

## 1. ip.src == 157.245.50.224

The image shows a Wireshark network capture. The top pane displays a Command Prompt window with the following commands and output:

```
PC:\Users\hp>ping http://aku.pengen.pw/
Ping request could not find host http://aku.pengen.pw/. Please check the name and try again.

PC:\Users\hp>ping aku.pengen.pw
Pinging aku.pengen.pw [157.245.50.224] with 32 bytes of data:
Reply from 157.245.50.224: bytes=32 time=104ms TTL=50
Reply from 157.245.50.224: bytes=32 time=259ms TTL=50
Reply from 157.245.50.224: bytes=32 time=171ms TTL=50
Reply from 157.245.50.224: bytes=32 time=90ms TTL=50

Ping statistics for 157.245.50.224:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 90ms, Maximum = 259ms, Average = 156ms

> Frame
> Ether
> InterC:\Users\hp>ping testing.mekanis.me
Pinging testing.mekanis.me [157.245.50.224] with 32 bytes of data:
Reply from 157.245.50.224: bytes=32 time=394ms TTL=50
Reply from 157.245.50.224: bytes=32 time=273ms TTL=50

Ping statistics for 157.245.50.224:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 273ms, Maximum = 394ms, Average = 333ms

Control-C
C:\Users\hp>
```

The bottom pane shows the packet list and packet details. The packet list is filtered for 'ip.src == 157.245.50.224'. The selected packet is an HTTP 401 Unauthorized response from 157.245.50.224 to 192.168.1.8.

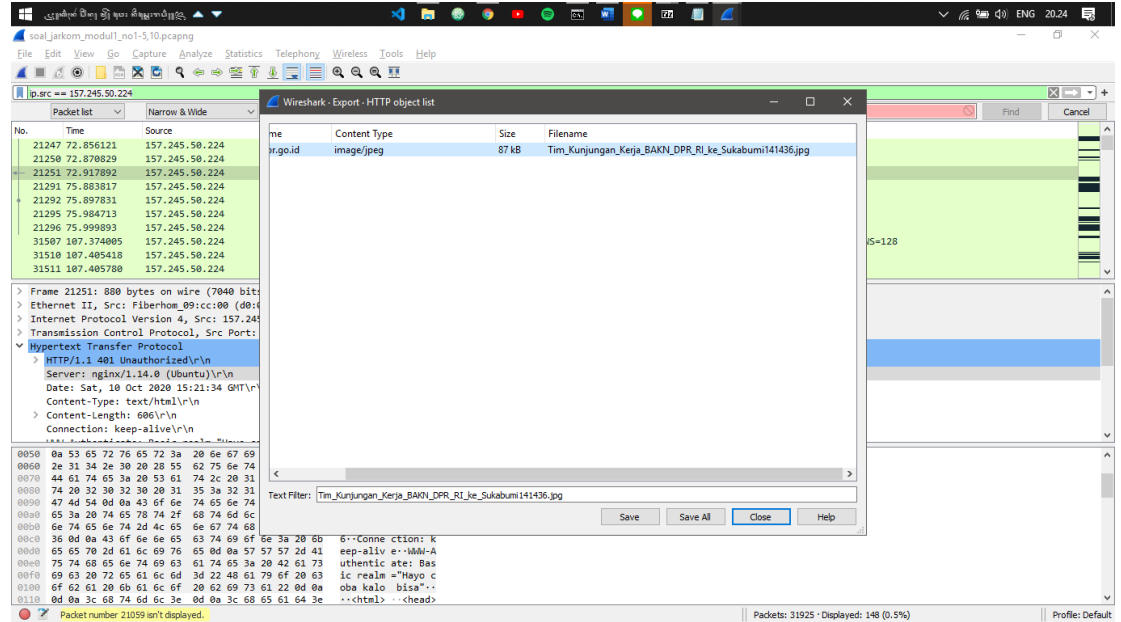
No.	Time	Source	Destination	Protocol	Length	Info
21247	72.856121	157.245.50.224	192.168.1.8	TCP	62	80 → 62375 [SYN, ACK] Seq=0 Ack=1 Win=4260 Len=0 MSS=1420 SACK_PERM=1
21250	72.870829	157.245.50.224	192.168.1.8	TCP	54	80 → 62375 [ACK] Seq=1 Ack=437 Win=4696 Len=0
21251	72.917892	157.245.50.224	192.168.1.8	HTTP	880	HTTP/1.1 401 Unauthorized (text/html)
21291	75.883817	157.245.50.224	192.168.1.8	TCP	60	80 → 62375 [ACK] Seq=927 Ack=938 Win=5197 Len=0
21292	75.897831	157.245.50.224	192.168.1.8	HTTP	509	HTTP/1.1 200 OK (text/html)
21295	75.984713	157.245.50.224	192.168.1.8	TCP	60	80 → 62375 [ACK] Seq=1282 Ack=1346 Win=5605 Len=0
21296	75.999893	157.245.50.224	192.168.1.8	HTTP	509	HTTP/1.1 200 OK (text/html)
31507	187.374005	157.245.50.224	192.168.1.8	TCP	66	80 → 62460 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1420 SACK_PERM=1 WS=128
31510	187.485418	157.245.50.224	192.168.1.8	TCP	54	80 → 62460 [ACK] Seq=1 Ack=432 Win=64128 Len=0
31511	187.485788	157.245.50.224	192.168.1.8	HTTP	893	HTTP/1.1 401 Unauthorized (text/html)

The packet details pane shows the following information for the selected packet:

- Frame 21251: 880 bytes on wire (7040 bits), 880 bytes captured (7040 bits) on interface \Device\NPF{D2ABF891-1186-446B-AC1D-6384A19F3AFD}, id 0
- Ethernet II, Src: Fiberhom\_09:cc:00 (d0:04:92:09:cc:00), Dst: IntelCor\_66:90:77 (ac:ed:5c:66:90:77)
- Internet Protocol Version 4, Src: 157.245.50.224, Dst: 192.168.1.8
- Transmission Control Protocol, Src Port: 80, Dst Port: 62375, Seq: 1, Ack: 437, Len: 826
- Hypertext Transfer Protocol
- HTTP/1.1 401 Unauthorized\r\n
- Server: nginx/1.14.0 (Ubuntu)\r\n
- Date: Sat, 10 Oct 2020 15:21:34 GMT\r\n
- Content-Type: text/html\r\n
- Content-Length: 606\r\n
- Connection: keep-alive\r\n

nginx/1.14.0 (Ubuntu)

## 2. Export objects -> HTTP



[@DPR\\_RI](#)

[DPR RI](#)

[@DPR\\_RI](#)

[DPR RI](#)

[WWW.DPR.GO.ID](http://WWW.DPR.GO.ID)

### 3. http.host == ppid.dpr.go.id

The screenshot shows a Windows Command Prompt window and a Wireshark network traffic analysis window.

**Command Prompt Output:**

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 90ms, Maximum = 259ms, Average = 156ms

C:\Users\hnp>ping testing.mekanis.me

Pinging testing.mekanis.me [157.245.50.224] with 32 bytes of data:
Reply from 157.245.50.224: bytes=32 time=394ms TTL=50
Reply from 157.245.50.224: bytes=32 time=273ms TTL=50

Ping statistics for 157.245.50.224:
  Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 273ms, Maximum = 394ms, Average = 333ms
Control-C
^C
C:\Users\hnp>ping ppid.dpr.go.id

Pinging ppid.dpr.go.id [118.98.77.162] with 32 bytes of data:
Reply from 118.98.77.162: bytes=32 time=75ms TTL=57
Reply from 118.98.77.162: bytes=32 time=63ms TTL=57
Reply from 118.98.77.162: bytes=32 time=176ms TTL=57

Ping statistics for 118.98.77.162:
  Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
  Minimum = 63ms, Maximum = 176ms, Average = 104ms
Control-C
^C
C:\Users\hnp>
```

**Wireshark Network Traffic Analysis:**

The Wireshark window shows a packet capture on the interface `soal_jarkom_modul1_no1-5.10.pcapng`. The filter is `http.host == ppid.dpr.go.id`. The packet list shows several HTTP requests and responses. The selected packet (No. 29776) is an HTTP POST request to `http://ppid.dpr.go.id/index/login` with a content type of `application/x-www-form-urlencoded`.

**Packet Details:**

- Cookie: `_ga=GA1.3.2623363055.1602343276; _gid=GA1.3.1067745816.1602343276; _gat_gtag_UA_32782980_1=1; PHPSESSID=g1d81kvag2rp0hchiqugnunlt5\r\n`
- [Full request URI: `http://ppid.dpr.go.id/index/login`]
- [HTTP request 3/6]
- [Prev request in frame: 29557]
- [Response in frame: 29776]
- [Next request in frame: 29778]
- File Data: 39 bytes
- HTML Form URL Encoded: `application/x-www-form-urlencoded`
- Form item: "username" = "10pemuda"
- Form item: "password" = "guncangdunia"

**Packet Bytes:**

The packet bytes section shows the raw data of the HTTP request, including the cookie and form data.

HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "username" = "10pemuda"
- Form item: "password" = "guncangdunia"

#### 4. http.authbasic

No.	Time	Source	Destination	Protocol	Length	Info
21290	75.869963	192.168.1.8	157.245.50.224	HTTP	555	GET / HTTP/1.1
21294	75.970612	192.168.1.8	157.245.50.224	HTTP	462	GET /favicon.ico HTTP/1.1
31651	115.916332	192.168.1.8	157.245.50.224	HTTP	574	GET / HTTP/1.1
31658	115.986325	192.168.1.8	157.245.50.224	HTTP	484	GET /networking_meme.png HTTP/1.1
31852	116.134666	192.168.1.8	157.245.50.224	HTTP	476	GET /favicon.ico HTTP/1.1

> Frame 21294: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on interface \Device\NPF\_{02A8FB91-1186-4468-AC10-6384A19F3AFD}, id 0  
 > Ethernet II, Src: IntelCor\_66:90:77 (acd:5c:66:90:77), Dst: Fiberhom\_09:cc:00 (d0:04:92:09:cc:00)  
 > Internet Protocol Version 4, Src: 192.168.1.8, Dst: 157.245.50.224  
 > Transmission Control Protocol, Src Port: 62375, Dst Port: 80, Seq: 938, Ack: 1282, Len: 408  
 > Hypertext Transfer Protocol  
 > GET /favicon.ico HTTP/1.1\r\n  
 Host: testing.mekansis.me\r\n  
 Connection: keep-alive\r\n  
 > Authorization: Basic bmFudG6EYmNcw==\r\n  
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.0.4240.75 Safari/537.36\r\n  
 Accept: image/avif,image/webp,image/apng,image/\*,\*/\*;q=0.8\r\n  
 Referer: http://testing.mekansis.me/\r\n

- 21290 75.869963 192.168.1.8 157.245.50.224 HTTP 555  
GET / HTTP/1.1
- 31651 115.916332 192.168.1.8 157.245.50.224 HTTP 574  
GET / HTTP/1.1
- 21294 75.970612 192.168.1.8 157.245.50.224 HTTP 462  
GET /favicon.ico HTTP/1.1
- 31852 116.134666 192.168.1.8 157.245.50.224 HTTP 476  
GET /favicon.ico HTTP/1.1
- 31658 115.986325 192.168.1.8 157.245.50.224 HTTP 484  
GET /networking\_meme.png HTTP/1.1

## 5. http.host == aku.pengen.pw

The image shows two screenshots. The top screenshot is from Wireshark, displaying a packet capture of an HTTP GET request to `aku.pengen.pw`. The packet list shows a GET request from 192.168.1.8 to 157.245.50.224. The packet details pane shows the request structure, including the host `aku.pengen.pw` and various headers like `Cache-Control`, `Authorization`, and `Accept`. The packet bytes pane shows the raw data of the request.

The bottom screenshot is from a web browser (Chrome) showing the page `aku.pengen.pw`. The page has a dark background and contains the following text:

19:28:34

**Sebutkan urutan konfigurasi pengkabelan T568B!**

Tuliskan jawaban anda pada kolom di bawah ini. Jangan lupa screenshot lalu masukkan ke laporan. (Tombol submit memang nggak ada. Makanya screenshot aja ya)

Putih Orange - Orange - Putih Hijau - Biru - Putih  
Biru - Hijau - Putih Coklat - Coklat

oohbbibbr

192.168.0.10

**IP MAN**

**VS**

The bottom screenshot also shows a small image of a person's face in a bowl, likely a reference to the 'IP MAN' meme.

## 6. ftp-data

The image displays two screenshots of the Wireshark network protocol analyzer. The top screenshot shows a packet capture of FTP data, with a list of packets and their details. The bottom screenshot shows a detailed view of a specific packet, highlighting the FTP protocol fields and the data payload.

**Top Screenshot: Packet List and Details**

No.	Time	Source	Destination	Protocol	Length	Info
1775	54.348066	127.0.0.1	127.0.0.1	FTP-DA...	65539	FTP Data: 65495 bytes (PASV) (STOR Answer.zip)
1777	54.348150	127.0.0.1	127.0.0.1	FTP-DA...	57952	FTP Data: 57908 bytes (PASV) (STOR Answer.zip)
1814	54.352256	127.0.0.1	127.0.0.1	FTP-DA...	181	FTP Data: 57 bytes (PASV) (MLSD)
2080	62.666427	127.0.0.1	127.0.0.1	FTP-DA...	1529	FTP Data: 1485 bytes (PASV) (STOR SlotKelasWatcher.py)
2134	62.679163	127.0.0.1	127.0.0.1	FTP-DA...	165	FTP Data: 121 bytes (PASV) (MLSD)
2284	67.011834	127.0.0.1	127.0.0.1	FTP-DA...	65539	FTP Data: 65495 bytes (PASV) (STOR Twibbon GERIGI ITS 2019.png)
2286	67.011987	127.0.0.1	127.0.0.1	FTP-DA...	65539	FTP Data: 65495 bytes (PASV) (STOR Twibbon GERIGI ITS 2019.png)
2287	67.012031	127.0.0.1	127.0.0.1	FTP-DA...	65539	FTP Data: 65495 bytes (PASV) (STOR Twibbon GERIGI ITS 2019.png)
2288	67.012092	127.0.0.1	127.0.0.1	FTP-DA...	36076	FTP Data: 36032 bytes (PASV) (STOR Twibbon GERIGI ITS 2019.png)
2325	67.023069	127.0.0.1	127.0.0.1	FTP-DA...	239	FTP Data: 195 bytes (PASV) (MLSD)
2742	80.821683	127.0.0.1	127.0.0.1	FTP-DA...	1472	FTP Data: 1428 bytes (PASV) (STOR Readme)

**Bottom Screenshot: Detailed View of Packet 3335**

Frame 3335: 61 bytes on wire (488 bits), 61 bytes captured (488 bits) on interface \Device\NPF\_{...}, id 0

Null/Loopback

Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1

0100 .... = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Identification: 0x6b19 (27417)

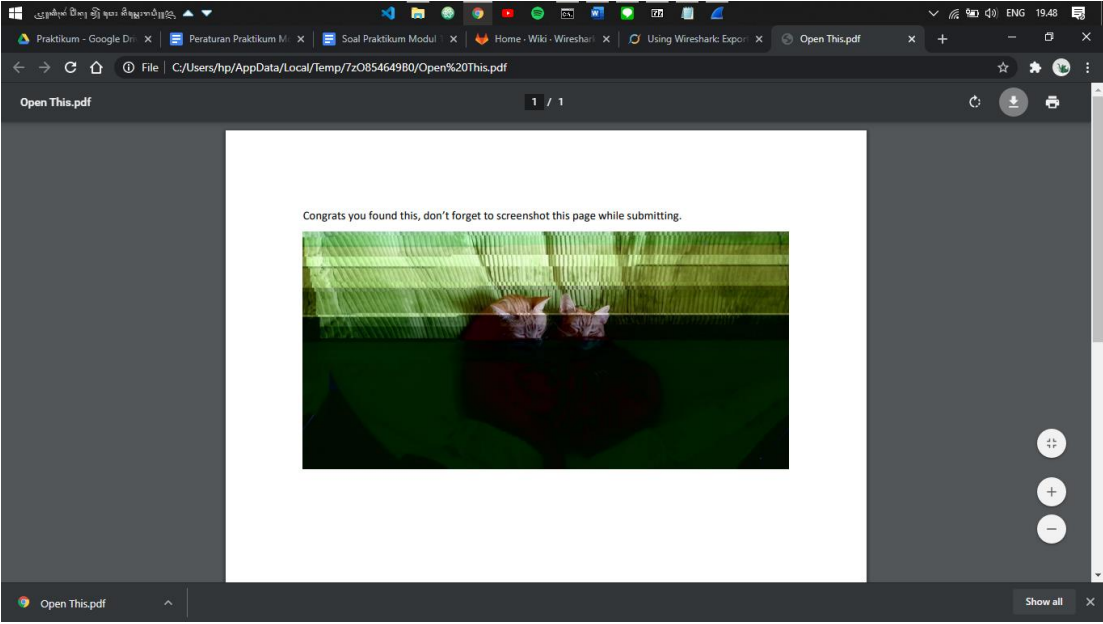
> Flags: 0x4000, Don't fragment

Fragment offset: 0

Time to live: 128

Protocol: TCP (6)

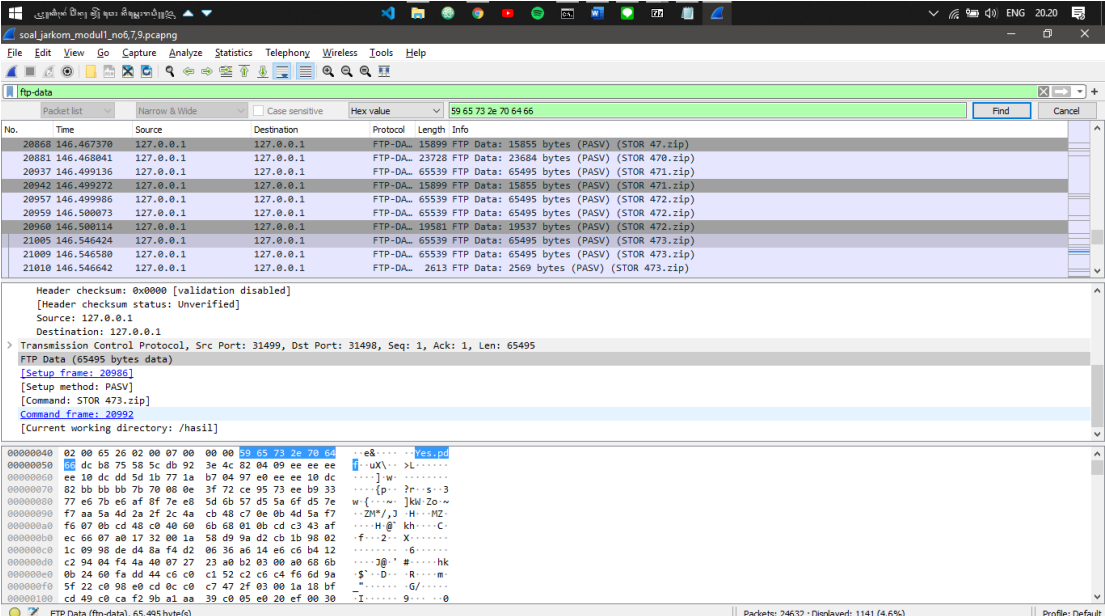
00000000 02 00 00 00 45 00 00 39 71 17 40 00 00 06 00 00 .....E..9 q@....  
00000010 7f 00 00 01 7f 00 00 01 77 c4 00 15 25 00 29 6c .....w.X..Y..l  
00000020 26 9f d1 17 50 18 27 f8 c8 19 00 00 53 54 4f 52 &...P...-STOR  
00000030 20 7a 69 70 6b 65 79 2e 74 78 74 00 0a .....zipkey. txt..





## 7. ftp-data

Yes.pdf => 59 65 73 2e 70 64 66



Header checksum: 0x0000 [validation disabled]  
[Header checksum status: Unverified]  
Source: 127.0.0.1  
Destination: 127.0.0.1  
> Transmission Control Protocol, Src Port: 31499, Dst Port: 31498, Seq: 1, Ack: 1, Len: 65495  
FTP Data (65495 bytes data)  
[Setup frame: 20986]  
[Setup method: PASV]  
[Command: STOR 473.zip]  
[Command frame: 20992]  
[Current working directory: /hasil]

00000040 02 00 65 26 02 00 07 00 00 00 59 65 73 2e 70 64 66 e8... Yes.pdf  
00000050 dc bd 75 58 5c db 92 3e 4c 02 04 09 ee ee ee 00 00 00 00 uX...L...  
00000060 ee 10 dc dd 5d 1b 77 1a b7 04 97 e0 ee ee 10 dc 00 00 }w...  
00000070 82 bb bb bb 7b 70 08 0e 3f 72 ce 95 73 ee b9 33 00 00 [p...3  
00000080 77 e6 7b e6 af 8f 7e e8 5d 6b 57 d5 5a 6f d5 7e w...kwZo~  
00000090 f7 aa 5a 4d 2a 2f 2c 4a cb 48 c7 0e 0b 4d 5a f7 00 00 -ZMj,1H-MZ  
000000a0 f6 07 0b cd 48 c8 40 68 6b 68 01 0b cd c3 43 af 00 00 -H@'kh...C  
000000b0 ec 66 07 a0 17 32 00 1a 58 d9 9a d2 cb 1b 98 02 00 00 -f...2...X...  
000000c0 1c 09 98 de d4 8a f4 d2 06 36 a6 14 e6 c6 b4 12 00 00 .....6...  
000000d0 c2 94 04 f4 4a 48 07 27 23 a0 b2 03 00 a0 60 60 00 ...3@'#...hk  
000000e0 0b 24 60 fa dd 44 c6 c0 c1 52 c2 c6 c4 f6 6d 9a 00 00 \$...D...R...m  
000000f0 5f 22 c0 98 e0 cd 0c c0 c7 47 2f 03 00 1a 18 bf 00 00 ".....G...  
00000100 cd 49 c0 ca f2 9b a1 aa 39 c0 05 e0 20 ef 00 30 00 00 I.....9...0

FTP Data (ftp-data), 65,495 byte(s)      Packets: 24632 · Displayed: 1141 (4.6%)      Profile: Default

Praktikum - G: X    Peraturan Pral: X    Soal Praktikum: X    Home - Wiki: X    Using Wiresh: X    Open This.pdf: X    Convert hexa: X    Yes.pdf: X

File | C:\Users\hp\AppData\Local\Temp\7z0064C24C9\Yes.pdf

Can You Find It?

Why you read this?  
Don't trust this writing  
You already warned  
Just leave  
SS ss tt ... don't tell anyone  
This writing actually contains secrets  
Page, image, hidden text?  
And some steganography?  
Back days were so wonderful  
To think and remember  
Work 😊

PS: Don't forget to screenshot this page

Open This.pdf      Show all



## 8. ftp.request && ip.addr == 198.246.117.106

Current filter: ftp.request && ip.addr == 198.246.117.106

No.	Time	Source	Destination	Protocol	Length	Info
158	36.024389	192.168.0.128	198.246.117.106	FTP	61	Request: CWD /
159	36.272134	198.246.117.106	192.168.0.128	FTP	83	Response: 250 CWD command successful.
160	36.272821	192.168.0.128	198.246.117.106	FTP	59	Request: PWD
161	36.519631	198.246.117.106	192.168.0.128	FTP	85	Response: 257 "/" is current directory.
162	36.521381	192.168.0.128	198.246.117.106	FTP	62	Request: TYPE A
164	36.768143	198.246.117.106	192.168.0.128	FTP	74	Response: 200 Type set to A.
165	36.768781	192.168.0.128	198.246.117.106	FTP	60	Request: PASV
166	37.016562	198.246.117.106	192.168.0.128	FTP	108	Response: 227 Entering Passive Mode (198,246,117,106,283,254).
167	37.018072	192.168.0.128	198.246.117.106	FTP	67	Request: RETR Readme
172	37.287311	198.246.117.106	192.168.0.128	FTP	95	Response: 150 Opening ASCII mode data connection.
173	37.327444	192.168.0.128	198.246.117.106	TCP	54	29243 → 21 [ACK] Seq=183 Ack=468 Win=5536 Len=0

Flags: 0x4000, Don't fragment  
 Fragment offset: 0  
 Time to live: 128  
 Protocol: TCP (6)  
 Header checksum: 0x9fc4 [validation disabled]  
 [Header checksum status: Unverified]  
 Source: 192.168.0.128  
 Destination: 198.246.117.106  
 Transmission Control Protocol, Src Port: 29743, Dst Port: 21, Seq: 90, Ack: 447, Len: 13  
 File Transfer Protocol (FTP)  
 RETR Readme\r\n  
 Request command: RETR

0000 bc 0f 9a 27 37 04 c8 3d d4 7e f3 ad 00 00 45 00 ...7...E  
 0010 00 35 5d 75 40 00 06 9f c4 c0 a0 00 00 c6 f6 ...Sj...  
 0020 75 6a 74 2f 00 15 10 a7 f3 9f cd 76 61 25 50 18 ujt/...x&P  
 0030 01 01 0a 46 00 00 52 45 54 52 20 52 65 61 64 6d ...F...RE TR Readm  
 0040 65 0d 0a

Time to live (p.ttl), 1 byte(s) | Packets: 2237 · Displayed: 31 (1.4%) | Profile: Default

167 37.018072 192.168.0.128 198.246.117.106 FTP 67  
 Request: RETR Readme

## 9. ftp

Current filter: ftp

No.	Time	Source	Destination	Protocol	Length	Info
430	15.650409	127.0.0.1	127.0.0.1	FTP	86	Response: 220-FileZilla Server version 0.9.41 beta
434	15.650572	127.0.0.1	127.0.0.1	FTP	89	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
436	15.650604	127.0.0.1	127.0.0.1	FTP	105	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
438	15.650779	127.0.0.1	127.0.0.1	FTP	54	Request: AUTH TLS
446	15.666646	127.0.0.1	127.0.0.1	FTP	84	Response: 502 SSL/TLS authentication not allowed
450	15.666872	127.0.0.1	127.0.0.1	FTP	54	Request: AUTH SSL
452	15.667546	127.0.0.1	127.0.0.1	FTP	84	Response: 502 SSL/TLS authentication not allowed
482	16.834584	127.0.0.1	127.0.0.1	FTP	56	Request: USER dhana
485	16.834934	127.0.0.1	127.0.0.1	FTP	77	Response: 331 Password required for dhana
490	16.835197	127.0.0.1	127.0.0.1	FTP	59	Request: PASS dhana123
494	16.835504	127.0.0.1	127.0.0.1	FTP	59	Response: 230 logged in

Frame 482: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface \Device\NPF\_{...} id 0  
 Null/Loopback  
 Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1  
 0100 .... = Version: 4  
 .... 0101 = Header Length: 20 bytes (5)  
 Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)  
 Total Length: 52  
 Identification: 0x6635 (26165)  
 Flags: 0x4000, Don't fragment  
 Fragment offset: 0  
 Time to live: 128  
 Protocol: TCP (6)

0000 02 00 00 00 00 00 34 66 35 40 00 00 06 00 00 ...4 f5@....  
 0010 7f 00 00 01 7f 00 00 01 77 a1 00 15 57 b2 32 5d .....w...W-2  
 0020 41 53 e6 19 50 18 27 f8 c1 bc 00 00 55 53 45 52 AS..P...-USER  
 0030 20 64 68 61 6e 61 0d 0a dhana..

Version (p.version), 1 byte(s) | Packets: 24632 · Displayed: 2683 (10.9%) | Profile: Default

USER dhana\r\n PASS dhana123\r\n

## 10. Find (Ctrl + F) -> Type: Hex -> "25 50 44 46"

The screenshot shows the Wireshark interface with a packet capture of a network session. The top toolbar includes buttons for File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main display area is divided into three panes: Packet list, Packet details, and Packet bytes.

**Packet list pane:** Shows a list of captured packets. The search filter "25 50 44 46" is applied. The list includes packets 283 through 292, with details such as Time, Source, Destination, Protocol, Length, and Info.

**Packet details pane:** Displays the details of the selected packet (No. 292). It shows the Window size value (237), Calculated window size (30336), Window size scaling factor (128), Checksum (0x58d5), and Checksum Status (Unverified). It also shows the Urgent pointer (0) and the SEQ/ACK analysis.

**Packet bytes pane:** Shows the raw data of the selected packet in hexadecimal and ASCII. The hex value "25 50 44 46" is highlighted in the first four bytes of the packet data.

**Status bar:** At the bottom, it indicates "A data segment used in reassembly of a lower-level protocol (tcp.segment\_data), 1,420 byte(s)". The bottom right corner shows "Packets: 31925 · Displayed: 31925 (100.0%)" and "Profile: Default".

soal\_jarkom\_modul1\_no1-5.10.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>->

Packet list: Narrow & Wide Case sensitive Hex value 25 50 44 46 Find Cancel

No.	Time	Source	Destination	Protocol	Length	Info
283	8.313549	192.168.1.8	66.96.225.225	TCP	54	62237 → 80 [ACK] Seq=1 Ack=1 Win=131840 Len=0
284	8.314267	192.168.1.8	66.96.225.225	HTTP	513	GET /dokjdih/document/uu/1759.pdf HTTP/1.1
285	8.329259	66.96.225.225	192.168.1.8	TCP	54	80 → 62237 [ACK] Seq=1 Ack=460 Win=38336 Len=0
286	8.341942	192.168.1.8	93.184.216.34	TCP	66	62238 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
287	8.342177	192.168.1.8	93.184.216.34	TCP	66	62239 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
288	8.342368	192.168.1.8	93.184.216.34	TCP	66	62240 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
289	8.342545	192.168.1.8	93.184.216.34	TCP	66	62241 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
290	8.354426	66.96.225.225	192.168.1.8	TCP	1474	80 → 62237 [ACK] Seq=1 Ack=460 Win=38336 Len=1420 [TCP segment of a reassembled PDU]
291	8.354491	192.168.1.8	66.96.225.225	TCP	54	62237 → 80 [ACK] Seq=460 Ack=1421 Win=131840 Len=0
292	8.355378	66.96.225.225	192.168.1.8	TCP	1474	80 → 62237 [ACK] Seq=1421 Ack=460 Win=38336 Len=1420 [TCP segment of a reassembled PDU]


[Calculated window size: 131840]  
[Window size scaling factor: 256]  
Checksum: 0xf4c8 [unverified]  
[Checksum Status: Unverified]  
Urgent pointer: 0  
> [SEQ/ACK analysis]  
> [Timestamps]  
TCP payload (459 bytes)  
▼ Hypertext Transfer Protocol  
> GET /dokjdih/document/uu/1759.pdf HTTP/1.1  
Host: www.dpr.go.id  
Connection: keep-alive

0000 d0 04 92 09 cc 00 ac ed 5c 66 90 77 00 00 45 00 .....f.w...E..  
0010 01 f3 eb ce 40 00 00 06 27 44 c0 a0 01 00 42 00 ....B...D...B..  
0020 c1 e1 f3 1d 00 50 bf 2d 6e 19 4f 99 3d e4 50 16 ....P...n.O...P..  
0030 02 03 f4 c8 00 00 47 45 54 20 2f 64 6f 6b 6a 64 .....GE T /dokjd  
0040 69 68 2f 64 6f 63 75 6d 65 6e 74 2f 75 75 2f 31 ih/docum ent/uu/1  
0050 37 35 39 2e 70 64 66 20 48 54 54 50 2f 31 2e 31 759.pdf HTTP/1.1  
0060 00 0a 40 6f 73 74 3a 20 77 7f 2e 64 70 72 2e ...Host: www.dpr.  
0070 67 6f 2e 69 64 6d 0a 43 6f 6e 6e 65 63 74 69 6f go.id: c onnectio  
0080 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55 n: keep- alive..U  
0090 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d pgrade-I nsecure..  
00a0 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65 Requests : 1: Use  
00b0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 r-Agent: Mozilla  
00c0 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 4e 54 /S.O (li ndows NT

soal\_jarkom\_modul1\_no1-5.10.pcapng Packets: 31925 · Displayed: 31925 (100.0%) Profile: Default

Praktikum - Google Drive x Peraturan Praktikum Modul 1 - x Soal Praktikum Modul 1 - Go x Extract PDF file from HTTP str x 1759.pdf

D:/Users/hp/Pictures/1759.pdf



**SALINAN**

**PRESIDEN  
REPUBLIK INDONESIA**

UNDANG-UNDANG REPUBLIK INDONESIA  
NOMOR 1 TAHUN 2020

TENTANG

PENGESAHAN PERSETUJUAN KEMITRAAN EKONOMI KOMPREHENSIF  
INDONESIA-AUSTRALIA (*INDONESIA-AUSTRALIA COMPREHENSIVE ECONOMIC  
PARTNERSHIP AGREEMENT*)

DENGAN RAHMAT TUHAN YANG MAHA ESA  
PRESIDEN REPUBLIK INDONESIA,

Menimbang : a. bahwa kegiatan perdagangan merupakan salah satu sektor