

## Progress Tambahan

### Kelompok 2

Dave Travis - 2201020008  
Muhammad Noval - 2201020014  
Rizsky Parsadanta R. - 2201020117  
Arya Winata - 2201020001

Judul proyek : Analisis Serangan Sniffing & Mitigasinya di Wireshark

Tujuan proyek : Melengkapi data project

Target proyek : - Jumlah paket tertangkap sebelum / sesudah enkripsi,  
- Latency tambahan akibat TLS,  
- Persentase keberhasilan penyadapan.

Pengantar:

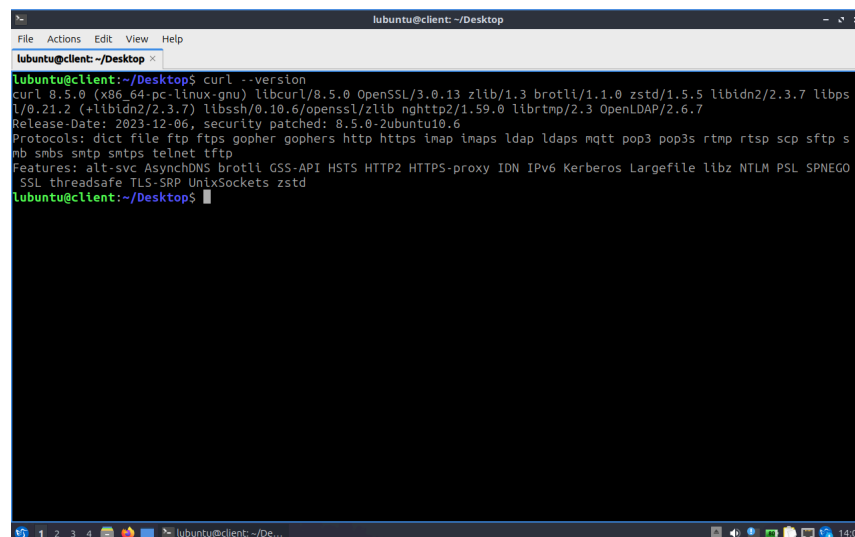
Pada progress kali ini akan difokuskan pada tahapan-tahapan tambahan yang didukung oleh screenshot yang ditangkap selama progress dilakukan. Lampiran-lampiran file capture juga akan disertakan saat pengiriman di link GitHub.

#### A. Jumlah paket tertangkap sebelum / sesudah enkripsi

##### 1. Sebelum enkripsi (HTTP)

Jumlah request POST yang akan dicoba untuk progress ini ialah 20 request per tahapan, dan akan diaplikasikan pada tahapan-tahapan berikutnya demi konsistensi data. Guna memudahkan tahapan request lebih dari satu, kami memutuskan menggunakan looping script sederhana menggunakan curl.

Untuk mengecek ketersediaan curl pada vm client (karena client yang request POST), gunakan command “*curl --version*”

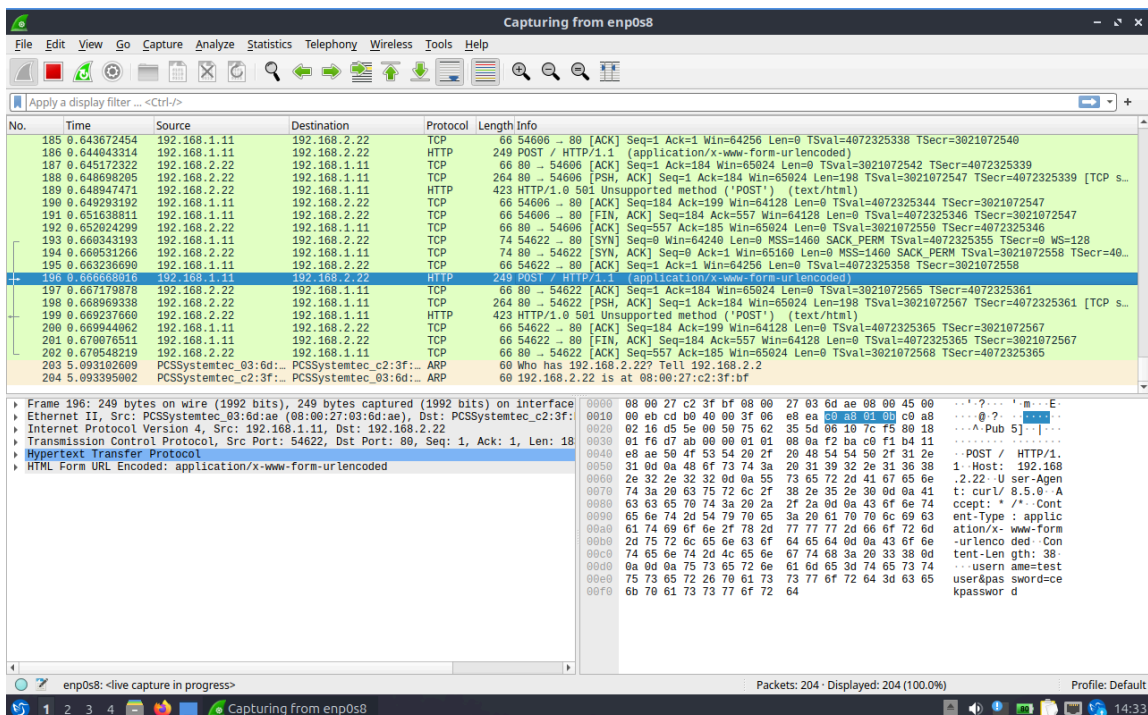


```
lubuntu@client: ~/Desktop
lubuntu@client:~/Desktop$ curl --version
curl 8.5.0 (x86_64-pc-linux-gnu) libcurl/8.5.0 OpenSSL/3.0.13 zlib/1.3 brotli/1.1.0 zstd/1.5.5 libidn2/2.3.7 libpsl
1/0.21.2 (+libidn2/2.3.7) libssh/0.10.6/openssl/zlib nghttp2/1.59.0 librtmp/2.3 OpenLDAP/2.6.7
Release-Date: 2023-12-06, security patched: 8.5.0-2ubuntu10.6
Protocols: dict file ftp ftps gopher gophers http https imap imaps ldap ldaps mqtt pop3 pop3s rtmp rtsp scp sftp s
mb snbss snmp snmp6 telnet tftp
Features: alt-svc AsynchDNS brotli GSS-API HSTS HTTP2 HTTPS-proxy IDN IPv6 Kerberos Largefile libz NTLM PSL SPNEGO
SSL threadsafe TLS-SRP UnixSockets zstd
lubuntu@client:~/Desktop$
```

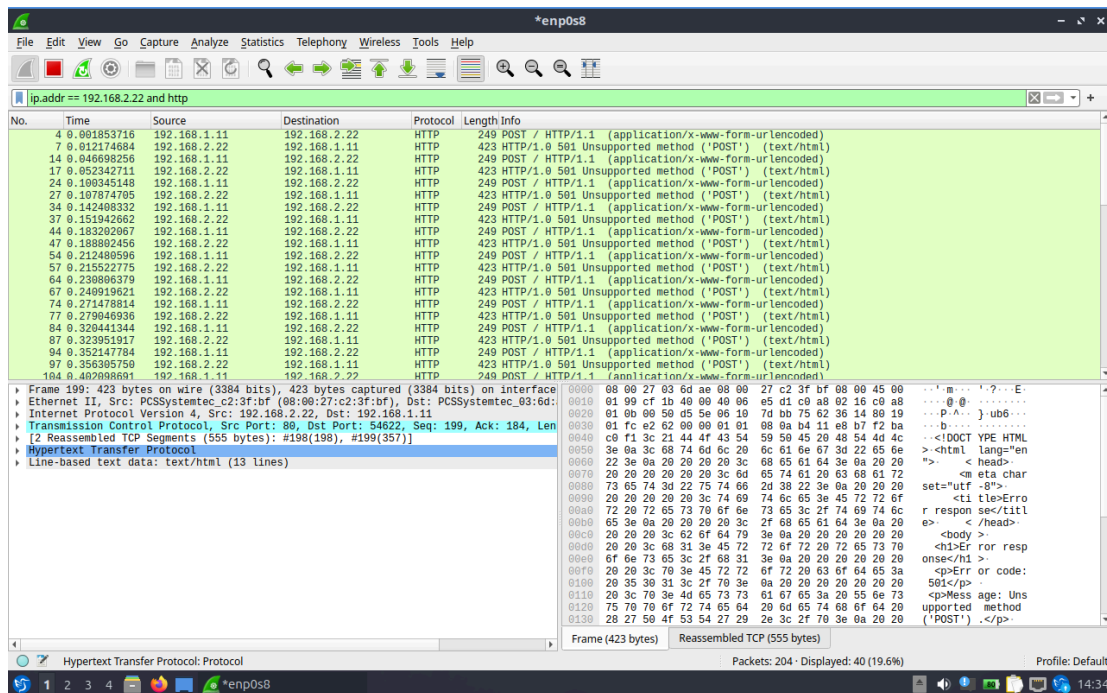
Jika sudah terinstall, maka selanjutnya kita buat script looping POST nya pada file bernama “*test\_post\_http.sh*” dengan kode sebagai berikut.

```
lubuntu@client: ~/Desktop
File Actions Edit View Help
lubuntu@client: ~/Desktop x
GNU nano 7.2 test_post_http.sh *
#!/bin/bash
for i in {1..20}; do
    curl -s -X POST http://192.168.2.22
        -d "username=testuser&password=cekpassword"
        -H "Content-Type: application/x-www-form-urlencoded"
done
```

Lalu kita simpan dan eksekusi file tersebut, maka request akan terkirim ke vm server, dan jika kita buka vm sniffer selagi membuka WireShark selama request berlangsung, maka akan terlihat seperti ini.



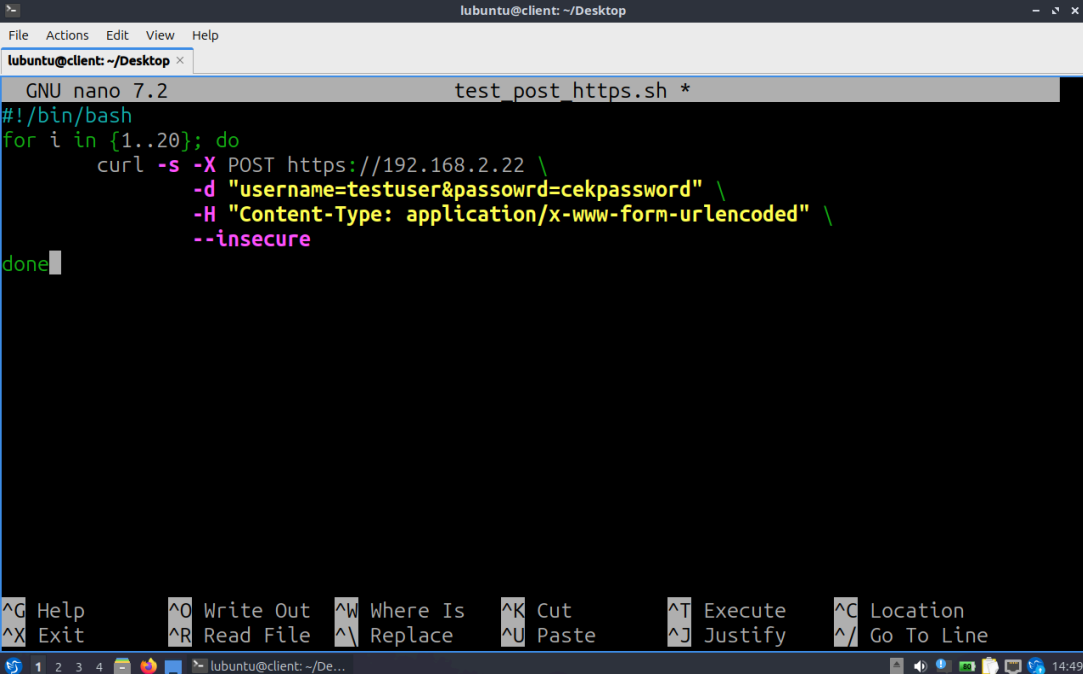
Total *packet* data sudah masuk hasil dari 20 kali request POST, dan masih bercampur-campur dengan packet lainnya, sehingga harus kita pakai filter HTTP dan IP target, yaitu vm server.



Terlihat pada tulisan di bawah kanan, **total paket** yang tercapture ialah **204 paket**, dan yang eksklusif pada **HTTP (pasca filtering)** ialah **40 paket** yang terlampirkan, alias **19,6% dari total paket** yang ditampilkan.

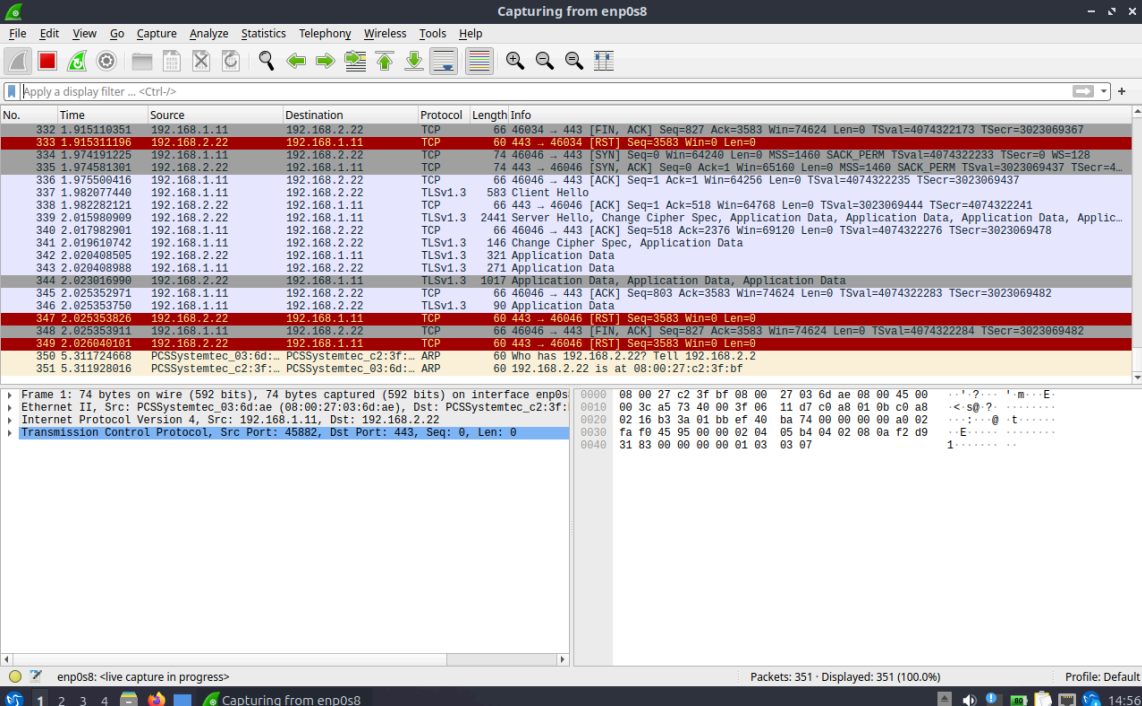
## 2. Pasca enkripsi (HTTPS)

Tahapan juga sama dengan HTTP, di mana request akan dilakukan 20 kali dengan menggunakan script looping sederhana menggunakan curl sebagai berikut.



```
GNU nano 7.2 test_post_https.sh *
#!/bin/bash
for i in {1..20}; do
    curl -s -X POST https://192.168.2.22 \
        -d "username=testuser&password=cekpassword" \
        -H "Content-Type: application/x-www-form-urlencoded" \
        --insecure
done
```

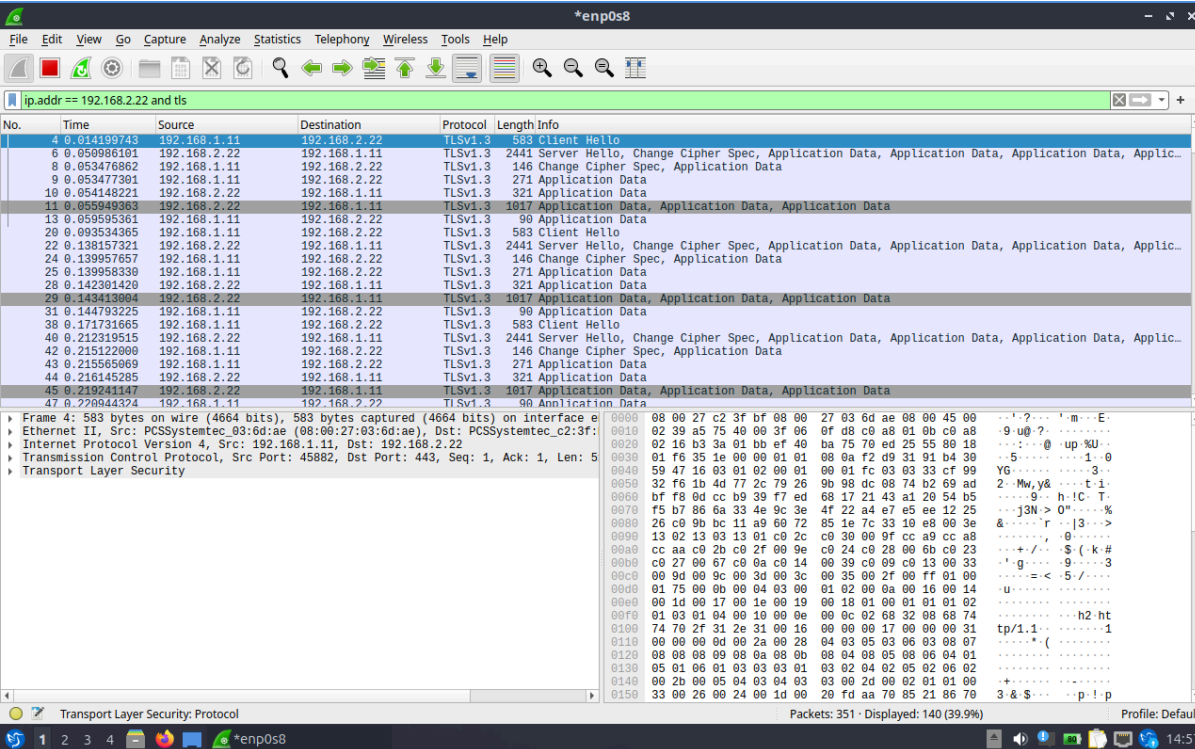
Lalu kita eksekusi file ini dan request akan kembali terkirimkan ke vm server, sehingga pada vm sniffer dapat tampilan seperti ini untuk total traffic nya.



The screenshot shows Wireshark capturing traffic on the enp0s8 interface. The packet list on the left shows various TCP and TLSv1.3 packets. The packet details pane on the right shows the structure of a packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
332	1.915110351	192.168.1.11	192.168.2.22	TCP	66	46034 → 443 [FIN, ACK] Seq=827 Ack=3583 Win=74624 Len=0 TSval=4074322173 TSecr=3023069367
333	1.915311196	192.168.2.22	192.168.1.11	TCP	60	443 → 46034 [RST] Seq=3583 Win=0 Len=0
334	1.9741911225	192.168.1.11	192.168.2.22	TCP	74	46046 → 443 [SYN] Seq=0 Win=0 Len=0 MSS=1460 SACK_PERM TSval=4074322233 TSecr=0 WS=128
335	1.974581301	192.168.2.22	192.168.1.11	TCP	74	443 → 46046 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3023069437 TSecr=4...
336	1.975509416	192.168.1.11	192.168.2.22	TCP	66	46046 → 443 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=4074322235 TSecr=3023069437
337	1.982077440	192.168.1.11	192.168.2.22	TLSv1.3	583	Client Hello
338	1.982202121	192.168.2.22	192.168.1.11	TCP	60	443 → 46046 [ACK] Seq=1 Ack=518 Win=64768 Len=0 TSval=3023069444 TSecr=4074322241
339	2.015080909	192.168.2.22	192.168.1.11	TLSv1.3	2441	Server Hello, Change Cipher Spec, Application Data, Application Data, Applic...
340	2.017982901	192.168.1.11	192.168.2.22	TCP	66	46046 → 443 [ACK] Seq=518 Ack=2376 Win=69120 Len=0 TSval=4074322276 TSecr=3023069478
341	2.019610742	192.168.1.11	192.168.2.22	TLSv1.3	146	Change Cipher Spec, Application Data
342	2.020408505	192.168.2.22	192.168.1.11	TLSv1.3	321	Application Data
343	2.020408998	192.168.1.11	192.168.2.22	TLSv1.3	271	Application Data
344	2.023016990	192.168.2.22	192.168.1.11	TLSv1.3	1017	Application Data, Application Data, Application Data
345	2.025352971	192.168.1.11	192.168.2.22	TCP	66	46046 → 443 [ACK] Seq=803 Ack=3583 Win=74624 Len=0 TSval=4074322283 TSecr=3023069482
346	2.025353750	192.168.1.11	192.168.2.22	TLSv1.3	90	Application Data
347	2.025353826	192.168.2.22	192.168.1.11	TCP	60	443 → 46046 [RST] Seq=3583 Win=0 Len=0
348	2.025353911	192.168.1.11	192.168.2.22	TCP	60	46046 → 443 [FIN] Seq=827 Ack=3583 Win=74624 Len=0 TSval=4074322284 TSecr=3023069482
349	2.026040101	192.168.2.22	192.168.1.11	TCP	60	443 → 46046 [RST] Seq=3583 Win=0 Len=0
350	5.311724668	PCSSystemtec_03:6d:...	PCSSystemtec_c2:3f:...	ARP	60	Who has 192.168.2.22? Tell 192.168.2.2
351	5.311928016	PCSSystemtec_c2:3f:...	PCSSystemtec_03:6d:...	ARP	60	192.168.2.22 is at 08:00:27:c2:3f:bf

Karena masih belum terfilter, maka kita implementasikan filter IP target (vm server) dan TLS, sehingga tampilan seperti ini.



No.	Time	Source	Destination	Protocol	Length	Info
4	0.014199743	192.168.1.11	192.168.2.22	TLSv1.3	583	Client Hello
6	0.050986101	192.168.2.22	192.168.1.11	TLSv1.3	2441	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Applic...
8	0.053476862	192.168.1.11	192.168.2.22	TLSv1.3	146	Change Cipher Spec, Application Data
9	0.053477391	192.168.1.11	192.168.2.22	TLSv1.3	271	Application Data
10	0.054148221	192.168.2.22	192.168.1.11	TLSv1.3	321	Application Data
11	0.055949363	192.168.2.22	192.168.1.11	TLSv1.3	1917	Application Data, Application Data, Application Data
13	0.059593561	192.168.1.11	192.168.2.22	TLSv1.3	90	Application Data
20	0.093534365	192.168.1.11	192.168.2.22	TLSv1.3	583	Client Hello
22	0.138157321	192.168.2.22	192.168.1.11	TLSv1.3	2441	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Applic...
24	0.139957657	192.168.1.11	192.168.2.22	TLSv1.3	146	Change Cipher Spec, Application Data
25	0.139958330	192.168.1.11	192.168.2.22	TLSv1.3	271	Application Data
28	0.142301420	192.168.2.22	192.168.1.11	TLSv1.3	321	Application Data
29	0.143413094	192.168.2.22	192.168.1.11	TLSv1.3	1917	Application Data, Application Data, Application Data
31	0.144793225	192.168.1.11	192.168.2.22	TLSv1.3	90	Application Data
38	0.171731665	192.168.1.11	192.168.2.22	TLSv1.3	583	Client Hello
40	0.212319515	192.168.2.22	192.168.1.11	TLSv1.3	2441	Server Hello, Change Cipher Spec, Application Data, Application Data, Application Data, Applic...
42	0.215122000	192.168.1.11	192.168.2.22	TLSv1.3	146	Change Cipher Spec, Application Data
43	0.215565069	192.168.1.11	192.168.2.22	TLSv1.3	271	Application Data
44	0.216145285	192.168.2.22	192.168.1.11	TLSv1.3	321	Application Data
45	0.219241147	192.168.2.22	192.168.1.11	TLSv1.3	1917	Application Data, Application Data, Application Data
47	0.228944324	192.168.1.11	192.168.2.22	TLSv1.3	90	Application Data

Frame 4: 583 bytes on wire (4664 bits), 583 bytes captured (4664 bits) on interface e...  
Ethernet II, Src: PCSSystemtec\_83:6d:ae (08:00:27:03:6d:ae), Dst: PCSSystemtec\_c2:3f:1...  
Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.2.22  
Transmission Control Protocol, Src Port: 45882, Dst Port: 443, Seq: 1, Ack: 1, Len: 5...  
Transport Layer Security

0000 00 00 27 c2 3f 0f 00 00 27 03 6d ae 00 00 45 00 ...?... 'm...E-  
0010 02 39 a5 75 40 00 3f 06 0f 08 c0 a8 01 00 c0 08 ...9 ub ?...  
0020 02 16 b3 3a 01 bb ef 40 ba 75 70 ed 25 55 08 18 ...: @ up %U...  
0030 01 f6 35 1e 00 00 01 01 00 0a f2 09 31 91 b4 30 ...5... 1...0  
0040 59 47 16 03 01 02 00 01 00 01 fc 03 03 33 cf 09 YG... 3...  
0050 32 f6 1b 4d 77 2c 79 26 90 98 dc 08 74 b2 69 ad 2... Mw, y& ... t...i...  
0060 bf f8 8d cc b9 39 f7 ed 68 17 21 43 a1 20 54 05 ...9... h-IC... T...  
0070 f5 b7 86 6a 33 4e 9c 3e 4f 22 a4 e7 e5 ee 12 25 ...j3N> 0"...%  
0080 26 c0 9b bc 11 a9 60 72 85 1e 7c 33 10 e8 00 3e &...r...|3...>  
0090 13 02 13 03 13 01 c0 2c c0 30 00 9f cc a9 cc a8 ...0...  
00a0 cc aa c0 2b c0 2f 00 9e c0 24 c0 28 00 6b c0 23 ...+/-... \$(-k-#  
00b0 c0 27 00 67 c0 6a c0 14 00 39 c0 09 c0 13 00 33 ...'g... 9...3  
00c0 00 9d 00 9c 00 3d 00 3c 00 35 00 2f 00 ff 01 00 ...==< 5/-...  
00d0 01 75 00 0b 00 04 03 00 01 02 00 0a 00 16 00 14 ...u...  
00e0 00 1d 00 17 00 1e 00 19 00 18 01 00 01 01 01 02 ...  
00f0 01 03 01 04 00 10 00 0e 00 0c 02 68 32 08 68 74 ...h2 ht  
0100 74 70 2f 31 2e 31 00 16 00 00 00 17 00 00 00 31 tp/1.1... 1  
0110 00 00 00 00 00 2a 00 28 04 03 05 03 06 03 08 07 ...\* ( ...  
0120 08 08 08 08 08 0a 08 0b 08 04 08 05 08 06 04 01 ...  
0130 05 01 06 01 03 03 03 01 03 02 04 02 05 02 06 02 ...  
0140 00 2b 00 05 04 03 04 03 03 00 2d 00 02 01 01 00 ...+...  
0150 33 00 26 00 24 00 1d 00 20 fd aa 70 85 21 86 70 3 & \$... -p ! p

Transport Layer Security: Protocol  
Packets: 351 · Displayed: 140 (39.9%)  
Profile: Default

Terlihat di bawah kanan, untuk tahapan ini **total paket** yang terkirim ialah **351 paket**, dengan **filter TLS** itu sendiri ialah **140 paket** yang terkirim, **sekitar 39,9% dari total paket**.

Dapat disimpulkan bahwa paket yang terkirim melalui HTTPS lebih menerima banyak paket karena enkripsi yang dilakukan.

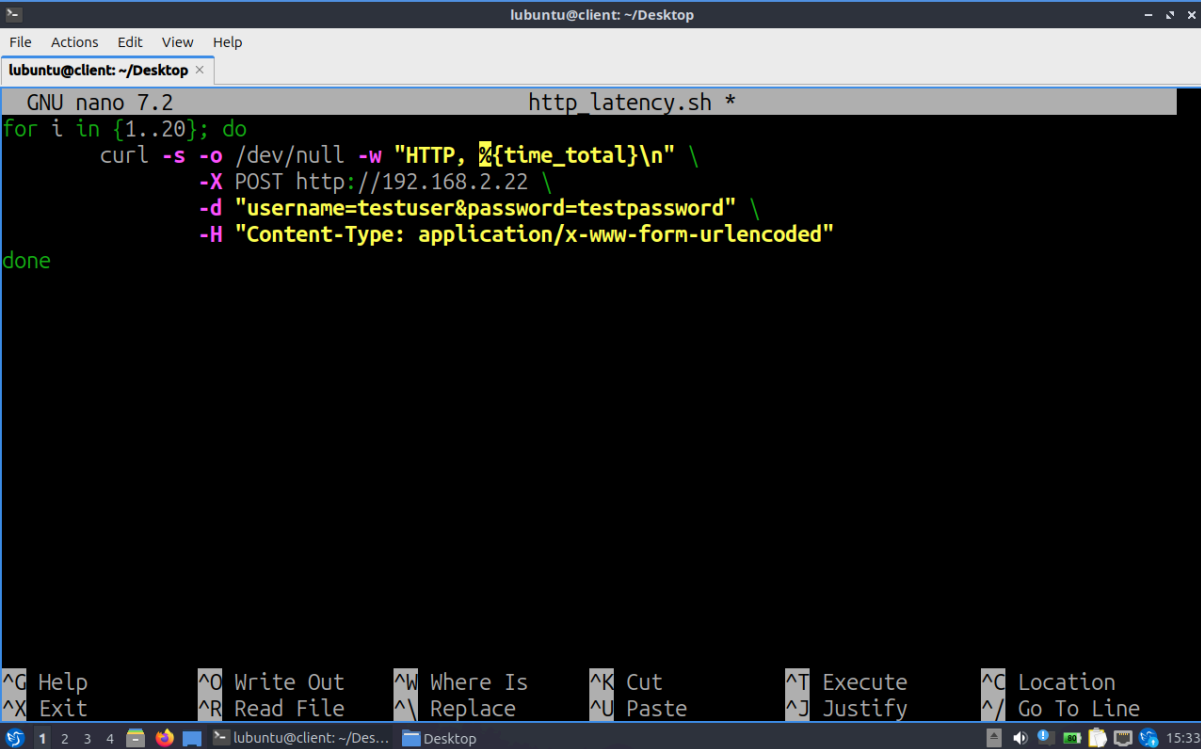
## B. Latency tambahan akibat TLS

Pada tahapan ini akan kita uji waktu respons (*latency*) dari HTTP dan HTTPS, dengan membandingkan lama respons tanpa enkripsi dan dengan enkripsi TLS untuk menghitung *overhead* performa yang ditimbulkan oleh enkripsi.

Perhitungan yang akan diukur ialah *end-to-end latency*, yaitu waktu kirim request hingga terima respons lengkap dengan satuan milidetik (ms) yang akan dilakukan dengan menggunakan “*curl -w*” (*built-in timing* di curl) sebanyak 20 kali untuk masing-masing HTTP dan HTTPS.

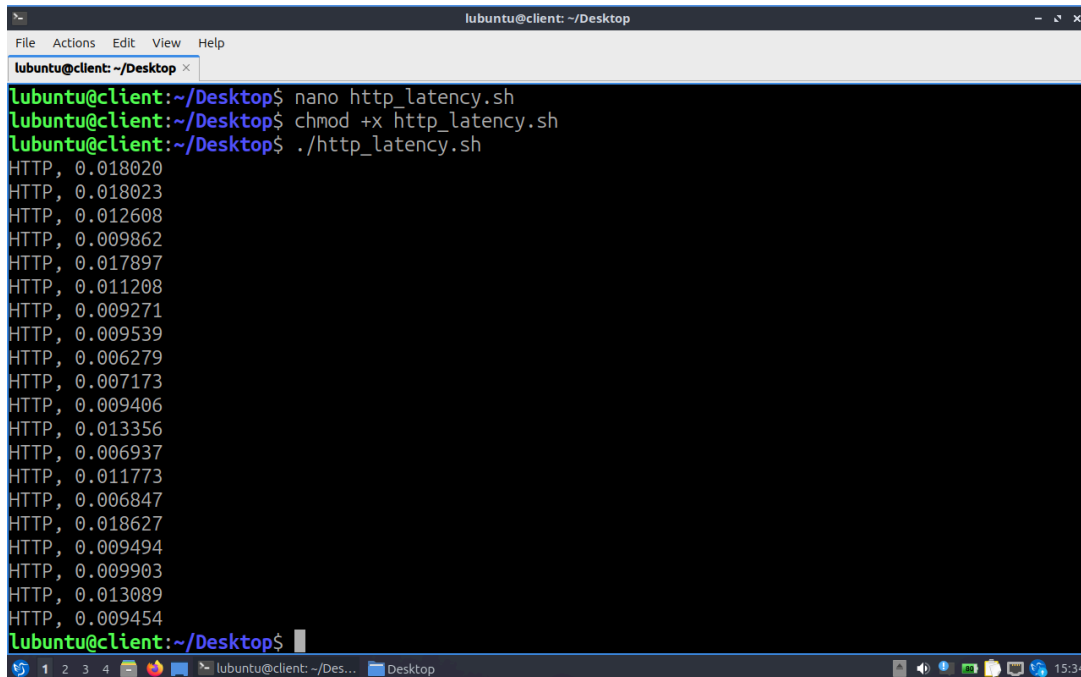
### 1. Latency HTTP

Percobaan ini juga akan menggunakan script looping otomatis dengan kode sebagai berikut.



```
lubuntu@client: ~/Desktop
File Actions Edit View Help
lubuntu@client: ~/Desktop x
GNU nano 7.2 http_latency.sh *
for i in {1..20}; do
  curl -s -o /dev/null -w "HTTP, %{time_total}\n" \
    -X POST http://192.168.2.22 \
    -d "username=testuser&password=testpassword" \
    -H "Content-Type: application/x-www-form-urlencoded"
done
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/_ Go To Line
1 2 3 4      lubuntu@client: ~/Des... Desktop 15:33
```

Setelah selesai dikonfigurasi, maka ketika dijalankan akan menampilkan hasil seperti ini.

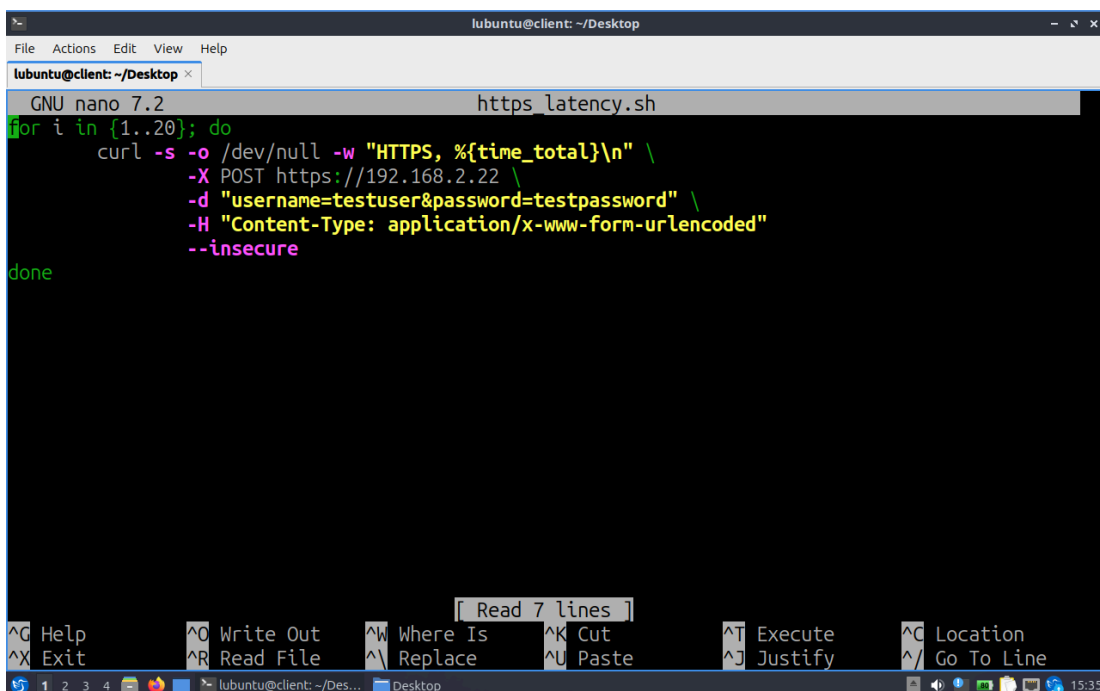


```
lubuntu@client: ~/Desktop
File Actions Edit View Help
lubuntu@client: ~/Desktop x
lubuntu@client:~/Desktop$ nano http_latency.sh
lubuntu@client:~/Desktop$ chmod +x http_latency.sh
lubuntu@client:~/Desktop$ ./http_latency.sh
HTTP, 0.018020
HTTP, 0.018023
HTTP, 0.012608
HTTP, 0.009862
HTTP, 0.017897
HTTP, 0.011208
HTTP, 0.009271
HTTP, 0.009539
HTTP, 0.006279
HTTP, 0.007173
HTTP, 0.009406
HTTP, 0.013356
HTTP, 0.006937
HTTP, 0.011773
HTTP, 0.006847
HTTP, 0.018627
HTTP, 0.009494
HTTP, 0.009903
HTTP, 0.013089
HTTP, 0.009454
lubuntu@client:~/Desktop$
```

Hasil dari perhitungan latensi ini akan kita simpan agar mempermudah perbandingannya dengan *latency* dari HTTPS.

## 2. Latency HTTPS

Tahapan yang sama dilakukan untuk HTTPS, dengan script sebagai berikut.



```
lubuntu@client: ~/Desktop
File Actions Edit View Help
lubuntu@client: ~/Desktop x
GNU nano 7.2 https_latency.sh
for i in {1..20}; do
    curl -s -o /dev/null -w "HTTPS, %{time_total}\n" \
        -X POST https://192.168.2.22 \
        -d "username=testuser&password=testpassword" \
        -H "Content-Type: application/x-www-form-urlencoded" \
        --insecure
done
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line
Read 7 lines
lubuntu@client: ~/Desktop
```

Setelah selesai dikonfigurasi, maka ketika dijalankan akan menampilkan hasil seperti ini.

```

lubuntu@client: ~/Desktop
File Actions Edit View Help
lubuntu@client: ~/Desktop x
lubuntu@client:~/Desktop$ nano https_latency.sh
lubuntu@client:~/Desktop$ chmod +x https_latency.sh
lubuntu@client:~/Desktop$ ./https_latency.sh
HTTPS, 0.084779
HTTPS, 0.071806
HTTPS, 0.078190
HTTPS, 0.056615
HTTPS, 0.077500
HTTPS, 0.077087
HTTPS, 0.087531
HTTPS, 0.069386
HTTPS, 0.079494
HTTPS, 0.066837
HTTPS, 0.083470
HTTPS, 0.075555
HTTPS, 0.078247
HTTPS, 0.058221
HTTPS, 0.085763
HTTPS, 0.079837
HTTPS, 0.081823
HTTPS, 0.066689
HTTPS, 0.080989
HTTPS, 0.068400
lubuntu@client:~/Desktop$

```

Setelah semua nya muncul, maka selanjutnya kita akan transfer angka-angka ini ke Excel, sehingga bisa kita hitung dengan rumus excel, yang mana:

- Rata-rata HTTP: =AVERAGE() semua nilai HTTP
- Rata-rata HTTPS: =AVERAGE() semua nilai HTTPS
- Overhead TLS: ((HTTPS\_avg - HTTP\_avg) / HTTP\_avg) \* 100%

	A	B	C	D	E	F	G	H
1								
2		HTTP		HTTPS			0,011438	
3		0,01802		0,084779		HTTP	0,075411	
4		0,018023		0,071806		Overhead TLS	5,592846	
5		0,012608		0,07819				
6		0,009862		0,056615				
7		0,017897		0,0775				
8		0,011208		0,077087				
9		0,009271		0,087531				
10		0,009539		0,069386				
11		0,006279		0,079494				
12		0,007173		0,066837				
13		0,009406		0,08347				
14		0,013356		0,075555				
15		0,006937		0,078247				
16		0,011773		0,058221				
17		0,006847		0,085763				
18		0,018627		0,079837				
19		0,009494		0,081823				
20		0,009903		0,066689				
21		0,013089		0,080989				
22		0,009454		0,0684				
23								
24								



Seperti yang bisa dilihat, bahwa **rata-rata latency HTTP ialah 11 ms** dan **rata-rata latency HTTPS ialah 75 ms**, dengan **overhead TLS** nya sebesar **~559,38%**, yang artinya **latency HTTPS hampir 6,6 kali lebih lambat** daripada HTTP.

### C. Persentase keberhasilan penyadapan

Pada bagian ini kita akan menguji seberapa sering penyerang berhasil mengekstrak password dari lalu lintas yang ditangkap, namun dalam logika simpel, dapat disimpulkan bahwa:

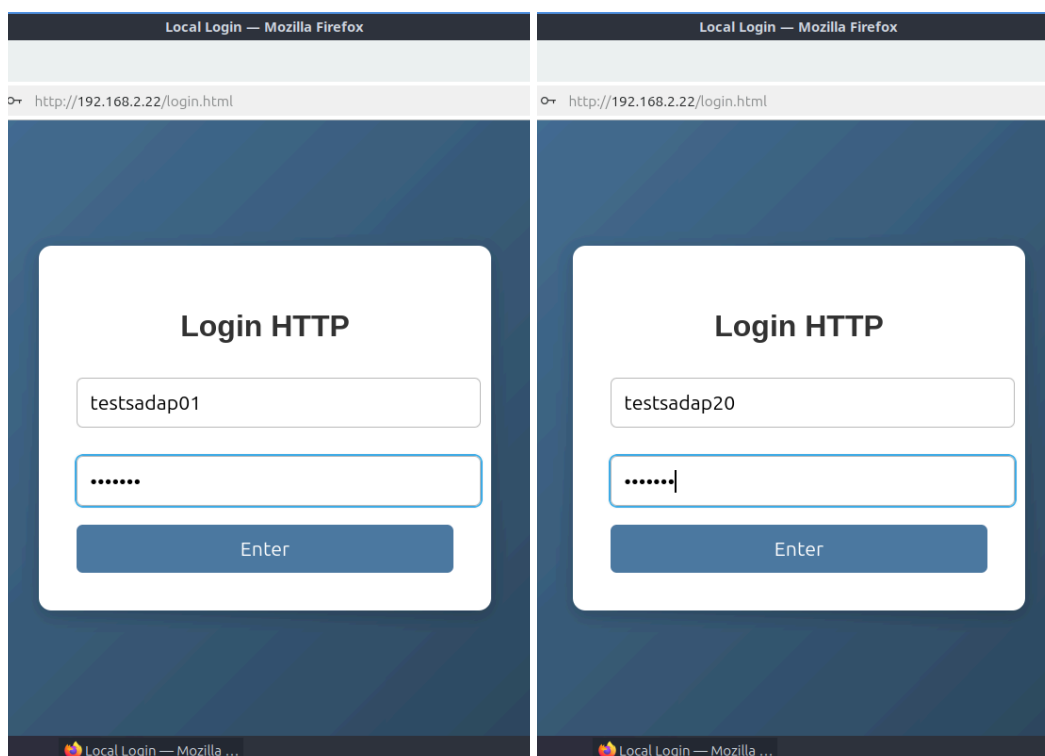
- HTTP yang mana password dalam plain text, seharusnya 100% berhasil.
- HTTPS yang mana password terenkripsi, seharusnya 0% berhasil.

Namun kita akan tetap melakukan eksperimen sehingga kita melihat secara langsung dan memiliki bukti atas kesimpulan kita.

Sama seperti sebelumnya, percobaan ini akan kita loop sebanyak 20 kali untuk tiap protokol, dan untuk memudahkan pengecekan, tahapan ini akan dilakukan secara manual, yaitu request POST melalui portal login untuk tiap-tiap protokol.

#### 1. HTTP

Data username dan password yang akan digunakan disini akan berubah secara minim guna membandingkan apakah ada perubahan dari tiap tahapan atau tidak, dengan contoh seperti berikut.



Ketika request dikirim, maka dapat terlihat untuk masing-masing request POST HTTP dapat terlihat *plain text* passwordnya.

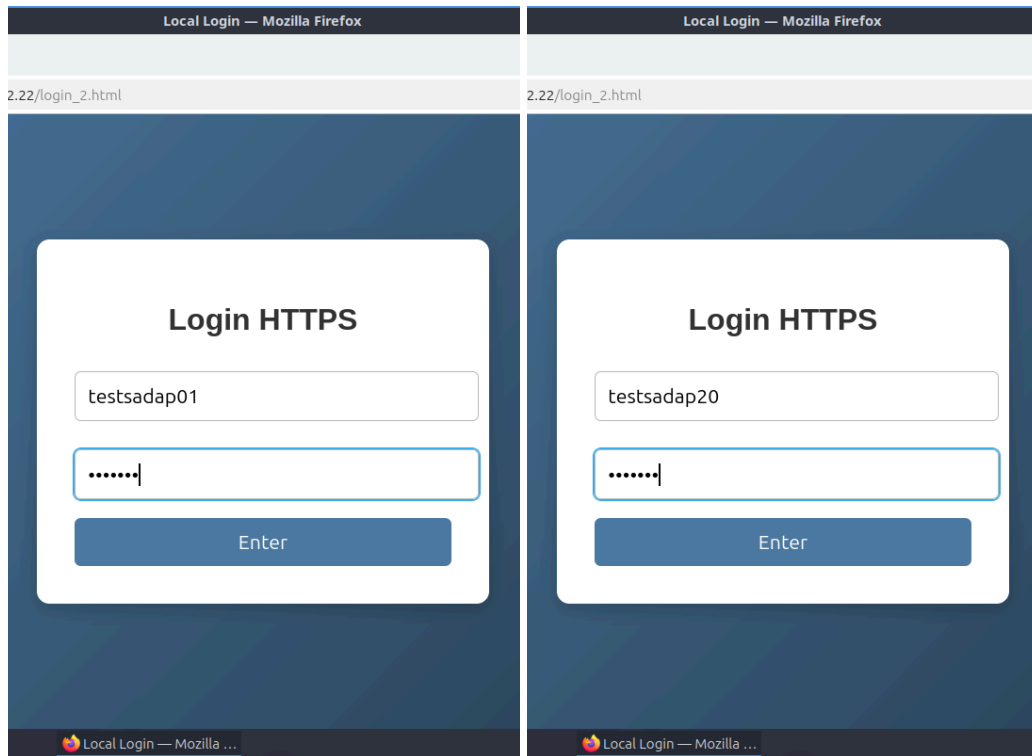
The top screenshot shows a list of captured packets in Wireshark. The selected packet is an HTTP POST request from 192.168.1.11 to 192.168.2.22. The details pane shows the request structure, including the form data: username='testsadap01' and password='sadap01'.

The bottom screenshot shows the details of the selected packet, which is an HTTP POST request from 192.168.1.11 to 192.168.2.22. The details pane shows the request structure, including the form data: username='testsadap20' and password='sadap20'.

Terbukti bahwa persentase keberhasilan penyadapan pada protokol HTTP ialah 100%, mengingat dikirimnya menggunakan plain text.

## 2. HTTPS

Sama seperti sebelumnya, data username dan password yang akan digunakan disini akan berubah secara minim guna membandingkan apakah ada perubahan dari tiap tahapan atau tidak, dengan contoh seperti berikut.



Ketika request dikirim, maka dapat terlihat untuk masing-masing request POST HTTPS dapat terlihat bahwa semua data telah terenkripsi, sehingga tidak memungkinkan untuk melihat data yang terkirim pada tiap paket POST.

Wireshark interface showing a TLS capture from interface enp0s8. The packet list shows a sequence of TLS messages: Client Hello, Server Hello, Change Cipher Spec, and Application Data. The selected packet (No. 15) is an Application Data packet containing encrypted data. The packet details pane shows the TLSv1.3 record structure, including the Opaque Type (Application Data) and the encrypted data (daa481f7ae5a71f0e9fc07331a863331).

No.	Time	Source	Destination	Protocol	Length	Info
4	0.004192...	192.168.1.11	192.168.2.22	TLSv...	24...	Client Hello
6	0.006750...	192.168.2.22	192.168.1.11	TLSv...	307	Server Hello, Change Cipher Spec, Application Data, Application Data
8	0.009821...	192.168.1.11	192.168.2.22	TLSv...	146	Change Cipher Spec, Application Data
9	0.010170...	192.168.1.11	192.168.2.22	TLSv...	720	Application Data
10	0.010773...	192.168.2.22	192.168.1.11	TLSv...	321	Application Data
11	0.014395...	192.168.2.22	192.168.1.11	TLSv...	762	Application Data, Application Data
15	0.020004...	192.168.1.11	192.168.2.22	TLSv...	90	Application Data

Frame 15: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface enp0s8, Src: PCSSystemtec\_03:6d:ae (08:00:27:03:6d:ae), Dst: 08:00:27:03:6d:ae (08:00:27:03:6d:ae), Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.2.22, Transmission Control Protocol, Src Port: 59976, Dst Port: 443, Transport Layer Security

TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 19

Encrypted Application Data: daa481f7ae5a71f0e9fc07331a863331

[Application Data Protocol: Hypertext Transfer Protocol]

Wireshark interface showing a TLS capture from interface https\_penyadapan\_percobaan\_20.pcapng. The packet list shows a sequence of TLS messages: Client Hello, Server Hello, Change Cipher Spec, and Application Data. The selected packet (No. 11) is an Application Data packet containing encrypted data. The packet details pane shows the TLSv1.3 record structure, including the Opaque Type (Application Data) and the encrypted data (976b0a55667c380980).

No.	Time	Source	Destination	Protocol	Length	Info
4	0.004715...	192.168.1.11	192.168.2.22	TLSv...	24...	Client Hello
6	0.006480...	192.168.2.22	192.168.1.11	TLSv...	307	Server Hello, Change Cipher Spec, Application Data, Application Data
8	0.009626...	192.168.1.11	192.168.2.22	TLSv...	146	Change Cipher Spec, Application Data
9	0.010242...	192.168.2.22	192.168.1.11	TLSv...	321	Application Data
10	0.010746...	192.168.1.11	192.168.2.22	TLSv...	720	Application Data
11	0.015335...	192.168.2.22	192.168.1.11	TLSv...	762	Application Data, Application Data
13	0.019109...	192.168.1.11	192.168.2.22	TLSv...	90	Application Data

Internet Protocol Version 4, Src: 192.168.2.22, Dst: 192.168.1.11

Transmission Control Protocol, Src Port: 443, Dst Port: 46982, Transport Layer Security

TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 312

Encrypted Application Data [truncated]: 976b0a55667c380980

[Application Data Protocol: Hypertext Transfer Protocol]

TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Protocol

Opaque Type: Application Data (23)

Version: TLS 1.2 (0x0303)

Length: 374

Encrypted Application Data [truncated]: 5165009780aa209044

[Application Data Protocol: Hypertext Transfer Protocol]

Sehingga kesimpulan sebelumnya benar, bahwa terdapat persentase 0% untuk data bocor pada protokol HTTPS.