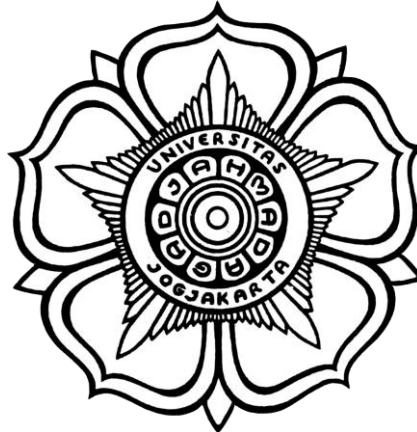


# **LAPORAN PRAKTIKUM KEAMANAN INFORMASI 1**

## **Pertemuan 5**

### **Ekstrak Executable dari PCAP dan Menafsirkan Data HTTP dan DNS untuk Mengisolasi Pelaku Ancaman**



Disusun Oleh :

Nama	:	Abu Alif Raharjo
NIM	:	21/479770/SV/19537
Hari, tanggal	:	Selasa, 14 Maret 2023
Dosen Pengampu	:	Anni Karimatul Fauziyyah, S. Kom., M. Eng.

**PROGRAM STUDI DIPLOMA IV TEKNOLOGI REKAYASA INTERNET**

**DEPARTEMEN TEKNIK ELEKTRO DAN INFORMATIKA**

**SEKOLAH VOKASI**

**UNIVERSITAS GADJAH MADA**

**2023**

## **A. Tujuan**

- Investigasi SQL Injection Attack
- Analisis Pre-Captured Logs dan Traffic Captures
- Investigasi DNS Data Exfiltration

## **B. Latar Belakang**

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.

Karena normalisasi file log itu penting, alat analisis log sering kali menyertakan fitur normalisasi log. Alat yang tidak menyertakan fitur tersebut sering mengandalkan plugin untuk normalisasi dan persiapan log. Tujuan dari plugin ini adalah untuk memungkinkan alat analisis log untuk menormalkan dan menyiapkan file log yang diterima untuk konsumsi alat. Alat Security Onion bergantung pada sejumlah alat untuk menyediakan layanan analisis log. ELK, Zeek, Snort dan SGUIL bisa dibilang alat yang paling banyak digunakan. ELK (Elasticsearch, Logstash, dan Kibana) adalah solusi untuk mencapai hal berikut:

- Menormalkan, menyimpan, dan mengindeks log dengan volume dan tarif tak terbatas.
- Menyediakan antarmuka pencarian dan API yang sederhana dan bersih.
- Menyediakan infrastruktur untuk mengingatkan, melaporkan, dan berbagi log.
- Sistem plugin untuk mengambil tindakan dengan log.
- Ada sebagai proyek sumber terbuka dan gratis sepenuhnya.

Zeek (sebelumnya disebut Bro) adalah kerangka kerja yang dirancang untuk menganalisis lalu lintas jaringan secara pasif dan menghasilkan log peristiwa berdasarkan itu. Setelah analisis lalu lintas jaringan, Zeek membuat log yang menjelaskan peristiwa seperti berikut: •

- Koneksi jaringan TCP/UDP/ICMP
- Aktivitas DNS
- Aktivitas FTP
- Permintaan dan balasan HTTPS
- Jabat tangan SSL/TLS

Snort dan SGUIL Snort adalah IDS yang bergantung pada aturan yang telah ditentukan sebelumnya untuk semua kejadian yang berbahaya. Snort melihat ke semua bagian dari paket jaringan (header dan payload), mencari pola yang ditentukan dalam aturannya. Saat, Snort mengambil tindakan yang ditentukan dalam aturan yang sama. SGUIL menyediakan antarmuka grafis untuk log dan peringatan Snort, memungkinkan analisis keamanan untuk beralih dari SGUIL ke

alat lain untuk informasi lebih lanjut. Misalnya, jika paket yang berpotensi berbahaya dikirim ke server web dan Snort memunculkan peringatan, SGUIL akan peringatan itu. Analis kemudian dapat mengklik kanan peringatan itu untuk mencari database ELSA atau Bro untuk pemahaman yang lebih baik tentang acara tersebut.

### C. Alat dan Bahan

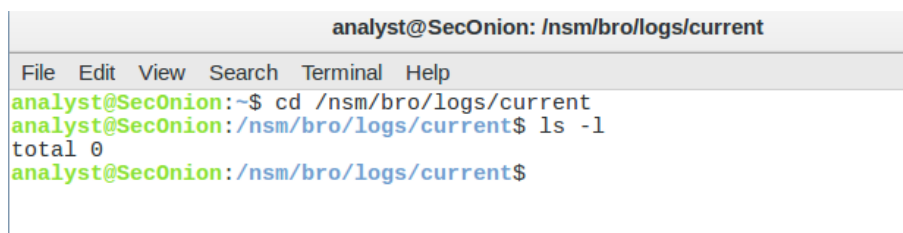
- PC dengan akses internet
- Aplikasi virtual CyberOps Workstation

### D. Instruksi Kerja

#### Persiapan Log File pada Security Onion Virtual Machine

1. Buka jendela terminal di Security Onion VM. Klik kanan Desktop. Di menu pop-up, pilih Buka Terminal.
2. Log Zeek disimpan di /nsm/bro/logs/. Seperti biasa dengan sistem Linux, file log diputar berdasarkan tanggal, diganti namanya dan disimpan di disk. File log saat ini dapat ditemukan di bawah direktori saat ini. Dari jendela terminal, ubah direktori menggunakan perintah berikut.

```
analyst@SecOnion:~$ cd /nsm/bro/logs/current
analyst@SecOnion:/nsm/logs/current$
```



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

Gunakan perintah ls -l untuk melihat file log yang dihasilkan oleh Zeek

3. Log snort dapat ditemukan di /nsm/sensor\_data/. Ubah direktori sebagai berikut.

```
analyst@SecOnion:/nsm/bro/logs/current$ cd /nsm/sensor_data
analyst@SecOnion:/nsm/sensor_data$
```

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

4. Gunakan perintah ls -l untuk melihat semua file log yang dihasilkan oleh Snort

```
analyst@SecOnion:/nsm/sensor_data$ ls -l
```

```
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
```

- Perhatikan bahwa Security Onion memisahkan file berdasarkan antarmuka. Karena image Security Onion VM memiliki dua antarmuka yang dikonfigurasi sebagai sensor dan folder khusus untuk data yang diimpor, tiga direktori disimpan. Gunakan perintah `ls -l seconion-eth0` untuk melihat file yang dihasilkan oleh antarmuka eth0.

```
analyst@SecOnion:/nsm/sensor_data$ ls -l seconion-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$
```

- Sementara direktori `/nsm/` menyimpan beberapa file log, file log yang lebih spesifik dapat ditemukan di bawah `/var/log/nsm/`. Ubah direktori dan gunakan perintah `ls` untuk melihat semua file log di direktori.

```
analyst@SecOnion:/nsm/sensor_data$ cd /var/log/nsm/
analyst@SecOnion:/var/log/nsm$ 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             so-setup.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$
```

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

```
analyst@SecOnion:/var/log/nsm$ cd ..
analyst@SecOnion:/var/log$ ls
```

```

sensor-clean.log.7.gz
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          sguil
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
boot.log             elasticsearch    mail.warn         user.log.1
bootstrap.log        error            messages          user.log.2.gz
btmtp                error.1          messages.1        user.log.3.gz
btmtp.1              error.2.gz       messages.2.gz     user.log.4.gz
cron.log             error.3.gz       messages.3.gz     wtmp
cron.log.1           error.4.gz       messages.4.gz     wtmp.1
cron.log.2.gz        faillog          mysql             Xorg.0.log
cron.log.3.gz        freq_server      nsm               Xorg.0.log.old
cron.log.4.gz        freq_server_dns ntpstats          Xorg.1.log
curator              fsck             redis
daemon.log           fsck             salt
analyst@SecOnion:/var/log$

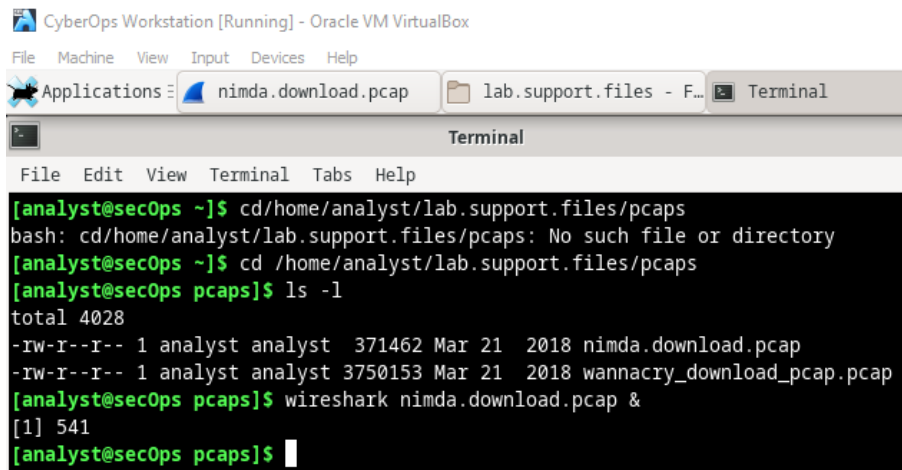
```

## Menganalisis Log yang Ditangkap sebelumnya dan Pengambilan Lalu Lintas

1. Ubah direktori ke folder lab.support.files/pcaps, dan dapatkan daftar file menggunakan perintah `ls -l`.

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

```
[analyst@secOps pcaps]$ ls -l
```



```

CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications: nimda.download.pcap lab.support.files - F... Terminal
Terminal
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ cd/home/analyst/lab.support.files/pcaps
bash: cd/home/analyst/lab.support.files/pcaps: No such file or directory
[analyst@secOps ~]$ cd /home/analyst/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]$ wireshark nimda.download.pcap &
[1] 541
[analyst@secOps pcaps]$

```

2. Keluarkan perintah di bawah ini untuk membuka file nimda.download.pcap di Wireshark.

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

```

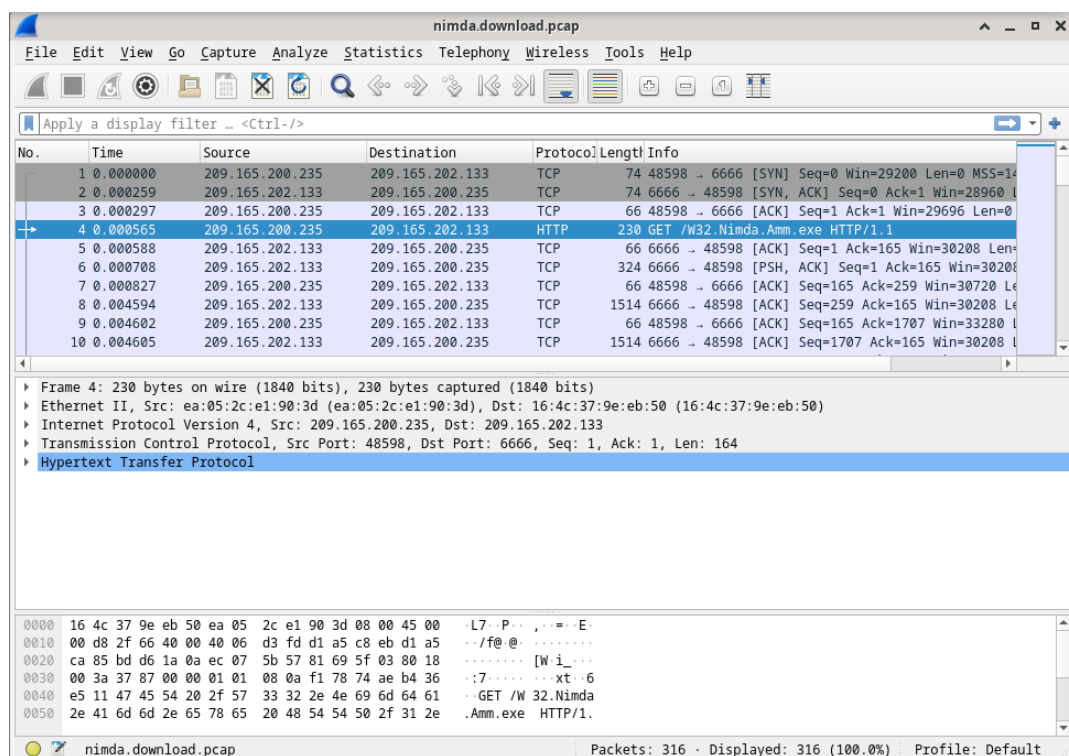
CyberOps Workstation [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications: nimda.download.pcap lab.support.files - F... Terminal

Terminal
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ cd/home/analyst/lab.support.files/pcaps
bash: cd/home/analyst/lab.support.files/pcaps: No such file or directory
[analyst@secOps ~]$ cd /home/analyst/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]$ wireshark nimda.download.pcap &
[1] 541
[analyst@secOps pcaps]$

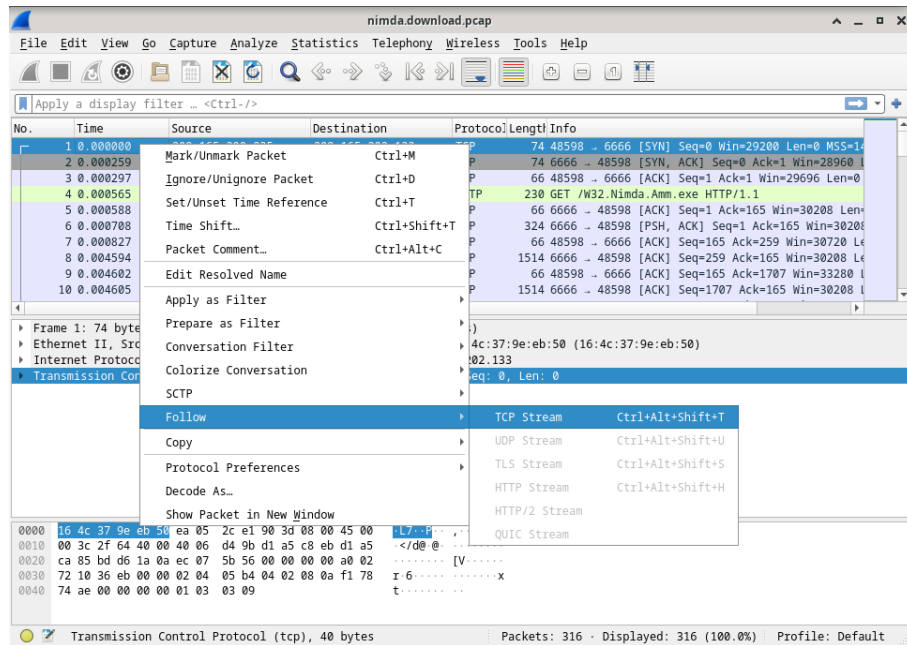
```

- File nimda.download.pcap berisi pengambilan paket yang terkait dengan unduhan malware yang dilakukan di lab sebelumnya. Pcap berisi semua paket yang dikirim dan diterima saat tcpdump sedang berjalan. Pilih paket keempat dalam tangkapan dan perluas Protokol Transfer Hypertext untuk ditampilkan seperti yang ditunjukkan di bawah ini.

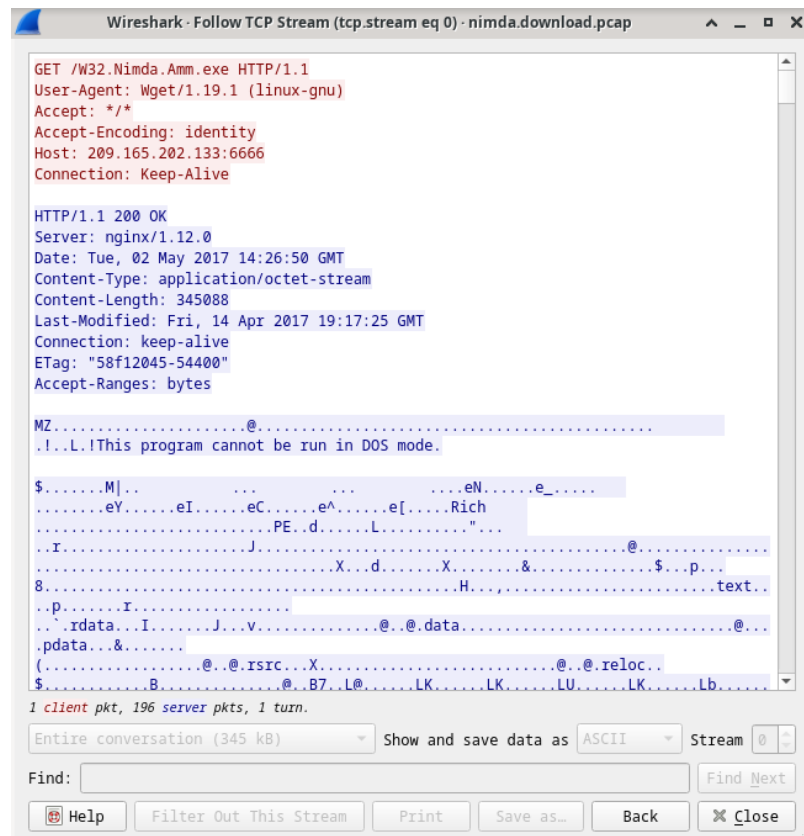


- Paket satu sampai tiga adalah jabat tangan TCP. Paket keempat menunjukkan permintaan file malware. Mengonfirmasi apa yang sudah diketahui, permintaan dilakukan melalui HTTP, dikirim sebagai permintaan GET.
- Karena HTTP berjalan di atas TCP, dimungkinkan untuk menggunakan fitur Follow TCP Stream Wireshark untuk membangun kembali transaksi

TCP. Pilih paket TCP pertama yang di capture, paket SYN. Klik kanan dan pilih Ikuti > TCP Stream.

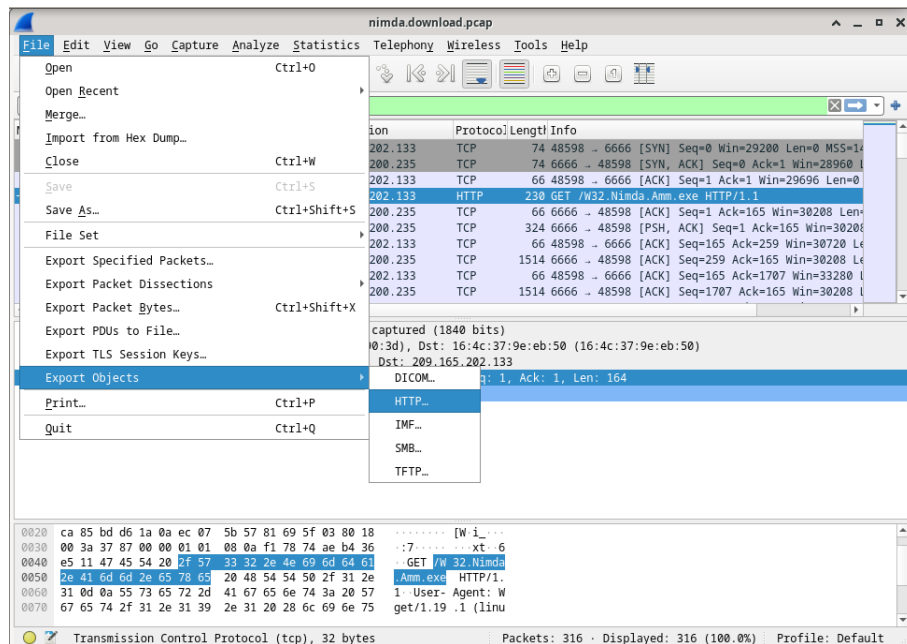


- Wireshark menampilkan jendela lain yang berisi detail untuk seluruh aliran TCP yang dipilih.

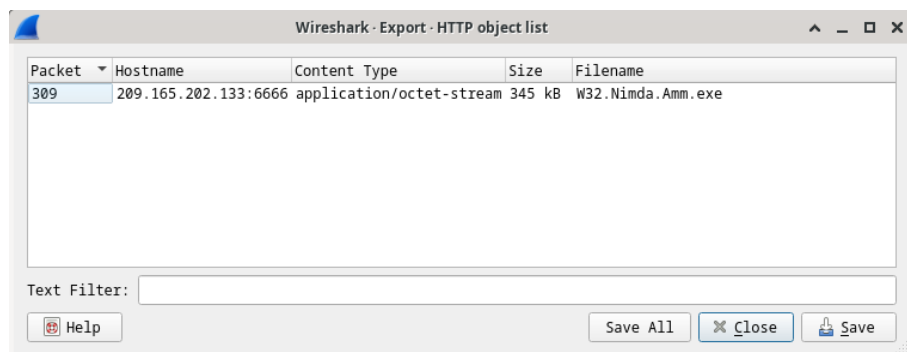


## Part 2: Extract Files yang di unduh dari PCAP

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



3. Wireshark akan menampilkan semua objek HTTP yang ada dalam aliran TCP yang berisi permintaan GET. Dalam hal ini, hanya file W32.Nimda.Amm.exe yang ada dalam pengambilan. Ini akan memakan waktu beberapa detik sebelum file ditampilkan.



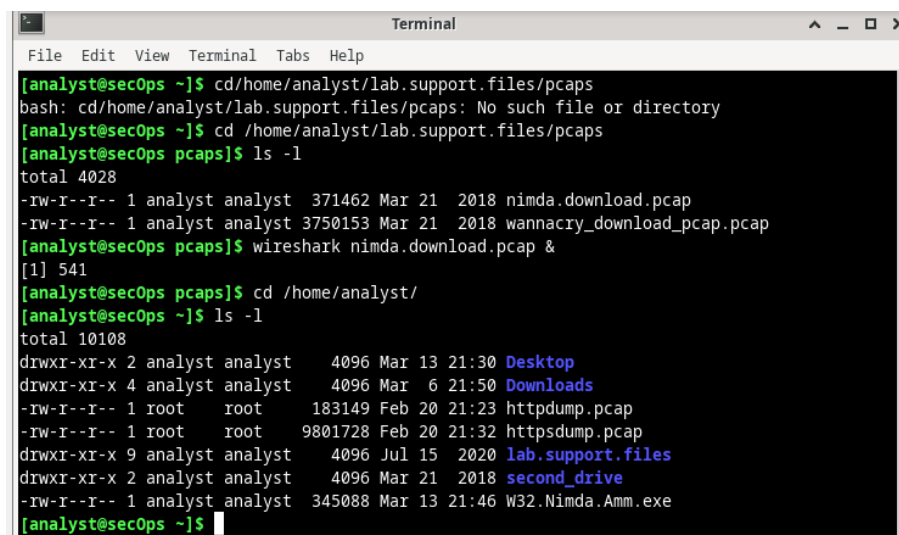
4. Di jendela daftar objek HTTP, pilih file W32.Nimda.Amm.exe dan klik Simpan Sebagai di bagian bawah layar.
5. Klik panah kiri hingga Anda melihat tombol Beranda. Klik Beranda lalu klik folder analisis (bukan tab analisis). Simpan file di sana.



6. Kembali ke jendela terminal Anda dan 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
```



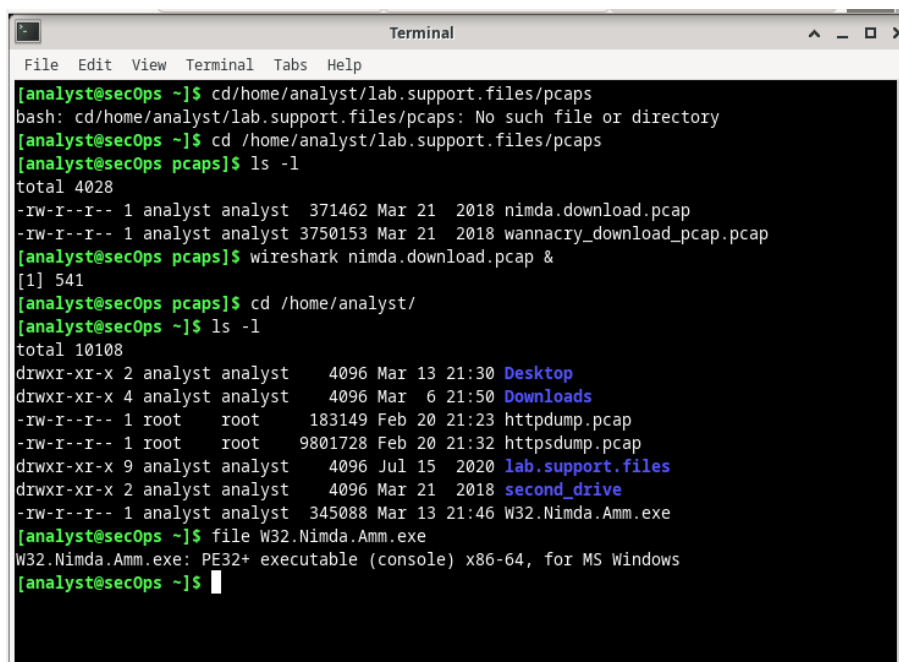
```
Terminal
File Edit View Terminal Tabs Help

[analyst@secOps ~]$ cd/home/analyst/lab.support.files/pcaps
bash: cd/home/analyst/lab.support.files/pcaps: No such file or directory
[analyst@secOps ~]$ cd /home/analyst/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]$ wireshark nimda.download.pcap &
[1] 541
[analyst@secOps pcaps]$ cd /home/analyst/
[analyst@secOps ~]$ ls -l
total 10108
drwxr-xr-x 2 analyst analyst 4096 Mar 13 21:30 Desktop
drwxr-xr-x 4 analyst analyst 4096 Mar 6 21:50 Downloads
-rw-r--r-- 1 root root 183149 Feb 20 21:23 httpdump.pcap
-rw-r--r-- 1 root root 9801728 Feb 20 21:32 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 21:46 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

7. Perintah file memberikan informasi tentang jenis file. Gunakan perintah file untuk mempelajari lebih lanjut tentang malware, seperti yang ditunjukkan di bawah ini:

```
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
```

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



```
Terminal
File Edit View Terminal Tabs Help

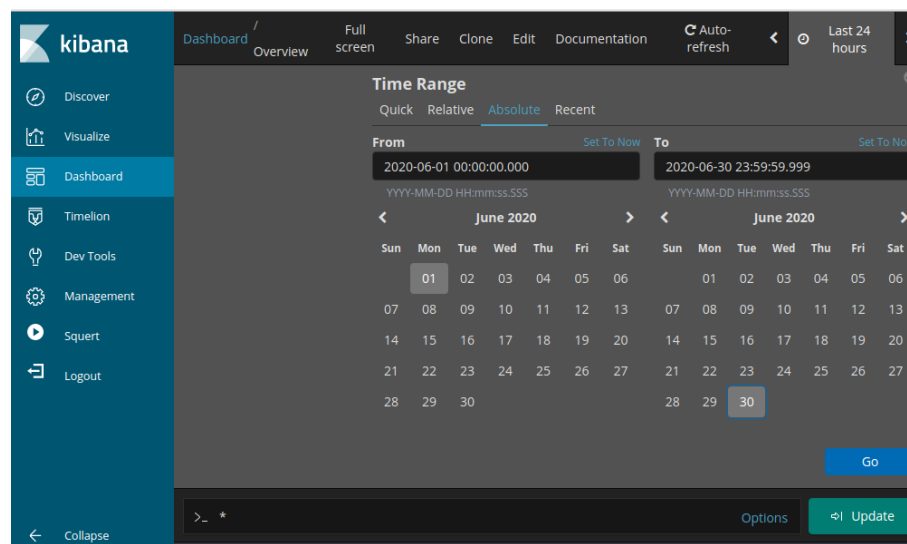
[analyst@secOps ~]$ cd/home/analyst/lab.support.files/pcaps
bash: cd/home/analyst/lab.support.files/pcaps: No such file or directory
[analyst@secOps ~]$ cd /home/analyst/lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download_pcap.pcap
[analyst@secOps pcaps]$ wireshark nimda.download.pcap &
[1] 541
[analyst@secOps pcaps]$ cd /home/analyst/
[analyst@secOps ~]$ ls -l
total 10108
drwxr-xr-x 2 analyst analyst 4096 Mar 13 21:30 Desktop
drwxr-xr-x 4 analyst analyst 4096 Mar 6 21:50 Downloads
-rw-r--r-- 1 root root 183149 Feb 20 21:23 httpdump.pcap
-rw-r--r-- 1 root root 9801728 Feb 20 21:32 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 21:46 W32.Nimda.Amm.exe
[analyst@secOps ~]$ file W32.Nimda.Amm.exe
W32.Nimda.Amm.exe: PE32+ executable (console) x86-64, for MS Windows
[analyst@secOps ~]$
```

## Investigasi SQL Injection Attack

1. Mulai Security Onion VM dan masuk dengan username analyst and the password cyberops.
2. Masukkan perintah `sudo so-status` untuk memeriksa status layanan. Status untuk semua layanan harus OK sebelum memulai analisis . Ini bisa memakan waktu beberapa menit.

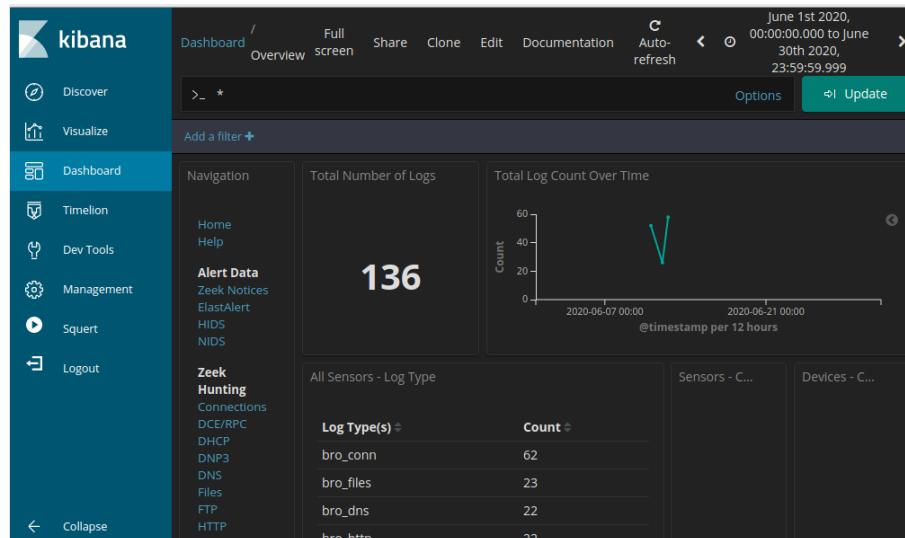
```
analyst@SecOnion: ~  
File Edit View Search Terminal Help  
analyst@SecOnion:~$ sudo so-status  
[sudo] password for analyst:  
Status: securityonion  
* sgul server [ OK ]  
Status: seconion-import  
* pcap_agent (sgul) [ OK ]  
* snort_agent-1 (sgul) [ OK ]  
* barnyard2-1 (spooler, unified2 format)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

3. Setelah Anda masuk, buka Kibana menggunakan pintasan di Desktop. Masuk dengan username analyst dan password cyberops.
4. Di sudut kanan atas jendela, klik 24 jam terakhir untuk mengubah ukuran Rentang Waktu sampel. Perluas rentang waktu untuk menyertakan peringatan yang menarik. Serangan injeksi SQL terjadi pada Juni 2020 jadi itulah yang perlu Anda targetkan. Pilih Absolute di bawah Rentang Waktu dan edit waktu Dari dan Ke untuk memasukkan seluruh bulan Juni di 2020. Klik Pergi untuk melanjutkan

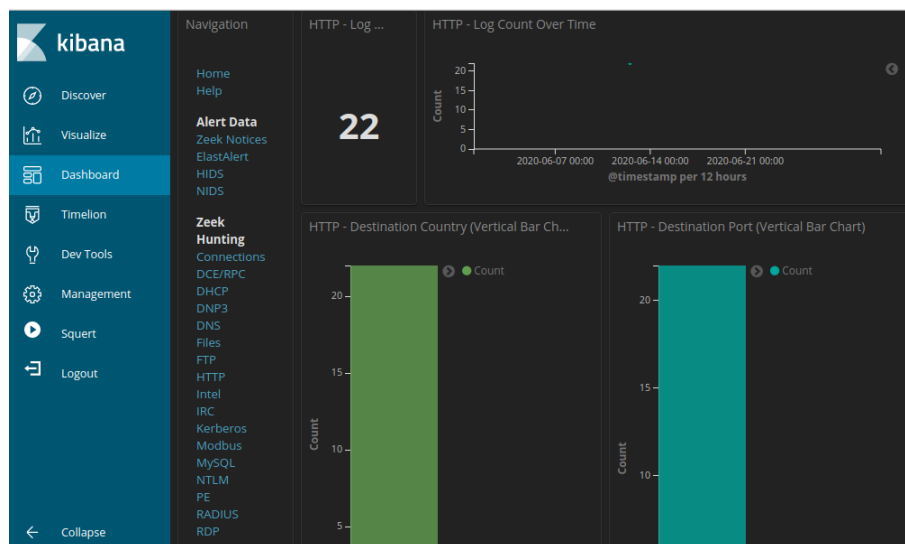


5. Perhatikan jumlah total log untuk seluruh bulan Juni 2020. Dasbor Anda harus serupa dengan yang ditunjukkan pada gambar. Luangkan waktu

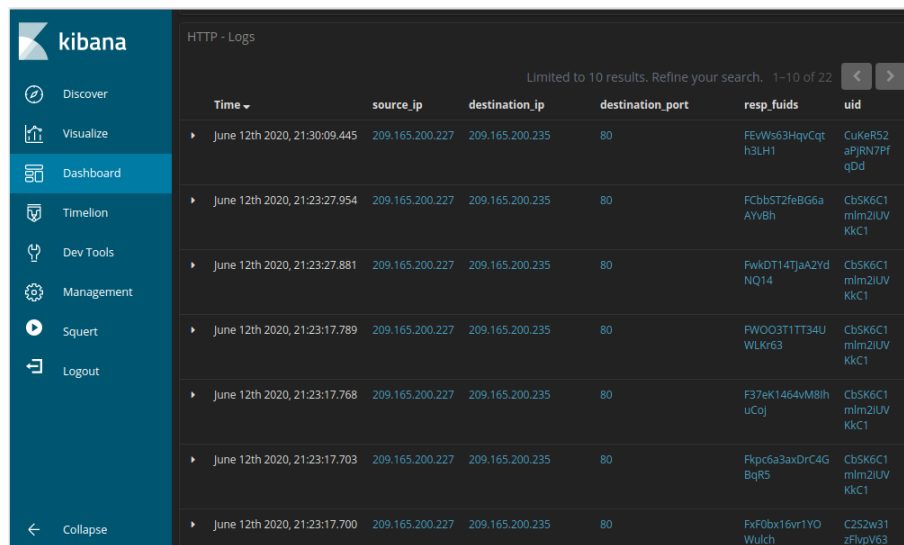
sejenak untuk menjelajahi informasi yang disediakan oleh antarmuka Kibana.



6. Karena aktor ancaman menilai data yang disimpan di server web, filter HTTP digunakan untuk memilih log yang terkait dengan lalu lintas HTTP. Pilih HTTP di bawah judul Zeek Hunting, seperti yang ditunjukkan pada gambar.



7. Gulir ke bawah ke Log HTTP. daftar 10 hasil pertama.



Kibana HTTP - Logs

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

Time	source_ip	destination_ip	destination_port	resp_fuids	uid
June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEWw53HqvCqt-h3LH1	CuKeR52aPjRN7Pf qDd
June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbbST2feBG6aAYv8h	Cb5K6C1mIm2iUVKkC1
June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TjaA2YdNQ14	Cb5K6C1mIm2iUVKkC1
June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWOQ3T1TT34UWLKr63	Cb5K6C1mIm2iUVKkC1
June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37ek1464vM8huCej	Cb5K6C1mIm2iUVKkC1
June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4GBqR5	Cb5K6C1mIm2iUVKkC1
June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YO Wulch	C252w31zFvpv63

8. Klik detail hasil pertama dengan mengklik panah yang ada di sebelah timestamp entri log. Perhatikan informasi yang tersedia.
9. Beberapa informasi untuk entri log ditautkan ke alat lain. Klik nilai di bidang alert \_id dari entri log untuk mendapatkan tampilan yang berbeda pada event tersebut.

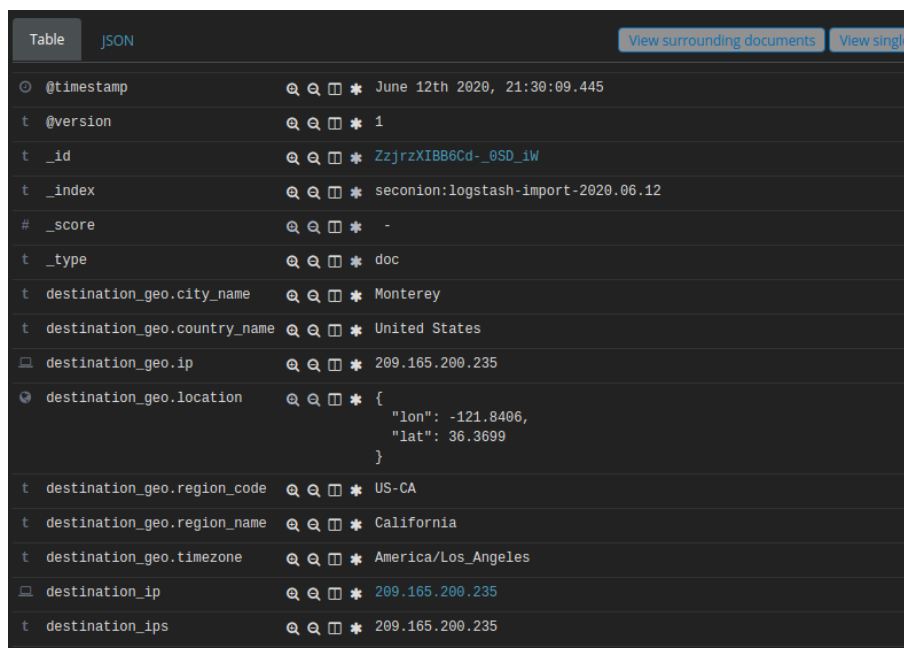


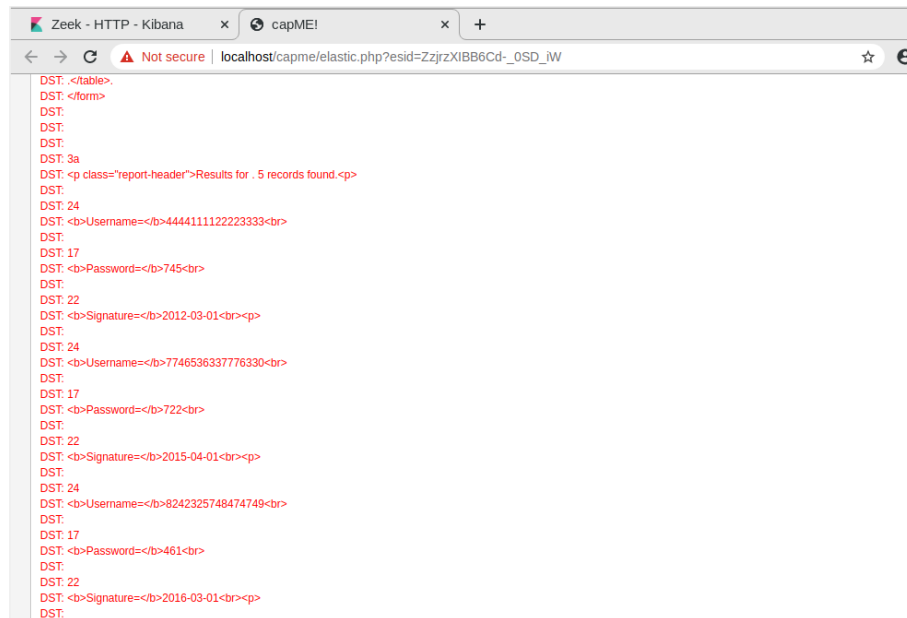
Table JSON

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

@timestamp	June 12th 2020, 21:30:09.445
@version	1
_id	ZzjrzXI8B6Cd-_0SD_1W
_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

10. Hasilnya terbuka di tab browser web baru dengan informasi dari capME!. capME! tab adalah antarmuka web yang memungkinkan Anda melihat transkrip pcap. Teks biru berisi permintaan HTTP yang dikirim dari sumber (SRC). Teks merah adalah tanggapan dari server web tujuan (DST).

11. Temukan keyword nama pengguna dalam transkrip. Gunakan Ctrl-F untuk membuka kotak pencarian. Gunakan tombol panah bawah di kotak pencarian untuk menelusuri kejadian yang ditemukan.

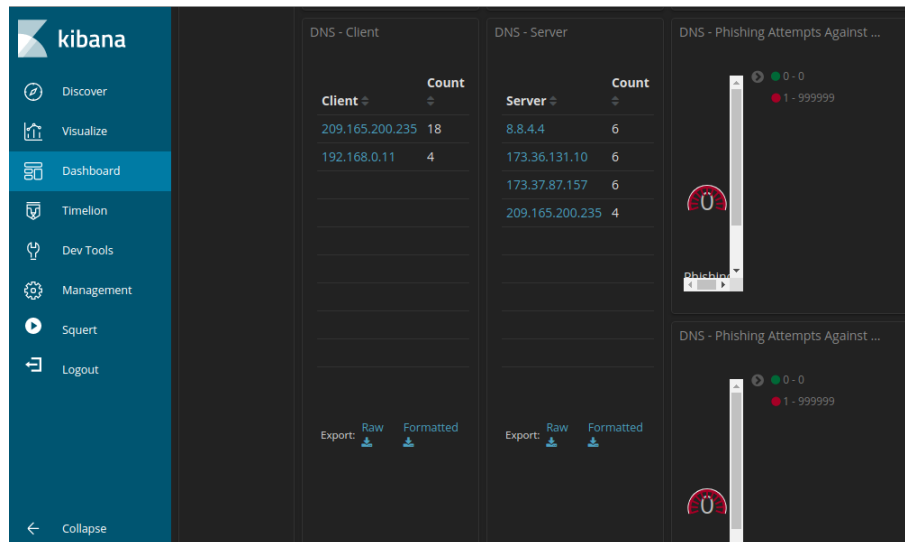


12. Dari bagian atas Dasbor Kibana, hapus semua filter dan istilah pencarian dan klik Beranda di bawah bagian Navigasi Dasbor. Periode Waktu masih harus mencakup Juni 2020.
13. Di area Dashboard yang sama, klik DNS di bagian Zeek Hunting. Perhatikan metrik Jumlah Log DNS dan diagram batang horizontal Port Tujuan.

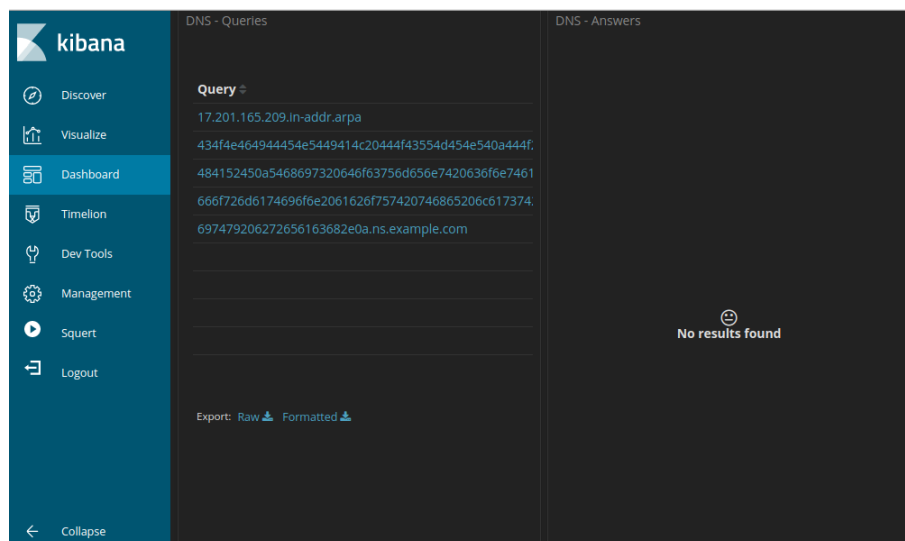


14. Gulir ke bawah jendela. Anda dapat melihat jenis kueri DNS teratas.

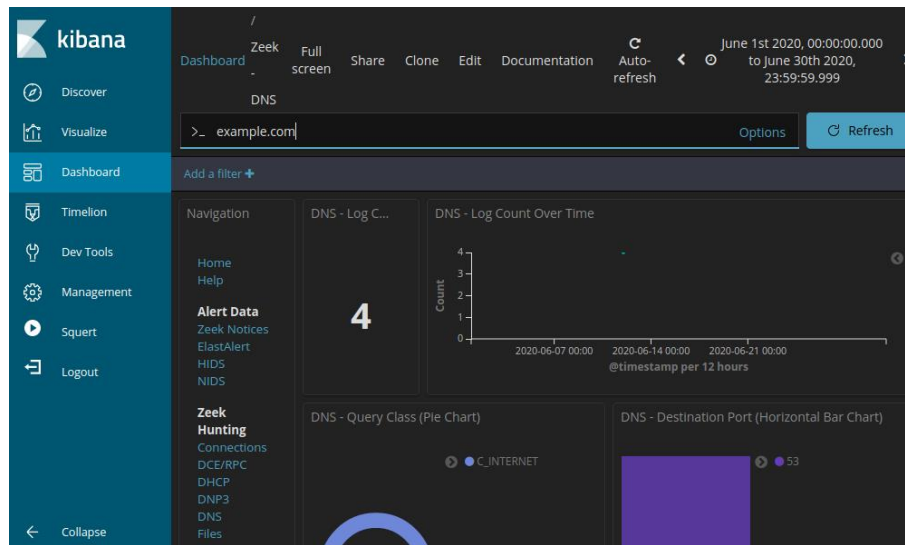
15. Dengan Menggulir lebih jauh ke bawah, Anda dapat melihat daftar klien DNS dan Server DNS teratas berdasarkan jumlah permintaan dan respons mereka.



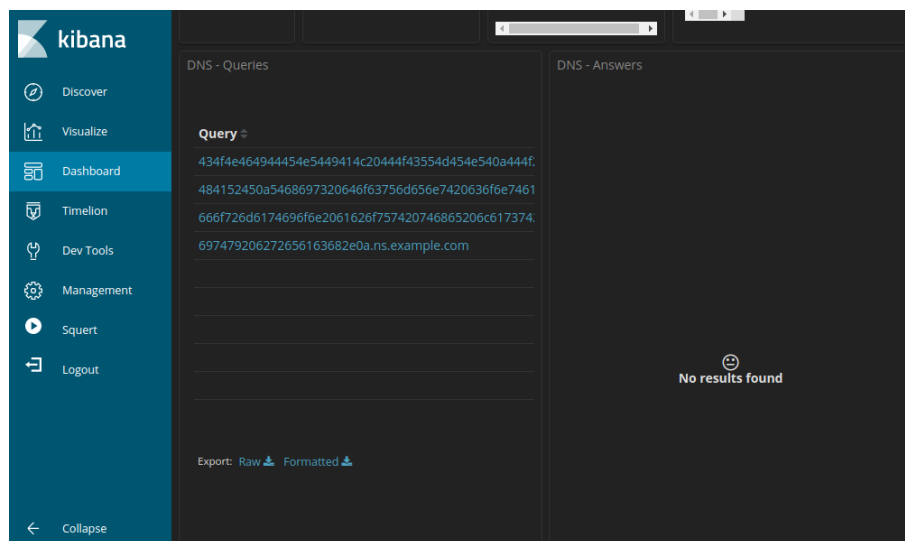
16. Menggulir lebih jauh ke bawah jendela, Anda dapat melihat daftar kueri DNS teratas berdasarkan nama domain. Perhatikan bagaimana beberapa kueri memiliki subdomain yang sangat panjang yang dilampirkan ke ns.example.com. Domain example.com harus diselidiki lebih lanjut



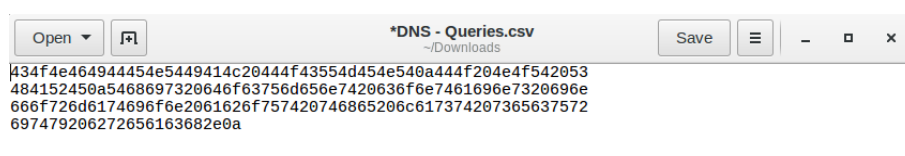
17. Gulir kembali ke bagian atas jendela dan masukkan example.com di bilah pencarian untuk memfilter example.com dan klik Perbarui. Perhatikan bahwa jumlah entri dalam Hitungan Log lebih kecil karena tampilan sekarang terbatas pada permintaan ke server example.com.



18. Lanjutkan untuk menggulir lebih jauh ke bawah untuk melihat empat entri log unik untuk kueri DNS ke example.com.  
Klik tautan Ekspor: Unduh untuk mengunduh kueri ke file eksternal. File CSV diunduh ke folder /home/analyst/Downloads.



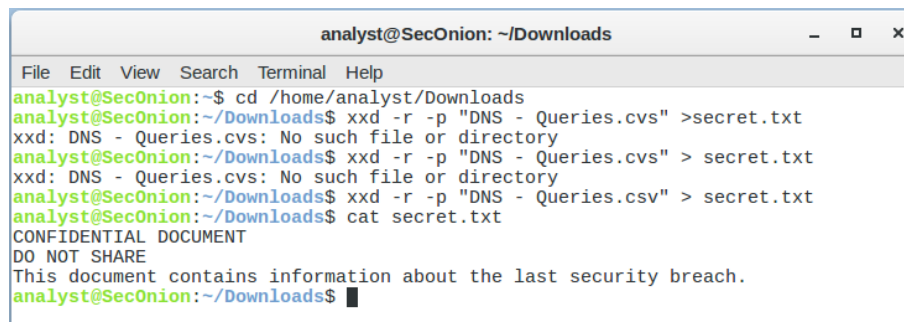
19. Arahkan ke folder /home/analyst/Downloads. Buka file menggunakan editor teks, seperti gedit. Edit file dengan menghapus teks di sekitar bagian heksadesimal dari subdomain, hanya menyisakan karakter heksadesimal. Pastikan untuk menghapus tanda kutip juga. Isi file Anda akan terlihat seperti informasi di bawah ini. Simpan file teks yang diedit dengan nama file asli.



20. 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 konsol.

```
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
```

```
analyst@SecOnion:~/Downloads$ cat secret.txt
```



```
analyst@SecOnion: ~/Downloads
File Edit View Search Terminal Help
analyst@SecOnion:~$ cd /home/analyst/Downloads
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
xxd: DNS - Queries.csv: No such file or directory
analyst@SecOnion:~/Downloads$ xxd -r -p "DNS - Queries.csv" > secret.txt
xxd: DNS - Queries.csv: No such file or directory
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$
```

## E. Pembahasan

Pada praktikum kali ini yaitu melakukan persiapan log file pada security onion *Virtual Machine*. Seperti biasa dengan sistem Linux, file log diputar berdasarkan tanggal, diganti namanya dan disimpan di disk. File log saat ini dapat ditemukan di bawah direktori saat ini dan gunakan perintah `ls-l` untuk melihat file log yang dihasilkan oleh Zeek. Security Onion dapat memisahkan file berdasarkan antarmuka. Karena image Security Onion VM memiliki dua antarmuka yang dikonfigurasi sebagai sensor dan folder khusus untuk data yang diimpor, tiga direktori disimpan. Gunakan perintah `ls -l seconion-eth0` untuk melihat file yang dihasilkan oleh antarmuka `eth0`. Sementara direktori `/nsm/` menyimpan beberapa file log, file log yang lebih spesifik dapat ditemukan di bawah `/var/log/nsm/`. Normalisasi log penting dan tergantung pada lingkungan yang digunakan. Alat populer menyertakan fitur normalisasi mereka sendiri, tetapi normalisasi log juga dapat dilakukan secara manual. Saat menormalkan dan menyiapkan file log secara manual, periksa ulang skrip untuk memastikan hasil yang diinginkan tercapai. Skrip normalisasi yang ditulis dengan buruk dapat mengubah data, secara langsung berdampak pada pekerjaan analisis.

### Menafsirkan Data HTTP dan DNS untuk Mengisolasi Pelaku Ancaman

Pada bagian ini kita akan menyelidiki eksploitasi di mana akses tidak sah dibuat ke informasi sensitif yang disimpan di server web. Anda akan menggunakan Kibana untuk menentukan sumber serangan dan informasi yang diakses oleh penyerang. Sebelumnya kita perlu melakukan perubahan pengaturan waktu untuk melihat data bulan Juni 2020. Di sudut kanan atas jendela, klik 24 jam terakhir untuk mengubah ukuran rentang waktu sampel. Perluas rentang waktu untuk menyertakan peringatan yang menarik. Serangan injeksi SQL terjadi pada Juni 2020 jadi itulah yang perlu Anda targetkan. Pilih Absolute di bawah rentang waktu dan edit waktu



from dan to untuk memasukkan seluruh bulan Juni di 2020. Filter HTTP digunakan untuk memilih log yang terkait dengan lalu lintas HTTP. Pilih HTTP di bawah judul Zeek Hunting, seperti yang ditunjukkan pada gambar. Nantinya dapat diketahui alamat IP sumber yaitu 209.165.200.227 dan alamat IP tujuan yaitu 209.165.200.235.

HTTP - Source IP Address		HTTP - Destination IP Address	
IP Address ▾	Count ▾	IP Address ▾	Count ▾
209.165.200.227	22	209.165.200.235	22

<div>kibana</div> <ul style="list-style-type: none"> <li>Discover</li> <li>Visualize</li> <li>Dashboard</li> <li>Timelion</li> <li>Dev Tools</li> <li>Management</li> <li>Squert</li> <li>Logout</li> </ul>	# destination_port	80
	t event_type	bro_http
	t host	d68c9368b6ae
	t ips	209.165.200.235, 209.165.200.227
	t message	{\"ts\":\"2020-06-12T21:30:09.445830Z\", \"uid\":\"CuKeR52aPjRN7PfQdD\", \"id_h\":\"209.165.200.227\", \"id_orig_p\":\"56194\", \"id_resp_h\":\"209.165.200.235\", \"id_resp_p\":\"80\", \"trans_depth\":1, \"method\":\"GET\", \"host\":\"209.165.200.235\", \"mutillidae/index.php?page=user-info.php&username='+union+select+cober,ccv,expiration,null+from+credit_cards+--+&password=&user-info-it-button=View+Account+Details\", \"referrer\":\"http://209.165.200.235/dae/index.php?page=user-info.php?version=1.1\", \"user_agent\":\"Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0\", \"request_body_len\":0, \"response_body_len\":23665, \"status_code\":200, \"status_msg\":\"HTTP: URI_Sqli\", \"resp_fuids\":\"FEVwS63HqvCqth3LH1\", \"resp_mime_types\":\"text/html\"}
	t method	GET
	t path	/nsm/import/bro-bro-WSLdfbf0/http.log
	t referrer	http://209.165.200.235/mutillidae/index.php?page=user-info.php
	# request_body_length	0
	t resp_fuids	FEVwS63HqvCqth3LH1
	t resp_mime_types	text/html
	# response_body_length	23,665
	t source_geo.city_name	Monterey

<div>kibana</div> <ul style="list-style-type: none"> <li>Discover</li> <li>Visualize</li> <li>Dashboard</li> <li>Timelion</li> <li>Dev Tools</li> <li>Management</li> <li>Squert</li> <li>Logout</li> </ul>	HTTP - Logs					
	Limited to 10 results. Refine your search. 1-10 of 22					
	Time ▾	source_ip	destination_ip	destination_port	resp_fuids	uid
	▶ June 12th 2020, 21:30:09.445	209.165.200.227	209.165.200.235	80	FEVwS63HqvCqth3LH1	CuKeR52aPjRN7PfQdD
	▶ June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbbST2feBG6aAYvBh	CbSK6C1mIm2lUVKkC1
	▶ June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkDT14TjaA2YdNQ14	CbSK6C1mIm2lUVKkC1
	▶ June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWOQ3T1TT34UWULr63	CbSK6C1mIm2lUVKkC1
	▶ June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37ek1464vM8ihuCoj	CbSK6C1mIm2lUVKkC1
	▶ June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4GBqR5	CbSK6C1mIm2lUVKkC1
	▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YOwulch	C252w31zFvpV63

Pada Log HTTP dapat ditemukan banyak informasi seperti nomor port tujuan yaitu 80, timestamp salah satunya yaitu June 12<sup>th</sup> 2020, 21:30:09:445, jenis eventnya adalah bro\_http, dan terdapat kolom pesan dalam menu message.

Langkah selanjutnya yaitu mereview hasil dengan mengklik nilai di bidang alert\_id dari entri log tadi untuk mendapatkan tampilan yang berbeda pada event tersebut. Nantinya akan terbuka di web baru dengan informasi dari capME yang merupakan antarmuka web yang memungkinkan kita melihat transkrip pcap. Teks biru berisi permintaan HTTP yang dikirim dari sumber (SRC). Teks merah adalah tanggapan dari server web tujuan (DST). Jika kotak input pada halaman web tidak terlindungi dengan baik dari input ilegal, pelaku ancaman dapat menyuntikkan string pencarian SQL atau kode lain yang dapat mengakses data yang terdapat dalam database yang ditautkan ke halaman web. Terdapat beberapa contoh usernam, password, dan signature yang telah dieskfiltrasi seperti contoh dibawah.

```

DST: 24
DST: <b>Username=</b>4444111122223333<br>
DST:
DST: 17
DST: <b>Password=</b>745<br>
DST:
DST: 22
DST: <b>Signature=</b>2012-03-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>7746536337776330<br>
DST:
DST: 17
DST: <b>Password=</b>722<br>
DST:
DST: 22
DST: <b>Signature=</b>2015-04-01<br><p>
DST:
DST: 24
DST: <b>Username=</b>8242325748474749<br>
DST:
DST: 17
DST: <b>Password=</b>461<br>
DST:
DST: 22
DST: <b>Signature=</b>2016-03-01<br><p>
DST:

```

Untuk bagian ke-4 yaitu menganalisis DNS exfiltration. Langkah selanjutnya yaitu filter DNS traffic dengan menghapus semua filter dan istilah pencarian dan klik beranda bawah bagian navigasi dasbor serta periode tetap pada Juni 2020. DNS di bagian Zeek Hunting. Perhatikan metrik jumlah Log DNS dan diagram batang horizontal port tujuan yaitu 22. Selanjutnya yaitu meninjau entri terkait DNS. Kita dapat melihat jenis kueri DNS teratas. Kita akan melihat catatan alamat (catatan A), alamat IPv6 catatan Quad A (AAAA), catatan NetBIOS (NB) dan catatan pointer untuk menyelesaikan nama host (PTR). Kita dapat melihat daftar client DNS dan server DNS teratas berdasarkan jumlah permintaan dan respon mereka. Dikethui alamat IP client yaitu 209.165.200.235 dengan jumlah permintaan 18 dan 192.168.0.11 dengan jumlah permintaan 4. Sementara server DNS yaitu 8.8.4.4, 173.36.131.10, 173.37.87.157 dengan masing-masing jumlah permintaan 6 dan 209.165.200.235 jumlah permintaan 4. Dikethui teks dari subdomain dari subdomain kueri DNS yaitu “DOKUMEN RAHASIA JANGAN BERBAGI. Dokumen ini berisi tentang pelanggaran keamanan terakhir. Hasil yang disiratkan tentang permintaan DNS khusus ini menunjukkan bahwa permintaan DNS terpisah,

permintaan terkoordinasi yang berisi konten tersembunyi. Signifikansi yang lebih besar dari hasilnya adalah bahwa permintaan DNS dapat digunakan untuk menyembunyikan pengiriman file dan melewati keamanan jaringan. Terdapat kemungkinan yang membuat queri DNS yang disandikan dan DNS dipilih sebagai sarana untuk mengekstrak data bahwa malware membuat ini dengan menelusuri dokumen di host dan menyandikan kontennya dalam heksadesimal dan kemudian membuat kueri DNS yang menggunakan string heksadesimal sebagai subdomain DNS. Permintaan DNS sangat umum dikirim dari jaringan ke internet, sehingga permintaan DNS mungkin tidak dipantau.

## **F. Kesimpulan**

Kesimpulan pada praktikum kali ini antara lain :

1. Normalisasi log penting dan tergantung pada lingkungan yang digunakan.
2. Alat populer menyertakan fitur normalisasi mereka sendiri, tetapi normalisasi log juga dapat dilakukan secara manual.
3. Saat menormalkan dan menyiapkan file log secara manual, periksa ulang skrip untuk memastikan hasil yang diinginkan tercapai. Skrip normalisasi yang ditulis dengan buruk dapat mengubah data, secara langsung berdampak pada pekerjaan analisis.
4. Kibana memiliki banyak dasbor dan visualisasi bawaan untuk pemantauan dan analisis.
5. capME! tab adalah antarmuka web yang memungkinkan Anda melihat transkrip pcap.
6. alamat IPv6 catatan Quad A (AAAA), catatan NetBIOS (NB) dan catatan pointer untuk menyelesaikan nama host (PTR). Anda juga dapat melihat kode respons DNS.

## **G. Daftar Pustaka**

fandii567gbr@gmail.com, F. H. (n.d.). *Bingung Apa itu DNS? Perhatikan Penjelasan Fungsi dan Cara Kerjanya*. Diskominfo.kuburayakab.go.id.  
<https://diskominfo.kuburayakab.go.id/read/58/bingung-apa-itu-dns-perhatikan-penjelasan-fungsi-dan-cara-kerjanya>

*Log File Adalah: Pengertian, Definisi, dan Penggunaan Katanya!* (n.d.). RM Digital. Retrieved March 20, 2023, from <https://rmdigital.co.id/kamus/log-file/>