Digital Forensic Analysis of Virtual Private Network Services using National Institute of Standards and Technology Method

Fajar Eko Prastyo
Department of Informatics
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

Imam Riadi
Department of Information System
Universitas Ahmad Dahlan
Yogyakarta of Indonesia

ABSTRACT
The use of Virtual Private Networks (VPNs) is on the rise to protect the privacy and security of network communications. However, the use of VPNs also complicates digital forensic investigations due to the encryption of data traffic. This study aims to analyze network traffic under conditions with and without a VPN using the National Institute of Standards and Technology (NIST) methodology. Data collection was conducted through internet activity simulations recorded using Wireshark and analyzed using NetworkMiner. The results show that VPNs can hide users' IP addresses and encrypt network communications, but digital artifacts such as the VPN server's IP address, DNS requests, communication sessions, timestamps, and network metadata can still be identified. Additionally, differences in network communication patterns were found between conditions without a VPN and with a VPN, particularly regarding the use of the TLS/SSL protocol. Based on these results, the NIST method proved effective in supporting digital forensic investigations of VPN-based network traffic in a systematic and structured manner.

Keywords
Digital Forensics, VPN, NIST, Wireshark, NetworkMiner, Network Traffic.

1. INTRODUCTION
Rapid advances in information technology have driven the adoption of Virtual Private Network (VPN) services as the primary choice for protecting privacy and ensuring security in digital data exchange. However, the widespread use of Virtual Private Networks also creates opportunities for cybercriminals to conceal their activities, such as in cases of fraud, hacking, or malware distribution [1]. This demonstrates the effectiveness of VPNs in protecting data traffic without compromising network performance, making them relevant for simulating encrypted traffic in digital forensic analysis [2]. Therefore, a systematic digital forensic approach is needed so that investigators can penetrate the layer of anonymity offered by Virtual Private Networks. The ADAM method, commonly used in cloud computing investigations, is considered unsuitable because it does not specifically handle encrypted networks in real time [3].

The National Institute of Standards and Technology (NIST) method is a widely used framework in digital forensics due to the comprehensiveness of its phases: collection, examination, analysis, and reporting. This method has proven effective in various cybersecurity contexts, including when integrated into modern approaches such as Zero Trust for network security in the digital age [4]. This is important because voice communication often serves as a hidden channel in digital crimes, which can technically be uncovered through the collection and examination stages of the NIST method [5]. Other forensic methods, such as those from the National Institute of Justice, are also frequently used, particularly in mobile forensic contexts, such as in cases of cyberbullying via Instagram and WhatsApp [6]. In a study on Facebook Lite using the NIST method, researchers successfully uncovered conversation artifacts and image files from the social media app with significant results [7].

Previous research has also evaluated the effectiveness of the NIST method in email forensic investigations, particularly in cases of sender address forgery or email spoofing, demonstrating NIST's ability to systematically analyze email metadata and headers [8]. In the context of Virtual Private Networks, the NIST framework allows investigators to focus on critical phases, particularly the collection of network logs and the analysis of data packets using tools such as Wireshark or Network Miner. When compared to forensic literacy-based methods in online learning (such as the forensic literacy model) [9], the NIST method performs optimally in this context because the validity of data transferred over a VPN network remains intact [10].

Researchers applied the Network Development Life Cycle approach to measure the effectiveness of the PPTP Virtual Private Network in maintaining data integrity in a web-based health reporting system. However, this method focuses more on system development and does not delve into the technical depth of digital forensic analysis [11]. On the other hand, the NIST approach can be adapted for Virtual Private Network environments as well as virtual router systems, as demonstrated in studies on Telegram and MiChat services that showed success in extracting voice notes and encrypted conversations [12]. Although it has greater resource requirements, this protocol is considered the most suitable for use in investigative scenarios due to its stability in managing encrypted data traffic [13].

Researchers successfully used the NIST method in a study of Telegram applications involved in online scams to uncover digital evidence in the form of videos, photos, and voice messages [14]. Additionally, a recent study on Android malware samples further demonstrated the NIST method's capability to uncover malicious applications disguised as image files via WhatsApp [15]. This underscores the flexibility of the NIST method in accommodating the latest protocol technologies during the digital evidence analysis process [16]. Various study results indicate that the NIST method offers a standardized, technical, and flexible approach to digital

forensic analysis in complex environments such as Virtual Private Networks. Although other methods exist, such as NIJ, ADAM, ENFSI, or SNI 27037, the NIST method has proven most capable of accommodating investigative needs from start to finish. Additional studies, such as those on Instagram, TikTok, and WhatsApp, further reinforce this claim [18]. Other studies include the implementation of PPTP Virtual Private Networks in local government environments to strengthen the security of health reporting systems [19], as well as legal-ethical reviews of Virtual Private Network usage from both Islamic and positive law perspectives [20].

2. LITERATURE STUDY

2.1 Virtual Private Network (VPN)

As shown in the figure above, the Virtual Private Network (VPN) workflow begins with the user's device connecting to the VPN server via an encrypted communication channel before accessing the internet. Figure 1 illustrates that all of the user's network traffic passes through the VPN server first, thereby hiding the user's original IP address and making data communication more secure during the information exchange process.

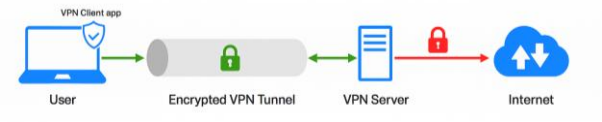

Figure 1: How a Virtual Private Network (VPN) Works

The L2TP/IPSec protocol not only encrypts communication content but also provides an additional layer of user authentication and protection against man-in-the-middle attacks or data sniffing [21]. Network performance remains optimal even during intensive data transmission. Furthermore, the use of Mikrotik devices is considered cost-effective and easy to implement in institutional environments such as government offices and campuses, making them suitable for supporting secure remote data access needs [22]. VPNs are widely used in both organizational and general-user environments because they provide a more secure, stable, and flexible connection for remote communication and data access over the internet [23].

2.2 Digital Forensics

Digital forensics is a multidisciplinary field focused on the identification, acquisition, analysis, interpretation, and reporting of electronic evidence from various digital devices such as computers, smartphones, networks, and cloud-based services. The stages of digital forensics include the identification of digital artifacts, the preservation of evidence through forensic imaging, the recovery of hidden or deleted data, the validation of findings, and the preparation of detailed analytical reports [24]. In addition, digital forensics is also used to uncover various cybercrimes through the identification and analysis of electronic evidence found on devices and in network traffic. The use of digital forensics can aid in the investigation of cases ranging from cyberbullying and digital data manipulation to the misuse of internet-based communication services [25].

2.3 National Institute of Standards and Technology (NIST)

The NIST Methodology is an international standard framework developed by the National Institute of Standards and Technology (United States) to provide systematic guidance for conducting digital forensic investigations. This framework consists of four main phases—collection, examination, analysis, and reporting—which aim to preserve the integrity and validity of digital evidence throughout the investigation process [26]. This study confirms that the NIST method is highly relevant for adoption in investigations of cases involving digital media, whether in financial, social, or other cyber contexts [27].

2.4 Digital Forensic Tools

Digital forensic tools are software programs used in cybercrime investigations to facilitate the structured identification, acquisition, analysis, and reporting of electronic evidence. The use of appropriate forensic tools is essential to preserving the authenticity, integrity, and validity of digital evidence throughout the investigation process [28].

Wireshark is an open-source network protocol analyzer widely used in digital network forensics to capture and analyze data packets in real time. It supports various protocols such as TCP/IP, HTTP, and DNS, as well as QoS parameters like latency, jitter, throughput, and packet loss, to detect anomalies or network attacks [29].

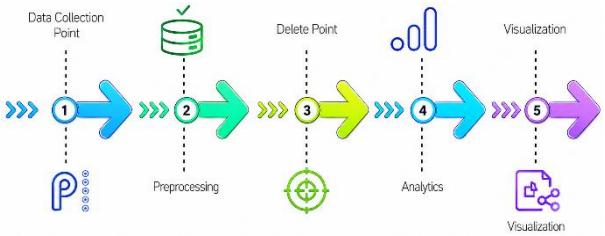

Figure 2 : Wireshark Stages

Figure 2 above illustrates the main steps involved in using Wireshark as a network forensics tool to analyze data traffic activity in detail and in real time. These steps include capturing network packets, filtering network traffic, identifying network protocols, and analyzing digital artifacts generated by network activity during monitoring.

NetworkMiner is a Network Forensic Analysis Tool (NFAT) designed to passively extract digital evidence from packet capture (PCAP) files without altering the original data. NetworkMiner was tested alongside Wireshark and WinDump in a virtual router environment to detect network attacks; the results showed that NetworkMiner was capable of extracting critical digital artifacts and reconstructing traffic patterns, although its memory usage was relatively high compared to other tools [30].

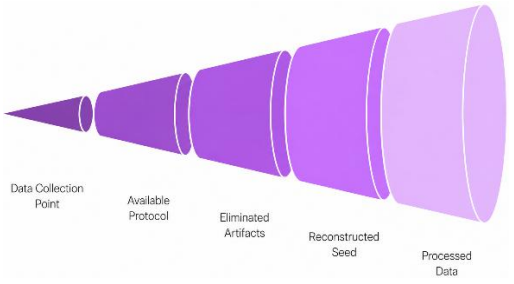

Figure 3 : NetworkMiner Stages

Figure 3 above illustrates the operational steps of the NetworkMiner tool in the network forensic analysis process. Selecting the appropriate tools is a key factor in the success of the investigation, particularly in preserving the authenticity, integrity, and admissibility of digital evidence obtained from VPN services.

3. RESEARCH METHOD

This study was conducted through a simulation of Virtual Private Network (VPN) usage in a controlled network environment to analyze network traffic characteristics and the resulting digital artifacts. The research subjects were Windows-based laptops connected to the internet via a Wi-Fi router. Testing scenarios were conducted under two conditions—without a VPN and with a VPN, using internet activities such as Google Search, YouTube streaming, and Speedtest. During the simulation process, network traffic was recorded using Wireshark to obtain packet capture data in .pcap format, which served as the primary source for the digital forensic investigation.

The analysis phase was conducted using NetworkMiner to extract digital artifacts from network capture files. The artifacts analyzed included host IP addresses, DNS requests, communication sessions, network parameters, timestamps, and traffic metadata. The investigation process was conducted in accordance with the National Institute of Standards and Technology (NIST) methodology, which consists of the collection, examination, analysis, and reporting phases. This approach was used to ensure that the investigation process was systematic, structured, and capable of producing valid digital information regarding network activity during VPN usage.

3.1 Research Scenario

The research scenario was designed to simulate the process of digital forensic investigation of network activity in both VPN-free and VPN-enabled environments. The simulation was conducted in a controlled testing environment and divided into the following three main phases:

1. Pre-Incident

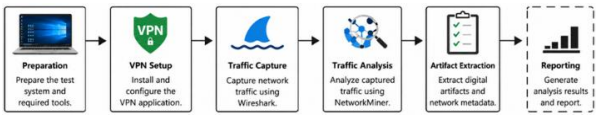

Figure 4 : Pre-Incident Simulation

The researchers set up a research environment consisting of laptops, an internet connection, a VPN application, and network forensic tools such as Wireshark and NetworkMiner. Wireshark was configured to capture network traffic, while NetworkMiner was prepared for the analysis of digital artifacts. This step was performed to ensure that all network activity could be properly recorded both with and without a VPN. Additionally, the network configuration was tested to ensure that the capture process ran stably and optimally throughout the simulation.

2. Incident

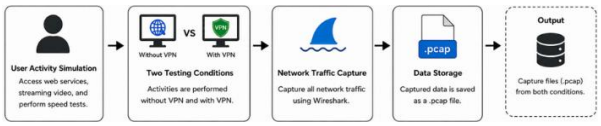

Figure 5 : Incident Simulation

The network activity simulation phase was conducted by accessing Google Search, streaming YouTube, and running Speedtest tests both with and without a VPN. All network traffic was recorded using Wireshark in .pcap format to capture real-time network communication data. This process aimed to generate digital artifacts such as IP addresses, DNS requests, communication sessions, and network metadata.

3. Post-Incident

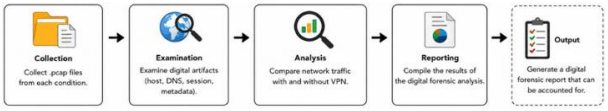

Figure 6 : Post-Incident Simulation

Once the capture process is complete, the .pcap file is analyzed using NetworkMiner to extract digital evidence from network activity. The analysis focuses on identifying hosts, communication protocols, network sessions, and traffic metadata. The entire investigation process is conducted in accordance with NIST methods, which include collection, examination, analysis, and reporting, to produce a systematic digital forensic report.

3.2 National Institute of Standards and Technology Framework

The digital forensic investigation in this study was conducted systematically using the four-phase method of the National Institute of Standards and Technology (NIST): collection, examination, analysis, and reporting, as shown in Figure 7 below:

Figure 7 : NIST Phases

1. Collection

Collecting digital evidence in the form of network traffic under conditions with and without a VPN. Data collection was performed using Wireshark to capture network packets in real time in .pcap format. The recorded network activities included Google Search, YouTube streaming, and Speedtest on a Windows-based laptop connected to the internet via a Wi-Fi router.

2. Examination

Examine and filter network capture data to identify relevant digital evidence. .pcap files are analyzed using Wireshark and further processed using NetworkMiner. The analysis focuses on identifying host IP addresses, DNS requests, communication sessions, network parameters, and traffic metadata that appear during VPN usage.

3. Analysis

Analyzing differences in network traffic characteristics between conditions with and without a VPN based on the digital artifacts identified. NetworkMiner was used to reconstruct network communication patterns, identify the use of encrypted protocols such as TLS/SSL, and analyze communication links between VPN clients and servers. The analysis also aimed to identify digital artifacts that remain detectable even when network communication is encrypted.

4. Reporting

Compiling the results of the digital forensic investigation into a systematic and objective report. The report summarizes all findings regarding the identification of digital artifacts, network communication patterns, and traffic metadata, as well as documentation of the investigative process using Wireshark and NetworkMiner as the basis for digital forensic analysis of the VPN service.

4. RESULTS AND DISCUSSION

This section presents the results of a digital forensic investigation into network activity both with and without a VPN. The process of collecting, examining, analyzing, and identifying digital artifacts was conducted systematically in accordance with the National Institute of Standards and Technology (NIST) methodology, which consists of the following stages: Collection, Examination, Analysis, and Reporting.

4.1 Collection

Collection is the initial stage of gathering and securing digital data without altering the authenticity of the information obtained. In this study, the collection process was conducted by capturing network traffic using Wireshark on a Windows-based laptop used for internet activities such as Google Search, YouTube streaming, and Speedtest testing—both with and without a VPN. All network activity was recorded in .pcap format as the primary digital evidence for the investigation process.

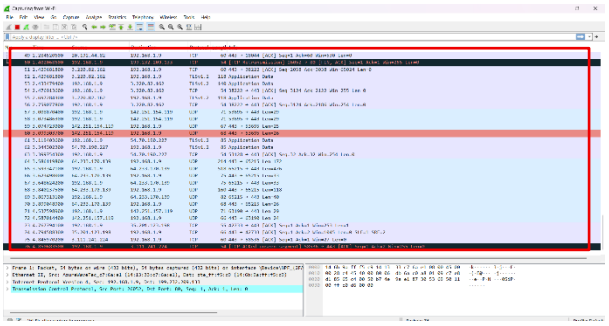

Figure 8 : The Process of Network Capture Using Wireshark

Based on the research scenario, the capture process was conducted under two different network conditions to identify changes in communication patterns resulting from the use of a VPN. The capture results revealed network communication activity using the TCP, TLS/SSL, DNS, and HTTPS protocols, including connections to the VPN server under encrypted conditions. After the collection process was completed, the capture files were prepared for the examination and extraction of digital artifacts using the NetworkMiner forensic tool.

4.2 Examination

The examination phase aims to systematically inspect, filter, and extract data from digital evidence while preserving the integrity of the original data. The examination process in this study was conducted using two network forensic tools: Wireshark and NetworkMiner. The use of these two tools aims to obtain a more comprehensive set of network digital artifacts while enabling the validation of analysis results based on the same captured data.

The initial analysis was conducted using Wireshark to perform packet analysis on network capture files in .pcap format. Wireshark was used to identify communication packets, IP addresses, network protocols, DNS requests, communication ports, and traffic statistics under conditions both with and without a VPN. The results of the analysis revealed differences in network traffic characteristics: without a VPN, communication proceeds directly to the destination server, whereas with a VPN, communication is more centralized toward the VPN server and dominated by the encrypted TLS/SSL protocol.

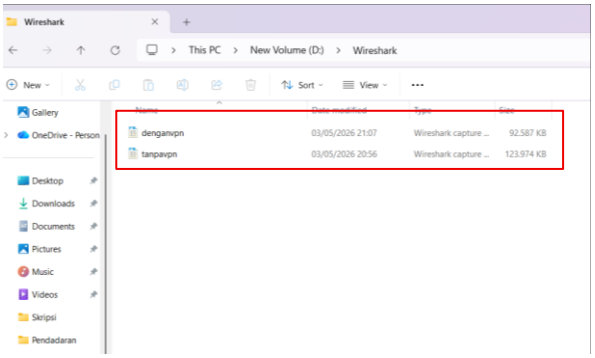

Figure 9 : Network Traffic Capture Results Using Wireshark

Next, the analysis process was conducted using NetworkMiner to automatically extract digital artifacts from network capture files. NetworkMiner successfully displayed various artifacts such as hosts, DNS requests, communication sessions, parameters, and network metadata from captures both with and without a VPN. In the absence of a VPN, information regarding hosts, DNS, and communication parameters is more clearly visible, whereas with a VPN, most communication is encrypted, resulting in more limited information that is primarily centered on the VPN server. The extraction results from both tools were then used as the basis for the analysis process to identify network communication patterns and digital artifacts generated during VPN usage.

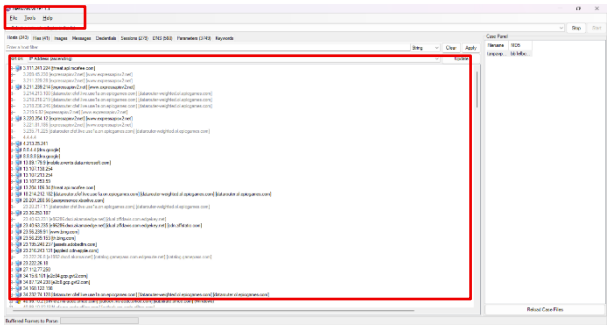

Figure 10 : Results of File Capture Extraction Without a VPN Using NetworkMiner

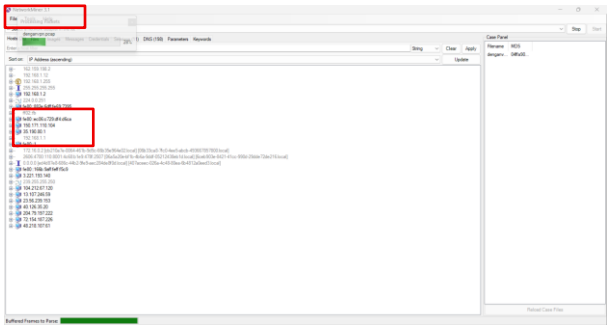

Figure 11 : Results of File Capture Extraction via VPN Using NetworkMiner

Based on Figures 10 and 11 above, the results of capturing and extracting files both with and without a VPN using NetworkMiner reveal differences in the characteristics of the network traffic that were successfully identified. Digital artifacts such as hosts, DNS requests, communication sessions, network parameters, and traffic metadata can be analyzed to identify network communication patterns under both conditions.

4.3 Analysis

The analysis phase is the process of identifying, comparing, and interpreting digital artifacts obtained from the examination of network capture files. Based on the results of the analysis using Wireshark and NetworkMiner, a comparison was made of network traffic characteristics under conditions with and without a VPN to determine the impact of VPN usage on the visibility of digital network artifacts.

The analysis focused on key artifacts such as hosts, DNS requests, sessions, parameters, and network metadata. In the absence of a VPN, the system successfully identified more hosts, DNS requests, communication sessions, and network parameters with greater clarity. Public IP addresses, destination domains, communication requests, and network activity details can be observed directly because communication occurs without tunneling mechanisms or additional encryption. This indicates that without a VPN, user activity is easier to reconstruct through network forensic investigation.

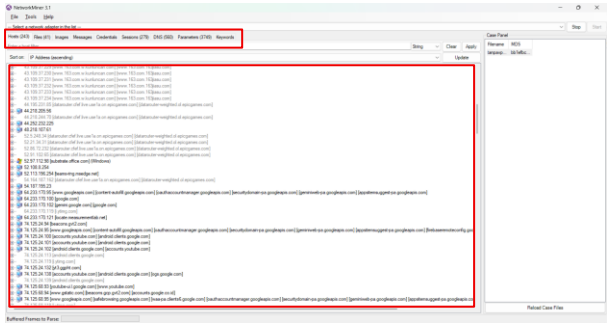

Figure 1 : Network artifact results under conditions without a VPN

Conversely, when a VPN is in use, the number of digital artifacts that can be identified decreases significantly. Most communication is routed through the VPN server, making it more difficult to observe the original host, DNS requests, and application-level communication parameters. VPN tunneling and encryption mechanisms encapsulate network traffic within an encrypted connection, making it more difficult to directly identify the details of user communication.

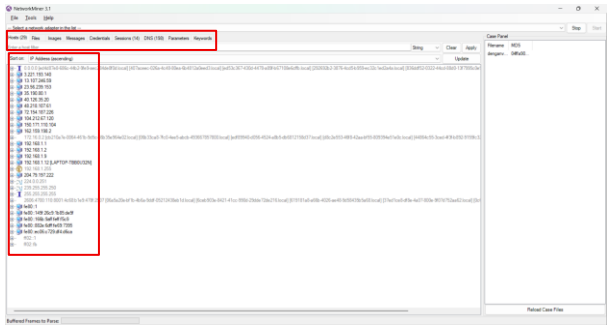

Figure 2 : Network artifact results under VPN conditions

Although using a VPN can mask the content of communications and limit the visibility of digital artifacts, network metadata such as timestamps, communication duration, packet counts, and the IP address of the VPN server can still be obtained. Thus, while a VPN enhances the privacy of users' communications, it does not eliminate all traces of digital artifacts in the course of a network forensic investigation.

4.4 Report

The reporting phase is the final stage in the National Institute of Standards and Technology (NIST) methodology, which aims to systematically and structurally compile all results of a digital forensic investigation. In this study, the reporting focuses on comparing the results of network traffic analysis under conditions with and without a VPN using Wireshark and NetworkMiner.

Based on the results of the investigation, both tools performed well in cross-validating the identification of various digital network artifacts, such as hosts, DNS requests, communication sessions, parameters, and network metadata. Wireshark excels in packet capture and detailed protocol analysis, while NetworkMiner is effective in extracting hosts and metadata and identifying network communications based on capture files.

The results show that traffic without a VPN is easier to analyze, whereas the use of a VPN encrypts most communications via tunneling and TLS/SSL, making communication details more limited. However, important metadata such as the VPN server IP address, timestamps, and session information can still be identified. Details of the digital artifact extraction results are shown in Table 1.

Table 1. Results of the Extraction of Digital Network Traffic Data

Digital Artifacts Category	Without a VPN	With a VPN
Host/IP Address	243	29
DNS Request	560	198
Communication Session	279	14
Parameters	3749	0
Network Metadata	155573	157460

Based on the table, network traffic without a VPN is easier to analyze than traffic with a VPN, where most of the communication is encrypted. A detailed comparison of digital artifacts under both conditions is shown in Table 2.

Table 2. Details of Digital Artifacts from Network Traffic Analysis

	Type of Artifact	Without a VPN	With a VPN
1	Host/IP Address	Many public hosts detected	Communication is server-centric
2	DNS Request	Domains clearly visible	Some DNS is obfuscated
3	Session	Sessions are diverse and open	Sessions are encrypted
4	Parameters	User-Agent, SNI, and HTTP GET visible	Mostly restricted
5	Protocol Dominan	HTTP, HTTPS, TCP	TLS/SSL is dominant
6	Payload	Some are readable	Payload is encrypted

The results show that a VPN enhances network privacy by hiding most communication details, but does not eliminate digital traces. To clarify the sequence of activities during

testing under conditions without a VPN, the network activity timeline is shown in Table 3 below.

Table 3. Timeline of Network Activity Without a VPN

Time	Activity	Condition
03-05-2026 13:46:40	Capture started	Without a VPN
03-05-2026 13:47:15	Google Search	Without a VPN
03-05-2026 13:50:28	YouTube streaming	Without a VPN
03-05-2026 13:53:11	Speedtest	Without a VPN
03-05-2026 13:55:04	Capture finished	Done

Next, the timeline of network activity under VPN conditions is shown in Table 4 below to illustrate the changes in network communication patterns after the VPN was enabled.

Table 4. Timeline of Network Activity Using a VPN

Time	Activity	Condition
03-05-2026 13:58:50	Capture started	With a VPN
03-05-2026 14:00:12	VPN is active	With a VPN
03-05-2026 14:01:26	Google Search	With a VPN
03-05-2026 14:03:45	YouTube streaming	With a VPN
03-05-2026 14:05:02	Speedtest	With a VPN
03-05-2026 14:06:40	Capture finished	Done

The timeline shows that once the VPN is active, the communication pattern shifts to an encrypted connection to the VPN server, making it more difficult to identify the details of the user's activity.

Overall, the use of a VPN significantly alters network traffic characteristics by enhancing communication privacy, although network metadata can still be used as digital evidence in forensic investigations.

5. CONCLUSION

Based on the results of research and digital forensic analysis of Virtual Private Network (VPN) services, a systematic investigation of network traffic was successfully conducted using the National Institute of Standards and Technology (NIST) methodology, which involves the stages of collection, examination, analysis, and reporting. The use of Wireshark and NetworkMiner proved effective in identifying, extracting, and analyzing digital network artifacts both in the absence of a VPN and when a VPN was in use.

The investigation successfully obtained various important digital artifacts, such as host/IP addresses, DNS requests, communication sessions, parameters, and network metadata from the capture files (.pcap) recorded during testing. The analysis results indicate that the use of a VPN significantly alters network traffic characteristics. Without a VPN, network communication is more transparent, allowing the destination domain, communication parameters, and part of the payload to be clearly identified. Meanwhile, with a VPN, network communication is dominated by encrypted protocols such as TLS/SSL via tunneling mechanisms, making communication details more limited.

This study demonstrates that VPNs can enhance network privacy by hiding users' real IP addresses and encrypting most communications. However, using a VPN does not eliminate digital traces, as artifacts such as the VPN server's IP address, communication metadata, timestamps, traffic patterns, and some DNS requests can still be analyzed during a digital forensic investigation.

Based on these results, the National Institute of Standards and Technology (NIST) method has proven effective as a digital forensic investigation framework for analyzing VPN-based network traffic, as it facilitates the structured and systematic identification, examination, analysis, and documentation of digital evidence.

6. REFERENCES

[1] F. Yasin, Abdul Fadlil, and Rusydi Umar, "Identifikasi bukti forensik jaringan virtual router menggunakan metode NIST," Jurnal Resti (Rekayasa Sistem dan Teknologi Informasi), vol. 5, no. 1, pp. 91–98, Feb. 2021, doi: 10.29207/resti.v5i1.2784.

[2] Y. Santoso and M. Raharjo, "Implementasi OpenVPN untuk work from home pada jaringan server di PT.Infokom Elektrindo," Media Jurnal Informatika, vol. 17, no. 1, 2025, doi: 10.35194/mji.v17i1.5040.

[3] K. Khairunnisak, H. Ashari, and A. P. Kuncoro, "Analisis forensik untuk mendeteksi keaslian citra digital menggunakan metode NIST," Jurnal Resistor (Rekayasa Sistem Komputer), vol. 3, no. 2, pp. 72–81, 2020.

[4] H. Haeruddin, S. E. Prasetyo, and A. W. Kaharuddin, "Optimalisasi keamanan jaringan di era digital menggunakan metode Zero Trust," Journal of Information System and Technology, vol. 5, no. 3, pp. 15–24, Dec. 2024, doi: 10.37253/joint.v5i3.9986.

[5] R. E. Putro and I. R. Widiasari, "Analisis keamanan komunikasi VoIP server portable dilengkapi OpenVPN menggunakan Linux Asterisk," Jurnal Media Informatika Budidarma, vol. 6, no. 2, p. 943, Apr. 2022, doi: 10.30865/mib.v6i2.3884.

[6] D. Yuliana, T. Yuniati, and B. P. Zen, "Analisis forensik terhadap kasus cyberbullying pada Instagram dan Whatsapp menggunakan metode National Institute of Justice (NIJ)," Cyber Security dan Forensik Digital, vol. 5, no. 2, pp. 52–59, 2023.

[7] R. A. Bintang, R. Umar, and A. Yudhana, "Analisis media sosial Facebook Lite dengan tools forensik menggunakan metode NIST," Techno (Jurnal Fakultas Teknik, Universitas Muhammadiyah Purwokerto), vol. 21, no. 2, pp. 125–130, 2020.

[8] I. Riadi, F. Tella, S. Informasi, F. Sains dan Teknologi Terapan, and U. Ahmad Dahlan, "Analisis forensik pada email menggunakan metode National Institute of Standards and Technology," MEI, 2022.

[9] A. R. Saraha, S. Umar, and N. Sugrah, "Model forensik literasi dalam pembelajaran daring di masa pandemi: Efektivitas pembelajaran dan responsnya," Jurnal Inovasi Pendidikan IPA, vol. 7, no. 1, pp. 22–33, Jul. 2021, doi: 10.21831/jipi.v7i1.34149.

[10] M. Affandi, "Implementasi Virtual Private Network (VPN) OpenVPN dengan keamanan sertifikat SSL pada Network Attached Storage (Nas) Freenas," Jurnal Impresi Indonesia (JII), vol. 1, no. 12, 2022.

[11] D. N. Amadi, A. Budiman, and P. Utomo, "Analysis of the effectiveness of VPN and PPTP protocol in E-Link Health Report Application Using NDLC Method," Journal of Information Systems and Informatics, vol. 6, no. 2, pp. 949–958, Jun. 2024, doi: 10.51519/journalisi.v6i2.746.

[12] N. A. I. Maniar and T. Yuniati, "Implementasi mobile forensic pada aplikasi Michat dan Telegram dengan Framework NIST 800-101," Cyber Security dan Forensik Digital, vol. 5, no. 2, pp. 60–65, 2023.

[13] F. Wahyu Christanto and C. Krisna Angga Riski, "Komparasi Quality of Service Protokol Virtual Private Network menggunakan PPTP, L2TP, SSTP, dan OpenVPN," Jurnal Telekomunikasi dan Komputer, vol. 15, no. 1, pp. 1–12, 2025, doi: 10.22441/incomtech.v15i1.23250.

[14] D. Mutiara Syafitri and F. Fachri, "Analisis forensik digital Telegram pada Android untuk cybercrime dengan kerangka National Institute of Standards and Technology (NIST)," Rabit : Jurnal Teknologi dan Sistem Informasi Univrab, vol. 10, no. 1, pp. 41–50, Jan. 2025, doi: 10.36341/rabit.v10i1.5402.

[15] A. Pujiyanta and I. Maulana, "Analisis forensik aplikasi penipuan berbasis Android menggunakan metode NIST," JIKA (Jurnal Informatika), vol. 8, no. 2, p. 187, Apr. 2024, doi: 10.31000/jika.v8i2.10575.

[16] S. T. Oktavia, D. F. Priambodo, N. Trianto, and R. Purwoko, "Comparative Quality of Service Analysis of VPN protocols on IPv6," Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI), vol. 12, no. 3, pp. 461–471, Jan. 2024, doi: 10.23887/janapati.v12i3.69264.

[17] A. FFaizal and A. Luthfi, "Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis," Journal of Information Systems and Informatics, vol. 6, no. 2, pp. 701–718, Jun. 2024, doi: 10.51519/journalisi.v6i2.717.

[18] M. A. D. Putra, A. W. Muhammad, B. P. Zen, R. Y. Kisworini, and T. Rohayati, "Analisis forensik pada Instagram dan TikTok dalam mendapatkan bukti digital dengan menggunakan metode NIST 800-86," Jurnal Sistem Informasi Galuh, vol. 2, no. 1, pp. 44–54, 2024.

[19] B. A. Gumelar, G. D. S. Putra, and D. N. Amadi, "Mikrotik VPN shielding E-Link Health Reports: Strengthening Data Security at Madiun Health Office," Journal of Information Systems and Informatics, vol. 5, no. 3, pp. 1194–1203, Sep. 2023, doi: 10.51519/journalisi.v5i3.524.

[20] J. Studi Islam dan Bahasa Arab, K. Anwar, and I. Muhammad Yunus, "AL-QIBLAH: Penggunaan aplikasi Virtual Private Network pada situs internet terblokir (studi komparatif hukum Islam dan hukum positif) use of Virtual Private Network Applications on Blocked Internet Sites (Comparative Study of Islamic Law and Positive Law)," vol. 2, no. 4, pp. 456–478, 2023, doi: 10.36701/qiblah.v2i4.

[21] H. FIkri, "Implementasi VPN server menggunakan protokol L2TP dan IPSEC pada PT. Multi Terminal Indonesia," Jurnal Teknologi Informasi, vol. 10, no. 2, pp. 116–126, 2024.

[22] Prayogi Wicaksana, F. Hadi, and Aulia Fitrul Hadi, "Perancangan implementasi VPN server menggunakan protokol L2TP dan IPSec sebagai keamanan jaringan," Jurnal KomtekInfo, pp. 169–175, Aug. 2021, doi: 10.35134/komtekinfo.v8i3.128.

[23] M. Iqbal, "Analysis of Security Virtual Private Network (VPN) Using OpenVPN," International Journal of Cyber-Security and Digital Forensics, vol. 8, no. 1, pp. 58–65, 2019, doi: 10.17781/P002557.

[24] H. S. Mikayla, A. Kusyanti, and P. H. Trisnawan, "Analisis forensik digital untuk investigasi kasus cyberbullying pada media sosial Tiktok," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 11, no. 5, pp. 1113–1124, Oct. 2024, doi: 10.25126/jtiik.2024118017.

[25] A. G. Prayogo and I. Riadi, "Digital Forensic Signal Instant Messages Services in Case of Cyberbullying using Digital Forensic Research Workshop Method," Int. J. Comput. Appl., vol. 184, no. 32, pp. 21–29, oct. 2022, doi: 10.5120/ijca2022922393.

[26] M. Syukri, I. Riadi, and T. Sutikno, "Validation and Evaluation of Browser Forensics Using Digital Forensic Approach Based on the National Institute of Standards and Technology (NIST) Framework," Jurnal Teknik Informatika (Jutif), vol. 6, no. 4, pp. 2516–2529, Sep. 2025, doi: 10.52436/1.jutif.2025.6.4.4977.

[27] D. Royadi, M. Asfi, and A. Sevtiana, "Implementasi metode standar NIST dalam analisis data forensik studi kasus penipuan salah transfer mencatut nama Wabup pada SMP Ar-rohman Krangkeng," LOFIAN: Jurnal Teknologi Informasi dan Komunikasi, vol. 3, no. 1, pp. 12–19, Aug. 2023, doi: 10.58918/lofian.v3i1.216.

[28] M. Hajar Akbar, U. Ahmad, D. Yogyakarta, and I. Sunardi, "Analysis of Steganography on Digital Evidence using General Computer Forensic Investigation Model Framework," 2020.

[29] K. Mochammad et al., "Artikel Nusantara Computer and Design Review pengukuran performa jaringan internet menggunakan Quality of Service dengan Wireshark," NCDR, vol. 3, no. 1, pp. 9–14, 2025.

[30] F. Firmansyah, A. Fadlil, and R. Umar, "Evaluasi optimalisasi alat forensik keamanan jaringan pada lalu lintas virtual router," Edu Komputika Journal, vol. 10, no. 2, pp. 81–92, 2023.

.