

**LAPORAN PRAKTIKUM  
KEAMANAN INFORMASI 1  
UNIT 7**



**DI SUSUN OLEH:**

Nama : Bintang Nur K  
NIM : 21/481453/SV/19790  
Kelas : RI4AA  
Hari, tanggal : Selasa, 14 Maret 2023  
Dosen Pengampu : Anni Karimatul Fauziyyah, S.Kom., M.Eng  
Asisten Praktikum : Gabriella Alvera Chaterine

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

## **UNIT 7**

### **IP & Enterprise Services Vulnerability**

#### **I. TUJUAN**

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

#### **II. 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 seringkali 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 SecurityOnion 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.

### III. ALAT DAN BAHAN

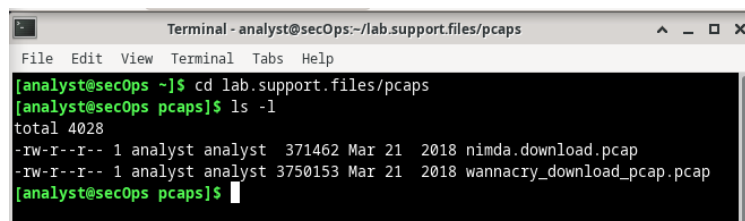
Alat dan Bahan yang dibutuhkan untuk melaksanakan praktikum adalah

- PC
- Koneksi Internet
- CyberOps Workstation VM

### IV. LANGKAH KERJA DAN HASIL

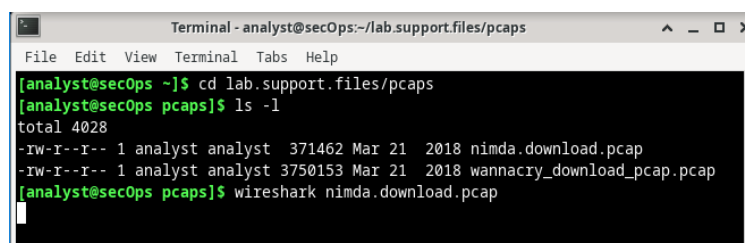
**Langkah 1:** Menganalisis Log yang Ditangkap sebelumnya dan Pengambilan Lalu Lintas

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



```
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]$
```

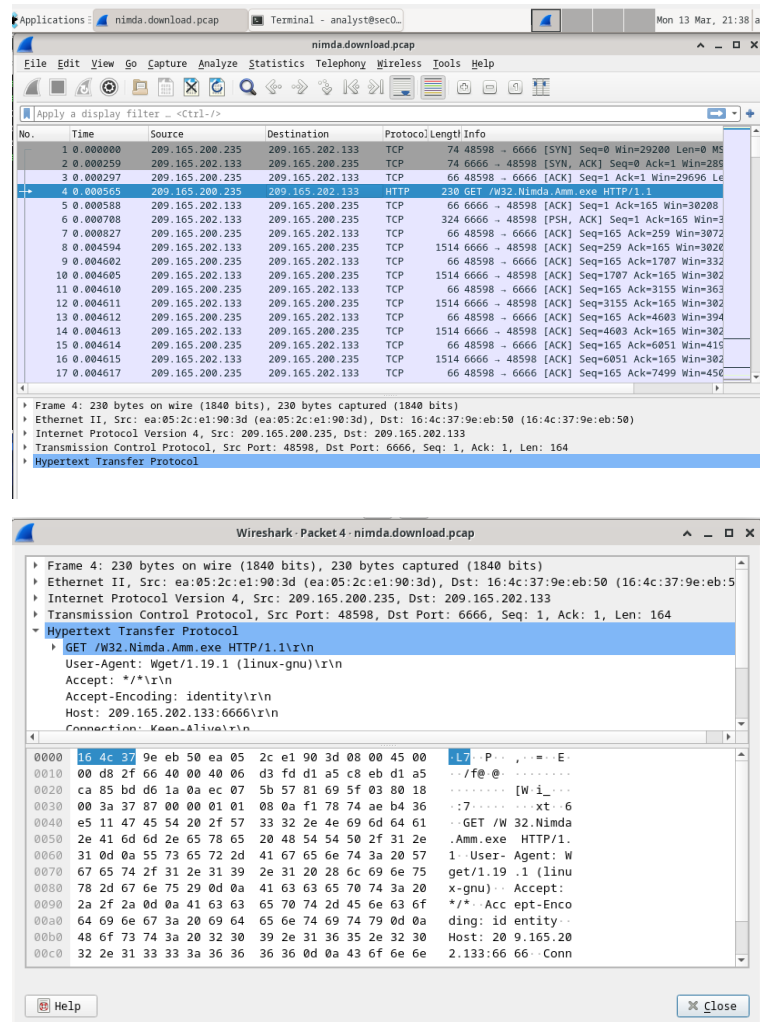
- b. Keluarkan perintah di bawah ini untuk membuka file `nimda.download.pcap` di *Wireshark*.



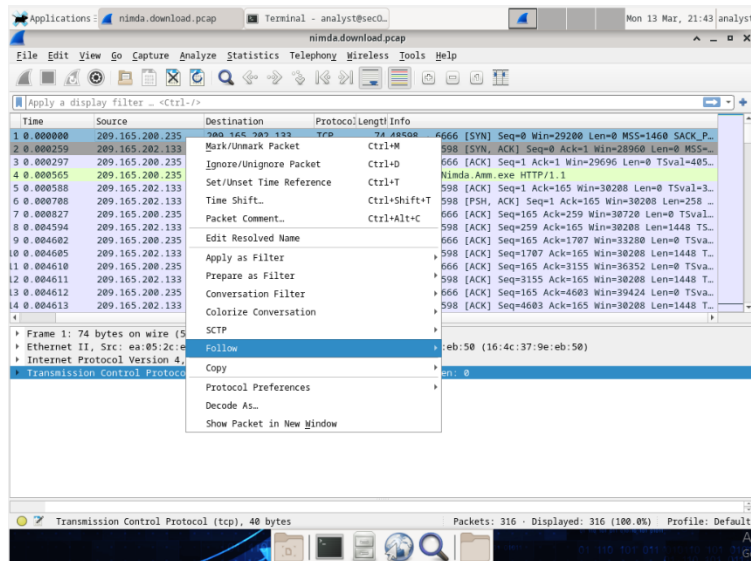
```
Terminal - analyst@secOps:~/lab.support.files/pcaps
File Edit View Terminal Tabs Help
[analyst@secOps ~]$ cd lab.support.files/pcaps
[analyst@secOps pcaps]$ ls -l
total 4028
-rw-r--r-- 1 analyst analyst 371462 Mar 21 2018 nimda.download.pcap
-rw-r--r-- 1 analyst analyst 3750153 Mar 21 2018 wannacry_download_pcap.pcap
[analyst@secOps pcaps]$ wireshark nimda.download.pcap
```

- c. 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.

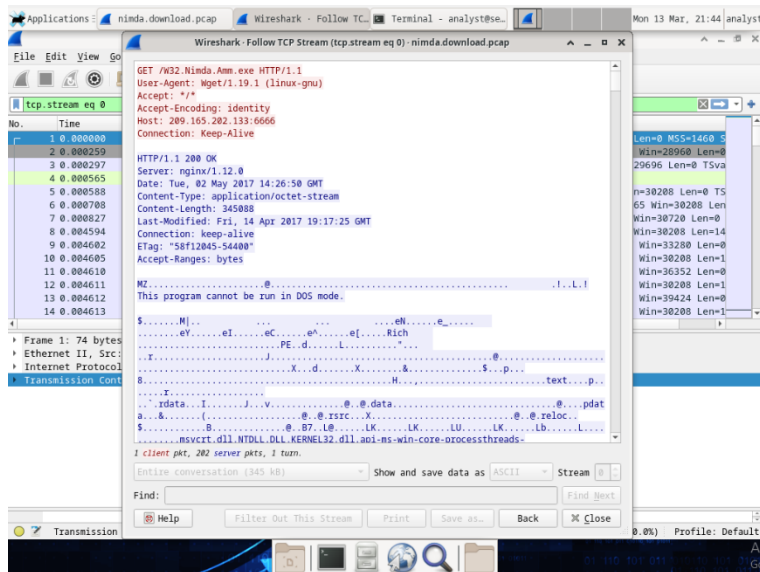
Pilih paket keempat dalam tangkapan dan perluas *Protokol Transfer Hypertext* untuk ditampilkan seperti yang ditunjukkan di bawah ini.



- d. 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.
- e. 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*.



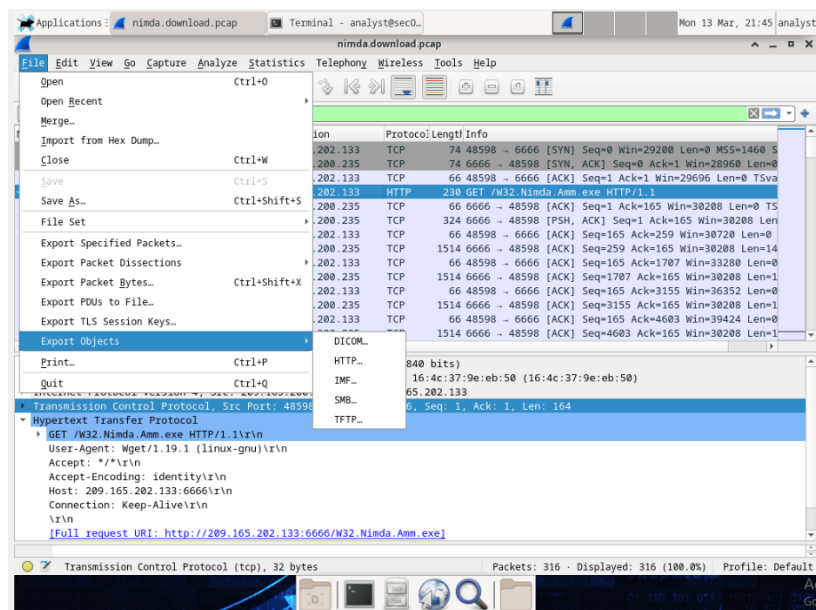
- f. *Wireshark* menampilkan jendela lain yang berisi detail untuk seluruh aliran TCP yang dipilih.



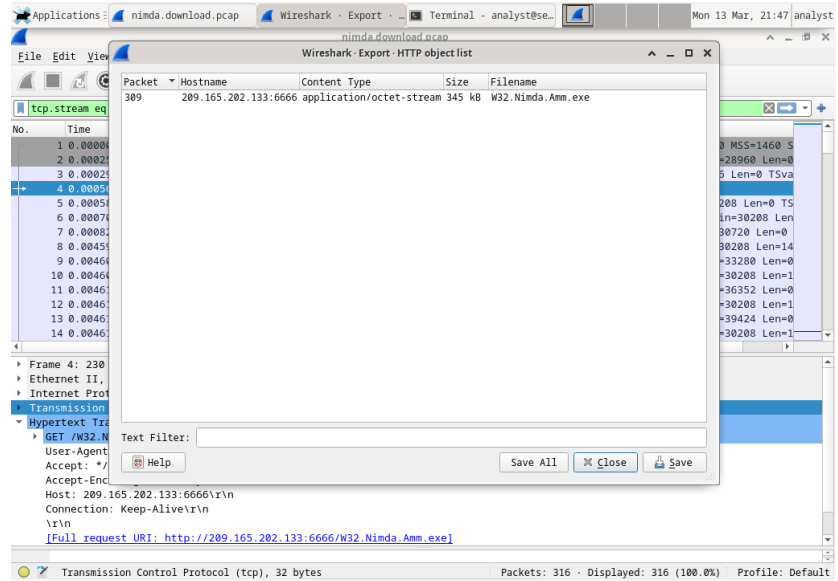
## Part 2: Extract Files yang di unduh dari PCAP

Karena file tangkapan berisi semua paket yang terkait dengan lalu lintas, PCAP unduhan dapat digunakan untuk mengambil file yang diunduh sebelumnya. Ikuti langkah-langkah di bawah ini untuk menggunakan *Wireshark* untuk mengambil *malware* Nimda

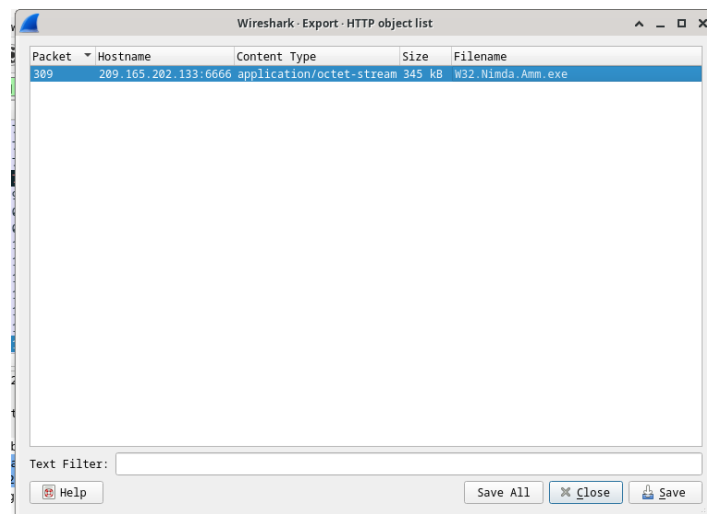
- 1) Dalam paket keempat dalam file nimda.download.pcap, perhatikan bahwa permintaan HTTP GET dihasilkan dari 209.165.200.235 menjadi 209.165.202.133. Kolom Info juga menunjukkan bahwa ini sebenarnya adalah permintaan GET untuk file tersebut.
- 2) Dengan paket permintaan GET yang dipilih, navigasikan ke File > Export Objects > HTTP, dari menu Wireshark.



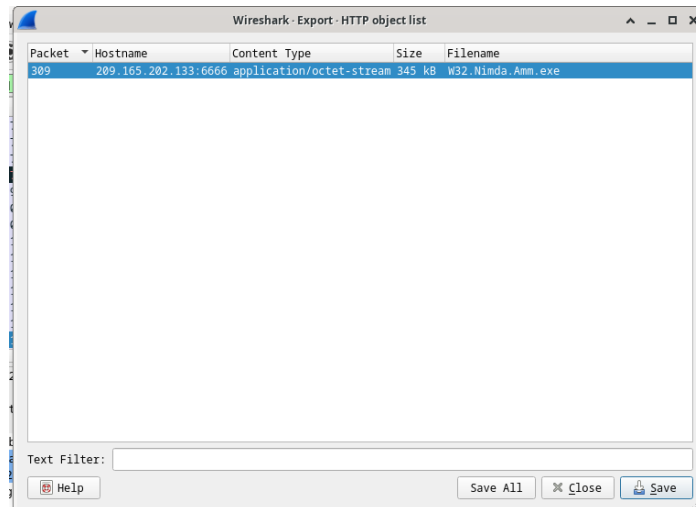
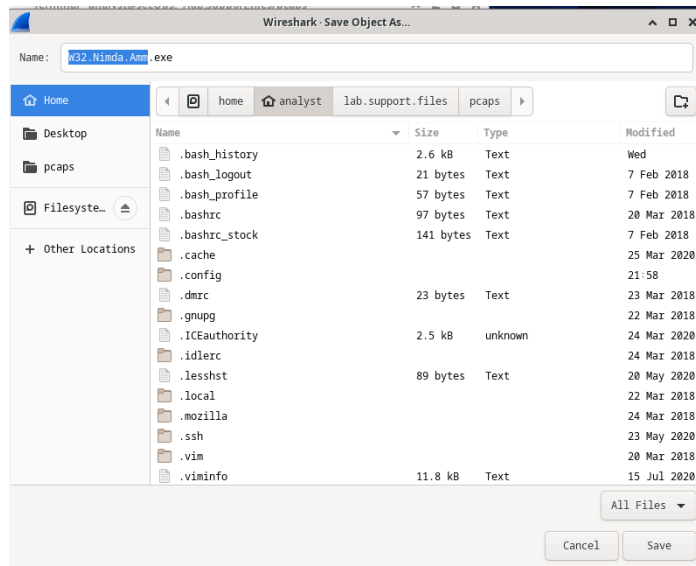
- 3) *Wireshark* akan menampilkan semua objek HTTP yang ada dalam aliran TCP yang berisi permintaan GET. Dalam hal ini, hanya file W32.Nimda.Amm.exe yang ada dalam pengambilan. Ini akan memakan waktu beberapa detik sebelum file ditampilkan



- 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 analis (bukan tab analis). 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.

```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
-rw-r--r-- 1 root root 4853760 Feb 20 21:26 httpdump.pcap
-rw-r--r-- 1 root root 2166003 Feb 20 21:33 httpsdump.pcap
drwxr-xr-x 9 analyst analyst 4096 Jul 15 2020 lab.support.files
-rw-r--r-- 1 analyst analyst 345088 Mar 13 21:54 nimda.download.pcap
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
[analyst@secOps ~]$ wireshark nimda.download.pcap
[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]$ wireshark nimda.download.pcap
^C
[analyst@secOps pcaps]$ cd /home/analyst
[analyst@secOps ~]$ ls -l
total 7216
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 4853760 Feb 20 21:26 httpdump.pcap
-rw-r--r-- 1 root root 2166003 Feb 20 21:33 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 21:58 W32.Nimda.Amm.exe
[analyst@secOps ~]$
```

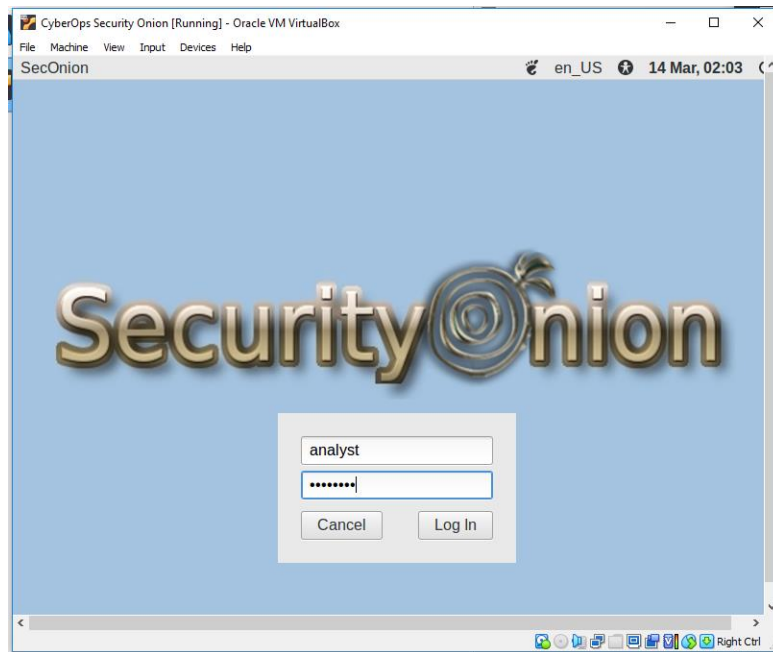
- 7) Perintah file memberikan informasi tentang jenis file. Gunakan perintah file untuk mempelajari lebih lanjut tentang malware, seperti yang ditunjukkan di bawah ini:

```
-rw-r--r-- 1 analyst analyst 345088 Mar 13 21:58 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 ~]$
```

## Persiapan Log File pada Security Onion Virtual Machine

Security Onion VM.

Luncurkan Security Onion VM dari Dasbor VirtualBox (username: analyst / password: cyberops).



## Zeek Logs pada Security Onion

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

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

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

## Snort Logs

- Log snort dapat ditemukan di `/nsm/sensor_data/`. Ubah direktori sebagai berikut.

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

- Gunakan perintah `ls -l` untuk melihat semua file log yang dihasilkan oleh Snor

```
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$
```

- 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
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$
```

## Various Logs

1. 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
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
securitonion             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$
```

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

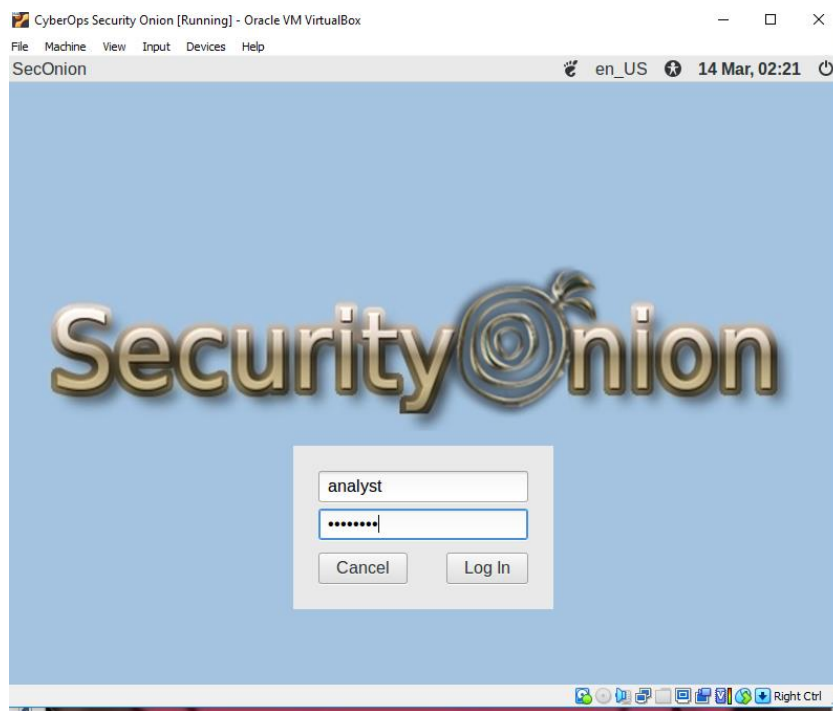
```
analyst@SecOnion:/var/log/nsm$ cd ..
analyst@SecOnion:/var/log$ ls
alternatives.log          bttmp.1          debug.4.gz        gpu-manager.log   messages.2.gz       syslog.5.gz
alternatives.log.1        cron.log         dmesg             installer         messages.3.gz       syslog.6.gz
alternatives.log.2.gz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

Summary.

## PRAKTIKUM LAB

### Langkah 1: Ubah jangka waktu /timeframe

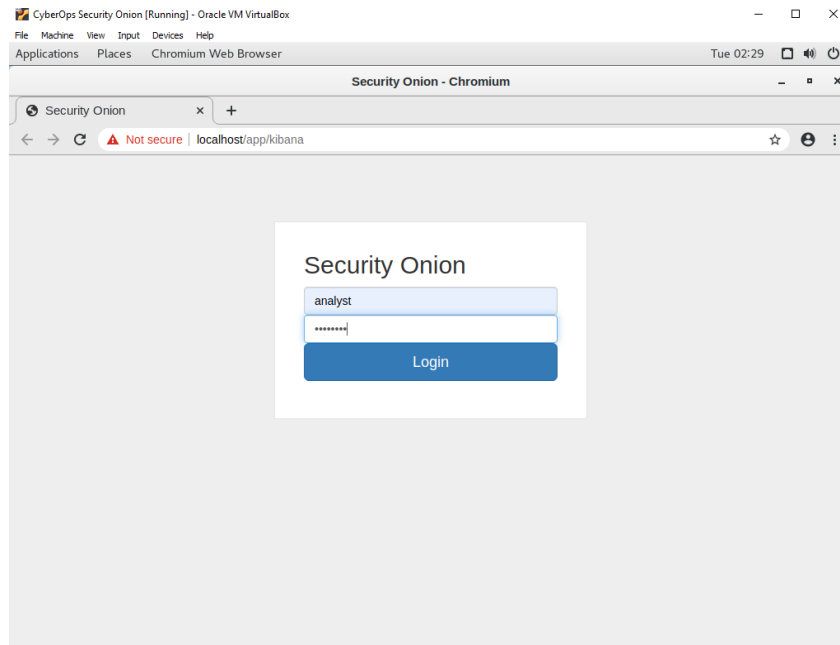
- A. Mulai Security Onion VM dan masuk dengan username analyst and the password cyberops.



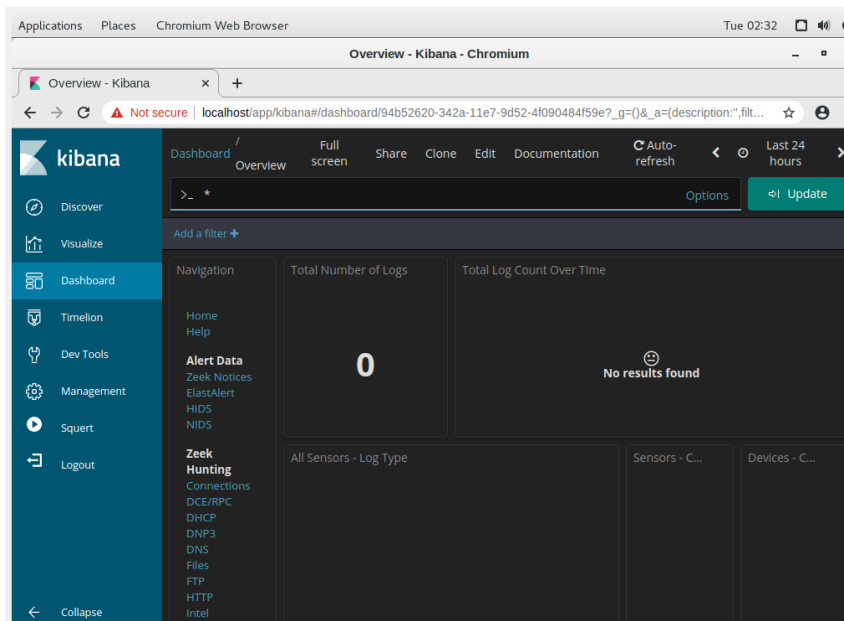
- B. Masukkan perintah `sudo so-status` untuk memeriksa status layanan. Status untuk semua layanan harus OK sebelum memulai analisis. Ini bisa memakan waktu beberapa menit

```
analyst@SecOnion: ~  
File Edit View Search Terminal Help  
analyst@SecOnion:/var/log$ cd  
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  
Logstash API/stats not yet available...still initializing. [ WARN ]  
* so-kibana [ OK ]  
* so-freqserver [ OK ]  
analyst@SecOnion:~$
```

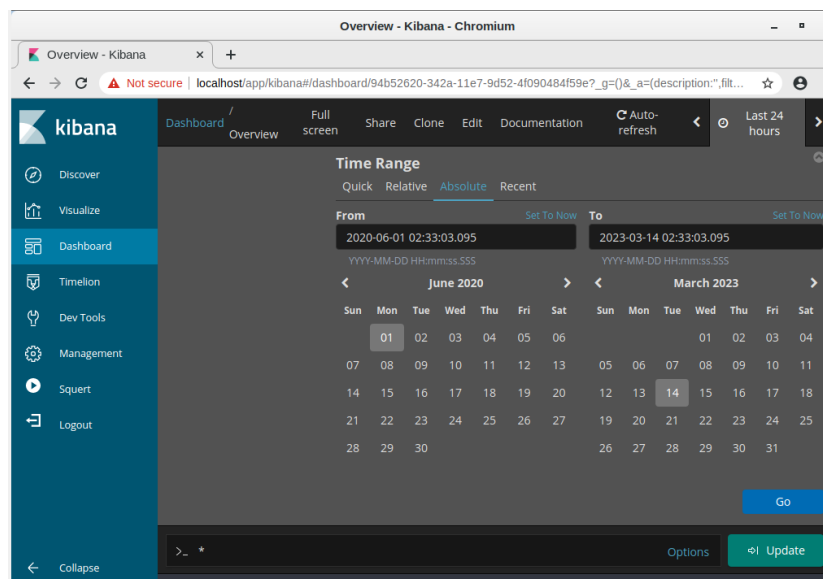
- C. Setelah Anda masuk, buka Kibana menggunakan pintasan di Desktop. Masuk dengan username analyst dan password cyberops.



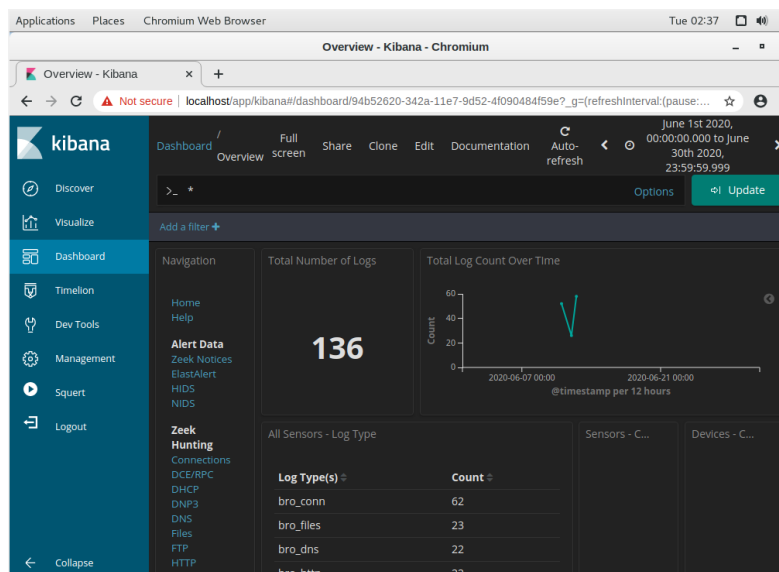
Di Security Onion, Kibana memiliki banyak dasbor dan visualisasi bawaan untuk pemantauan dan analisis. Anda juga dapat membuat dasbor dan visualisasi khusus Anda sendiri untuk memantau lingkungan jaringan khusus Anda. Catatan: Dasbor Anda mungkin tidak memiliki hasil apa pun dalam 24 jam terakhir.



- D. 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

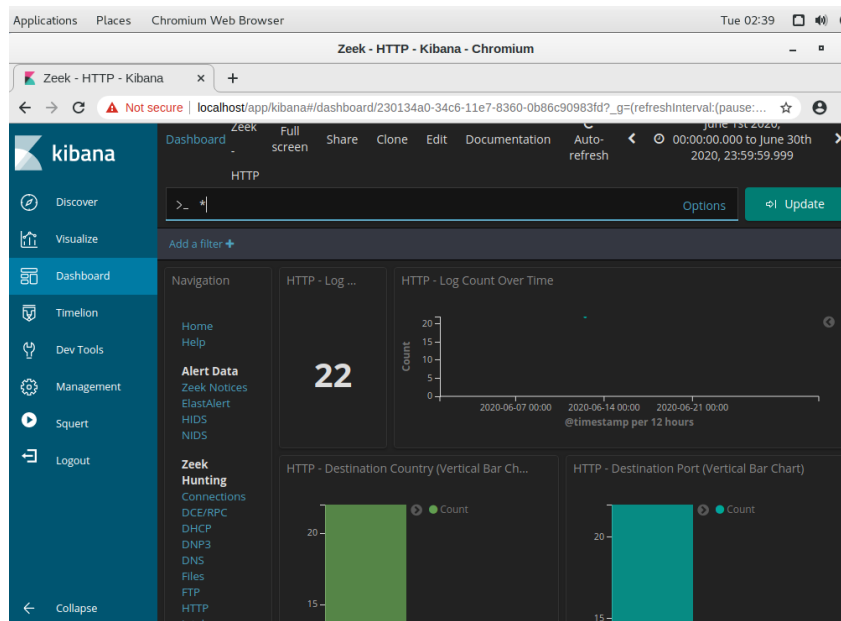
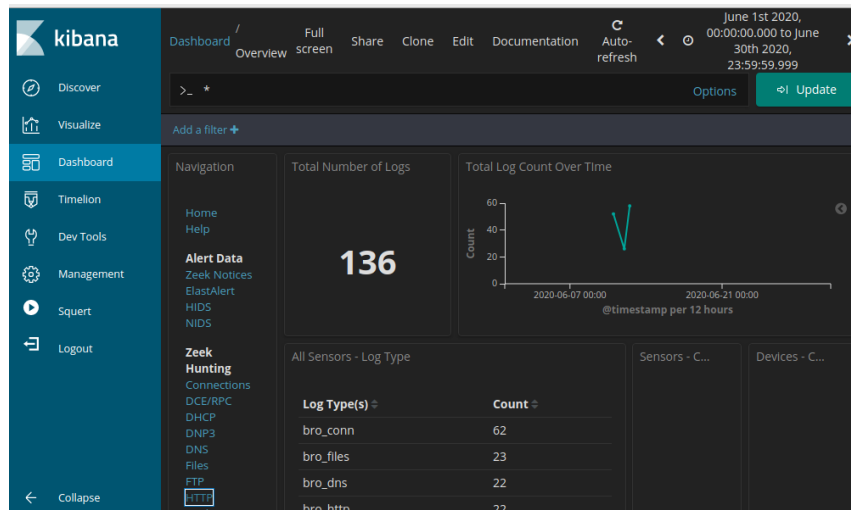


- E. Perhatikan jumlah total log untuk seluruh bulan Juni 2020. Dasbor Anda harus serupa dengan yang ditunjukkan pada gambar. Luangkan waktu sejenak untuk menjelajahi informasi yang disediakan oleh antarmuka Kibana.



## Langkah 2: Filter dari HTTP traffic

- F. 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



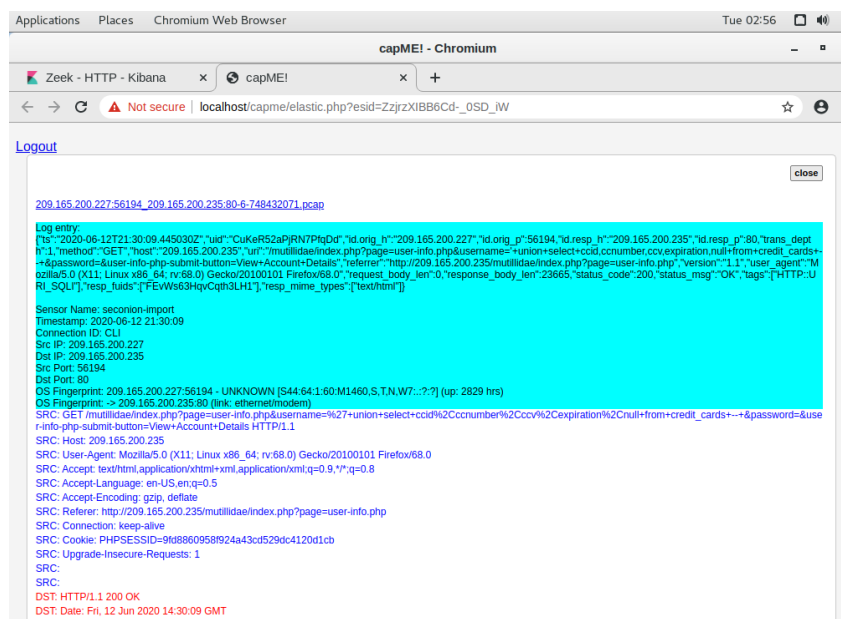


Langkah 3: Review hasil.

G. 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
@timestamp	June 12th 2020, 21:30:09.445		
@version	1		
_id	ZzjrZXlB86Cd_0SD_1W		
_index	seconion:logstash-import-2020.06.12		
_score	-		

H. 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)



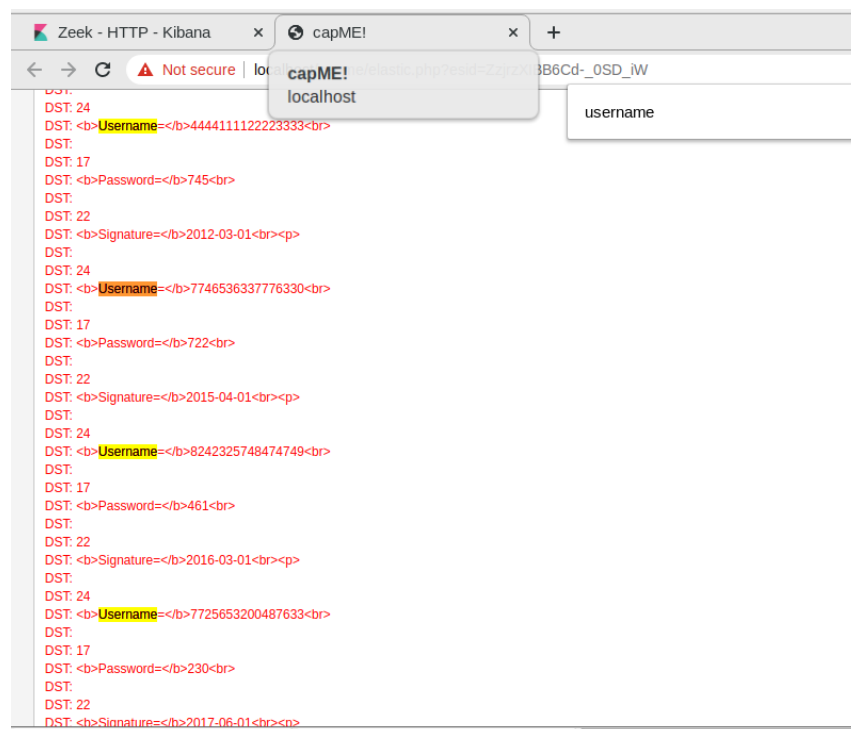
I. Di bagian entri Log, yang ada di awal transkrip, perhatikan bagian `username='+union+select+ccid,ccnumber,ccv,expiration,null+from+credit_cards+--&password=` menunjukkan bahwa seseorang mungkin telah mencoba untuk menyerang browser web menggunakan injeksi SQL untuk melewati otentikasi. Kata kunci, `union` dan `select`, adalah perintah yang digunakan dalam mencari informasi dalam database SQL.

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

```
Log entry:
{"ts": "2020-06-12T21:30:09.445030Z", "uid": "CuKeR52aPJRN7PfqDd", "id.orig_h": "209.165.200.227", "id.orig_p": "56194", "id.resp_h": "209.165.200.235", "id.resp_p": "80", "trans_dept": "1", "method": "GET", "host": "209.165.200.235", "uri": "/mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit_cards+&password=&user-info-submit-button=View+Account+Details", "referrer": "http://209.165.200.235/mutillidae/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": "OK", "tags": ["HTTP::URI_SQLI"], "resp_fuids": ["FEvW563HqvCqth3LH1"], "resp_mime_types": ["text/html"]}
```

Sensor Name: seconion-import  
Timestamp: 2020-06-12 21:30:09  
Connection ID: CLI  
Src IP: 209.165.200.227  
Dst IP: 209.165.200.235  
Src Port: 56194  
Dst Port: 80  
OS Fingerprint: 209.165.200.227:56194 - UNKNOWN [S44:64:1:60:M1460,S,T,N,W7::?:?] (up: 2829 hrs)  
OS Fingerprint -> 209.165.200.235:80 (link: ethernet/modem)  
SRC: GET /mutillidae/index.php?page=user-info.php&username=%27+union+select+ccid%2Cccnumber%2Cccv%2Cexpiration%2Cnull+from+credit\_cards+&password=&user-info-submit-button=View+Account+Details HTTP/1.1

- J. 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.



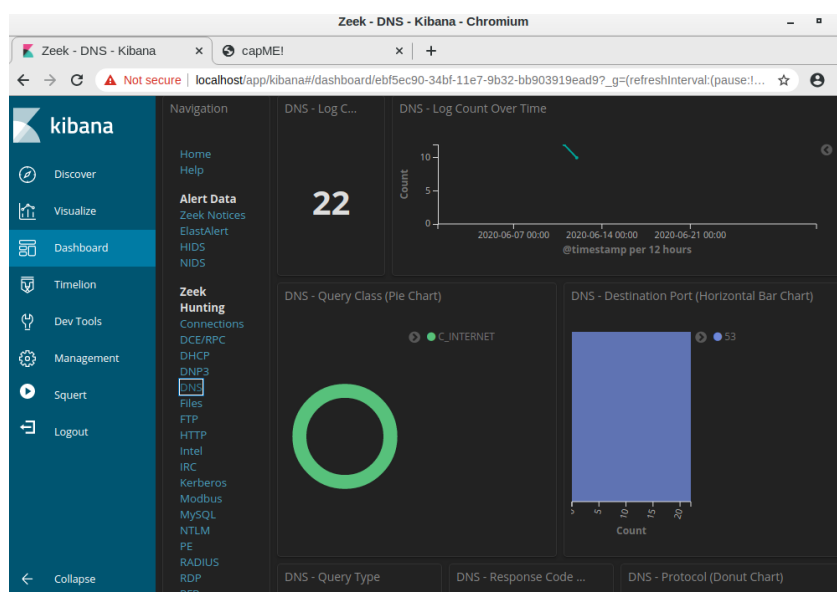
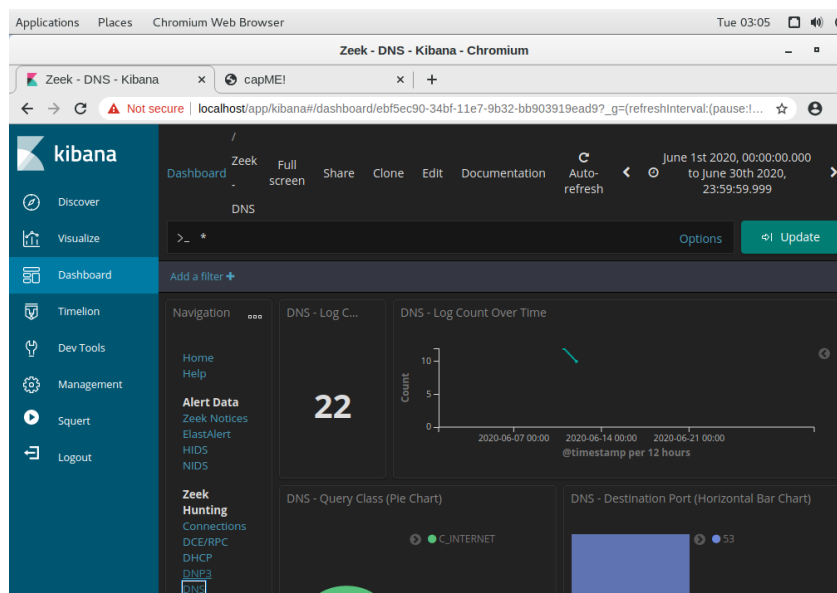
Anda dapat melihat di mana istilah nama pengguna digunakan di antarmuka web yang ditampilkan kepada pengguna. Namun, jika Anda melihat lebih jauh ke bawah, sesuatu yang tidak biasa dapat ditemukan.

#### Bagian 4: Analisis DNS exfiltration.

##### Langkah 4: Filter DNS traffic.

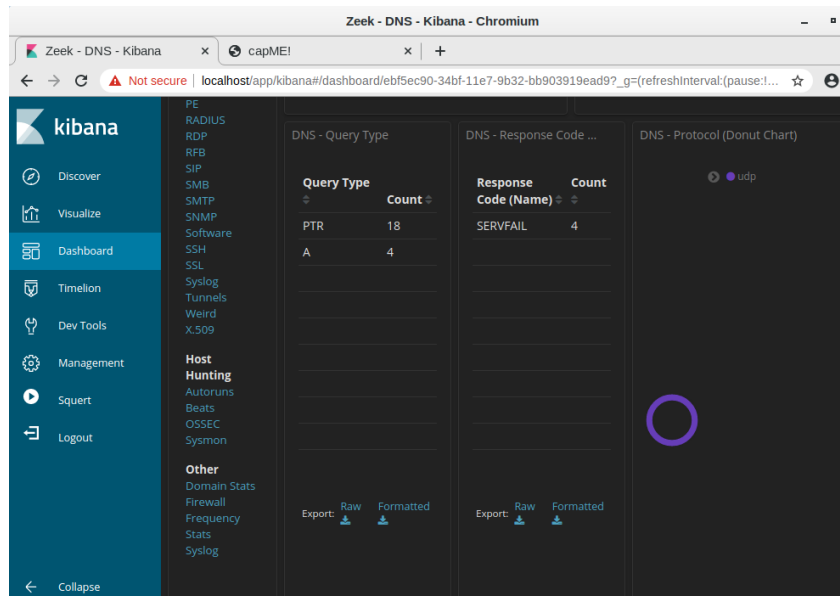
K. Dari bagian atas Dasbor Kibana, hapus semua filter dan istilah pencarian dan klik Beranda di bawah bagian Navigasi Dasbor. Periode Waktu masih harus mencakup Juni 2020.

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

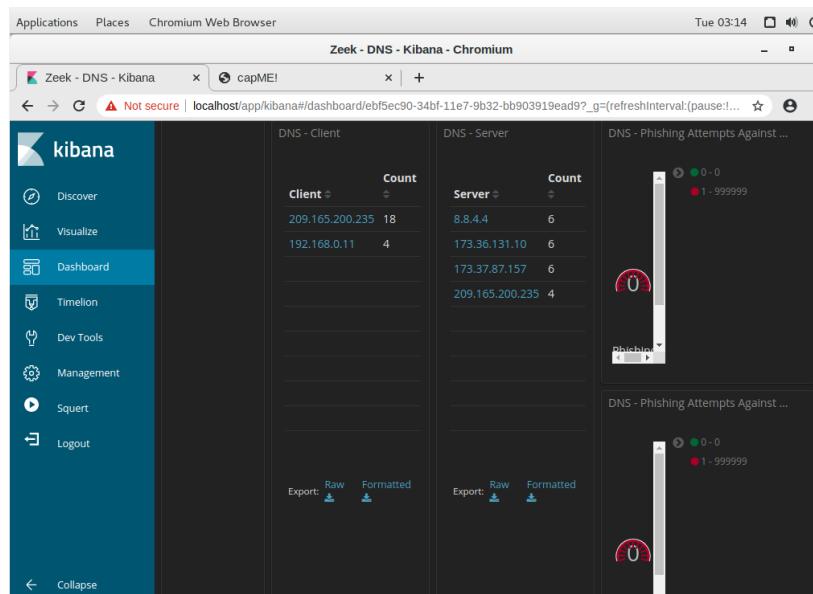


## Langkah 5: Tinjau entri terkait DNS

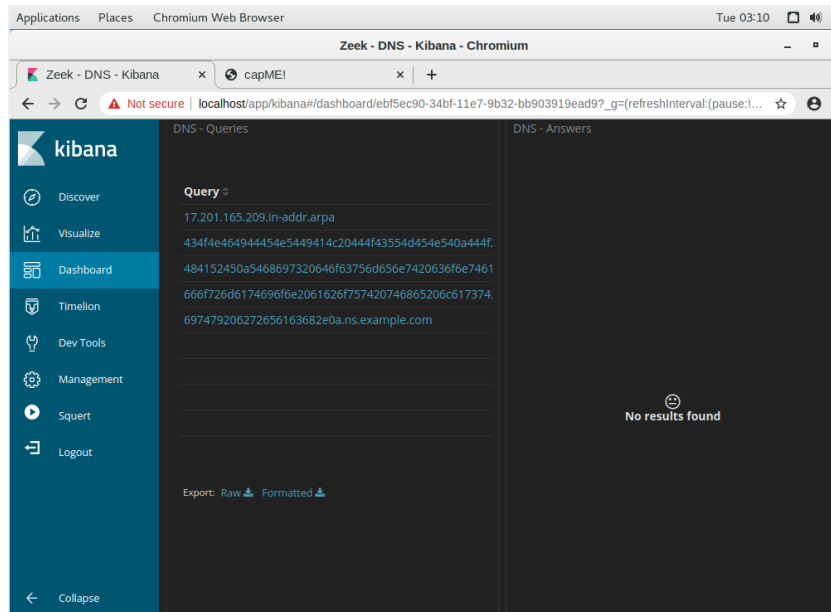
M. Gulir ke bawah jendela. Anda dapat melihat jenis kueri DNS teratas. Anda mungkin melihat catatan alamat (catatan A), alamat IPv6 catatan Quad A (AAAA), catatan NetBIOS (NB) dan catatan pointer untuk menyelesaikan nama host (PTR). Anda juga dapat melihat kode respons DNS



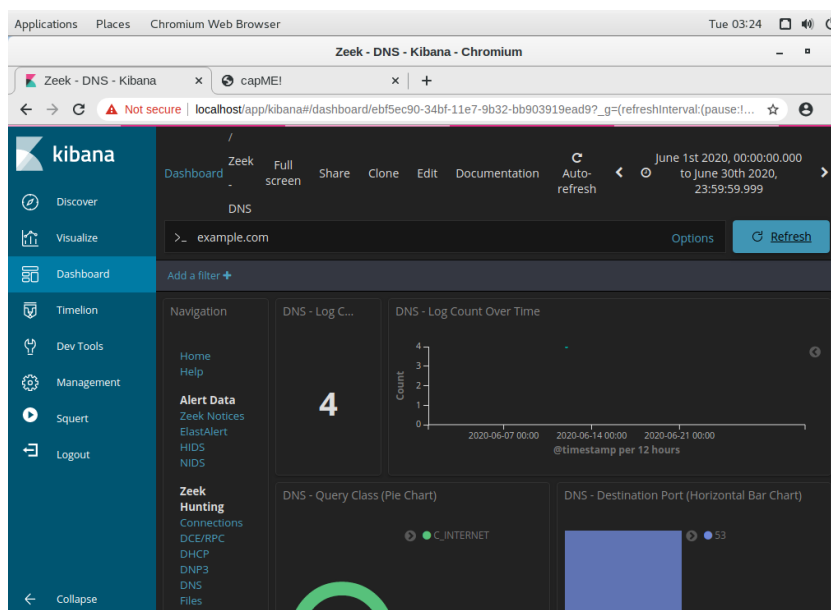
N. Dengan Menggulir lebih jauh ke bawah, Anda dapat melihat daftar klien DNS dan Server DNS teratas berdasarkan jumlah permintaan dan respons mereka. Ada juga metrik untuk jumlah upaya DNS Phishing, yang juga dikenal sebagai pharming DNS, spoofing, atau poisoning



- O. Menggulir lebih jauh ke bawah jendela, 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

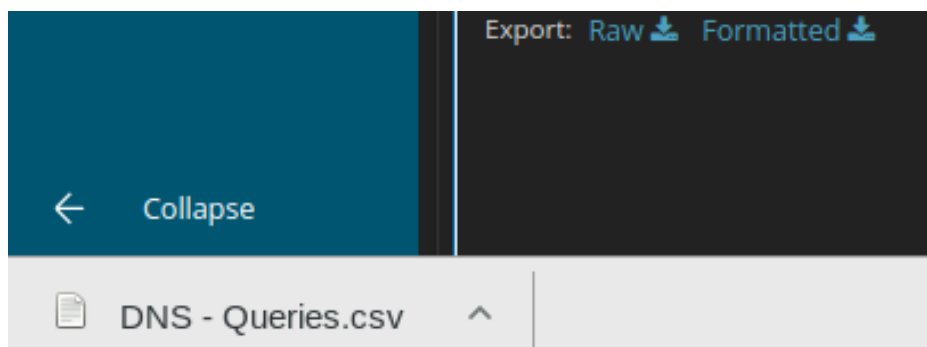
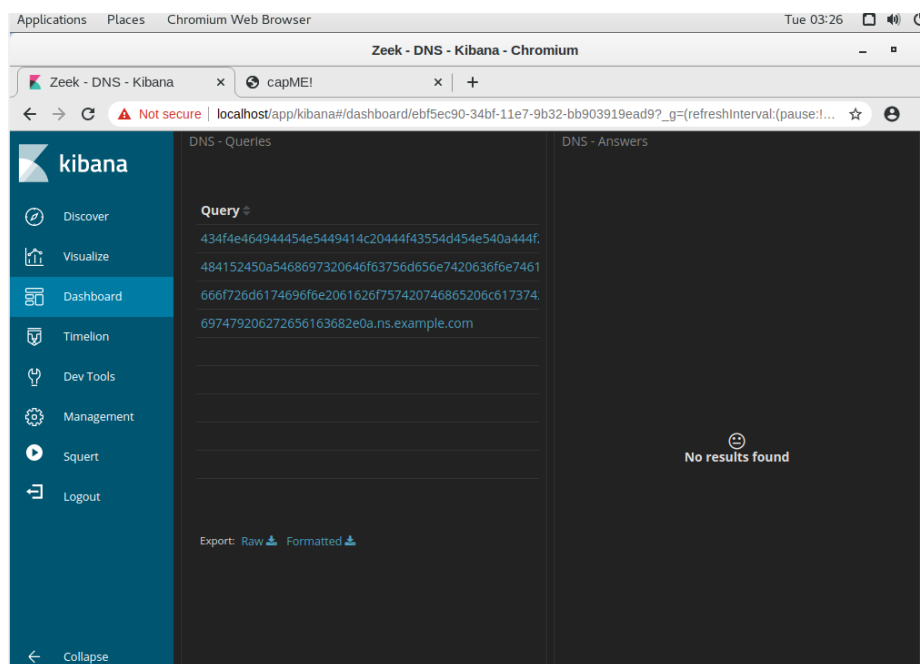


- P. Gulir kembali ke bagian atas jendela dan masukkan example.com di bilah pencarian untuk memfilter example.com dan klik Perbarui. Perhatikan bahwa jumlah entri dalam Hitungan Log lebih kecil karena tampilan sekarang terbatas pada permintaan ke server example.com

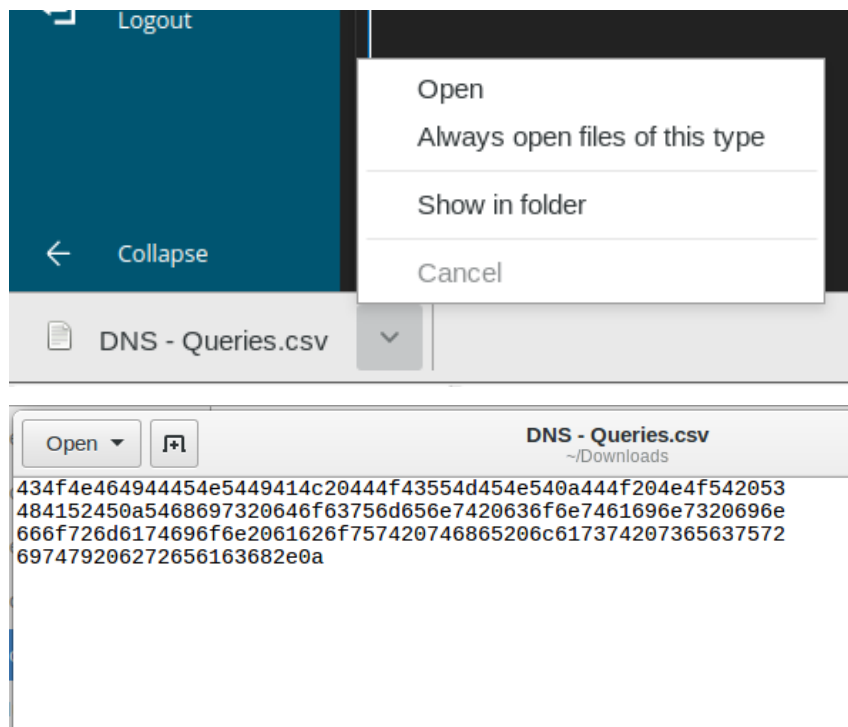


## Langkah 6: Tentukan data yang diekstraksi

Q. Lanjutkan untuk menggulir lebih jauh ke bawah untuk melihat empat entri log unik untuk kueri DNS ke example.com. Perhatikan bagaimana kueri ke subdomain panjang yang mencurigakan yang dilampirkan ke ns.example.com. String panjang angka dan huruf di subdomain terlihat seperti teks yang dikodekan ke dalam heksadesimal (0-9, a-f) daripada nama subdomain yang sah. Klik tautan Ekspor: Unduh untuk mengunduh kueri ke file eksternal. File CSV diunduh ke folder /home/analyst/Downloads



- R. 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



- S. 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:~$ 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$
```

## **V. ANALISIS**

Pada praktikum keamanan informasi 1 kali ini melakukan Ekstrak Executable dari PCAP dan Menafsirkan Data HTTP dan DNS untuk Mengisolasi Pelaku Ancaman serta melakukan persiapan Log File pada Security Onion Virtual Machine.

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 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. Analisis kemudian dapat mengklik kanan peringatan itu untuk mencari database ELSA atau Bro untuk pemahaman yang lebih baik tentang acara tersebut.

### **Pertanyaan:**

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

Jawab:

Simbol yang ditampilkan adalah tebakan terbaik Wireshark untuk memahami data biner sambil mendekodekannya sebagai teks.

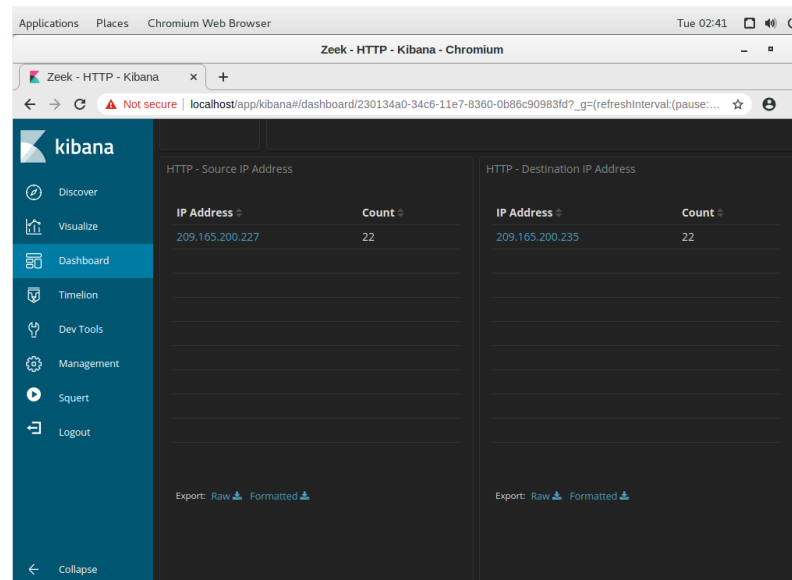


Simbol adalah konten sebenarnya dari file yang diunduh. Karena ini adalah file biner, Wireshark tidak tahu bagaimana merepresentasikannya

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

Karena penangkapan dimulai tepat sebelum pengunduhan dan berhenti tepat setelahnya. Tidak ada lalu lintas lain yang ditangkap saat penangkapan aktif.

3. Apa alamat IP sumber? Apa alamat IP tujuan?



Fungsi IP address yang utama adalah memudahkan proses komunikasi di dalam jaringan computer.

#### 4. Berapa nomor port tujuan?

Applications Places Chromium Web Browser Tue 02:43

Zeek - HTTP - Kibana - Chromium

Zeek - HTTP - Kibana x +

Not secure localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?\_g=(refreshInterval:(pause:...)

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	FEvW563HqvCqt h3LH1	CuKaR52 apjRN7P qDd
▶ June 12th 2020, 21:23:27.954	209.165.200.227	209.165.200.235	80	FCbb5T2feBG6a AYv8h	Cb5K6C1 mIm2lUV KkC1
▶ June 12th 2020, 21:23:27.881	209.165.200.227	209.165.200.235	80	FwkOT14Tja2Yd NQ14	Cb5K6C1 mIm2lUV KkC1
▶ June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWO03T1TT34U WLK63	Cb5K6C1 mIm2lUV KkC1
▶ June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37ek1464vM8lh uCoj	Cb5K6C1 mIm2lUV KkC1
▶ June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4G BqR5	Cb5K6C1 mIm2lUV KkC1
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YO Wulch	C252w31 zFvpV63 kPa

← Collapse

Applications Places Chromium Web Browser Tue 02:44

Zeek - HTTP - Kibana - Chromium

Zeek - HTTP - Kibana x +

Not secure localhost/app/kibana#/dashboard/230134a0-34c6-11e7-8360-0b86c90983fd?\_g=(refreshInterval:(pause:...)

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

▶ June 12th 2020, 21:23:17.789	209.165.200.227	209.165.200.235	80	FWO03T1TT34U WLK63	Cb5K6C1 mIm2lUV KkC1
▶ June 12th 2020, 21:23:17.768	209.165.200.227	209.165.200.235	80	F37ek1464vM8lh uCoj	Cb5K6C1 mIm2lUV KkC1
▶ June 12th 2020, 21:23:17.703	209.165.200.227	209.165.200.235	80	Fkpc6a3axDrC4G BqR5	Cb5K6C1 mIm2lUV KkC1
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FxF0bx16vr1YO Wulch	C252w31 zFvpV63 kPa
▶ June 12th 2020, 21:23:17.700	209.165.200.227	209.165.200.235	80	FuZtB17PkhDulv nG4	C43RGFez op5b3qz 6
▶ June 12th 2020, 21:23:17.699	209.165.200.227	209.165.200.235	80	FxgVdq18u4TH8 RSEK9	C4KeAa3 plgDqfa AQy8
▶ June 12th 2020, 21:23:17.698	209.165.200.227	209.165.200.235	80	F1sqn240m9nW ZsMvvc	C4KeAa3 plgDqfa AQy8

← Collapse

5. Apa timestamp dari hasil pertama? Apa jenis event? Apa yang termasuk dalam kolom pesan?

Applications Places Chromium Web Browser Tue 02:46

Zeek - HTTP - Kibana - Chromium

Zeek - HTTP - Kibana x +

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

kibana

Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Squert

Logout

Collapse

HTTP - Logs

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	FEVWs63HqvCqt h3LH1	CuKeR52 aPJRN7PF qDd

Table JSON View surrounding documents View single

@timestamp	June 12th 2020, 21:30:09.445
@version	1
_id	ZzjrzXIB8Cd-_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

kibana

Discover

Visualize

Dashboard

Timelion

Dev Tools

Management

Squert

Logout

Collapse

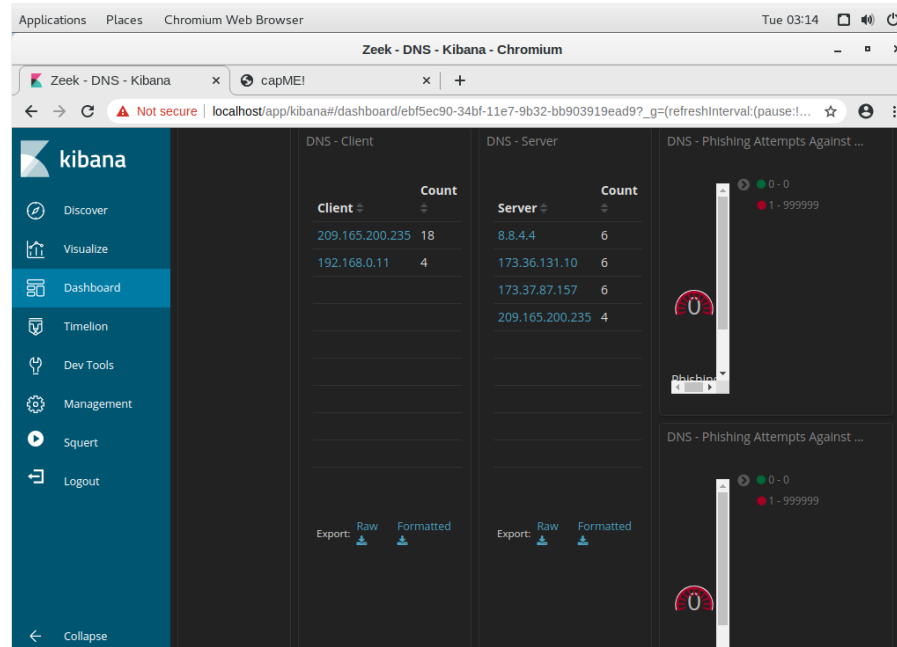
HTTP - Logs

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
ips	209.165.200.235, 209.165.200.227

Discover	HTTP - Logs
Visualize	
Dashboard	destination_port 80
Timelion	event_type <b>pro-http</b>
Dev Tools	host d68c9360b6ae
Management	ips 209.165.200.235, 209.165.200.227
Squert	message {"ts":"2020-06-12T21:30:09.445030Z","uid":"CvKaR52aPjRN7PfqDu","id.orig_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","url":"/mutillidae/index.php?page=user-info.php&username=*union+select+ccid,ccber,ccv,expiration,null+from+credit_cards+--+&password=user-info-php-...it-button=View+Account+Details","referrer":"http://209.165.200.235/mutillidae/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":"OK","s":["HTTP::URI_SQLI"],"resp_fuids":["FEVws63HqvCqth3LH1"],"resp_mime_t":["text/html"]}
Logout	method GET
	path /nsm/import/bro/bro-W5Ldfbf0/http.log
	referrer http://209.165.200.235/mutillidae/index.php?page=user-info.php
	request_body_length 0

6. Apa yang Anda lihat nanti dalam transkrip tentang nama pengguna? Pada hal ini kita bisa menemukan ataupun melihat dimana istilah nama pengguna atau username digunakan di antarmuka web yang ditampilkan kepada pengguna.

7. Sebutkan alamat IP klien dan server DNS



## **VI. KESIMPULAN**

Setelah melaksanakan praktikum yang saya dapatkan adalah

- Dengan memiliki IP address setiap perangkat yang menggunakan internet dapat terhubung satu sama lain. Sehingga antar perangkat bisa saling berkomunikasi
- Sebelum menggunakan DNS, mapping domain dahulu menggunakan file hosts.txt.
- Sniffer (juga dikenal sebagai penganalisa jaringan atau penganalisa paket) adalah perangkat lunak atau perangkat keras yang dapat mencegah dan mencatat lalu lintas di jaringan. Alat tersebut menangkap setiap paket yang mengalir melintasi infrastruktur dan menganalisis isinya.

## **VII. DAFTAR PUSTAKA**

Prak KI 1. (2023). Materi Pertemuan 5. Retrieved Maret 20, 2023, from Elok UGM

Fandii Hazuarni, fandii567gbr@gmail.com. (2020, March). *Bingung APA ITU DNS? Perhatikan Penjelasan Fungsi Dan Cara Kerjanya*. Dinas Komunikasi dan Informatika Kabupaten Kuburaya. Retrieved March 25, 2023, from <https://diskominfo.kuburayakab.go.id/read/58/bingung-apa-itu-dns-perhatikan-penjelasan-fungsi-dan-cara-kerjanya>

Paessler AG. (2023, March 1). *Free network sniffer: PRTG lets you...* Paessler. Retrieved March 26, 2023, from [https://www.paessler.com/network\\_sniffer?gclid=Cj0KCQjwt\\_qgBhDFARIsABcDjOefSgVWgJonRQYwrwR0rXrdHIFp8CUfDfUvx95wUEYIq3mLR6PBwdYaAvt3EALw\\_wcB](https://www.paessler.com/network_sniffer?gclid=Cj0KCQjwt_qgBhDFARIsABcDjOefSgVWgJonRQYwrwR0rXrdHIFp8CUfDfUvx95wUEYIq3mLR6PBwdYaAvt3EALw_wcB)