Accredited Ranking SINTA 2
Decree of the Director General of Higher Education, Research and Technology, No. 158/E/KPT/2021
Validity period from Volume 5 Number 2 of 2021 to Volume 10 Number 1 of 2026

Published online on: **http://jurnal.iaii.or.id**

JURNAL RESTI
(Rekayasa Sistem dan Teknologi Informasi)
Vol. 7 No. 2 (2023) 208 - 217 ISSN Media Electronic: 2580-0760

TAARA Method to Processing on the Network Forensics in the Event of an ARP Spoofing Attack

Agus Wijayanto[1], Imam Riadi[2], Yudi Prayudi[3]
[1]Information Technology, Universitas Mulia
[2]Department of Information System, Universitas Ahmad Dahlan
[3]Department of Informatics, Universitas Islam Indonesia
[1]aguswijayanto@universitasmulia.ac.id, [2]imam.riadi@is.uad.ac.id, [3]prayudi@uii.ac.id

Abstract

According to reports in 2021 by Kaspersky, requests for investigations into suspicious network activity, such as ARP Spoofing, which can result in sophisticated attacks, reached up to 22%. Several difficulties with examining network systems have been overcome thanks to network forensic investigations. This study aims to perform a network forensic analysis of ARP spoofing attacks using Wireshark forensic tools and Network Miner with a sniffer design process to capture traffic on the router side. In order to gather reliable evidence, this study employs the TAARA method as a network forensic investigation process. Based on the research conducted, it can be demonstrated that an attack took place from eight PCAP files. The information that was gathered, such as the IP address and MAC address of the attacker, the IP address and MAC address of the target, and the date and time of the attack are examples of evidence information that was gathered. This study also shows that network forensic operations can use the Wireshark forensic tool to obtain more detailed data.

Keywords: *ARP spoofing, tazmen sniffer protocol, TAARA, network forensics*

1. Introduction

One of the IT industry's organizations, Kaspersky, has disclosed the findings of its 2021 study on response incidents, reaching up to 22%. Based on reports of 22% of investigation requests related to suspicious network activity [1]. ARP Spoofing or Poisoning attacks are one type of network activity that falls under this category. ARP Spoofing is a straightforward attack that, if successful, can open the door to more complex attacks [2]. The effect of an ARP Spoofing assault is that it can generate additional attacks, such as a Man in the Middle attack, which is typically used to listen to the victim's network traffic. This is one of the potential consequences of the attack. ARP Spoofing attacks are also frequently used as a method for creating denial of service attacks, which can render network systems inoperable by overloading server resources and preventing those resources from catering to the needs of genuine network users. Because ARP spoofing is an assault that can be utilized to attack the target in a relatively short amount of time, a rapid investigation is required in order to counteract this attack effectively. However, in an investigation, not only speed but also scientific proof are required so that the evidence already gathered has weight in the eyes of the law [3].

One of the investigative approaches utilized for the network forensics investigation process is TAARA, which stands for Trigger Acquire Analysis Report and Action. TAARA, which evolved from the Threat Assessment and Remediation Analysis Methodology, has a smaller scope and fewer resources for dealing with cyber threats or cybercrime [4]. Network forensics is a method of collecting, recording, and analyzing network traffic in order to obtain information about cyber threats or attacks, which is then used to describe the actual events that occurred [5], [6]. However, it does not end with the investigative process of gathering digital evidence. During the investigation, cyberthreats or attacks involving network technology may continue. In contrast to computer forensics, all computer activities are halted during the investigation process. Network forensics, in this view, supplements mitigation efforts to improve network security [7].

In a previous study, the network forensics process resolved several cyber attacks by employing a general forensic investigation methodology [8–11]. A previous study described the network forensics process during a flooding attack. The flooding attack is part of a Denial of Service (DoS) attack, which is a sophisticated network attack that overloads web server resources and

Accepted: 14-10-2022 | Received in revised: 13-02-2023 | Published: 03-03-2023

poses a serious threat to network infrastructure. The investigation process follows the forensic process model, with four stages beginning with collection, continuing with examination, analysis, and concluding with report [12], [13]. Other studies use the forensic process model when performing network forensics on MITM attacks, which are part of advanced network attacks [14]. MITM attacks are frequently linked to credential theft, which is considered a cybercrime, and a method for sniffing the victim's network traffic communications against the gateway that are exchanged between users in some systems covertly [15], [16] . Among the cybercrime attacks mentioned, the effect of the ARP spoofing attack initiator is one example [17–19].

Several studies on ARP spoofing attacks have one fundamental problem in common: confirming that a device has executed ARP instructions using only detection methods [20]. Valid proof against ARP spoofing attacks would be a time-consuming process. The investigation process may employ either dead or live forensic techniques [21–23]. However, a forensic investigation method or framework must be used as a guide in each stage of the investigation [24], [25]. Every stage or phase will always come into contact with digital evidence that is easily damaged [26].

Previous research has only focused on investigative approaches on the host side to find evidence of ARP spoofing attacks. This study completes the form of network forensic investigation through an approach on the router device side using a packet sniffer that includes a packet sniffer protocol (TZSP).

This study aims to conduct a network forensic analysis of ARP spoofing attacks to obtain any evidence that can be extracted through an investigative approach on the router side. This study uses the TAARA method as an investigation method, which is considered appropriate as a network forensic process with the stages of mitigating ARP spoofing attacks, which can lead to dangerous follow-up attacks. The research objectives were determined and then sequenced as follows: (i) to perform a simulated ARP spoofing attack as a case study material, (ii) to collect data with forensic procedures, (iii) to learn the results of case study analysis, (iv) to generate evidence reports, and (v) to validate the evidence.

2. Research Methods

This research was done in the Computer Laboratory at the Faculty of Computer Science at Mulia University in Balikpapan from February to September 2022. Research materials and tools are needed to help reach research objectives during the implementation phase. The research material is a dataset of ARP spoofing attack simulations made in the Computer Laboratory. The research tools are Wireshark, network miner, arpspoof, kickthemout, ettercap, bettercap, twenty-seven computers, and the network infrastructure, which includes a CCR1009 router and a US-48 PoE switch.

The research method is the stage in research that is used to achieve results that are consistent with the formulation and objectives of the problem [27]. The algorithm was chosen in the form of a flowchart by adding the TAARA stages. The research methods flowchart is shown in Figure 1.

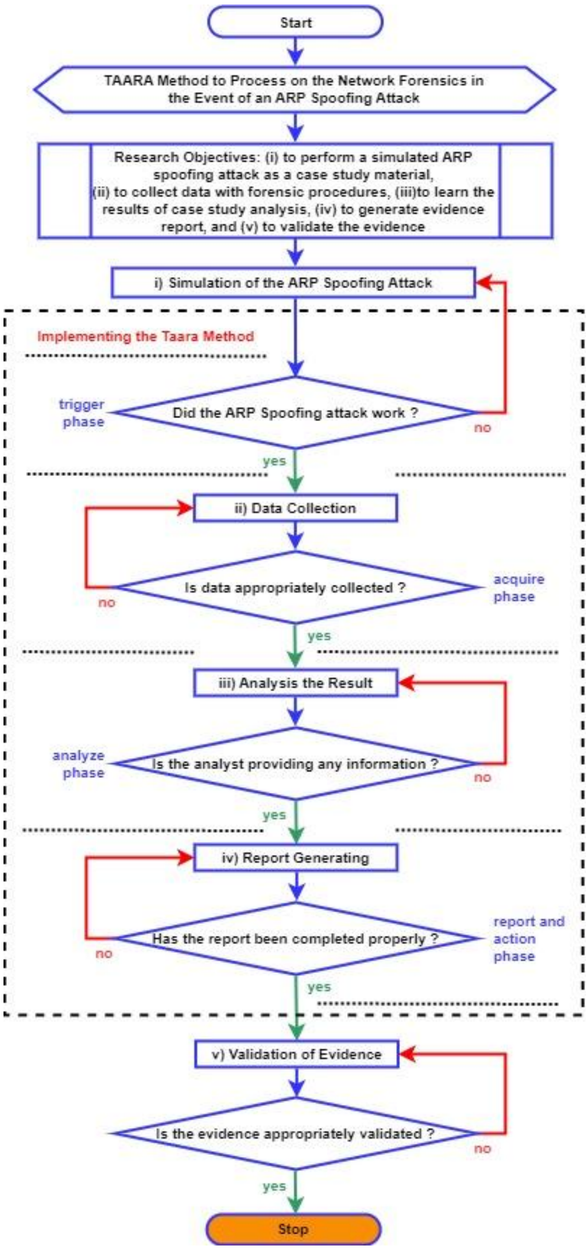

Figure 1. The research methods flowchart

According to Figure 1, which depicts the adoption of the TAARA approach into the research flow as a forensic investigation process, TAARA comprises five steps, which are as follows: The trigger is the initial stage; a trigger is any activity conducted in response to

DOI: https://doi.org/10.29207/resti.v7i2.4589

an assault that gives the investigator the instruction to begin an investigation into the incident. The second stage is acquire; the process of gathering all sorts of evidence and information to build a hypothesis about the cause of an assault is referred to as acquire.

The stage of acquisition is a reaction to a suspicious behavior trigger that occurred in the stage before it. The next stage is analyze: analyze the process of collecting evidence and existing information, then correlate them so that they raise questions regarding the attacks that occurred. Next is the report. The report is the preparation of a report based on the analysis results, documenting all activities related to the findings.

3. Results and Discussions

Based on the case simulation, an investigational design was offered by capturing network traffic on the router side using the sniffer method. The implementation of the TAARA method serves as a foundation for analyzing ARP spoofing attacks.

3.1 Performing on the Simulation of an ARP Spoofing Attack as a Case Study

In this study, evidence is gathered by simulating cases in real networks. Then, we use the results of this scenario to create a dataset of network traffic capture. A fictional scenario of the case simulation is shown in Figure 2.

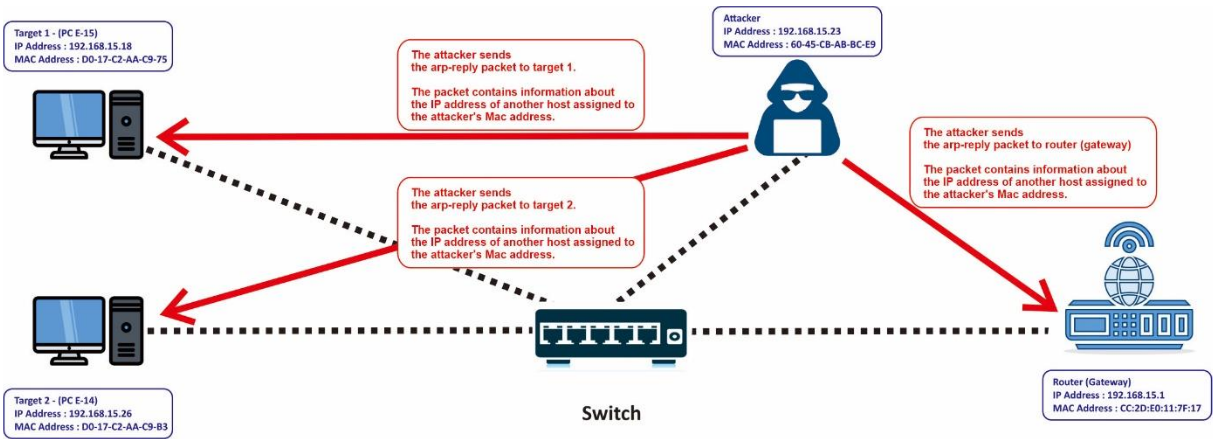

Figure 2. A fictional scenario of the case simulation

Guided by Figure 2 it is shown, that the illustrates an attacker with IP address 192.168.15.23 and Mac address 60-45-CB-AB-BC-E9 targeting two computer devices. The first machine has IP address 192.168.15.18 and Mac address D0-17-C2-AA-C9-75, while the second computer has IP address 192.168.15.26 and Mac address D0-17-C2-AA-C9-B3.

The attacker sends an ARP-reply despite the lack of an ARP-request in order to modify the target's ARP table.

The attacker takes advantage of a router, which is typically the gateway for all computer devices and has the identity IP address 192.168.15.1 Mac address CC-2D-E0-11-7F-17. ARP spoofing is an attack that exploits flaws in the ARP protocol in order to change a victim's ARP table cache contents. A depict how the attack was carried out by sending ARP-reply packets. The attacker sends an ARP-reply packet to IP address 192.168.15.18 is shown in Figure 3.

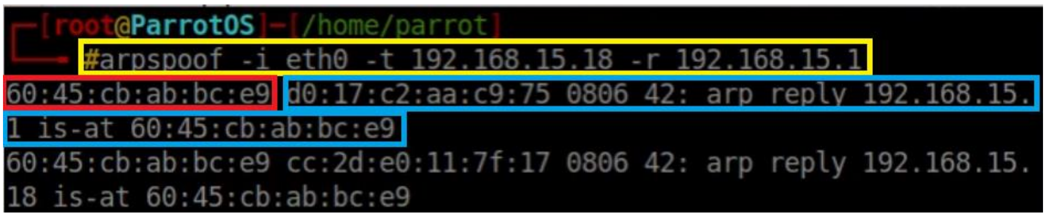

Figure 3. The attacker sends an ARP-reply packet to IP address 192.168.15.18

Based on Figure 3 it can be explained that the depiction of a scenario for carrying out an ARP spoofing attack against the target IP address 192.168.15.18 is highlighted in the yellow box. The message is colored red and blue, showing that the target, who has the mac address D0-17-C2-AA-C9-75, is receiving the packet in the form of an ARP-reply alerting them that IP address 192.168.15.1 has the mac address 60-45-cb-ab-bc-e9. Meanwhile, the IP address 192.168.15.26 is the next target, using the same attack approach, namely sending the ARP-reply packet. The attacker sends an ARP-reply packet to IP address 192.168.15.26 is shown in Figure 4.

DOI: https://doi.org/10.29207/resti.v7i2.4589

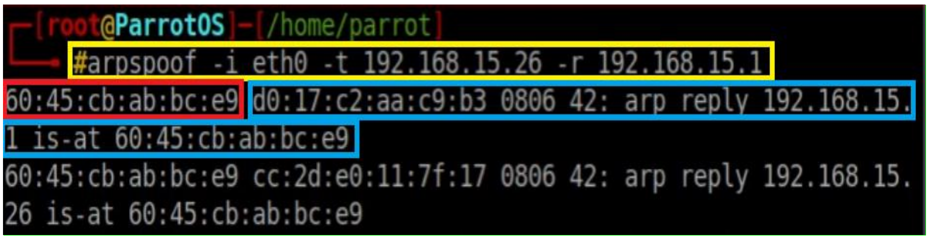

Figure 4. The attacker sends an ARP-reply packet to IP address 192.168.15.26

Based on Figure 4, it can be explained that when the attack simulation is launched, the process of recording network traffic on the router side is also started. This network traffic data is then used for examination purposes.

3.2 Collecting the Data

A process design for the network traffic that was collected. The design process sniffer is shown in Figure 5.

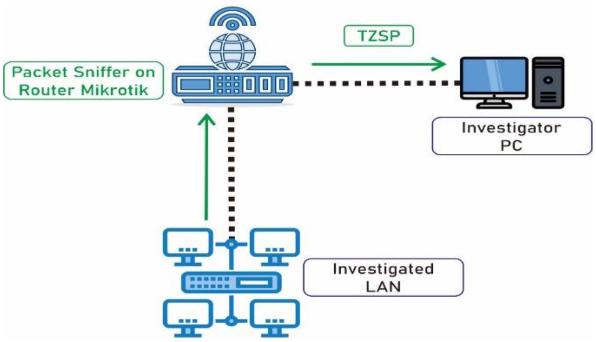

Figure 5. The design process sniffer

Based on Figure 5, it can be explained, that the process of sniffing, which takes place on the router's end, is transmitted in a remote fashion to the investigator's personal computer. The flow of the investigation procedure starts with the sniffer method on the router's side. This approach makes use of the sniffer technique and transmits it toward the LAN region that is being investigated. The Tazmen Sniffer Protocol (TZSP), which encapsulates various other protocols, is next transmitted as into packet sniffer to the PC Investigator.

While the attack simulation is underway, traffic is being recorded simultaneously. This recording produces eight PCAP files based on the attack simulation. The evidence file must be duplicated because the original file, which is known as such, needs to be protected from damage. Testing the evidence file's integrity using the Linux terminal's md5sum command is required prior to replication. Figure 6 shows eight PCAP files in total, each with a different MD5 hash value displayed in red and the file names displayed in blue. Sniffer output from the router side yields eight PCAP files is shown in Figure 6.

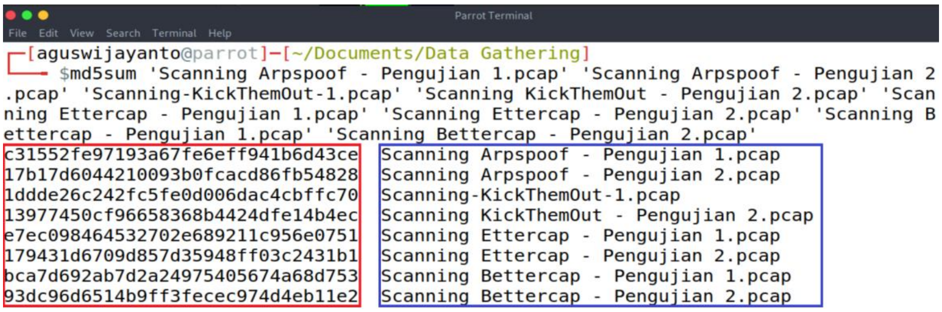

Figure 6. Sniffer output from the router side yields eight PCAP files

Based on Figure 6 it can be explained, in order to validate the validity of evidence files that were obtained using acquisition methods that involved duplication, network miner forensic tools are utilized to do analysis on the evidence files and compare their MD5 values. In order to compare the MD5 values, this step must first be taken. This evaluation will not only shield the evidence from additional scrutiny in the future by other investigators, but it will also ensure that the acquired evidence retains its integrity. Those are two very important outcomes of this process. Figure 6 demonstrates that comparing the MD5 value of each PCAP file check to the md5sum check provided in Figure 7 results in the same hash value.

DOI: https://doi.org/10.29207/resti.v7i2.4589

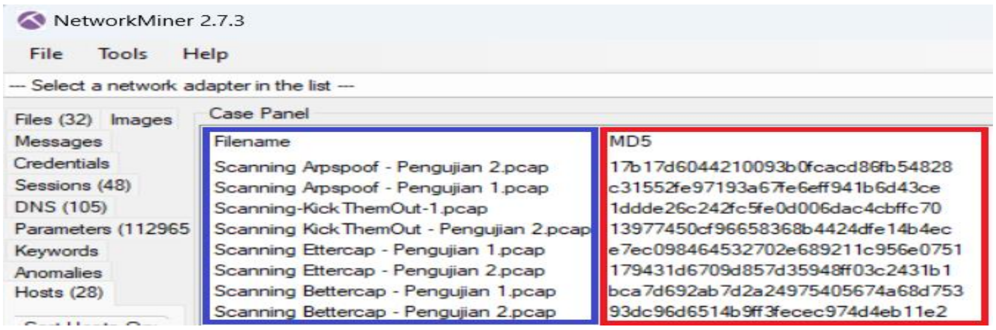

Figure 7. MD5 hash validation

3.3 Learning the Result

Analysis is a step of investigation that goes further in-depth and focuses on signs of an attack that has already happened. The ARP protocol will be the subject of this analysis. The first check is connected to the ARP protocol by filtering on the name field; this analysis seeks to map the IP address with the MAC address based on the initial timestamp. Process on the Computer-E15 in translating the IP address to the Mac address is shown in Figure 8.

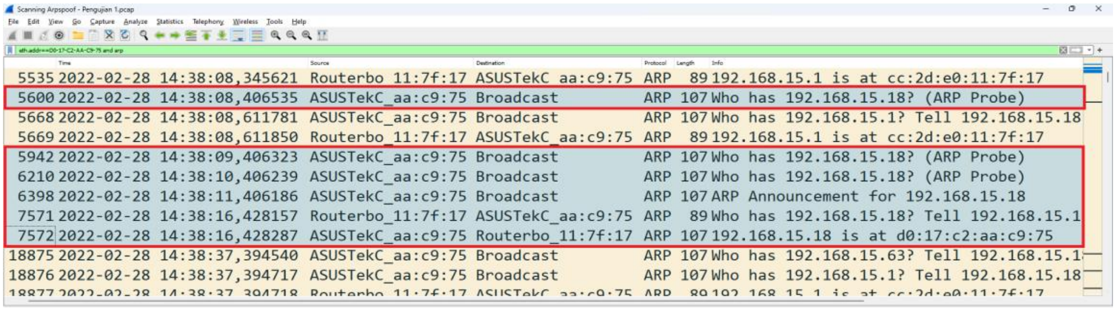

Figure 8. Process on the Computer-E15 in translating the IP address to the Mac address

Based on Figure 8 it can be explained, that starting in frame 5600, PC E-15 broadcasts messages across the local network to translate IP 192.168.15.18 to its Mac Address D0-17-C2-AA-C9-75. The broadcast messages are repeated and are visible in frames 5942 and 6210. ARP Probe, which is an ARP-Request that asks for a response if the request for an IP address has one already, is described in the frame that has been mentioned. Frame 6398 announces that IP 192.168.15.18 is claimed by Mac Address D0-17-C2-AA-C9-75 when no response is received. On frame 7571, communication continues using the ARP protocol as the router with Mac Address CC-2D-E0-11-7F-17 queries Mac Address D0-17-C2-AA-C9-75 for the IP address of 192.168.15.18. According to frame 7572, the IP Address 192.168.15.18 has currently been translated to the Mac Address D0-17-C2-AA-C9-75.

Process on the Computer-E14 in translating the IP address to the Mac address is shown in Figure 9.

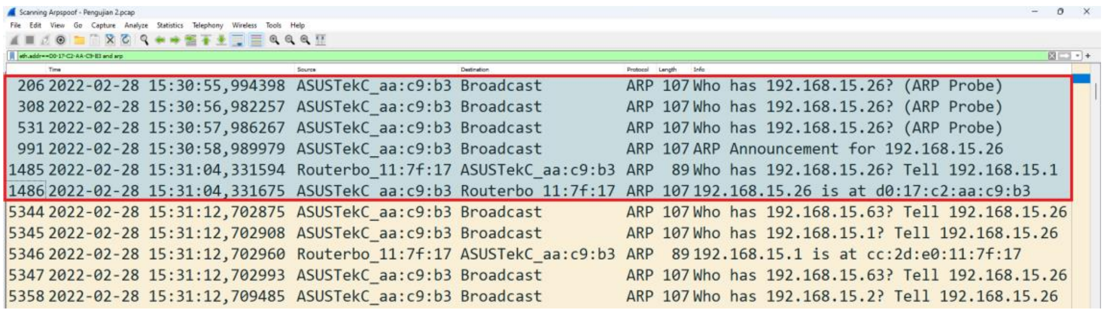

Figure 9. Process on the Computer-E14 in translating the IP address to the Mac address

Based on Figure 9 it can be explained, that PC E-14 process then doesn't differ all that much from the PC E-15 process's explanation. The local network visible in frames 206, 308, and 531 receives a broadcast message from a device with the Mac address D0-17-C2-AA-C9-B3. The device then announces its ownership of the IP address 192.168.15.26 via an ARP announcement in frame 991. Frame 1486 from this device informs the router that MAC address D0-17-C2-AA-C9-B3 has been given IP address 192.168.15.26.

Network mining tools are also utilized in the investigation, although they can only supply limited information in this ARP spoofing attack case study depicted. Examination using the Network Miner Tool is shown in Figure 10.

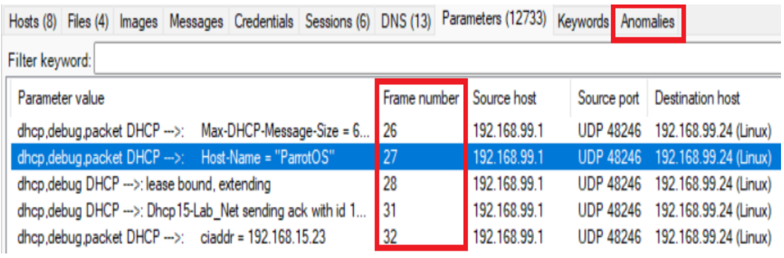

Figure 10. Examination using the Network Miner tool

Based on Figure 10 it can be explained that several frames cannot be read or displayed. Frames 26, 27, 28, 31, and 32 are visible; however, frames 29 and 30 are unreadable. Unreadable frames were discovered throughout the same stages of examination of the other PCAP file.

The network miner menu's anomaly section shows that no suspicious signs were discovered while it was in use. Thus, it can be said that the network miner is no more effective for investigating this instance than the Wireshark tool. However, as illustrated in Figure 7 in section 3.2, network miners are particularly helpful for MD5 validation testing.

From comparing the two inspection tools, it can be seen that the Wireshark tool can provide details for each IP address, which are then translated to MAC addresses for each device based on the timestamp. The IP address was translated to Mac address devices E-14 and E-15 for the first time is shown in Table 1.

Table 1. The IP address was translated to Mac address devices E-14 and E-15 for the first time

No.	Filename	Timestamp	Device	Frame
1	Scanning Arpspoof - Pengujian 1.pcap	Feb 28, 2022 14:37:58	E-15	7572
2	Scanning Arpspoof - Pengujian 2.pcap	Feb 28, 2022 15:31:04 Feb 28, 2022 15:31:27	E-14 E-15	1486 11262
3	Scanning-KickThemOut-1.pcap	Feb 28, 2022 10:54:20	E-15	11657
4	Scanning KickThemOut - Pengujian 2.pcap	Feb 28, 2022 13:45:20 Feb 28, 2022 13:45:37	E-14 E-15	1481 6356
5	Scanning Ettercap - Pengujian 1.pcap	Mar 3, 2022 14:24:47	E-15	9375
6	Scanning Ettercap - Pengujian 2.pcap	Mar 3, 2022 14:50:21 Mar 3, 2022 14:50:45	E-14 E-15	1353 10220
7	Scanning Bettercap - Pengujian 1.pcap	Mar 2, 2022 11:37:02	E-15	11566
8	Scanning Bettercap - Pengujian 2.pcap	Mar 3, 2022 10:50:18 Mar 3, 2022 10:50:40	E-14 E-15	2019 9418

Based on Table 1 it can be explained, that the analysis above creates a record which will show that the IP addresses 192.168.15.18 and 192.168.15.26 have been translated to each device's Mac address complete with a date based on the findings of the analysis using the Wireshark tool.

The next step is to conduct an analysis in order to collect information about the attacker's device that duplicates the IP address listed in Table 1. Evidence of IP Address Duplication for 192.168.15.18 is shown in Figure 11.

Based on Figure 11 it can be explained, that depicts the analysis performed with the Wireshark tool. There are three red squares in ascending order. The first red box represents the packet list window, which displays the frame number, time, source, destination, protocol, and info. The second and third red boxes are included in the packet details pane. From the packet detail pane frame 127439, it is evident that the IP address for IP 192.168.15.18 has been duplicated by MAC Address 60-45-CB-AB-BC-E9. The IP address 192.168.15.18 was already translated in Table 1 and assigned to the MAC address D0-17-C2-AA-C9-75. The evidence of IP Address Duplication for 192.168.15.26 is shown in Figure 12.

Based on Figure 12 it can be explained, that the analysis procedure is largely the same as that in Figure 11. The investigation conducted shows that the IP address 192.168.15.26 has been duplicated. Frame 45301 contains all of this information, including the time the IP address duplication took place. The same process is used for all PCAP files' analysis, which entails filtering for the term "arp.duplicate-address-detected." Analyzing the PCAP files "Scanning-KickThemOut-1.pcap" and "Scanning KickThemOut - Pengujian 2.pcap," different information was discovered. The IP

DOI: https://doi.org/10.29207/resti.v7i2.4589

address discovered in the duplicate is the Gateway Router's IP Address. The Gateway Router's IP address was discovered during the duplication. Although the primary targets were E-15 and E-14, no duplicate IP addresses were discovered. This demonstrates the usage of many attack tools, each of which can have a different effect on the exploitation process. The IP Address Proof discovered in the duplicates is the Gateway Router IP address. The evidence of IP address duplication for 192.168.15.1 is shown in Figure 13.

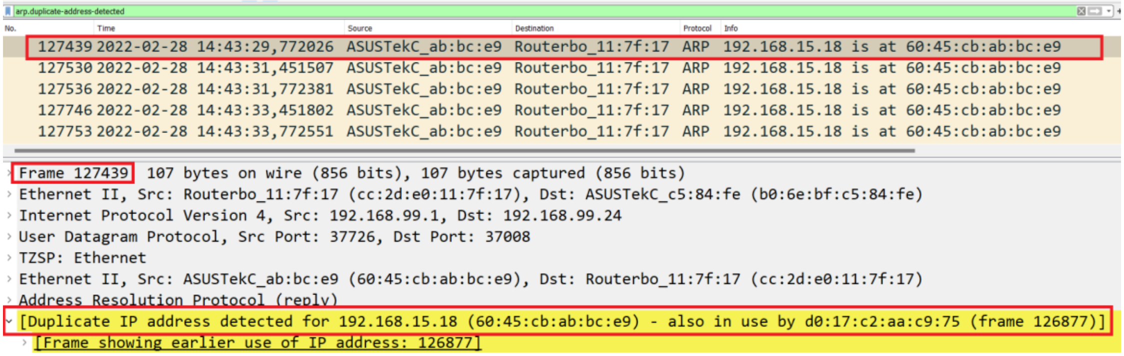

Figure 11. Evidence of IP address duplication for 192.168.15.18

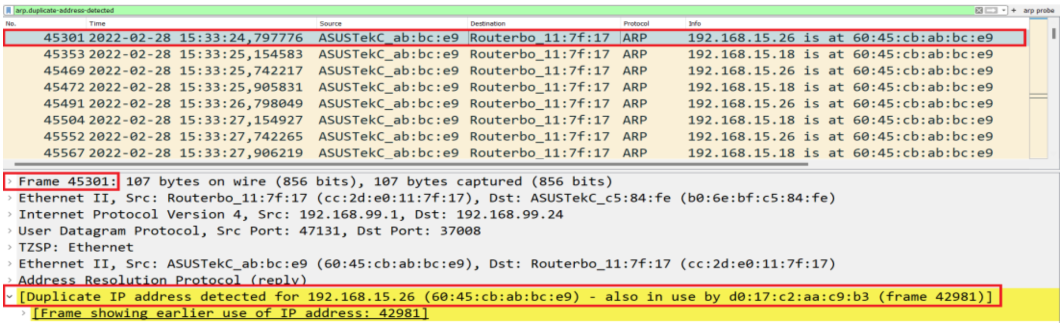

Figure 12. The evidence of IP address duplication for 192.168.15.26

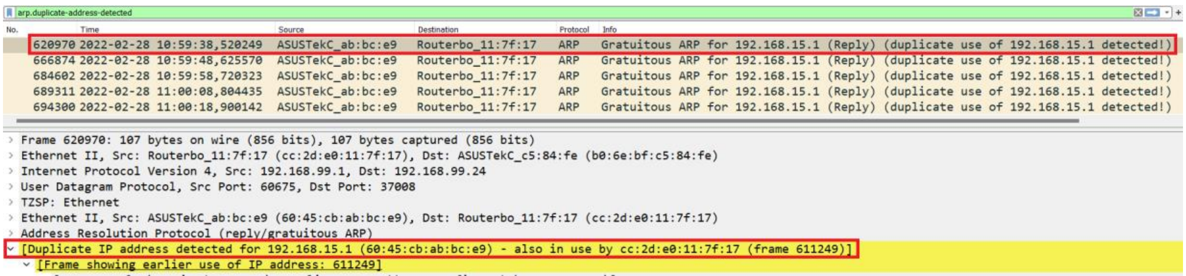

Figure 13. The evidence of IP address duplication for 192.168.15.1

Based on Figure 13 it can be explained, that an examination of the PCAP file produced by an ARP spoofing attack using the kickthemout tool. In contrast to other evidence acquired, the information obtained is ARP-free. However, the attacker can still be identified if he or she has duplicated the IP address 192.168.15.1 that should be utilized by the gateway router with the MAC address CC-2-E0-11-7-17-17. The results of this analysis provided proof of IP duplication in the eight PCAP files that were gathered and displayed. Results of evidence analysis information is shown in Table 2.

Table 2. Results of evidence analysis information

Filename	IP address duplication detected
Scanning Arpspoof - Pengujian 1.pcap	Proven to duplicate the E-15 target
Scanning Arpspoof - Pengujian 2.pcap	Proven to duplicate the E-15 and E-14 target
Scanning-KickThemOut-1.pcap	Proven to duplicate the Router Gateway
Scanning KickThemOut - Pengujian 2.pcap	Proven to duplicate the Router Gateway
Scanning Ettercap - Pengujian 1.pcap	Proven to duplicate the E-15 target
Scanning Ettercap - Pengujian 2.pcap	Proven to duplicate the E-15 and E-14 target
Scanning Bettercap - Pengujian 1.pcap	Proven to duplicate the E-15 target
Scanning Bettercap - Pengujian 2.pcap	Proven to duplicate the E-15 and E-14 target

DOI: https://doi.org/10.29207/resti.v7i2.4589

3.4 Reporting the Evidence

This stage will present all the activities carried out from the previous step in the form of a report. Reports provide information regarding the attack, including details of the attacker and victim, and can reconstruct the attack as the incident occurred. Writing reports on ARP spoofing attacks using the TAARA stages is a serious goal of this project. To make the report stage's contents easier to understand, the findings of the exposure report based on the attack's evidence will attempt. The evidence reports is shown in Table 3.

Table 3. The evidence report

Filename	IP Attacker	Mac Attacker	IP Victim	Mac Victim	Timestamp	Frame Information
Scanning Arpspoof - Pengujian 1.pcap	192.168.15.23	60-45-cb-ab-bc-e9	192.168.15.18	D0-17-C2-AA-C9-75	28/02/2022 14:43:30	127439
Scanning Arpspoof - Pengujian 2.pcap	192.168.15.23	60-45-cb-ab-bc-e9	192.168.15.26	D0-17-C2-AA-C9-B3	28/02/2022 15:33:23	45034
			192.168.15.18	D0-17-C2-AA-C9-75	28/02/2022 15:33:25	45301
Scanning-KickThemOut-1.pcap	192.168.15.23	60-45-cb-ab-bc-e9	192.168.15.1	CC-2D-E0-11-7F-17	Feb 28, 2022 10:59:38	620970
Scanning KickThemOut - Pengujian 2.pcap	192.168.15.23	60-45-cb-ab-bc-e9	192.168.15.1	CC-2D-E0-11-7F-17	Feb 28, 2022 13:54:12	145141
Scanning Ettercap - Pengujian 1.pcap	192.168.15.23	60-45-cb-ab-bc-e9	192.168.15.18	D0-17-C2-AA-C9-75	03/03/2022 14:28:12	78204
Scanning Ettercap - Pengujian 2.pcap	192.168.15.23	60-45-cb-ab-bc-e9	192.168.15.26	D0-17-C2-AA-C9-B3	03/03/2022 14:54:33	58080
			192.168.15.18	D0-17-C2-AA-C9-75	03/03/2022 14:54:33	58076
Scanning Bettercap - Pengujian 1.pcap	192.168.15.23	60-45-cb-ab-bc-e9	192.168.15.18	D0-17-C2-AA-C9-75	02/03/2022 11:45:53	537266
Scanning Bettercap - Pengujian 2.pcap	192.168.15.23	60-45-cb-ab-bc-e9	192.168.15.26	D0-17-C2-AA-C9-B3	03/03/2022 10:54:15	55490
			192.168.15.18	D0-17-C2-AA-C9-75	03/03/2022 10:54:15	55489

Based on Table 3 it can be explained, that reveals that after collecting and analyzing a total of 8 files, it has been determined that an ARP Spoofing attack has happened. Each frame in table 4 contains evidence of attack information beginning with the Attacker's IP Address and MAC Address, the Target's IP Address and the Victim's MAC Address, and the Timestamp. With the aid of Wireshark, an investigation of the sniff method on the router's side can be conducted to discover indications of an attack.

The report that is made includes recommendations for actions. The findings of the TAARA method-applied ARP spoofing investigation guide the actions to be taken in order to stop additional ARP spoofing assaults. When signs of an attack are discovered, prompt preventative action can be done. Isolating the attacker's MAC address can be done in this situation as a first defensive measure.

3.5 Validation of the Evidence

The validation stage is to ensure that the results of the network forensics process are true, accurate, and credible and that data integrity can be accounted for so that this has value in the eyes of the law. According to [28] the validation of forensic results at least has the properties of repeatable and reproducible so that it is feasible to be used as digital evidence. The repeatability validation of the attack test of the four tools produces a PCAP file by utilizing the Wireshark analysis tool, which is then examined on the PCAP file using the Wireshark itself and the network miner. For the results of the network miner, there is no evidence of attack information. The validation results are shown in Table 4.

Table 4. Validation result

Filename	Wirehark Tools				
	IP Attacker	Mac Attacker	IP Target	Mac Target	Timestamp
Scanning Arpspoof - Pengujian 1.pcap	Found	Found	Found	Found	Found
Scanning Arpspoof - Pengujian 2.pcap	Found	Found	Found	Found	Found
Scanning-KickThemOut-1.pcap	Found	Found	Found	Found	Found
Scanning KickThemOut - Pengujian 2.pcap	Found	Found	Found	Found	Found
Scanning Ettercap - Pengujian 1.pcap	Found	Found	Found	Found	Found
Scanning Ettercap - Pengujian 2.pcap	Found	Found	Found	Found	Found
Scanning Bettercap - Pengujian 1.pcap	Found	Found	Found	Found	Found
Scanning Bettercap - Pengujian 2.pcap	Found	Found	Found	Found	Found

DOI: https://doi.org/10.29207/resti.v7i2.4589

Filename	Network Miner Tools				
	IP Attacker	Mac Attacker	IP Target	Mac Target	Timestamp
Scanning Arpspoof - Pengujian 1.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning Arpspoof - Pengujian 2.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning-KickThemOut-1.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning KickThemOut - Pengujian 2.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning Ettercap - Pengujian 1.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning Ettercap - Pengujian 2.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning Bettercap - Pengujian 1.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning Bettercap - Pengujian 2.pcap	Not Found	Not Found	Not Found	Not Found	Not Found

Based on Table 4 it can be explained, that the length of time that a validation test is conducted is what differentiates repeatability testing from reproducibility testing. The process of reproducibility takes place over an extended period of time using the same items and tools. In the stage before this one, the tools that were utilized have also been validated for their reproducibility. In the results of a repeatability and reproducibility validation, it was found that the performance of Wireshark displays positive results when compared to network miners for information on ARP spoofing attacks on the use of the TZSP protocol.

4. Conclusion

Based on the results and discussions, the scanning process using a router device can capture network traffic involving the Tazmen sniffer protocol. The TAARA investigative method approach can be used immediately in the process of network forensic investigations, particularly on ARP spoofing attacks. Implementing this method results in the ability to direct and dig up evidence of ARP spoofing attacks launched against targets. A total of eight PCAP files of ARP spoofing attack cases have been identified, each with information on the attacker, the victim, and the time of the incident. The TAARA method directs the action process to prevent further ARP spoofing attacks by blocking the attacker's Mac address immediately. The new findings show that ARP Spoofing attack testing tools have distinct characteristics, such as kickthemout tools that necessitate extra effort when examining evidence of ARP spoofing attacks. Meanwhile, the validation results show that the network forensic tool, Wireshark, outperforms network mining tools in conducting inspections. In future work, there are many attack testing tools freely available on the internet; it is necessary to conduct a comparative study taking into account the characteristics of the tools, which may have different ways of working, making network forensic examinations more difficult.

Reference

[1] Kaspersky, (2021). *Incident Response Analyst Report 2021.* [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/13085018/Incident-Response-Analyst-Report-eng-2021.pdf

[2] T. Girdler and V.G. Vassilakis, "Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks and Blacklisted MAC Addresses," *Computers & Electrical Engineering*, vol. 90, p. 106990, Mar. 2021, https://doi.org/10.1016/j.compeleceng.2021.106990.

[3] G. Tully, N. Cohen, D. Compton, G. Davies, R. Isbell, and T. Watson, "Quality standards for digital forensics: Learning from experience in England & Wales," *Forensic Science International: Digital Investigation*, vol. 32, p. 200905, Mar. 2020, https://doi.org/10.1016/j.fsidi.2020.200905.

[4] R. Umar, I. Riadi, and R.S. Kusuma, "Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method," *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, vol. 6, no. 2, pp. 133–140, May 2021, https://doi.org/10.22219/kinetik.v6i2.1225.

[5] R. Rizal, I. Riadi, and Y. Prayudi, "Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device," *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, vol. 7, no. 4, pp. 382–390, Dec. 2018, http://dx.doi.org/10.17781/P002477.

[6] A. Yudhana, I. Riadi, and F. Ridho, "DDoS Classification Using Neural Network and Naïve Bayes Methods for Network Forensics," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, 2018, https://doi.org/10.14569/IJACSA.2018.091125.

[7] M. Hikmatyar, Y. Prayudi, and I. Riadi, "Network Forensics Framework Development using Interactive Planning Approach," *Int J Comput Appl*, vol. 161, no. 10, pp. 41–48, Mar. 2017, https://doi.org/10.5120/ijca2017913352.

[8] H. Abdulla, H. Al-Raweshidy, and W.S. Awad, "ARP Spoofing Detection for IoT Networks Using Neural Networks," *SSRN Electronic Journal*, 2020, https://doi.org/10.2139/ssrn.3659129.

[9] D. Spiekermann, J. Keller, and T. Eggendorfer, "Network forensic investigation in OpenFlow networks with ForCon," *Digit Investig*, vol. 20, pp. S66–S74, Mar. 2017, https://doi.org/10.1016/j.diin.2017.01.007.

[10] I. Riadi, J. Eko Istiyanto, and A. Ashari, "Log Analysis Techniques using Clustering in Network Forensics," *International Journal of Computer Science and Information Security*, vol. 10, no. 7, 2012, http:// arxiv.org/abs/1307.0072.

[11] R.Y. Patil and S.R. Devane, "Network Forensic Investigation Protocol to Identify True Origin of Cyber Crime," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 5, pp. 2031–2044, May 2022, https://doi.org/10.1016/j.jksuci.2019.11.016.

[12] D. Mualfah and I. Riadi, "Network Forensics For Detecting Flooding Attack On Web Server," *International Journal of Computer Science and Information Security*, vol. 15, no. 2, 2017, [Online]. Available: https://sites.google.com/site/ijcsis/

[13] M. Alim, I. Riadi, and Y. Prayudi, "Live Forensics Method for Analysis Denial of Service (DOS) Attack on Routerboard," *Int J Comput Appl*, vol. 180, no. 35, pp. 23–30, Apr. 2018, https://doi.org/10.5120/ijca2018916879.

[14] D. Saputra, "Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 66–73, 2019, https://doi.org/10.17781/P002558.

[15] I. Riadi, R. Umar, I. Busthomi, and A.W. Muhammad, "Block-hash of blockchain framework against man-in-the-middle attacks," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*,

DOI: https://doi.org/10.29207/resti.v7i2.4589

vol. 8, no. 1, p. 1, May 2021, https://doi.org/10.26594/register.v8i1.2190.

[16] H.H. Satyanegara and K. Ramli, "Implementation of CNN-MLP and CNN-LSTM for MitM Attack Detection System," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 3, pp. 387–396, Jun. 2022, https://doi.org/10.29207/resti.v6i3.4035.

[17] M. Data, "The Defense Against ARP Spoofing Attack Using Semi-Static ARP Cache Table," in *2018 International Conference on Sustainable Information Engineering and Technology (SIET)*, Nov. 2018, pp. 206–210. https://doi.org/10.1109/SIET.2018.8693155.

[18] M. Zengliang, L. Guodong, W. Hongyan, and W. Yong, "Dynamic Trust Model of ARP Real-Time Intrusion Detection Based on Extended Subjective Logic," in *2020 IEEE International Conference on Power, Intelligent Computing and Systems (ICPICS)*, Jul. 2020, pp. 615–618. https://doi.org/10.1109/ICPICS50287.2020.9201994.

[19] M.S. Song, J.D. Lee, Y.S. Jeong, H.Y. Jeong, and J.H. Park, "DS-ARP: A New Detection Scheme for ARP Spoofing Attacks Based on Routing Trace for Ubiquitous Environments," *The Scientific World Journal*, vol. 2014, pp. 1–7, 2014, https://doi.org/10.1155/2014/264654.

[20] V. Rohatgi and S. Goyal, "A Detailed Survey for Detection and Mitigation Techniques against ARP Spoofing," in *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Oct. 2020, pp. 352–356. https://doi.org/10.1109/I-SMAC49090.2020.9243604.

[21] V.R. Kebande, R.A. Ikuesan, N.M. Karie, S. Alawadi, K.K.R. Choo, and A. Al-Dhaqm, "Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments," *Forensic Science International: Reports*, vol. 2, p. 100122, Dec. 2020, https://doi.org/10.1016/j.fsir.2020.100122.

[22] Sunardi, I. Riadi, and A. Sugandi, "Forensic Analysis of Docker Swarm Cluster using Grr Rapid Response Framework," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 2, 2019, https://doi.org/10.14569/IJACSA.2019.0100260.

[23] R. Umar, I. Riadi, and B.F. Muthohirin, "Live forensics of tools on android devices for email forensics," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 4, p. 1803, Aug. 2019, https://doi.org/10.12928/telkomnika.v17i4.11748.

[24] Nickson. M. Karie, V.R. Kebande, H.S. Venter, and K.K.R. Choo, "On the importance of standardising the process of generating digital forensic reports," *Forensic Science International: Reports*, vol. 1, p. 100008, Nov. 2019, https://doi.org/10.1016/j.fsir.2019.100008.

[25] J. Hou, Y. Li, J. Yu, and W. Shi, "A Survey on Digital Forensics in Internet of Things," *IEEE Internet Things J*, vol. 7, no. 1, pp. 1–15, Jan. 2020, https://doi.org/10.1109/JIOT.2019.2940713.

[26] A. Yudhana, I. Riadi, and B. Putra, "Digital Forensic on Secure Digital High Capacity using DFRWS Method," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 6, pp. 1021–1027, Dec. 2022, https://doi.org/10.29207/resti.v6i6.4615.

[27] D. Faroek, R. Umar, and I. Riadi, "Classification Based on Machine Learning Methods for Identification of Image Matching Achievements," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 6, no. 2, pp. 198–206, Apr. 2022, https://doi.org/10.29207/resti.v6i2.3826.

[28] R. Umar, I. Riadi, and G.M. Zamroni, "Mobile Forensic Tools Evaluation for Digital Crime Investigation," *Int J Adv Sci Eng Inf Technol*, vol. 8, no. 3, p. 949, Jun. 2018, https://doi.org/10.18517/ijaseit.8.3.3591.

DOI: https://doi.org/10.29207/resti.v7i2.4589