

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 -l
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]$
```

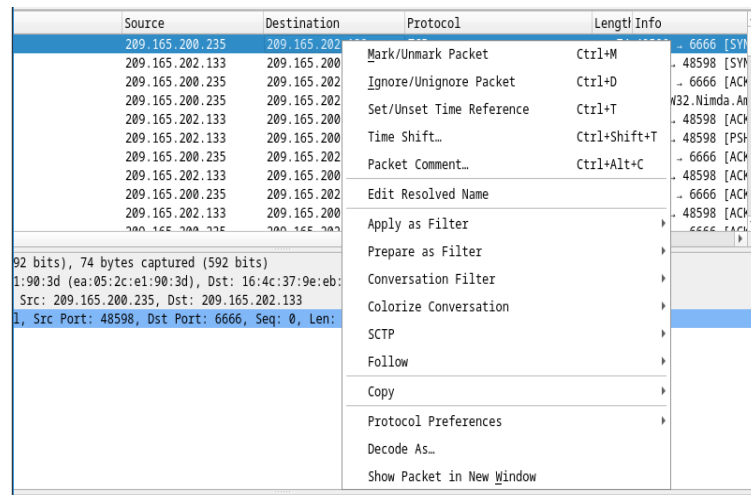
### Perintah untuk membuka file nimda.download.pcap di Wireshark

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

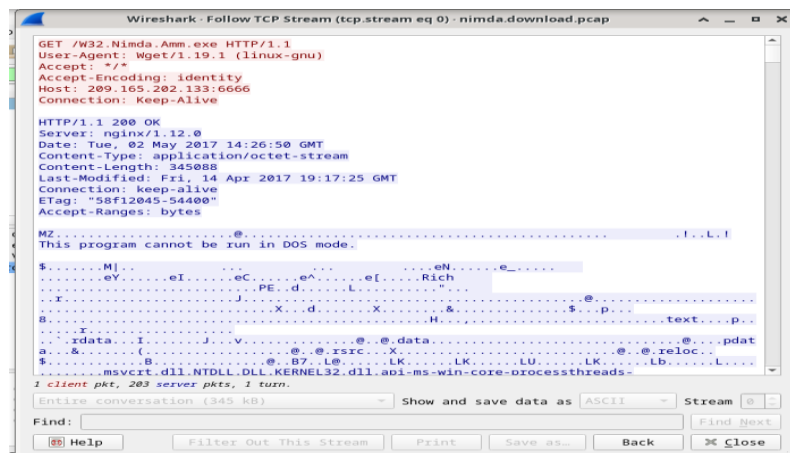
Pcap berisi semua paket yang dikirim dan diterima saat tcpdump sedang berjalan. Paket satu sampai tiga adalah jabat tangan TCP. Paket keempat menunjukkan permintaan file malware. Mengonfirmasi apa yang sudah diketahui, permintaan dilakukan melalui HTTP, dikirim sebagai permintaan GET.

[illegible]

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



Wireshark akan menampilkan detail untuk seluruh aliran TCP yang dipilih.

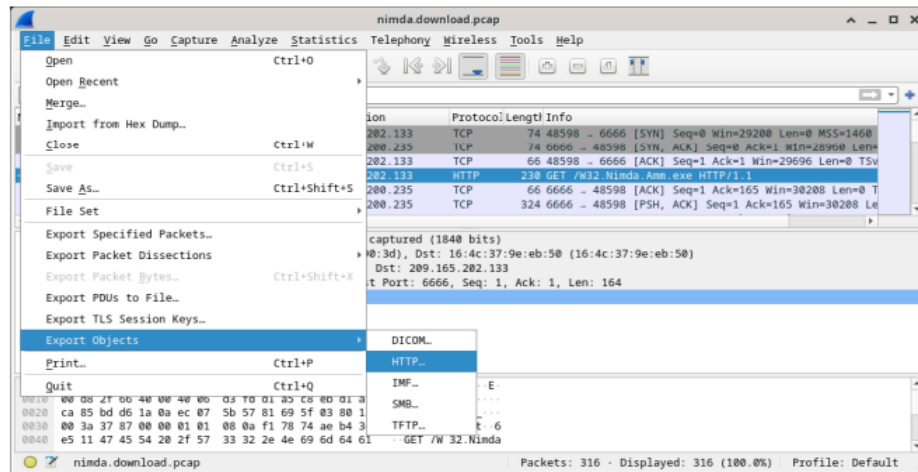


## 2). Extract Files yang di unduh dari PCAP

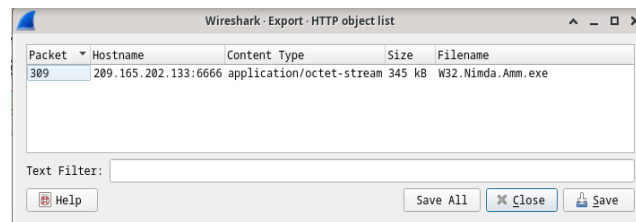
Pada paket keempat dalam file nimda.download.pcap, perhatikan bahwa permintaan HTTP GET dihasilkan dari 209.165.200.235 menjadi 209.165.202.133. Kolom Info juga menunjukkan bahwa ini sebenarnya adalah permintaan GET untuk file tersebut.

3	0.000621	209.165.200.235	209.165.202.133	TCP	66 6666 → 48598 [ACK] Seq=
4	0.000565	209.165.200.235	209.165.202.133	HTTP	230 GET /W32.Nimda.Amm.exe
5	0.000588	209.165.202.133	209.165.200.235	TCP	66 6666 → 48598 [ACK] Seq=

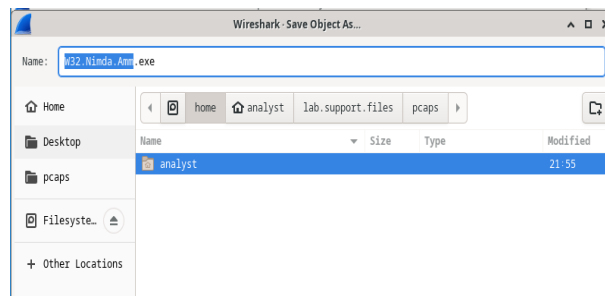
Dengan paket permintaan GET yang dipilih, navigasikan ke File > Export Objects > HTTP, dari menu Wireshark.



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@sec0ps pcaps]$ cd /home/analyst
[analyst@sec0ps ~]$ 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@sec0ps ~]$
```

Perintah untuk memberikan informasi tentang jenis file.

```
[analyst@sec0ps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@sec0ps ~]$
```

## 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:

```
Terminal - analyst@SecOnion: /nsm/bro/logs/current
File Edit View Terminal Tabs Help
analyst@SecOnion:~$ cd /nsm/bro/logs/current
analyst@SecOnion:/nsm/bro/logs/current$ ls -l
total 0
analyst@SecOnion:/nsm/bro/logs/current$
```

- 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

```
analyst@SecOnion:/nsm/bro/logs/current$ cd /nsm/sensor_data
analyst@SecOnion:/nsm/sensor_data$ ls -l
total 12
drwxrwxr-x 7 sguil sguil 4096 Jun 19 2020 seconion-eth0
drwxrwxr-x 5 sguil sguil 4096 Jun 19 2020 seconion-eth1
drwxrwxr-x 7 sguil sguil 4096 Jun 19 2020 seconion-import
analyst@SecOnion:/nsm/sensor_data$
```

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

```
analyst@SecOnion:/nsm/sensor_data$ ls -l seconion-eth0
total 28
drwxrwxr-x 2 sguil sguil 4096 Jun 19 2020 argus
drwxrwxr-x 3 sguil sguil 4096 Jun 19 2020 dailylogs
drwxrwxr-x 2 sguil sguil 4096 Jun 19 2020 portscans
drwxrwxr-x 2 sguil sguil 4096 Jun 19 2020 sancp
drwxr-xr-x 2 sguil sguil 4096 Jun 19 2020 snort-1
-rw-r--r-- 1 sguil sguil 5594 Jun 19 2020 snort-1.stats
-rw-r--r-- 1 root root 0 Jun 19 2020 snort.stats
analyst@SecOnion:/nsm/sensor_data$
```

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

```
analyst@Sec0nion:/nsm/sensor_data$ cd /var/log/nsm
analyst@Sec0nion:/var/log/nsm$ ls
eth0-packets.log      sensor-newday-argus.log
netsniff-sync.log    sensor-newday-http-agent.log
ossec_agent.log       sensor-newday-pcap.log
seconion-eth0         so-elastic-configure-kibana-dashboards.log
seconion-import       so-elasticsearch-pipelines.log
securityonion         sosetup.log
sensor-clean.log      so-zeek-cron.log
sensor-clean.log.1.gz squert-ip2c-5min.log
sensor-clean.log.2.gz squert-ip2c.log
sensor-clean.log.3.gz squert_update.log
sensor-clean.log.4.gz watchdog.log
sensor-clean.log.5.gz watchdog.log.1.gz
sensor-clean.log.6.gz watchdog.log.2.gz
sensor-clean.log.7.gz
```

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

```
Sec0nion:/var/log/nsm$ cd ..
Sec0nion:/var/log$ ls
aves.log      daemon.log.1      gpu-manager.log  samba
aves.log.1    daemon.log.2.gz   installer        sguild
aves.log.2.gz daemon.log.3.gz   kern.log         so-boot.log
aves.log.3.gz daemon.log.4.gz   kern.log.1       syslog
aves.log.4.gz debug            kern.log.2.gz    syslog.1
              debug.1          kibana           syslog.2.gz
              debug.2.gz       lastlog          syslog.3.gz
              debug.3.gz       lightdm          syslog.4.gz
              debug.4.gz       logstash         syslog.5.gz
1              dmesg            lpr.log          syslog.6.gz
2.gz          domain_stats     mail.err          syslog.7.gz
3.gz          dpkg.log         mail.info         unattended-upgrades
4.gz          dpkg.log.1       mail.log          user.log
              elastalert       mail.warn         user.log.1
              elasticsearch    messages          user.log.2.gz
              error          messages.1        user.log.3.gz
              error.1          messages.2.gz     user.log.4.gz
              error.2.gz       messages.3.gz     wtmp
              error.3.gz       messages.4.gz     wtmp.1
              error.4.gz       mysql             Xorg.0.log
3.gz          faillog         nsm               Xorg.0.log.old
4.gz          freq_server     ntpstats          Xorg.1.log
              freq_server_dns  redis
log           fsck            salt
Sec0nion:/var/log$
```

# Investigasi SQL Injection Attack

## I. Alat dan Bahan

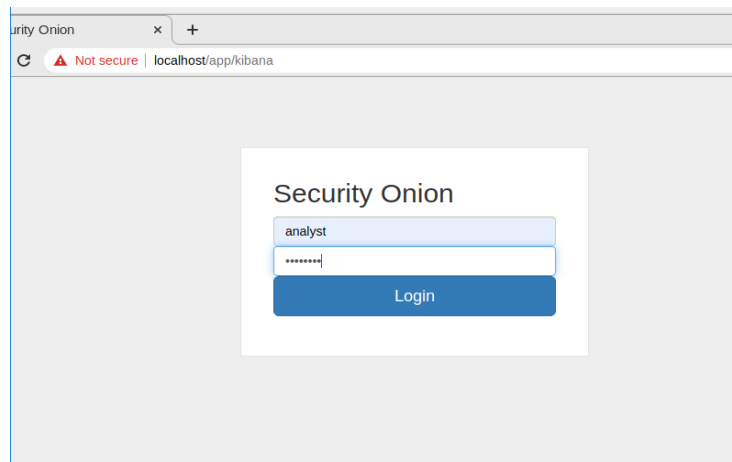
Mesin virtual CyberOps Workstation

## 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

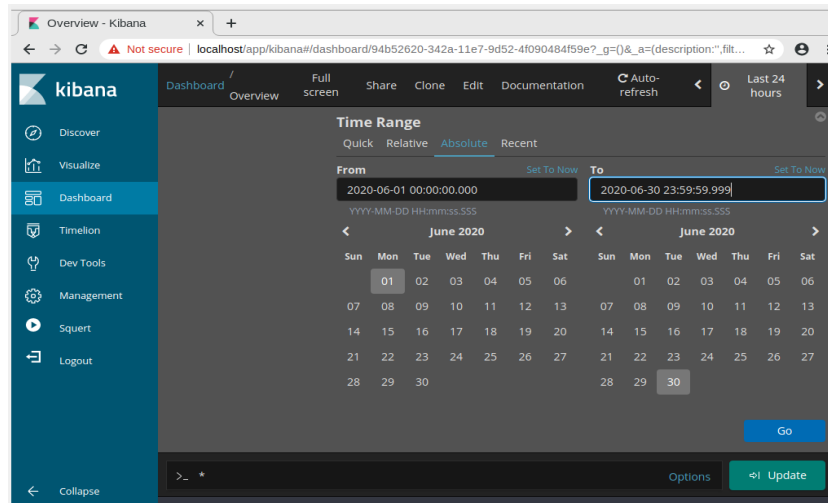
```
analyst@Sec0nion:/$ sudo so-status
[sudo] password for analyst:
Status: securityonion
  * sgul server [ OK ]
Status: seconion-import
  * pcap_agent (sgul) [ OK ]
  * snort_agent-1 (sgul) [ OK ]
  * barnyard2-1 (spooler, unified2 format) [ OK ]
Status: Elastic stack
  * so-elasticsearch [ OK ]
  * so-logstash [ OK ]
  * so-kibana [ OK ]
  * so-freqserver [ OK ]
analyst@Sec0nion:/$
```

Selanjutnya buka kibana di browser dan masuk menggunakan username dan password

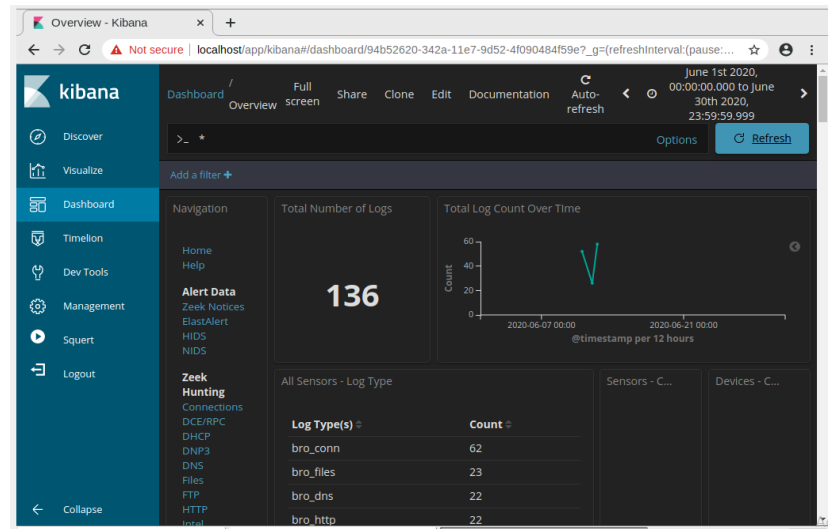


Klik 24 jam terakhir untuk mengubah ukuran Rentang Waktu sampel. Serangan injeksi SQL terjadi pada Juni 2020 jadi itulah yang perlu ditargetkan

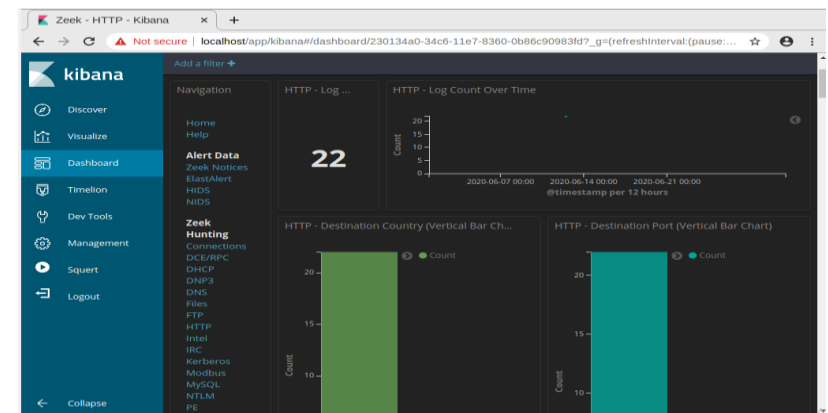


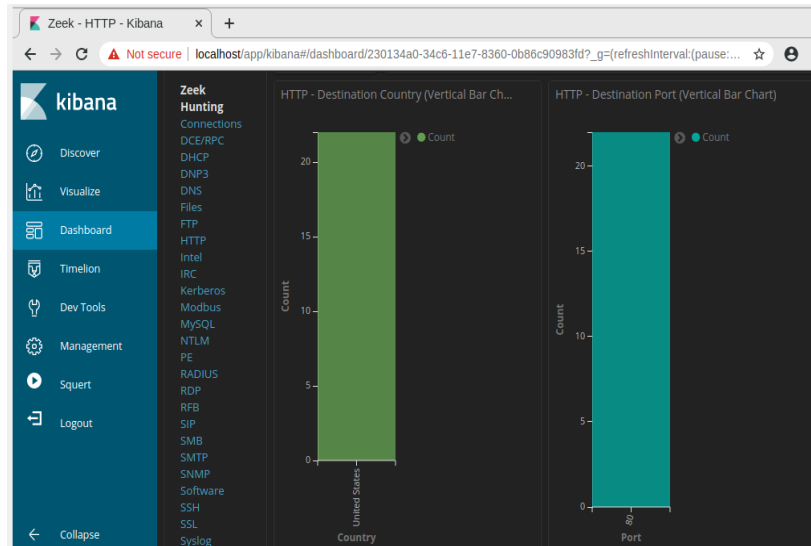


Perhatikan jumlah total log untuk seluruh bulan Juni 2020.



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

June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEWws63HqvCqt h3LH1	CuKeR52 aPJRN7PF qDd
<div> <div>Table</div> <div>JSON</div> <div>View surrounding documents</div> <div>View single</div> </div>					
@timestamp				June 12th 2020, 21:30:09.445	
@version				1	
_id				ZzjrZXIBB6Cd-_0SD_iW	
_index				seconion:logstash-import-2020.06.12	
_score				-	
_type				doc	
destination_geo.city_name				Monterey	
destination_geo.country_name				United States	
destination_geo.ip				209.165.200.235	
destination_geo.location				{ "lon": -121.8486, "lat": 36.3699 }	

Temukan keyword nama pengguna dalam transkrip

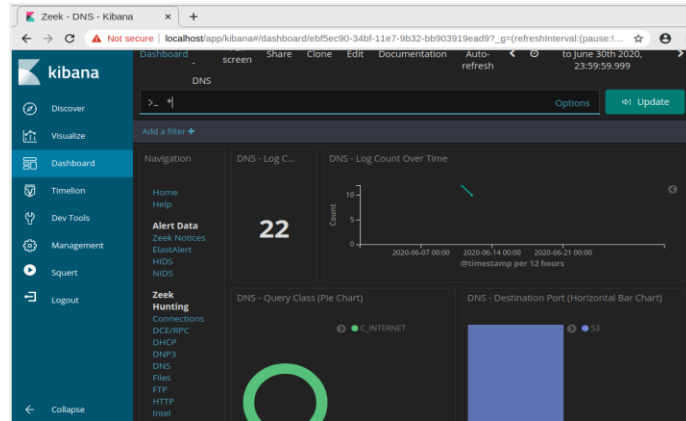
```

DST: <b>Username=</b>7746536337776330<br>
DST: 17
DST: <b>Password=</b>722<br>
DST: 22
DST: <b>Signature=</b>2015-04-01<br><p>
DST: 24
DST: <b>Username=</b>8242325748474749<br>
DST: 17
DST: <b>Password=</b>461<br>
DST: 22
DST: <b>Signature=</b>2016-03-01<br><p>
DST: 24
DST: <b>Username=</b>7725653200487633<br>
DST: 17
DST: <b>Password=</b>230<br>
DST: 22
DST: <b>Signature=</b>2017-06-01<br><p>
DST: 24

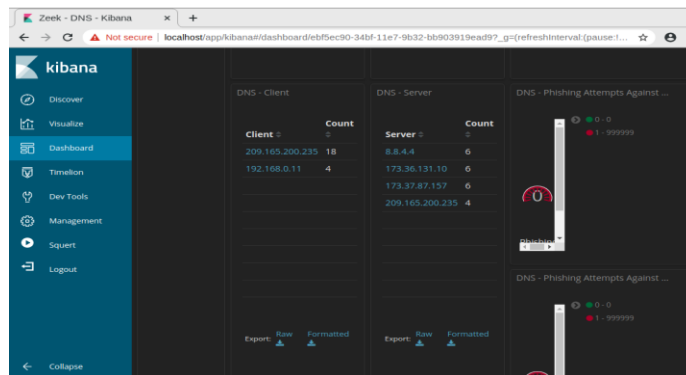
```

#### 4) Analisis DNS exfiltration

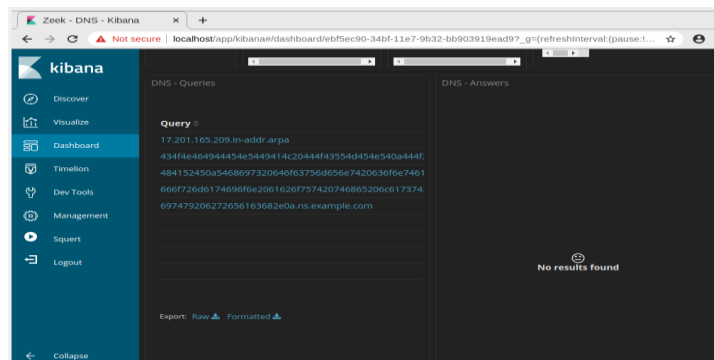
Filter DNS traffic, Di area Dashboard yang sama, klik DNS di bagian Zeek Hunting. Perhatikan metrik Jumlah Log DNS dan diagram batang horizontal Port Tujuan



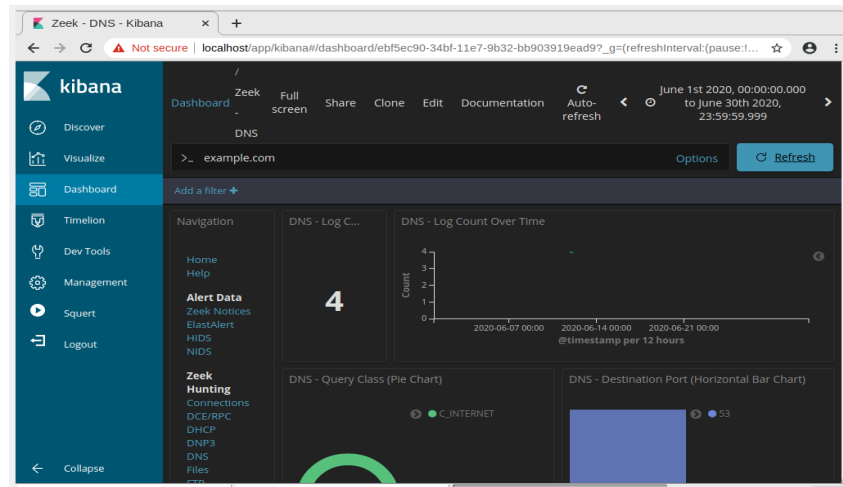
Daftar klien DNS dan Server DNS teratas berdasarkan jumlah permintaan dan respons mereka.



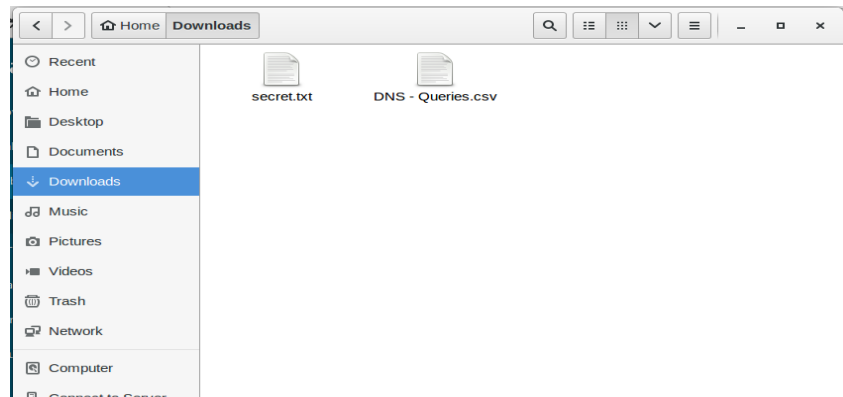
Daftar kueri DNS teratas berdasarkan nama domain.



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

```
analyst@SecOnion:~$ cd \Downloads
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
analyst@SecOnion:~/Downloads$ cat secret.txt
CONFIDENTIAL DOCUMENT
DO NOT SHARE
This document contains information about the last security breach.
analyst@SecOnion:~/Downloads$
```