Modul 1 WIRESHARK

TUJUAN PEMBELAJARAN:

- 1. Mengenalkan pada mahasiswa tentang konsep wireshark
- 2. Mahasiswa memahami konsep pengiriman dengan traceroute
- 3. Mahasiswa memahami proses fragmentasi

DASAR TEORI

Wireshark merupakan software untuk melakukan analisa lalu-lintas jaringan komputer, yang memiliki fungsi-fungsi yang amat berguna bagi profesional jaringan, administrator jaringan, peneliti, hingga pengembang piranti lunak jaringan.

Wireshark dapat membaca data secara langsung dari Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN, dan koneksi ATM.

I¥¥¥¥¥ ⊨⊠x22≜ < + + + + 722 □□ < < < □ ¥ 8 * 5							
ilten	en 🔹 Expression Clear Apply						
lo. +	Time	Source	Destination	Protocol	Info		
	1 0.000000	IntelCon_bat57:6c	Broadcast	ARP	who has 167.205.67.17 Tell 167.205.67.124		
	2 0.898984	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.1? Tell 167.205.67.124		
	3 1.899045	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.1? Tell 167.205.67.124		
	4 2.970706	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.1? Tell 167.205.67.124		
	5 18.900010	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124? Tell 0.0.0.0		
	6 18.900294	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 239.255.250 for any source		
	7 18.912888	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x3b571104		
	8 19.400094	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 239.255.255.250 for any source		
	9 19.900093	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124? Tell 0.0.0.0		
	10 20.361292	167.205.67.124	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
	11 20.900138	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.124? Tell 0.0.0.0		
	12 21.136266	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.1? Tell 167.205.67.124		
	13 21.900198	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.1? Tell 167.205.67.124		
	14 21.931754	167.205.67.124	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
	15 21.946727	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources		
	16 21.980052	167.205.67.124	167,205.67,127	NBNS	Registration NB SYSADMIN-PC<00>		
	17 21.992460	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.1? Tell 167.205.67.124		
	18 22.027172	167.205.67.124	224.0.0.252	UDP	Source port: 61492 Destination port: 11mmr		
	19 22.127344	167.205.67.124	224.0.0.252	UDP	Source port: 61492 Destination port: 11mm		
	20 22.327957	167.205.67.124	224.0.0.252	UDP	Source port: 49914 Destination port: 11mmr		
	21 22,400255	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.252 for any sources		
	22 22.428390	167.205.67.124	224.0.0.252	UDP	Source port: 49914 Destination port: 11mm		
	23 22.729293	167.205.67.124	167.205.67.127	NBN5	Registration NB SYSADMIN-PC<00>		
	24 22.900256	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.1? Tell 167.205.67.124		
	25 23.395198	167.205.67.124	239.255.255.250	SSDP	M-SEARCH * HTTP/1.1		
	26 23.479327	167.205.67.124	167.205.67.127	NBNS	Registration NB SYSADMIN-PC<00>		
	27 23.480302	0.0.0.0	255.255.255.255	DHCP	DHCP Request - Transaction ID 0x3b571104		
	28 23.900303	IntelCor_ba:57:6c	Broadcast	ARP	who has 167.205.67.17 Tell 167.205.67.124		
	29 24.229377	167.205.67.124	167.205.67.127	NBNS	Registration NB SY5ADMIN-PC<00>		
	30 24.385057	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.251 for any sources		
	31 24.400362	167.205.67.124	224.0.0.22	IGMP	V3 Membership Report / Join group 224.0.0.251 for any sources		
	32 24,841474	167.205.67.124	224.0.0.251	MDNS	Standard query ANY sysadmin-PC, local, "Qu" question		
	33 24.932701	167.205.67.124	239, 255, 255, 250	SSNP	M-SEARCH * HTTP/1,1		

Gambar 1. Tampilan wireshark

Tools ini bisa menangkap paket-paket data/informasi yang berjalan dalam jaringan. Semua jenis paket informasi dalam berbagai format protokol pun akan dengan mudah ditangkap dan dianalisa. Karenanya tak jarang tool ini juga dapat dipakai untuk sniffing (memperoleh informasi penting seperti password email atau account lain) dengan menangkap paket-paket yang berjalan di dalam jaringan dan menganalisanya. Namun tools ini hanya bisa bekerja didalam dalam jaringan melalui LAN/Ethernet Card yang ada di PC

Untuk struktur dari packet sniffer terdiri dari 2 bagian yaitu packet analyzer pada layer application dan packet capture pada layer operating system (kernel).



Gambar 2. Struktur Packet Sniffer

Struktur dari wireshark graphical user interface adalah sebagai berikut :

- a. Command menu
- b. Display filter specification : untuk memfilter packet data
- c. Listing of captured packets : paket data yang tertangkap oleh wireshark
- d. Details of selected packet header : data lengkap tentang header dari suatu packet
- e. Packet contents : isi dari suatu packet data



Gambar 3. Struktur Wireshark



Untuk mengetahui jalur yang ditempuh untuk mencapai suatu node, traceroute mengirimkan 3 buah paket probe tipe UDP dari port sumber berbeda, dengan TTL bernilai 1. Saat paket tersebut mencapai router next-hop, TTL paket akan dikurangi satu sehingga menjadi 0, dan router next-hop akan menolak paket UDP tersebut sembari mengirimkan paket ICMP Time-to-Live Exceeded ke node asal traceroute tersebut. Dengan cara ini, pengirim traceroute tahu alamat IP pertama dari jalur yang ditempuh.

TUGAS PENDAHULUAN

1. Download paket wireshark dan pingplotter dari http://lecturer.eepisits.edu/~zenhadi/kuliah/NGN

PERCOBAAN

A. Pengenalan Wireshark

1. Bukalah wireshark. Dan mulai mengcapture paket data dengan memilih Capture | Options. Pilihlah interface card yang digunakan untuk menangkap paket data yang lewat seperti gambar berikut.

Wireshark: Capture Options			
Capture			
Interface: NETGEAR GA302T Gigabit Adapter (Microsoft's Packa	t Scheduler) : \Device\NPF_{1FC4 -		
IP address: 192.168.1.46			
Link-layer header type: Ethernet 💌 Buffer size: 1	megabyte(s) Wireless Settings		
Capture packets in promiscuous mode			
Limit each packet to 68			
Capture Filter:	•		
Capture Fie(s)	Display Options		
File: Browse	🔽 Update list of packets in real time		
Use multiple files	The subscription of the sector to the		
Thext file every 1 megabyte(s)	I Automatic scroling in live capture		
Next file every 1 minute(s)	🔲 Hide capture info dialog		
🗹 King buffer with 🛛 🔤 files	Name Blassà trian		
Stop capture after 1			
Stop Capture	I Enable MAC name resolution		
after 1 packet(s)	Enable network name resolution		
🗌 after 1 megabyte(s) 🗸 🔻			
I after I minute(s) V	Enable transport name resolution		
Help	<u>S</u> tart <u>C</u> ancel		

2. Mulai lakukan pengamatan data dengan menekan tombol start :

I	Wireshark: Capture from NETGEAR GA302 📃 🗆 🗙							
	Captured Pa	ickets						
	Total	12	% of total					
	SCTP	0		D.0%				
	тер	12		100.0%				
	LCP	0		0.0%				
	ICMP	0		D.0%				
	ARP	0		D.0%				
	OSPE	0		D.0%				
	GRE	0		0.0%				
	NetBIO5	0		D.0%				
	IPX	0		D.0%				
	VINES	0		D.0%				
	Other	0		0.0%				
I	Running 00:00:21							
<u>H</u> elp S <u>t</u> op								

3. Sementara wireshark jalan, lakukan koneksi ke : http://gaia.cs.umass.edu/wireshark-labs/INTRO-wireshark-file1.html

Setelah muncul tampilan pada browser kemudian stop wireshark, Capture | Stop. Perhatikan pada bagian Protocol, ada banyak protocol yang ditampilkan. Untuk memfilter hanya protocol http saja yang ditampilkan lakukan filtering seperti berikut :

	Realtek RTL8102E PC	I-E Fast Ethernet NIC	[Wireshark 1.6.5 (SVN Rev 4042	9 from /trunk-1.6]
Eil	le <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze	<u>Statistics</u> Telephony <u>T</u> ools	Internals <u>H</u> elp	
		🕒 🖬 🗶 🤔	占 🔍 🗢 🔿 春 .		⊖, Q, 00, 🖭 🔐 🗵 畅 % 💢
Fil	ter: http			▼ Expression	Clear Apply
No.	. Time	Source	Destination	Protocol L	ength Info
	68 1.094188	192.168.1.101	209.85.175.120	HTTP	507 GET /gb/images/b_8d5afc09.png HTTP/1.1
	79 1.189706	192.168.1.101	. 74.125.235.24	HTTP	795 GET /extern_js/f/CgJpZBICaWQrMFo4ACwrMA44ACwr
	81 1.200405	74.125.235.24	192.168.1.101	HTTP	864 HTTP/1.0 200 OK (PNG)
	94 1.281082	209.85.175.12	0 192.168.1.101	HTTP	1414 HTTP/1.0 200 OK (PNG)
	106 1.343261	74.125.235.24	192.168.1.101	HTTP	263 HTTP/1.0 200 OK (PNG)
	125 1.461065	74.125.235.24	192.168.1.101	HTTP	447 HTTP/1.0 200 OK (PNG)
	144 1.590928	74.125.235.24	192.168.1.101	HTTP	237 HTTP/1.0 200 OK (text/javascript)
	151 1.771018	192.168.1.101	209.85.175.94	HTTP	757 GET /generate_204 HTTP/1.1
	154 1 806144	200 85 175 0/	102 168 1 101	нттр	361 HTTP/1 0 204 No Content
	188 17.240931	192.168.1.101	128.119.245.12	НТТР	552 GET /wireshark-labs/INTRO-wireshark-file1.htm
	191 1/.000010	120.119.243.1	.2 192.108.1.101	HILP	155 HTTP/1.0 200 OK (LEXL/HLMT)
	193 20.908005	192.168.1.101	128.119.245.12	HTTP	436 GET /favicon.ico HTTP/1.1
	196 21.439286	128.119.245.1	.2 192.168.1.101	HTTP	348 HTTP/1.0 404 Not Found (text/html)
1					- F

Catat dan amati header paket dan content datanya.

- 4. Dari HTTP GET message diatas yang dikirim dari komputer anda ke gaia HTTP server. Amatilah data berikut pada informasi header packet dan juga content informasi yang dikandungnya :
 - a. Ethernet frame
 - b. IP datagram

- c. TCP segment
- d. HTTP message

B. Pengamatan Traceroute IP

- 1. Download program pingplotter, dan gunakan dengan MS. Windows.
- 2. Setting sebagai berikut :
 - Address to trace : gaia.cs.umass.edu

of time to trace : 3 (3 kali pengiriman paket)

Trace Interval : 1 second

Atur packet size (in bytes) : 56, dari Edit | Options | Packet

1	Options				? ×	
	- General - Display Packet - Internet - Auto-Save - Route Changes - Email Settings	Packet Settings Packet Settings Packet Type: Time to wait for p Packet Packet Type: Packet Pa	ttings (CMP Using Windows DLL (default) ping replies (in ms): 3000 send delay (in ms): 40 ket size (in bytes): 56 et fragmentation? CP header byte: 00000000 Base 2 trace all hops trace all hops currency Options dded Name Lookups current requests: 45 o* Options t #+Program Name/Version) Apply OK		Cancel	
9 gaia.cs.umass.edu - PingPlotte	r Standard					
File Edit View Help	_					
Address to Trace:	Targe	t Name: gaia.cs	s.umass.edu			0-200 ms
gaia.cs.umass.edu	Samo	IP: 128.11	19.245.12	M		201-500 ms
gaia.cs.umass.edu	Hop PL9	% IP	DNSName	Avg	Cur	Graph
www.google.com	1	192.168.1.1		0	0 >	0 356
www.download.com	2 6	57 10.252.204.1		19	ERR	69.67% packet loss
www.pingpiotter.com	3 3	33 192.168.179.9		13	9	33% packet loss
216.92.150.222 Nessoft Site by IP	4	192.168.179.2		12	10	*
	5	192.168.179.2		13	10	*
	6	202.9.85.1	core.eepis-its.edu	11	12	¥ 📕
	7	202.9.85.254	gtw-pens-telkom.eepis-its.edu	10	11	*
	8	118.97.6.37		14	12	×
	9	61.5.118.193		52	38	*
	10	180.252.1.206		52	38	×
	11	4.59.50.121	xe-10-3-0.edge6.LosAngeles1.Lev	249	251	→
	12	4.69.144.126	vlan70.csw2.LosAngeles1.Level3.r	222	219	× 1
	13 10	00 -				100.00% packet loss
Sampling	14 10	00 -				100.00% packet loss
# of times to trace: 3	15 10	00 -				100.00% packet Jóss
a of times to face.	16 10	- UU -				100.00% packet loss
Trace Interval: 1 second	1/ 10	4.69.137.37	ae-73-73.ebr3.losAngeles1.Level5	22	22	Introduce pactor loss
Statistics	19	4.69.132.9	ae-3-3.ebr1.SanJose1.Level3.net	27	27	k l
Samples to include: 11	20	4.69.135.186	ae-2-2.ebr2.NewYork1.Level3.net	94	94	×
samples to include:	21	128.119.240.253	nscs1bbs1.cs.umass.edu	155	356	\longrightarrow
Trace	22 10	00 -				100.00% gartaet loss
Trace	23	4.69.148.38	ae-72-72.csw2.NewYork1.Level3.r	17	22	× -
Trace Count: 3	Disp	played Samples: 1 to	3			11. 11.

- 3. Aktifkan wireshark untuk mulai mengcapture paket, dan tekan tombol Trace pada pingplotter.
- 4. Matikan wireshark jika sudah selesai, lakukan filter paket ICMP agar hanya paket ICMP yang ditampilkan.
- 5. Pilih ICMP Echo Request message yang pertama yang dikirim oleh komputer anda, dan expand bagian paket Internet Protocol.



- 6. Dari informasi diatas, jawablah pertanyaan berikut :
 - a. Berapa IP address komputer anda?
 - b. Di dalam IP packet header, berapa value pada upper layer protocol field ?
 - c. Berapa banyak byte dalam IP header dan payload dari IP datagram ?
 - d. Apakah IP datagram di fragmen ? jelaskan.
- 7. Lakukan pengamatan dari paket ICMP yang pertama dan berikutnya dengan melakukan sorting pada paket ICMP (klik pada bagian source di wireshark), dan amatilah pada bagian paket Internet Protocol. Jawablah pertanyaan berikut:

a. Field mana dari IP datagram yang selalu berubah dari paket yang dikirim dari komputer anda ?

b. Field mana yang selalu konstan? Field mana yang harus selalu konstan?

8. Carilah paket ICMP TTL-exceeded replies yang dikirim ke komputer anda oleh router yang pertama, dan jawab pertanyaan berikut :

a. Berapa nilai Identification field dan TTL field ?

b. Apakah nilai tersebut tetap tidak berubah untuk semua ICMP TTL-exceeded replies ? Mengapa ?

C. Pengamatan Fragmentation

1. Ulangi langkah B. 1 – 4, tetapi dengan merubah ukuran paket menjadi 2000.

(Deptions	? <mark>×</mark>
General — Display — Packet * — Internet — Auto-Save — Route Changes — Email Settings	Packet Settings Packet Settings Packet Type: ICMP Using Windows DLL (default) Time to wait for ping replies (in ms): 3000 Packet send delay (in ms): 40 Packet size (in bytes): 2000 Allow packet fragmentation? Image: Concurrency Options Threading / Concurrency Options Use non-threaded Name Lookups Maximum concurrent requests: 45 Advanced "Cargo" Options Image: String Value: File: Apply OK Cancel

- 2. Pada wireshark, amati pada bagian Internet Protocol dan jawab pertanyaan berikut:
 - a. Pilih paket pertama yang dikirim ke tujuan, apakah IP datagram mengalami fragmentation ?
 - b. Jika iya, informasi apa saja pada IP header yang mengindikasikan datagram telah diframentasi ? Berapa panjang IP datagram ini ?
 - c. Lakukan pengamatan pada fragmen kedua dari IP datagram yang terfragmentasi. Informasi apa dalam IP header yang mengindikasikan bahwa ini bukan fragmen datagram yang pertama ? Apakah ada fragmen lainnya ?
 - d. Informasi apa yang berubah dari IP header fragmen pertama dan kedua ?
- 3. Ulangi langkah C. 1 dengan merubah ukuran paket menjadi 3500, dan jawab pertanyaan berikut :
 - a. Berapa banyak fragmen yang dihasilkan ?
 - b. Field apa yang berubah dalam IP header diantara fragmen-fragmen di atas ?

LAPORAN RESMI

- 1. Berikan kesimpulan hasil praktikum yang anda lakukan.
- 2. Bandingkan hasilnya jika dilakukan proses traceroute dari linux dengan merubahrubah isi paket data.