

Lab 4: Malware Analysis

Objective

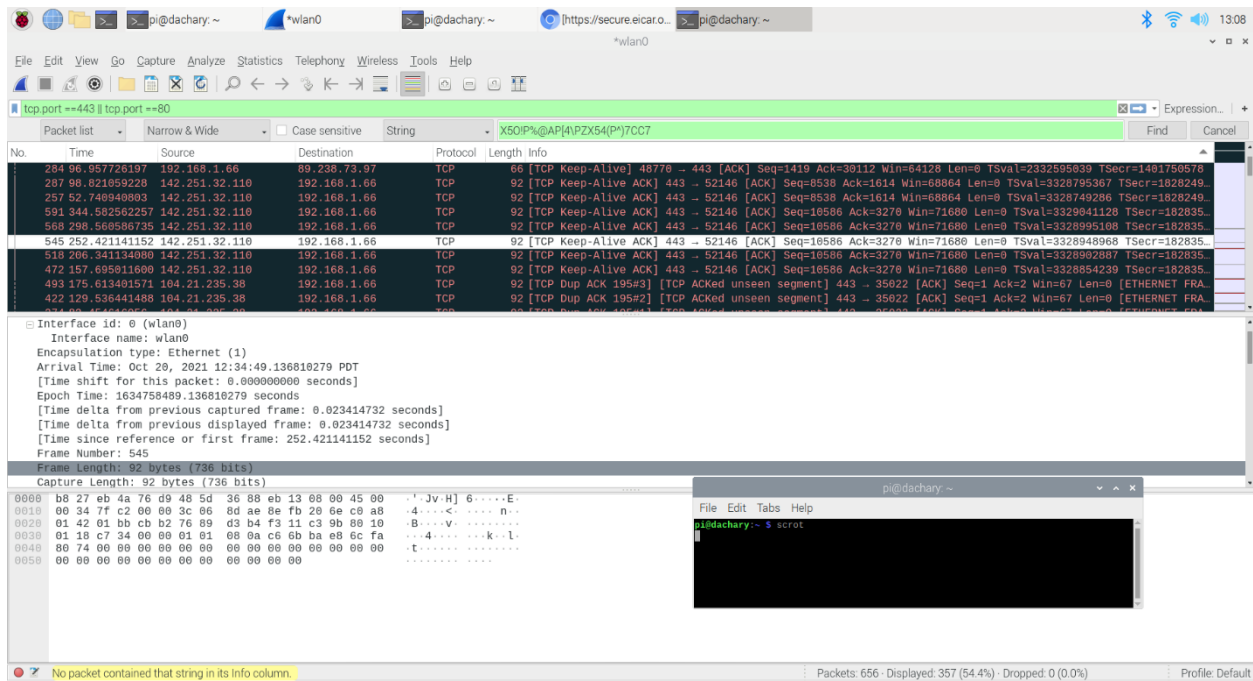
The goal of this lab is to analyze some of the test malware files using various tools. This lab will go over various tools that are used to see downloaded malwares in a system.

Resources Required:

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

Steps

- 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.



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

Lab 4

[illegible]

- 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.

The screenshot shows a Kali Linux terminal window with the following content:

```

pi@dachary: ~
File Edit Tabs Help

pi@dachary:~$ sudo su
root@dachary:/home/pi# cd /opt/zeek/logs/current
root@dachary:/opt/zeek/logs/current# grep -i eicar *.log
dns.log:1634761356.213036    CqHjWZ9H8aa3btEbh      192.168.1.66      42871  192.168.1.1      53      udp      48366      0.010748      www.eicar.org      1      C      INTERNET      1      A      0      NOERROR      F      F      TT
    89.238.73.97      82785.000000      F      192.168.1.66      37208      192.168.1.1      53      udp      14424      0.007644      www.eicar.org      1      C      INTERNET      1      A      0      NOERROR      F      F      TT
    89.238.73.97      82772.000000      F      192.168.1.66      48782      89.238.73.97      443      TLSv13      TLS_AES_256_GCM_SHA384      x25519      www.eicar.org      F      -      -      T      CslI      -      -      -      -
    ssl.log:1634761356.369502      Cu843n3XyLkLSchXf      192.168.1.66      48786      89.238.73.97      443      TLSv13      TLS_AES_256_GCM_SHA384      x25519      www.eicar.org      F      -      -      T      CslI      -      -      -      -
    ssl.log:1634761869.308224      CQRBJ9V9Al3ShrT6      192.168.1.66      48786      89.238.73.97      443      TLSv13      TLS_AES_256_GCM_SHA384      x25519      www.eicar.org      F      -      -      T      CslI      -      -      -      -
root@dachary:/opt/zeek/logs/current# exit
pi@dachary:~$ scroll

```

Lab 4

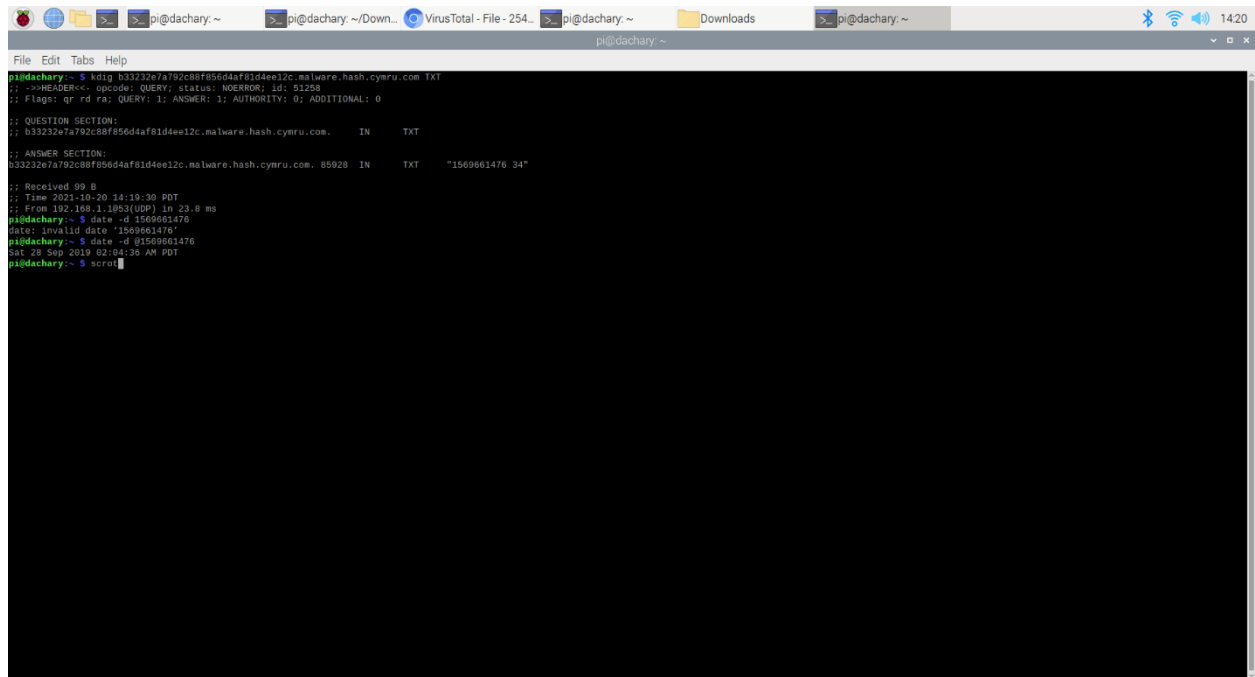
- d. Why didn't we see string while using https?
We don't see the string while using https because the https session is encrypted while http packets contain the hyperlinks to https and easily visible as a plain string.
- e. Zeek is recording security event or just log?
Looking at the log file, it only 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.

```
pi@dachary: ~/Downloads
File Edit Tabs Help
;; ANSWER SECTION:
44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com. 86400 IN TXT "1634644379 68"
;; Received 99 B
;; Time 2021-10-20 13:49:09 PDT
;; From 192.168.1.100(UDP) in 47.5 ms
pi@dachary:~/Downloads $ kdig 44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com TXT
;;->>HEADER<<: opcode: QUERY, status: NOERROR, id: 23429
;; Flags: qr rd ra QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0
;; QUESTION SECTION:
;; 44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com. IN TXT
;; ANSWER SECTION:
e496bf99266f7c9a1f0637d238dab.malware.hash.cymru.com. 86400 IN TXT "1511792012 70"
;; Received 99 B
;; Time 2021-10-20 13:52:54 PDT
;; From 192.168.1.100(UDP) in 44.8 ms
pi@dachary:~/Downloads $ kdig 44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com TXT
;;->>HEADER<<: opcode: QUERY, status: NOERROR, id: 39182
;; Flags: qr rd ra QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0
;; QUESTION SECTION:
;; 44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com. IN TXT
;; ANSWER SECTION:
44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com. 86127 IN TXT "1634644379 68"
;; Received 99 B
;; Time 2021-10-20 13:53:37 PDT
;; From 192.168.1.100(UDP) in 2.6 ms
pi@dachary:~/Downloads $ kdig ccebf415d8475d45b0a114f208b0ff.malware.hash.cymru.com TXT
;;->>HEADER<<: opcode: QUERY, status: NOERROR, id: 42068
;; Flags: qr rd ra QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0
;; QUESTION SECTION:
;; ccebf415d8475d45b0a114f208b0ff.malware.hash.cymru.com. IN TXT
;; ANSWER SECTION:
ccebf415d8475d45b0a114f208b0ff.malware.hash.cymru.com. 86400 IN TXT "1555615118 71"
;; Received 99 B
;; Time 2021-10-20 13:54:09 PDT
;; From 192.168.1.100(UDP) in 119.4 ms
pi@dachary:~/Downloads $ sort
pi@dachary:~/Downloads $ date -d @1634644379
Tue 19 Oct 2021 04:52:59 AM PDT
pi@dachary:~/Downloads $ date -d @1511792012
Mon 27 Nov 2017 06:13:32 AM PST
pi@dachary:~/Downloads $ date -d @1634644379
Tue 19 Oct 2021 04:52:59 AM PDT
pi@dachary:~/Downloads $ date -d @1555615118
Thu 18 Apr 2019 12:18:38 PM PDT
pi@dachary:~/Downloads $ sort
```

```
pi@dachary: ~/Downloads
File Edit Tabs Help
44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com. 86400 IN TXT "1634644379 68"
;; Received 99 B
;; Time 2021-10-20 13:49:09 PDT
;; From 192.168.1.100(UDP) in 47.5 ms
pi@dachary:~/Downloads $ kdig 44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com TXT
;;->>HEADER<<: opcode: QUERY, status: NOERROR, id: 23429
;; Flags: qr rd ra QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0
;; QUESTION SECTION:
;; 44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com. IN TXT
;; ANSWER SECTION:
e496bf99266f7c9a1f0637d238dab.malware.hash.cymru.com. 86400 IN TXT "1511792012 70"
;; Received 99 B
;; Time 2021-10-20 13:52:54 PDT
;; From 192.168.1.100(UDP) in 44.8 ms
pi@dachary:~/Downloads $ kdig 44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com TXT
;;->>HEADER<<: opcode: QUERY, status: NOERROR, id: 39182
;; Flags: qr rd ra QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0
;; QUESTION SECTION:
;; 44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com. IN TXT
;; ANSWER SECTION:
44d8b012feab8f3d6e2e1278abb02f.malware.hash.cymru.com. 86127 IN TXT "1634644379 68"
;; Received 99 B
;; Time 2021-10-20 13:53:37 PDT
;; From 192.168.1.100(UDP) in 2.6 ms
pi@dachary:~/Downloads $ kdig ccebf415d8475d45b0a114f208b0ff.malware.hash.cymru.com TXT
;;->>HEADER<<: opcode: QUERY, status: NOERROR, id: 42068
;; Flags: qr rd ra QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0
;; QUESTION SECTION:
;; ccebf415d8475d45b0a114f208b0ff.malware.hash.cymru.com. IN TXT
;; ANSWER SECTION:
ccebf415d8475d45b0a114f208b0ff.malware.hash.cymru.com. 86400 IN TXT "1555615118 71"
;; Received 99 B
;; Time 2021-10-20 13:54:09 PDT
;; From 192.168.1.100(UDP) in 119.4 ms
pi@dachary:~/Downloads $ sort
```

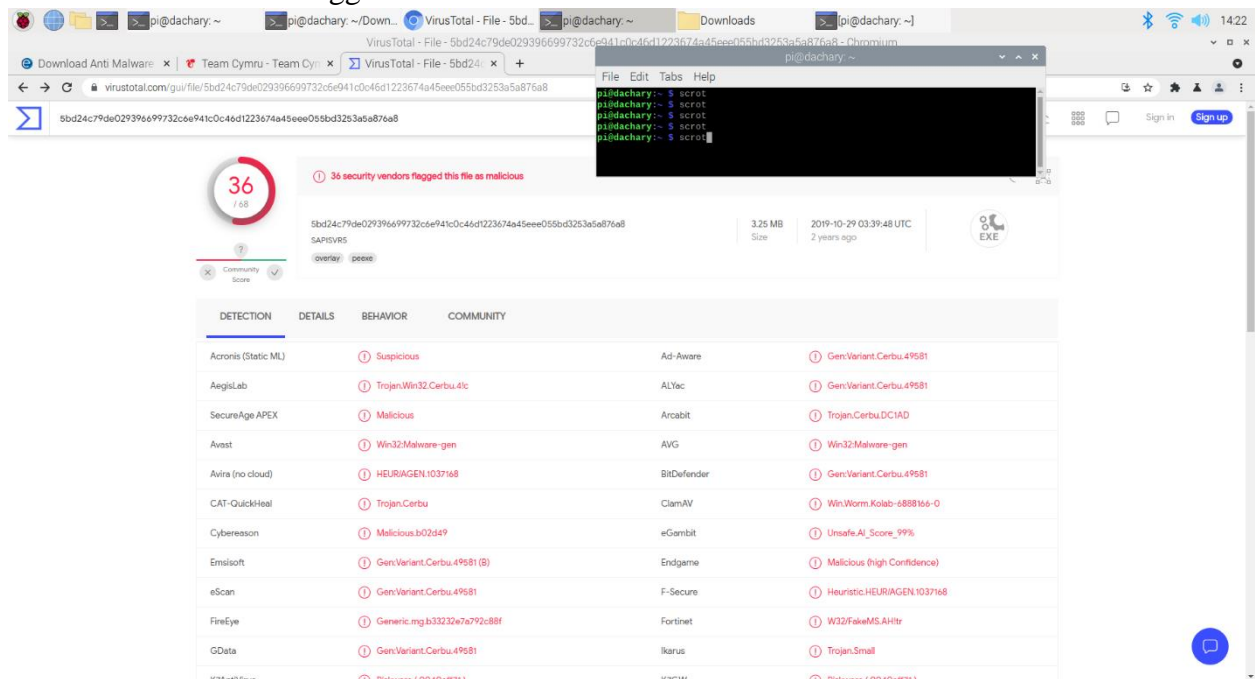
Lab 4

- 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.



```
pi@dachary: ~  
pi@dachary: ~$ kdig b3323267a792c88f856d4af81d4ee12c.malware.hash.cymru.com.TXT  
;;>>>HEADER<<< opcode: QUERY; status: NOERROR; id: 51258  
;; Flags: qr rd ra; QUERY: 1; ANSWER: 1; AUTHORITY: 0; ADDITIONAL: 0  
  
;; QUESTION SECTION:  
;; b3323267a792c88f856d4af81d4ee12c.malware.hash.cymru.com. IN TXT  
  
;; ANSWER SECTION:  
b3323267a792c88f856d4af81d4ee12c.malware.hash.cymru.com. 85928 IN TXT "1569661476"  
  
;; Received 99 B  
;; Time 2021-10-20 14:19:39 PDT  
;; From 192.168.1.1053 (00P) in 23.8 ms  
pi@dachary: ~$ date -d 1569661476  
date: invalid date "1569661476"  
pi@dachary: ~$ date -d @1569661476  
Sat 28 Sep 2019 02:14:38 AM PDT  
pi@dachary: ~$
```

- 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.



VirusTotal - File - 5bd24c79de029396699732c6e941c0c46d1223674a45eee055bd3253a5a876a8

36 / 68 security vendors flagged this file as malicious

5bd24c79de029396699732c6e941c0c46d1223674a45eee055bd3253a5a876a8
SAPISVR5
3.25 MB
2019-10-29 03:39:48 UTC
2 years ago

DETECTION	DETAILS	BEHAVIOR	COMMUNITY
Acronis (Static ML)	⚠ Suspicious	Ad-Aware	⚠ Gen:Variant.Cerbu.49581
AegisLab	⚠ Trojan.Win32.Cerbu.4/c	ALYac	⚠ Gen:Variant.Cerbu.49581
SecureAge APEX	⚠ Malicious	Arcabit	⚠ Trojan.Cerbu.DC1AD
Avast	⚠ Win32/Malware-gen	AVG	⚠ Win32/Malware-gen
Avira (no cloud)	⚠ HEUR/AGEN.1037168	BitDefender	⚠ Gen:Variant.Cerbu.49581
CAT-QuickHeal	⚠ Trojan.Cerbu	ClamAV	⚠ Win/Worm.Kolab-688166-O
Cyberesson	⚠ Malicious.b02d49	eGambit	⚠ Unsafe.AI_Score_99%
Emnisoft	⚠ Gen:Variant.Cerbu.49581 (B)	Endgame	⚠ Malicious (high Confidence)
eScan	⚠ Gen:Variant.Cerbu.49581	F-Secure	⚠ Heuristic.HEUR/AGEN.1037168
FireEye	⚠ Generic.mg.b3323267a792c88f	Fortinet	⚠ W32/FakeMS.AH/tr
GData	⚠ Gen:Variant.Cerbu.49581	Ikarus	⚠ Trojan.Small
K7AntiVirus	⚠ Disinfect / (P)J2WFFP11	K7CW	⚠ Disinfect / (P)J2WFFP11