Nama : Ratih Gustifa
NIM : 09011281320007
Mata Kuliah : Keamanan Jaringan Komputer

Analisa Snort Pada Website www.stationary.co.id

Snort adalah NIDS yang bekerja dengan menggunakan *signature detection*, berfungsi juga sebagai *sniffer* dan *packet logger*. Snort pertama kali di buat dan dikembangkan oleh Marti Roesh, lalu menjadi sebuah opensource project. Versi komersial dari snort dibuat oleh Sourcefire (www.sourcefire.com).Snort memiliki karakteristik, sebagai berikut:

1. Berukuran kecil – *Source code* dan *rules* untuk rilis 2.1.1 hanya 2256k.
2. *Portable* untuk banyak OS – Telah diporting ke Linux, Windows, OSX, Solaris, BSD,dll.
3. Cepat – Snort mampu mendeteksi serangan pada network 100Mbps.
4. Mudah dikonfigurasi – Snort sangat mudah dikonfigurasi sesuai dengan kebutuhan network kita. Bahkan kita juga dapat membuat *rule* sendiri untuk mendeteksi adanya serangan baru.
5. Free – Kita tidak perlu membayar sepeser pun untuk menggunakan snort. Snort bersifat open source dan menggunakan lisensi GPL.

Pada Tugas kali ini akan dianalisa hasil Snort pada Proses Scanning di website www.stationary.co.id, yang pertama di lakukan adalah :

1. Membuka wireshark , wireshark ini di install dengan menggunakan perintah

 # sudo apt-get install wireshark

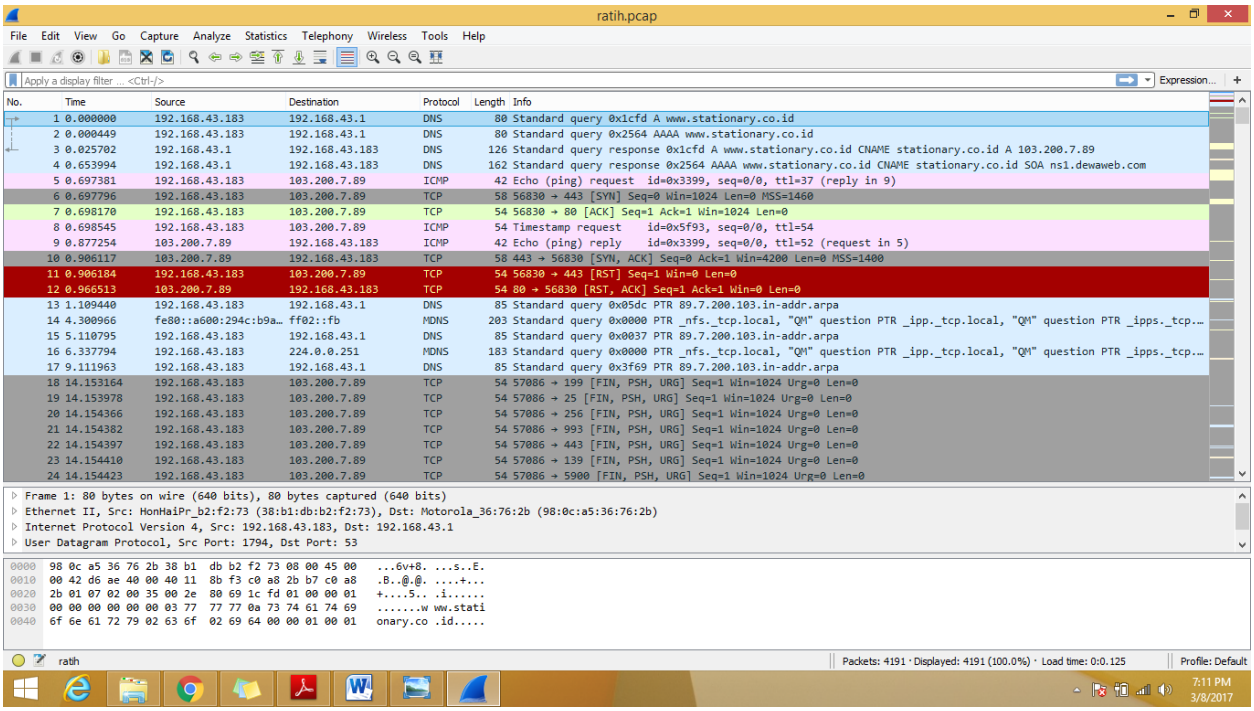
Selanjutnya klik start pada wireshark

2. lakukan scanning pada website www.stationary.co.id dengan menggunakan perintah

 # nmap –sF www.stationary.co.id

Proses scanning kali ini akan dilakukan sebanyak 3 kali, selama proses scanning wireshark akan mengcapture nya

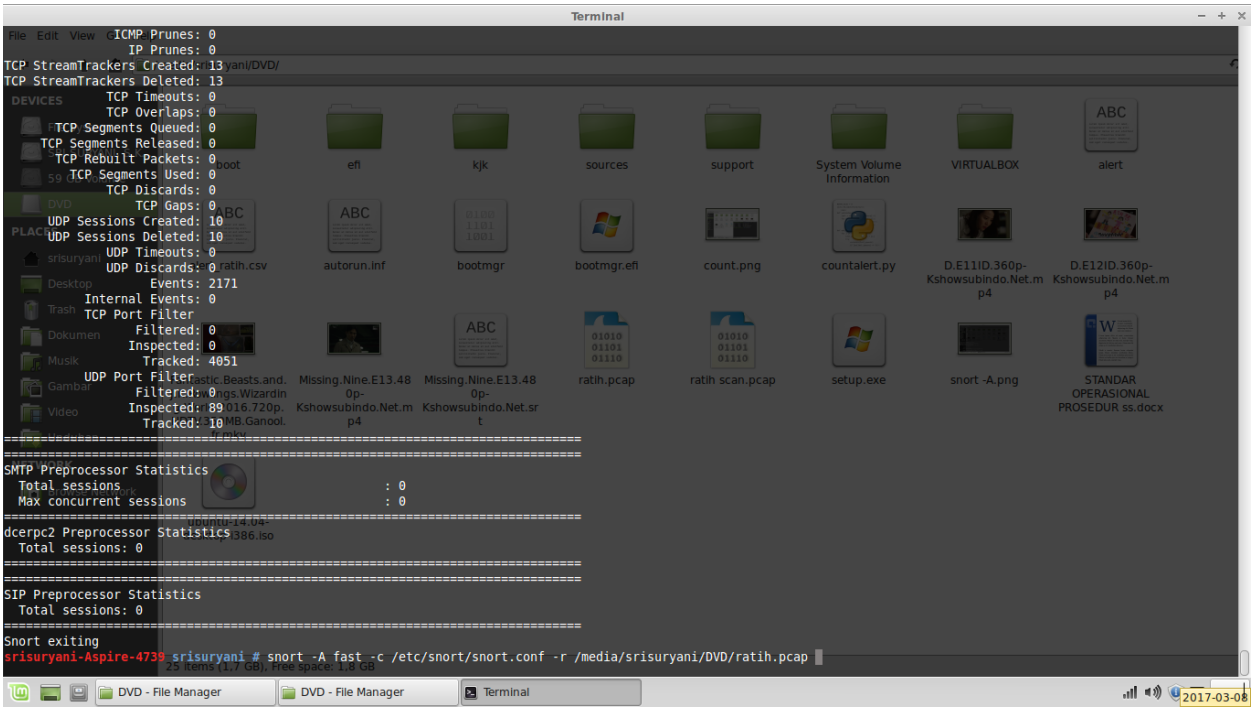
Nama : Ratih Gustifa
NIM : 09011281320007
Mata Kuliah : Keamanan Jaringan Komputer



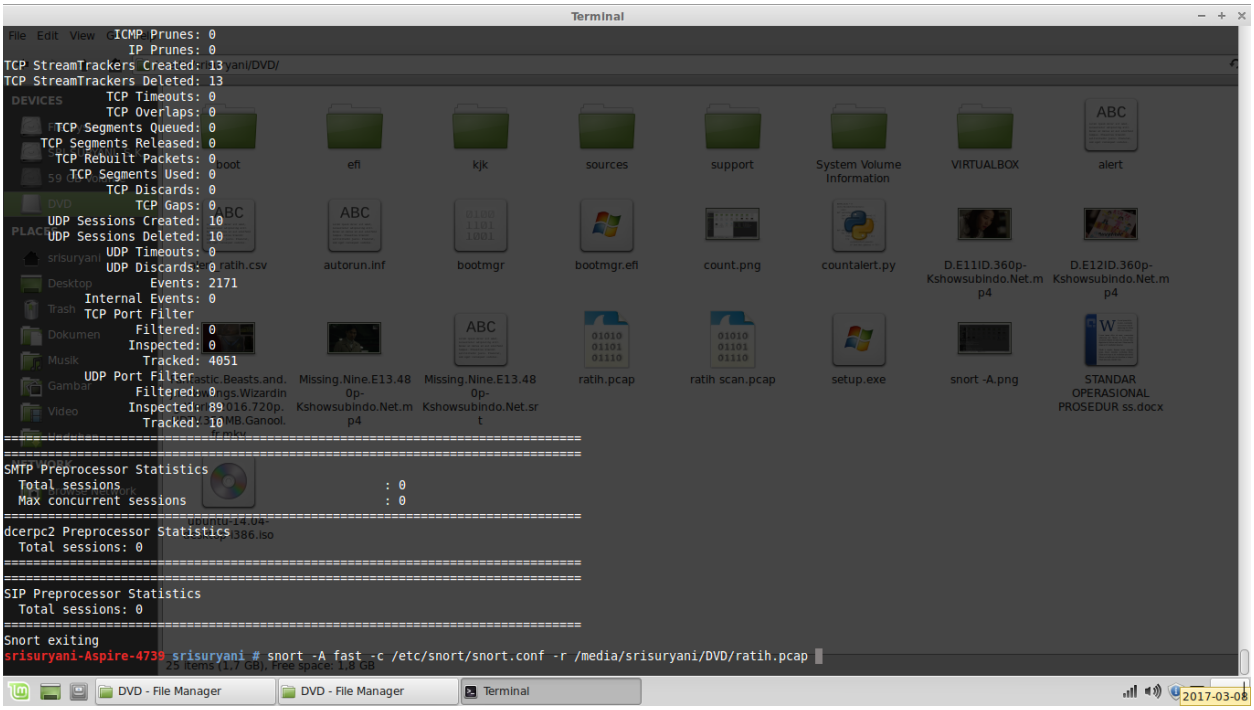
3. selanjutnya simpan hasil capture di wireshark dengan format .pcap

4. lalu compile hasil .pcap dengan menggunakan snort . perintah yang digunakan yaitu

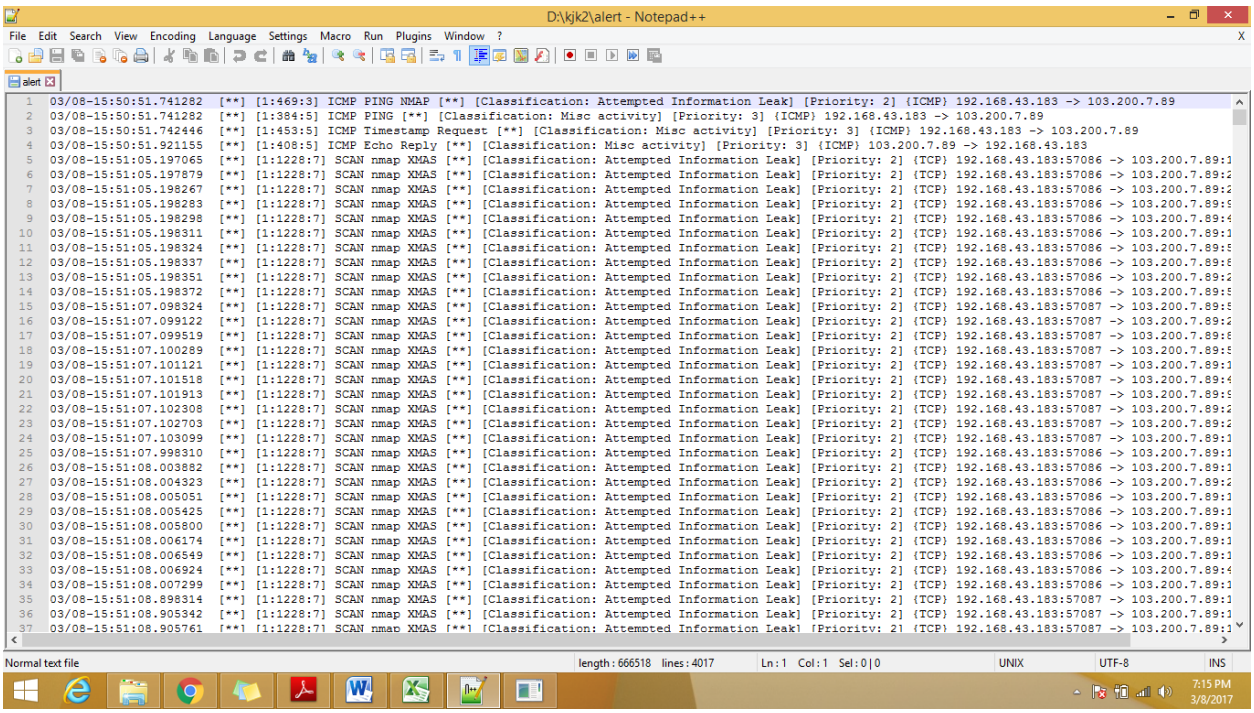
 # snort –A fast –c /etc/snort/snort.conf –r [letak tempat dimana file pcap disimpan]



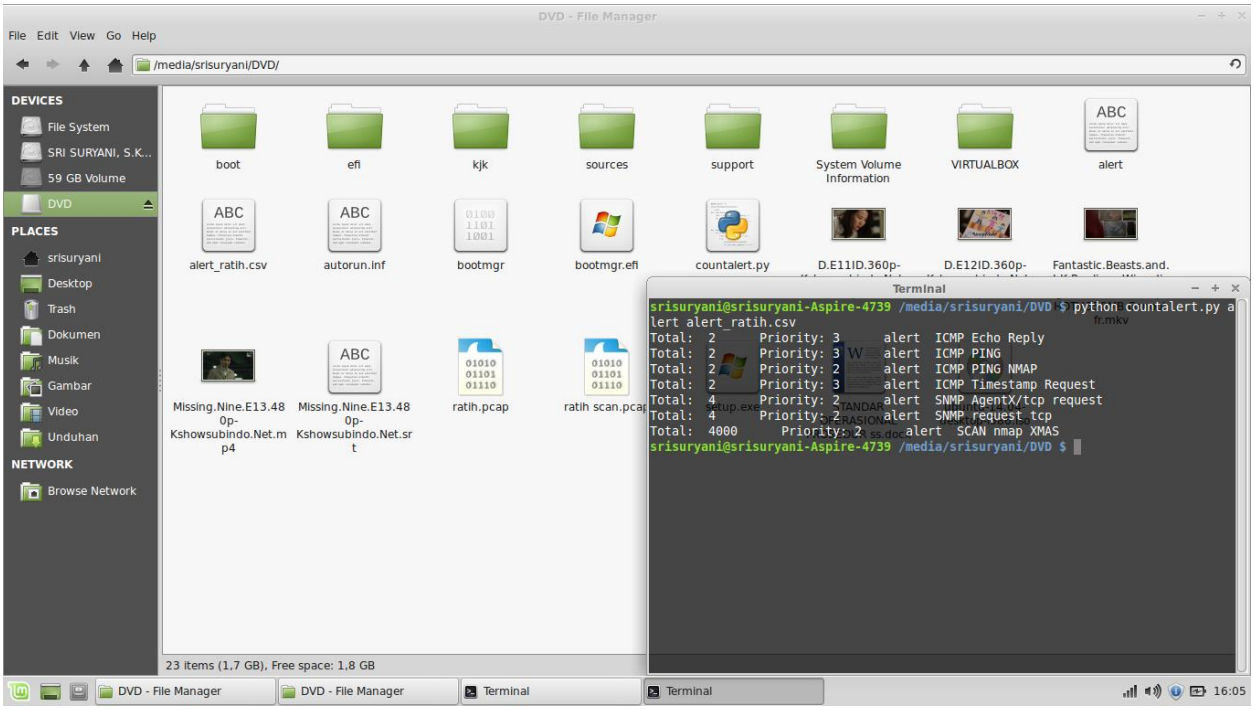
Nama : Ratih Gustifa
NIM : 09011281320007
Mata Kuliah : Keamanan Jaringan Komputer



5. lalu akan di dapat sejumlah alert yang selanjutnya di kelompokkan sesuai dengan type nya



Nama : Ratih Gustifa
NIM : 09011281320007
Mata Kuliah : Keamanan Jaringan Komputer



Pada Hasil Snort Tersebut di tampilkan dalam bentuk tabel sebagai berikut :

No	Alert	Jumlah	Priority
1	ICMP Echo Reply	2	3
2	ICMP PING	2	3
3	ICMP PING NMAP	2	2
4	ICMP Timestamp Request	2	3
5	SNMP AgentX/tcp request	4	2
6	SNMP request tcp	4	2
7	SCAN nmap XMAS	4000	2

Grafik yang nya :