

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

DNS Attack



DI SUSUN OLEH

Nama : M Abdul Aziz
NIM : 21/474516/SV/18951
Hari, Tanggal : Selasa, 14 Maret 2023
Kelas : RI4AA

**LABORATORIUM PERANGKAT KERAS DAN LUNAK
PROGRAM SARJANA TERAPAN (DIV) TEKNOLOGI
REKAYASA INTERNET
DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA
SEKOLAH VOKASI
UNIVERSITAS GADJAH MADA
2023**

Praktikum Keamanan Informasi 1

DNS Attack

I. Tujuan

—

II. Latar Belakang

III. Alat & Bahan

— S

IV. Instruksi Kerja

1. S

Langkah 1 Menganalisis log yg ditangkap sebelumnya dan pengambilan lalu lintas

a. S

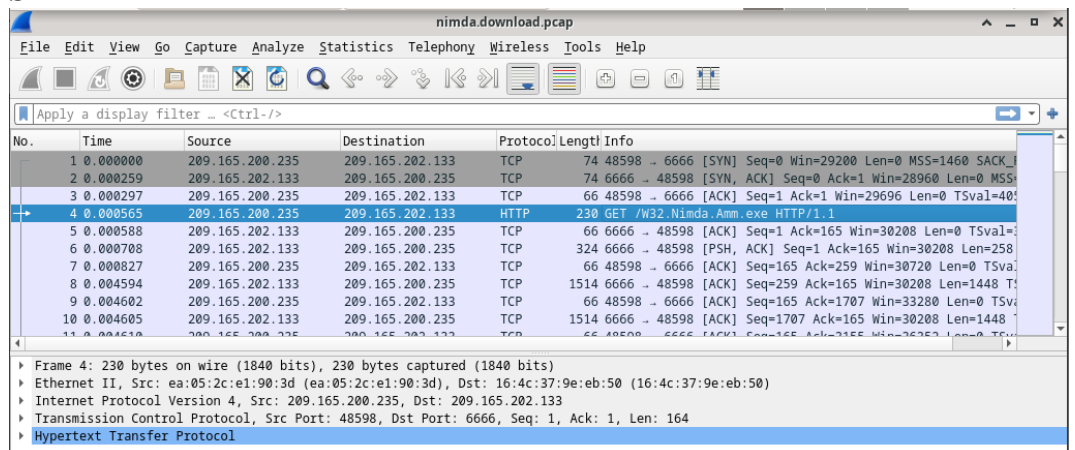
```
Terminal - analyst@secOps:~/lab.support.files/pcaps
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ cd lab.support.files/pcaps
[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]$
```

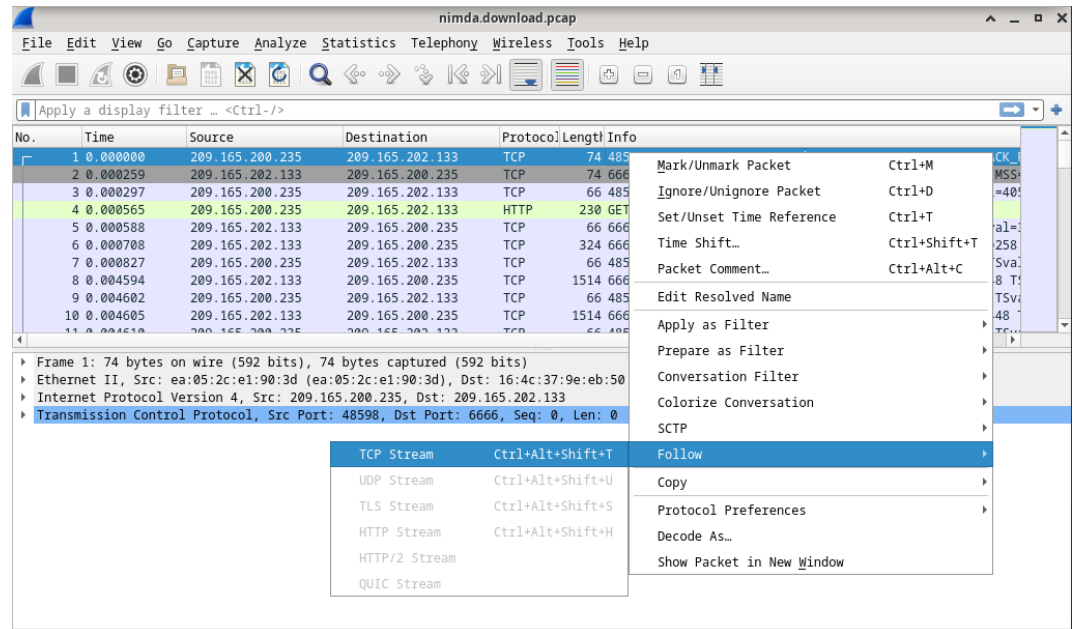
b. S

```
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
[1] 569
[analyst@secOps pcaps]$
```

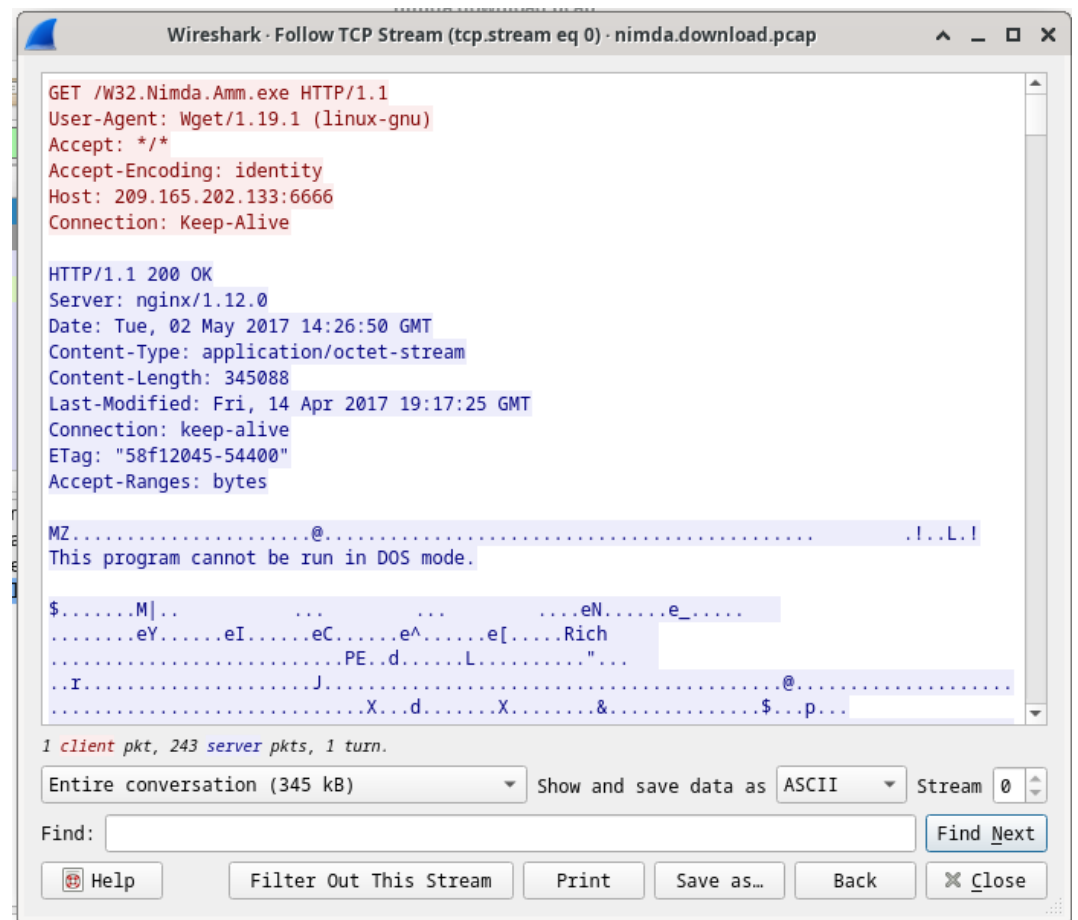
c. S



- d. S
e. S



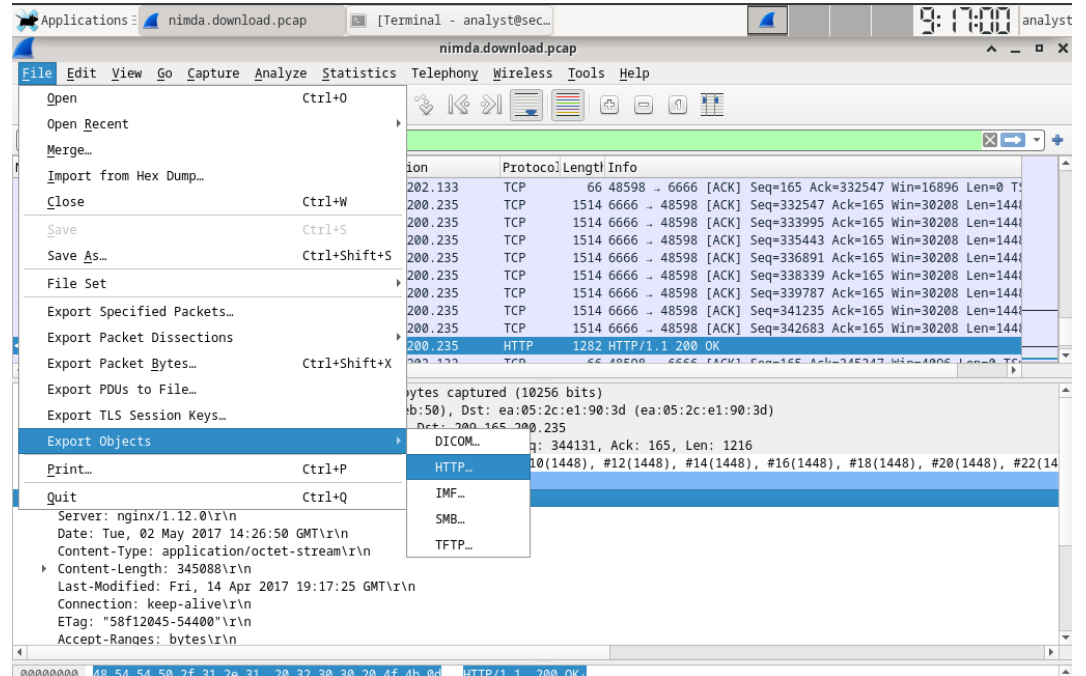
- f. S



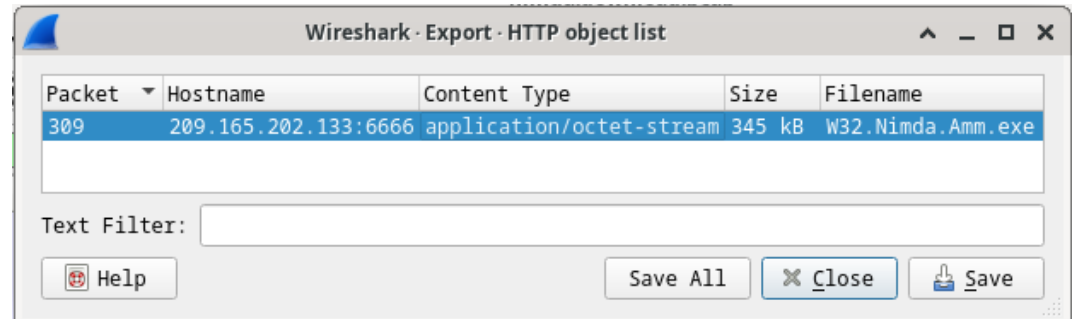
Langkah 2: Extract Files yang di unduh dari PCAP

a. S

b. S

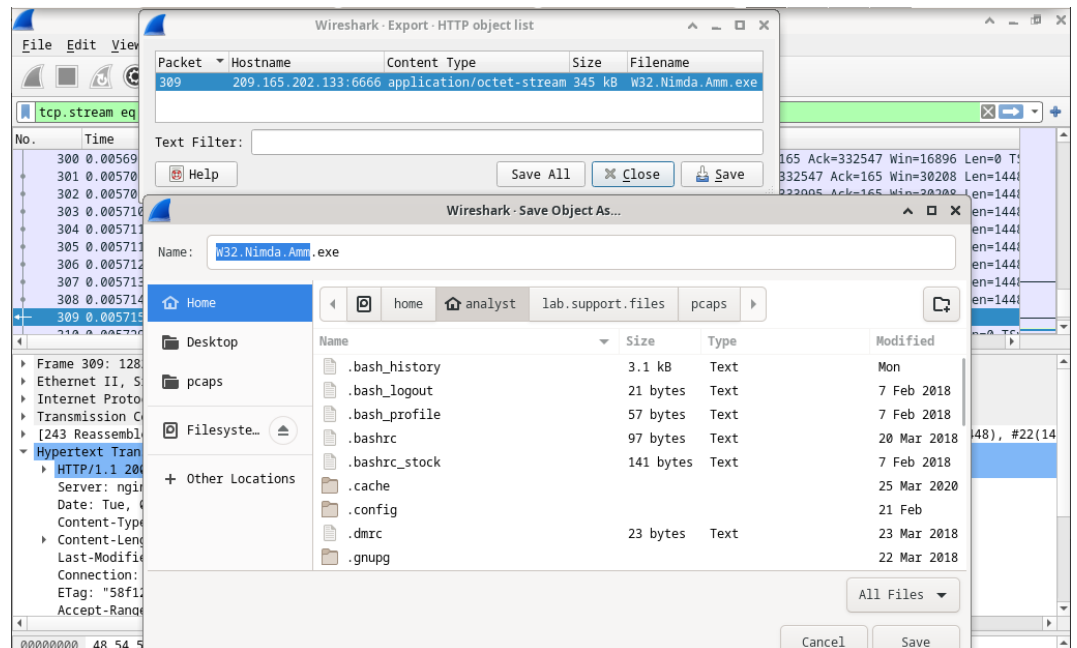


c. S

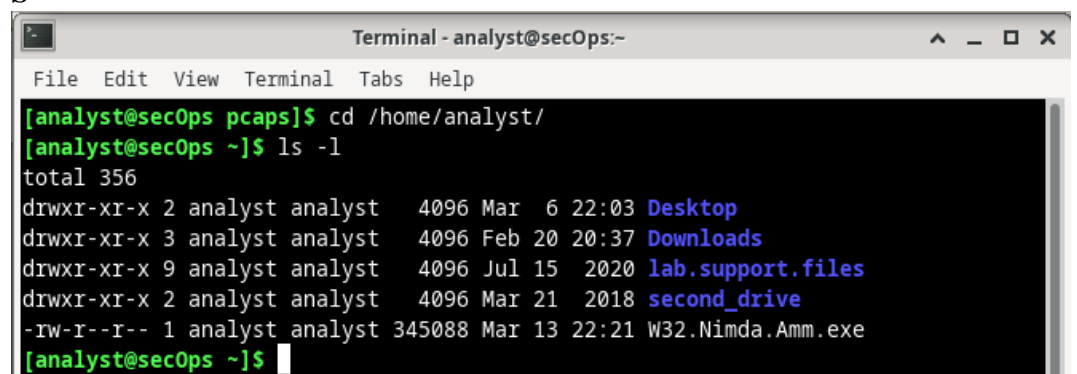


d. S

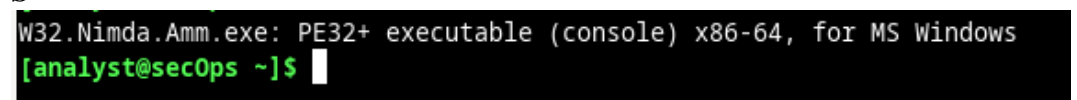
e. S



f. S



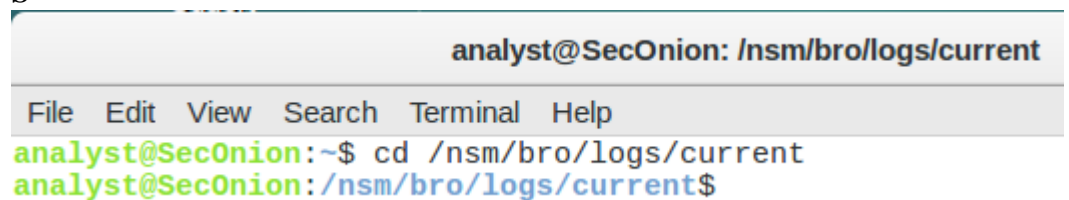
g. S



Persiapan Log File pada Security Onion VM

- Buka vm security onion
- Zeek logs

- Buka terminal
- S



- S

```
analyst@SecOnion:/nsm/bro/logs/current$ ls -l
total 0
analyst@SecOnion:/nsm/bro/logs/current$ █
```

iii. Snort logs

- S

```
analyst@SecOnion: /nsm/sensor_data
File Edit View Search Terminal Help
analyst@SecOnion:~$ cd /nsm/sensor_data/
```

- S

```
analyst@SecOnion: /nsm/sensor_data
File Edit View Search Terminal Help
analyst@SecOnion:~$ 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$
```

- D

```
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
```

iv. Various logs

- S

```

analyst@SecOnion: /var/log/nsm
File Edit View Search Terminal Help
analyst@SecOnion:/var/log/nsm$ cd
analyst@SecOnion:~$ cd /var/log/nsm/
analyst@SecOnion:/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
analyst@SecOnion:/var/log/nsm$ █

```

- S

```

analyst@SecOnion: /var/log
File Edit View Search Terminal Help
analyst@SecOnion:/var/log/nsm$ cd /var/log/
analyst@SecOnion:/var/log$ ls
alternatives.log          debug.4.gz             messages.3.gz
alternatives.log.1        dmesg                 messages.4.gz
alternatives.log.2.gz     domain_stats          mysql
alternatives.log.3.gz     dpkg.log              nsm
alternatives.log.4.gz     dpkg.log.1            ntpstats
alternatives.log.5.gz     elastalert            redis
apache2                  elasticsearch          salt
apt                      error                 samba
auth.log                 error.1               sguild
auth.log.1               error.2.gz            so-boot.log
auth.log.2.gz            error.3.gz            syslog
auth.log.3.gz            error.4.gz            syslog.1
auth.log.4.gz            faillog               syslog.2.gz
boot                     freq_server            syslog.3.gz
boot.log                 freq_server_dns        syslog.4.gz
bootstrap.log            fsck                   syslog.5.gz
btmtp                    gpu-manager.log        syslog.6.gz
btmtp.1                  installer              syslog.7.gz
cron.log                 kern.log               ubuntu-advantage.log
cron.log.1               kern.log.1             ubuntu-advantage-timer.log
cron.log.2.gz            kern.log.2.gz          unattended-upgrades
cron.log.3.gz            kibana                 user.log
cron.log.4.gz            lastlog                user.log.1
curator                  lightdm                user.log.2.gz
daemon.log               logstash               user.log.3.gz
daemon.log.1             lpr.log                user.log.4.gz
daemon.log.2.gz          mail.err               wtmp
daemon.log.3.gz          mail.info              wtmp.1
daemon.log.4.gz          mail.log               Xorg.0.log
debug                    mail.warn              Xorg.0.log.old
debug.1                  messages               Xorg.1.log
debug.2.gz               messages.1
debug.3.gz               messages.2.gz
analyst@SecOnion:/var/log$ █

```

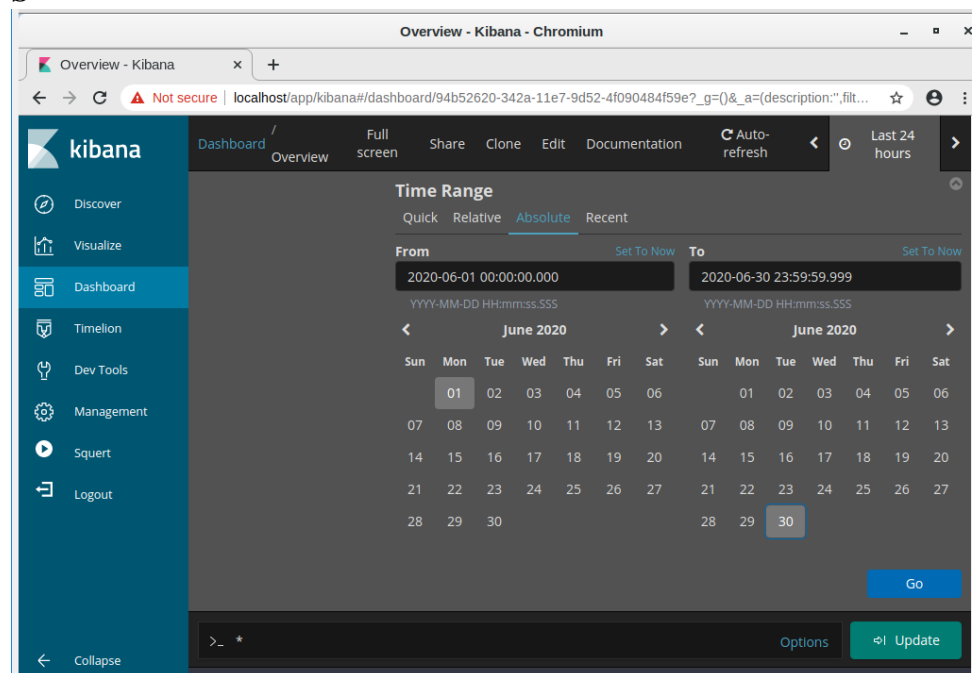
Part 3: Langkah 1: Investigasi SQL Injection Attack

a. Ubah jangka waktu/timeframe

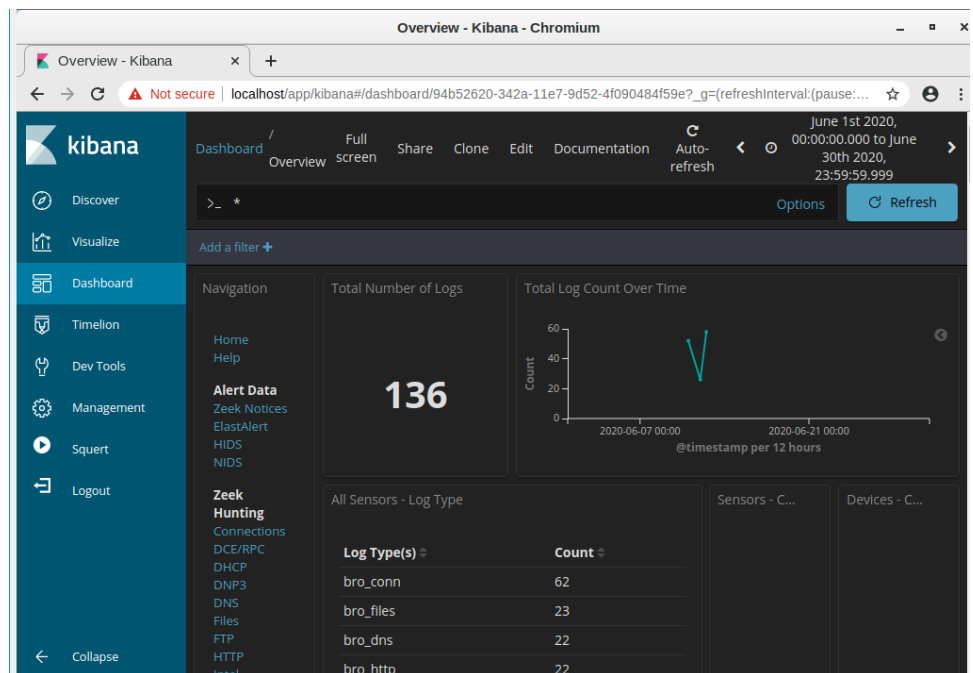
- Start security onion VM
- S

```
analyst@SecOnion: ~  
File Edit View Search Terminal Help  
analyst@SecOnion:~$ sudo so-status  
Status: securityonion  
* sgul server [ OK ]  
Status: seconion-import  
* pcap_agent (sguil) [ OK ]  
* snort_agent-1 (sguil) [ OK ]  
* barnyard2-1 (spooler, unified2 format) [ OK ]  
Status: Elastic stack  
* so-elasticsearch [ OK ]  
* so-logstash [ OK ]  
* so-kibana [ OK ]  
* so-freqserver [ OK ]  
analyst@SecOnion:~$
```

• S

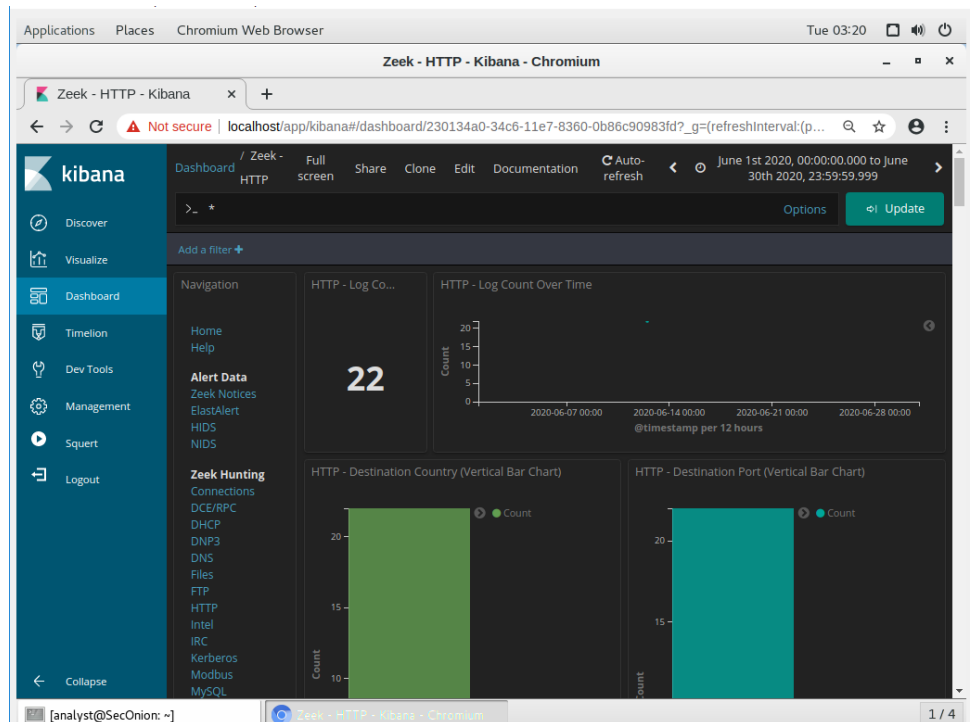


• S



b. Filter dari HTTP Traffic

- S



- S

Zeek - HTTP - Kibana - Chromium

Zeek - HTTP - Kibana x +

localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(refreshInterval:(p...)

Limited to 10 results. Refine your search. 1-10 of 22

Time	source_ip	destination_ip	destination_port	resp_fuids	uid	_id
June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvW63HqvCqth3LH1	CuKeR52aPjRN7PqDd	ZjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbb5T2feBG6aAYvBh	Cb5K6C1mim2iUVKkC1	ZjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TjaAYdNQ14	Cb5K6C1mim2iUVKkC1	ZjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWO03T1TT34UWkR63	Cb5K6C1mim2iUVKkC1	ZDjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37eK1464vM8ihuc0j	Cb5K6C1mim2iUVKkC1	YjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4GBqR5	Cb5K6C1mim2iUVKkC1	YjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YOVulch	C252w31zFvpV63kPa	XjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	Fui2tB17PXhDulvng4	Cr3RGFezop5b3qz6	YDjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:17.699	209.165.200.227	209.165.200.235	80	FxgYdg18u4TH8RSEK3	C4KeAa3pLgDqfaAQyG	VTjrzXIBB6Cd-_OSD_IW
June 12th 2020, 21:23:17.698	209.165.200.227	209.165.200.235	80	F1sqnz420m9nW2sMVc	C4KeAa3pLgDqfaAQyG	WTjrzXIBB6Cd-_OSD_IW

Limited to 10 results. Refine your search. 1-10 of 22

[analyst@SecOnion: ~] Zeek - HTTP - Kibana - Chromium 1 / 4

• S

Zeek - HTTP - Kibana - Chromium

Zeek - HTTP - Kibana x +

localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?_g=(refreshInterval:(p...)

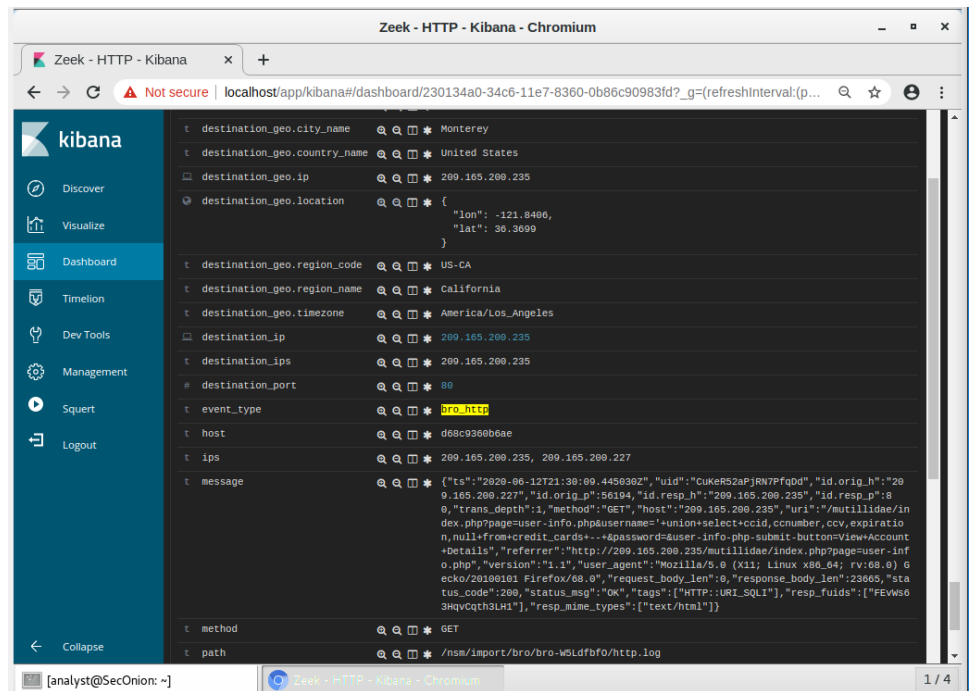
Limited to 10 results. Refine your search. 1-10 of 22

Time	source_ip	destination_ip	destination_port	resp_fuids	uid	_id
June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEvW63HqvCqth3LH1	CuKeR52aPjRN7PqDd	ZjrzXIBB6Cd-_OSD_IW

Table JSON View surrounding documents View single document

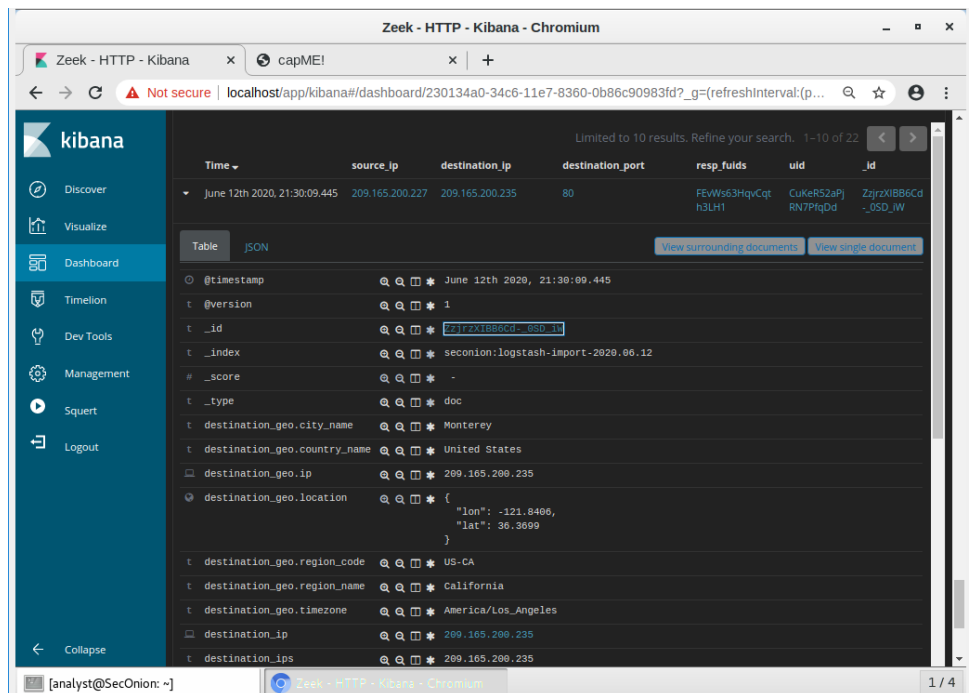
- @timestamp June 12th 2020, 21:30:09.445
- @version 1
- _id ZjrzXIBB6Cd-_OSD_IW
- _index seconion:logstash-import-2020.06.12
- _score -
- _type doc
- destination_geo.city_name Monterey
- destination_geo.country_name United States
- destination_geo.ip 209.165.200.235
- destination_geo.location { "lon": -121.8406, "lat": 36.3099 }
- destination_geo.region_code US-CA
- destination_geo.region_name California
- destination_geo.timezone America/Los_Angeles
- destination_ip 209.165.200.235
- destination_ips 209.165.200.235
- destination_port 80
- event_type bro_http

[analyst@SecOnion: ~] Zeek - HTTP - Kibana - Chromium 1 / 4



c. Review Hasil

- S



- S



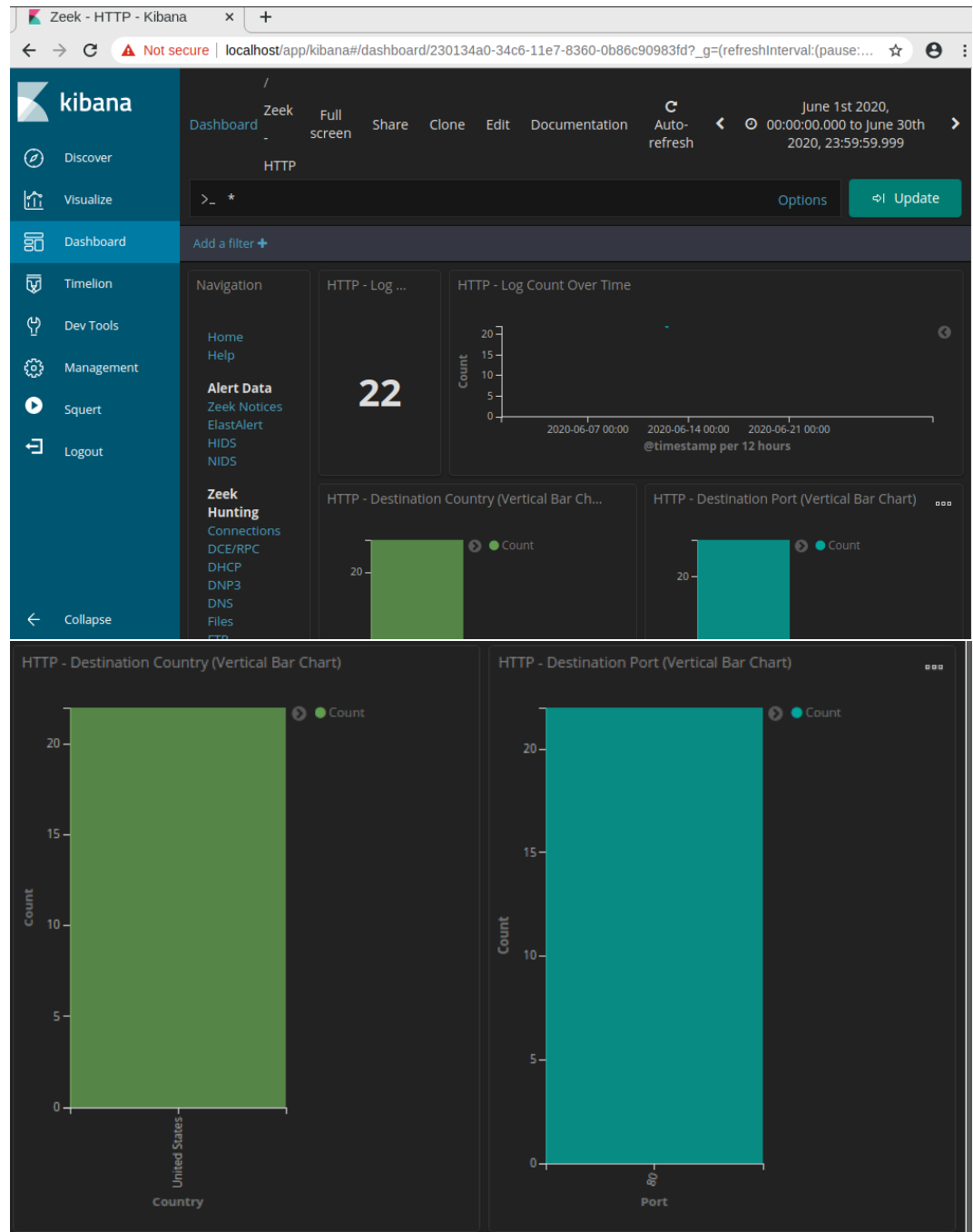
- **S**



Part 4: Analysis DNS Exfiltration

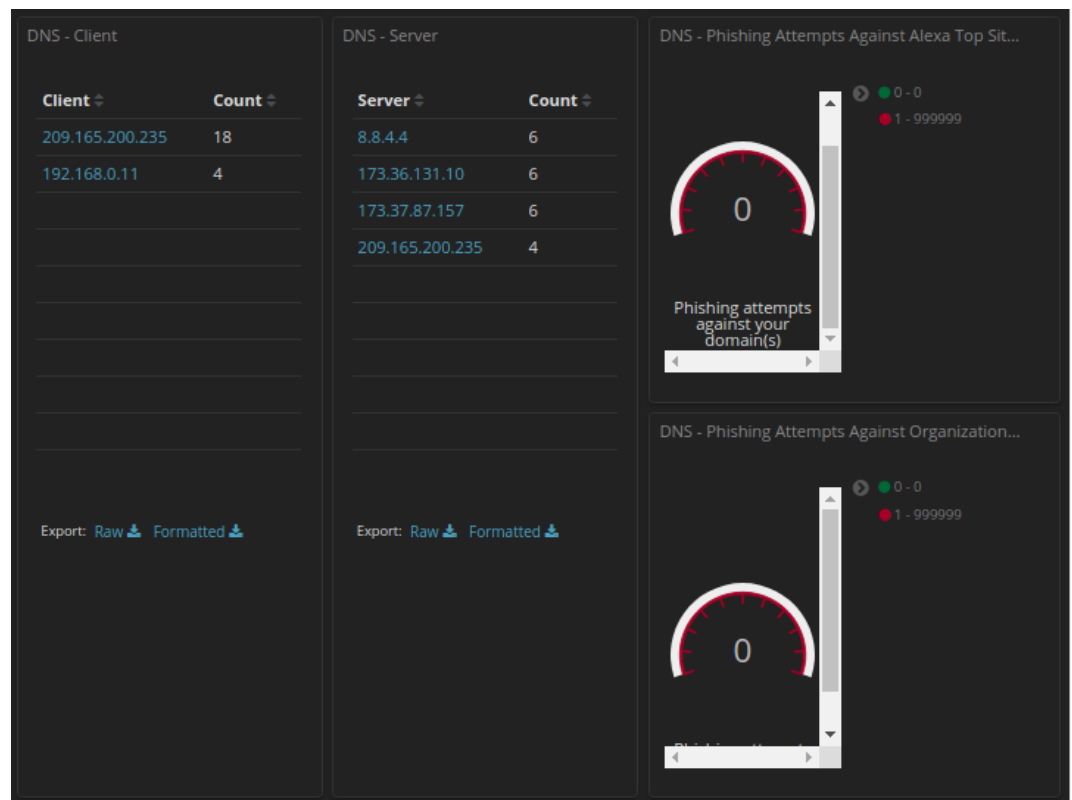
a. Filter DNS Traffic

- S
- S

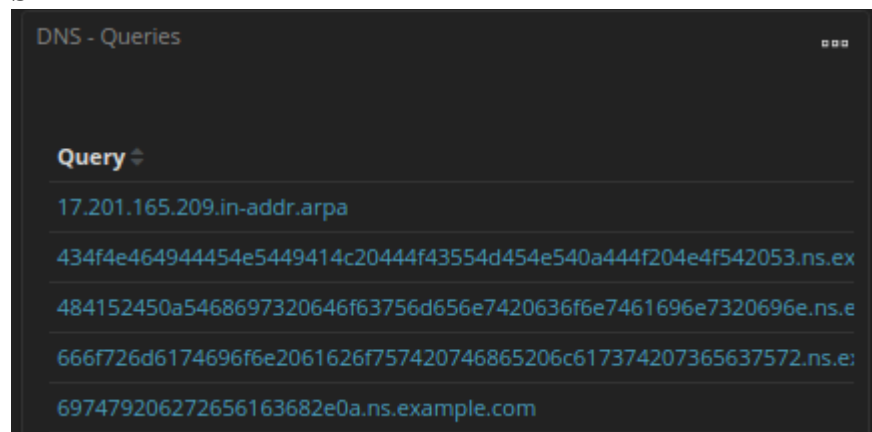


b. Tinjau entri terkait DNS

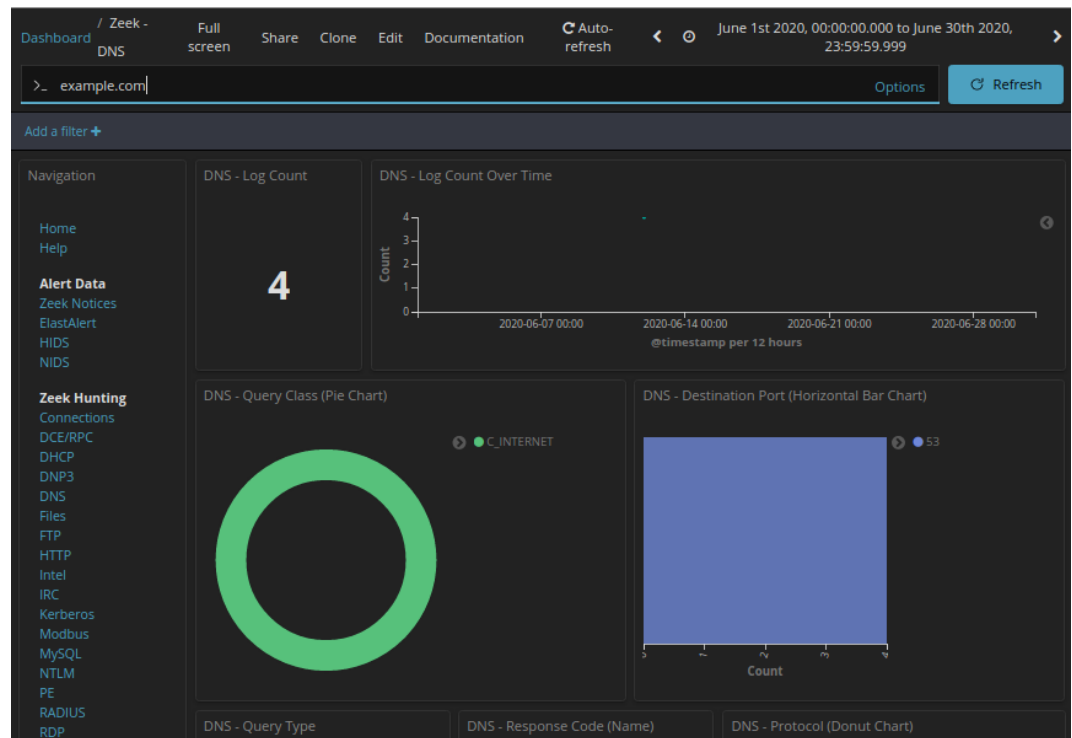
- S
- S



- S



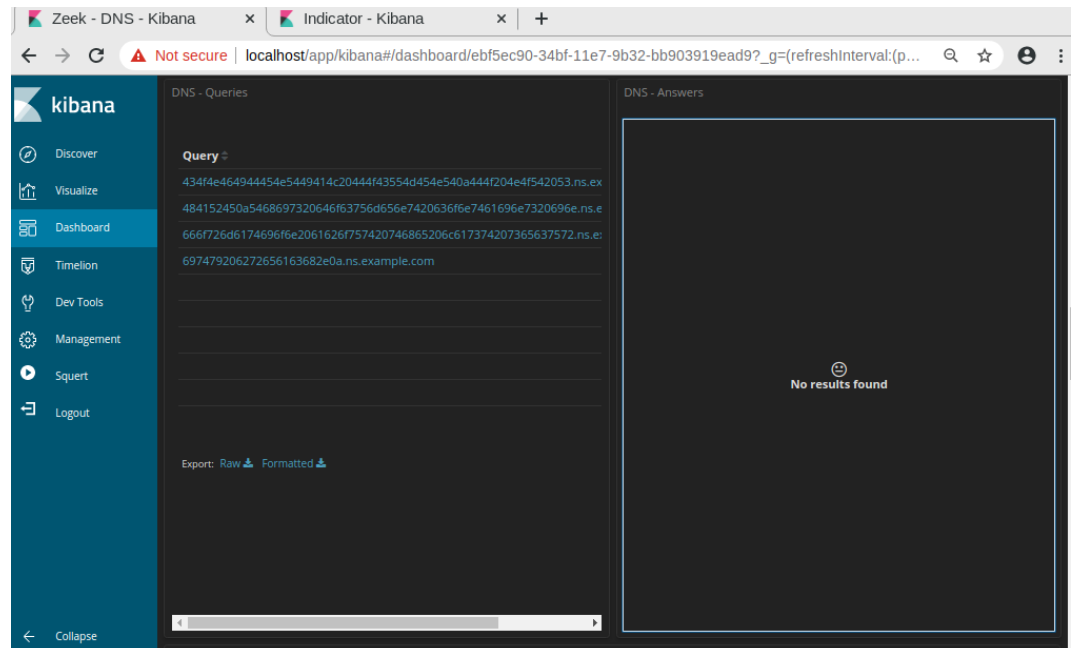
- S



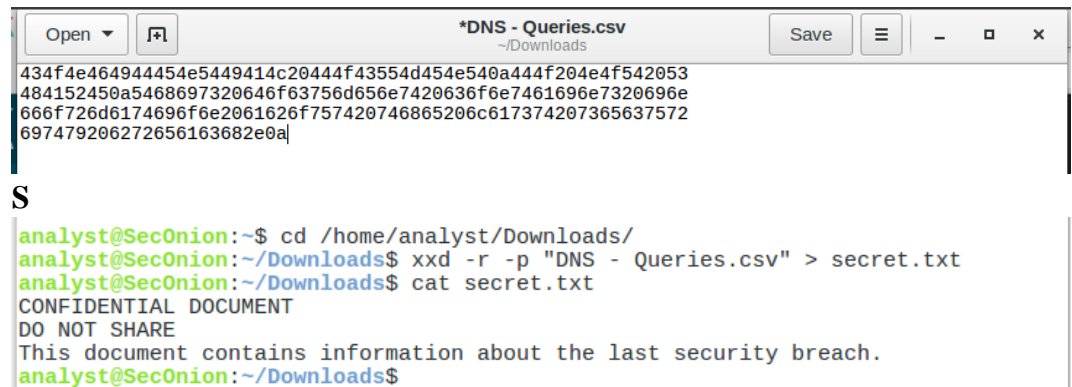
c. Tentukan data yang di ekstraksi

- S

- S



- S



The image shows a file editor window titled '*DNS - Queries.csv' with the path '~/Downloads'. The file contains three lines of hexadecimal data. Below the editor, a terminal window shows the following commands and output:

```
analyst@SecOnion:~$ cd /home/analyst/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$
```

- S

II. Pembahasan

III. Kesimpulan

Pada praktikum kali ini dapat disimpulkan bahwa :

- 1.

IV. Daftar Pustaka

Klopmart. (February 23, 2021). 2 Kegunaan Solder, Komponen Beserta Jenis-Jenisnya. Retrieved August 21, 2022, from <https://www.klopmart.com/article/detail/kegunaan-solder>