Research Article

Detection Suspicious Activities on Network Package Traffic

Nunu Kustian, Anggit Ilham Tantowi, Herlinda, Dudi Parulian, Erlin Windia Ambarsari

Informatics Department, Universitas Indraprasta PGRI, Jakarta, Indonesia

Abstract.
One problem of computer network security was that unauthorized people had access to websites on the internet—the way to interject malicious programs that aim to send viruses and even commit data theft. Therefore, it was critical to understand the types of attacks in the different forms of crime that can not only harm organizational infrastructure but also affect financially. Detection of criminal activities was carried out with the help of Wireshark Software to view data packets, which indicated criminal programs carried out by intruders secretly on the official website. The capture packets on the running network had suspicious packets as evidence that led to malware infections. Therefore, both the owner and website users needed security protection by planning strategies to overcome criminal activities that infect websites.

Keywords: malicious programs, malware, network package traffic, Wireshark

Corresponding Author: Nunu Kustian; email: kustiannunu@gmail.com

Published 26 May 2023

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the ICASI Conference Committee.

1. Introduction

Technology has become a necessity daily for working, studying, and other activities that require an internet network. Therefore, the security of browsing sites needs monitoring [1]. Nevertheless, not all people pay attention to surfing sites that have a vulnerability. It makes an unauthorized persons benefit. The exposure of information made computer network users are required to be more alert of various threats that exist on the internet. One of them is the threat of malware (malicious software). The harm's impact varies, including data theft, data destruction, and even data deletion. Therefore, network traffic paves the way for malware to infiltrate and infect packets on websites [2]. Many packet loads, such as usernames, passwords, site addresses, user IPs, program support files, and others, are carried in network traffic. The reason is to discover and examine what packets are received and transmitted by a machine. The Wireshark program observes

How to cite this article: Nunu Kustian, Anggit Ilham Tantowi, Herlinda, Dudi Parulian, Erlin Windia Ambarsari, (2023), "Detection Suspicious Activities on Network Package Traffic" in *International Conference on Advance & Scientific Innovation*, KnE Life Sciences, pages 23–33. DOI 10.18502/kss.v8i9.13316

the activity of arriving and outgoing network packets on the computer, which captures all packet activity on network traffic. It is possible to scan malware.

As internet users must carefully browse a website, irresponsible persons' disclosure of sensitive information is a concern. When a website requests personal data, we must first verify its legitimacy. In malware-infected websites, it serves as a pointer to files that packets might deliver to computer users. As a result, to avoid malware crimes, we must seek to examine abnormalities on web pages.

2. Methods

When the malware installs itself in a system, it is preferable to perform a more thorough network traffic analysis, followed by network forensics to reconstruct the malware crime. Investigation with reconstructing network traffic occurrences shows that users had previously accessed malware [3], known as network forensics. We utilize a Wireshark application in this study, and the approach for gathering logs from network traffic is as follows.

2.1. Wireshark

Wireshark is a network troubleshooting program capable of recording, scanning, and capturing every log of data packets that run directly on the internet network and originate from various protocols and then show the findings in real-time. We may install Wireshark on various operating systems, including Windows, Mac OS, and LINUX [4]. Wireshark performs the following tasks:

a. Packet Capture: Wireshark can listen to network connections in real-time and capture all packet data traffic-flow activities.

b. Filtering: Filter function for selecting the data we wish to see.

c. Visualization: Conversations in the network flow can visualize and insert directly into the middle of the running data packet network.

2.2. Malicious Programs

Irresponsible people create malicious programs to commit crimes that usually infiltrate websites and target website users.

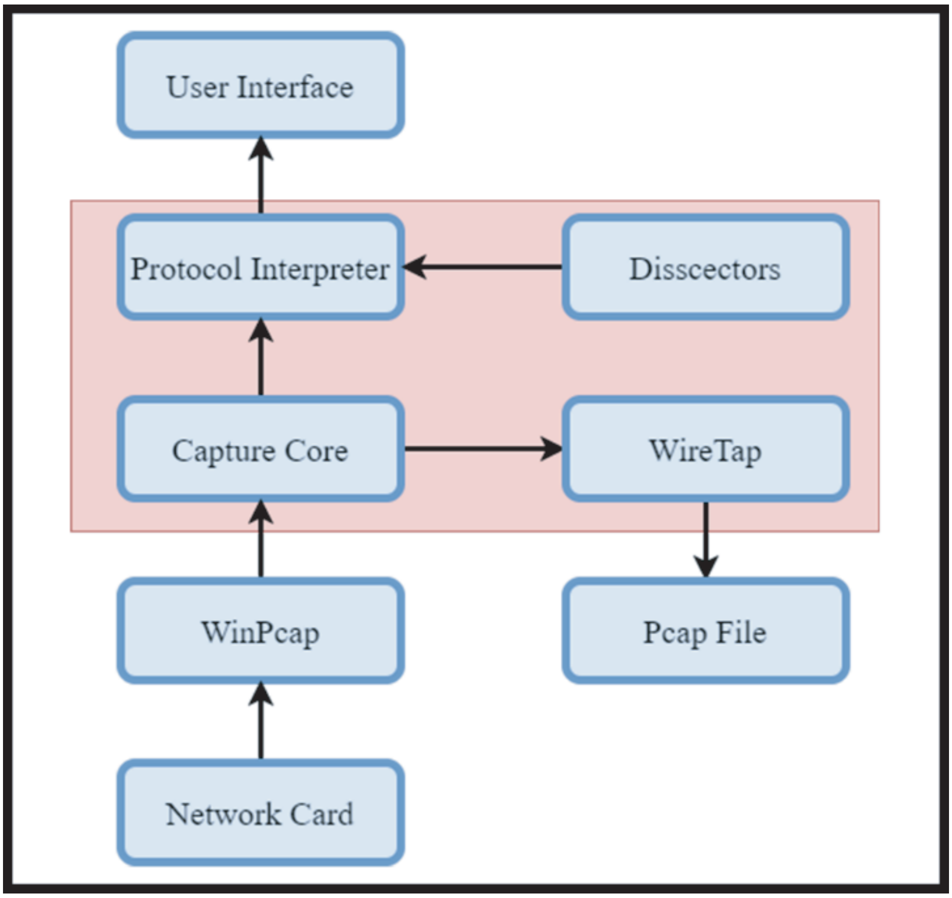


Figure 1: Wireshark Architechture[5].

2.3. Malicious Software

Malware is an application known as a malicious program designed to damage devices by accessing computers via the internet and stealing essential assets that are confidential [6], causing financial and life losses. Likewise, based [7], attackers create malicious software programs to spread infections security systems in the network that attackers can easily access and steal important information in achieving their malicious goals. Cyber attackers take many actions, which as sending junk mail and phishing.

2.4. Network Package Traffic

The vast amount of data available on the internet has a significant impact on both personal and business interests. When dealing with potentially hazardous data, network traffic analysis is critical. The volume of data that flows across a computer network at any given moment is known as network traffic. It is converted into a data packet and transmitted before being reassembles by a cross-receiving device or computer [8].

2.5. Literature Review

The study of [9] performs protocol penetration testing on webmail www.http://stmail.nptu.ed.tw, which used the Wireshark tool to capture the information in the webmail. Furthermore, it compared the data with the use of HTTP and HTTPS on the website tested. The result of the study is that the HTTPS protocol is more secure than HTTP. Data integrity, server authentication, and data confidentiality had more guaranteed in data transmission. The destination server interacts with each other and the data sent is transmitted with encryption techniques. It is imperative to maintain information when using usernames and passwords and even the data sent consistently to perform the encoding.

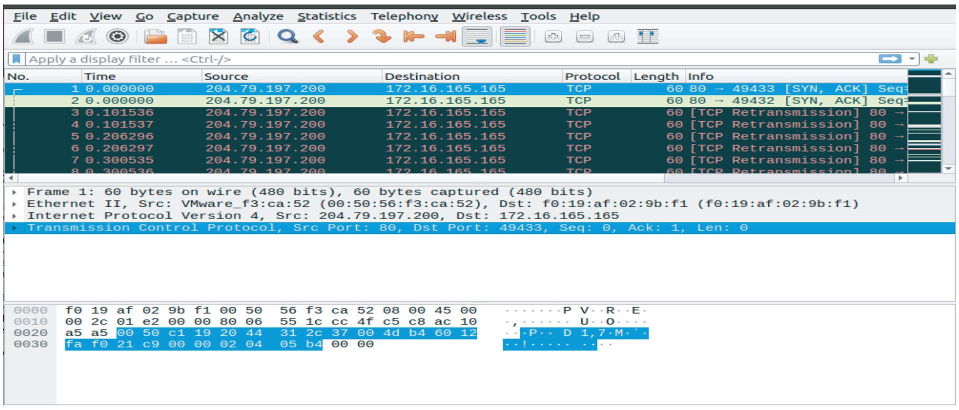
[10] research website with the link www.abpweddings.com using the Wireshark tool in testing to penetrate whether the website is safe or not. It discovered the system's vulnerability by analyzing data packets recorded through filters in the Wireshark tool with the packet sniffing method, namely filtering data packets against traffic, especially HTTP POST protocol activities. The results of this study prove that the analyzed web is not safe to visit. Therefore, it failed or experienced damage in the web system.

3. Result and Discussion

The foundational is observing the source and destination IPS connected with the protocol used and the information given. We analyze the results of the traffic report data packets captured using the Wireshark application, which displays several devices connected to several networks that we can monitor. We choose the WIFI network to use and capture the network device monitored. Therefore, It indicated that there was malware in the traffic, we searched for the report, and the results were as follows:

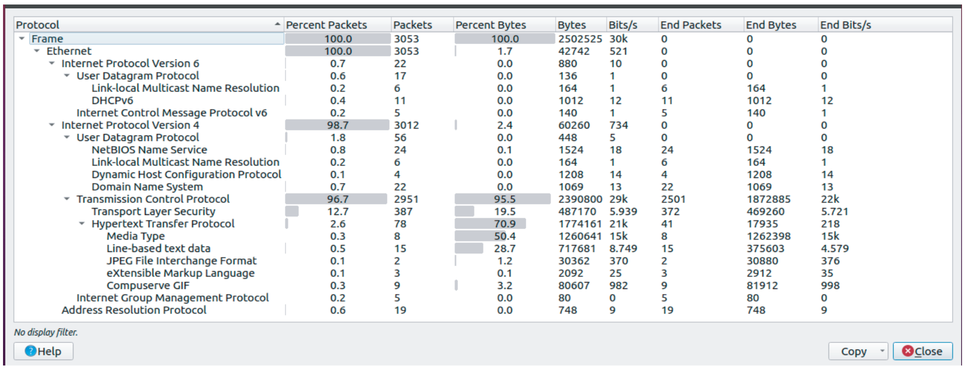
The first thing we have to do when receiving a capture in Figure 2 is to understand what kind of used protocol is in the traffic capture. For example, when we use the statistics menu, then obtain summarized information in Figure 3.

The windows display in Figure 3 shows a summary of protocol activity. For example, we observe IP version 6 and IP version 4, which traffic is 98%. The exciting part, i.e.,


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time       Source           Destination      Protocol Length Info
   1 0.000000   204.79.197.200   172.16.165.165   TCP          60 80 → 49433 [SYN, ACK] Seq=
   2 0.000000   204.79.197.200   172.16.165.165   TCP          60 80 → 49432 [SYN, ACK] Seq=
   3 0.101536   204.79.197.200   172.16.165.165   TCP          60 [TCP Retransmission] 80 →
   4 0.101537   204.79.197.200   172.16.165.165   TCP          60 [TCP Retransmission] 80 →
   5 0.206296   204.79.197.200   172.16.165.165   TCP          60 [TCP Retransmission] 80 →
   6 0.206297   204.79.197.200   172.16.165.165   TCP          60 [TCP Retransmission] 80 →
   7 0.300535   204.79.197.200   172.16.165.165   TCP          60 [TCP Retransmission] 80 →
   8 0.300536   204.79.197.200   172.16.165.165   TCP          60 [TCP Retransmission] 80 →

▸ 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
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 49433, Seq: 0, Ack: 1, Len: 0

0000  f0 19 af 02 9b f1 00 50  56 f3 ca 52 08 00 45 00   ·······P V··R··E·
0010  00 2c 01 e2 00 00 80 06  55 1c cc 4f c5 c8 ac 10   ·,······ U··O····
0020  a5 a5 00 50 c1 19 20 44  31 2c 37 00 4d b4 60 12   ···P·· D 1,7·M·`·
0030  fa f0 21 c9 00 00 02 04  05 b4 00 00               ··!····· ····
```

Figure 2: Window Traffic in Wireshark.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▾ Frame	100.0	3053	100.0	2502525	30k	0	0	0
▾ Ethernet	100.0	3053	1.7	42742	521	0	0	0
▾ Internet Protocol Version 6	0.7	22	0.0	880	10	0	0	0
▾ User Datagram Protocol	0.6	17	0.0	136	1	0	0	0
Link-local Multicast Name Resolution	0.2	6	0.0	164	1	6	164	1
DHCPv6	0.4	11	0.0	1012	12	11	1012	12
Internet Control Message Protocol v6	0.2	5	0.0	140	1	5	140	1
▾ Internet Protocol Version 4	98.7	3012	2.4	60260	734	0	0	0
▾ User Datagram Protocol	1.8	56	0.0	448	5	0	0	0
NetBIOS Name Service	0.8	24	0.1	1524	18	24	1524	18
Link-local Multicast Name Resolution	0.2	6	0.0	164	1	6	164	1
Dynamic Host Configuration Protocol	0.1	4	0.0	1208	14	4	1208	14
Domain Name System	0.7	22	0.0	1069	13	22	1069	13
▾ Transmission Control Protocol	96.7	2951	95.5	2390800	29k	2501	1872885	22k
Transport Layer Security	12.7	387	19.5	487170	5.939	372	469260	5.721
▾ Hypertext Transfer Protocol	2.6	78	70.9	1774161	21k	41	17935	218
Media Type	0.3	8	50.4	1260641	15k	8	1262398	15k
Line-based text data	0.5	15	28.7	717681	8.749	15	375603	4.579
JPEG File Interchange Format	0.1	2	1.2	30362	370	2	30880	376
eXtensible Markup Language	0.1	3	0.1	2092	25	3	2912	35
Compuserve GIF	0.3	9	3.2	80607	982	9	81912	998
Internet Group Management Protocol	0.2	5	0.0	80	0	5	80	0
Address Resolution Protocol	0.6	19	0.0	748	9	19	748	9

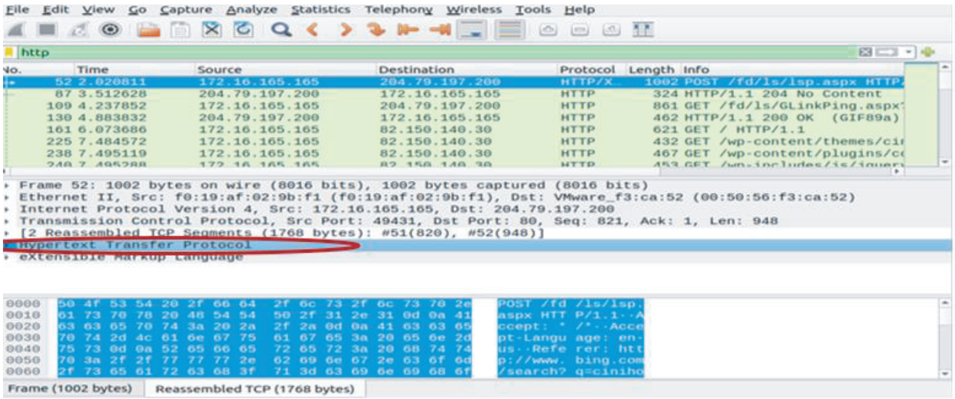
No display filter.

Figure 3: Protocol Hierarchy Statistics.

when we monitor TCP and UDP traffic, we know everything is going on. UDP can usually be used to acquire machine-related information such as DHCP and DNS requests. We observe the application-level traffic according to the graph. HTTP (HyperText Transfer Protocol) activity shows that related to the web traffic. We took Dotnet malware traffic detection via packet capture, where all users were downloading malware. Therefore, we found it in HyperText Transfer Protocol. In the standard view, we can monitor all the protocols (Figure 2). However, since we detect HD traffic, we use “filter” by typing filter in the window in Figure 2. If the windows in Figure 3 are closed, the HTTP traffic and all the traffic associated with it are filtered and use a request method called HTTP point request so that the HTTP request filter shows the gateway for posting requests made from source to destination. The HTTP filter is as follows:

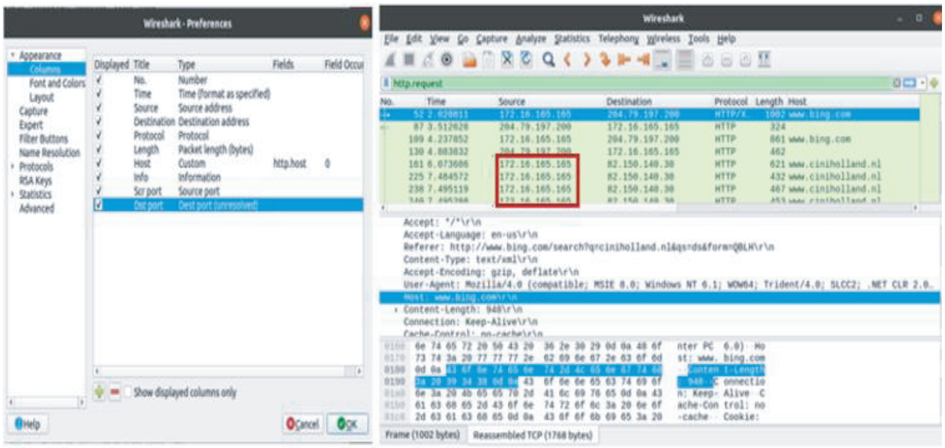
We can monitor all the protocol literature information with expands *Hypertext Transfer Protocol*. We were using the HTTP section, and when we image it, we can monitor it, which contain the actual hostname.

Figure 5.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Frame (1002 bytes)
Reassembled TCP (1768 bytes)

```
No.   Time       Source          Destination     Protocol  Length Info
   52 2.020811   172.16.165.165  204.79.197.200  HTTP/X…   1002 POST /fd/ls/lsp.aspx HTTP/
   87 3.512628   204.79.197.200  172.16.165.165  HTTP       324 HTTP/1.1 204 No Content
  109 4.237852   172.16.165.165  204.79.197.200  HTTP       861 GET /fd/ls/GLinkPing.aspx?
  130 4.883832   204.79.197.200  172.16.165.165  HTTP       462 HTTP/1.1 200 OK  (GIF89a)
  161 6.073686   172.16.165.165  82.150.140.30   HTTP       621 GET / HTTP/1.1
  225 7.484572   172.16.165.165  82.150.140.30   HTTP       432 GET /wp-content/themes/cir
  238 7.495119   172.16.165.165  82.150.140.30   HTTP       467 GET /wp-content/plugins/cc
  240 7.495288   172.16.165.165  82.150.140.30   HTTP       453 GET /wp-includes/js/jquery

▸ 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
▸ Transmission Control Protocol, Src Port: 49431, Dst Port: 80, Seq: 821, Ack: 1, Len: 948
▸ [2 Reassembled TCP Segments (1768 bytes): #51(820), #52(948)]
▸ Hypertext Transfer Protocol
▸ eXtensible Markup Language

0000  50 4f 53 54 20 2f 66 64  2f 6c 73 2f 6c 73 70 2e   POST /fd /ls/lsp.
0010  61 73 70 78 20 48 54 54  50 2f 31 2e 31 0d 0a 41   aspx HTT P/1.1··A
0020  63 63 65 70 74 3a 20 2a  2f 2a 0d 0a 41 63 63 65   ccept: * /*··Acce
0030  70 74 2d 4c 61 6e 67 75  61 67 65 3a 20 65 6e 2d   pt-Langu age: en-
0040  75 73 0d 0a 52 65 66 65  72 65 72 3a 20 68 74 74   us··Refe rer: htt
0050  70 3a 2f 2f 77 77 77 2e  62 69 6e 67 2e 63 6f 6d   p://www. bing.com
0060  2f 73 65 61 72 63 68 3f  71 3d 63 69 6e 69 68 6f   /search? q=ciniho
```

Figure 4: HTTP Filter.



Displayed	Title	Type	Fields	Field Occu
✓	No.	Number		
✓	Time	Time (format as specified)		
✓	Source	Source address		
✓	Destination	Destination address		
✓	Protocol	Protocol		
✓	Length	Packet length (bytes)		
✓	Host	Custom	http.host	0
✓	Info	Information		
✓	Scr port	Source port		
☑	Dst port	Dest port (unresolved)		

```
No.   Time       Source          Destination     Protocol  Length Host
   52 2.020811   172.16.165.165  204.79.197.200  HTTP/X…   1002 www.bing.com
   87 3.512628   204.79.197.200  172.16.165.165  HTTP       324
  109 4.237852   172.16.165.165  204.79.197.200  HTTP       861 www.bing.com
  130 4.883832   204.79.197.200  172.16.165.165  HTTP       462
  161 6.073686   172.16.165.165  82.150.140.30   HTTP       621 www.ciniholland.nl
  225 7.484572   172.16.165.165  82.150.140.30   HTTP       432 www.ciniholland.nl
  238 7.495119   172.16.165.165  82.150.140.30   HTTP       467 www.ciniholland.nl
  240 7.495288   172.16.165.165  82.150.140.30   HTTP       453 www.ciniholland.nl

    Accept: */*\r\n
    Accept-Language: en-us\r\n
    Referer: http://www.bing.com/search?q=ciniholland.nl&qs=ds&form=QBLH\r\n
    Content-Type: text/xml\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0…
    Host: www.bing.com\r\n
  ▸ Content-Length: 948\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n

0160  6e 74 65 72 20 50 43 20  36 2e 30 29 0d 0a 48 6f   nter PC  6.0)··Ho
0170  73 74 3a 20 77 77 77 2e  62 69 6e 67 2e 63 6f 6d   st: www. bing.com
0180  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68   ··Conten t-Length
0190  3a 20 39 34 38 0d 0a 43  6f 6e 6e 65 63 74 69 6f   : 948··C onnectio
01a0  6e 3a 20 4b 65 65 70 2d  41 6c 69 76 65 0d 0a 43   n: Keep- Alive··C
01b0  61 63 68 65 2d 43 6f 6e  74 72 6f 6c 3a 20 6e 6f   ache-Con trol: no
01c0  2d 63 61 63 68 65 0d 0a  43 6f 6f 6b 69 65 3a 20   -cache·· Cookie:
```

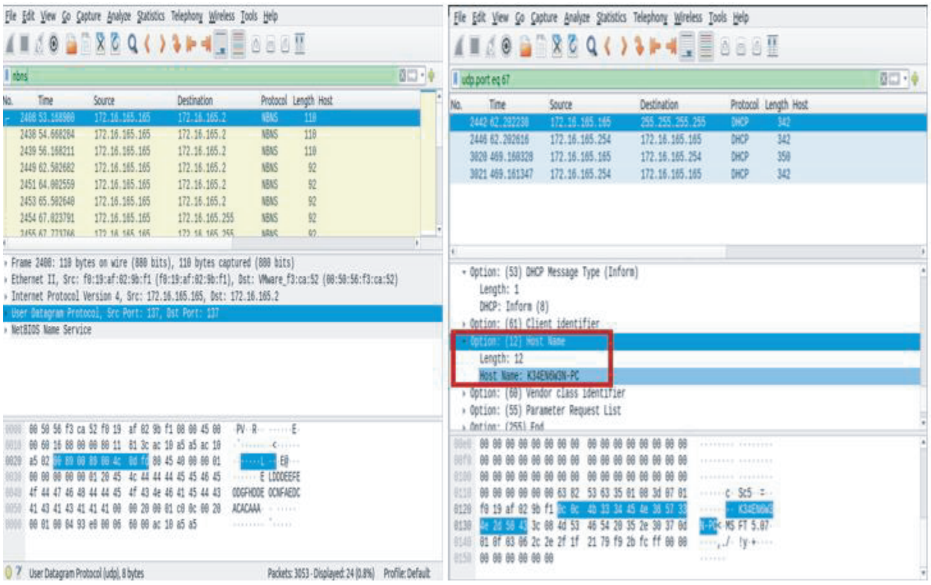
Figure 5: Wireshark Preference.

In Figure 5, The detected that the Window Virtual Machine got infected. The infecting IP address is 172.16.165.165, and based on Figure 6, the hostname of the Windows VM that got infected is K34EN6W3N-PC. We discovered through the NBNS or DHCP traffic and filtering with udp.port.eq.67.

Based on Figure 7, the MAC address of the infected is f0: 19:af:02:9b:f1, and the IP address of the compromised website is 82.150.140.30.

Figure 8 detected the IP address, and the domain name of the compromised website is 82.150.140.30, www.ciniholland.nl. The IP address and domain name that shipped the Exploit Kit and malware is 37.200.69.143, and the domain name that shipped the Exploit Kit and malware is stand.trustandprobaterealty.com

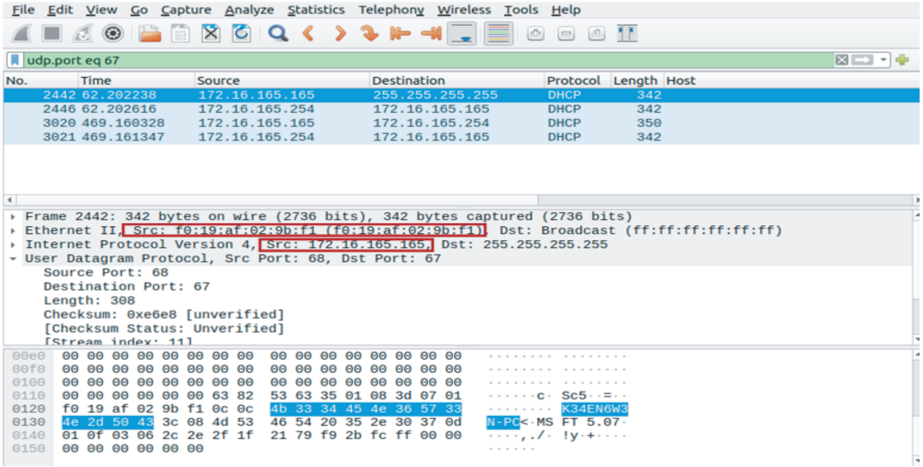
Based on Figure 9, the iframe code obtained from the malware source with the address http://stand.trustandprobaterealty.com/PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM0 and the redirect URL that points to the Exploit Kit (EK) landing page is http://24-corp-shop.com/. Search the URL that leads to the Exploit Kit (EK) page by typing the keyword


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
nbns
No.  Time          Source          Destination      Protocol Length Host
2400 53.168980     172.16.165.165  172.16.165.2     NBNS     110
2438 54.668284     172.16.165.165  172.16.165.2     NBNS     110
2439 56.168211     172.16.165.165  172.16.165.2     NBNS     110
2449 62.582682     172.16.165.165  172.16.165.2     NBNS     92
2451 64.082559     172.16.165.165  172.16.165.2     NBNS     92
2453 65.582640     172.16.165.165  172.16.165.2     NBNS     92
2454 67.023791     172.16.165.165  172.16.165.255   NBNS     92
2455 67.773766     172.16.165.165  172.16.165.255   NBNS     92

Frame 2400: 110 bytes on wire (880 bits), 110 bytes captured (880 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: 172.16.165.2
User Datagram Protocol, Src Port: 137, Dst Port: 137
NetBIOS Name Service

0000  00 50 56 f3 ca 52 f0 19  af 02 9b f1 08 00 45 00   ·PV··R·· ······E·
0010  00 60 16 88 00 00 80 11  81 3c ac 10 a5 a5 ac 10   ·`······ ·<······
0020  a5 02 00 89 00 89 00 4c  0d fd 80 45 40 00 00 01   ·······L ··E@····
0030  00 00 00 00 00 01 20 45  4c 44 44 44 45 45 46 45   ······ E LDDDEEFE
0040  4f 44 47 46 48 44 44 45  4f 43 4e 46 41 45 44 43   ODGFHDDE OCNFAEDC
0050  41 43 41 43 41 41 41 00  00 20 00 01 c0 0c 00 20   ACACAAA· ·······
0060  00 01 00 04 93 e0 00 06  60 00 ac 10 a5 a5         ········ `·····

User Datagram Protocol (udp), 8 bytes      Packets: 3053 · Displayed: 24 (0.8%)      Profile: Default
```

```
udp.port eq 67
No.  Time          Source          Destination      Protocol Length Host
2442 62.202238     172.16.165.165  255.255.255.255  DHCP     342
2446 62.202616     172.16.165.254  172.16.165.165   DHCP     342
3020 469.160328    172.16.165.165  172.16.165.254   DHCP     350
3021 469.161347    172.16.165.254  172.16.165.165   DHCP     342

  Option: (53) DHCP Message Type (Inform)
    Length: 1
    DHCP: Inform (8)
  Option: (61) Client identifier
  Option: (12) Host Name
    Length: 12
    Host Name: K34EN6W3N-PC
  Option: (60) Vendor class identifier
  Option: (55) Parameter Request List
  Option: (255) End

00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 08 3d 07 01   ······c· Sc5··=··
0120  f0 19 af 02 9b f1 0c 0c  4b 33 34 45 4e 36 57 33   ········ K34EN6W3
0130  4e 2d 50 43 3c 08 4d 53  46 54 20 35 2e 30 37 0d   N-PC<·MS FT 5.07·
0140  01 0f 03 06 2c 2e 2f 1f  21 79 f9 2b fc ff 00 00   ····,./· !y·+····
0150  00 00 00 00 00 00                                  ······
```

Figure 6: Infected VM Windows Detection Display.

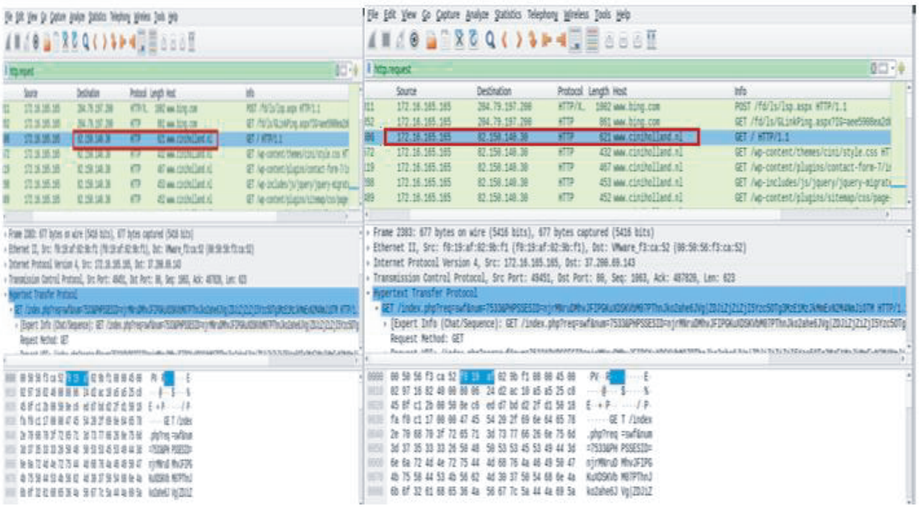

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
udp.port eq 67
No.        Time         Source            Destination        Protocol  Length  Host
     2442  62.202238    172.16.165.165    255.255.255.255    DHCP         342
     2446  62.202616    172.16.165.254    172.16.165.165     DHCP         342
     3020  469.160328   172.16.165.165    172.16.165.254     DHCP         350
     3021  469.161347   172.16.165.254    172.16.165.165     DHCP         342

▸ Frame 2442: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits)
▸ Ethernet II, Src: f0:19:af:02:9b:f1 (f0:19:af:02:9b:f1), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
▸ Internet Protocol Version 4, Src: 172.16.165.165, Dst: 255.255.255.255
▾ User Datagram Protocol, Src Port: 68, Dst Port: 67
    Source Port: 68
    Destination Port: 67
    Length: 308
    Checksum: 0xe6e8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 11]

00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 08 3d 07 01   ······c· Sc5··=··
0120  f0 19 af 02 9b f1 0c 0c  4b 33 34 45 4e 36 57 33   ········ K34EN6W3
0130  4e 2d 50 43 3c 08 4d 53  46 54 20 35 2e 30 37 0d   N-PC<·MS FT 5.07·
0140  01 0f 03 06 2c 2e 2f 1f  21 79 f9 2b fc ff 00 00   ····,./· !y·+····
0150  00 00 00 00 00 00                                  ······
```

Figure 7: Display MAC Address and IP Address.

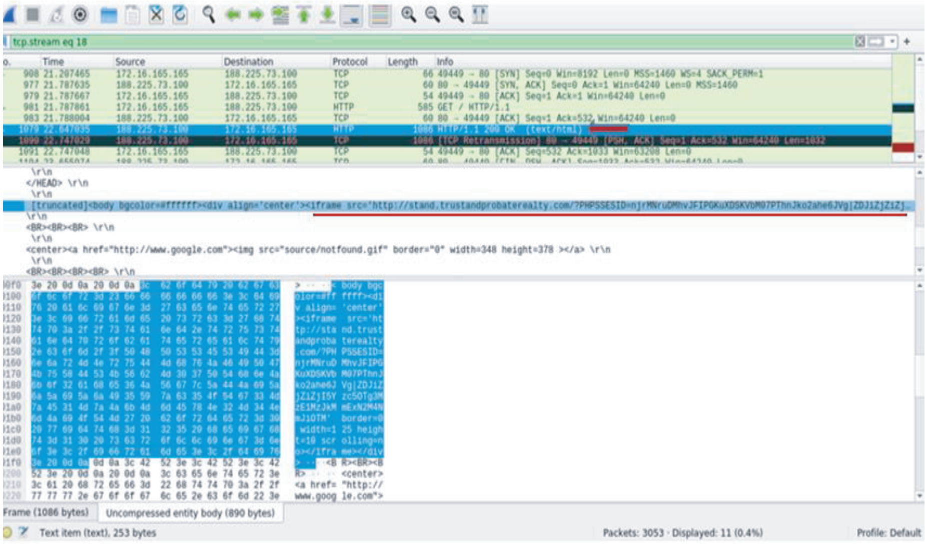
tcp.stream eq 18, then the HTTP protocol with the description 200 OK and the extension HTML. An exploit kit is a malicious program packaged in the form of encryption to carry out attacks and cause malware where the attack quickly infects the end user's system so that there are gaps in the weakness of the computer and avoid detection from the software security side. Exploit Kits designed by cybercriminals are usually easily obtained on black markets with many variations of Exploit Kits, one of which is Exploit Blackhole [11].

Figure 10 had indications of several suspected malware files; besides the landing page containing the IE Exploit CVE-2013-2551, the other types of exploits posted by EK, i.e., a Java Exploit and Flash Exploit, which detected by exporting objects. It indicated



```
http.request
Source          Destination     Protocol Length Host              Info
172.16.165.165  204.79.197.200  HTTP/X.  1082 www.bing.com        POST /fd/ls/lsp.aspx HTTP/1.1
172.16.165.165  204.79.197.200  HTTP      861 www.bing.com        GET /fd/ls/GLinkPing.aspx?IG=aee5980ea2d
172.16.165.165  82.150.140.30   HTTP      621 www.ciniholland.nl  GET / HTTP/1.1
172.16.165.165  82.150.140.30   HTTP      432 www.ciniholland.nl  GET /wp-content/themes/cini/style.css HT
172.16.165.165  82.150.140.30   HTTP      467 www.ciniholland.nl  GET /wp-content/plugins/contact-form-7/i
172.16.165.165  82.150.140.30   HTTP      453 www.ciniholland.nl  GET /wp-includes/js/jquery/jquery-migrat
172.16.165.165  82.150.140.30   HTTP      452 www.ciniholland.nl  GET /wp-content/plugins/sitemap/css/page-

› Frame 2383: 677 bytes on wire (5416 bits), 677 bytes captured (5416 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: 37.200.69.143
› Transmission Control Protocol, Src Port: 49451, Dst Port: 80, Seq: 1063, Ack: 487820, Len: 623
˅ Hypertext Transfer Protocol
  › GET /index.php?req=swf&num=7533&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJ1ZjZ1ZjI5Yzc50TgzMzE1MzJkMmExN2M4NmJiOTM HTTP/1.
    › [Expert Info (Chat/Sequence): GET /index.php?req=swf&num=7533&PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJ1ZjZ1ZjI5Yzc50Tg
      Request Method: GET
```

Figure 8: Display Domain Name and IP Address.



```
tcp.stream eq 18
No.  Time       Source          Destination     Protocol Length Info
908  21.207465  172.16.165.165  188.225.73.100  TCP        66 49449 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
977  21.787635  188.225.73.100  172.16.165.165  TCP        60 80 → 49449 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
979  21.787667  172.16.165.165  188.225.73.100  TCP        54 49449 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
981  21.787861  172.16.165.165  188.225.73.100  HTTP      585 GET / HTTP/1.1
983  21.788004  188.225.73.100  172.16.165.165  TCP        60 80 → 49449 [ACK] Seq=1 Ack=532 Win=64240 Len=0
1079 22.647035  188.225.73.100  172.16.165.165  HTTP     1086 HTTP/1.1 200 OK  (text/html)
1090 22.747029  188.225.73.100  172.16.165.165  TCP      1086 [TCP Retransmission] 80 → 49449 [PSH, ACK] Seq=1 Ack=532 Win=64240 Len=1032
1091 22.747048  172.16.165.165  188.225.73.100  TCP        54 49449 → 80 [ACK] Seq=532 Ack=1033 Win=63208 Len=0

  \r\n
 </HEAD> \r\n
  \r\n
  [truncated]<body bgcolor=#ffffff><div align='center'><iframe src='http://stand.trustandprobaterealty.com/?PHPSSESID=njrMNruDMhvJFIPGKuXDSKVbM07PThnJko2ahe6JVg|ZDJ1ZjZ1Zj…
 \r\n
 <BR><BR><BR> \r\n
  \r\n
 <center><a href="http://www.google.com"><img src="source/notfound.gif" border="0" width=348 height=378 ></a> \r\n
  \r\n
 <BR><BR><BR><BR> \r\n

00f0  3e 20 0d 0a 20 0d 0a 3c  62 6f 64 79 20 62 67 63   > ·· ·· < body bgc
0100  6f 6c 6f 72 3d 23 66 66  66 66 66 66 3e 3c 64 69   olor=#ff ffff><di
0110  76 20 61 6c 69 67 6e 3d  27 63 65 6e 74 65 72 27   v align= 'center'
0120  3e 3c 69 66 72 61 6d 65  20 73 72 63 3d 27 68 74   ><iframe  src='ht
0130  74 70 3a 2f 2f 73 74 61  6e 64 2e 74 72 75 73 74   tp://sta nd.trust
0140  61 6e 64 70 72 6f 62 61  74 65 72 65 61 6c 74 79   andproba terealty
0150  2e 63 6f 6d 2f 3f 50 48  50 53 53 45 53 49 44 3d   .com/?PH PSSESID=
0160  6e 6a 72 4d 4e 72 75 44  4d 68 76 4a 46 49 50 47   njrMNruD MhvJFIPG
0170  4b 75 58 44 53 4b 56 62  4d 30 37 50 54 68 6e 4a   KuXDSKVb M07PThnJ
0180  6b 6f 32 61 68 65 36 4a  56 67 7c 5a 44 4a 69 5a   ko2ahe6J Vg|ZDJiZ

Frame (1086 bytes)   Uncompressed entity body (890 bytes)
Text item (text), 253 bytes                              Packets: 3053 · Displayed: 11 (0.4%)     Profile: Default
```

Figure 9: Display Preview Pane.

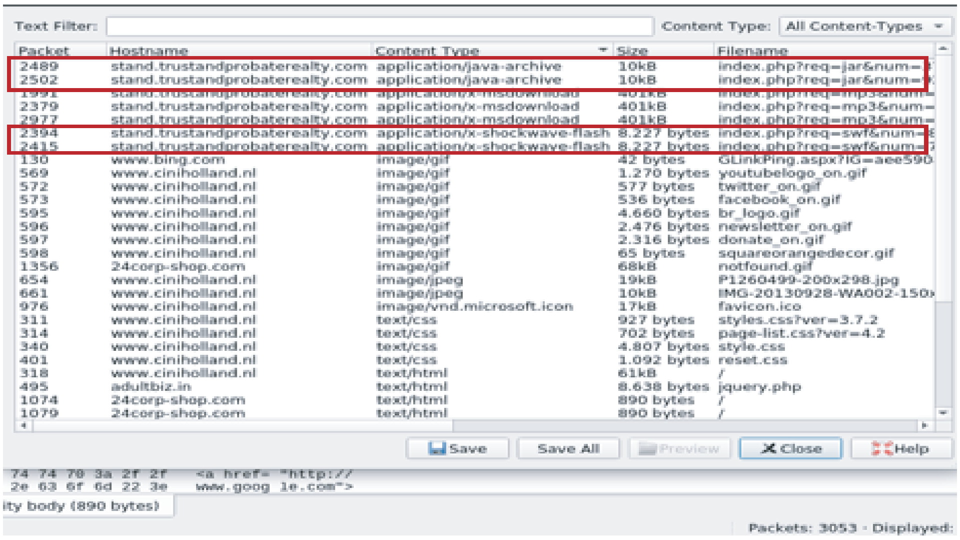
that the exploit payload was sent 3 times (payload is encrypted although created as x-msdownload). Figure 11 discovers how often the load was sent by typing the keyword HTTP containing “Content-Length: 401811”.

In Figure 12, observe the name of the Exploit Kit, and it displayed with the Snort warning by sending a pcap to VirusTotal (https://virustotal.com). VirusTotal is a free online service antivirus engine for analyzing URLs and files from worms, trojans, viruses, and various malicious programs.

https://www.virustotal.com/gui/file/0e3fac547536f773bf1a21180a2294a10be97e956f091d24

detection

ET CURRENT_EVENTS **Goon/Infinity** *URI Struct EK Landing May 05 2014*



Text Filter: Content Type: All Content-Types

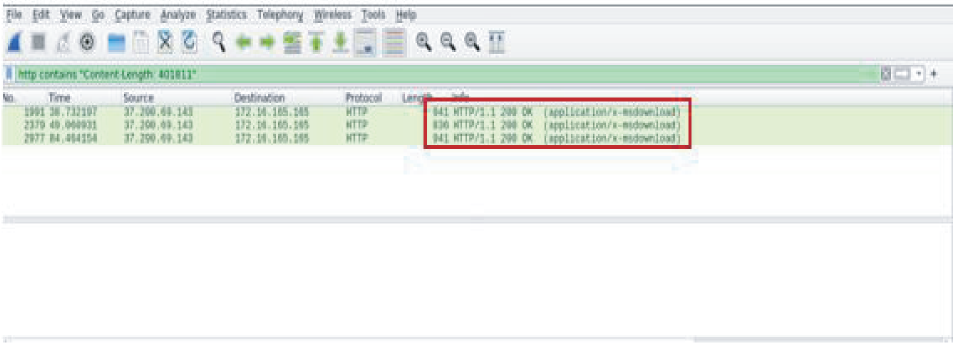
Packet	Hostname	Content Type	Size	Filename
2489	stand.trustandprobaterealty.com	application/java-archive	10kB	index.php?req=jar&num=
2502	stand.trustandprobaterealty.com	application/java-archive	10kB	index.php?req=jar&num=
1991	stand.trustandprobaterealty.com	application/x-msdownload	401kB	index.php?req=mp3&num=
2379	stand.trustandprobaterealty.com	application/x-msdownload	401kB	index.php?req=mp3&num=
2977	stand.trustandprobaterealty.com	application/x-msdownload	401kB	index.php?req=mp3&num=
2394	stand.trustandprobaterealty.com	application/x-shockwave-flash	8.227 bytes	index.php?req=swf&num=
2415	stand.trustandprobaterealty.com	application/x-shockwave-flash	8.227 bytes	index.php?req=swf&num=
130	www.bing.com	image/gif	42 bytes	GLinkPing.aspx?IG=aee590
569	www.ciniholland.nl	image/gif	1.270 bytes	youtubelogo_on.gif
572	www.ciniholland.nl	image/gif	577 bytes	twitter_on.gif
573	www.ciniholland.nl	image/gif	536 bytes	facebook_on.gif
595	www.ciniholland.nl	image/gif	4.660 bytes	br_logo.gif
596	www.ciniholland.nl	image/gif	2.476 bytes	newsletter_on.gif
597	www.ciniholland.nl	image/gif	2.316 bytes	donate_on.gif
598	www.ciniholland.nl	image/gif	65 bytes	squareorangedecor.gif
1356	24corp-shop.com	image/gif	68kB	notfound.gif
654	www.ciniholland.nl	image/jpeg	19kB	P1260499-200x298.jpg
661	www.ciniholland.nl	image/jpeg	10kB	IMG-20130928-WA002-150x
976	www.ciniholland.nl	image/vnd.microsoft.icon	17kB	favicon.ico
311	www.ciniholland.nl	text/css	927 bytes	styles.css?ver=3.7.2
314	www.ciniholland.nl	text/css	702 bytes	page-list.css?ver=4.2
340	www.ciniholland.nl	text/css	4.807 bytes	style.css
401	www.ciniholland.nl	text/css	1.092 bytes	reset.css
318	www.ciniholland.nl	text/html	61kB	/
495	adultbiz.in	text/html	8.638 bytes	jquery.php
1074	24corp-shop.com	text/html	890 bytes	/
1079	24corp-shop.com	text/html	890 bytes	/

```
74 74 70 3a 2f 2f    <a href= "http://
2e 63 6f 6d 22 3e    www.goog le.com">
```

ity body (890 bytes)

Packets: 3053 · Displayed:

Figure 10: Display Capture Other Exploit(s).



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http contains "Content Length: 401811"

No.	Time	Source	Destination	Protocol	Length	Info
1991	38.732197	37.200.69.143	172.16.165.165	HTTP	841	HTTP/1.1 200 OK (application/x-msdownload)
2379	49.060931	37.200.69.143	172.16.165.165	HTTP	836	HTTP/1.1 200 OK (application/x-msdownload)
2977	84.464154	37.200.69.143	172.16.165.165	HTTP	841	HTTP/1.1 200 OK (application/x-msdownload)

Figure 11: Payload Sent.

ET CURRENT_EVENTS **RIG EK** *Landing URI Struct*

ET CURRENT_EVENTS **GoonEK** *encrypted binary (3)*

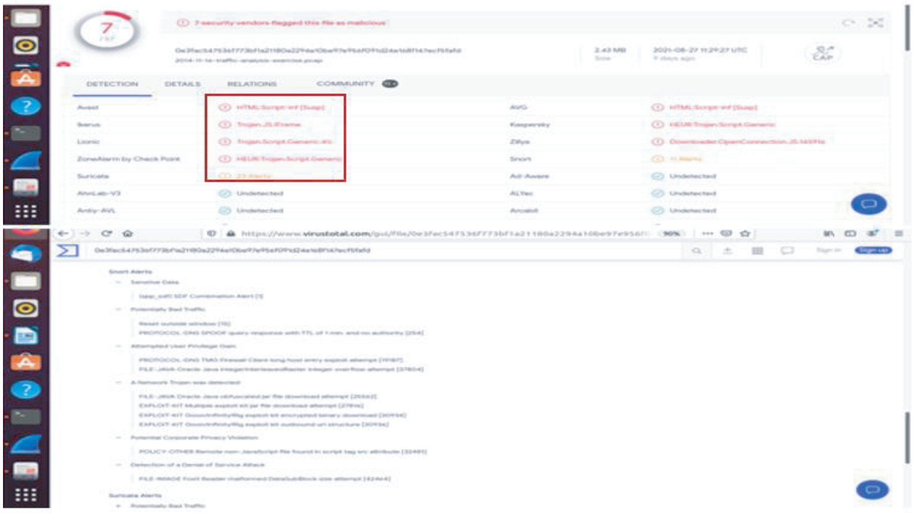


Figure 12: Wireshark Software Report Result File Name.

The analysis results using VirusTotal that the copied pcap file was infected and dangerous because the infected contained HTML: Script-inf as suspect and Trojan. JS.Iframe and Trojan.Script Viruses. The use of Wireshark can be one of the analytical steps and to anticipate by looking at the packet load sent by the website and received by the user's computer. Knowing what is going through network traffic using Wireshark can be used to reference whether the website is safe from malware or not.

4. Conclusions

There are some circumstances that Wireshark is not an Intrusion Detection System (IDS). Wireshark cannot open encrypted data on network traffic and can not tell whether the IP used by the packet sender on the network traffic is genuine or not. We must know how network traffic operates and protocols to avoid irresponsible because human knowledge is better than many powerful tools. Likewise, owners so that irresponsible parties do not infiltrate them, it is better to carry out routine maintenance on the website and use anti-malware on the server so that when malware is detected entering the server, it is removed immediately by the anti-malware program.

Acknowledgments

References

[1] Furnell S, Collins E. Cyber security: What are we talking about? *Comput Fraud Secur*. 2021;2021(7):6–11.

[2] Sikos LF. Packet analysis for network forensics: A comprehensive survey. *Forensic Sci Int Digit Investig*. 2020;32:200892.

[3] Avasthi D. “Network forensic analysis with efficient preservation for SYN attack.” *Int J Comput Appl.* 2012;46(24):17–22. [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Network+Forensic+Analysis+with+Efficient+Preservation+for+SYN+Attack#0

[4] “Wireshark.” https://www.wireshark.org/

[5] Vancea CM, Dobrota V, Wireshark AP. “SNMP Agent for WLAN networks.” no. 216041, 1998.

[6] Sibi Chakkaravarthy S, Sangeetha D, Vaidehi V. A survey on malware analysis and mitigation techniques. *Comput Sci Rev*. 2019;32:1–23.

[7] Babu NM, Murali G. “Malware detection for multi cloud servers using intermediate monitoring server.” *Int Conf Energy Commun Data Anal Soft Comput (ICECDS)*. 2017;3609–3612. 2018.

[8] Goli YD, Ambika R. “Network traffic classification techniques-A review.” *Proc Int Conf Comput Tech Electron Mech Syst (CTEMS)* 2018;219–222.

[9] Navabud P. “Analyzing thewebmail using Wireshark.” pp. 1237–1239.

[10] Sandhya S, Purkayastha S, Joshua E, Deep A. “Assessment of website security by penetration testing using Wireshark.” *2017 4th Int Conf Adv Comput Commun Syst (ICACCS)* 2017;4–7. https://doi.org/10.1109/ICACCS.2017.8014711.

[11] Malecki F. Defending your business from exploit kits. Comput Fraud Secur. 2013;2013(6):19–20.