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.

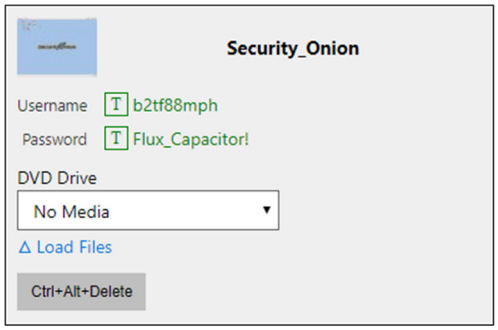
Resources

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

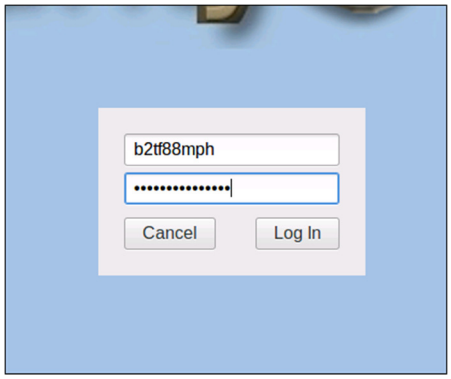
Wireshark Cheat Sheet

Log in to the Lab Machine

Select the **Security_Onion** machine on the Machines Tab.

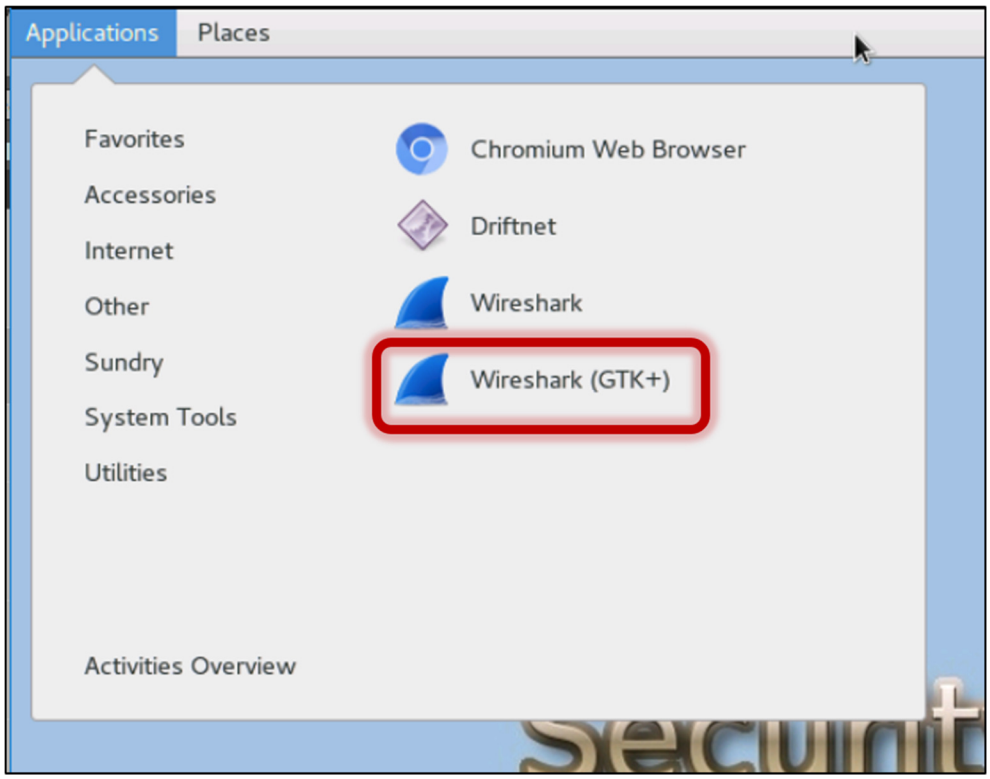


Enter the Username and Password on the **Security_Onion** machine, and click Log In.



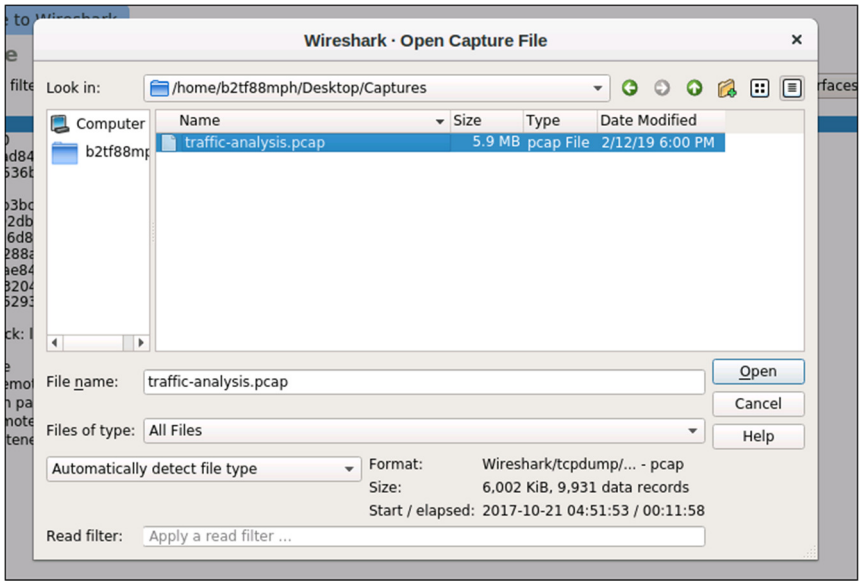
`Open Wireshark`

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+)**.



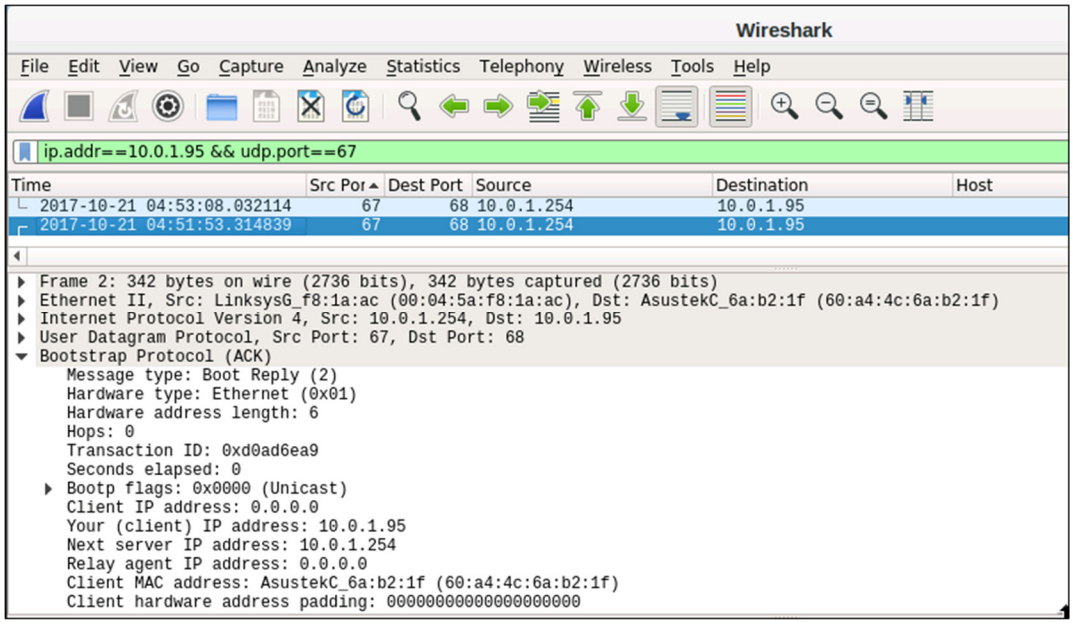
On the Main Menu, click on **File** and click on **Open**.

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

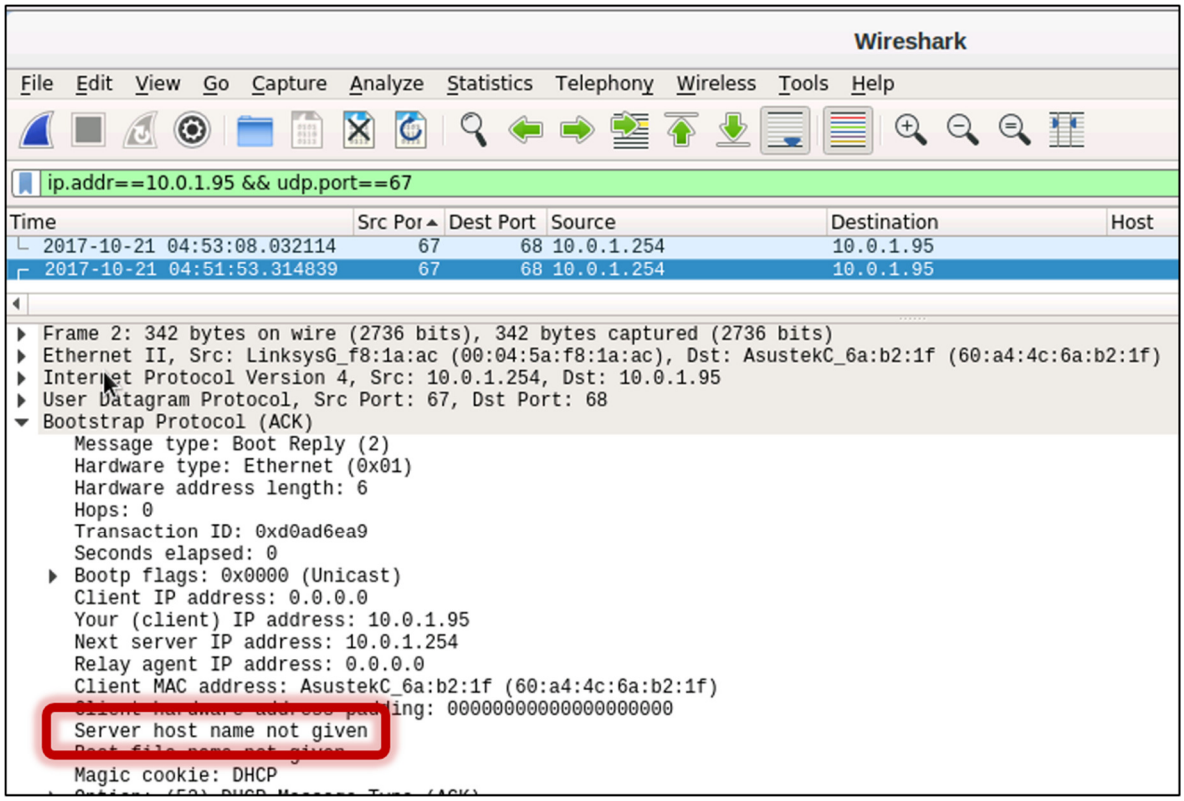


1.0 Traffic Analysis

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

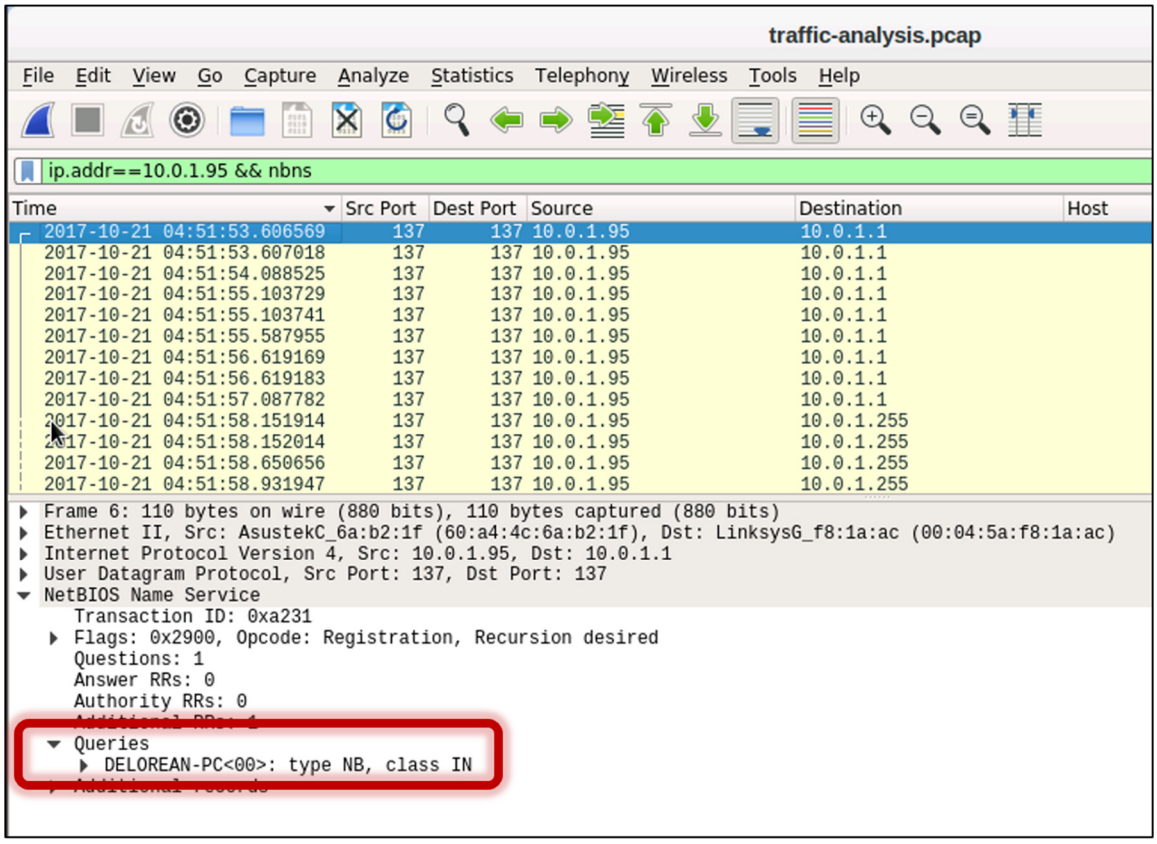


1.2 Look for the traffic at 04:51:53.3. Expand the `Bootstrap Protocol` section and scroll down to see if a hostname exists.

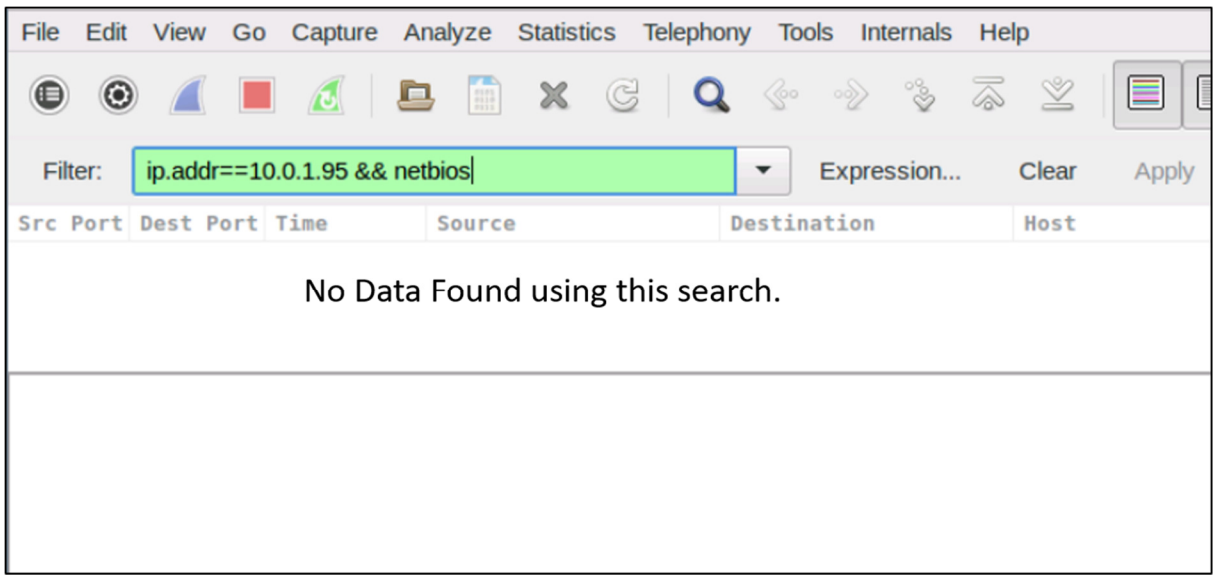


If the hostname is not avialable via **DHCP**, it can possibly be found through **NetBios**.

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.

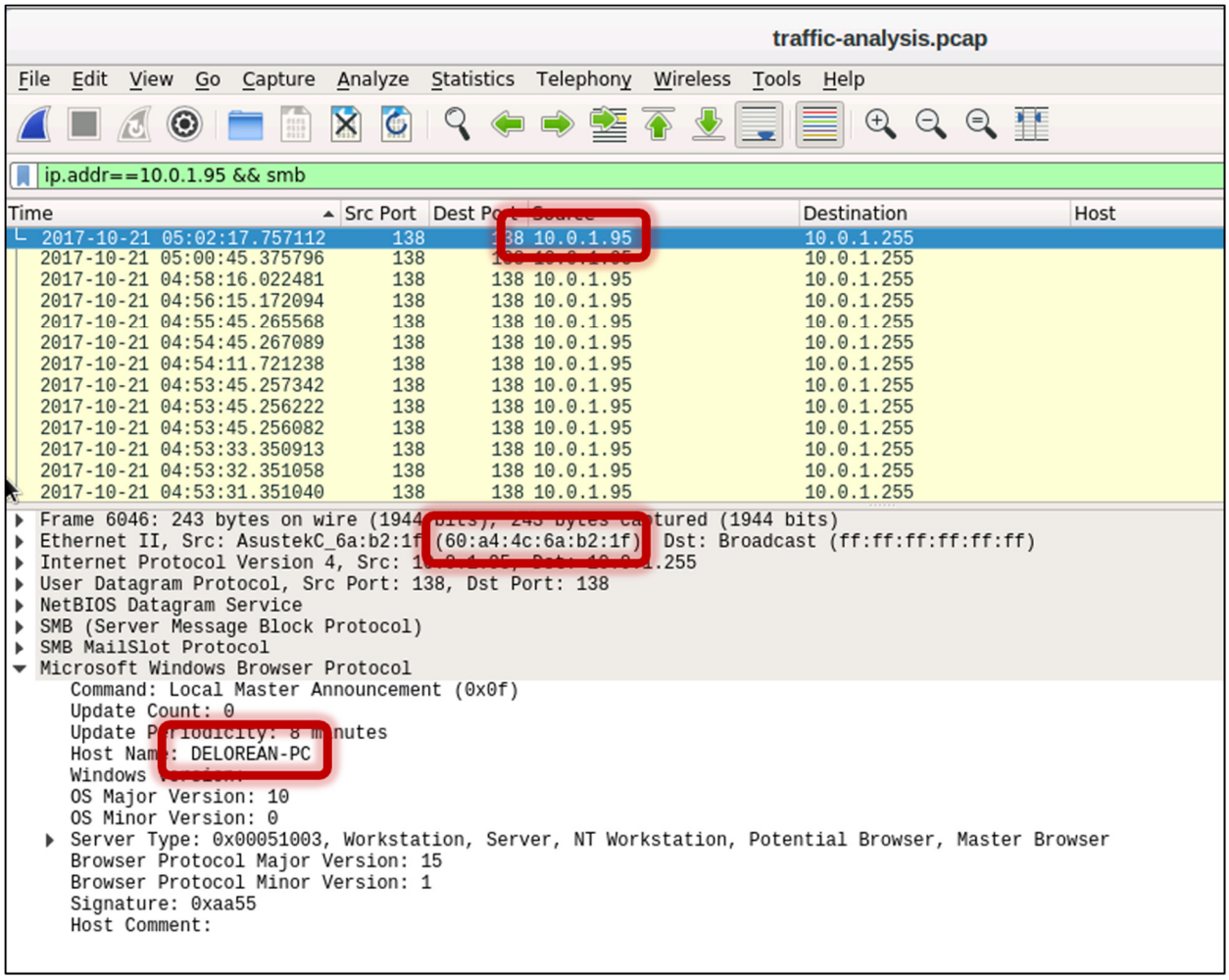


1.4 Now we have a host name. You can also find Windows hosts by using `ip.addr==10.0.1.95 && netbios` which in this case returned no information.



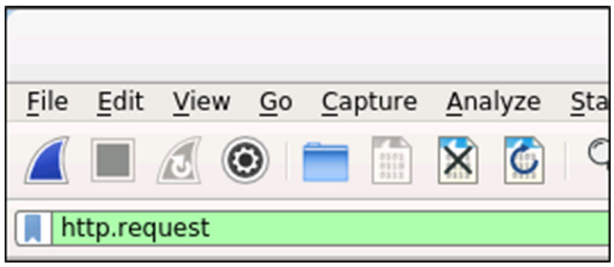
You can also use `ip.addr==10.0.1.95 && smb`, if **DHCP** or **NBNS** traffic is not providing the proper results. Using these search methods, we have also obtained the name of the workgroup for the computer.

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.

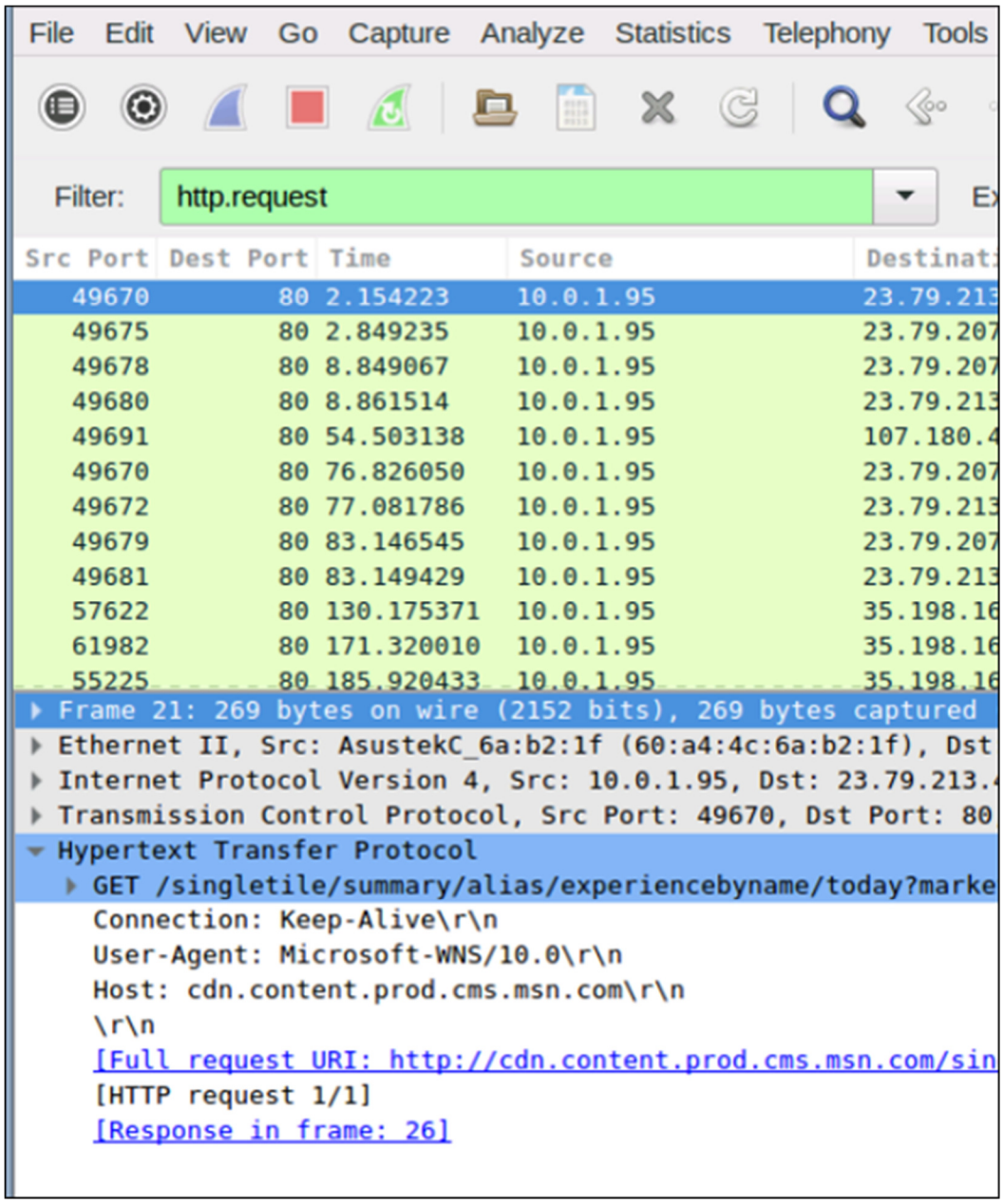


2.0 Filtering Web Traffic

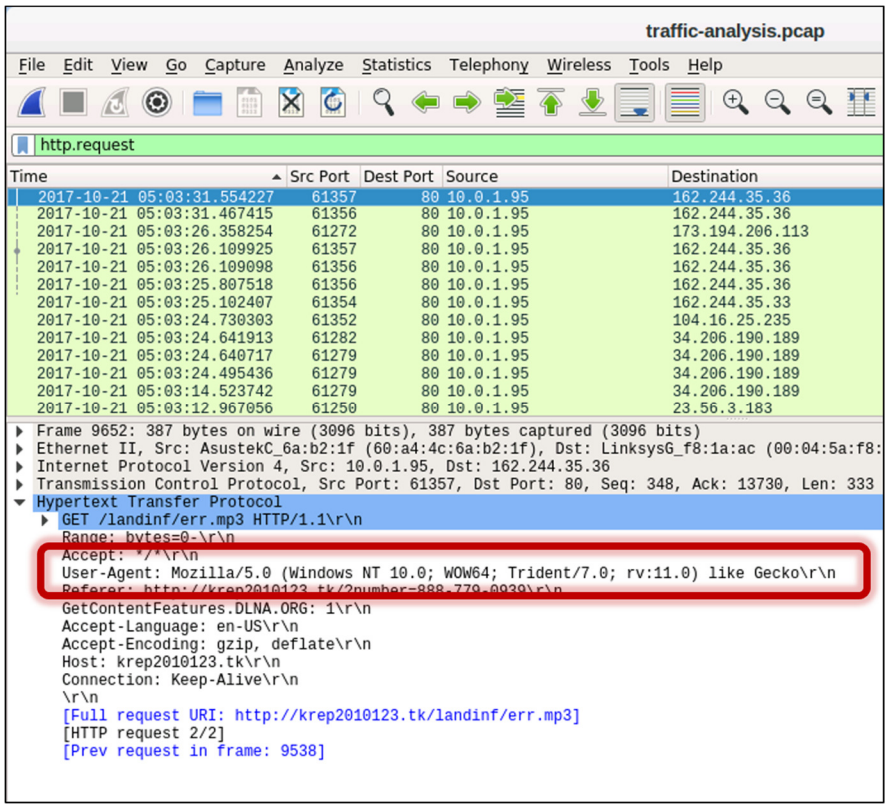
2.1 In the Filter box type `http.request`



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

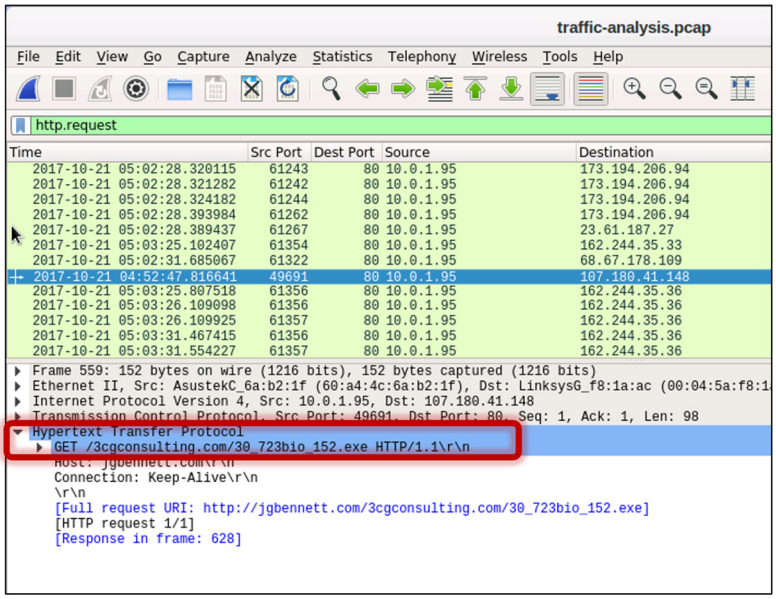


2.3 Look at User Agent: Microsoft-WNS/10.0 – This shows us that the host is a Windows 10 machine.

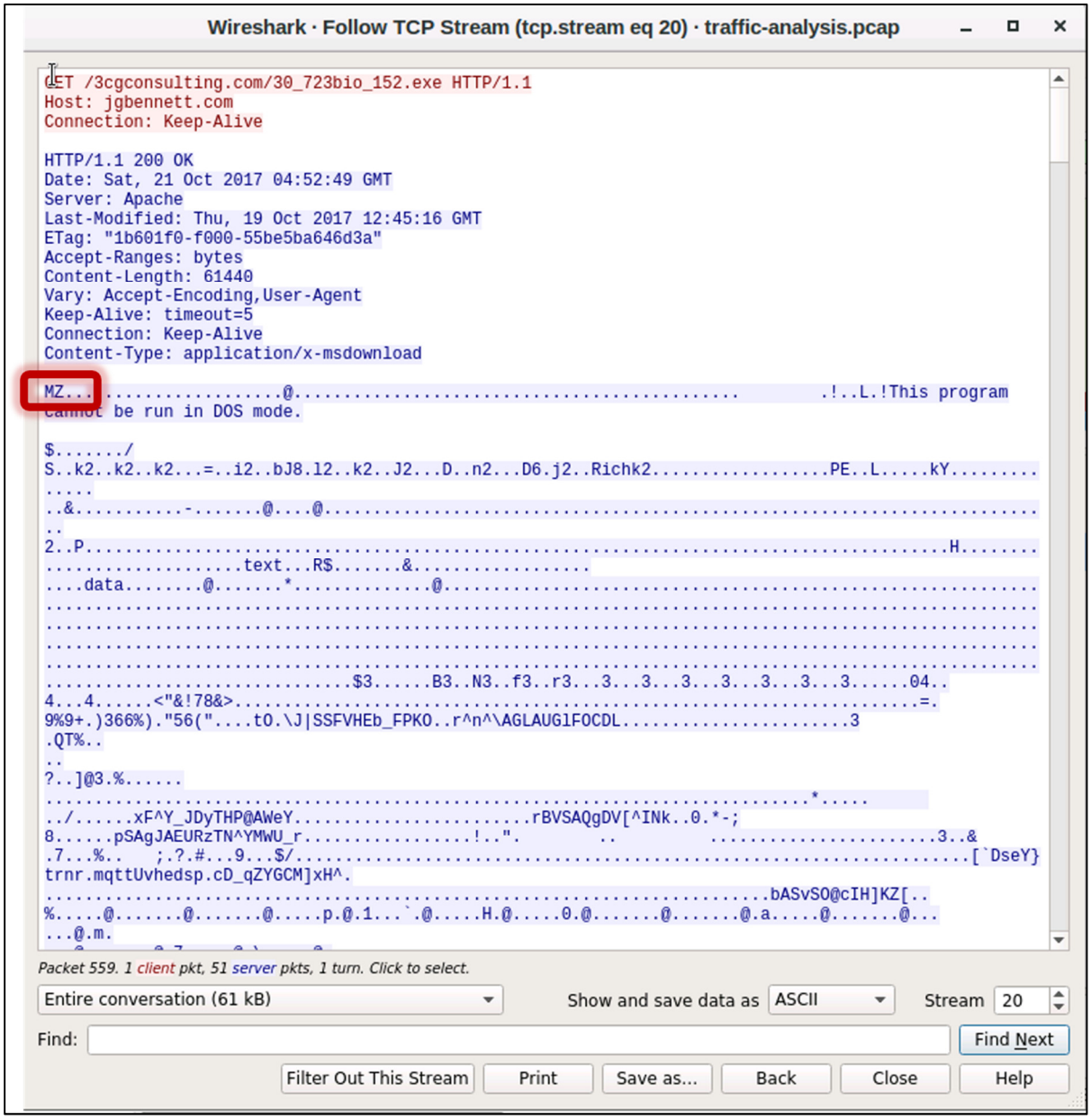


2.4 Take a few moments and look at the traffic you have found. See anything interesting?

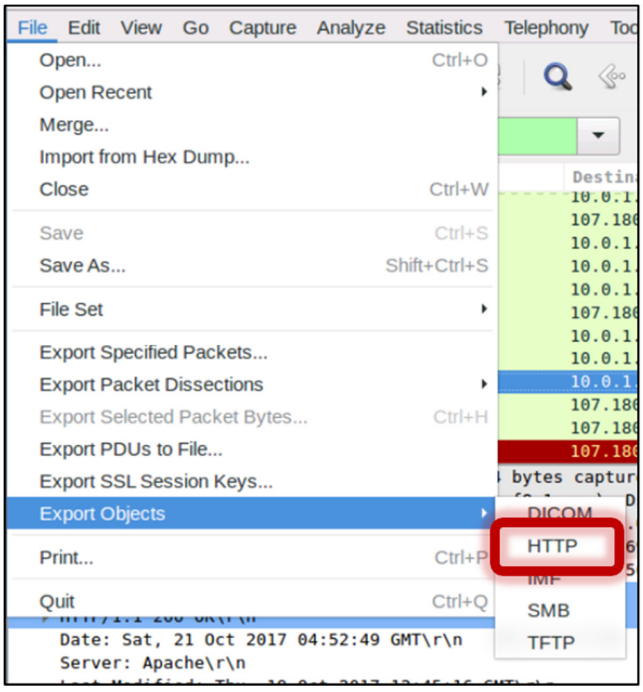
2.5 The request to jgbennett.com looks interesting as it appears that an executable file was downloaded.



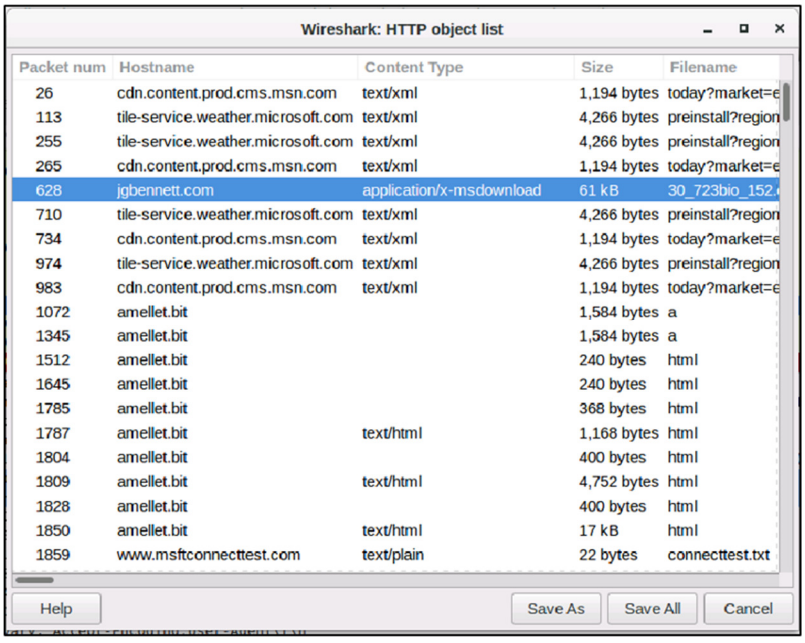
2.6 Right-click and select **Follow TCP Stream**. We can see that it was an executable that was downloaded by looking at the magic number.



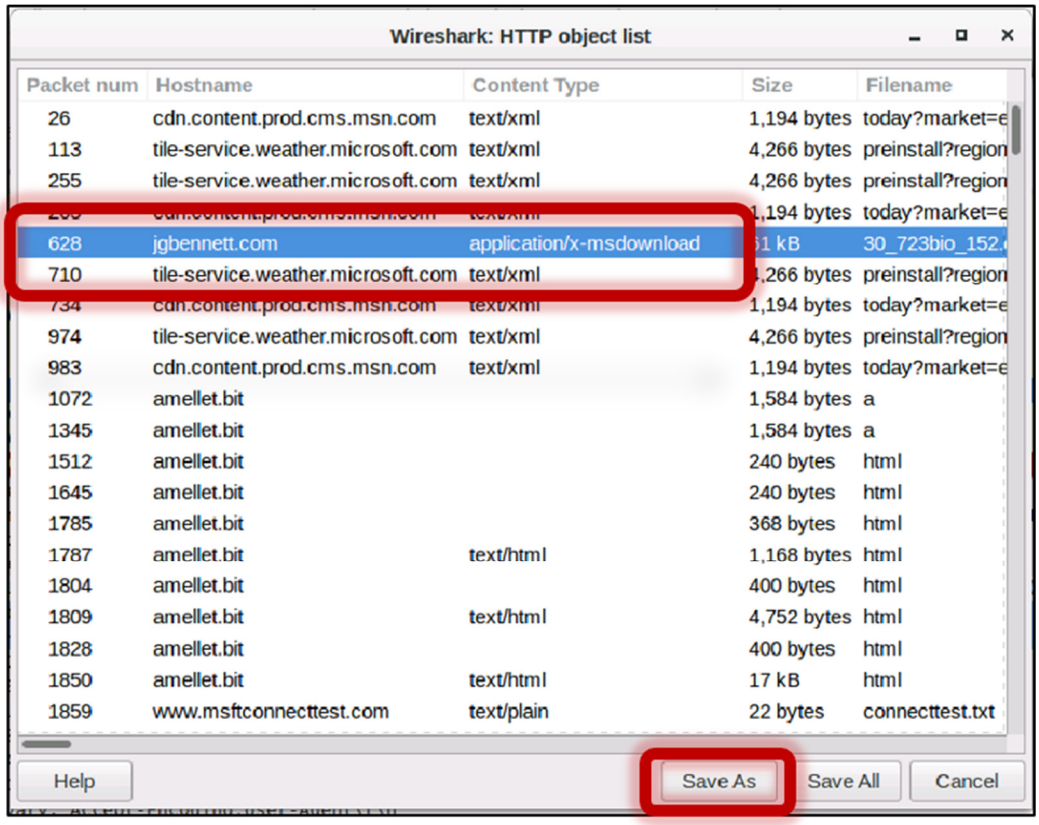
2.7 Using Wireshark, we can extract the file from the TCP stream. In Wireshark, click on **File**, then move your mouse over **Export Objects**, then click on **HTTP**.



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



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

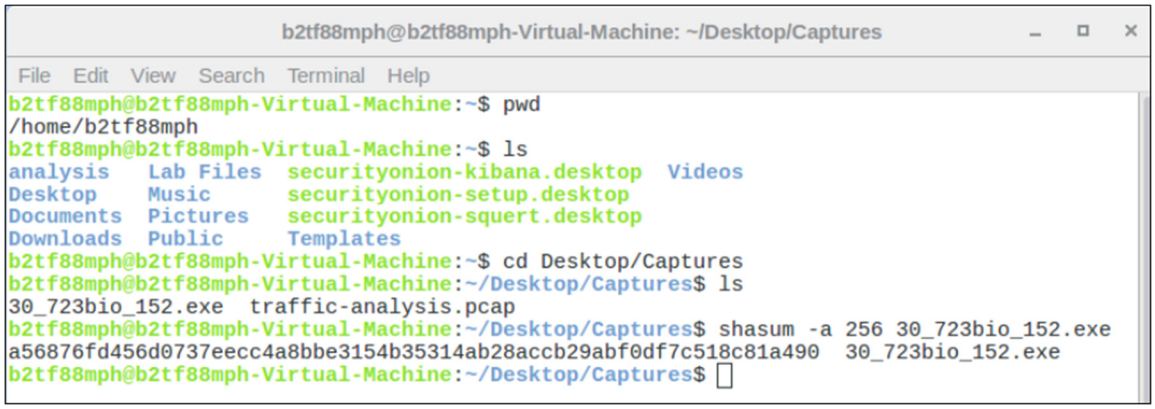


2.10 Save the file in the Captures folder.

3.0 Investigate the File

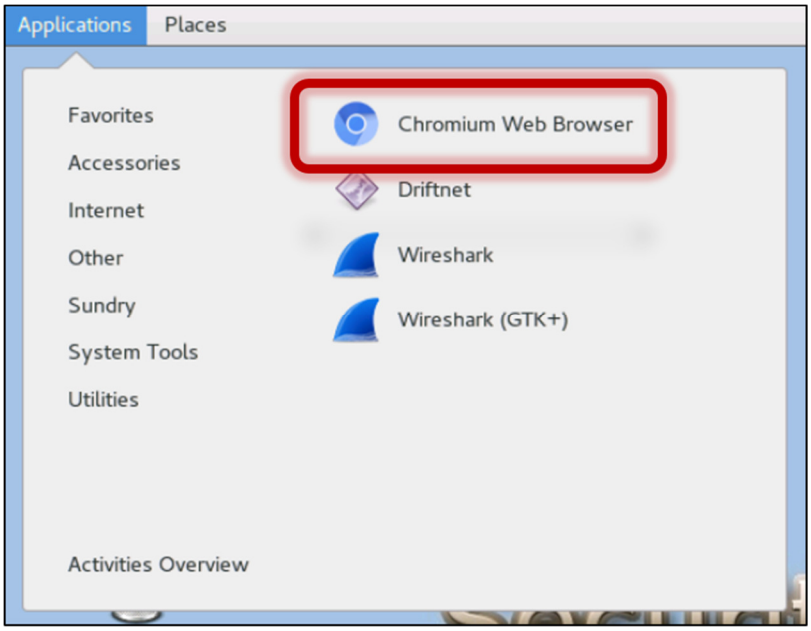
Now that we have found a Windows executable file, we can do some research into the file. We don't want to open an unknown file without precautions. One thing we can do is get the file hash of the executable file we extracted and research the hash value.

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.

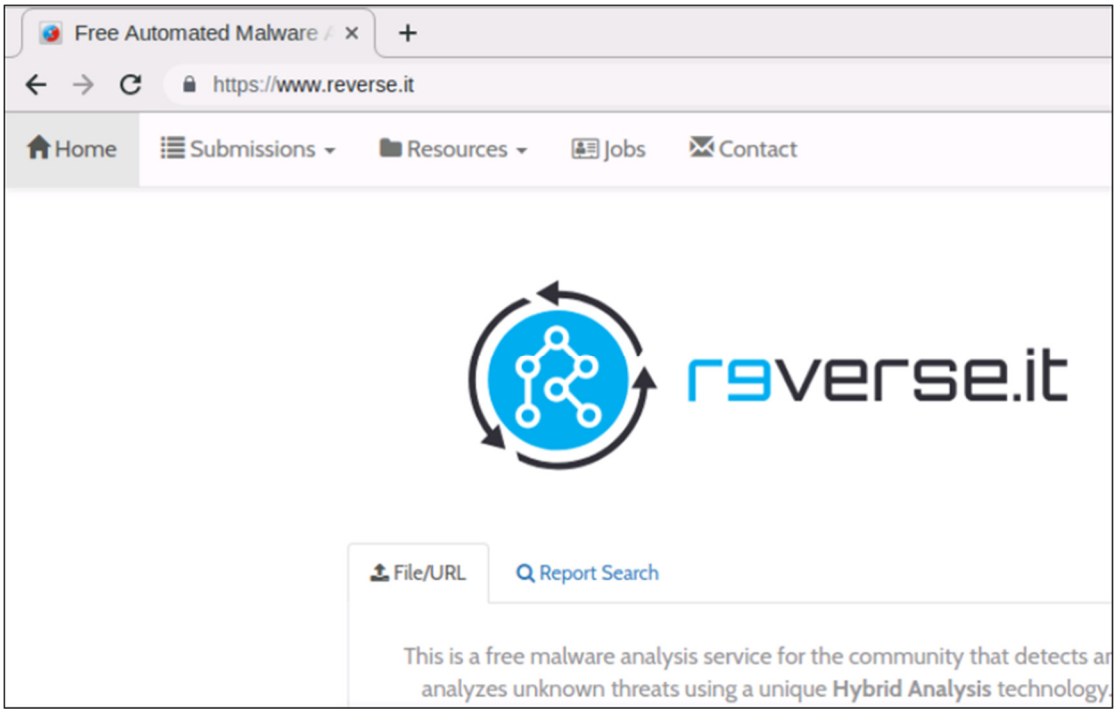


3.2 The file hash should
be: `a56876fd456d0737eecc4a8bbe3154b35314ab28accb29abf0df7c518c81a490`

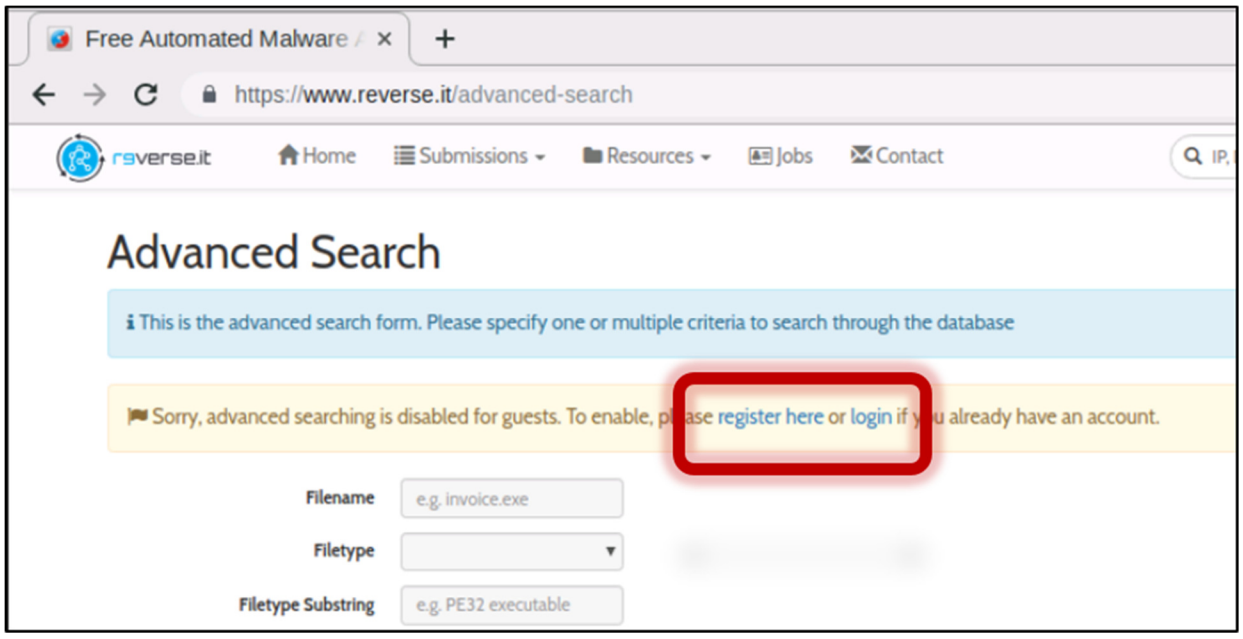
3.3 Open a web browser. The web browser for **Security_Onion** is called **Chromium Web Browser**. Click on **Applications**, then move your mouse over **Internet**, and click on **Chromium Web Browser**.



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



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

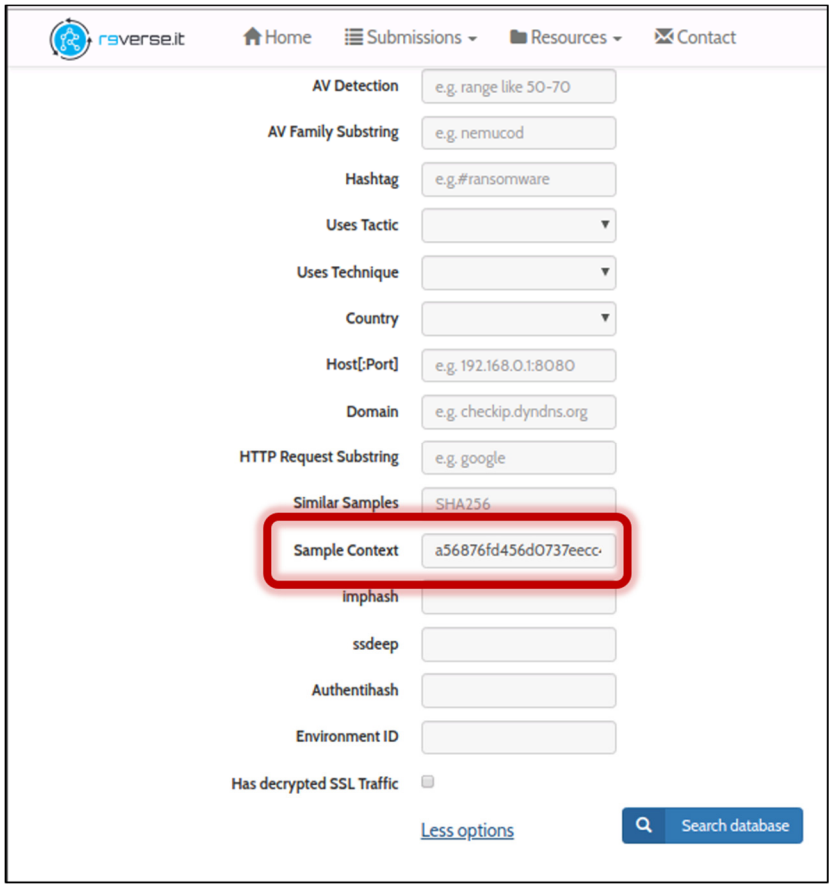


3.6 Login to your e-mail to validate the account.

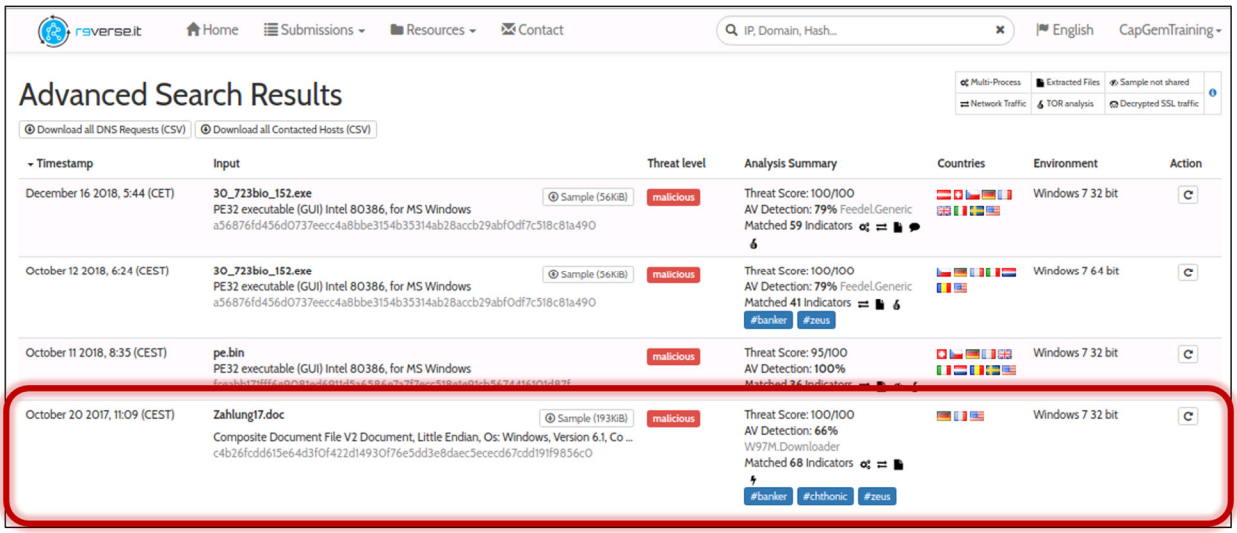
3.7 Login to https://www.reverse.it.

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**.

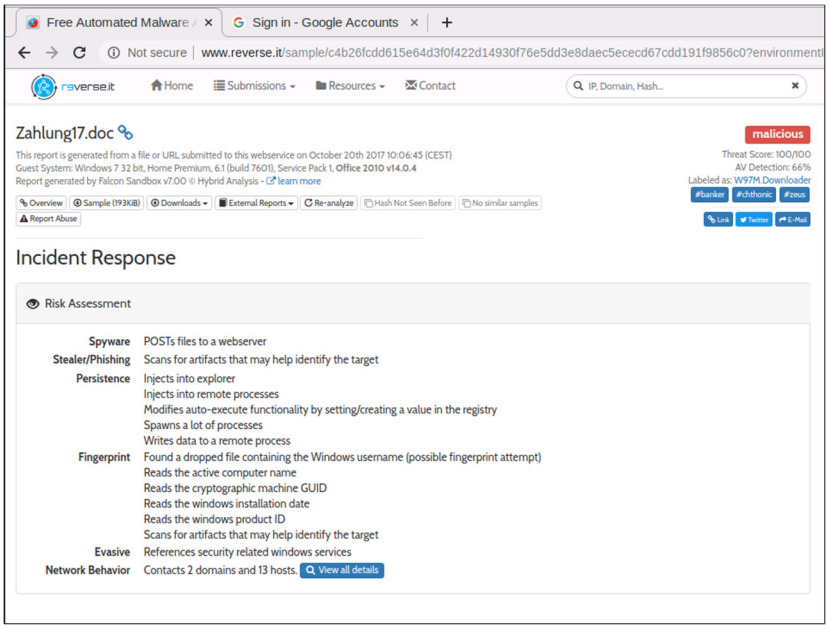


3.10 The first couple of files are the same file we extracted from the pcap. But there is a new file as well; if you scroll down you will find a Word document 'Zahlung17.doc'. Note: If you are keen on your German than you will realize that Zahlung translates to payment.

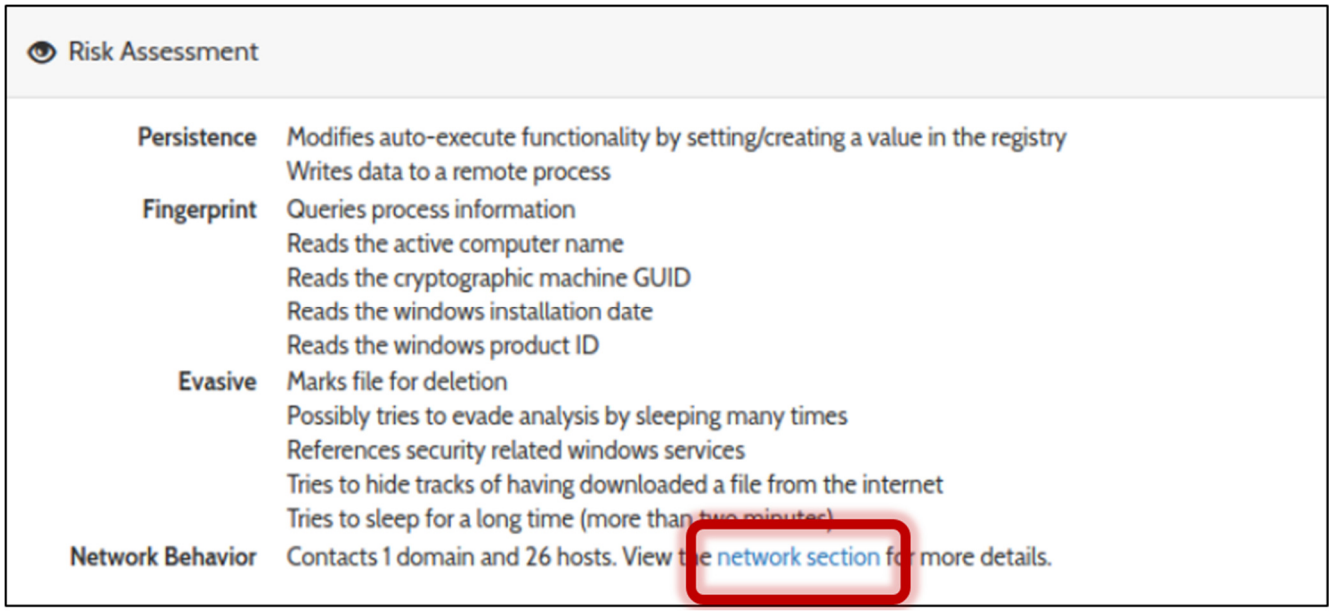


3.11 Double-click on the file you wish to learn more about.

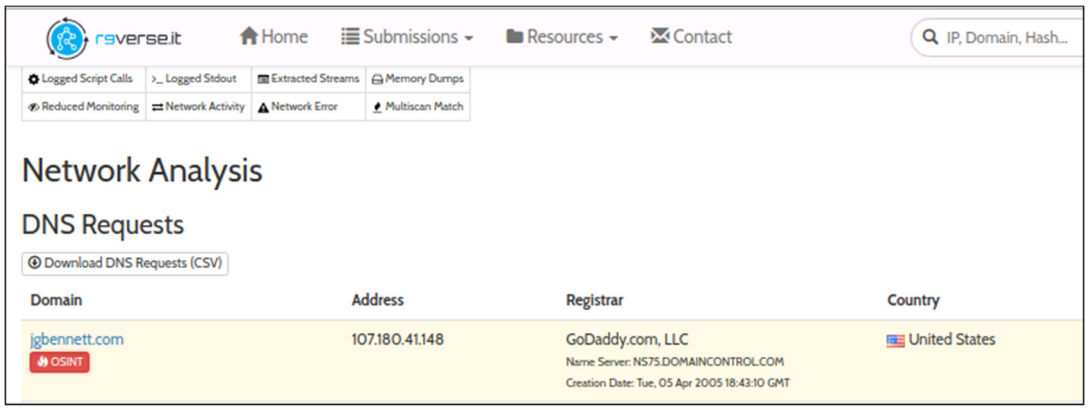
3.12 The Risk Assessment section gives a good list of Indicators of Compromise.



3.13 Click on the `network section` link beside Network Behavior.

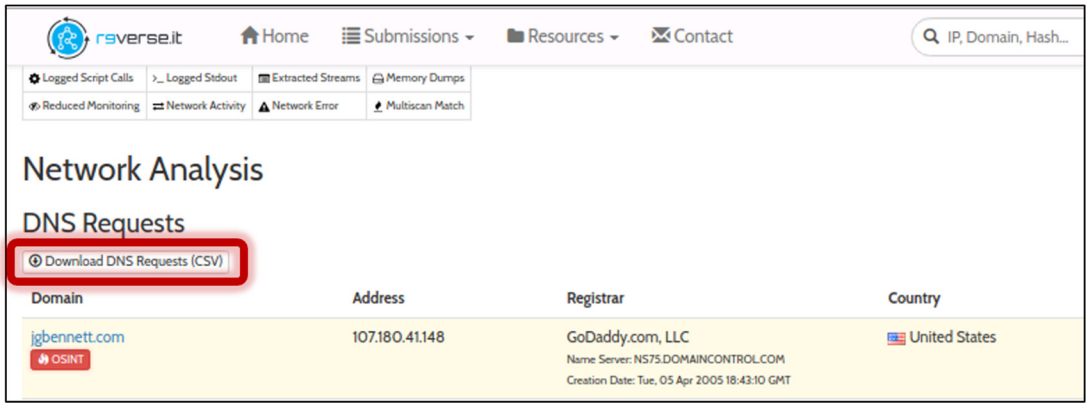


3.14 This give us a listing of DNS Requests, Contacted Hosts, and HTTP Traffic.



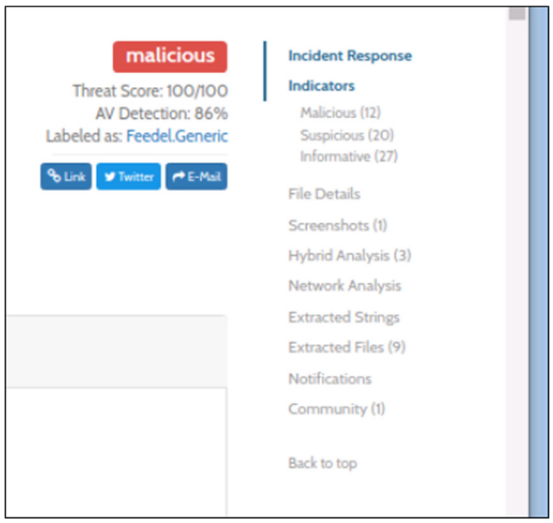
3.15 Download the Indicators by clicking **Download DNS Requests (CSV)**

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

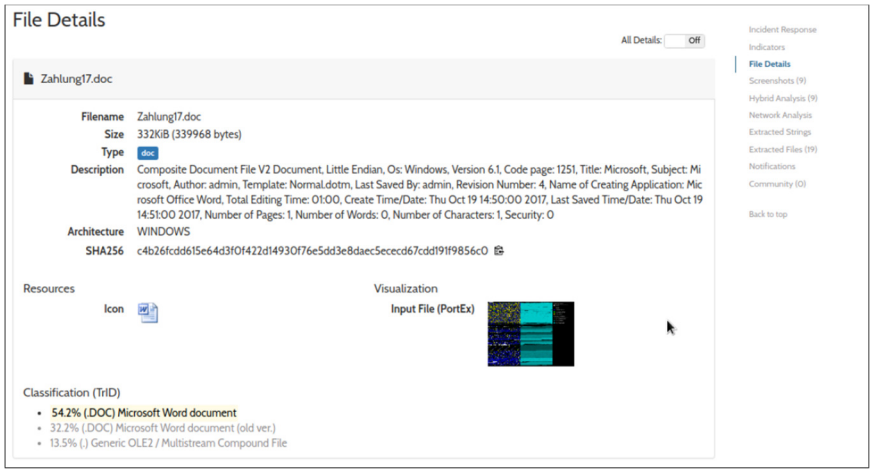


3.16 Compare the traffic to the pcap using Wireshark.

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



3.18 You will see the SHA256 hash of the file c4b26fcdd615e64d3f0f422d14930f76e5dd3e8daec5ececd67cdd191f9856c0



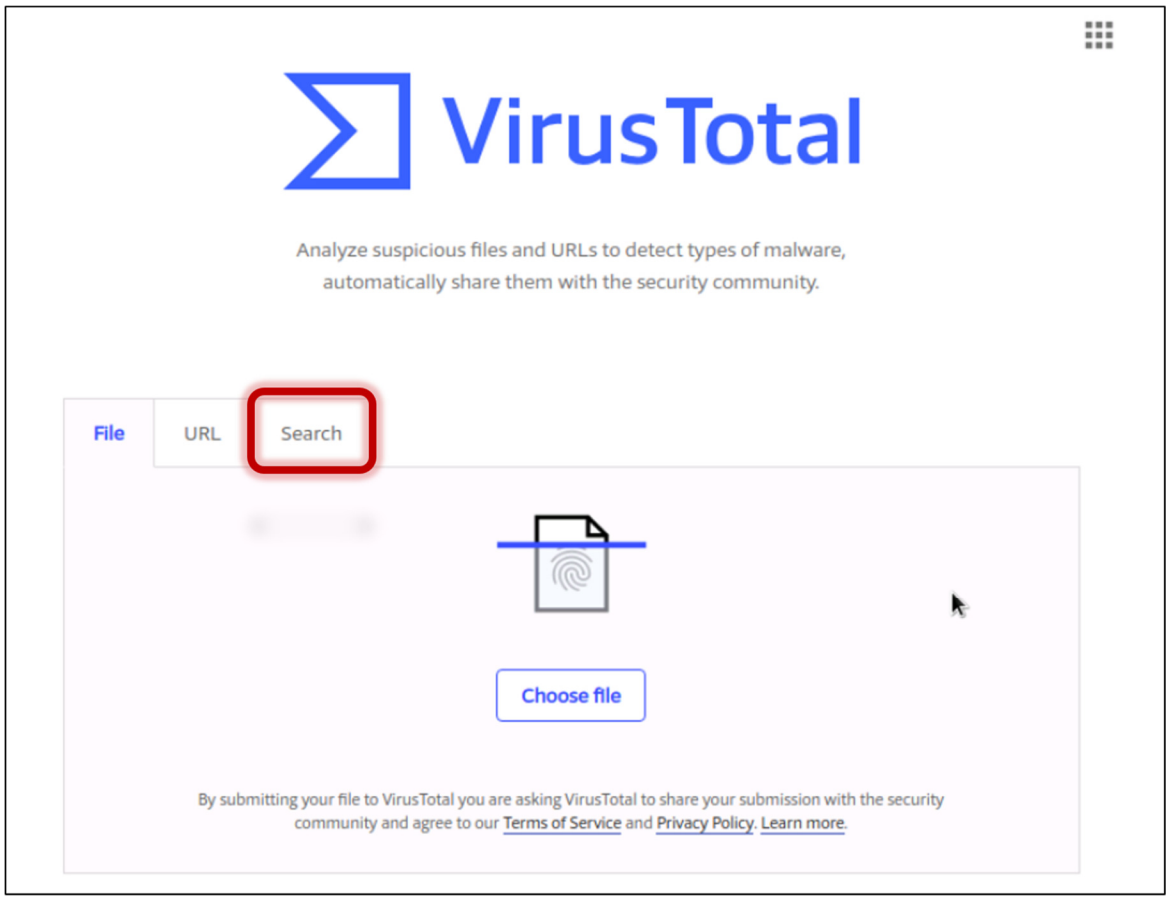
Explore the information available for a bit, see what else you can find that might assist in your investigation!

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

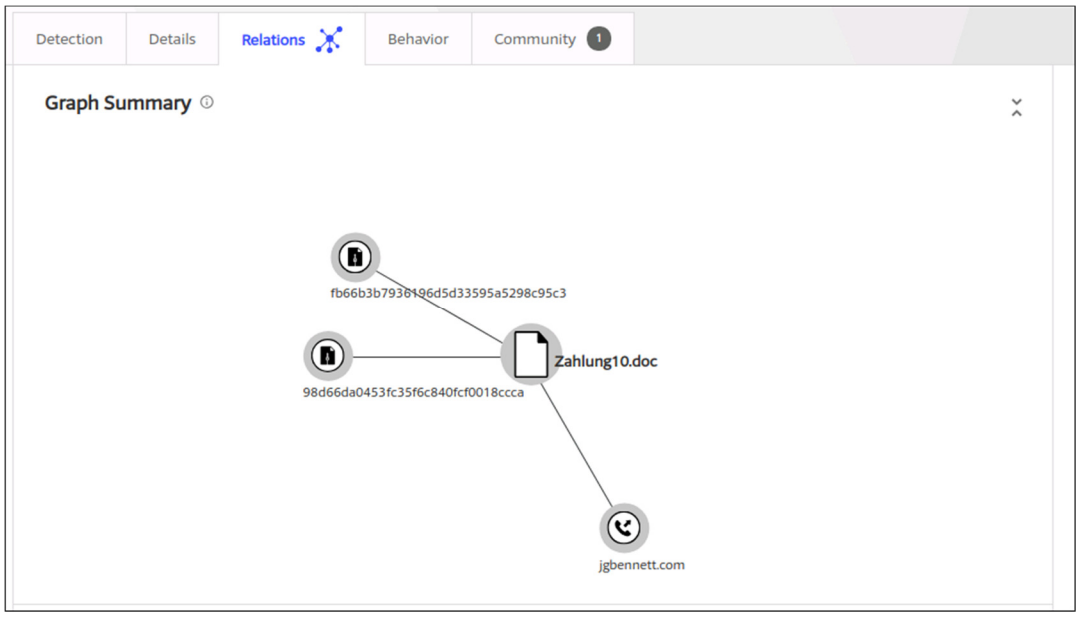
4.1 Open a web browser or new tab in your current browser and navigate to https://www.virustotal.com.

4.2 Click the **Search** tab.



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

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

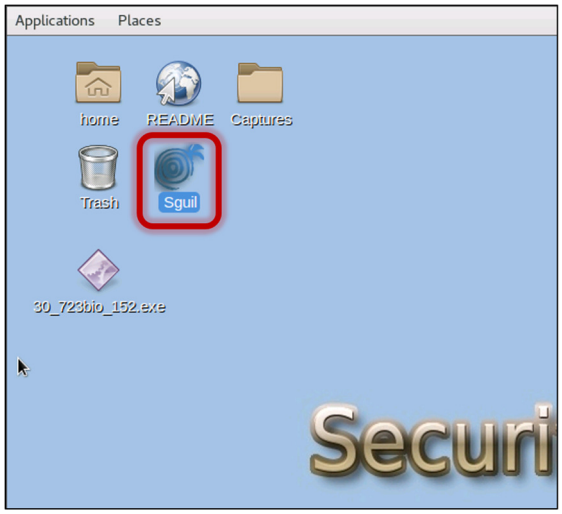


4.5 This means the file was included in some kind of zipped folder. Perhaps a download from the website or an email.

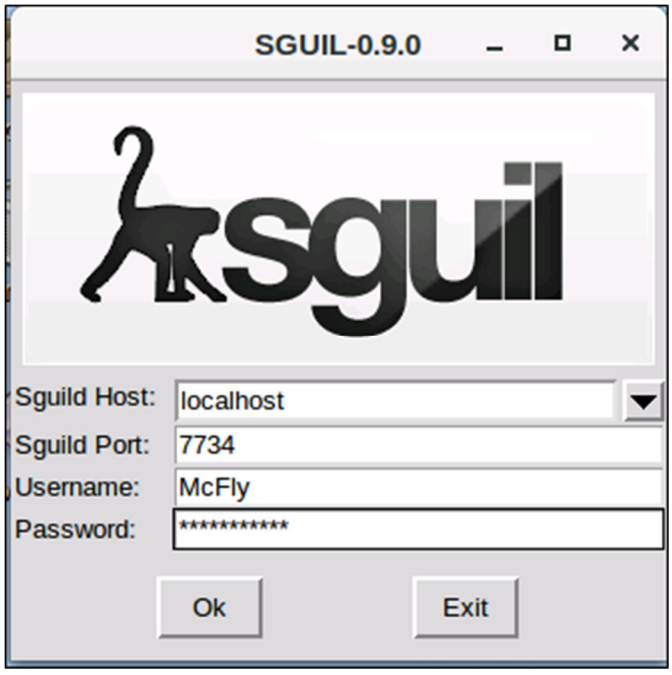
We have a lot of good information to do some research. We know that the malware is reaching out to amellet.bit. A Google search of "amellet.bit malware" will result in the information this malware is related to the **Chthonic Banking Trojan**.

5.0 Using Sguil for File Analysis

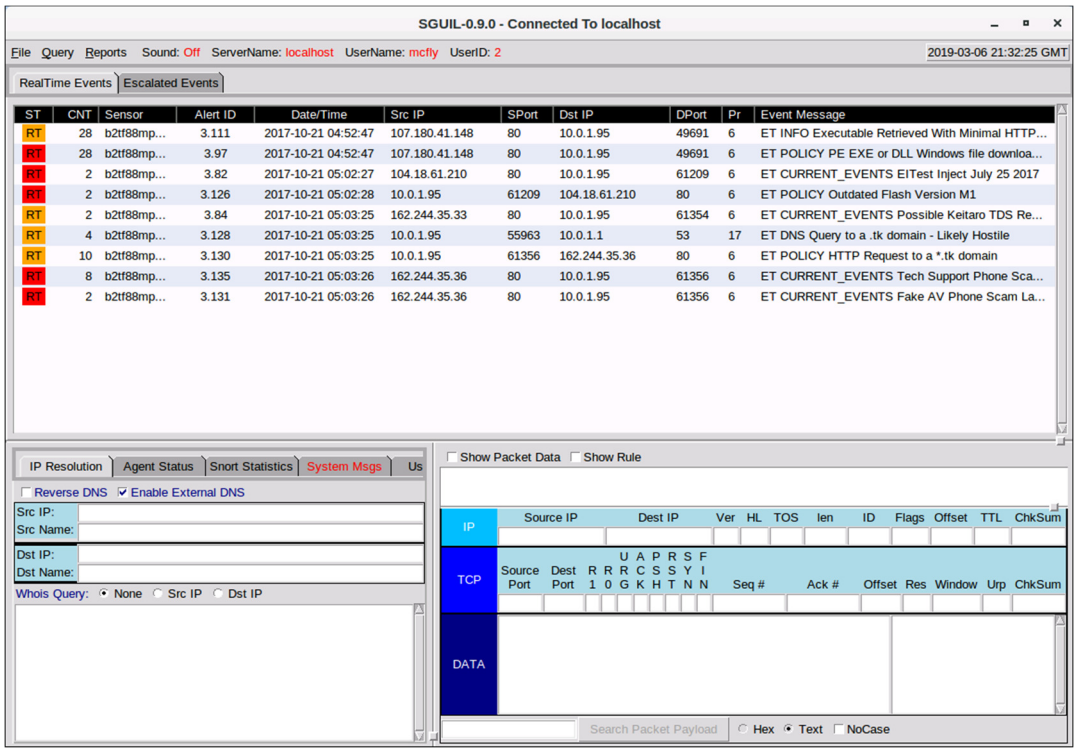
5.1 Open Sguil from the Desktop.



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

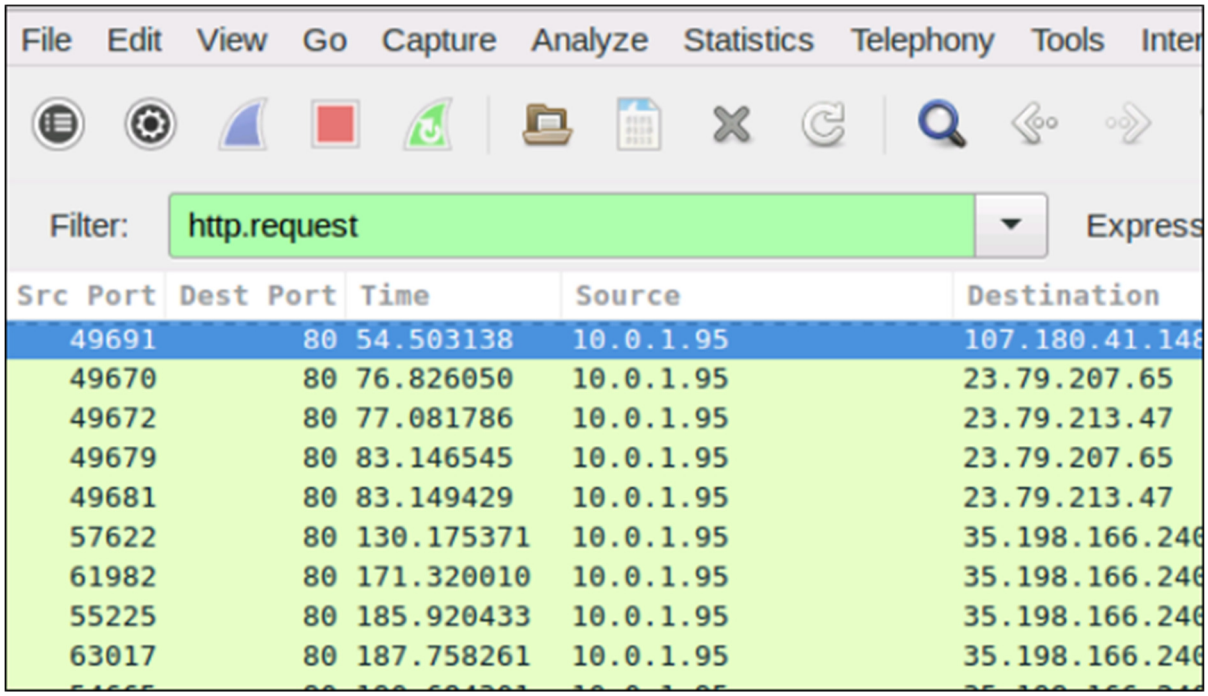


5.3 Look at the alerts to determine what the malware is doing.

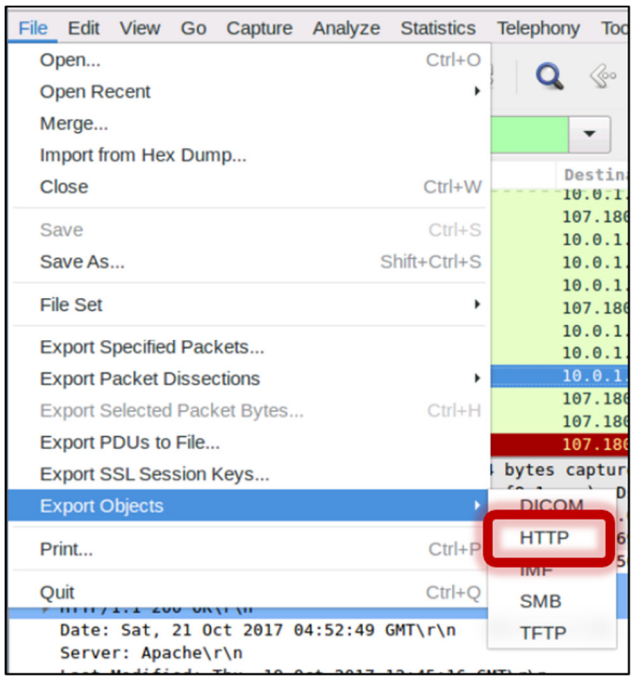


5.4 The activity shows that the malware is downloaded and then attempts to beacon. After the beacon, the malware appears to redirect to a fake tech support/help desk page.

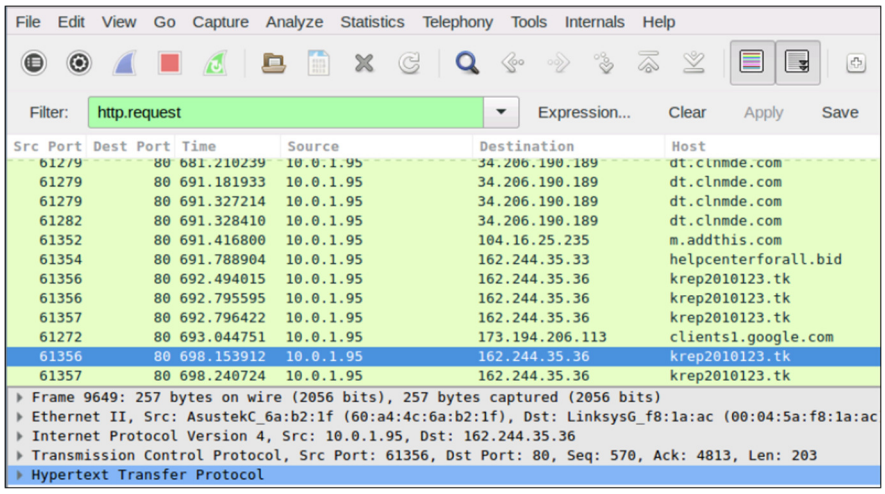
Go back to Wireshark and look at the pcap again using the `http.request` filter.



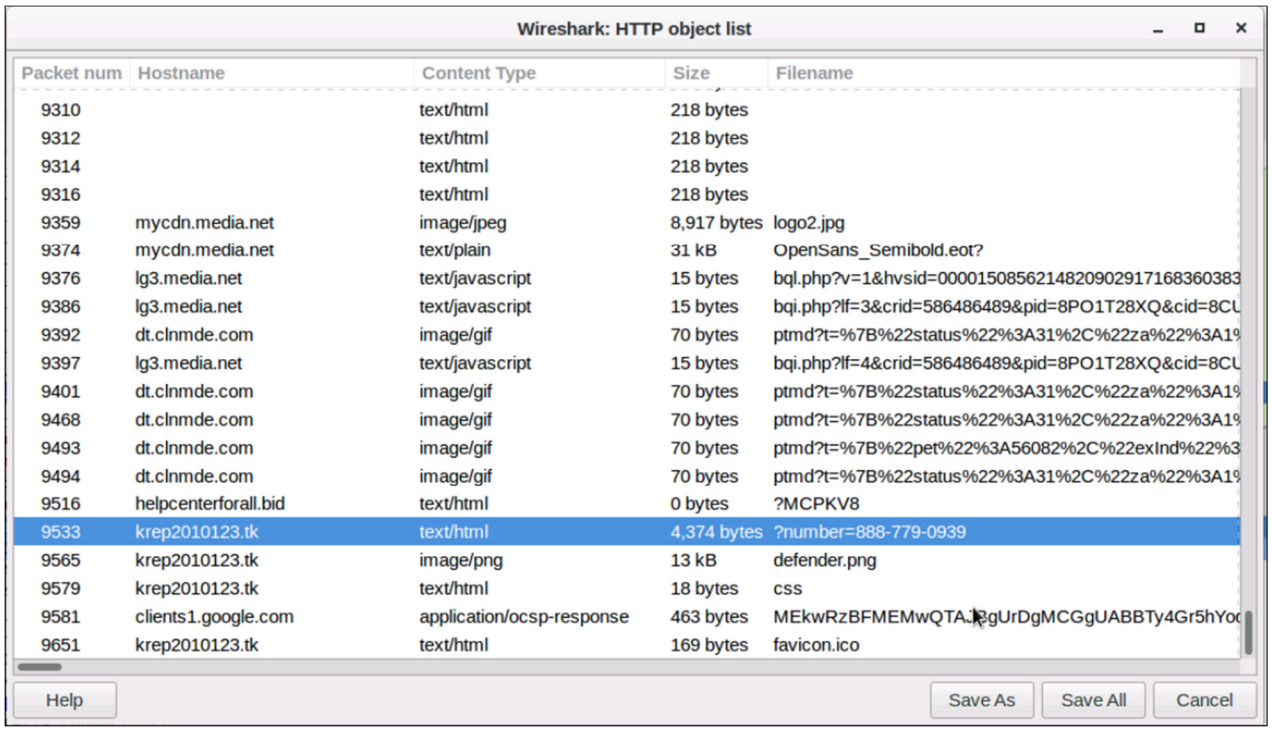
5.5 In Wireshark, click on **File**, move your mouse over **Export Objects**, and click on **HTTP**.



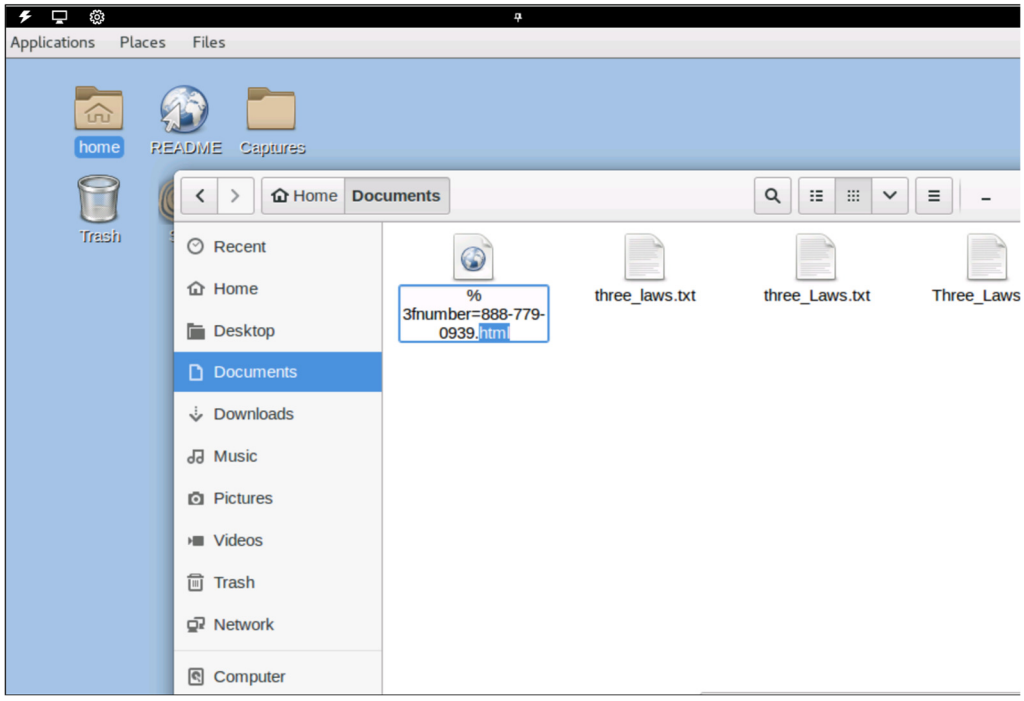
5.6 If we scroll down to the bottom of the requests, we see a request from krep2010123.tk, look for the one with a phone number.



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

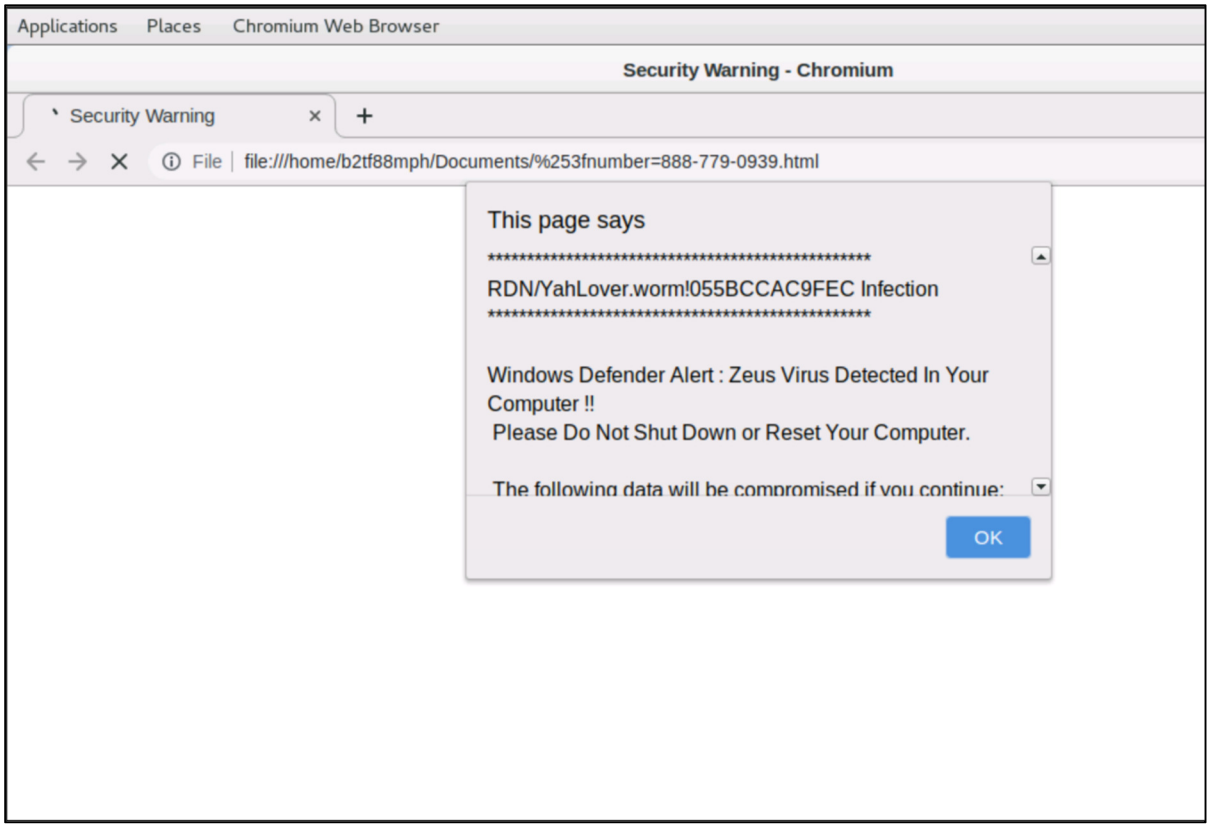


5.8 Navigate to the location where you saved the file and open it. You will need to add the **.html** file extension.



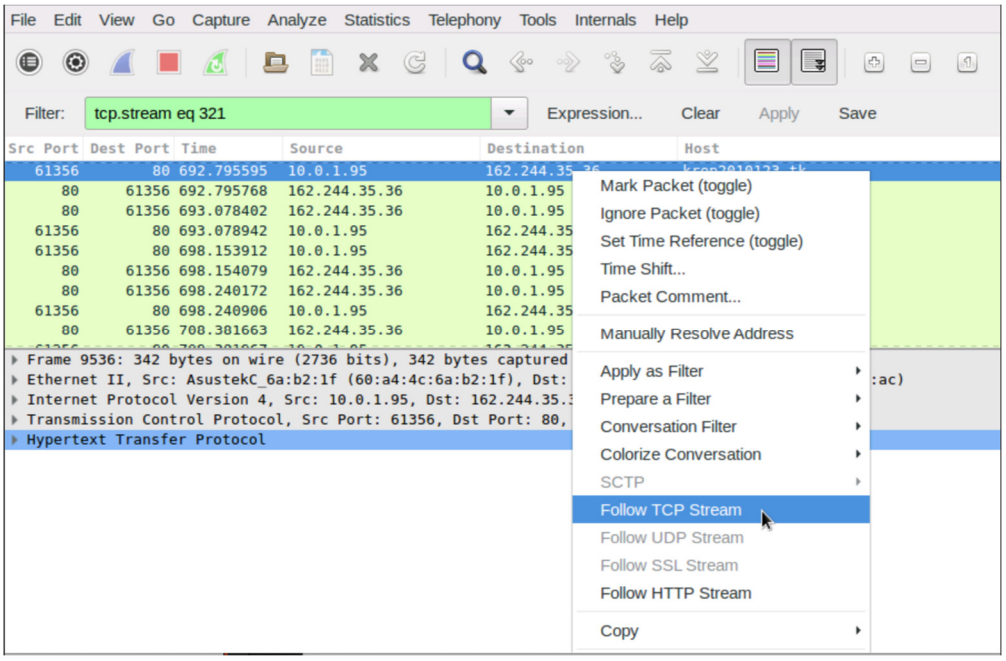
5.9 You should open a fake web page that looks like an anti-virus alert.

What caused the fake anti-virus page?

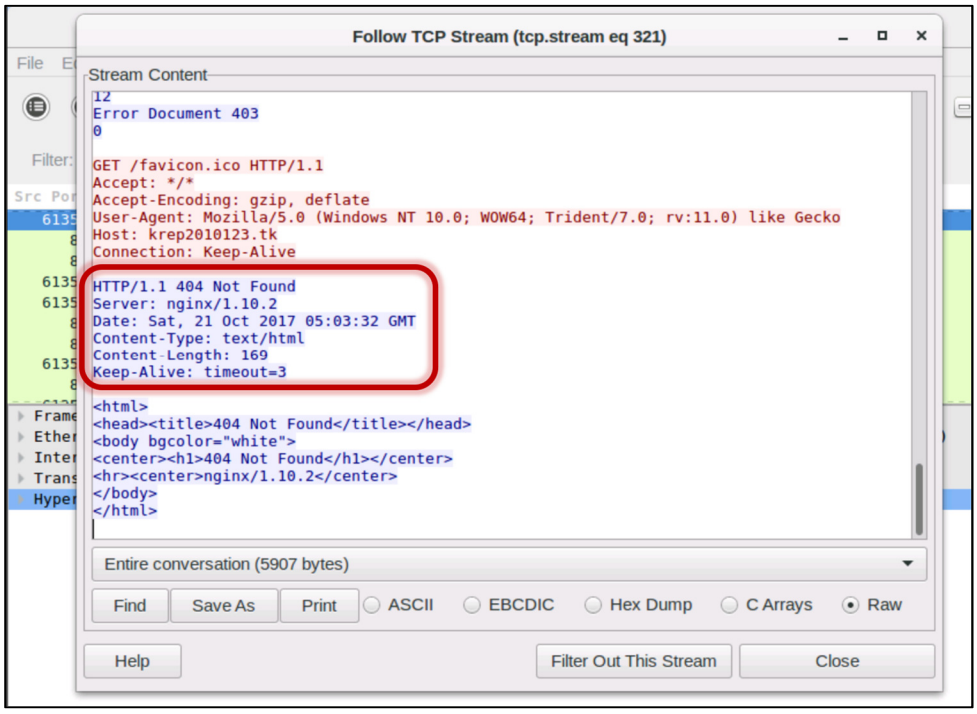


6.0 Continue Investigating

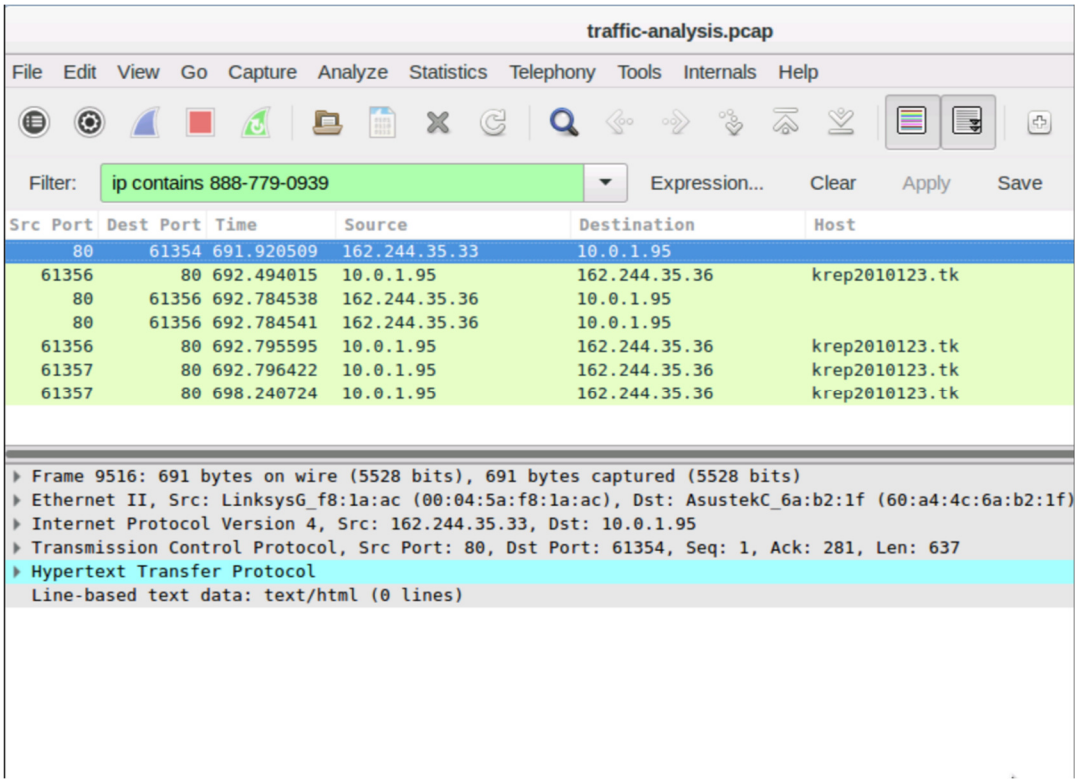
6.1 Right-click the request and select **Follow TCP Stream**.



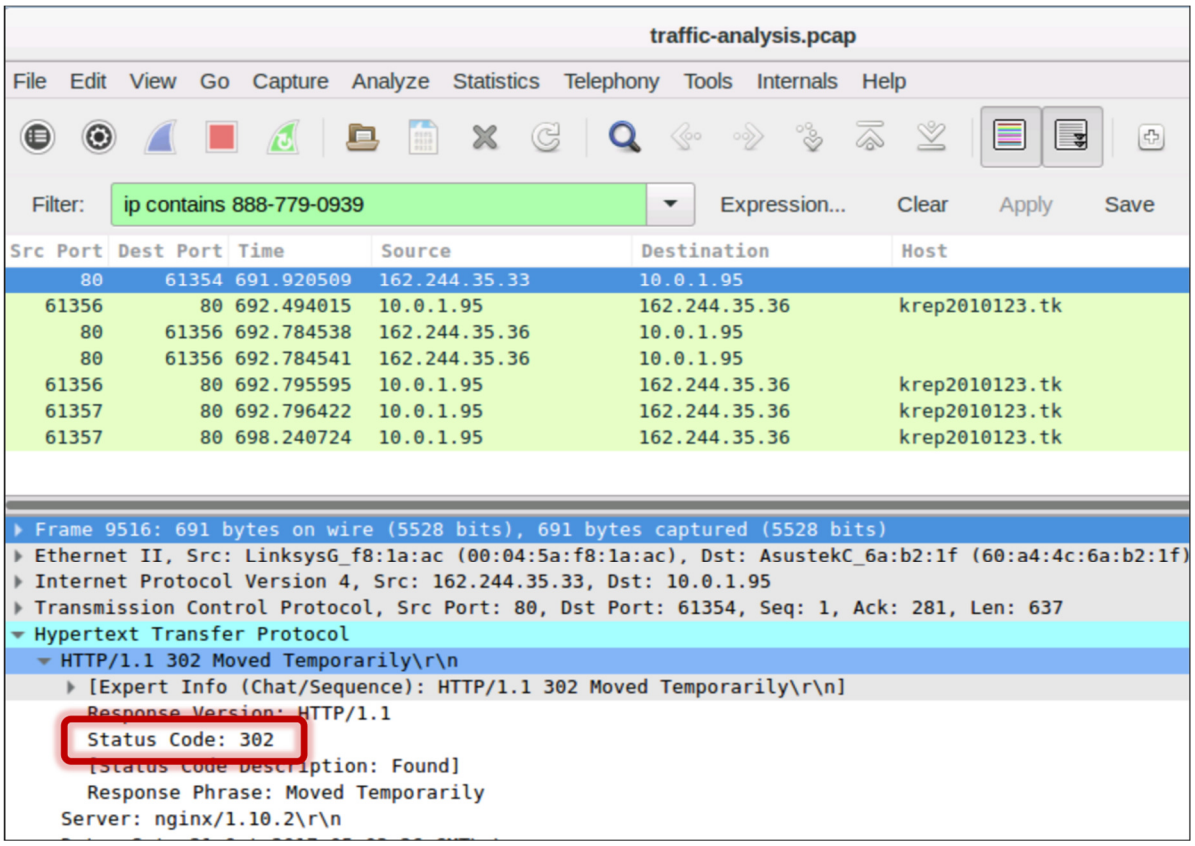
6.2 It doesn't appear to have a referrer in the HTTP headers.



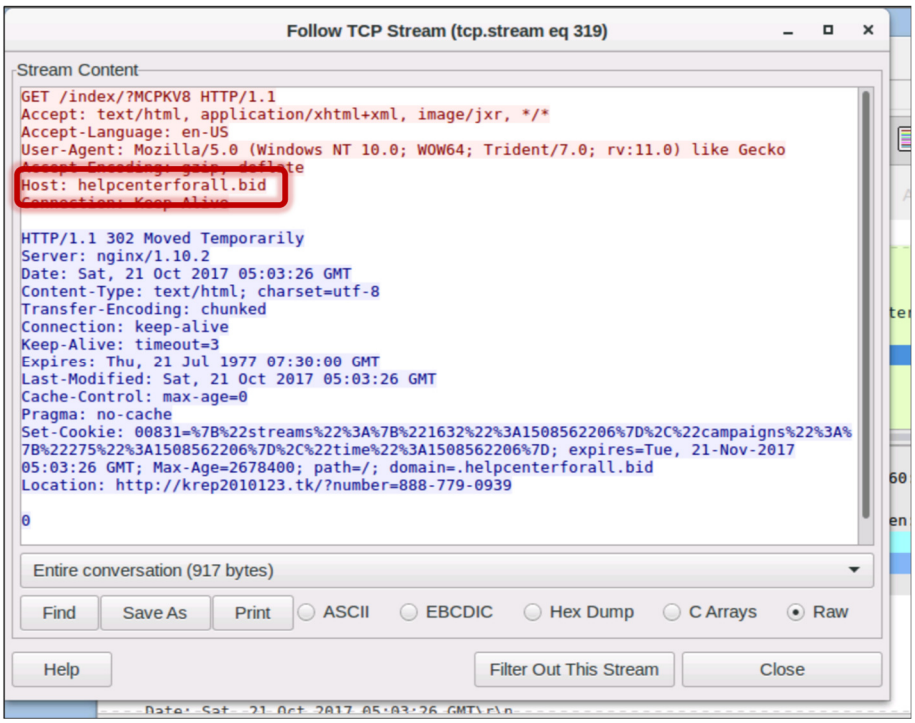
6.3 Use the filter `ip contains 888-779-0939` and then we can work our way through the traffic flow.



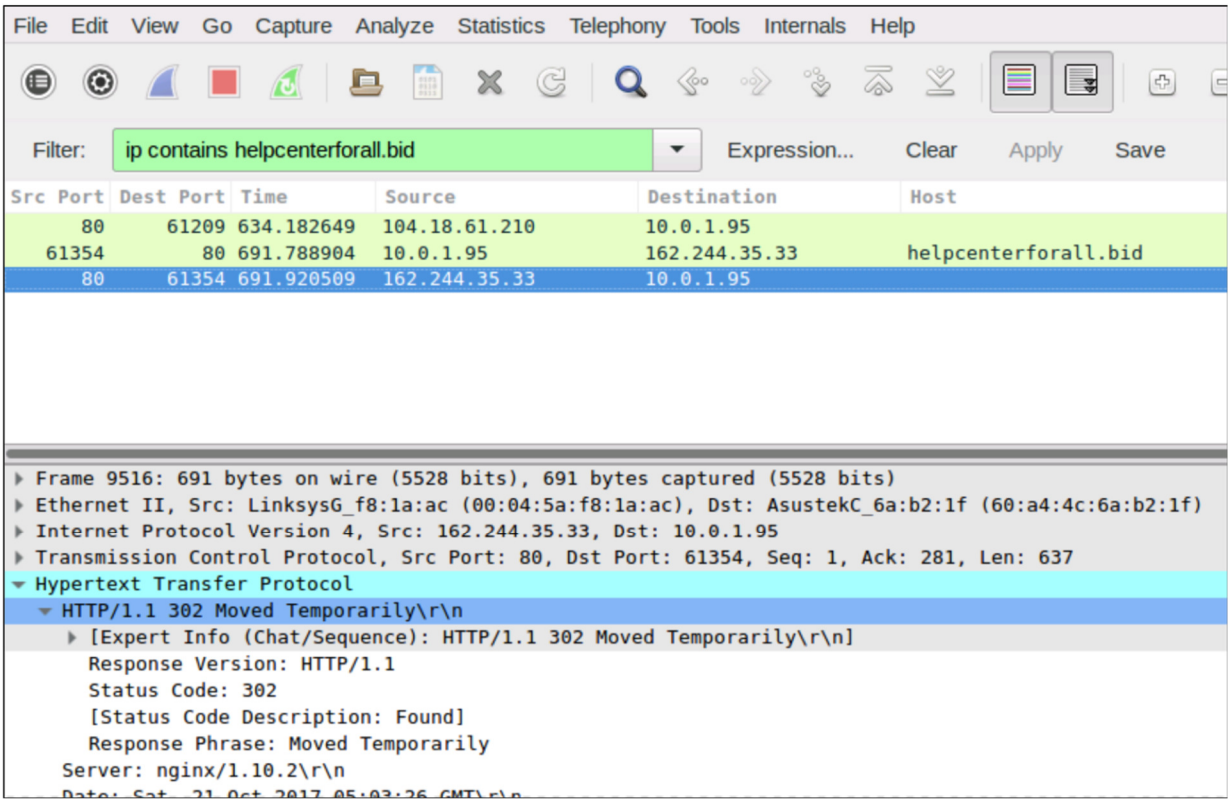
6.4 The first request should be a 302 response.



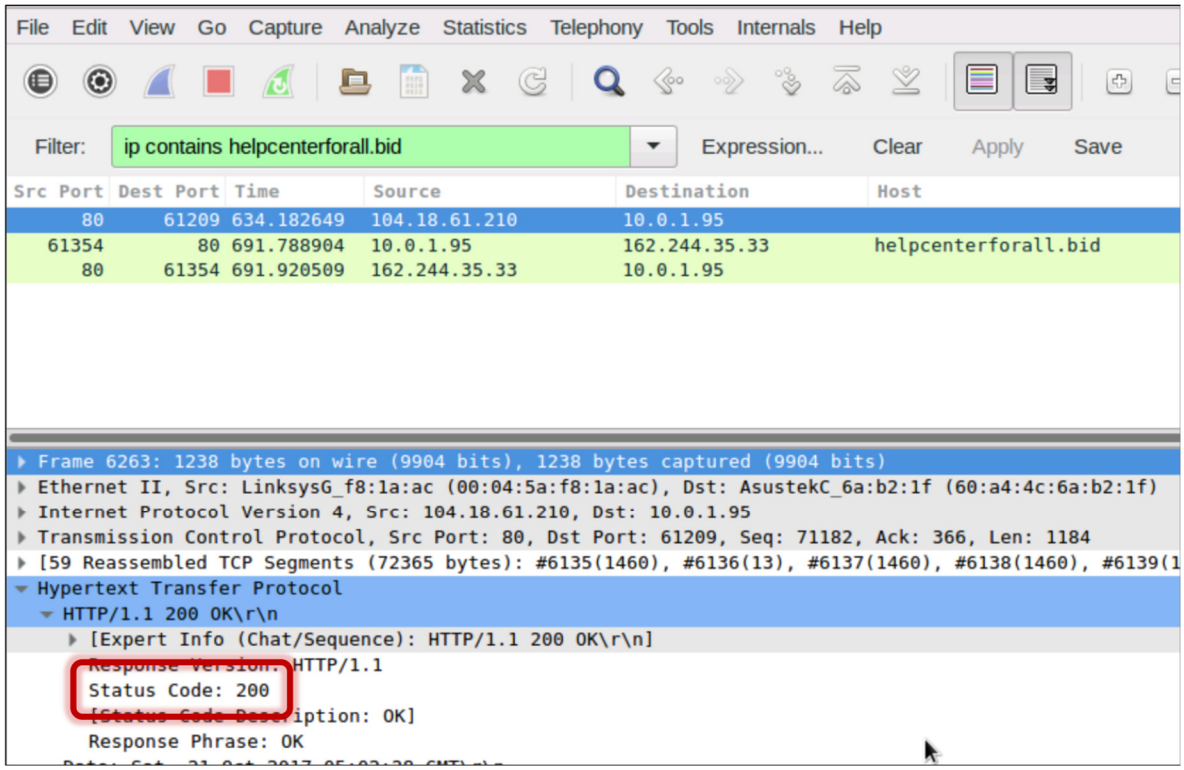
6.5 Follow the TCP Stream and we find the website `helpcenterforall.bid`



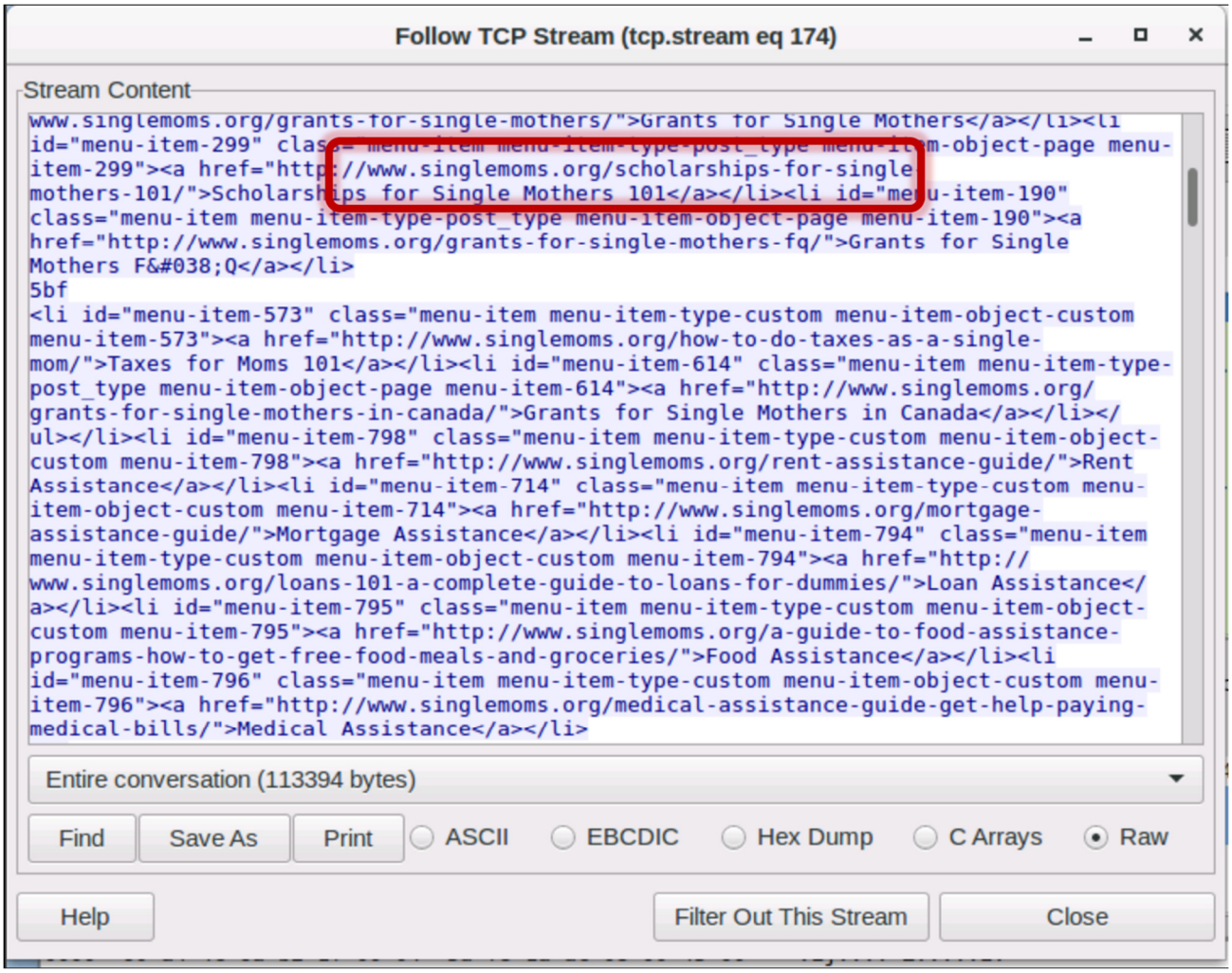
6.6 Use the filter for `ip contains helpcenterforall.bid`



6.7 The first request contains a 200 response.



6.8 Follow the TCP stream to find the request came from `www.singlemoms.com`



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.