Exp04

Matteo Di Fabio: 264339  
Luca Genovese: 264364

1. To identify all the involved systems it is necessary to use the following instruction command line: *“tshark -r traffic1.pcap -T fields -e ip.dst ip.src | sort | uniq”* that extract and sort, uniquely, all the IP addresses into pick-up file from the provided pcap file.

Here there are all the detected addresses:

* 189.126.11.82
* 192.168.115.238
* 200.149.77.224
* 66.7.200.69
* 66.7.200.72
* 8.8.4.4

An alternative way to find them is using Wireshark’s file menu bar option *“Statistics -> Endpoints”*

1. To identify the geolocalisation we decided to use an online tool (“<https://whatismyipaddress.com/ip-lookup>”) to try to obtain these information. The obtained results are the following:
   * 189.126.11.82

ISP: Calcontec Tel.ecomunicacoes E Informatica Ltda

Organization: Calcontec Tel.ecomunicacoes E Informatica Ltda

Services: None detected

Assignment: Likely Static IP

Continent: South America

Country: Brazil

Latitude: -22.8305 (22° 49′ 49.80″ S)

Longitude: -43.2192 (43° 13′ 9.12″ W)

* + 200.149.77.224  
    ISP: Oi Internet

Organization: Oi Internet

Services: None detected

Type: Broadband

Assignment: Likely Static IP

Continent: South America

Country: Brazil

State/Region: Rio de Janeiro

City: Niterói

Latitude: -22.922 (22° 55′ 19.20″ S)

Longitude: -43.1025 (43° 6′ 9.00″ W)

* + 66.7.200.69

ISP: HostDime.com

Organization: HostDime.com

Services: None detected

Type: Corporate

Assignment: Likely Static IP

Continent: North America

Country: United

Latitude: 37.751 (37° 45′ 3.60″ N)

Longitude: -97.822 (97° 49′ 19.20″ W)

* 66.7.200.72

ISP: HostDime.com

Organization: HostDime.com

Services: None detected

Type: Corporate

Assignment: Likely Static IP

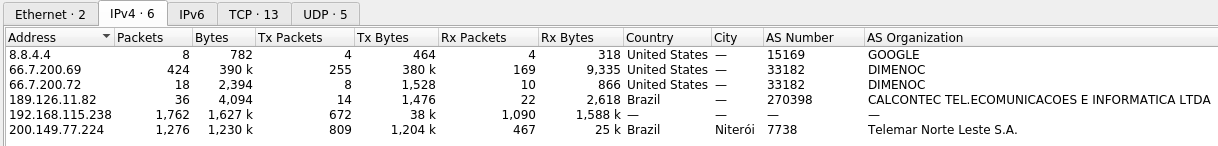
Continent: North America

Country: United

Latitude: 37.751 (37° 45′ 3.60″ N)

Longitude: -97.822 (97° 49′ 19.20″ W)

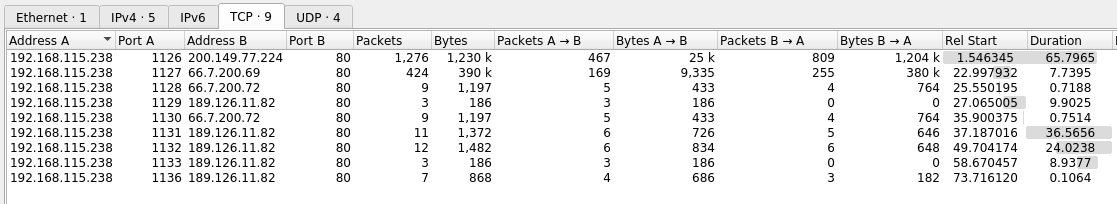
To identify the location of the hosts, it is also possible to use a bash command or a tool in Wireshark *“Statistics -> Endpoints”.* To use this tool, it is necessary to install download a geolocalisation database (GeoLite2-ASN and GeoLite2-City from http://www.maxmind.com) and then insert it in Wireshark. The extracted informations from the captured packet are the following:



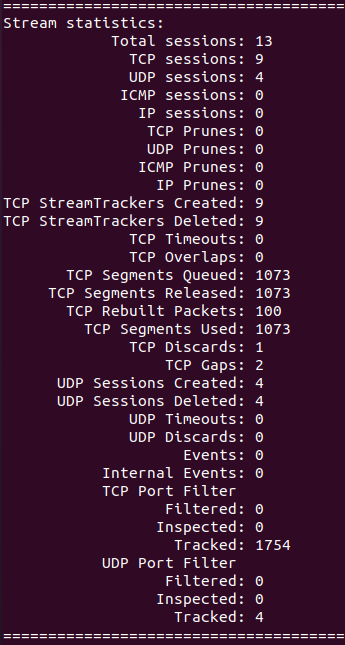
The IP from which the victim download the malware is ‘66.7.200.69’.

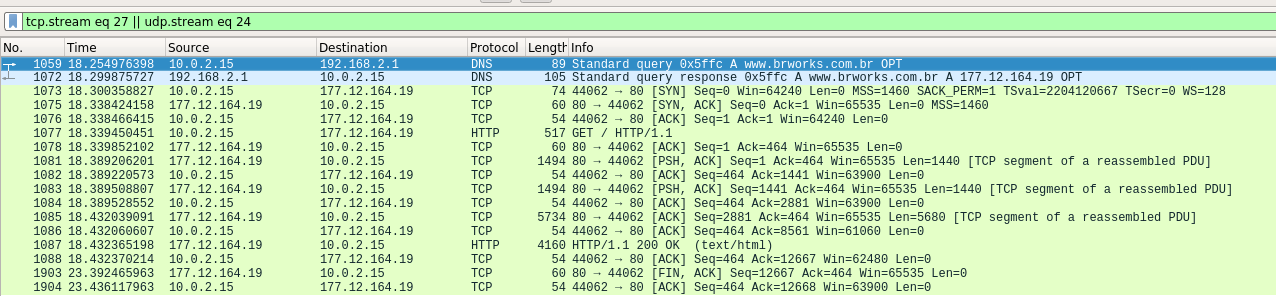
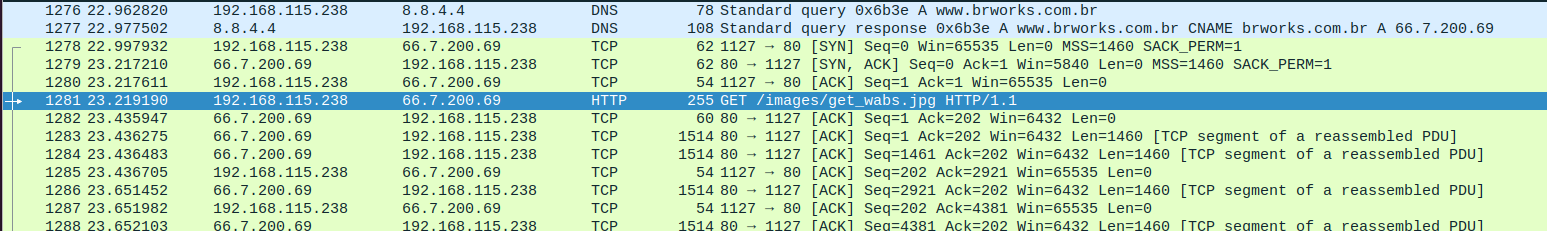
1. To identify the number of TCP session it is possible to use a bash command (tshark and/or snort) or a tool in Wireshark *“Statistics -> Conversation”.* The obtained results are 9 TCP sessions with a total of 1756 exchanged packets:

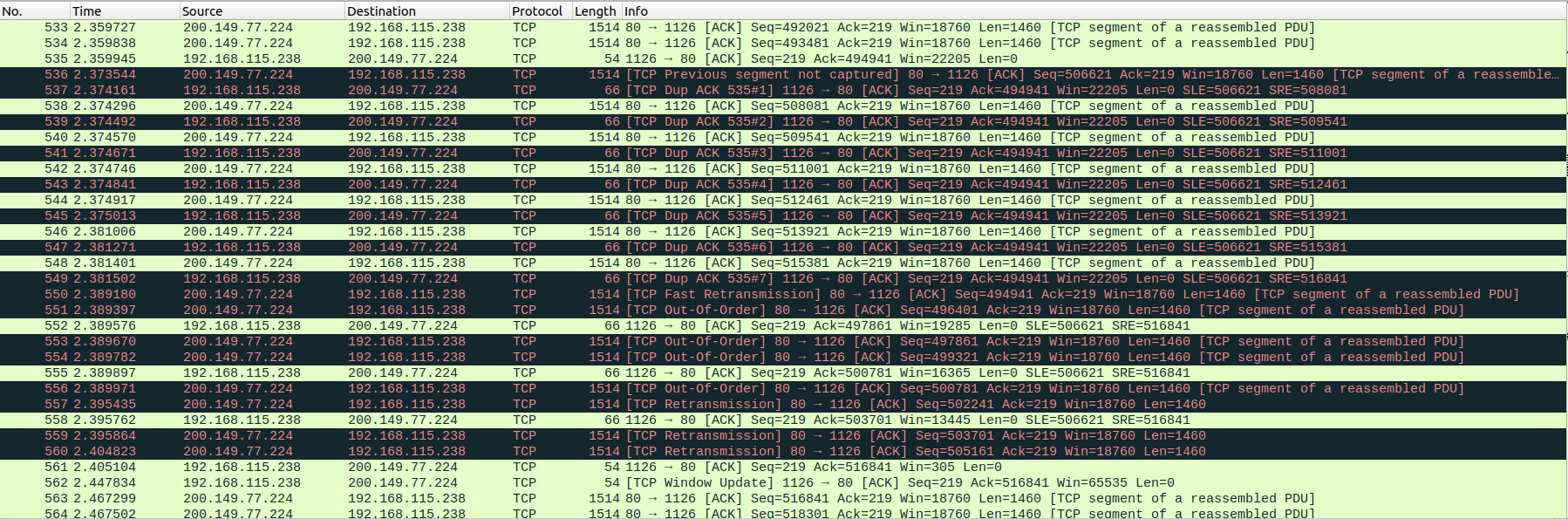
* 192.168.115.238 on port 1126 <-> 200.149.77.224 on port 80 packets: 1276
* 192.168.115.238 on port 1127 <-> 66.7.200.69 on port 80 packets: 424
* 192.168.115.238 on port 1128 <-> 66.7.200.72 on port 80 packets: 9
* 192.168.115.238 on port 1129 <-> 189.126.11.82 on port 80 packets: 3
* 192.168.115.238 on port 1130 <-> 66.7.200.72 on port 80 packets: 9
* 192.168.115.238 on port 1131 <-> 189.126.11.82 on port 80 packets: 11
* 192.168.115.238 on port 1132 <-> 189.126.11.82 on port 80 packets: 12
* 192.168.115.238 on port 1133 <-> 189.126.11.82 on port 80 packets: 3
* 192.168.115.238 on port 1136 <-> 189.126.11.82 on port 80 packets: 7

screenshot in wireshark

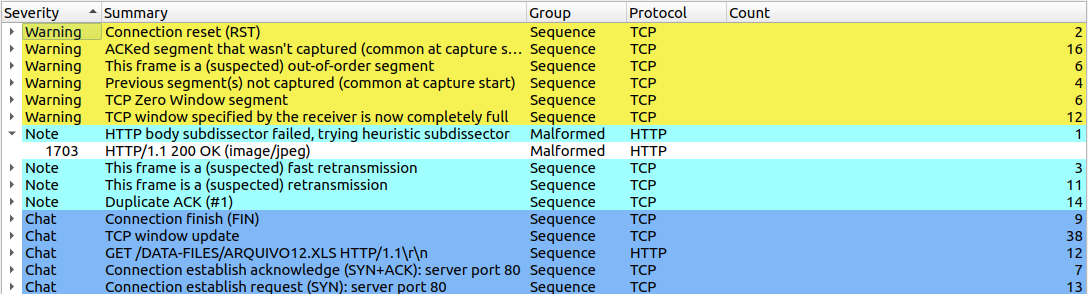
screenshot of result using snort



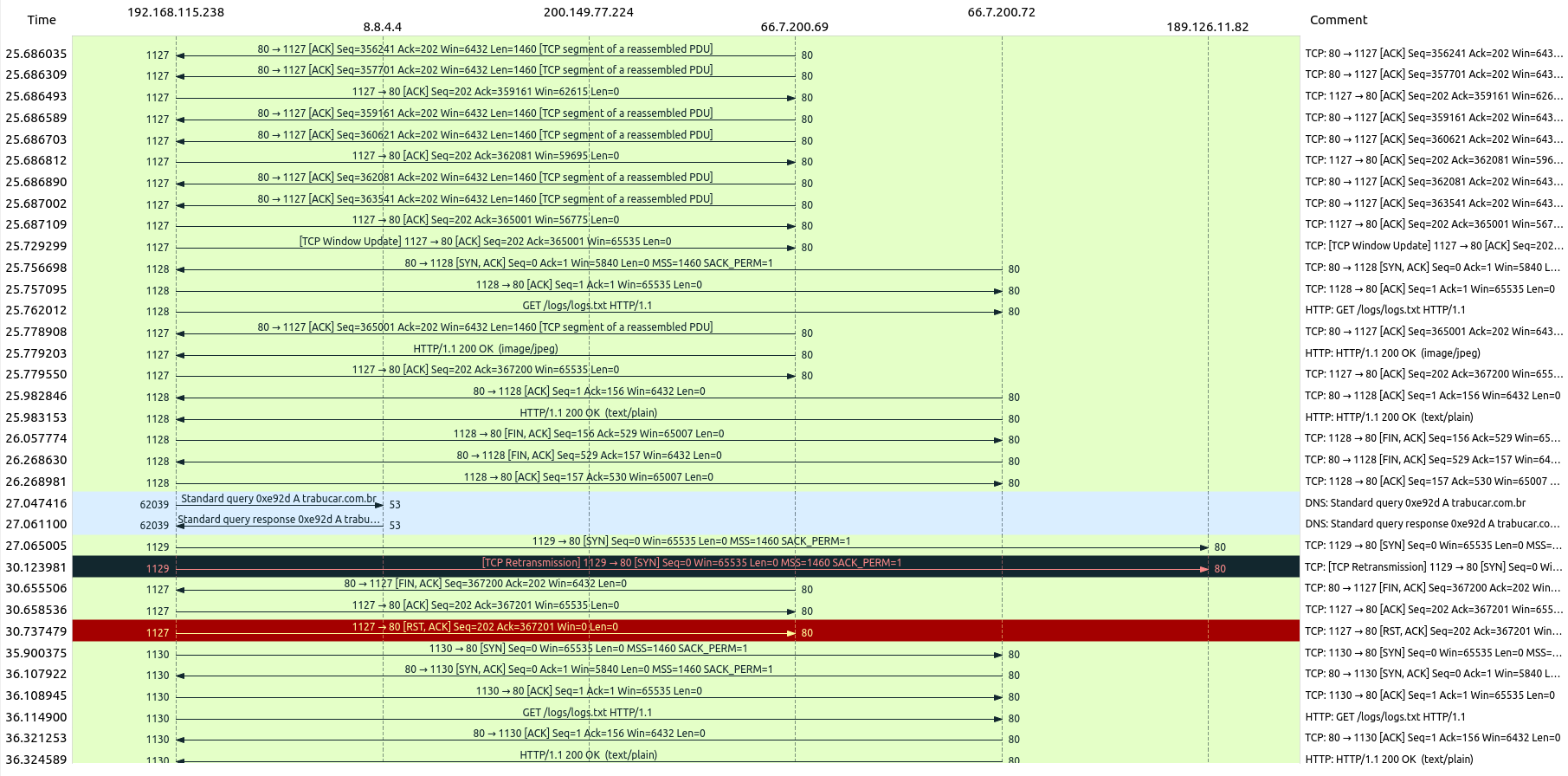
1. The attack that we detected is a DNS spoofing (DNS Shadow server) on Google DNS *“8.8.4.4”* after the query request of *“*[*www.brworks.com.br*](http://www.brworks.com.br)*”* that the victim (*“192.168.115.238”)* does. As this kind of attack is characterized by providing an answer before the correct answer (from Google DNS in this case) and in this way the answer that arrives late will be discarded from the client as duplicate.  
   The attack lasts the time needed by the attacker to answer before Google DNS so as it is possible to observe it takes 0.0014682 seconds.  
   In this second case instead we try to emulate the same query with our PC and as we can see we receive a different IP (the right one): ‘177.12.164.19’.  
   The duration of the total connection and consequently download the file *‘get\_wabs.jpg’* (that is the malware that we identify as malicious) and finally close the session with ‘66.7.200.69’: so 7,7395 seconds.
2. To identify the attack we have analyzed all the packet using the default view and the flow graph using *“Statistics->FLow Graph”.*

In this first analysis we just note some packets loss, that were detected by WireShark and after a while restransmited as expected for the TCP protocol. At this point the only weird behaviour is that the first connection was closed just after a long time, after all the other connection were closed. Another anomaly was in the SYN packet (1712) for the website “trabucar.com.br” in the last connection *‘189.126.11.82’*. As after a long time the client did not received a response, the SYN is retransmitted by the client in the packet 1713 (after 3 seconds) and then again after 6 seconds in 1726 (from the second retransmission).

After that preliminary analyses we didn’t find any anomaly, so at this point we decided to used the tool *“Analysis->Expert information”* and as we can observe at the packet 1703 on 66.7.200.69 connection, is detected a malformed packet.

Now, knowing that it is possible to make some specific analysis on these packet (around 1703) with flow graph and it is possible to note that the client make a query request to download an image: *‘get\_wabs.jpg’.*

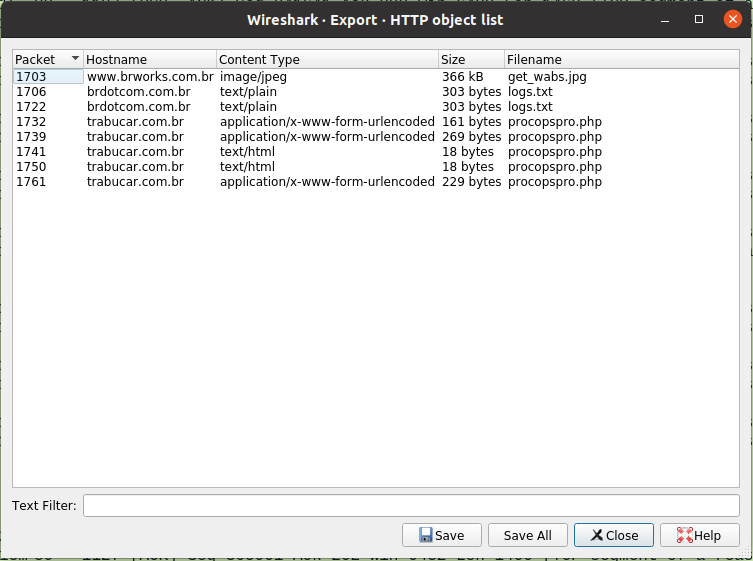
As it is explained in answer 6 we export this file to be able to analyse it in VirusTotal website and this file was identified as a malware.

Knowing that we continued our analysis and because of this image is the malware, downloaded on client (victim’s machine), now it is necessary to understand why the victim downloaded this file.   
 As it is possible to observe the client/victim, make a query request to access on “<https://www.brworks.com.br/>” and he received back *“66.7.200.69”*. Now as it is explained in answer 4 the attacker (that is a man in the middle) carry out a DNS spoofing (Shadow server) attack.

We can just suppose that this is the attack, as we didn’t identify an evident prove that this kind of attack has been carried out by a man in the middle. In fact for this reason it is much better to sniff not on the client-local NS but on geographical route,

for example, between the local-NS and the root-NS. So if a wrong answer is provided to local-NS, this will be cached and therefore will be provided to all clients on the local network that will make this query.

Note: we can’t know if this IP is changed in these years as the capture is made in the year 2010 and the emulation in 2020.

1. Yes, we identify the file *‘get\_wabs.jpg’* as malicious file through the webapp virustotal.com that analyse an uploaded file using a lot different antivirus in parallel.  
   We have followed the following steps to recognize the malicious file:
   1. In Wireshark we have downloaded all the files downloaded during the traffic.pcap capture using the window bar function *“File->Export Objects->HTTP”* and clicked on save all to take all the files.
   2. Upload all files on virustotal.com and find out if the uploaded file is a malware.   
      This is the result with the file *‘get\_wabs.jpg’* downloaded from 66.7.200.69:  
      As it is possible to observe the *‘get\_wabs.jpg’* is detected by 55 over 68 antivirus like a malware: some identify it like a trojan other like a Spyware, but in general like a malware.   
      