

## PRAKTIKUM 11: ANALISA PAKET DATA

**Pertemuan ke** : 11

**Total Alokasi Waktu** : 90 menit

- Materi : 15 menit
- Pre-Test : 15 menit
- Praktikum : 45 menit
- Post-Test : 15 menit

**Total Bobot Penilaian** : 100%

- Pre-Test : 20 %
- Praktik : 30 %
- Post-Test : 50 %

**Pemenuhan CPL dan CPMK:**

CPL-07	Mampu memilih, membuat dan menerapkan teknik, sumber daya, penggunaan perangkat teknik modern dan implementasi teknologi informasi untuk memecahkan masalah.
CPMK-04	Memahami pentingnya keamanan sistem dan jaringan komputer (wireless Network security)

### 11.1. DESKRIPSI CAPAIAN PEMBELAJARAN

Setelah mengikuti praktikum ini mahasiswa diharapkan mampu:

1. Memahami dan mampu menerapkan konsep wireless network security, snapping paket data

### 11.2. INDIKATOR KETERCAPAIAN PEMBELAJARAN

Indikator ketercapaian diukur dengan:

CPL-07	CPMK-04	Mahasiswa mampu analisis paket data dengan metode snapping paket data menggunakan wireshark.
--------	---------	--

### 11.3. TEORI PENDUKUNG

Wireshark merupakan salah satu network analysis tool atau disebut juga dengan protocol analysis tool atau packet sniffer. Wireshark dapat digunakan untuk troubleshooting jaringan, analisis keamanan, pengembangan software dan protocol, serta untuk keperluan edukasi. Wireshark merupakan software gratis, sebelumnya, wireshark dikenal dengan nama Ethereal. Packet sniffer sendiri diartikan sebagai sebuah program atau tool yang memiliki kemampuan untuk 'mencegat' dan melakukan pencatatan terhadap traffic data dalam jaringan. Selama terjadi aliran data dalam, packet sniffer dapat menangkap protocol data unit (PDU), melakukan decoding serta melakukan analisis terhadap isi paket berdasarkan spesifikasi RFC atau spesifikasi-spesifikasi yang lain.

Dalam berbagai kalangan praktisi Wireshark berguna antara lain untuk :

- Network administrator, untuk troubleshooting
- Teknisi keamanan jaringan memakainya untuk mengawasi jaringan

- Developer, untuk debug implementasi protocol
- Awam memakainya untuk belajar protocol jaringan

Fitur-fitur wireshark :

- Tersedia untuk Windows dan Unix
- Capturing paket data secara live dari suatu jaringan
- Menampilkan informasi paket secara sangat detail
- Membuka dan menyimpan paket data yang sudah di-capture
- Import dan export paket data dari program capturing lain
- Paket filter dalam berbagai kriteria
- Mencari paket data dalam berbagai kriteria
- Membuat statistic data.

Menu pada Wireshark :

- File : Open, merge, save, print, export, capture, quit
- Edit : mencari paket, referensi waktu, menandai paket, konfigurasi profil, set preferences
- View : menangani tampilan data dicapture termasuk pewarnaan, zooming, dll
- Go : untuk menuju ke paket tertentu
- Capture : memulai dan stop capturing, mengedit filter
- Analyze : memanipulasi filter, enable atau disable protocol yang diinginkan, dll
- Statistics : menampilkan berbagai statistic, termasuk garis besar paket yang ditampilkan.

#### 11.4. HARDWARE DAN SOFTWARE

Hardware dan software yang digunakan dalam praktikum ini yaitu:

1. Komputer.
2. Sistem operasi Linux/Windows
3. Wireshark

#### 11.5. PRE-TEST

Jawablah pertanyaan berikut (**Total Skor: 100**):

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-03	CPMK-01	Apa itu Wireshark?	30
2.	CPL-07	CPMK-04	Jelaskan kegunaan Wireshark!	70

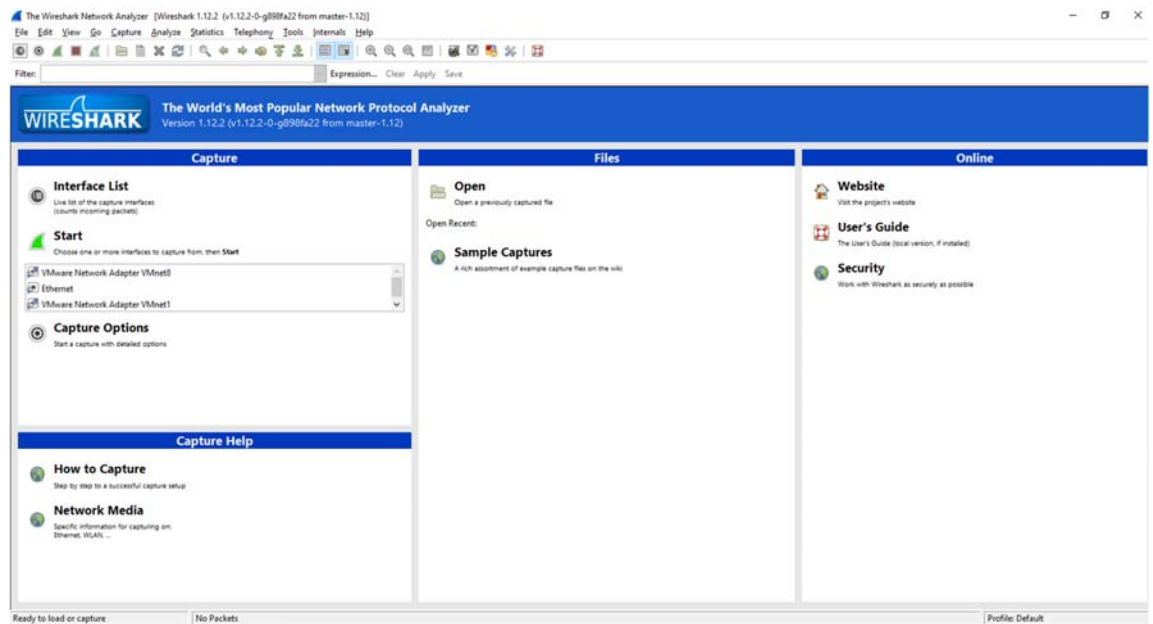
#### 11.6. LANGKAH PRAKTIKUM

**Aturan Penilaian (Total Skor: 100):**

No	CPL	CPMK	Pertanyaan	Dokumen Pendukung	Skor
1.	CPL-07	CPMK-04	Selesaikan langkah praktikum a – i	Hasil praktikum langkah a – i	100

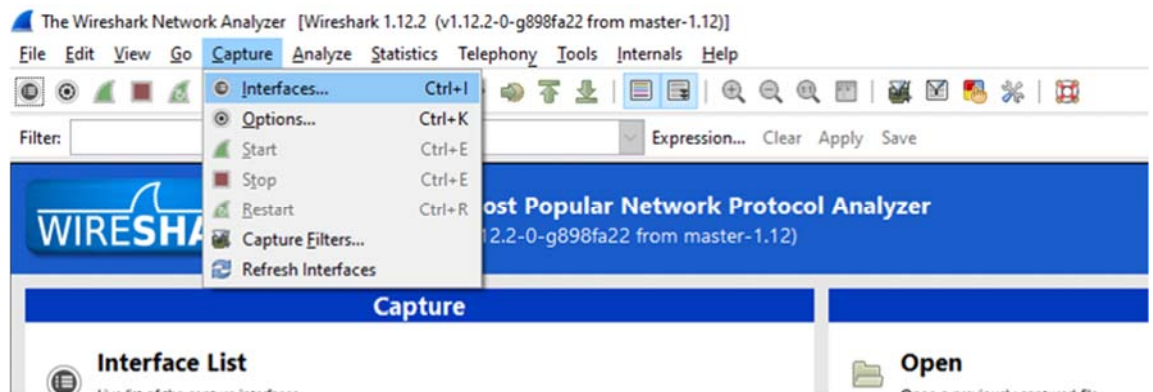
**Langkah-Langkah Praktikum:**

- Pastikan Wireshark telah terinstall
- Jalankan wireshark, akan muncul tampilan awal dari wireshark



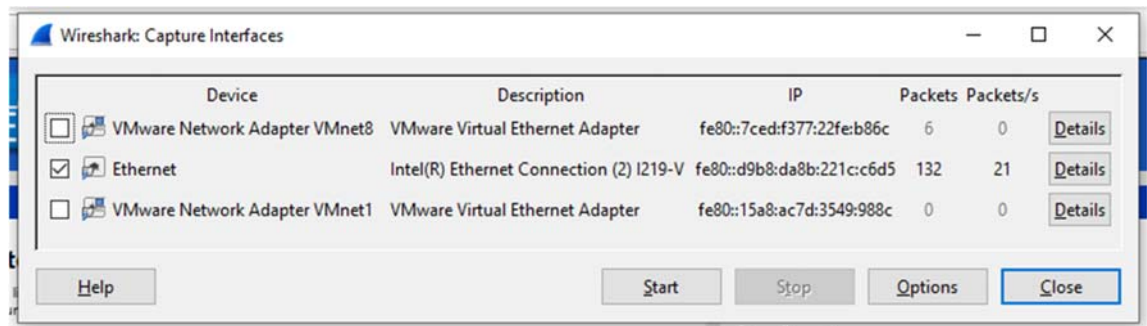
Gambar 11. 1 Halaman interface saat membuka wireshark

- Untuk memulai menangkap paket-paket data, pilih menu **Capture** lalu pilih **Interface**



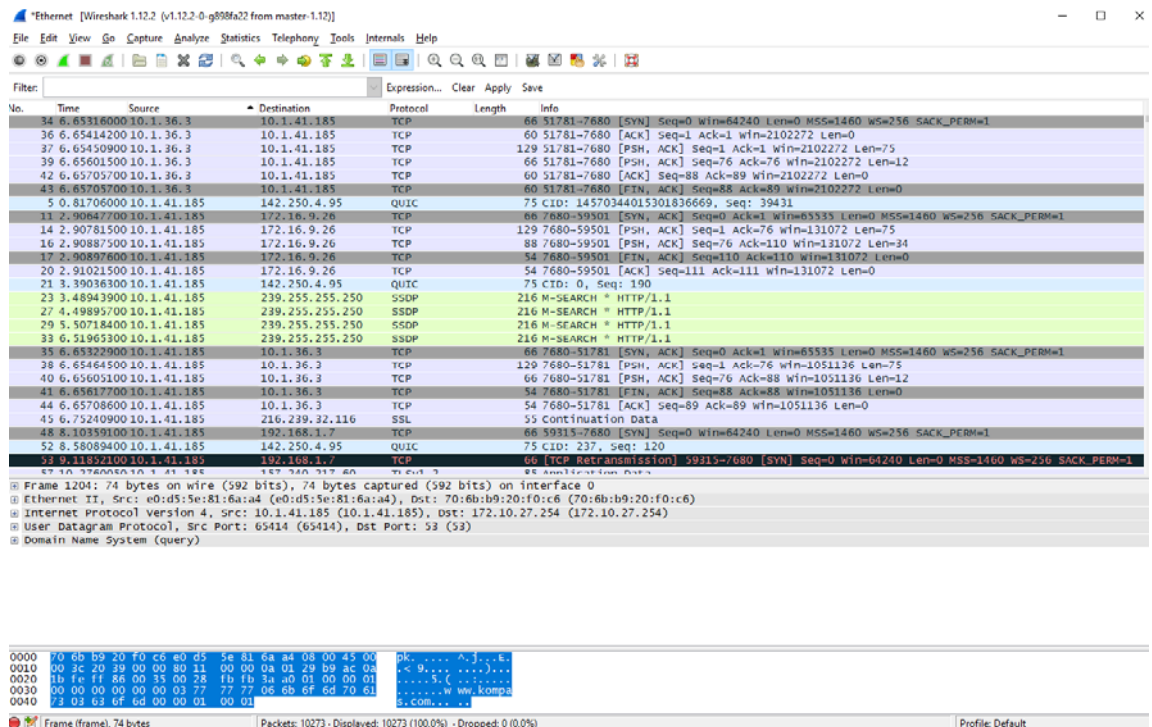
Gambar 11. 2 interface capture

Maka akan muncul tampilan untuk memilih interface yang akan kita Analisa

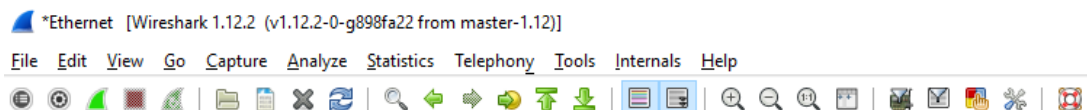


Gambar 11. 3 Pilihan yang akan ditangkap

- d. Pilih lokasi yang akan kita capture, misal kita pilih Ethernet, maka centang pada bagian yang kita pilih lalu klik Start untuk memulai pengcapturean data. Wireshark akan segera mengcapture paket-paket data yang melintas pada jaringan computer, berikut tampilan utama saat wireshark bekerja :



Gambar 11. 4 Halmaan utama saat capturing berlangsung



Gambar 11. 5 Menu dalam tampilan capturing



Gambar 11. 6 Display filter

Untuk memunculkan filter bisa juga menggunakan CTRL+F untuk memfilter

No.	Time	Source	Destination	Protocol	Length	Info
34	6.65316000	10.1.36.3	10.1.41.185	TCP	66	51781-7680 [SYN] Seq=0 win=64240 Len=0 MSS=1460 WS=256 SA
36	6.65414200	10.1.36.3	10.1.41.185	TCP	60	51781-7680 [ACK] Seq=1 Ack=1 win=2102272 Len=0
37	6.65450900	10.1.36.3	10.1.41.185	TCP	129	51781-7680 [PSH, ACK] Seq=1 Ack=1 win=2102272 Len=75
39	6.65601500	10.1.36.3	10.1.41.185	TCP	66	51781-7680 [PSH, ACK] Seq=76 Ack=76 win=2102272 Len=12
42	6.65705700	10.1.36.3	10.1.41.185	TCP	60	51781-7680 [ACK] Seq=88 Ack=89 win=2102272 Len=0
43	6.65705700	10.1.36.3	10.1.41.185	TCP	60	51781-7680 [FIN, ACK] Seq=88 Ack=89 win=2102272 Len=0
5	0.81706000	10.1.41.185	142.250.4.95	QUIC	75	CID: 14570344015301836669, Seq: 39431
11	2.90647700	10.1.41.185	172.16.9.26	TCP	66	7680-59501 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=146
14	2.90781500	10.1.41.185	172.16.9.26	TCP	129	7680-59501 [PSH, ACK] Seq=1 Ack=76 win=131072 Len=75
16	2.90887500	10.1.41.185	172.16.9.26	TCP	88	7680-59501 [PSH, ACK] Seq=76 Ack=110 win=131072 Len=34
17	2.90897600	10.1.41.185	172.16.9.26	TCP	54	7680-59501 [FIN, ACK] Seq=110 Ack=110 win=131072 Len=0
20	2.91021500	10.1.41.185	172.16.9.26	TCP	54	7680-59501 [ACK] Seq=111 Ack=111 win=131072 Len=0
21	3.39036300	10.1.41.185	142.250.4.95	QUIC	75	CID: 0, Seq: 190
23	3.48943900	10.1.41.185	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
27	4.49895700	10.1.41.185	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
29	5.50718400	10.1.41.185	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
33	6.51965300	10.1.41.185	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
35	6.65322900	10.1.41.185	10.1.36.3	TCP	66	7680-51781 [SYN, ACK] Seq=0 Ack=1 win=65535 Len=0 MSS=146
38	6.65464500	10.1.41.185	10.1.36.3	TCP	129	7680-51781 [PSH, ACK] Seq=1 Ack=76 win=1051136 Len=75
40	6.65605100	10.1.41.185	10.1.36.3	TCP	66	7680-51781 [PSH, ACK] Seq=76 Ack=88 win=1051136 Len=12
41	6.65617700	10.1.41.185	10.1.36.3	TCP	54	7680-51781 [FIN, ACK] Seq=88 Ack=88 win=1051136 Len=0
44	6.65708600	10.1.41.185	10.1.36.3	TCP	54	7680-51781 [ACK] Seq=89 Ack=89 win=1051136 Len=0
45	6.75240900	10.1.41.185	216.239.32.116	SSL	55	Continuation Data
48	8.10359100	10.1.41.185	192.168.1.7	TCP	66	59315-7680 [SYN] Seq=0 win=64240 Len=0 MSS=1460 WS=256 SA
52	8.58089400	10.1.41.185	142.250.4.95	QUIC	75	CID: 237, Seq: 120
53	9.11852100	10.1.41.185	192.168.1.7	TCP	66	[TCP Retransmission] 59315-7680 [SYN] Seq=0 win=64240 Len=0

Gambar 11. 7 Daftar paket yang berhasil ditangkap

```

# Frame 109: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
# Ethernet II, Src: e0:d5:5e:81:6a:a4 (e0:d5:5e:81:6a:a4), Dst: 70:6b:b9:20:f0:c6 (70:6b:b9:20:f0:c6)
# Internet Protocol Version 4, Src: 10.1.41.185 (10.1.41.185), Dst: 74.125.200.100 (74.125.200.100)
# User Datagram Protocol, Src Port: 49967 (49967), Dst Port: 443 (443)

```

Gambar 11. 8 detail dari paket yang terpilih

```

0000  70 6b b9 20 f0 c6 e0 d5 5e 81 6a a4 08 00 45 00  pk. .... ^.j...E.
0010  00 40 82 c9 40 00 80 11 00 00 0a 01 29 b9 4a 7d  .@..@... .....)J}
0020  c8 64 c3 2f 01 bb 00 2c 46 d9 47 f2 93 13 8a 19  .d./... F.G....}
0030  64 d2 26 42 08 bd 7f f2 2f eb 59 69 3a c6 3f 1f  d.&B.... /.yi:..?
0040  69 d9 5a 08 a0 2a 4f 3e bd 8a 3e 7d d6 65       i.Z...*O> ...}.e

```

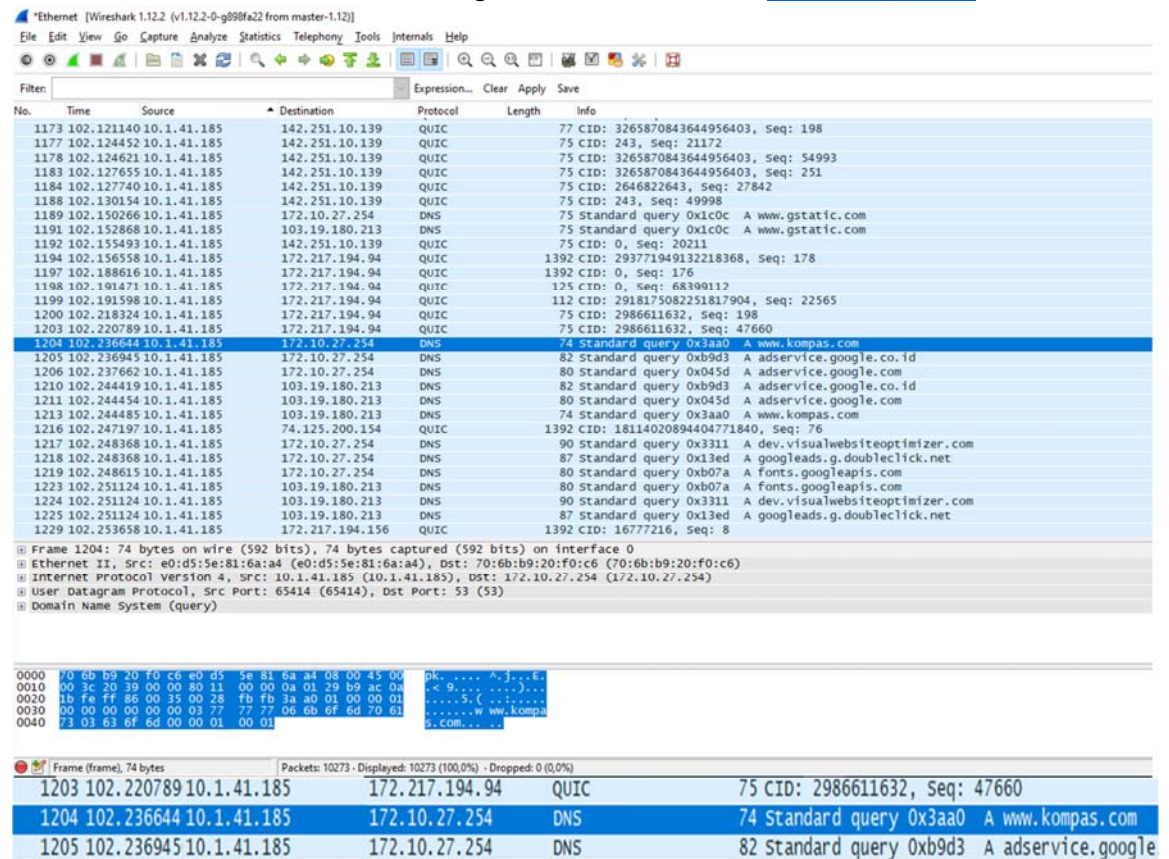
Gambar 11. 9 detail paket dalam format heksadesimal

Pada bagian gambar 11.7 daftar paket, terdapat kolom-kolom sebagai berikut:

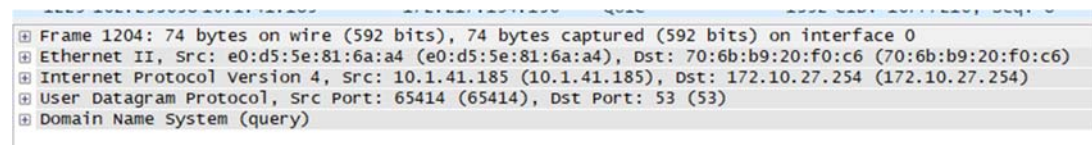
- Time : menampilkan waktu saat paket tersebut tertangkap
- Source : menampilkan IP sumber dari paket data
- Destination : menampilkan IP tujuan dari paket data
- Protocol : Menampilkan protocol yang dipakai oleh paket data
- Info : menampilkan informasi detail dari paket data



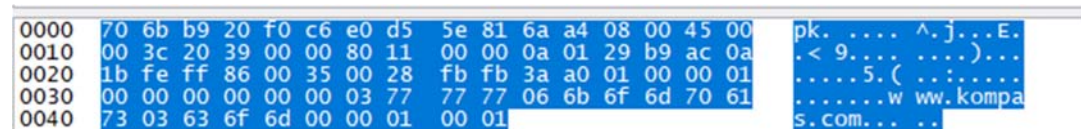
- e. Buka web browser dan bukalah sembarang website atau situs misal [www.kompas.com](http://www.kompas.com)



Gambar 11. 10 hasil tangkapan Ketika mengakses Kompas.com



Gambar 11. 11 Detail dari web Kompas.com



Gambar 11. 12 detail dari web Kompas dalam format heksadesimal

- Setelah masuk browser hentikan proses pada wireshark dengan klik **Stop** pada menu capture, dari gambar langkah e terlihat paket-paket data yang tertangkap termasuk [www.kompas.com](http://www.kompas.com)
- Analisis paket data [www.kompas.com](http://www.kompas.com) , sebagai berikut:
- Untuk memastikan IP kita dan IP URL yang kita analisis gunakan command prompt, akan muncul jendela console command prompt, ketik ipconfig, akan keluar hasil seperti dibawah ini
- Sedangkan untuk mengetahui IP URL dengan mengetikkan **ping URL**

Ketik → c:\> ping [www.kompas.com](http://www.kompas.com)

### 11.7. POST TEST

Jawablah pertanyaan berikut (**Total Skor: 100**):

No	CPL	CPMK	Pertanyaan	Skor
1.	CPL-07	CPMK-04	Silahkan gunakan Wireshark untuk menganalisis 2 situs lain.	100

### 11.8. HASIL CAPAIAN PRAKTIKUM

Diisi oleh asisten setelah semua assessment dinilai.

No	Bentuk Assessment	CPL	CPMK	Bobot	Skor (0-100)	Nilai Akhir (Bobot x Skor)
1.	Pre-Test	CPL-07	CPMK-04	20%	100	20
2.	Praktik	CPL-07	CPMK-04	30%	100	30
3.	Post-Test	CPL-07	CPMK-04	50%	100	50
<b>Total Nilai</b>						100

**LEMBAR JAWABAN PRE-TEST DAN POST-TEST PRAKTIKUM**

<b>Nama :</b> <b>NIM :</b>	<b>Asisten:</b> <b>Paraf Asisten:</b>	<b>Tanggal:</b> <b>Nilai:</b>
-------------------------------	--	----------------------------------

--



## DAFTAR PUSTAKA

<https://help.ubuntu.com/community/IptablesHowTo>  
<https://help.ubuntu.com/8.04/serverguide/C/firewall.html>



**LABORATORIUM  
S1 INFORMATIKA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS AHMAD DAHLAN**



**2023**