Developing Guidelines for Computer Forensics Investigation in Indonesia

Irfan Syamsuddin

TABLE OF CONTENTS

Abstract

This research is inspired by the launch of the cyber crime unit of the Indonesian National Police last year. The function of the cyber crime unit is to respond computer crimes specifically addressed to Indonesia. The discussion is begun with computer crime issues and its impacts. Various security technologies are also described. It is then continued with a brief explanation of computer crime cases in Indonesia and how they damage Indonesian reputation in virtual world. To observe this, interviews with the cyber crime unit personnel are used to collect data. It was found that until recently there has been no proper digital evidence examinations conducted in dealing with those cases in court. It is realized by the cyber crime unit that computer forensics methodology is urgently needed to combat computer crimes and bring the perpetrators in court with intact digital evidence. However, there have been no guidelines that can be used by the cyber crime unit to assist them in conducting computer forensics investigations. This is become the main concern of this study. Therefore, this study is proposed to develop guidelines for computer forensics investigation as the starting point of the following steps. It is intended to assist the cyber crime unit of the Indonesian National Police to conduct effective computer forensics investigations in Indonesia.

Keywords: computer forensics, digital evidence, computer security, cyber crime, computer related crime.

List of Figures

List of Tables

Chapter 1 Introduction

1.1. Background to the Research

Several decades ago, people could not imagine that computers would become the most important tools in human lives. Government institutions, business organisations, from small to large scales, academic institutions, and individuals heavily rely on computer technologies. This trend is also influenced by the fast growing area of computer technologies, both hardware and software, which has become part of the life style this century. In short, computers bring advantages in simplifying people's tasks in many aspects of life.

Nevertheless, it is widely cited that computer related crimes has become main issues of today's society due to its impacts. This is a real fact that computer technologies do not only offer effective and efficient way to deal with life, but also have a potential risk. Large business organizations and individuals have experienced hazardous impacts of misused technology. Credit card fraud, viruses, web hacking, and other terms of computer related crimes have been widely exposed and studied in recent years. Huge financial losses have been regularly reported. This is an obvious sign on how risky interconnected computers on the Internet are nowadays. Many criminals use computers to conduct traditional crime because they difficult to detect and can be done remotely (Wall, 2001).

On the other hand, many security technologies are developed in order to deal with digital crimes. However, recent experiences show that there has been no individual technology that could perfectly combat the increasing types and number of computer crimes. Therefore, it is widely argued that computer crimes could not be fully addressed by sophisticated security technologies and there would always be possible security holes that could be exploited by criminals.

It is believed that computer forensics could fulfil the limitations of security technologies and prosecute undetected computer criminals. Computer forensics combines the technical aspect of computer technologies, legal considerations and the management of digital evidence. It is a method of examining computer crime and retrieves electronic evidence to be presented in court.

However, if the investigation is not conducted appropriately based on clear guidelines, then the results are likely to be difficult to present in court. This means prosecution could not be established. Therefore, any institutions that deal with computer forensics investigations should put the guidelines in place as a priority step in securing computer and information systems.

1.2. Research Topic

This research supported by literature reviews taken from books, journal articles and other academic resources as well as results of interviews. Based on those, this study will cover several essential areas to address the research questions.

The first topic of research concerns the nature of computer crime in Indonesia. Types of computer crime are sometimes different from one country to another. Computer crime also influenced by the growth of the Internet users, availability of law in particular country, and government support. Therefore, these factors should be searched and collected. It would be meaningful to assist further discussion and analysis.

The next topic is related to international guidelines from computer forensics organizations and experts. Understanding the scope of each guideline will benefit to this research in terms of meeting the appropriate guidelines for the object research. Advice from computer forensics experts is required to be used as additional resources to broad perspective about computer forensics guidelines.

The final topic is the proposed guidelines as the outcome of this dissertation. It begins with the importance of guidelines in assisting computer forensics investigators. It is the followed by the guidelines that covers all aspects of computer forensics.

1.3. Research Approach

This research is based on the requirement of developing effective computer forensics investigation team in developing countries. The chosen research object is the cyber crime unit of the Indonesian National Police at which intensive interviews are carried out. The reason of choosing it because the Indonesian National Police has just been developed the cyber crime unit that is expected requiring supports from academic point of views. This study is conducted to give positive contribution for the cyber crime unit in handling cyber crimes investigation based on computer forensics frameworks.

Further research is conducted by reviewing various literature reviews from journal articles, textbooks and web sites. The aim of this stage is to obtain wider perspective about the topic, what developments have been made in the chosen topic as well as revealing any gaps where more research required.

Several guidelines that are already available are considered as useful resources to enrich the research analysis and final discussion. Together, this will form fundamental framework to build guidelines to assist the cyber crime unit of the Indonesian National Police.

1.4. Structure of Dissertation

The dissertation is divided into eight chapters. Chapter 2 explains in depth the literature review on computer security and it is followed by clear explanations about computer forensics. The significance of this research is explained in chapter 3. This includes the impact of cyber crime and its relation to the computer forensics requirements, benefits to be gained from this research, and implications without computer forensics.

Subsequently, chapter 4 describes the chosen research method that is qualitative based supported by data gathered via interview. Other research methods are also discussed in this chapter to be compared with chosen methodology. Chapter 5 deals with organisational context of research that briefly describes the cyber crime unit of the Indonesian National Police where data for this dissertation is collected. After that, an analysis of the collected data is discussed in chapter 6. Next, chapter 7 contains the proposed guidelines that were developed after extensive research. Several international guidelines are combined in this chapter. Finally, chapter 8 contains summary of the dissertation as well as the limitations. It also explores possible further research taken from this study.

Chapter 2 Literature Review

2.1. Chapter Introduction

This chapter discusses the structure of the Internet particularly the TCP/IP protocols. In addition, the weaknesses of the Internet structures will be described and analysed to meet correlation with increasing computer crime attacks. This chapter is ended with brief description of computer forensics and digital evidence.

2.2. Structure of the Internet

The Internet has experienced a dramatic change in the last two decades. Previously, services available for users were electronic mail, ftp and www. In contrast, the Internet today also includes various multimedia facilities such as teleconference, video steaming and many other services. As a consequence of the booming number of the Internet users in the last several years, significant changes of the Internet have occurred and it has to become more complex.

The physical structure of Internet is based on connection between server and clients such as local area network (LAN) where the server provides information to be accessed by clients. It is then developed into wide area network (WAN) as the connection of several LANs, and then continues to build metropolitan area network (MAN). Now, the Internet is a vast global connection of many computers around the world. Anyone can be directly connected to the global network (Internet) simply with telephone connection to an Internet Service Provider

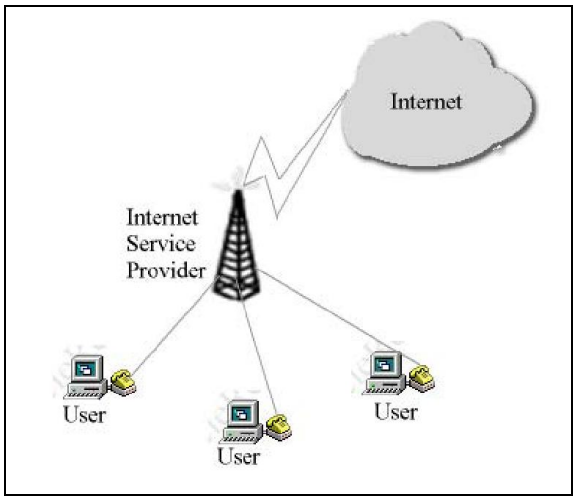

Figure 2.1. The structure of Internet connection with ISP.

For home users, Internet Service Providers (ISPs) offer various ways to get connected to the Internet from dial up (telephone line), broadband, to wireless connections. It simplify individual personal computer to be instantly connected to worldwide computer networks (figure 2.1). In addition to the physical structure, the structure of Internet also can be viewed from domain name structure.

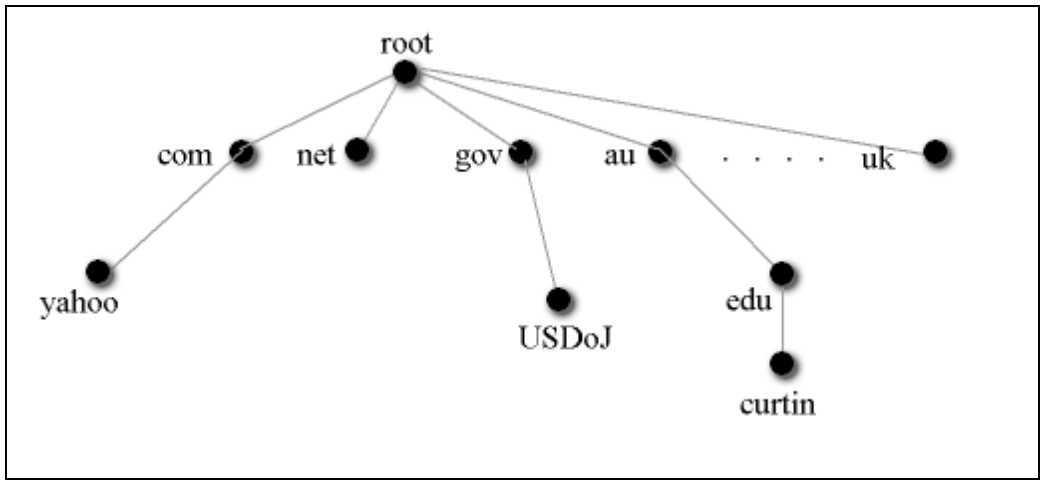

Figure 2.2. The structure of Domain Name Space.

Adapted from: http://www.cs.colorado.edu/~tor/sadocs/dns/

As can be seen from the graph, there are several levels of domain name space. They are root level domain at the top, continued by top level domain (.com, .net, .au and .uk) and the level domain (www.yahoo.com and www.usdoj.gov). Besides, there is also nation based domain name such as .au for Australia and .uk for the United Kingdom.

To discuss deeply about the structure of the Internet, fundamentals of the Internet architecture will be explained below.

2.2.1. Internet Protocols

Due to inflexibility of computers, specific rules called protocol are needed to enable them directly communicate each other. TCP/IP is the basic of the Internet protocol regardless of different types of computers and LANs. In short, various computer networks can communicate via TCP/IP protocol.

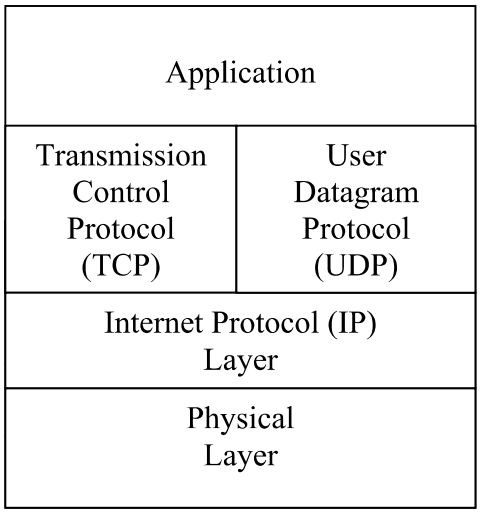

Figure 2.3. TCP/IP layers.

Source: Merkow & Breithaupt (2000), The Complete Guide to Internet Security.

As can be seen from figure 2.3., TCP/IP is derived from open system interconnections (OSI) that use four layers to transmit packet data over the Internet. The four layers are:

- Physical layer
- Internet Protocol layer.
- Transport layer consist of TCP and UDP
- Application layer with HTTP, Telnet, FTP and SMTP.

From the transmitter side, each layer transmits packet data from the previous layer to the next one while giving additional headers as a sign of each packet. On the other hand, the receivers obtain packet data based on these with headers. Finally, the actual data appears in the application layer (Tittle, 2001).

The specific characteristic of the Internet protocols is that they are public domain and how they work is published freely and can be used by anyone. In addition, checksum not only applies to the headers of a packet but to the entirely packet. These are considered as hidden holes that could be utilized for inappropriate computer use (Merkow & Breithaupt, 2000). It is clear that due to security holes already exist within the TCP/IP protocol, there is a security problems faced by everyone using the Internet (Peter Dell).

2.2.2. Internet Vulnerabilities

It is clearly known that the Internet applies an open standard of computer connection and communication. Hence, vulnerabilities of such communication cannot be avoided. Besides, it has been proved that basic development of Internet protocols is only to robust packet data transmission and there was only little concern about security (Merkow & Breithaupt, 2000).

As described in the previous section, TCP IP is considered as a key factor of the Internet weaknesses, there are also several factors of Internet vulnerabilities:

- Complexity of configuration

  “Many companies and individuals connect systems to the Internet with little thought to the complexity of system administration and the increased potential

contact, and also it is relatively cheap compared to traditional terrorist methods (Denning, 1999).

Insecure information technology infrastructure is also another attractive chance for cyber terrorists to show their abilities to create mass disruption. Sofaer and Goodman (2001) convinced that there have been many warnings about cyber terrorist threats, however collaborative actions to deal with it are still limited. Consequently, transnational responses by many nations around the world should be done intensively to counter cyber terrorism (Sofaer & Goodman, 2001).

2.4. Computer Crime Trends

Most computer crimes take advantages of the Internet vulnerabilities. Due to the openness of the Internet connection, it is likely to become a wide door for intruders to conduct attacks from outside of the systems. Related to this, it is reported that there has been a significant increase in the percentage of computer attack using the Internet as a gate (figure 2.5).

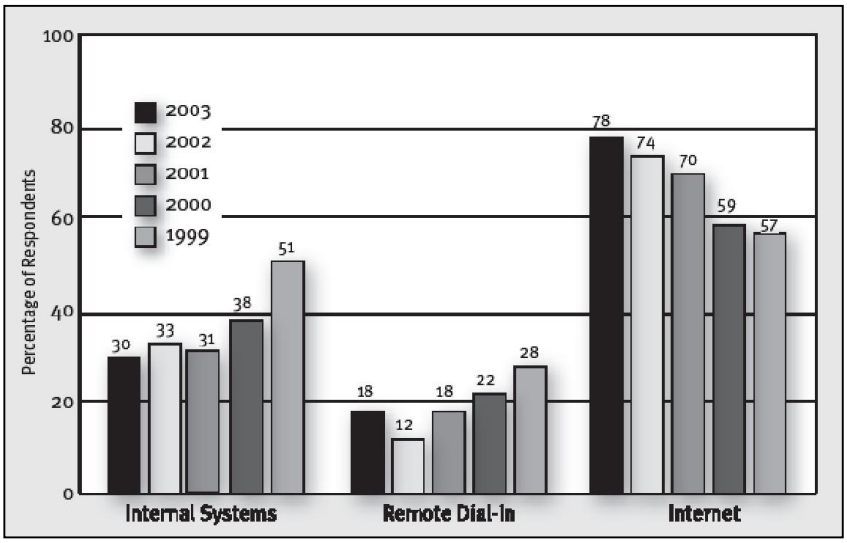

Figure 2.5 Points of computer attack

Source : CSI/FBI (2003), Computer Crime and Security Survey

The above graph shows the percentage of respondents who experienced computer attacks from three different points of attack: Internal Systems, Remote Dial-In and the Internet from 1999 to 2003.

It is clearly shown that the Internet is cited as the most frequent spot of attack to the respondents' systems, compare to two other types of connection. In addition, while Internal Systems and Remote Dial-In experienced a fluctuation in the percentage of points of computer attack, the Internet clearly shows a significant improvement during the period of 1999 to 2003. For example, there was a decrease by 10% of Remote Dial-In from 1999 to 2003. Similarly, the percentage of Internal Systems dropped from 51% in 1999 to 30% in 2003. In contrast, the percentage of the Internet as the frequent point of attack jumped from 57 % to 78% in 2003. Therefore, there should be a big concern for improving security guards on the Internet connection.

Along with the number of computer attacks, its type also varies from system penetration that has minimal impact to denial of service that can cause harm to large scale systems. Such crimes also cause financial loss both for individuals and even more for business organisations.

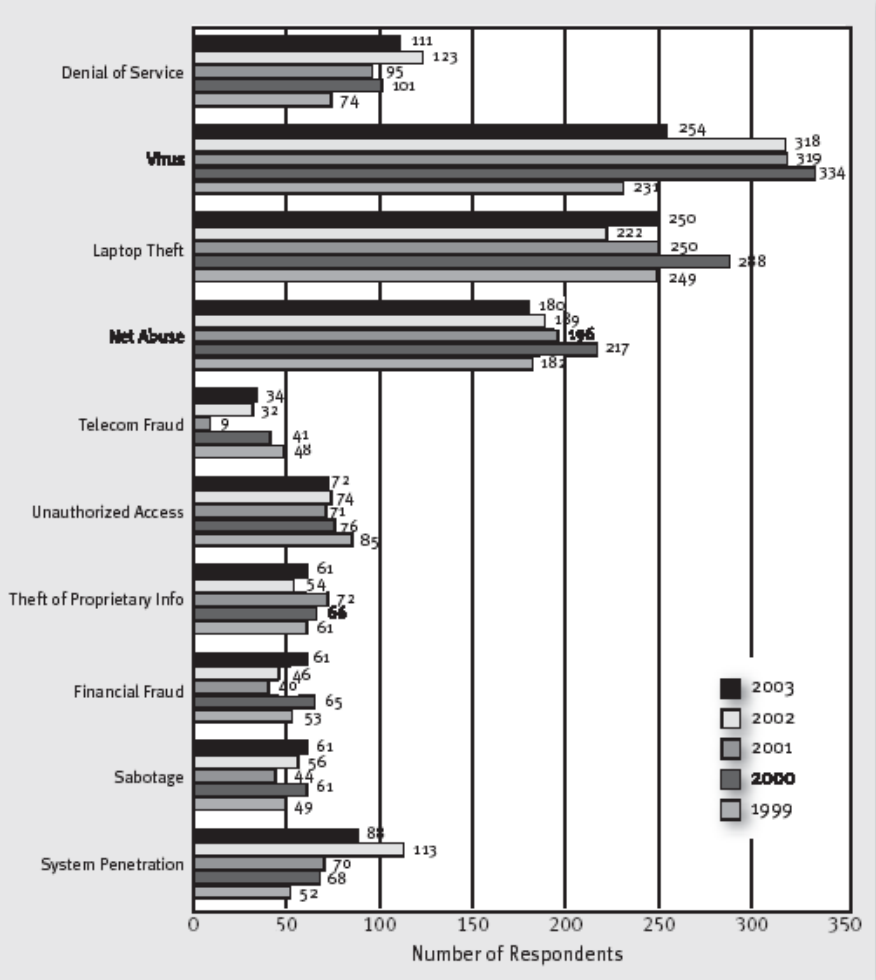

Figure 2.6. Types of attack in organisations reporting financial loss (by number)
Source : CSI/FBI (2003), Computer Crime and Security Survey

Likewise, reports from the Centre for Emergency Response Team (CERT) at Carnegie Mellon University found that there was a large increase in the number of computer crime incidents over the past decade.

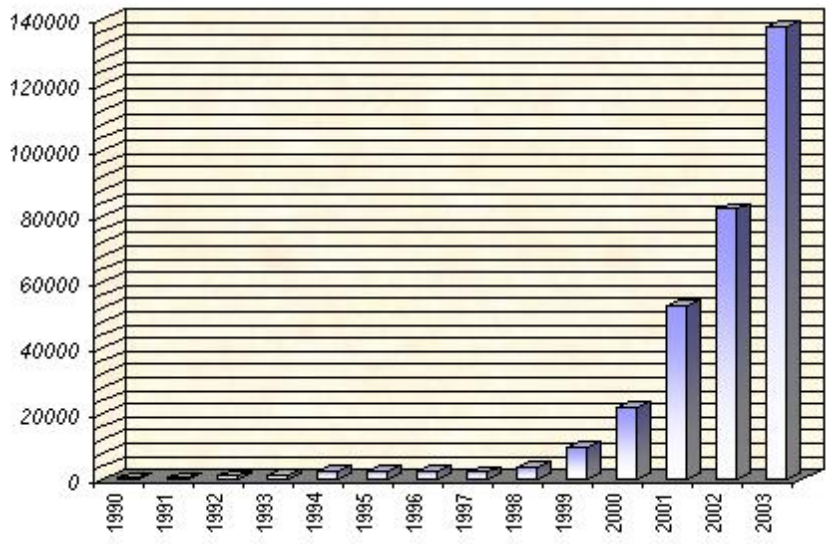

Figure 2.7 The number of computer crime incident from 1988 to 2003
Adapted from: CERT (2003), CERT/CC Statistics 1988-2003.

The latest security report (figure 2.7) from CERT shows that there has been a dramatic increase in the number of computer crime attack particularly since the beginning of the 21st century. In the period 2001 to 2003, the number of such incidents has risen significantly to less than 140,000 cases, more than twice as many as in 2001.

Studies by CERT about the trends of computer crime have concluded some points. The most important point is that there are several factors involved in the increasing number of computer crime incidents as follows:

2.4.1. Increasing Sophistication of Attack Tools

Attack tool developers are using more advanced techniques. Attack tool signatures are more difficult to discover through analysis and more difficult to detect through signature-based systems such as antivirus software and intrusion detection systems.

There are three important characteristics in this issue: anti-forensic nature, dynamic behavior, and modularity of the tools.

• Anti-forensics.

"Attackers use techniques that obfuscate the nature of attack tools. This makes it more difficult and time consuming for security experts to analyze new attack tools and to understand new and rapidly developing threats. Analysis often includes laboratory testing and reverse engineering" (Householder, et.al , 2002:5).

• Dynamic behavior.

"Early attack tools perform attack steps in single defined sequences. Today's automated attack tools can vary their patterns and behaviors based on random selection, predefined decision paths, or through direct intruder management" (Householder, et.al , 2002:5).

• Modularity of attack tools.

"Unlike early attack tools that implement one type of attack, tools can now be changed quickly by upgrading or replacing portions of the tool. This causes rapidly evolving attacks and, at the extreme, polymorphic tools that self-evolve to be different in each instance" (Householder, et.al , 2002:5).

2.4.2. Faster Discovery of Vulnerabilities

There is a new trend that vulnerabilities can be discovered in a faster time. It is possibly due to the increasing demand of particular software which leads to less software control and testing before being available to the public commercially (Householder, et.al , 2002:6).

As can be seen from figure 2.8 below, there has been a dramatic increase in the number of reported software vulnerability, particularly since 2000.

How money was lost	Respondents with quantified losses		Lowest reported		Highest reported		Average loss		Total annual loss	
	2002	2003	2002	2003	2002	2003	2002	2003	2002	2003
Theft/breach of proprietary or confidential information	4	7	10,000	3,000	150,000	150,000	72,500	36,857	290,000	258,000
Unauthorised privileged access	8	10	1,000	1,000	50,000	200,000	13,275	32,200	106,200	322,000
Financial fraud	7	8	500	10,000	600,000	1,400,000	115,288	440,625	807,000	3,525,000
Telecommunications fraud	2	6	1,000	200	100,000	250,000	50,500	69,200	101,000	415,200
Sabotage of data or networks	5	3	1,000	5,000	1,000,000	100,000	204,600	41,667	1,023,000	125,000
Web site defacement	-	8	-	500	-	30,000	-	7,313	-	58,500
Denial of service attack	8	16	1,500	300	100,000	200,000	22,688	24,831	181,500	397,300
Degradation of network performance associated with heavy scanning	7	14	1,500	1,000	100,000	200,000	23,071	37,729	161,500	528,200
Wiretapping	1	0	1,000	0	1,000	0	1,000	0	1,000	0
Telecom eavesdropping	1	1	10,000	4,000	10,000	4,000	10,000	4,000	10,000	4,000
Virus, worm, trojan infection	23	66	100	200	100,000	400,000	38,743	33,695	891,100	2,223,900
Laptop theft	48	82	2,000	1,999	100,000	350,000	26,331	27,539	1,263,900	2,258,183
System penetration by outsider	7	7	1,000	2,000	40,000	50,000	26,143	21,571	183,000	151,000
Unauthorised access to information by insider	5	3	5,000	2,000	100,000	250,000	29,000	87,333	145,000	262,000
Insider abuse of internal computer resources, access or e-mail	17	30	100	500	200,000	400,000	36,300	42,417	617,100	1,272,500
Total annual losses	2003: 126 respondents/58%; 2002: 75 respondents/80%								5,781,300	11,800,783

Figure 3.2. Total amount financial loss from computer crimes in Australia

Source : AusCERT (2003), Computer Crime and Security Survey.

Similarly, this survey found that financial fraud, laptop theft, virus, Trojan and worm were the largest sources of financial loss from 2002 to 2003. The amount of total annual loss due to financial fraud increased more than four times from AU$ 807,000 in 2002 to AU$ 3,525,000 in 2003. Likewise, virus, worm and Trojan were responsible for the increasing total annual loss by almost 250% from only AU$ 891,100 in 2002 to AU$ 2,223,900 in 2003. This trend was followed by laptop theft which is cited as the source of more than AU$.258 million total financial loss in 2003.

In brief, the total amount of financial loss has experienced a significant increase from AU$ 5,781,300 in 2002 to AU$ 11800783 in 2003. This number is clear evidence that many organisations in Australia are still under the threats of computer crimes even though some security hardening tools have been provided such as firewalls and intrusion detection systems.

This report confirms that the applications of various security technologies could not prevent financial loss during the period. This is a big question to the quality of such security hardening tools.

3.3. The Importance of Research

Based on the fact that computer crimes still become a nightmare for organisations utilizing information technology in operation, any attempts aimed to analyze and solve the problems are encouraged and highly required. Research in the area of computer and information security has been done intensively in recent years, although they could not address security problems at all. Therefore, computer forensics as new field can be offered to answer security technologies' lack in presenting cyber crime perpetrators in court.

In particular, the importance of this research can be viewed from where the data is taken from. The data is mostly picked up from the Indonesian National Police that has begun to be concerned with computer crime in which Indonesia is sometimes cited in several international security related publications.

A recent 2004 survey conducted by Verisign shows that Indonesia is the top of ten countries in terms of fraudulent transactions on the Internet (figure 3.3). However, it is also noted that even though the original country's specific IP address is suspected in this survey, it is also possible that hackers from other countries utilize them to conduct cyber crimes.

Top Countries[3] By Percentage of Fraudulent Transactions

Country	Ranking
Indonesia	1
Nigeria	2
Pakistan	3
Ghana	4
Israel	5
Egypt	6
Turkey	7
Lebanon	8
Bulgaria	9
India	10

Figure 3.3. Top ten countries of fraudulent transaction

Source: Verisign (2004), Internet Security Intelligence Briefing January 2004.

Based on the fact, both limited technical resources for security and inadequate security awareness is cited as the basis of high security breaches addressed to Indonesian IT infrastructures. Therefore, the Indonesian government should be concerned about this condition and work together with others in combating cyber crimes.

In addition, information and communication security is already a worldwide issue. Therefore, Indonesia should involve in this area by supporting information sharing with other security related institutions in different countries.

Without computer forensics methodology, evidence examinations could not establish. This result is misconduct of investigations or difficulties in proofing the evidence of computer crimes. Although digital evidence could be gathered, there is no adequate method to examine the intact of that data. As a consequence, perpetrators of computer crime are might untouchable (Casey, 2002a).

3.4. Benefits of the Research

The benefits of this research at least can be viewed from education and guidelines development.

- Education

In terms of educational perspective, this research is supposed to give positive contribution to the following parties. There are four main benefits of this research.

Firstly, benefits for general computer users. They need skills on how appropriately to use the computers both software and hardware as well as power supply and knowing what to do if the computer crashes. Therefore, basic knowledge of computer forensics such as steps to deal with computer failure and how to avoid it are very useful.

The next benefits are to professionals such as network administrators and programmers. The ongoing research of security and computer forensics is useful for this group as they are responsible to provide comfortable computer facilities such as computer network and the Internet connections. It is widely cited that Internet link is the highest source of computer attacks, therefore knowledge and skills to provide safeguard is the most important aspect for them. As a result, security and forensics are highly valued by them.

The third benefit can be gained by law enforcements. This group needs clear understanding on how to deal with cyber crime with digital evidence, regardless location where they deal with the real problems due to the increasing cyber attacks in recent years. It is not only for those who live in the developed country such the United States, the United Kingdom and Australia who face the cyber crime problems, their counterparts from developing countries such as in Asia and Africa also deal with similar troubles. Therefore, knowledge and experience sharing is urgent in order to deal with cyber crimes which possibly involve many people from different countries. Accordingly, research in computer forensics and security is urgently required to combat the dynamic forms of cyber crime.

Finally, this research will benefit students and academics that are enthusiastic to improve skills to answer the escalating cyber crime problems. Until recently, there is little academic research done in this area. While only limited academic institutions have attempted to provide courses and research in computer forensics area, the academic resources are also limited. Therefore, various research perspectives would improve computer forensics study.

- Guidelines Development

The main aim of this research is to offer affirmative contribution for law enforcement in Indonesia in computer forensics investigations. The whole picture of computer forensics investigations should be specified to help them understanding the importance of computer forensics.

As a developing country with numerous internal and external problems, the Indonesian government cannot cope all aspects including cyber crime issues. In 2003, the Indonesian government through the Indonesian National Police established a cyber crime unit that responsible in handling computer related crimes. Previously, computer crime cases are handled like other criminal cases. Therefore, the cyber crime unit is expected to handle such cases in a better way. However, lack of skills and facilities as well as unavailability of clear and well-explained guidelines have been considered as the main reasons of ineffective outcomes of their operations.

work place). On the other hand, around twelve percent of them employ private Internet connection at home and the rest use computer facilities at schools.

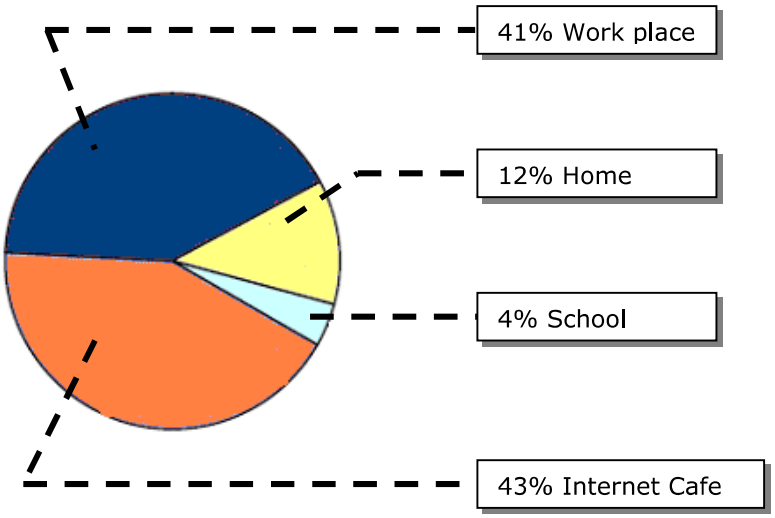

Figure 6.2. Percentage of source Internet access.
Source : APJII (2003), Statistic of Internet User 2003.

The last characteristic is based on age ranges. As can be seen from figure 6.3, these can be categorized as three groups. The group of age 20 – 29 is believed to account for approximately 40% of all Internet users. This number is followed by the group of age between 30 and 39 who about 35%. Conversely, those at the age of 19 accounted for about 15% while the two other groups are only 9% and 1%.

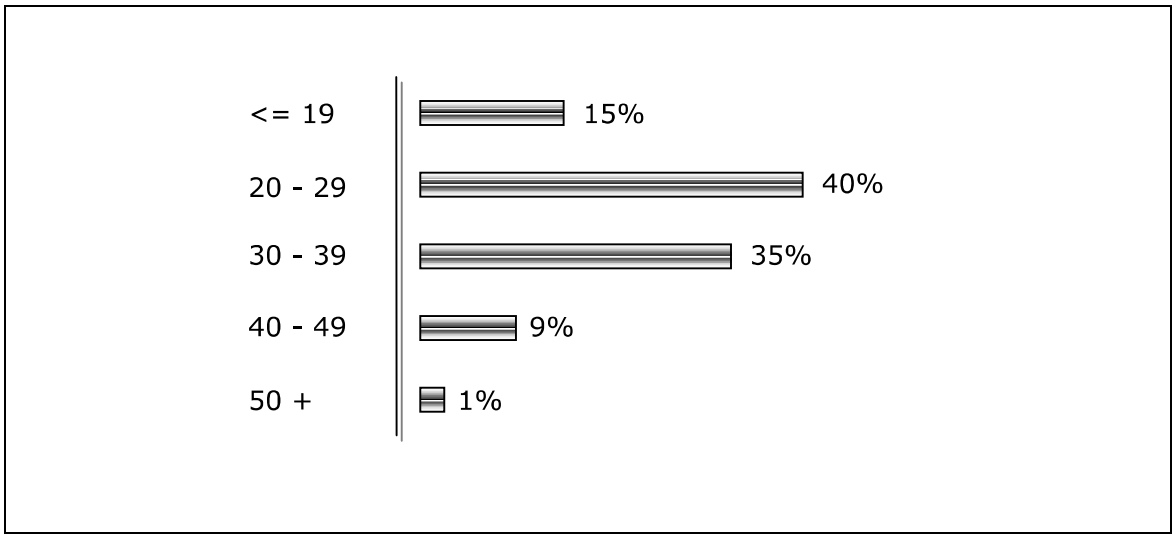

Figure 6.3. Percentage of users based on age.
Source : APJII (2003), Statistic of Internet User 2003.

Those three characteristics are drawn as the background in conducting a breadth and depth discussion about computer related crime incidents, addressed to Indonesia.

In terms of computer crime, it is confirmed that until recently there has been no absolute statistic results that combine all information about types of computer crime and its percentage. Prior to the development of the cyber crime unit, there have been several cases related to computer crime activities brought to court by the police and law enforcement in Indonesia using conventional law.

The type of computer related crime cases and its amount in Indonesia could be seen in table 6.1.

No	Type of Crime	Amount each year		
		2001	2002	2003
1	Online Fraud	1	1	1
2	Web defacement	> 200	> 500	> 600
3	Credit card fraud	85	115	202
4	Pornography	4	8	13

Table 6.1. Amount of computer related crime cases in Indonesia from 2001 to 2003. Source: The Indonesian National Police

As can be seen from the above table, there were four types of computer related cases in Indonesia reported during the period of 2001 to 2003. They are online fraud, web defacement, credit card fraud and pornography which will be described more deeply.

- **Online fraud**

  Online fraud refers to any activities regarding web content deception or illegal online activities. There are one case related to this particular matter in 2001, 2002 and 2003 (table 6.1).

  The first case in 2001 was Internet banking fraud suffered by Bank Central Asia (BCA) located in Jakarta. It occurred when BCA announced implementation new online banking system that enabled their costumers to perform their transactions online via www.klikbca.com .

  The management argued that the system was secure enough to protect digital transactions as security hardening tools were implemented such as firewalls and 128 bit Secure Socket Layer. In fact, this was not completely true since someone then publicly announced a week after, that he had obtained several Personal Identification Number (PIN) codes and passwords of BCA's consumers. His aim was to inform the

bank management that what they promote about security of their online banking system was not completely true (Detik, 2001).

The perpetrator convinced the bank that the systems could still be cheated by registering two domain names called www.kilkbca.com and www.klikbac.com (slightly different from the original domain name www.klikbca.com). In addition, these two domain names have similar frontpage to the original one operated by BCA (www.klikbca.com). BCA's customers who mistype the domain name would find the same frontpage which was in fact a replication one. While they were doing transactions, PIN numbers and passwords were directly sent to the perpetrator's database as well as to BCA back end system. Due to the perpetrator's aim is considered as non criminal intention, but informing the importance of security especially to the bank institution, therefore there was no prosecution (Detik, 2001).

The second case in 2002 is related to domain name as well. Mustika Ratu, a large Indonesian cosmetic industry wanted to register its domain name. However, the domain name called www.mustikaratu.com was already registered by someone from Indonesia. It was advised that the only way to get the name was by buying the name from the recent owner at higher value.

On the other hand, the company considered it as an illegal action against the law. Thus, the case was brought to court and the result was that the domain name should be given to the company while the first registrar received as much as its original price (MediaIndonesia Online, 2003).

The third case occurred in 2003, regarding online gambling operated by someone who hosted www.tebaknomor.com outside of Indonesia. It was found that this web site had attracted young people to perform gambling online. By law enforcement, it was stated as an illegal activity because there was no licence given to the operator to

run the business. Nevertheless, due to limited facilities and cooperation, the perpetrator could not be identified and the systems are still alive until now. As, a result this case is then closed without further investigations (Gatra Online, 2004).

- **Web defacement**

  Web defacement is the most frequent case found in this study (table 6.1). This is divided into internal and external cases (table 6.2). While internal cases refer to local perpetrators who deface either local or international web sites, external cases refer to attackers from outside Indonesia who deface Indonesian web sites.

  As can be seen from table 6.2, there has been a dramatic change in the percentage of web attack sources between external and internal from 2001 to 2003. Overall, internal attack shows a dramatic increase since the middle of this period.

Year	Percentage source of attack	
	Internal	External
2001	20%	80%
2002	58%	42%
2003	65%	35%

Table 6.2. Percentage of web defacement attack sources

Source: The Indonesian National Police

In addition, internal attacks represented only about 20% of the whole web defacement attacks on Indonesian web sites in 2001. Conversely, in 2002 the pattern changed where attack from inside was almost three times to 58%. In addition, this trend continued to increase in 2003 to 65%.

- **Credit card fraud**

  Credit card fraud is the second biggest case of computer crime in Indonesia. Besides, it is sometimes reported that carders (a terms for person who conducts

credit card fraud) from Indonesia are also responsible to huge financial losses in electronic commerce transactions in the world since 2002 (Verisign, 2003). Chat rooms are usually used by carders exchanged stolen credit cards.

The number of credit card fraud cases in Indonesia between 2001 and 2003 can be seen from table 6.1. In general, there is a gradual increase in the number of credit card fraud cases in the period. Whilst, there were 85 cases accounted by police in 2001, the number was up to 115 cases in 2002. In addition, this continued to increase to hit approximately 202 cases reported in 2003. However, from all cases reported to police, there is only less than 50% of cases which could be revealed. The main reasons are inadequate technology and skills of police in dealing with such criminals. In addition, less cooperation with other professional organization, is also cited for why such criminals difficult to catch.

Unfortunately, the police still use conventional ways to perpetrators of such illegal activities. Usually, the investigations begins after receiving complaint reports from those who suffered from credit card fraud then matching it with reports from public. Another useful source for investigators is taken from delivery companies such as UPS, DHL and Indonesian Post, that are always utilized by carders to receive stolen goods from fraudulent transactions using stolen credit cards. Based on this information, some perpetrators could be caught while others are still untouchable.

- **Pornography**

  Generally, pornography in any forms is illegal from the point of view of Indonesian law. However, this seems difficult to prevent particularly since many pornographic web sites are available on the Internet.

  As can be seen from table 6.1, the overall trend of Internet pornography in Indonesia experienced a slight increase between the period of 2001 and 2003. It is clear that there was a slight increase in the number of pornographic case from only 4 cases

- To provide guidance for computer forensics investigators on how to manage and prepare an effective investigation team as well as how to conduct cyber investigations.
- To acquire skills required for dealing with different types of environment where computer crimes occur.
- To be standard reference for each steps of an investigation processes.
- To minimize mishandling evidence that might result in dismissal from a court.

In short, the guidelines are intended to provide clear framework as standard operations for the cyber crime unit of the Indonesian National Police. It is expected that the guidelines will help the cyber crime unit to provide better investigations in the future.

7.3. Computer forensics preparation

Prior to conducting investigations, adequate preparations should be done in several levels such as team development, adequate education and skills and well maintained computer forensics laboratory and office.

7.3.1. Team development.

Human resources are the first stage to provide prior to any steps in this field. This is the most important step to fulfil before others. Computer forensics team or cyber crime unit in Indonesia consists of several staff members and a chief. Regardless of at what level this unit is in the police institution, it should be independent and free from intervention from any directions. The quality of result would depend on how independent the unit is in conducting investigations as well as the level of solidity between staff and chief. While, the chief is responsible to manage the team members based on the case they are dealing with, all staff should be eager eagerness to work together under the leader's supervision.

Digital crime investigation is a unique job that needs specific staff with particular professional skills. Due to its specification, there are several attitudes important to a computer forensics investigator as shown in figure 7.1.

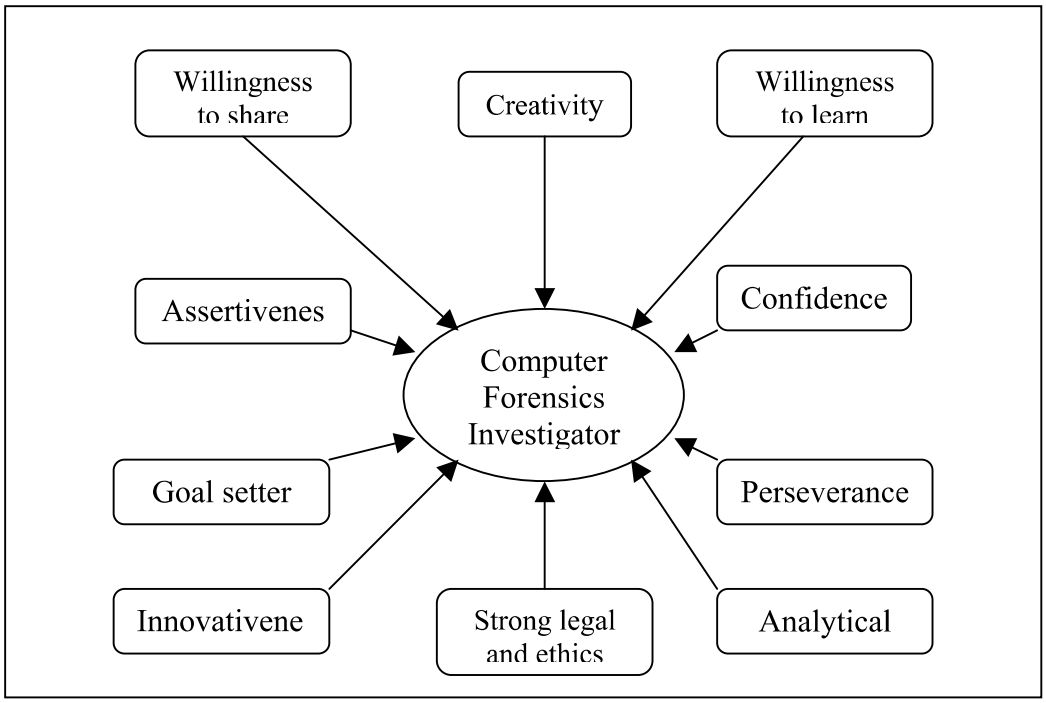

Figure 7.1. Attitudes desired of a computer forensics investigator.

Adapted from: Robbins,et.al. (1998), Organisational Behaviour; and Kneitner & Kinicki (1995), Organisational Behaviour.

Computer forensics investigators should have deep analysis skills and creativity as well as innovation in determining many possibilities of a particular case or a new case. They should also feel confident in investigating a difficult case resulting in difficult conclusions. At the same time, goal setting should be established in all situations as well as perseverance in any conditions.

Moreover, while computer forensics investigators should be confident, they should also have strong legal and ethics understanding. In order to improve skills and abilities, they should develop willingness to share and learn motivation regarding new cases and new technologies found by counterparts in other countries.

In terms of the cyber crime unit at the Indonesian National Police, staff recruitment for this unit is approved only within the police organization. It was found that there was no evidence that staff recruitment considering such necessary attitudes in selection. Besides, selection of cyber crime staffs are mostly based on computer skills they have and how interested they are to computer related cases. Under these conditions, the personnel are responsible to handle computer forensics investigation under the name of the cyber crime unit of the Indonesian National Police.

7.3.2. Education

To deal properly with specific problems, specific education and training are required, which is also true in computer forensics field. Unlike other field, computer forensics is the combination between many fields, such as information security, hardware and software computing, law and management. According to Yasinsac and others (2003), computer forensics education can be explored from two paradigms, namely technical and managerial aspects.

The first aspect deals with computer related subjects such as computer hardware, digital media, networking, and the Internet. On the other hand, the management aspect explores the non-technical side, such as investigation management, presentation, reporting, and cyber law.

It is recommended that all staff of cyber crime unit have fist undertake both aspects of computer forensics education. This is to develop comprehensive understanding of how to deal with computer crime under good management rules.

Hannan and others (2003) confirm that within the context of forensic computing investigation, “skills may include (but not be limited to) a methodological approach to the investigation, interview communication techniques, case management, preparation of court documentation, preservation of physical aspects of evidence and investigation, documentation of process, appropriate use of resources and critical thinking”.

According to Armstrong (2003), there are eight skills which are required by those who are responsible to conduct computer forensics investigations. The skills are "fundamentals of computer forensics, international guidelines and practices, different operating systems, structure of file systems, computer forensics tools and techniques, data recovery and evidence imaging, legal perspective and court proceeding, and finally expert witness role".

In addition, Armstrong and Russo (2004) affirm that proper computer forensics skills and knowledge to law enforcement should cover the following areas:

- "Handling of computers at the scene of a crime and the initial investigation of crimes where computer systems or other electronic devices may contain evidence. Therefore, basic knowledge and skills are required to deal with different operating systems and computer architecture, computer networking, as well as Internet functions that might be contain potential evidence.
- Producing verifiable images of electronic media and data for subsequent investigation. A detailed knowledge regarding computer and network hardware, wireless technologies, software, encryption, computer media forensics and operating systems is required.
- Retrieving evidence from computer systems and other electronic devices for prosecutions of crimes. To perform such actions, more detailed knowledge of computer hardware, wireless technologies, encryption hardware and software, computer media forensics, network architectures, application and operating systems, databases and Virtual Private Networks are required.
- Analysis and reporting of electronic evidence. Knowledge requirements for this including operating systems and software tools for computer forensics, standards, methodologies and approaches to evidence gathering and cases building, lateral thinking and problem solving techniques.

- Presentation of evidence and cross-examination in a court of law. This requires knowledge of criminal as well as civil law, past case history, operating systems and software tools for computer forensics, means of authenticating evidence, standards, methodologies, defensive strategies, and admissibility of evidence in court.
- Computer security measures to protect the integrity, confidentiality, and availability of their own computer systems and networks" (Armstrong and Russo, 2004:2).

Similarly, it is also advised that before dealing with the real computer crime scene, investigators should have knowledge and skills related to investigation management planning, storing and transporting digital evidence according to legal guidelines, various types of operating systems and applications, collecting, preserving, and analysing evidence of a computer crime incident, and updated computer forensics tools (Stephenson, 2000:225).

7.3.3. Office and Laboratory

Providing a special office and laboratory is a basic requirement for investigators. A sophisticated forensics laboratory will influence the quality of forensics investigators, because they are able to analyze the evidence in more detail.

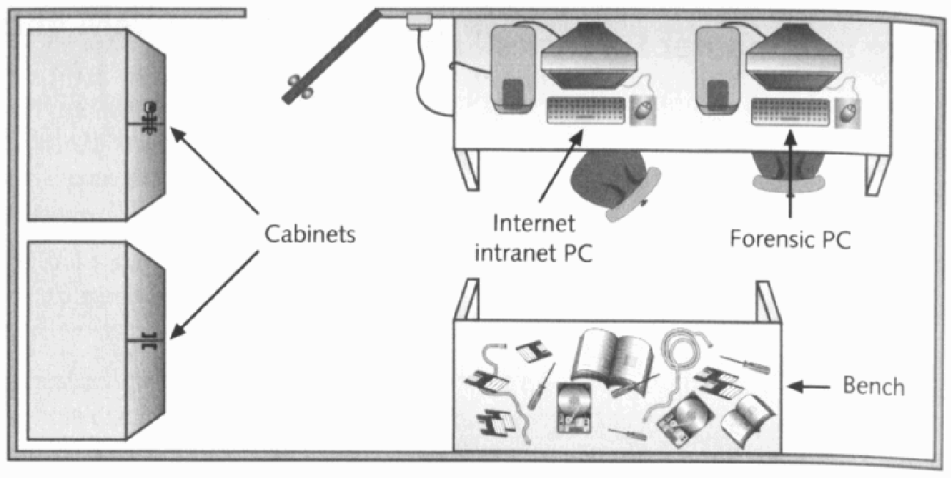

Figure 7.2. Small forensics laboratory

Source : Nelson et.al. (2004), Guide to Computer Forensics Investigations.

The above graph shows a model of a simple computer forensics laboratory. It consists of one PC for Internet/ intranet communication and another one used as a forensics PC. A larger laboratory needs more PCs for conducting forensics analysis, commonly called forensics workstations (Nelsons et.al, 2004).

If there are more complex investigations to be faced, then more sophisticated laboratory facilities should be provided, for instance providing more PCs for forensics workstations with different operating systems such as Windows, Linux, and UNIX (Nelsons et.al, 2004).

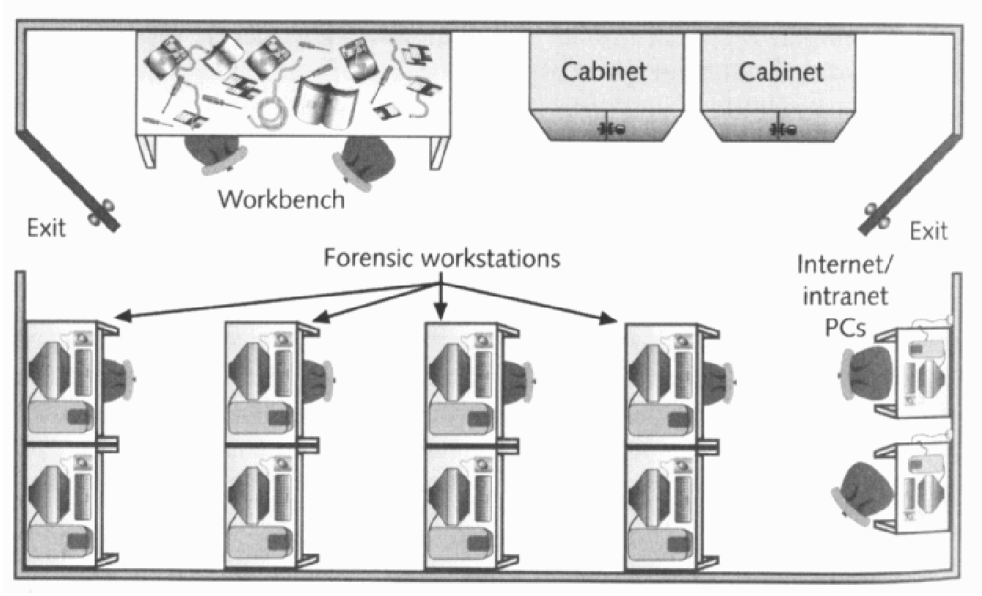

Figure 7.3. Larger forensics laboratory

Source : Nelson et.al. (2004), Guide to Computer Forensics Investigations.

The above graph shows a more complex laboratory for conducting complex investigations. There are more PCs with different operating systems are utilized for different sources of digital evidence.

It is advised that police departments in major cities have various hardware and software, from the old technology to the latest (Nelsons et.al, 2004). The reason is because they should be ready to deal with various machines with a range of software from the latest one to the newest. It is also recommended that for every 250,000 people in a geographic region, there should be at least one law-enforcement computer investigator PC (Nelsons et.al, 2004:184). This is to keep the quality of investigations.

7.4. Background of the Guidelines

When examining a computer setup, there are two general categories the examination: live/real-time examination or an off-line duplication. Which of these types is necessary depends on the situation. When dealing with a network intrusion or a server and network setup which cannot be made unavailable, live examination is the route taken. If total

the report of the case while determining evidentiary weight. However, all steps should always be under control to ensure comprehensive results.

To sum up, the following are five tables as summary guidelines of computer forensics investigations.

	Team Development	**Description**
	Human Resource Management	Managerial systems in recruiting members of the cyber crime investigator team
	Computer Skills	Technical computer skills as the basic knowledge in conducting cyber investigations.
	Law Skills	Knowledge of law regarding cyber crimes
	Attitudes	Desired attitudes for a member of a specific purpose team such as cyber crime investigator.
	Independence	The level of independence in revealing the fact of a computer related crime accident.

Table 7.1. Team Development Guidelines

	Laboratory Physical Layout	Description
	Appropriate Space	Space is required by the investigators to feel comfortable when carrying out an investigation.
	Appropriate Lighting	Lighting is also required especially when dealing with hardware based evidence.
	PC for Internet / Intranet Connection	Connection is required to get contact outside the office.
	PCs for Forensics Workstations	Forensics workstations are the most important facilities in the laboratory where all evidence are processed.
	Cabinets	Cabinets are used for storing everything related to the cases being investigated, to guarantee safety.
	Bench	This is the space where tools required for investigation process should be put.

Table 7.2. Computer Forensics Laboratory Guidelines

	Guidelines
1	Evidence identification
	- Identify possible evidence - Ensure the usability of evidence - Identify the author of the evidence
2	Records construction
	- Set up date and time of the environment systems - Document date and time of records, when they are created and or altered - Ensure the reliability of computer programs and application
4	Evidence acquisition
	- Collect evidence - Observe hidden files, unallocated and slack disk space - Create copy of the evidence - Do not work with the original evidence - Evidence tagging and tamper proofing - Document all processes
4	Evidence control
	- Best evidence rule - Chain of custody
5	Computer forensics analysis
	- Create copy image of original evidence - Examine data offset - Examine unallocated and slack disk space - Identify header value of files - Data recovery - Searching specific hexadecimal values - Verify the bit stream of image copy
6	Crime reconstruction
	- Interpret the crime - Story line of investigations - Chain of custody documentation
7	Reporting and presentation
	- Narrative report of the whole investigation - Informative presentation in layman's perspective

Table 7.3. Computer Forensics Processes Guidelines

Skills	
	Technical
	Computer Hardware (from old to latest technology)
	Computer Software (from various software)
	Operating Systems (Linux, Windows, UNIX, Mac)
	Network Architecture (TCP/IP, router, VPN, firewall, IDS)
	Network Technology (Cisco, Allied Telesyn)
	Databases (Oracle, Ms SQL, Postgre)
	Encryption (Symmetric, Asymmetric)
	Computer Media Forensics
	Computer Forensics Tools
	Evidence Authentication
	Non Technical
	Civil and criminal law
	Past case history
	Standards
	Methodologies
	Defensive strategies
	Evidence admissible in court

Table 7.4. Skills and education guidelines

7.6. Chapter Conclusion

Based on the research findings, it is suggested that guidelines should be firstly available to assist the cyber crime unit of the Indonesian National Police.

In short, the main proposed guidelines consists of seven steps, namely evidence identification, records construction, evidence acquisition, evidence control, computer forensics analysis, crime reconstruction and reporting and presentation. Besides, there are also several additional guidelines that are considered necessary to have, for example team development guidelines, computer forensics laboratory guidelines, and skills and education guidelines.