2015	01.06.2015

Source: EnigmaSoft (2018) and Council of Europe (2018)

However, *Zippo Mfg. Co.* v. *Zippo Dot Com* (1997) laid the foundation for many issues in cybercrimes.

In this case, the district court found that Zippo Dot Com had purposefully availed itself in Pennsylvania by virtue of Zippo Dot Com's interactive website and contracts of 3,000 individuals and seven internet providers in Pennsylvania, allowing them to download electronic messages, which formed the bases of the lawsuit. By conducting electronic commerce with Pennsylvania residents, the non-resident California Corporation was determined to have purposefully availed itself of doing business in Pennsylvania. The court used a three-pronged test for determining whether the exercise of specific personal jurisdiction over a non-resident defendant is appropriate: the defendant must have sufficient minimum contacts with the forum state, the claim asserted against the defendant must arise out of those contacts and the exercise of jurisdiction must be reasonable.

In an Indian case, *India TV Independent News Service (Pvt) Ltd* v. *India Broadcast Live LLC, MIPR* (2007), the court held that a mere fact that a website is accessible in a particular place itself is not sufficient for the courts of that place to exercise personal jurisdiction over the owners of the website. However, in case a website is not merely passive but is interactive, permitting the browsers to not only access the contents thereof but also subscribe to the services provided by the owners, then the position is different. This position was confirmed in the Banyan Tree case (2009). Banyan Tree Holdings, a company registered in Singapore, ventured across the globe. An Indian company, Township Developers adopted the name "Banyan Tree" for marketing in the website which was interactive and accessible across India. The Singapore company approached Delhi High Court and possessed the requisite jurisdiction, as the services of the defendants were being offered to residents of Delhi through brochures. Having considered the "universality, ubiquity and utility" of the internet and the World Wide Web, which were all indicative that the High Court possessed the jurisdiction to hear the matter.

In *Casio India Co. Limited* v. *Ashita Tele Systems Pvt. Limited* (2003), Delhi High Court held that once a website can be accessed from Delhi, it is enough to invoke the territorial jurisdiction of the court. The court observed that where a defendant that clearly does business over the internet enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the internet, personal jurisdiction is proper. However, where a defendant only posts information on the internet accessible to users in foreign jurisdictions, the court could not exercise personal jurisdiction

where the website was merely passive. Where the defendant uses an interactive website to host information and exchange the same with the user, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website. However, in *Toys "R" Us, Inc.* v. *Step Two, S.A* (2003) when the trademark was used on a New Jersey-based plaintiff's as well as the Spanish defendant's website, although the defendant operated an interactive website for persons residing in New Jersey, the court went on to state that a commercially interactive website by itself was insufficient to establish jurisdiction, and additionally there had to be evidence of direct targeting of consumers in the area. The court also used the "effects test" according to which courts can exercise jurisdiction in cases where the acts were committed outside its jurisdiction but were intentionally aimed at the forum state with its effects felt in the forum state. Thus, even if the effects are experienced in the forum state, the defendant must have a "manifest intention" to target the forum state, with contacts either through the Web (in which case, the interactivity of the website ought to be a relevant consideration) or through a non-internet-based activity.

These cases show the complexity and difficulties of implementing cyber laws in the international context. To minimize the complexities, some norms have been developed to mitigate cross-country barriers in implementing laws. Bilateral arrangements, mutual legal assistance treaties and a common minimum of standards of behaviour are among other things. Awareness of the high risk of cybercrimes was amplified subsequent to Snowden revelations. Some countries are trying to come up with their own secured national networks to mitigate exposed risks. According to Patrizio (2013), the BRICS nations – Brazil, Russia, India, China, and South Africa – are building their own high-speed internet free of the US influence. This kind of fragmentation of the internet is likely to be accelerated in future, bypassing the dangers of surveillance and monitoring from foreign shores.

4. Development of cyber laws in BIMSTEC countries

The Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) was established in 1997 as a regional organization comprising seven member states, i.e. Bangladesh, India, Myanmar, Sri Lanka, Thailand, Nepal, and Bhutan, lying in the littoral and adjacent areas of the Bay of Bengal constituting a contiguous regional unity. These countries cooperate in different areas of sharing assistance to the member countries. They have conducted workshops and training sessions on cybercrimes and cyber forensics. However, strengthening cyberlaws in BIMSTEC countries is not a prime area of cooperation of the initiative.

First legislation which was related to cybercrimes in BIMSTEC countries was enacted by India in 2000. The Focus of Information Technology Act, No. 21 of 2000, was to address crimes related to information technology. Section 75 of the Act states that the Act applies for offence or contravention committed outside India to any offence or contravention committed outside India by any person irrespective of his nationality if the act or conduct constituting the offence or contravention involves a computer, a computer system or a computer network located in India. This Act has been amended in 2008 to include digital signatures. However, Section 75 has not been amended.

Bangladesh enacted the Information and Communication Technology Act, No. 39 of 2006, to first introduce legislation which is related to cybercrimes in 2006. Section 4 of the Act states if any person commits offence or contravention under the Act outside of Bangladesh which is punishable under the Act if he commits it in Bangladesh, then the Act shall apply as such he commits offence or contravention in Bangladesh. Section 4.2 states that if any person commits offence or contravention in Bangladesh under the Act from

outside Bangladesh using a computer, a computer system or a computer network located in Bangladesh, then the Act shall apply as such the entire process of the offence or contravention took place in Bangladesh. Section 4.3 further ads that if any person from within Bangladesh commits offence or contravention outside of Bangladesh under the Act, then the Act shall apply against him as such the entire process of the offence or contravention took place in Bangladesh.

Myanmar has not developed a comprehensive law related to cybercrimes. However, some aspects are covered in the electronic transactions law and the telecommunications law of the country. Section 33(a) of the Electronic Transactions Law stipulates that any person found using electronic technology to do "any act detrimental to the security of the State, or the prevalence of law and order, or community peace and tranquillity" may be punished by a minimum of seven years imprisonment.

Sri Lanka enacted the Computer Crime Act, No. 24 of 2007, to strengthen the legal framework for cybercrimes. Section 2 of the Act states that the provisions of the Act shall apply where a person commits an offence under the Act while being present in Sri Lanka or outside Sri Lanka; the computer, computer system or information affected or which was to be affected, by the act which constitutes an offence under the Act, was at the material time in Sri Lanka or outside Sri Lanka; the facility or service, including any computer storage, or data or information processing service, used in the commission of an offence under this Act was at the material time situated in Sri Lanka or outside Sri Lanka; or the loss or damage is caused within or outside Sri Lanka by the commission of an offence under this Act, to the State or to a person resident in Sri Lanka or outside Sri Lanka.

Thailand enacted the Computer Crime Act, B.E.2550 (2007), after a period of nine years since its initial draft. Sections 5 to 17 describe the offences which are covered under the Act.

These sections cover illegal accessing of a computer system and data, damages caused to the third parties owing to illegal access, any act by electronic means to eavesdrop a third party's computer data in the process of being sent in a computer system and not intended for the public interest. Nepal introduced the law of cybercrimes by enacting the Electronic Transactions Act, 2063 (2008), to cover a list of offences related to cybercrimes extending throughout Nepal as well as any person residing anywhere by committing an offence in contravention to the provisions of the Act. Bhutan introduced Bhutan Information Communication Media Act in 2006, and this Act has been repealed in 2018 by introducing the Information, Communications and Media Act of Bhutan 2018. Chapter 22 of this Act describes a list of offences covered by the Act.

5. Conclusion

Implementing a sound legal framework in a continuously evolving technological environment is a big challenge for many countries. One of the most difficult tasks that investigators of cybercrimes are facing today is to identify the applicable laws for a cybercrime. Dual criminality is common and it is usually necessary for two countries to cooperate on a specific criminal matter. However, the laws of each country do not have to exactly be the same in carrying out the prosecutions. Limitations of adequate resources of jurisdictions are another challenge in implementing evolving cyber laws.

Having studied the risk-based AML/CFT supervision, Jayasekara (2018) states that technical assistance is required to low-income countries to upgrade the level of compliance owing to the lack of expertise in these countries. Cyber laws are also considered an emerging discipline that requires expert knowledge. Therefore, it is required to provide technical assistance to emerging countries for constant training and updated instruments for developing experts. Availability of a strong network of contacts is a must in implementing

cyber laws. Obtaining data is another challenge faced by law enforcement agencies. Sometimes traceability of electronic communication is questionable. Laws allow for timely access by law enforcement agencies. However, in practice, situations arise where there are huge time gaps from detection to obtaining data. This slow process may hinder the effectiveness of timely sharing of information with foreign law enforcement partners. In some cases, privacy issues affect investigations. However, law enforcement's ability to identify criminals is enhanced by having access to traffic data. Therefore, jurisdictions have to take different approaches to balance privacy concerns with law enforcement access while requiring appropriate data retention periods. Most importantly, countries have to develop a mechanism to share evidence with other countries. Domestic law has to be structured in a way to allow evidence obtained in a foreign country to take actions against cybercrimes. However, in practice, potential evidentiary problems such as the authenticity of the evidence, the chain of custody of the evidence and the quality of forensics and witnesses affect the law enforcement process. To avoid most of the concerns, countries have signed mutual legal assistance treaties. Law enforcement agencies have to consider accommodating electronic evidence in such treaties. If not, they have to consider revising treaties to provide efficient and satisfactory evidentiary requirements, as they create legal obligations to assist.

Apart from the legal framework to prevent cybercrimes, countries can consider evolving technology itself to mitigate cybercrimes. With respect to data security, ensuring authentication, authorization, integrity, confidentiality and non-repudiation during storage, retrieval and transmission of data or information is required. Therefore, technologies such as biometrics, secure X, secure transmission, end-to-end security with block chains, secure software and secure hardware, among other methods, can be used to protect the data. In the current context, blockchain technology has revolutionized the data security paradigm. The blockchain is a distributed replicated database that allows secure transmission between two entities without a central authority. Experts and researchers use the term to identify the whole technology ecosystem behind digital assets exchange among participants of the same network with no intermediates Thus, digital assets can be traced, and in this way, participants can identify counterfeit assets; in addition, the distributed ledger increases the safety of information and transaction, preventing double spending and money theft through hacking attacks, because information is not collected in one single place.

References

Banyan Tree case (2009), 894/2008 (Delhi High Court 2009). *Casio India Co. Limited* v. *Ashita Tele Systems Pvt. Limited*, 2003 (27) PTC 265 (Delhi High Court 2003)

Conger, K. (2018), "Uber settles data breach investigation for $148 million", The New York Times, New York, NY, available at: www.nytimes.com/2018/09/26/technology/uber-data-breach.html

Council of Europe (2018), "Chart of signatures and ratifications of treaty 185", Council of Europe, Paris, available at: www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=SDfz9MQr

EnigmaSoft (2018), "Top 20 countries found to have the most cybercrime", EnigmaSoft, Dublin, available at: www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

Gorman, S. (2013), "Annual US Cybercrime costs estimated at $100 billion", The Wall Street Journal, available at: www.wsj.com/articles/SB10001424127887324328904578621880966242990

Hugener, C. Mavros, K. and Courbe, J. (2017), "Financial services trends: moving beyond the old-fashioned centralized IT model", PwC, Chicago, available at: www.strategyand.pwc.com/media/file/2017-Financial-Services-Trends.pdf

India TV Independent News Service (Pvt) Ltd v. *India Broadcast Live LLC, MIPR* (2007), (2) 396, 2007 (35) PTC 177 Del (Delhi High Court 2007)

Jayasekara, S.D. (2018), "Challenges of implementing an effective risk-based supervision on anti-money laundering and countering the financing of terrorism under the 2013 FATF methodology", *Journal of Money Laundering Control*, Vol. 21 No. 4, pp. 601-615.

Lewis, J. (2018), "Economic impact of cybercrime-no slowing down", McAfee, Santa Clara, available at: www.mcafee.com

McGinn, M. (2018), "Cybercrime costs financial-services sector more than any other industry, with breach rate tripling over past five years. Accenture", available at: www.businesswire.com/news/home/20180213005282/en/Cybercrime-Costs-Financial-Services-Sector-Industry-Breach-Rate

Patrizio, A. (2013), "BRIC nations plan their own "independent internet", IT World, available at: www.itworld.com/article/2705173/networking-hardware/bric-nations-plan-their-own–independent-internet-.html

Pfaffenbach, K. (2018), "Germany creates cybersecurity squads, allocates funds for new spy satellite", RT Question More, available at: www.rt.com/news/366386-germany-cyber-security-spy-satellite/

Quizlet (2018), "How is evidence admissible and relevant", available at: https://quizlet.com/194627063/itp-375-quizlet-flash-cards/

Statista (2018), "Cyber crime: biggest online data breaches 2007-2018", The Statistics Portal, available at: www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/

Toys "R" Us, Inc. v. *Step Two, S.A* (2003), 318 F.3d 446 (3d Cir. 2003) (United States Court of Appeals 2003)

US-CERT (2018), "Computer forensics", *United States Computer Emergency Readiness Team*, Vol. 11 No. 28, available at: www.us-cert.gov/sites/default/files/publications/forensics.pdf

Yahoo! Inc. v. *La Ligue Contre Le Racisme et l'antisémitisme* (LICRA) (2000), (Tribunal de grande instance 2000). *Zippo Mfg. Co.* v. *Zippo Dot Com*, 952 F.Supp. 1119 (W.D. Pa. 1997) (District Court 1997)

Corresponding author
Sisira Dharmasri Jayasekara can be contacted at: sisiradj@cbsl.lk