

## SAT1: 007: Malware Traffic Analysis

### Overview

This lab will give an overview of how to analyze malware traffic and respond to an incident resulting from an IDS alert.

In many cases if your investigation reveals an infected computer, you will need to locate and remove the host from the network. Often times, the only information you have available is an IP address to identify the host. The IP address of the offending host is 10.0.1.95.

***Time: 45 Minutes***

### Learning Objectives

Upon completion of this lab, you should be able to:

1. Open a PCAP file and locate possible files in the traffic.
2. Filter web traffic to identify information of interest.
- 3.

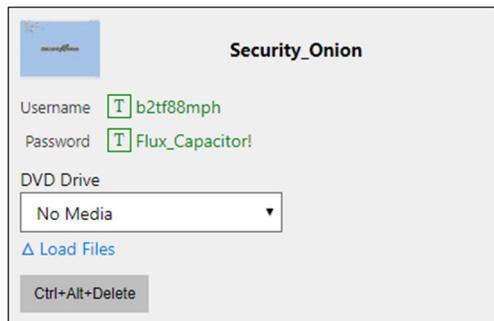
### Resources

The following documents have been provided to assist you in this lab.

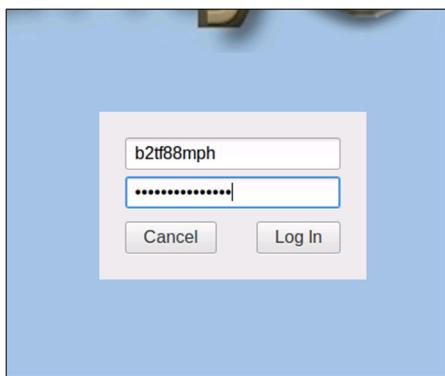
[Wireshark Cheat Sheet](#)

### Log in to the Lab Machine

Select the **Security\_Onion** machine on the Machines Tab.

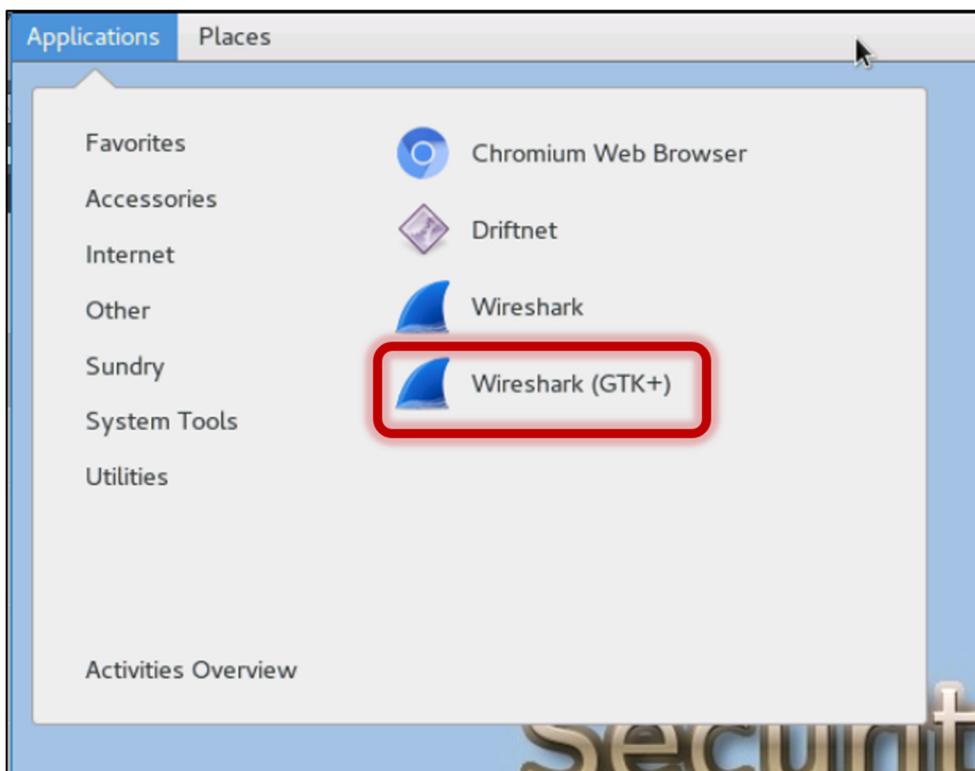


Enter the Username and Password on the **Security\_Onion** machine, and click Log In.



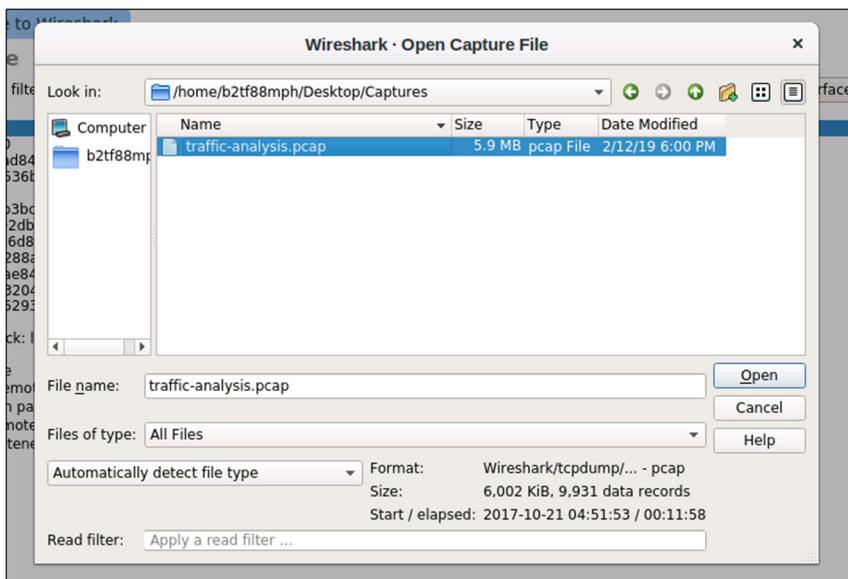
### [Open Wireshark](#)

First, you will need to open the Wireshark application. In **Security Onion**, Wireshark can be found by clicking **Applications**, then move your mouse over **Internet**, and click on **Wireshark (GTK+)**.



On the Main Menu, click on **File** and click on **Open**.

Navigate to the folder on the Desktop named 'Captures' and select the file **traffic-analysis.pcap**.



## 1.0 Traffic Analysis

1.1 In the Wireshark Filter box type: `ip.addr==10.0.1.95 && udp.port==67`.

Time	Src Port	Dest Port	Source	Destination	Host
2017-10-21 04:53:08.0322114	67	68	10.0.1.254	10.0.1.95	
2017-10-21 04:51:53.314839	67	68	10.0.1.254	10.0.1.95	

Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)  
Ethernet II, Src: LinksysG\_f8:1a:ac (00:04:5a:f8:1a:ac), Dst: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f)  
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 10.0.1.95  
User Datagram Protocol, Src Port: 67, Dst Port: 68  
Bootstrap Protocol (ACK)  
Message type: Boot Reply (2)  
Hardware type: Ethernet (0x01)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0xd0ad6ea9  
Seconds elapsed: 0  
Boot flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 10.0.1.95  
Next server IP address: 10.0.1.254  
Relay agent IP address: 0.0.0.0  
Client MAC address: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f)  
Client hardware address padding: 00000000000000000000000000000000

1.2 Look for the traffic at 04:51:53.3. Expand the **Bootstrap Protocol** section and scroll down to see if a hostname exists.



Wireshark

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.1.95 && udp.port==67

Time	Src Port	Dest Port	Source	Destination	Host
2017-10-21 04:53:08.032114	67	68	10.0.1.254	10.0.1.95	
2017-10-21 04:51:53.314839	67	68	10.0.1.254	10.0.1.95	

Frame 2: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)  
Ethernet II, Src: LinksysG\_f8:1a:ac (00:04:5a:f8:1a:ac), Dst: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f)  
Internet Protocol Version 4, Src: 10.0.1.254, Dst: 10.0.1.95  
User Datagram Protocol, Src Port: 67, Dst Port: 68  
Bootstrap Protocol (ACK)  
Message type: Boot Reply (2)  
Hardware type: Ethernet (0x01)  
Hardware address length: 6  
Hops: 0  
Transaction ID: 0xd0ad6ea9  
Seconds elapsed: 0  
Bootp flags: 0x0000 (Unicast)  
Client IP address: 0.0.0.0  
Your (client) IP address: 10.0.1.95  
Next server IP address: 10.0.1.254  
Relay agent IP address: 0.0.0.0  
Client MAC address: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f)  
Client hardware address padding: 000000000000000000000000  
Server host name not given  
Boot file name not given  
Magic cookie: DHCP  
Options (50) DHCP Message Type (ACK)

If the hostname is not available via **DHCP**, it can possibly be found through **NetBios**.

1.3 Next, type `ip.addr==10.0.1.95 && nbns` in the Filter box. If the information is not in the Info, then expand the NetBIOS name service and look for the query.



traffic-analysis.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.1.95 && nbns

Time	Src Port	Dest Port	Source	Destination	Host
2017-10-21 04:51:53.606569	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:53.607018	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:54.088525	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:55.103729	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:55.103741	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:55.587955	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:56.619169	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:56.619183	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:57.087782	137	137	10.0.1.95	10.0.1.1	
2017-10-21 04:51:58.151914	137	137	10.0.1.95	10.0.1.255	
2017-10-21 04:51:58.152014	137	137	10.0.1.95	10.0.1.255	
2017-10-21 04:51:58.650656	137	137	10.0.1.95	10.0.1.255	
2017-10-21 04:51:58.931947	137	137	10.0.1.95	10.0.1.255	

▶ Frame 6: 110 bytes on wire (880 bits), 110 bytes captured (880 bits)  
▶ Ethernet II, Src: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f), Dst: LinksysG\_f8:1a:ac (00:04:5a:f8:1a:ac)  
▶ Internet Protocol Version 4, Src: 10.0.1.95, Dst: 10.0.1.1  
▶ User Datagram Protocol, Src Port: 137, Dst Port: 137  
▼ NetBIOS Name Service  
    Transaction ID: 0xa231  
    Flags: 0x2900, Opcode: Registration, Recursion desired  
    Questions: 1  
    Answer RRs: 0  
    Authority RRs: 0  
    Additional RRs: 1  
    ▼ Queries  
        ▶ DELOREAN-PC<00>; type NB, class IN  
    , Additional records

1.4 Now we have a host name. You can also find Windows hosts by using `ip.addr==10.0.1.95 && netbios` which in this case returned no information.

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr==10.0.1.95 && netbios Expression... Clear Apply

Src Port	Dest Port	Time	Source	Destination	Host
No Data Found using this search.					

You can also use `ip.addr==10.0.1.95 && smb`, if **DHCP** or **NBNS** traffic is not providing the proper results. Using these search methods, we have also obtained the name of the workgroup for the computer.



At this point, you should have the MAC address ([60:a4:4c:6a:b2:1f](#)), IP addresss ([10.0.1.95](#)), and DELOREAN-PC as a host name.

traffic-analysis.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.0.1.95 && smb

Time	Src Port	Dest Port	SOURCE	Destination	Host
2017-10-21 05:02:17.757112	138	88	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 05:00:45.375796	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:58:16.022481	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:56:15.172094	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:55:45.265568	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:54:45.267089	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:54:11.721238	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:53:45.257342	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:53:45.256222	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:53:45.256082	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:53:33.350913	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:53:32.351058	138	138	10.0.1.95	10.0.1.255	10.0.1.255
2017-10-21 04:53:31.351040	138	138	10.0.1.95	10.0.1.255	10.0.1.255

Frame 6046: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)  
Ethernet II, Src: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f) Dst: Broadcast (ff:ff:ff:ff:ff:ff)  
Internet Protocol Version 4, Src: 10.0.1.95, Dst: 10.0.1.255  
User Datagram Protocol, Src Port: 138, Dst Port: 138  
NetBIOS Datagram Service  
SMB (Server Message Block Protocol)  
SMB MailSlot Protocol  
Microsoft Windows Browser Protocol  
    Command: Local Master Announcement (0x0f)  
    Update Count: 0  
    Update Periodicity: 8 minutes  
    Host Name: DELOREAN-PC  
    Windows  
    OS Major Version: 10  
    OS Minor Version: 0  
    Server Type: 0x00051003, Workstation, Server, NT Workstation, Potential Browser, Master Browser  
    Browser Protocol Major Version: 15  
    Browser Protocol Minor Version: 1  
    Signature: 0xaaa55  
    Host Comment:

## 2.0 Filtering Web Traffic

2.1 In the Filter box type `http.request`

File Edit View Go Capture Analyze Sta

http.request



2.2 Select any traffic, expand the **Hypertext Transfer Protocol** section.

File Edit View Go Capture Analyze Statistics Telephony Tools

Filter: http.request

Src	Port	Dest	Port	Time	Source	Destination
49670		80	2.154223		10.0.1.95	23.79.213.
49675		80	2.849235		10.0.1.95	23.79.207.
49678		80	8.849067		10.0.1.95	23.79.207.
49680		80	8.861514		10.0.1.95	23.79.213.
49691		80	54.503138		10.0.1.95	107.180.4.
49670		80	76.826050		10.0.1.95	23.79.207.
49672		80	77.081786		10.0.1.95	23.79.213.
49679		80	83.146545		10.0.1.95	23.79.207.
49681		80	83.149429		10.0.1.95	23.79.213.
57622		80	130.175371		10.0.1.95	35.198.16.
61982		80	171.320010		10.0.1.95	35.198.16.
55225		80	185.920433		10.0.1.95	35.198.16.

Frame 21: 269 bytes on wire (2152 bits), 269 bytes captured  
Ethernet II, Src: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f), Dst:  
Internet Protocol Version 4, Src: 10.0.1.95, Dst: 23.79.213.  
Transmission Control Protocol, Src Port: 49670, Dst Port: 80  
Hypertext Transfer Protocol  
GET /singletile/summary/alias/experiencebyname/today?marke  
Connection: Keep-Alive\r\nUser-Agent: Microsoft-WNS/10.0\r\nHost: cdn.content.prod.cms.msn.com\r\n\r\n[Full request URI: http://cdn.content.prod.cms.msn.com/sin  
[HTTP request 1/1]  
[Response in frame: 26]



2.3 Look at User Agent: Microsoft-WNS/10.0 – This shows us that the host is a Windows 10 machine.

Screenshot of Wireshark showing network traffic analysis for 'traffic-analysis.pcap'. The 'http.request' tab is selected. A specific request is highlighted with a red box, showing the following details:

Frame 9652: 387 bytes on wire (3096 bits), 387 bytes captured (3096 bits)  
Ethernet II, Src: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f), Dst: Linksys6\_f8:1a:ac (00:04:5a:f8:  
Internet Protocol Version 4, Src: 10.0.1.95, Dst: 162.244.35.36  
Transmission Control Protocol, Src Port: 61357, Dst Port: 80, Seq: 348, Ack: 13730, Len: 333  
HTTP/1.1 200 OK [HTTP request 2/2]  
[Full request URI: http://krep2010123.tk/2umber-888-779-0030]

The User-Agent field is highlighted and shows: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Time	Src Port	Dest Port	Source	Destination
2017-10-21 05:03:31.554227	61357	80	10.0.1.95	162.244.35.36
2017-10-21 05:03:31.467415	61356	80	10.0.1.95	162.244.35.36
2017-10-21 05:03:26.358254	61272	80	10.0.1.95	173.194.206.113
2017-10-21 05:03:26.109925	61357	80	10.0.1.95	162.244.35.36
2017-10-21 05:03:26.109908	61356	80	10.0.1.95	162.244.35.36
2017-10-21 05:03:25.807518	61356	80	10.0.1.95	162.244.35.36
2017-10-21 05:03:25.102407	61354	80	10.0.1.95	162.244.35.33
2017-10-21 05:03:24.730303	61352	80	10.0.1.95	104.16.25.235
2017-10-21 05:03:24.641913	61282	80	10.0.1.95	34.206.190.189
2017-10-21 05:03:24.640717	61279	80	10.0.1.95	34.206.190.189
2017-10-21 05:03:24.495436	61279	80	10.0.1.95	34.206.190.189
2017-10-21 05:03:14.523742	61279	80	10.0.1.95	34.206.190.189
2017-10-21 05:03:12.967056	61250	80	10.0.1.95	23.56.3.183

2.4 Take a few moments and look at the traffic you have found. See anything interesting?

2.5 The request to jgbennett.com looks interesting as it appears that an executable file was downloaded.

Screenshot of Wireshark showing network traffic analysis for 'traffic-analysis.pcap'. The 'http.request' tab is selected. A specific request is highlighted with a red box, showing the following details:

Frame 559: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits)  
Ethernet II, Src: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f), Dst: Linksys6\_f8:1a:ac (00:04:5a:f8:  
Internet Protocol Version 4, Src: 10.0.1.95, Dst: 107.180.41.148  
Transmission Control Protocol, Src Port: 49691, Dst Port: 80, Seq: 1, Ack: 1, Len: 98  
HTTP/1.1 200 OK [HTTP request 1/1]  
[Full request URI: http://jgbennett.com/3cgconsulting.com/30\_723bio\_152.exe]

The User-Agent field is highlighted and shows: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Time	Src Port	Dest Port	Source	Destination
2017-10-21 05:02:28.320115	61243	80	10.0.1.95	173.194.206.94
2017-10-21 05:02:28.321282	61242	80	10.0.1.95	173.194.206.94
2017-10-21 05:02:28.324182	61244	80	10.0.1.95	173.194.206.94
2017-10-21 05:02:28.393984	61262	80	10.0.1.95	173.194.206.94
2017-10-21 05:02:28.389437	61267	80	10.0.1.95	23.61.187.27
2017-10-21 05:03:25.102407	61354	80	10.0.1.95	162.244.35.33
2017-10-21 05:03:21.685067	61322	80	10.0.1.95	68.67.178.199
2017-10-21 04:52:47.816641	49691	80	10.0.1.95	107.180.41.148
2017-10-21 05:03:25.807518	61356	80	10.0.1.95	162.244.35.36
2017-10-21 05:03:26.109908	61356	80	10.0.1.95	162.244.35.36
2017-10-21 05:03:26.109925	61357	80	10.0.1.95	162.244.35.36
2017-10-21 05:03:31.554227	61357	80	10.0.1.95	162.244.35.36



2.6 Right-click and select **Follow TCP Stream**. We can see that it was an executable that was downloaded by looking at the magic number.

Wireshark · Follow TCP Stream (tcp.stream eq 20) · traffic-analysis.pcap

```
GET /3cgconsulting.com/30_723bio_152.exe HTTP/1.1
Host: jgbennett.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Sat, 21 Oct 2017 04:52:49 GMT
Server: Apache
Last-Modified: Thu, 19 Oct 2017 12:45:16 GMT
ETag: "1b601f0-f000-55be5ba646d3a"
Accept-Ranges: bytes
Content-Length: 61440
Vary: Accept-Encoding,User-Agent
Keep-Alive: timeout=5
Connection: Keep-Alive
Content-Type: application/x-msdownload

MZ...@.....!This program
cannot be run in DOS mode.

$..../
S..k2..k2...=..i2..bJ8.12..k2..J2...D..n2...D6.j2..Richk2.....PE..L.....kY.....
...
..&.....-.....@...@...
...
2..P.....text..RS.....&.....
....data.....@.....*.....@.....
.....
.....
.....
$3.....B3..N3..f3..r3..3..3..3..3..3..3..3..3..04..
4..4.....<"&!78&>
9%9+.)366%)."56("....to.\J|SSFVHEb_FPK0..r^n\AGLAUG1FOCDL.....3
.QT%..
?..]@3%.....
.....
./.....xF^Y_JDyTHP@AWeY.....rBVSAQgDV[^INK..0.*-;
8.....pSAgJAEURzTN^YMWU_r.....!..". ... .....3..&
.7...%. ;.?#..9...$/.....
trnr.mqttUvhedsp.cD_qZYGCM]xH.....bASvS0@cIH]KZ[..
%.....@.....@.....p..0..1.....@.....H..@.....0..@.....@.....@.....@.....
....@.m.
```

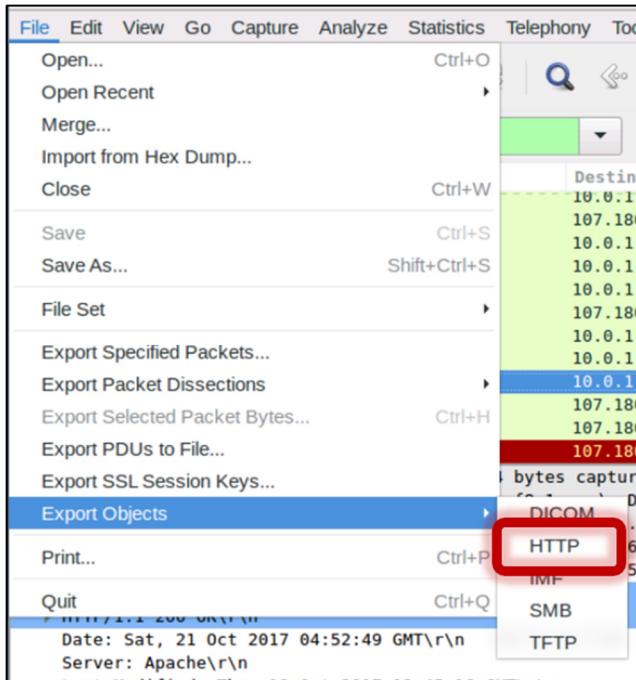
Packet 559. 1 client pkt, 51 server pkts, 1 turn. Click to select.

Entire conversation (61 kB) Show and save data as ASCII Stream 20 Find Next

Filter Out This Stream Print Save as... Back Close Help



2.7 Using Wireshark, we can extract the file from the TCP stream. In Wireshark, click on **File**, then move your mouse over **Export Objects**, then click on **HTTP**.



2.8 This will produce an **HTTP Object List**.

Packet num	Hostname	Content Type	Size	Filename
26	cdn.content.prod.cms.msn.com	text/xml	1,194 bytes	today?market=e
113	tile-service.weather.microsoft.com	text/xml	4,266 bytes	preinstall?region
255	tile-service.weather.microsoft.com	text/xml	4,266 bytes	preinstall?region
265	cdn.content.prod.cms.msn.com	text/xml	1,194 bytes	today?market=e
628	jgbennett.com	application/x-msdownload	61 kB	30_723bio_152.e
710	tile-service.weather.microsoft.com	text/xml	4,266 bytes	preinstall?region
734	cdn.content.prod.cms.msn.com	text/xml	1,194 bytes	today?market=e
974	tile-service.weather.microsoft.com	text/xml	4,266 bytes	preinstall?region
983	cdn.content.prod.cms.msn.com	text/xml	1,194 bytes	today?market=e
1072	amellet.bit		1,584 bytes	a
1345	amellet.bit		1,584 bytes	a
1512	amellet.bit		240 bytes	html
1645	amellet.bit		240 bytes	html
1785	amellet.bit		368 bytes	html
1787	amellet.bit	text/html	1,168 bytes	html
1804	amellet.bit		400 bytes	html
1809	amellet.bit	text/html	4,752 bytes	html
1828	amellet.bit		400 bytes	html
1850	amellet.bit	text/html	17 kB	html
1859	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt

2.9 We can see that there is an executable file associated with jgbennett.com. Select the file and click **Save As**.



Wireshark: HTTP object list					
Packet num	Hostname	Content Type	Size	Filename	
26	cdn.content.prod.cms.msn.com	text/xml	1,194 bytes	today?market=e	
113	tile-service.weather.microsoft.com	text/xml	4,266 bytes	preinstall?region	
255	tile-service.weather.microsoft.com	text/xml	4,266 bytes	preinstall?region	
260	cdn.content.prod.cms.msn.com	text/xml	1,194 bytes	today?market=e	
628	jgbennett.com	application/x-msdownload	51 kB	30_723bio_152.exe	
710	tile-service.weather.microsoft.com	text/xml	4,266 bytes	preinstall?region	
734	cdn.content.prod.cms.msn.com	text/xml	1,194 bytes	today?market=e	
974	tile-service.weather.microsoft.com	text/xml	4,266 bytes	preinstall?region	
983	cdn.content.prod.cms.msn.com	text/xml	1,194 bytes	today?market=e	
1072	amellet.bit		1,584 bytes	a	
1345	amellet.bit		1,584 bytes	a	
1512	amellet.bit		240 bytes	html	
1645	amellet.bit		240 bytes	html	
1785	amellet.bit		368 bytes	html	
1787	amellet.bit	text/html	1,168 bytes	html	
1804	amellet.bit		400 bytes	html	
1809	amellet.bit	text/html	4,752 bytes	html	
1828	amellet.bit		400 bytes	html	
1850	amellet.bit	text/html	17 kB	html	
1859	www.msftconnecttest.com	text/plain	22 bytes	connecttest.txt	

2.10 Save the file in the Captures folder.

### 3.0 Investigate the File

Now that we have found a Windows executable file, we can do some research into the file. We don't want to open an unknown file without precautions. One thing we can do is get the file hash of the executable file we extracted and research the hash value.

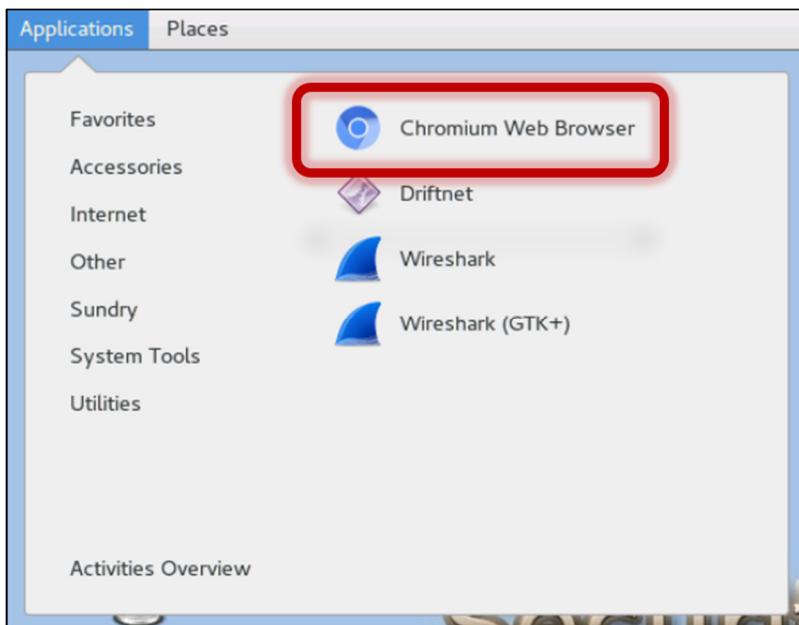
3.1 Open a terminal and navigate to the folder where you saved the executable. Type `shasum -a 256 30_723bio_152.exe` and press Enter.

```
b2tf88mph@b2tf88mph-Virtual-Machine: ~/Desktop/Captures
File Edit View Search Terminal Help
b2tf88mph@b2tf88mph-Virtual-Machine:~$ pwd
/home/b2tf88mph
b2tf88mph@b2tf88mph-Virtual-Machine:~$ ls
analysis  Lab Files  securityonion-kibana.desktop  Videos
Desktop   Music    securityonion-setup.desktop
Documents  Pictures  securityonion-squert.desktop
Downloads  Public   Templates
b2tf88mph@b2tf88mph-Virtual-Machine:~$ cd Desktop/Captures
b2tf88mph@b2tf88mph-Virtual-Machine:~/Desktop/Captures$ ls
30_723bio_152.exe  traffic-analysis.pcap
b2tf88mph@b2tf88mph-Virtual-Machine:~/Desktop/Captures$ shasum -a 256 30_723bio_152.exe
a56876fd456d0737eecc4a8bbe3154b35314ab28accb29abf0df7c518c81a490  30_723bio_152.exe
b2tf88mph@b2tf88mph-Virtual-Machine:~/Desktop/Captures$ 
```



3.2 The file hash should  
be: a56876fd456d0737eecc4a8bbe3154b35314ab28accc29abf0df7c518c81a490

3.3 Open a web browser. The web browser for **Security Onion** is called **Chromium Web Browser**. Click on **Applications**, then move your mouse over **Internet**, and click on **Chromium Web Browser**.



3.4 Navigate to <https://www.reverse.it>

The screenshot shows a web browser window with the following details:

- Address Bar:** Displays the URL <https://www.reverse.it>.
- Header:** Shows navigation icons (back, forward, search, etc.) and the current URL.
- Menu Bar:** Includes links for Home, Submissions, Resources, Jobs, and Contact.
- Content Area:** Features a large blue circular logo with a white network graph icon. To the right of the logo, the text "reverse.it" is displayed in a stylized font.
- Input Fields:** At the bottom left, there are fields for "File/URL" and "Report Search".
- Description:** A text box at the bottom states: "This is a free malware analysis service for the community that detects and analyzes unknown threats using a unique Hybrid Analysis technology."



3.5 You will need to create an account. The only required info is email, password and username.

Free Automated Malware [+](#)

<https://www.reverse.it/advanced-search>

reverse.it Home Submissions Resources Jobs Contact IP

## Advanced Search

This is the advanced search form. Please specify one or more criteria to search through the database

Sorry, advanced searching is disabled for guests. To enable, please [register here](#) or [login](#) if you already have an account.

Filename e.g. invoice.exe

Filetype

Filetype Substring e.g. PE32 executable

3.6 Login to your e-mail to validate the account.

3.7 Login to <https://www.reverse.it>.

File/URL Report Search

Search through 7.4M+ Indicators of Compromise (IOCs).

IP, Domain, Hash... [Search](#)

OR

[Advanced Search](#)



### 3.8 Select **Advanced Search**.

3.9 Select **More Options**, and enter the sha hash we calculated. `a56876fd456d0737eecc4a8bbe3154b35314ab28accb29abf0df7c518c81a490` in the **Sample Context** box, and click **Search Database**.

The screenshot shows the reverse.it search interface with the 'Advanced Search' tab selected. The 'Sample Context' field is highlighted with a red box and contains the SHA256 hash value. Other fields include 'Similar Samples' (set to SHA256), 'imphash', 'ssdeep', 'Authentihash', and 'Environment ID'. A checkbox for 'Has decrypted SSL Traffic' is unchecked. At the bottom are 'Less options' and 'Search database' buttons.

Filter Type	Value
AV Detection	e.g. range like 50-70
AV Family Substring	e.g. nemucod
Hashtag	e.g.#ransomware
Uses Tactic	(dropdown menu)
Uses Technique	(dropdown menu)
Country	(dropdown menu)
Host[:Port]	e.g. 192.168.0.1:8080
Domain	e.g. checkip.dyndns.org
HTTP Request Substring	e.g. google
Similar Samples	SHA256
Sample Context	a56876fd456d0737eecc4a8bbe3154b35314ab28accb29abf0df7c518c81a490
imphash	(empty)
ssdeep	(empty)
Authentihash	(empty)
Environment ID	(empty)
Has decrypted SSL Traffic	<input type="checkbox"/>



3.10 The first couple of files are the same file we extracted from the pcap. But there is a new file as well; if you scroll down you will find a Word document 'Zahlung17.doc'. Note: If you are keen on your German than you will realize that Zahlung translates to payment.

The screenshot shows the reverse.it search interface with the results for an advanced search. The results table includes columns for Timestamp, Input, Threat level, Analysis Summary, Countries, Environment, and Action. A red box highlights the row for 'Zahlung17.doc'.

Timestamp	Input	Threat level	Analysis Summary	Countries	Environment	Action
December 16 2018, 5:44 (CET)	30_723bio_152.exe PE32 executable (GUI) Intel 80386, for MS Windows a56876fd456d0737ecc4abbbe3154b35314ab28accb29abf0df7c518c81a490	malicious	Threat Score: 100/100 AV Detection: 79% Feedel.Generic Matched 59 Indicators	Flag icons for various countries	Windows 7 32 bit	<a href="#">View</a>
October 12 2018, 6:24 (CEST)	30_723bio_152.exe PE32 executable (GUI) Intel 80386, for MS Windows a56876fd456d0737ecc4abbbe3154b35314ab28accb29abf0df7c518c81a490	malicious	Threat Score: 100/100 AV Detection: 79% Feedel.Generic Matched 41 Indicators	Flag icons for various countries	Windows 7 64 bit	<a href="#">View</a>
October 11 2018, 8:35 (CEST)	pe.bin PE32 executable (GUI) Intel 80386, for MS Windows a56876fd456d0737ecc4abbbe3154b35314ab28accb29abf0df7c518c81a490	malicious	Threat Score: 95/100 AV Detection: 100% Matched 74 Indicators	Flag icons for various countries	Windows 7 32 bit	<a href="#">View</a>
October 20 2017, 11:09 (CEST)	Zahlung17.doc Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Co ... c4b26fcdd615e64d3f0f422d14930f76e5dd3e8daec5ececd67ddd191f9856c0	malicious	Threat Score: 100/100 AV Detection: 66% W97MDownloader Matched 68 Indicators	Flag icons for various countries	Windows 7 32 bit	<a href="#">View</a>

3.11 Double-click on the file you wish to learn more about.

3.12 The Risk Assessment section gives a good list of Indicators of Compromise.

The screenshot shows the analysis page for the Word document 'Zahlung17.doc'. It includes sections for Overview, Risk Assessment, and Incident Response. The Risk Assessment section lists various malicious behaviors observed:

Category	Description
Spyware	POSTs files to a webserver
Stealer/Phishing	Scans for artifacts that may help identify the target
Persistence	Injects into explorer
Fingerprint	Injects into remote processes
Evasive	Modifies auto-execute functionality by setting/creating a value in the registry
Network Behavior	Spawns a lot of processes
	Writes data to a remote process
	Reads the active computer name
	Reads the cryptographic machine GUID
	Reads the windows installation date
	Reads the windows product ID
	Scans for artifacts that may help identify the target
	References security related windows services
	Contacts 2 domains and 13 hosts

3.13 Click on the network section link beside Network Behavior.



Risk Assessment	
Persistence	Modifies auto-execute functionality by setting/creating a value in the registry Writes data to a remote process
Fingerprint	Queries process information Reads the active computer name Reads the cryptographic machine GUID Reads the windows installation date Reads the windows product ID
Evasive	Marks file for deletion Possibly tries to evade analysis by sleeping many times References security related windows services Tries to hide tracks of having downloaded a file from the internet Tries to sleep for a long time (more than two minutes)
Network Behavior	Contacts 1 domain and 26 hosts. View the <a href="#">network section</a> for more details.

3.14 This give us a listing of DNS Requests, Contacted Hosts, and HTTP Traffic.

The screenshot shows the reverse.it interface with the 'Network Analysis' tab selected. Under 'DNS Requests', it lists a single entry:

Domain	Address	Registrar	Country
jgbennett.com OSINT	107.180.41.148	GoDaddy.com, LLC Name Server: NS75.DOMAINCONTROL.COM Creation Date: Tue, 05 Apr 2005 18:43:10 GMT	United States

3.15 Download the Indicators by clicking **Download DNS Requests (CSV)**

Did you notice anything else about the traffic? Any web urls we might have seen already?

The screenshot shows the reverse.it interface with the 'Network Analysis' tab selected. Under 'DNS Requests', the 'Download DNS Requests (CSV)' button is highlighted with a red box. The table data is identical to the previous screenshot:

Domain	Address	Registrar	Country
jgbennett.com OSINT	107.180.41.148	GoDaddy.com, LLC Name Server: NS75.DOMAINCONTROL.COM Creation Date: Tue, 05 Apr 2005 18:43:10 GMT	United States



3.16 Compare the traffic to the pcap using Wireshark.

3.17 On the right hand side of the web page, click **File Details**.

malicious

Threat Score: 100/100  
AV Detection: 86%  
Labeled as: Feedel.Generic

Link Twitter E-Mail

Incident Response

Indicators

Malicious (12)  
Suspicious (20)  
Informative (27)

File Details

Screenshots (1)  
Hybrid Analysis (3)  
Network Analysis  
Extracted Strings  
Extracted Files (9)  
Notifications  
Community (1)

Back to top

3.18 You will see the SHA256 hash of the file

c4b26fcdd615e64d3f0f422d14930f76e5dd3e8daec5eecd67cdd191f9856c0

File Details

Zahlung17.doc

All Details:  Off

Filename: Zahlung17.doc  
Size: 332KB (339968 bytes)  
Type: doc  
Description: Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1251, Title: Microsoft, Subject: Microsoft, Author: admin, Template: Normal.dotm, Last Saved By: admin, Revision Number: 4, Name of Creating Application: Microsoft Office Word, Total Editing Time: 01:00, Create Time/Date: Thu Oct 19 14:50:00 2017, Last Saved Time/Date: Thu Oct 19 14:51:00 2017, Number of Pages: 1, Number of Words: 0, Number of Characters: 1, Security: 0  
Architecture: WINDOWS  
SHA256: c4b26fcdd615e64d3f0f422d14930f76e5dd3e8daec5eecd67cdd191f9856c0

Resources

Icon

Classification (TriD)

- 54.2% (.DOC) Microsoft Word document
- 32.2% (.DOC) Microsoft Word document (old ver.)
- 13.5% (.) Generic OLE2 / Multistream Compound File

Incident Response

File Details

Screenshots (9)  
Hybrid Analysis (9)  
Network Analysis  
Extracted Strings  
Extracted Files (19)  
Notifications  
Community (0)

Back to top

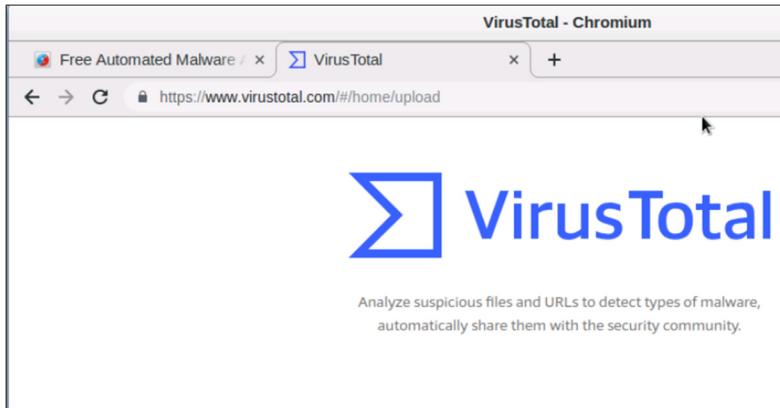
Explore the information available for a bit, see what else you can find that might assist in your investigation!

At this point, you should know that the malware ultimately came from a Word document. However, where did the Word Document come from?



#### 4.0 Online Tools

4.1 Open a web browser or new tab in your current browser and navigate to <https://www.virustotal.com>.



4.2 Click the **Search** tab.





4.3 Paste the file hash for your file in the **Search** bar.

Terms of Service and [Privacy Policy](#). [Learn more](#)'."/>

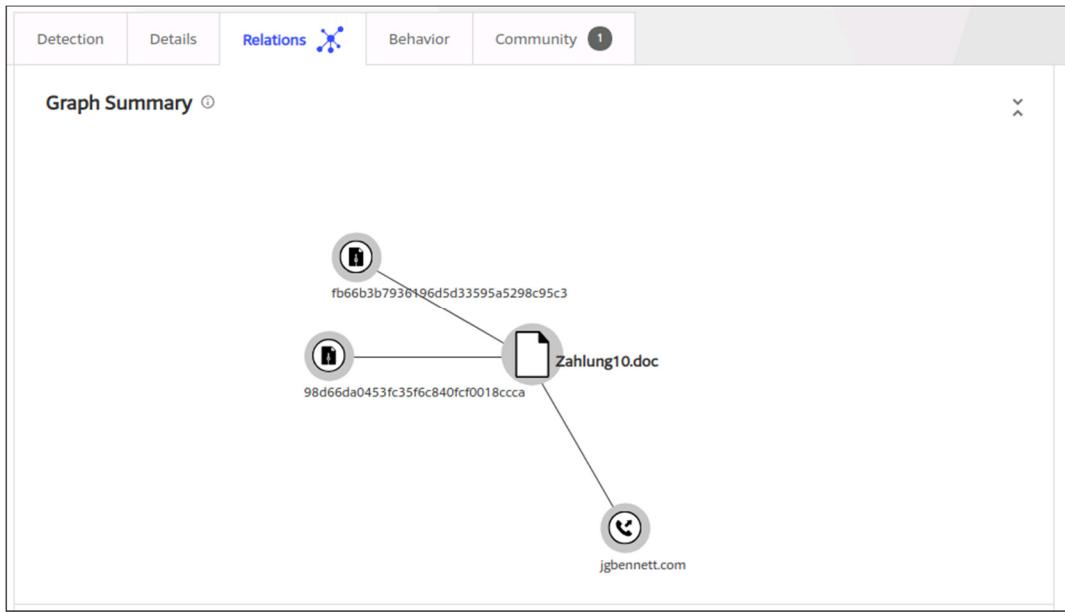
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.

File URL Search

c4b26fcdd615e64d3f0f422d14930f76e5dd3e8daec5eecd67cd191f9856c0

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our [Terms of Service](#) and [Privacy Policy](#). [Learn more](#)

4.4 If you click on the **Relations** tab, you can see the file has two compressed parents.



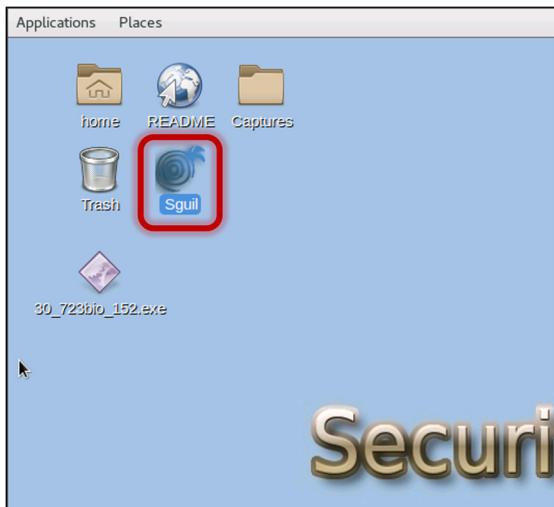
4.5 This means the file was included in some kind of zipped folder. Perhaps a download from the website or an email.



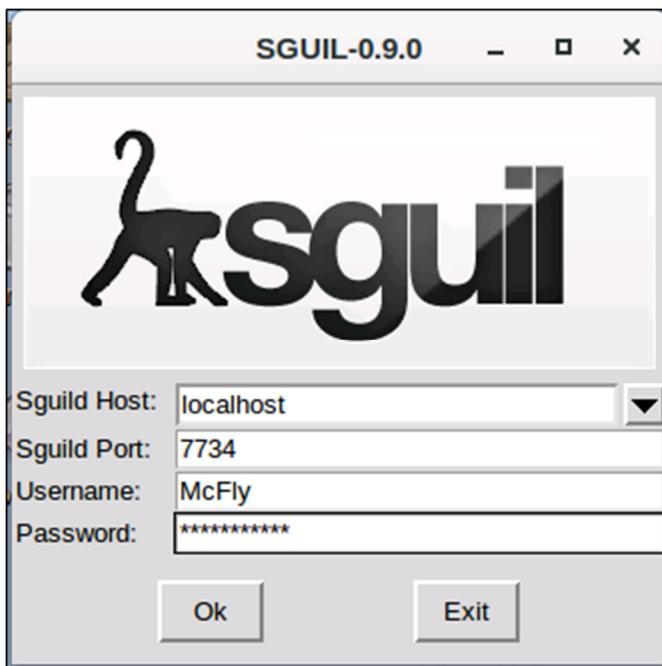
We have a lot of good information to do some research. We know that the malware is reaching out to amellet.bit. A Google search of “amellet.bit malware” will result in the information this malware is related to the **Chthonic Banking Trojan**.

## 5.0 Using Sguil for File Analysis

5.1 Open Sguil from the Desktop.



5.2 Log in using McFly as the Username, and DeLorean88! for the Password.





5.3 Look at the alerts to determine what the malware is doing.

The screenshot shows the SGUIL-0.9.0 interface connected to localhost. The top menu bar includes File, Query, Reports, Sound: Off, ServerName: localhost, UserName: mcify, and UserID: 2. The status bar indicates the date and time: 2019-03-06 21:32:25 GMT. The main window displays a table of RealTime Events with columns: ST, CNT, Sensor, Alert ID, Date/Time, Src IP, Sport, Dst IP, DPort, Pr, and Event Message. Below the table is a packet analysis section with tabs for IP Resolution, Agent Status, Snort Statistics, System Msgs, and Us. It shows a list of hosts (Src IP, Src Name, Dst IP, Dst Name) and a Whois Query dropdown. The bottom half of the window is a packet list with columns: IP, Source IP, Dest IP, Ver, HL, TOS, len, ID, Flags, Offset, TTL, ChkSum. A detailed view of a selected TCP packet is shown, with columns: Source Port, Dest Port, R, R, R, C, S, Y, I, Seq #, Ack #, Offset, Res, Window, Urp, ChkSum. The payload section shows the word "DATA".

5.4 The activity shows that the malware is downloaded and then attempts to beacon. After the beacon, the malware appears to redirect to a fake tech support/help desk page.

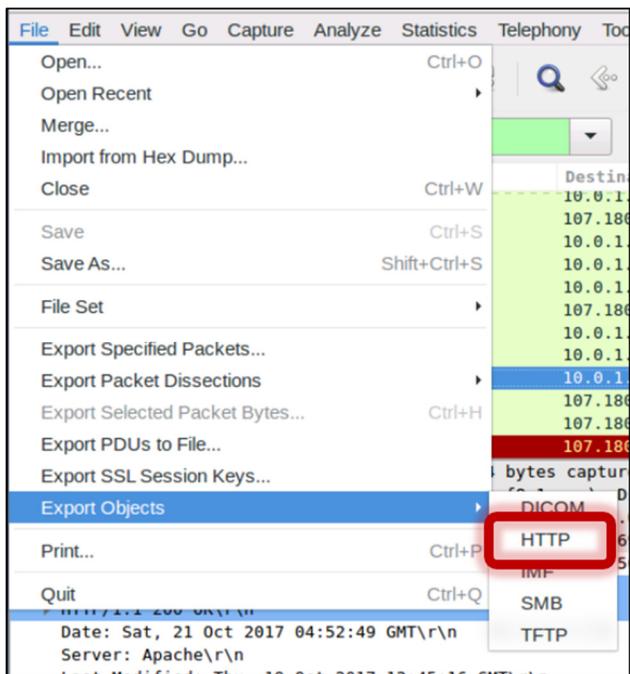
Go back to Wireshark and look at the pcap again using the `http.request` filter.

The screenshot shows the Wireshark interface with a green filter bar containing the text `http.request`. The main pane displays a list of network traffic entries. The columns are: Src Port, Dest Port, Time, Source, and Destination. The list includes several entries from port 49691 to 63017, with destinations ranging from 107.180.41.148 to 35.198.166.246. The entries are color-coded in a green-to-yellow gradient.

Src Port	Dest Port	Time	Source	Destination
49691	80	54.503138	10.0.1.95	107.180.41.148
49670	80	76.826050	10.0.1.95	23.79.207.65
49672	80	77.081786	10.0.1.95	23.79.213.47
49679	80	83.146545	10.0.1.95	23.79.207.65
49681	80	83.149429	10.0.1.95	23.79.213.47
57622	80	130.175371	10.0.1.95	35.198.166.246
61982	80	171.320010	10.0.1.95	35.198.166.246
55225	80	185.920433	10.0.1.95	35.198.166.246
63017	80	187.758261	10.0.1.95	35.198.166.246



5.5 In Wireshark, click on **File**, move your mouse over **Export Objects**, and click on **HTTP**.



5.6 If we scroll down to the bottom of the requests, we see a request from krep2010123.tk, look for the one with a phone number.

Src Port	Dest Port	Time	Source	Destination	Host
512/9	80	681.210239	10.0.1.95	34.206.190.189	dt.clnmde.com
61279	80	691.181933	10.0.1.95	34.206.190.189	dt.clnmde.com
61279	80	691.327214	10.0.1.95	34.206.190.189	dt.clnmde.com
61282	80	691.328410	10.0.1.95	34.206.190.189	dt.clnmde.com
61352	80	691.416800	10.0.1.95	104.16.25.235	m.addthis.com
61354	80	691.788904	10.0.1.95	162.244.35.33	helpcenterforall.bid
61356	80	692.494015	10.0.1.95	162.244.35.36	krep2010123.tk
61356	80	692.795595	10.0.1.95	162.244.35.36	krep2010123.tk
61357	80	692.796422	10.0.1.95	162.244.35.36	krep2010123.tk
61272	80	693.044751	10.0.1.95	173.194.206.113	clients1.google.com
61356	80	698.153912	10.0.1.95	162.244.35.36	krep2010123.tk
61357	80	698.240724	10.0.1.95	162.244.35.36	krep2010123.tk

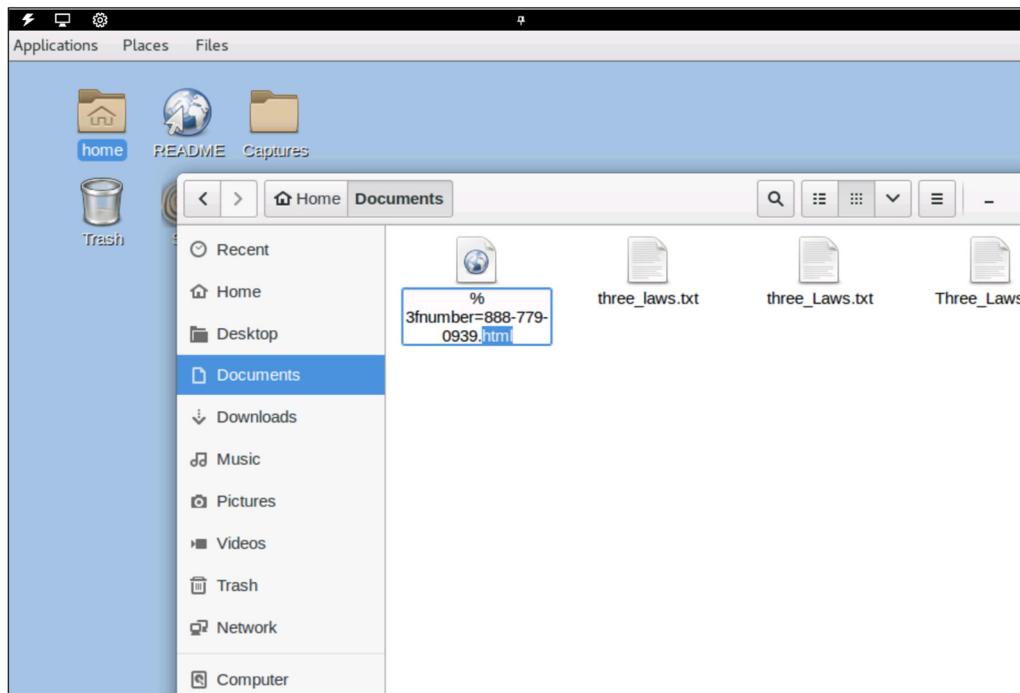
Frame 9649: 257 bytes on wire (2056 bits), 257 bytes captured (2056 bits)  
Ethernet II, Src: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f), Dst: LinksysG\_f8:1a:ac (00:04:5a:f8:1a:ac)  
Internet Protocol Version 4, Src: 10.0.1.95, Dst: 162.244.35.36  
Transmission Control Protocol, Src Port: 61356, Dst Port: 80, Seq: 570, Ack: 4813, Len: 203  
Hypertext Transfer Protocol



5.7 This will produce an **HTTP Object List**, select the file and click **Save As**.

Packet num	Hostname	Content Type	Size	Filename
9310		text/html	218 bytes	
9312		text/html	218 bytes	
9314		text/html	218 bytes	
9316		text/html	218 bytes	
9359	mycdn.media.net	image/jpeg	8,917 bytes	logo2.jpg
9374	mycdn.media.net	text/plain	31 kB	OpenSans_Semibold.eot?
9376	lg3.media.net	text/javascript	15 bytes	bql.php?v=1&hvsid=0000150856214820902917168360383
9386	lg3.media.net	text/javascript	15 bytes	bqi.php?If=3&crid=586486489&pid=8PO1T28XQ&cid=8CL
9392	dt.clnmde.com	image/gif	70 bytes	ptmd?t=%7B%22status%22%3A31%2C%22za%622%3A1%
9397	lg3.media.net	text/javascript	15 bytes	bqi.php?If=4&crid=586486489&pid=8PO1T28XQ&cid=8CL
9401	dt.clnmde.com	image/gif	70 bytes	ptmd?t=%7B%22status%22%3A31%2C%22za%622%3A1%
9468	dt.clnmde.com	image/gif	70 bytes	ptmd?t=%7B%22status%22%3A31%2C%22za%622%3A1%
9493	dt.clnmde.com	image/gif	70 bytes	ptmd?t=%7B%22pet%22%3A56082%2C%22exInd%22%3
9494	dt.clnmde.com	image/gif	70 bytes	ptmd?t=%7B%22status%22%3A31%2C%22za%622%3A1%
9516	helpcenterforall.bid	text/html	0 bytes	?MCPKV8
9533	krep2010123.tk	text/html	4,374 bytes	?number=888-779-0939
9565	krep2010123.tk	image/png	13 kB	defender.png
9579	krep2010123.tk	text/html	18 bytes	css
9581	clients1.google.com	application/ocsp-response	463 bytes	MEkwRzBFMEMwQTAJbgUrDgMCGgUABBTy4Gr5hYoo
9651	krep2010123.tk	text/html	169 bytes	favicon.ico

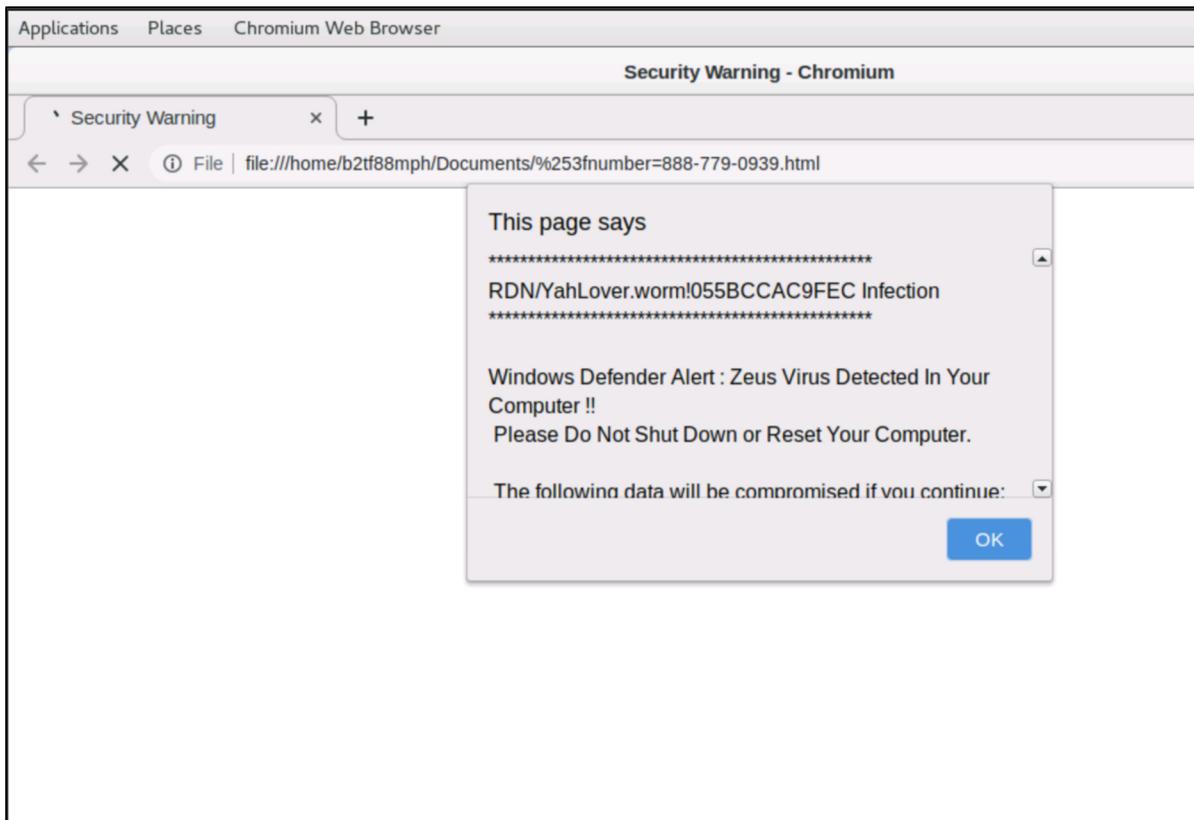
5.8 Navigate to the location where you saved the file and open it. You will need to add the **.html** file extension.





5.9 You should open a fake web page that looks like an anti-virus alert.

What caused the fake anti-virus page?





## 6.0 Continue Investigating

6.1 Right-click the request and select **Follow TCP Stream**.

The screenshot shows the Wireshark interface with a list of network frames. A context menu is open over the 8th frame, which is an HTTP request. The menu options include: Mark Packet (toggle), Ignore Packet (toggle), Set Time Reference (toggle), Time Shift..., Packet Comment..., Manually Resolve Address, Apply as Filter, Prepare a Filter, Conversation Filter, Colorize Conversation, SCTP, Follow TCP Stream (which is highlighted in blue), Follow UDP Stream, Follow SSL Stream, Follow HTTP Stream, and Copy.

6.2 It doesn't appear to have a referrer in the HTTP headers.

The screenshot shows the 'Follow TCP Stream' dialog box. The 'Stream Content' pane displays the raw HTTP response. The 'Keep-Alive' header is highlighted with a red box. The response content includes:

```
HTTP/1.1 404 Not Found
Server: nginx/1.10.2
Date: Sat, 21 Oct 2017 05:03:32 GMT
Content-Type: text/html
Content-Length: 169
Keep-Alive: timeout=3

<html>
<head><title>404 Not Found</title></head>
<body bgcolor="white">
<center><h1>404 Not Found</h1></center>
<hr><center>nginx/1.10.2</center>
</body>
</html>
```

At the bottom of the dialog, there are buttons for Find, Save As, Print, ASCII, EBCDIC, Hex Dump, C Arrays, Raw, Help, Filter Out This Stream, and Close.

6.3 Use the filter ip contains 888-779-0939 and then we can work our way through the traffic flow.



traffic-analysis.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip contains 888-779-0939 Expression... Clear Apply Save

Src Port	Dest Port	Time	Source	Destination	Host
80	61354	691.920509	162.244.35.33	10.0.1.95	
61356	80	692.494015	10.0.1.95	162.244.35.36	krep2010123.tk
80	61356	692.784538	162.244.35.36	10.0.1.95	
80	61356	692.784541	162.244.35.36	10.0.1.95	
61356	80	692.795595	10.0.1.95	162.244.35.36	krep2010123.tk
61357	80	692.796422	10.0.1.95	162.244.35.36	krep2010123.tk
61357	80	698.240724	10.0.1.95	162.244.35.36	krep2010123.tk

▶ Frame 9516: 691 bytes on wire (5528 bits), 691 bytes captured (5528 bits)  
▶ Ethernet II, Src: LinksysG\_f8:1a:ac (00:04:5a:f8:1a:ac), Dst: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f)  
▶ Internet Protocol Version 4, Src: 162.244.35.33, Dst: 10.0.1.95  
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 61354, Seq: 1, Ack: 281, Len: 637  
▶ Hypertext Transfer Protocol  
Line-based text data: text/html (0 lines)

6.4 The first request should be a 302 response.

traffic-analysis.pcap

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip contains 888-779-0939 Expression... Clear Apply Save

Src Port	Dest Port	Time	Source	Destination	Host
80	61354	691.920509	162.244.35.33	10.0.1.95	
61356	80	692.494015	10.0.1.95	162.244.35.36	krep2010123.tk
80	61356	692.784538	162.244.35.36	10.0.1.95	
80	61356	692.784541	162.244.35.36	10.0.1.95	
61356	80	692.795595	10.0.1.95	162.244.35.36	krep2010123.tk
61357	80	692.796422	10.0.1.95	162.244.35.36	krep2010123.tk
61357	80	698.240724	10.0.1.95	162.244.35.36	krep2010123.tk

▶ Frame 9516: 691 bytes on wire (5528 bits), 691 bytes captured (5528 bits)  
▶ Ethernet II, Src: LinksysG\_f8:1a:ac (00:04:5a:f8:1a:ac), Dst: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f)  
▶ Internet Protocol Version 4, Src: 162.244.35.33, Dst: 10.0.1.95  
▶ Transmission Control Protocol, Src Port: 80, Dst Port: 61354, Seq: 1, Ack: 281, Len: 637  
▶ Hypertext Transfer Protocol  
  HTTP/1.1 302 Moved Temporarily\r\n    [Expert Info (Chat/Sequence): HTTP/1.1 302 Moved Temporarily\r\n    Response Version: HTTP/1.1  
    Status Code: 302  
    [status\_code description: Found]  
    Response Phrase: Moved Temporarily  
    Server: nginx/1.10.2\r\n



## 6.5 Follow the TCP Stream and we find the website helpcenterforall.bid

```
Follow TCP Stream (tcp.stream eq 319)

-Stream Content-
GET /index/?MCPKV8 HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: helpcenterforall.bid
Connection: Keep-Alive

HTTP/1.1 302 Moved Temporarily
Server: nginx/1.10.2
Date: Sat, 21 Oct 2017 05:03:26 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Keep-Alive: timeout=3
Expires: Thu, 21 Jul 1977 07:30:00 GMT
Last-Modified: Sat, 21 Oct 2017 05:03:26 GMT
Cache-Control: max-age=0
Pragma: no-cache
Set-Cookie: 00831=%7B%22streams%22%3A%7B%221632%22%3A1508562206%7D%2C%22campaigns%22%3A%7B%22275%22%3A1508562206%7D%2C%22time%22%3A1508562206%7D; expires=Tue, 21-Nov-2017 05:03:26 GMT; Max-Age=2678400; path=/; domain=.helpcenterforall.bid
Location: http://krep2010123.tk/?number=888-779-0939

0

Entire conversation (917 bytes)
Find Save As Print ASCII EBCDIC Hex Dump C Arrays Raw
Help Filter Out This Stream Close
Date: Sat, 21 Oct 2017 05:03:26 GMT\r\n
```

## 6.6 Use the filter for ip contains helpcenterforall.bid

Src Port	Dest Port	Time	Source	Destination	Host
80	61209	634.182649	104.18.61.210	10.0.1.95	
61354	80	691.788904	10.0.1.95	162.244.35.33	helpcenterforall.bid
80	61354	691.920509	162.244.35.33	10.0.1.95	

```
Frame 9516: 691 bytes on wire (5528 bits), 691 bytes captured (5528 bits)
Ethernet II, Src: LinksysG_f8:1a:ac (00:04:5a:f8:1a:ac), Dst: AsustekC_6a:b2:1f (60:a4:4c:6a:b2:1f)
Internet Protocol Version 4, Src: 162.244.35.33, Dst: 10.0.1.95
Transmission Control Protocol, Src Port: 80, Dst Port: 61354, Seq: 1, Ack: 281, Len: 637
Hypertext Transfer Protocol
  HTTP/1.1 302 Moved Temporarily\r\n
    [Expert Info (Chat/Sequence): HTTP/1.1 302 Moved Temporarily\r\n]
      Response Version: HTTP/1.1
      Status Code: 302
      [Status Code Description: Found]
      Response Phrase: Moved Temporarily
      Server: nginx/1.10.2\r\n
      Date: Sat, 21 Oct 2017 05:03:26 GMT\r\n
```



6.7 The first request contains a 200 response.

The screenshot shows the Wireshark interface with a green filter bar at the top containing the text "ip contains helpcenterforall.bid". Below the filter are three rows of network traffic. The first row has blue headers and green bodies. The second row has a blue header and a green body. The third row has a blue header and a green body. The details pane below the traffic list shows a tree structure for frame 6263. The "HTTP/1.1 200 OK\r\n" node is expanded, revealing its children: "Response Version: HTTP/1.1", "Status Code: 200", "[status\_code\_description: OK]", and "Response Phrase: OK". The "Status Code: 200" entry is highlighted with a red rectangular box.

Src Port	Dest Port	Time	Source	Destination	Host
80	61209	634.182649	104.18.61.210	10.0.1.95	
61354	80	691.788904	10.0.1.95	162.244.35.33	helpcenterforall.bid
80	61354	691.920509	162.244.35.33	10.0.1.95	

Frame 6263: 1238 bytes on wire (9904 bits), 1238 bytes captured (9904 bits)  
Ethernet II, Src: LinksysG\_f8:1a:ac (00:04:5a:f8:1a:ac), Dst: AsustekC\_6a:b2:1f (60:a4:4c:6a:b2:1f)  
Internet Protocol Version 4, Src: 104.18.61.210, Dst: 10.0.1.95  
Transmission Control Protocol, Src Port: 80, Dst Port: 61209, Seq: 71182, Ack: 366, Len: 1184  
[59 Reassembled TCP Segments (72365 bytes): #6135(1460), #6136(13), #6137(1460), #6138(1460), #6139(1)  
Hypertext Transfer Protocol  
HTTP/1.1 200 OK\r\n[Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]  
Response Version: HTTP/1.1  
Status Code: 200  
[status\_code\_description: OK]  
Response Phrase: OK

6.8 Follow the TCP stream to find the request came from [www.singlemoms.com](http://www.singlemoms.com)



Follow TCP Stream (tcp.stream eq 174)

Stream Content

```
www.singlemoms.org/grants-for-single-mothers/">Grants for Single Mothers</a></li><li id="menu-item-299" class="menu-item menu-item-type-post_type menu-item-object-page menu-item-299"><a href="http://www.singlemoms.org/scholarships-for-single-mothers-101/">Scholarships for Single Mothers 101</a></li><li id="menu-item-190" class="menu-item menu-item-type-post_type menu-item-object-page menu-item-190"><a href="http://www.singlemoms.org/grants-for-single-mothers-fq/">Grants for Single Mothers F#038;Q</a></li>
5bf
<li id="menu-item-573" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-573"><a href="http://www.singlemoms.org/how-to-do-taxes-as-a-single-mom/">Taxes for Moms 101</a></li><li id="menu-item-614" class="menu-item menu-item-type-post_type menu-item-object-page menu-item-614"><a href="http://www.singlemoms.org/grants-for-single-mothers-in-canada/">Grants for Single Mothers in Canada</a></li></ul></li><li id="menu-item-798" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-798"><a href="http://www.singlemoms.org/rent-assistance-guide/">Rent Assistance</a></li><li id="menu-item-714" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-714"><a href="http://www.singlemoms.org/mortgage-assistance-guide/">Mortgage Assistance</a></li><li id="menu-item-794" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-794"><a href="http://www.singlemoms.org/loans-101-a-complete-guide-to-loans-for-dummies/">Loan Assistance</a></li><li id="menu-item-795" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-795"><a href="http://www.singlemoms.org/a-guide-to-food-assistance-programs-how-to-get-free-food-meals-and-groceries/">Food Assistance</a></li><li id="menu-item-796" class="menu-item menu-item-type-custom menu-item-object-custom menu-item-796"><a href="http://www.singlemoms.org/medical-assistance-guide-get-help-paying-medical-bills/">Medical Assistance</a></li>
```

Entire conversation (113394 bytes)

ASCII  EBCDIC  Hex Dump  C Arrays  Raw

We have now found the offending malware and the offending website.

At this point, we have enough information to provide a thorough narrative and evidence for effective incident response.

Great job, you have completed LAB007!

Thank You, you may now close this module.