Forensik Jaringan Terhadap Serangan ARP Spoofing Menggunakan Metode TAARA

Agus Wijayanto
20917002

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia
2023

Lembar Pengesahan Pembimbing

Forensik Jaringan Terhadap Serangan ARP Spoofing Menggunakan Metode TAARA

Agus Wijayanto

20917002

Yogyakarta, Januari 2023

Pembimbing I	Pembimbing II
Dr. Imam Riadi, S.Pd., M.Kom.	Dr. Yudi Prayudi, S.Si., M.Kom.

Lembar Pengesahan Penguji

Forensik Jaringan Terhadap Serangan ARP Spoofing Menggunakan Metode TAARA

Agus Wijayanto

20917002

Yogyakarta, Januari 2023

Tim Penguji,

Dr. Imam Riadi, S.Pd., M.Kom.
Ketua

Dr. Yudi Prayudi, S.Si., M.Kom.
Anggota I

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Anggota II

Mengetahui,
Ketua Program Studi Informatika Program Magister
Universitas Islam Indonesia

Irving Vitra Paputunga, S.T., M.Sc., Ph.D.

Abstrak

Forensik Jaringan Terhadap Serangan ARP Spoofing Menggunakan Metode TAARA

Data pengguna internet tiap tahun mengalami peningkatan, segala bentuk aktivitas baik di organisasi maupun individu kini tidak terlepas dari penggunaan sebuah jaringan. Kemudahan akses informasi menggunakan jaringan menjadi hal positif bagi setiap orang namun disisi lain terdapat hal negatif hasil aktivitas dari pihak yang tidak bertanggungjawab diantaranya melalui serangan *ARP Spoofing*. Teknik penyerangan yang dilakukan dengan mencoba memanipulasi *ARP table cache* sehingga pengguna yang sah dalam jaringan tersebut menjadi tidak dapat melakukan aktivitasnya dengan normal dan penyerang berpotensi melakukan serangan berikutnya. Komunikasi jaringan pada *local area network* dimulai ketika *host* mengirimkan sebuah paket *ARP* secara *broadcast* dengan membawa sebuah alamat *IP* tujuan, *host* yang memiliki alamat *IP* akan membalas dengan mengirimkan *ARP* secara *unicast*. Proses tersebut juga yang digunakan oleh penyerang untuk melakukan serangan spoofing dengan mengirimkan informasi palsu ke pada *host* yang sah dalam jaringan. Saat serangan dilakukan maka *host* akan memperbarui *ARP Table cache* yang dimiliki tanpa disadari, hal ini terjadi juga karena pada protokol *ARP* bersifat stateless atau tidak ada sebuah mekanisme pemeriksaan. Sehingga saat ada *ARP reply* yang datang ke *host* maka tidak akan dilakukan pemeriksaan terkait dengan kebenaran alamat *IP* dan *MAC*, dan akan disimpan pada *ARP Table cache*. Penelitian ini bertujuan untuk mendapatkan informasi bukti dari mana sumber serangan dilancarkan dengan mendapatkan *MAC address*, *IP address* penyerang dan kapan waktu serangan tersebut terjadi. Beberapa *tools* digunakan untuk melakukan sebuah analisa serangan yaitu *wireshark* dan *tcpdump*. Proses forensik jaringan ini akan menggunakan metode *Trigger, Acquire, Analysis, Report, Action (TAARA)* sebagai kerangka kerja untuk menjamin segela bentuk proses aktivitas mulai dari serangan terjadi hingga proses laporan barang bukti. Dengan mengikuti sebuah kerangka kerja maka sebuah bukti yang ditemukan akan memiliki sebuah nilai dan dapat dipertanggung jawabkan saat proses penyampaian hasil dari analisa yang dilakukan.

Kata kunci

arp spoofing,tazmen sniffer protocol, taara, network forensics

Abstract

Network Forensics Against ARP Spoofing Attack Using TAARA Method

Internet user data has increased every year, all forms of activity both in organizations and individuals are now inseparable from the use of a network. Ease of access to information using the network is a positive thing for everyone, but on the other hand there are negative things as a result of activities from irresponsible parties, including through ARP Spoofing attacks. The attack technique is carried out by trying to manipulate the ARP cache table so that legitimate users on the network do not carry out their activities normally and can prevent the next attack. Network communication on a local area network begins when a host sends a broadcast ARP packet carrying a destination IP address, the host having that IP address responds by sending ARP unicast. This process is also used by attackers to carry out spoofing attacks by sending false information to legitimate hosts on the network. When an attack is carried out, the host will unwittingly store the ARP Table cache, this also happens because the ARP protocol is stateless or there is no checking mechanism. So that when an ARP reply comes to the host, it will not check the correctness of the IP and MAC addresses, and will be stored in the ARP Table cache. This study aims to obtain evidence of information from where the source of the attack was launched by obtaining the MAC address, IP address of the attacker, and when the attack occurred. Some of the tools used to perform attack analysis are wireshark and tcpdump. This network forensic process will use the Trigger, Acquire, Analysis, Report, Action (TAARA) method as a framework to guarantee all forms of activity processes, from attacks that occur to the process of reporting evidence. By following a framework, what is found will have a value and can be accounted for during the process of sending the results of the analysis carried out.

Keywords

arp spoofing, tazmen sniffer protocol, taara, network forensics,

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, 20 Januari 2023

Agus Wijayanto, S.Kom

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Agus Wijayanto, Imam Riadi, Yudi Prayudi (2022). Network Forensics Against Address Resolution Protocol Spoofing Attacks Using Trigger Acquire Analysis Report Action Methods. (Register: Jurnal Ilmiah Teknologi Sistem Informasi, Volume 8 Issue 2 2022)

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Agus Wijayanto	Mendesain eksperimen (60%) Menulis *paper* (70%)
Dr. Imam Riadi, S.Pd., M.Kom Dr. Yudi Prayudi, S.Si., M.Kom	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)

Halaman Kontribusi

"**Tidak ada kontribusi dari pihak lain**".

Halaman Persembahan

Alhamdulillah segala puji hanya Milik Allah Subhana Wa Ta'ala yang selalu memberikan rahmatnya kepada setiap makhluk,

Alhamdulillah, hasil dari kerja keras ini saya persembahkan untuk keluarga:

"Kedua orang tua"

Bapak Rusianto dan Ibu Suiswati

"Istriku Tercinta"

Desi Apriani

"Keluarga besar dari Mertua"

Bapak (alm) Rusman Mamma dan Ibu Asni Nawir

"Keluarga Besar Yayasan Airlangga Balikpapan"

Terkhusus Bapak Panca Sugiarto dan Ibu Elly

Kata Pengantar

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Alhamdulillah segala puji bagi Allah Subhana Wa Ta'ala atas segala rahmat, taufik, dan hidayah-Nya sehingga penulisan laporan tesis sebagai salah satu syarat menyelesaikan studi Pascasarjana Magister Informasika Fakultas Teknologi Industri Universitas Islam Indonesia dapat terselesaikan. Sholawat serta salam semoga tetap tercurahkan kepada Nabi Muhammad Shalallahu alaihi Wassalam, para sahabat, keluarga, dan pengikutnya.

Dalam penyususan laporan tesis ini tidak lepas dari bimbingan, dukungan dan bantuan dari berbagai pihak. Oleh karena itu dalam kesempatan ini, dengan kerendahan hati ucapan terima kasih disampaikan dengan setulus-tulusnya kepada:

1. Allah Subhana Wa Ta'ala, yang telah melimpahkan Rahmat dan Karunia-Nya sehingga penulis diberikan kesehatan, kekuatan untunk dapat menyelesaikan laporan tesis ini.
2. Orang tua, istri, dan keluarga yang selalu memberikan dukungan.
3. Bapak Rektor dan seluruh jajaran Universitas Islam Indonesia.
4. Bapak Dr. Imam Riadi, S.Pd., M.Kom. Bapak Dr. Yudi Prayudi, S.Si., M.Kom dan Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom selalu dosen Pembimbing dan Penguji yang telah memberikan pengarahan, masukan, serta selalu memberikan dorongan semangat selama studi.
5. Dosen Magister Informatika Universitas Islam Indonesia serta jajaran staf Program Pascasarjana.
6. Rekan-rekan Magister Informatika terkhusus Konsentrasi Forensika Digital yang selalu saling berbagi ilmu dan pengalamannya.
7. Semua pihak yang telah memberikan dorongan motivasi yang tak bisa disebutkan satu-persatu.

Saya menyadari bahwa dalam penulisan dan penyususan laporan tesis ini masih banyak terdapat kekurangan, sehingga penulisan mengucapkan permohonan maaf dan sangat mengharapkan saran dan kritik yang membangun untuk penyempurnaan di masa mendatang.

Yogyakarta, 2023

Agus Wijayanto

Daftar Isi

Daftar Tabel

Daftar Gambar

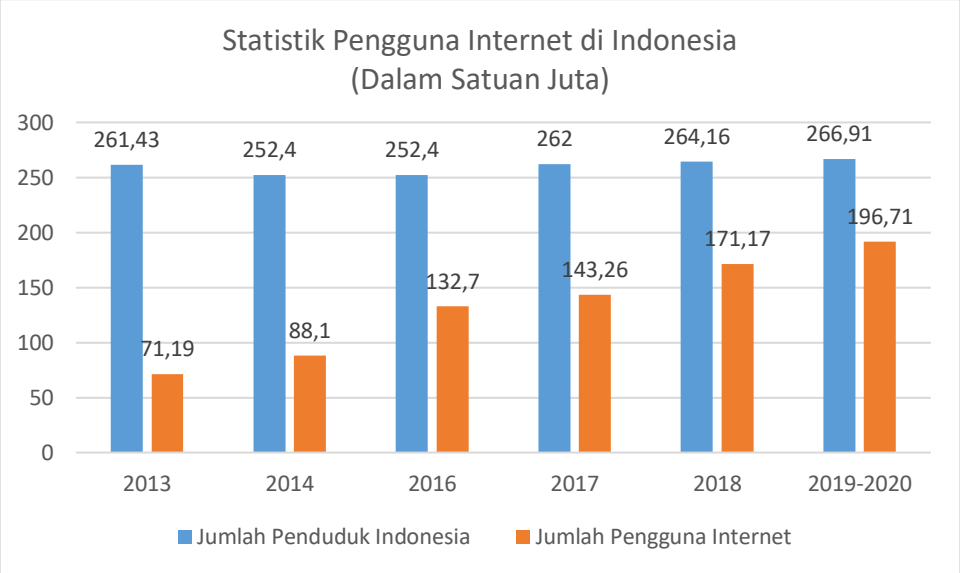
Glosarium

ARP	- Address Resolution Protocol
TZSP	- Tazmen Sniffer Protocol
DOS	- Denial of Service
APJII	- Asosiasi Penyedia Layanan Internet Indonesia
MITM	- Man In The Middle
ICMP	- Internet Control Message Protocol
PC	- Personal Computer
IP	- Internet Protocol
MAC	- Media Access Control
GUI	- Graphics User Interface
CLI	- Command Line Interface
TCP	- Transmission Control Protocol
NFAT	- Network Forensics Analysis Tools

BAB 1
Pendahuluan

1.1 Latar Belakang

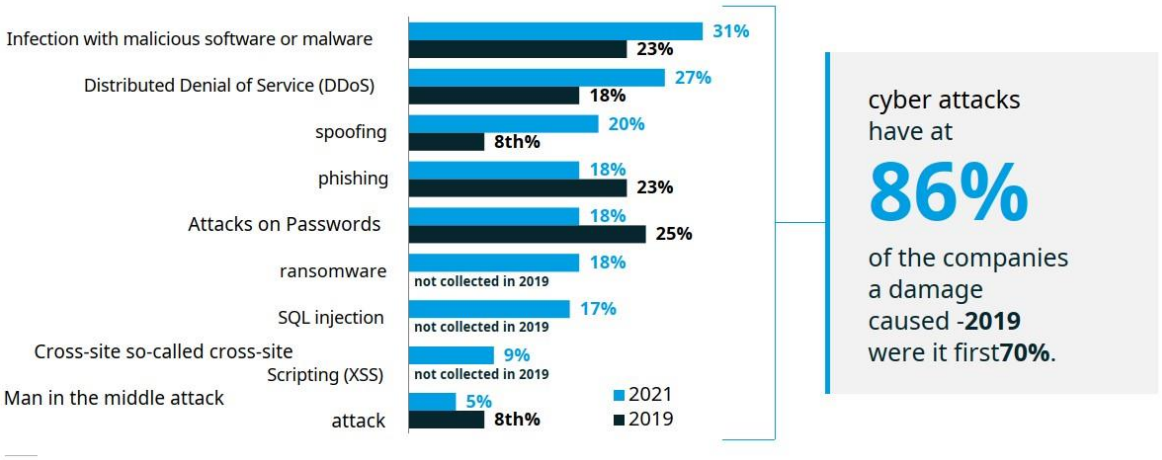
Penggunaan layanan internet sudah menjadi kebutuhan pokok dikalangan masyarakat, setiap hari seseorang tidak lepas dengan aktivitas didunia maya memanfaatkan jaringan. Menurut hasil survey yang dilakukan oleh APJII penetrasi pengguna internet mengalami kenaikan setiap tahunnya, dari jumlah penduduk Indonesia yang mencapai 266,91 juta orang sebanyak 73,7% atau 196,71 juta merupakan pengguna internet (APJII, 2020).



Gambar 1.1 Statistik pengguna internet di Indonesia.

Data yang ditampilkan pada gambar 1.1 tidak menutup kemungkinan di tahun berikutnya akan mengalami peningkatan pengguna yang lebih tinggi. Penetrasi terhadap penggunaan internet tidak lepas dari pengguna jaringan baik dari skala kecil sampai skala yang besar, baik dari personal, organisasi swasta maupun pemerintah. Kemudahan dalam menggunakan jaringan tidak hanya berpangaruh dalam hal positif seperti halnya membantu aktifitas sosial, pendidikan, pekerjaan, dan lain sebagainya. Dampak lain dari kemudahan ini, menghasilkan banyak model *cyber attack* yang sangat merugikan berbagai pihak.

Data pada Tahun 2021 menunjukkan bahwa, serangan siber menyebabkan 86% kerusakan pada perusahaan. Peningkatan paling tinggi yaitu pada *spoofing* mencapai 12% dihitung mulai dari peningkatan di tahun 2019 (Berg & Selen, 2021).



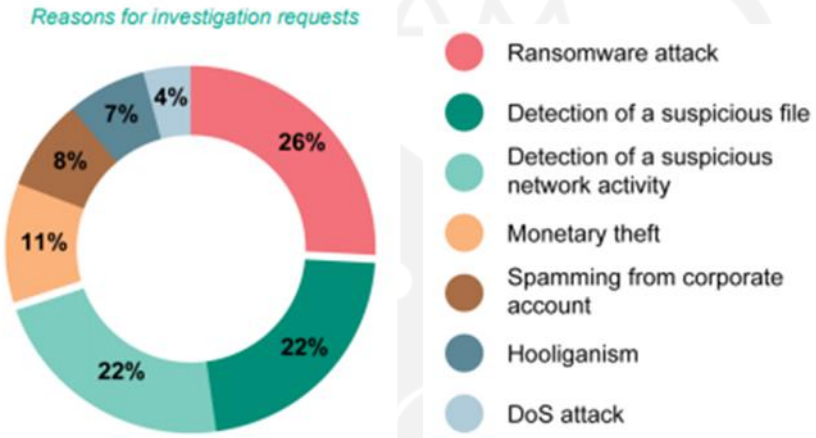
Gambar 1.2 Data serangan siber

Spoofing dalam serangan siber sendiri merupakan sebuah tindakan penipuan dengan memanfaatkan media teknologi untuk mengelabui korban, seolah-olah penyerang merupakan *host* yang terverifikasi (Zhao et al., 2020). Salah satu dari jenis *spoofing* yaitu *ARP Spoofing* dengan mengekploitasi protokol *ARP* (Scott et al., 2017). Protokol *ARP* dirancang tanpa adanya fitur keamanan untuk mengautentikasi sehingga rentan terhadap serangan *spoofing*. Sedangkan *ARP* adalah salah satu protokol penting didalam *TCP/IP* untuk mentranslasikan alamat *IP Address* ke Alamat *MAC Address*. Protokol *ARP* ini akan selalu dilibatkan di dalam sebuah jaringan baik skala kecil maupun besar untuk membangun sebuah interkoneksi (Hijazi & Obaidat, 2018).

Secara hirarki, *host* mendapatkan alamat *IP Address* dari perangkat Router secara dinamis setelah adanya komunikasi melalui protokol *ARP* yang mengirimkan sebuah pesan secara *broadcast* ke setiap *host* yang terhubung ke dalam jaringan lokal. Hal ini dapat dimanfaatkan oleh penyerang untuk melancarkan serangan *ARP Spoofing* dengan mengirimkan paket *ARP* untuk menautkan Alamat *MAC Address* penyerang dengan alamat IP Korban dan juga Router sebagai penyedia alamat *IP address* dinamis untuk jaringan lokal. Router umumnya menjadi ujung perangkat untuk terhubung ke internet, sehingga memungkinkan serangan *ARP Spoofing* ini dilanjutkan ke *Man in The Middle Attack* maupun *Denial of Service* dengan korban semua *host* yang terhubung langsung ke perangkat Router (Brown & Willink, 2018).

ARP Spoofing bagian aktivitas siber berkaitan dengan *network attack*, menjadi sebuah titik krusial terjadinya serangan berikutnya yang dapat menyebabkan kerusakan hingga menimbulkan kerugian bagi organisasi maupun individu. *Network attack* yang dilancarkan oleh seseorang dibalik sebuah teknologi harus dapat diidentifikasi, berpegang pada *locard's exchange principle*, setiap bentuk aktivitas melibatkan dua objek atau bahkan

lebih dipastikan akan meninggalkan suatu bentuk bukti. Pengumpulan bukti dari hasil pemantuan ataupun perekaman lalu lintas jaringan untuk membantu pemeriksaan sehingga mendapatkan informasi bukti merupakan suatu bidang ilmu dari digital forensik yang dikenal dengan nama *Network forensic* (Mate & Kapse, 2015). Metode investigasi forensik pada penerapan *network forensic* dibutuhkan untuk membantu seorangan investigator untuk menjaga bukti digital yang mudah mengalami kerusakan (Divakaran et al., 2017). Laporan dari salah satu perusahaan IT, Kaspersky merilis permintaan investigasi terhadap beberapa serangan siber ditampilkan pada gambar 1.3 (kaspersky, 2021).



Gambar 1.3 Presentase permintaan investigasi.

Sumber: *Incident Response Analytics Report* (kaspersky, 2021)

Gambar 1.3 menginformasikan bahwa permintaan investigasi siber terhadap aktivitas jaringan yang mencurigakan mencapai 22% dan serangan *ARP* termasuk tindakan yang dapat menimbulkan sebuah aktivitas yang mencurigakan di dalam sebuah jaringan. Investigasi forensik diperlukan untuk membantu menemukan bukti serangan *ARP Spoofing*, sehingga dapat merekronstruksi serangan yang terjadi. Invesitgasi forensik merupakan pendekatan yang sesuai untuk mendapatkan bukti digital, dimana didalamnya mencakup prosedur dan teknik yang digunakan untuk membuktikan sebuah insiden siber. Proses investigasi forensik saat ini telah diarahkan pada teknologi dan alat yang tersedia, hal ini selain menjadi *support* untuk proses pemeriksaan juga menjadi tantangan tersendiri untuk membantu proses investigasi forensik jaringan (Meghanathan et al., 2009).

Salah satu pendekatan investigasi untuk proses investigasi forensik jaringan adalah TAARA, yang merupakan singkatan dari *Trigger, Acquire, Analysis, Report,* dan *Action*. Menurut (Umar et al., 2021b), TAARA yang dikembangkan dari Metodologi Penilaian Ancaman dan Analisis Remediasi memiliki dinilai memiliki cakupan yang lebih kecil dan sumber daya yang lebih sedikit untuk menghadapi ancaman dunia maya atau kejahatan dunia

maya. TAARA digunakan untuk pendekatan investigasi forensik yang selanjutnya akan di eveluasi berdasarkan serangan *ARP Spoofing*.

1.2 Rumusan Masalah

Merujuk pada latar belakang yang telah dipaparkan, dapat merumuskan masalah penelitian sebagai berikut:

1. Bagaimana melakukan proses investigasi serangan *ARP Spoofing* dengan pendekatan pada sisi router ?
2. Bagaimana melakukan proses investigasi jaringan dari serangan *ARP Spoofing* menggunakan metode TAARA untuk memvalidasi barang bukti?
3. Bagaimana melakukan pemeriksaan menggunakan alat forensik jaringan ?

1.3 Batasan Masalah

Agar penelitian ini fokus pada pokok permasalahan yang telah dirumuskan pada bagian sebelumnya, maka ruang pambahasan penelitian akan diteteap sebagai berikut:

1. Simulasi serangan dilakukan di kampus Universitas Mulia Balikpapan pada segmen Laboratorium Jaringan dan segmen ruang IT.
2. Jenis serangan *ARP Spoofing* dibatasi untuk merusak tabel *ARP* pada *host* yang terverifikasi menggunakan Arpspoof, Bettercap, Ettercap, KickThemOut.
3. Pendeteksian indikasi serangan menggunakan XARP sebagai alert pada sisi user.
4. Proses Investigasi menggunakan metode TAARA.
5. Alat bantu forensik jaringan menggunakan Wireshark dan Network Miner.
6. Proses perekaman lalu lintas jaringan menggunakan pendekatan pada sisi router dengan memanfaatkan *packet sniffer*.
7. Tahapan investigasi forensik mengimplementasikan model TAARA, sehingga dapat mengevaluasi berdasarkan kasus serangan yang diteliti.

1.4 Tujuan Penelitian

Tujuan penelitian yang diharapkan dari penelitian sebagai berikut:

1. Menganalisis serangan *ARP Spoofing* dengan pendekatan di sisi router
2. Melakukan serangkaian tahapan dengan metode TAARA untuk memvalidasi barang bukti digital.
3. Melakukan evaluasi terhadap alat forensik jaringan

1.5 Manfaat Penelitian

Berdasarkan latar belakang masalah, rumusan masalah, batasan masalah, dan penjelasan tujuan penelitian di atas, maka dari hasil penelitian ini diharapkan dapat memberikan manfaat yaitu:

1. Bagi Perkembangan Keilmuan
   a. Dapat menjadikan sebuah panduan dalam melakukan proses investigasi tertama yang melibatkan forensika jaringan
   b. Sebagai bentuk pendalaman keilmuan di bidang forensika jaringan
2. Bagi Peneliti lain

   Sebagai salah satu referensi dalam melakukan penelitian terutama dalam penelitian di bidang forensika jaringan
3. Bagi Penulis

   Diharapkan dari penelitian ini dapat memberikan wawasan tambahan baik dalam segi teori maupun praktik.

1.6 Sistematika Penulisan

Dalam penyusuan penulisan ini untuk memberikan gambaran terkait dengan penjelasan maka digunakan sebuah sistematika penulisan sebagai berikut:

BAB I PENDAHULUAN

Pada Bab ini menjelaskan Pendahuluan yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian, sistematika penulisan, serta *literature review.*

BAB II LANDASAN TEORI

Pada Bab ini menjelaskan teori-teori yang terkait yang berhubungan dengan serangan jaringan dan proses investigasi.

BAB III METODOLOGI PENELITIAN

Pada Bab ini membahas tentang langkah-langkah penelitian, kebutuhan perangkat keras dan perangkat lunak yang akan digunakan serta mekanisme pengumpulan data melibatkan infrastruktur jaringan Laboratorium Fakultas Ilmu Komputer Universitas Mulia.

BAB IV HASIL DAN PEMBAHASAN

Bab ini berisi pembahasan penyelesaian masalah dengan menggunakan metode investigasi forensic dan analisis pengujian yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Kesimpulan dan saran, berisi kesimpulan dari penelitian dan saran yang memerhatikan keterbatasan temuan dalam penelitian dan rekomendasi untuk penelitian selanjutnya.

BAB 2
Tinjauan Pustaka

2.1 Pendahuluan

Serangan *ARP Spoofing* merupakan salah satu jenis serangan *spoofing* yang dapat mengakibatkan serangan lanjutan. Metode serangan *ARP Spoofing* memanfaatkan kerentanaan dari protokol *ARP* (Sharma et al., 2017). ARP merupakan protokol yang digunakan untuk memetakan *IP Address* dengan *MAC Address*. Router sebagai *gateway* melakukas *ARP request* ketika ada paket masuk untuk menemukan *MAC Address host*. Begitu pula sebaliknya, pada sisi *host* yang terhubung juga melakukan *ARP request* ke setiap *host* yang ada pada jaringan tersebut. Pesan *request* tersebut di *broadcast* ke setiap *host* yang terhubung, dan ketika perangkat mengenali IP yang disiarkan merupakan kepemilikannya maka perangkat tersebut mengirimkan *ARP-reply* kepada pengirim *ARP-request* tanpa adanya metode keamanan untuk memverifikasi (Riadi et al., 2020).

Metode serangan *ARP Spoofing* dijalankan dengan mengirimkan *ARP-reply* tanpa adanya permintaan berupa *ARP-request* sehingga penyerang akan mampu memperbarui *table ARP* milik korban dengan menambahkan *MAC Address* beserta *IP Address* milik penyerang (Hafizh et al., 2020). Serangan ARP Spoofing ini mampu menghasil serangan berkelanjutan seperti halnya penolakan layanan jaringan dengan teknik *Denial of Service* ataupun membaca lalu lintas jaringan menggunakan *Man in The Middle Attack* (Saputra, 2019).

Pada beberapa penelitian sebelumnya yang telah dilakukan dalam pencegahan kerentanan yang biasa dimanfaatkan untuk serangan ARP *Spoofing* menggunakan algoritma *multiplicative enhancement* dan *additive reduction* (Anathi & Vijayakumar, 2020), melakukan sebuah pembatasan *traffic* dengan menjalankan verifikasi *MAC address* di mana akan melakukan sebuah prediksi terhadap pengguna jaringan yang sah. Pendekatan ini dapat diterapkan pada ekosistem industri. Penelitian lain menggunakan fitur *Software-Defined Network* (SDN) di mana fokus yang dilakukan yaitu pada mekanisme pencegehan dari serangan spoofing (Ibrahim et al., 2020).

SDN menjadi jawaban saat ini menggantikan jaringan konvensional yang memiliki masalah keamanan. Implementasi IDPS (Girdler & Vassilakis, 2021) dalam mengamankan jaringan dari spoofing dengan melakukan empat jenis percobaan yang biasa terjadi pada serangan *spoofing*, yaitu *ARP request attack, reply attack, reply destination* dan *blacklist*

MAC address menghasilkan tinggkat *false positive* nol dan semua paket dapat terdeteksi. Sedangkan pada penelitian yang dilakukan oleh (Rohatgi & Goyal, 2020) berkaitan dengan *survey* untuk mengetahui teknik-teknik untuk mencegah serangan *ARP spoofing.* Beberapa diantaranya membahas tentang penggunaan *static ARP* dimana proses pemetaan *IP address* dengan *MAC* dilakukan secara manual dan ini memiliki kekurangan ketika skala jaringan lebih besar. Teknik *Secure Unicast ARP* dengan memanfaatkan server DHCP+ namun selain menyiapkan server harus memodifikasi *ARP* pada setiap *host*. Berikutnya teknik dengan menyediakan sebuah arsitektur untuk menyelesaikan permasalahan serangan dengan menyiapkan dua protokol pada server setiap protokol memiliki fungsi masing-masing, satu protokol akan menjalankan fungsi *invite-accept* sedang protokol berikutnya menjalankan fungsi *request-reply* namun teknik ini memiliki kekurangan dalam skenario praktis. Beberapa teknik lain juga dijelaskan pada penelitian tersebut namun tidak memberikan penilaian khusus ataupun sebuah rekomendasi terhadap teknik terbaik yang dapat dilakukan untuk mencegah serangan *spoofing.*

Pendeteksian serangan *ARP* (Miao et al., 2020) mengusulkan *Dynamic Trust Model ARP Real-Time Intrusion Detection Extended Subjective Logic* untuk mengatasi perilaku perangkat yang dianggap melakukan intrusi *ARP*, hal ini dianggap mampu dalam memeriksa paket arp di lingkungan dinamis perangkat lunak. Penelitian berikutnya pencegahan dengan menggunakan motode *semi-static* oleh (Data, 2018), pencegahan tersebut bekerja dengan cara memulihkan ARP *table cache* tanpa harus melakukan sebuah modifikasi terhadap ARP. Teknik yang diterapkan pada penelitian tersebut memiliki tiga prosedur pertama dengan mendaftar alamat *IP* dan *MAC* yang sudah di-*cache* pada *ARP table cache,* kemudian melakukan validasi dan yang terakhir menetapkan alamat IP dan MAC yang valid sebagai catatan statis dengan begitu ketika terjadi sebuah serangan maka akan dipulihkan. Namun dalam penelitian tersebut teknik ini hanya digunakan pada *host* sendiri dan tidak dapat melindungi *host* lain sehingga dibutuhkan sebuah pengembangan protokol untuk komunisi antara *host* satu dengan yang lain.

Pembahasan lain terkait *ARP spoofing* bagaimana melakukan pencegahan memanfaatkan *Network Intrusion Detection Systems* (Bhirud & Katkar, 2011) Dengan membuat sebuah *firewall* dibangun menggunakan pemrograman *java* dan menyiapkan perangkat dengan dua NIC, kemudian program tersebut akan mengeksekusi paket yang melewati NIC satu apakah bisa diteruskan keluar melalui NIC ke dua atau akan memutusnya. Namun mekanisme tersebut tidak dapat melakukan identifikasi serangan jika sumber dan tujuan berada pada *local area network* yang sama.

Forensik jaringan merupakan suatu bentuk aktivitas yang dilakukan dalam upaya melakukan sebuah proses pengumpulan, perekaman, serta analisa berkaitan dengan lalu lintas dalam sebuah jaringan untuk mencari sumber serangan dan juga untuk menukan hal-hal lain terkait insiden yang terjadi (Rizal et al., 2018). Sedangkan dua metode untuk pengambilan barang bukti menurut (Yuwono et al., 2019) ada dua teknik yang digunakan yakni menggunakan metode *live forensic* dan juga *dead forensic*. Pengambilan bukti saat sebuah sistem dalam kondisi menyala merupakan metode *live forensic*, sedangkan pengambilan barang bukti penggunaan *log* yang terdapat pada sistem adalah metode *dead forensic.*

Bentuk investigasi *forensic digital* mulai dari terjadinya sebuah insiden sampai dengan laporan harus memenuhi segala aspek untuk mendapatkan bukti digital yang sah dan dapat dibuktikan secara ilmiah (Riadi et al., 2017) Bukti digital menjadi bagian terpenting dalam sebuah ilmu forensik digital (Agarwal et al., 2011). Bukti digital itu sendiri memiliki sifat mudah rusak atau rawan terhadap perubahan (Ruuhwan et al., 2016) Dalam melakukan investigasi, seorang investigator juga harus memperhatikan hukum yang berlaku dalam menangani bukti digital dan mengikuti prosedur kerangka kerja (Supriyono et al., 2019). Kerangka kerja yang dilakukakan dapat menggunakan beberapa metode. Penelitian sebelumnya dilakukan oleh (Riadi et al., 2020) menggunakan metode *National Institute of Standard Technologi (NIST)* dalam menganalisis bukti serangan *ARP Spoofing*. Pada penelitian tersebut di dapatkan hasil sumber serangan berasal hinggal kapan waktu terjadinya serangan tersebut.

Tabel 2.1 Literatur Review

Literatur	Latar Belakang	Kasus Penelitian	Teknik Deteksi	Metode Akuisisi	Metode Investigasi Forensik
(Umar et al., 2021)	Perkembangan teknologi yang semakin pesat diikuti dengan kejahatan siber dimana ransomware menjadi ancaman bagi infrastruktur. Serangan virus dengan ukuran file yang kecil membuat tidak mudah untuk dideteksi.	Malware Ryuk Ransomware	-	Live forensic	TAARA
(Anathi & Vijayakumar, 2020)	Pertumbuhan eksponensial dalam penggunaan jaringan menjadi target utama bagi penyerang. Serangan spoofing rumit untuk dideteksi, beberapa teknik pendeteksian serangan justru salah dalam mengklasifikasikan penyerang sesungguhnya	ARP Spoofing	MAC address verification with multiplicative increase and additive decrease algorithm based	-	-
(Ibrahim et al., 2020)	Jaringan konvensional dianggap memiliki beberapa masalah keamanan. SDN sebagai jawaban	ARP Spoofing, Software	Pox Controller Extended with ARP spoofing and ARP	-	-

	untuk masalah yang terjadi dengan mengimplementasi SDN ARP Spoofing dapat diatasi namun masalah lain muncul Ketika jaringan semakin kompleks sehingga menyebabkan traffik meningkat.	Defined-Network	broadcast prevention algorithm		
(Rohatgi & Goyal, 2020)	Era kehidupan saat ini sepenuhnya condong kepada internet. Setiap sektor membutuhkan sebuah jaringan baik publik atau swasta. Banyak peneliti membahas tentang keamanan jaringan dan Arp spoofing memfasilitasi berbagai serangan	Survey deteksi dan mitigasi dari serangan ARP Spoofing	-	-	-
(Girdler & Vassilakis, 2021)	SDN merupakan sebuah pendekatan yang memungkinkan implementasi konfigurasi global secara menyeluruh dengan menggunakan controller.	ARP Spoofing, Software Defined-Network	Intrusion Detection and Prevention System (IDPS) SDN based	-	-

	Permintaan yang cukup besar terkait SDN lebih dari $100 milliar pada tahun 2025 akan menyebabkan peningkatan serangan.				
(Miao et al., 2020)	Perkembangan ilmu pengetahuan dan teknologi beberapa tahun terakhir semakin luas, berbagai program aplikasi jaringan, informasi di internet lebih beragam. Semua penguji dalam pendeteksian intrusi ARP memilki masalah dasar yakni tidak dapat memastikan secara mutlak pada lingkungan dinamis bahwa perangkat melakukan intrusi ARP	ARP Spoofing	Dynamic Trust Model of ARP Real-Time Intrusion Detection based on Extended Subjective Logic (DTMARID-ESL)	-	-
(Umar et al., 2021a)	Serangan kejahatan siber dengan virus ransomware beberapa tahun terakhir. Virus ransomware mirip dengan malware lain, namun memiliki karakteristik yang berbeda.	Conti ransomware	-	Live forensic	-

(Sistem, Riadi, Fadlil, et al., 2021)	Bukti digital merupakan informasi yang rapuh jika salah dalam penanganan, diantara bukti yakni optical drive. Penggunaan metode forensik dibutuhkan untuk menangani sebuah kasus kejahatan digital untuk mendukung proses investigasi.	Investigasi bukti digital optical drive	-	-	NIST
(Sistem, Riadi, Umar, et al., 2021)	Perkembangan teknologi seperti halnya smartphone, media sosial serta banyak pengguna internet saat ini banyak disalahgunakan melalui instans messenger. Terjadi peningkatan kejahatan tertama pada ujaran kebencian.	Investigasi bukti digital aplikasi viber	-	-	NIST
(Sistem, Riadi, Fadlil, et al., 2021)	Internet berperan penting dalam segala aktivitas dan mengalami peningkatan tiap harinya. Salah satu fasilitas internet adalah email dan dalam kemudahan menggunakannya muncul ancaman serius.	Email spoofing	-	-	NIST

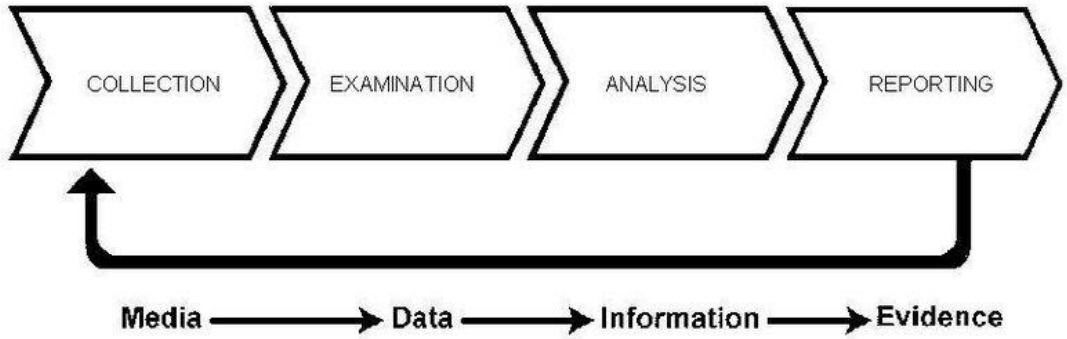
2.2 Konsep Pengetahuan

2.2.1 Digital Forensik

Digital forensik menurut (Muhammad Nuh Al- Azhar, 2012) merupakan suatu ilmu pengetahuan pada bidang teknologi komputer yang digunakan untuk kepentingan hukum (*pro justice*) dalam membuktikan tindak kejahatan yang melibatkan penggunaan teknologi atau *computer crime* mengikuti kaidah-kaidah ilmiah (*scientific*) untuk mendapatkan bukti digital. Proses untuk mendapatkan bukti digital sendiri merupakan sebuah seni untuk memulihkan ataupun menganalisis sebuah konten dari perangkat digital. Secara umum digital forensik berperan memfasilitasi investigasi baik metodologi, teknik, kerangka investigasi forensik untuk menggalih, menyelidiki media dan perangkat penyimpanan digital dalam lingkungan yang terkendali, melestarikan bukti asli sesuai dengan kriteria, dan menjamin bahwa setiap artefak yang ditemukan dapat digunakan sebagai bukti dalam prosedur hukum, baik pidana, perdata, atau lainnya.

Digital forensik dalam penjelasan lain merupakan tahapan yang saling berkaitan dimulai proses mengidentifikasi, melestarikan, menganalisis dan menyajikan bukti digital dengan cara yang dapat diterima (Selamat et al., 2008). Penjelasan lain tentang digital forensik menurut (Tully et al., 2020) yaitu proses mengekstraksi data dari sistem digital atau media penyimpanan data, mengubahnya menjadi format yang dapat digunakan, dan kemudian menafsirkannya untuk mendapatkan informasi untuk digunakan dalam penyelidikan atau bukti untuk digunakan dalam penuntutan pidana. Digital forensik juga terkadang disebut juga dengan forensika komputer atapun forensika jaringan, keduanya walaupun memiliki perbedaan namun memiliki tujuan yang sama yaitu bagaimana melestarikan bukti digital sehingga mampu merekonstruksi kejahatan siber yang terjadi dengan tetap memenuhi persyaratan hukum.

Forensika digital pada awalnya lebih dikenal dengan sebutan forensik komputer hal ini disebabkan bukti yang dikumpulkan terbatas hanya pada sebuah perangkat komputer. Namun, forensika digital mengalami perkembangan sebagai bidang independen dengan bersamaannya pertumbuhan penggunaan teknologi yang tidak terbatas pada perangkat komputer. Pertumbuhan teknologi membawa sebuah variasi kemampuan penyimpanan dan pengiriman data hingga meningkatnya kejahatan siber mendorong proses digital forensik untuk menjawab permasalahan siber. *National Institute of Standard and Technology* (NIST) (Riadi et al., 2018) merekomendasikan tahapan dasar dalam proses forensik digital yaitu *Collection, Examination, Analysis, Reporting*.



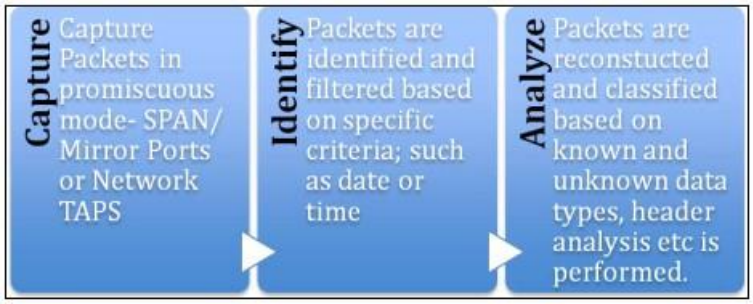
Gambar 2.1 Tahapan NIST

1. *Collection* merupakan tahapan mengumpulkan, mengidentifikasi, memberi label, merekam, dan mengambil data dari sumber data yaitu perangkat keras dengan menjaga integritas data asli, menjaga integritas data dengan mengisolasi bukti fisik dan membackup data dengan mengkloning atau file gambar dari item fisik bukti.
2. *Examination* merupakan tahapan pengolahan data yang telah dikumpulkan dengan menerapkan metode baik manual maupun otomatis dengan memastikan integritas data tetep terjaga, sehingga dapat memberikan penilaian terkait data yang diekstraksi.
3. *Analysis* adalah proses menganalisis dari hasil pemeriksaan secara teknis yang dibenarkan oleh undang-undang yang berlaku untuk memperoleh informasi guna menjawab permasalahan yang ada pada tahapan sebelumnya dan melakukan pendokumentasian.
4. *Reporting* yakni tahapan melaporkan hasil analisis yang mencakup deskripsi tindakan yang dilakukan, penjelasan tentang alat dan prosedur. Serta melaporkan hasil analisis yang mencakup deskripsi tindakan yang dilakukan, penjelasan tentang alat dan prosedur.

2.2.2 Forensika Jaringan

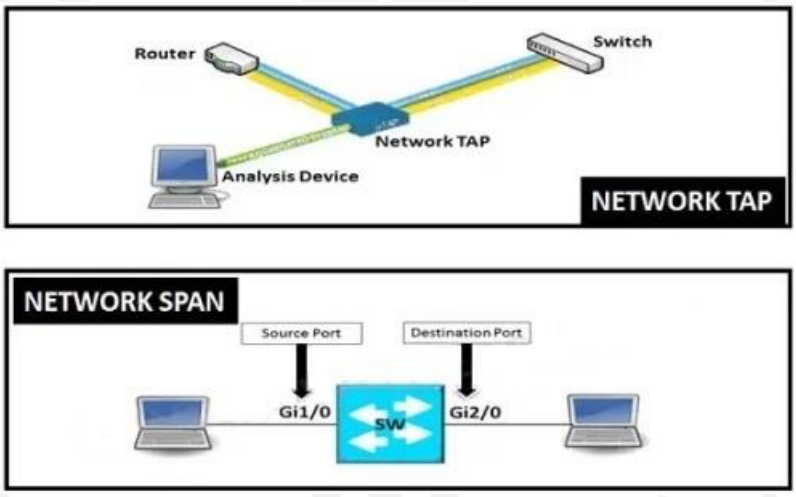
Forensik jaringan adalah salah satu sub-cabang forensik digital di mana data yang dianalisis adalah lalu lintas jaringan yang menuju dan dari sistem yang sedang diamati. Definisi forensika jaringan menurut (Yudhana et al., 2018) adalah proses menangkap, merekam, dan menganalisis aktivitas jaringan untuk menemukan bukti digital adanya penyerangan atau kejahatan yang dilakukan yang dilakukan dengan menggunakan jaringan komputer sehingga

pelakunya dapat dituntut sesuai hukum yang berlaku. Secara umum, proses forensika jaringan berupa CIA (*Capture, Identify and Analyze*).



Gambar 2.2 Proses CIA Forensika Jaringan

1. *Capturing* merupakan tahapan yang dilakukan untuk mendapatkan data lalu lintas jaringan. Proses ini umumnya memiliki dua metode yaitu *Mode SPAN* dan *Network TAP*.



Gambar 2.3 Ilustrasi *Nework TAP* dengan *Network SPAN*

2. *Identify* adalah tahapan untuk mengidentifikasi melalui pemfilteran berdasarkan kriteria tertentu sepertinya protokol TCP.
3. *Analyze* merupakan tahapan untuk menganalisa *packet* atau *frame* tertentu untuk dapat memahami apa yang sebenarnya terjadi.

Forensika jaringan menurut (Khan et al., 2016) merupakan suatu mekanisme untuk memfasilitasi penyelidikan dengan merekam setiap paket maupun peristiwa yang terjadi melalui lalu lintas jaringan. Forensik jaringan dijelaskan oleh (Jayakrishnan, 2018) memiliki sifat data yang sungguh dinamis, penyelidikan tidak mungkin dilakukan jika tahapan khusus yang membedakan antara forensik jaringan dan forensik komputer tidak dijalankan. Tahapan ini berupa pengaturan untuk menangkap lalu lintas jaringan. Banyak model forensika jaringan pada dasarnya memiliki konsep yang sama pada proses awal yakni bagaimana proses untuk menangkap dan menyimpan lalu lintas jaringan.

2.2.3 Serangan Siber

Serangan siber merupakan tindakan yang dilancarkan oleh penyerang baik individu maupun kelompok untuk merusak sebuah sistem yang menyebabkan kerugian baik materil maupun non-materil. Menurut (Kumar Singh et al., 2019) penyerang ini diklasifikasikan menjadi 3 diantaranya:

1. *Black Hat* merupakan peretas yang memiliki tujuan untuk merusak sistem dengan motif mendapatkan keuntungan dari target yang diretas.
2. *White Hat* adalah *hacker* yang memiliki otoritas untuk melindungi asset digital dan umumnya dipekerjakan untuk melawan peretas jahat.
3. *Grey Hat* merupakan salah satu peretas yang berdiri diantara *black hat* dan *white hack,* sehingga terkadang peretas ini dapat memiliki niatan merusak sistem ataupun memberikan informasi terkait *vulnerability*.

Umumnya serangan siber memanfaatkan kerentanan yang kemudian dimanfaatkan untuk mendapatkan akses ke dalam sistem sehingga penyerang dapat memperoleh dan mengakses data yang dibutuhkan.

2.2.4 ARP Spoofing

ARP Spoofing merupakan serangan inisiator dengan memanfaatkan kerentanan pada protokol *ARP*. Kerentanan ini dijelaskan oleh (Rohatgi & Goyal, 2020) bahwa *ARP* tidak akan melakukan autentikasi untuk memvalidasi *arp-reply* berasal dari perangkat yang benar. Secara singkat Teknik serangan ini akan meracuni dan merusak tabel *IP* dengan menyisipkan *MAC Address* penyerang dengan *IP Address* yang sah. Serangan ini menjadi inisator serangan lanjutan, umumnya serangan yang dilancarkan berikutnya yaitu MiTM.

2.2.5 Man In The Middle

Serangan ini merupakan salah satu serangan lanjutan dampak dari serangan *ARP Spoofing* dengan menyadap komunikasi antar *host* yang sah(Zhao et al., 2020). Serangan ini menyerang saluran komunikasi dan dapat melakukan modifikasi data antara *host* satu dengan *host* lainnya. Serangan MiTM umumnya dilakukan untuk melakukan pencurian data dengan sereangan lain yakni *Wifi Eavesdropping* dan dapat melakukan pembajakan email jika protokol yang digunakan tidak aman.

2.2.6 Denial of Service

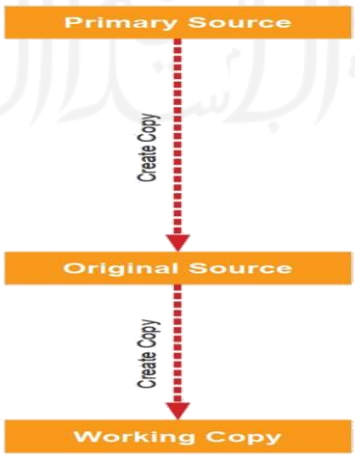
Serangan ini umumnya dilancarkan kepada server agar tidak dapat memberikan layanannya kepada *host* yang mengirimkan permintaan layanan. *Denial of Service* akan memastikan server terus melayani permintaan yang diberikan oleh penyerang tanpa menghiraukan

permintaan dari *host* ataupun pengguna yang sah (Alharbi et al., 2017). Tujuan lain dari serangan ini agar jaringan kembali membangun koneksi seperti awal dan menyiarkan semua kredensial sehingga hal ini kemudian dapat dimanfaatkan kembali oleh penyerang untuk dikumpulkan untuk serangan berikutnya.

2.2.7 Bukti Digital

Bukti digital mengacu pada data apa pun yang dikumpulkan secara digital yang dapat digunakan untuk mengkonfirmasi atau menyangkal teori tentang insiden yang sedang diselidiki. Istilah lain sering juga disebut dengan bukti elektronik yang didefinisikan segala informasi yang disimpan pada perangkat komputer dalam bentuk digital namun tidak hanya terbatas pada komputer dapat mencakup audio, video, foto, ataupun perangkat elektronik (Subektiningsih et al., 2018). Bukti digital pada dasarnya memiliki sifat yang rapuh, perubahan walaupun hanya satu bit pada bukti digital akan mempengaruhi keasliannya hingga berpengaruh pada tidak diterimanya di peradilan. Aturan dasar dalam penanganan bukti digital harus dipenuhi, denngan memperhatikan:

1. Aturan Pertama. Jangan pernah salah menangani bukti. Penanganan sumber data potensial yang didapat dari media penyimpanan seperti hardisk ataupun RAM. Penangana penyimpanan tersebut tidak bisa disamakan karena melihat sifat proses kerja media tersebut memiliki perbedaan. Penanganan yang salah akan menghilangkan dapat merusak bukti digital yang ada.
2. Aturan Kedua, Jangan pernah melakukan pekerjaan forensik pada bukti asli. Setiap interaksi yang dibuat oleh investigator kepada bukti asli. Seperti halnya perubahasan kecil pada metadata terkait dengan *timestamps* dapat langsung berubah saat kita mengaksesnya sehingga bukti ini menjadi dikompromikan. Umumnya alur dalam melakukan pekerjaan terhadap bukti asli ditampilkan sebagai berikut.



Gambar 2.4 Alur Pengananan Untuk Pemeriksaan Sumber Bukti

Primary Source merupakan sumber asli dari bukti, sumber ini segera dibuat replikanya dapat dilakukan pada lingkungan kejadian ataupun diluar lingkungan dengan prosedur yang sesuai. Hasil dari replika ini disebut dengan *Original Source,* dari File tersebut kemudian dilakukan *copy* untuk menghasil *Working Copy. Working copy* ini yang kemudian digunakan untuk pemeriksaan atau analisis bukti digital.

3. Aturan Ketiga, Dokumentasi semua aktivitas. Sebaik hasil yang didapatkan adalah tahapan proses yang lengkap dengan pendokumentasian hingga menghasilkan kesimpulan akhir apakah bukti yang didapatkan mengkonfirmasi ataupun menyangkal peristiwa yang terjadi, Mendokumentasikan setiap langkah untuk mengumpulkan secuil bukti dengan mencatat setiap titik proses yang dilakukan menjadi hal yang sangat penting, karena setiap ketidaksesuaian hasil dengan proses maka dapat menyebabkan penutupan kasus yang sedang ditangani.

2.2.8 Network Forensics Tools

Investigasi forensik jaringan tidak lepas dari data lalu lintas jaringan untuk memantau, memeriksa, menganalisa setiap data yang melintas menggunakan alat bantu teknologi forensik jaringan. *Network Forensics Analysis Tools* sering disingkat dengan NFAT adalah salah satu dari lima kategori alat forensik jaringan yang dapat merekam lalu lintas jaringan secara lengkap memungkinkan pengguna untuk mengevaluasi lalu lintas jaringan sesuai dengan kebutuhan dan mengidentifikasi karakteristik kunci dari lalu lintas tersebut (Pluskal et al., 2020). Tabel berikut menampilkan berbagai macam alat forensik berdasarkan kategori.

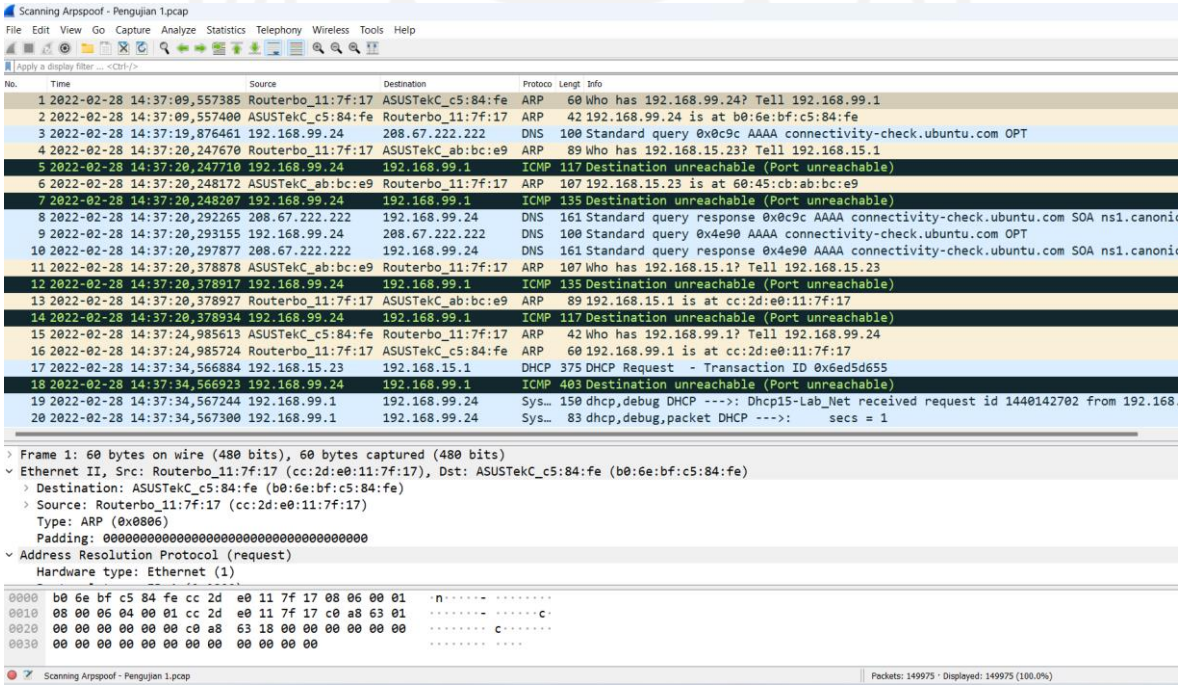
Tabel 2.2 Alat Forensik Jaringan

No	Kategori				
	Network Forensic Analysis Tools	**Vulnerability Assessment**	**Network Sniffing and Packet Analyzing Tools**	**Network Minitoring Tools**	**Intrusion Detection System**
1	NetDetector	Metasploit	TCPDump	IPTraf	Snort
2	NetIntercept	Nessus	Wireshark	VisualRoute	Bro
3	OmniPeek	Wikto	Snort	Ntop	
4	PyFlag	Acunetic Web Vulnerability Scanner	Nmap	TCPStat	

5	Xplico	Yersinia	Tshark		
6		Nikto	Aircrack-ng		
7			Network Miner		
8			Kismet		
9			EmailTrackerPro		
10			Angry IP Scanner		

2.2.9 Wireshark

Wireshark merupakan salah satu alat forensik yang dapat dipergunakan untuk mengalisis paket dan berbagai protol seperti *ICMP, ARP, TCP, SMTP* dan lain sebagainya. Wireshark memiliki model yang lebih bersahabat dikarenakan menggunakan *GUI* sehingga interaksi antara pengguna dengan alat forensik ini lebih dimudahkan. Wireshark sendiri adalah *platform* yang berjalan di *GNU/Linux* yang menggunakan *Libpcap* untuk menangkap paket dari jaringan.

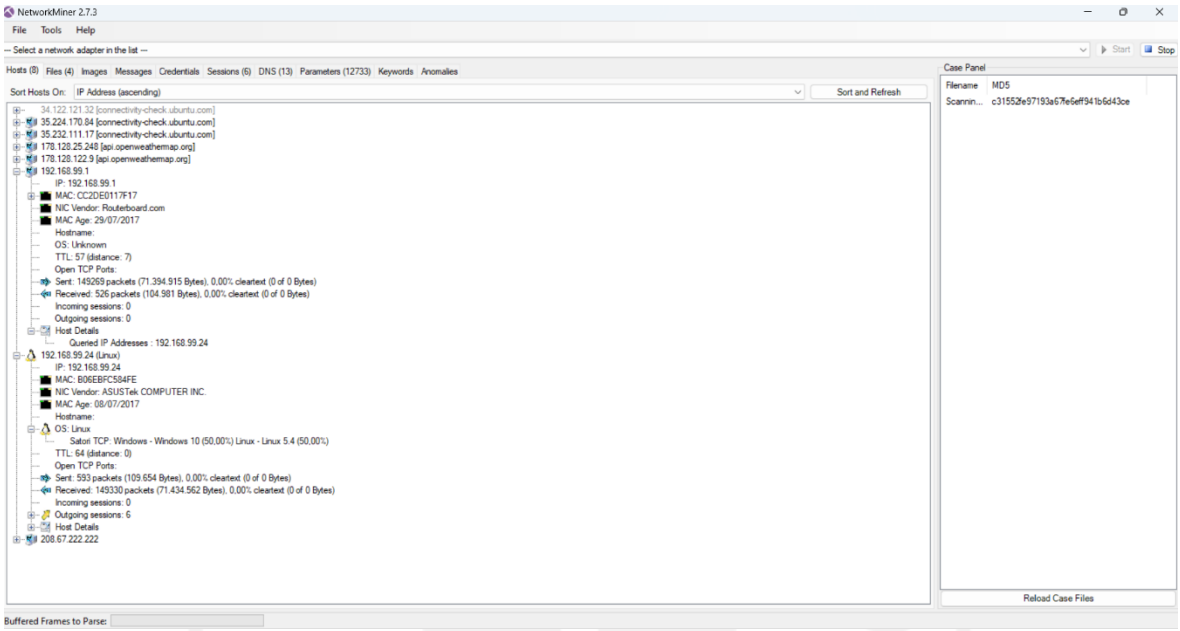


Gambar 2.5 Wireshark

2.2.10 Network Miner

Salah satu alat forensik jariangan yang dapat digunakan untuk melakukan *sniffing* yaitu *Network Miner*. *Network Miner* ini merupakan salah satu alat *open source* yang biasa digunakan untuk melakukan ekstraksi sebuah artefak dari file PCAP seperti untuk mendapatkan file, kata sandi, email, dan gambar. Alat ini dapat mengumpulkan informasi secara detail yang disatukan ke dalam tiap *host* jaringan. Network Miner dirancanang

terutama untuk sistem operasi *Windows*, tetapi juga dapat dijalankan pada sistem operasi berbasiskan Linux OS.

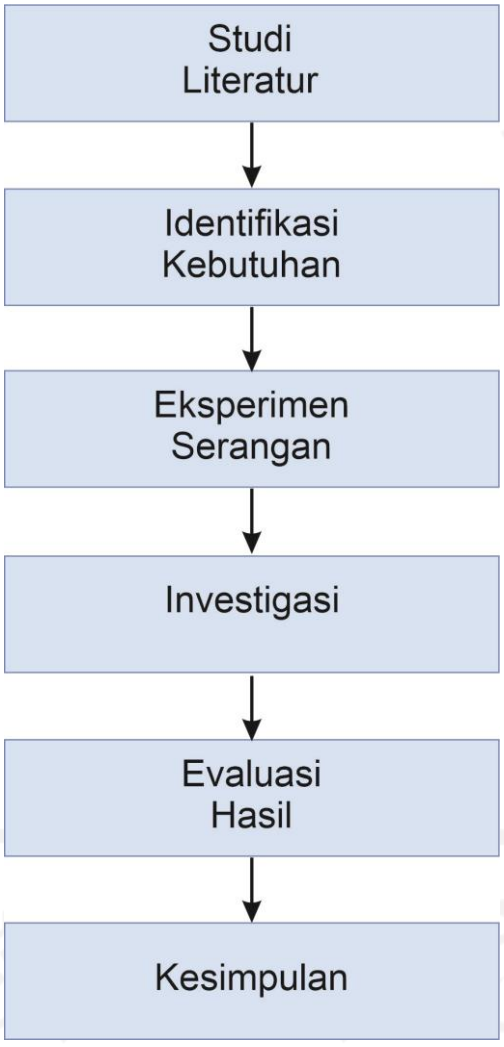


Gambar 2.6 Network Miner

BAB 3
Metodologi

3.1 Langkah Penelitian

Alur metodologi ini meliputi beberapa tahapan yang dilakukan secara berurutan untuk menuntun penelitian mulai dari awal hingga akhir. Gambar 3.1 merupakan diagram alir penelitian yang dijalankan.



Gambar 3.1 Diagram Alur Penelitian

3.2 Uraian Metodologi

3.2.1 Studi Literatur

Studi Literatur. Dalam penelitian yang dilakukan merujuk pada studi kepustakaan dimana teori-teori diambil dari sebuah literatur yang kredibel dan serta referensi yang digunakan dalam konteks yang relevan dengan penelitian yang diangkat. Adapun referensi utama yang digunakan diantaranya yakni jurnal ilmiah terakreditasi, jurnal internasional dan buku.

Sedangkan sebagai tambahan referensi juga menggunakan akses website seperti APJII laporan penetrasi pengguna internet, *Kaspersky Report*.

3.2.2 Identifikasi Kebutuhan

Identifikasi merupakan langkah yang dipersiapkan guna menunjang penelitian, ada beberapa kebutuhan baik peralatan dan Infrastruktur Jaringan. Hal ini dilakukan mengingat perbedaan mendasar antara *network forensic* dengan *computer forensic*, dimana *network forensic* memerlukan sebuah pengaturan untuk dapat menangkap lalu lintas jaringan.

1. Kebutuhan Peralatan

Kebutuhan peraltan disini menyangkut dengan software dan hardware yang ditampilkan pada tabel 3.1.

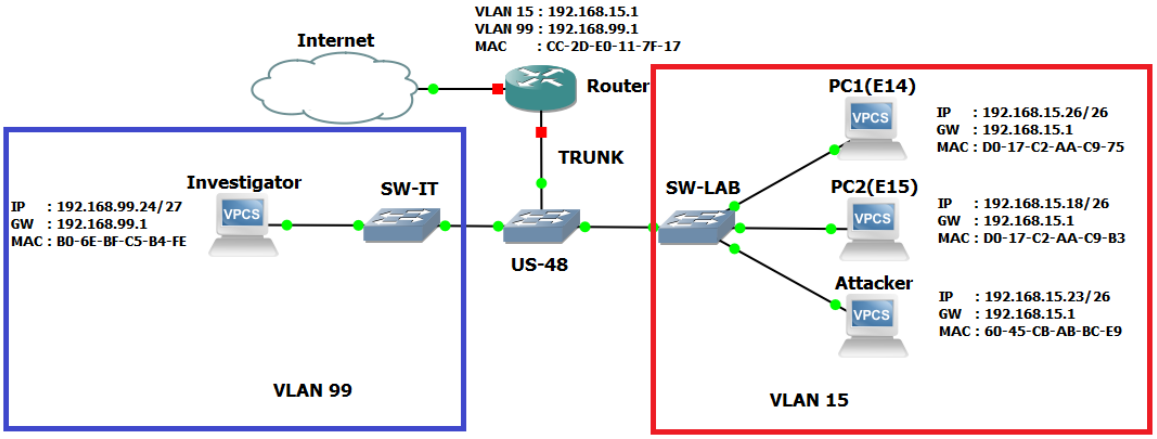
Tabel 3.1 Kebutuhan Sofware dan Hardware

No	Hardware dan Software	Keterangan
1	Laptop Asus X441UV Processor Intel Core I3 6006 RAM 12 GB	Komputer Penyerang
2	Asus Intel Core I7-4770 RAM 16 GB	Komputer Investigator
3	27 units Komputer Laboratorium	*Host* Terverifikasi
4	Router Mikrotik CCR1009-7G-1C-1S+	Peralatan Jaringan
5	Unifi US-48 PoE 500w	
6	Switch TP-Link	
7	Wireshark	Alat forensik Jaringan
8	Network Miner	
9	Arpspoof	Alat untuk serangan *ARP Spoofing*
10	KickThemOut	
11	Ettercap	
12	Bettercap	
13	Xarp	Alat deteksi *ARP Spoofing*

2. Kebutuhan Infrastruktur Jaringan

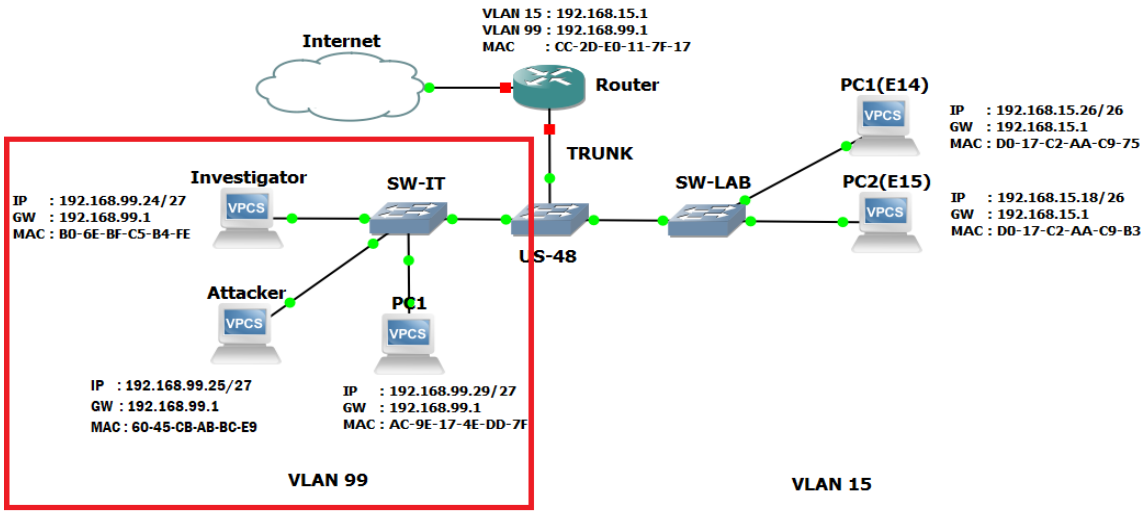
Dalam memenuhi kebutuhan dalam pengambilan data serangan, penulis menggunakan lingkungan jaringan nyata yaitu di Universitas Mulia Balikpapan. Adapun segmen yang digunakan untuk pengambilan data berada pada Vlan Laboratorium Jaringan dan Vlan IT. Alasan kami menggunakan beberapa segmen tersebut untuk menghindari gangguan pada keseluruhan jaringan yang ada di Universitias Mulia. Dalam penelitian pengujian *ARP*

Spoofing, topologi yang digunakan dapat mewakili topologi di lingukungan lain sebab data lalu lintas jaringan akan dihasilkan dari perangkat Router yang umumnya penggunaan perangkat ini pasti digunakan juga di lingkungan jaringan lain. Untuk mengilustrasikan infrastruktur jaringan pengujian ditampilkan pada gambar 3.2 dan gambar 3.3.



Gambar 3.2 Topologi Jaringan Pengujian 1

Pada gambar 3.2 terdapat dua segmen yang ditandai dengan kotak berwarna merah yang menunjukkan Vlan 15, Pada Vlan 15 terdapat 27 *host* aktif, yang kemudian 2 *host* didalamnya akan menjadi target dari serangan *ARP Spoofing*. Segmen berikutnya ditandai dengan kotak berwarna biru menunjukkan Vlan 99. Pada Vlan 99 adalah lokasi steril yang diguanakan oleh tim IT untuk *monitoring* semua segmen jaringan. Pada topologi pertama ini penyerang melancarkan serangan pada segmen yang berbeda dengan Investigator yang berada pada segmen IT. Pengambilan data selanjutnya menggunakan topologi lain di mana Penyerang berada pada satu segmen dengan Investigator ditampilkan pada gambar 3.3.



Gambar 3.3 Topologi Jaringan Pengujian 2

Topologi yang ditampilkan pada gambar 3.2 dan 3.3 menjadi topologi pengujian serangan yang dijelaskan pada bagian 3.2.3. Adapun detail pengaturan IP untuk topologi jaringan 1 ditampilkan pada tabel 3.2 dan tabel 3.3 untuk Topologi Jaringan 2.

Tabel 3.2 Detail IP Topologi Jaringan 1

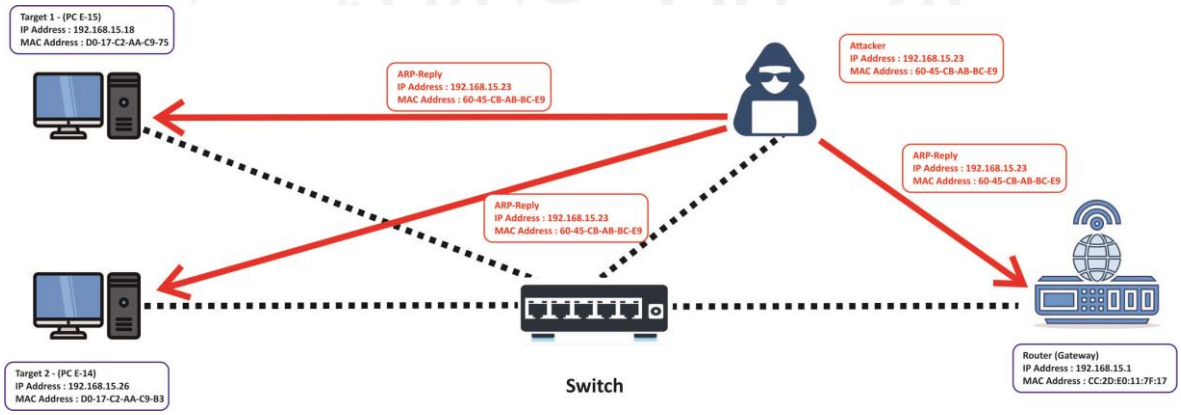
Device	Vlan	IP Address	Netmask	Gateway
Router	15	192.168.15.1	255.255.255.192	-
	99	192.168.99.1	255.255.255.224	-
Attacker	15	192.168.15.23	255.255.255.192	192.168.15.1
27 Host Active	15	192.168.15.2 – 192.168.15.61	255.255.255.192	192.168.15.1
Victim 1	15	192.168.15.18	255.255.255.192	192.168.15.1
Victim 2	15	192.168.15.26	255.255.255.192	192.168.15.1
Investigator	99	192.168.99.24	255.255.255.224	192.168.99.1

Tabel 3.3 Detail IP Topologi Jaringan 2

Device	Vlan	IP Address	Netmask	Gateway
Router	15	192.168.15.1	255.255.255.192	-
	99	192.168.99.1	255.255.255.224	-
Attacker	99	192.168.99.25	255.255.255.224	192.168.99.1
Victim	99	192.168.99.29	255.255.255.224	192.168.99.1
Investigator	99	192.168.99.24	255.255.255.224	192.168.99.1

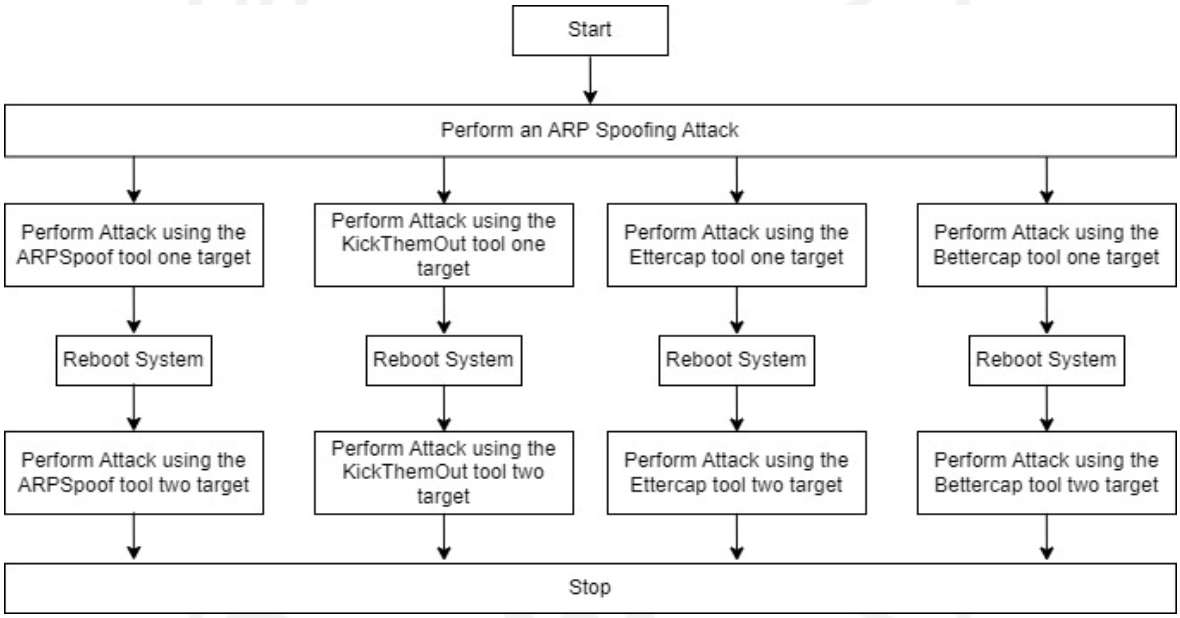
3.2.3 Eksperimen Serangan

Simulasi serangan *ARP Spoofing* dibedakan menjadi 2 berdasarkan Topologi Jaringan pada gambar 3.2 dan 3.3 yaitu tata letak penyerang dan target. Hal ini dimaksudkan untuk mendapatkan beberapa sampel data terkait serangan *ARP Spoofing*. Adapun skenario serangan pada Topologi 1, dilancarkan serangan sebanyak 8 kali serangan. Kemudian untuk skenario serangan pada Topologi 2, dilancarkan sebanyak 4 kali serangan. Serangan ini dibangun dengan beberapa alat serangan *ARP Spoofing* sesuai di tabel 3.1. Skenario serangan yang dibangun ditampilkan pada gambar 3.4.



Gambar 3.4 Skenario Serangan

Gambar 3.4 menggambarkan penyerang dengan *IP Address* 192.168.15.23 dan *MAC Address* 60-45-cb-ab-bc-e9 yang menargetkan dua perangkat komputer. Mesin pertama memiliki *IP Address* 192.168.15.18 dan *MAC Address* D0-17-C2-AA-C9-75, sedangkan komputer kedua memiliki *IP Address* 192.168.15.26 dan *MAC Address* D0-17-C2-AA-C9-B3. Penyerang mengirimkan *ARP-Reply* meskipun tidak ada *ARP-Request* untuk memodifikasi tabel *ARP* target. Penyerang memanfaatkan sebuah router, yang biasanya menjadi gateway untuk semua perangkat komputer dan memiliki identitas *IP Address* 192.168.15.1 *MAC Address* CC: 2D: E0: 11: 7F: 17. *ARP spoofing* adalah serangan yang mengeksploitasi kelemahan pada Protokol *ARP* untuk mengubah isi *cache* tabel *ARP*. Sedangkan alur serangan ditampilkan pada gambar 3.5.



Gambar 3.5 Alur Serangan *ARP Spoofing*

Pada gambar 3.5 serangan ARP dibangun menggunakan empat alat yang diantaranya arpspoof, kickthemout, Ettercap, dan bettercap.

1. *ARPSpoof* adalah alat dengan CLI. Penyerang akan mencoba untuk mendapatkan informasi tentang *host* aktif di jaringan, dan tidak ada fitur pemindaian di arpspoof. Menggunakan alat arp-scan untuk mendapatkan *IP* target dalam skenario pemindaian. setelah mendapatkan informasi, target dapat diserang. Berikut referensi penggunaan ARPSpoof.

arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host Keterangan : - [-I interface] adalah antaramuka NIC yang digunakan untuk melakukan serangan

- [-c own|host|both] merupakan optional yang dapat digunakan untuk menentukan target alamat *hardware* saat memulihkan konfigurasi *ARP*.
- [-t target] option yang digunakan untuk menentukan target, jika option ini dilewati makan semua *host* dalam satu LAN akan menjadi target serangan.
- [-r] merupakan parameter untuk merusak *table arp* pada kedua *host* (*host* dan *target*), option ini berlaku dalam keadaan pengguanaan *option* -t secara bersamaan
- host merupakan letak untuk mencegat lalu lintas, umumnya pada *gateway* lokal

Implementasi serangan menggunakan alat arpspoof ditampilkan pada gambar 3.5.

```
┌─[root@ParrotOS]─[/home/parrot]
└──╼ #arpspoof
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host
┌─[✗]─[root@ParrotOS]─[/home/parrot]
└──╼ #arpspoof -i eth0 -t 192.168.15.1 -r 192.168.15.18
```

Gambar 3.6 Implementasi serangan menggunakan alat arpspoof

2. *KickThemOut* adalah alat berbasis python. Fitur pemindaian dibangun ke dalam alat, sehingga tidak memerlukan agen lain untuk mencari informasi target, dan alat berbasis python akan menandai serangan dengan deskripsi spoofing yang dimulai. Saat alat ini digunakan untuk memindai, *host* aktif akan ditampilkan pada dashbord dengan masing-masing memiliki nomor urutan yang kemudian nomor tersebut dijadikan sebagai parameter untuk *host* yang ditarget. Implementasi serangan pada gambar 3.7.

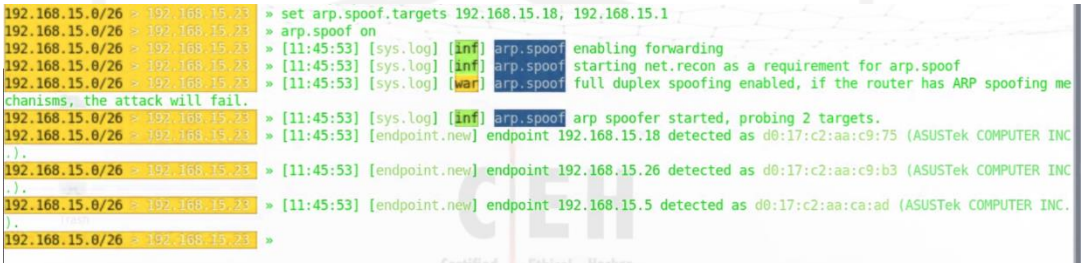
```
clear - Parrot Terminal                                  ×   python3 kickthemout.py - Parrot Terminal
 [0] 192.168.15.1      CC:2D:E0:11:7F:17      Routerboard.com (N/A)
 [1] 192.168.15.2      D0:17:C2:AA:CA:79      ASUSTek COMPUTER INC. (N/A)
 [2] 192.168.15.3      D0:17:C2:AA:F5:DA      ASUSTek COMPUTER INC. (N/A)
 [3] 192.168.15.4      D0:17:C2:AA:CA:61      ASUSTek COMPUTER INC. (N/A)
 [4] 192.168.15.5      D0:17:C2:AA:CA:AD      ASUSTek COMPUTER INC. (N/A)
 [5] 192.168.15.7      D0:17:C2:AA:F4:8C      ASUSTek COMPUTER INC. (N/A)
 [6] 192.168.15.8      74:D4:35:22:FD:C0      GIGA-BYTE TECHNOLOGY CO., (N/A)
 [7] 192.168.15.12     D0:17:C2:AA:F5:29      ASUSTek COMPUTER INC. (N/A)
 [8] 192.168.15.16     74:D4:35:22:F5:BA      GIGA-BYTE TECHNOLOGY CO., (N/A)
 [9] 192.168.15.17     74:D4:35:23:C2:FF      GIGA-BYTE TECHNOLOGY CO., (N/A)
[10] 192.168.15.18     D0:17:C2:AA:C9:75      ASUSTek COMPUTER INC. (N/A)
[11] 192.168.15.19     D0:17:C2:AA:C9:3B      ASUSTek COMPUTER INC. (N/A)
[12] 192.168.15.20     74:D4:35:22:FD:E9      GIGA-BYTE TECHNOLOGY CO., (N/A)
[13] 192.168.15.21     74:D4:35:22:FD:BF      GIGA-BYTE TECHNOLOGY CO., (N/A)
[14] 192.168.15.22     74:D4:35:22:FD:BE      GIGA-BYTE TECHNOLOGY CO., (N/A)
[15] 192.168.15.24     74:D4:35:23:B7:42      GIGA-BYTE TECHNOLOGY CO., (N/A)
[16] 192.168.15.25     74:D4:35:22:F7:06      GIGA-BYTE TECHNOLOGY CO., (N/A)
[17] 192.168.15.26     D0:17:C2:AA:C9:B3      ASUSTek COMPUTER INC. (N/A)
[18] 192.168.15.27     D0:17:C2:AA:C9:A4      ASUSTek COMPUTER INC. (N/A)
[19] 192.168.15.41     D0:17:C2:AA:F5:EE      ASUSTek COMPUTER INC. (N/A)
[20] 192.168.15.42     D0:17:C2:AA:F4:77      ASUSTek COMPUTER INC. (N/A)
[21] 192.168.15.43     D0:17:C2:AA:F5:D5      ASUSTek COMPUTER INC. (N/A)
[22] 192.168.15.47     D0:17:C2:AA:F5:E4      ASUSTek COMPUTER INC. (N/A)
[23] 192.168.15.50     74:D4:35:22:FE:34      GIGA-BYTE TECHNOLOGY CO., (N/A)
[24] 192.168.15.51     74:D4:35:22:FE:1A      GIGA-BYTE TECHNOLOGY CO., (N/A)
[25] 192.168.15.52     D0:17:C2:AA:C9:71      ASUSTek COMPUTER INC. (N/A)

Choose devices to target (comma-separated): 10,17,0
```

Gambar 3.7 Implementasi Serangan Menggunakan alat KickThemOut

3. *Ettercap* adalah aplikasi dengan GUI yang menyediakan banyak fitur serangan lanjutan yang khusus digunakan untuk menyerang target. Sementara itu, pencarian informasi oleh *host* pemindaian aktif juga ditemukan di alat ini. Melalui GUI, semua *host* yang aktif akan terdeteksi dan ditampilkan di dashboard Ettercap. Serangan arp dapat dieksekusi ketika target telah ditambahkan. Implementasi serangan pada gambar 3.8

Gambar 3.8 Implementasi Serangan Menggunakan Alat Ettercap

4. *Bettercap* merupakan salah satu alat untuk pengujian keamanan jaringan dan memiliki banyak fitur untuk melakukan serangan berikutnya. Pencarian informasi *host* aktif dapat dipindai langsung menggunakan alat ini. Pemindaian menunjukkan bahwa *host* saat ini aktif di jaringan internal. Implementasi serangan ditunjukkan pada gambar 3.9



Gambar 3.9 Implementasi Serangan Menggunakan Alat Bettercap

3.2.4 Metode Investigasi Forensik

Proses investigasi ini menggunakan metode TAARA sebagai acuan untuk menyelesaikan penelitian ini dan secara lengkap akan dibahas hasilnya pada Bab 4. Metode TAARA memiliki beberapa tahapan, seperti terlihat pada Gambar.

Gambar 3.10 Metode TAARA

Gambar 3.10 merupakan tahapan metode TAARA dimana setiap tahapan dihubungkan dengan tahapan berikutnya untuk mengarahkan proses forensik jaringan.

1. *Trigger* adalah suatu tindakan yang dilakukan sebagai reaksi terhadap penyerangan yang memerintahkan penyidik untuk melakukan penyelidikan.
2. *Acquire* adalah tindakan mengumpulkan segala bentuk bukti dan informasi untuk menduga penyebab suatu peristiwa penyerangan. Acquire adalah respons terhadap pemicu aktivitas mencurigakan di tahap sebelumnya.
3. *Analyze* merupakan proses pengumpulan bukti dan informasi yang ada, kemudian dikorelasikan sehingga menimbulkan pertanyaan terkait penyerangan yang terjadi.
4. *Report* adalah penyusunan laporan berdasarkan hasil analisis dengan mendokumentasikan seluruh kegiatan yang berkaitan dengan temuan yang diperoleh.
5. *Action* adalah rekomendasi aktif sesuai dengan isi laporan.

Bagian hasil dan pembahasan akan memberikan penjelasan rinci tentang metode ini.

3.2.5 Evaluasi Hasil

Tahapan ini merupakan proses mengevaluasi hasil penerapan terkait dengan komparasi alat forensik yang digunakan dalam hal ini wireshark dan network miner untuk memvalidasi bukti yang didapatkan dari proses investigasi forensik.

3.2.6 Kesimpulan

Tahapan ini merupakan kesimpulan dari keseluruhan penelitian yang dilakukan dalam bentuk laporan.

BAB 4

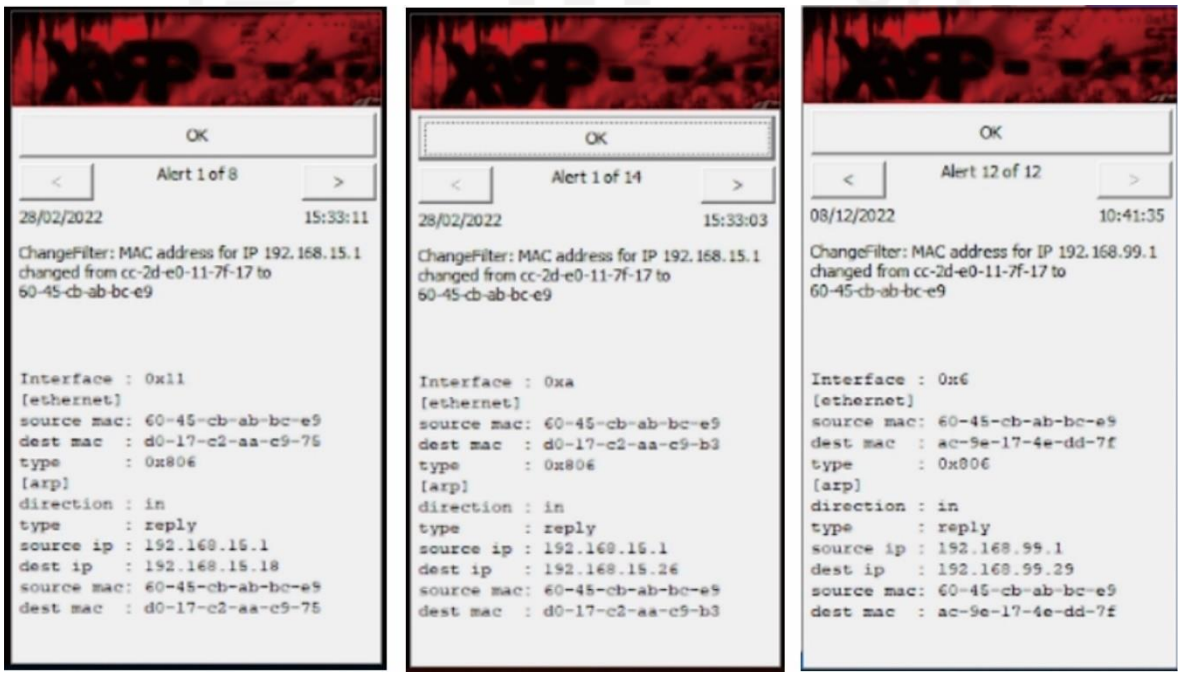
Hasil dan Pembahasan

Bab ini membahas secara lengkap dari penelitian yang diangkat tentang analisis serangan *ARP Spoofing* dengan menerapkan metode TAARA sebagai metode investigasi forensik jaringan. TAARA memiliki 5 tahapan yaitu *Trigger, Acquire, Analyze, Report, Action* yang akan diuraikan secara detail pada bagian pembahasan ini.

4.1 Trigger

Trigger merupakan tahapan awal dalam metode TAARA yakni sebagai pemicu untuk segera dilakukannya investigasi. Dalam skenario kasus serangan *ARP Spoofing* aplikasi alert dari XARP menjadi pemicu untuk dilakukan investigasi. XARP merupakan aplikasi untuk mendeteksi adanya indikasi seranagan ARP Spoof. Namun, dalam penelitian yang dilakukan (Hafizh et al., 2020) menunjukkan bahwa dengan hanya penerapan XARP tidak dapat memastikan bahwa serangan yang terjadi benar-benar serangan *ARP Spoofing*.

Kelemahan dari alat pendeteksian XARP ini terletak pada *Security Level* yang memiliki 4 level yaitu *aggressive, high, basic, minimal*. Maka dari hasil pendeteksian ini perlu dilakukan investigasi untuk memastikan apakah serangan yang terjadi benar faktanya. *Log* pada XARP dapat diakuisisi namun tidak dapat di eksplorasi lebih lanjut baik menggunakan Wireshark ataupun Network Miner. Gambar 4.1 merupakan *trigger* untuk dilakukan investigasi.



Gambar 4.1 Deteksi adanya indikasi serangan *ARP Spoofing* dengan menggunakan XARP

Pada gambar 4.1 merupakan *alert* dari XARP pada sisi *client* yang menunjukkan *IP address* 192.168.15.1 (gambar 1 dan 2 pengujian topologi 1), dan 192.168.99.1 (pengujian di topologi 2) melakukan *reply*, namun dengan *source mac* yang sama yaitu 60:45:CB:AB:BC:E9 (dalam skenario merupakan *MAC Address* penyerang. Alert ini yang kemudian digunakan sebagai trigger untuk menindak lanjuti proses investigasi di tahap selanjutnya.

4.2 Acquire

Dalam proses pengumpulan ini akan melihat proses awal investigasi yang melibatkan studi tentang *trigger* yang menentukan tindakan selanjutnya. Dalam proses pengumpulan ini terdapat beberapa komponen penting yakni proses observasi dengan menggali informasi dari pihak-pihak terkait, pengumpulan *packet capture* (PCAP) trafik lalu lintas jaringan menggunakan perekaman melalui sisi router dengan *packet sniffer*, dan *logging* yang merupakan fitur dari pada RouterOS Mikrotik.

4.2.1 Mengumpulkan Informasi

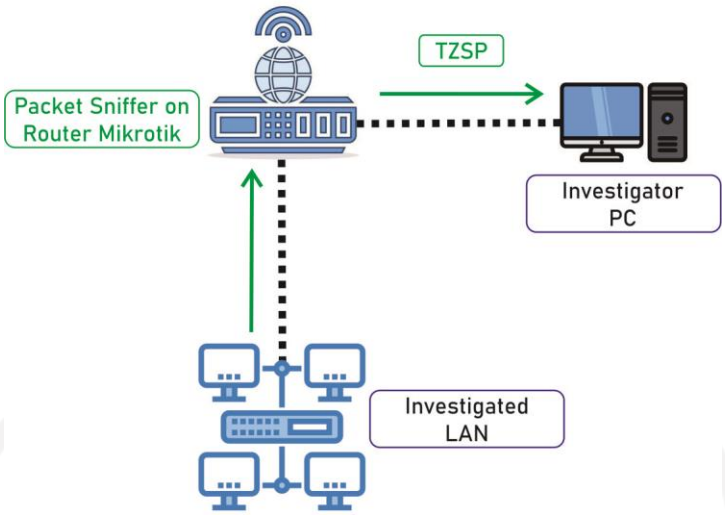
Observasi lapangan berkaitan dengan *trigger* yang terjadi sehingga pendalaman terkait informasi apa saja yang dapat dikumpulkan. Dalam kasus ini beberapa informasi yang diberikan terkait dengan *trigger* yang terjadi pada beberapa *host* yang terindikasi mendapatkan serangan *ARP Spoofing*. Berdasarkan informasi yang didapatkan dapat menyimpulkan beberapa informasi yang ditampilkan pada tabel 4.1.

Tabel 4.1 Detail informasi dari observasi lapangan

Perangkat Terindikasi menjadi Target Serangan ARP Spoofing	**Vlan**	**IP Address**	**Mac Address**	**Gateway**
E-14	15	192.168.15.26	D0-17-C2-AA-C9-75	192.168.15.1
E-15	15	192.168.15.18	D0-17-C2-AA-C9-B3	192.168.15.1
DESKTOP-OSMI5DB	99	192.168.99.29	AC-9E-17-4E-DD-7F	192.168.99.1
ROUTER	-	192.168.15.1 192.168.99.1	CC:2D:E0:11:7F:17	-

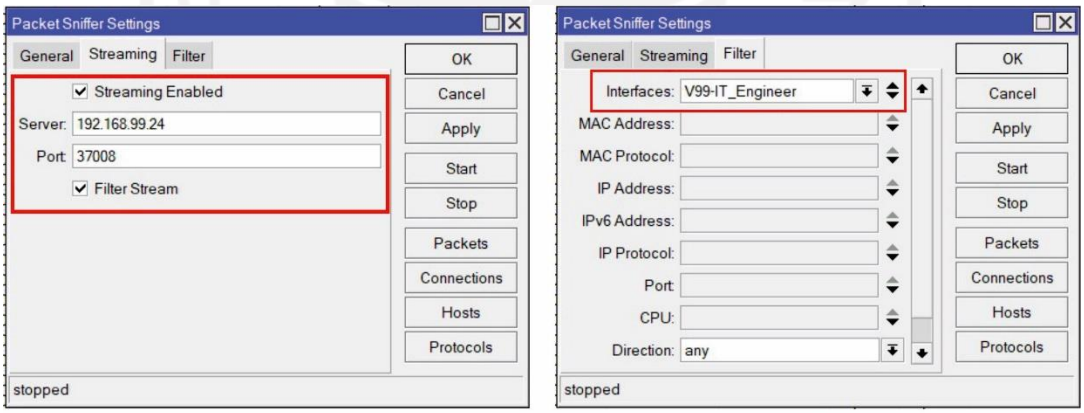
4.2.2 Mengumpulkan Bukti Digital

Seperti dijelaskan di bagian 2.2.2 bahwa investigasi melibatkan jaringan akan melibatkan tahap *capture.* Pada penelitian ini proses *capture* ini dilakukan pada sisi router dengan teknik *sniffer* yang diilustrasikan pada gambar 4.2.



Gambar 4.2 Proses *sniffer* dari sisi Router

Router akan melakukan proses *sniffer* terhadap jaringan local yang digunakan untuk proses pengujian serangan *ARP Spoofing*, dalam hal ini sesuai ditampilkan pada bagian 3.2.2 yaitu vlan 15 dan vlan 99. Proses *capture* yang dijalankan oleh router mikrotik menghasilkan sebuah protokol TZSP (*Tazmen Sniffer Protocol*) yang dikirimkan ke PC Investigator. Secara pengaturan ditampilkan pada gambar 4.3.

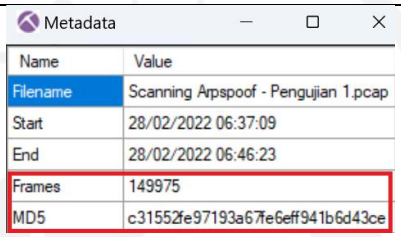
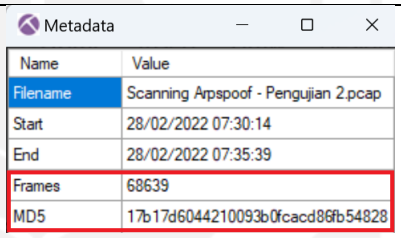
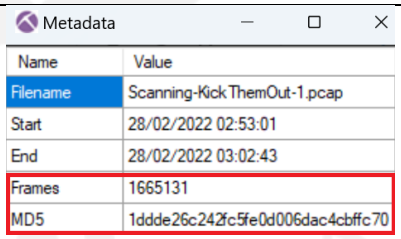
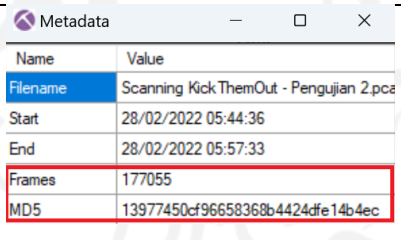
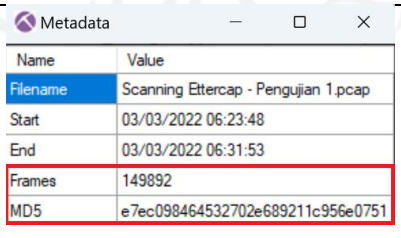


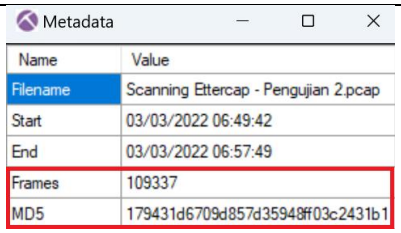
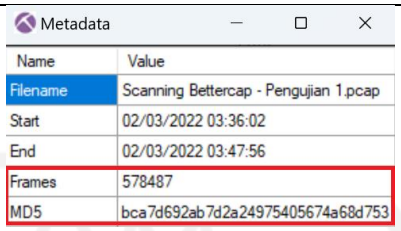
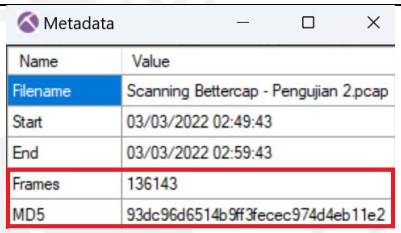
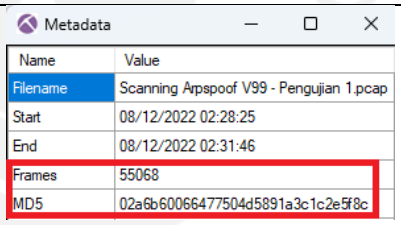
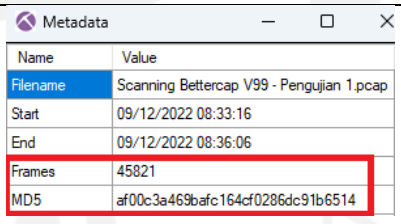
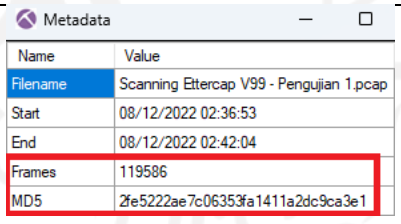
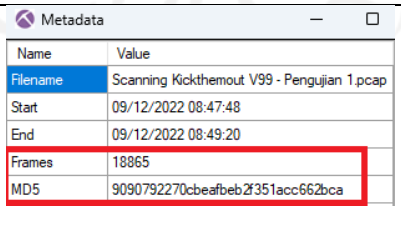
Gambar 4.3 Pengaturan *Packet Sniffer* pada Sisi Router

Pada gambar 4.3 bagian A adalah pengaturan untuk mengaktifkan *streaming sniff* dengan memilih server 192.168.99.24 sebagai PC Investigator, port yang digunakan menggunakan 37008 sehingga pada sisi PC Investigator juga diharuskan open port 37008 untuk menerima *Packet Sniffer* yang dikirimkan oleh router. Pada bagian *Filter Stream* merupakan personalisasi dari pada gambar 4.3 bagian B. Pengaturan yang terlihat pada gambar 4.3 bagian B menunjukkan *Interfaces* V99 IT_Engineer, hal ini menunjukkan *sniffer* yang dilakukan akan mengarah ke interfaces teresebut.

Hasil pada tahapan ini yaitu mengumpulkan semua file dari hasil *capture* yang dilakukan pada sisi router, File yang dikumpulkan pertama dilakukan pemeriksaan dengan menggunakan hashing. Pemeriksaan Hash MD5 yang pertama mengggunakan *Network Miner*, pemeriksaan ini juga akan memvalidasi integritas bukti yang dikumpulkan jika dikemudian hari akan dilakukan pemeriksaan oleh investigator lainnya, Hasil pengumpulan ini ditampikan dalam tabel 4.2.

Tabel 4.2 Pengumpulan data dengan pemeriksaan menggunakan alat Network Miner

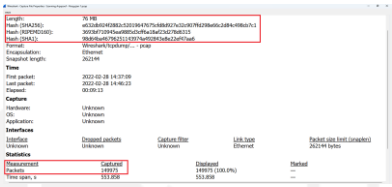
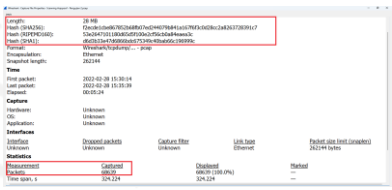
File	MD5 Hash	Screen Recording	Packet/Frames
Scanning Arpspoof 1 (PCAP1)	c31552fe97193a67fe6eff941b6d43ce		149975 Packet
Scanning Arpspoof 2 (PCAP2)	17b17d6044210093b0fcacd86fb54828		68639 Packet
Scanning KickThemOut 1 (PCAP3)	1ddde26c242fc5fe0d006dac4cbffc70		1665131 Packet
Scanning KickThemOut 2 (PCAP4)	13977450cf96658368b4424dfe14b4ec		177055 Packet
Scanning Ettercap 1 (PCAP5)	e7ec0984645327027e689211c956e0751		149892 Packet

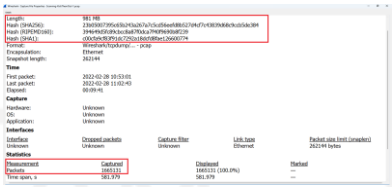
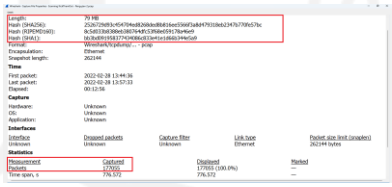
Scanning Ettercap 2 (PCAP6)	179431d6709d857d35948ff03c2431b1		109337 Packet
Scanning Bettercap 1 (PCAP7)	bca7d692ab7d2a24975405674a68d753		578487 Packet
Scanning Bettercap 2 (PCAP8)	93dc96d6514b9ff3fecec974d4eb11e2		136143 Packet
Scanning Arpspoof V99 - Pengujian 1.pcap (PCAP 9)	02a6b60066477504d5891a3c1c2e5f8c		55068 Packet
Scanning Bettercap V99 - Pengujian 1.pcap (PCAP 10)	af00c3a469bafc164cf0286dc91b6514		45821 Packet
Scanning Ettercap V99 - Pengujian 1.pcap (PCAP 11)	2fe5222ae7c06353fa1411a2dc9ca3e1		119586 Packet
Scanning Kickthemout V99 - Pengujian 1.pcap (PCAP 12)	9090792270cbeafbeb2f351acc662bca		18865 Packet

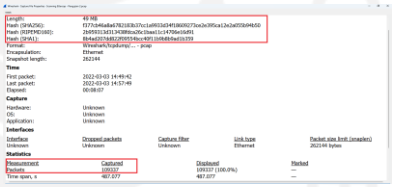
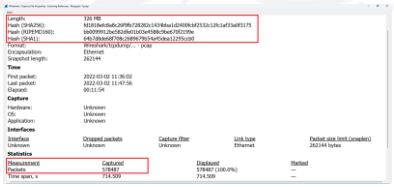
Pemeriksaan kedua digunakan alat wireshark, pemeriksaan ini juga bertujuan untuk memvalidasi file bukti untuk menjaga integeritas data yang diperoleh. Pengguaan wireshark untuk pengujian nilai *Hash* terdapat beberapa metode algoritma kriptografi menggunakan

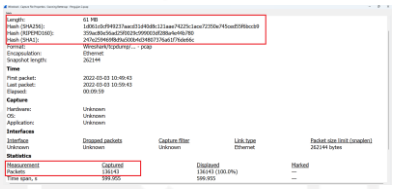
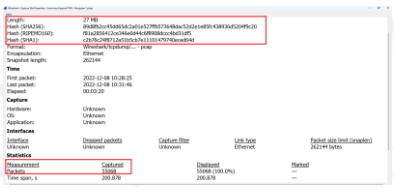
Hash SHA256, RIPEMD160, SHA1. Detail pemeriksaan untuk File bukti yang dikumpulkan menggunakan wireshark ditampilkan pada tabel 4.3.

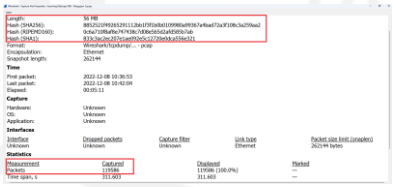
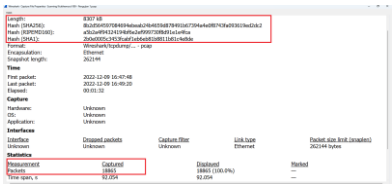
Tabel 4.3 Pengumpulan data dengan pemeriksaan menggunakan alat Wireshark

File	Hash	Screen Recording	Packet/Frames
Scanning Arpspoof 1 (PCAP1)	**Hash (SHA256):** e632db924f2882c52019647675cfd8d927e32c907ffd298e66c2d84c498cb7c1 **Hash (RIPEMD160):** 3693bf710945ea9885d3cff6a18af23d278d6315 **Hash (SHA1):** 98d64ba46796251143974a492843e8e22ef47aa6		149975 Packet
Scanning Arpspoof 2 (PCAP2)	**Hash (SHA256):** f2ecde1cbe867852b68fb07ed244079b841a167f6f3c0d28cc2a8263728391c7 **Hash (RIPEMD160):** 53e2647101180d65d5f100e2cf56cb0a84eaea3c **Hash (SHA1):** d6d3b33e47d6866bdc675349c40bab66c196999c		68639 Packet

Scanning KickThemOut 1 (PCAP3)	**Hash (SHA256):** 23b05007395c65b243a267a7c5cd56eefd8b527d4cf7c43839d68c9ccb5de384 **Hash (RIPEMD160):** 394649d5fc89cbcc8a87f0dca7f40f9690b8f239 **Hash (SHA1):** c00cfa9cf83f91dc7292a18dcfd8fae126600774		1665131 Packet
Scanning KickThemOut 2 (PCAP4)	**Hash (SHA256):** 2526729d93c454704ed8268ded8b816ee5566f3a8d479318eb2347b770fe57bc **Hash (RIPEMD160):** 8c5d033b8388eb380764dfc53f68e059178a46e9 **Hash (SHA1):** bb3bd091958377434086c833e41e1d66b344e5a9		177055 Packet
Scanning Ettercap 1 (PCAP5)	**Hash (SHA256):** 1470099519f68d050748cb3243fcff257fc9ca737a19094b347e45dcb0e86dd3		149892 Packet

	Hash (RIPEMD160): edd691afa50cd5937cc798de25f9923a6d8191e6 **Hash (SHA1):** 5c99955ad57d98d124e930847e092ff6ba5e83e4		
Scanning Ettercap 2 (PCAP6)	**Hash (SHA256):** f377cb46a8a6782183b37cc1a9933d34f18609273ce2e395ca12e2a055b94b50 **Hash (RIPEMD160):** 2b959313d313438fdca26c1baa11c14706e16d91 **Hash (SHA1):** 8b4ad207dd822f09554bcc40f11b9b8b9ad1b359		109337 Packet
Scanning Bettercap 1 (PCAP7)	**Hash (SHA256):** fd1818efc8a8c26f9fb728282c1434bba1d2400fcbf2532c12fc1af33a0f3175 **Hash (RIPEMD160):** bb0099912be582dfe01b03e4588c9be670f2199e		578487 Packet

	Hash (SHA1): 64b7d8de68f708c2689679b54a45dea12295ccb0		
Scanning Bettercap 2 (PCAP8)	**Hash (SHA256):** 1d061c0cf949237aacd31d40d8c121aae74225c1ace72350e745ced55f6bccb9 **Hash (RIPEMD160):** 359ac80e56ad25f0029c999003df288a4e44b780 **Hash (SHA1):** 247e259469f8d9a500b4d34807376a61f76de66c		136143 Packet
Scanning Arpspoof V99 - Pengujian 1.pcap (PCAP 9)	**Hash (SHA256):** 89d8fb2cc45dd65dc2a01e527ffb573648dac52d2e1e85fc438936d5204f9c20 **Hash (RIPEMD160):** f81a2856412ce346e0d44c6f8908dccc4bd31df5 **Hash (SHA1):** c2b76c24f8712a51b5cb7e11101479740eced64d		55068 Packet

Scanning Bettercap V99 - Pengujian 1.pcap (PCAP 10)	**Hash (SHA256):** 3a8b1e91a62cafc76b454fbc6611d8e527900054a617a53fdda869d3660678c1d **Hash (RIPEMD160):** 859eb1b45a364cebb545d7268ff1e2b6db3f10dd **Hash (SHA1):** e24c333f4d5c891b3360a66ac74c01d832a54ec9		45821 Packet
Scanning Ettercap V99 - Pengujian 1.pcap (PCAP 11)	**Hash (SHA256):** 8852521f49265291112bb1f3f1b0b0109980a99367a4bad72a3f108c3a259aa2 **Hash (RIPEMD160):** 0c6a710f8af8e747438c7d08e565d2afd585b7ab **Hash (SHA1):** 833c3ac2ec207e1ae092e5c12720e0dca556e321		119586 Packet
Scanning Kickthemout V99 - Pengujian	**Hash (SHA256):** 8b2d564597084694ebeab24b4659d878491b67394a4e0f8743fa093619ed2dc2Hash **(RIPEMD160):**		18865 Packet

1.pcap (PCAP 12)	a5b2a4f94324194bf6e2ef999730f8d91e1e4fca **Hash (SHA1):** 2b0e0005c3453fcabf1eb6eb81b8811b81c4e8de		

Tabel 4.2 dan tabel 4.3 merupakan pemeriksaan awal untuk pengumpulan data dengan menggunakan dua alat forensik bertujuan untuk validasi terkait dengan integritas data yang dikumpulkan. Tahapan ini memvalidasi apabila suatu saat jika data diubah atau ditempa, nilai hash juga akan berubah. Dari kedua alat forensik ini didapatkan sebuah informasi tentang metadata dan uji validasi diantaranya

Alat Forensik	Hashing				Frames / Packet	Times		Length / Size
	MD 5	SHA256	RIPEMD160	SHA1		First Packet	End Packet	
Wireshark	x	✓	✓	✓	✓	✓	✓	✓
Network Miner	✓	x	x	x	✓	✓	✓	✓

4.2.3 Logging Mikrotik

Logging atau *log* merupakan fitur yang dimiliki RouterOS Mikrotik yang mencatat aktivitas dari router mikrotik seperti halnya *system, dhcp, info, warning, debug, hotspot* dan lain sebagainya yang kemudian dapat di ekspor seperti yang ditampilkan pada gambar 4.4.

Log

Freeze

#	Time	Buffer	Topics	Message
832	Jan/31/2023 11:08:19	memory	dhcp, debug, packet	DHCP --->: Domain-Name = "wifi.univmulia.net"
833	Jan/31/2023 11:08:22	memory	hotspot, info, debug	2213074 (10.20.9.18): trying to log in by http-chap
834	Jan/31/2023 11:08:22	memory	hotspot, info, debug	HOTSPOT --->: 2213074 (10.20.9.18): trying to log in by http-chap
835	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): local user not found
836	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): sending RADIUS authentication request
837	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): Access-Accept from RADIUS
838	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): user profile <Mahasiswa> from RADIUS
839	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): using profile <Mahasiswa>
840	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): interim-update <60> from RADIUS
841	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): rate limit <5242880/7340032 0/0 0/0 0/0 0 5242880/7340032> from RADIUS
842	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): adding ip->user binding
843	Jan/31/2023 11:08:22	memory	hotspot, debug	HOTSPOT --->: 2213074 (10.20.9.18): adding queue <5242880/7340032 0/0 0/0 0/0 0 5242880/7340032>
844	Jan/31/2023 11:08:22	memory	hotspot, account, info, debug	2213074 (10.20.9.18): logged in
845	Jan/31/2023 11:08:22	memory	hotspot, account, info, debug	HOTSPOT --->: 2213074 (10.20.9.18): logged in
846	Jan/31/2023 11:08:31	memory	hotspot, debug	HOTSPOT --->: V2-Hotspot: dhcp host 10.20.6.16 removed: keepalive timeout
847	Jan/31/2023 11:08:45	memory	dhcp, debug	DHCP --->: Dhcp2-Hotspot received request id 3390822304 from 0.0.0.0 '1:32:6:9c:ca:65:a0'
848	Jan/31/2023 11:08:45	memory	dhcp, debug, packet	DHCP --->: ciaddr = 0.0.0.0
849	Jan/31/2023 11:08:45	memory	dhcp, debug, packet	DHCP --->: chaddr = 32:06:9C:CA:65:A0
850	Jan/31/2023 11:08:45	memory	dhcp, debug, packet	DHCP --->: Msg-Type = request
851	Jan/31/2023 11:08:45	memory	dhcp, debug, packet	DHCP --->: Client-Id = 01-32-06-9C-CA-65-A0
852	Jan/31/2023 11:08:45	memory	dhcp, debug, packet	DHCP --->: Address-Request = 10.20.3.164
853	Jan/31/2023 11:08:45	memory	dhcp, debug, packet	DHCP --->: Max-DHCP-Message-Size = 1500
854	Jan/31/2023 11:08:45	memory	dhcp, debug, packet	DHCP --->: Class-Id = "HUAWEI:android:YAL"

Gambar 4.4 Sistem *logging* mikrotik

Logging dari RouterOS Mikrotik dikumpulkan secara remote yang dikirimkan kepada PC Investigator. *Logging* ini memiliki keterbatasan tidak dapat diperiksa oleh alat

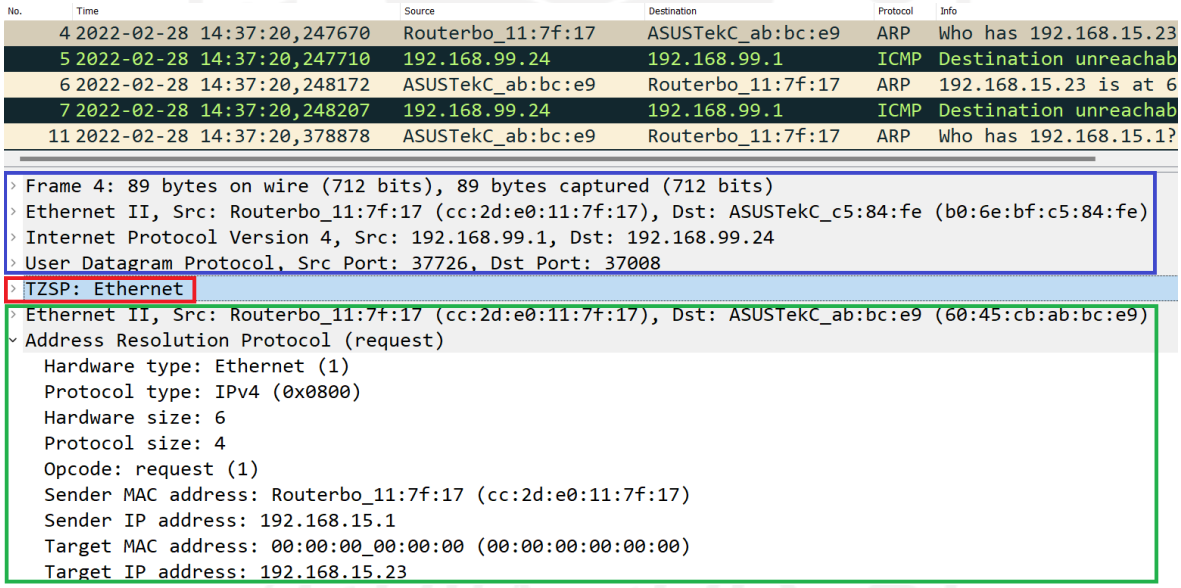
bantu forensik Wireshark dan juga Network Miner. Adapun 3 File *logging* yang berhasil didapatkan sebagai Berikut:

Tabel 4.4 *Logging* file RouterOS Mikrotik

File	Hash MD5
ccr-univmulia.2022.02.28.log	34745c9aa384ff9ff09d7e68e092aef0
ccr-univmulia.2022.03.02.log	882c1135be783dcbd7fc9b7b6b5ac983
ccr-univmulia.2022.03.03.log	1a0906f25cdc4abf845e5e78505e0756

4.3 Analyze

Data yang berhasil dikumpulkan dari tahapan sebelumnya menunjukkan terdapat dua belas file dalam bentuk format .pcap yang dapat dianalisa baik menggunakan alat forensik network miner dan juga alat wireshark. Analisis merupakan tahapan pemeriksaan lebih mendalam terkait dengan indikasi serangan yang terjadi. File PCAP yang dihasilkan dari sisi router menggunakan *packet sniffer* memperlihatkan sebuah protokol TZSP, mengenkapsulasi protokol lainnya yang ditunjukkan pada gambar 4.5.



Gambar 4.5 Protokol TZSP

Gambar 4.5 merupakan sebuah hasil komunikasi dari *packet sniffer* yang dijalankan dari sisi router yang kemudian dikirimkan kepada PC Investigator. Layer ini berisikan informasi antara Router dengan *IP Address* 192.168.99.1 berkomunikasi dengan PC Investigator dengan *IP Address* 192.168.99.24 ditandai warna biru. *Packet Sniffer* yang dijalankan oleh router menghasilkan sebuah protokol TZSP ditandai dengan warna merah. Protokol tersebut mengankapsulasi protokol lain yang sedang di *sniffer* oleh router,

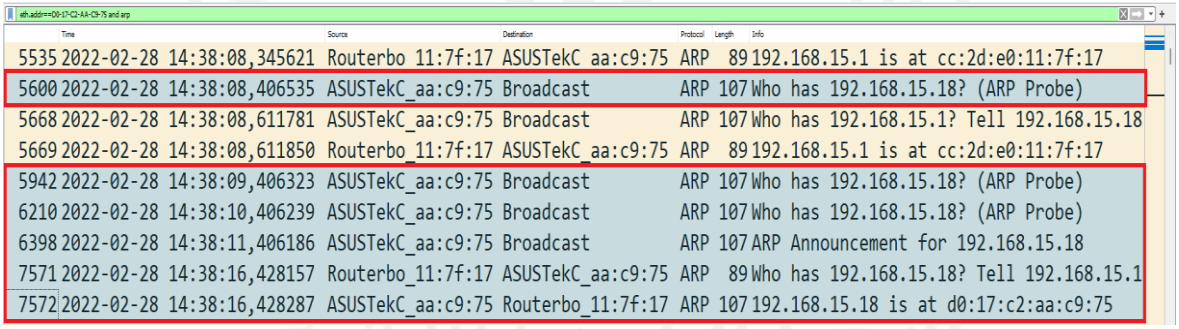
didalamnya terdapat komunikasi antara Router dengan PC Penyerang menggunakan protokol *ARP* ditandai kotak berwarna hijau.

Kondisi ini merupakan keadaan normal dimana router melalui protokol *ARP* dengan *Opcode* berupa *arp-request* menanyakan kepemilikin *IP Address* 192.168.15.23 dengan target *MAC Address* 00:00:00:00:00:00, yang menunjukkan *IP Address* tersebut belum terikat dengan *MAC Address* manapun pada frame 4. File PCAP lainnya yang dihasilkan dari *packet sniffer* menunjukkan hal yang sama bahwa di dalam didalam protokol TZSP memiliki informasi protokol lainnya.

Proses analisis berikutnya berfokus pada protokol *ARP* berdasarkan kasus serangan *ARP Spoofing.* Pemeriksaan yang pertama akan melihat bagaimana kondisi berdasarkan informasi yang telah didapat di bagian 4.2.1 terkait protokol *ARP* dengan memfilter berdasarkan f*ield name* untuk masing-masing *MAC Address* perangkat yang menjadi target.

Filter Keyword di Alat Wireshark*:*
eth.addr==D0-17-C2-AA-C9-75 and arp
eth.addr==D0-17-C2-AA-C9-B3 and arp
eth.addr==AC-9E-17-4E-DD-7F and arp

Hasil Analisa ditampilkan pada gambar 4.6 untuk PC E-15, gambar 4.7 untuk PC E-14 dan gambar 4.8 untuk DESKTOP-OSMI5DB.

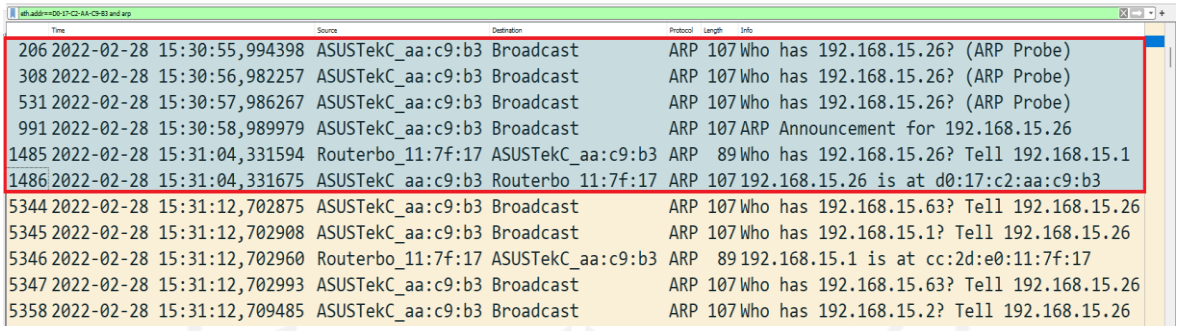


	Time	Source	Destination	Protocol	Length	Info
5535	2022-02-28 14:38:08,345621	Routerbo_11:7f:17	ASUSTekC_aa:c9:75	ARP	89	192.168.15.1 is at cc:2d:e0:11:7f:17
5600	2022-02-28 14:38:08,406535	ASUSTekC_aa:c9:75	Broadcast	ARP	107	Who has 192.168.15.18? (ARP Probe)
5668	2022-02-28 14:38:08,611781	ASUSTekC_aa:c9:75	Broadcast	ARP	107	Who has 192.168.15.1? Tell 192.168.15.18
5669	2022-02-28 14:38:08,611850	Routerbo_11:7f:17	ASUSTekC_aa:c9:75	ARP	89	192.168.15.1 is at cc:2d:e0:11:7f:17
5942	2022-02-28 14:38:09,406323	ASUSTekC_aa:c9:75	Broadcast	ARP	107	Who has 192.168.15.18? (ARP Probe)
6210	2022-02-28 14:38:10,406239	ASUSTekC_aa:c9:75	Broadcast	ARP	107	Who has 192.168.15.18? (ARP Probe)
6398	2022-02-28 14:38:11,406186	ASUSTekC_aa:c9:75	Broadcast	ARP	107	ARP Announcement for 192.168.15.18
7571	2022-02-28 14:38:16,428157	Routerbo_11:7f:17	ASUSTekC_aa:c9:75	ARP	89	Who has 192.168.15.18? Tell 192.168.15.1
7572	2022-02-28 14:38:16,428287	ASUSTekC_aa:c9:75	Routerbo_11:7f:17	ARP	107	192.168.15.18 is at d0:17:c2:aa:c9:75

Gambar 4.6 Proses PC E-15 meresolusi *IP Address* 192.168.15.18 ke *MAC Address* D0-17-C2-AA-C9-75

Dalam prosesnya PC E-15 menerjemahkan IP 192.168.15.18 ke *MAC Address* nya D0-17-C2-AA-C9-75 dimulai dari *frame* 5600 dengan melakukan *broadcast message* keseluruh jaringan lokal, *broadcast message* dilakukan kembali yang ditunjukkan pada frame 5942 dan 6210. Pada *frame* yang telah disebutkan terdapat keterangan *ARP Probe* yang merupakan *ARP-Request* dimana permintaan ini meminta sebuah tanggapan apabila permintaan *IP address* telah ada yang memiliki. Saat permintaan tanggapan tidak ada respon, *frame* 6398 mengumumkan bahwa IP 192.168.15.18 diklaim kepemilikannya oleh *MAC*

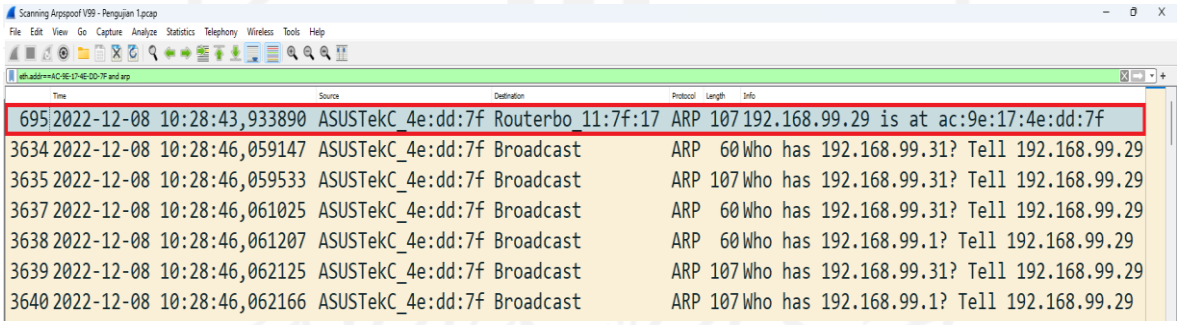
Address D0-17-C2-AA-C9-75. Kemudian komunikasi melalui protokol ARP ini dilanjutkan pada *frame* 7571, router dengan *MAC Address* CC:2D:E0:11:7F:17 menanyakan "siapa yang memiliki IP 192.168.15.18 kepada *MAC Address* D0-17-C2-AA-C9-75. *Frame* 7572 menjelaskan bahwa saat ini *IP Address* 192.168.15.18 telah diterjemahkan ke *MAC Address* D0-17-C2-AA-C9-75.



	Time	Source	Destination	Protocol	Length	Info
206	2022-02-28 15:30:55,994398	ASUSTekC_aa:c9:b3	Broadcast	ARP	107	Who has 192.168.15.26? (ARP Probe)
308	2022-02-28 15:30:56,982257	ASUSTekC_aa:c9:b3	Broadcast	ARP	107	Who has 192.168.15.26? (ARP Probe)
531	2022-02-28 15:30:57,986267	ASUSTekC_aa:c9:b3	Broadcast	ARP	107	Who has 192.168.15.26? (ARP Probe)
991	2022-02-28 15:30:58,989979	ASUSTekC_aa:c9:b3	Broadcast	ARP	107	ARP Announcement for 192.168.15.26
1485	2022-02-28 15:31:04,331594	Routerbo_11:7f:17	ASUSTekC_aa:c9:b3	ARP	89	Who has 192.168.15.26? Tell 192.168.15.1
1486	2022-02-28 15:31:04,331675	ASUSTekC_aa:c9:b3	Routerbo_11:7f:17	ARP	107	192.168.15.26 is at d0:17:c2:aa:c9:b3
5344	2022-02-28 15:31:12,702875	ASUSTekC_aa:c9:b3	Broadcast	ARP	107	Who has 192.168.15.63? Tell 192.168.15.26
5345	2022-02-28 15:31:12,702908	ASUSTekC_aa:c9:b3	Broadcast	ARP	107	Who has 192.168.15.1? Tell 192.168.15.26
5346	2022-02-28 15:31:12,702960	Routerbo_11:7f:17	ASUSTekC_aa:c9:b3	ARP	89	192.168.15.1 is at cc:2d:e0:11:7f:17
5347	2022-02-28 15:31:12,702993	ASUSTekC_aa:c9:b3	Broadcast	ARP	107	Who has 192.168.15.63? Tell 192.168.15.26
5358	2022-02-28 15:31:12,709485	ASUSTekC_aa:c9:b3	Broadcast	ARP	107	Who has 192.168.15.2? Tell 192.168.15.26

Gambar 4.7 Proses PC E-14 meresolusi *IP Address* 192.168.15.26 ke *MAC Address* D0-17-C2-AA-C9-B3

Kemudian proses PC E-14 tidak jauh berbeda dengan penjelasan yang dipaparkan pada proses PC E-15. Sebuah perangkat dengan *MAC Address* D0-17-C2-AA-C9-B3 mengirimkan *broadcast message* ke jaringan local ditunjukkan pada *frame* 206, 308, dan 531. Kemudian pada *frame* 991 Perangkat tersebut menginformasikan melalui *ARP Announcement* terkait kepemilikan *IP Address* 192.168.15.26. *Frame* 1486 perangkat ini menginformasikan kepada Router bahwa IP 192.168.15.26 telah ditetapkan untuk *MAC Address* D0-17-C2-AA-C9-B3.



	Time	Source	Destination	Protocol	Length	Info
695	2022-12-08 10:28:43,933890	ASUSTekC_4e:dd:7f	Routerbo_11:7f:17	ARP	107	192.168.99.29 is at ac:9e:17:4e:dd:7f
3634	2022-12-08 10:28:46,059147	ASUSTekC_4e:dd:7f	Broadcast	ARP	60	Who has 192.168.99.31? Tell 192.168.99.29
3635	2022-12-08 10:28:46,059533	ASUSTekC_4e:dd:7f	Broadcast	ARP	107	Who has 192.168.99.31? Tell 192.168.99.29
3637	2022-12-08 10:28:46,061025	ASUSTekC_4e:dd:7f	Broadcast	ARP	60	Who has 192.168.99.31? Tell 192.168.99.29
3638	2022-12-08 10:28:46,061207	ASUSTekC_4e:dd:7f	Broadcast	ARP	60	Who has 192.168.99.1? Tell 192.168.99.29
3639	2022-12-08 10:28:46,062125	ASUSTekC_4e:dd:7f	Broadcast	ARP	107	Who has 192.168.99.31? Tell 192.168.99.29
3640	2022-12-08 10:28:46,062166	ASUSTekC_4e:dd:7f	Broadcast	ARP	107	Who has 192.168.99.1? Tell 192.168.99.29

Gambar 4.8 Proses PC DESKTOP-OSMI5DB meresolusi *IP Address* 192.168.99.29 ke *MAC Address* AC-9E-17-4E-DD-7F

Untuk proses pada PC DESKTOP-OSMI5DB ditunjukkan pada gambar 4.7 dengan informasi yang didapatkan melalui *frame* 695 bahwa *IP Address* 192.168.99.29 telah ditranslasikan ke *MAC Address* AC-9E-17-4E-DD-7F. Dari hasil ini maka dapat ditarik kesimpulan untuk masing-masing *IP Address* yang diterjemahkan ke dalam *MAC Address* masing-masing perangkat yang kemudian ditampilkan pada tabel .

Tabel 4.5 Waktu Pertama kali *IP Address* di terjemahkan ke *MAC Address* Perangkat E-14, E-15, DESKTOP-OSMI5DB

No	File PCAP	Timestamp	Device	Frame
1	Scanning Arpspoof 1 (PCAP1)	Feb 28, 2022 14:37:58	E-15	7572
2	Scanning Arpspoof 2 (PCAP2)	Feb 28, 2022 15:31:04	E-14	1486
		Feb 28, 2022 15:31:27	E-15	11262
3	Scanning KickThemOut 1 (PCAP1)	Feb 28, 2022 10:54:20	E-15	11657
4	Scanning KickThemOut 2 (PCAP2)	Feb 28, 2022 13:45:20	E-14	1481
		Feb 28, 2022 13:45:37	E-15	6356
5	Scanning Ettercap 1 (PCAP1)	Mar 3, 2022 14:24:47	E-15	9375
6	Scanning Ettercap 2 (PCAP2)	Mar 3, 2022 14:50:21	E-14	1353
		Mar 3, 2022 14:50:45	E-15	10220
7	Scanning Bettercap 1 (PCAP1)	Mar 2, 2022 11:37:02	E-15	11566
8	Scanning Bettercap 2 (PCAP2)	Mar 3, 2022 10:50:18	E-14	2019
		Mar 3, 2022 10:50:40	E-15	9418
9	Scanning Arpspoof V99 - Pengujian 1.pcap	Dec 8, 2022 10:28:43	DESKTOP-OSMI5DB	695

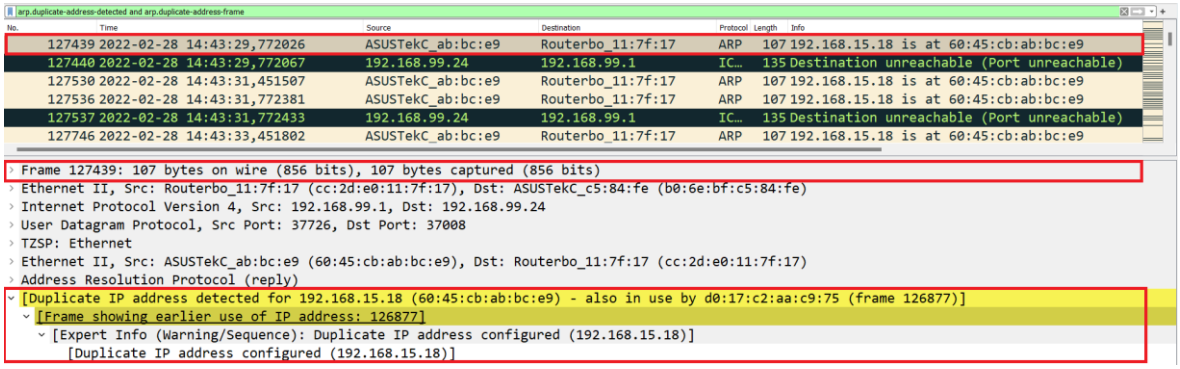
10	Scanning Bettercap V99 - Pengujian 1.pcap	Dec 9, 2022 16:33:44	DESKTOP-OSMI5DB	5093
11	Scanning Ettercap V99 - Pengujian 1.pcap	Dec 8, 2022 10:37:07	DESKTOP-OSMI5DB	3527
12	Scanning Kickthemout V99 - Pengujian 1.pcap	Dec 9, 2022 16:48:07	DESKTOP-OSMI5DB	3559

Analisis diatas menjadi sebuah catatan yang akan menunjukkan bahwa *IP address* 192.168.15.18, 192.168.15.26, dan 192.168.99.29 telah diterjemahkan ke masing-masing *MAC Address* perangkat lengkap dengan timestamp berdasarkan hasil analisa menggunakan alat wireshark. Wireshark memiliki fitur yang lebih lengkap untuk melakukan filter berdasarkan *field name*.

Tahap berikutnya melakukan analisis untuk mendapatkan informasi berkaitan dengan perangkat penyerang yang melakukan duplikasi terhadap *IP Address* yang masing-masing telah diterjemahkan ke *MAC Address* berdasarkan tabel 4.4. Proses ini menggunakan alat wireshark dengan memfilter pada setiap bukti *file pcap* yang dikumpulkan.

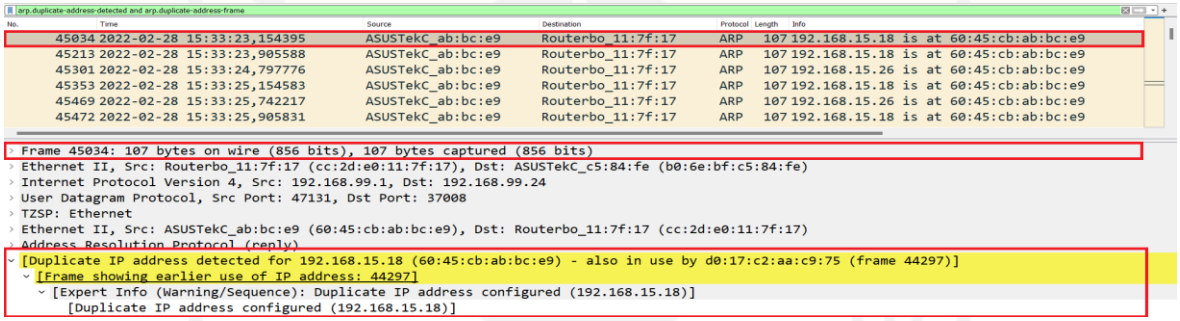
Filter Keyword di alat Wireshark
arp.duplicate-address-detected
arp.duplicate-address-frame

Hasil dari pemeriksaan menunjukkan adanya informasi bahwa telah terjadi duplikasi *IP Address* dari masing-masing bukti file pcap.

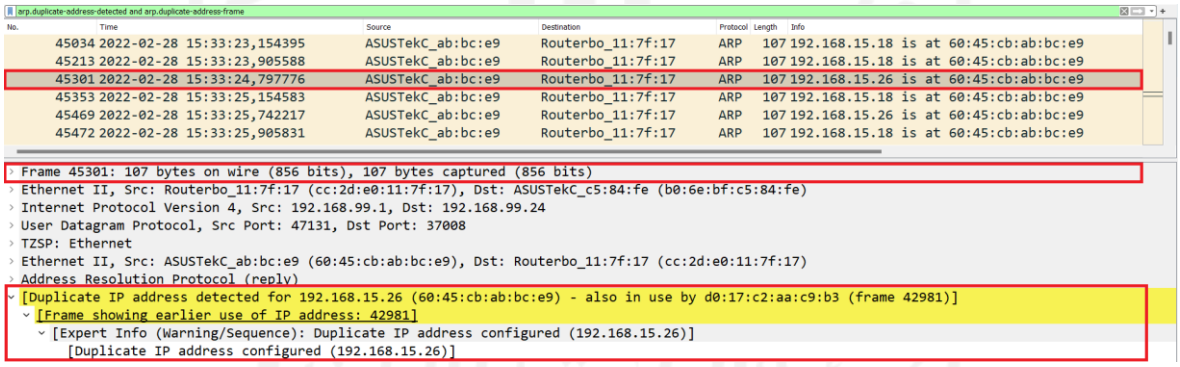


Gambar 4.9 Bukti Duplikasi *IP Address* 192.168.15.18 pada File PCAP 1

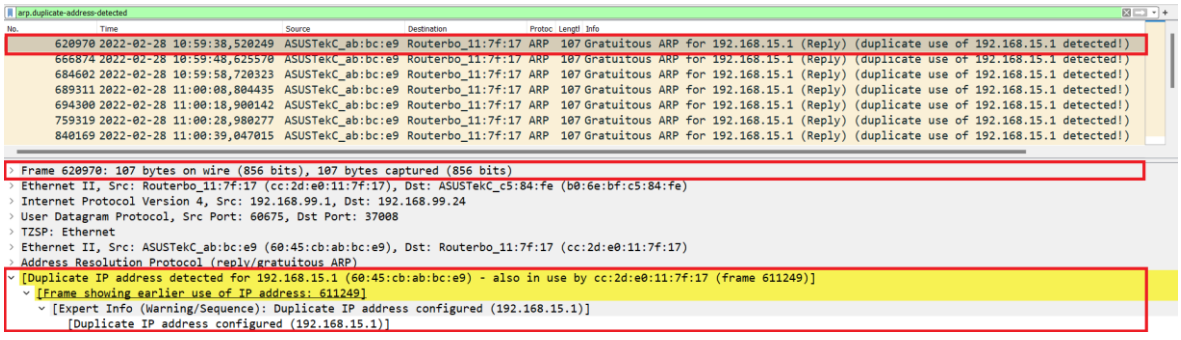
Pada gambar 4.9 menampilkan informasi bahwa telah terjadi duplikasi *IP Address* 192.168.15.18 oleh *MAC Address* 60-45-CB-AB-BC-E9 yang sebelumnya telah diterjemahkan ke *MAC Address* D0-17-C2-AA-C9-75 pada file PCAP 1. Bukti yang lain juga didapatkan yang ditunjukkan pada gambar 4.10, 4.11, 4.12, dan 4.13.



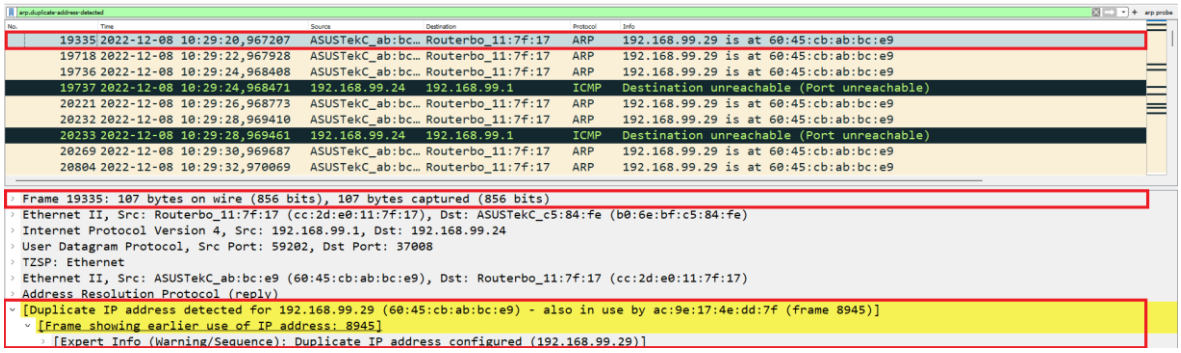
Gambar 4.10 Bukti Duplikasi *IP Address* 192.16815.18 pada File PCAP 2



Gambar 4.11 Bukti Duplikasi *IP Address* 192.16815.26 pada File PCAP 2

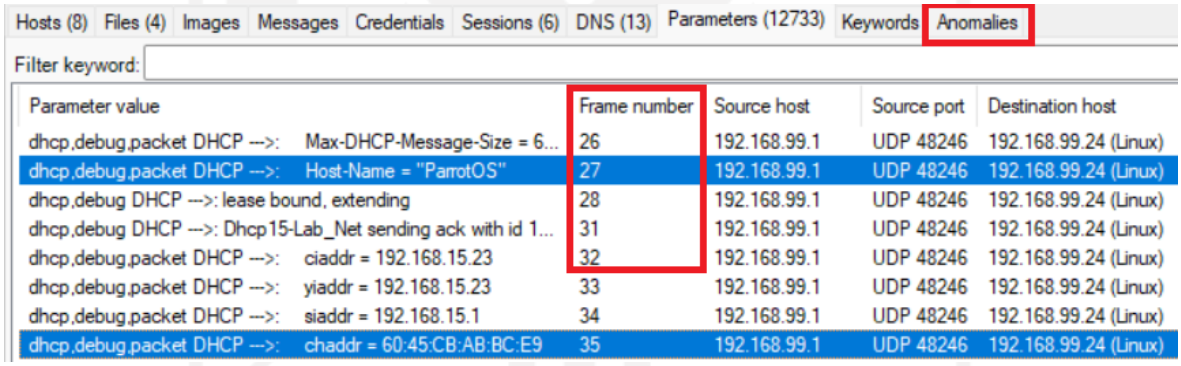


Gambar 4.12 Bukti Duplikasi *IP Address* 192.168.15.1 pada File PCAP 3



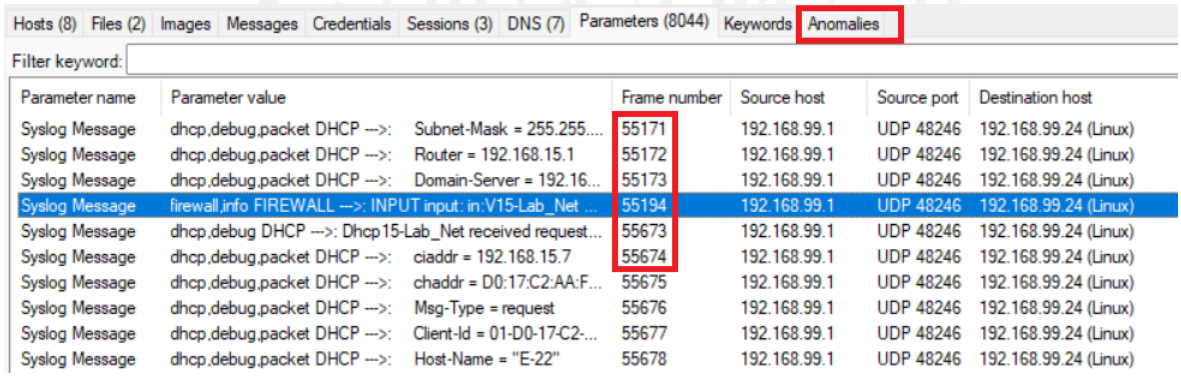
Gambar 4.13 Bukti Duplikasi *IP Address* 192.168.99.29 pada File PCAP 1

Gambar 4.9 hingga 4.13 dapat memberikan informasi kepada investigator telah terjadi duplikasi *IP Address*, informasi ini juga dapat dikorelasikan dengan tabel 4.4 tentang Waktu Pertama kali *IP Address* di terjemahkan ke *MAC Address*. Alat berikutnya yang digunakan yaitu Network Miner, network miner dapat digunakan untuk memeriksa file PCAP yang pada tahap sebelumnya telah dikumpulkan namun memiliki keterbatasan saat digunakan seperti yang ditampilkan pada gambar 4.14.



Gambar 4.14. Pemeriksaan Menggunakan Network Miner File PCAP 1

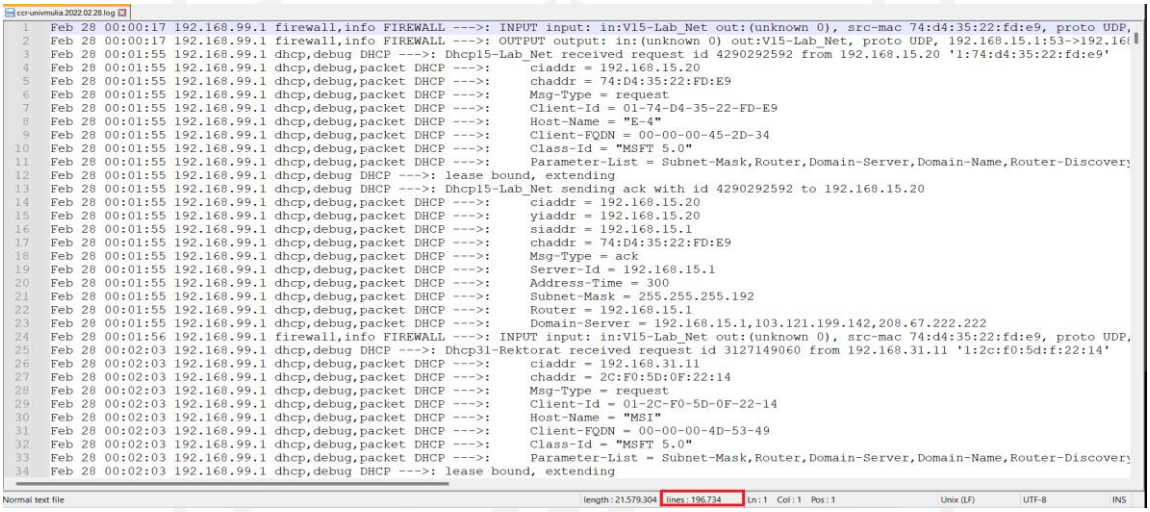
Seperti yang terlihat pada gambar 4.13, beberapa frame tidak dapat dibaca atau ditampilkan. Frame 26, 27, 28, 31, dan 32 terlihat, namun frame 29 dan 30 tidak dapat dibaca. File PCAP lain yang diperiksa menggunakan Network Miner menunjukkan hasil yang sama, bahwa frame yang dapat dibaca tidak lengkap ditampilkan pada gambar 4.15.



Gambar 4.15 Pemeriksaan Menggunakan Network Miner file PCAP 2

Frame yang tidak lengkap ditunjukkan pada gambar 4.15, terlihat pada kotak merah setelah frame 55172, 55173, kemudian ke frame 55194, 55673, 55674. Sedangkan bagian anomali pada menu Network Miner menunjukkan bahwa tidak ada tanda-tanda mencurigakan yang ditemukan saat sedang digunakan untuk pemeriksaan. Dengan demikian, dapat dikatakan bahwa Network Miner tidak lebih efektif untuk menyelidiki kejadian ini daripada alat wireshark. Namun, seperti yang diilustrasikan pada tebel 4.2 di bagian 4.2.2, Network miner sangat membantu untuk mendapatkan informasi nilai MD5.

Eksplorasi terakhir pada file *logging* yang merupakan salah satu fitur dari RouterOS yang diekspor dalam bentuk .log. File tersebut tidak dapat dianalisa menggunakan kedua alat forensik, sehingga hanya dapat dilakukan pengamatan manual seperti yang ditampilkan pada gambar 4.16.



Gambar 4.16 *Logging* RouterOS Mikrotik

File *logging* yang ditunjukkan pada gambar 4.16 merupakan hasil ekspor, file yang memiliki jumlah baris 196.734 tersebut tidak cukup membantu sebab tidak dapat dilakukan pemeriksaan atau analisis lebih mendalam menggunakan alat forensik Wireshark maupun Network miner, sehingga memerlukan waktu yang cukup lama jika dilakukan pengamatan manual. Sehingga beberapa tantangan berikutnya terkait dengan file bukti yang dapat dibaca dan diekplorasi ditampilkan dalam tabel 4.6.

Tabel 4.6 Eksplorasi file bukti dengan alat forensik

No	Generating File	Format	Alat Forensik	
			Wireshark	Network Miner
1	File Log XARP	.log	Unsupported	Unsupported
2	File Logging RouterOS	.log	Unsupported	Unsupported
3	Packet Sniffer Router	.pcap	Support	Support

4.4 Report

Tahapan ini akan menyajikan semua kegiatan yang dilakukan dari proses sebelumnya dalam bentuk laporan. Laporan memberikan informasi mengenai serangan, termasuk detail penyerang dan korban, dan dapat merekonstruksi serangan saat insiden terjadi. Menulis laporan tentang serangan spoofing arp menggunakan tahapan TAARA adalah tujuan serius dari proyek ini. Untuk memudahkan pemahaman isi laporan tahapan, maka temuan laporan paparan berdasarkan bukti penyerangan akan coba ditampilkan pada tabel 4.5.

Tabel 4.7 Laporan Bukti Serangan *ARP Spoofing*

No	File PCAP	Alokasi IP yang Terverifikasi	Timestamp	Frame Number	Attacker	Victim	Times Attack	Frame Number
1	**PCAP 1**	192.168.15.18	28/02/2022 14:37:58	7572	192.168.15.23	192.168.15.18	28/02/2022 14:43:30	127439
2	**PCAP 2**	192.168.15.26	28/02/2022 15:31:04	1486	192.168.15.23	192.168.15.26	28/02/2022 15:33:23	45034
		192.168.15.18	28/02/2022 15:31:27	11262	192.168.15.23	192.168.15.18	28/02/2022 15:33:25	45301
3	**PCAP 3**	192.168.15.18	28/02/2022 10:54:20	11657	192.168.15.23	192.168.15.18	28/02/2022 10:59:39	625068
4	**PCAP 4**	192.168.15.26	28/02/2022 13:45:20	1481	192.168.15.23	192.168.15.26	28/02/2022 13:54:41	147202
		192.168.15.18	03/03/2022 13:45:37	6356	192.168.15.23	192.168.15.18	03/03/2022 13:54:27	145984
5	**PCAP 5**	192.168.15.18	03/03/2022 14:24:47	9375	192.168.15.23	192.168.15.18	03/03/2022 14:28:12	78204
6	**PCAP 6**	192.168.15.26	03/03/2022 14:50:21	1353	192.168.15.23	192.168.15.26	03/03/2022 14:54:33	58080
		192.168.15.18	03/03/2022 14:50:45	10220	192.168.15.23	192.168.15.18	03/03/2022 14:54:33	58076
7	**PCAP 7**	192.168.15.18	02/03/2022 11:37:02	11566	192.168.15.23	192.168.15.18	02/03/2022 11:45:53	537266
8	**PCAP 8**	192.168.15.26	03/03/2022 10:50:18	2019	192.168.15.23	192.168.15.26	03/03/2022 10:54:15	55490
		192.168.15.18	03/03/2022 10:50:40	9418	192.168.15.23	192.168.15.18	03/03/2022 10:54:15	55489
9	**PCAP 9**	192.168.99.29	08/12/2022 10:28:43	695	192.168.99.25	192.168.99.29	08/12/2022 10:29:20	19335
10	**PCAP 10**	192.168.99.29	09/12/2022 16:33:44	5093	192.168.99.25	192.168.99.29	09/12/2022 16:34:45	21286

11	**PCAP 11**	192.168.99.29	08/12/2022 10:37:07	3527	192.168.99.25	192.168.99.29	08/12/2022 10:41:34	108104
12	**PCAP 12**	192.168.99.29	09/12/2022 16:48:07	3559	192.168.99.25	192.168.99.29	09/12/2022 16:48:49	16145

Tabel 4.5 ini menjelaskan bagaimana serangan dibuktikan dan direkontruksikan ulang. Serangan *ARP Spoofing* mencoba merusak tabel *ARP*, namun melalui investigasi forensik jaringan beberapa kesimpulan dapat ditarik diantaranya:

1. *IP Address* dan *MAC Address* yang telah dipetakan menjadi dasar pertama dengan melihat timestamp.
2. *Filter* yang dapat digunakan menunjukkan bahwa telah terjadi duplikasi alamat *IP Address* yang pada point pertama telah dipetakan ke tiap perangkat.

4.5 Action

Tahapan investigasi terakhir *Action,* dengan berdasarkan laporan investigator dapat memberikan pernyataan untuk menjawab serangkaian insiden yang terjadi bahwa, telah terjadi sebuah insiden berupa serangan *ARP Spoofing* dengan melibatkan tiga perangkat utama yang menjadi target dan router sebagai titik mencegat lalu lintas jaringan. Berdasarkan laporan, waktu terjadinya insiden telah didapatkan dan dipaparkan pada bagian hasil sehingga dapat mengetahui juga lokasi segmen Laboratorium Komputer dan segmen IT yang mengalami insiden serangan *ARP Spoofing*.

Metode Serangan *ARP Spoofing*, dari berbagai literatur mengindikasikan digunakan sebagai jalan untuk melancarkan serangan lanjutan seperti Man in The Middle untuk melalukan pencurian kredensial dari pengguna, atapun serangan Denial of Service yang dapat mengakibatkan lumpuhnya infrastruktur jaringan. Insiden serangan dipicu akibat kerentanan protokol *ARP* yang bersifat stateless stateless atau tidak adanya mekanisme pengamanan untuk mengautentikasi ketika *IP address* dan *MAC Address* telah dipetakan. Sehingga ini dapat dimanfaatkan oleh penyerang untuk merusak tabel *ARP* dengan beberapa alat diantaranya ARPSpoof, KickThemOut, Bettercap, Ettercap.

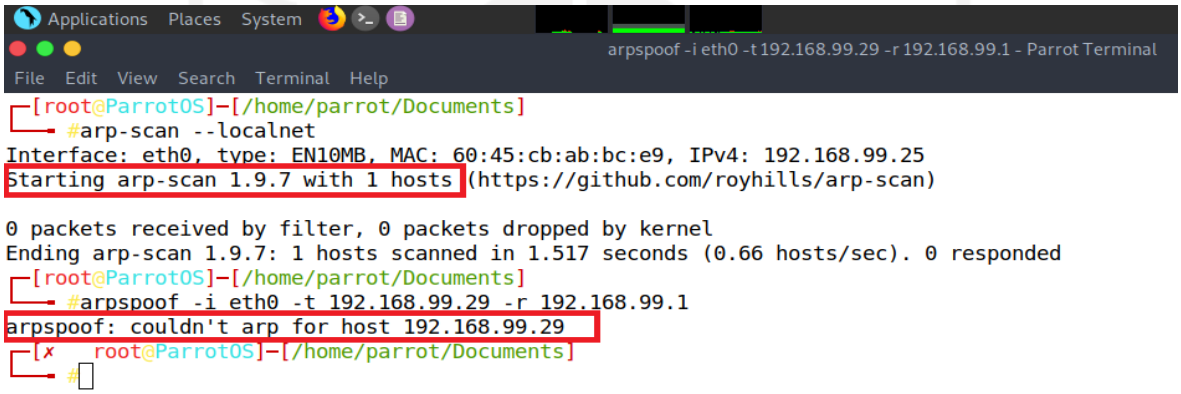
Bentuk rekomendasi berdasarkan hasil pengujian *ARP Spoofing* yang telah dilakukan, yaitu dibagi dalam dua sisi yaitu Keamanan Jaringan dan Investigasi Forensik yang dapat dijalankan berkaitan dengan hasil yang didapat.

4.5.1 Keamanan Jaringan

Metode serangan *ARP Spoofing* sepenuhnya memanfaatkan kerentanan pada protokol *ARP* yang dirancang tanpa adanya fitur keamanan sehingga penyerang dapat mengekploitasi celah pada protokol ini. Teknik kerja dari serangan *ARP Spoofing* sendiri umumnya mencari

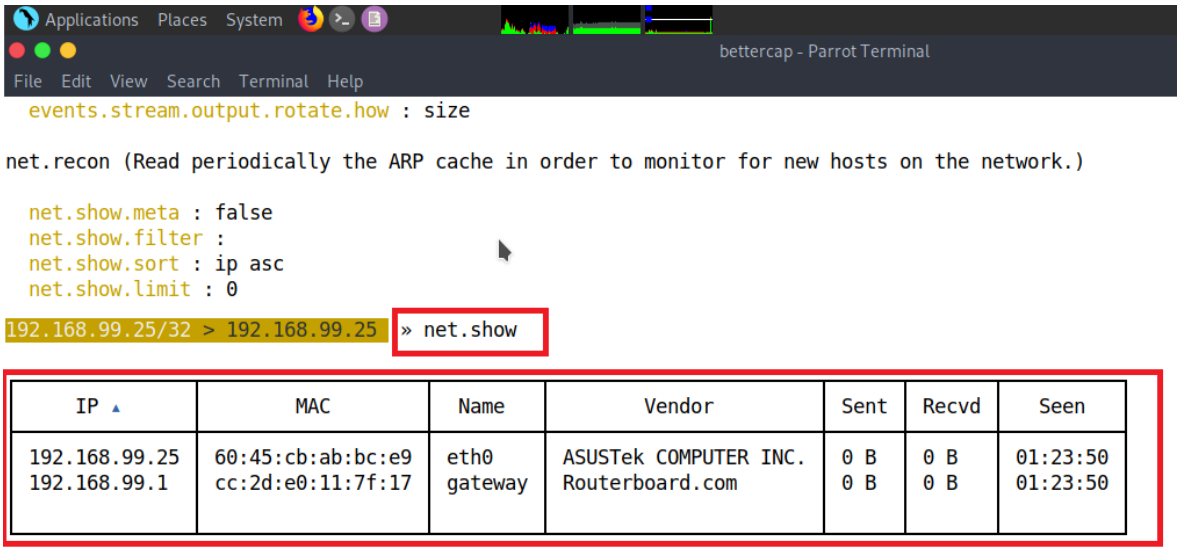
host aktif dengan mengirimkan pesan *ARP* pada jaringan. Ketika penyerang berhasil mendapatkan *host* aktif, maka penyerang dapat merusak tabel *ARP* pada perangkat korban dengan paket *arp-reply* yang dikirimkan tanpa adanya permintaan *arp-request.*

Berdasarkan cara kerja serangan *ARP Spoofing* dengan memindai perangkat *host* aktif, kemudian dilakukan pengujian pengamanan pada sisi router dengan membatasi tiap perangkat menggunakan *netmask* 32 yang artinya *host* hanya bisa mendeteksi perangkatnya sendiri di dalam jaringan lokal dengan alokasi *IP Address* yang diberikan oleh router. Pengamanan ini akan membatasi *host* mengirimkan paket arp secara *broadcast* ke dalam satu jaringan karena pembatasan *netmask* 32 tidak dapat mengetahui *host aktif* di jaringan. Metode ini mampu membatasi serangan *ARP Spoofing* seperti yang ditampilkan pada gambar 4.14 dan 4.15.



Gambar 4.17 Pengujian ARP Spoof 1 setelah pengaturan netmask

Gambar 4.17 menunjukkan pemindaian menggunakan protokol *ARP* dapat dibatasi sehingga *host* yang aktif di jaringan tidak dapat di ekploitasi. Metode serangan *ARP Spoofing* ketika di jalankan menunjukkan kegagalan dengan pesan tidak dapat menggunakan protokol *ARP* untuk *host* yang diserang dalam hal ini perangkat dengan *IP Address* 192.168.99.29.



Gambar 4.18 Pengujian ARP Spoof 2 setelah pengaturan netmask

Pada gambar 4.18 menunjukkan hasil yang sama, pengujian eksploitasi untuk memindai *host* aktif di jaringan dapat dibatasi sehingga metode pembatasan pada netmask 32 mampu digunakan untuk mengamankan jaringan dari eksploitasi dari kerentanan protokol *ARP*.

4.5.2 Investigasi Forensik

Selama proses investigasi forensik terhadap serangan *ARP Spoofing*, terdapat beberapa catatan, yaitu:

1. XARP sebagai alat untuk mendeteksi hanya sekedar memberikan *alert* sehingga tidak cukup untuk digunakan sebagai bukti adanya sebuah serangan, hal ini diperkuat dengan kelemahan yang dimiliki alat ini tidak dapat memastikan apakah *alert* yang muncul merupakan serangan nyata dari *ARP Spoofing* (Hafizh et al., 2020). XARP yang digunakan merupakan versi *free* ini menyimpan informasi terkait dengan *alert* namun, *log* XARP ini tidak dapat di akuisisi atau dianalisa lebih lanjut menggunakan alat forensik lain sehingga diperlukan metode lain untuk merekam lalu lintas jaringan.
2. *Log* pada mikrotik juga tidak dapat digunakan untuk investigasi, *log* ini hanya memberikan catatan terkait dengan beberapa informasi seperti *system*, *dhcp*, *firewall*, dan lain sebagainya, namun tidak memberikan informasi bahwa serangan telah terjadi.
3. Bahwa proses ini sepenuhnya didukung dari hasil perekaman/*capture* pada sisi router untuk menghasilkan sebuah *packet capture* dari lalu lintas jaringan. Metode ini mampu membantu investigator untuk mendapatkan bukti yang kemudian dapat

dilakukan pemeriksaan dan analisa untuk menemukan informasi bukti adanya serangan *ARP Spoofing*.

4. Berdasarkan hasil pemeriksaan dan analisa terhadap serangan *ARP Spoofing*, Investigasi forensik membutuhkan alat untuk membantu proses penggalian bukti, alat Wireshark mampu memberikan informasi baik dari hirarki pemetaan *IP Address* dengan *MAC Address* hingga membuktikan adanya sebuah duplikasi terhadap *IP Address* yang digunakan oleh penyerang.

4.6 Evaluasi Hasil

Terdapat dua evaluasi yang akan dibahas pada bagian ini yaitu yang pertama untuk menjawab apakah Metode TAARA dapat diterapkan untuk mengakomodir investigasi forensika jaringan terhadap serangan *ARP Spoofing*, sedangkan evaluasi kedua berkaitan dengan alat forensik jaringan untuk pemeriksaan pada hasil *capture* dari sisi router.

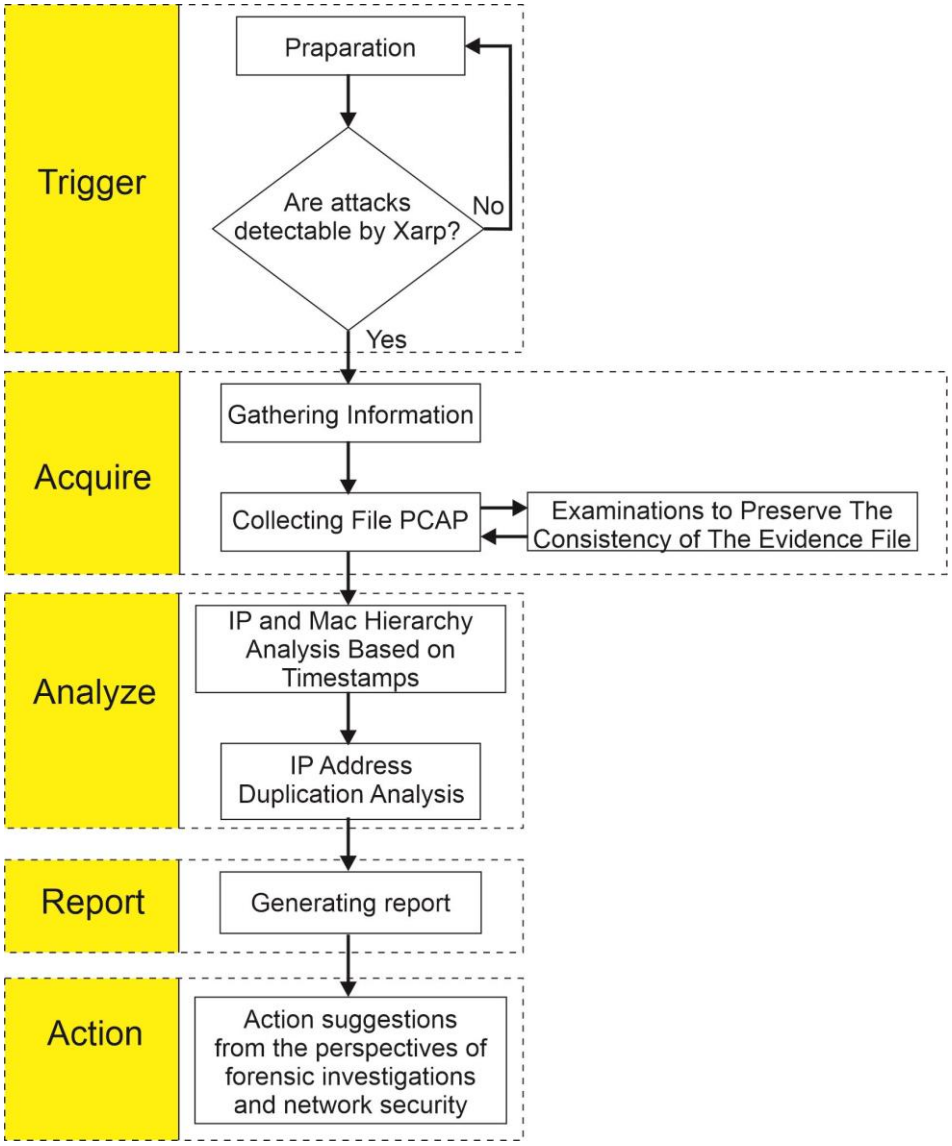
4.6.1 Metode Investigasi Forensik

Pengimplementasian metode TAARA sebagai tahapan untuk melakukan investigasi forensik jaringan terhadap serangan *ARP Spoofing* dengan melihat hasil dari investigasi yang dijalankan. Metode TAARA dapat dijalankan untuk proses investigasi, terdapat kelebihan dan kekurangan berdasarkan proses tahapan investigasi ini. Kelebihan metode TAARA yaitu

1. Model TAARA memiliki tahapan untuk tanggap insiden sehingga dapat mengarahkan investigator untuk menjalankan tahapan per tahapannya dengan cepat.
2. TAARA diturunkan dari TARA yaitu sebuah metodologi untuk *Threat Assessment & Remediation Analysis* sehingga dirancang untuk tujuan memberikan penilaian sehingga dapat mengurangi kerentanan dan memberikan sebuah pendekatan baik itu teknik maupun prosedur untuk menekan resiko akibat serangan siber.

Sedangkan, disisi lain TAARA juga memiliki kekurangan namun tidak signifikan berdasarkan hasil evaluasi dari serangan *ARP Spoofing*. Perlu dijabarkan bahwa dimana letak setiap tahapan terutama pada bagian *trigger*. Karena akan menjadi kerancuan ketika tidak ada proses yang melandasi tahapan *trigger*. Tahap berikutnya yakni *Acquire* memerlukan penjabaran yaitu didalamnya mencakup tindakan untuk mengumpulkan informasi berkaitan dengan observasi dilapangan. Selain itu tahap *collecting* file bukti terdapat di fase ini, dan ditambahkan dengan tahap pemeriksaan yang hal ini akan menjamin file yang dikumpulkan tidak akan dimanipulasi dikemudian hari. Dau tahap perlu dijelaskan untuk menghindari tindakan-tindakan yang dapat mengacaukan proses investigasi. Untuk tahap berikutnya yakni *Analyze, Report* dan *Action* selayaknya seperti pada model-model

lain. *analyze* ada dua fase yang perlu dianalisa yakni menganalisa *history* dari kepemilikan *IP Address* dengan *MAC Address* berdasarkan *timestamp* dan tahap berikutnya melakukan Analisa terkait dengan duplikasi *IP*. *Report* adalah tahapan untuk pemaparan terkait hasil dari tahap-tahap sebelumnya yang kemudian diakhiri dengan Tahapan *Action*, yaitu tindakan ini bisa berupa jawaban terkait insiden yang terjadi dan tindakan teknis. Adapun penjabaran dari metode TAARA ditampilkan pada gambar 4.16.



Gambar 4.19 Bagan Penjabaran Metode TAARA

Gambar 4.16 merupakan penjabaran metode TAARA dalam menangani kasus serangan *ARP Spoofing*, yaitu:

1. *Trigger*, tahap ini mencakup *Preparation* sebagai bentuk persiapan sistem untuk dapat digunakan dalam mendukung proses forensik jaringan. Tahap berikutnya yaitu *Detection,* tahap ini merupakan pendeteksian memanfaatkan *tools* XARP sesuai dengan penjelasan pada bagian 4.1. Alat ini memiliki kekurangan dalam mendeteksi

apakah *alert* yang muncul merupakan serangan sesungguhnya ataupun bukan merupakan sebuah serangan, namun dengan mendeteksi sebagai *alert* ini dapat digunakan sebagai *Trigger* untuk segera menjalankan proses investigasi. XARP memiliki *log*, namun pemeriksaan hanya dilakukan secara pengamatan manual. Penggunaan alat forensik seperti Wireshark dan Network miner tidak dapat digunakan untuk memeriksa ataupun menganalisa lebih lanjut *log* dari XARP ini. Sehingga perlu dilakukan investigasi mengguanakan *packet capture* dari hasil *packet sniffer* di sisi router.

2. *Acquire*, pada tahap ini sesuai dengan skenario serangan *ARP Spoofing* terdapat 3 tahapan untuk menjalankan proses ini yaitu yang pertama *gathering information* lapangan yang dapat digali kepada pihak terkait seperti administrator jaringan, pengguna lab saat insiden terjadi. Tahap berikutnya yaitu *Collecting* yaitu yang berkaitan dengan pengumpulan bukti, sehingga berdasarkan investigasi yang dijalankan tahapan ini mengumpulkan bukti *file* PCAP untuk kemudian diamankan. Tahapan yang ketiga yaitu berjalan bersamaan dengan tahapan *collecting* yaitu Examination yang bertujuan untuk mengamankan bukti untuk menjaga konsistensi atau integritas bukti melalui pemeriksaan *Hash*.
3. *Analyze*, tahapan ini seperti pada umumnya yaitu analisa untuk mendapatkan informasi terkait apa yang sebenarnya terjadi. Tahapan serangan *ARP Spoofing* berdasarkan skenario menunjukkan bahwa sebelum terjadi sebuah serangan, bukti yang didapatkan yaitu korelasi antara *IP Address* yang diterjemahkan ke *MAC Address* merupakan bukti awal berdasarkan waktu. Proses berikutnya yaitu analisa terkait dengan duplikasi *IP Address*, sehingga dapat ditemukan informasi bahwa *IP* yang di duplikasi sebelumnya telah digunakan oleh *MAC Address* yang pertama.
4. *Report*, merupakan tahapan laporan yang umumnya menyertakan apa saja yang dilakukan selama proses investigasi dijalankan. Di dalam tahap laporan juga semua bukti informasi serangan disimpulkan, yang mencakup identitas dari penyerang, identitas korban, waktu insiden terjadi.
5. *Action*, merupakan tahapan akhir didalam metode TAARA. Action adalah bentuk tanggap terkait dengan insiden yang terjadi dan dituangkan ke dalam *Report.* Tahapan ini dibahas pada bagian 4.5. Tidak ada tambahan terkait dengan tahapan ini.

Sehingga dapat disimpulkan Tahapan TAARA dapat membantu investigator untuk menangani kasus sereangan *ARP Spoofing*. Penelitian ini juga mengevaluasi perlu

penjabaran tentang metode ini khususnya di tahapan *Trigger, Acquire, Analyze.* Sedangkan untuk tahapan *Report* dan *Action* tidak ada tambahan tahapan.

4.6.2 Evaluasi alat forensik

Tahapan ini bertujuan untuk melihat kemampuan terkait dengan *supporting* sebuah alat forensik. Evaluasi ini merujuk pada skenario yang telah dilakukan dengan menerapkan proses *sniffer* pada sisi router untuk menginvestigasi jaringan lokal. Proses *sniffer* ini menghasilkan *Packet Capture* (PCAP) yang didalamnya terdapat *Tazmen Sniffer Protocol* (TZSP), yang kemudian file PCAP ini dianalisa menggunakan Wireshark dan Network Miner. Adapun detail yang didapatkan ditampilkan pada tabel berikut 4.6.

Tabel 4.8 Validasi alat forensik

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
Scanning Arpspoof V99 - Pengujian 1.pcap	Found	Found	Found	Found	Found
Scanning Bettercap V99 - Pengujian 1.pcap	Found	Found	Found	Found	Found
Scanning Ettercap V99 - Pengujian 1.pcap	Found	Found	Found	Found	Found
Scanning Kickthemout V99 - Pengujian 1.pcap	Found	Found	Found	Found	Found
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
Scanning Arpspoof V99 - Pengujian 1.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning Bettercap V99 - Pengujian 1.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning Ettercap V99 - Pengujian 1.pcap	Not Found	Not Found	Not Found	Not Found	Not Found
Scanning Kickthemout V99 - Pengujian 1.pcap	Not Found	Not Found	Not Found	Not Found	Not Found

Validasi ini didapatkan berdasarkan hasil pada bagian pembahasan pada tahapan analisa. Penggunaan alat Network miner pada skenario kasus ini tidak banyak memberikan informasi sehingga bukti serangan tidak dapat didefinisikan. Sedangkan penggunaan alat wireshark dapat dengan lengkap memberikan informasi insiden yang terjadi.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan proses hasil dan pembahasan dari proses forensika jaringan terhadap serangan *ARP Spoofing* menggunakan tahapan yang ada pada di Metode TAARA, maka dapat ditarik kesimpulan yaitu:

1. Bahwa menganalisis serangan *ARP Spoofing* dengan pendekatan pada sisi router untuk menangkap lalu lintas jaringan dengan melakukan *sniffer* dapat membantu investigator untuk mendapatkan hasil bukti dari serangan *ARP Spoofing*. Pendekatan ini melibatkan *Tazmen Sniffer Protocol* ketika *packet* dikirimkan ke PC Investigator. Analisis dapat dilakukan dengan cara mengkorelasikan penggunaan *IP Address* yang diterjemahkan ke *MAC Address* berdasarkan *timestamp* pertama kali, kemudian dikuatkan dengan menganalisis *packet* yang berisikan informasi duplikasi *IP Address*. Berdasarkan delapan *file* PCAP dari simulasi serangan *ARP Spoofing*, semuanya berhasil diindentifikasi sehingga didapatkan informasi lengkap dari mulai identitas Penyerang, identitas target yang keduanya terdapat informasi *IP Address* dan *MAC Address*, dan yang terakhir informasi terkait dengan waktu insiden tersebut terjadi.
2. Evaluasi metode TAARA terhadap proses investigasi studi kasus serangan *ARP Spoofing* menunjukkan bahwa TAARA dapat digunakan untuk membantu dalam proses investigasi forensika jaringan ini. Namun, perlu penjabaran dalam penerapan tahapan TAARA berdasarkan proses investigasi serangan *ARP Spoofing*. Tahapan yang perlu di perjelas yaitu tahapan *Trigger* yang didalamnya menyangkut terkait dengan *preparation* dan *detection.* Tahapan berikutnya yaitu *acquire* yang perlu dijabarkan sehingga didalamnya terdapat tahapan *Information Gathering*, *Collection* dan *Examination* terhadap bukti yang dikumpulkan.
3. Evaluasi terkait dengan alat bantu untuk menganalisa *file* PCAP khusus dalam implementasi skenario serangan *ARP Spoofing* ini dengan pendekatan pada sisi router yang melibatkan *Tazmen Sniffer Protocol*. Hasil menunjukkan bahwa alat Wireshark lebih *powerfull* dibandingkan dengan alat Network Miner Free untuk mendapatkan informasi serangan *ARP Spoofing*.

5.2 Saran

1. Penelitian selanjutnya diharapkan dapat lebih banyak menggunakan alat-alat pengujian serangan melihat kesimpulan pertama bahwa, implementasi alat serangan yang berbeda seperti KickThemOut ternyata dapat menghasil bukti yang berbeda, walaupun target serangannya sama.
2. Penelitian selanjutnya diharapkan dapat mengikuti perkembangan metode serangan terkait dengan *ARP Spoofing* guna untuk pengembangan tahapan atau model investigasi jaringan.

Daftar Pustaka

Agarwal, A., Gupta, M., Gupta, S., & Gupta, S. C. (2011). Systematic digital forensic investigation model. *International Journal of Computer Science and Security (IJCSS)*, *5*(1), 118–131.

Alharbi, T., Layeghy, S., & Portmann, M. (2017). Experimental evaluation of the impact of DoS attacks in SDN. *2017 27th International Telecommunication Networks and Applications Conference, ITNAC 2017*, *2017-Janua*, 1–6. https://doi.org/10.1109/ATNAC.2017.8215424

Anathi, M., & Vijayakumar, K. (2020). An intelligent approach for dynamic network traffic restriction using MAC address verification. *Computer Communications*, *154*, 559–564. https://doi.org/10.1016/j.comcom.2020.02.021

APJII. (2020). Laporan Survei Internet APJII 2019 – 2020. *Asosiasi Penyelenggara Jasa Internet Indonesia*, *2020*, 1–146.

Sharma, L., Kaur Bijral, R., Gupta, A., & sen Sharma, L. (2017). Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. *Article in International Journal of Advanced Computer Research*, *8*(5). https://doi.org/10.26483/ijarcs.v8i5.4016

Berg, A., & Selen, S. (2021). *bitkom 2021*. *August*, 19.

Bhirud, S. G., & Katkar, V. (2011). Light weight approach for IP-ARP spoofing detection and prevention. *Asian Himalayas International Conference on Internet*. https://doi.org/10.1109/AHICI.2011.6113951

Brown, J. D., & Willink, T. J. (2018). ARP Cache Poisoning and Routing Loops in ad Hoc Networks. *Mobile Networks and Applications*, *23*(5), 1306–1317. https://doi.org/10.1007/s11036-018-1039-6

Data, M. (2018). The Defense Against ARP Spoofing Attack Using Semi-Static ARP Cache Table. *3rd International Conference on Sustainable Information Engineering and Technology, SIET 2018 - Proceedings*, 206–210. https://doi.org/10.1109/SIET.2018.8693155

Divakaran, D. M., Fok, K. W., Nevat, I., & Thing, V. L. L. (2017). Evidence gathering for network security and forensics. *DFRWS 2017 EU - Proceedings of the 4th Annual DFRWS Europe*, *20*, S56–S65. https://doi.org/10.1016/j.diin.2017.02.001

Girdler, T., & Vassilakis, V. G. (2021). Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks

and Blacklisted MAC Addresses. *Computers and Electrical Engineering*, *90*(July 2020), 106990. https://doi.org/10.1016/j.compeleceng.2021.106990

Hafizh, M. N., Riadi, I., & Fadlil, A. (2020). Forensik Jaringan Terhadap Serangan ARP Spoofing menggunakan Metode Live Forensic. *Jurnal Telekomunikasi Dan Komputer*, *10*(2), 111. https://doi.org/10.22441/incomtech.v10i2.8757

Hijazi, S., & Obaidat, M. S. (2018). Address resolution protocol spoofing attacks and security approaches: A survey. *Security and Privacy*, e49. https://doi.org/10.1002/spy2.49

Ibrahim, H. Y., Ismael, P. M., Albabawat, A. A., & Al-Khalil, A. B. (2020). A Secure Mechanism to Prevent ARP Spoofing and ARP Broadcasting in SDN. *Proceedings of the 2020 International Conference on Computer Science and Software Engineering, CSASE 2020*, 13–19. https://doi.org/10.1109/CSASE48920.2020.9142092

Jayakrishnan, A. R. (2018). Empirical Survey on Advances of Network Forensics in the Emerging Networks. *International Journal of Cyber-Security and Digital Forensics*, *7*(1), 38–46. https://doi.org/10.17781/P002320

kaspersky. (2021). *Incident Response Analyst Report 2021*. https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2021/09/13085018/Incident-Response-Analyst-Report-eng-2021.pdf

Khan, S., Gani, A., Wahab, A. W. A., Shiraz, M., & Ahmad, I. (2016). Network forensics: Review, taxonomy, and open challenges. *Journal of Network and Computer Applications*, *66*, 214–235. https://doi.org/10.1016/j.jnca.2016.03.005

Kumar Singh, N., Mahajan, V., Aniket, A., Pandya, S., Panchal, R., Mudgal, U., & Bhatt, M. (2019). Identification and Prevention of Cyber Attack in Smart Grid Communication Network. *2019 International Conference on Information and Communications Technology (ICOIACT)*, 5–10. https://doi.org/10.1109/ICOIACT46704.2019.8938559

Mate, M. H., & Kapse, S. R. (2015). Network Forensic Tool - Concept and Architecture. *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, 711–713. https://doi.org/10.1109/CSNT.2015.204

Meghanathan, N., Allam, S. R., & Moore, L. A. (2009). TOOLS AND TECHNIQUES FOR NETWORK FORENSICS. In *International Journal of Network Security & Its Applications (IJNSA)* (Vol. 1, Issue 1).

Miao, Z., Liu, G., Wang, H., & Wang, Y. (2020). Dynamic Trust Model of ARP Real-Time Intrusion Detection Based on Extended Subjective Logic. *Proceedings of 2020 IEEE International Conference on Power, Intelligent Computing and Systems, ICPICS 2020*, *1705*, 615–618. https://doi.org/10.1109/ICPICS50287.2020.9201994

Muhammad Nuh Al- Azhar, MSc. (2012). *Digital Forensic: Practical Guidelines for Computer Investigation*.

Pluskal, J., Breitinger, F., & Ryšavý, O. (2020). Netfox detective: A novel open-source network forensics analysis tool. *Forensic Science International: Digital Investigation*, *35*. https://doi.org/10.1016/j.fsidi.2020.301019

Riadi, I., Fadlil, A., & Hafizh, M. N. (2020). Analisis Bukti Serangan Address Resolution Protocol Spoofing menggunakan Metode National Institute of Standard Technology. *Edumatic : Jurnal Pendidikan Informatika*, *4*(1), 21–29. https://doi.org/10.29408/edumatic.v4i1.2046

Riadi, I., Yudhana, A., & Anshori, I. (2017). Analisis Forensik Aplikasi Instant Messenger pada Smartphone Berbasis Android. *Jurnal Insand Comtech*, *2*(2), 25–32.

Riadi, I., Yudhana, A., Caesar, M., & Putra, F. (2018). Forensic Tool Comparison on Instagram Digital Evidence Based on Android with The NIST Method. *Scientific Journal of Informatics*, *5*(2), 2407–7658. http://journal.unnes.ac.id/nju/index.php/sji

Rizal, R., Riadi, I., & Prayudi, Y. (2018). Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. *International Journal of Cyber-Security and Digital Forensics (IJCSDF)*, *7*(4), 382–390.

Rohatgi, V., & Goyal, S. (2020). A detailed survey for detection and mitigation techniques against ARP spoofing. *Proceedings of the 4th International Conference on IoT in Social, Mobile, Analytics and Cloud, ISMAC 2020*, 352–356. https://doi.org/10.1109/I-SMAC49090.2020.9243604

Ruuhwan, R., Riadi, I., & Prayudi, Y. (2016). Penerapan Integrated Digital Forensic Investigation Framework v2 (IDFIF) pada Proses Investigasi Smartphone. *Jurnal Edukasi Dan Penelitian Informatika (JEPIN)*, *2*(1). https://doi.org/10.26418/jp.v2i1.14369

Saputra, D. (2019). Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method. *International Journal of Cyber-Security and Digital Forensics*, *8*(1), 66–73. https://doi.org/10.17781/p002558

Scott, B., Xu, J., Zhang, J., Brown, A., Clark, E., Yuan, X., Yu, A., & Williams, K. (2017). An interactive visualization tool for teaching ARP spoofing attack. *Proceedings -*

Frontiers in Education Conference, FIE, *2017-Octob*, 1–5. https://doi.org/10.1109/FIE.2017.8190531

Selamat, S. R., Yusof, R., & Sahib, S. (2008). Mapping Process of Digital Forensic Investigation Framework. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 8, Issue 10).

Sistem, R., Riadi, I., Fadlil, A., Aulia, M. I., Informasi, S. S., Dahlan, U. A., Elektro, S., Dahlan, U. A., Studi, P., Informatika, T., & Dahlan, U. A. (2021). *Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)*. *1*(10), 820–828.

Sistem, R., Riadi, I., Umar, R., Syahib, M. I., Informasi, S. S., Dahlan, U. A., Informatika, S. T., & Dahlan, U. A. (2021). *Akuisisi Bukti Digital Viber Messenger Android Menggunakan Metode National Institute of Standards and Technology (NIST)*. *1*(10), 45–54.

Subektiningsih, Prayudi, Y., & Riadi, I. (2018). Digital Forensics Workflow as A Mapping Model for People, Evidence, and Process in Digital Investigation. *International Journal of Cyber-Security and Digital Forensics*, *7*, 294+. https://link.gale.com/apps/doc/A570819767/AONE?u=anon~5850c42d&sid=googleScholar&xid=9f19e9d5

Supriyono, A. R., Sugiantoro, B., & Prayudi, Y. (2019). Eksplorasi Bukti Digital Pada Smart Router Menggunakan Metode Live Forensics. *Infotekmesin*, *10*(2), 1–8. https://doi.org/10.35970/infotekmesin.v10i2.48

Tully, G., Cohen, N., Compton, D., Davies, G., Isbell, R., & Watson, T. (2020). Quality standards for digital forensics: Learning from experience in England & Wales. *Forensic Science International: Digital Investigation*, *32*. https://doi.org/10.1016/j.fsidi.2020.200905

Umar, R., Riadi, I., & Kusuma, R. S. (2021a). Analysis of Conti Ransomware Attack on Computer Network with Live Forensic Method. *IJID (International Journal on Informatics for Development)*, *10*(1), 53–61. https://doi.org/10.14421/ijid.2021.2423

Umar, R., Riadi, I., & Kusuma, R. S. (2021b). *Network Forensics Against Ryuk Ransomware Using Trigger , Acquire , Analysis , Report , and Action (TARA) Methods*. *4*, 197–204.

Yudhana, A., Riadi, I., & Putra, B. (2018). *DDoS Classification Using Neural Network and Naïve Bayes Methods For Network Forensics Abstrak Kunci : DDoS , IDS , JST , Naïve Bayes*. *9*(11), 177–183.

Yuwono, D. T., Fadlil, A., & Sunardi, S. (2019). Performance Comparison of Forensic Software for Carving Files using NIST Method. *Jurnal Teknologi Dan Sistem Komputer*, *7*(3), 89–92. https://doi.org/10.14710/jtsiskom.7.3.2019.89-92

Zhao, Y., Guo, R., & Lv, P. (2020). ARP Spoofing Analysis and Prevention. *Proceedings - 2020 5th International Conference on Smart Grid and Electrical Automation, ICSGEA 2020*, 572–575. https://doi.org/10.1109/ICSGEA51094.2020.00130