LAPORAN PRAKTIKUM

KEAMANAN INFORMASI 1

PERTEMUAN 5

DISUSUN OLEH

Nama : Riva Mahyuli

NIM : (21/478139/SV/19241)

Kelas : R1AA

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

2023

Ekstrak Executable dari PCAP dan Menafsirkan Data HTTP dan

DNS untuk Mengisolasi Pelaku Ancaman

I. Alat dan Bahan :

- Mesin virtual CyberOps Workstation

II. Langkah Kerja

1). Menganalisis Log yang Ditangkap sebelumnya dan Pengambilan Lalu Lintas

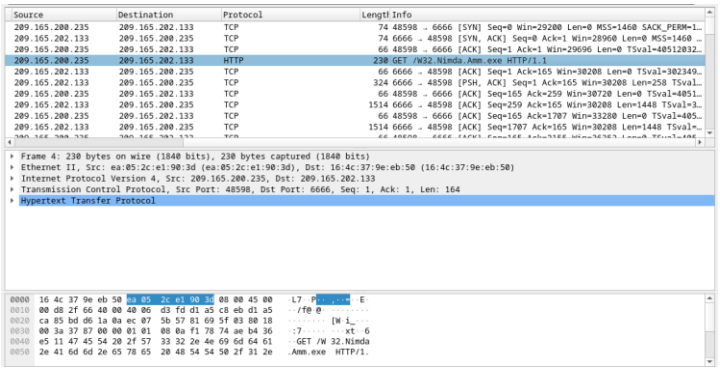
Mengubah direktori ke folder lab.support.files/pcaps, dan dapatkan daftar file menggunakan perintah ls –l.

```
[analyst@secOps ~]$ /home/analyst/lab.support.files/pcaps
bash: /home/analyst/lab.support.files/pcaps: Is a directory
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -1
nimda.download.pcap
wannacry_download_pcap.pcap
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst  371462 Mar 21  2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21  2018 wannacry_download_pcap.pcap
[analyst@secOps pcaps]$
```

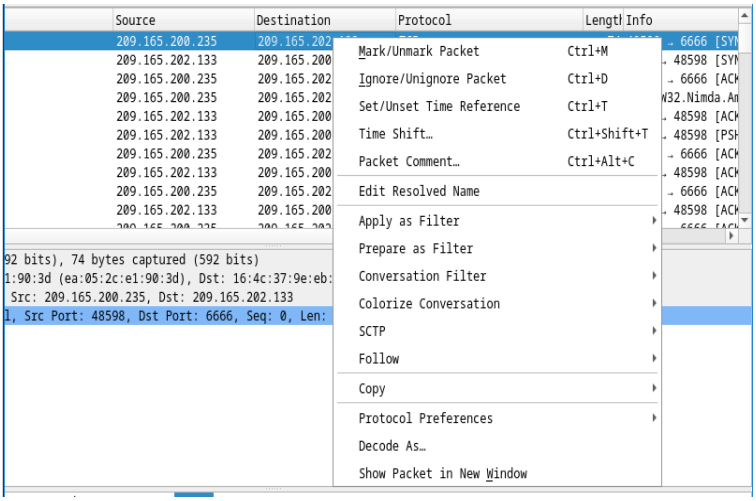
Perintah untuk membuka file nimda.download.pcap di Wireshark

```
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
[2] 632
```

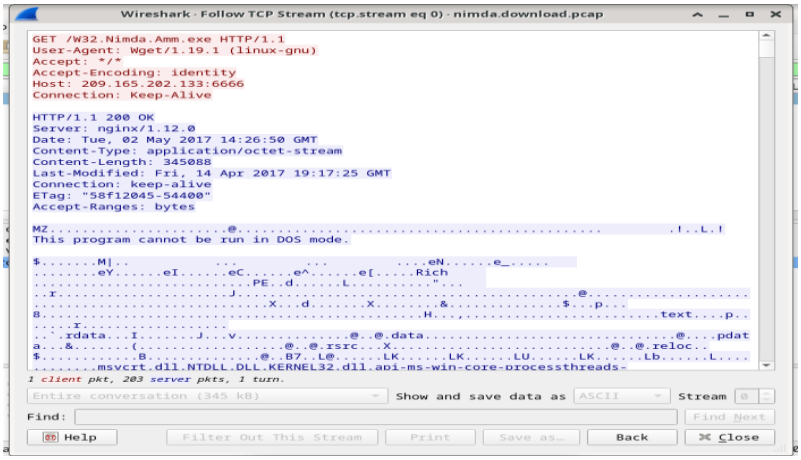
Pcap berisi semua paket yang dikirim dan diterima saat tcpdump sedang berjalan. Paket satu sampai tiga adalah jabat tangan TCP. Paket keempat menunjukkan permintaan file malware. Mengonfirmasi apa yang sudah diketahui, permintaan dilakukan melalui HTTP, dikirim sebagai permintaan GET.



Selanjutnya pilih paket TCP yang berada di baris pertama. Klik kanan > follow > TCP Stream.

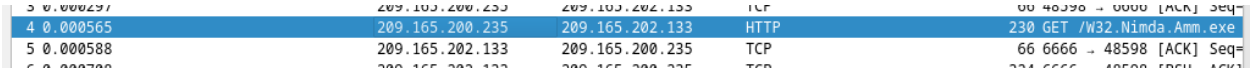


Wireshark akan menampilkan detail untuk seluruh aliran TCP yang dipilih.

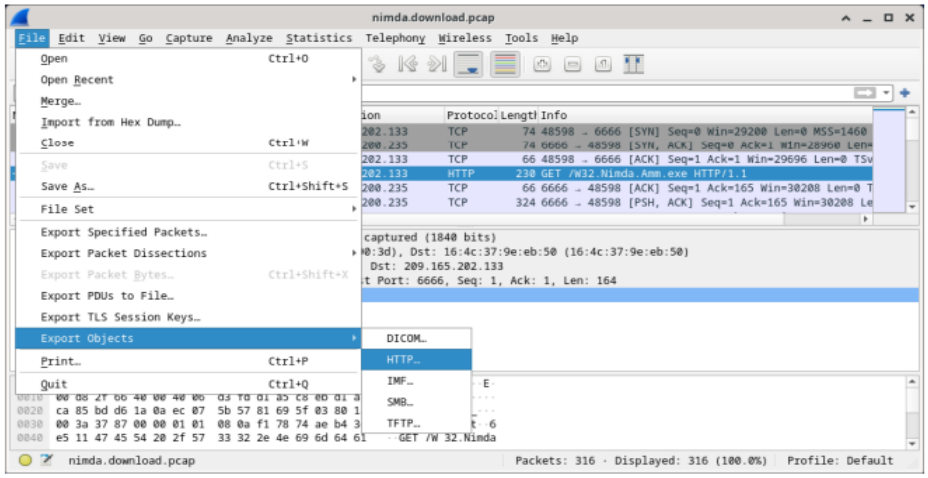


2). Extract Files yang di unduh dari PCAP

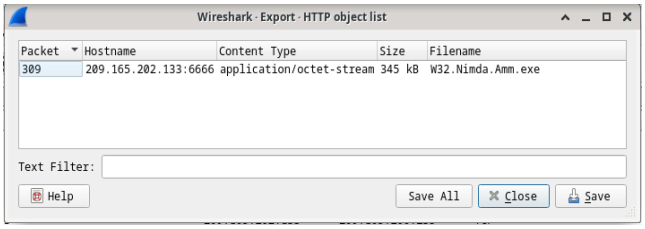
Pada paket keempat dalam file nimda.download.pcap, perhatikan bahwa permintaan HTTP GET dihasilkan dari 209.165.200.235 menjadi 209.165.202.133. Kolom Info juga menunjukkan bahwa ini sebenarnya adalah permintaan GET untuk file tersebut.



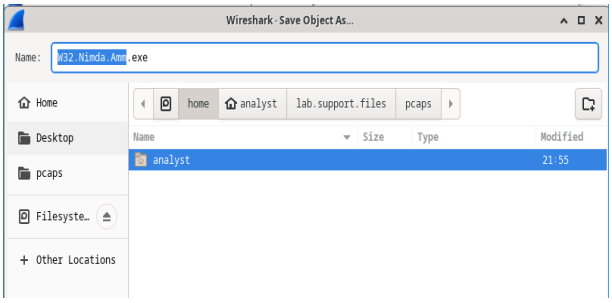
Dengan paket permintaan GET yang dipilih, navigasikan ke File > Export Objects > HTTP, dari menu Wireshark.



Wireshark akan menampilkan semua objek HTTP yang ada dalam aliran TCP yang berisi permintaan GET.



Lalu simpan file yang telah ditampilkan wireshark



Di terminal pastikan file telah disimpan ubah direktori ke folder /home/analyst dan daftarkan file di folder tersebut menggunakan perintah ls -l.

```
[analyst@secOps pcaps]$ cd  /home/analyst
[analyst@secOps ~]$ ls -l
total 3268
drwxr-xr-x 2 analyst analyst    4096 Mar 13 21:54 analyst
drwxr-xr-x 2 analyst analyst    4096 May 20  2020 Desktop
drwxr-xr-x 3 analyst analyst    4096 Apr  2  2020 Downloads
-rw-r--r-- 1 root    root       9238 Feb 20 20:41 httpdump.pcap
-rw-r--r-- 1 root    root    2965504 Feb 20 21:48 httpsdump.pcap
drwxr-xr-x 9 analyst analyst    4096 Jul 15  2020 lab.support.files
drwxr-xr-x 2 analyst analyst    4096 Mar 21  2018 second_drive
-rw-r--r-- 1 analyst analyst  345088 Mar 13 21:55 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

Perintah untuk memberikan informasi tentang jenis file.

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

Persiapan Log File pada Security Onion Virtual Machine

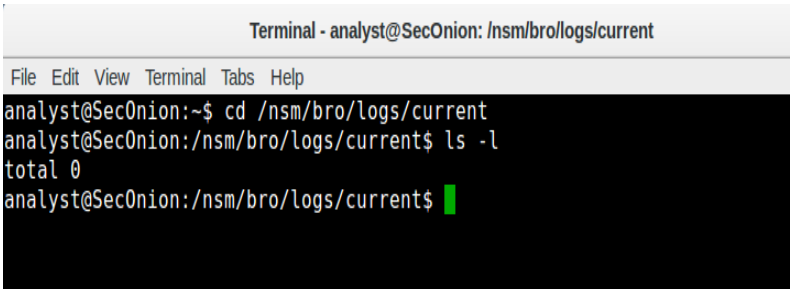
Alat dan Bahan

- Security Onion Virtual Machine

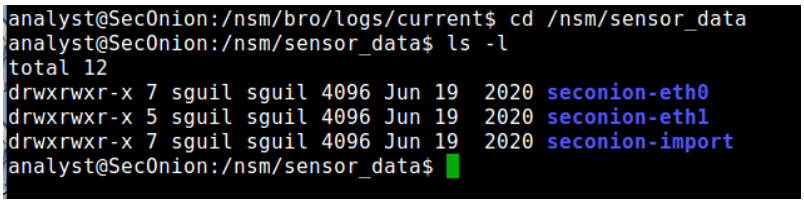
Langkah Kerja

1) Jalankan Security Onion VM dari Dasbor VirtualBox

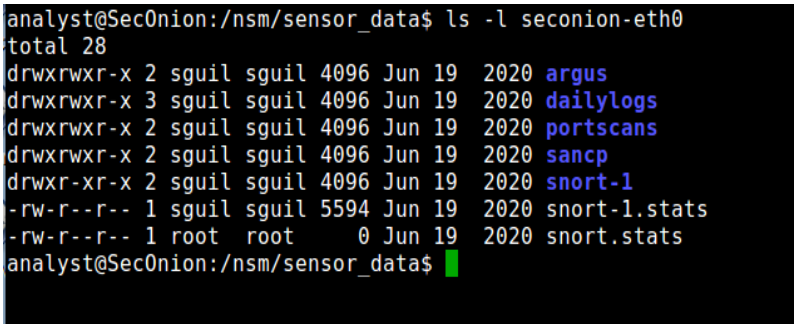
2) Zeek Logs pada Security Onion, ubah direktori menggunakan perintah berikut.Gunakan perintah ls -l untuk melihat file log yang dihasilkan oleh Zeek:



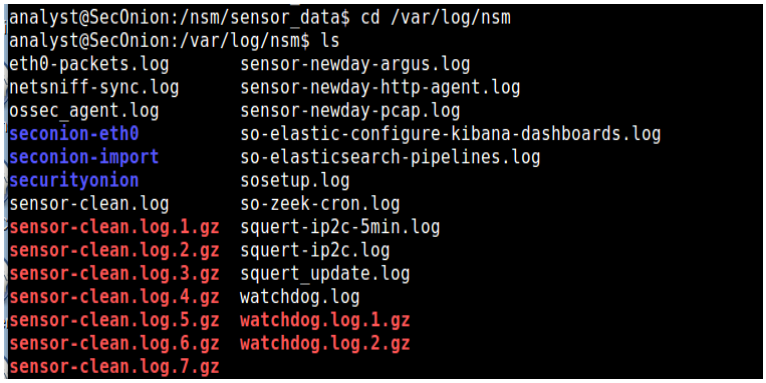
3) Log snort dapat ditemukan di /nsm/sensor_data/. Ubah direktori dan gunakan perintah ls -l untuk melihat semua file log yang dihasilkan oleh Snort



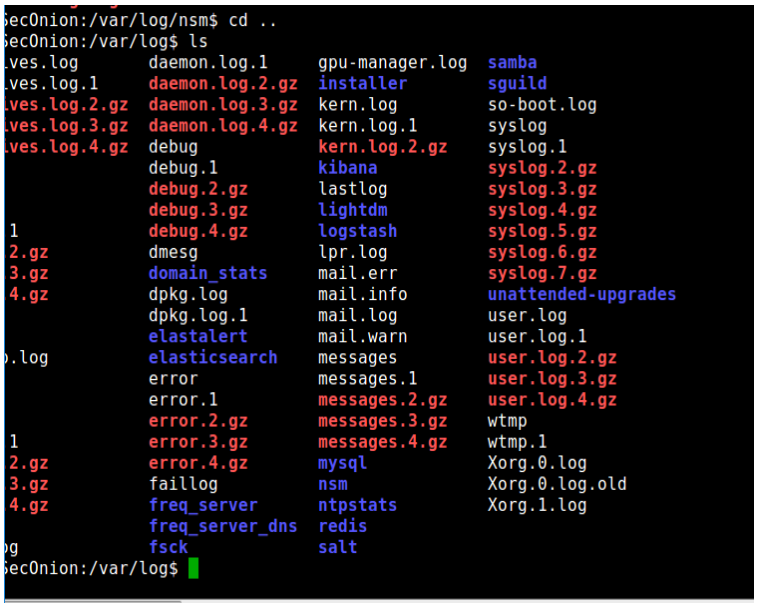
Gunakan perintah ls –l seconion-eth0 untuk melihat file yang dihasilkan oleh antarmuka eth0.



4) Various Logs, ubah direktori dan gunakan perintah ls untuk melihat semua file log di direktori.



Log ELK dapat ditemukan di direktori /var/log. Ubah direktori dan gunakan perintah ls untuk membuat daftar file dan direktori.



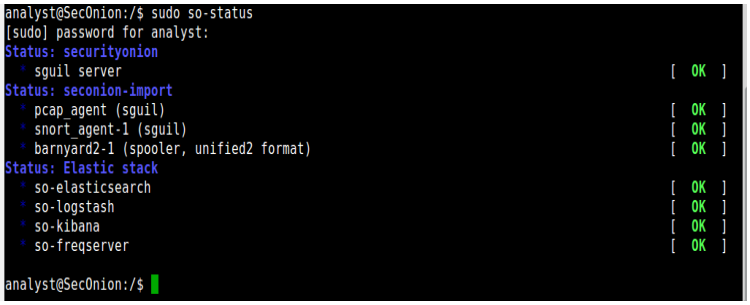
Investigasi SQL Injection Attack

I. Alat dan Bahan

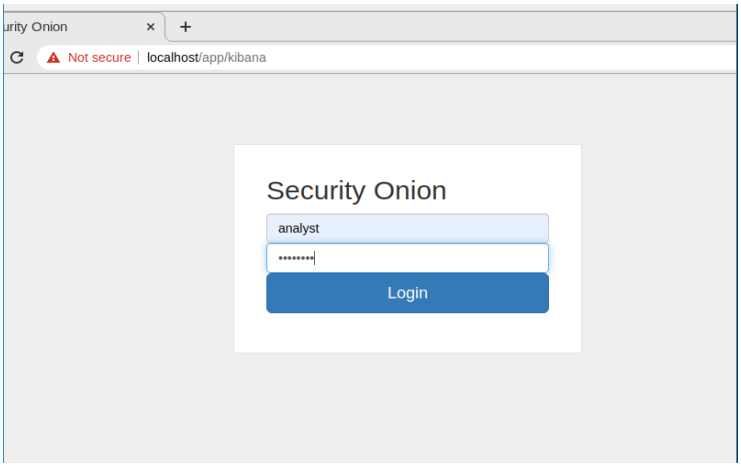
Mesin virtual CyberOps Workstation

II. Langkah kerja

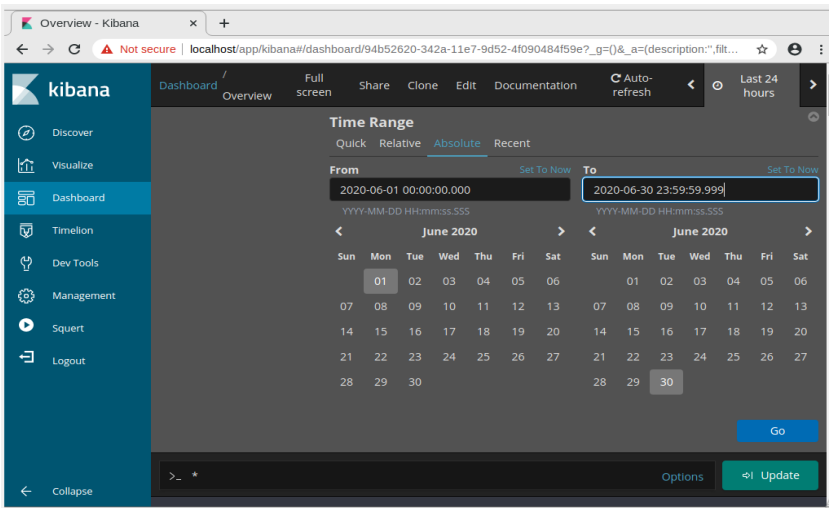
1) Ubah jangka waktu /timeframe, Masukkan perintah sudo so-status di terminal untuk memeriksa status layanan. Status untuk semua layanan harus OK sebelum memulai analisis



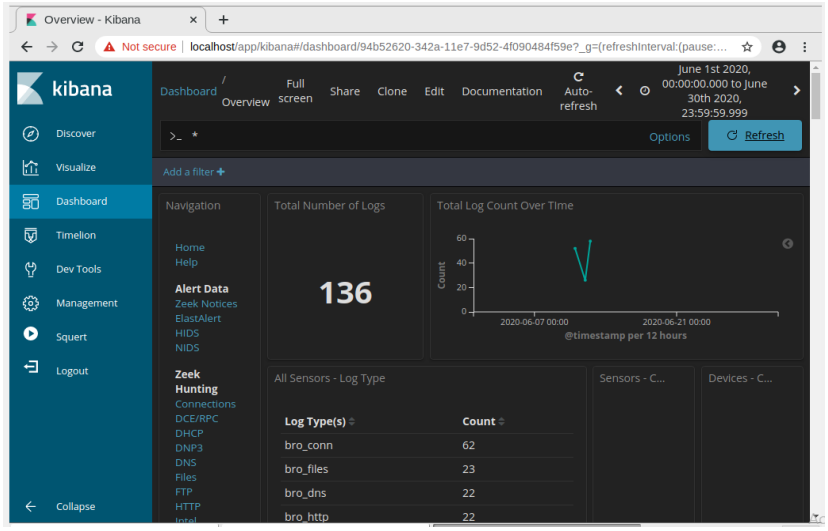
Selanjutnya buka kibana di browser dan masuk menggunakan username dan password



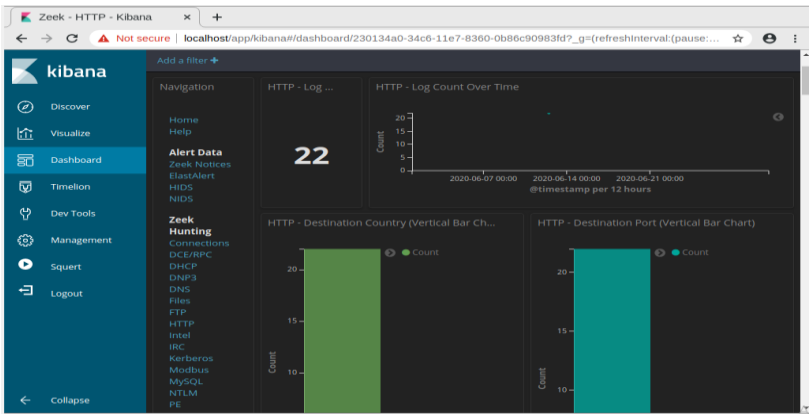
Klik 24 jam terakhir untuk mengubah ukuran Rentang Waktu sampel. Serangan injeksi SQL terjadi pada Juni 2020 jadi itulah yang perlu ditargetkan



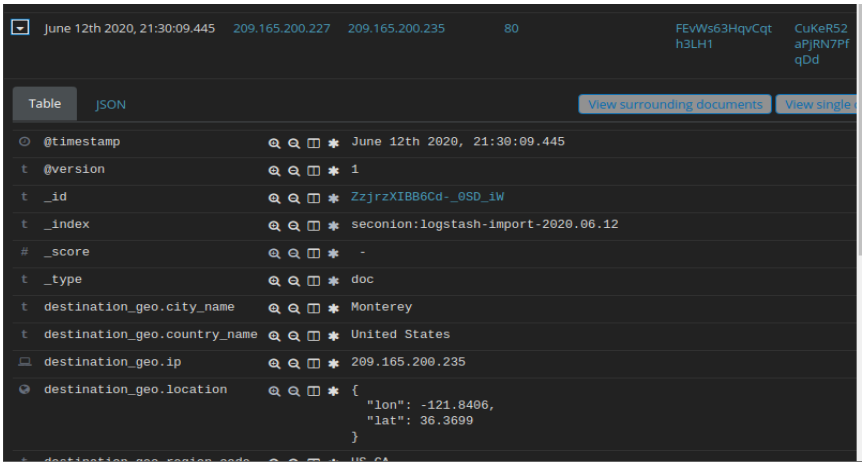
Perhatikan jumlah total log untuk seluruh bulan Juni 2020.



2) Filter dari HTTP traffi digunakan untuk memilih log yang terkait dengan lalu lintas HTTP. Pilih HTTP di bawah judul Zeek Hunting.



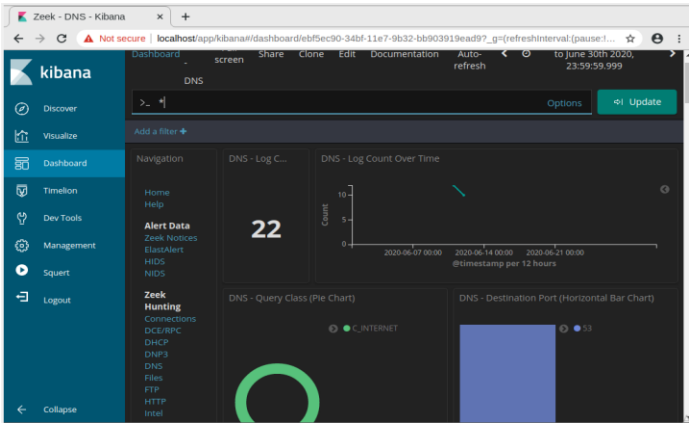
3) Review hasil, klik nilai di bidang alert _id dari entri log untuk mendapatkan tampilan yang berbeda pada event tersebut



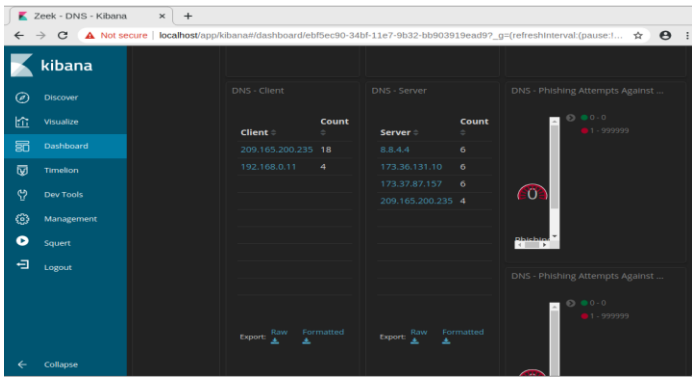
Temukan keyword nama pengguna dalam transkrip

4) Analisis DNS exfiltration

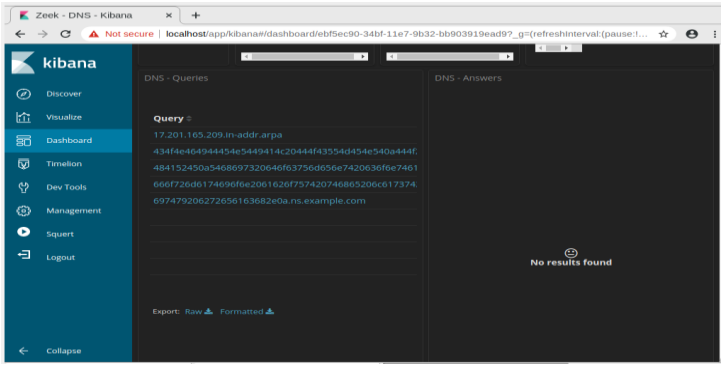
Filter DNS traffic, Di area Dashboard yang sama, klik DNS di bagian Zeek Hunting. Perhatikan metrik Jumlah Log DNS dan diagram batang horizontal Port Tujuan



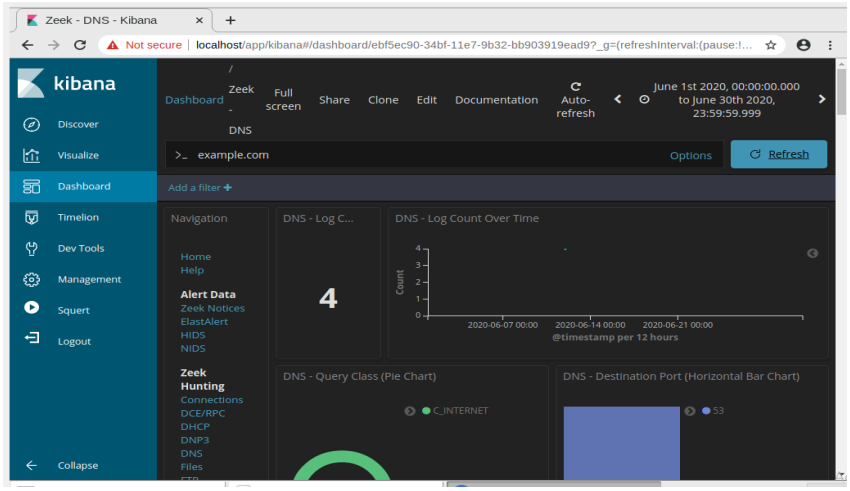
Daftar klien DNS dan Server DNS teratas berdasarkan jumlah permintaan dan respons mereka.



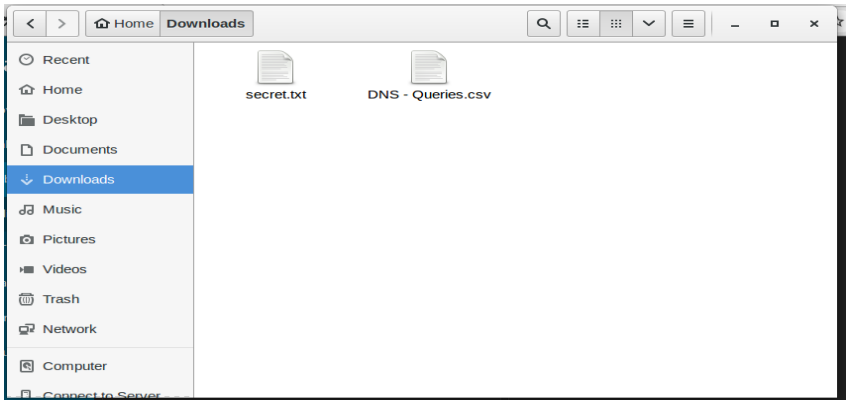
Daftar kueri DNS teratas berdasarkan nama domain.



Masukkan example.com di bilah pencarian untuk memfilter example.com dan klik Perbarui.



5) Tentukan data yang diekstraksi, File CSV diunduh ke folder /home/analyst/Downloads



Di terminal, gunakan perintah xxd untuk memecahkan kode teks dalam file CSV dan menyimpannya ke file bernama secret.txt. Gunakan cat untuk menampilkan konten secret.txt ke konso