

**KEAMANAN JARINGAN KOMPUTER**  
**“IDS SNORT”**



Nama: Saros Sakiyana

NIM: 09011181320038

**JURUSAN SISTEM KOMPUTER**  
**FAKULTAS ILMU KOMPUTER**  
**UNIVERSITAS SRIWIJAYA**

**2017**

## Hasil dari rekaman file menggunakan wireshark:

The screenshot shows a Wireshark capture of network traffic. The packet list pane displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
441	23.6498010	23.58.248.94	10.100.203.196	TCP	60	443-58455 [FIN, ACK] Seq=86 Ack=1 Win=1013 Len=0
442	23.7494460	10.102.226.187	255.255.255.255	DB-LSP-	367	Dropbox LAN sync Discovery Protocol
443	23.7612310	10.102.226.187	10.102.239.255	DB-LSP-	367	Dropbox LAN sync Discovery Protocol
444	23.7648270	10.102.226.187	255.255.255.255	DB-LSP-	367	Dropbox LAN sync Discovery Protocol
445	23.7911700	23.58.248.94	10.100.203.196	TCP	60	[TCP Retransmission] 443-58455 [FIN, ACK] Seq=86 Ack=1 Win=1013 Len=0
446	23.8629930	10.100.203.196	210.210.179.94	TCP	66	542-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
447	24.1756040	ubiquiti_e6:74:ab	Broadcast	ARP	60	who has 192.168.200.25? Tell 192.168.200.106
448	24.3330880	10.100.203.196	210.210.179.94	TCP	66	[TCP Retransmission] 58890-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
449	24.3333220	10.100.203.196	210.210.179.94	TCP	66	[TCP Retransmission] 58891-443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
450	24.3866570	10.100.203.196	210.210.179.94	TCP	66	[TCP Retransmission] 58893-443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
451	24.8960170	10.100.203.196	210.210.179.94	TCP	66	[TCP Retransmission] 58894-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
452	24.9163130	23.58.248.94	10.100.203.196	TLSv1.2	139	[TCP Retransmission] Encrypted Alert
453	24.9193120	192.168.200.105	255.255.255.255	UDP	201	Source port: 43342 Destination port: 10001
454	24.9207760	IntelCor_1f:c6:ba	Broadcast	ARP	60	who has 10.102.224.1? Tell 10.102.224.40
455	24.9230250	192.168.200.104	255.255.255.255	UDP	198	Source port: 45119 Destination port: 10001
456	26.1970340	23.58.248.94	10.100.203.196	TLSv1.2	139	[TCP Retransmission] Encrypted Alert
457	26.1988020	54:dc:1d:14:84:c8	Broadcast	ARP	60	who has 10.100.224.1? Tell 10.100.225.95
458	26.2010850	fe80::c829:3d02:d0ff02::c	Broadcast	SSDP	208	M-SEARCH * HTTP/1.1
459	26.3159360	192.168.200.123	255.255.255.255	UDP	197	Source port: 46922 Destination port: 10001
460	26.3185130	ubiquiti_e6:74:ab	Broadcast	ARP	60	who has 192.168.200.25? Tell 192.168.200.106
461	26.8671680	10.100.203.196	210.210.179.94	TCP	66	[TCP Retransmission] 542-80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
462	28.9303330	10.100.203.196	10.100.203.255	NBNS	92	Name query NB WPAD<00>
463	28.9314380	fe80::116e:aa43:1f2ff02::1:3	Broadcast	LLMNR	84	Standard query 0x2da6 A wpad
464	28.9317860	10.100.203.196	224.0.0.252	LLMNR	64	Standard query 0x2da6 A wpad

The packet details pane for packet 464 shows:

- Frame 464: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0
- Ethernet II, Src: Azurewav\_7a:3e:38 (dc:85:de:7a:3e:38), Dst: IPv4mcast\_fc (01:00:5e:00:00:fc)
- Internet Protocol Version 4, Src: 10.100.203.196 (10.100.203.196), Dst: 224.0.0.252 (224.0.0.252)
- User Datagram Protocol, Src Port: 63796 (63796), Dst Port: 5355 (5355)
- Link-Local Multicast Name Resolution (query)

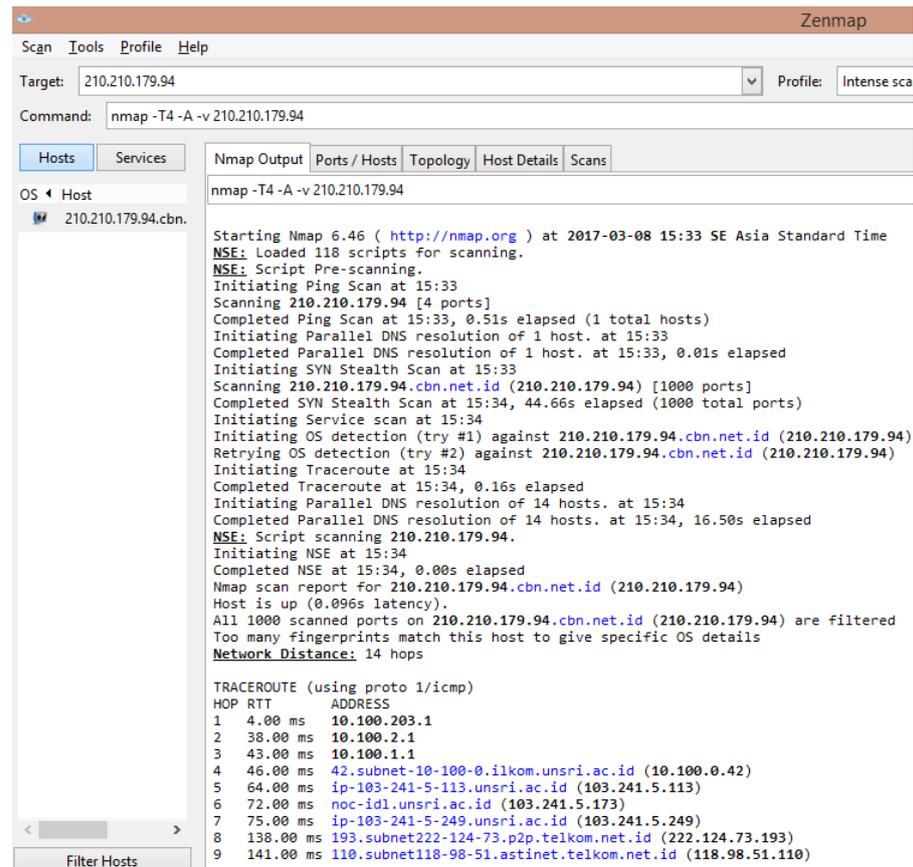
The packet bytes pane shows the raw data in hexadecimal and ASCII:

```

0000 01 00 5e 00 00 fc dc 85 de 7a 3e 38 08 00 45 00  ..^.....z>8..E.
0010 00 32 0e bf 00 00 01 11 f3 d7 0a 64 cb c4 e0 00  .2.....d....
0020 00 fc f9 34 14 eb 00 1e 33 eb 2d a6 00 00 00 01  ...4....3:.....
0030 00 00 00 00 00 00 04 77 70 61 64 00 00 01 00 01  .....w pad.....
    
```

Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp. Untuk domain yang ditujuh adalah olx.co.id dengan menggunakan ip 210.210.179.94, dan protokol menggunakan tcp yang berwarna merah

## Domain (Target) : olx.co.id dengan ip 210.210.179.94



The screenshot shows the Zenmap interface with the following details:

- Target:** 210.210.179.94
- Profile:** Intense sca
- Command:** nmap -T4 -A -v 210.210.179.94
- Hosts:** 210.210.179.94.cbn.

**Nmap Output:**

```
nmap -T4 -A -v 210.210.179.94

Starting Nmap 6.46 ( http://nmap.org ) at 2017-03-08 15:33 SE Asia Standard Time
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 15:33
Scanning 210.210.179.94 [4 ports]
Completed Ping Scan at 15:33, 0.51s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:33
Completed Parallel DNS resolution of 1 host. at 15:33, 0.01s elapsed
Initiating SYN Stealth Scan at 15:33
Scanning 210.210.179.94.cbn.net.id (210.210.179.94) [1000 ports]
Completed SYN Stealth Scan at 15:34, 44.66s elapsed (1000 total ports)
Initiating Service scan at 15:34
Initiating OS detection (try #1) against 210.210.179.94.cbn.net.id (210.210.179.94)
Retrying OS detection (try #2) against 210.210.179.94.cbn.net.id (210.210.179.94)
Initiating Traceroute at 15:34
Completed Traceroute at 15:34, 0.16s elapsed
Initiating Parallel DNS resolution of 14 hosts. at 15:34
Completed Parallel DNS resolution of 14 hosts. at 15:34, 16.50s elapsed
NSE: Script scanning 210.210.179.94.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Nmap scan report for 210.210.179.94.cbn.net.id (210.210.179.94)
Host is up (0.096s latency).
All 1000 scanned ports on 210.210.179.94.cbn.net.id (210.210.179.94) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 14 hops

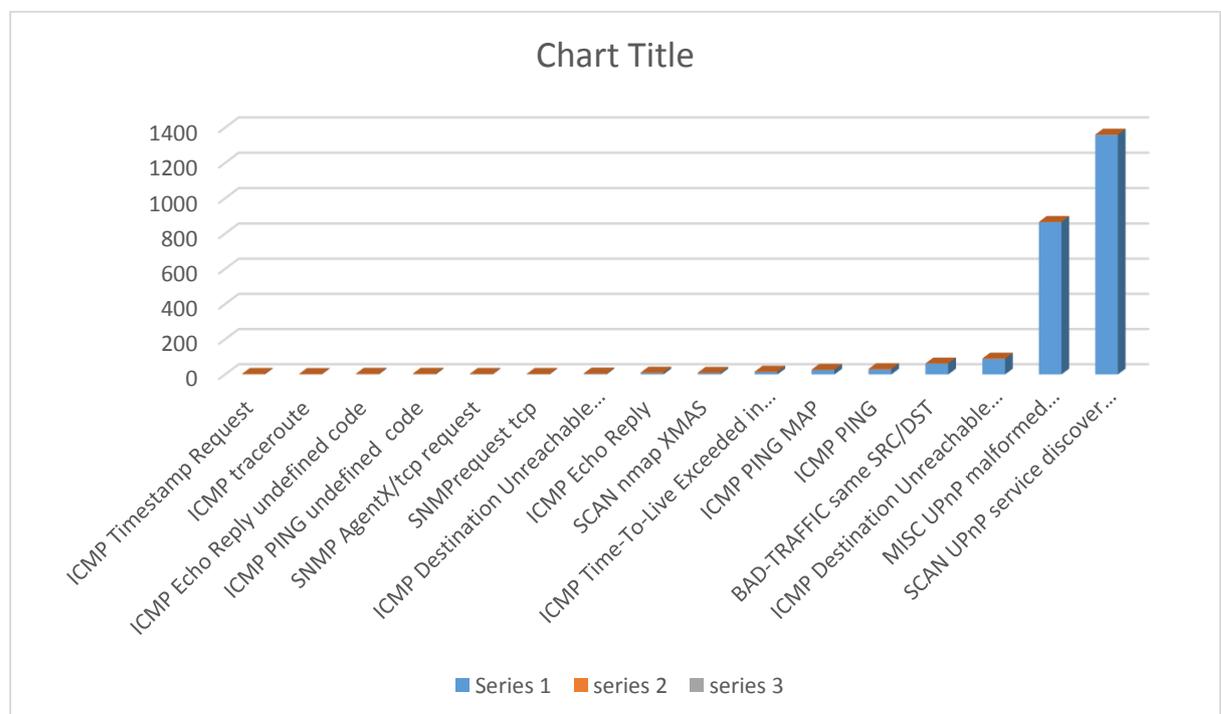
TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 4.00 ms 10.100.203.1
2 38.00 ms 10.100.2.1
3 43.00 ms 10.100.1.1
4 46.00 ms 42.subnet-10-100-0.ilkom.unsri.ac.id (10.100.0.42)
5 64.00 ms ip-103-241-5-113.unsri.ac.id (103.241.5.113)
6 72.00 ms noc-id1.unsri.ac.id (103.241.5.173)
7 75.00 ms ip-103-241-5-249.unsri.ac.id (103.241.5.249)
8 138.00 ms 193.subnet222-124-73.p2p.telkom.net.id (222.124.73.193)
9 141.00 ms 110.subnet118-98-51.astinet.telkom.net.id (118.98.51.110)
```

Pada domain yang kita tujuh misalnya **olx.co.id** mencetak xml ke co.id dan mengisi seluruh output standart dengan hasil interaktif yang sama yang akan ditampilkan pada nmap

## Hasil alert:

alert\_saros.csv.csv - Excel

	A	B	C	D	E	F	G	H	I	J	K
1	Total: 1	Priority: 3	alert	ICMP Timestamp Request							
2	Total: 1	Priority: 2	alert	ICMP traceroute							
3	Total: 2	Priority: 3	alert	ICMP Echo Reply	undefined code						
4	Total: 2	Priority: 3	alert	ICMP PING	undefined code						
5	Total: 2	Priority: 2	alert	SNMP AgentX/tcp request							
6	Total: 2	Priority: 2	alert	SNMP request tcp							
7	Total: 3	Priority: 3	alert	ICMP Destination Unreachable	Port Unreachable						
8	Total: 8	Priority: 3	alert	ICMP Echo Reply							
9	Total: 8	Priority: 2	alert	SCAN nmap XMAS							
10	Total: 13	Priority: 3	alert	ICMP Time-To-Live Exceeded in Transit							
11	Total: 25	Priority: 2	alert	ICMP PING NMAP							
12	Total: 28	Priority: 3	alert	ICMP PING							
13	Total: 61	Priority: 2	alert	BAD-TRAFFIC same SRC/DST							
14	Total: 88	Priority: 3	alert	ICMP Destination Unreachable	Network Unreachable						
15	Total: 865	Priority: 2	alert	MISC UPnP malformed advertisement							
16	Total: 1358	Priority: 3	alert	SCAN UPnP service discover attempt							



pada percobaan diatas hasil alertnya berjumlah 16 alert. Pada grafik diatas alert yang tertinggi adalah scan upnp service discover attempt 1358 dengan total : 1358. dan untuk alert yang terendah adalah icmp timestamp request adalah 1 dengan total: 1