

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1
Unit 3 – Pemantauan Trafik HTTP dan HTTPS dengan menggunakan
Wireshark



DISUSUN OLEH

Nama : Sofiyanatul Munawaroh
NIM : 21/474781/SV/19035
Hari, Tanggal : Selasa, 21 Februari 2023
Kelas : RI4AA

LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI
REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023

Praktikum Keamanan Informasi 1

Unit 3 – c

I. Tujuan

- Merekam dan menganalisis trafik HTTP.
- Merekam dan menganalisis 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.

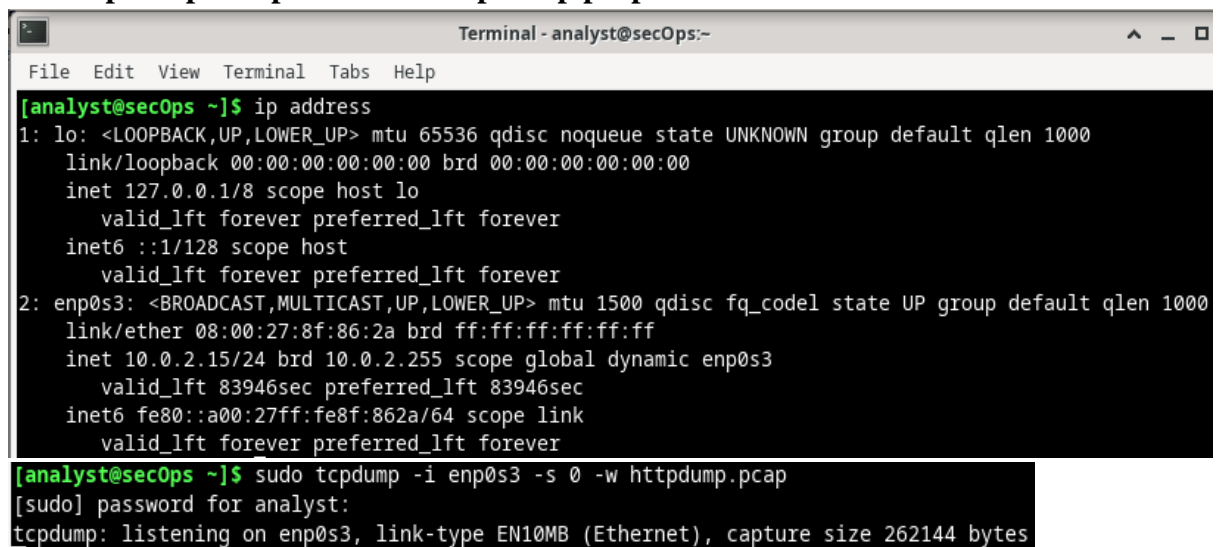
Terlepas dari HTTP atau HTTPS, hanya disarankan untuk bertukar data dengan situs web yang Anda percayai. Hanya karena sebuah situs menggunakan HTTPS tidak berarti itu adalah situs yang dapat dipercaya. Pelaku ancaman biasanya menggunakan HTTPS untuk menyembunyikan aktivitas mereka.

III. Alat dan Bahan

- CyberOps Workstation Virtual Machine.
- Wireshark.
- Koneksi Internet.

IV. Instruksi Kerja

1. Jalankan VM dan *Login*.
2. Buka terminal dan menjalankan **tcpdump** untuk merekam trafik http dengan perintah **sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap**.

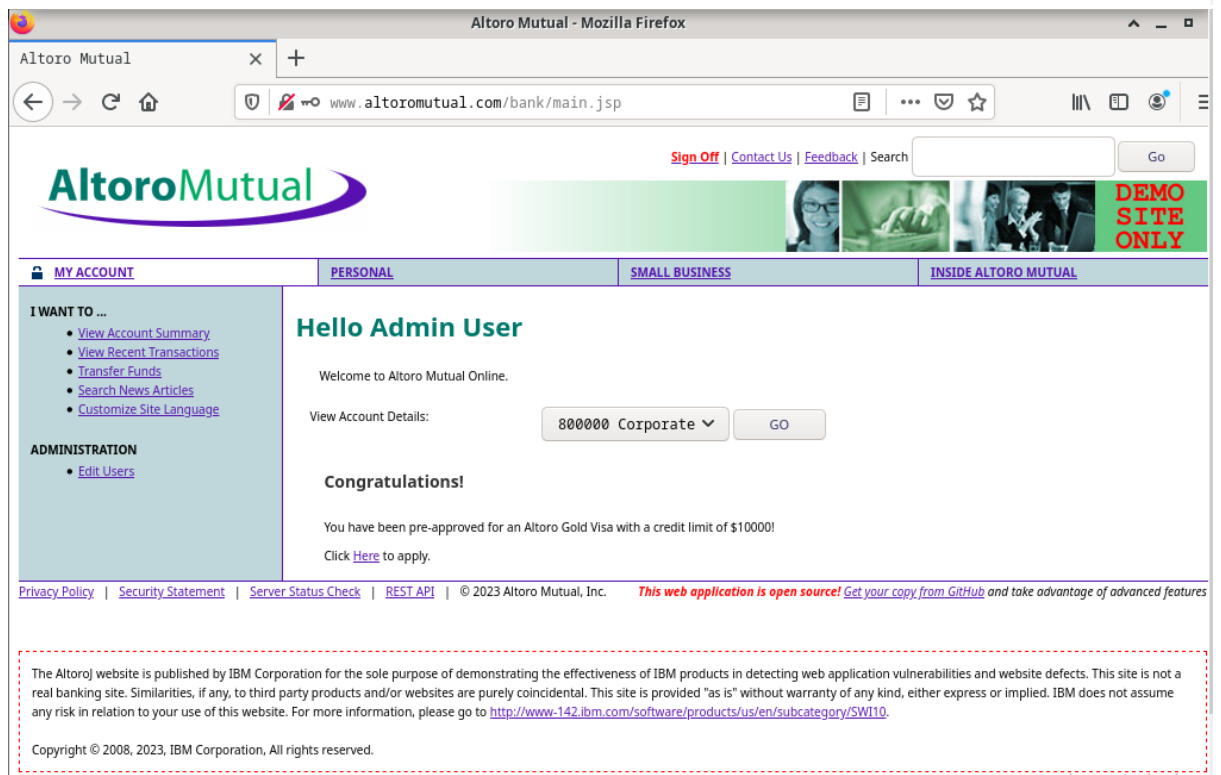
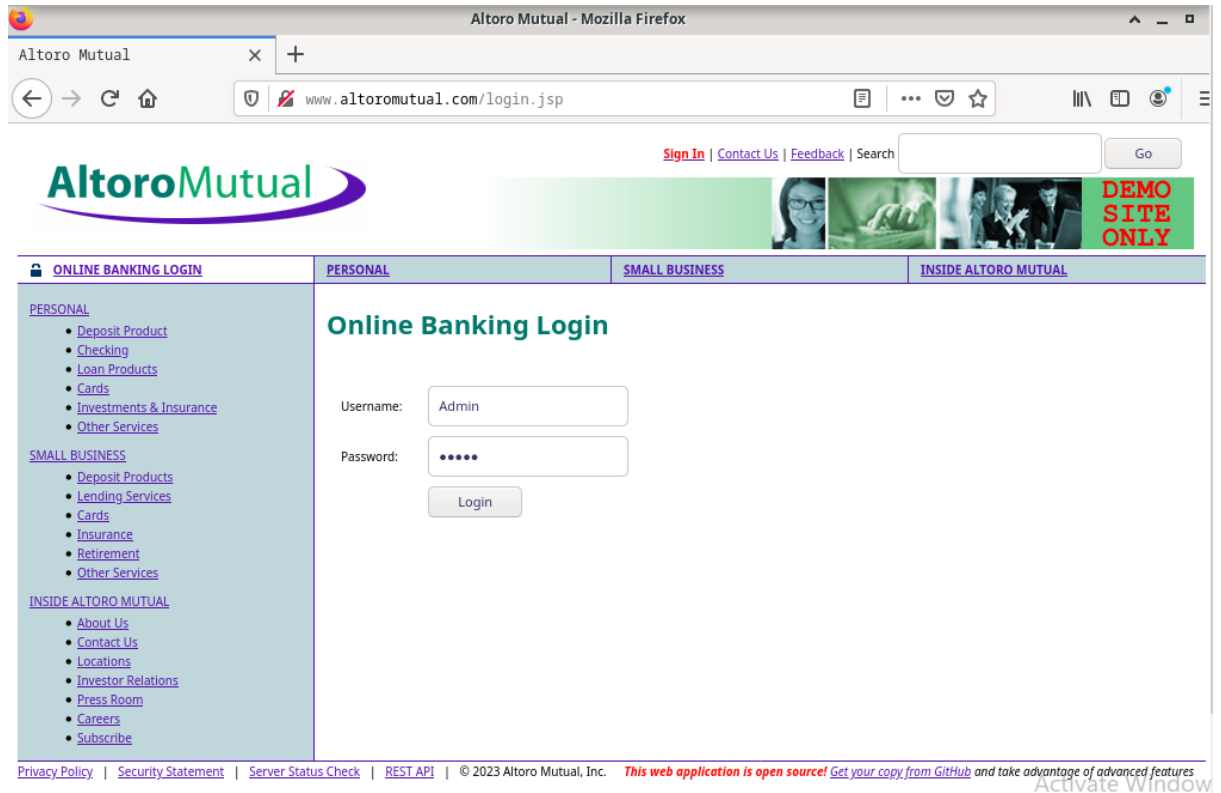


```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:8f:86:2a brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic enp0s3
        valid_lft 83946sec preferred_lft 83946sec
    inet6 fe80::a00:27ff:fe8f:862a/64 scope link
        valid_lft forever preferred_lft forever

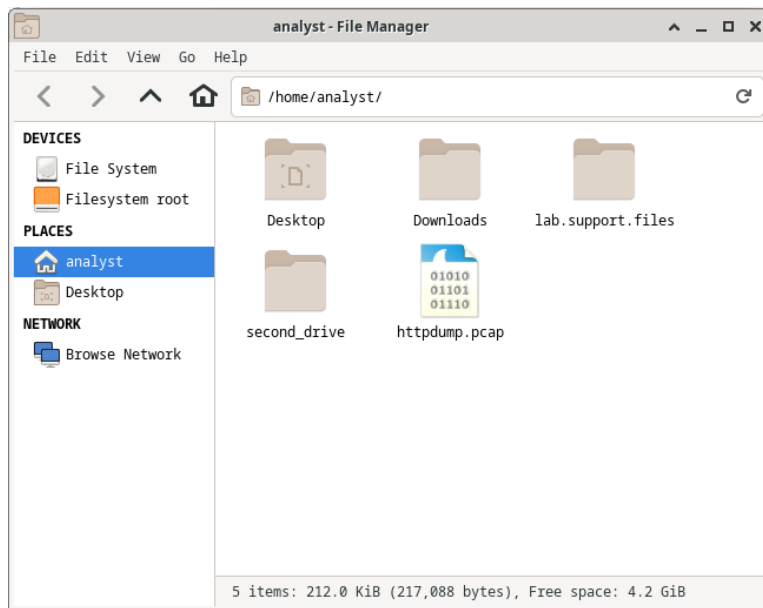
[analyst@secOps ~]$ sudo tcpdump -i enp0s3 -s 0 -w httpdump.pcap
[sudo] password for analyst:
tcpdump: listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

3. Buka link <http://www.altoromutual.com/login.jsp> melalui browser di CyberOps Workstation VM. Login dengan user dan password = **Admin**.

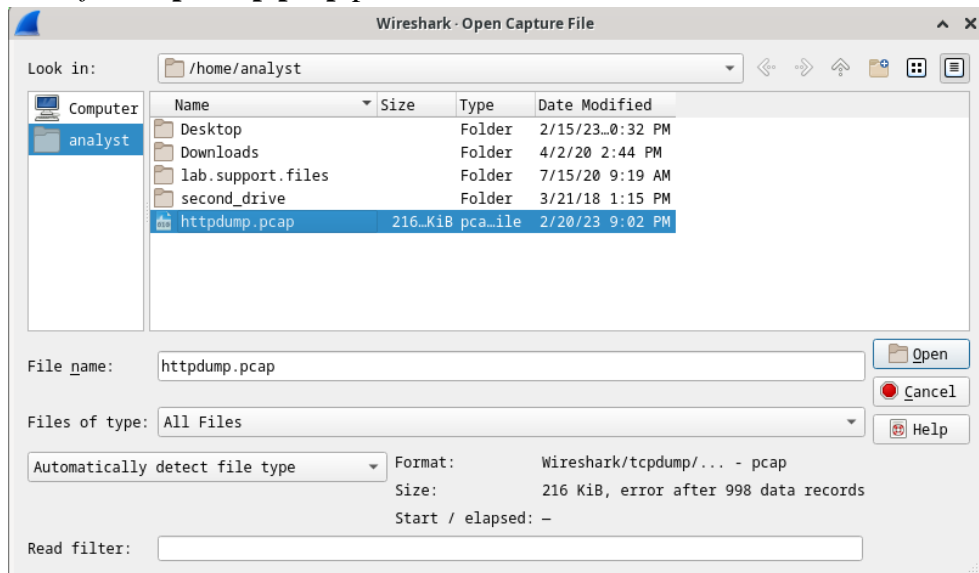


4. Merekam Paket HTTP.

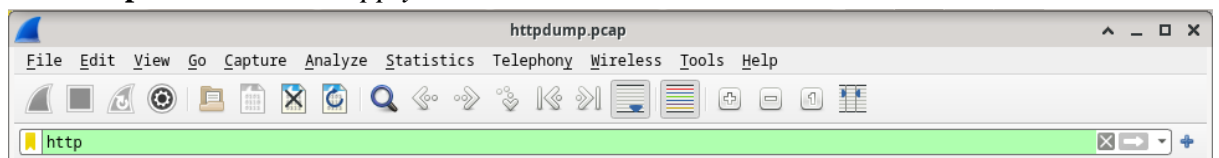
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan ke dalam file bernama httpdump.pcap. File ini terletak pada folder /home/analyst/.



5. Buka file **httpdump.pcap** pada Wireshark.



6. Filter **http** kemudian klik *Apply*.



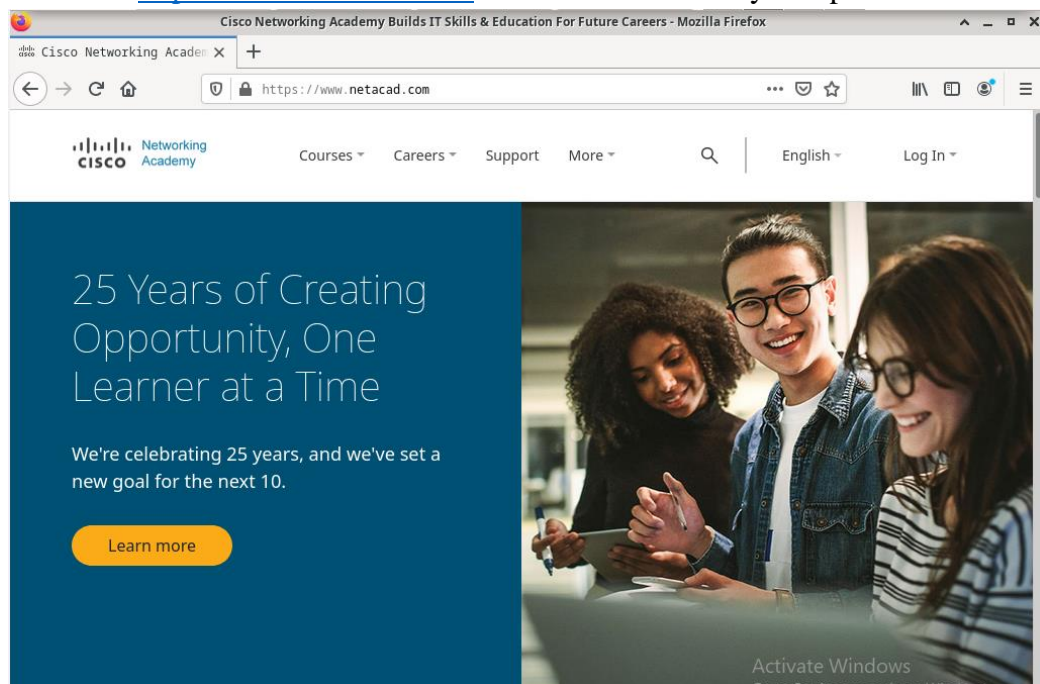
7. Pilih **POST**, lalu klik pada **HTML Form Url Encoded...** untuk mengetahui **uid** dan **password**.

No.	Time	Source	Destination	Protocol	Length	Info
510	26.159734	10.0.2.15	65.61.137.117	HTTP	359	GET /favicon.ico HTTP/1.1
520	26.390437	65.61.137.117	10.0.2.15	HTTP	7132	HTTP/1.1 404 Not Found (text/html)
653	59.997057	10.0.2.15	34.107.221.82	HTTP	342	GET /success.txt HTTP/1.1
657	60.777924	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
664	60.797512	10.0.2.15	34.107.221.82	HTTP	347	GET /success.txt?ipv4 HTTP/1.1
679	61.494383	34.107.221.82	10.0.2.15	HTTP	270	HTTP/1.1 200 OK (text/plain)
895	130.408107	10.0.2.15	65.61.137.117	HTTP	637	POST /doLogin HTTP/1.1 (application/x-www-form-urlencoded)
899	130.690978	65.61.137.117	10.0.2.15	HTTP	327	HTTP/1.1 302 Found
901	130.696155	10.0.2.15	65.61.137.117	HTTP	618	GET /bank/main.jsp HTTP/1.1
907	131.214531	65.61.137.117	10.0.2.15	HTTP	3546	HTTP/1.1 200 OK (text/html)

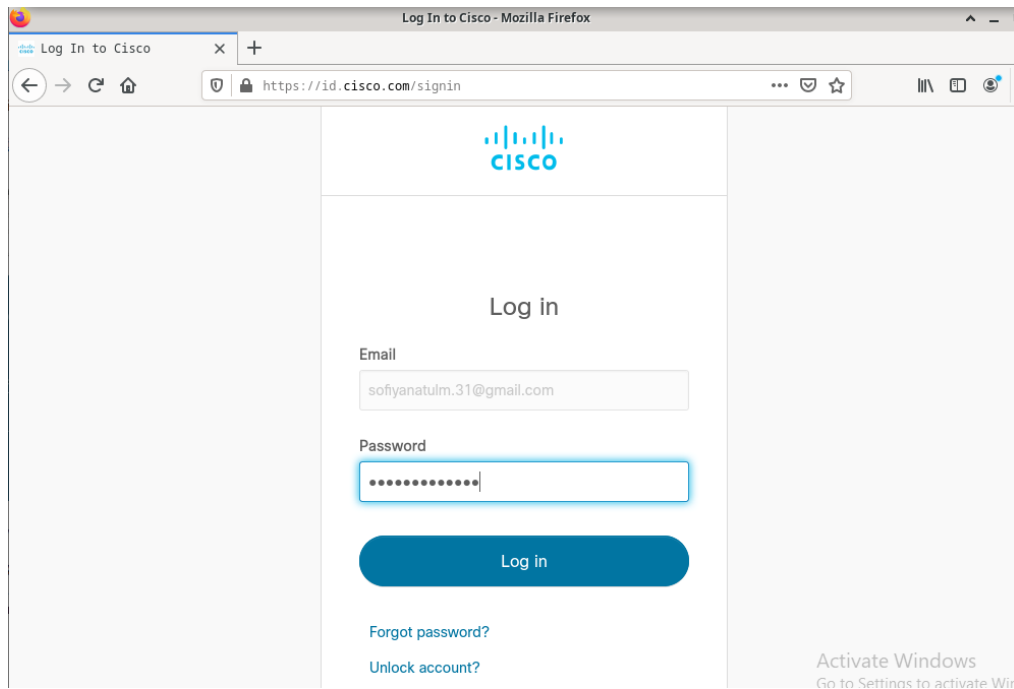
▶ Frame 895: 637 bytes on wire (5096 bits), 637 bytes captured (5096 bits)
 ▶ Ethernet II, Src: PcsCompu_8f:86:2a (08:00:27:8f:86:2a), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)
 ▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117
 ▶ Transmission Control Protocol, Src Port: 54788, Dst Port: 80, Seq: 1, Ack: 1, Len: 583
 ▶ Hypertext Transfer Protocol
 ▶ HTML Form URL Encoded: application/x-www-form-urlencoded
 ▶ Form item: "uid" = "Admin"
 ▶ Form item: "passwd" = "Admin"
 ▶ Form item: "btnSubmit" = "Login"

8. Kemudian hentikan proses perekaman *traffic* http dengan menggunakan kombinasi tombol **ctrl+c**.
9. Buka kembali terminal dan jalankan **tcpdump** untuk merekam trafik https dengan perintah **sudo tcpdump -i enp0s3 -s 0 -w httpsdump.pcap**.

```
[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
```
10. Buka link <https://www.netacad.com/> melalui *browser* di *CyberOps Workstation VM*.

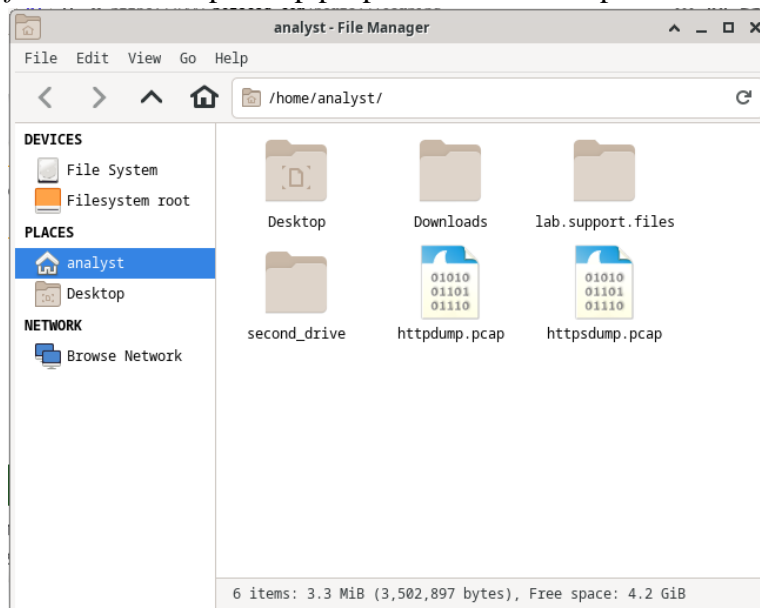


11. *Login* menggunakan akun netacad yang dimiliki.

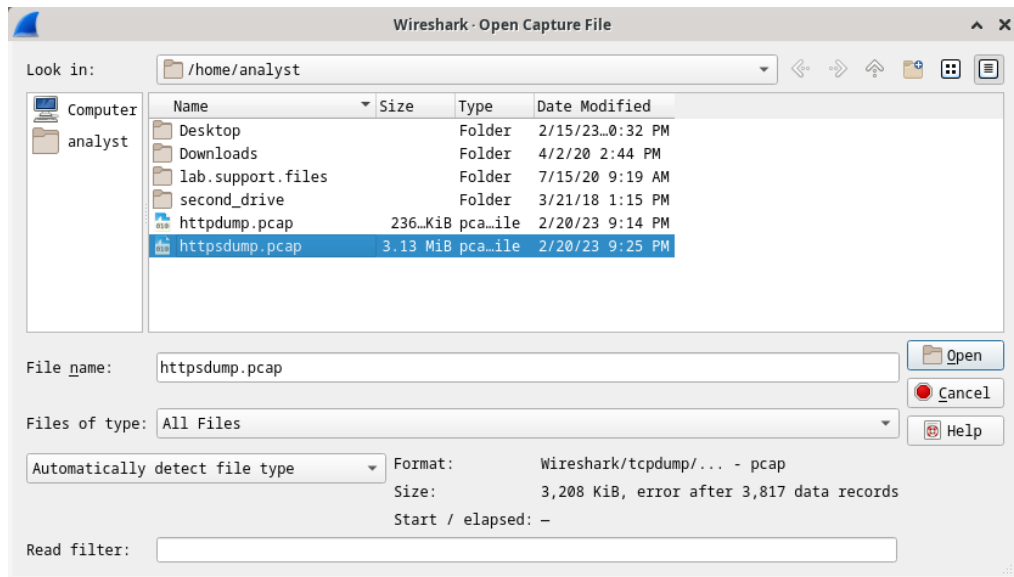


12. Merekam Paket HTTPS.

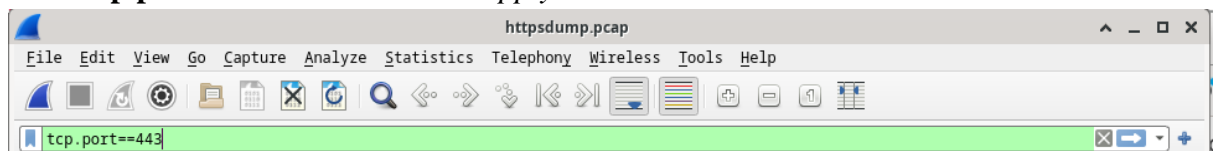
Tcpdump yang dieksekusi pada langkah sebelumnya, kemudian disimpan ke dalam *file* bernama **httpsdump.pcap**. *File* ini terletak pada folder **/home/analyst/**.



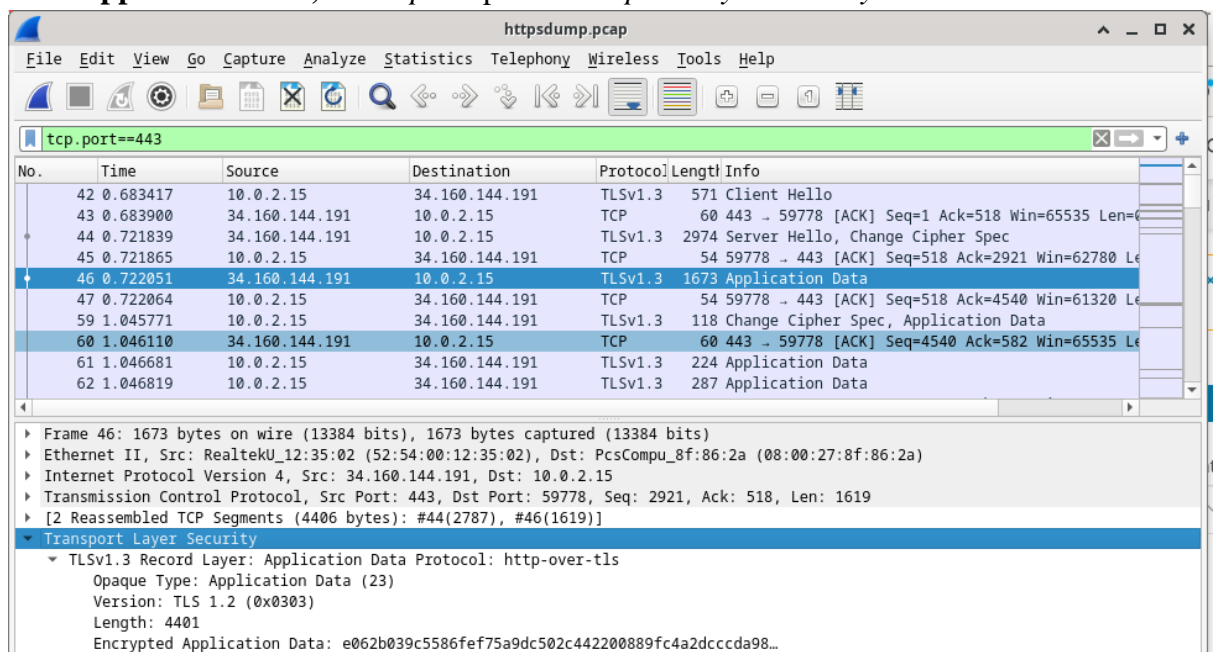
13. Buka *file* **httpsdump.pcap** pada Wireshark.



14. Filter **tcp.port==443** kemudian klik *Apply*.



15. Pilih **Application Data**, lalu *expand* pada *Transport Layer Security*.



V. Hasil dan Pembahasan

Pada pertemuan ini (Unit 3- Pemantauan Trafik HTTP dan HTTPS dengan menggunakan Wireshark) dilakukan perekaman trafik jaringan yang dapat diakses menggunakan Wireshark, jaringan yang direkam pada praktikum ini adalah HTTP dan HTTPS. *Syntax* atau perintah yang digunakan untuk menjalankan perekaman trafik atau tcpdump yaitu **sudo tcpdump -i enp0s3 -s 0 -w [nama file].pcap**. Setelah dijalankan, kita perlu mengakses suatu *web* yang menggunakan protokol jaringan yang ingin direkam. Pertama yaitu melakukan perekaman HTTP, maka yang perlu diakses adalah

web yang menggunakan protokol HTTP (pada praktikum ini mengakses *web* <http://www.altoromutual.com/login.jsp>). Setelah itu, tcpdump yang dieksekusi sebelumnya telah tersimpan ke dalam *file* bernama *httpdump.pcap* yang akan dibuka menggunakan Wireshark. Kemudian, perlu dilakukan *filtering traffic* "http" pada Wireshark dan cari trafik yang mengandung POST. Karena pada saat mengakses *web* "AltoroMutual" kita memasukkan *user-id* dan *password*, maka pada hasil *traffic* POST tersebut dapat dilihat terdapat UID atau *user-id* dan *Password* yang kita gunakan sebelumnya saat mengakses *web* dengan protokol HTTP tersebut. Hal ini dapat terjadi karena protokol HTTP tidak memiliki enkripsi dari data yang kita gunakan untuk mengakses suatu situs.

Selanjutnya, kita akan merekam trafik jaringan dengan protokol HTTPS. Oleh karena itu, jalankan kembali *syntax* tcpdump tetapi dengan nama *file* yang berbeda yaitu *httpsdump.pcap*. Kemudian akses *web* yang menggunakan protokol HTTPS (pada praktikum ini mengakses *web* <https://www.netacad.com/>). Setelah itu, tcpdump yang dieksekusi sebelumnya telah tersimpan ke dalam *file* bernama *httpsdump.pcap* yang akan dibuka menggunakan Wireshark. Kita perlu melakukan *filtering traffic* "tcp.port==443" pada Wireshark karena *port* HTTPS adalah 443 dan cari trafik yang *Application Data*. Karena *web* yang diakses menggunakan protokol HTTPS, maka dari hasil perekaman *user-id* dan *password* akan terenkripsi. Hal tersebut dikarenakan pada protokol HTTPS menggunakan SSL/TLS untuk mengenkripsi koneksi antara *web browser* dengan *web server*.

VI. Kesimpulan

1. HTTP tidak memiliki enkripsi dari data karena belum memanfaatkan sertifikat keamanan SSL.
2. HTTPS sudah menggunakan SSL/TLS untuk enkripsi data sehingga lebih *secure*.

VII. Daftar Pustaka

Wijayanti, Naning. (2022). *Perbedaan HTTP dan HTTPS: Ini Penyebab HTTPS Lebih Aman!*. Diakses pada 26 Februari dari <https://www.niagahoster.co.id/blog/perbedaan-http-dan-https/>