

Tapping Login Website Menggunakan Wireshark
Tugas 3 Keamanan Jaringan Komputer



Oleh :

Siti Aisyah

09011181621024

Kelas : SK8P Indralaya

Dosen pengampu : Deris Stiawan, M.T., Ph.D.

Jurusan Sistem Komputer
Fakultas Ilmu Komputer
Universitas Sriwijaya

-Tapping Website

1. Website Http (unsecured)

- a. Contoh website yang tidak menggunakan http



Home

Pengguna tidak ditemukan

Login

Nama pengguna

Password

Username (untuk login sbg PNS) : Nip Baru 18 digit.
Password (untuk login sbg PNS) : Nama depan PNS (sebelum spasi pertama) dengan huruf kecil.
Contoh: Untuk PNS a/n Aulia Pradipta, passwordnya adalah "aulia".

Login

- b. Input data ke dalam kolom username dan password (tidak masalah data valid atau tidak).



BKN

Badan Kepegawaian Negara

🏠 Home

Pengguna tidak ditemukan

Login

Nama pengguna

ichaicha

Password

.....|

Username (untuk login sbg PNS) : Nip Baru 18 digit.

Password (untuk login sbg PNS) : Nama depan PNS (sebelum spasi pertama) dengan huruf kecil.

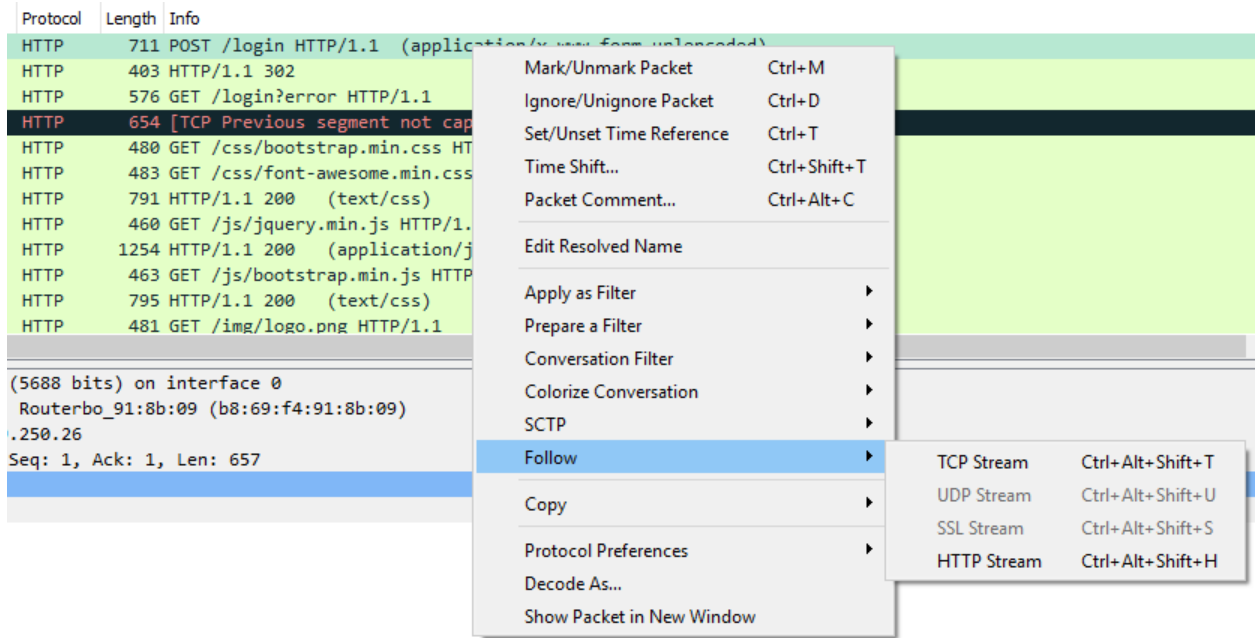
Contoh: Untuk PNS a/n Aulia Pradipta, passwordnya adalah "aulia".

Login

- Jalankan Capture Wireshark terlebih dahulu sebelum menekan "submit"
- Lalu hentikan capture wireshark.
- Lakukan analisis terhadap packet yang telah di capture. Pertama filter packet http menggunakan "http.request.method==post".

Source	Destination	Protocol
172.17.178.228	103.89.250.26	HTTP

- Pada bagian info akan terdapat tulisan .login atau /login. Atau dalam kasus ini /index.asp. Kemudian klik kanan pada packet tersebut lalu follow > tcp stream.



- g. Selanjutnya akan muncul window sebagai berikut. Username dan password akan tampil dengan jelas dalam text tersebut.

```
Wireshark · Follow TCP Stream (tcp.stream eq 1) · Wi-Fi

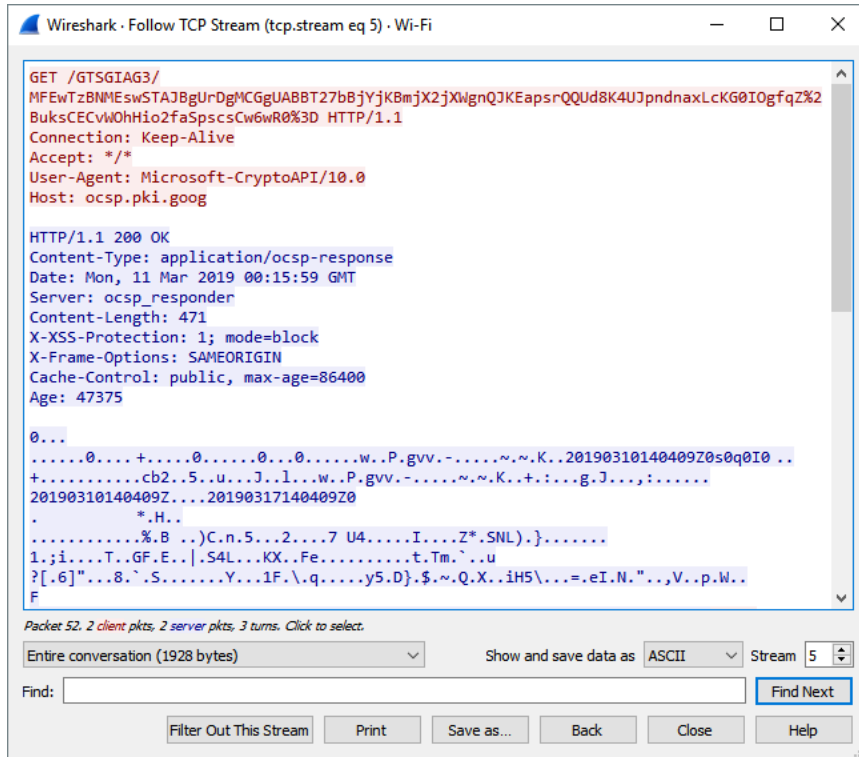
POST /login HTTP/1.1
Host: ip-jasn.bkn.go.id
Connection: keep-alive
Content-Length: 37
Cache-Control: max-age=0
Origin: http://ip-jasn.bkn.go.id
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 UBr
7.0.185.1002 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://ip-jasn.bkn.go.id/login
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.8
Cookie: JSESSIONID=1F33CA160D0E22463B7EABE8E1468752

username=ichaicha&password=SitiAisyahHTTP/1.1 302
Server: nginx/1.10.2
Date: Mon, 11 Mar 2019 06:17:47 GMT
Content-Length: 0
Connection: keep-alive
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
X-Frame-Options: DENY
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Location: http://ip-jasn.bkn.go.id/login?error

GET /login?error HTTP/1.1
Host: ip-jasn.bkn.go.id
Connection: keep-alive
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/55.0.2883.87 UBr
7.0.185.1002 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Referer: http://ip-jasn.bkn.go.id/login
```

2. Website Https (secured)

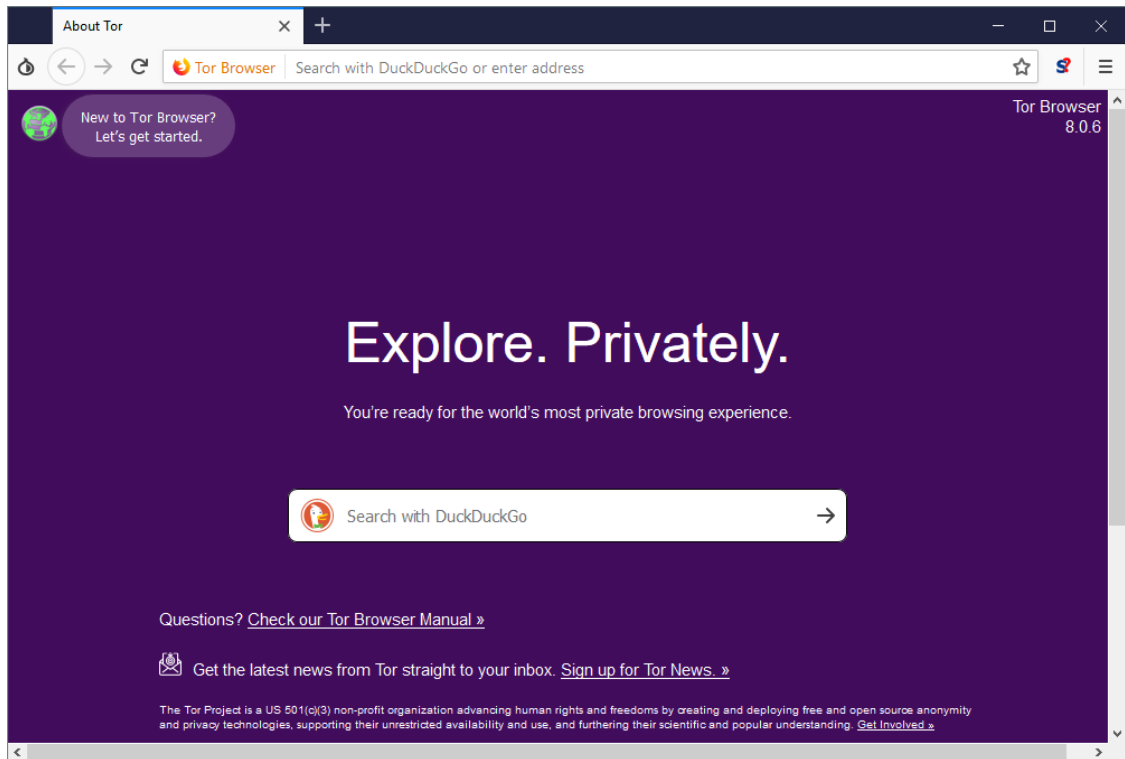
- a. Tampilan TCP stream ketika melakukan login ke website yang terenkripsi.



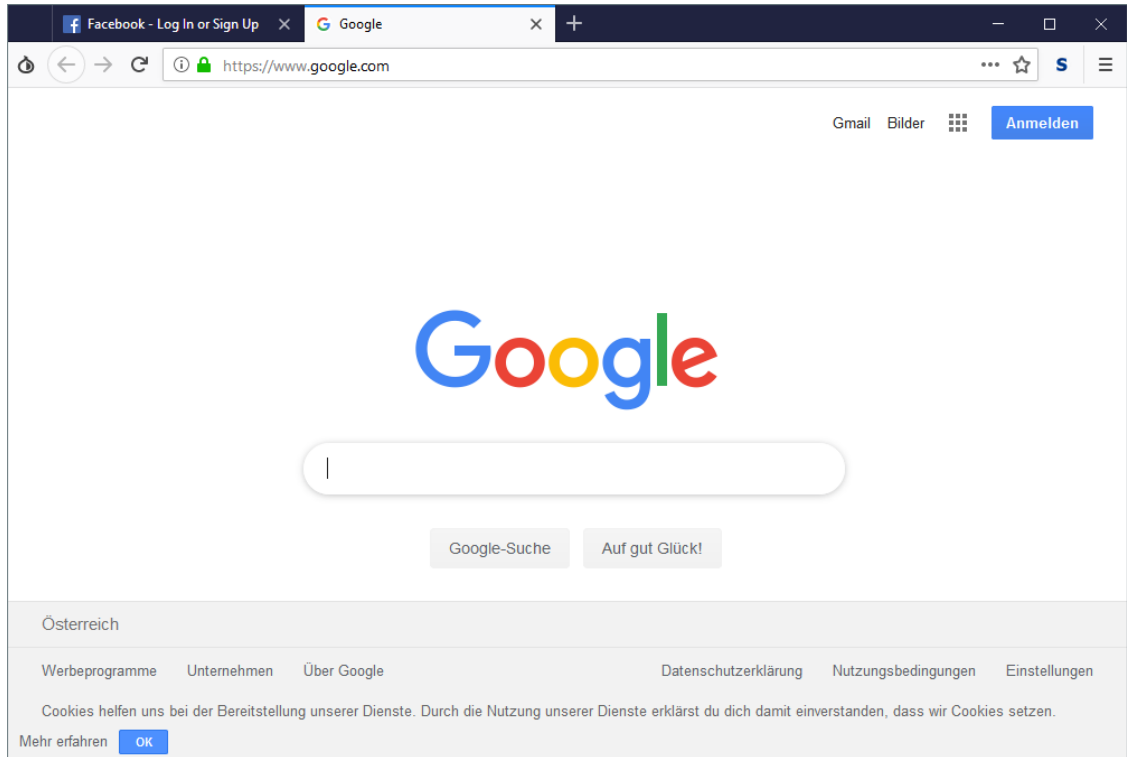
Gambar 1 Data capture yang ditampilkan hanya akan nampak seperti susunan karakter yang acak, sehingga tidak dapat dibaca oleh attacker.

-Akses Web Melalui Tor

- Jalankan Tor Browser dan pastikan sambungan berhasil.

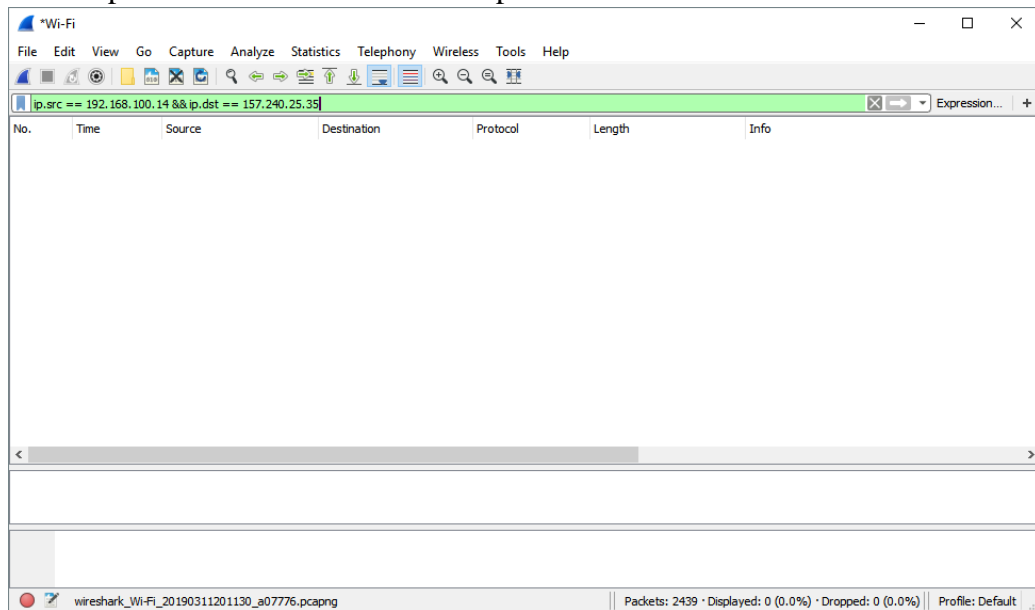


- b. Mulai capture packet menggunakan Wireshark.
- c. Pergi ke web yang diinginkan, misalnya facebook atau google.
 - facebook.com [157.240.25.35]
 - google.com [216.239.38.120]
 - komputer lokal [192.168.100.14]



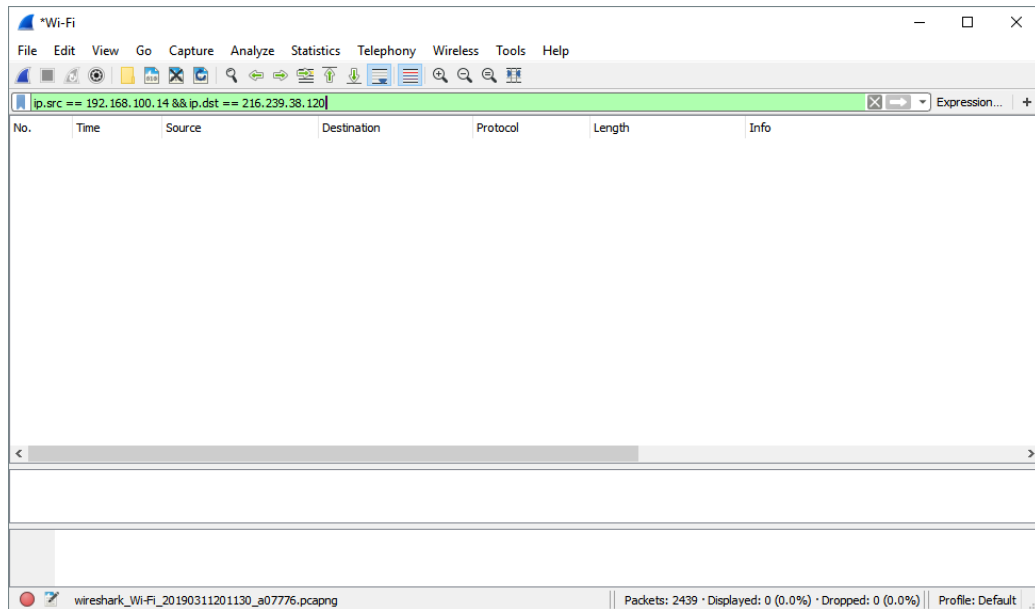
d. Analisis hasil capture.

- Filter “ip.src == 192.168.100.14 && ip.dst == 157.240.25.35”



Gambar 2 Tidak ada packet dari komputer lokal yang dikirimkan langsung ke IP facebook

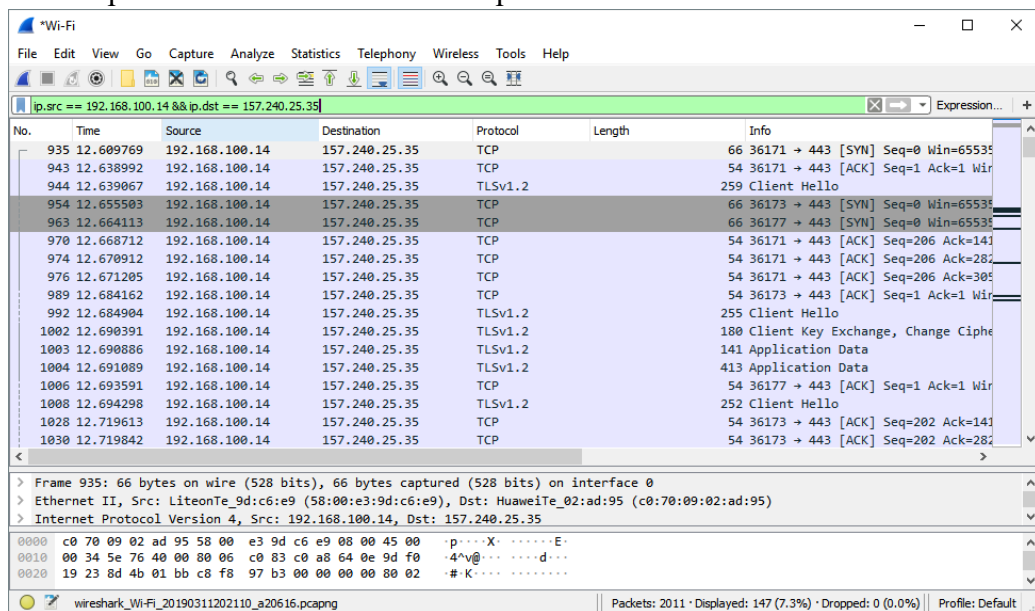
- Filter “ip.src == 192.168.100.14 && ip.dst == 216.239.38.120”



Gambar 3 Begitu pula sambungan ke IP google

e. Perbandingan menggunakan browser biasa.

- Filter “`ip.src == 192.168.100.14 && ip.dst == 157.240.25.35`”



Gambar 4 Capture packet saat mengakses facebook melalui Microsoft Edge

- Filter “`ip.src == 192.168.100.14 && ip.dst == 216.239.38.120`”

No.	Time	Source	Destination	Protocol	Length	Info
402	2.983348	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=1740 Ack=71
403	2.983430	192.168.100.14	216.239.38.120	TLSv1.2	100	Application Data
405	3.153985	192.168.100.14	216.239.38.120	TLSv1.2	184	Application Data
408	3.187894	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=1916 Ack=71
410	3.188004	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=1916 Ack=71
412	3.188554	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=1916 Ack=71
413	3.188758	192.168.100.14	216.239.38.120	TLSv1.2	100	Application Data
415	3.435824	192.168.100.14	216.239.38.120	TLSv1.2	323	Application Data
418	3.468814	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=2231 Ack=71
420	3.469383	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=2231 Ack=71
422	3.469640	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=2231 Ack=71
423	3.469705	192.168.100.14	216.239.38.120	TLSv1.2	100	Application Data
424	3.524588	192.168.100.14	216.239.38.120	TLSv1.2	595	Application Data
428	3.554897	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=2818 Ack=71
430	3.555017	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=2818 Ack=71
432	3.555472	192.168.100.14	216.239.38.120	TCP	54	36151 → 443 [ACK] Seq=2818 Ack=71
433	3.556542	192.168.100.14	216.239.38.120	TLSv1.2	100	Application Data

> Frame 433: 100 bytes on wire (800 bits), 100 bytes captured (800 bits) on interface 0
 > Ethernet II, Src: LiteonTe_9d:c6:e9 (58:00:e3:9d:c6:e9), Dst: HuaweiTe_02:ad:95 (c0:70:09:02:ad:95)
 > Internet Protocol Version 4, Src: 192.168.100.14, Dst: 216.239.38.120

```

0000 c0 70 09 02 ad 95 58 00 e3 9d c6 e9 08 00 45 00  p...X.....E
0010 00 56 5d 24 40 00 80 06 79 5f c0 a8 64 0e d8 ef  V]#@...y..d...
0020 26 78 8d 37 01 bb 97 22 ba 2e 52 72 0d 6f 50 18  &x?..."..R-cP

```

wireshark_Wi-Fi_20190311202110_a20616.pcapng | Packets: 2011 · Displayed: 202 (10.0%) · Dropped: 0 (0.0%) | Profile: Default

Gambar 5 Capture packet dengan mengakses google menggunakan browser yang sama, terlihat bahwa packet akan dikirimkan langsung dari komputer lokal ke google