
ANALISA MONITORING SNIFFING PAKET DATA JARINGAN LOKAL PADA DINAS KOMUNIKASI DAN INFORMATIKA KOTA PRABUMULIH

¹Ranti Wulandari, ^{2*}Tamsir Ariyadi

^{1,2}Teknik Komputer, Fakultas Vokasi, Universitas Bina Darma
*tamsirariyadi@binadarma.ac.id

Abstract – In the network there are many other types of data packets and each has a different function and interrelated, which contains information such as passwords, usernames, address of a site, the internet protocol (IP). As for the problem on the internet that exist at the Department of Communications and Informatics there is no monitoring and user activity that allows freedom to access the internet, it does not prevent someone from accessing negative content on the internet. In answering the problems found, this final project aims to see the level of network security that passes on the internet and the results monitoring include capture filtered data packet, focused on capturing protocol data packets http containing post data containing information about access browser connected. on the internet. Doing experiments sniffing using the application in Wireshark order to get information about activities that are happening on http such as viewing access web that is connected to the internet. The results of this final project can be concluded, it is very easy to carry out the process of capturing data packets automatically real time over a network interface, can display very detailed information that passes on the http protocol, the results of the information are very important and can be seen. IP Addresses, usernames, passwords. As well as access information browser using wireshark.

Keywords: Wireshark, Sniffing, Paket Data.

Abstrak - Di dalam jaringan banyak terdapat jenis-jenis paket data dan masing-masing mempunyai fungsi yang berbeda dan saling berkaitan, yang mengandung informasi seperti password, username, alamat sebuah situs, internet protokol (IP). Adapun masalah pada jaringan internet yang ada pada Dinas Komunikasi dan Informatika belum adanya monitoring dan aktifitas user yang memungkinkan kebebasan untuk mengakses internet tidak menutupi bagi seseorang dapat mengakses konten-konten yang bersifat negatif yang berada di internet. Dalam menjawab Permasalahan yang ditemukan, tugas akhir ini bertujuan untuk melihat tingkat keamanan jaringan yang melintas pada internet dan adapun hasil monitoring meliputi capture paket data yang difilter, difokuskan menangkap packet data protokol http yang berisikan data post yang terdapat informasi mengenai akses browser yang sedang terhubung pada jaringan internet. Melakukan percobaan sniffing dengan menggunakan aplikasi wireshark guna untuk mendapatkan informasi mengenai aktifitas yang sedang terjadi pada http seperti melihat akses web yang terhubung pada internet. Hasil dari tugas akhir ini adalah dapat disimpulkan, sangat memudahkan dalam melakukan proses Capture paket data secara real time melalui sebuah network interface, bisa menampilkan informasi-informasi yang sangat detail yang melintas pada protokol http, hasil dari informasi sangat penting dan bisa melihat. IP Address, username, password. Serta informasi akses browser menggunakan wireshark.

Kata kunci: Wireshark, Sniffing, Paket Data.

1. Pendahuluan

Perkembangan zaman yang begitu cepat pada jaringan komputer telah banyak mengalami perubahan yang begitu pesat, atau yang lebih sering dikenal dengan sebutan internet, saat ini penggunaan jaringan internet sudah menjadi kebutuhan bagi setiap individu maupun perusahaan.

Jaringan internet ini mampu menyambungkan hampir kesemua komputer yang ada untuk bisa saling bertukar informasi. Didalam jaringan banyak terdapat jenis-jenis paket data dan masing-masing mempunyai fungsi yang berbeda dan saling berkaitan. Yang mengandung informasi seperti password, alamat sebuah situs, username, internet protocol (IP), dan lain-lain. Dibalik kemudahan mengakses internet terdapat ancaman yang dapat mengganggu lalu lintas jaringan sehingga dapat menyebabkan hilang data atau informasi bahkan sampai terganggunya proses pekerjaan didalam suatu perusahaan. Saat mengirim data dari client ke server atau sebaliknya, di sinilah kemungkinan terjadi tindakan sniffing. Sniffing adalah bentuk cybercrime dimana pelaku mencuri unsertname dan password orang lain secara sengaja maupun tidak sengaja, kemudian digunakan untuk penipuan atas nama korban. Maka dari itu diperlukan tools jaringan untuk memonitoring dan menganalisa paket data yang melintas pada jaringan lokal, yang berguna untuk mengatasi aktivitas yang dilakukan pengguna jaringan dengan akses internet disana. Wireshark merupakan perangkat lunak dan termasuk salah satu protokol analisis yang disebut dengan protokol aplikasi analisis atau paket sniffer jaringan. Wireshark bisa digunakan untuk mengetahui kejadian apa yang sedang terjadi saat kita melakukakn interaksi dengan internet.

2. Tinjauan Pustaka

2.1 Analisa

Analisa sistem adalah kegiatan untuk mengindentifikasi sistem yang sedang berjalan untuk mengetahui kekurangan yang ada supaya dapat memodifikasi sesuai kebutuhan yang diperlukan [1]. Analisa merupakan proses menguraikan konsep menjadi bagian yang lebih sederhana lagi dengan tujuan mengidentifikasi sehingga solusi lebih jelas lagi sesuai kebutuhan [2].

2.2 Monitoring Jaringan

Monitoring jaringan adalah kegiatan untuk mengelola suatu sistem jaringan di server atau area tertentu, sistem monitoring ini digunakan untuk mempermudah teknisi dalam melakukan pemantauan secara rutin kondisi jaringan di server. Selain itu mempermudah dalam pemantauan koneksi internet dan bisa juga memantau bandwidth user yang sedang digunakan [3]. Monitoring Jaringan adalah Penggunaan sistem yang terus-menerus memonitor jaringan komputer untuk Komponen yang melambat atau gagal dan yang memberitahukan administrator Jaringan (melalui e-mail, SMS, atau alarm lainnya) [4].

2.3 Jaringan Komputer

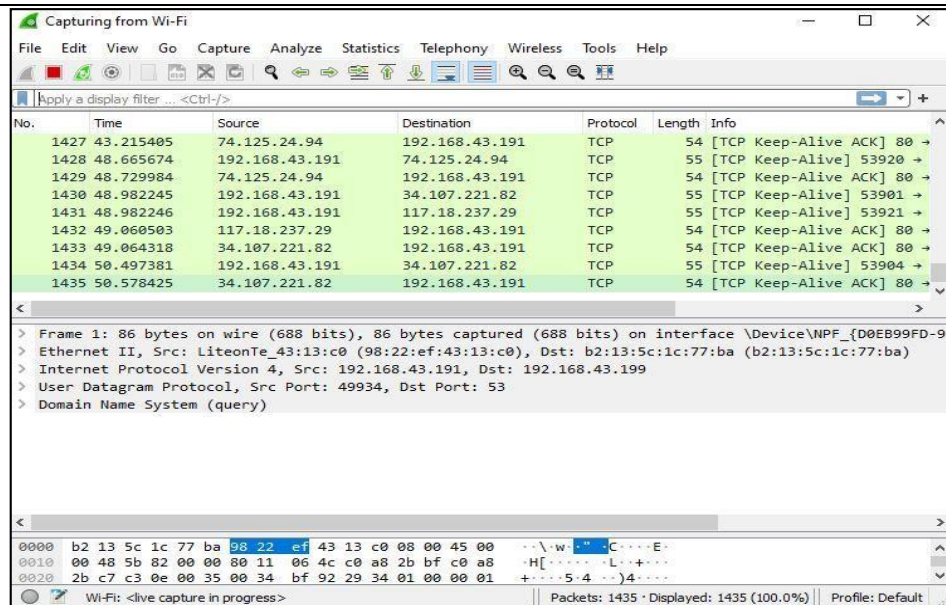
Jaringan komputer merupakan Sebuah jaringan telekomunikasi yang membolehkan node-node untuk saling berbagi sumber daya (resources). Jadi pada jaringan komputer setiap komputer yang terhubung pada jaringan dapat melakukan pertukaran data dengan komputer lainnya, melalui suatu data link (media Kabel atau media *Nirkabel/wireless*. Contoh jaringan yang populer adalah internet [5].

2.4 Sniffing

Sniffing dalam Pengertian yaitu mengendus, sedangkan dalam ilmu keamanan jaringan sniffing merupakan aktifitas menangkap paket-paket data yang lewat dalam sebuah jaringan. Sniffing sendiri biasanya digunakan untuk mengkap informasi-informasi vital dari sebuah jaringan seperti password, email text dan file sniffing [6]. *Sniffing* merupakan proses pengendusan paket data pada sistem jaringan komputer, yang diantaranya dapat memonitoring dan menangkap semua lalu lintas jaringan yang lewat tanpa peduli kepada siapa paket itu di kirimkan [7].

3. Metodologi Penelitian

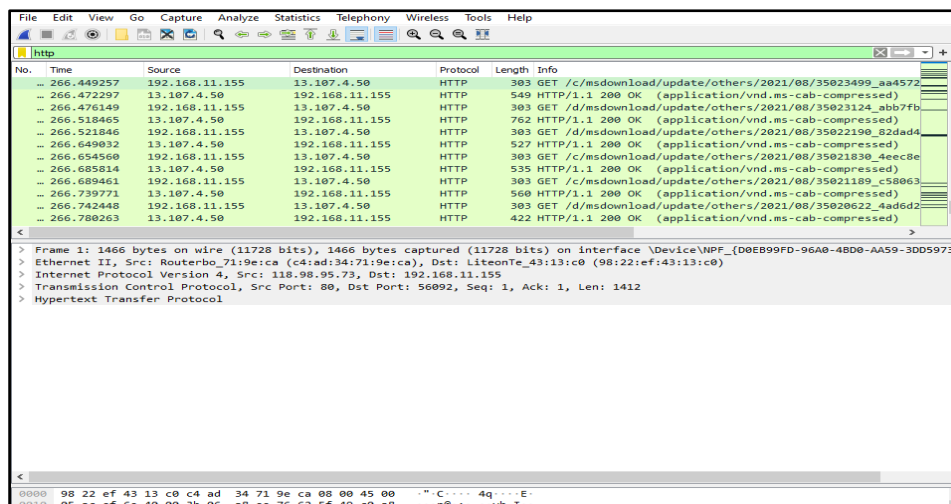
Action research ditandai dengan pendekatan systematic inquiry yang memiliki kriteria tertentu. Action Research harus dapat membedakan perbedaan antara ciri tindakan dan penelitian, harus adanya keterlibatan langsung bukan hanya sebagai pengamat. Dalam penelitian ini penulis menggunakan metode action research yang dibagi dalam 5 tahapan yaitu:



Gambar 2. Proses Capture Paket Data

4.3 Filtering Protokol HTTP

Disini penulis akan melakukan filtering paket data yang melewati protokol *HTTP*, selanjutnya ketikkan *HTTP* pada kolom *Address Filter*.

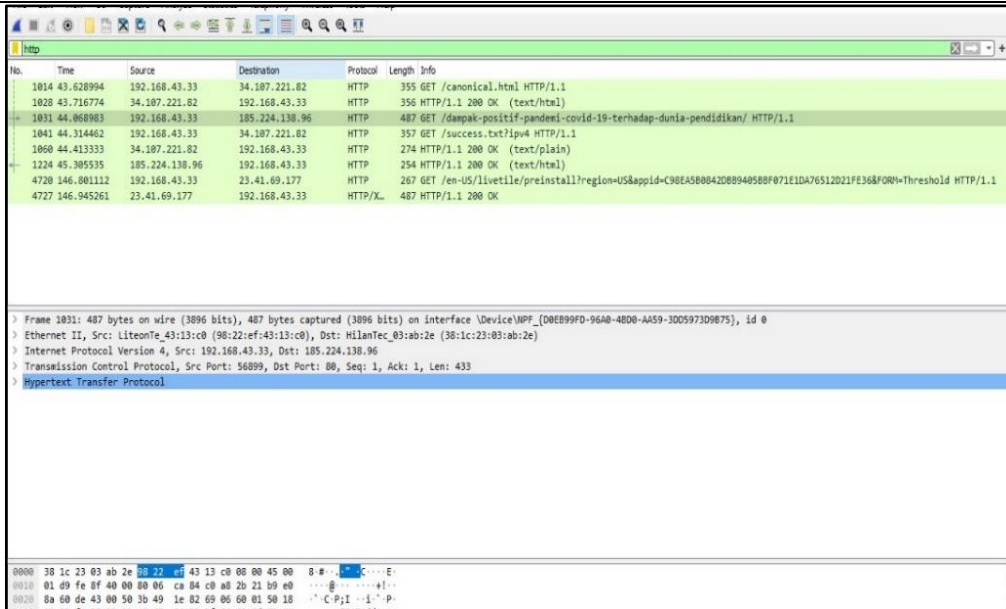


Gambar 3. Filtering protokol HTTP

4.4 Sniffing & Analisis

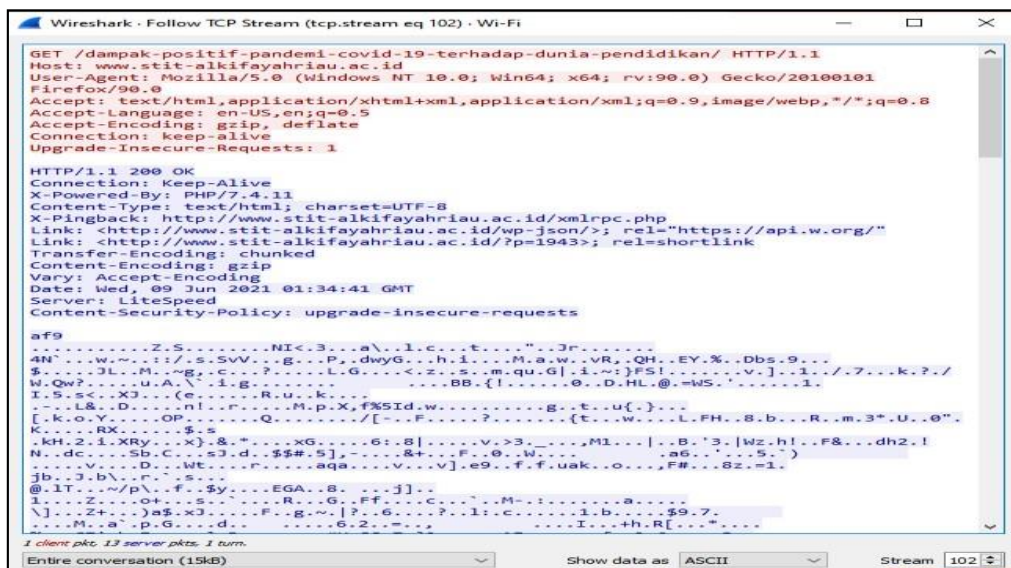
Setelah melakukan filtering berikutnya dilakukan analisis paket data yang melewati protokol *HTTP* yang berisikan data post atau get yang terdapat informasi- informasi mengenai aktivitas jaringan yang di lakukan perangkat yang beralamat IP. Snifing situs yang diakses dalam wireshark:

- 1) Paket-paket data dari situs yang telah diakses tadi akan tercapture dan sudah di lakukan filtering.
- 2) Berikutnya pilih dari paket-paket yang mengirimkan pesan Get. Lalu paketnya akan tercapture maka akan terlihat situs apa yang sedang di buka.
- 3) Contoh satu dalam protokol http. Dalam box *http* terlihat permintaan source dan destination. Src 192.168.43.33 Dst 185.224.138.96 HTTP487GET/dampak–positif–pademi-covid-19-tehadap-dunia pendidikan/HTTP/1.1.



Gambar 4. Stit-alkifayahriau.ac.id

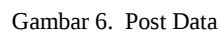
Bisa dianalisis yaitu user-agent yang dipakai menggunakan Mozilla /5.0 (Windows NT 10.0; Win64; rv:90.0) Gecko/20100101 Firefox/90.0. Dan host: stit-alkifayahriau.ac.id, selain itu dapat diketahui date yaitu pada date wed, 09 jun 2021 01:32:41 GMT dan Full Request Get Uri: http://dampak-positif-pandemi-covid-19-terhadap-dunia-pendidikan/. Disini bisa dilihat bahwa adanya aktivitas yang sedang mengakses laman web. Gambar capture TCP Stream wireshark dibawah ini dapat melihat info get yang sedang di buka.



Gambar 5. TCP Stream

4.5 Snifing UserName&Password yang Melintas Protokol HTTP

Setelah itu melakukan capturing dan filtering paket pada protokol HTTP, dan lakukan analisis paket yang berisikan data post yang sudah login src 192.168.11.55 dst 103.108.141.83 http port 1228 (application /-www- form-urlencoded)



The screenshot displays the Wireshark interface with a network capture of an HTTP GET request. The packet list on the left shows packet 25 selected, which is an HTTP GET request from 10.180.141.83 to 10.180.141.83. The packet details pane shows the structure of the HTTP request, including Host, User-Agent, Accept, Accept-Language, Accept-Encoding, Content-Type, Content-Length, Origin, Connection, Referer, and cookies. The packet bytes pane shows the raw data of the request.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
25	0.000000	10.180.141.83	10.180.141.83	HTTP	404	GET //filestreamingservice/files/d32fde-4ef1-4654-b1e7-558649e3a179P1-6303801834BP2-404BP3-28P4-40P4Q2/Q6sCoB...

Packet Details:

- Host: 10.180.141.83/vrtn
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:92.0) Gecko/20100101 Firefox/92.0/vrtn
- Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8/vrtn
- Accept-Language: en-US,en;q=0.5/vrtn
- Accept-Encoding: gzip, deflate/vrtn
- Content-Type: application/x-www-form-urlencoded/vrtn
- Content-Length: 81/vrtn
- Origin: http://10.180.141.83/vrtn
- Connection: keep-alive/vrtn
- Referer: http://10.180.141.83/login/vrtn
- Cookie: KSMF-T0X6WeyJpd161j3ULHDPNkxayQWQWNRBj8Q0Q0t2cPS1InZbHvH1jui0516k0y6wv0InckAeePw0n10uQsQd7J2W5Gk29ARctDXK21jWpQ01I2R88H4WPKC3jTW0z0y1nd5mk1d8C1

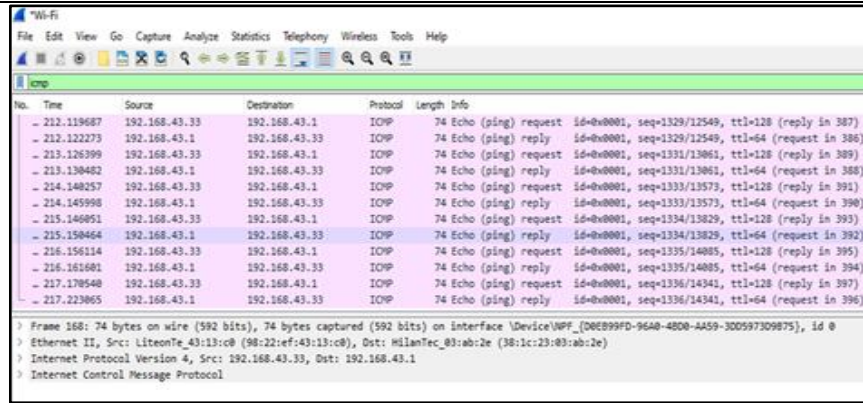
Packet Bytes:

```

0000  04 0e 81 48 00 50 83 22 4f 43 13 c0 00 45 00  ...dq...C...E-
0010  04 0e 81 48 00 80 06 53 b5 c0 00 90 00 67 0c  ...@...@...P...
0020  75 3f e1 00 50 83 74 c9 9a f6 24 c1 11 50 18  ......t...S...P-
  
```

Dapat dilihat dalam box html from terdapat hasil dari sniffing aktifitas perangkat dengan IP 103.108.141.83 yang sedang membuka sebuah laman website yang berisikan password yang melintas pada protokol Http.





No.	Time	Source	Destination	Protocol	Length	Info
212.119687		192.168.43.33	192.168.43.1	ICMP	74	Echo (ping) request id=0x0001, seq=1329/12549, ttl=128 (reply in 387)
212.122273		192.168.43.1	192.168.43.33	ICMP	74	Echo (ping) reply id=0x0001, seq=1329/12549, ttl=64 (request in 386)
213.126399		192.168.43.33	192.168.43.1	ICMP	74	Echo (ping) request id=0x0001, seq=1331/13061, ttl=128 (reply in 389)
213.130482		192.168.43.1	192.168.43.33	ICMP	74	Echo (ping) reply id=0x0001, seq=1331/13061, ttl=64 (request in 388)
214.148257		192.168.43.33	192.168.43.1	ICMP	74	Echo (ping) request id=0x0001, seq=1333/13573, ttl=128 (reply in 391)
214.145998		192.168.43.1	192.168.43.33	ICMP	74	Echo (ping) reply id=0x0001, seq=1333/13573, ttl=64 (request in 390)
215.146951		192.168.43.33	192.168.43.1	ICMP	74	Echo (ping) request id=0x0001, seq=1334/13829, ttl=128 (reply in 393)
215.150464		192.168.43.1	192.168.43.33	ICMP	74	Echo (ping) reply id=0x0001, seq=1334/13829, ttl=64 (request in 392)
216.156114		192.168.43.33	192.168.43.1	ICMP	74	Echo (ping) request id=0x0001, seq=1335/14085, ttl=128 (reply in 395)
216.161681		192.168.43.1	192.168.43.33	ICMP	74	Echo (ping) reply id=0x0001, seq=1335/14085, ttl=64 (request in 394)
217.170540		192.168.43.33	192.168.43.1	ICMP	74	Echo (ping) request id=0x0001, seq=1336/14341, ttl=128 (reply in 397)
217.223065		192.168.43.1	192.168.43.33	ICMP	74	Echo (ping) reply id=0x0001, seq=1336/14341, ttl=64 (request in 396)

Gambar 11. Tampilan Lalu Lintas Ping yang Masuk pada Wireshark

Dari gambar diatas dapat dilihat lalu lintas serangan dos yang mengirim data terus menerus pada IP 192.168.43.33 yang terdeteksi oleh wireshark, dari kolom source terdapat IP dari komputer penyerang yaitu 192.168.43.1 yang melakukan peyerangan. Dan pada kolom destination adalah IP 192.168.43.33 yang merupakan komputer target.

5. Kesimpulan

Hasil dari tugas akhir ini adalah dapat disimpulkan, sangat memudahkan dalam melakukan proses Capture paket data secara real time melalui sebuah network interface, bisa menampilkan informasi-informasi yang sangat detail yang melintas pada protokol http, hasil dari informasi sangat penting dan bisa melihat IP Adress, username, password. Serta informasi akses browser menggunakan wireshark. Dan dari hasil percobaan serangan dos dapat terjadi apabila komputer penyerang dan komputer target saling berkomunikasi didalam network yang sama dan bisa melakukan penyerangan sebanyak mungkin ke IP yang ditargetkan. Aplikasi wireshark ini hanya bisa digunakan untuk memonitoring jaringan dan tidak bisa melakukan tindakan seperti troubleshoot langsung ke interface, wireshark sendiri bisa menjadi alat seseorang admin untuk memonitoring jaringan dan memudahkan dalam proses analisa secara real time.

Referensi

- [1] R. S. Didi, "Implementasi dan Analisis Jaringan menggunakan Wireshark, Chain and Tabela, Network Minner" *Candikia*, Vol. XVI, 2018, 120-125,.
- [2] S. H. Yopi, "Analisa Monitoring Lalu Lintas Paket Data pada Jaringan Lokal, *Snit*, 2011, 296-303.
- [3] R. Primartha, *Manajemen Jaringan Komputer*, Bandung, 2019.
- [4] I. Sofana, *Jaringan Komputer berbasis Mikrotik*, Bandung, 2017.
- [5] M. Angga, "Analisis Keamanan Jaringan dari Serangan Paket Data Sniffing di PT. Raden Syaid Kantor Pos Piayu Kota Batam, *Comasie*, Vol.03, No.05, 2020, 107-108.
- [6] A. Mahmud, *Sniffing Jaringan menggunakan Wireshark*, Jaringan Komputer, 2019, 1-4.
- [7] H. Rahma, "Analisa Pencegahan Aktifitas Ilegal didalam Jaringan dengan Wireshark", *Journal*, Vol.4, No. 1, 2020, 11-23.