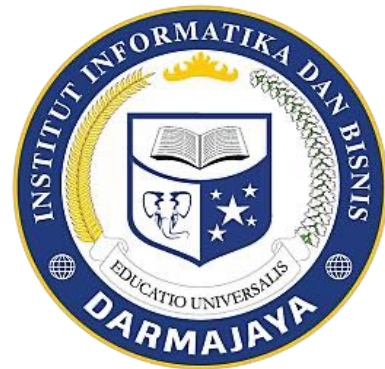


*Bahan Ajar*

## Modul Praktikum

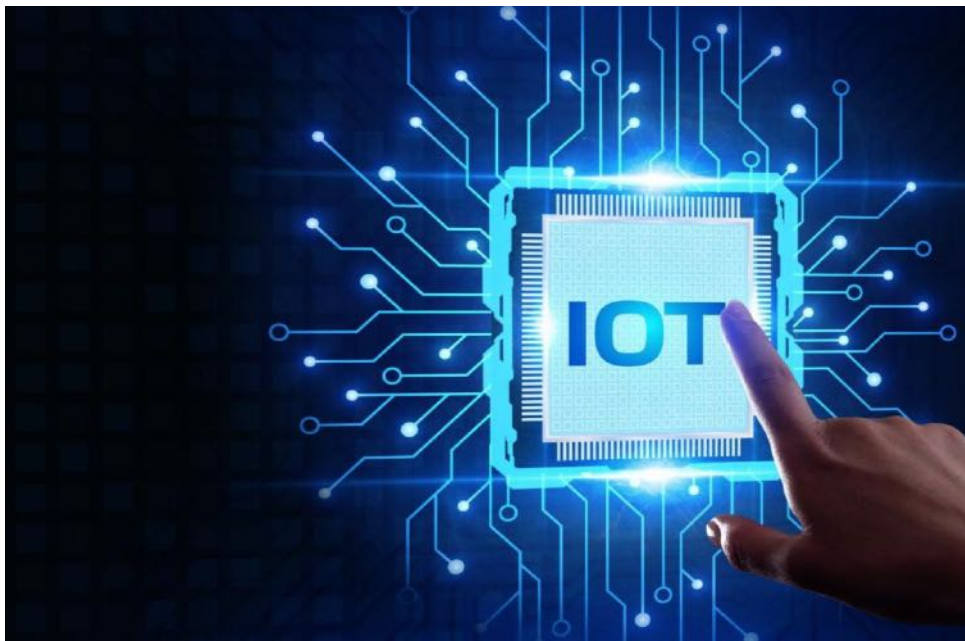
# INTERNET of THINGS (IoT Security)

Kode Matakuliah: SKO21431



Penyusun:

Bayu Nugroho. S.Kom., M.Eng



**PROGRAM STUDI SISTEM KOMPUTER  
FAKULTAS ILMU KOMPUTER  
INSTITUT INFORMATIKA DAN BISNIS DARMAJAYA  
2023**

## DAFTAR ISI

Halaman Judul.....	1
DAFTAR ISI.....	2
Modul 1.....	4
Installation IoT Server (WMware).....	4
JOBSHEET 1.....	11
Modul 2.....	12
Installation IoT Server (Windows Server).....	12
JOBSHEET 2.....	21
Modul 3.....	22
Installation IoT Server (XAMPP).....	22
JOBSHEET 3.....	25
Modul 4.....	26
Wireshark Installation (Windows).....	26
JOBSHEET 4.....	36
Modul 5.....	37
Wireshark Installation (Linux).....	37
JOBSHEET 5.....	46
Modul 6.....	47
Wireshark Menu.....	47
JOBSHEET 6.....	52
Modul 7.....	54
Capturing Live Network Data (http Protocol).....	54
JOBSHEET 7.....	56

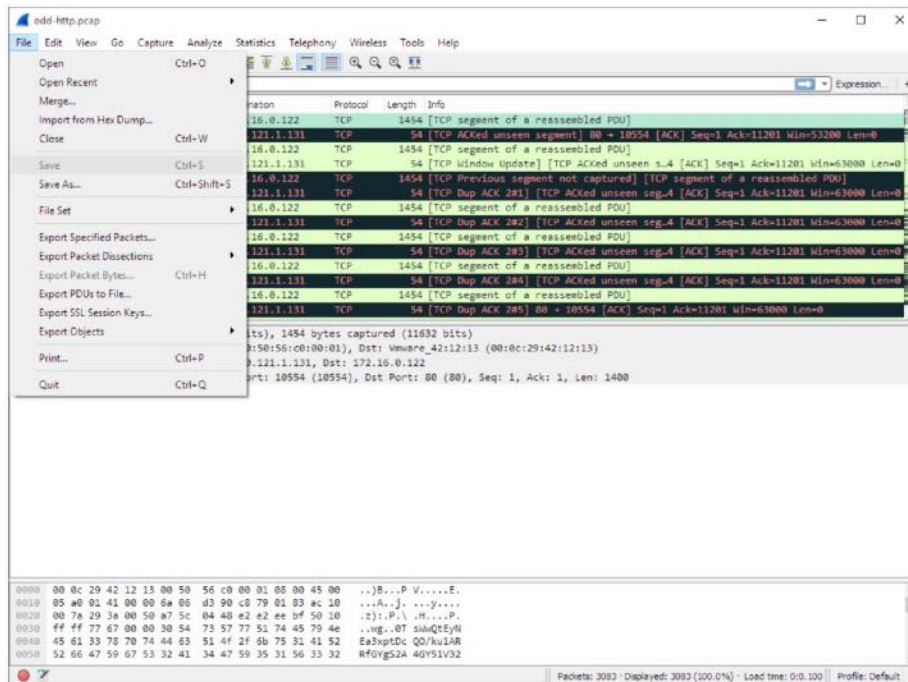
Modul 8.....	57
Ujian Tengah Semester (UTS).....	57
Modul 9.....	58
Capturing Live Network Data (tcp Protocol).....	58
JOBSHEET 9.....	58
Modul 10.....	59
Capturing Live Network Data (udp Protocol).....	59
JOBSHEET 10.....	59
Modul 11.....	60
Capturing Live Network Data (telnet Protocol).....	60
JOBSHEET 11.....	60
Modul 12.....	61
Capturing Live Network Data (ssh Protocol).....	61
JOBSHEET 12.....	61
Modul 13.....	62
Capturing Live Network Data (arp Protocol).....	62
JOBSHEET 13.....	62
Modul 14.....	63
IoT Controlling For Smart Home System.....	63
JOBSHEET 14.....	63
Modul 15.....	64
IoT Security For Smart Home System.....	64
JOBSHEET 15.....	64
Modul 16.....	65
Ujian Akhir Semester (UAS).....	65

# Modul 6

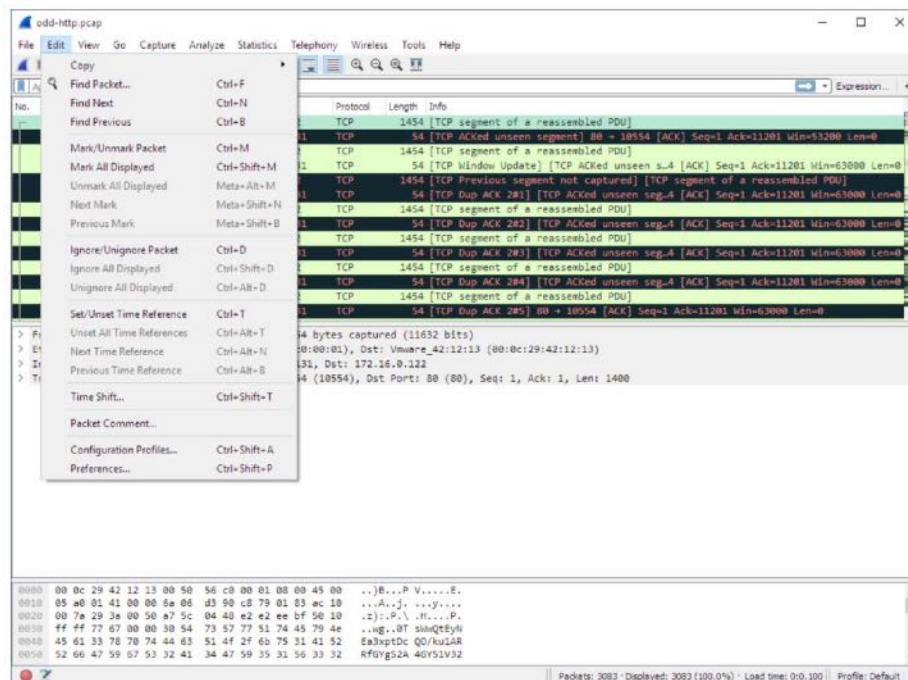
## Wireshark Menu

The Wireshark file menu contains the fields shown:

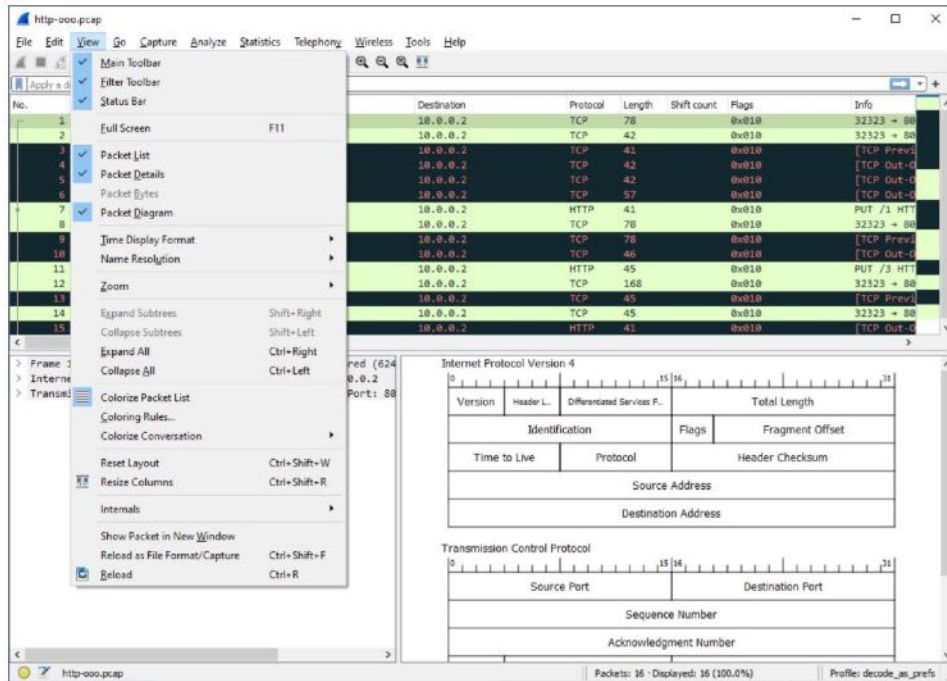
File:



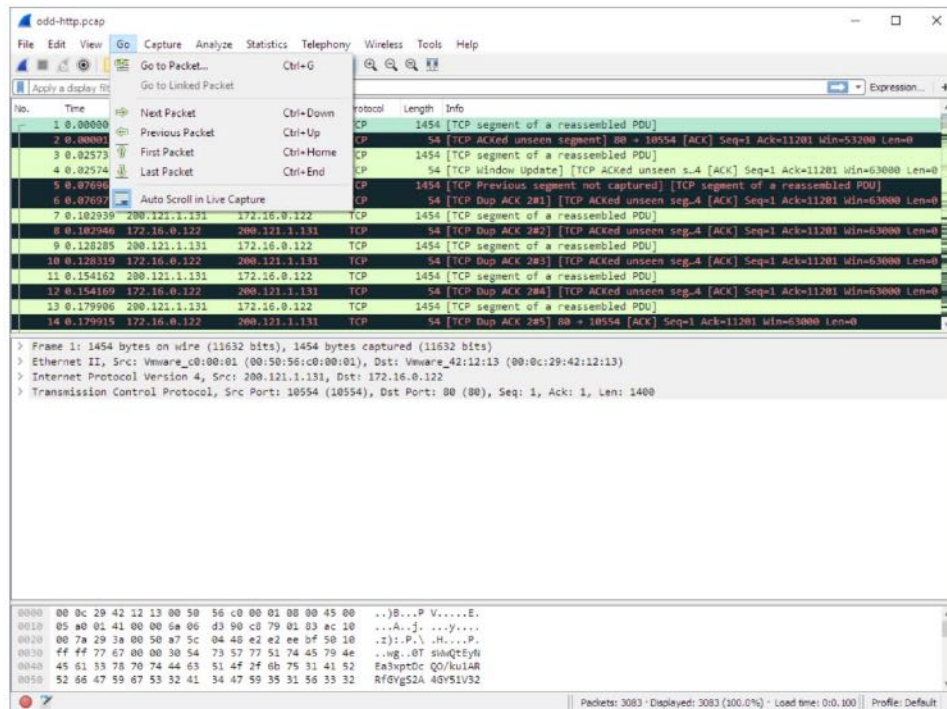
Edit:



View:



Go:



## Capture:

The screenshot shows the Wireshark interface with a capture of an HTTP GET request. The main pane displays a list of captured packets, with the selected packet (No. 2) being a TCP segment. The details pane shows the structure of the packet, including the Ethernet II header, the IP header, and the TCP header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.0	10.0.0.0	TCP	1454	[TCP segment of a reassembled PDU]
2	0.000011	10.0.0.0	10.0.0.0	TCP	1454	[TCP ACKed unseen segment] Seq=10954 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
3	0.025738	10.0.0.0	10.0.0.0	TCP	1454	[TCP segment of a reassembled PDU]
4	0.025749	10.0.0.0	10.0.0.0	TCP	54	[TCP Window Update] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
5	0.076967	200.121.1.131	172.16.0.122	TCP	1454	[TCP Previous segment not captured] [TCP segment of a reassembled PDU]
6	0.076978	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 281] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
7	0.102939	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
8	0.102946	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 282] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
9	0.128285	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
10	0.128310	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 283] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
11	0.154162	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
12	0.154169	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 284] [TCP ACKed unseen seq=4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13	0.179906	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
14	0.179915	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 285] Seq=10954 [ACK] Seq=1 Ack=11201 Win=63000 Len=0

Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)  
 > Ethernet II, Src: Vmware\_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware\_42:12:13 (00:0c:29:42:12:13)  
 > Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122  
 > Transmission Control Protocol, Src Port: 10954 (10954), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400

## Analyze:

The screenshot shows the Wireshark interface with the analysis of a selected TCP segment. The main pane displays a list of captured packets, with the selected packet (No. 2) being a TCP segment. The details pane shows the structure of the packet, including the Ethernet II header, the IP header, and the TCP header. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.0.0.0	10.0.0.0	TCP	78	32323 → 80 [ACK] Seq=1 Ack=1 Win=8192 Len=38
2	0.000001	10.0.0.0	10.0.0.0	TCP	42	32323 → 80 [ACK] Seq=39 Ack=1 Win=8192 Len=2
3	0.000002	10.0.0.0	10.0.0.0	HTTP	41	[TCP Previous segment not captured] Continuation
4	0.000004	10.0.0.0	10.0.0.0	TCP	42	[TCP Out-Of-Order] 32323 → 80 [ACK] Seq=41
5	0.000004	10.0.0.0	10.0.0.0	TCP	42	[TCP Out-Of-Order] 32323 → 80 [ACK] Seq=41
6	0.000005	10.0.0.0	10.0.0.0	TCP	57	[TCP Out-Of-Order] 32323 → 80 [ACK] Seq=43
7	0.000006	10.0.0.0	10.0.0.0	HTTP	41	Continuation
8	0.000007	10.0.0.0	10.0.0.0	TCP	78	32323 → 80 [ACK] Seq=62 Ack=1 Win=8192 Len=38

Frame 1: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface  
 > Internet Protocol Version 4, Src: 10.0.0.0, Dst: 10.0.0.0  
 > Transmission Control Protocol, Src Port: 32323, Dst Port: 80  
 Source Port: 32323  
 Destination Port: 80  
 [Stream index: 0]  
 [TCP Segment Len: 38]  
 Sequence Number: 1 (relative sequence number)  
 Sequence Number (raw): 100  
 [Next Sequence Number: 39 (relative sequence number)]  
 Acknowledgment Number: 1 (relative ack number)  
 Acknowledgment number (raw): 0  
 0101 ... = Header Length: 20 bytes (5)  
 > Flags: 0x010 (ACK)  
 Window: 8192

## Statistic:

The screenshot shows the Wireshark interface with the 'Statistics' window open. The left pane lists various statistics categories, including:

- Resolved Addresses
- Protocol Hierarchy
- Conversations
- Endpoints
- Packet Lengths
- I/O Graph
- Service Response Time
- DHCP (BOOTP) Statistics
- ONC-RPC Programs
- 25Wnet
- ANCP
- BACnet
- Collectd
- DNS
- Flow Graph
- HART-IP
- HPFEEDS
- HTTP
- HTTP2
- Sametime
- TCP Stream Graphs
- UDP Multicast Streams
- IPv4 Statistics
- IPv6 Statistics

The right pane shows a detailed view of a selected packet (Frame 1454), displaying its structure and raw bytes. The packet is a TCP segment with the following details:

- Length: 1454 bytes
- Info: [TCP segment of a reassembled PDU]
- 54 [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- 54 [TCP Window Update] [TCP ACKed unseen s..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- 1454 [TCP Previous segment not captured] [TCP segment of a reassembled PDU]
- 54 [TCP Dup ACK 281] [TCP ACKed unseen seg..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- 1454 [TCP segment of a reassembled PDU]
- 54 [TCP Dup ACK 282] [TCP ACKed unseen seg..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- 1454 [TCP segment of a reassembled PDU]
- 54 [TCP dup ACK 283] [TCP ACKed unseen seg..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- 1454 [TCP segment of a reassembled PDU]
- 54 [TCP dup ACK 284] [TCP ACKed unseen seg..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- 1454 [TCP segment of a reassembled PDU]
- 54 [TCP Dup ACK 285] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0

The packet bytes pane shows the raw data: 0000 00 0c 29 42 12 13 00 50 56 c0 00 01 08 00 45 00 ..)B...P V.....E.

## Telephony:

The screenshot shows the Wireshark interface with the 'Telephony' window open. The left pane lists various telephony-related statistics categories, including:

- VoIP Cells
- ANSI
- GSM
- IAX2 Stream Analysis
- LTE
- ISUP Messages
- MTP3
- RTP
- RTSP
- SCTP
- SMPP Operations
- UCP Messages
- H.225
- SIP Flows
- SIP Statistics
- WAP-WSP Packet Counter

The right pane shows a detailed view of a selected packet (Frame 1454), displaying its structure and raw bytes. The packet is a TCP segment with the following details:

- Length: 1454 bytes
- Info: [TCP segment of a reassembled PDU]
- ACKed unseen segment] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- segment of a reassembled PDU]
- Window Update] [TCP ACKed unseen s..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- Previous segment not captured] [TCP segment of a reassembled PDU]
- Dup ACK 281] [TCP ACKed unseen seg..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- segment of a reassembled PDU]
- Dup ACK 282] [TCP ACKed unseen seg..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- segment of a reassembled PDU]
- Dup ACK 283] [TCP ACKed unseen seg..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- segment of a reassembled PDU]
- Dup ACK 284] [TCP ACKed unseen seg..4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
- segment of a reassembled PDU]
- Dup ACK 285] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0

The packet bytes pane shows the raw data: 0000 00 0c 29 42 12 13 00 50 56 c0 00 01 08 00 45 00 ..)B...P V.....E.

## Wireless:

The screenshot shows a Wireshark capture of wireless traffic. The main pane displays a list of packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 14 is selected, and the packet details pane shows the following structure:

- Frame 14: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
- Ethernet II, Src: Vmware\_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware\_42:12:13 (00:0c:29:42:12:13)
- Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
- Transmission Control Protocol, Src Port: 10554 (10554), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 1400
- Application Data (application/javascript)

The packet bytes pane shows the raw hex and ASCII data for the selected packet.

## Tools:

The screenshot shows a Wireshark capture of SMTP traffic. The main pane displays a list of packets. Packet 14 is selected, and the packet details pane shows the following structure:

- Frame 14: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
- Ethernet II, Src: Cradlepoint\_3c:17:c2 (00:e0:1c:3c:17:c2), Dst: Netgear\_d9:81:60 (00:1f:33:d9:81:60)
- Internet Protocol Version 4, Src: 10.10.1.4, Dst: 74.53.140.153
- Transmission Control Protocol, Src Port: 1470, Dst Port: 25, Seq: 52, Ack: 355, Len: 18
- Simple Mail Transfer Protocol

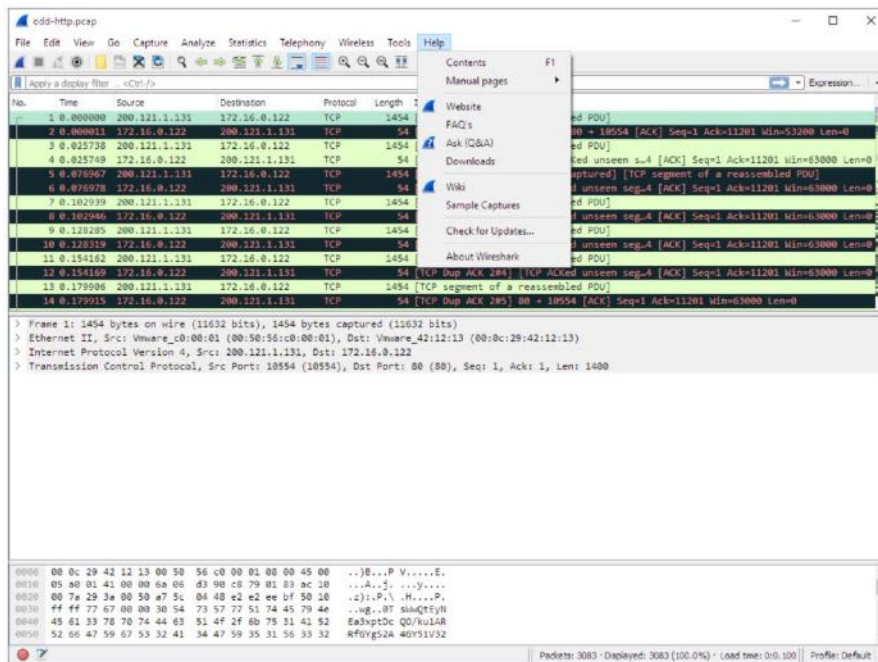
The packet bytes pane shows the raw hex and ASCII data for the selected packet, including the SMTP command: `EHLO`.

A dialog box titled "Wireshark - Firewall ACL Rules - smtp.pcap" is open, showing the following rules for packet 14:

- # Windows Firewall (neth) rules for smtp.pcap, packet 14.
- # Source port.
- add portopening tcp 1470 Wireshark DISABLE
- # Destination port.
- add portopening tcp 25 Wireshark DISABLE
- # IPv4 source address and port.
- add portopening tcp 1470 Wireshark DISABLE 10.10.1.4
- # IPv4 destination address and port.
- add portopening tcp 25 Wireshark DISABLE 74.53.140.153

The dialog box also includes options to create rules for Windows Firewall (neth), Inbound, and Deny, along with Save, Close, Copy, and Help buttons.

## Help:



## JOB SHEET 6

Jelaskan fungsi menu “Main Toolbar” di bawah ini:

Toolbar Icon	Toolbar Item	Menu Item
	Start	Capture → Start
	Stop	Capture → Stop
	Restart	Capture → Restart
	Options...	Capture → Options...
	Open...	File → Open...
	Save As...	File → Save As...
	Close	File → Close
	Reload	View → Reload

Toolbar Icon	Toolbar Item	Menu Item
	Go Back	Go → Go Back
	Go Forward	Go → Go Forward
	Go to Packet...	Go → Go to Packet...
	Go To First Packet	Go → First Packet
	Go To Last Packet	Go → Last Packet
	Auto Scroll in Live Capture	View → Auto Scroll in Live Capture
	Colorize	View → Colorize

LAPORAN HASIL PERCOBAAN: