International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:7, 2018

# An Analysis of Digital Forensic Laboratory Development among Malaysia's Law Enforcement Agencies

Sarah K. Taylor, Miratun M. Saharuddin, Zabri A. Talib

***Abstract*—**Cybercrime is on the rise, and yet many Law Enforcement Agencies (LEAs) in Malaysia have no Digital Forensics Laboratory (DFL) to assist them in the attrition and analysis of digital evidence. From the estimated number of 30 LEAs in Malaysia, sadly, only eight of them owned a DFL. All of the DFLs are concentrated in the capital of Malaysia and none at the state level. LEAs are still depending on the national DFL (CyberSecurity Malaysia) even for simple and straightforward cases. A survey was conducted among LEAs in Malaysia owning a DFL to understand their history of establishing the DFL, the challenges that they faced and the significance of the DFL to their case investigation. The results showed that the while some LEAs faced no challenge in establishing a DFL, some of them took seven to 10 years to do so. The reason was due to the difficulty in convincing their management because of the high costs involved. The results also revealed that with the establishment of a DFL, LEAs were better able to get faster forensic result and to meet agency's timeline expectation. It is also found that LEAs were also able to get more meaningful forensic results on cases that require niche expertise, compared to sending off cases to the national DFL. Other than that, cases are getting more complex, and hence, a continuous stream of budget for equipment and training is inevitable. The result derived from the study is hoped to be used by other LEAs in justifying to their management the benefits of establishing an in-house DFL.

***Keywords*—**Digital forensics, digital forensics laboratory, digital evidence, law enforcement agency.

## I. Introduction

CYBERSECURITY Malaysia (CSM) is an agency under the Ministry of Science, Technology and Innovation, and since 2002, acts as a national DFL for Malaysia's LEAs. To date, CSM has been handling cases from more than 30 agencies. CSM offers purely Digital Forensics (DF) service; the agency is not a part of LEAs and does not have an investigation unit. The hired DF examiners are from various computer backgrounds.

After 15 years of operating, CSM's directions have changed. Due to the rapid rise of cybercrime, the agency now would like to focus more on complex cases and those that require research work. LEAs are hoped to conduct basic digital investigations on their own.

Sarah K. Taylor, Miratun A. Saharuddin and Zabri A. Talib are with the Digital Forensic Department of CyberSecurity Malaysia, 7, Jalan Tasik, Sapura@Mines, The Mines Resort City, Seri Kembangan, 43300, Selangor, Malaysia (e-mail: sarah@cybersecurity.my, miratun.madihah@cybersecurity.my, zabri@cybersecurity.my).

## II. Cybercrime in Malaysia

It is known for a fact that the cybercrime rate is surging in Malaysia. In 2018, according to the Police Commercial Crimes Investigations Department (CCID), in just three months, already RM60 million was reported lost to scammers [1]. According to Joseph Carson, Chief Security Scientist at Thycotic, as a result of companies not moving quick enough to new technologies, cyber-attacks have been deemed one of the greatest threats and concerns to eight global economies - the USA, Germany, Estonia, Japan, Holland, Switzerland, Singapore and Malaysia [2]. In 2017, Malaysia had lost RM179.3 million to cybercrime activities [3]. In the same year, Malaysia had seen the biggest ever data breach involving 46.2 million mobile users' data [4]. In 2016, statistics of incident cases reported to CSM show fraud cases detected in cyberspace jumped 20% compared to 2015 [5]. In the same year too, CSM discovered over 2,100 servers belonging to government agencies, banks, universities and business were compromised and up for sale on an underground cybercrime shopping website [6]. On average, almost 10,000 online incidents are reported to CSM each year.

The LEAs in Malaysia clearly need to strengthen its capacity and capability to combat the surge of cybercrime. One of the ways is by building up and strengthening its DF in order to put the criminals behind the bars.

## III. Digital Forensics

### *A. Digital Evidence*

The nature of digital evidence is different from physical evidence. It is latent, easily altered, damaged, or destroyed; crosses jurisdictional borders quickly and easily and can be time sensitive [7]. It is also ubiquitous yet difficult to manage.

Reference [8] in their research pointed out four challenges of digital evidence. The first is that it is difficult to handle and not all of them are obviously human readable. The risk of inaccurate interpretation is higher compared to physical evidence. The second challenge is that digital evidence is an abstraction of some event or digital object, thus it is impossible to get a full view of what has happened. For example, artefacts that indicate an email was sent out from a computer can be extracted from a server log, however, artefacts such as mouse click and keystrokes could not be discovered. The third challenge is data from a computer can be easily altered or changed without leaving any obvious traces. The forth and the last one is that due to the interconnectivity

of one computer to another, evidence is usually created or retrieved from different sources. For example, a web page viewed as a single record by the user is actually come from many data sources (i.e. pictures from files, values from databases, information from system registry).

Based on these facts, and therefore, examination and analysis of the digital evidence must be handled with care.

### *B. DF Laboratory*

To minimize the risk of contamination and misinterpretation, digital evidence is best to be analyzed in a controlled environment [9], [10]. The investigation of billions of bytes of digital data is similar to the investigation of a house where an investigator must look at thousands of objects, fibers, and surface areas and use his experience to identify potential evidence that should be conducted in a laboratory for analysis [11].

A DFL shall provide a conducive environment for a DF examiner to comfortably examine and analyze digital evidence. The DFL shall be properly controlled in terms of its equipment management, temperature and humidity management as well as limiting the number of people who can access the laboratory, hence minimizing contamination.

The DFL should also be responsible to track the use and attrition of forensic evidence (digital evidence) in the criminal justice system from the crime scenes [12].

### *C. LEA and DFL around the World*

The prominence of digital evidence in nearly every aspect of life has naturally raised its importance within the context of law enforcement operations [13].

About 14 years ago, in 2004, due to the importance of DF, the US National Institute of Justice published a special report for LEAs on the forensic examination of digital evidence [14]. This report was used by the DF examiners in the LEAs as a guideline to conduct analysis on digital evidence.

According to Wildan and Slay [15] in their research (2005), DF teams and a DFL are now common place within Australia, particularly associated with law enforcement and intelligence agencies. The establishment of a DFL within Australia has predominantly been aligned with LEAs.

Across the globe, computer forensics is becoming so usual that DFLs are not only found in LEAs, but also in private companies, research centers and universities [16].

As a summary, LEAs across the country view the DF as an important element to their investigation that they have long started establishing own DF team and DFL.

### *D. LEA and DF in Malaysia*

From an estimation of 30 LEAs in Malaysia, unfortunately only eight of them own a DFL. All the DFLs are located at the headquarters, and none of them located at the state level. Despite the increase in cybercrime rates around the globe, many LEAs in Malaysia are still lacking, and some even do not have proper equipment and facility to execute a digital investigation.

The Internet regulatory body, Malaysian Communication 4 (MCMC), estimated that currently there are 24.5 millions of active Internet users in Malaysia [17]. Assuming one DFL has five analysts; with the total of only eight DFLs in Malaysia, this gives a ratio of one DF examiner to 525,000 people in Malaysia; that is 1:525,000! For comparison sake, the ratio of a doctor to the population in Malaysia is 1:632 [18]. The number of DF examiners in Malaysia's LEAs is obviously too low.

Interactions with LEAs found that that the biggest challenge for them to setup their own DFL is to convince management. The management views that they should rely on centralized DFL instead of having own DFL because of the high cost. They also view DF as a part of IT services, hence there is no need to have dedicated team to conduct DF cases. To date, no research has been conducted yet on the DFL topic in the Malaysian context. Hence, this research is conducted to understand the development of DFLs in Malaysia.

## IV. Research Objectives

This research has been conducted in order to fulfill the following objectives:

i. To understand the history and the issues in establishing a DFL,
ii. To understand current development of DFLs in Malaysia, and
iii. To gather the lessons learned as much as possible from each DFL that may be used by other LEAs in establishing a DFL.

The findings from the survey will be analyzed and put into a conclusion. The ultimate objective of this research is so that LEAs can use the findings to support their justification for having an in-house DFL to their management.

## V. Research Method

The researcher aims to study the development of DFL in Malaysia, the challenges and the need to have own DFL. The study compares perspective from different LEAs in Malaysia.

The method used in this research is by using structured interview method, using open and close ended questions. LEAs that owned a DFL shall be the target of this interview since researchers would like to explore on their experience of setting up a DFL. Their experience shall assist other LEAs in establishing a DFL. The respondents from each DFL are the Laboratory Directors and their staff.

Analysis will then be conducted on the answers and the results will be summarized into findings.

## VI. Result

Respondents' participation for this interview was 75%. Six out of eight LEAs owning a DFL in Malaysia have participated in the interview session. All respondents were the agencies' Laboratory Directors and the DF examiners.

The findings from the interview are summarized into five major findings.

*A. All of the Respondents (100%) Agreed that It Is Necessary to Establish Own DFL, Despite the High Cost, Due to the Increase in Cybercrime Cases. The DFL Shall Support the Case Investigation*

All respondents strongly agreed that LEAs must have its own DFL. The fundamental objective of them establishing their own DFL despite the high cost was because cybercrime cases were rapidly increased from year to year, hence they need to have own DFL to support their investigation instead of relying on a centralized DFL. Their number of case backlogs was also rising rapidly and exhibit storage size is becoming so massive due to constant technology advancement.

There were also sensitive cases as well as internal cases that they could not afford to send to other DFLs, hence the establishment of the DFL.

*B. Some 83% of the Respondents Agreed that by Having Own DFL, They Are Able to Get Faster Forensic Result and Meet Own Service Level Agreement (SLA)*

The majority of respondents agreed that prior to the establishment of their DFL they faced a challenge to meet up with their agencies' timeline expectations. Critical cases such as abduction of a child or domestic inquiry case involving top management required fast forensic results. But the investigation unit struggled to meet this because they had to rely on the SLA of other DFL, which on average was a minimum three months. A request can be issued to expedite the forensic results, but even when this was offered, their case would still be put into a critical case queue.

They could not afford to rely on other DFLs anymore since the process of managing and handing over digital evidence, i.e. transportation, registration, briefing session, to other DFLs, already took a lot of time, despite the criticality of the case.

Prior to the establishment of the DFL, criminal cases took longer time to solve. With an in-house DFL, now they were able to meet their own SLA based on priority of case.

The other 14% felt that their examiners are lacking the skill, hence sending the case to a national DFL may expedite the result. However, they agreed that, they were able to meet agency's SLA for critical cases with the establishment of the DFL.

*C. Some 67% of the Respondents Agreed that, Despite Sending Cases to a National DFL, Each LEA Must Have Its Own DFL Due to the Uniqueness of Each Case*

Some cases from different LEAs are unique and require niche skills and experience to discover the data and translate it into meaningful results. Hence, it requires a DF examiner with an investigative background in that subject matter of expertise (i.e. financial, pharmaceutical, accounting, veterinarian) to conduct the analysis.

Whereas in a national DFL such as CSM, the hired DF examiners are usually coming from computer and information background, therefore have limitations in producing more meaningful results when it comes to a certain niche subject matter. However, for complex cases that require research work or cases that involve new technology, all respondents agreed that they need to work together with a national DFL to solve them.

All of the respondents felt that it is appropriate to have a combination role of investigator and DF examiner, meaning to have their own DFL in LEAs due to following reasons:

1. Some Cases Require a DF Examiner to Have Specific Knowledge and Skill

A classic example is how money is being laundered. To analyze such case, it requires deep understanding and skill of both accounting and finance. Simply relying on keywords is not sufficient to analyze such cases. The DF examiner must have investigation skills as well as specific knowledge relating to money laundering.

Another example is the various terms used to refer to one drug, for instance 'Paracetamol'. 'Paracetamol' has various other terms such as 'PCM', 'acetaminophen', 'Panadol', 'pain killer' and many more. These terms are familiar to a pharmacist, but not to a computer expert.

2. A Person Who is a Certified DF Examiner but not a LEA Officer Might Lack a Criminal Investigative Background for Recognizing Evidence when They See It

Some DF cases require more than just conducting a keywords search. For example, extracting the motives behind the crime; what triggers the criminal? How it happened and when it happened? This may not be related to the listed keywords at all but the information is required in order to understand the chronology of events.

The experience and skills gained through the investigation process enables the analyst to produce better and more meaningful DF results. Not only that, it can reduce the risk of communication errors should the investigator submit the digital evidence to other DFLs for analysis. These findings, surprisingly, are aligned with the result of a survey conducted by Diana Tan in 2017 [19]. The still unpublished survey discovered that 68% from total of 103 respondents from LEAs of various countries agreed that it is appropriate to have a combination role of investigator and DF examiner for the same reasons.

*D. Half of the Respondents (50%) Agreed that the Biggest Challenge to Setup a DFL Was to Convince Their Management*

From the total six LEAs being interviewed, only three of them gained the full support of their management to establish a DFL. These LEAs took between two to three years to establish their DFL. These LEAs did not have any issue at all in establishing a DFL as well as procuring forensic equipment, maintaining license and attend technical trainings.

The rest of the LEAs, however, took quite a long time to establish their DFL - ranging from five to seven years. There was even one LEA that took 10 years to establish a DFL. The reason was because the difficulty in convincing their management.

Most of the management teams at these LEAs were not from a computer background. They viewed DF as part of IT services, and hence they did not see the need to setup a

dedicated team and laboratory.

They also faced difficulty to procure forensic tools as these procurements need to be reviewed and verified by the IT department, and most of the time the IT department lack of knowledge in DF. A classic example is procuring a forensic workstation such as FRED or a Talino. These machines are very expensive compared to a normal workstation such as DELL or HP, but they are able to conduct really fast keyword searches, are able to conduct simultaneous analysis on multiple hard disks and are stable enough to handle heavy loads; hence, saving a lot of time and cost. But since the price was really high, the procurement was rejected by the IT department.

*E. All of the Respondents (100%) Agreed that Cases Are Getting More Complex, Especially with the Involvement of New Technology. Continuous Purchases of New Equipment and Sending Staff for Training Are Inevitable*

All of the respondents agreed that cases they received were getting more complex and criminals were using more sophisticated tools to conduct crimes. All of the respondents agreed that a steady budget must be dedicated to their DFL on an annual basis for the maintenance and purchase of a new of DF equipment, and for trainings. Analysis could yield better results if the DFL has greater access to more sophisticated technology.

Without the budget, the DFL could not survive as most of DF equipment, especially forensic software, requires a yearly licensing fee. The hardware also requires some budget for maintenance, as certain parts such as cables and power supply would easily get damaged from a heavy usage.

## VII. Discussion

Although LEAs across the world are strengthening their DF capacity and capability, sadly in Malaysia, most LEAs still find difficulty in catching up. Despite the advancement of technology and the high Internet penetration in Malaysia [20], some are even struggling to convince their management the need to have a DFL.

A DFL is needed in order to analyze digital evidence in a secure and controlled environment. It is also important to analyze digital evidence in a DFL to eliminate the risk of contamination, hence making it admissible into the court with ease.

It is worth to mention here that some of the respondents faced difficulty to retain their staff. Due to career advancement, some of the trained DF examiners had to be relocated to other branches. Training new staff requires more budget and time, causing delays in the production of forensic results.

It is also worth to mention that all the established DFLs in Malaysia are located at headquarters, which means they are concentrated in the area of Kuala Lumpur and Selangor. There is no DFL at all in the 13 other states across Malaysia. To get a DF service, some of the investigators had to drive up to five hours to the headquarters with the evidence, and some even had to take flights, which is also costly and time consuming.

To justify the relevancy of a DFL to management, the respondents have shared some tips through the interview sessions. One of the methods is by calculating the number of man-hours taken to solve all DF cases against the fees that one needs to pay if the case is sent to private companies. Another one is to calculate the total of the money lost to the crimes submitted to the DFL. Some of the respondents also took a smart move by using critical cases or high-profile cases, when they were still juicy, to justify the need to setup a DFL, as well as to purchase more equipment or to add more DF examiners.

## VIII. Conclusion

The conclusion made from the study is the reason the LEAs established their own DFL was to assist their investigation. Due to the surge of cybercrime rates, they had no other option but to establish a DFL, despite the high cost. Some LEAs were taking painstaking years to setup a DFL, but eventually the DFL will be established.

By having an in-house DFL, the LEAs were able to produce faster results and they were able to meet their SLA, hence more criminal cases can be solved in a reasonable timeframe.

Lesson learned from this study shows that, other LEAs that are still considering the establishment of an in-house DFL, may want to start the process now since eventually the agency will inevitably need one. The researchers have shown the trend of LEAs at the global level as well as local LEAs to support this finding.

## References

[1] Ramendran, Charles. “Half billion ringgit losses due to surge in cyber crime”, *The Sun Daily*, March 5, 2018. Accessed May, 2018. http://www.thesundaily.my/news/2018/03/06/half-billion-ringgit-losses-due-surge-cyber-crime.

[2] Jay, Jay. “Cybercrime ranks among top three global risks in 2018, says WEF report”, Teiss Cracking Cyber Security, January 17, 2018. Accessed May, 2018. https://teiss.co.uk/news/cyber-crime-top-global-risk-wef/.

[3] Tan, Royce. “Cybercrime a serious threat to nation”, *The Star Online*, Sept 21, 2017. Accessed April, 2018. https://www.thestar.com.my/news/nation/2017/09/21/cybercrime-a-serious-threat-to-nation-malaysians-lost-rm1793mil-to-financial-crime-last-year-says-mi/.

[4] Latiff, Rozanna & Wagstaff, Jeremy. “Malaysia investigating reported leak of 46 million mobile users' data”, *Reuters*, November 1, 2017. Accessed May, 2018. https://www.reuters.com/article/us-malaysia-cyber/malaysia-investigating-reported-leak-of-46-million-mobile-users-data-idUSKBN1D13JM.

[5] Saieed, Zunaira. “Cybercrime surge in Malaysia”, *The Star Online,* May 20, 2017. Accessed April, 2018. https://www.thestar.com.my/business/business-news/2017/05/20/rates-of-cyber-crime-higher-now/.

[6] “More than 2,100 servers in Malaysia have been hacked, says cybersecurity agency”, *The Straits Times*, June 17, 2016. Accessed April, 2018. https://www.straitstimes.com/asia/se-asia/more-than-2100-servers-in-malaysia-have-been-hacked-says-cybersecurity-agency.

[7] M. B. Mukasey, J. L. Sedgwick and D. W. Hagy, “Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition,” National Institute of Justice(NIJ). April, 2008. Special Report.

[8] S. Rekhis, J. Krichene and N. Boudriga, "Cognitive-Maps Based Investigation of Digital Security Incidents," 2008 Third International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, 2008, pp. 25-40. doi: 10.1109/SADFE.2008.20.

[9] W. E. Ringle, J. D. Franklin and S. C. Bell, “Searches and Seizures, Arrests and Confessions,” 2nd ed, C. Boardman Company, 1979, pp 138.

[10] J. Sammons, "The Basics of Digital Forensics The Primer for Getting Started in Digital Forensics" 2nd ed, Ed. Syngress, 2012, pp. 103-115.
[11] B. Carrier and E. Spafford, "Getting Physical with the Digital Investigation Process," International Journal of Digital Evidence Vol 2, 2, (Electronic version) Fall 2003.
[12] T. McEwen, "The Role and Impact of Forensic Evidence in the Criminal Justice System," National Institute of Justice, December 13, 2010.
[13] Garris, John, "Tackling the Unique Digital Forensic Challenges for Law Enforcement in the Jurisdiction of the Ninth U.S. Circuit Court," SANS Institute InfoSec Reading Room, November 17, 2017. https://www.sans.org/reading-room/whitepapers/legal/tackling-unique-digital-forensic-challenges-law-enforcement-jurisdiction-ninth-us-circuit-court-38145.
[14] J. Ashcroft, D. Daniels and S. Hart, "Forensic Examination of Digital Evidence: A Guide for Law Enforcement," National Institute of Justice(NIJ). April, 2004. Special Report.
[15] T. Wilsdon and J. Slay, "Digital forensics: exploring validation, verification & certification," First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05), 2005, pp. 48-55, doi: 10.1109/SADFE.2005.11.
[16] Quintiliano, Paulo & Costa, João & Deus, Flavio & de Sousa Junior and Rafael, "Computer Forensic Laboratory: Aims, Functionalities, Hardware and Software," 2013, doi: 72-75. 10.5769/C2013010.
[17] Malaysian Communications and Multimedia Commission. (2017). *Internet Users Survey 2017*. ISSN 1823-2523. Available from Malaysian Communications and Multimedia Commission Web site: https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/MCMC-Internet-Users-Survey-2017.pdf.
[18] Department of Statistics Malaysia. (2017). *Social Statistics Bulletin, Malaysia, 2017*. Available from Department of Statistics Malaysia Web site: https://www.dosm.gov.my/v1/index.php?r=column/pdfPrev&id=aktTTjhhRHd1aHBCZGF1N01aaTl3dz09.
[19] D. Tan, "Establishing A Digital Forensics Laboratory for Law Enforcement Agency: A Proposal for Ministry of Health, Malaysia," 2018, University College of Dublin, unpublished.
[20] Department of Statistics Malaysia. (2018). *ICT Use and Access By Individuals and Households Survey Report, Malaysia, 2017*. Available from Department of Statistics Malaysia Web site: https://www.dosm.gov.my/v1/index.php?r=column/cthemeByCat&cat=395&bul_id=bHBzbWxkWElxRDlmaU81Q3R2ckRkZz09&menu_id=amVoWU54UTl0a21NWmdhMjFMMWcyZz09.