BAB 2. TCP/IP Model

2.1 Tujuan

- Mahasiswa mampu melakukan identifikasi transmisi data menggunakan model TCP/IP
- Mahasiswa mampu melakukan identifikasi layer dari model TCP/IP
- Mahasiswa mampu menggunakan aplikasi untuk mengidentifikasi data dari model TCP/IP

2.2 Dasar Teori

2.2.1 OSI Layer

OSI adalah referensi komunikasi dari Open System Interconnection. OSI model digunakan sebagai referensi untuk membahas spesifikasi protokol. OSI model terdiri dari 7 layer seperti pada tabel 1.

Layer #	Nama	Unit	Deskripsi/Fungsi
		Enkapsulasi	
7	Application	Data	Mendefinisikan pelayanan (services)
			komunikasi pada suatu aplikasi
6	Presentation	Data	Mendefinisikan format data
5	Session	Data	Mendefinisikan memulai,
			pengontrolan dan mengakhiri
			komunikasi
4	Transport	Segment	Mendefinisikan jenis pengiriman
3	Network	Paket	Mendefinisikan pengiriman dari titik
			ke titik.
2	Data Link	Frame	Mendefinisikan cara pengaturan
			pengiriman data
1	Physical	bit	Mendifinisikan bentuk interface dari
			sebuah media transmisi

Tabel 1. OSI Layer

Dimana setiap layer memiliki fungsi dan contoh masing-masing.

2.2.2 TCP/IP Model

TCP/IP (singkatan dari Transmission Control Protocol/Internet Protocol), adalah gabungan dari protokol TCP dan IP sebagai sekelompok protokol yang mengatur komunikasi data dalam proses tukar-menukar data dari satu komputer ke komputer lain di dalam jaringan Internet yang akan memastikan pengiriman data sampai ke alamat yang dituju. Protokol ini tidaklah dapat berdiri sendiri, karena memang protokol ini berupa kumpulan protokol (Protocol Suite).

Arsitektur TCP/IP tidaklah berbasis OSI Layer, tetapi menggunakan model referensi DARPA. Seperti pada gambar 11., TCP/IP mengimplementasikan arsitektur berlapis yang terdiri atas empat lapis. Empat lapis ini, dapat dipetakan terhadap model OSI layer. Empat lapis ini, disebut juga DARPA Model atau DOD Model.



Gambar 11. OSI Layer vs TCP/IP Protocol Suite.

2.3 Pengenalan Aplikasi

2.3.1 Wireshark

Wireshark adalah aplikasi penganalisa paket jaringan (Network Packet Analyzer). Sebuah software penganalisa paket jaringan yang bekerja dengan cara menangkap paket jaringan dan mencoba untuk menampilkan data paket yang tertangkap dengan detail.

Wireshark bersifat open source.

Contoh penggunaan wireshark:

- Administrator jaringan menggunakan untuk melakukan penangan masalah jaringan
- Network security engineer menggunakan untuk memeriksa keamanan jaringan
- Developer menggunakan untuk melakukan debug pada implementasi protokol
- Umum digunakan untuk mempelajari internal protokol jaringan

Wireshark memiliki fitur:

- Tersedia untuk UNIX dan Windows.
- Menangkap paket data langsung dari network interface.
- Tampilan paket dengan informasi protokol yang sangat rinci.
- Open dan Save data paket yang dicapture.
- Import dan Eksport paket data dari dank e banyak program capture lainnya.
- Menyaring paket data dengan berbagai macam kriteria.
- Warnai layar paket berdasarkan filter.

2.3.2 Cara penggunaan Wireshark

Langkah-langkah menggunakan wireshark

1. Klik ikon...



2. Kemudian akan tampil aplikasi wireshark dengan diawali spash screen.



3. Tampilan awal program Wireshark.

\varTheta 😑 🕤 📉 🕅 🕅 🕅 🕅 🕅 🕅	Network Analyzer [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-]	1.12)]
Eile Edit View Go Capture Analyze Statistics Telephony	Eools Internals <u>H</u> elp	
	👱 🔲 💽 🔍 🔍 🔍 🖾 🔛 🎆 🗶 🗮	ŝ
Express	ion Clear Apply save	
WIRESHARK Version 1.12.0 (v1.12.0-0-g4fab	Network Protocol Analyzer #1a from master-1.12)	
Capture	Files	Online
 Interface List Les bis of the capture instrates Loss one or insere interfaces to capture from, then Start Choose one or insere interfaces to capture from, then Start Choose one or insere interfaces to capture from, then Start Wei-Fic end Thunderbolt Bridge: bridge0 Thunderbolt Bridge: bridge0 Thunderbolt 2: en2 P 2020 Thunderbolt 1: en3 Capture Options Start a capture with detailed options Capture Help De bot to the narrested formes metric 	Open a previously cantured file Open R. Carter as File/Open menu or toolbar item Sample Captures Anch assortment of example capture files on the wiki	 Website Visit the project's website User's Cate (andie) The ther's (cate (andie version) Security Work with Wireshark as securely as possible
Network Medie		
Ready to load or capture No Packets		Profile: Default

4. Keterangan menu wireshark.



5. Melakukan CAPTURE data menggunakan wireshark. Pilih menu INTERFACE.



6. Pilih interface yang kita gunakan, kemudian klik start.

Device	Description	IP	Packets	Packets/s
🗹 🙊 en0 🔵		fe80::1610:9fff:fed6:df3f	489	10
🗆 📂 bridge0		none	0	0
🗆 🔊 en2		none	0	0
🗆 🔊 p2p0		none	0	0
🗆 🔊 en3		none	0	0
🗆 🖈 lo0		::1	4	0
Help	Star	t Stop	ions	₩ Close

7. Setelah mengaktifkan interfaces, Wireshark akan beraksi membaca semua data yang berada di jaringan.

00			X Capturing from Wi-Fi:	en0 [Wireshark	x 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]	
Eile Ed	it ⊻iew <u>G</u> o	Capture Analyze Statistics	Telephony Tools In	ternals <u>H</u> elp		
	🙇 💻 🔝		• 🛩 👐 🕆 👱 📭			
Filter:			▼ Expression ⊂	lear Apply	Save	
No	Time	Course	Destination	Brotocol	Langth Info	14
140.	P 4 005644000	10 252 37 30	202 0 05 23	FIOCOCOT	J Length mito	- C
4	9 4 895979888	202 9 85 33	10 252 37 38	TCP	66 443-5794 [FIN ACK] Seg-1 ACK=1 Win=277 [en=0 [SVal=2202679420 [Sec=22233]	7
5	0.4.096011000	10 252 37 38	202 9 85 33	TCP	66 ITCP 0ut-0f-0rder1 52794-443 IFTN ACK1 Sen=1 Ack=112 Win=8106 Jen=0 TSva1=8224	723
5	1 4 098572000	202 9 85 33	10 252 37 38	TCP	66.443-57794 [4(K] Senall2 4rk=2 Win=277 Jen=0 TSval=202679447 TSerr=822472353	
5	2 4,098636000	10.252.37.38	202.9.85.33	TCP	66 [TCP Dup ACK 50#1] 52794-443 [ACK] Seg=2 Ack=112 Win=8196 Len=0 TSval=822472356	TS
5	3 4.239929000	00:19:e7:a4:31:8d	Spanning-tree-(for-bri	dges)STP	60 Conf. Root = 32768/37/00:0d:bc:78:ea:80 Cost = 6027 Port = 0x800d	_
5	4 4.288419000	14:10:9f:d6:df:3f	58:6d:8f:cc:84:74	EAPOL	113 Key (Group Message 2 of 2)	- 1
5	5 4.288449000	58:6d:8f:cc:84:74	14:10:9f:d6:df:3f	EAPOL	145 Key (Group Message 1 of 2)	- 1
5	6 5.630600000	fe80::351e:7d1a:7288:2669	ff02::1:2	DHCPv6	151 Solicit XID: 0xf5176a CID: 000100011b5385d0446d57daa029	
5	8 6.824396000	10.252.37.38	202.9.85.49	TCP	78 52864-443 [SYN] Seg=0 Win=65535 Len=0 MSS=1460 WS=16 TSval=822475075 TSecr=0 SA	CK
5	9 6.829309000	202.9.85.49	10.252.37.38	TCP	74 443-52864 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK PERM=1 TSval=1338	782
6	0 6.829401000	10.252.37.38	202.9.85.49	TCP	66 52864-443 [ACK] Seq=1 Ack=1 Win=131760 Len=0 TSval=822475080 TSecr=1338782944	
6	1 6.829680000	10.252.37.38	202.9.85.49	TLSv1	583 Client Hello	
6	2 6.832374000	202.9.85.49	10.252.37.38	TCP	66 443-52864 [ACK] Seq=1 Ack=518 Win=6912 Len=0 TSval=1338782944 TSecr=822475080	
6	3 6.832887000	202.9.85.49	10.252.37.38	TLSv1	211 Server Hello, Change Cipher Spec, Encrypted Handshake Message	
6	4 6.832958000	10.252.37.38	202.9.85.49	TCP	66 52864-443 [ACK] Seq=518 Ack=146 Win=131616 Len=0 TSval=822475083 TSecr=13387829	45
6	5 6.833825000	10.252.37.38	202.9.85.49	TLSv1	125 Change Cipher Spec, Encrypted Handshake Message	
6	6 6.834075000	10.252.37.38	202.9.85.49	TLSv1	1500 Application Data, Application Data	
6	7 6.837956000	202.9.85.49	10.252.37.38	TCP	66 443-52864 [ACK] Seq=146 Ack=2011 Win=9792 Len=0 TSval=1338782946 TSecr=82247508	4
6	8 7.267773000	10.252.37.1	224.0.0.10	EIGRP	74 Hello	
6	9 8.087831000	fe80::cacb:b8ff:fe5e:2d3	ff02::1:2	DHCPv6	161 Solicit XID: 0xb75860 CID: 00030001c8cbb85e02d3 IAA: ::	
	0 8.189018000	00:19:e7:a4:31:8d	Spanning-tree-(for-bri	dges)STP	60 Conf. Root = 32768/37/00:0d:bc:78:ea:80 Cost = 6027 Port = 0x800d	-
7	1 9 407341666	24 · fd · 52 · 23 · 65 · 7d	Broadcast	ARP	47 Who has 10 252 37 12 Toll 10 252 37 225	
▷ Frame	1: 84 bytes or	n wire (672 bits), 84 bytes o	aptured (672 bits) on i	nterface 0		
Ethern	et II, Src: 44	1:6d:57:da:a0:29 (44:6d:57:da	:a0:29), Dst: IPv6mcast	_01:00:03 (33:	::33:00:01:00:03)	
Intern	et Protocol Ve	ersion 6, Src: fe80::351e:7d1	a:7288:2669 (fe80::351e	:7d1a:7288:266	69), Dst: ff02::1:3 (ff02::1:3)	
D User D	atagram Protoc	ol, Src Port: 50267 (50267),	Dst Port: 5355 (5355)			
▷ Link-l	ocal Multicas	t Name Resolution (query)				
0000 33	33 00 01 00 0	3 44 60 57 0a a0 29 86 00 6	0 00 33Dm W)			
0020 7d	1a 72 88 26 6	9 ff 02 00 00 00 00 00 00 0	0 00 }.r.&i			
0030 00	00 00 01 00 0	3 c4 5b 14 eb 00 1e cf f0 3	4 ed4			
0040 00	00 00 01 00 0	0 00 00 00 00 04 77 70 61 6	4 00 wpad			
0050 00	01 00 01					
😑 💅 W i -	Fi: en0: <live< td=""><td>capture in Packets: 126</td><td>· Displayed: 126 (100.0</td><td>%)</td><td>Profile: Default</td><td>1</td></live<>	capture in Packets: 126	· Displayed: 126 (100.0	%)	Profile: Default	1

Terlihat banyak data yang dapat dicapture. Keterangan:

-B	
Source	Alamat IP pengirim
Destination	Alamat IP tujuan
Protocol	Jenis protokol yang digunakan, seperti TCP, DHCP, dll
Length	Panjang data yang dikirimkan
Info	Informasi isi data yang dikirimkan

8. Ketikkan ICMP pada filter box untuk melakukan penyaringan data yang akan ditampilkan sehingga hanya data PING yang akan ditampilkan.

			S 🗧 🔶 🐳 🐴 🛓		R. 🔍 🖭 📓	i 🗹 🔁	36 🔀			
Filter:	icmp		▼ Expression	Clear Apply S	ave					
No.	Time	Source	Destination	Protocol	ength Info					
	2 0.094776000	10.252.37.38	10.252.1.1	I CMP	78 Echo (pin	g) request	id=0xf186,	seq=2177/33032,	ttl=2 (reply in 3)	_
	3 0.097593000	10.252.1.1	10.252.37.38	ICMP	78 Echo (pin	g) reply	id=0xf186,	seq=2177/33032,	ttl=254 (request in 2)	
	11 0.594944000	10.252.37.38	10.252.1.1	ICMP	78 Echo (pin	g) request	id=0xf186,	seq=2433/33033,	ttl=1 (no response found!)	
	12 0.598607000	10.252.37.1	10.252.37.38	ICMP	70 Time-to-l	ive exceed	ed (Time to	live exceeded in	transit)	
	13 1.096137000	10.252.37.38	10.252.1.1	ICMP	78 Echo (pin	g) request	id=0xf186,	seq=2689/33034,	ttl=2 (reply in 14)	
	14 1.100135000	10.252.1.1	10.252.37.38	ICMP	78 Echo (pin	g) reply	id=0xf186,	seq=2689/33034,	ttl=254 (request in 13)	
	16 1.596443000	10.252.37.38	10.252.1.1	ICMP	78 Echo (pin	g) request	id=0xf186,	seq=2945/33035,	ttl=1 (no response found!)	
	17 1.600182000	10.252.37.1	10.252.37.38	ICMP	70 Time-to-l	ive exceed	ed (Time to	live exceeded in	transit)	
	18 2.097619000	10.252.37.38	10.252.1.1	ICMP	78 Echo (pin	g) request	id=0xf186,	seq=3201/33036,	ttl=2 (reply in 19)	
	19 2.102048000	10.252.1.1	10.252.37.38	ICMP	78 Echo (pin	g) reply	1d=0x†186,	seq=3201/33036,	ttl=254 (request in 18)	
	21 2.598768000	10.252.37.38	10.252.1.1	1 CMP	78 Echo (pin	g) request	1d=0x†186,	seq=3457/33037,	ttl=1 (no response found!)	_
-	22 2.602505000	10.252.37.1	10.252.37.38	1 CMP	70 Time-to-U	ive exceed	ed (lime to	Live exceeded in	transit)	
	31 3.099945000	10.252.37.38	10.252.1.1	TCMP	78 Echo (pin	g) request	1d=0x1186,	seq=3/13/33038,	ttl=2 (reply in 32)	
	32 3.103804000	10.252.1.1	10.252.57.30	TCMP	70 Echo (pin	g) repty	id=0x1186,	seq=3/13/33038,	ttl=254 (request in 51)	
	35 3.600029000	10.252.37.30	10.252.1.1	TCMP	78 Echo (pin	iyo oxcood	10-0X1180,	live exceeded in	trancit)	
-	39 4 101946000	10.252.37.39	10.252.1.1	LCMP	78 Echo (pin	a) request	id-0xf186	seg=4225/33040	ttl-2 (reply in 40)	
	10 4 105862000	10.252.37.30	10.252.1.1	TCMP	78 Echo (pin	g) request	id=0xf186,	seq=4225/33040,	ttl=254 (request in 30)	
	44 4 602472000	10 252 37 39	10 252 1 1	TCMP	78 Echo (pin	 a) request 	id-0xf186	seq=4491/33041	ttl-1 (no response found))	
	45 4 605712000	10.252.37.1	10.252.37.38	TCMP	70 Time.to.1	ive exceed	d (Time to	live exceeded in	transit)	
	46 5.103260000	10.252.37.38	10.252.1.1	LCMP	78 Echo (pin	 a) request 	id=0xf186.	seg=4737/33042.	ttl=2 (reply in 47)	
	47 5.107920000	10.252.1.1	10.252.37.38	ICMP	78 Echo (pin	 g) reply 	id=0xf186.	seg=4737/33042.	ttl=254 (request in 46)	
	51 5.604415000	10.252.37.38	10.252.1.1	ICMP	78 Echo (pin	g) request	id=0xf186.	seg=4993/33043.	ttl=1 (no response found!)	
Frame Ether Inter Inter	2: 78 bytes on net II, Src: 14: net Protocol Ver net Control Mess	wire (624 bits), 78 10:9f:d6:df:3f (14:1 sion 4, Src: 10.252. age Protocol	bytes captured (624 bits) or 0:9f:d6:df:3f), Dst: 00:24:1 37.38 (10.252.37.38), Dst: 1	interface 0 7:ee:65:4b (00:24 0.252.1.1 (10.252	:f7:ee:65:4b) .1.1)					

Profile: Default

9. Penjelasan data

Filter: ic	mp		Expression Clea	ar Apply Sav	e		
No.	Time	Source	Destination	Protocol Le	ngth Info		
1	0.000000000	10.252.37.38	10.252.1.1	ICMP	78 Echo (ping)		
2	0.003783000	10.252.37.1	10.252.37.38	ICMP	70 Time-to-live		
5	0.500405000	10.252.37.38	10.252.1.1	ICMP	78 Echo (ping)		
6	0.505574000	10.252.1.1	10.252.37.38	ICMP	78 Echo (ping)		
9	1.000588000	10.252.37.38	10.252.1.1	ICMP	78 Echo (ping)		
	70 butos on 1	vice (624 bits) 70 butes a	antured (624 hits) on int		70 7' ' ' ' '		
✓ Frame 9 Inter	face id: 0 (en	(624 DILS), 78 Dytes C	aptured (624 bits) on inte	eriace v			
Encan	sulation type.	Ethernet (1)					
Arriv	al Time: Sen 1	6 2014 19:10:42 925807000	WTR				
[Time	shift for thi	s packet: 0 00000000 secon	dsl				
Enoch	Time: 1410869	442 925807000 seconds	a31				
[Time	delta from pr	evious captured frame: 0.19	9844000 seconds]				
[Time	delta	s displayed frame: 0.4	95014000 seconds]				
[Time	si		000 seconds]				
Frame	/ Netw	ork					
Frame	/ Interfa	ace ts)					
Captu		bits)					
[Fram		⁵¹ ,					
[Fram	e∖ Ethern	iet II					
[Prot	0/	ether Internet	work				
[Colo	ring Rule Name	ICMP]	Pv4				
[Coloring Rule String: icmp Layer, II V4							
Kethernet IIScr: 14:10:9f:d6:df:3f (14:10:9r:do:df:3f), Dst: 00:24:f7:ee:65:4b (00:24:f7:ee:65:4b)							
Internet Protocol Version 4, Src: 10.252.37.38 (10.252.37.38), Dst: 10.252.1.1 (10.252.1.1)							
Internet Control Message Protocol							
0000 00 0	4 67 00 65-46-				***		

2.4 Persiapan Praktikum

- 1. Modul praktikum
- 2. PC yang dilengkapi dengan aplikasi Wireshark
- 3. Jaringan aktif
- 4. Lembar Laporan Praktikum (Lampiran)
- 5. Koneksi LAN dan Internet

2.5 Langkah-langkah Praktikum

2.5.1 Menjalankan aplikasi wireshark

1. Mahasiswa melakukan pengecekan apakah pada PC yang dipakai sudah terinstall aplikasi wireshark ?!!

2. Apabila belum terinstall, mahasiswa harus melakukan installasi di PC yang digunakan !!!

Untuk OS Linux Debian/Ubuntu: dhoto@mypc \$ su root@mypc # apt-get install wireshark

Untuk OSX:

- Download wireshark dan XQuartz
- Lakukan konfigurasi XQuartz pada wireshark

Untuk Windows:

- Download wireshark

- Klik 2x pada installer wireshark
- 3. Klik ikon Wireshark !!!
- 4. Klik pada menu CAPTURE dan memilih INTERFACES.
- 5. Pilih interface yang akan digunakan untuk mengrekam data.
- 6. Klik Start.
- Pada OS linux, jalankan aplikasi TERMINAL dan ketik perintah PING yang digunakan untuk melakukan pengecekan jaringan (tanpa tanda \$):
 \$ ping 10.252.1.1
- 8. Kembali ke aplikasi wireshark, hentikan rekam data dengan cara klik tombol merah pada wireshark. Ambil data untuk jenis tipe: icmp dengan cara memfilter di aplikasi wireshark dan lakukan screen shot pada tampilan wireshark yang kalian gunakan.

2.5.2 Melakukan rekam data untuk jenis protokol tertentu

- 1. Lakukan praktikum seperti kegiatan 2.5.1 dari nomer 4 s/d 8.
- 2. Ganti kegiatan pada no 7, dengan kegiatan berikut:
 - a. Jalankan aplikasi terminal dan ketik perintah NSLOOKUP yang digunakan untuk mengetahui IP dari suatu tujuan (tanpa tanda \$):
 \$ nslookup www.pens.ac.id
 - Ambil data untuk jenis tipe: dns
 - b. Jalankan aplikasi web browser dan arahkan ke alamat: <u>ftp://newfs.pens.ac.id</u>

Download salah satu data yang ada di alamat tersebut !!! Ambil data untuk jenis tipe: ftp

c. Jalankan aplikasi web browser dan arahkan ke alamat: http://www.pens.ac.id

Ambil data untuk jenis tipe: http

3. Untuk masing-masing kegiatan diatas, laporkan data yang telah direkam sesuai dengan layer pada TCP/IP model. Gunakan lembar Laporan praktikum 2. TCP/IP Model. (Lampiran)

2.6 Lampiran

Laporan praktikum 2. TCP/IP Model

:

:

:

Kegiatan Nama NRP

Data layer

Application layer

Host-to-host layer

Internetwork layer

Network Interface layer

== <u>http://lecturer.pens.ac.id/~dhoto</u> ==