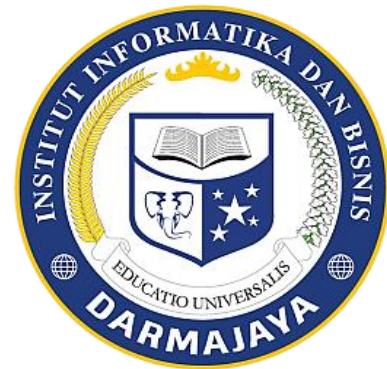


Bahan Ajar

Modul Praktikum

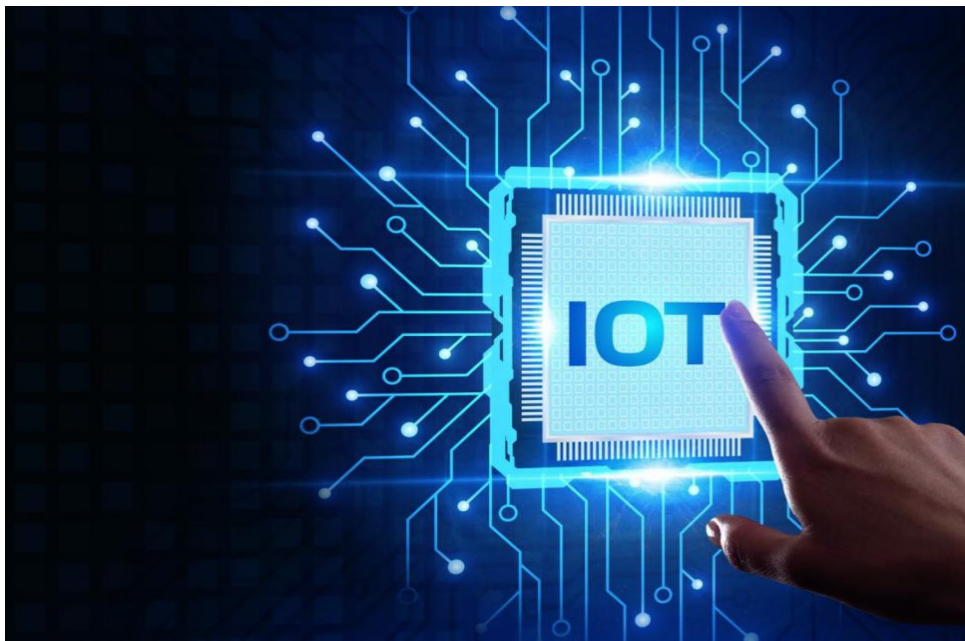
INTERNET of THINGS (IoT Security)

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

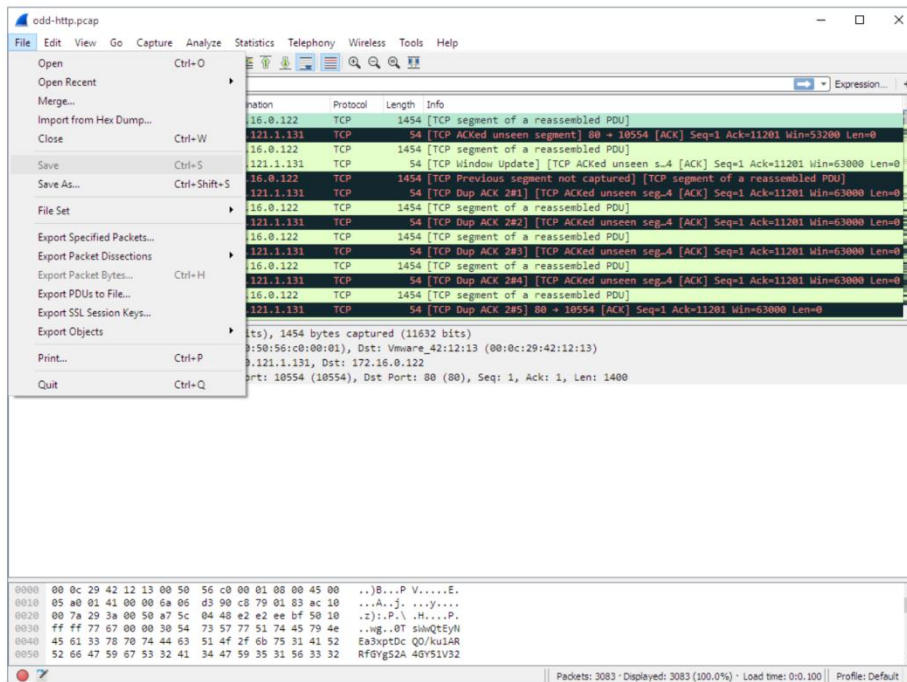
Modul 8.....	57
Ujian Tengah Semester (UTS).....	57
Modul 9.....	58
Capturing Live Network Data (tcp Protocol).....	58
JOBSHEET 9.....	58
Modul 10.....	59
Capturing Live Network Data (udp Protocol).....	59
JOBSHEET 10.....	59
Modul 11.....	60
Capturing Live Network Data (telnet Protocol).....	60
JOBSHEET 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

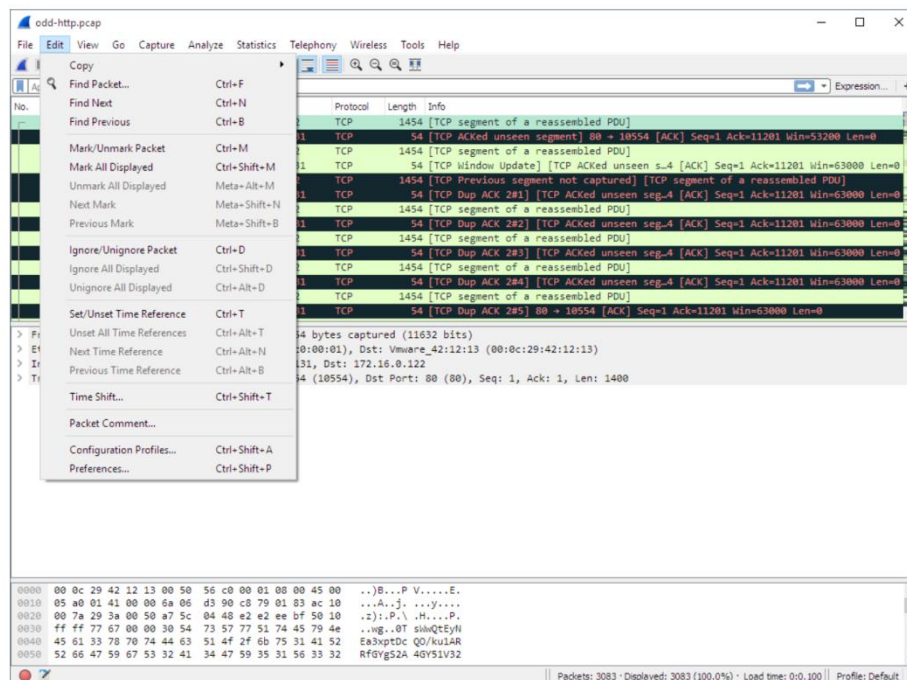
Wireshark Menu

The Wireshark file menu contains the fields shown:

File:



Edit:



View:

The screenshot shows the Wireshark application window titled 'http-ooo.pcap'. The 'View' menu is open, displaying various options for customizing the interface. The background shows a packet capture list with columns for No., Time, Destination, Protocol, Length, Shift count, Flags, and Info. The selected packet (No. 7) is highlighted in green.

Go:

The screenshot shows the Wireshark application window titled 'odd-http.pcap'. The 'Go' menu is open, displaying options for navigating through the packet capture. The background shows a packet capture list with columns for No., Time, Protocol, Length, and Info. The selected packet (No. 14) is highlighted in green.

Capture:

The screenshot shows the Wireshark interface with a capture named 'odd-http.pcap'. The packet list pane displays a list of captured packets, with the selected packet being a TCP segment of a reassembled PDU. The packet details pane shows the following layers:

- 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

The packet bytes pane shows the raw hex and ASCII data of the captured packet.

Analyze:

The screenshot shows the Wireshark interface with a capture named 'http-ooo.pcap'. The packet list pane displays a list of captured packets, with the selected packet being a TCP segment. The packet details pane shows the following layers:

- Ethernet II, Src: 10.0.0.0, Dst: 10.0.0.0
- Internet Protocol Version 4, Src: 10.0.0.0, Dst: 10.0.0.0
- Transmission Control Protocol, Src Port: 32323, Destination Port: 80, [Stream index: 0], [TCP Segment Len: 38]

The packet bytes pane shows the raw hex and ASCII data of the captured packet.

Statistic:

The screenshot shows the Wireshark interface with the 'Statistics' pane open. The 'Protocol Hierarchy' tree on the left lists various protocols, with 'HTTP' selected. The main pane displays a list of 1454 TCP segments, including reassembled PDUs and duplicate ACKs. The packet details pane shows the structure of a TCP segment (80 bytes) with sequence number 1, acknowledgment number 1, and length 1400. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination
1	0.000000	200.121.1.131	172.16.0.122
2	0.000011	172.16.0.122	200.121.1.131
3	0.025738	200.121.1.131	172.16.0.122
4	0.025749	172.16.0.122	200.121.1.131
5	0.076967	200.121.1.131	172.16.0.122
6	0.076978	172.16.0.122	200.121.1.131
7	0.102939	200.121.1.131	172.16.0.122
8	0.102946	172.16.0.122	200.121.1.131
9	0.128285	200.121.1.131	172.16.0.122
10	0.128319	172.16.0.122	200.121.1.131
11	0.154162	200.121.1.131	172.16.0.122
12	0.154169	172.16.0.122	200.121.1.131
13	0.179906	200.121.1.131	172.16.0.122
14	0.179915	172.16.0.122	200.121.1.131

Telephony:

The screenshot shows the Wireshark interface with the 'Telephony' pane open. The 'SIP Flows' section is selected, showing a list of SIP messages. The main pane displays a list of 1454 TCP segments, including reassembled PDUs and duplicate ACKs. The packet details pane shows the structure of a TCP segment (80 bytes) with sequence number 1, acknowledgment number 1, and length 1400. The packet bytes pane shows the raw hex and ASCII data.

No.	Time	Source	Destination
1	0.000000	200.121.1.131	172.16.0.122
2	0.000011	172.16.0.122	200.121.1.131
3	0.025738	200.121.1.131	172.16.0.122
4	0.025749	172.16.0.122	200.121.1.131
5	0.076967	200.121.1.131	172.16.0.122
6	0.076978	172.16.0.122	200.121.1.131
7	0.102939	200.121.1.131	172.16.0.122
8	0.102946	172.16.0.122	200.121.1.131
9	0.128285	200.121.1.131	172.16.0.122
10	0.128319	172.16.0.122	200.121.1.131
11	0.154162	200.121.1.131	172.16.0.122
12	0.154169	172.16.0.122	200.121.1.131
13	0.179906	200.121.1.131	172.16.0.122
14	0.179915	172.16.0.122	200.121.1.131

Wireless:

odds-http.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Bluetooth ATT Server Attributes
Bluetooth Devices
Bluetooth HCI Summary
WLAN Traffic

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	200.121.1.131	172.16.0.122	TCP	1454	[ACK] Seq=1 Ack=11201 Win=53200 Len=0
2	0.000011	172.16.0.122	200.121.1.131	TCP	54	[ACK] Seq=1 Ack=11201 Win=63000 Len=0
3	0.025738	200.121.1.131	172.16.0.122	TCP	1454	[TCP segment of a reassembled PDU]
4	0.025749	172.16.0.122	200.121.1.131	TCP	54	[TCP Window Update] [TCP ACKED unseen s=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 2#1] [TCP ACKED unseen seg-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 2#2] [TCP ACKED unseen seg-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	0.128319	172.16.0.122	200.121.1.131	TCP	54	[TCP Dup ACK 2#3] [TCP ACKED unseen seg-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 2#4] [TCP ACKED unseen seg-4 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
13	0.179986	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 2#5] [ACK] Seq=1 Ack=11201 Win=63000 Len=0

> Frame 14: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits) on interface 0
 > 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

0000 00 0c 29 42 12 13 00 50 56 c0 00 01 08 00 45 00 ..J.B...P.V.....E.
 0010 05 a0 01 41 00 00 6a 06 d3 90 c8 79 01 83 ac 10 ...A..j...y....
 0020 00 7a 29 3a 00 50 a7 5c 04 48 e2 e2 ee bf 50 10 .:):.P.\.H....P.
 0030 ff ff 77 67 00 00 30 54 73 57 77 51 74 45 79 4e ...ng..0T shwQtEYH
 0040 45 61 33 78 70 74 44 63 51 4f 2f 08 75 31 41 52 fa3pPDC QQ/KuLdR
 0050 52 66 47 59 67 53 32 41 34 47 59 35 31 56 33 32 RfGyS2A 46Y51V32

Packets: 3083 · Displayed: 3083 (100.0%) · Load time: 0:0.100 Profile: Default

Tools:

smtp.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Firewall ACL Rules
Credentials
Lua

No.	Time	Source	Destination	Protocol	Length	Info
8	1.073326	74.53.140.153	10.10.1.4	TCP	60	25 → 1470 [ACK] Seq=182 Ack=10 Win=5840 Len=0
9	1.074123	74.53.140.153	10.10.1.4	SMTP	191	S: 250-xx90.websitewelcome.com Hello GP [122.162.143.15]
10	1.076669	10.10.1.4	74.53.140.153	SMTP	66	C: AUTH LOGIN
11	1.419021	74.53.140.153	10.10.1.4	SMTP	72	S: 334 VXjlc=5hbUj6
12	1.419595	10.10.1.4	74.53.140.153	SMTP	84	C: User: Z3VycGFydGFwQHhhdHJpb3RzLmlu
13	1.761484	74.53.140.153	10.10.1.4	SMTP	72	S: 334 UGFz=3dvcQ6
14	1.762058	10.10.1.4	74.53.140.153	SMTP	72	C: Pass: chVuamFIQDEyHw==
15	2.121738	74.53.140.153	10.10.1.4	SMTP	84	S: 235 Authentication succeeded
16	2.122354	10.10.1.4	74.53.140.153	SMTP	90	C: MAIL FROM: <gurpartap@patriots.in>

> Frame 14: 72 bytes on wire (576 bits), 72 bytes captured (576 bits) on interface 0
 > 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
 Password: chVuamFIQDEyHw==

Wireshark - Credentials - smtp.pcap

Packet No.	Protocol	Username	Additional Info
14	SMTP	Z3VycGFydGFwQHhhdHJpb3RzLmlu	Username in packet 12

Close

Wireshark - Firewall ACL Rules - smtp.pcap

```
# Windows Firewall (netsh) 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
```

Create rules for Windows Firewall (netsh) Inbound Deny

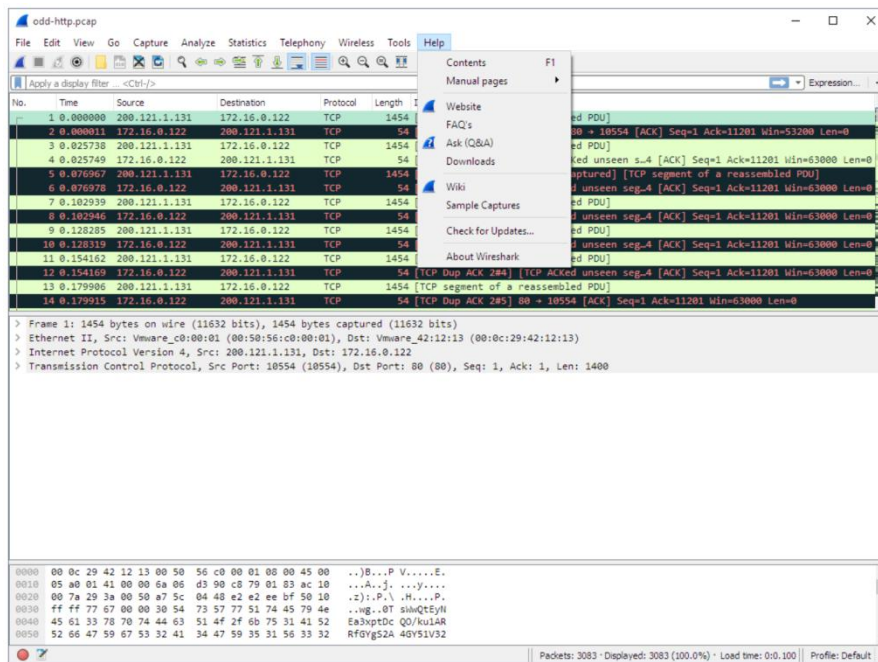
Save Close Copy Help

0020 8c 99 05 be 00 19 7e c4 53 e4 ae ec 63 12 50 18S...c:P
 0030 fe 9d 54 b1 00 00 63 48 56 75 61 6d 46 69 51 44 ...T...ch VuamFIQD
 0040 45 79 4d 77 3d 3d 0d 0eEYHw==

Password (smtp.auth.password), 16 bytes

Packets: 60 · Displayed: 60 (100.0%) Profile: smtp_default

Help:



JOBSHEET 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: