

## 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](http://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](mailto: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

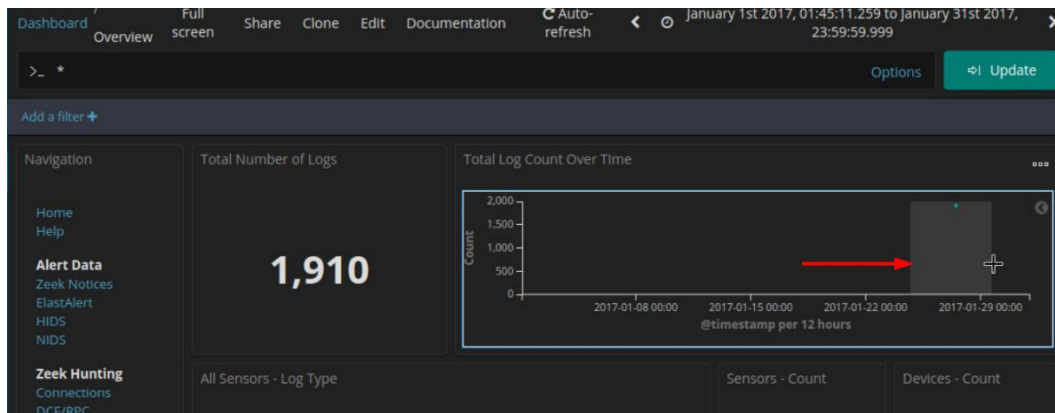
In Part 1, use Kibana to answer the following questions. To help you get started, you are informed that the attack took place at some time during January 2017. You will need to pinpoint the exact time.

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

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

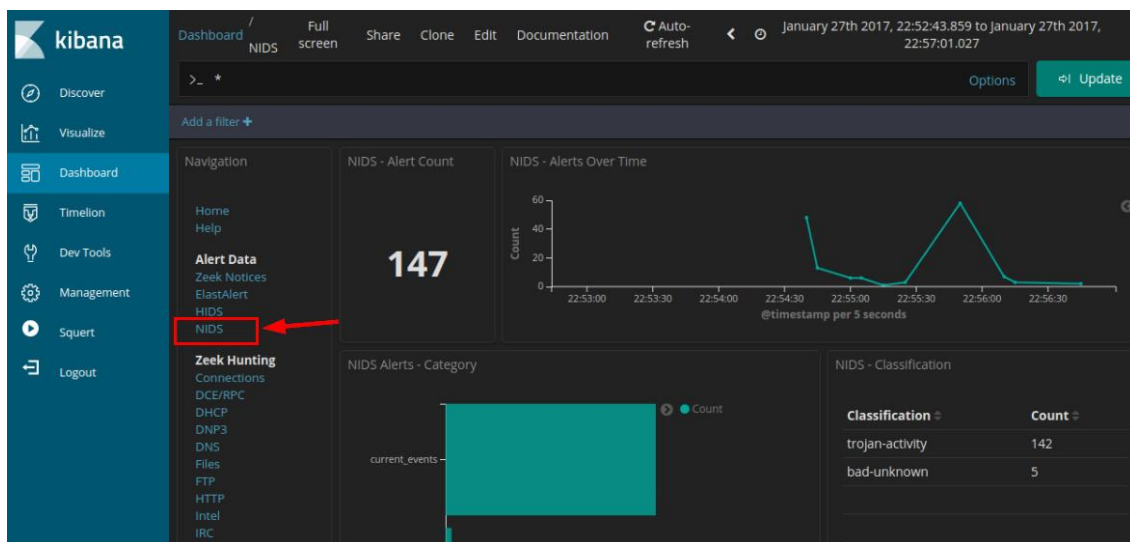
clicking and dragging to select an area around the graph data point. You may need to repeat this process until you see some detail in the graph.



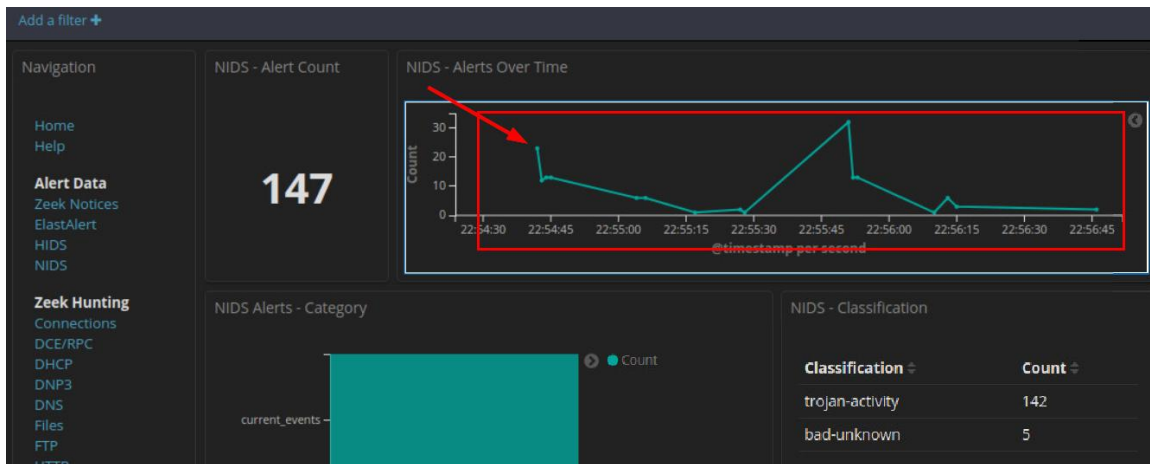
**Note:** Use the <Esc> key to close any dialog boxes that may be interfering with your work.

### Step 2: Locate the Event in Kibana

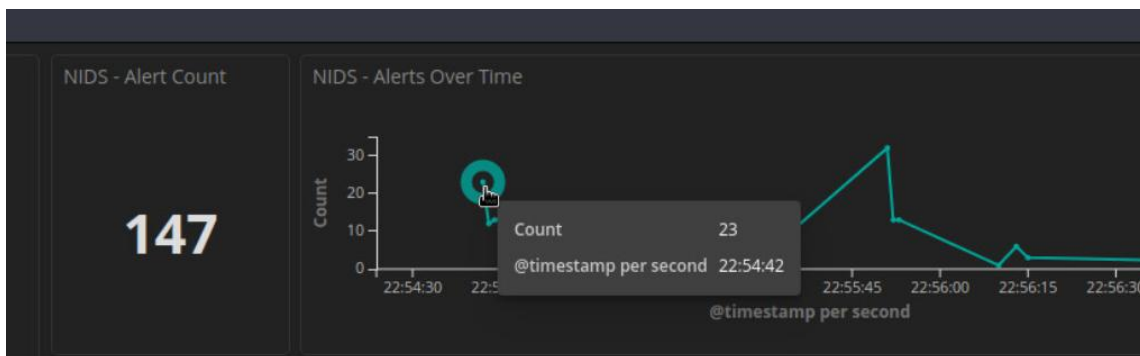
- After narrowing the time range in the main Kibana dashboard, go to the **NIDS** Alert Data dashboard by clicking NIDS.



- 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.



- 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 Kibana dashboard for NIDS alerts. The 'Alert Data' section shows a total count of 147. The 'NIDS Alerts - Category' section shows a bar chart for 'current\_events'. The 'NIDS - Alerts Over Time' section shows a line graph of alert counts over time. The 'NIDS Alerts' section shows a list of alerts. The first event is expanded, showing details for the alert at 22:54:43.000.

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	bKR2kXIbXqASK9Rj3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	baR2kXIbXqASK9Rj3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bqR2kXIbXqASK9Rj3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	bvR2kXIbXqASK9Rj3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	ckR2kXIbXqASK9Rj3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	caR2kXIbXqASK9Rj3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	cqR2kXIbXqASK9Rj3jKE

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

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

What is the source IP address in the alert?

What is the destination IP address in the alert?

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

What is the classification of the alert?

What is the destination geo country name?

- 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?

What is the severity of the exploit?

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

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!

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

Limited to 10 results. Refine your search. 1-10 of 35

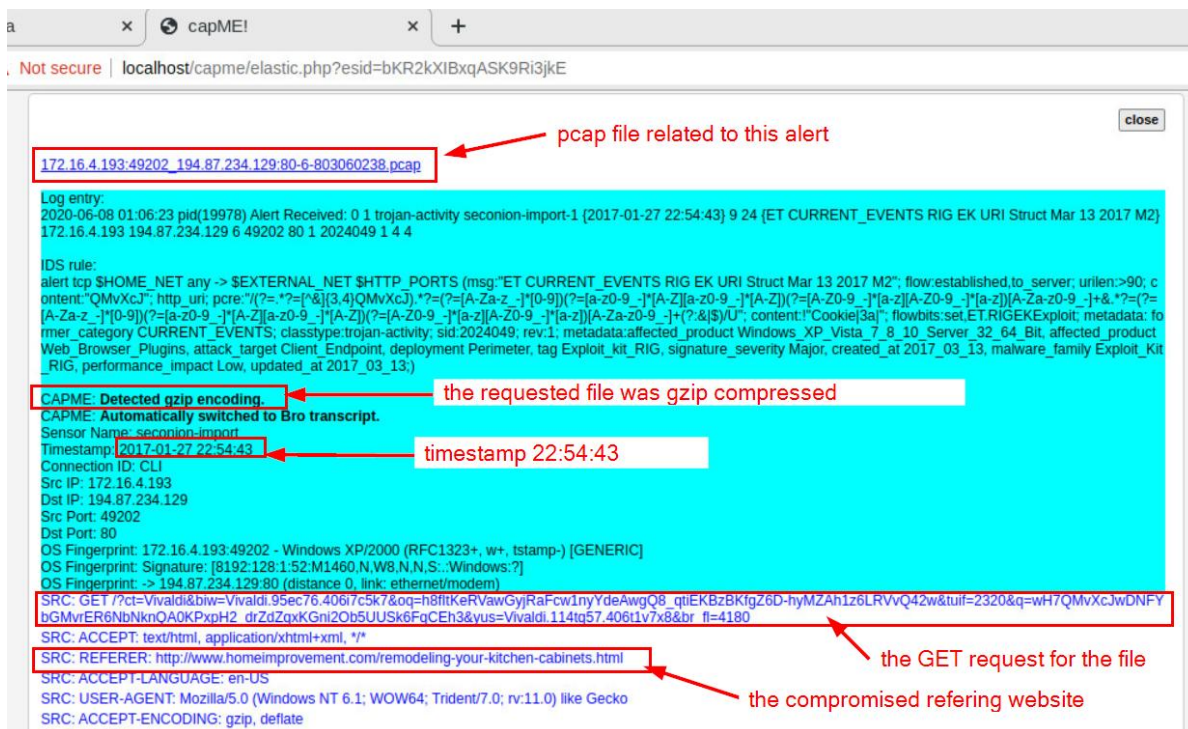
Time	source_ip	source_port	destination_ip	destination_port	_id
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bKR2kXI8xqASK9Ri3jkE

Table JSON View surrounding documents View single document

@timestamp	January 27th 2017, 22:54:43.000
@version	1
_id	bKR2kXI8xqASK9Ri3jkE
_index	seconion:logstash-import-2017.01.27
_score	-
_type	doc

## Lab - Investigating a Malware Exploit

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.



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?

What URL did the browser refer the user to?

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.

- Close the CapME! browser tab.
- From the top of the NIDS Alert Dashboard click the **HTTP** entry located under **Zeek Hunting** heading.
- 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**.
- Scroll down to the HTTP - Sites section of the dashboard.

What are some of the websites that are listed?

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?

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

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

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

### 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.
- 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.

- 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.

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

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

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



### 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.

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2							
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-...	Event History Transcript Transcript (force new) Wireshark Wireshark (force new)	2:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...		2:54:42	139.59.160.143	80	172.16.4.193
RT	15	seconion-...		2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...		2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...		2:54:43	172.16.4.193	49202	194.87.234.129

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?

- 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 Transcript Transcript (force new) Wireshark Wireshark (force new)	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...		2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...		2:54:43	172.16.4.193	49202	194.87.234.129
RT	52	seconion-...		2:54:44	194.87.234.129	80	172.16.4.193
RT	1	seconion-...		2:55:17	172.16.4.193	58978	90.2.1.0

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

What kind of request was involved?

Were any files requested?

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

How the content encoded?

- 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?

What was the first request?

Who was the referrer?

Who was the host server request to?

Was the response encoded?

What was the second request?

Who was the host server request to?

Was the response encoded?

What was the third request?

Who was the referrer?

What was the Content-Type of the third response?

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

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?

- 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?

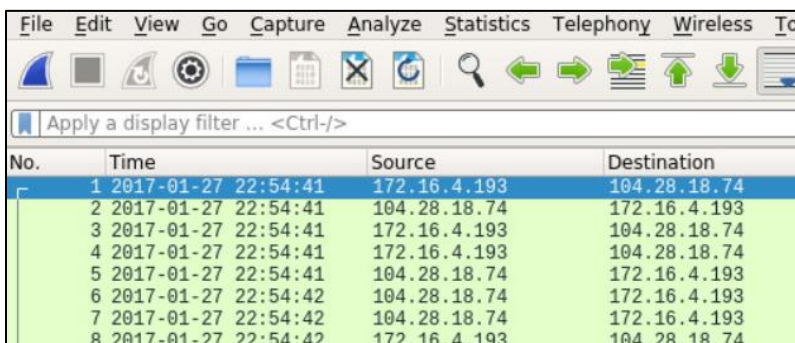
### Part 3: Use Wireshark to Investigate an Attack

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



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

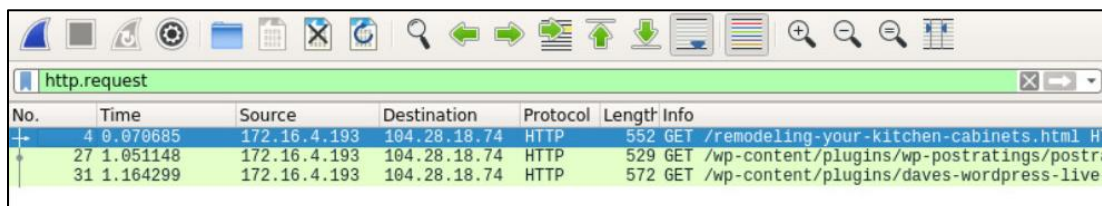
- In Sguil, right-click the alert ID 5.2 (Event Message **ET CURRENT\_EVENTS Evil Redirector Leading to EK Jul 12 2016**) and pivot to select Wireshark from the menu. The pcap that is associated with this alert will open in Wireshark.
- The default Wireshark setting uses a relative time per-packet which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



No.	Time	Source	Destination
1	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
2	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
3	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
4	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
5	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
6	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
7	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
8	2017-01-27 22:54:42	172.16.4.193	104.28.18.74

### Step 2: Investigate HTTP Traffic.

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



No.	Time	Source	Destination	Protocol	Length	Info
4	0.070685	172.16.4.193	104.28.18.74	HTTP	552	GET /remodeling-your-kitchen-cabinets.html HT
27	1.051148	172.16.4.193	104.28.18.74	HTTP	529	GET /wp-content/plugins/wp-postratings/postrat
31	1.164299	172.16.4.193	104.28.18.74	HTTP	572	GET /wp-content/plugins/daves-wordpress-live-

- 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](http://www.homeimprovement.com) website?

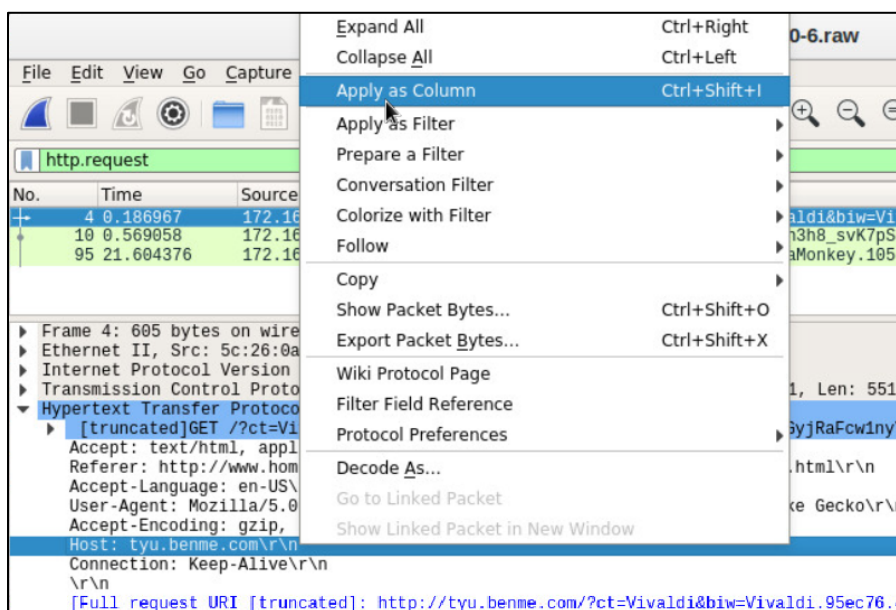
### Step 3: View HTTP Objects.

- 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.
- 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:

What is the http request for?

What is the host server?

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

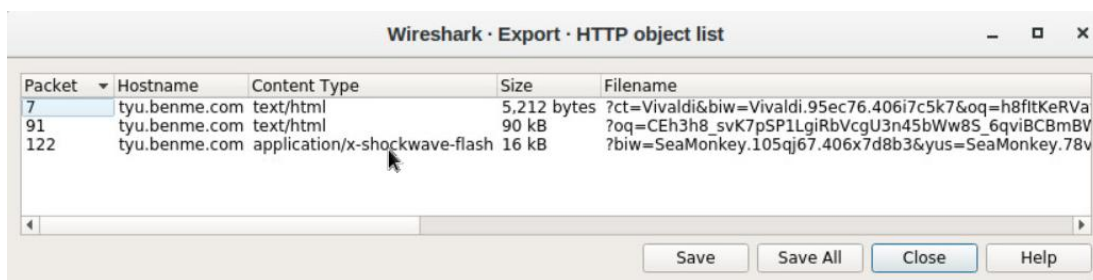


- g. To make room for the Host column right-click the Length column header and uncheck it. This will remove the Length column from the display.
- h. The names of the servers are now clearly visible in the Host column of the packet list.

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

- a. 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.



- 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](http://www.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 **%3fbw=SeaMonkey**. Use the **ls -l** command with **grep** to filter out the filename with the pattern **seamonkey**. The option **-i** ignores the case distinction.

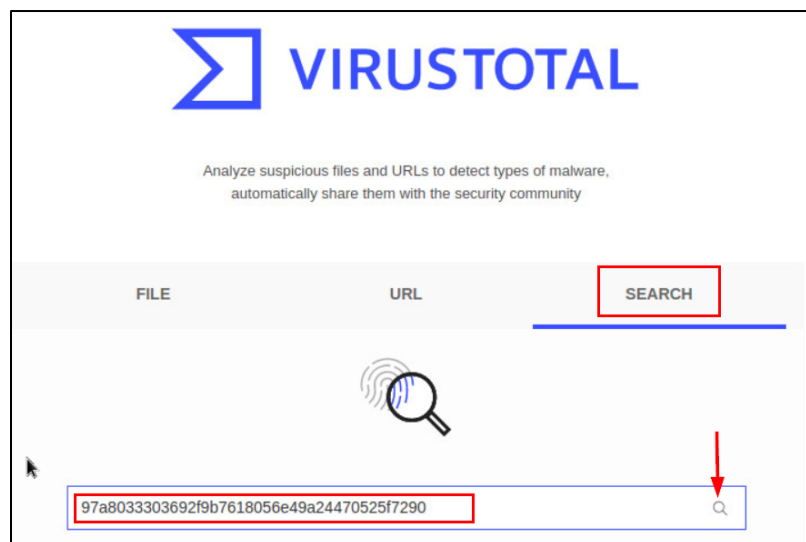
```
analyst@SecOnion:~$ ls -l | grep -i seamonkey
-rw-r--r-- 1 analyst analyst 16261 Jun  9 05:50
%3fbw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYG
OAq3jxbTfgFplIgIUv1Cpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoag9MildZqqZGX_k7fDfF-
qoVzcCgWRxfs&ct=SeaMonkey&tuif=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
%3fbw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl\
=2957&oq=pLLYGOAq3jxbTfgFplIgIUv1Cpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoag9MildZqqZGX_k7fDfF-
qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
97a8033303692f9b7618056e49a24470525f7290 %3fbw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMo
nkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUv1Cpaqq3UbTykKZhJKB9BSKaA9E-
-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.
- e. Open a web browser and go to **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.



- 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?

- 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.

Are there any similarities to the earlier alerts?

Are the files similar? Do you see any differences?

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

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

- 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?

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

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

- j. Go to [virustotal.com](https://www.virustotal.com) and do a URL search for the .top domain used in the attack.

What is the result?

- 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.

What are the filenames if any?