Jurnal Politeknik Caltex Riau
Terbit Online pada laman https://jurnal.pcr.ac.id/index.php/jkt/
| e- ISSN : 2460-5255 (Online) | p- ISSN : 2443-4159 (Print) |

# ANALISIS *ADDRESS RESOLUTION PROTOCOL POISONING ATTACK* PADA ROUTER WLAN MENGGUNAKAN METODE *LIVE FORENSICS*

**Syaifuddin[1], Denar Regata Akbi[2] dan Ahmad Gholib Tammami[3]**

[1]Universitas Muhammadiyah Malang, Teknik Informatika, email: saifuddin@umm.ac.id
[2]Universitas Muhammadiyah Malang, Teknik Informatika, email: dnarregata@umm.ac.id
[3]Universitas Muhammadiyah Malang, Teknik Informatika, email: golibtamami@gmail.com

**Abstrak**

*Perkembangan teknologi pada zaman sekarang membuat hampir setiap orang menjadikan Wireless Local Area Network sebagai kebutuhan. Beberapa badan usaha bahkan instansi sudah lebih memilih menggunakan teknologi wireless dikarenakan pemakaiannya yang sangat mudah, akan tetapi masih sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless. Address Resolution Protocol Poisoning Attack merupakan salah satu jenis serangan pada jaringan wireless dengan akses terbuka dan juga sangat mudah dilakukan dengan menggunakan berbagai aplikasi, salah satu contoh aplikasi yang dapat digunakan adalah Netcut. Serangan tersebut mampu mengendus data frame dan melakukan modifikasi traffic atau bahkan menghentikan traffic internet. Pada kasus ini serangan dapat dianalisis menggunakan metode live forensics karena data yang diteliti berupa volatile bersifat sementara dan hanya dapat ditemukan pada penyimpanan Random Access Memory atau pada traffic jaringan. Volatile data hanya akan ada pada saat sistem masih menyala, sehingga perilaku dari attacker serta informasi bukti digital yang dapat diketahui berupa IP Address dan MAC Address source destination yang dianalisis menggunakan aplikasi Wireshark. Terdapat pendeteksian pada penelitian ini dengan menggunakan aplikasi Instruction Detection System Snort yang dapat mengirimkan alert ketika sistem diserang.*

***Kata kunci:*** *ARP Poisoning, Live Forensics, Volatile Data*

**Abstract**

*Nowdays, the development of technology makes Wireless Local Area Network a necessity for almost everyone. Various kinds of jobs can also be connected through a technology wireless, because it's easy to use, but most of them pay less attention to data communication security on wireless networks. One type of attack on Wireless Local Area Network with open access is the address resolution protocol poisoning and its very easy to use with some applications. Netcut is one example of an application can to be used. Attackers can find the data frames and modify or even stop the internet traffic, because the data studied is in the form of volatile data that can be found only in RAM storage or on network traffic, so the attack in this case can be analyzed by using the live forensics method. Volatile data will only exist when the system is still on, so that digital evidence information and the behavior of the attacker who carried out the attack can be*

Dokumen diterima pada 19 Maret, 2021
Dipublikasikan pada 31 Mei, 2021

*identified form of an IP Address and MAC Address source destination an analyzed using the Wireshark application, There is a detection in this case by using the Instruction Detection System Snort an application which is can send alerts when the system is attacked.*

***Keywords:*** *ARP Poisoning, Live Forensics, Volatile Data*

## 1. Pendahuluan

*Wireless Local Area Network (WLAN)* merupakan jaringan *Local Area Network (LAN)* yang memberikan koneksi jaringan ke pengguna dengan menggunakan media *radio frequency (RF)* dan *infrared* (IR) [1]. Beberapa badan usaha bahkan instansi sudah lebih memilih menggunakan teknologi *WLAN* dikarenakan pemakaiannya yang sangat mudah, akan tetapi hanya sedikit yang memperhatikan keamanan komunikasi data pada jaringan *wireless* tersebut [2]. *Man In The Middle Attack (MITM)* merupakan salah satu jenis serangan pada jaringan *Local Area Network (LAN)* atau *WLAN* dengan akses terbuka. Dari cara tersebut penyerang mampu mengendus *data frame* dan melakukan modifikasi *traffic* atau bahkan menghentikan *traffic (ARP poisoning)* [3] [4]. Konsep dasar dari *ARP poisoning* atau *spoofing* adalah dengan memanfaakan *ARP cache* untuk memberikan identitas/alamat *server* atau *gateaway* palsu kepada pengguna jaringan, dengan begitu *attacker* dapat memodifikasi *traffic* jaringan [5]. Jika dibiarkan, serangan tersebut dapat mengganggu lalu lintas jaringan sehingga dapat memutuskan koneksi internet pada perangkat yang terhubung ke jaringan. Oleh karena itu dibutuhkan penelitian yang dapat mendeteksi perilaku dari serangan *ARP poisoning* [6].

*Digital forensics* muncul sebagai suatu ilmu pengetahuan dan keahlian yang berkembang secara terus menerus dalam mengidentifikasi, mengoleksi, menganalisis serta menguji bukti-bukti digital [7]. Pada umumnya terdapat dua jenis analisis *digital forensics* yaitu *dead forensics* dan *live forensics* [8]. *Dead forensics* adalah teknik analisis yang membutuhkan data yang tersimpan pada penyimpan eksternal atau *hardisk*. Sedangkan *live forensics* merupakan teknik analisis yang melibatkan data-data yang berjalan pada sistem, seperti yang terdapat pada *RAM, Router, network process, memory, swap file, running system process* sehingga dapat memberikan gambaran dari proses pada sistem yang berjalan [9] [10]. *Live analysis* merupakan cara terbaik untuk menyelidiki sistem target [11] sehingga dalam penelitian ini dilakukan analisis perilaku dari serangan *ARP poisoning* menggunakan metode *live forensics* dikarenakan data-data yang akan dianalisis berada pada jaringan *wireless*. *Router* merupakan perangkat yang posisinya sangat sensitif dan kritis pada sebuah jaringan karena dapat mencegat, memodifikasi lalu lintas, serta dapat bertindak sebagai *sniffer* dalam memonitor jaringan, sehingga hal tersebut membuat *Router* menjadi sasaran umum untuk dapat diserang [12]. Oleh sebab itu fokus penelitian analisis *live forensics* ini terdapat pada *Router WLAN* karena informasi yang terkandung pada *Router* berupa *volatile data* yang berhubungan dengan analisis *live forensics* [12] [13]. Pengambilan informasi tersebut dilakukan dengan cara memonitoring *traffic* jaringan pada *Router* dengan menggunakan aplikasi *Wireshark* yang memang dipergunakan untuk pemeriksaan keamanan jaringan serta mengatasi permasalahan jaringan [7]. Sedangkan untuk pendeteksian serangan *ARP poisoning* dan pemantauan lalu lintas jaringan *wireless* menggunakan aplikasi *Instrusion Detection System (IDS). IDS* akan memberitahukan jika terjadi aktifitas yang mencurigakan atau *illegal* [14].

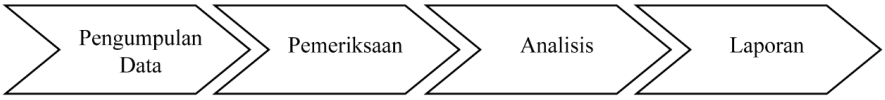
Pada penelitian yang dilakukan oleh Dedy Saputra (dalam artikel yang berjudul "*Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method*") yang meneliti tentang analisis jaringan *forensics* terhadap serangan MITM menggunakan metode *live forensics* dengan melakukan simulasi serangan menggunakan aplikasi Ettercap yang bertujuan untuk menyadap aktivitas dari pengguna jaringan (*sniffing*) sehingga dapat mengetahui informasi seperti *username* dan *password* dari aktivitas korban. Hasil analisis *live forensics* dapat terlihat pada aplikasi Wireshark, *attacker* terdeteksi mendapatkan *username* dan *password* dan mengakses halaman *website* menggunakan Iceweasel pada Kali Linux serta terdapat pemberitahuan

peringatan oleh IDS Snort bahwa telah terjadinya serangan MITM yang ditampilkan pada *command promt* [15]. Pada penelitian sebelumnya yang dilakukan oleh Nita Hildayanti (dalam artikel yang berjudul "*Forensics Analysis of Router On Computer Networks Using Live Forensics Method*") [7] masih sebatas meneliti perilaku korban yang terkena serangan *ARP Poisoning* menggunakan aplikasi Netcut.

Pada penjelasan penelitian rujukan tersebut mengindikasikan bahwa serangan MITM salah satu contohnya adalah ARP Poisoning masih menjadi ancaman bagi para pengguna koneksi *wireless* sehingga pada penelitian ini penulis meneliti dan menganalisis serangan ARP Poisoning dengan metode *live forensics* menggunakan aplikasi Wireshark yang bertujuan untuk menemukan bukti digital dari serangan, yang meliputi beberapa parameter penelitian yaitu IP Address dan MAC Address *source destination*, *protocol* jaringan yang digunakan, serta pendeteksian serangan menggunakan aplikasi IDS Snort dengan memonitoring jaringan secara *realtime*. Penelitian *live forensics* ini dilakukan pada dua kondisi, yaitu saat proses observasi jaringan (sebelum serangan) dan pada saat proses penyerangan, hal ini bertujuan untuk memudahkan dalam mengetahui perbedaan karakteristik data penelitian. Hasil dari penelitian ini dapat dijadikan bukti digital dalam melakukan laporan tindakan pidana serta dapat juga dijadikan tolak ukur dalam melakukan pengamanan jaringan.

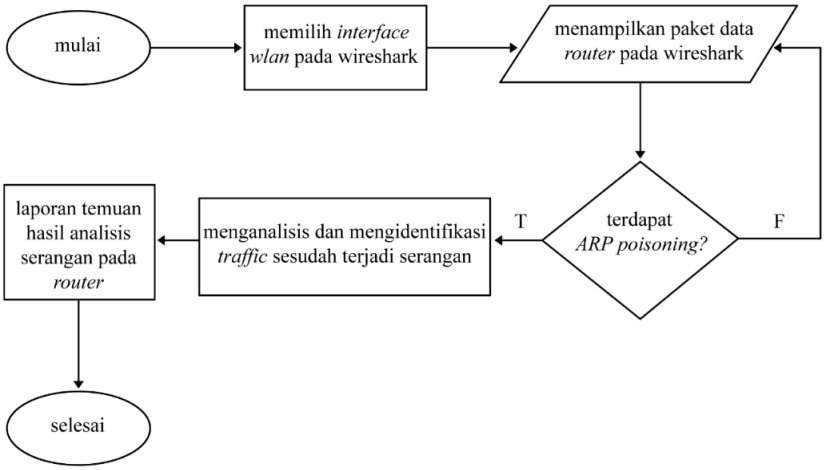
## 2. Metode Penelitian

### 2.1 Live Forensics




**Gambar 1. Tahapan Pengujian Forensics** [7]

Pada pengujian *forensics* terdapat beberapa tahapan yang dapat dilihat pada gambar 1 di atas. Tahapan pertama dalam melakukan *forensics* jaringan adalah pengumpulan data yang didapatkan pada saat proses observasi jaringan yang dilakukan disaat sebelum pengujian serangan dan pengumpulan data disaat sesudah pengujian serangan, hal ini bertujuan untuk dapat memudahkan klasifikasi data *normal* dengan data yang tidak *normal*. Selanjutnya dilakukan pemeriksaan terhadap data yang telah dikumpulkan, data yang dimaksud meliputi beberapa parameter penelitian yaitu IP Address dan MAC Address *source destination* dan *protocol* data yang digunakan. Hasil analisis dari aktivitas data yang mencurigakan dapat dijadikan laporan dalam penelitian. Sedangkan untuk tahapan proses live forensics terbagi dari beberapa bagian proses, yaitu sebagai berikut :

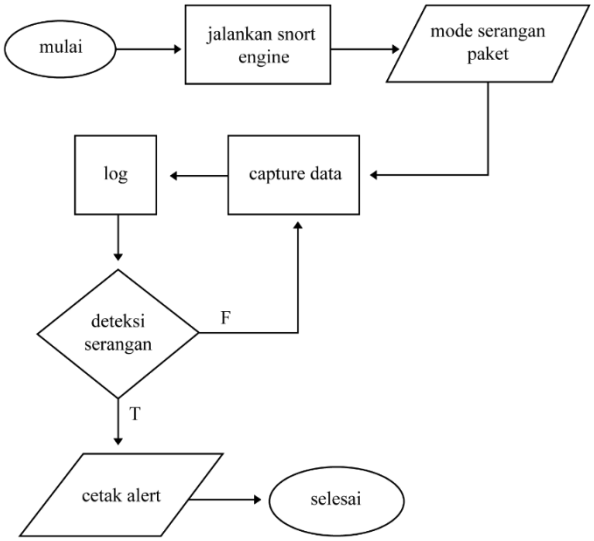



**Gambar 2. Flowchart Proses *Live Forensics***

Tahap awal pada metode penelitian berdasarkan Gambar 2 di atas dimulai dengan memilih *interface* perangkat jaringan yang digunakan pada aplikasi *Wireshark*. Pada penelitian ini menggunakan *interface WLAN* untuk melakukan implementasi analisis serangan *ARP Poisoning*. Setelah itu *Wireshark* dapat menampilkan *traffic* jaringan dari aktivitas pengguna yang melalui *Router WLAN* sehingga data tersebut yang akan dianalisis untuk menemukan bukti digital pada kasus penelitian ini. Tahap selanjutnya melakukan proses serangan *ARP poisoning* dengan memutuskan koneksi salah satu pengguna pada jaringan *WLAN* sehingga korban tidak dapat lagi mengakses internet. Selanjutnya informasi dari *traffic* dapat dianalisis untuk mengidentifikasi perilaku serangan secara *live forensics* dari hasil percobaan *ARP poisoning attack*. Setelah mengetahui informasi dari serangan maka dapat dilakukan pembuatan laporan dengan melampirkan *variable* atau komponen dari serangan yang melewati *Router*.

## 2.2 Pendeteksian

Pada tahap ini terdapat beberapa rancangan untuk mendeteksi serangan *ARP poisoning*, yaitu menggunakan *Intrusion Detection System (IDS)* berbentuk *Snort*. Pendeteksian ini berguna untuk memperkuat bukti digital dari hasil analisis *live forensics* pada aplikasi *Wireshark*. Berikut merupakan skema pendeteksian pada *Snort*




**Gambar 3. *Flowchart* Sistem Deteksi Serangan** [17]

Tahap pertama untuk mendeteksi serangan dapat dilihat pada gambar 3 yaitu menjalankan aplikasi *IDS Snort* yang sudah terpasang pada *system* perangkat. *Snort* diketahui dapat melakukan *capture data* pada jaringan dan mengirimkan *alert* yang berasal dari *rules* yang diterapkan. Pengiriman *alert ARP Spoofing* ditentukan pada kode *Snort rules* yang dapat dikonfigurasi dan diaktifkan pada *file* konfigurasi yang berada di direktori */etc/snort/snort.conf* ,berikut contoh konfigurasi pengaktifan *rules* pada *file* konfigurasi *Snort.*

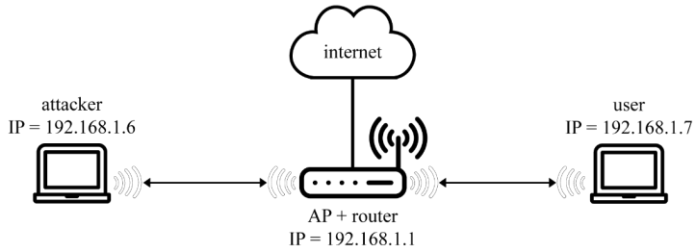
```
"preprocessor arpspoof: -unicast"
"preprocessor arpspoof_detect_host: ip_address mac_address"
```

Sedangkan lokasi *rules* untuk *alert* dalam mengerjakan perintah dari konfigurasi yang telah diaktifkan dapat ditemukan pada *file rules Snort* yang berada di direktori */etc/snort/preproc_rules/preprocessor.rules* ,dengan contoh *rules* sebagai berikut.

```
"alert ( msg: "ARPSPOOF_ARP_CACHE_OVERWRITE_ATTACK"; sid: 4; gid:
112; rev: 1; metadata: rule-type preproc ; classtype:bad-unknown; )"
```

## 3. Perancangan

### 3.1 Skenario Pengujian Arsitektur Jaringan




**Gambar 4. Pengujian Skenario Analisis *Forensics***

Pada tahap ini dilakukan pembangunan sebuah jaringan WLAN yang digunakan untuk proses penelitian. Perangkat dari arsitektur jaringan seperti yang dapat dilihat pada contoh gambar 4 merupakan skenario pengujian *forensics* pada tahap pertama yang berjalan *normal* tanpa adanya serangan dengan adanya dua perangkat yang meliputi *attacker* dan *user* pada jaringan, dengan satu Router WLAN yang digunakan untuk menghubungkan kedua perangkat tersebut. Dalam pengujian tersebut *attacker* melakukan ARP Poisoning sehingga korban tidak dapat mengakses internet melalui Router. Pengujian analisis *forensics* dilakukan pada perangkat korban dengan menggunakan aplikasi Wireshark dengan memfokuskan beberapa parameter penelitian yaitu, yaitu IP Address dan MAC Address *source destination*, *protocol* yang digunakan, serta pendetektian serangan menggunakan aplikasi Snort sehingga diharapkan hasil dari analisis tersebut dapat menemukan bukti digital dari serangan ARP Poisoning.

### 3.2 Pengujian Deteksi Serangan

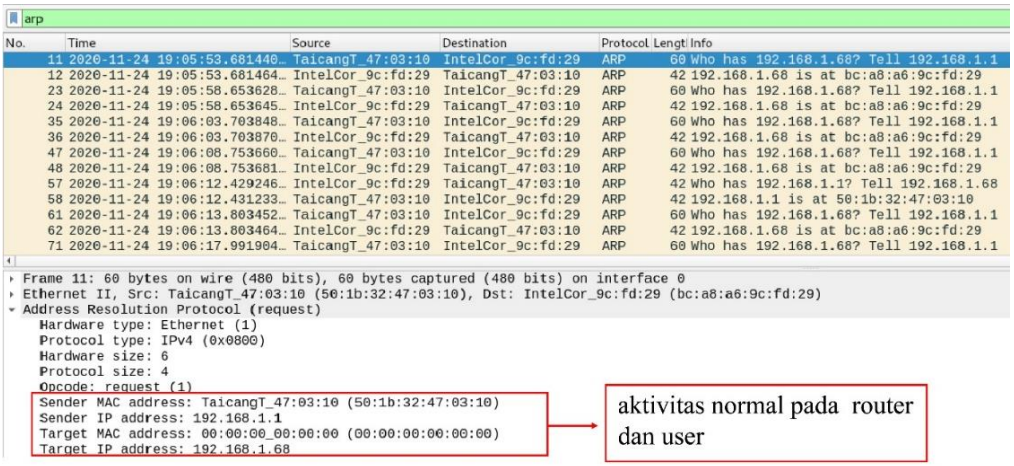
Pendeteksian dilakukan menggunakan aplikasi *IDS Snort* dengan tahapan pertama yaitu melakukan konfigurasi *rules* Snort yang digunakan sebagai perintah pendeteksian serangan dan selanjutnya menjalankan aplikasi IDS Snort pada perangkat *user* (korban) sehingga Snort dapat memonitoring dan membaca setiap paket yang melewati jaringan [14]. Semua data paket hasil monitoring akan tersimpan pada *log* Snort dan jika terjadi sebuah serangan yang sesuai dari *rules* yang telah di konfigurasi sebelumnya, maka Snort dapat mendeteksi dan mengirimkan *alert* sesuai *rules* yang telah tetapkan.

## 4. Hasil dan Pembahasan

### 4.1 Proses Observasi pada jaringan *Router WLAN*

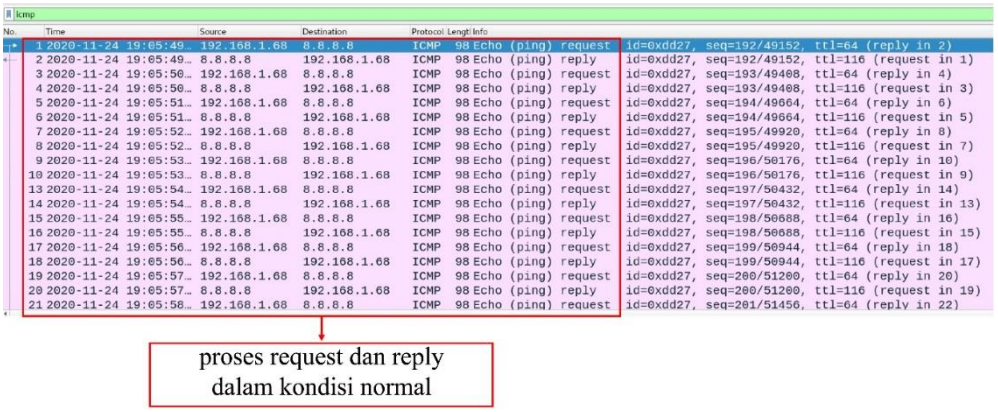
Sebelum melakukan pengujian penelitian *live forensics*, proses pengujian ini diawali dengan melakukan observasi terhadap *Router WLAN* yang dijadikan objek penelitian. Proses monitoring pada observasi ini dilakukan sebelum pengujian serangan. Pada penelitian ini memfokuskan penarikan beberapa *variable data* dari hasil proses monitoring jaringan yang dapat dijadikan bukti digital pada Router dengan berdasarkan penelitian yang telah dilakukan oleh (Tobias Fiebig, 2013) [16], di antaranya yaitu *IP Address* (*source, destination*), *MAC Address* (*target, sender*), dan terdapat *variable* tambahan berupa *protocol* yang digunakan, serta informasi deteksi *(alert)*

dan *log* pada aplikasi Snort. Berikut merupakan hasil monitoring pada saat sebelum dilakukannya pengujian serangan atau pada kondisi normal.




**Gambar 5. Kondisi Aktivitas Jaringan Pada *Protocol ARP* Saat Sebelum Serangan**

Pada gambar 5 di atas dapat dilihat bahwa didapatkan informasi berupa *IP Address* dengan alamat 192.168.1.1 dan *MAC Address* dengan alamat 50:1b:32:47:03:10 mengirimkan pesan *ARP request* yang berisi permintaan untuk mendapatkan alamat *IP Address* dari setiap alamat *MAC Address* pengguna yang terhubung pada jaringan *Router WLAN*, dalam kasus ini alamat *IP* yang ditujukan yaitu 192.168.1.68. Rincian informasi *broadcast* dapat dilihat pada *variable ARP Request* yang menampilkan Target *MAC Address* : 00:00:00:00:00:00 yang berarti sebuah pesan *broadcast* yang ditujukan kepada setiap pengguna. Berdasarkan informasi tersebut dapat disimpulkan bahwa *IP Address* 192.168.1.1 yang memiliki *MAC Address* 50:1b:32:47:03:10 merupakan sebuah alamat yang dimiliki oleh *IP Router WLAN*. Pada observasi ini juga dilakukan pemeriksaan terhadap lalu lintas jaringan dalam mengakses internet melalui *Router*. Dalam tahap ini dilakukan pengujian *ping* ke alamat layanan *DNS Google* yaitu 8.8.8.8 berikut merupakan hasil pengujiannya.

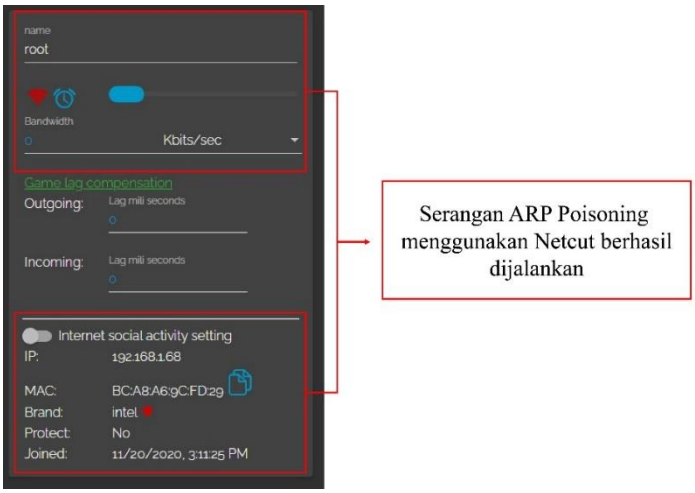



**Gambar 6. *Respond Client* dan *Server* Sebelum Serangan**

Tampilan dari gambar 6 di atas menunjukkan bahwa proses melakukan ping dari alamat perangkat yang ada di jaringan menuju *DNS Google* berhasil dan menandakan jika perangkat masih dapat terhubung ke internet. Hal ini dapat dilihat pada paket *request* pada *variable source* yang beralamat 192.168.1.68 dan melakukan *request* ke *DNS* yang beralamat 8.8.8.8 dan *request* tersebut berhasil mendapatkan paket *reply* dari alamat tujuan, kondisi tersebut menandakan bahwa lalu lintas pada jaringan masih berjalan dengan normal.

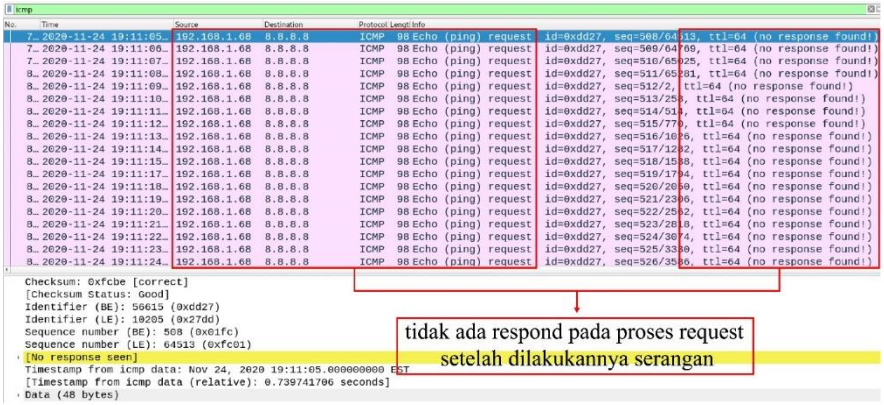
## 4.2 Pengujian Serangan Menggunakan Netcut

Pada tahapan ini aplikasi *Netcut* dijalankan pada perangkat *Windows* yang digunakan oleh *attacker* dan sebelumnya sudah terhubung pada jaringan. *Target* dari serangan ini tertuju pada perangkat peneliti dengan alamat *IP Address* 192.168.1.68 seperti tampilan pada gambar berikut ini.




**Gambar 7. Serangan *ARP Posioning* Menggunakan Aplikasi *Netcut***

Serangan yang ditujukan pada pada korban dengan berdasarkan gambar 7 di atas bahwa serangan pada *target* berhasil dilakukan. Pada gambar tersebut dapat diketahui jika serangan mengarah kepada *IP* 192.168.1.68 dengan *MAC Address* bc:a8:a6:9c:fd:29. Penyerangan tersebut mengakibatkan terputusnya koneksi internet pada perangkat korban sehingga korban tidak dapat lagi terhubung ke internet, hal tersebut dapat dilihat pada gambar berikut.




**Gambar 8. Kondisi *Request* dan *Reply* Setelah Serangan**

Pada gambar 8 di atas dapat diketahui bahwa tidak adanya *respond* dari alamat yang diakses, dalam kasus ini yaitu alamat *DNS google* dan kondisi ini menandakan sedang terjadinya gangguan koneksi sehingga paket tidak dapat terkirim, hal ini merupakan salah satu penyebab dari serangan *ARP poisoning* dengan menggunakan aplikasi *Netcut* tersebut.

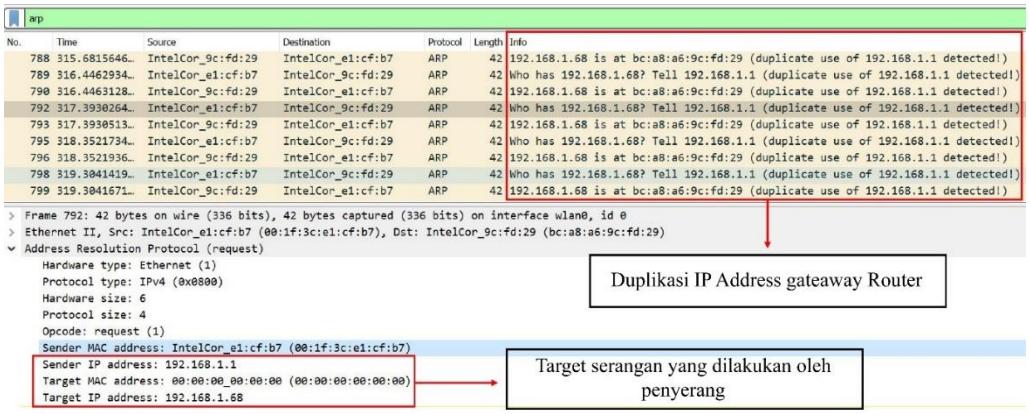
## 4.3 Analisis *Live Forensics*

Pada tahapan analisis dilakukan menggunakan metode *live forensics* dengan memonitoring *traffic* jaringan disaat serangan sedang berlansung sebagai tahap untuk pengumpulan data sehingga dapat dilakukan penarikan data berupa *IP Address source* dan *destination*, *MAC Address source*

dan *destination*, serta *protocol* yang digunakan pada paket. Komponen penarikan data tersebut merupakan fokus utama pada proses pemeriksaan forensik ini.

**a. *IP Address***

Berikut merupakan tampilan dari hasil monitoring pada aplikasi *Wireshark* disaat terjadinya serangan.

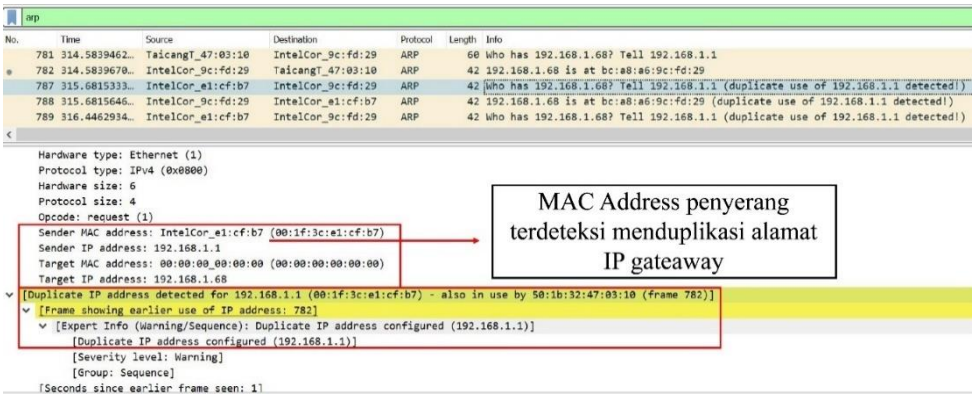



**Gambar 9. Pendeteksian Duplikasi *IP Gateaway***

Pada gambar 9 di atas dapat diketahui bahwa aplikasi *Wireshark* telah mendeteksi adanya proses *duplicate IP gateaway* sehingga penyerang dalam hal ini mampu mengkontrol koneksi internet pengguna yang ada di dalam jaringan. Pada kasus ini aktivitas penyerang dari tampilan di atas terpantau melakukan *broadcast* untuk mencoba mencari alamat *MAC Address* pada alamat *IP target* yang dituju, dalam penelitian ini *target* serangan berada pada alamat 192.168.1.68 sehingga penyerang mampu mengelola koneksi internet korban, hal ini didasarkan pada alamat *gateaway* yang dapat dimanipulasi sehingga setiap paket yang dikirim oleh korban tidak akan sampai pada alamat yang sebenarnya.

**b. *MAC Address***

Alamat *MAC Address* merupakan sebuah identitas unik yang dimiliki oleh setiap perangkat yang dapat terhubung pada suatu jaringan. Proses investigasi dapat memanfaatkan alamat unik ini untuk mengidentifikasi sebuah serangan *ARP Poisoning*, contohnya pada gambar berikut ini.




**Gambar 10. Pendeteksian MAC Address Attacker dari *Duplicate IP Gateaway***

Gambar 10 di atas menunjukkan dua alamat *MAC Address* yang menggunakan alamat *IP gateaway* sehingga hal ini bisa dikatakan merupakan sebuah aktifitas yang mencurigakan. Jika dilihat pada penelitian disaat aktivitas masih berjalan normal, alamat *IP Address gateaway* memiliki *MAC Address* yang berlamat pada 50:1b:32:47:03:10 dan dapat dikatakan jika alamat

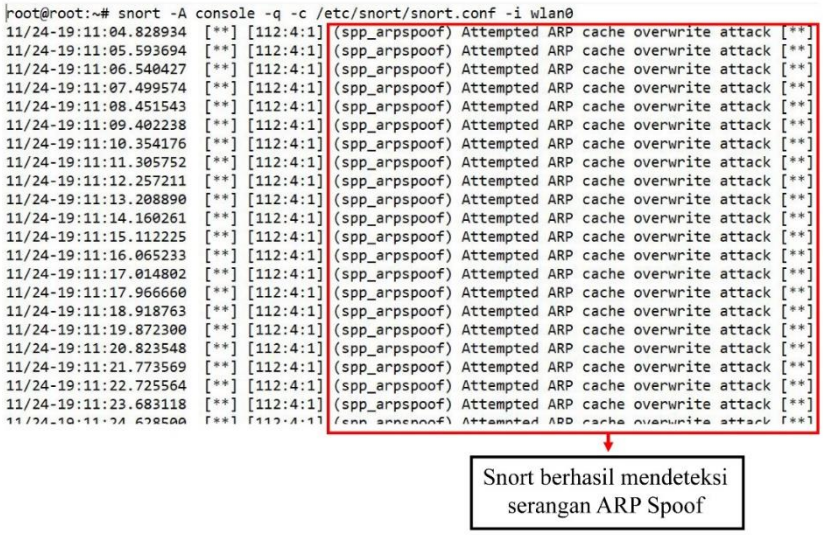
tersebut merupakan alamat asli dari *gateaway Router*, sehingga jika dilihat pada gambar 11 di atas dapat diketahui *MAC Address* yang beralamat 00:1f:3c:e1:cf:b7 dipastikan merupakan alamat perangkat dari *attacker*.

**c. *Protocol***

Dalam proses observasi, aktivitas *protocol ARP* berjalan dengan normal dalam membantu proses komunikasi *Router* dengan perangkat-perangkat lain, hingga saat proses investigasi serangan, *ARP* mendeteksi aktivitas *duplicate IP gateaway* serta *MAC Address* yang digunakan oleh *attacker*. Selain itu penelitian ini juga memanfaatkan *protocol ICMP (Internet Control Message Protocol)* pada sisi korban sebagai ukuran dalam menguji pengiriman paket disaat proses observasi maupun dalam tahapan pengujian penyerangan. Hasil *reply* atau *respond* dari *request* packet tersebut yang dijadikan tolak ukur dalam keberhasilan pengujian serangan.

**d. *Snort***

Informasi pendeteksian serangan pada aplikasi *Snort* dapat dijadikan bukti penguat dalam penelitian ini**.** Berikut merupakan tampilan informasi pendeteksian serangan *ARP Poisoning*.




**Gambar 11. Deteksi serangan *ARP poisoning* pada *Snort***

Pada gambar 11 di atas diketahui bahwa *Snort* mampu mendeteksi serangan *ARP Poisoning* disaat pengujian serangan dijalankan. Pendeteksian ini berupa *alert* pada perangkat korban yang berisi informasi jenis serangan yang berlansung, tetapi *Snort* tidak memberikan informasi detail dari *attacker* sehingga diperlukan investigasi *live forensics* menggunakan aplikasi *Wireshark*.

## 4.4 Hasil Analisis Pengujian Serangan *ARP poisoning*

Berdasarkan hasil pengujian serangan *ARP poisoning* yang sudah dilakukan menggunakan aplikasi *Netcut*, maka dapat diketahui informasi serangan melalui investigasi analisis dengan menggunakan metode *live forensics* yang telah peneliti lakukan. Hasil analisis serangan *ARP Poisoning* pada *Router WLAN* lebih lanjut dapat disimpulkan pada tabel hasil analisis *variable* penelitian berikut.

**Tabel 1**. **Hasil analisis pengujian serangan *ARP poisoning* pada *Router WLAN***

| No | Variable | Sebelum Serangan | Sesudah Serangan |
|---|---|---|---|
| 1 | *IP Address dan MAC Address (Source)* | 192.168.1.1 - 50:1b:32:47:03:10 (alamat *Router gateaway*) | 192.168.1.1 - 00:1f:3c:e1:cf:b7 (alamat *attacker*) |
| 2 | *IP Address dan MAC Address (Destination)* | 192.168.1.68 - bc:a8:a6:9c:fd:29 (*user* terkoneksi internet) | 192.168.1.68 - bc:a8:a6:9c:fd:29 (koneksi internet *user* terputus) |
| 3 | *Protocol* | *ARP* dan *ICMP* berjalan dengan normal. | *ARP* mendeteksi adanya *duplicate IP* dan tidak ada respon pada *ICMP* paket *request*. |
| 4 | *Snort* | Snort tidak mengirimkan *alert* apapun kepada *user*. | Selama proses penyerangan berlansung, Snort mengirimkan *alert* kepada *user* berupa pesan "*attempted ARP cache overwrite attack*" |

## 5. Kesimpulan dan Saran

### 5.1 Kesimpulan

Pada hasil penelitian dari serangan *ARP poisoning* pada *Router WLAN* menggunakan metode *live forensics* dapat ditarik beberapa penemuan penelitian yang dapat disimpulkan sebagai berikut:

1. Analisis serangan ARP Poisoning pada Router WLAN, didapatkan informasi dari proses penelitian berupa data observasi pada saat sebelum serangan dan data pada saat sesudah serangan. Data disaat observasi meliputi IP Address dan MAC Address asli dari Router *gateaway* yaitu 192.168.1.1 - 50:1b:32:47:03:10 dari data tersebut aktivitas pada jaringan masih berjalan dengan normal, hal ini ditandai dengan paket *request* pada *user* berhasil mendapatkan *reply* dari alamat tujuan, sehingga dapat disimpulkan bahwa paket yang lewat dari alamat gateaway tersebut benar.
2. Pada saat pengujian serangan, didapatkan informasi *attacker* berupa alamat MAC Address yaitu 00:1f:3c:e1:cf:b7 yang melakukan *duplicate* alamat IP Address *gateaway* Router 192.168.1.1 dan mengirimkan pesan *broadcast* menggunakan *protocol* ARP terhadap *target* serangannya yang beralamat 192.168.1.68 - bc:a8:a6:9c:fd:29 sehingga alamat tersebut tidak mendapatkan alamat *gateaway* Router yang sesungguhnya. Hal ini berdampak pada koneksi internet korban, dikarenakan setiap paket yang akan dikirim oleh korban tidak akan sampai pada alamat tujuan yang sebenarnya, *attacker* dalam hal ini melakukan proses pengubahan alamat *gateaway* dengan cara memanfaatkan ARP *cache* jaringan. Sedangkan untuk pendeteksian, Snort berhasil mengirimkan *alert* pada perangkat *user* berupa pesan "*attempted ARP cache overwrite attack*" sehingga *user* dapat memastikan jika sedang berlansungnya serangan ARP.

**DAFTAR PUSTAKA**

[1] R. Hartono and A. Purnomo, "Wireless Network 802.11," *D3 Ti Fmipa Uns*, vol. 1, no. 1, pp. 1–23, 2011.

[2] C. Megawati, F. Teknik, and P. S. Ekstensi, "Keamanan Jaringan Wireless Berbasis Linux Platform Dan Dd-Wrt Firmware," 2012.

[3] F. Teknik, U. N. Surabaya, J. T. Informatika, F. Teknik, U. N. Surabaya, and A. Point, "MONITORING JARINGAN WIRELESS TERHADAP SERANGAN PACKET SNIFFING DENGAN MENGGUNAKAN IDS Achmad Rizal Fauzi I Made Suartana Abstrak."

[4] P. Arote, "Detection and Prevention against ARP Poisoning Attack using Modified ICMP and Voting," no. January 2015, 2016, doi: 10.1109/CINE.2015.34.

[5] P. Studi, T. Informatika, S. Tinggi, and T. Adisutjipto, "Membangun sistem keamanan arp spoofing memanfaatkan arpwatch dan addons firefox," pp. 49–58, 2012.

[6] Y. Mirsky, N. Kalbo, Y. Elovici, and A. Shabtai, "Vesper: Using Echo Analysis to Detect Man-in-the-Middle Attacks in LANs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 6. pp. 1638–1653, 2019, doi: 10.1109/TIFS.2018.2883177.

[7] N. Hildayanti and I. Riadi, "Forensics Analysis of Router On Computer Networks Using Live Forensics Method," no. May, 2019, doi: 10.17781/P002559.

[8] M. Kolhe, "Live Vs Dead Computer Forensic Image Acquisition," vol. 8, no. 3, pp. 455–457, 2017.

[9] K. F. Digital, P. Studi, M. Teknik, P. Pascasarjana, F. Teknologi, and U. I. Indonesia, "METODE LIVE FORENSICS UNTUK ANALISIS SERANGAN DENIAL OF SERVICE ( DoS ) PADA ROUTER MUHAMMAD ALIM ZULKIFLI METODE LIVE FORENSICS UNTUK ANALISIS SERANGAN DENIAL OF SERVICE ( DoS ) PADA ROUTER," 2018.

[10] I. Riadi, "INVESTIGASI LIVE FORENSIK DARI SISI PENGGUNA UNTUK MENGANALISA INVESTIGASI LIVE FORENSIK DARI SISI PENGGUNA UNTUK MENGANALISA SERANGAN MAN IN THE MIDDLE ATTACK BERBASIS EVIL TWIN," no. April, 2017, doi: 10.33096/ilkom.v9i1.103.1-8.

[11] S. Rahman and M. N. A. Khan, "Review of Live Forensic Analysis Techniques," *Int. J. Hybrid Inf. Technol.*, vol. 8, no. 2, pp. 379–388, 2015, doi: 10.14257/ijhit.2015.8.2.35.

[12] V. Data, C. Procedures, A. V. Data, and T. Incident, "Chapter 9 Collecting the Volatile Data from a Router Solutions in this chapter : Before You Connect to the Cisco Router," doi: 10.1016/B978-1-59749-418-2.00009-0.

[13] S. Syaifuddin, Z. Sari, and M. K. Masduqi, "Analysis of Uapush Malware Infection using Static and Behavior Method on Android," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 3, no. 1, pp. 81–90, 2018, doi: 10.22219/kinetik.v3i1.265.

[14] P. Laboratorium and J. Komputer, "IMPLEMENTASI INTRUSION SYSTEM ( IDS ) SNORT," pp. 1–4.

[15] D. Saputra and I. Riadi, "Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method," no. May, 2019, doi: 10.17781/P002558.

[16] T. Fiebig, "Forensic DHCP Information Extraction from Home Routers," 2013.

[17] M. Akbar and I. Pendahuluan, "PERANCANGAN SOFTWARE IDS SNORT UNTUK PENDETEKSIAN SERANGAN INTERRUPTION ( Netcut ) PADA JARINGAN WIRELESS."