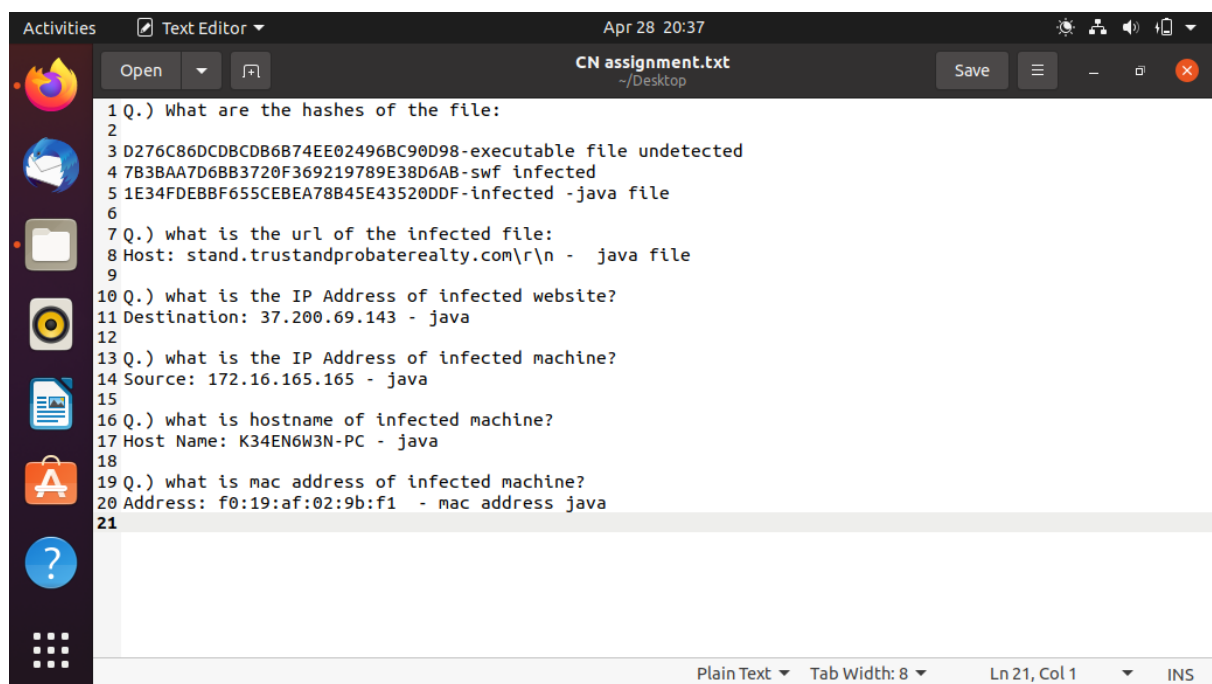


COMPUTER NETWORKS LAB
INDUSTRY PROBLEM – MALWARE TRAFFIC ANALYSIS USING
WIRESHARK
SCREENSHOTS

Team Member Names and SRNs:-

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



The screenshot shows a Linux desktop with a text editor window titled "CN assignment.txt" open. The window contains a list of 21 questions and answers related to malware analysis. The questions are numbered 1 through 21, and the answers are provided for each. The text editor window is located in the center of the screen, with a sidebar on the left showing various application icons. The status bar at the bottom of the window indicates the current line and column (Ln 21, Col 1) and the file encoding (INS).

```
1 Q.) What are the hashes of the file:
2
3 D276C86DCDBCDB6B74EE02496BC90D98-executable file undetected
4 7B3BAA7D6BB3720F369219789E38D6AB-swf infected
5 1E34FDEBBF655CEBEA78B45E43520DDF-infected -java file
6
7 Q.) what is the url of the infected file:
8 Host: stand.trustandprobaterealty.com\r\n - java file
9
10 Q.) what is the IP Address of infected website?
11 Destination: 37.200.69.143 - java
12
13 Q.) what is the IP Address of infected machine?
14 Source: 172.16.165.165 - java
15
16 Q.) what is hostname of infected machine?
17 Host Name: K34EN6W3N-PC - java
18
19 Q.) what is mac address of infected machine?
20 Address: f0:19:af:02:9b:f1 - mac address java
21
```

Activities Firefox Web Browser Apr 28 20:37

Online MD5 Hash Generator x VirusTotal - File - e2e33b x +

https://www.virustotal.com/gui/file/e2e33b802a0d939d07bd8291f23484c2f68c

VIRUSTOTAL

SUMMARY DETECTION DETAILS COMMUNITY 10

34 security vendors and no sandboxes flagged this file as malicious

34 / 56

Community Score

Activities Firefox Web Browser Apr 28 20:36

Online MD5 Hash Generator x VirusTotal - File - ce5d1c4 x +

https://www.virustotal.com/gui/file/ce5d1c41f6ca739f6c69f175a8f688334df2e

VIRUSTOTAL

SUMMARY DETECTION DETAILS COMMUNITY

No security vendors and no sandboxes flagged this file as malicious

0 / 57

Community Score

Activities Wireshark Apr 28 20:35

Wireshark · Export · HTTP object list

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:

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 HT...
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 (1708 bytes)

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

