

LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1

PERTEMUAN 5

**(EKSTRAK EXECUTABLE DARI PCAP DAN MENAFSIRKAN DATA
HTTP DAN DNS UNTUK MENGISOLASI PELAKU ANCAMAN)**



DISUSUN OLEH

NAMA : ADITYA DARMASAPUTRA

NIM : 21/480255/SV/19599

KELAS : RI4AA

DOSEN : ANNI KARIMATUL FAUZIYYAH, S.Kom., M.Eng.

SARJANA TERAPAN TEKNOLOGI REKAYASA INTERNET

DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA

SEKOLAH VOKASI

UNIVERSITAS GADJAH MADA

YOGYAKARTA

2023

A. Tujuan

1. Investigasi SQL Injection Attack.
2. Analisis Pre-Captured Logs dan Traffic Captures.
3. Investigasi DNS Data Exfiltration.

B. Alat dan Bahan

1. Software steganografi
2. CyberOps Workstation virtual machine
3. Security Onion virtual machine
4. PC
5. Internet

C. Landasan Teori

Melihat log sangat penting, tetapi juga penting untuk memahami bagaimana transaksi jaringan terjadi pada tingkat paket. Di lab ini, Anda akan menganalisis lalu lintas dalam file pcap yang diambil sebelumnya dan mengekstrak file yang dapat dieksekusi dari file tersebut.

MySQL adalah database populer yang digunakan oleh banyak aplikasi web. Sayangnya, injeksi SQL adalah teknik peretasan web yang umum. Ini adalah teknik injeksi kode di mana penyerang mengeksekusi pernyataan SQL berbahaya untuk mengontrol server database aplikasi web.

Server nama domain (DNS) adalah direktori nama domain, dan mereka menerjemahkan nama domain menjadi alamat IP. Layanan ini dapat digunakan untuk mengekstrak data. Personel keamanan siber telah menentukan bahwa eksploitasi telah terjadi, dan data yang berisi PII mungkin telah diekspos ke pelaku ancaman. Di lab ini, Anda akan menggunakan Kibana untuk menyelidiki eksploitasi guna menentukan data yang dieksfiltrasi menggunakan HTTP dan DNS selama serangan.

Kibana adalah alat visualisasi dan eksplorasi data *open-source* yang digunakan untuk analisis log dan time-series, pemantauan aplikasi, dan kasus penggunaan intelijen operasional. Kibana menawarkan fitur yang kuat dan mudah digunakan seperti histogram, grafik garis, diagram lingkaran, dan dukungan geospasial built-in dan menyediakan integrasi ketat dengan Elasticsearch, analitik populer dan mesin pencari, yang membuat

Kibana menjadi pilihan default untuk memvisualisasikan data yang disimpan dalam Elasticsearch.

D. Data

Cyberops Workstation

1. Log in software cyberops workstation dan buka terminalnya. Ketik `cd lab.support.files/pcpas` untuk masuk ke direktorinya. Lalu ketik `ls -l` untuk menampilkan daftar files.

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

2. Ketik `wireshark nimda.download.pcap` untuk membuka wireshark nimda.

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

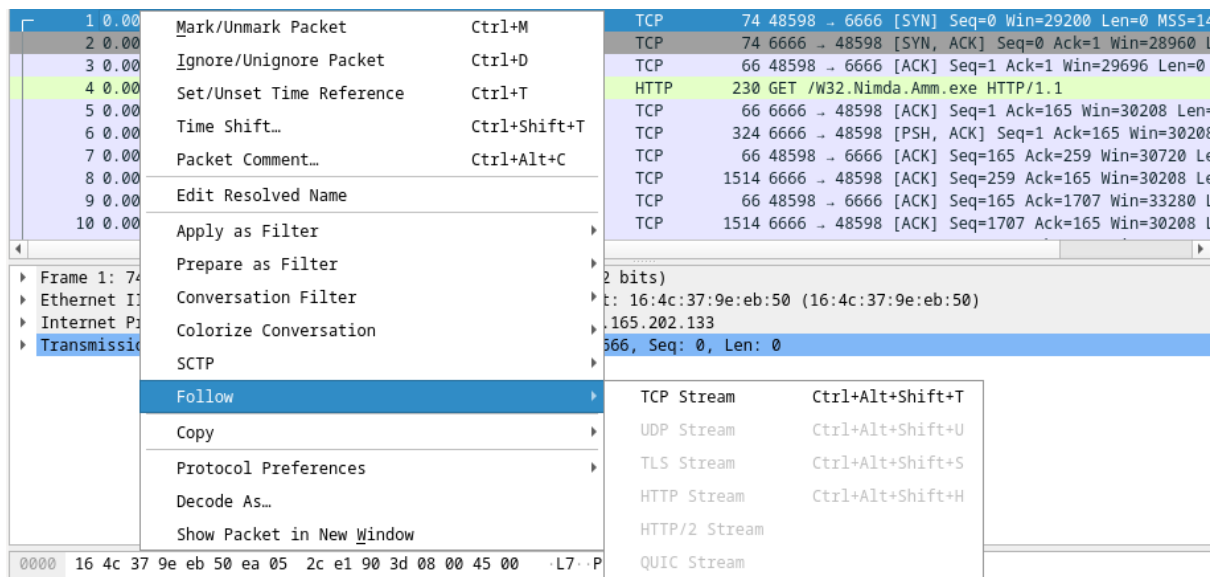
3. Masuk ke baris ke 4 pada wireshark dan klik **Hypertext Transfer Protocol**, maka akan terdapat kode di bawahnya.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	209.165.200.235	209.165.202.133	TCP	74	48598 → 6666 [SYN] Seq=0 Win=29200 Len=0 MSS=14
2	0.000259	209.165.202.133	209.165.200.235	TCP	74	6666 → 48598 [SYN, ACK] Seq=0 Ack=1 Win=28960 L
3	0.000297	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=1 Ack=1 Win=29696 Len=0
4	0.000565	209.165.200.235	209.165.202.133	HTTP	230	GET /w32.Nimda.Amm.exe HTTP/1.1
5	0.000588	209.165.202.133	209.165.200.235	TCP	66	6666 → 48598 [ACK] Seq=1 Ack=165 Win=30208 Len=
6	0.000708	209.165.202.133	209.165.200.235	TCP	324	6666 → 48598 [PSH, ACK] Seq=1 Ack=165 Win=30208
7	0.000827	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=259 Win=30720 Le
8	0.004594	209.165.202.133	209.165.200.235	TCP	1514	6666 → 48598 [ACK] Seq=259 Ack=165 Win=30208 Le
9	0.004602	209.165.200.235	209.165.202.133	TCP	66	48598 → 6666 [ACK] Seq=165 Ack=1707 Win=33280 L
10	0.004605	209.165.202.133	209.165.200.235	TCP	1514	6666 → 48598 [ACK] Seq=1707 Ack=165 Win=30208 L

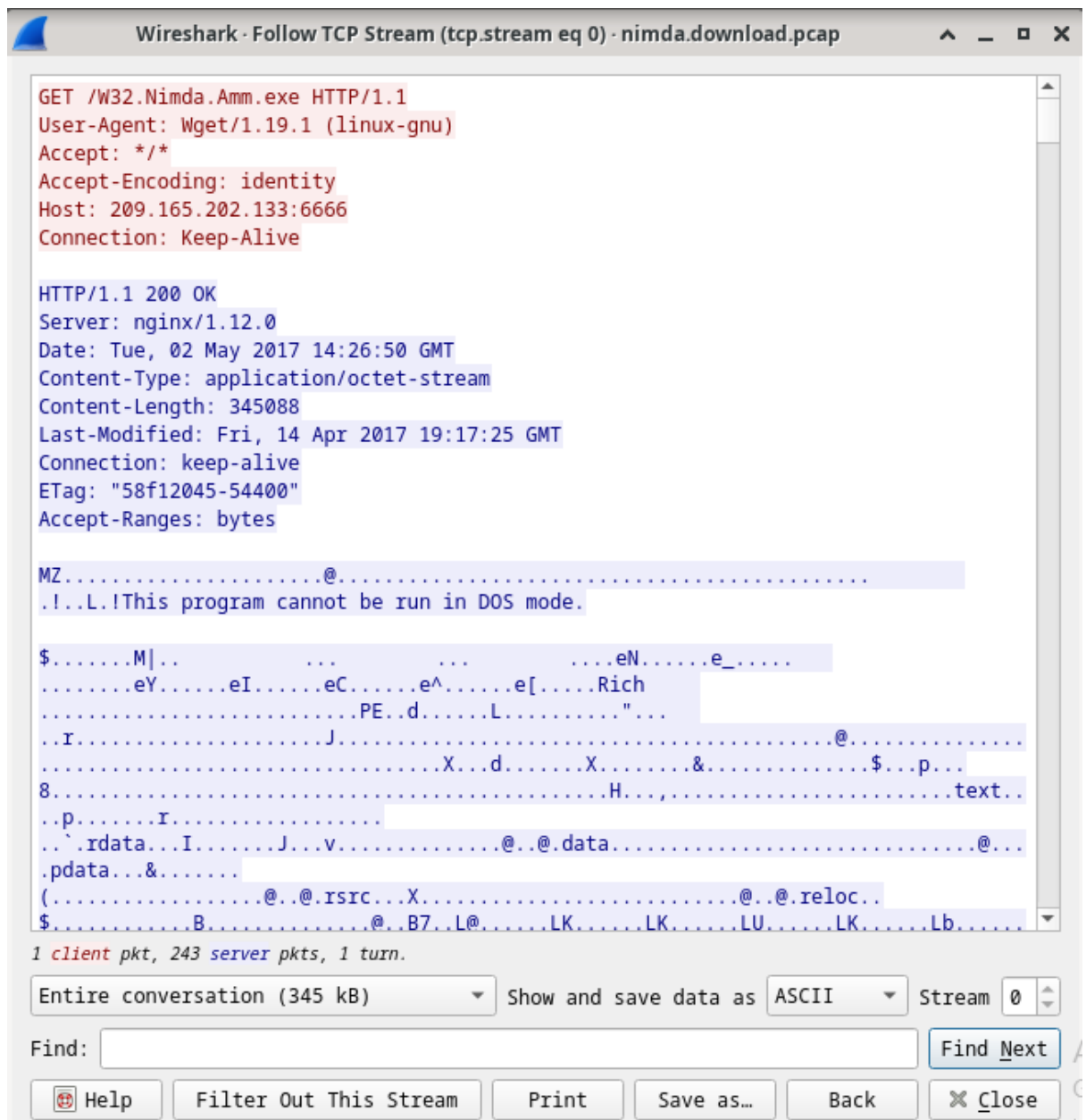
Frame 4: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits)
Ethernet II, Src: ea:05:2c:e1:90:3d (ea:05:2c:e1:90:3d), Dst: 16:4c:37:9e:eb:50 (16:4c:37:9e:eb:50)
Internet Protocol Version 4, Src: 209.165.200.235, Dst: 209.165.202.133
Transmission Control Protocol, Src Port: 48598, Dst Port: 6666, Seq: 1, Ack: 1, Len: 164
Hypertext Transfer Protocol

```
0040  e5 11 47 45 54 20 2f 57 33 32 2e 4e 69 6d 64 61  .GET /W 32.Nimda
0050  2e 41 6d 6d 2e 65 78 65 20 48 54 54 50 2f 31 2e  .Amm.exe HTTP/1.
0060  31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 57  1-User-Agent: W
0070  67 65 74 2f 31 2e 31 39 2e 31 20 28 6c 69 6e 75  get/1.19 .1 (linu
0080  78 2d 67 6e 75 29 0d 0a 41 63 63 65 70 74 3a 20  x-gnu)... Accept:
0090  2a 2f 2a 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f  */* Acc ept-Enco
```

4. Masuk ke baris 1 dan klik kanan baris tersebut, pilih **Follow** dan klik **TCP Stream**.



5. Akan muncul tampilan TCP stream yang dipilih.



Pertanyaan :

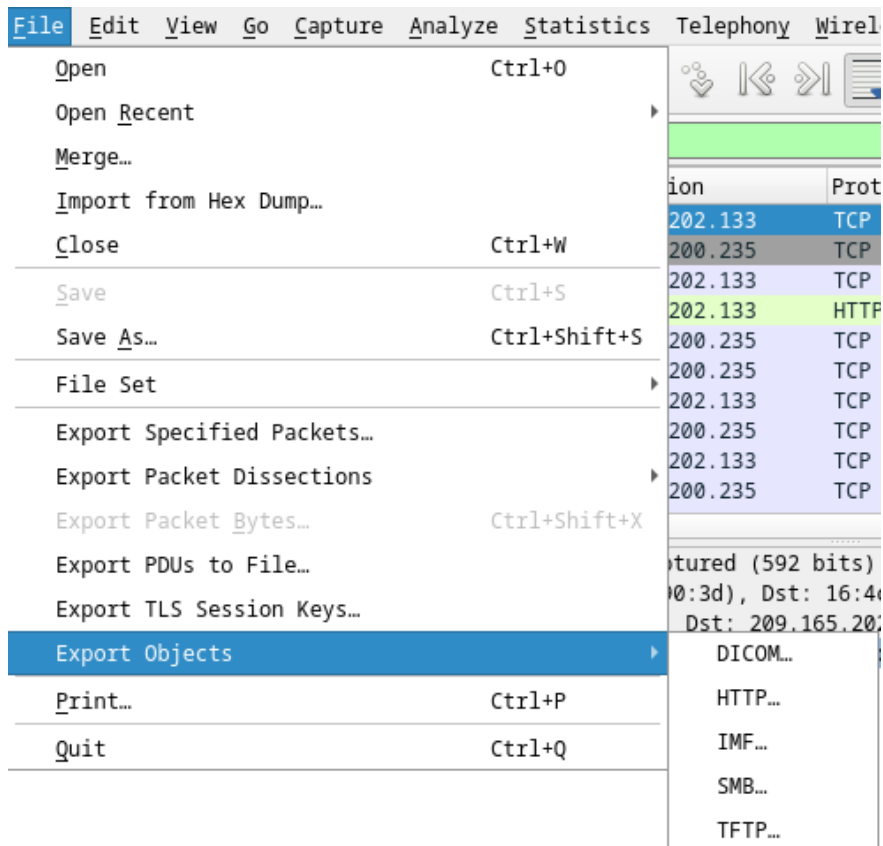
Apa semua simbol yang ditampilkan di jendela Ikuti TCP Stream? jelaskan.

Jawab :

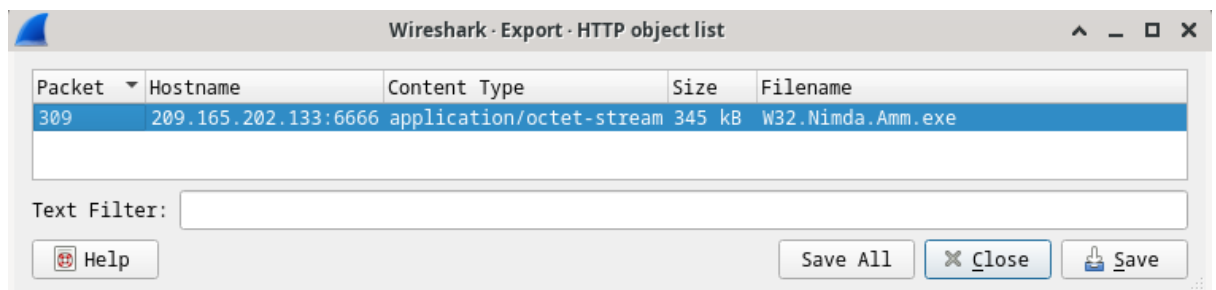
Menampilkan semua data yang dikirim dalam sebuah koneksi TCP tertentu, termasuk header dan payload.

- ‘.’ : Merupakan representasi dari karakter kosong (spasi), biasanya digunakan untuk mempermudah pembacaan data dalam format teks.

6. Buka menu **File > Export Objects > HTTP**.



7. Wireshark akan menampilkan file HTTP yang ada pada TCP stream.



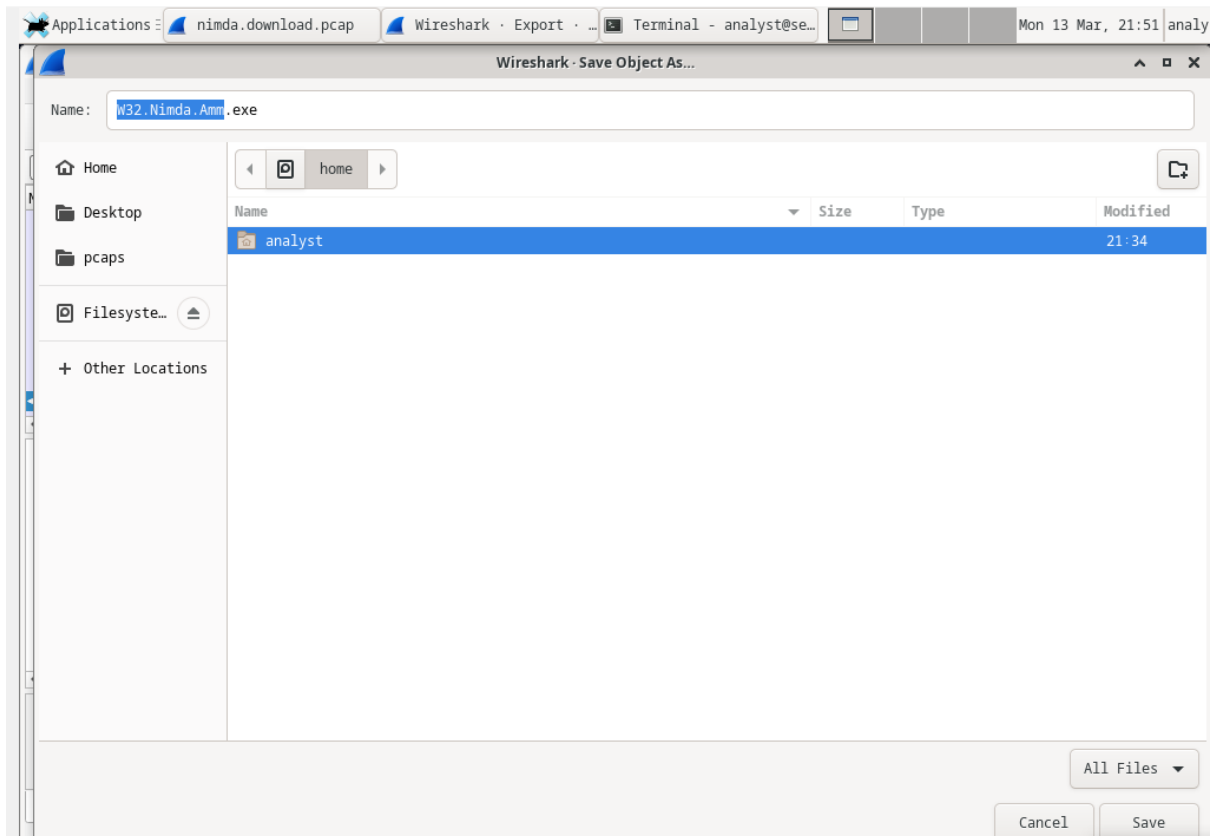
Pertanyaan :

Mengapa W32.Nimda.Amm.exe satu-satunya file yang di capture?

Jawab :

Karena masuk ke dalam TCP stream pada HTTP.

8. Setelah itu, simpan file W32 nimda pada direktori **home/analyst**, klik save.



9. Masuk kembali ke terminal dan ubah ke direktori analyst dengan mengetikkan **cd /home/analyst**. Ketik **ls -l** untuk melihat files pada direktori tersebut.

```
[analyst@secOps pcaps]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 396
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 31157 Mar 1 20:00 httpdump.pcap
-rw-r--r-- 1 root root 8192 Feb 20 21:06 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 21:52 W32.Nimda.Amm.exe
```

10. Ketik file **W32.Nimda.Amm.exe** untuk melihat informasi malware.

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

Security Onion

1. Log in security onion dan buka terminal. Ketik **cd /nsm/bro/logs/current**. Setelah itu, ketik **ls -l**.

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

2. Masuk ke direktori sensor_data dengan mengetikkan **cd /nsm/sensor_data** dan ketik **ls -l** untuk melihat file pada direktori tersebut. Ketik **ls -l seconion-eth0**.

```
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$ 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
```

3. Masuk ke direktori nsm dengan mengetikkan **cd /var/log/nsm** dan **ls**.

```
analyst@SecOnion:/nsm/sensor_data$ 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
```

4. Ketik **cd..** untuk balik ke direktori sebelum nsm dan ketik **ls**.


```

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

```

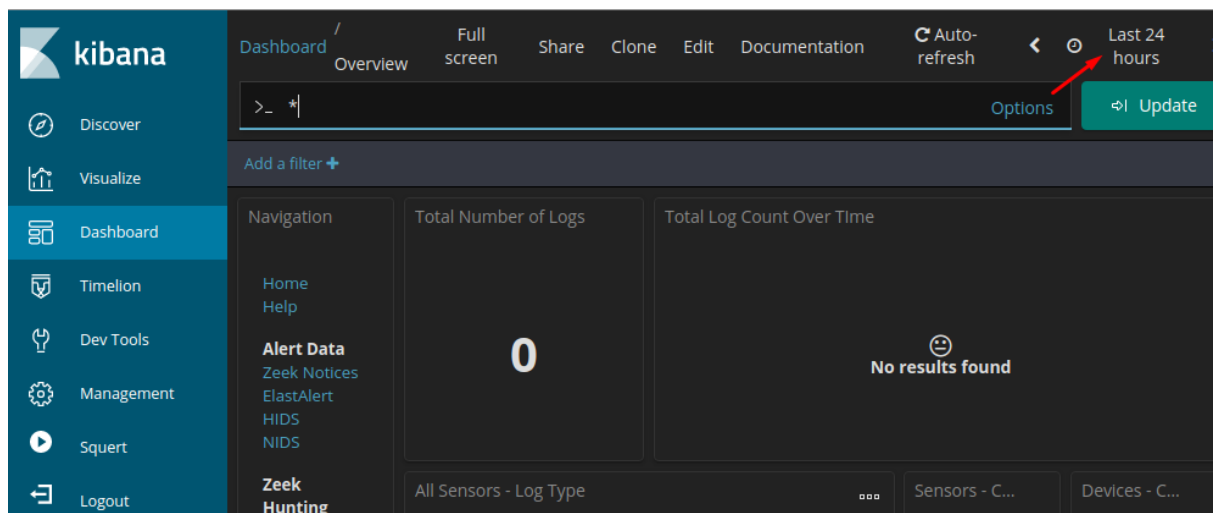
5. Ketik **sudo so-status** dan login menggunakan password cyberops.

```

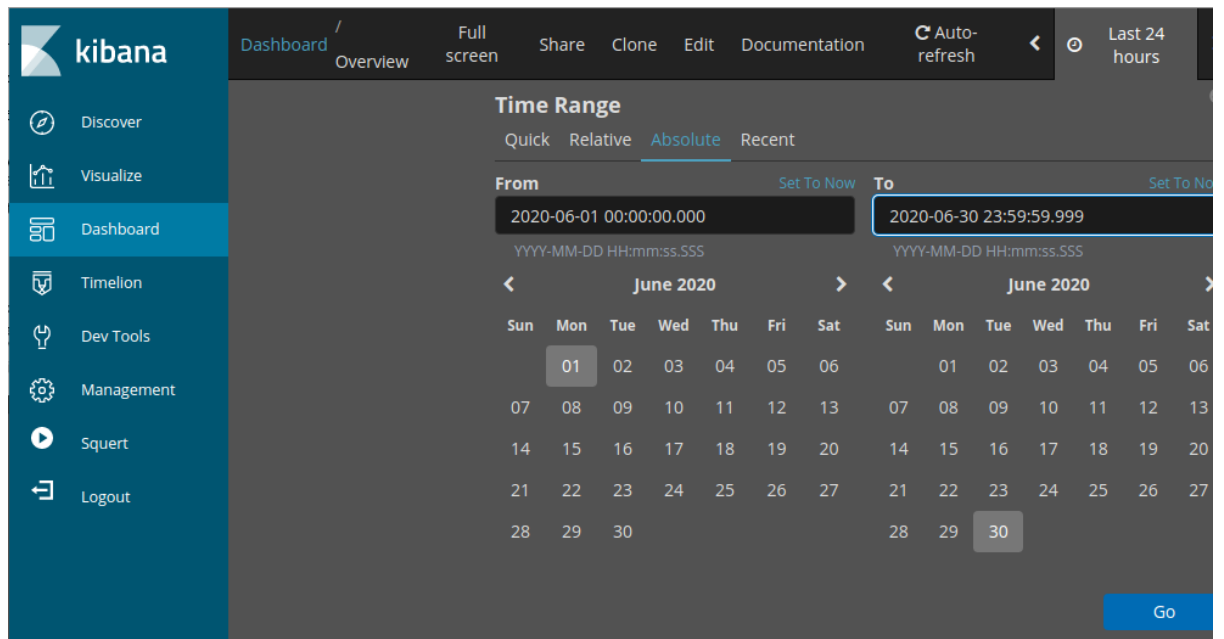
analyst@SecOnion:/var/log$ sudo so-status
[sudo] password for analyst:
Status: securityonion
* sguild server
Status: seconion-import
* pcap_agent (sguil)
* snort_agent-1 (sguil)
* barnyard2-1 (spooler, unified2 format)
Status: Elastic stack
* so-elasticsearch
* so-logstash
* so-kibana
* so-freqserver

```

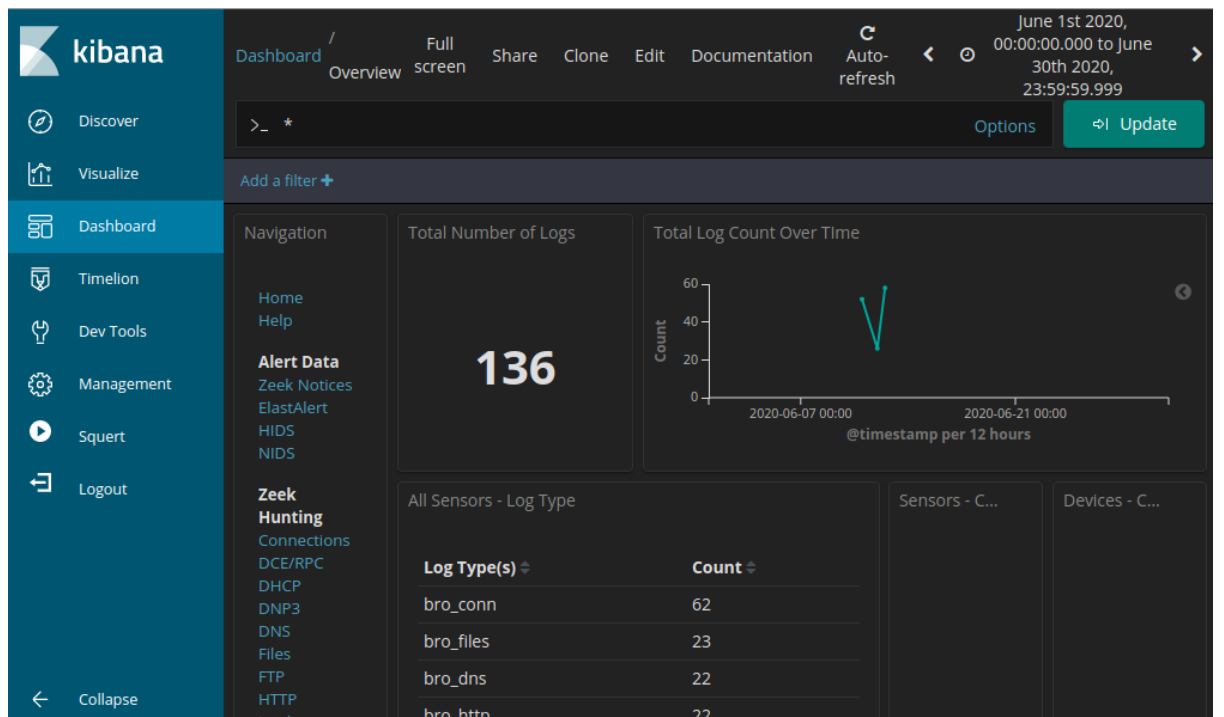
6. Pada desktop security onion, buka web kibana dan klik waktu yang ditunjukkan anak panah.



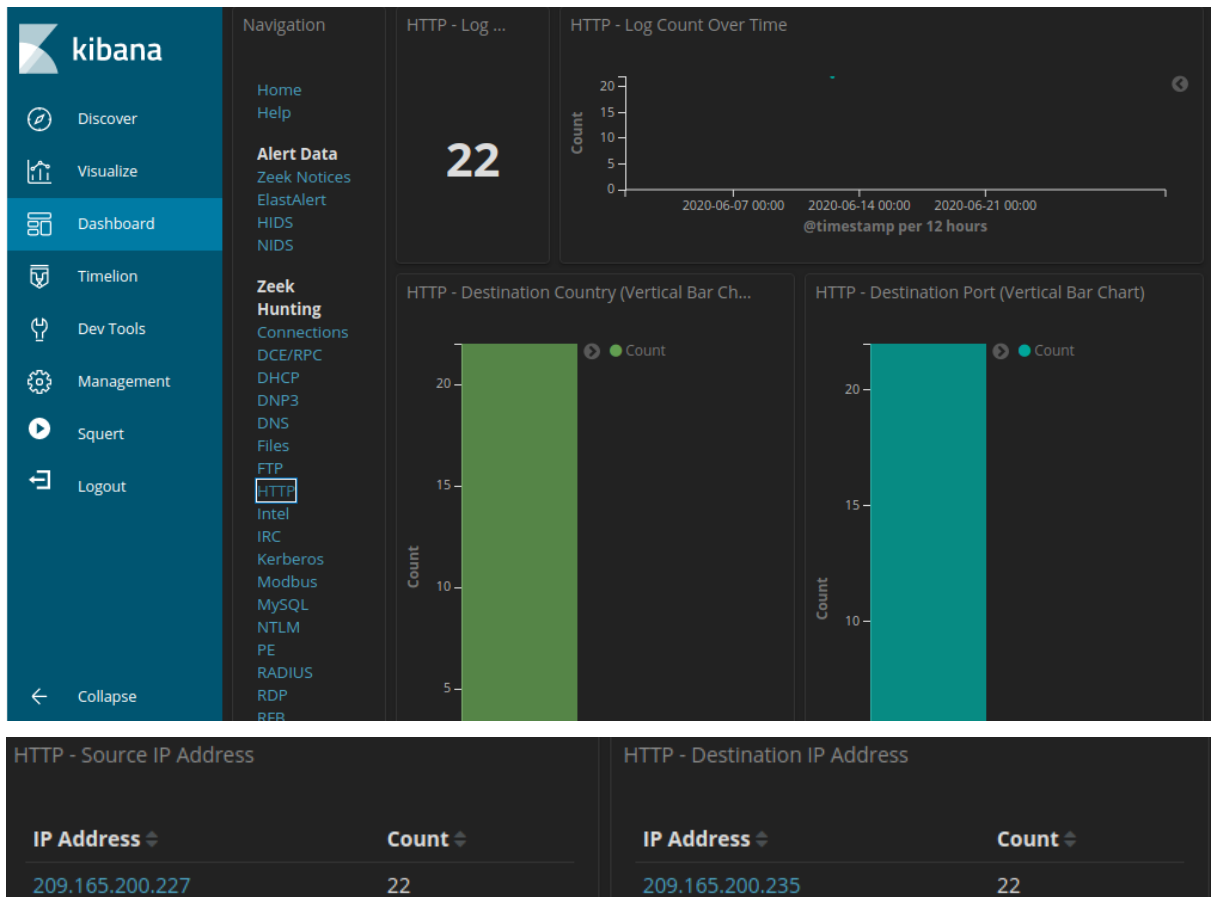
7. Atur waktu dari **from** ke **to** sesuai dengan gambar. Kita akan melihat satu bulan penuh pada bulan Juni tahun 2020.



8. Perhatikan total lognya.



9. Perhatikan pada bagian zeek hunting dan klik bagian HTTP.



Pertanyaan :

Apa alamat IP sumber?

Apa alamat IP tujuan?

Berapa nomor port tujuan?

Jawab :

- IP sumbernya adalah 209.165.200.227.
- IP tujuannya adalah 209.165.200.235.
- Nomor port tujuan adalah 80.

10. Scroll bagian paling bawah sehingga anda akan menemukan 10 log HTTP pertama. Jangan lupa klik panah baris paling atas sehingga akan menampilkan berbagai informasi.

Time ▾	source_ip	destination_ip	destination_port	resp_fuids	uid	
▶ June 12th 2020, 21:23:17.564	209.165.200.227	209.165.200.235	80	F8nPIA4w1BMn DDZ2A4	CW4Ta04 A319dbq kjWk	1 (t
▶ June 12th 2020, 21:23:17.689	209.165.200.227	209.165.200.235	80	FbzXZf35Pr7X0R 4Ne4	Cr3RGFez op5b3qJz 6	1 t 5
▶ June 12th 2020, 21:23:17.689	209.165.200.227	209.165.200.235	80	FFr52q1c7MxEP2 qhKc	CW4Ta04 A319dbq kjWk	1 t 5
▶ June 12th 2020, 21:23:17.690	209.165.200.227	209.165.200.235	80	FsYE4H1zukKoKs WwNc	COoObq 4g2QxfBf eR1J	1 t 5
▶ June 12th 2020, 21:23:17.691	209.165.200.227	209.165.200.235	80	FGPr363LFDTMU cwBR2	C2S2w31 zFlvpV63 kPa	1 t 5
▶ June 12th 2020, 21:23:17.691	209.165.200.227	209.165.200.235	80	FSe1Dl1uoGRJy7 yeHg	CbSK6C1 mlm2iUV KkC1	1 t t
▶ June 12th 2020, 21:23:17.692	209.165.200.227	209.165.200.235	80	F8NDop2CVNuTI f8Mud	C4KeAa3 pLgDqfa AQyg	1 t 5
▶ June 12th 2020, 21:23:17.698	209.165.200.227	209.165.200.235	80	F1sqnz4z0m9nW	C4KeAa3	1

@timestamp	June 12th 2020, 21:23:17.564
@version	1
_id	UjjrzXIBB6Cd-_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": -121.8406, "lat": 36.3699 }
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
host	d68c9360b6ae

```

t message {
  "ts": "2020-06-12T21:23:17.564555Z",
  "uid": "CW4Ta04A319dbqkjWk",
  "id": "209.165.200.227",
  "id.orig_p": 56178,
  "id.resp_h": "209.165.200.235",
  "resp_p": 80,
  "trans_depth": 1,
  "method": "GET",
  "host": "209.165.200.235",
  "mutillidae": "",
  "referrer": "http://209.165.200.235/",
  "version": "1.1",
  "ent": "Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0",
  "request_body_len": 0,
  "response_body_len": 24255,
  "status_code": 200,
  "s_msg": "OK",
  "tags": [],
  "resp_fuids": ["F8nPIA4w1BMnDDZ2A4"],
  "resp_mis": ["text/html"]}

```

Pertanyaan :

Apa timestamp dari hasil pertama?

Apa jenis event?

Apa yang termasuk dalam kolom pesan?

Apa pentingnya informasi ini?

Jawab :

- Menampilkan tanggal 12 Juni 2020 jam 21:23:17.564.
- Jenis event yang dimaksud adalah bro_http.
- Kolom pesan menampilkan id, jenis method, status, dan lain-lain.
- Informasi ini ditampilkan untuk mempermudah pencarian.

11. Klik kode pada _id di pojok kanan atas untuk membuka browser berisi capME.

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

	source_ip	destination_ip	destination_port	resp_fuids	uid	_id
2th 2020, 21:23:17.564	209.165.200.227	209.165.200.235	80	F8nPIA4w1BMnDDZ2A4	CW4Ta04A319dbqkjWk	UjrrzXIBB6Cd-0SD_iW

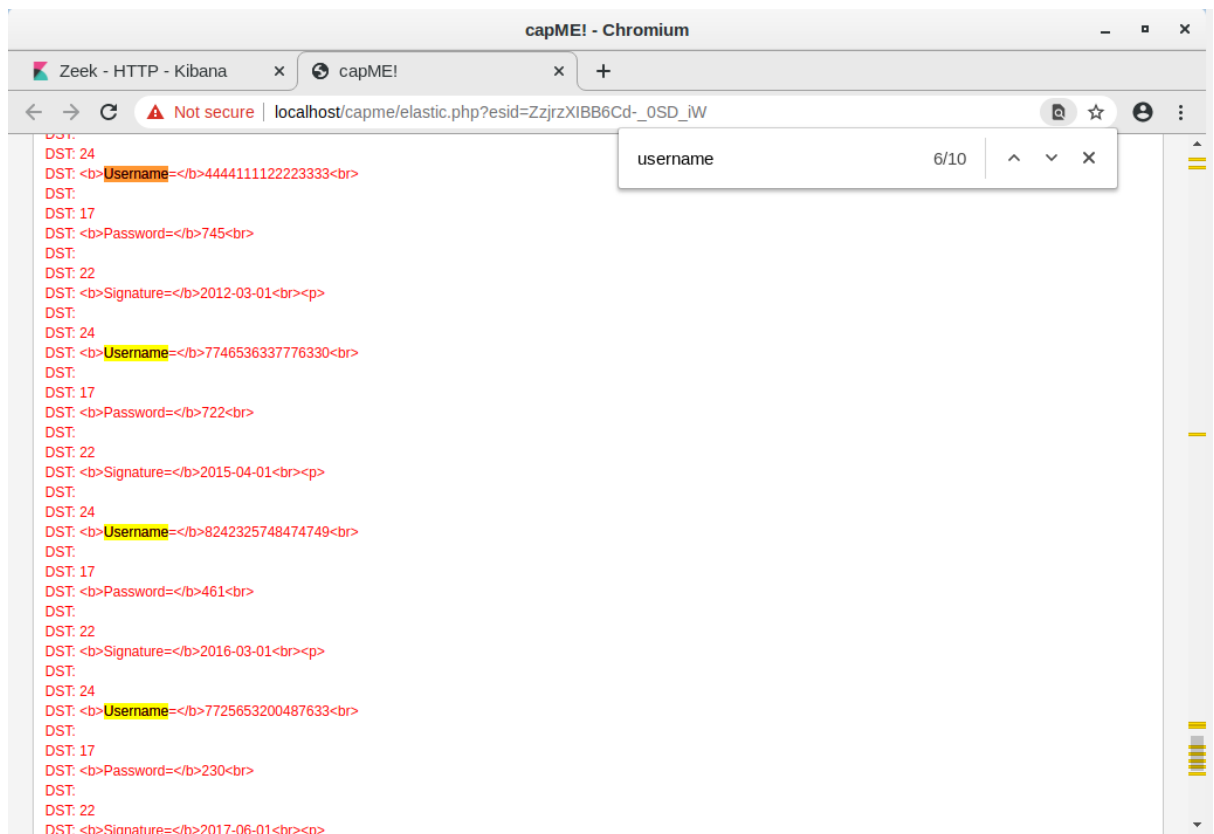
JSON [View surrounding documents](#) [View single document](#)

timestamp June 12th 2020, 21:23:17.564

id 1

UjrrzXIBB6Cd-0SD_iW

12. Buka bar pencarian dan ketik username untuk mengetahui nama pengguna.



Pertanyaan :

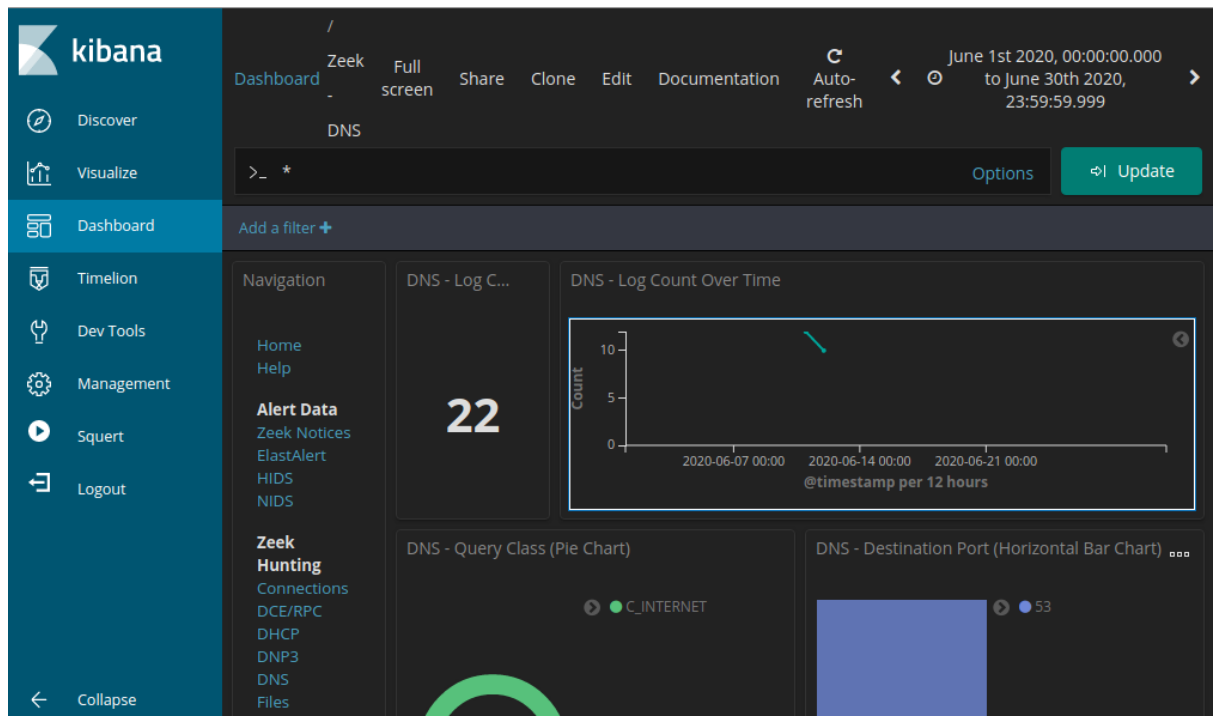
Apa yang Anda lihat nanti dalam transkrip tentang nama pengguna?

Berikan beberapa contoh username, password, dan signature yang telah diekstraksi.

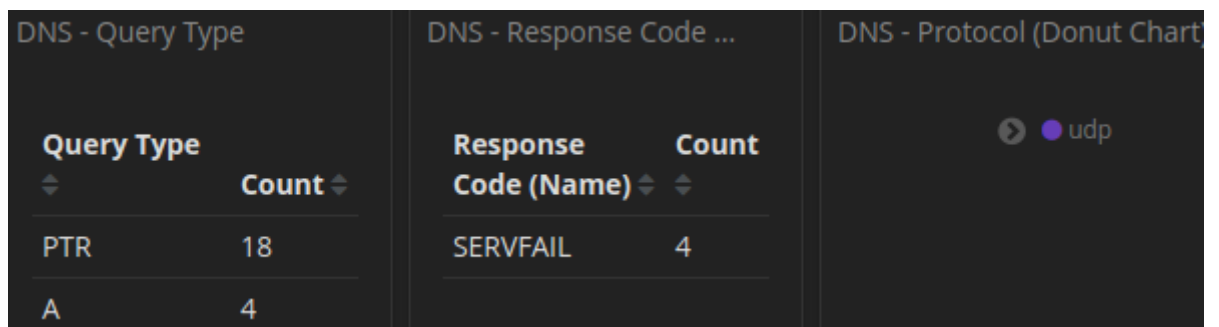
Jawab :

- Transkrip nilai nantinya dikonversi menjadi huruf yang dapat menampilkan nama pengguna.
- Saya belum sempat untuk mencobanya.

13. Pada dashboard, perhatikan zeek hunting dan klik bagian DNS. Perhatikan lognya.



14. Scroll kebawah dan temukan query type dan response code DNS.



15. Scroll kebawah dan temukan server-client DNS.

DNS - Client		DNS - Server		DNS - Phishing Attempts Against ...	
Client	Count	Server	Count		
209.165.200.235	18	8.8.4.4	6		
192.168.0.11	4	173.36.131.10	6		
		173.37.87.157	6		
		209.165.200.235	4		

16. Scroll bagian paling bawah dan temukan daftar query DNS berdasarkan domain.

Query
17.201.165.209.in-addr.arpa
434f4e464944454e5449414c20444f43554d454e540a444f:
484152450a5468697320646f63756d656e7420636f6e7461:
666f726d6174696f6e2061626f757420746865206c617374:
697479206272656163682e0a.ns.example.com

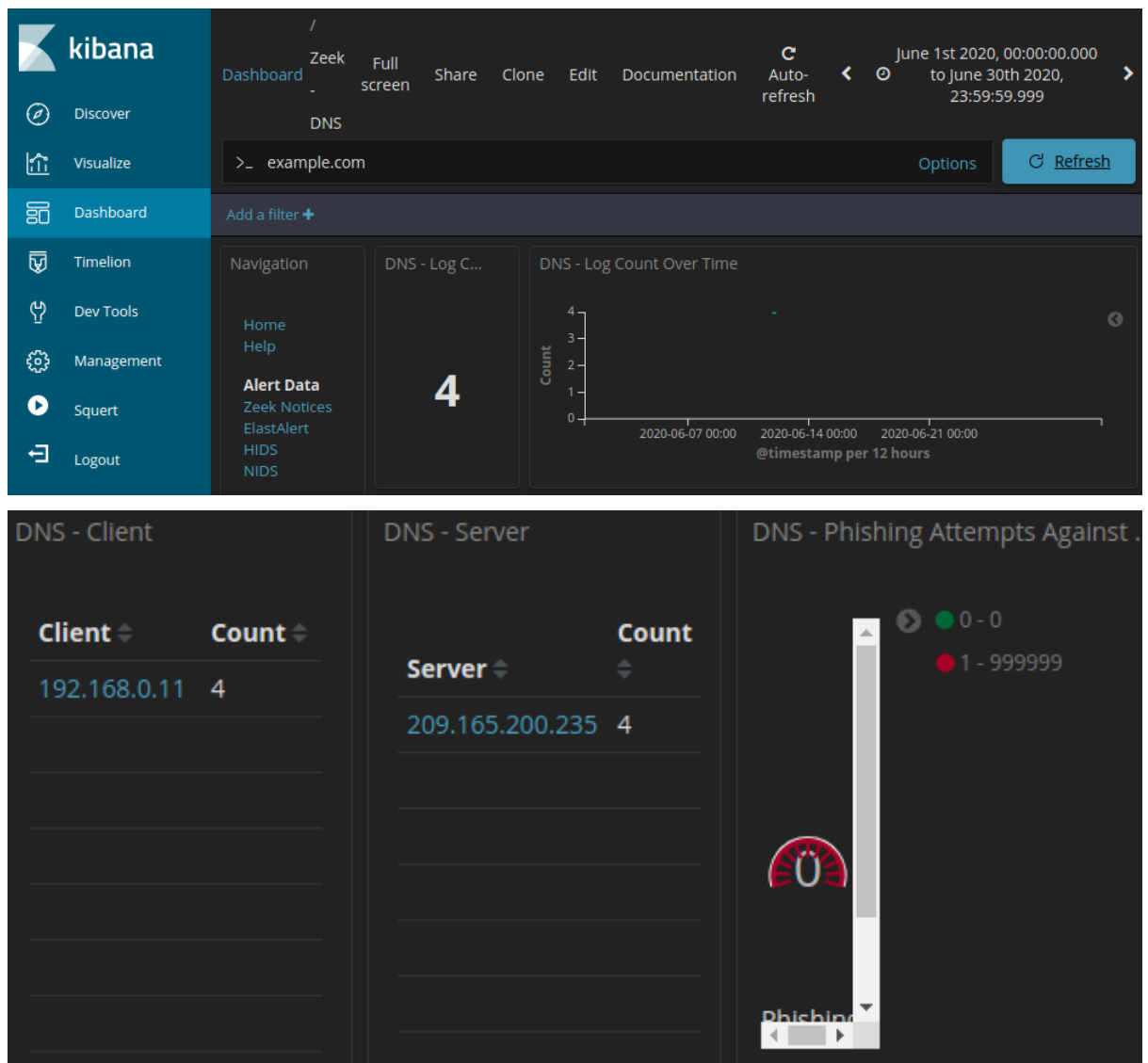
17. Scroll bagian paling atas pada bar pencarian dan ketikkan example.com Log akan memfilter server example.com. Klik update.

>_ example.com

Options

Update

18. Perhatikan log count pada server example.com. Scroll juga bagian bawahnya sehingga muncul server-client DNS.



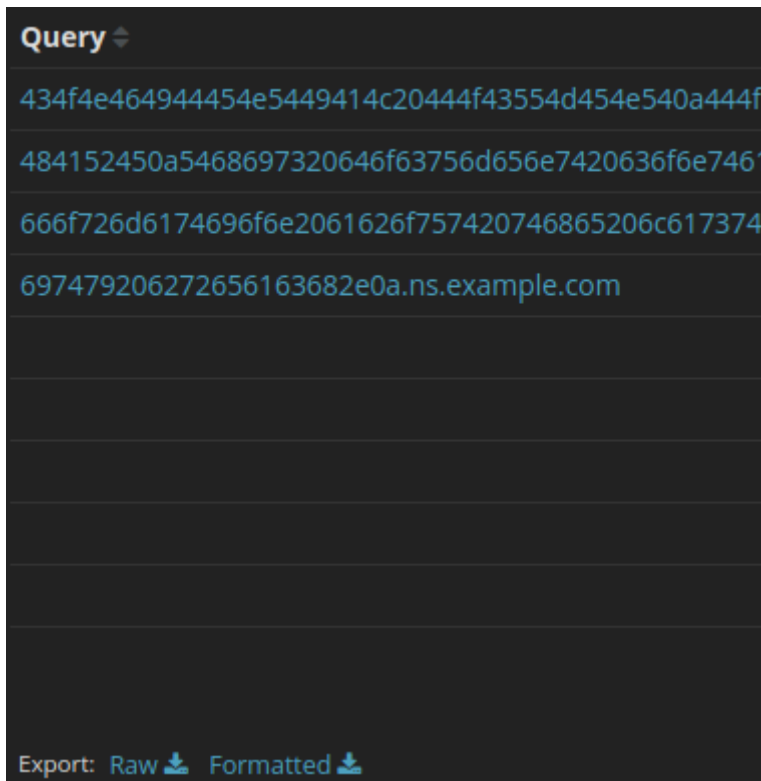
Pertanyaan :

Sebutkan alamat IP klien dan server DNS.

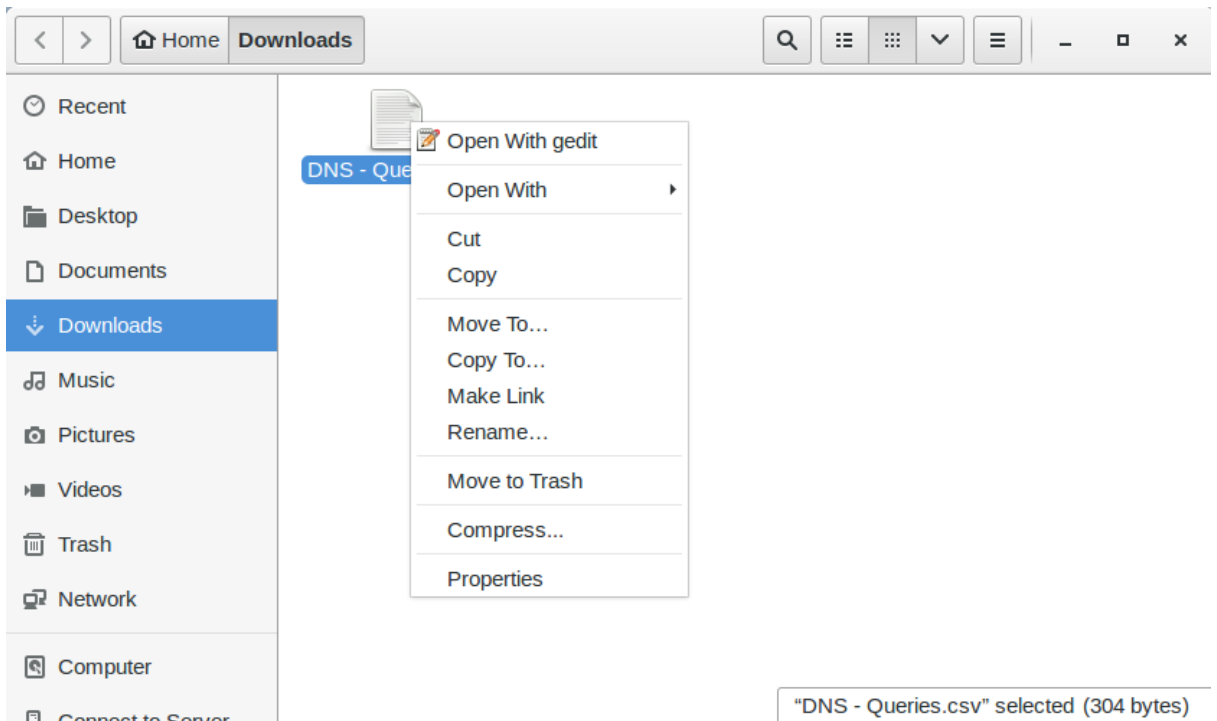
Jawab :

- IP kliennya adalah 192.168.0.11 dan IP servernya adalah 209.165.200.235.

19. Scroll ke bagian paling bawah dan download file CSV pada **Export : Formatted**.



20. Cari file CSV yang sudah di download dengan membuka home di desktop dan pilih bagian download, buka menggunakan gedit.



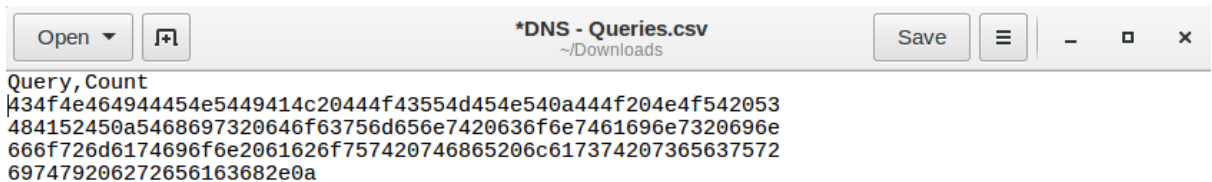
21. Edit teks dengan menghapus tanda petik dan bagian setelah teks hexadecimal.

Sebelum



```
Query, Count
"434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053|.ns.example.com",1
"484152450a5468697320646f63756d656e7420636f6e7461696e7320696e.ns.example.com",1
"666f726d6174696f6e2061626f757420746865206c617374207365637572.ns.example.com",1
"697479206272656163682e0a.ns.example.com",1
```

Sesudah



```
Query, Count
|434f4e464944454e5449414c20444f43554d454e540a444f204e4f542053
484152450a5468697320646f63756d656e7420636f6e7461696e7320696e
666f726d6174696f6e2061626f757420746865206c617374207365637572
697479206272656163682e0a
```

22. Terakhir, buka terminal dan masuk ke direktori downloads dengan mengetikkan **cd Downloads**. Lalu ketik **xxd -r -p "DNS - Queries.csv" > secret.txt**. Setelah itu, ketik **cat secret.txt** untuk menampilkan konten.

```
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.
```

E. Pembahasan

Pada praktikum kali ini diminta untuk menjalankan web kibana untuk menganalisis log dalam satu waktu.

Pada software cyberops workstation dijalankan untuk menganalisis malware dengan paket nimda dengan bantuan wireshark. Setelah file pcap dibuka, kita buka paket keempat pada wireshark dimana itu merupakan permintaan malware. Buka TCP stream untuk melihat data HTTP yang berada pada TCP stream. Data tersebut berisi encoding, host, tanggal, status koneksi, dan lain-lain. Setelah data di capture, kita akan ekstrak file dari pcap dengan membuka HTTP pada export object. File nimda ditampilkan karena hanya paket ini yang berisi permintaan GET pada TCP stream. Setelah dilihat pada terminal maka aplikasi nimda akan muncul. Kita juga bisa melihat jenis file dan versi nimda yang digunakan dengan perintah file.

Pada software security onion dijalankan untuk menganalisis serangan injeksi pada server menggunakan kibana. Pada tahap persiapan, kita akan melihat file log berdasarkan waktu yang sedang terjadi. Setelah mengetahui direktori log, lanjut untuk masuk ke tujuan utama. Perintah **sudo so-status** untuk memastikan semua layanan bekerja dengan baik. Lalu buka web kibana dan atur waktu untuk menampilkan serangan yang terjadi pada waktu itu.

Jumlah log yang muncul adalah 136. Kita akan memperkecil log yang akan dicari pada protokol HTTP pada zeek hunting. Saat kita scroll kebawah kita akan melihat IP sumber dan tujuan yang terbaca dengan menggunakan port 80. Kita bisa melihat data detail pada informasi 10 log teratas. Kita buka kode id untuk lebih memberikan informasi melalui web capME. Teks biru berisi request dan teks merah berisi response. Kita bisa menemukan user mana saja dan password yang digunakan untuk masuk pada daftar capME tersebut.

Setelah itu terdapat kejanggalan pada permintaan DNS pada zeek hunting. Terdapat 22 log dengan menuju ke port 53. Scroll kebawah dan anda akan menemukan IP server dan client yang diakses ke DNS. Pada upaya phishing memberikan nilai 0 dimana bernilai tidak adanya upaya phishing yang terjadi. Terdapat juga query type dan response code. Saat di scroll lagi kebawah terdapat daftar query yang Panjang dan banyak dengan domain example.com. Kita harus filter server example.com yang digunakan untuk mengetahui informasi tentang domain tersebut. Terdapat permintaan server dan client pada domain tersebut dengan total 4 log count. Kita download file CSV yang berisi teks berbentuk hexadesimal lalu kita analisis isi pesannya. Setelah file kita edit lalu kita simpan pada direktori analyst. Masuk kembali ke terminal dan ketikkan **xxd -r -p "DNS – Queries.csv"** > **secret.txt** untuk memecahkan kode yang sudah kita simpan tadi berdasarkan file yang ada pada query DNS. Ketik perintah cat untuk menampilkan isi pesan yang sudah kita crack/pecahkan.

F. Kesimpulan

Kibana digunakan untuk menganalisis file log dan dapat difilter berdasarkan waktu penyerangan, serta memberikan informasi tentang data penyerangan tersebut.

G. Daftar Pustaka

- *Mulai Gunakan Kibana dengan Google Cloud Platform Sekarang*. (2021, September 6). PointStar Indonesia. Retrieved March 20, 2023, from <https://www.pointstar.co.id/kibana/>
- Modul pertemuan 6_1 dan 7 Keamanan Informasi 1