LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

UNIT 3

PEMANTAUAN TRAFIK HTTP DAN HTTPS DENGAN MENGGUNAKAN WIRESHARK

Disusun oleh :

Nama	: Aura Nisa' Hidayat
NIM	: 21/482690/SV/19983
Kelas	: TRI A
Dosen Pengampu	: Anni Karimatul Fauziyyah, S.Kom., M.Eng.
Hari, Tanggal	: Selasa, 21 Februari 2023

PROGRAM STUDI DIV TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

2023

Laporan Praktikum Kamanan Informasi 1

Unit 3: Pemantauan Trafik HHTP dan HTTPS dengan Menggunakan *Wireshark*

I. TUJUAN

- Merekam dan menganalisa trafik http
- Merekam dan menganalisa trafik https

II. LATAR BELAKANG

HyperText Transfer Protocol (HTTP) adalah protokol lapisan aplikasi yang menyajikan data melalui browser web. Dengan HTTP, tidak ada perlindungan untuk pertukaran data antara dua perangkat yang berkomunikasi. Dengan HTTPS, enkripsi digunakan melalui algoritma matematika. Algoritma ini menyembunyikan arti sebenarnya dari data yang sedang dipertukarkan. Hal ini dilakukan melalui penggunaan sertifikat yang dapat dilihat nanti di lab ini. Terlepas dari HTTP atau HTTPS, hanya disarankan untuk bertukar data dengan situs web yang Anda percayai. Hanya karena sebuah situs menggunakan HTTPS tidak berarti itu adalah situs yang dapat dipercaya. Pelaku ancaman biasanya menggunakan HTTPS untuk menyembunyikan aktivitas mereka. Di lab ini, Anda akan menjelajahi dan menangkap lalu lintas HTTP dan HTTPS menggunakan Wireshark.

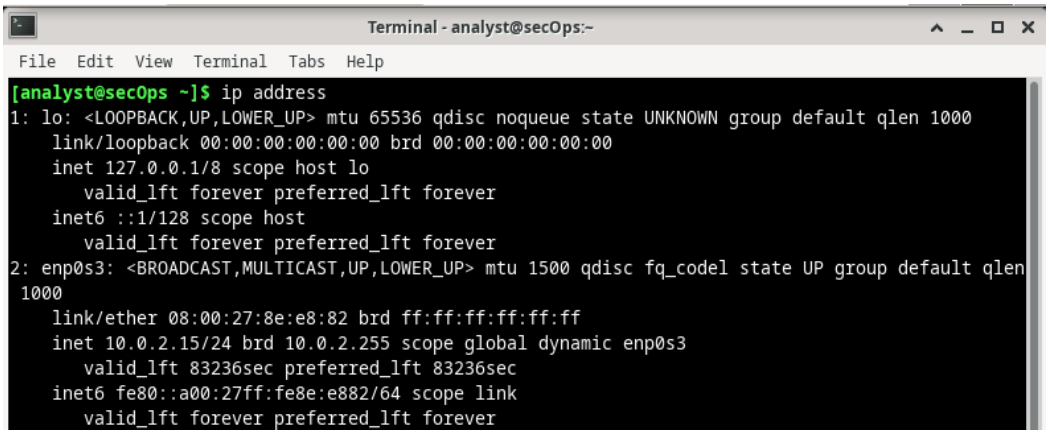
Wireshark adalah sebuah aplikasi *capture paket data* berbasis *open-source* yang berguna untuk memindai dan menangkap trafik data pada jaringan internet. Wireshark mendukung banyak format file paket capture/trace termasuk **.cap** dan **.erf**. Wireshark berfungsi untuk pekerjaan analisis jaringan. Cara kerjanya yaitu dengan ‘menangkap’ paket-paket data dari protokol-protokol yang berbeda dari berbagai tipe jaringan yang umum ditemukan di dalam trafik jaringan internet. Paket-paket data tersebut ‘ditangkap’ lalu ditampilkan di jendela hasil *capture* secara *real-time*. Cara kerja aplikasi ini sangat mirip dengan **tcpdump** namun memiliki tampilan antar muka yang lebih mudah dipahami dan lebih mudah dioperasikan.

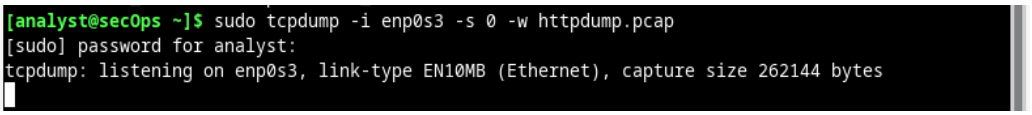
III. ALAT DAN BAHAN

- CyberOps Workstation VM
- Koneksi internet

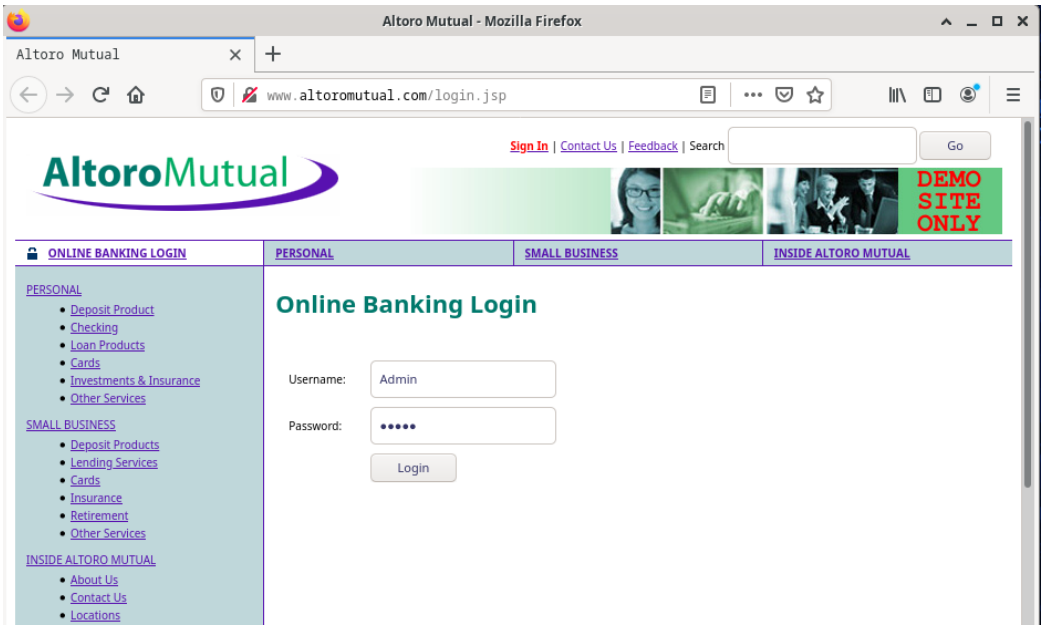
IV. INSTRUKSI KERJA

1. Menjalankan *virtual machine* dan login dengan *username* analyst dan *password* cybercops
2. Membuka terminal dan menjalankan **tcpdump**, kemudian melakukan pengecekan alamat IP.

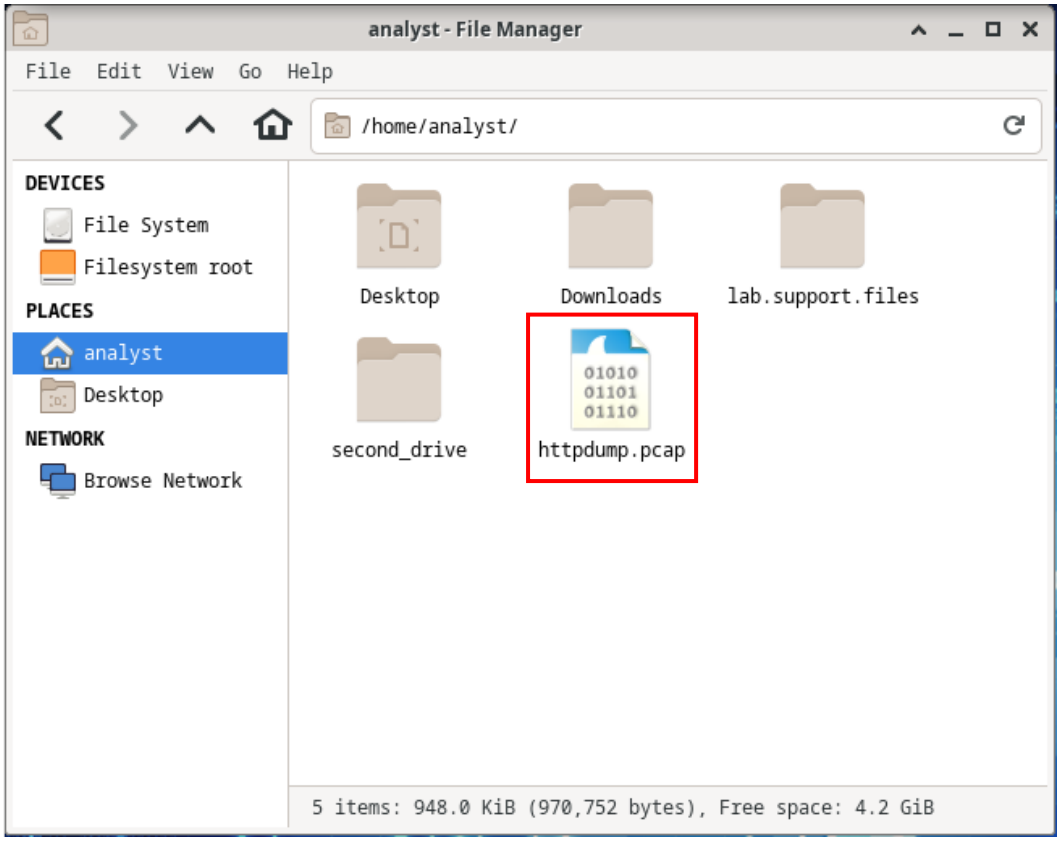




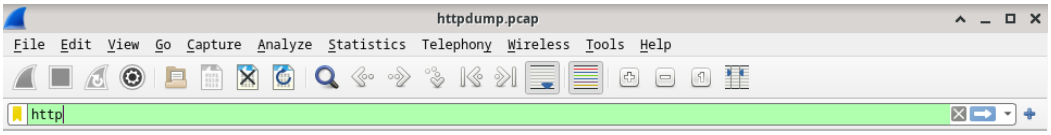
3. Selanjutnya membuka link http://www.altoromutual.com/login.jsp melalui *browser* di CyberOps Workstation VM.
   Username: Admin
   Password: Admin



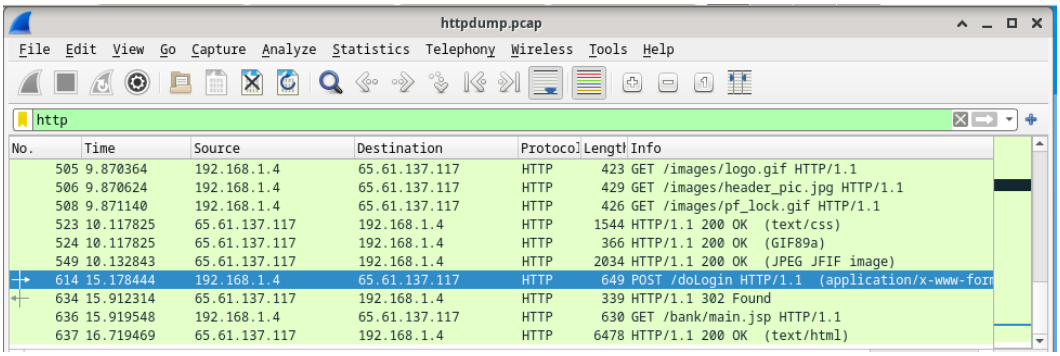
4. Kemudian merekam paket **HTTP**
   tcpdump yang dieksekusi pada langkah sebelumnya disimpan dalam file Bernama **httpdump.pcap** yang terletak pada folder /home/analyst/.



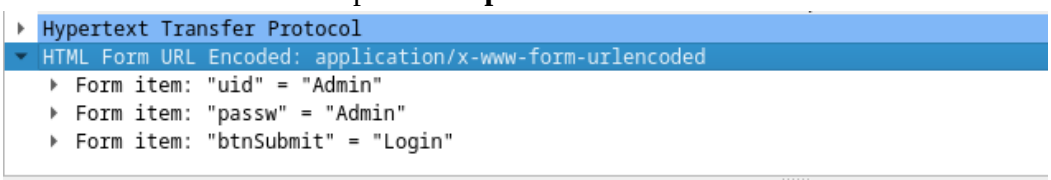
5. Lalu filter **http** dan klik *apply*.



6. Pilih **POST.**



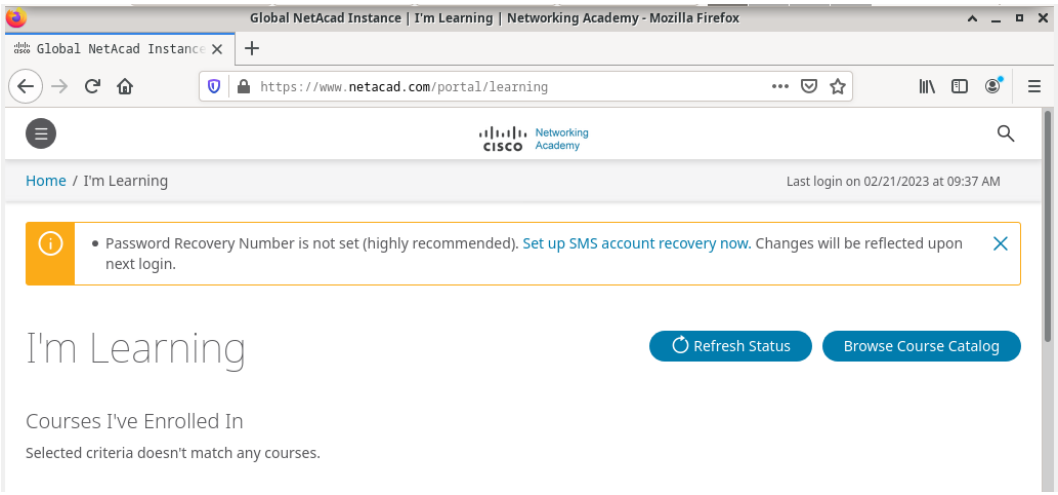
7. Melakukan analisis terhadap **uid** dan **passw**



8. Berganti dengan merekam paket **HTTPS**

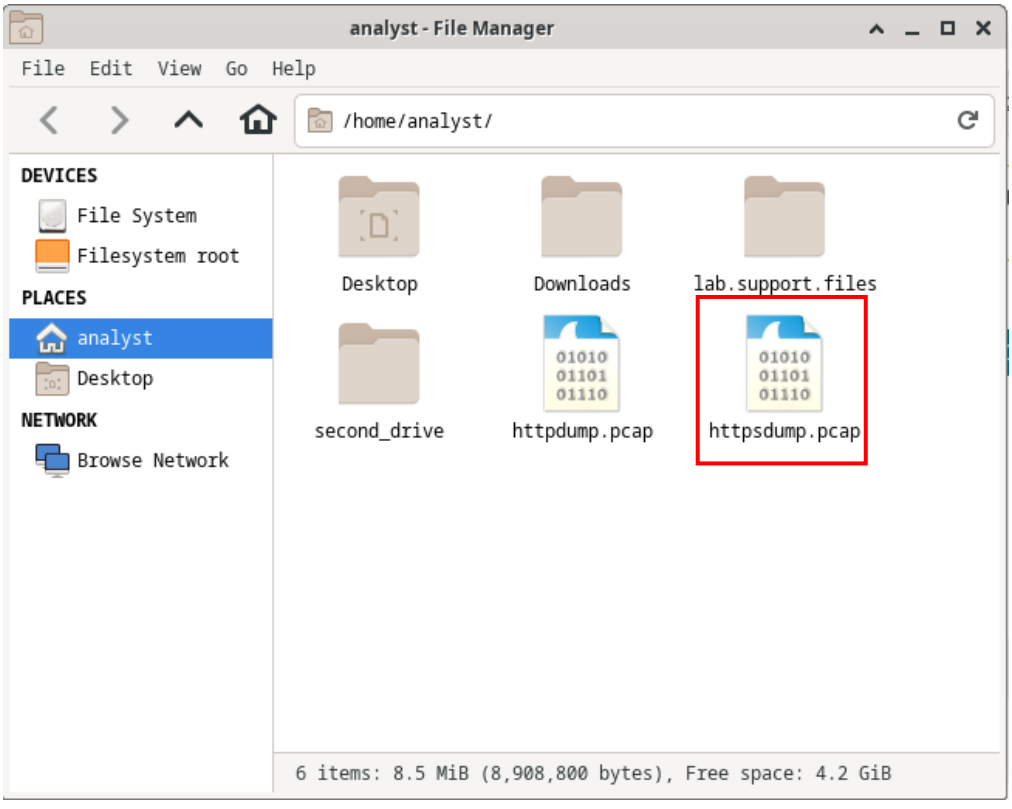
```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

9. Membuka link https://www.netacad.com/ melaui *browser* pada CyberOps Workstation VM.

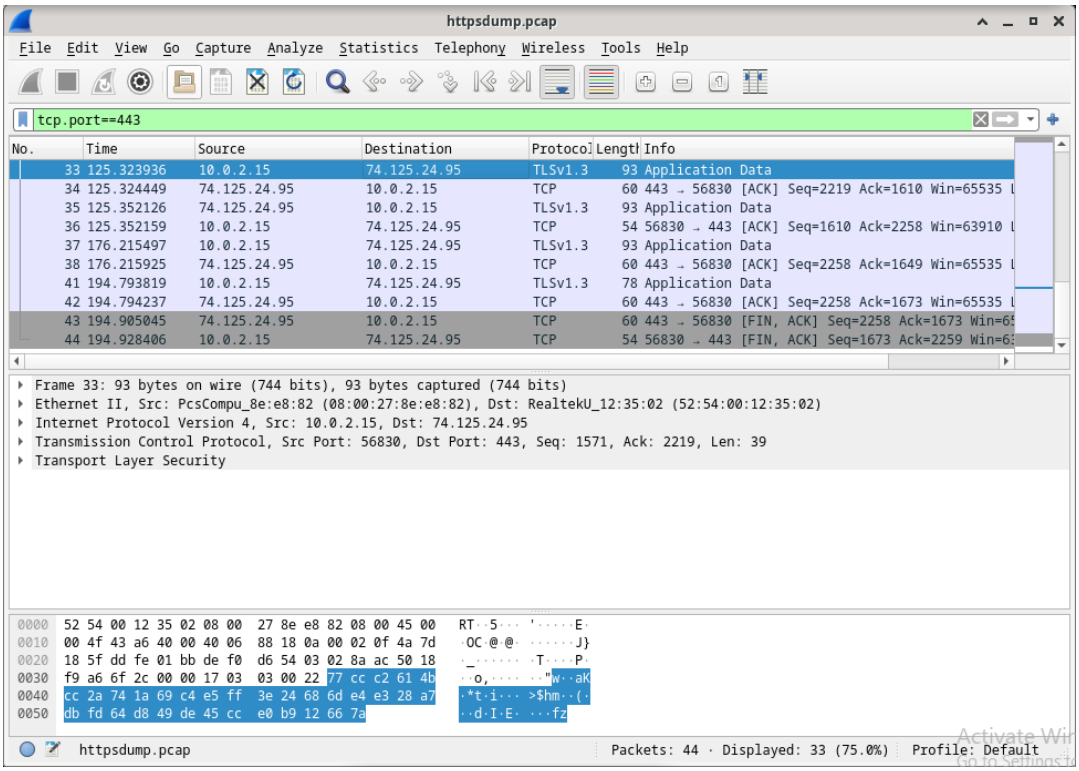


10. Kemudian login dengan memasukkan username beserta password.

11. Lalu melihat rekaman paket HTTPS, tcpdump yang dieksekusi pada Langkah sebelumnya kemudian disimpan kedalam file bernama **httpsdump.pcap** pada folder /home/analyst/.



12. Melakukan filter **tcp.port==443** dan pilih ***Application Data.***



V. PEMBAHASAN

Tcpdump merupakan sebuah alat atau *tool packet sniffing* dan *packet analyzing* untuk system administrator yang tujuannya memecahkan masalah konektivitas di Linux. *Tool* ini dapat digunakan untuk menangkap (*capture*), memfilter (*filter*), dan menganalisis lalu lintas jaringan (*analyze network traffic*) seperti paket TCP/IP. Tcpdump pada umumnya digunakan sebagai alat keamanan karena tcpdump menyimpan informasi yang di tangkap dalam file *pcap* dan dapat dibuka melalui *wireshark.*

Pada praktikum ini dibagian pengecekan alamat IP terdapat perintah:

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
```

Yang mana perintah ini akan memulai tcpdump dan merekam *network traffic* pada interface **enp0s3** sebesar 262144 byte. Perintah **-i** berfungsi untuk memenentukan interface pada enp0s3, kemudian perintah **-s** untuk menentukan panjang *snapshot* pada setiap paket. Selanjutnya terdapat perintah **-w** yang berfungsi untuk menulis hasil perintah tcpdump ke file. Kemudian login ke Altoro Mutual untuk menambahkan file ekstensi semua system operasi dan aplikasi dapat merekam file ***httpdump.pcap*** lalu akan dicetak ke file manager. Rekaman paket HTTP menunjukkan pesan informasi mengenai “uid”, “password”, beserta “btnSubmit” untuk URL encoded: application/xwww-form-urlencoded.

Begitu pula untuk merekam paket ***https*** dilakukan hal yang sama dengan perintah:

```
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap
```

Perintah yang digunakan sama, untuk merekam paket ***https*** perlu melakukan login Netacad melalui *browser* di CyberOps Workstation VM. Setelah login secara otomatis paket https terekam dan tersimpan kedalam file manager dengan nama ***httpsdump.pcap***. Langkah berikutnya melakukan filter port 443 yang merupakan port standar untuk layanan HTTPS. Port 443 aman untuk melakukan transaksi, karena terbukti bahwa 95% situs aman menggunakan port 443 untuk transfer.

VI. KESIMPULAN

Dari praktikum keamanan informasi kali ini dapat disimpulkan bahwa:

1. Tcpdump merupakan sebuah alat atau *tool* untuk memecahkan masalah konektivitas di Linux.
2. Tcpdump digunakan untuk menangkap (*capture*), memfilter (*filter*), dan menganalisis lalu lintas jaringan.
3. *HyperText Transfer Protocol* (HTTP) adalah protokol lapisan aplikasi yang menyajikan data melalui browser.
4. *HyperText Transfer Protocol Secure* (HTTPS) menggunakan algoritma matematika.
5. Wireshark adalah sebuah aplikasi *capture paket data* berbasis *open-source* yang berguna untuk memindai dan menangkap trafik data pada jaringan internet.

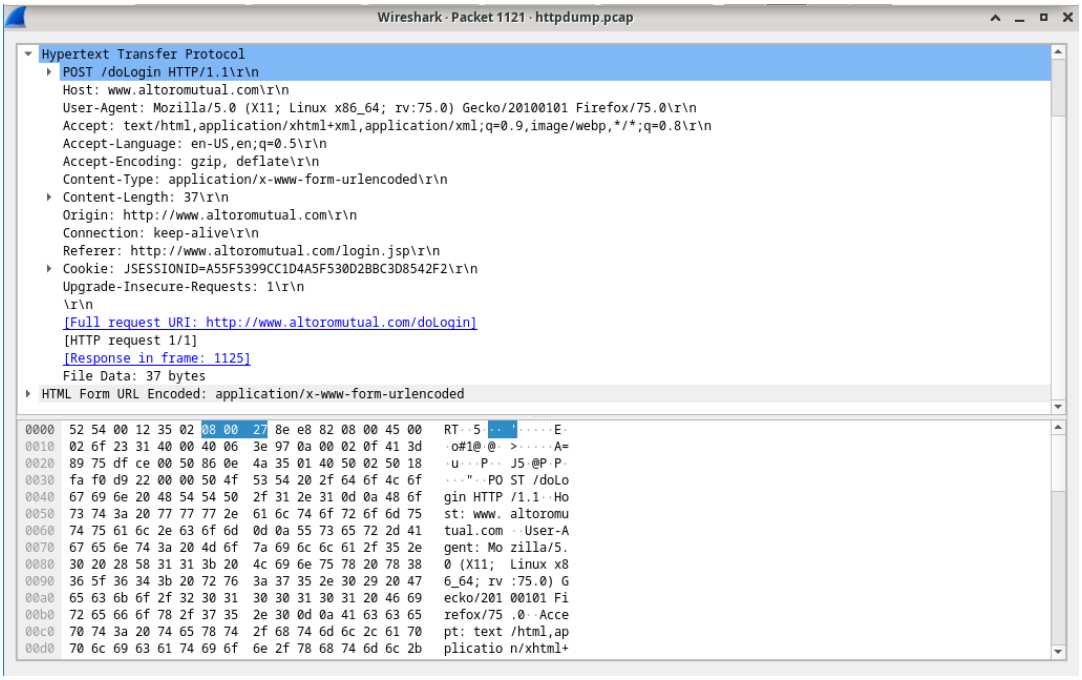
DAFTAR PUSTAKA

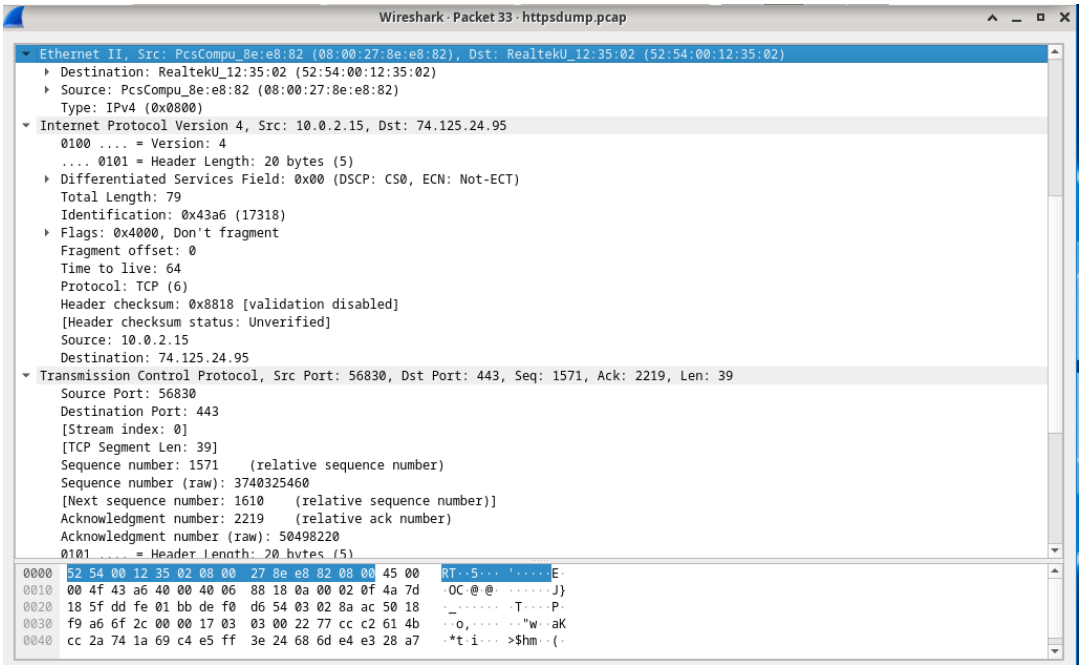
Hanim, N. (2021, Januari 9). *Cara Menggunakan Perintah tcpdump di Linux*. Retrieved Februari 26, 2023, from Belajar Linux ID: https://belajarlinux.id/cara-menggunakan-perintah-tcpdump-di-linux/

Saputro, N. (2022, Juni 11). *Kenali Pengertian Wireshark Beserta Fungsi dan Cara Kerjanya, Lengkap!* Retrieved Februari 26, 2023, from Nesabamedia: https://www.nesabamedia.com/pengertian-wireshark/

What is Port 443? A Technical Guide for HTTPS Port 443. (n.d.). Retrieved Februari 26, 2023, from SSL2BUY: https://www.ssl2buy.com/wiki/port-443#:~:text=Port%20443%20is%20used%20explicitly,port%20443%20for%20secure%20transfers.

LAMPIRAN


Wireshark · Packet 1121 · httpdump.pcap
Hypertext Transfer Protocol
POST /doLogin HTTP/1.1\r\n
Host: www.altoromutual.com\r\n
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:75.0) Gecko/20100101 Firefox/75.0\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
Accept-Language: en-US,en;q=0.5\r\n
Accept-Encoding: gzip, deflate\r\n
Content-Type: application/x-www-form-urlencoded\r\n
Content-Length: 37\r\n
Origin: http://www.altoromutual.com\r\n
Connection: keep-alive\r\n
Referer: http://www.altoromutual.com/login.jsp\r\n
Cookie: JSESSIONID=A55F5399CC1D4A5F530D2BBC3D8542F2\r\n
Upgrade-Insecure-Requests: 1\r\n
\r\n
[Full request URI: http://www.altoromutual.com/doLogin]
[HTTP request 1/1]
[Response in frame: 1125]
File Data: 37 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded


Wireshark · Packet 33 · httpsdump.pcap
Ethernet II, Src: PcsCompu_8e:e8:82 (08:00:27:8e:e8:82), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
Destination: RealtekU_12:35:02 (52:54:00:12:35:02)
Source: PcsCompu_8e:e8:82 (08:00:27:8e:e8:82)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 74.125.24.95
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 79
Identification: 0x43a6 (17318)
Flags: 0x4000, Don't fragment
Fragment offset: 0
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x8818 [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.15
Destination: 74.125.24.95
Transmission Control Protocol, Src Port: 56830, Dst Port: 443, Seq: 1571, Ack: 2219, Len: 39
Source Port: 56830
Destination Port: 443
[Stream index: 0]
[TCP Segment Len: 39]
Sequence number: 1571 (relative sequence number)
Sequence number (raw): 3740325460
[Next sequence number: 1610 (relative sequence number)]
Acknowledgment number: 2219 (relative ack number)
Acknowledgment number (raw): 50498220