Lab 4: Malware Analysis

Objective

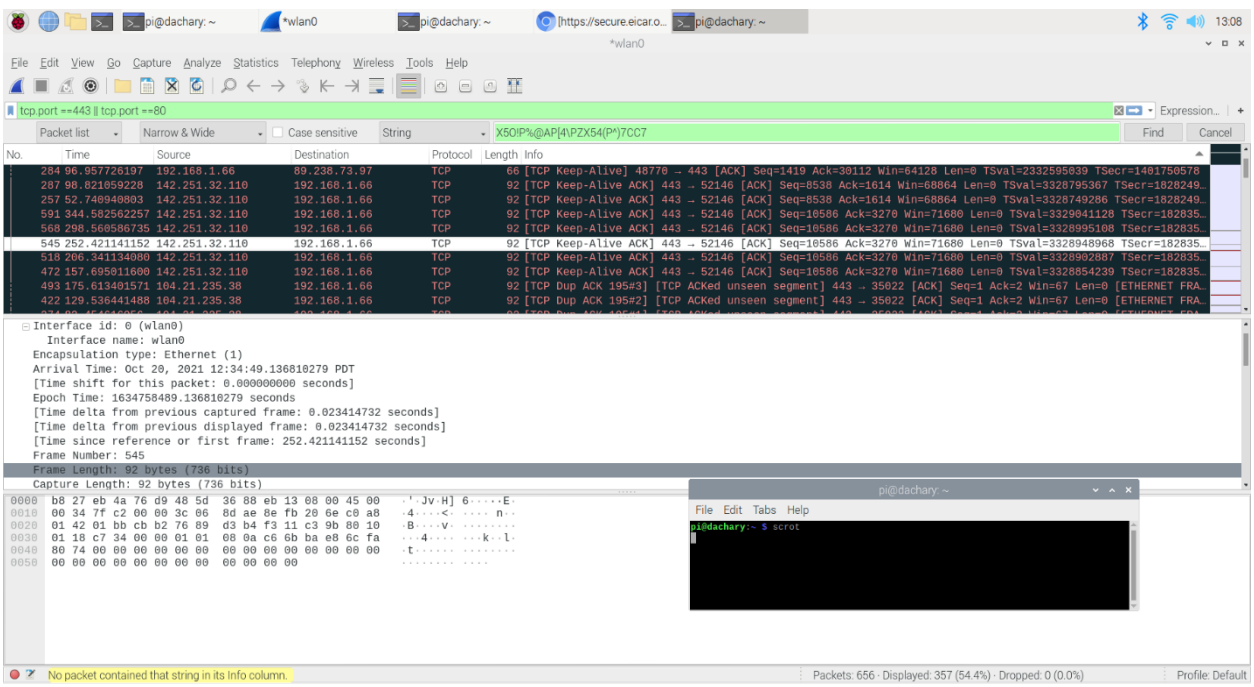
The goal of this lab is to analyze some of the test malware files using various tools. This lab will go over various tools that are used to see downloaded malwares in a system.

Resources Required:

Properly configured raspberry pi, Wireshark, Total Virus and Linux knowledge.

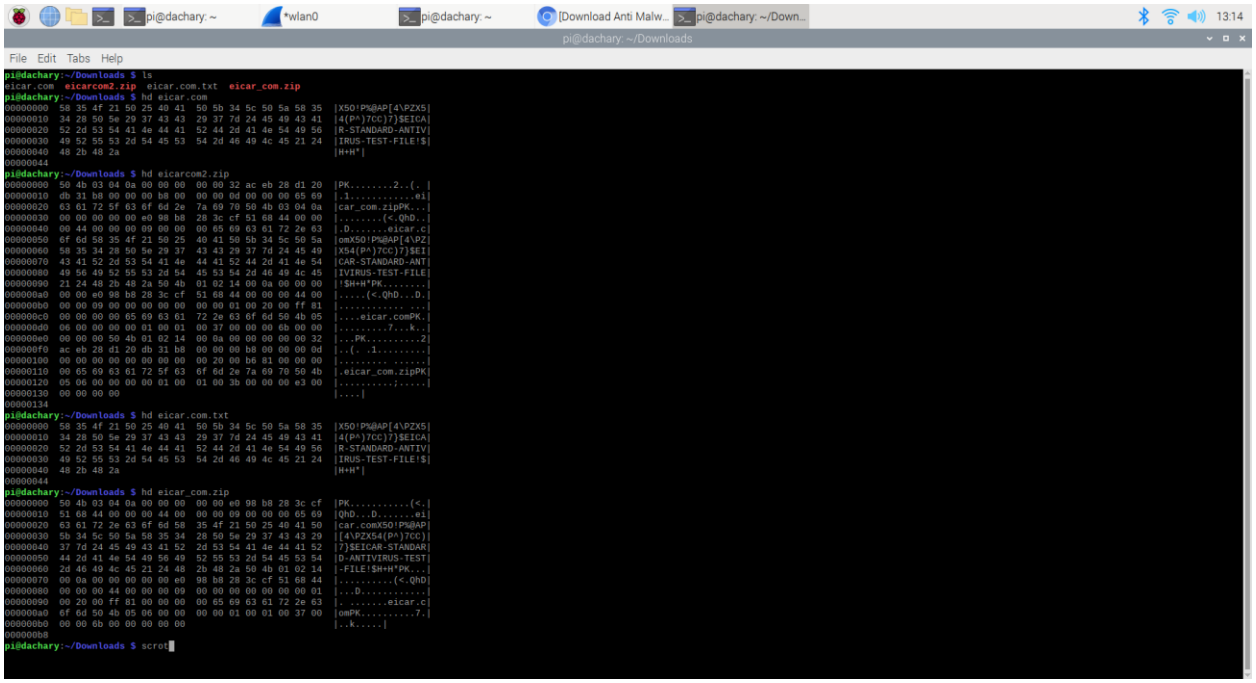
Steps

a. The first step is to download and configure Wireshark on raspberry. After the installation use command **wireshark &** to run Wireshark in the background. Once the Wireshark is up and running set display filter for HTTP or HTTPS by using **tcp.port ==80 || tcp.port ==443.** Then start capturing packet and download four test files from the given website. (https://www.eicar.org). Once all files are downloaded, stop capture and search the given string. If we downloaded from http we would be able to see the strings. Since, http download was not working the https download will not show the string combination in Wireshark. The outcome of the Wireshark capture with not found string is shown below.

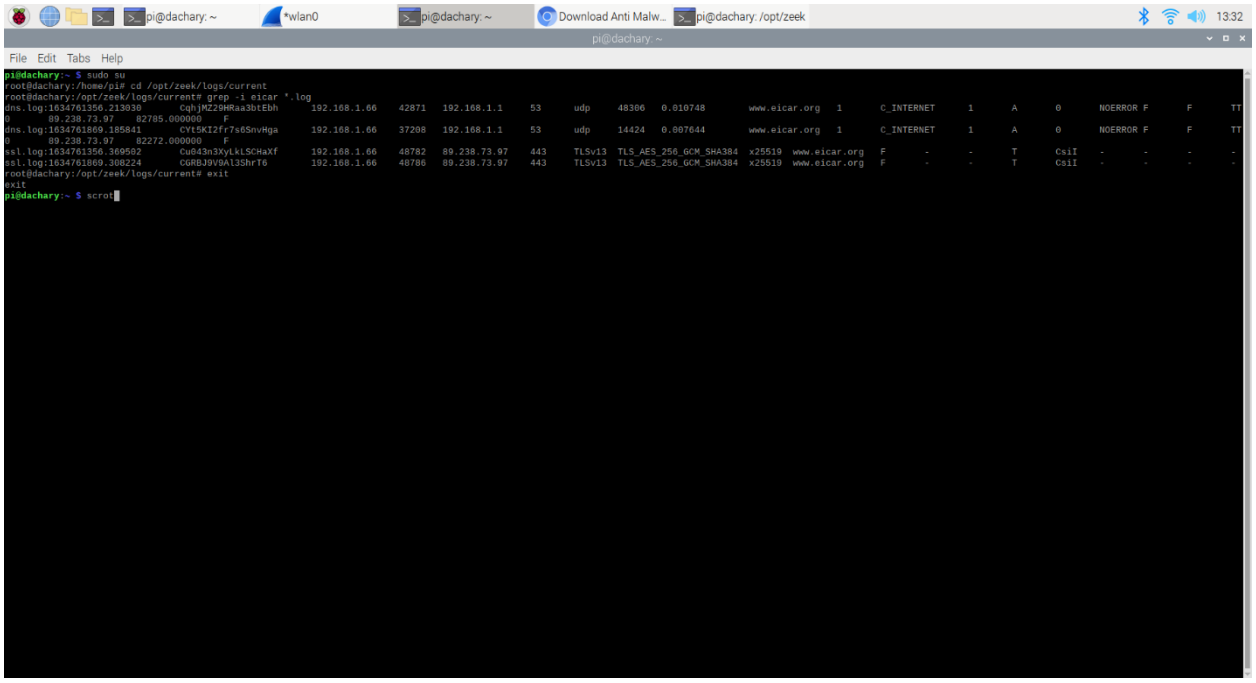


b. The hex dump of all these files is shown in the screenshot below:

Lab 4



c. Now, stop the Wireshark process and run Zeek, while zeek is running download those four files again and find the logs of those files using “grep -i eicar *.log” command inside the /opt/zeek/logs/current directory to see current logs. The output of the log file is shown in the screenshot below.

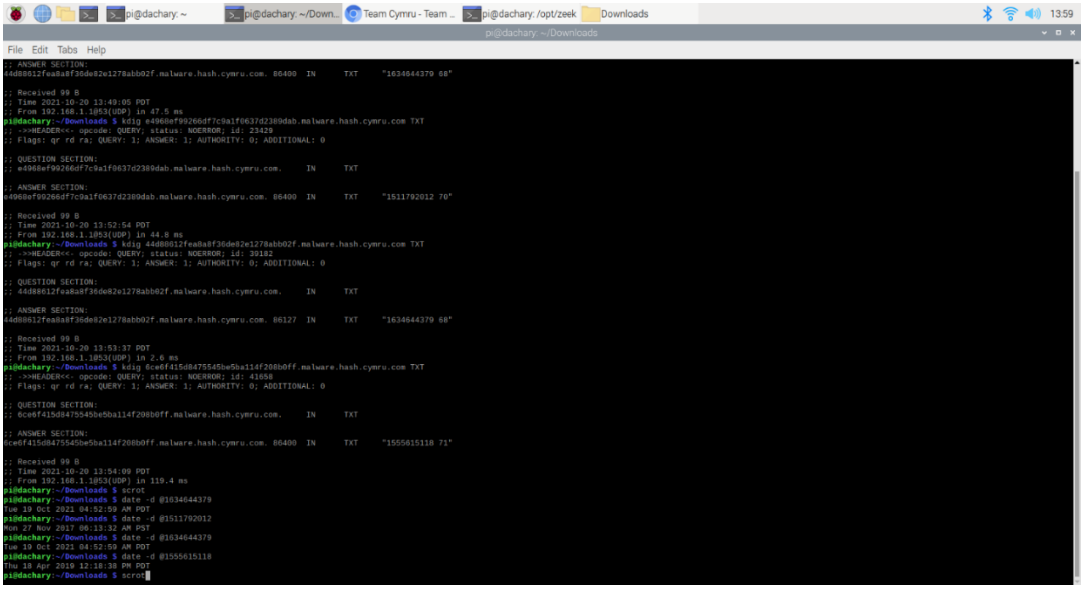


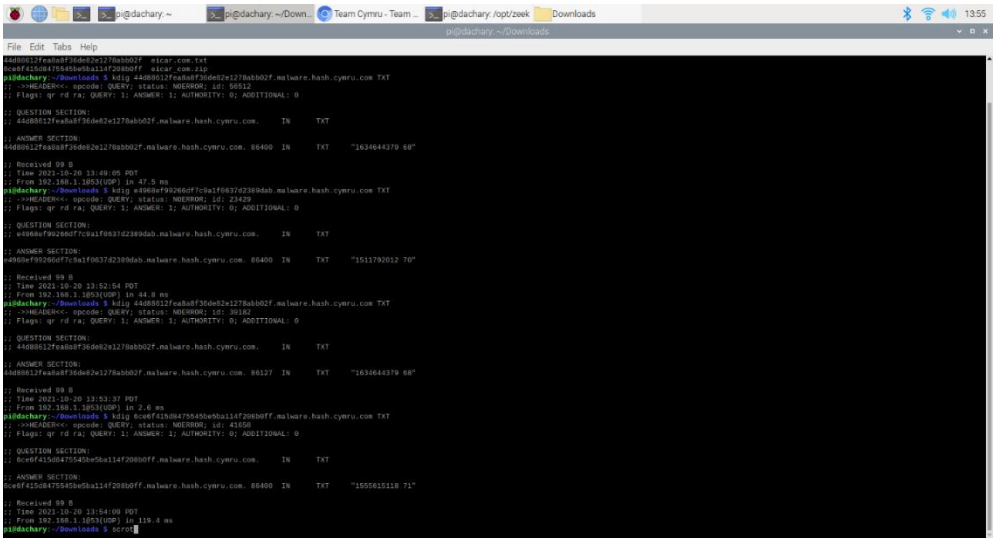
Lab 4

d. Why didn't we see string while using https?
We don't see the string while using https because the https session is encrypted while http packets contain the hyperlinks to https and easily visible as a plain string.

e. Zeek is recording security event or just log?
Looking at the log file, it only shows the downloaded file from the website. Thus, it seems like it only records security event. If it was just a log it should have been a lot of handshakes and all packets to and from the server.

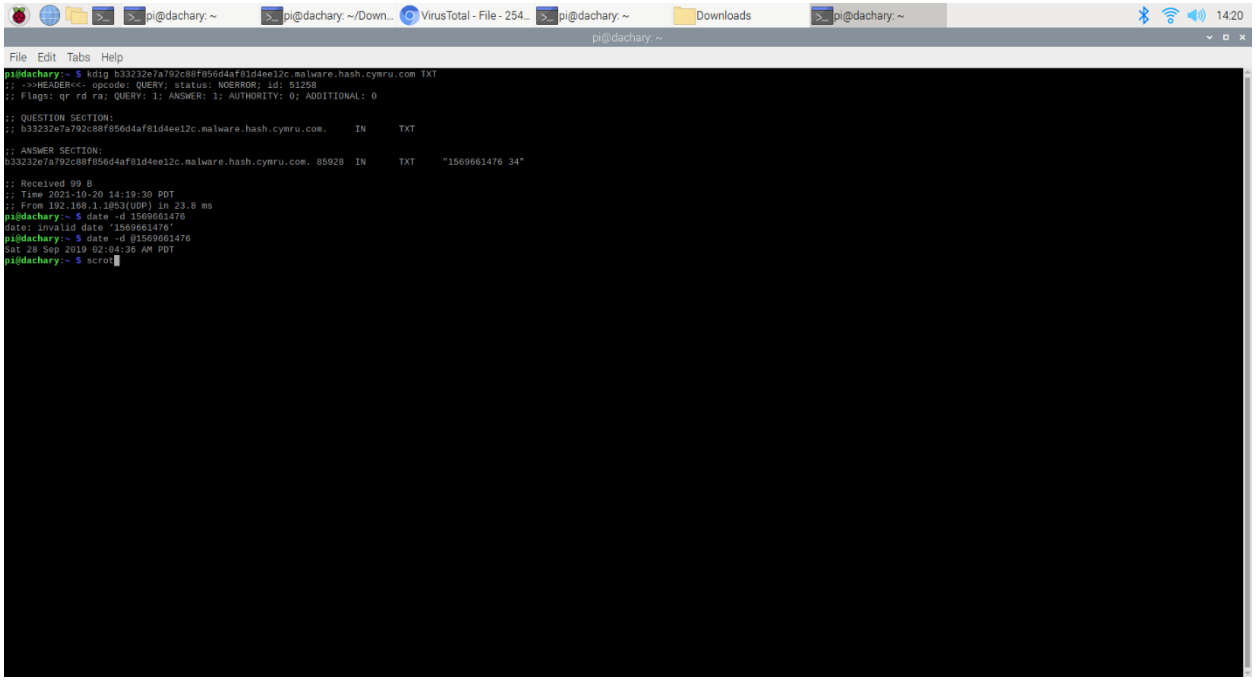
f. Kdig command: The output of the kdig command to all the hashes obtained by using md5 <filename> from the given Malware Hash Repository (MHR0 is shown in the screenshot below. The Malware Hash Repository (MHR) at cymru.com allows for simple online virus checking of file hashes.





Lab 4

g. Kdig of b33232: Similarly, I looked up the kdig as done in the above step for a given hash and the output was as follows.



h. Virustotal: The result of the virus total of the same hash in above step is shown below. This shows that the hash is flagged 36 times as malicious.