CYBER FORENSIC CHALLENGES

FADI ABU ZUHRI

INTRODUCTION

The increase in the number of people using networked digital devices has led to incidences of crime that call for forensic investigations (Brown, 2015). The existence of Cyber Forensics skills has made it possible to gather evidence from such devices. The evidence collected is used in courts to establish the crime and bring Cyber criminals to justice. Cyber Forensic investigators and analysts are often entrusted with the task of finding, recording, analysing, and reporting of digital evidence. The whole process of gathering forensic evidence has a number of challenges. These challenges are categorized into five broad areas: hardware challenges, software challenges, cloud forensic challenges, legal challenges and human challenges (Karie, & Venter, 2015; Lindsey, 2006; Mohay, 2005).

HARDWARE CHALLENGES

Hardware challenges are linked to the needs of the modulated technology and enhancements of the hardware. Studies suggested that some criminal suspects change the hard disk within their devices before the Cyber Forensic expert can gain access to the device (National Institute of Justice, 2002; Brown, 2015). In such cases, the suspects use the write blockers to shift information between the two hard disks. The main effect is that a forensic examination of the new hard disk, may not display some of the relevant evidence. On the other hand, the evidence gathered from the new hard disk will lack consistency, and may not be apparent (Brown, 2015; Spafford, 2006).

Further, the evidence gathered from a device that was reset, may accentuate the problem since during the reset process, a small portion of the backup information is likely to have been reinstalled. For example, different mobile devices have hard disks that have enmeshed algorithm that are responsible for erasing the data automatically. Since the technology for collecting information from unused devices or devices where information was deleted by a user is still under development, there is likely to be some delays in obtaining such information. It is for this reasons that some Cyber Forensic experts have reported tremendous challenges in retrieving information from content that was deleted from the device (Spafford, 2006).

SOFTWARE CHALLENGES

The current era of technological advancements and changes in gathering forensic evidence has resulted into the birth of *Platform as a Service* (*PaaS*) and *Software as a Service* (*SaaS)*, which have brought a number of changes into the computing structure. The use of new software and new technology has brought about a number of challenges. One of the challenges is lined to the well-developed device operating system. The current operating systems have been log enabled, and now requires a Cyber Forensic expert to gather background information on the device, which includes the information on accessibility of the application, usage of the application, and the level of information provided by the specific user of the application. Even though the new development appears like a progress for the different devices, the development requires some time for it to mature (Spafford, 2006; Giordano & Maciag, 2002).

Several challenges have been reported on the application accessibility since the application and the operating system are defined differently (Giordano & Maciag, 2002). For example, any alteration made on the file content may not be tracked until it is compared with subsequent/previous file versions or, if it is compared with the modified version of the time stamp. In case the Cyber Forensic expert suspects some manipulation on the document, it would be a challenge to determine the extent of manipulation (Brown, 2015).

Further, some forms of applications and log information that are collected by the application or the operating system, could be useful as evidence in certain cases. Despite the usefulness of the application, the awareness of its use is still at an infant stage making it difficult for the Cyber Forensic experts to ensure the effective use of the application. For example, an operating system like Windows 8 will collect information on all the Wi-Fi networks that have been accessed together with the transmission of the data. The information gathered would help investigations, such as those investigations that involve theft of data or in cases of network intrusion. However, a correlation between the gathered information, from the sources, and the event violation in the gathered information is a concept under research and experimentation (Giordano & Maciag, 2002).

The high number of mobile messaging applications available across the globe uses a software that automatically erase the information that is shared. The main challenge here is that it will be complex for a Cyber Forensic expert to gather such information that was deleted. Another

challenge is the encryption in different mobile devices with intention of having the information protected especially during the process of gathering data. For example, gathering data from encrypted mobile chat applications may pose a challenge in certain situations. Contrary to popular belief all mobile chat applications are not encrypted. Certain mobile chats allow a secure connection between the sender and the receiver with no option to retrieve the message after a set time period. Other sessions are simply saved as text messages in the phone storage allowing anyone with the mobile phone passcode to access all stored messages. Even without a passcode, it is technically possible for the chat server to provide chat history with the right encryption key. The decryption of devices may be a challenge to some investigations where the storage or device itself is encrypted (Giordano & Maciag, 2002).

Not handing over mobile device PIN and passwords could lead to legal consequences in certain countries. For example, not giving passwords can get someone arrested according to Schedule 7 of Terrorism Act in the United Kingdom (legislation.gov.uk, 2008; Mandhai, 2017).

CLOUD FORENSIC CHALLENGES

Cloud computing is now used by smart mobile devices. The flexibility and scalability of cloud computing poses a huge challenge to forensic investigation (Lopez, Moon, & Park, 2016). The data in these devices, maybe able to be accessed everywhere hence posing another challenge to the investigators. It is a challenge for the investigator to locate the data in a way that ensures the privacy rights of the users. The investigators require the knowledge on anti-forensic tools, practices, and tools that help ensure that the forensic analysis is done accordingly (Spafford, 2006; Lopez, Moon, & Park, 2016).

Cloud-based applications also enable users to ensure that data is accessed from various devices. For example, if one of the two devices of a single user is compromised and both devices lead to some changes in the application, it would be difficult for the Cyber Forensic expert to identify the real source of the change. High risks may compromise credentials and theft of the identity in an environment that is cloud-based and lead to changes that are unknown such as the evidence remaining unknown. On the other hand, an email viewed using a user's smart mobile device and deleted may not be traced easily. In most cases, it would be difficult to examine severs of the mail and identify the evidence of the deleted communication (Lopez, Moon, & Park, 2016).

LEGAL CHALLENGES

There have been some changes in the data protection and privacy regulations in different countries across the globe (Garrie & Morrissy, 2014). Cyber laws and regulations in different jurisdiction vary and many do not take into account, the complexity in collecting forensic evidence. For example, in the machine of a suspect, the information that is available is likely to have some personal information that could be crucial in an investigation. However, accessibility to such private information is likely to be considered as a violation of user privacy (Spafford, 2006).

On the other hand, the era of companies giving some provision to their employees to use their individual devices in accessing the official communication is likely to contribute to several challenges involved in data gathering. Accessing the email of a user, for instance, using webmail and a smart mobile device together with downloading the involved attachments is an example of theft of personal data. In the current era, collecting specific information from a user device is in itself a challenge (Kaur & Kaur, 2012).

HUMAN CHALLENGES

Cyber Forensic experts are tasked with collecting and analysing the role of identifying criminals and going through all the evidence gathered against the criminals. These are well-trained professionals working for the public law enforcement agencies or in the private sector to perform roles that are associated to the collection and analysis of forensic evidence. The Cyber Forensic experts also come up with reports that are majorly used in the legal settings for investigations. Besides working in the laboratory, Cyber Forensic experts take up the role of applying the techniques of forensic investigation in the field uncovering the data that is relevant for the court (Karie & Venter, 2015).

The Cyber Forensic experts have the ability of recovering data, which was deleted previously, hidden in the mobile folds, or encrypted. The court, in most cases, calls the Cyber Forensic experts to provide testimony in the court and elaborate on the evidence reports during a given investigation. As such, the Cyber Forensic investigators get involved in complicated cases that may include examining Internet abuse, determining the digital resources that are misused, verifying the offenders' alibis, and examining how the network was used to come up with

forensic threats. There are times when the Cyber Forensic expert is expected to offer support to cases that deal with intrusions, breaching of data, or any form of incident. Through the application of the relevant software and techniques, the device, system or the platform is examined for any kind of evidence on the persons involved on the crime (Karie, & Venter, 2015).

In a forensic examination, data is retrieved from the digital devices, which are considered to be evidence required for the investigations. In most cases, a systematic approach may be used to analyse the evidence, which would be presented in the court at the time of the proceedings. At an early stage of the investigation, the Cyber Forensic expert is required to get involved in gathering evidence. Early engagement in the investigation process helps the Cyber Forensic expert to be in a position to restore all the content without causing damage to the integrity (Karie, & Venter, 2015).

There are different types of forensic cases that are handled by the Cyber Forensic experts. Some of the cases deal with intruders getting into the victim' devices and stealing their data, other cases, are for the crime offenders who launch attacks on several websites or those who try to gain some access to the names of the users and the password so as to engage in identity fraud. A Cyber Forensic expert has the ability to explore the type of fraud committed by analysing the evidence and using the required techniques. Despite the reason behind the investigation, the experts go through the process procedurally to ensure the findings recorded or gathered are sound. After opening a given case, the items that would be seized include the digital devices, software, and other media equipment's so as to run the investigation. In the retrieval process, the items considered essential will be gathered so as to give the analyst everything that would be required for the testimony (Karie, & Venter, 2015).

Another human-related challenge faced by Cyber Forensics is spoliation (Cavaliere 2001; Mercer 2004). Spoliation occurs when the person handling evidence fails to preserve, alters evidence, or destroys evidence that could be useful in pending ligation (Watson, 2004). Spoliation may be caused by negligent on the part of the party handling the litigation or handling evidence and intentional destroying evidence by the handler.

OTHER CHALLENGES

Elsewhere, in a literature-based study, Karie and Venter (2015) identified and categorized cyber forensic challenges into four: technical challenges, law enforcement or legal system challenges, personal-related challenges and operational challenges.

Technical Challenges were identified as vast volume of data; bandwidth restrictions; encryption; volatility of digital evidence; incompatibility among heterogeneous forensic techniques; the digital media's limited lifespan; emerging devices and technologies, sophistication of digital crimes; anti-forensics; emerging cloud forensic challenge.

Legal Challenges were identified as jurisdiction, admissibility of digital forensic techniques and tools; prosecuting digital crimes; privacy; ethical issues; lack of sufficient support for civic prosecution or legal criminal prosecution.

Personnel-related Challenges were identified as semantic disparities in Cyber Forensics; insufficient qualified Cyber Forensic personnel; insufficient forensic knowledge and the reuse among personnel; strict Cyber Forensic investigator licensing requirements; and lack of formal unified digital forensic domain knowledge.

Lastly, Operational Challenges were identified as significant manual analysis and intervention; incidence detection, prevention and response; lack of standardized procedures and processes; and trust of Audit Trails (Vaciago, 2012; Mercuri, 2009; Bassett, Bass, & O'Brien, 2006; Liu, & Brown, 2006; Richard, & Roussev, 2006; Arthur, & Hein, 2004; Mohay, 2005).

CONCLUSION

This paper revealed several challenges faced by Cyber Forensics. These challenges can be categorized into five: hardware, software, cloud, legal and human. They can also be categorized into technical challenges, law enforcement or legal system challenges, personal-related challenges, and operational challenges. While the available literature has sufficient details on the technical aspects of Cyber Forensic investigation, the human element only seems to touch the surface. There is a huge gap in terms of understanding the emotional and cultural aspects of the stakeholders involved in the investigation process. This calls for a review of Cyber Forensics where elements of Emotional Intelligence (EQ), Cultural Intelligence (CQ) and People Intelligence (PQ) are further investigated for a better understanding.

REFERENCES

1. Arthur, K.K., & Hein, S.V. (2004). An investigation into computer forensic tools. Proceedings of the ISSA conference; Midrand, South Africa. Piscataway, NJ: IEEE Computer Society Publishers; 1–11.
2. Bassett, R., Bass, L., & O'Brien, P. (2006). Computer forensics: an essential ingredient for cyber security. J Inform Sci Technol; 3:22–32.
3. Brown, C. (2015) Investigating and prosecuting cybercrime: Forensic dependencies and Barriers to Justice. *International Journal of Cyber Criminology*, 9 (1): 55-119.
4. Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. Revision 2. National Institute of Standards and Technology; 2012 Aug.; NIST Special Publication 800-61
5. Cavaliere, F. J. (2001). "The Web-wise Lawyer," *Practical Lawyer;* 47(4): 9-10.
6. Garrie, D. & Morrissy, D. (2014). Digital forensic evidence in the courtroom: Understanding content and quality. *Northwest Journal of technology and intellectual property*, 12 (2): 121.
7. Giordano, J & Maciag, C. (2002). Cyber forensic: A military operations perspective. *International Journal of digital evidence*, 1 (2): 1-13.
8. Kaur, R & Kaur, A. (2012). Digital Forensics. *International Journal of Computer Application*, 50(5): 0975-887.
9. Karie, N.M., & Venter, H.S. (2015). Taxonomy of challenges for digital forensics. Journal Forensics, Sci, *60(4*): 885-893.
10. Liu, V., & Brown, F. (2006). Bleeding-edge anti-forensics. Proceedings of the InfoSec World Conference & Expo; Orlando, FL. Washington, DC: NIST Special Publication; 800–86.
11. Lopez, E.M. & Moon, S.Y., & Park, H.J. (2016). Scenario-Based Digital Forensics Challenges in Cloud Computing. *Symmetry*, *8* (107): 2-20.
12. Lindsey, T. (2006). Challenges in Digital Forensics. Retrieved on 8th May 2017 from http://www.dfrws.org/2006/proceedings/Lindsey-press.pdf

13. legislation.gov.uk. (2008). Counter-Terrorism Act 2008. Retrieved May 23, 2017, from http://www.legislation.gov.uk/ukpga/2008/28/schedule/7

14. Mandhai, S. (2017, May 15). Cage activist faces charges for not giving up passwords. Retrieved May 23, 2017, from http://www.aljazeera.com/news/2017/05/cage-activist-faces-charges-giving-passwords-170515130616563.html

15. Mercer, L. D. (2004). "Characteristics and Preservation of Digital Evidence," *FBI Law Enforcement Bulletin* 73(3): 28-34.

16. Mercuri, R. (2009). Criminal defense challenges in computer forensics. Proceedings of the Digital Forensics and Cyber Crime Conference, Albany, NY. Berlin/Heidelberg: Springer Berlin Heidelberg Publishers.

17. Mohay, G. (2005). Technical Challenges and Directions for Digital Forensics in 1st International Workshop on Systematic Approaches to Digital Forensic Engineering.

18. National Institute of Justice. (2002). *Results from Tools and Technology Working Group, Governors Summit on Cybercrime and Cyber terrorism*, Princeton NJ.

19. Richard, G.G., & Roussev, V. (2006). Digital forensics tools – the next generation. Hershey, PA: Idea Group Inc; 76–91.

20. Vaciago, G. (2012). Cloud computing and data jurisdiction: a new challenge for digital forensics. Proceedings of the third International Conference on Technical and Legal Aspects of the e-Society; Valencia, Spain. IARIA XPS Press; 7–12.

21. Spafford E. (2006). Some Challenges in Digital Forensics. In: Olivier M.S., Shenoi S. (eds) Advances in Digital Forensics II. IFIP Advances in Information and Communication, vol 222. Springer, Boston, MA

22. Watson, L. M. (2004). "Anticipating electronic discovery in commercial cases," *Michigan Bar Journal.* 83(31), 23-45.