CyberSecurity dan Forensik Digital e-ISSN: 2615-8442
Vol. 6, No. 2, November 2023, hlm. 62-68

Analisis Dan Monitor *Sniffing* Paket Data Jaringan Lokal Dengan *Network Analyzer Wireshark*

Rahma Milan Sari[1], Tri Rochmadi[2].

[12]Universitas Alma Ata
Email: [1]rahmamilansari@gmail.com, [2]trirochmadi@almaata.ac.id

Abstrak

Teknologi menjadi peran penting bagi kehidupan di era globalisasi, perkembangan zaman telah merubah segala aspek dalam kehidupan manusia baik di bidang sosial, budaya, serta teknologi. Proses transfer data dari client ke server memungkinkan terjadinya cybercrime berupa tindakan sniffing. Penelitian ini menggunakan pendekatan kualitatif dengan model penelitian action research. Penelitian dilakukan sebagai data yang diberikan dan digunakan instansi guna menjadi bahan pertimbangan dan masukan dalam upaya meningkatkan keamanan jaringan yang lebih baik, dan untuk mengevaluasi jaringan lokal terhadap cybercrime sniffing. Hasil dari penelitian yang telah dilakukan pada *website* ditemukan satu website yang teridentifikasi masih menggunakan protokol HTTP, hasil analisis pada website tersebut menunjukan beberapa informasi pribadi seperti username dan password yang memungkinkan informasi dapat dengan mudah disalahgunakan oleh pihak tak bertanggungjawab. Website lain yang dianalisis dengan protokol HTTPS tidak menampilkan informasi pribadi, bahkan terdapat informasi berupa kode yang sulit untuk dibaca pada detail follow TCP stream. Website dengan protokol HTTPS sudah terenkripsi, dimana informasi yang keluar masuk tidak mudah untuk diketahui dan lalu lintas paket data aman didalammnya. Pada penelitian ini penelitit melakukan monitor dan analisis website berprotokol http dan https dengan tindakan sniffing, penelitian ini sebagai evaluasi dan peningkatan pengetahuan akan keamanan pada jaringan. Analisis website berprotokol https dilakukan sebagai perbandingan dengan website berprotokol http yang belum didilakukan oleh peneliti terdahulu.

Kata kunci: *Teknologi, Jaringan, Action Research, Sniffing.*

Analyze And Monitor Local Network Package Data Sniffing Using Wireshark Network Analyzer

Abstract

Technology is an important role for life in the era of globalization, the times have changed all aspects of human life in the fields of social, culture, and technology. The process of transferring data from client to server allows cybercrime in the form of sniffing. This research uses a qualitative approach with an action research model. The research was conducted as data provided and used by agencies to be taken into consideration and input in an effort to improve better network security, and to evaluate local networks against cybercrime sniffing. The results of the research that has been carried out on the website found one website that was identified as still using the HTTP protocol, the results of the analysis on the website show some personal information such as usernames and passwords that allow information to be easily misused by irresponsible parties. Other websites analyzed with the HTTPS protocol do not display personal information, there is even information in the form of code that is difficult to read in the TCP stream follow details. Websites with the HTTPS protocol are encrypted, where information in and out is not easy to know and data packet traffic is safe in it. In this research, researchers monitor and analyze http and https protocol websites with sniffing actions, this research is an evaluation and increase knowledge of security on the network. Analysis of https protocol websites is done as a comparison with http protocol websites that have not been done by previous researchers.

Keywords: *Technology, Networking, Action Research, Sniffing.*

1. PENDAHULUAN

Teknologi menjadi peran penting bagi kehidupan pada era globalisasi seperti sekarang ini Perkembangan zaman telah mengubah seluruh aspek kehidupan manusia baik di bidang sosial, budaya, serta teknologi (Majid and Purwanto, 2021). Dalam kegiatan proses transfer data menggunakan teknologi komunikasi untuk mempermudah pekerjaan serta kebutuhan sehari-hari (Huda, 2020). Dalam proses transfer data diperlukan jaringan untuk menghubungkan perangkat yang akan digunakan. Pada suatu jaringan terdapat beberapa jenis paket data, salah satunya paket data yang di dalamnya terdapat informasi terkait kata sandi, *username*, dan alamat *web*. Sedangkan informasi

protokol seperti sumber, tujuan, jenis data adalah sebuah *packet header* (Majid and Purwanto, 2021). Penggunaan router wireless pada jaringan rumahan juga memiliki celah keamanan yang dapat dimanfaatkan oleh pihak yang tidak bertanggung jawab sehingga memiliki potensi ancaman keamanan data bagi para penggunanya(Kusuma et al., 2023)

Dalam mengirim data dari client ke server atau sebaliknya, memungkinkan terjadinya tindakan sniffing. Sniffing merupakan tindakan cybercrime dimana pelaku mencuri username dan password orang lain, akun yang telah dicuri akan disalahgunakan oleh pelaku untuk tindakan penipuan atas nama korban bahkan sampai merusak atau menghapus data milik korban (Novenzo Ihsana and Maslan, 2020). Sebagai contoh pengguna komputer yang terhubung dengan jaringan komputer, dengan aktifitas *sniffing* nama pengguna serta *password* pengguna bisa diketahui atau *di capture* oleh seorang yang melakukan *sniffing*.

Namun sniffing tidak hanya digunakan dengan tujuan kejahatan saja, sesuai dengan penggunaannya, namun kebanyakan sniffing digunakan dengan tujuan buruk untuk memperoleh keuntungan sebanyak-banyaknya dari data tersebut. Dibutuhkan tindakan monitoring secara langsung untuk mengetahui paket data pada suatu jaringan, dengan tujuan untuk mendapatkan informasi kemudian menganalisa paket data yang melintas. Perangkat lunak *wireshark* digunakan dalam proses *sniffing*, perangkat ini dapat menganalisa sebuah jaringan dan bisa sebagai referensi untuk memperbaiki masalah jaringan melalui proses *capturing*. Sistem *capture* ini bisa menentukan apa saja yang dibutuhkan di dalam memonitor jaringan, seluruh proses yang berjalan akan *tercapture* secara langsung.

Pada penelitian ini peneliti melakukan monitor dan analisis *website* berprotokol http dan https dengan tindakan *sniffing*, penelitian ini sebagai evaluasi dan peningkatan pengetahuan akan keamanan pada jaringan. Analisis *website* berprotokol https dilakukan sebagai perbandingan dengan *website* berprotokol http yang belum dilakukan oleh peneliti terdahulu.

2. . TINJAUAN PUSTAKA

Pencurian data dilakukan ketika data dikirim menuju beberapa terminal tetapi sebelum sampai tujuan data sudah dialihkan ke pengguna lain yang tidak bertanggung jawab untuk memotong, mengubah, bahkan mencuri data upaya untuk keamanan yang terhubung dengan internet maka harus dipersiapkan dengan benar, agar nantinya efektif melindungi dan meminimalisir serangan (Novenzo Ihsana and Maslan, 2020)

Aplikasi *wireshark* memonitor semua paket data yang keluar masuk melalui antarmuka yang sudah ditentukan oleh pengguna sebelumnya lalu akan ditampilkan secara terperinci (Majid and Purwanto, 2021).

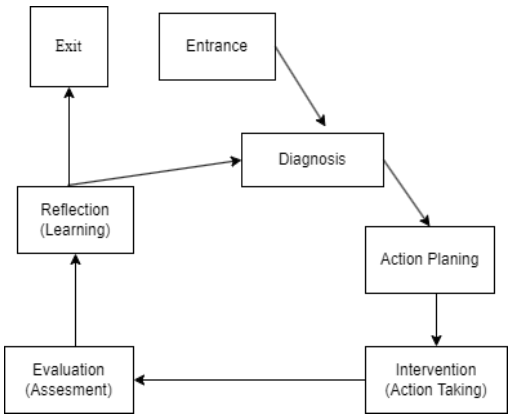
Proses memonitoring jaringan bisa dilakukan di sebuah instansi atau perusahaan sebagai tindakan untuk memproteksi jaringan. Pihak instansi memerlukan tools jaringan untuk monitoring lalu lintas jaringan untuk mengetahui aktivitas yang dilakukan pengguna jaringan dengan akses internet disana, bahkan dapat membentuk tim *security operation center* (SOC) badan yang bertanggung jawab terhadap keamanan jaringan internet. Memonitoring dan menganalisis diperlukan apabila terjadi insiden kejahatan siber, apalagi sekarang banyak terjadi *phising* dan *social engineering*. Tujuan dari penelitian ini sebagai data yang diberikan dan digunakan oleh pihak IT instansi guna menjadi bahan pertimbangan dan masukkan dalam upaya meningkatkan keamanan jaringan yang lebih baik, dan untuk mengevaluasi keamanan jaringan lokal terhadap *packet sniffing*.

3. METODOLOGI

Penelitian ini menggunakan pendekatan kualitatif. Penelitian kualitatif menurut *Creswell* (2008) mendefinisikannya sebagai suatu pendekatan untuk menemukan dan memahami suatu fenomena sentral. Untuk mengungkap fenomena sentral tersebut peneliti melakukan wawancara partisipan dengan mengajukan pertanyaan umum dan cukup luas. Informasi yang disampaikan oleh partisipan kemudian dikumpulkan, biasanya berupa kata-kata atau teks, kemudian dianalisis. Hasil analisis dapat berupa deskripsi, uraian, atau bahkan berupa topik, dan data yang diperoleh peneliti memunculkan wawasan untuk menangkap makna yang terdalam (Semiawan, n.d.). Model penelitian yang digunakan dalam penelitian ini adalah *Action Research* dengan mendeskripsikan, menginterpretasikan dan menjelaskan sebuah situasi sosial pada waktu yang bersamaan dengan melakukan perubahan maupun intervensi bertujuan untuk perbaikan atau partisipasi (Hasan, 2009). Menurut Gunawan, *action research* yaitu tindakan perbaikan yang perencanaan, pelaksanaan, dan evaluasinya dikerjakan secara sistematik sebab itu validitas dan reliabilitas sampai tingkat riset. *Action research* juga merupakan proses yang melibatkan siklus aksi berdasarkan pada refleksi, umpan balik, bukti, dan evaluasi terhadap aksi sebelumnya dan keadaan terkini. Penelitian tindakan berfokus untuk memberikan kontribusi pada pemecahan masalah praktis dalam situasi problematik mendesak pada pencapaian tujuan ilmu sosial melalui kolaborasi patungan dalam rangka kerja etis yang saling berterima (M. Askari Zakariah, Vivi Afriani, 2020). Model *action research* dilaksanakan sedikitnya oleh dua orang terdiri dari peneliti dan partisipan *client* yang berasal dari akademisi maupun masyarakat. Dengan demikian tujuan yang akan dicapai tidak hanya pada

situasi organisasi saja, melainkan dapat dikembangkan menjadi aplikasi maupun teori yang dihasilkan akan dipublikasi dengan tujuan riset (Tafui, 2019).

Berikut merupakan siklus metode *Action Research*:



Gambar 1. Siklus Metode *Action Research*
Sumber: Irvan S Tafui (2019) (Tafui, 2019).

a. *Diagnosing*

Langkah pertama ialah mengidentifikasi masalah pokok yang ada, pada packet data protokol HTTP dan HTTPS pada jaringan Universitas Alma Ata, dimana akan dilakukannya *action research* dan melakukan wawancara mengenai masalah yang ada, kemudian data wawancara dibandingkan dengan hasil analisis paket data. Adanya tahap wawancara untuk menyatukan keterangan pada tahap selanjutnya. Pada langkah ini penulis ingin mengetahui permasalahan yang terjadi, dan menemukan titik poin yang akan di analisis.

b. *Action Planning*

Mendalami hasil masalah yang telah didapat pada saat melakukan diagnosa, mengenai masalah yang dialami partisipan dan peneliti. Tahap berikutnya membuat jadwal penelitian yang akan dilakukan, seperti membuat jadwal memonitor di Universitas Alma Ata, peneliti dan partisipan berkolaborasi dalam proses penelitian, seperti halnya melakukan *capture* data pada jaringan dilanjutkan dengan memonitor dan menganalisisnya.

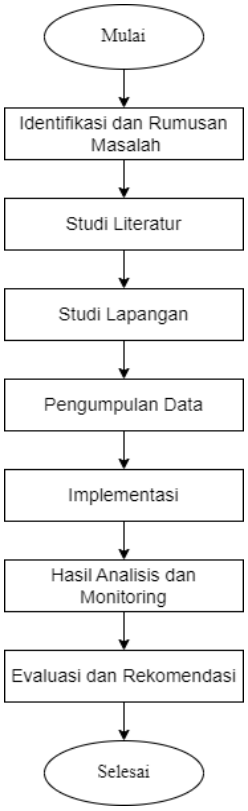
c. Action Talking

Selanjutnya melakukan tindakan dimana peneliti mengimplementasikan rencana tindakan dengan menginstalasi wireshark dan bagaimana menjalankannya untuk mendapatkan data capture dari lalu lintas jaringan untuk memantau dan menganalisa pada paket data jaringan tersebut. Kolaborasi antara peneliti dan partisipan pada setiap tahap dimulai dari perencanaan, pelaksanaan, pemanfaatan, dan pembelajaran akan menumbuhkan rasa kesadaran akan kejahatan siber yang suatu saat dapat menyerang sehingga partisipan dapat melindungi dan mencegah kejahatan sniffing. Partisipan berperan penting dalam keamanan paket data jaringan, sehingga partisipan aktif mutlak dibutuhkan.

d. *Evaluating*

Pada tahap evaluasi hasil implementasi yang dilakukan peneliti melihat kembali hasil wawancara dan hasil analisa dan monitoring paket data jaringan, apakah hasilnya sama atau saling bertentangan, apabila kedua data cocok dapat ditarik kesimpulan mengenai aktivitas yang telah dilakukan

e. *Learning*



Peneliti menganalisa semua kinerja dan memaparkan hasil pada tahap terakhir, kemudian hasil tersebut bertujuan untuk pembelajaran dalam tindakan berikutnya.

3.1. Tahap Alur Penelitian

Gambar 2. Alur Penelitian

Awal dari tahapan ini dimulai dengan mengindetifikasi masalah yang ada kemudian merumuskan dan menentukan batasan masalah. Setelah itu melakukan studi literatur untuk mengetahui berbagai penelitian terdahulu terkait dengan penelitian yang dilakukan, dan melakukan diagnosis untuk mencari metode yang relevan dengan permasalahan dan metode untuk merumuskan masalah. Tahap selanjutnya studi lapangan dengan melakukan observasi dan diagnosis pada objek penelitian yaitu paket data jaringan bertujuan untuk mengetahui permasalahan terkait keamanan lalu lintas jaringan dan mengetahui paket

data jaringan pada *server* tertentu yang nantinya dimonitoring, dan juga melakukan wawancara dengan narasumber terkait lalu lintas paket data pada jaringan. Selanjutnya pengumpulan data dengan melakukan wawancara, pada bagian ini akan dijelaskan terkait bagaimana melakukan pengambilan data terhadap masalah, bagaimana pihak penanggungjawab jaringan diwawancarai terhadap pengoperasian jaringan Langkah berikutnya implementasi berupa tahapan dari rencana tindakan analisis dan monitoring dari data capture dengan ketentuan waktu dan tempat. Langkah selanjutnya yaitu pemaparan hasil monitoring jaringan dan analisis paket data *capture*, kemudian tahap evaluasi dan rekomendasi dalam penelitian hasil dari monitoring dan analisis yang dilakukan pada jaringan, nantinya akan didapat usulan perbaikkan dari hasil wawancara, dan monitoring dan analisis.

4. PEMBAHASAN

4.1. Pengambilan Data

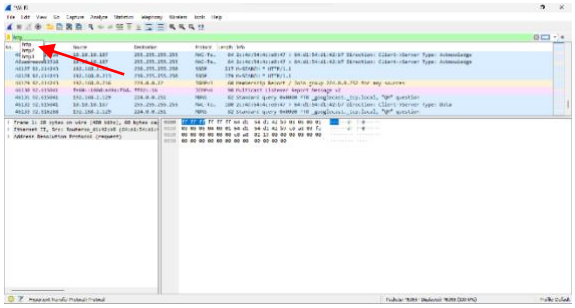
Dalam langkah pengambilan data dilakukan *sniffing* pada jaringan, dengan melakukan pengangkapan paket data *(capture)* mengenai aktifitas yang melintas pada jaringan dan protokol *http* guna mendapatkan informasi seperti memantau akses *browser* yang sedang berjalan, situs yang dikunjungi menggunakan *wireshark*.

Proses pengambilan data dilakukan dengan membuat jadwal dalam monitoring dan analisis paket data jaringan, dilakukan selama 5 hari pada jam produktif jam 09:00-12:00 WIB dan 13:00-15:00 WIB.

4.2. Monitoring Dan Analisis

4.2.1. Filtering Paket Data HTTP

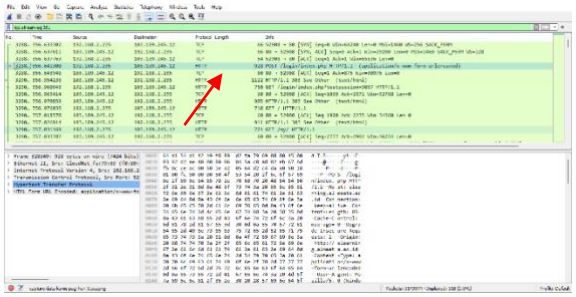
Filtering paket data yang melewati protokol *HTTP* dan *HTTPS* dengan ketik *HTTP* pada kolom *display filter*.



Gambar 3 Display Filter Dengan HTTP

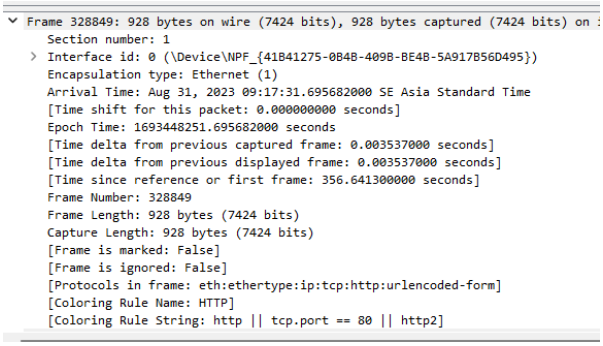
Banyaknya data yang terekan menyulitkan untuk dianalisis, maka dilakukan filter data untuk memudahkan dalam menganalisis protokol. Dengan tampilan seperti dibawah sudah dilakukan *filtering* protokol HTTP.

4.2.2. Melakukan Analisis pada paket yang berisi data POST



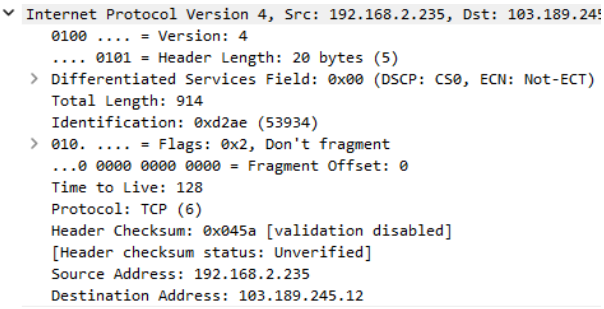
Gambar 4 Paket Yang Barisi data POST

Pada salah satu data POST terdapat informasi seperti alamat IP 192.168.2.235 *source* dan 103.189. 245. 12 *destination*, pada protokol berisi *HTTP* dan panjang paket 928 *bytes*. Tampilan hasil dari detail paket data seperti *detail* data *frame*, *internet protocol*, *transmission control*, *Hypertext Transfer Protocol*, dan fitur *Follow TCP* untuk melihat informasi paket data. Berikut tampilan detail paket data:



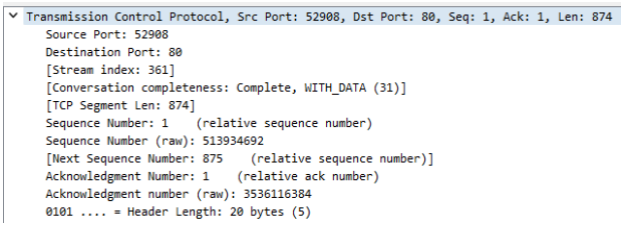
```
Frame 328849: 928 bytes on wire (7424 bits), 928 bytes captured (7424 bits) on
    Section number: 1
  > Interface id: 0 (\Device\NPF_{41B41275-0B4B-409B-BE4B-5A917B56D495})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 31, 2023 09:17:31.695682000 SE Asia Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1693448251.695682000 seconds
    [Time delta from previous captured frame: 0.003537000 seconds]
    [Time delta from previous displayed frame: 0.003537000 seconds]
    [Time since reference or first frame: 356.641300000 seconds]
    Frame Number: 328849
    Frame Length: 928 bytes (7424 bits)
    Capture Length: 928 bytes (7424 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:http:urlencoded-form]
    [Coloring Rule Name: HTTP]
    [Coloring Rule String: http || tcp.port == 80 || http2]
```

Gambar 5 Detail Paket Data Frame



```
Internet Protocol Version 4, Src: 192.168.2.235, Dst: 103.189.245
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 914
    Identification: 0xd2ae (53934)
  > 010. .... = Flags: 0x2, Don't fragment
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: TCP (6)
    Header Checksum: 0x045a [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.2.235
    Destination Address: 103.189.245.12
```

Gambar 6 Detail Paket Data Internet Protocol

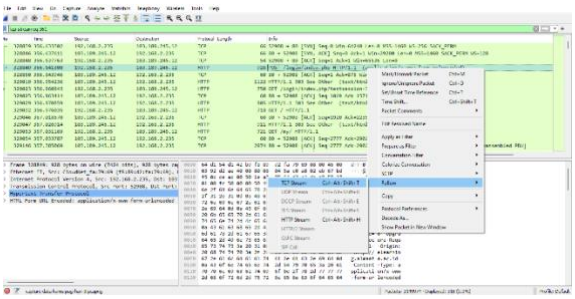


```
Transmission Control Protocol, Src Port: 52908, Dst Port: 80, Seq: 1, Ack: 1, Len: 874
    Source Port: 52908
    Destination Port: 80
    [Stream index: 361]
    [Conversation completeness: Complete, WITH_DATA (31)]
    [TCP Segment Len: 874]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 513934692
    [Next Sequence Number: 875    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3536116384
    0101 .... = Header Length: 20 bytes (5)
```

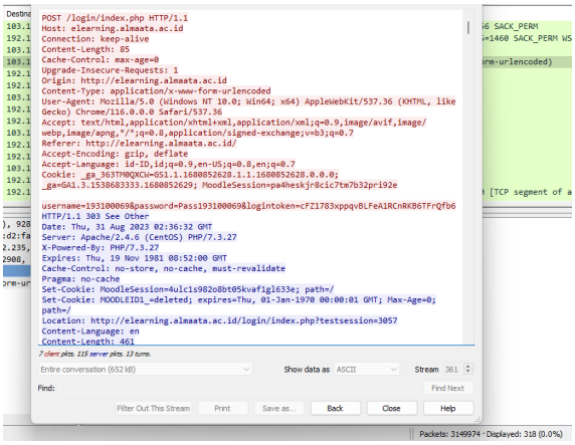
Gambar 7 Detail Transmission Control Protocol

Gambar 8 Detail Hypertext Transfer Protocol

Pada detail paket data *transmission control protocol* menunjukan pada *source* menggunakan *port*: 52908, pada *destination* menggunakan *port*: 80. *Website* yang telah diakses dapat diketahui pada detail paket data *hypertext transfer protocol* yaitu *host* *earlerning*.instansi.ac.id, dengan permintaan HTTP POST dengan *user agent* atau keterangan pengguna mengakses dengan *windows* 10, dan *google crome*. Adapun cara lain untuk mengetahui terkait informasi paket data dengan fitur *follow TCP stream*, dengan klik kanan pada baris paket data kemudian pilih *follow* kemudian pilih *TCP stream* permintaan akan diproses dan akan menampilkan informasi terkait paket data. berikut merupakan gambar dari *TCP stream*:



Gambar 9. Follow TCP Stream

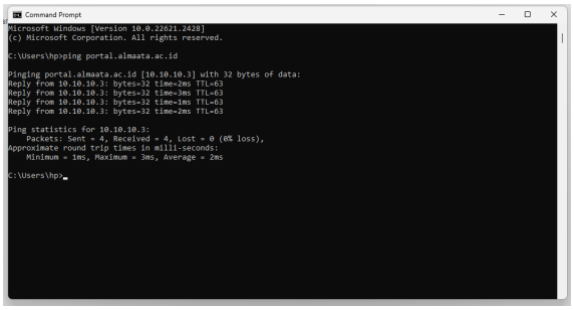


Gambar 10 Tampilan Hasil Follow TCP Stream

Informasi terkait detail paket tertera pada perintah *follow* TCP *stream* dari keterangan aktifitas *login*, *host* dari *website* yang diakses, informasi *website* yang diakses, waktu akses, bahasa konten, panjang konten, hingga *username* dan *password*. Informasi yang berwarna merah merupakan perintah dari *client*, sedangkan informasi berwarna biru berasal dari *server* membalas *client*. Tertera versi http yang dipakai ialah HTTP/1.1, *host* atau *web* yang sedang dibuka *elearning*.instansi.ac.id, koneksi berjalan atau aktif (*keep-alive*), *username*, *password* dan *login* token juga tertera. *Sniffing* informasi terkait *username*, *password* juga dapat diketahui melalui *HTML from URL Encoded*, terdapat item yang menunjukan *username*, *password* dan *login token*. Berikut merupakan gambar *HTML from URL Encoded.*

Gambar 11 HTML From Encoded

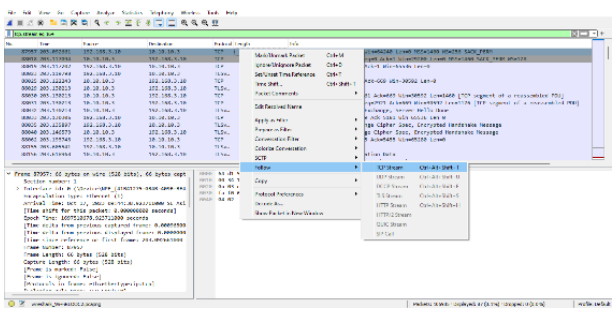
Langkah untuk analisis *website* berprotokol HTTPS yang diakses dengan cara melakukan ping pada *command prompt* guna mendeteksi *IP websitenya*. Dengan cara buka *command prompt* kemudian ketikan ping diikuti nama *website* yang akan dituju seperti gambar dibawah ini:



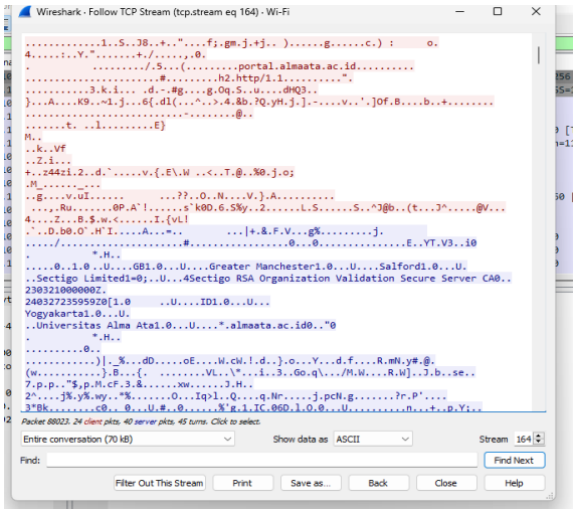
Gambar 12 Tampilan Command Prompt

Dapat diketahui setelah melakukan pemanggilan IP dengan CMD didapat alamat IP website yaitu 10.10.10.3.

Follow TCP *Stream* untuk melihat detail paket https, dengan langkah yang sama seperti langkah pada *follow* protokol http. Dengan klik kanan pada baris data dengan IP website yang telah diketahui pilih *follow* kemudian pilih *TCP stream*.



Gambar 13 Follow TCP Stream



Gambar 14 Hasil *Follow TCP Stream* HTTPS

Informasi yang ditampilkan berupa sekumpulan kode acak pada jejak pertukaran data yang terjadi di *website*, sulit untuk mengetahui informasi apa saja yang terjadi. Berbeda pada *follow* TCP http semua informasi tertera dengan jelas seperti *host* hingga *username* dan *password*, pada *follow* TCP https hanya terbaca "portal.almaata.ac.id", "http", "Yogyakarta1.0", "Universitas Alma Ata1.0", "almaata.ac.id0", saja yang terbaca. Total HTTP dan HTTPS *packets* yang sudah *dicapture* terlihat pada tabel 1

Table 1.Total HTTP/HTTPS *packets*

NO	Hari	HTTP packets		HTTPS packets	
		Pagi	Siang	Pagi	Siang
1.	Senin	123388	146031	29063	31355
2.	Selasa	233164	147998	106146	76675
3.	Rabu	244819	175023	99024	18727
4.	Kamis	248285	154083	86448	13425
5.	Jumat	247927	162777	29625	13719

Proses *capture* data selama 5 hari dengan memonitor paket data yang melewati salah satu jaringan di ruangan instansi, jaringan yang digunakan cukup lancar, namun semakin banyak digunakan jaringan sedikit lambat karena pada jam produktif akan banyak pengguna. Saat melakukan *capture* data banyak sekali lalu lintas dan banyak juga data keluar masuk, paket data yang melintas berbagai jenis protokol dan jenis interaksi. Penelitian ini berfokus pada analisis *website* instansi dengan protokol HTTP dan HTTPS untuk dianalisis. Dari hasil *capture* banyak paket data yang terrekam kemudian dilakukan analisis salah satu dari website yang diakses menggunakan jaringan tersebut, hasil monitor paket data dengan berbagai jenis protokol dan jenis interaksi yang terjadi masih menggunakan protokol HTTP yang dapat dengan mudah diketahui password, usename, waktu akses, kegiatan yang dilakukan, perangkat yang digunakan, dan masih banyak detail informasi lainnya. Sedangkan website lain sudah menggunakan protokol HTTPS yang artinya telah terenkripsi dan saat dianalisis interaksi detail paket hanya menampilkan kode acak yang informasinya sulit dibaca dan diketahui ketika dilakukan sniffing.

5. KESIMPULAN DAN SARAN

Pada penelitian ini penelitit melakukan monitor dan analisis website berprotokol http dan https dengan tindakan sniffing, penelitian ini sebagai evaluasi dan peningkatan pengetahuan akan keamanan pada jaringan. Analisis website berprotokol https dilakukan sebagai perbandingan dengan website berprotokol http yang belum dilakukan oleh peneliti terdahulu. Kondisi jaringan pada saat proses *capture* data cukup lancar pada pagi hari namun semakin siang jaringan lambat karena banyak pengguna yang menggunakan jaringan.

Dari hasil *capture* banyak paket data yang terrekam kemudian dilakukan analisis salah satu dari website yang diakses menggunakan jaringan tersebut, hasil monitor paket data dengan berbagai jenis protokol dan jenis interaksi yang terjadi masih menggunakan protokol HTTP yang dapat dengan mudah diketahui password, usename, waktu akses, kegiatan yang dilakukan, perangkat yang digunakan, dan masih banyak detail informasi lainnya. Sedangkan satu website lain sudah menggunakan protokol HTTPS yang artinya telah terenkripsi dan saat dianalisis interaksi detail paket hanya menampilkan kode acak yang sulit dibaca dan diketahui ketika dilakukan sniffing. Hal tersebut bisa saja menjadi sasaran pihak yang tidak bertanggungjawab menyalahgunakan bahkan melakukan kejahatan dengan informasi pribadi saat saling tukar data.

Diketahui pada analisis sebuah *website* lebih aman menggunakan protokol HTTPS yang sudah terenkripsi, apabila masih menggunakan HTTP informasi pribadi seperti *username*, *password* bahkan sampai detail data dengan mudahnya bisa diketahuai pada aktifitas yang sedang berjalan. Sehingga lebih aman menggunakan protokol HTTPS yang sudah terenkripsi dan aman. Website dengan protokol HTTPS mempunyai ciri terdapat logo gembok pada alamat website, sebaliknya pada website berprotokol HTTP tidak ada karena tidak enkripsi. Wireshark mempunyai kelebihan pada tindakan *sniffing* dan bisa menjadi acuan seorang pada bidang jaringan untuk memonitoring jaringan secara langsung dan analisisnya, untuk organisasi dapat dibentuk tim *Security Operation Center* (SOC) sebagai upaya tindakan *Cyber Crime.*

DAFTAR PUSTAKA

Hasan, 2009. Action Research : Desain Penelitian Integratif untuk Mengatasi Permasalahan Masyarakat. *AKSES: Jurnal Ekonomi dan*

Bisnis, 4(8), p.12.

Huda, I.A., 2020. Perkembangan Teknologi Informasi Dan Komunikasi (Tik) Terhadap Kualitas Pembelajaran Di Sekolah Dasar. Jurnal Pendidikan dan Konseling (JPDK), 2(1), pp.121–125. https://doi.org/10.31004/jpdk.v1i2.622.

Kusuma, M., Hariyadi, D., Kurniawan, H., Fikri, F. and Muttaqin, F., 2023. Pengujian sistem keamanan wireless router pada ekosistem rumah cerdas berbasis NIST sp800-115. Jurnal CoSciTech (Computer Science and Information Technology), [online] 4(3), pp.645–650. https://doi.org/10.37859/COSCITECH.V4I3.6315.

M. Askari Zakariah, Vivi Afriani, KH.M.Z., 2020. Metodologi Penelitian Kualitatif, kuantitatif, Action Research, Research and Development (R n D).

Majid, A. and Purwanto, T.D., 2021. Analisis Dan Monitoring Sniffing Paket Data Jaringan Lokal Bps Sumseldengan Network Analyzer Wireshark. Seminar Hasil Penelitian Vokasi (SEMHAVOK), 03(1), pp.102–109.

Novenzo Ihsana, A. and Maslan, A., 2020. Analisis Keamanan Jaringan Dari Serangan Paket Data Sniffing Di Pt Raden Syaid Kantor Pos Piayu Kota Batam. Jurnal Comasie, 03(05), pp.107–117.

Semiawan, P.D.C.R., n.d. Metode Penelitian Kualitatif. Grasindo.

Tafui, I.S., 2019. Analisi Performa Jaringan Pada Kampus I Itn Malang Menggunakan Metode Action Research.