

1. ip.src == 157.245.50.224

The image displays two screenshots of a network traffic analysis using Wireshark. The top screenshot shows a Command Prompt window with a ping command being executed. The bottom screenshot shows the Wireshark interface with a packet list and packet details view.

Command Prompt Output:

```

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

C:\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

C:\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
C:\Users\hp>

```

Wireshark Packet List:

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	107.374005	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	107.485418	157.245.50.224	192.168.1.8	TCP	54	80 → 62460 [ACK] Seq=1 Ack=432 Win=64128 Len=0
31511	107.485788	157.245.50.224	192.168.1.8	HTTP	893	HTTP/1.1 401 Unauthorized (text/html)

Wireshark Packet Details:

- 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

Wireshark Packet Bytes:

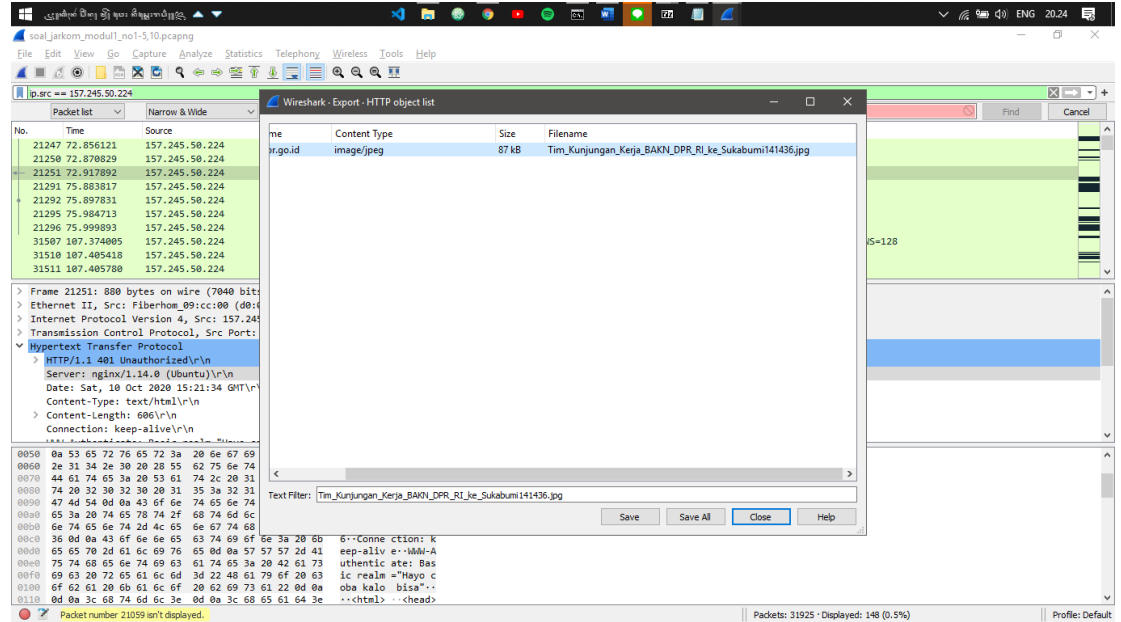
```

0050 0a 51 65 72 76 65 72 3a 20 6e 67 69 6e 78 2f 31  Server: nginx/1
0060 7e 31 34 3e 30 20 28 55 62 75 6e 74 75 29 0d 0a  1.14.0 (Ubuntu)
0070 44 61 74 65 3a 20 53 61 74 2c 20 31 30 20 4f 63  Date: Sa t, 10 Oc
0080 74 20 32 30 32 30 20 31 35 3a 32 31 3a 33 34 20  t 2020 1 5:21:34
0090 47 4d 54 0d 0a 43 6f 6e 74 65 6e 74 2d 54 79 70  GMT-Con tent-Type
00a0 65 3a 20 74 65 78 74 2f 68 74 6d 6c 0d 0a 43 6f  e: text/ html·Co
00b0 6e 74 65 6e 74 2d 4c 65 6e 67 74 68 3a 20 36 30  ntent-Le ngth: 60
00c0 36 0d 0a 43 6f 6e 65 63 74 69 6f 6e 3a 20 6b 6 6-Conne ction: k
00d0 65 65 78 2d 61 6c 69 76 65 0d 0a 57 57 57 2d 41 eep-ally e·MMW-A
00e0 75 74 68 65 6e 74 69 63 61 74 65 3a 20 42 61 73  uthentic ate: Bas
00f0 69 63 20 72 65 61 6c 6d 3d 22 48 61 79 6f 20 63 ic realm="Hayo c
0100 6f 62 61 20 6b 61 6c 6f 20 62 69 73 61 22 0d 0a oba kalo bisa"·
0110 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e  <html> ·<head>

```

nginx/1.14.0 (Ubuntu)

2. Export objects -> HTTP



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 set to `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=GA1.3.262363055.1602343276; _gid=GA1.3.1067745816.1602343276; _gat_gtag_UA_32782980_1=1; PHPSESSID=g1d81kvag2rp0hchiqugnunlt5\r\n\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:

```
0200  6e 2d 55 53 2c 65 6e 3b 71 3d 30 2e 39 0d 0a 43  n-US,en;q=0.9;C
0200  6f 6f 60 69 65 3a 20 5f 67 61 3d 47 41 31 2e 33  ookie:_ga=GA1.3
0200  2e 32 36 32 33 36 33 30 35 35 2e 31 36 30 32 33  .262363055-16023
0200  34 33 32 37 36 3b 20 5f 67 69 64 3d 47 41 31 2e  43276;_gid=GA1.
0200  32 3e 31 30 36 37 37 34 35 38 31 36 2e 31 36 30  3.1067745816-160
0200  32 33 34 33 32 37 36 30 20 5f 67 61 74 5f 67 74  2343276;_gat_gt
0200  61 67 5f 55 41 5f 33 32 37 38 32 39 30 30 5f 31  ag_UA_32782980-1
02f0  34 31 3b 20 50 40 50 53 45 53 53 49 44 34 67 69  =1;PHPSESSID=gi
0300  64 38 31 6b 76 61 67 32 72 70 30 68 63 69 68 71  d81kvag2rp0hchic
0310  75 67 6e 75 6e 6c 74 35 0d 0a 0d 0a 75 73 65 72  ugnunlt5\r\n\r\n
0320  0e 61 6d 63 63 63 63 63 63 63 63 63 63 63 63 63  user
0330  73 73 77 6f 72 64 3d 67 75 6e 63 61 6e 67 64 75  password=guncangd
0340  6e 69 61 61 61 61 61 61 61 61 61 61 61 61 61 61  nlt5
```

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

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

4. http.authbasic

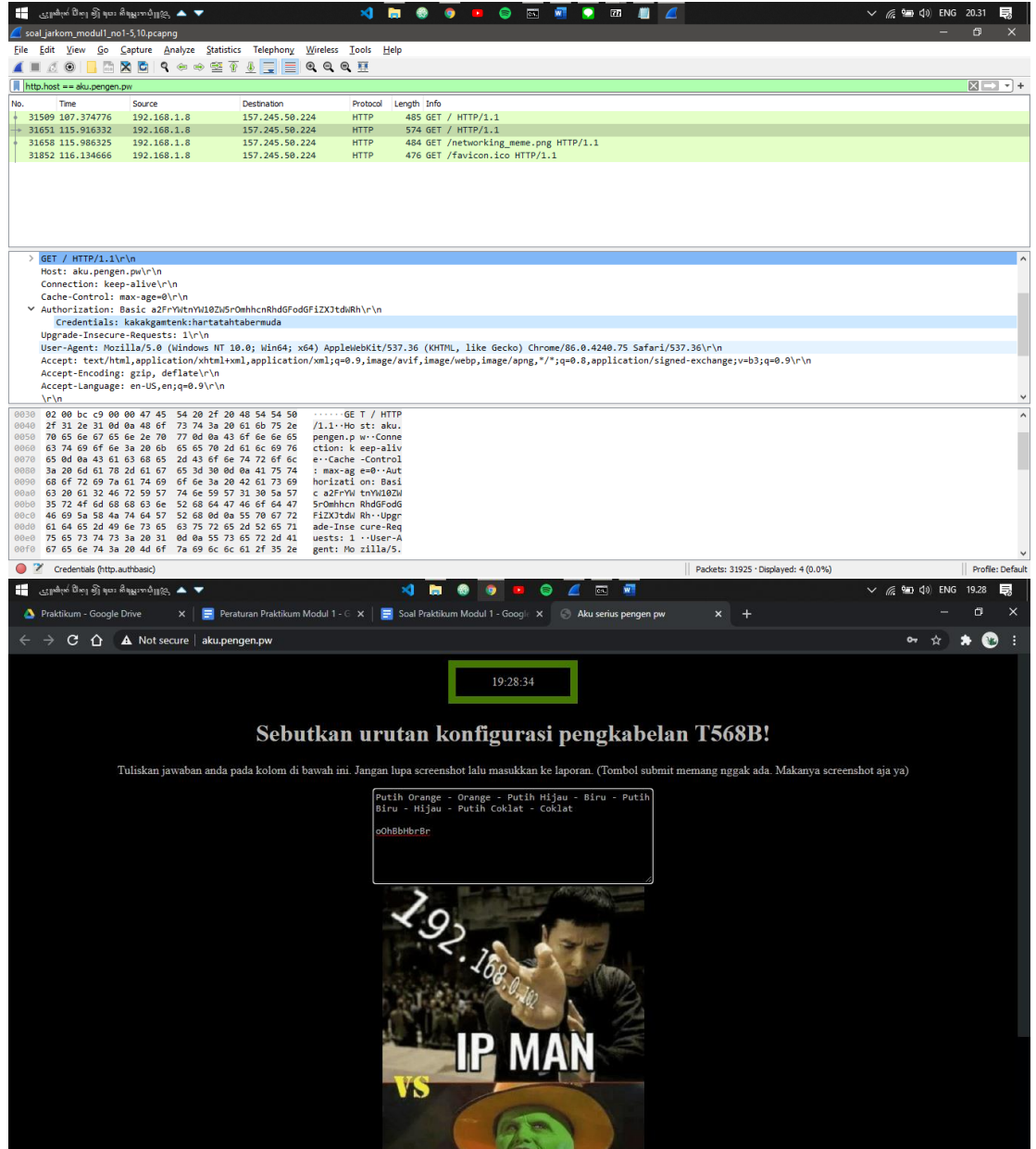
No.	Time	Source	Destination	Protocol	Length	Info
21290	75.869963	192.168.1.8	157.245.50.224	HTTP	555	GET / HTTP/1.1
21294	75.970612	192.168.1.8	157.245.50.224	HTTP	462	GET /favicon.ico HTTP/1.1
31651	115.916332	192.168.1.8	157.245.50.224	HTTP	574	GET / HTTP/1.1
31658	115.986325	192.168.1.8	157.245.50.224	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_{D2A8FB91-1186-4468-AC1D-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.mekanis.me\r\n
    Connection: keep-alive\r\n
    Authorization: Basic bmFudG6G6YmNcw==\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.mekanis.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 a Wireshark 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 show the request line `GET / HTTP/1.1` and various headers including `Host: aku.pengen.pw`, `Connection: keep-alive`, `Cache-Control: max-age=0`, `Authorization: Basic a2FrYnRnYU10ZW5rOmhhcnRhdGdGfDZkdWdhRnRn`, `Upgrade-Insecure-Requests: 1`, `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`, `Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9`, `Accept-Encoding: gzip, deflate`, and `Accept-Language: en-US,en;q=0.9`. The packet bytes show the raw HTTP request.

The bottom screenshot is a web browser showing a quiz question. The question is: "Sebutkan urutan konfigurasi pengkabelan T568B!". The instructions say: "Tuliskan jawaban anda pada kolom di bawah ini. Jangan lupa screenshot lalu masukkan ke laporan. (Tombol submit memang nggak ada. Makanya screenshot aja ya)". The answer field contains the text: "Putih Orange - Orange - Putih Hijau - Biru - Putih Biru - Hijau - Putih Coklat - Coklat". Below the answer field is a meme image of a man pointing at the camera with the text "192.168.0.10 IP MAN VS" and a green face in a bowl.

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)

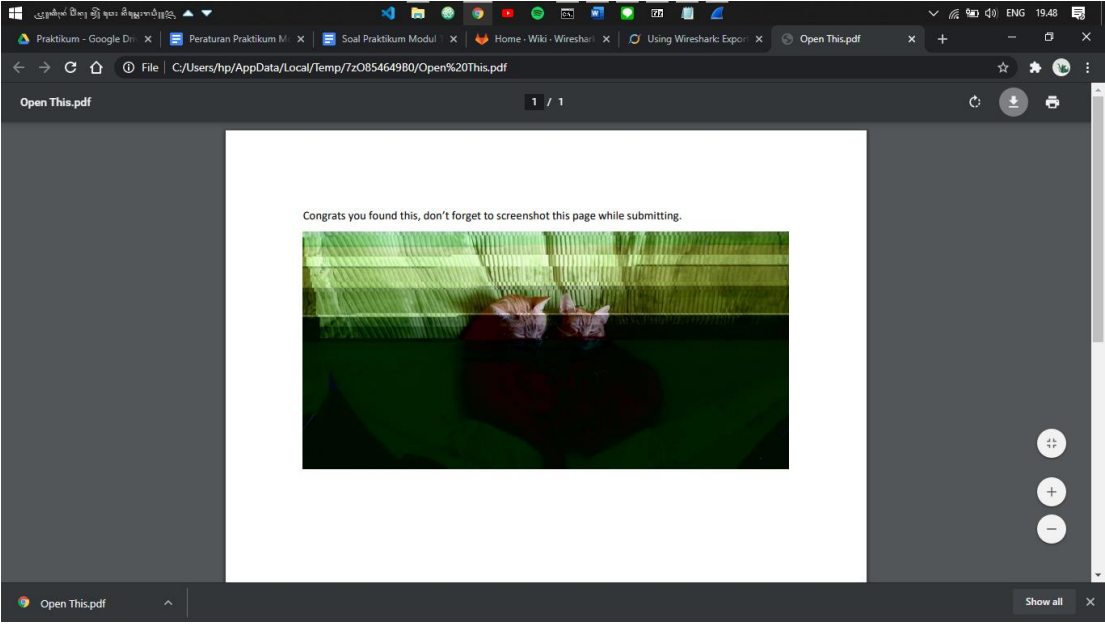
> Flags: 0x4000, Don't fragment

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 00E..9 q@....
00000010 7f 00 00 01 7f 00 00 01 77 c4 00 15 25 00 29 6cw.X..Yl
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 0d 0a zipkey. txt...



7. ftp-data

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

The image shows a screenshot of a computer screen with two windows. The top window is Wireshark, displaying a packet capture of an FTP session. The bottom window is a web browser showing a PDF file named 'Yes.pdf'.

Wireshark Packet Capture:

- Filter: ftp-data
- Search: 59 65 73 2e 70 64 66
- Packet list shows several FTP data packets (20868 to 21010).
- Packet details for packet 20892 (FTP Data) show the command: STOR 473.zip.
- Packet bytes show the hex value: 59 65 73 2e 70 64 66, which corresponds to the ASCII string "Yes.pdf".

Web Browser:

- Address bar: C:\Users\hp\AppData\Local\Temp\7z0064C24C9\Yes.pdf
- Page content: A dark-themed page with the text "Can You Find It?" and a list of questions.

Page Content:

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

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=488 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 78 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 492: 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 5dw...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: A table showing captured packets. The search filter "25 50 44 46" is applied. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info.

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 /dokjdi/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=30336 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=30336 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=30336 Len=1420 [TCP segment of a reassembled PDU]

Packet details: The selected packet (No. 292) is expanded, showing the following details:

- Window size value: 237
- [Calculated window size: 30336]
- [Window size scaling factor: 128]
- Checksum: 0x58d5 [unverified]
- [Checksum Status: Unverified]
- Urgent pointer: 0
- > [SEQ/ACK analysis]
- > [Timestamps]
- TCP payload (1420 bytes)
- [\[Reassembled PDU in frame: 872\]](#)
- TCP segment data (1420 bytes)

Packet bytes: The raw data of the selected packet is displayed in hexadecimal and ASCII. The search filter "25 50 44 46" is applied, and the corresponding bytes are highlighted in the hex view.

01e0 0d 0a 25 50 44 46 2d 31 2e 33 0d 25 e2 e3 cf d3 --255046-1.3%....
01f0 0d 0a 31 20 30 20 6f 62 6a 0d 0a 3c 3c 2f 43 72 --1 0 ob j--<</Cr
0200 65 61 74 69 6f 6e 44 61 74 65 20 28 44 3a 32 30 eationDa te (D:20
0210 32 30 30 33 31 32 31 36 30 30 35 33 20 30 37 27 20031216 0853+07'
0220 30 30 27 29 0d 0a 2f 4d 6f 64 44 61 74 65 20 28 00')-/N oDate (
0230 44 3a 32 30 32 30 33 31 32 32 30 34 39 30 36 D:202003 12204906
0240 2b 30 37 27 30 30 27 29 0d 0a 2f 43 72 65 61 74 +07'00') -:/Creat
0250 6f 72 28 28 43 61 6e 6f 6e 20 29 0d 0a 2f 50 72 or (Cano n)-:/Pr
0260 6f 64 75 61 65 72 20 28 20 29 0d 0a 3c 3c 0d 0a oducer ()->>>.
0270 65 6e 64 6f 62 6a 0d 0a 32 20 30 20 6f 62 6a 0d endobj- 2 0 obj-
0280 0a 3c 3c 2f 54 79 70 65 20 2f 43 61 74 61 6c 6f -<</Type /Catalo
0290 67 0d 0a 2f 4f 75 74 6c 69 6e 65 73 20 32 33 37 g-/Outl ines 237
02a0 20 30 20 52 0d 0a 2f 50 61 67 65 73 20 33 20 30 0 R-/P ages 3 0

A data segment used in reassembly of a lower-level protocol (tcp.segment_data), 1,420 byte(s)

Packets: 31925 · Displayed: 31925 (100.0%) 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@...D...B
0020 c1 e1 f3 1d 00 50 bf 2d 6e 19 4f 99 3d e4 50 16P...nO...P
0030 02 03 f4 c8 00 00 47 45 54 20 2f 64 6f 6b 6a 64GE T /dokjd
0040 69 60 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 77 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 (Wi 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

11. dst port 21 || src port 21

Capturing from Npcap Loopback Adapter (dst port 21 || src port 21)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>->

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	127.0.0.1	127.0.0.1	TCP	56	52325 → 21 [SYN] Seq=0 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
2	0.000213	127.0.0.1	127.0.0.1	TCP	56	21 → 52325 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=65495 WS=256 SACK_PERM=1
3	0.000365	127.0.0.1	127.0.0.1	TCP	44	52325 → 21 [ACK] Seq=1 Ack=43 Win=2619648 Len=0
4	0.004147	127.0.0.1	127.0.0.1	FTP	86	Response: 220-FileZilla Server version 0.9.41 beta
5	0.004251	127.0.0.1	127.0.0.1	TCP	44	52325 → 21 [ACK] Seq=1 Ack=43 Win=2619648 Len=0
6	0.005895	127.0.0.1	127.0.0.1	FTP	89	Response: 220-written by Tim Kosse (Tim.Kosse@gmx.de)
7	0.005956	127.0.0.1	127.0.0.1	TCP	44	52325 → 21 [ACK] Seq=1 Ack=88 Win=2619648 Len=0
8	0.006036	127.0.0.1	127.0.0.1	FTP	105	Response: 220 Please visit http://sourceforge.net/projects/filezilla/
9	0.006078	127.0.0.1	127.0.0.1	TCP	44	52325 → 21 [ACK] Seq=1 Ack=149 Win=2619648 Len=0
10	0.006207	127.0.0.1	127.0.0.1	FTP	54	Request: AUTH TLS
11	0.006333	127.0.0.1	127.0.0.1	TCP	44	21 → 52325 [ACK] Seq=149 Ack=33 Win=2619648 Len=0

Total Length: 52
Identification: 0x2dcd (11725)
> Flags: 0x0000, Don't fragment
Fragment offset: 0
Time to live: 128
Protocol: TCP (6)
Header checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source: 127.0.0.1
Destination: 127.0.0.1
> Transmission Control Protocol, Src Port: 21, Dst Port: 52325, Seq: 0, Ack: 1, Len: 0

0000 02 00 00 00 45 00 00 34 2d cd 40 00 00 06 00 00E..4.....
0010 7f 00 00 01 7f 00 00 01 00 15 cc 65 ff 68 f4 7cf.....
0020 00 53 00 77 60 12 ff 00 4c 36 00 00 02 04 ff 0fS.....
0030 01 03 03 06 01 01 04 071.....

Transmission Control Protocol (tcp), 32 bytes

Packets: 57 · Displayed: 57 (100.0%)

Profile: Default

20:42 12/10/2020

12. src port 80

Capturing from Wi-Fi (src port 80)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>->

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	103.94.190.11	192.168.43.218	TCP	66	80 → 52836 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM=1 WS=128
2	0.000594	103.94.190.11	192.168.43.218	TCP	66	80 → 52837 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1400 SACK_PERM=1 WS=128
3	0.067195	103.94.190.11	192.168.43.218	TCP	54	80 → 52836 [ACK] Seq=1 Ack=1230 Win=17152 Len=0
4	0.078414	103.94.190.11	192.168.43.218	HTTP	298	HTTP/1.1 200 OK
5	0.507302	103.94.190.11	192.168.43.218	TCP	1454	[TCP Previous segment not captured] 80 → 52836 [ACK] Seq=1645 Ack=2524 Win=19712 Len=1400
6	0.507302	103.94.190.11	192.168.43.218	TCP	1454	[TCP Out-Of-Order] 80 → 52836 [ACK] Seq=245 Ack=2524 Win=19712 Len=1400
7	0.507894	103.94.190.11	192.168.43.218	TCP	1454	80 → 52836 [ACK] Seq=3045 Ack=2524 Win=19712 Len=1400
8	0.507894	103.94.190.11	192.168.43.218	TCP	488	80 → 52836 [PSH, ACK] Seq=4445 Ack=2524 Win=19712 Len=434
9	0.949415	103.94.190.11	192.168.43.218	TCP	71	[TCP Previous segment not captured] 80 → 52836 [PSH, ACK] Seq=6279 Ack=3740 Win=22272 Len=17
10	0.949415	103.94.190.11	192.168.43.218	TCP	1454	[TCP Out-Of-Order] 80 → 52836 [ACK] Seq=4879 Ack=3740 Win=22272 Len=1400
11	0.955755	103.94.190.11	192.168.43.218	TCP	66	80 → 52836 [FIN, RST] Seq=4879 Ack=3740 Win=0 Len=0 MSS=1400 SACK_PERM=1 WS=128

> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF{0988E85D-0A40-444F-9E11-B19C2C4614CC}, id 0
> Ethernet II, Src: XiaomiCo_99:92:ef (0c:98:3b:99:92:ef), Dst: HonHaiPr_44:e1:39 (dc:a2:66:44:e1:39)
> Internet Protocol Version 4, Src: 103.94.190.11, Dst: 192.168.43.218
> Transmission Control Protocol, Src Port: 80, Dst Port: 52836, Seq: 0, Ack: 1, Len: 0

0000 dc a2 66 44 e1 39 dc 00 3b 99 92 ef 00 00 45 40 ...FD..8.....E@
0010 00 34 00 00 40 00 32 06 36 98 67 5e be 0b c0 a8 ...4..@ 2 6 g.....
0020 2b da 00 50 ce 64 db 0b 04 3d aa 37 6e b7 80 12 ...+P d...7n.....
0030 39 00 5d 5c 00 00 02 04 05 78 01 01 04 02 01 03 9 J\....x.....
0040 05 07

Source or Destination Hardware Address (eth.addr), 6 bytes

Packets: 14 · Displayed: 14 (100.0%)

Profile: Default

20:46 12/10/2020

13. dst port 443

The screenshot shows a Wireshark capture of network traffic filtered by 'dst port 443'. The packet list shows several packets, with the selected packet being a TCP segment (No. 1) from 192.168.43.218 to 172.217.194.100, Seq=552427, Ack=1, Win=257, Len=1. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.218	172.217.194.100	TCP	55	552427 → 443 [ACK] Seq=1 Ack=1 Win=257 Len=1 [TCP segment of a reassembled PDU]
2	1.076125	192.168.43.218	54.248.206.32	TCP	66	52479 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	1.900873	192.168.43.218	54.248.206.32	TCP	54	52479 → 443 [ACK] Seq=1 Ack=1 Win=16445440 Len=0
4	1.901640	192.168.43.218	54.248.206.32	TLSv1.2	428	Client Hello
5	2.364809	192.168.43.218	216.239.38.120	TLSv1.2	146	Application Data
6	2.365338	192.168.43.218	216.239.38.120	TLSv1.2	929	Application Data
7	2.366465	192.168.43.218	54.248.206.32	TCP	54	52479 → 443 [ACK] Seq=375 Ack=146 Win=16408320 Len=0
8	2.367348	192.168.43.218	54.248.206.32	TLSv1.2	1454	Change Cipher Spec, Encrypted Handshake Message
9	2.367348	192.168.43.218	54.248.206.32	TLSv1.2	978	Application Data
10	2.370192	192.168.43.218	216.239.38.120	TLSv1.2	133	Application Data

14. src host <ip>

The screenshot shows a Wireshark capture of network traffic filtered by 'src host 192.168.43.218'. The packet list shows several packets, with the selected packet being a TCP segment (No. 1) from 192.168.43.218 to 74.125.200.100, Seq=542661, Ack=443, Win=253, Len=0. The packet details pane shows the Ethernet II, Internet Protocol Version 4, and Transport Layer Security layers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
6	0.004308	192.168.43.218	74.125.200.100	TLSv1.2	298	Application Data
7	0.004493	192.168.43.218	74.125.200.100	TLSv1.2	93	Application Data
8	0.004559	192.168.43.218	74.125.200.100	TLSv1.2	1098	Application Data
9	0.260840	192.168.43.218	74.125.200.95	TCP	54	52661 → 443 [ACK] Seq=1023 Ack=40 Win=253 Len=0
10	0.260958	192.168.43.218	74.125.200.100	TCP	66	52626 → 443 [ACK] Seq=1328 Ack=425 Win=257 Len=0 SLE=600 SRE=666
11	0.261110	192.168.43.218	74.125.200.100	TCP	54	52626 → 443 [ACK] Seq=1328 Ack=666 Win=256 Len=0
12	0.263137	192.168.43.218	74.125.200.100	TLSv1.2	93	Application Data
13	0.713690	192.168.43.218	74.125.200.95	TCP	54	52661 → 443 [ACK] Seq=1023 Ack=961 Win=257 Len=0
14	0.715695	192.168.43.218	74.125.200.95	TLSv1.2	93	Application Data
15	0.716611	192.168.43.218	74.125.200.95	TCP	54	52661 → 443 [ACK] Seq=1062 Ack=1602 Win=254 Len=0

15. dst host monta.if.its.ac.id

Capturing from Wi-Fi (dst host monta.if.its.ac.id)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl>->

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.43.218	103.94.190.11	TCP	66	52788 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
2	0.001783	192.168.43.218	103.94.190.11	TCP	66	52789 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
3	0.252828	192.168.43.218	103.94.190.11	TCP	66	52790 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
4	0.254723	192.168.43.218	103.94.190.11	TCP	54	52788 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
5	0.254832	192.168.43.218	103.94.190.11	TCP	54	52789 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
6	0.255457	192.168.43.218	103.94.190.11	HTTP	1283	GET / HTTP/1.1
7	0.613547	192.168.43.218	103.94.190.11	TCP	54	52790 → 80 [ACK] Seq=1 Ack=1 Win=65792 Len=0
8	0.653741	192.168.43.218	103.94.190.11	TCP	54	52788 → 80 [ACK] Seq=1230 Ack=245 Win=65536 Len=0
9	0.713637	192.168.43.218	103.94.190.11	HTTP	1348	GET /index.php/berita/lihatBerita HTTP/1.1
10	1.304709	192.168.43.218	103.94.190.11	TCP	1348	[TCP Retransmission] 52788 → 80 [PSH, ACK] Seq=1230 Ack=245 Win=65536 Len=1294

Ethernet II, Src: MonHaiPr_44:e1:39 (dca2:66:44:e1:39), Dst: XiaomiCo_99:92:ef (0c:98:38:99:92:ef)

Destination: XiaomiCo_99:92:ef (0c:98:38:99:92:ef)

Address: XiaomiCo_99:92:ef (0c:98:38:99:92:ef)

.....0..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Source: MonHaiPr_44:e1:39 (dca2:66:44:e1:39)

Address: MonHaiPr_44:e1:39 (dca2:66:44:e1:39)

.....0..... = LG bit: Globally unique address (factory default)

.....0..... = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 192.168.43.218, Dst: 103.94.190.11

0100 = Version: 4

0000 0c 98 38 99 92 ef dc a2 66 44 e1 39 08 00 45 00 ..S.....fD:9...E..

0010 00 34 aa 52 40 00 00 06 3e 85 c0 a0 2b da 67 5e ..4.R@...>...+g^..

0020 be 00 ce 35 00 50 95 05 9a ba 00 00 00 00 00 02 ..5P.....

0030 fa f0 63 3d 00 00 02 04 05 b4 01 03 03 08 01 01 ..c=.....

0040 04 02 ..

Specifies if this is a locally administered or globally unique (IEEE assigned) address (eth.dst.lg), 3 bytes

Packets: 18 · Displayed: 18 (100.0%)

Profile: Default

Type here to search

20:40 12/10/2020