KEAMANAN JARINGAN KOMPUTER

“IDS SNORT”

Nama: Saros Sakiyana

NIM: 09011181320038

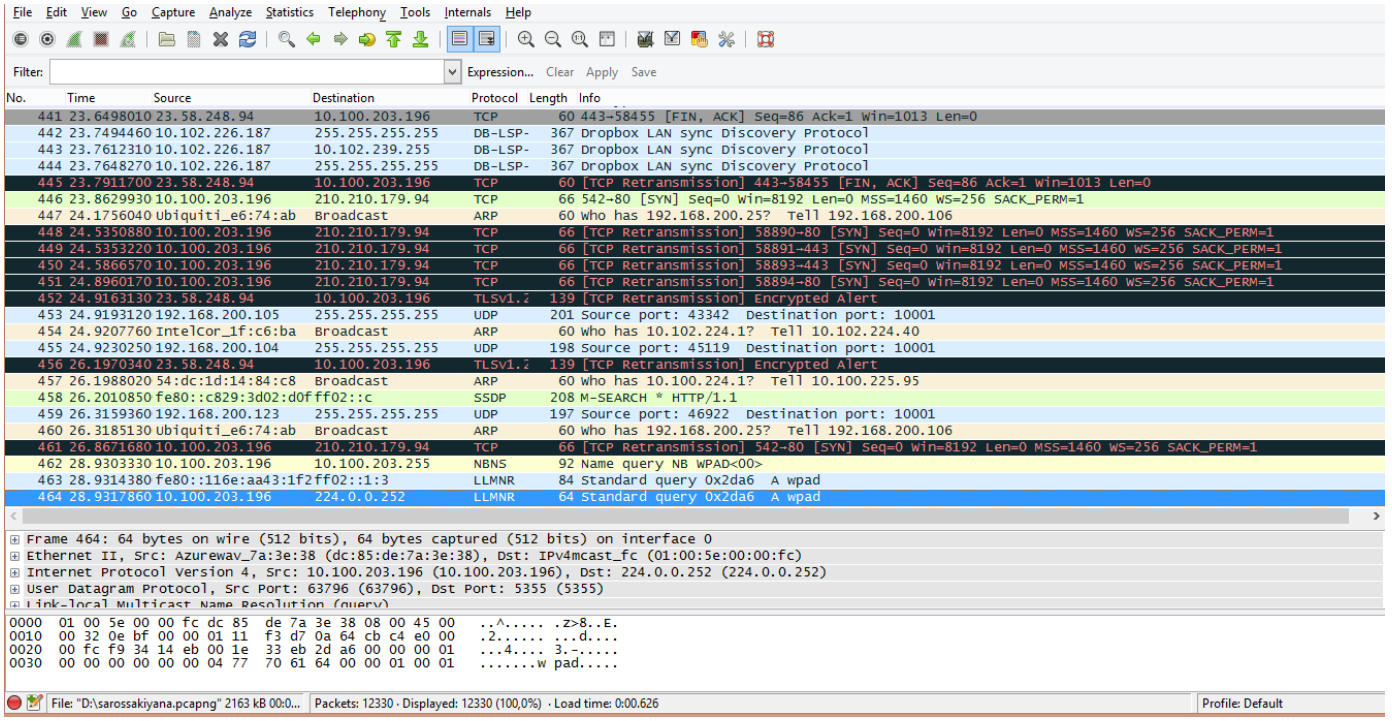
JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

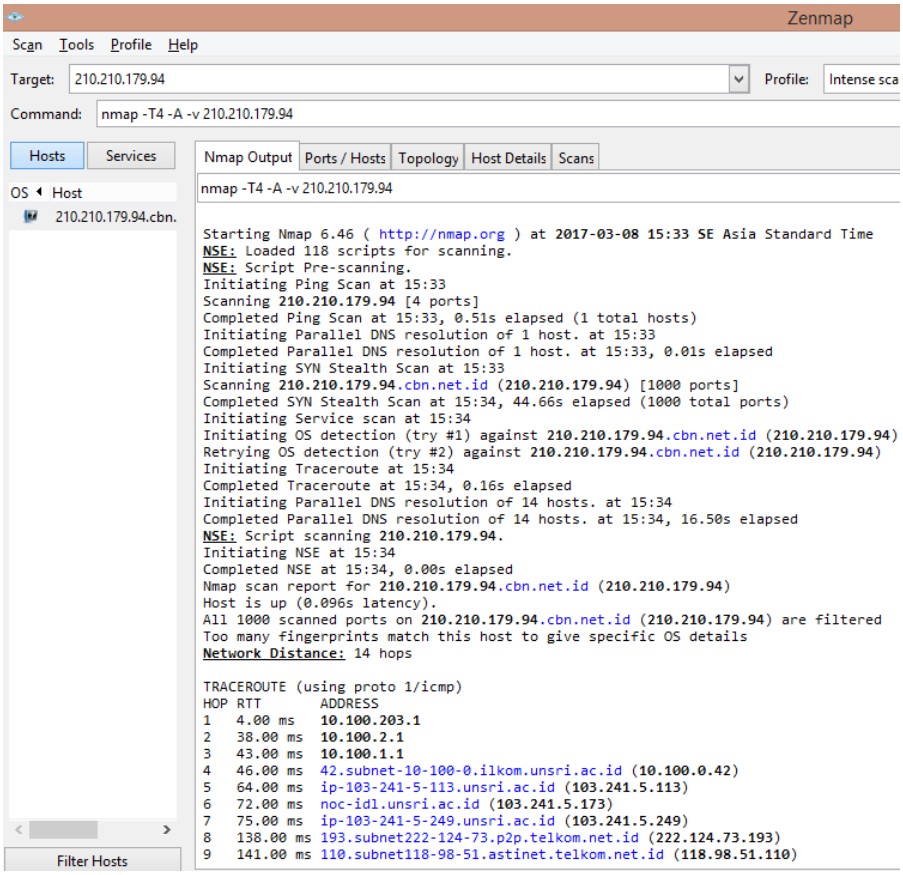
2017

Hasil dari rekaman file menggunakan wireshark:



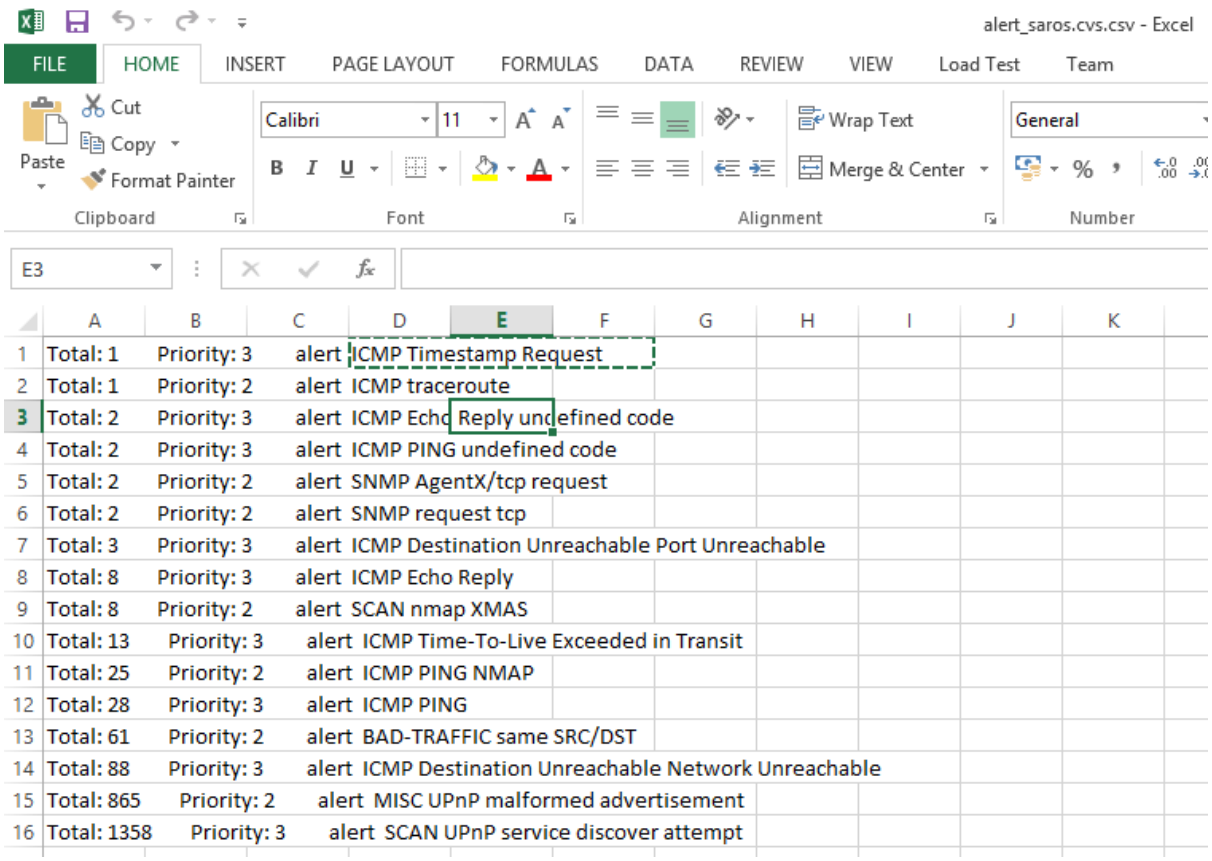
Gambar diatas menunjukkan paket-paket yang lewat pada jaringan kita, tiap warna mempunyai identitas untuk protokol yang lewat. Hijau untuk http, merah tcp, abu – abu arp. Untuk domain yang ditujuh adalah olx.co.id dengan menggunakan ip 210.210.179.94, dan protokol menggunakan tcp yang berwarna merah

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



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

Hasil alert:



alert_saros.cvs.csv - Excel

FILE HOME INSERT PAGE LAYOUT FORMULAS DATA REVIEW VIEW Load Test Team

Cut Copy Format Painter Paste — Clipboard

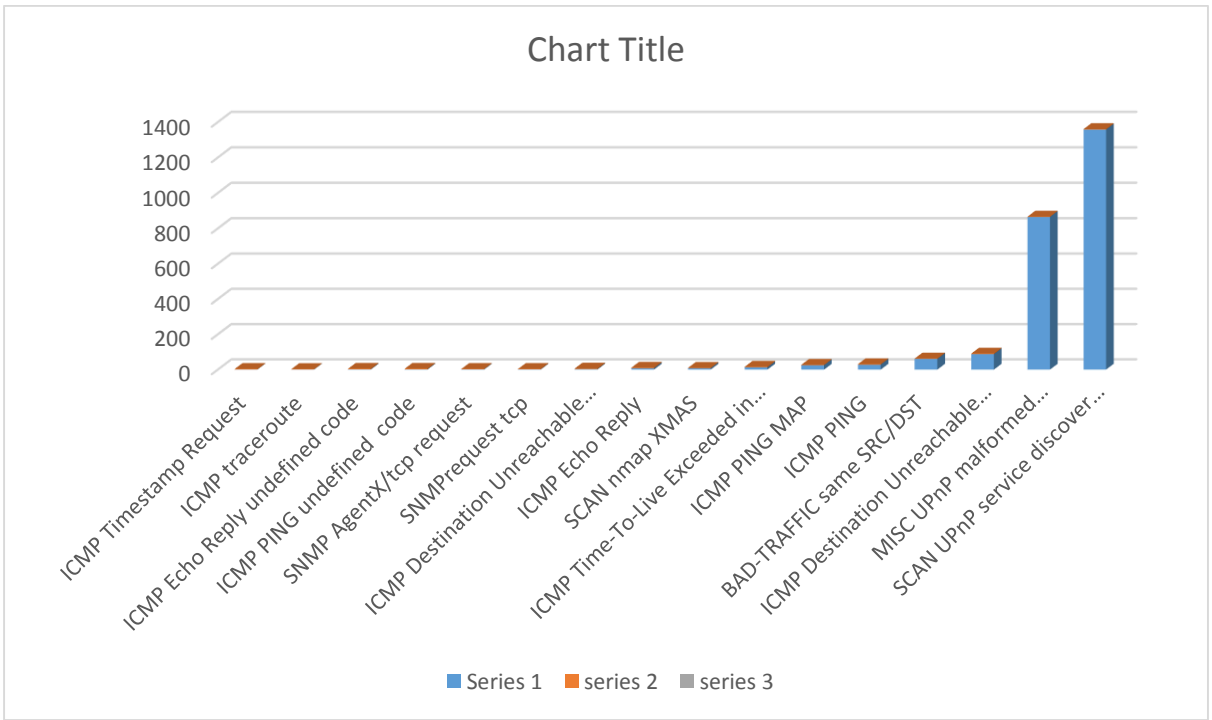
Calibri 11 — Font

Wrap Text Merge & Center — Alignment

General — Number

E3

	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 1300 dengan total : 1358.dan untuk alert yang terendah adalah icmp timestamp request adalah 0 dengan total: 1