COMPUTER NETWORKS LAB
INDUSTRY PROBLEM – MALWARE TRAFFIC ANALYSIS USING WIRESHARK
REPORT

Team Member Names and SRNs:-

1. Vinti Agrawal	PES2UG20CS385
2. Vishwa Mehul Mehta	PES2UG20CS389
3. Vismaya R	PES2UG20CS391

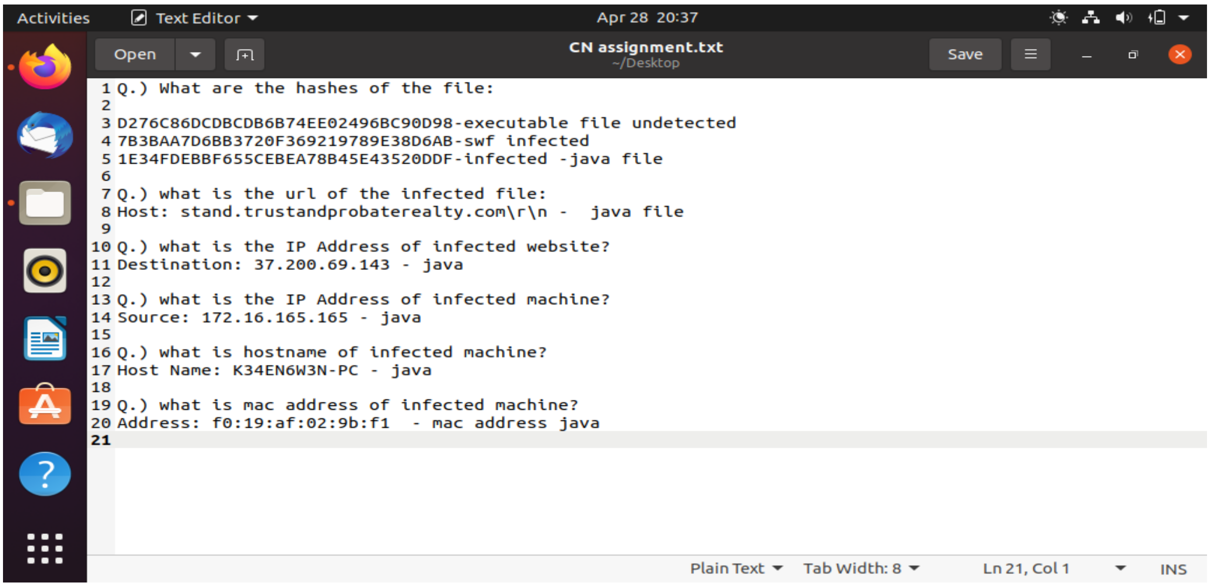
The following questions have been answered after analyzing the wireshark capture when a web page with files that may contain malware were downloaded.

We extracted the files that were downloaded in the capture and then they were uploaded to a hash generator. This hash was then searched in the VirusTotal website to find out if the file was infected. The website shows the degree of malware content in the file with that hash.

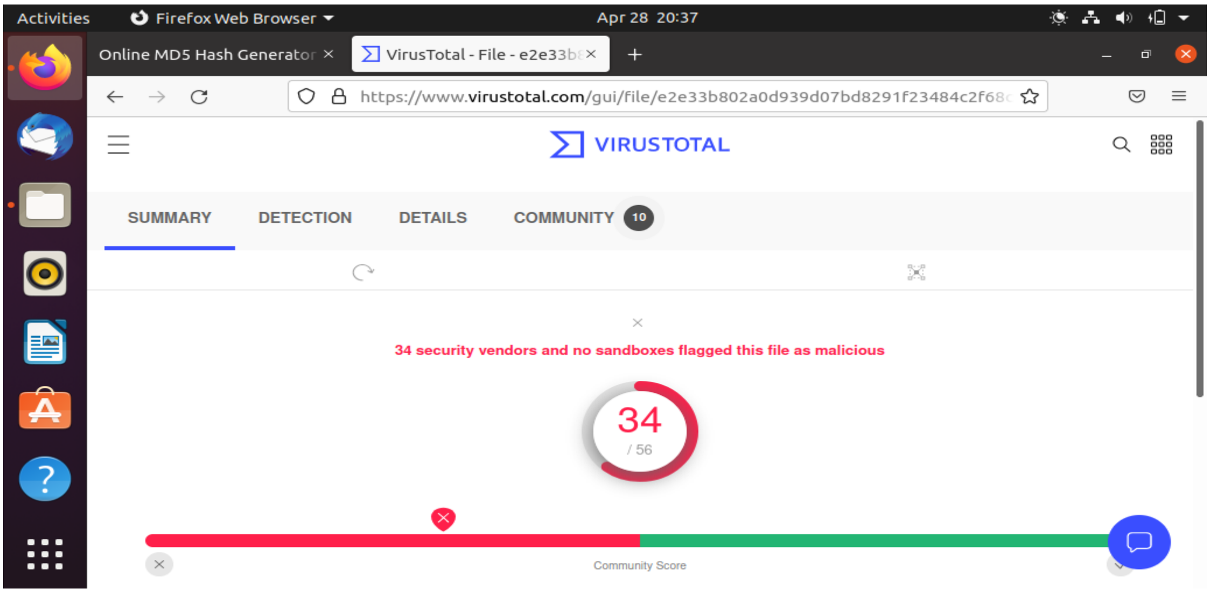
Now if the file was malware free it was safe to assume that the website and the file is safe to use and load.

If on the other hand if the file is infected then we find the host name and host url of the website from which the file was extracted and also the source and destination IP Addresses along with the MAC Address of the host machine.

This method is used to analyse the traffic that may contain malware and prevent us from downloading these files to protect our systems from threats.

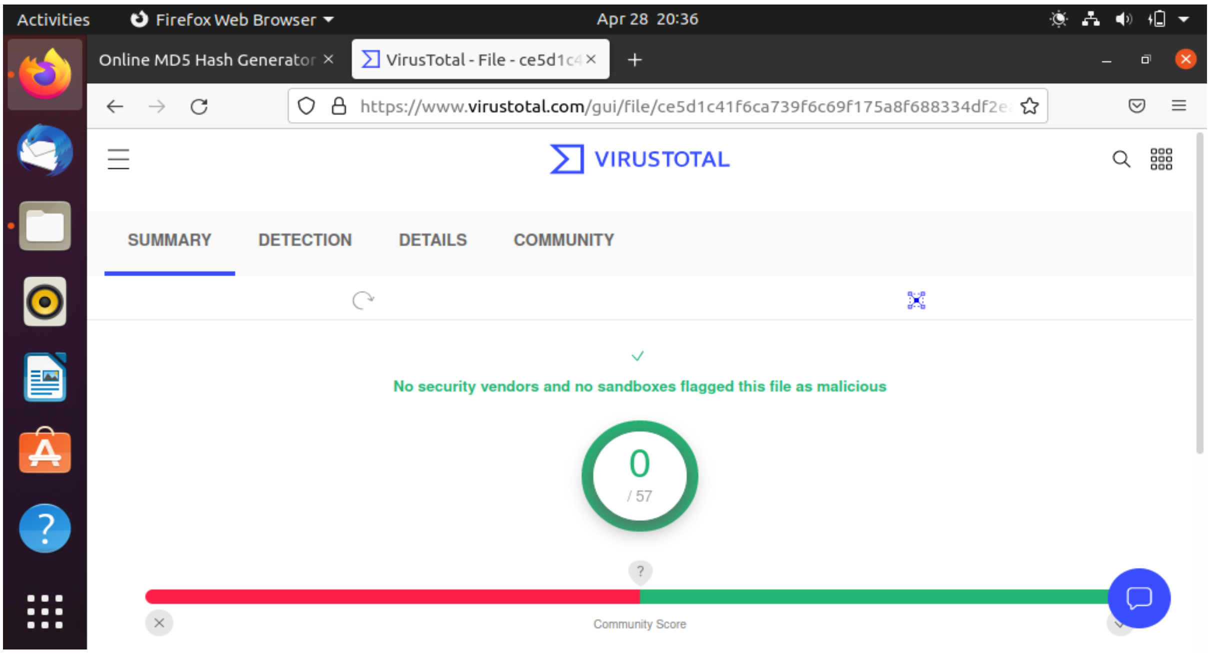


```
Q.) What are the hashes of the file:

D276C86DCDBCDB6B74EE02496BC90D98-executable file undetected
7B3BAA7D6BB3720F369219789E38D6AB-swf infected
1E34FDEBBF655CEBEA78B45E43520DDF-infected -java file

Q.) what is the url of the infected file:
Host: stand.trustandprobaterealty.com\r\n -  java file

Q.) what is the IP Address of infected website?
Destination: 37.200.69.143 - java

Q.) what is the IP Address of infected machine?
Source: 172.16.165.165 - java

Q.) what is hostname of infected machine?
Host Name: K34EN6W3N-PC - java

Q.) what is mac address of infected machine?
Address: f0:19:af:02:9b:f1  - mac address java
```



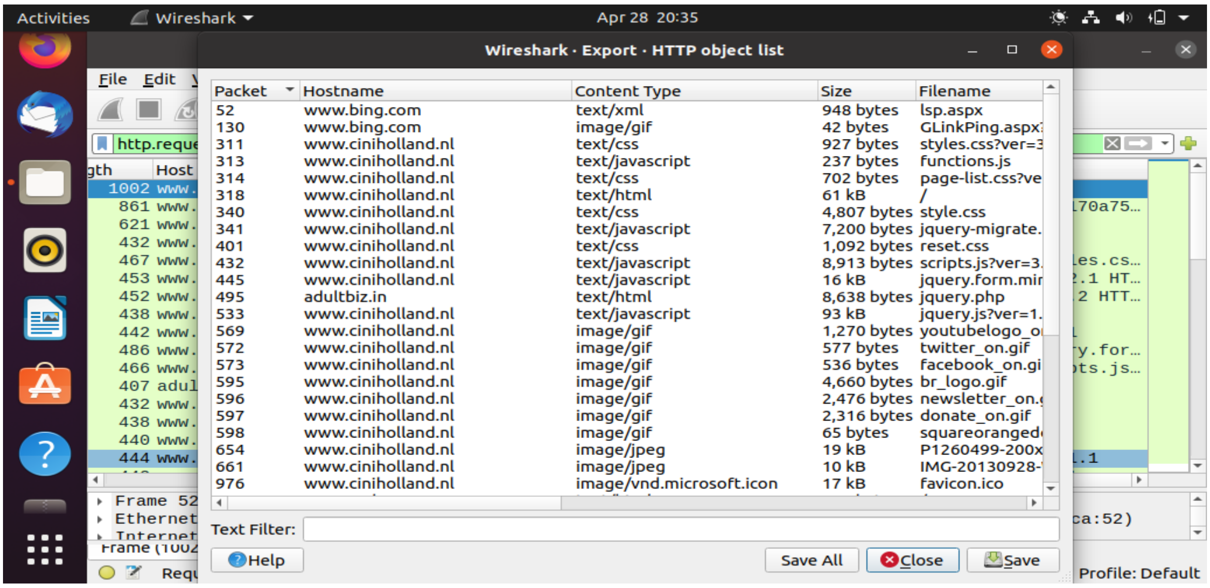
Activities
Firefox Web Browser
Apr 28 20:37
Online MD5 Hash Generator
VirusTotal - File - e2e33b
https://www.virustotal.com/gui/file/e2e33b802a0d939d07bd8291f23484c2f68
VIRUSTOTAL
SUMMARY
DETECTION
DETAILS
COMMUNITY 10
34
/ 56
Community Score

34 security vendors and no sandboxes flagged this file as malicious



Activities
Firefox Web Browser
Apr 28 20:36
Online MD5 Hash Generator
VirusTotal - File - ce5d1c
https://www.virustotal.com/gui/file/ce5d1c41f6ca739f6c69f175a8f688334df2e
VIRUSTOTAL
SUMMARY
DETECTION
DETAILS
COMMUNITY
0
/ 57
Community Score

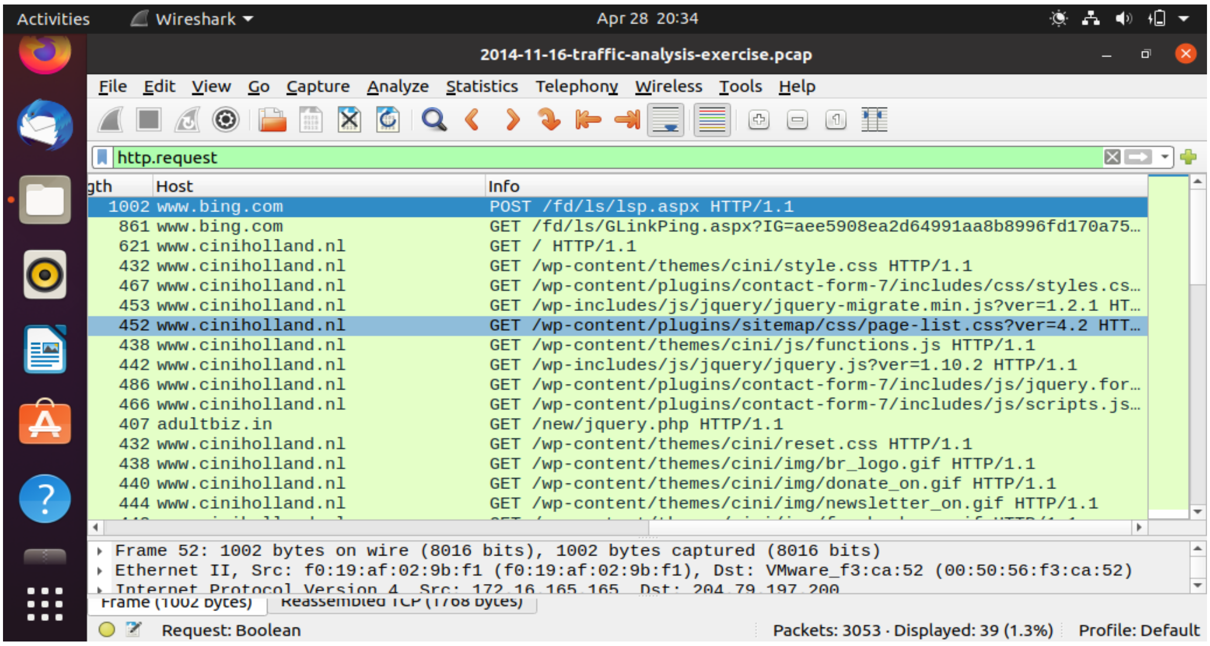
No security vendors and no sandboxes flagged this file as malicious



Packet	Hostname	Content Type	Size	Filename
52	www.bing.com	text/xml	948 bytes	lsp.aspx
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx
311	www.ciniholland.nl	text/css	927 bytes	styles.css?ver=3
313	www.ciniholland.nl	text/javascript	237 bytes	functions.js
314	www.ciniholland.nl	text/css	702 bytes	page-list.css?ve
318	www.ciniholland.nl	text/html	61 kB	/
340	www.ciniholland.nl	text/css	4,807 bytes	style.css
341	www.ciniholland.nl	text/javascript	7,200 bytes	jquery-migrate.
401	www.ciniholland.nl	text/css	1,092 bytes	reset.css
432	www.ciniholland.nl	text/javascript	8,913 bytes	scripts.js?ver=3.
445	www.ciniholland.nl	text/javascript	16 kB	jquery.form.mir
495	adultbiz.in	text/html	8,638 bytes	jquery.php
533	www.ciniholland.nl	text/javascript	93 kB	jquery.js?ver=1.
569	www.ciniholland.nl	image/gif	1,270 bytes	youtubelogo_o
572	www.ciniholland.nl	image/gif	577 bytes	twitter_on.gif
573	www.ciniholland.nl	image/gif	536 bytes	facebook_on.gi
595	www.ciniholland.nl	image/gif	4,660 bytes	br_logo.gif
596	www.ciniholland.nl	image/gif	2,476 bytes	newsletter_on.
597	www.ciniholland.nl	image/gif	2,316 bytes	donate_on.gif
598	www.ciniholland.nl	image/gif	65 bytes	squareorange
654	www.ciniholland.nl	image/jpeg	19 kB	P1260499-200x
661	www.ciniholland.nl	image/jpeg	10 kB	IMG-20130928-
976	www.ciniholland.nl	image/vnd.microsoft.icon	17 kB	favicon.ico

Text Filter:

Help
Save All
Close
Save
Profile: Default



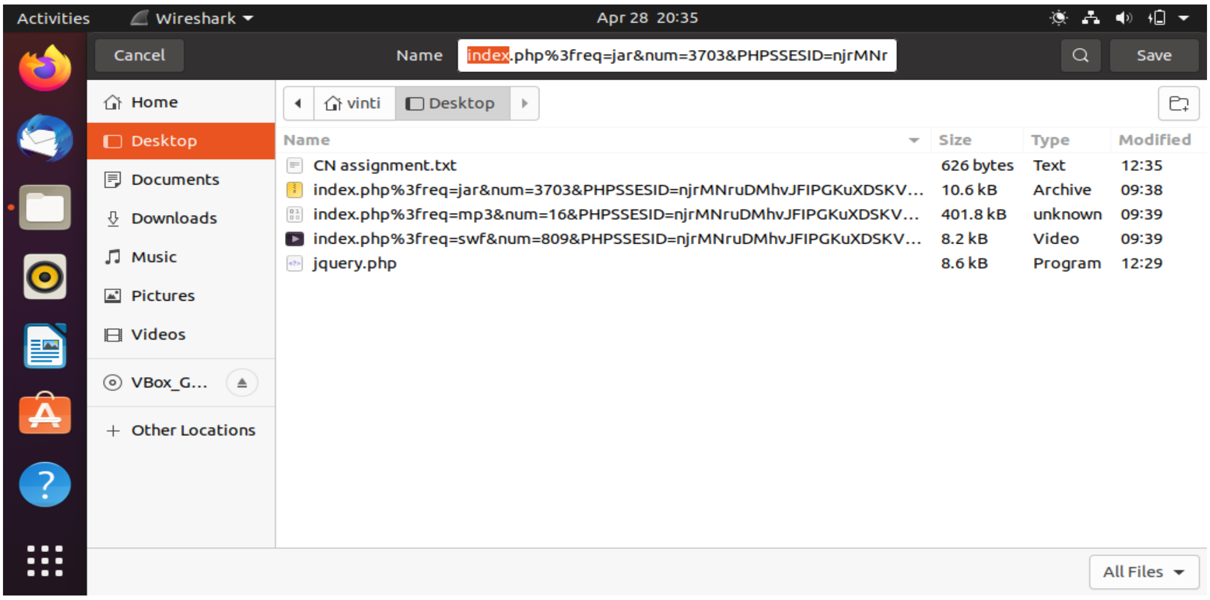
Activities
Wireshark
Apr 28 20:34
2014-11-16-traffic-analysis-exercise.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request

```
gth  Host                  Info
1002 www.bing.com          POST /fd/ls/lsp.aspx HTTP/1.1
 861 www.bing.com          GET /fd/ls/GLinkPing.aspx?IG=aee5908ea2d64991aa8b8996fd170a75…
 621 www.ciniholland.nl    GET / HTTP/1.1
 432 www.ciniholland.nl    GET /wp-content/themes/cini/style.css HTTP/1.1
 467 www.ciniholland.nl    GET /wp-content/plugins/contact-form-7/includes/css/styles.cs…
 453 www.ciniholland.nl    GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HT…
 452 www.ciniholland.nl    GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTT…
 438 www.ciniholland.nl    GET /wp-content/themes/cini/js/functions.js HTTP/1.1
 442 www.ciniholland.nl    GET /wp-includes/js/jquery/jquery.js?ver=1.10.2 HTTP/1.1
 486 www.ciniholland.nl    GET /wp-content/plugins/contact-form-7/includes/js/jquery.for…
 466 www.ciniholland.nl    GET /wp-content/plugins/contact-form-7/includes/js/scripts.js…
 407 adultbiz.in           GET /new/jquery.php HTTP/1.1
 432 www.ciniholland.nl    GET /wp-content/themes/cini/reset.css HTTP/1.1
 438 www.ciniholland.nl    GET /wp-content/themes/cini/img/br_logo.gif HTTP/1.1
 440 www.ciniholland.nl    GET /wp-content/themes/cini/img/donate_on.gif HTTP/1.1
 444 www.ciniholland.nl    GET /wp-content/themes/cini/img/newsletter_on.gif HTTP/1.1

Frame 52: 1002 bytes on wire (8016 bits), 1002 bytes captured (8016 bits)
Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: VMware_f3:ca:52 (00:50:56:f3:ca:52)
Internet Protocol Version 4, Src: 172.16.165.165, Dst: 204.79.197.200
```

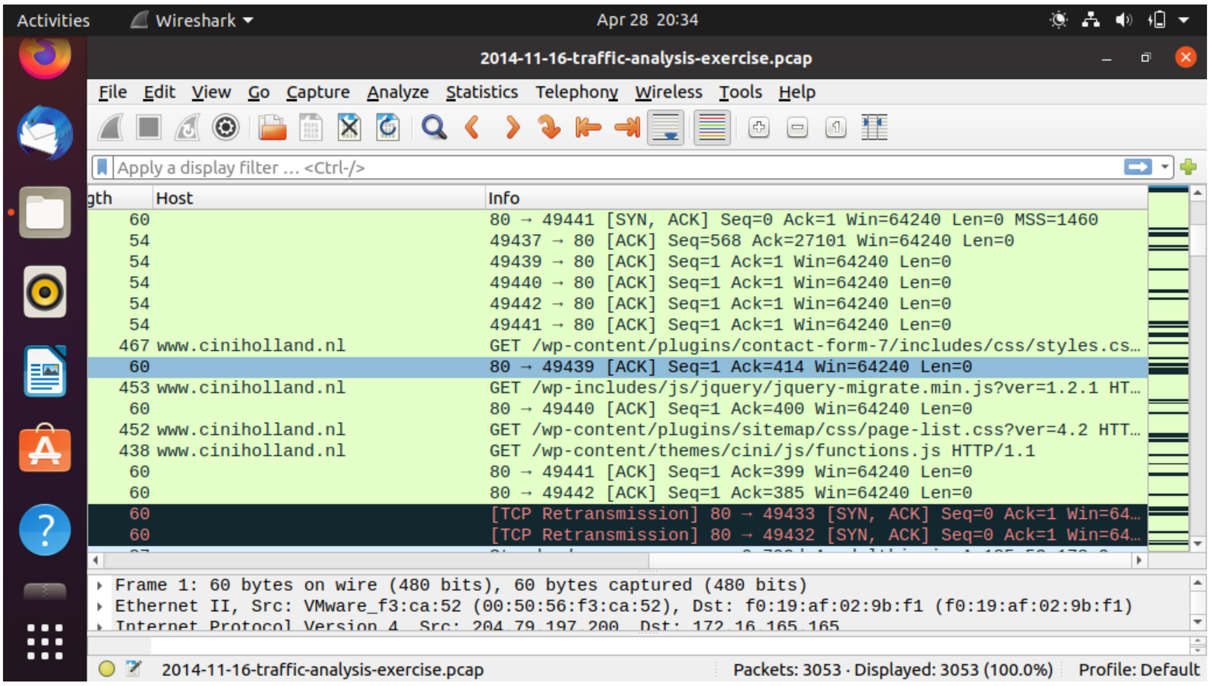
Frame (1002 bytes) Reassembled TCP (1768 bytes)

Request: Boolean   Packets: 3053 · Displayed: 39 (1.3%)   Profile: Default



Name index.php%3freq=jar&num=3703&PHPSSESID=njrMNr

Name	Size	Type	Modified
CN assignment.txt	626 bytes	Text	12:35
index.php%3freq=jar&num=3703&PHPSSESID=njrMNruDMhvJFIPGKuXDSKV…	10.6 kB	Archive	09:38
index.php%3freq=mp3&num=16&PHPSSESID=njrMNruDMhvJFIPGKuXDSKV…	401.8 kB	unknown	09:39
index.php%3freq=swf&num=809&PHPSSESID=njrMNruDMhvJFIPGKuXDSKV…	8.2 kB	Video	09:39
jquery.php	8.6 kB	Program	12:29

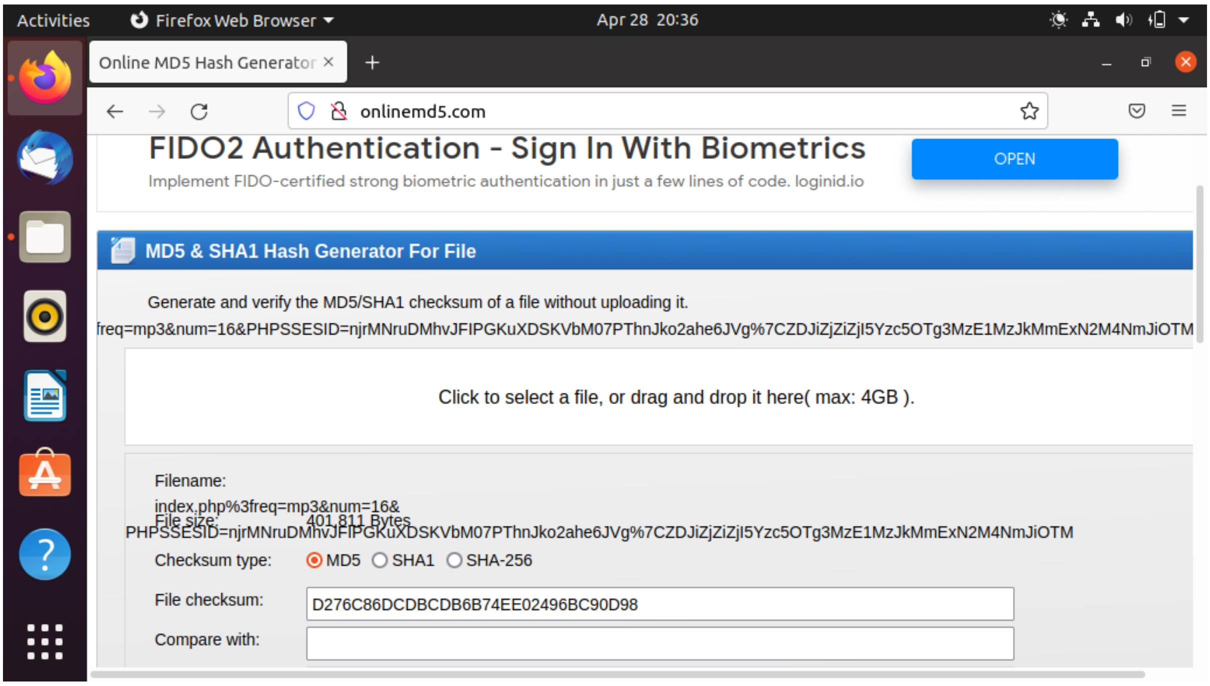

Activities
Wireshark
Apr 28 20:34
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

2014-11-16-traffic-analysis-exercise.pcap

```
gth  Host                   Info
  60                        80 → 49441 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  54                        49437 → 80 [ACK] Seq=568 Ack=27101 Win=64240 Len=0
  54                        49439 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  54                        49440 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  54                        49442 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  54                        49441 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 467 www.ciniholland.nl     GET /wp-content/plugins/contact-form-7/includes/css/styles.cs…
  60                        80 → 49439 [ACK] Seq=1 Ack=414 Win=64240 Len=0
 453 www.ciniholland.nl     GET /wp-includes/js/jquery/jquery-migrate.min.js?ver=1.2.1 HT…
  60                        80 → 49440 [ACK] Seq=1 Ack=400 Win=64240 Len=0
 452 www.ciniholland.nl     GET /wp-content/plugins/sitemap/css/page-list.css?ver=4.2 HTT…
 438 www.ciniholland.nl     GET /wp-content/themes/cini/js/functions.js HTTP/1.1
  60                        80 → 49441 [ACK] Seq=1 Ack=399 Win=64240 Len=0
  60                        80 → 49442 [ACK] Seq=1 Ack=385 Win=64240 Len=0
  60                        [TCP Retransmission] 80 → 49433 [SYN, ACK] Seq=0 Ack=1 Win=64…
  60                        [TCP Retransmission] 80 → 49432 [SYN, ACK] Seq=0 Ack=1 Win=64…
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
› Ethernet II, Src: VMware_f3:ca:52 (00:50:56:f3:ca:52), Dst: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1)
› Internet Protocol Version 4, Src: 204.79.197.200, Dst: 172.16.165.165
```

2014-11-16-traffic-analysis-exercise.pcap   Packets: 3053 · Displayed: 3053 (100.0%)   Profile: Default



FIDO2 Authentication - Sign In With Biometrics

Implement FIDO-certified strong biometric authentication in just a few lines of code. loginid.io

MD5 & SHA1 Hash Generator For File

Generate and verify the MD5/SHA1 checksum of a file without uploading it.

freq=mp3&num=16&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM

Click to select a file, or drag and drop it here(max: 4GB).

Filename: index.php%3freq=mp3&num=16&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg%7CZDJiZjZiZjI5Yzc5OTg3MzE1MzJkMmExN2M4NmJiOTM

File size: 401,811 Bytes

Checksum type: ● MD5 ○ SHA1 ○ SHA-256

File checksum: D276C86DCDBCDB6B74EE02496BC90D98

Compare with: