

Pengenalan Alat Bantu: Wireshark

Tentang Wireshark

- Wireshark merupakan sebuah perangkat lunak *open source* untuk memonitor trafik pada jaringan
- Dengan Wireshark, kita dapat mempelajari cara protokol bekerja.
- Wireshark dapat diunduh di <https://wireshark.org> dan tersedia untuk berbagai sistem operasi komputer.



Tampilan Wireshark

The screenshot displays the Wireshark interface with the following components:

- Packet Lists:** A table showing captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info.
- Packet Details:** A hierarchical tree view showing the structure of the selected packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol.
- Packet Bytes:** A hex dump of the selected packet's raw bytes, with corresponding ASCII characters shown to the right.

No.	Time	Source	Destination	Protocol	Length	Info
4420	97.4/1640	192.168.0.196	192.168.0.135	ICP	176	51/11 → 8009 [PSH, ACK] Seq=2091 ACK=2091 Win=
4421	97.478650	192.168.0.135	192.168.0.196	TCP	176	8009 → 51711 [PSH, ACK] Seq=2091 Ack=2201 Win=
4422	97.478713	192.168.0.196	192.168.0.135	TCP	66	51711 → 8009 [ACK] Seq=2201 Ack=2201 Win=2046
4423	97.788591	192.168.0.196	54.172.73.98	TCP	54	[TCP Keep-Alive] 54293 → 443 [ACK] Seq=780 Ack
4424	97.997860	192.168.0.102	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
4425	98.102865	54.172.73.98	192.168.0.196	TCP	66	[TCP Keep-Alive ACK] 443 → 54293 [ACK] Seq=288
4426	98.240533	192.168.0.102	239.255.255.250	SSDP	167	M-SEARCH * HTTP/1.1
4427	98.512387	103.49.221.172	192.168.0.196	TLSv1	97	Application Data

```
> Frame 879: 544 bytes on wire (4352 bits), 544 bytes captured (4352 bits) on interface en0, id 0
> Ethernet II, Src: Apple_99:e8:00 (6c:40:08:99:e8:00), Dst: TendaTec_0d:88:d0 (cc:2d:21:0d:88:d0)
> Internet Protocol Version 4, Src: 192.168.0.196, Dst: 167.205.59.96
> Transmission Control Protocol, Src Port: 54377, Dst Port: 80, Seq: 1, Ack: 1, Len: 478
< Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: www.itb.ac.id\r\n
    Connection: keep-alive\r\n
    .....
```

```
0000 cc 2d 21 0d 88 d0 6c 40 08 99 e8 00 08 00 45 00  --!...l@ .....E.
0010 02 12 00 00 40 00 40 06 94 4c c0 a8 00 c4 a7 cd  ....@.@. .L.....
0020 3b 60 d4 69 00 50 cb 4e da e6 ec ab cc a8 80 18  ;`i.P-N .....
0030 08 0a 29 86 00 00 01 01 08 0a 02 fd 4d 8a 48 ae  ..)..... .M.H.
0040 84 19 47 45 54 20 2f 20 48 54 54 50 2f 31 2e 31  ..GET / HTTP/1.1
0050 0d 0a 48 6f 73 74 3a 20 77 77 77 2e 69 74 62 2e  ..Host: www.itb.
0060 61 63 2e 69 64 0d 0a 43 6f 6e 6e 65 63 74 69 6f  ac.id.C onnectio
0070 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d 0a 55  n: keep- alive..U
0080 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72 65 2d  pgrade-I nsecure-
0090 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 73 65  Requests : 1..Use
```

→ Packet Lists

→ Packet Details

→ Packet Bytes