A Study on Secure Communication for Digital Forensics Environment

Yudi Prayudi, Ahmad Ashari

Abstract— The growth of information technology and the complexity of cybercrime, requires digital forensics activities that are interconnected. This needs to be supported by a secure communication channel. Security and trust are an important issue in digital forensics because it would be associated with integrity and authenticity of digital evidence. The use of a VPN technology either through SSL or IPSec protocol can serve as a solution to fulfil the needs of secure communication. Based on the characteristics, IPSec is more appropriate to be used as a connection between the law enforcement offices which are located site-to-site, while SSL VPN can be used as a solution to the needs of remote access to support mobility of the first responders/digital investigators.

Index Terms— *Secure Communication*, *Trust System*, *VPN*, *IPSec*, *SSL*, *Digital Forensics*

1 INTRODUCTION

According to [1], digital forensics is the use of scientific methods in the investigation process of digital evidence in an attempt to understand and reconstruction of an event. While according to [2], digital forensics is the use of science and methods for finding, collecting, securing, analyzing, interpreting and presenting digital evidence related to the case happening for the reconstruction of events as well as the legitimacy of the judicial process.

To perform event reconstruction, each stage and activities of the digital forensics are supported with high qualification of individual's ability and availability of a variety of tools. There are many different types of tools to support digital forensics activities. In this case, [3] and [4] have identified some of the basic techniques and methodologies in solving problems of digital forensics along with tools that are often used by investigators. In practice, all the tools and devices to support digital forensics activities will be centered in a laboratory.

Based on the characteristics, in general laboratory or working environment for digital forensics can be distinguished into two types; based on the characteristics of the laboratory or working environment for the digital forensics can be broadly divided into two types, the first type laboratory that is closed in nature and the second one is interconnected. In a closed environment, all digital forensics activities are conducted in a limited environment can only be accessed by certain staff, utilize stand-alone computers, and do not involve a complex computer network. Meanwhile, for the interconnected environment, digital forensics architecture and system include a number of parties, have the capability of remote access, and are supported by an infrastructure that is complex but remains focused on the secure and trusted system. In Indonesia, although most of the activities of digital forensics are conducted in a closed environment, following a trend in the characteristics of digital workers as well as digital evidence and cybercrime, the interconnected environment seems to be the work environment needed in future digital forensics.

In the future, besides utilizing several tools, digital forensics activities are also supported by a number of applications and integrated information systems. One of them is as developed by [5] through I-Polink tools as a model for Knowledge Management System to assist in the investigation of digital forensics. In addition, some other tools also start to be widely used to support collaboration and sharing mechanism among the investigators, for example, case management tools, e-discovery, etc. Thus, the interconnected system will become a requirement for future working environment in digital forensics.

Digital forensic activities itself according to [6] will involve several parties, such as first responder, forensics investigator, court expert witness, law enforcement personnel, police officer, victim, suspect and passerby. The involvement of many parties would generate a very complex interaction mechanism that should be facilitated by an adequate infrastructure. First responder and the investigator are the actors in the digital forensics that have a high level of mobility and the need for interconnected systems to perform remote access to the system and the main database owned by law enforcement. For the sake of those activities, the need for a digital forensics infrastructure that is secure and trusted is very important.

Digital forensics activities involve storage mechanisms as well as access and sharing analysis of digital evidence. All digital forensics activities must be guaranteed free from various efforts that will lead to the integrity and quality of the evidence and analysis process. For this reason, one of the challenges is to build infrastructure that will guarantee the security from vulnerability and attacks to the content of the evidence or other information resulted from analysis and investigation process [7].

Almost all digital forensics activity is attempting to help a community and law enforcement to disclose the illegal activity and cybercrime. However, it also needs to consider how if the system and the environment of digital forensics itself that become the target of illegal activities and cybercrime. In this

- *Yudi Prayudi is currently working as a researcher at Department Of Informatics Universitas Islam Indonesia, Indonesia. E-mail: prayudi@uii.ac.id*
- *Ahmad Ashari is currently working as a researcher at Department Of Computer Science and Electronics, Gadjah Mada University, Indonesia, E-mail: ahmad.ashari@ugm.ac.id*

case, [8] mentions that many law enforcement infrastructures are open and vulnerable toward attacks from certain parties; one of which is the number of gaps in the lines of communication between officers. According to [9], the infrastructures supporting the activity of the police, firemen and medical staff belong to the infrastructures that are completely secure. The use of commercial networks and public networks is a very risky option for infrastructure. Therefore, based on internal studies, [9] suggest the use of encrypted channels or virtual private networks (VPNs) as a solution to the infrastructure.

In the domain of law enforcement, security is a top priority [10]. This domain will intersect with a number of data and information that are very sensitive. When they are not protected with a good security system, this condition will bring a negative impact. One of the security implementations is the use of an appropriate infrastructure such as secure communication channel that meets the standards and security requirements. Therefore, a secure communication channel is the solution that will be explored further in this paper. In addition, this paper will discuss some issues on security and trust in digital forensics, and then proposed alternative solutions as a secure communication channel especially for VPN technology. In another part of this paper will also discuss the problems that may be encountered in the application of VPN technology in the digital forensics environment.

2 Issues on Security and Trust in Digital Forencis

The rapid growth of computer technology where networking, sharing, collaboration and connectedness become its main strength has resulted in increasing complexity of cybercrime. Based on the current technology, according to [11] and [12], organized crime is one of the main characteristics of today's cybercrime activity. Even, according to [13], many of the current activities of cybercrime cannot be classified/identified when referring to conventional categorization of a crime. That is why over time, the complexity and variation of cybercrime activities have risen. This certainly becomes a challenge for law enforcement.

Based on the idea of [14], the increase in cybercrime activity will lead to the growing number of potential digital evidence that must be acquired and analyzed, since currently people tend to have multiple devices that are interconnected and synchronized with each other. According to [15] this condition enables the birth of new characteristics of digital evidence known as correlated evidence. In addition, investigation processes in the future will tend to be a correlation and linking criminal behavior using several datamining techniques from different database owned by law enforcement.

According to [16], a digital forensics activity requires methodology and technology that are well-developed and reliable. This is necessary to ensure that all processes, analyzes and reports on findings of digital evidence are truly objective and trusted. Therefore, technological infrastructure is one of the issues that need more attention. This one is driven by the shift in the environmental investigation that was previously physical-based to be digital-based. In this new investigation environment, the ability to remote access, digital data/document sharing, and collaborative working becomes the main characteristic. On the other hand, the convenience in digital investigation environmental has become a loophole for security issues and system vulnerability that will have an impact on the integrity of digital evidence.

Meanwhile, [17] argues that the increasing use of digital evidence in juridical processes must be supported by a secure environment to support the fulfillments of requirements in the use of digital evidence in legal proceedings. One of which is the use of log data. In this research area, [17] tried to build a secure logging protocol to ensure that the use of the protocol, supports the use of the log data as one type of digital evidence. Nevertheless, some protocols tested in the study were not able to meet security and legal requirement as expected. Thus, according to (Accorsi, 2009), the use of log data as digital evidence still has many weaknesses in terms of the legal aspects.

Based on the idea of [18], the traditional approach to digital forensics activities is by doing an event reconstruction based on a number of findings from the available evidence. The current technology, surprisingly, enables a lot of tools that in nature can produce new evidence, which any time can serve as the raw material for digital forensics analysis. For example, there is a device installed in a vehicle that can record the activities of the driver. The records can be a basis for the insurance companies to accept or reject a claim. This is similar to the vehicle speed detection device in a road. In this case, the data recorded in the device will automatically become the evidence of the occurrence of an event because the data resulted are automated. However, it should be ascertained beforehand that the attached tool is secure, trusted and also meets the requirements of evidence according to the prevailing law.

The characteristic of trust in the digital forensics process will increase the probative value of digital evidence. According to [19], problems will arise when the investigators are confronted with some digital evidence that interpretation contradicts to one another. Thus, it must be decided which digital evidence is valid. In other conditions, more complex use of information technology also results in a condition where there are a few tools or applications that support the automatic retrieval of digital evidence. Investigators must be able to ensure that the tools or software agent applied in digital forensics environment are trusted so that the resulted digital evidence can be used in the investigation process.

However, there are things that still have not been studied further by previous researchers, particularly about the importance of security on law enforcement infrastructure or digital investigator. Workstations or computers of the investigators are likely to connect to the Internet, either for the purpose of acquisition and analysis of digital evidence, communication among law enforcement/investigators, interconnected case management or other resource access by connecting to the server. According to [20], this potentially allows the presence of attack or malware infection against law enforcement system. This risk should be a consideration for network managers at the law enforcement infrastructure.

It is in line with the opinion of [21], that network-based attacks now are a major challenge for security on a number of

strategic infrastructures of the government, healthcare, financial and power sectors, and law enforcement. This statement is supported by data from Moen (2007) cited by [22] that nearly 80% of the web-based applications in several strategic government infrastuctures have vulnerability toward attack, particularly cross-site scripting and SQL injection.

According to [23], in a society, trust is a basic requirement of the technology adoption process. Users tend to avoid the use of a particular technology in a perceived lack of concern that the security of the technology is argued. In this context, a number of computer services are still perceived as having low level of trust by the users, namely computer services for the cloud, enterprise, and mobile platforms. In this case, according to [24], trust is not simply obtained from a document that contains a warranty claim provided by the service provider, but must also be attested and verified by a third party.

As a result, according to [23], a solution to improve trust is through two aspects, namely:

- Enforce the security properties required by the users, that is to provide protection against the users' data, as well as security of the computing platforms used.
- Give users guarantees that the desired security properties are being enforced. Considering users are not directly involved in the control process toward security and do not know the power of computing platforms used, then the users need to be given a guarantee that the infrastructure being run is completely safe. In this case, the guarantee that can be given is through trusted computing hardware and trusted certifier that is offline.

There are three different terminologies, secure channel, confidential channel and authentic channel. Secure channel is a way to do data transfer safely against tampering and overhearing efforts. Meanwhile, confidential channel is a way to do data transfer that is resistant to overhearing attempts although does not always resist tampering. In addition, authentic channel is a way to transfer data that is not affected to tampering although not necessarily resistant to overhearing attempts. For the purposes of law enforcement, it is necessary to choose a secure channel because using confidential or authentic channel only is not enough. In this case, [25] call this channel as the bidirectional secure channel.

According to [9], there are a number of criteria as a reference for selecting a secure and trusted infrastructure, namely the ability:

- To give protection from wiretapping. Capability of end-to-end encryption is the standard capability of a secure infrastructure that guarantees the process of transferring information from one party to the other party.
- To give protection from the possibility of corrupted information/data. The infrastructure must be able to protect from injection attempts, so the information/data obtained by the other party are not misleading, and to protect the integrity of the public data that are sensitive and stored in the storage infrastructure.
- To protect interface and communication between the elements of the network so as to block unauthorized users to access each element in the network.
- To protect from data exfiltration efforts. Strict authentication scheme and access control have to be done in order for unrelated parties cannot access sensitive information.
- To protect from Denial of Service (DoS) attacks. Currently, there are many ways to perform DoS attacks; thus the infrastructure must be designed to be able to detect and isolate the system that contains DoS.
- To secure Operations, Administration, and Maintenance (OAM) of the network. This capability is important because under certain conditions, the activities of OAM will be the key to network reconfiguration process or for improving the level of security, bandwidth allocation, and connectivity.

3 VPN AS A SOLUTION

Implementing a secure and trusted system is not as easy as imagined. There must be several things to consider, such as the cost and benefit. On the implementation, integrating the implementation of access control design through firewalls, NAT (network address translation) and PKI (public key infrastructure) require a resource that is not simple. According to [26], securing data in a network is a complex duty, moreover, from time to time, the attempts to do the attacks as well as data modification and interruption are increasing. In providing a guarantee toward the confidentiality, integrity and authenticity of data communication on a network, it requires completion from a range of viewpoints.

Based on the previous section, a simple solution that can be applied to meet the needs of a secure system is by implementing the VPN (Virtual Private Network) technology. VPN is a private data network that makes use of the public telecommunication infrastructure and maintains privacy through the use of a tunneling protocol and security procedures. VPN is an extension of the intranet in the form of a special communication channel on the Internet. This service is used by companies that require a special communication space on the Internet. VPN creates a secure connection and allows the remote computers to act as though they are in a LAN network. A VPN is a private network in nature with medium public network (public) that is used to connect a remote site safely [27].

VPN combines two networking concepts: Virtual networking, which enables users which are geographically distributed to use this network, and hosts network to be able to interact with the same entity; and Private networking that enables private networks incorporate data protection with guaranteed confidentiality among hosts on a virtual network, allowing trust relationships to be established and enforced on the network. According to [28], VPNs can traverse untrusted networks, as well as share a physical network with untrusted parties.

The core of the Virtual Private Network technology is tunneling where the data or packets are encapsulated and then sent through the Internet as a medium called tunnel. When the packets arrive at the destination, the packets are then encapsulated again to be returned to the original format. A VPN creates a virtual "tunnel" connecting the two endpoints. The traffic within the VPN tunnel is encrypted, so that other users of the public Internet cannot readily view intercepted communications. According to ([29], tunneling is a method of using an

internetwork infrastructure to transfer data (frames or packets) for one network over another network. Then, those data are encapsulated by tunneling protocol in a frame using an additional header. The additional header provides routing information so that the encapsulated data can traverse the intermediate.

According to the [28], in general the implementation of VPN is based on some protocol selections, namely: MPLS, PPTP, L2TP, IPSEC, and SSL/TLS. Then, [28] also mention that the MPLS protocol, PPTP, L2TP operates at layer 2 of the OSI reference model, are point-to-point in nature, and establish connectivity between sites over a virtual circuit. Virtual circuit itself is a logical end-to-end connection between two endpoints in a network, and can span multiple elements and multiple physical segments of a network. In addition, according to [28], the two most used VPN technologies are IPSEC and SSL, while according to [30], three main protocols that are mostly used for VPN are L2TP, IPSec and SSL/TLS. IPSec runs on layer 3 (network layer), while SSL operates on layer 7 (application layer) of the OSI model. An overview of VPN technology solution can be seen from the illustration in Figure 1.

Furthermore, Lakbabi [28] mentions that VPN technology that was widely used initially was the IPSec protocol, and it was designed for site-to-site communication between branch offices. It was featured as an economical solution to improve the accessibility of the company due to remote access capabilities through a public Internet network. During a certain period, the application of IPSec VPN was the only alternative for applying the concept of secure remote access. When there was more and more demand to perform remote access via mobile, then IPSec VPN was no longer able to meet those needs due to limitations in detecting untrusted end point locations. To deal with the problem, recently another alternative has been developed based on the SSL protocol, namely SSL VPN.

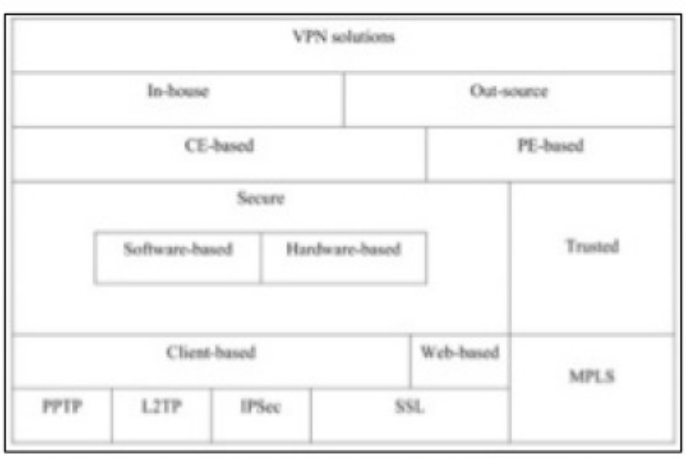

Figure 1. VPN Technology as a General Solution From [29]

IP Sec is an open standard framework developed by the Internet Engineering Task Force (IETF). According to [30], IPSec is designed to provide security for network traffic through Internet Protocol layer by providing access control, data integrity, data origin authentication, data confidentiality, and replay protection and limited traffic flow confidentiality. To support those features, the IPSec provides two security protocols i.e. Authentication Header (AH) and Encapsulating Security Payload (ESP), which can be applied by end hosts or by security gateways along the routing path.

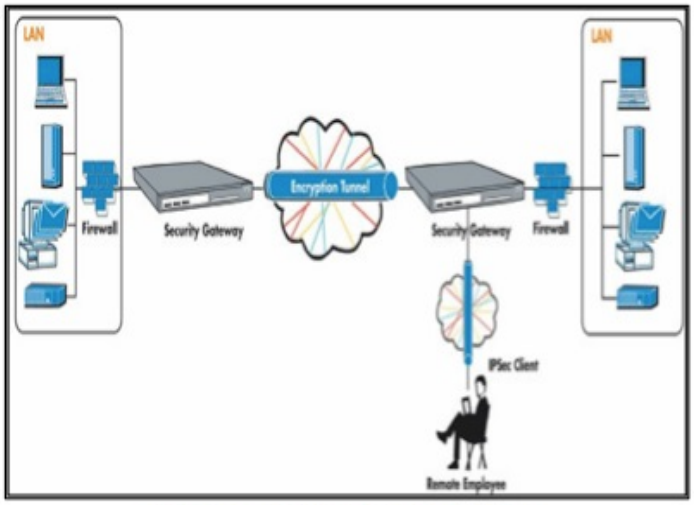

Figure 2. Architecture of IPSec VPN

Users can only access the VPN by using that specific IPSec client. IPSec VPN access is tied to a specific machine (laptop, desktop) and often for a specific user. This can provide stronger security but may limit accessibility and mobility. IPSec clients may also require manual configuration, making them somewhat difficult to use for nontechnical workers. The architecture for IPSec VPN is illustrated in Figure 2.

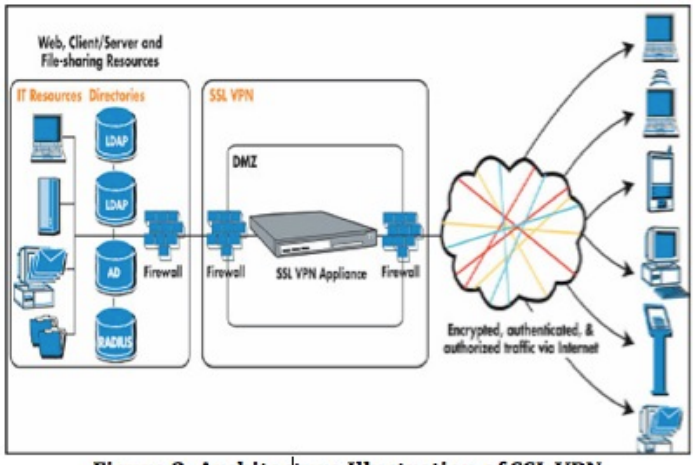

Figure 3. Architecture Illustration of SSL VPN

Meanwhile, SSL VPN is a virtual private network based on SSL (Secure Socket Layer) protocol. According to [31], SSL VPN solves the problem of secure remote access to a private network, which effectively avoids adopting the private line access scheme that requires higher cost, more space, and longer assembly time.

According to [32], there are two types of SSL VPN, namely SSL Portal VPN and SSL Tunnel VPN. The type of SSL VPN allows users to use a single standard SLL connection to the website for the sake of security against access to multiple networks services. This is called as a portal because it is a single page that opens to another resource. On the other hand, the type of SSL Tunnel VPN allows users to use a specific web browser to safely access various services of other networks including the application and protocol, which are non-web-based. Through SSL Tunnel, web browser can maintain active contents that cannot be handled by SSL Portal, such as Java, JavaScript, ActiveX, and flash application. The application of SSL VPN is illustrated in Figure 3.

To implement SSL VPN technology, it can be done by utilizing several tools, such as OpenVPN and Softether. Softeher is an open source-based SSL VPN solution which main concept is multi-protocol VPN software. Softether has interoperability with almost any type of protocol (L2TP, IPSec, EtherIP, L2TPv3, and SSL VPN) and supports all products of a vendor such as Cisco VPN Routers and MS-SSTP VPN Clients.

According to [33], due to the characteristics such as ease of deployment and perfect security quality, SSL VPN is often selected as a solution to secure communication. This selection is certainly by taking into account other similar technologies such as IPSec, L2TP, and PPTP. In principle, SSL VPN is the best choice for a remote access solution while IPSEC VPN is the best choice for site-to-site VPN communication. Furthermore, [34] argues that overall the use of SSL VPN delivers flexibility and convenience but still considers a high-level security for the benefit of remote access.

The use of SSL VPN also supports strong user-level authentication as well as very granular application level access control through application proxies. Thus, SSL VPN is generally used as the best solution for those who want high security combined with flexibility and very granular access control. Furthermore, according to [34] there are three advantages of using SSL VPN, namely the security aspect, flexibility and cost reduction. Through SSL VPN, the use of SSL is to provide services to users through authorization and secure access to the web, client server, and file-sharing resource. SSL VPN will do user authentication to ensure that only authorized users who have access to specific resources that are permitted by security setting of an institution.

On the other hand, SSL is the standard protocol for managing the security of message transmission on the Internet. SSL is a security protocol that is on a higher layer than IPSec. If IPSec runs on the network layer, SSL runs on the application layer. Because SSL operates at the application layer, it can provide policies and access control that are required for the benefit of a secure remote access. Since SSL is available in all modern browsers, SSL VPN can empower the mobility of the client's remote access to reduce the cost and complexity of installation, and complexity when implementing IPSec. SSL VPN solution is seen as increasing workers' productivity and reducing IT overhead

4 Discussion

The advantages in using VPN are always associated with reduced cost, space, and time required for installation. Nonetheless, the biggest benefit of VPN is on security and trust system offered. According to [26], IPSec and SSL are the most robust and most potential tools available for securing communications over the Internet.

The needs of secure communication for digital forensics environment can be met through VPN technology selection (either SSL or IPSec). VPN technology is a solution that meets a number of requirements in accordance with the characteristics of digital forensics itself. Table 1 shows the VPN technology selection framework from the viewpoint of 5W and 1H. The use of this point of view is in accordance with the characteristics of a mindset that becomes a reference in digital forensics.

Table 1. VPN as a Secure Communication Solution in Digital Forensics

Who	What	Where	When	Why	How
First Responder	Digital Evidence	Server Computer	Anytime	Authenticity	SSL VPN
Investigator	Chain Of Custody	Client Computer		Integrity	IPSec VPN
Attorney	Crime Database	Mobile Computer	Anywhere	Authorization	
Court Expert	Crime Analysis Apps	End-user device		Admissibility	
Law Enforcement Officer	Digital Forensics Tools	Internet		Confidentiality	
Police Officer	Confidential Information			Vulnerability	
Victim / Suspect				Attack	
Passerby					
Lawyer					
Judge					

On the Internet network that is vulnerable to a variety of threats during the data communication process, the existence of a guarantee for the privacy and protection of data is the most important thing expected by all parties. In this case, according to [29] and [35], there are some aspects that are guaranteed by VPN, namely:

- Authentication, data traffic is ensured to be originated from a trusted source. VPN access rights are based on the traffic source's identity, which should be verified.
- Access Control toward a number of resources, which can be managed because it involves parties that have an obvious role. Every VPN must enforce access controls that determine who is permitted to use private resources.
- Confidentiality that is a guarantee of information privacy through the restriction for unauthorized users to perform data reading in public links. Private traffic transmitted over the public links should be encrypted to prevent "man in the middle" eavesdropping.
- Data Integrity that is verification of data to ensure that the data do not change during the data transmission process through the public links. The VPN must also be able to discard any traffic that has been injected, modified, dropped, or replayed in transit.

A technology offered through VPN, either IPSec or SSL VPN, in principle, has met the standard requirement for a secure and trusted system as explained by [29], [35], and [9]. However, it is still possible for the presence of potential attacks against the VPN infrastructure. In this case, [36] men-

tions a number of attacks that might occur in a VPN, namely:

- VPN hijacking that is an attempt to take over the VPN connection from a remote client and then impersonate that client on the connecting network.
- Client-side risk, this occurs because the client's computer may be connected to other computers that the security system is not protected. This risk includes the spread of malware caused by unprotected security system on client's computer or other computers on the intranet.

Based on the information above, it is seen that attacks or vulnerability of VPN are not solely caused by the weaknesses of the security technology provided by the VPN (IPSec or SSL VPN), but also due to things outside VPN technology that cannot be predicted and controlled. Thus, it can be concluded that VPN provides the right solution for a secure communication channel.

Furthermore, although the data cited by Gartner (Phifer, 2008) show the tendency of changing trend in users from using IPSec to SSL VPN due to the demand of 90% mobile workers nowadays who require remote access to support their mobility, but it does not necessarily mean that IPSec is no longer used at all. IPSec VPN is still an appropriate technology for the purpose of point-to-point access. This solution is precisely used for conditions under which a connection between two parties on two specific locations must always be maintained. Meanwhile, SSL VPN is the right solution to meet the needs of remote access required by mobile workers today.

A number of researchers, namely [26], [28], [34] have attempted to compare IPSec and SSL VPN. However, to decide which one is the best technology for fulfilling the need of an institution depends on criteria and characteristics of the institution. Both IPSec and SSL provide a secure access to the corporate network to support their business.

Table 2. Characteristics of the Use of Secure Communication

	IPSec VPN	SSL VPN
Characteristic	Fixed connection, Managed corporate device, Site-to-site, Robust firewall functionality.	Transient connection, Varying devices, Remote employee, business partner, customer, enables access management policy enforcement.
Uses	Interconnected between Police Office, Court and attorney office, Forensics Lab.	Remote access from main server to serve first responder, investigator, law enforcement officer, lawyer, judge, attorney, expert.

Therefore, based on the need for a digital forensics environment, both IPSec VPN and SSL VPN can be used as a solution for secure communication channel. Digital forensics environment characteristics in practice require two types of connection needs, namely, site-to-site and remote access. Site-to-site model is a communication model where the main offices are interconnected with other offices or external parties. In the context of laws in Indonesia, site-to-site communication is required to link all police offices, ranging from district, regional, up to national level as well as for the connection between law enforcement institutions. On the contrary, remote access is necessary to facilitate the mobility of officers or first responders who are directly related to the acquisition and imaging of evidence, as well as investigators who make the crime analysis or seconded expert in the handling of certain cases. Table 2 shows the use of the secure communication solution in a digital forensics environment.

Based on Table 2, VPN as the secure communication solution can be applied to the scheme as illustrated in Figure 4.

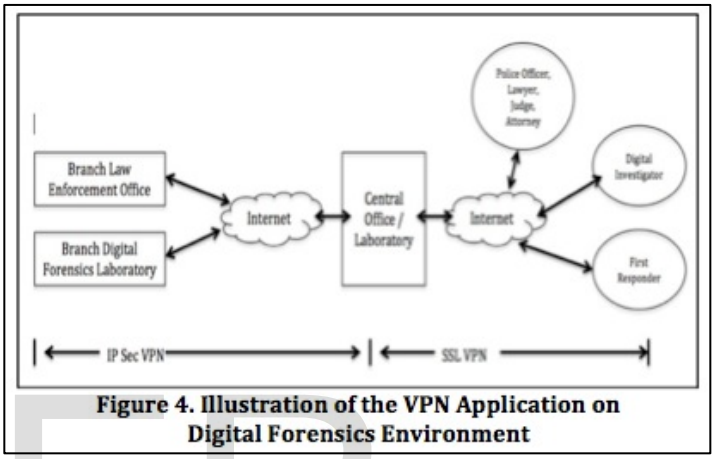

Figure 4. Illustration of the VPN Application on Digital Forensics Environment

5 Conclusion and Further Research

Although currently most of the digital forensics activities are done in a closed environment, in the future digital forensics activities will utilize an interconnected system based on the availability of computer networks and the Internet. One thing to note is how to provide a secure communication channel as the infrastructure for a digital forensics environment. There are a number of criteria and requirements to support secure communication channel. To meet the criteria, the available technology is through the use of VPN. Some protocols can be chosen to implement the VPN, but there are two widely used protocols, namely IPSec and SSL VPN.

The increasing need for remote access as demanded by mobile workers has made the usage of SSL VPN far more popular than IPSec. However, the actual selection of IPSec and SSL VPN is determined by the characteristics and criteria of the institution. In principle, the IPSec and SSL VPN have given the basis for trust and secure communication infrastructure. In the digital forensics environment, both IPSec and SSL VPN can be used as necessary. Considering the characteristic of IPSec is more appropriate for site-to-site connection, IPSec can then serve as a solution for the secure communication channel that connects between police offices or other law enforcement agencies, including between digital forensics laboratories. Meanwhile, SSL VPN is a great choice for remote access, so the mobility of first responders, investigators, officers, lawyers, and experts can be facilitated through the implementation of SSL VPN as the secure communication solution.

The content of this paper is a conceptual study of the use

of a secure communication channel. To get a clear and real depiction of the use of secure communication channel in digital forensics environment, further research needs to be performed. One thing that should be done by the next researches is realizing a digital forensics environment in an interconnected system. Softether as a multi-protocol of opensource-based VPN can serve as a tool to support the implementation. Another issue that can be researched is the incorporation of some protocols (hybrid or dual protocol) as a VPN solution in an institution.

REFERENCES

[1] S. Raghavan, "Digital forensic research: current state of the art," *CSI Trans. ICT*, vol. 1, no. 1, pp. 91–114, Nov. 2012.

[2] A. Agarwal, M. Gupta, and S. Gupta, "Systematic Digital Forensic Investigation Model," *Int. J. Comput. Sci. Secur.*, vol. 5, no. 1, pp. 118–134, 2011.

[3] E. K. Mabuto and H. S. Venter, "State of the art of Digital Forensic Techniques," in *Information Security for South Africa (ISSA)*, 2011.

[4] K. K. Sindhu and B. B. Meshram, "Digital Forensic Investigation Tools and Procedures," *Int. J. Comput. Netw. Inf. Secur.*, vol. 4, no. 4, pp. 39–48, May 2012.

[5] I. Gunawan and Y. Prayudi, "I-Polink sebagai Model Knowledge Management System untuk Membantu Investigasi Forensika Digital," in *Konferensi Nasional Sistem dan Informatika (KNS&I)*, 2014.

[6] J. Cosic, G. Cosic, J. Ćosić, and Z. Ćosić, "Chain of Custody and Life Cycle of Digital Evidence," *Computer Technology and Aplications*, vol. 3, pp. 126–129, Feb-2012.

[7] M. Burmester, "A trusted computing architecture for critical infrastructure protection," in *4th International Conference On Information, Intelligence, Systems and Applications (IISA)*, 2013, pp. 1–6.

[8] F. Cohen, "The State of the Art and What We are Missing," in *1st Chinese Conferemce on Digital Forensics*, 2012, pp. 1–21.

[9] A. R. McGee, M. Coutière, and M. E. Palamara, "Public Safety Network Security Considerations," *Bell Labs Tech. J.*, vol. 17, no. 3, pp. 79–86, Dec. 2012.

[10] M. Chau, D. Zeng, and H. Chen, "Building an Infrastructure for Law Enforcement Information Sharing and Collaboration : Design Issues and Challenges," 2001.

[11] R. Broadhurst, P. Grabosky, M. Alazab, and S. Chon, "Organizations and Cyber crime : An Analysis of the Nature of Groups engaged in Cyber Crime," *Int. J. Cyber Criminol.*, vol. 8, no. 1, pp. 1–20, 2014.

[12] M. A. Tariq, J. Brynielsson, and H. Artman, "Framing the Attacker in Organized Cybercrime," in *European Intelligence and Security Informatics Conference Framing*, 2012, pp. 30–37.

[13] D. J. Neufeld, "Understanding Cybercrime," in *2010 43rd Hawaii International Conference on System Sciences*, 2010, pp. 1–10.

[14] F. N. Dezfoli, A. Dehghantanha, R. Mahmoud, and N. F. Binti, "Digital Forensic Trends and Future," *Int. J. Cyber-Security Digit. Forensics*, vol. 2, no. 2, pp. 48–76, 2013.

[15] A. O. Flaglien, "Cross-Computer Malware Detection in Digital Forensics," Gjovik University Collage, 2010.

[16] Y. Lin, T. Wu, C. Hsu, and Y. Chou, "Standard Operating Procedure and Privilege Management in Taiwan Digital Forensics," in *Future Generation Communication and Networking (FGCN Volume:2)*, 2007, pp. 154–158.

[17] R. Accorsi, "Safekeeping Digital Evidence with Secure Logging Protocols : State of the Art and Challenges," *2009 Fifth Int. Conf. IT Secur. Incid. Manag. IT Forensics*, no. 1, pp. 94–110, 2009.

[18] N. Kuntze, C. Rudolph, T. Kemmerich, and B. Endicott, "Chapter 1 Scenarios For Reliable And Secure Digital Evidence," in *Ninth Annual IFIP WG 11.9 International Conference*, 2013, pp. 1–13.

[19] M. Wojcik, H. Venter, J. Eloff, and M. Oliver, "Applying Machine Trust Models to Forensics Investigations," in *IFIP Advances in Information and Communication Technology*, 2006, pp. 55–65.

[20] S. Thorpe, "An Experinmental Survey Towards Engaging Trustable Hypervisor Log Evidence Within a Cloud Forensics Environment," *Int. J. Comput. Sci. Inf. Technol.*, vol. 4, no. 6, pp. 125–141, 2012.

[21] E. Casey, *Digital Evidence and Computer Crime*. London, UK: Elsevier Academic Press, 2011, p. 590.

[22] T. K. Priyambodo and Y. Prayudi, "Information Security Strategy on Mobile Device Based eGovernment," in *ADVCIT 2014*, 2014, vol. X, no. X, pp. 1–7.

[23] N. M. C. Santos, "Improving Trust in Cloud , Enterprise , and Mobile Computing Platforms," Universitat de Saarlandes, 2013.

[24] N. Paladi, "Trusted Computing and Secure Virtualization in Cloud Computing," Lulea University Of Technology, 2012.

[25] U. M. Maurer and P. E. Schmid, "A Calculus for Secure Channel Establishment in Open Networks," in *European Symposium on Research in Computer Security (ESORICS)*, 1994.

[26] A. Alshamsi and T. Saito, "A Technical Comparison of IPSec and SSL," 2004.

[27] M. W. Murhammer, H. J. Lee, A. Schmid, O. Atakan, Z. Badri, and B. J. Cho, *A Comprehensive Guide to Virtual Private Networks , Volume II : IBM Nways Router Solutions*,

vol. II. IBM International Technical Support Organization, 1999, p. 642.

[28] A. Lakbabi, G. Orhanou, L. Mathematiques, and U. Mohammed, "VPN IPSEC & SSL Technology," in *International Conference on Next Generation Networks and Services (NGNS)*, 2012, no. December, pp. 202–208.

[29] A. A. Jaha, "Selecting and Implementing Proper Virtual Private Network (VPN) Solution for Libyan Industrial Sector," The High Institute of Industry, Misurata Libya, 2008.

[30] H. Dudani, "Virtual Private Networks for Peer-to-Peer Infrastructures," Technische Universit¨ at Darmstadt, 2012.

[31] K. Wu, J. He, and S. Chen, "Test and Analysis of Sensitive Factors of SSL VPN on Kylin," in *lnternational Conference on Electrical and Control Engineering (ICECE), 2011 I*, 2011, pp. 3207–3211.

[32] S. Frankel, P. Hoffman, A. Orebaugh, and R. Park, "Guide to SSL VPNs," 2008.

[33] Z. Yanjun, W. Binjun, and Z. Wei, "SSL VPN System Based on Simulated Virtual NIC," in *Fourth International Conference on Networking and Distributed Computing*, 2013, pp. 70–74.

[34] S.-H. Sun, "The advantages and the implementation of SSL VPN," in *2nd IEEE International Conference on Software Engineering and Service Science (ICSESS)*, 2011, pp. 548–551.

[35] L. Phifer, "Mix-n-Match VPNs : IPsec and SSL," *WatchGuard Technologies, Inc*, 2008. [Online]. Available: http://www.corecom.com/external/livesecurity/mixnmatch.htm. [Accessed: 18-Jan-2015].

[36] HKSAR, "VPN Security," Hongkong, 2008. Available: http://www.infosec.gov.hk/english/technical/files/vpn.pdf

Web Site:

OpenVPN : https://openvpn.net/

Softether : https://www.softether.org/