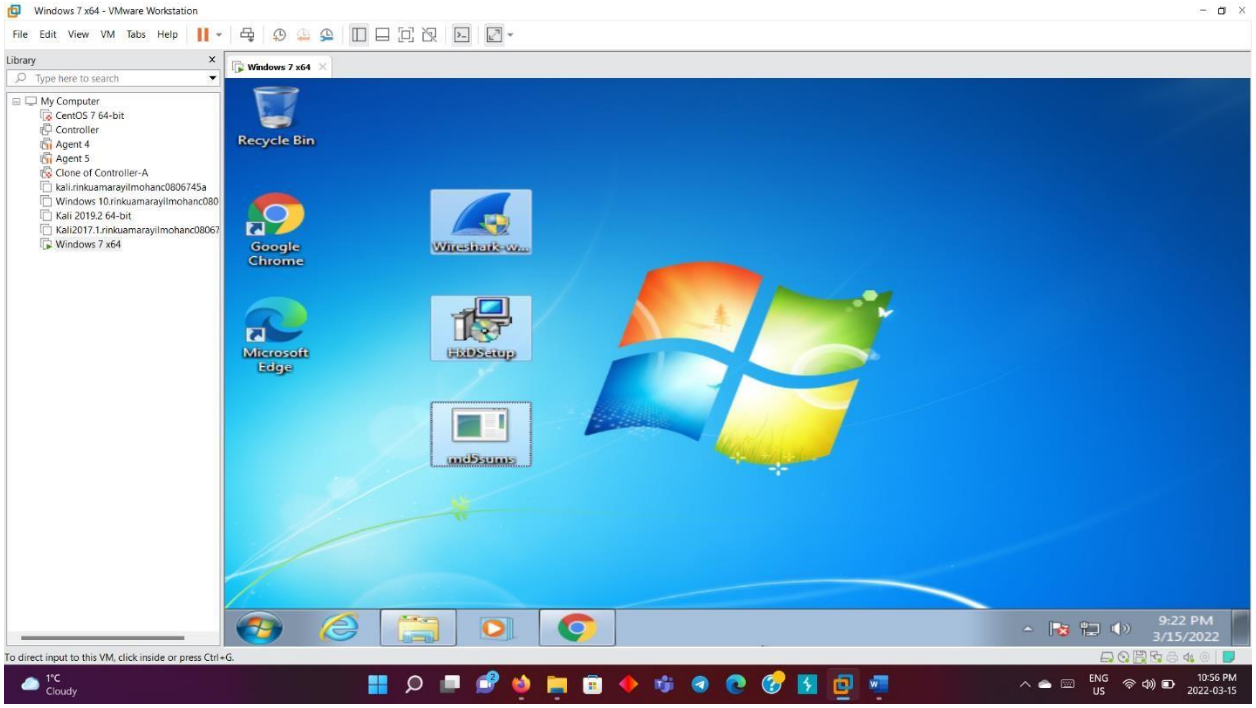
Table of Contents

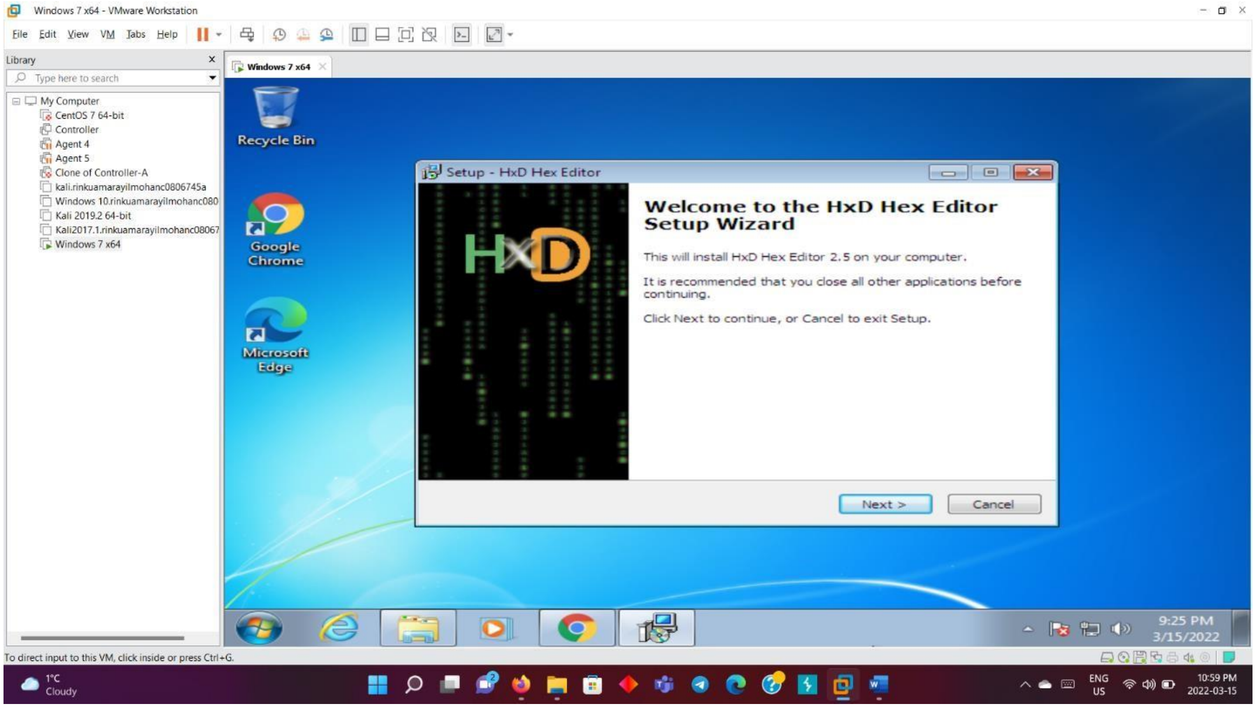
Abstract

In this in class activity we'll try to identify Malware on a device using Wireshark. We'll also try to use Hex Editor and other tools to confirm whether the detected file is a Malware or not to separate standard internet traffic from threats. Wireshark is a data packet analyzer which can be utilized in multiple ways when working with networks and network devices. Hex Editor is a computer software that enables us to edit binary data in computer files.

Part 1- Network Forensic

Step 1: To perform the lab exercise, we first download all the 3 software's.





Setup - HxD Hex Editor

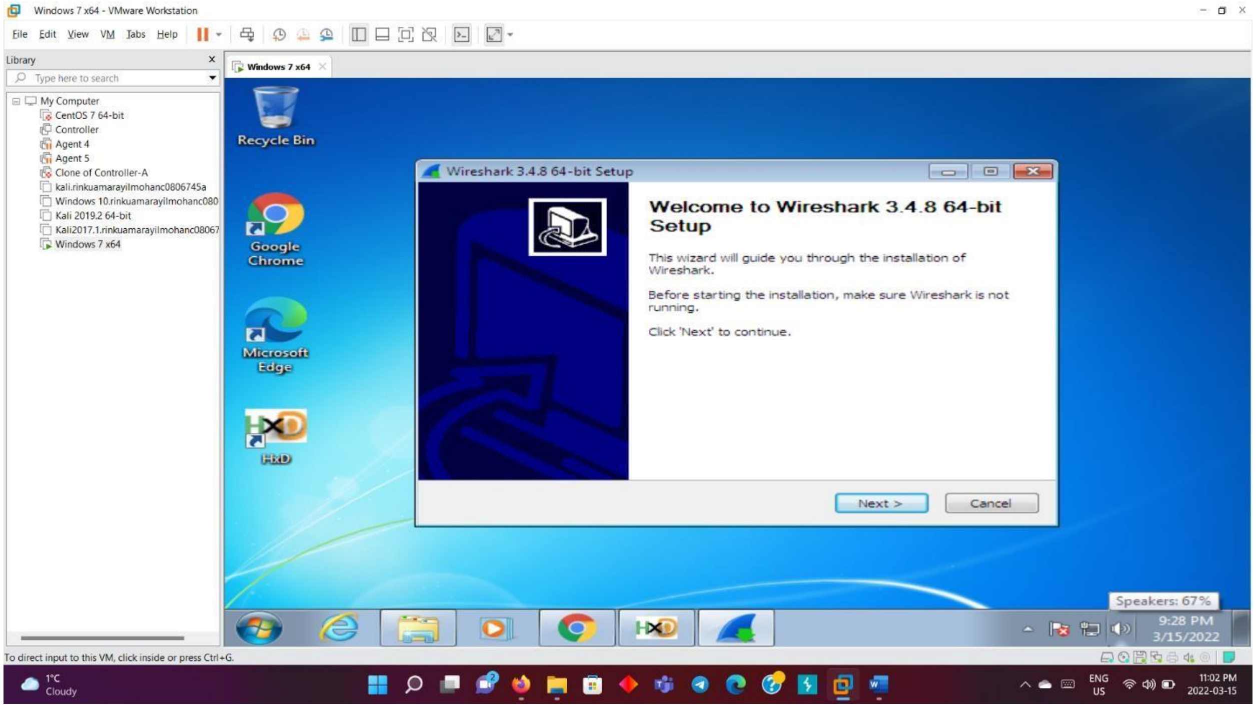
Welcome to the HxD Hex Editor Setup Wizard

This will install HxD Hex Editor 2.5 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Install HXD Editor



Wireshark 3.4.8 64-bit Setup

Welcome to Wireshark 3.4.8 64-bit Setup

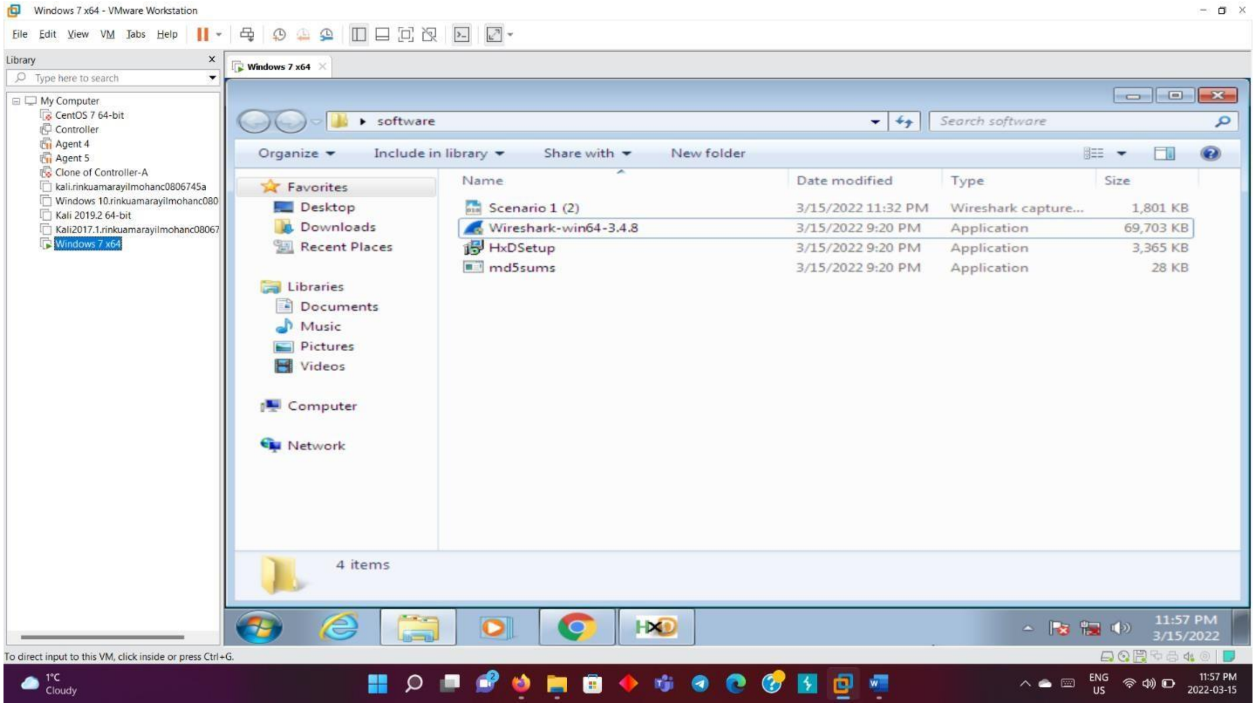
This wizard will guide you through the installation of Wireshark.

Before starting the installation, make sure Wireshark is not running.

Click 'Next' to continue.

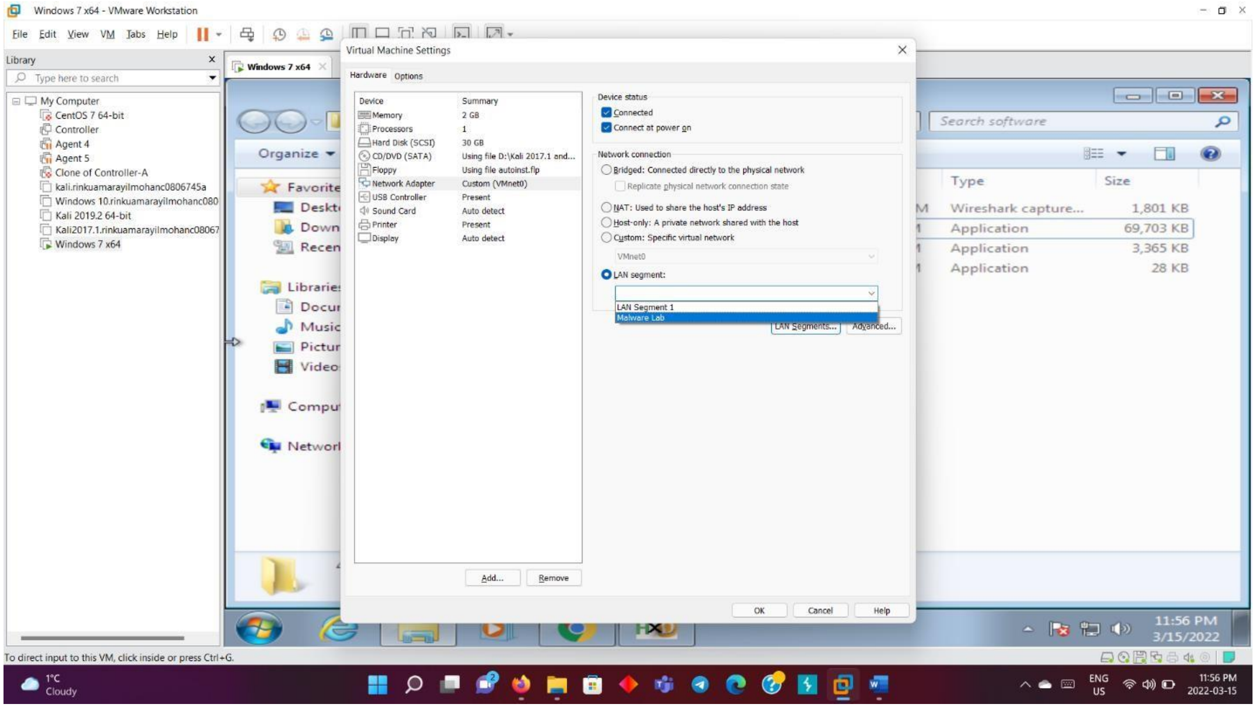
Now install Wireshark

Download the malware file Scenario 1



Name	Date modified	Type	Size
Scenario 1 (2)	3/15/2022 11:32 PM	Wireshark capture...	1,801 KB
Wireshark-win64-3.4.8	3/15/2022 9:20 PM	Application	69,703 KB
HxDSetup	3/15/2022 9:20 PM	Application	3,365 KB
md5sums	3/15/2022 9:20 PM	Application	28 KB

Change the network settings by changing to LAN segment> add a new lan segment named Malware Lab.



Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	30 GB
CD/DVD (SATA)	Using file D:\Kali 2017.1 and...
Floppy	Using file autoinst.flp
Network Adapter	Custom (VMnet0)
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Device status

☑ Connected

☑ Connect at power on

Network connection

○ Bridged: Connected directly to the physical network

□ Replicate physical network connection state

○ NAT: Used to share the host's IP address

○ Host-only: A private network shared with the host

○ Custom: Specific virtual network

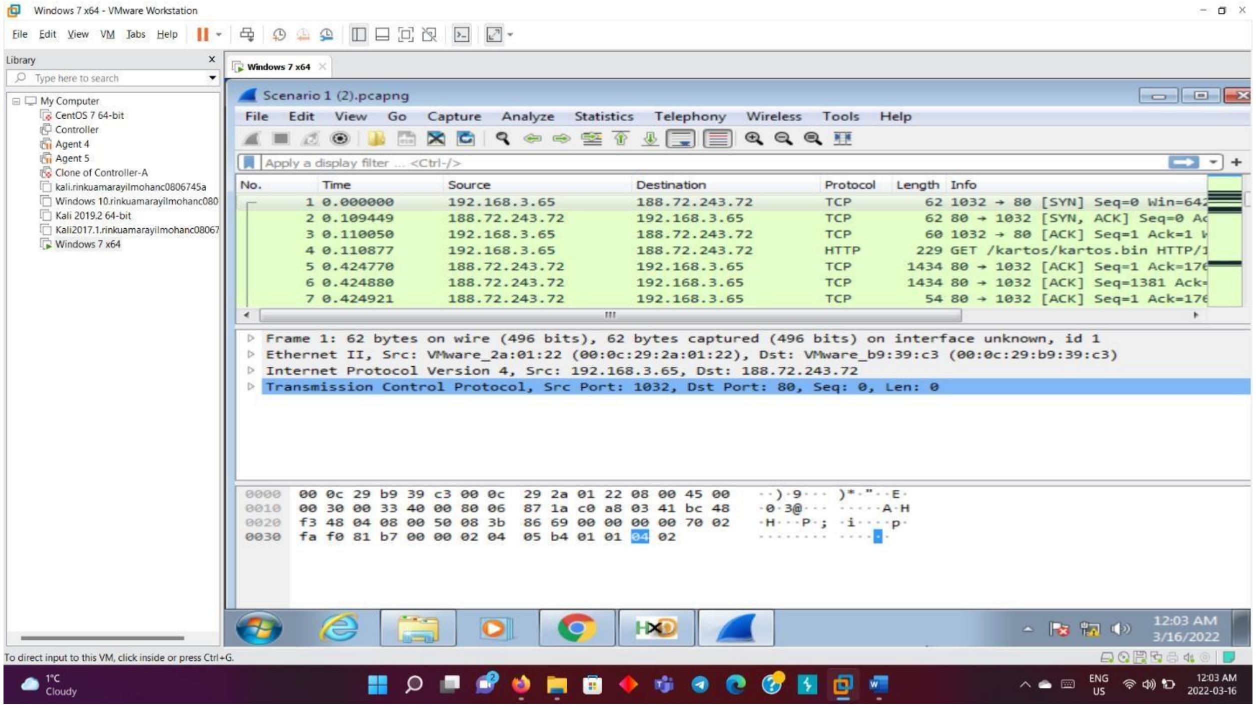
VMnet0

● LAN segment:

LAN Segment 1

Malware Lab

Once we select the network as malware lab, it will disable the network connection. And the malware will get isolated.



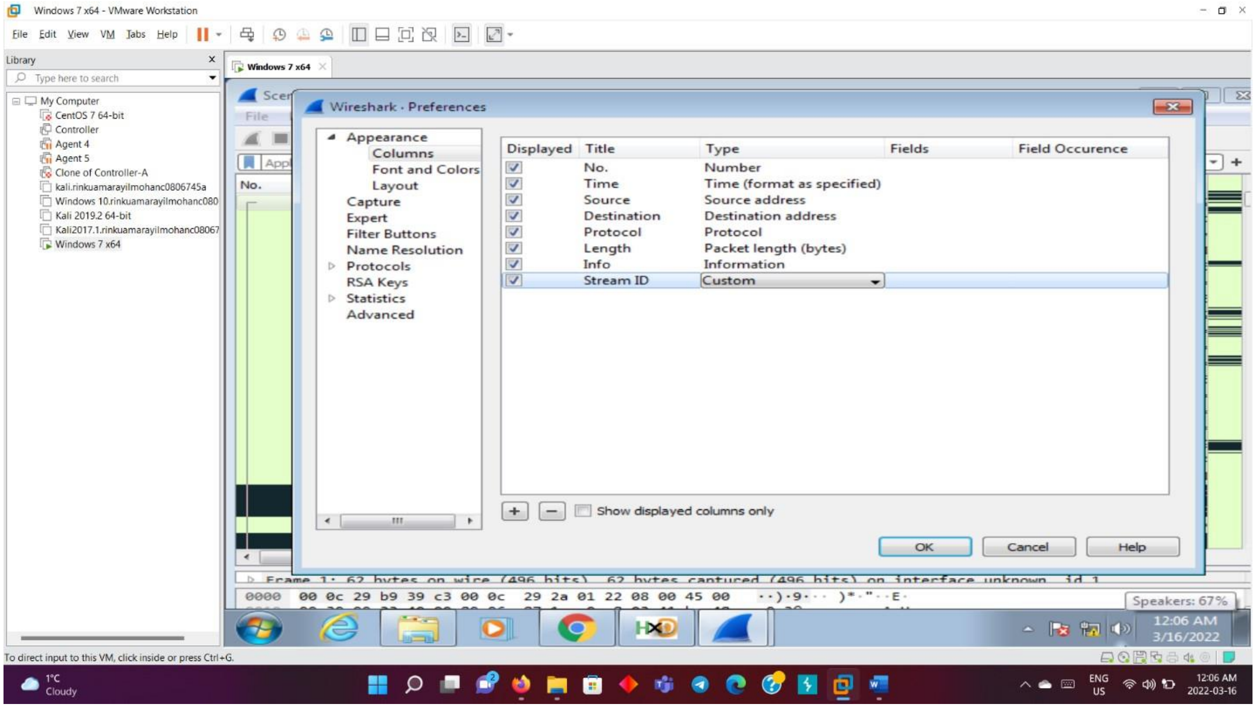
Scenario 1 (2).pcapng

```
No.  Time        Source          Destination     Protocol Length Info
   1 0.000000    192.168.3.65    188.72.243.72   TCP          62 1032 → 80 [SYN] Seq=0 Win=642
   2 0.109449    188.72.243.72   192.168.3.65    TCP          62 80 → 1032 [SYN, ACK] Seq=0 Ac
   3 0.110050    192.168.3.65    188.72.243.72   TCP          60 1032 → 80 [ACK] Seq=1 Ack=1 W
   4 0.110877    192.168.3.65    188.72.243.72   HTTP        229 GET /kartos/kartos.bin HTTP/1
   5 0.424770    188.72.243.72   192.168.3.65    TCP        1434 80 → 1032 [ACK] Seq=1 Ack=176
   6 0.424880    188.72.243.72   192.168.3.65    TCP        1434 80 → 1032 [ACK] Seq=1381 Ack=
   7 0.424921    188.72.243.72   192.168.3.65    TCP          54 80 → 1032 [ACK] Seq=1 Ack=176

▷ Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface unknown, id 1
▷ Ethernet II, Src: VMware_2a:01:22 (00:0c:29:2a:01:22), Dst: VMware_b9:39:c3 (00:0c:29:b9:39:c3)
▷ Internet Protocol Version 4, Src: 192.168.3.65, Dst: 188.72.243.72
▷ Transmission Control Protocol, Src Port: 1032, Dst Port: 80, Seq: 0, Len: 0

0000  00 0c 29 b9 39 c3 00 0c  29 2a 01 22 08 00 45 00   ··)·9··· )*·"··E·
0010  00 30 00 33 40 00 80 06  87 1a c0 a8 03 41 bc 48   ·0·3@··· ·····A·H
0020  f3 48 04 08 00 50 08 3b  86 69 00 00 00 00 70 02   ·H···P·; ·i····p·
0030  fa f0 81 b7 00 00 02 04  05 b4 01 01 04 02         ········ ······
```

Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
CentOS 7 64-bit
Controller
Agent 4
Agent 5
Clone of Controller-A
kali.rinkuamarayilmohanc0806745a
Windows 10.rinkuamarayilmohanc080
Kali 2019.2 64-bit
Kali2017.1.rinkuamarayilmohanc08067
Windows 7 x64
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
12:03 AM
3/16/2022
To direct input to this VM, click inside or press Ctrl+G.
1°C
Cloudy
ENG
US
12:03 AM
2022-03-16

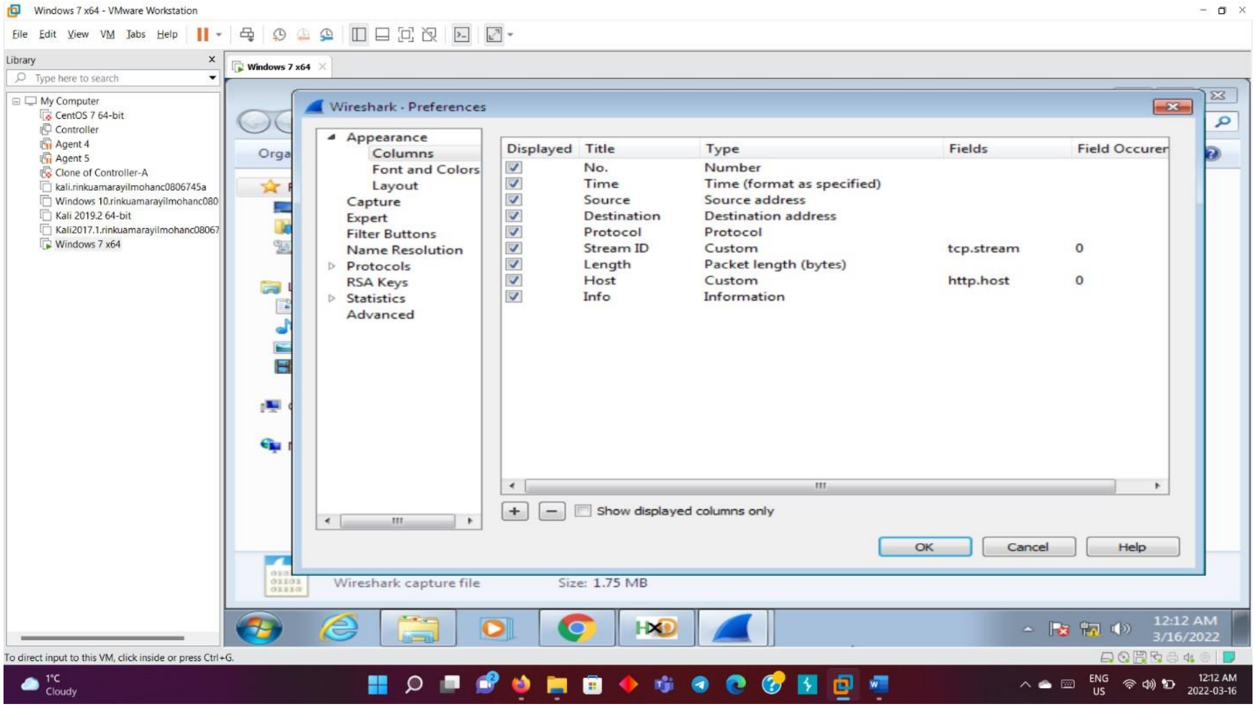
Now we right click and open the scenario file with wireshark.

Right click on the source and add new column. Name it as Stream ID and provide the number as Custom, field as tcp.stream, and field occurrence as 0.



Wireshark · Preferences

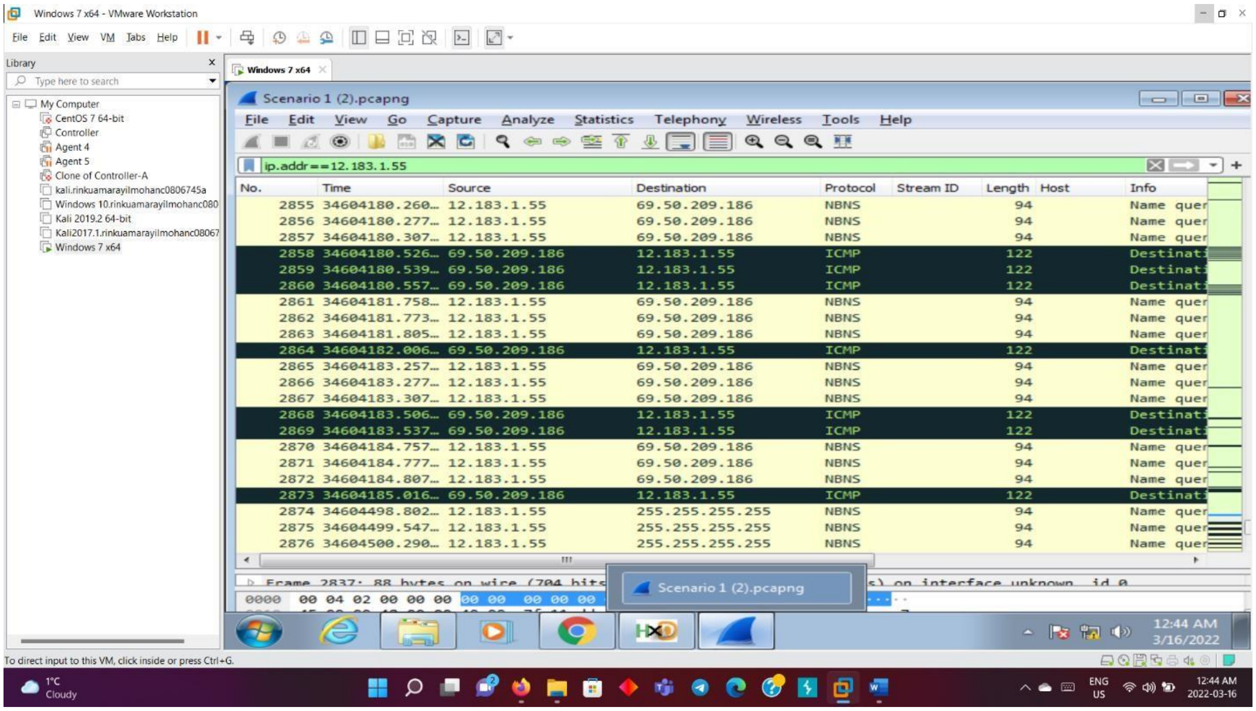
Displayed	Title	Type	Fields	Field Occurence
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☑	Length	Packet length (bytes)		
☑	Info	Information		
☑	Stream ID	Custom		



Displayed	Title	Type	Fields	Field Occurer
☑	No.	Number		
☑	Time	Time (format as specified)		
☑	Source	Source address		
☑	Destination	Destination address		
☑	Protocol	Protocol		
☑	Stream ID	Custom	tcp.stream	0
☑	Length	Packet length (bytes)		
☑	Host	Custom	http.host	0
☑	Info	Information		

□ Show displayed columns only

Add another column as Host and rearrange it.

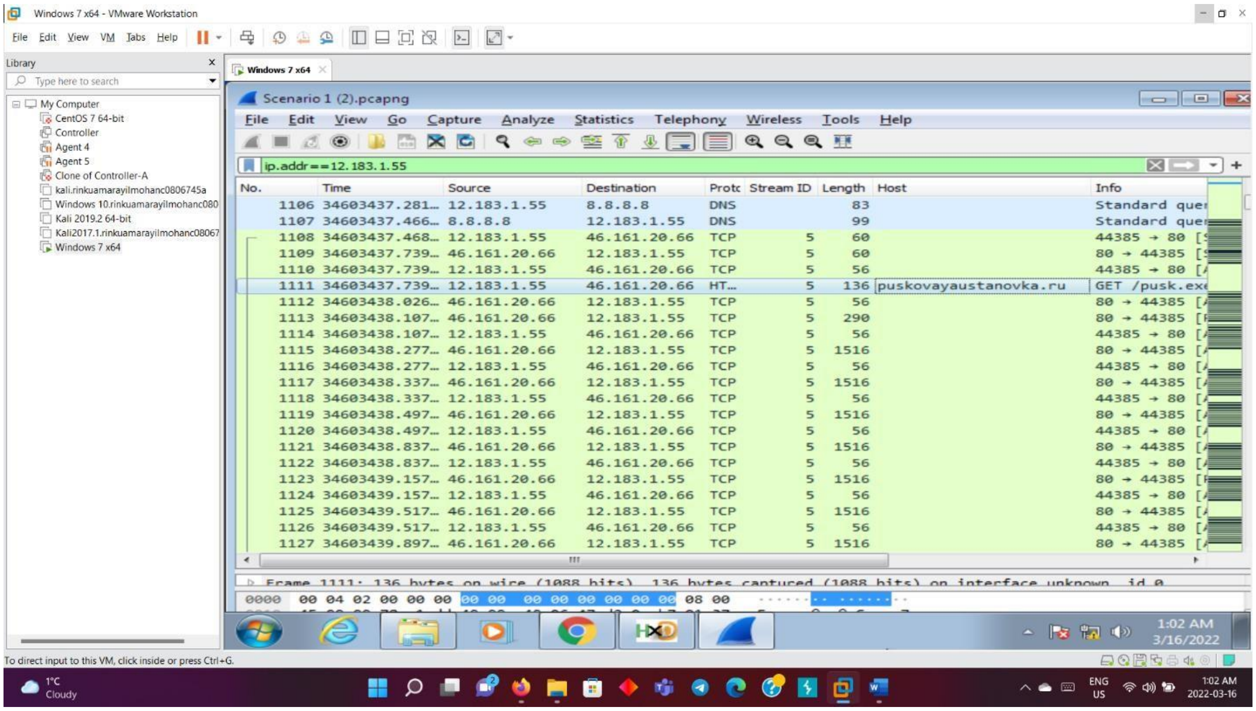

Windows 7 x64 - VMware Workstation
Scenario 1 (2).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==12.183.1.55

No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
2855	34604180.260…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2856	34604180.277…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2857	34604180.307…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2858	34604180.526…	69.50.209.186	12.183.1.55	ICMP		122		Destinati
2859	34604180.539…	69.50.209.186	12.183.1.55	ICMP		122		Destinati
2860	34604180.557…	69.50.209.186	12.183.1.55	ICMP		122		Destinati
2861	34604181.758…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2862	34604181.773…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2863	34604181.805…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2864	34604182.006…	69.50.209.186	12.183.1.55	ICMP		122		Destinati
2865	34604183.257…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2866	34604183.277…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2867	34604183.307…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2868	34604183.506…	69.50.209.186	12.183.1.55	ICMP		122		Destinati
2869	34604183.537…	69.50.209.186	12.183.1.55	ICMP		122		Destinati
2870	34604184.757…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2871	34604184.777…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2872	34604184.807…	12.183.1.55	69.50.209.186	NBNS		94		Name quer
2873	34604185.016…	69.50.209.186	12.183.1.55	ICMP		122		Destinati
2874	34604498.802…	12.183.1.55	255.255.255.255	NBNS		94		Name quer
2875	34604499.547…	12.183.1.55	255.255.255.255	NBNS		94		Name quer
2876	34604500.290…	12.183.1.55	255.255.255.255	NBNS		94		Name quer

```
Frame 2837: 88 bytes on wire (704 bits ... s) on interface unknown, id 0
0000  00 04 02 00 00 00 00 00  00 00 00
```

Now filter the victim machine: 12.183.1.55



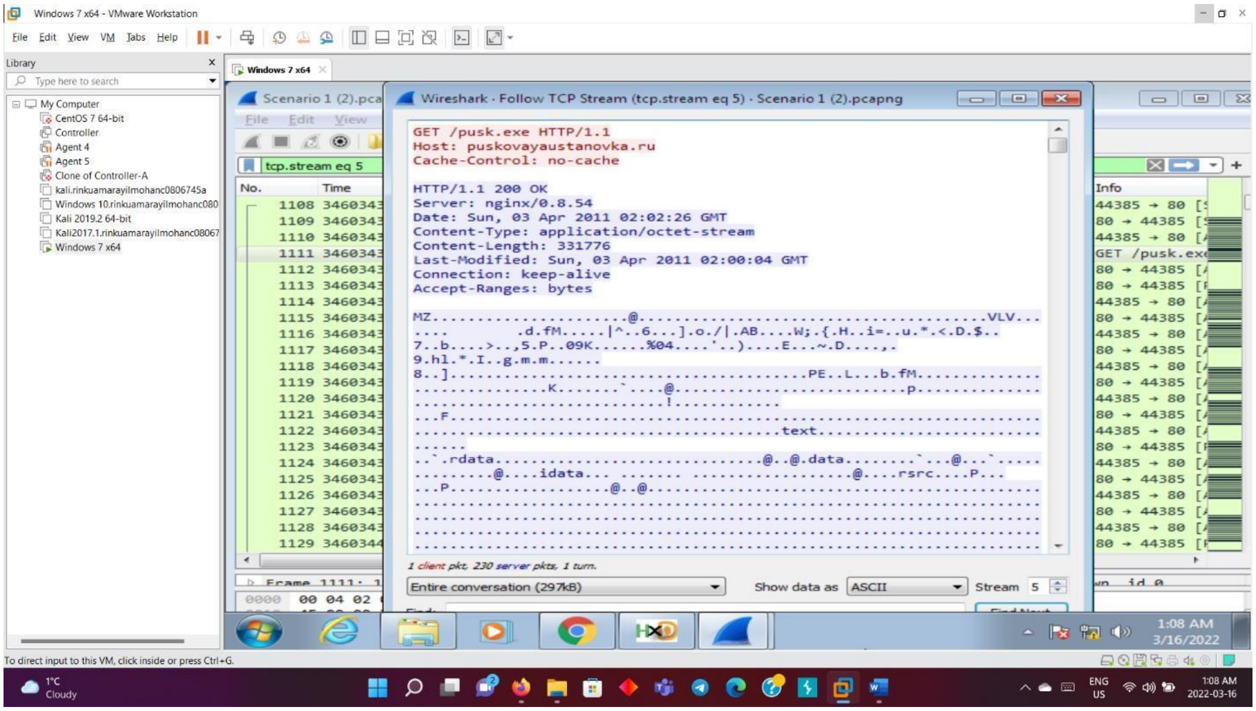
Windows 7 x64 - VMware Workstation
Scenario 1 (2).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
ip.addr==12.183.1.55

No.   Time              Source         Destination    Protc Stream ID Length Host                    Info
 1106 34603437.281…     12.183.1.55    8.8.8.8        DNS                 83                         Standard quer
 1107 34603437.466…     8.8.8.8        12.183.1.55    DNS                 99                         Standard quer
 1108 34603437.468…     12.183.1.55    46.161.20.66   TCP           5     60                         44385 → 80 [
 1109 34603437.739…     46.161.20.66   12.183.1.55    TCP           5     60                         80 → 44385 [
 1110 34603437.739…     12.183.1.55    46.161.20.66   TCP           5     56                         44385 → 80 [
 1111 34603437.739…     12.183.1.55    46.161.20.66   HT…           5    136 puskovayaustanovka.ru   GET /pusk.exe
 1112 34603438.026…     46.161.20.66   12.183.1.55    TCP           5     56                         80 → 44385 [
 1113 34603438.107…     46.161.20.66   12.183.1.55    TCP           5    290                         80 → 44385 [
 1114 34603438.107…     12.183.1.55    46.161.20.66   TCP           5     56                         44385 → 80 [
 1115 34603438.277…     46.161.20.66   12.183.1.55    TCP           5   1516                         80 → 44385 [
 1116 34603438.277…     12.183.1.55    46.161.20.66   TCP           5     56                         44385 → 80 [
 1117 34603438.337…     46.161.20.66   12.183.1.55    TCP           5   1516                         80 → 44385 [
 1118 34603438.337…     12.183.1.55    46.161.20.66   TCP           5     56                         44385 → 80 [
 1119 34603438.497…     46.161.20.66   12.183.1.55    TCP           5   1516                         80 → 44385 [
 1120 34603438.497…     12.183.1.55    46.161.20.66   TCP           5     56                         44385 → 80 [
 1121 34603438.837…     46.161.20.66   12.183.1.55    TCP           5   1516                         80 → 44385 [
 1122 34603438.837…     12.183.1.55    46.161.20.66   TCP           5     56                         44385 → 80 [
 1123 34603439.157…     46.161.20.66   12.183.1.55    TCP           5   1516                         80 → 44385 [
 1124 34603439.157…     12.183.1.55    46.161.20.66   TCP           5     56                         44385 → 80 [
 1125 34603439.517…     46.161.20.66   12.183.1.55    TCP           5   1516                         80 → 44385 [
 1126 34603439.517…     12.183.1.55    46.161.20.66   TCP           5     56                         44385 → 80 [
 1127 34603439.897…     46.161.20.66   12.183.1.55    TCP           5   1516                         80 → 44385 [

Frame 1111: 136 bytes on wire (1088 bits), 136 bytes captured (1088 bits) on interface unknown, id 0
0000  00 04 02 00 00 00 00 00 00 00 00 00 00 00 08 00
```

We can see suspicious communication from the above screenshot highlighted in blue.

Communicated from the victim machine :12.183.1.55, communicated to the ip address : 46.161.20.66

Browsed to the website :puskovayaustanovka.ru that belongs to the mentioned ip address : 46.161.20.66



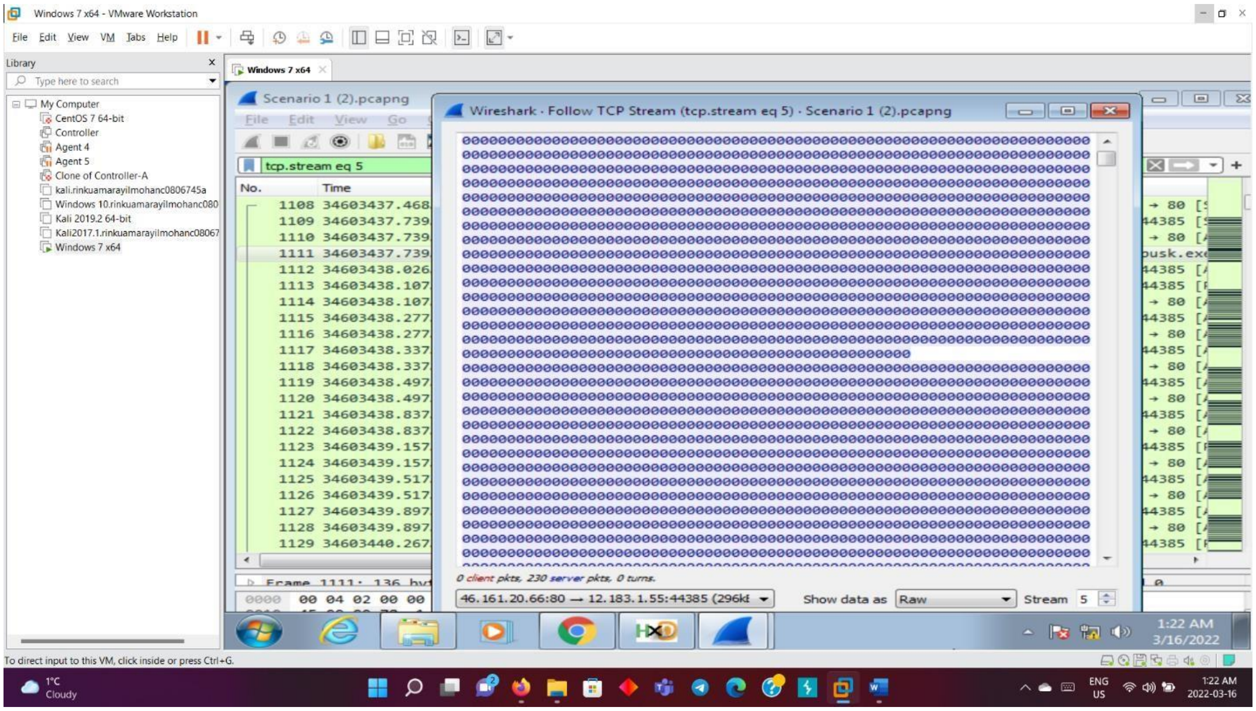
Windows 7 x64 - VMware Workstation
Wireshark · Follow TCP Stream (tcp.stream eq 5) · Scenario 1 (2).pcapng

```
GET /pusk.exe HTTP/1.1
Host: puskovayaustanovka.ru
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx/0.8.54
Date: Sun, 03 Apr 2011 02:02:26 GMT
Content-Type: application/octet-stream
Content-Length: 331776
Last-Modified: Sun, 03 Apr 2011 02:00:04 GMT
Connection: keep-alive
Accept-Ranges: bytes

MZ......................@...................................VLV...
....          .d.fM.....|^..6...].o./|.AB....W;.{.H..i=..u.*.<.D.$..
7..b....>..,5.P..09K......%04....'..)....E...~.D....,.
9.hl.*.I..g.m.m......
8..]......................................PE..L...b.fM..............
................K.......`....@............................p..............
...............................!............
...F..................................................................
.....................................text.............................
......
..`.rdata...........................@..@.data........`...@...`.....
.........@....idata...  .......  ..................@....rsrc....P...
...P..................@..@...........................................

1 client pkt, 230 server pkts, 1 turn.
Entire conversation (297kB)    Show data as ASCII    Stream 5
```

When we right click on the host name >click follow>TCP Stream, we get the details of the suspicious link along with the host name.

There could be 2 probabilities, either the client would have downloaded the file which contains the malware, or the other possibility could be that the machine would have had the malware already and the malware could have downloaded the effected file.

MZ is the windows executable file



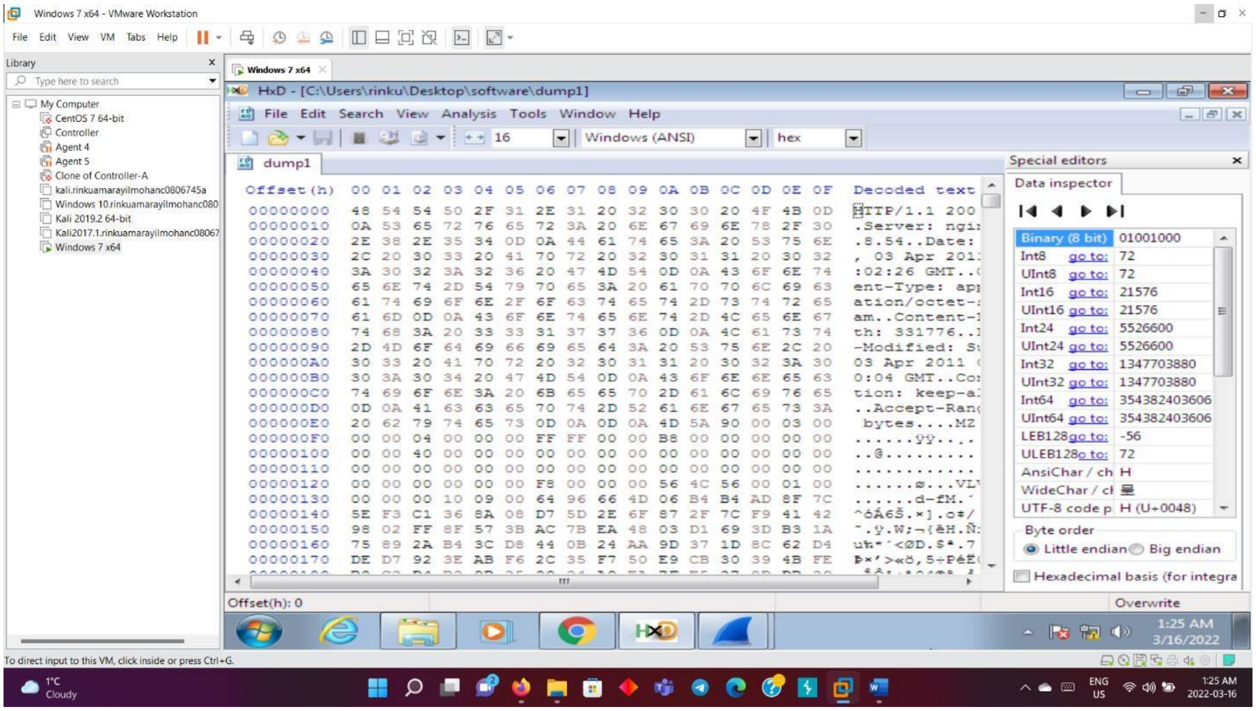
Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Controller
Agent 4
Agent 5
Clone of Controller-A
kali.rinkuamarayilmohanc0806745a
Windows 10.rinkuamarayilmohanc080
Kali 2019.2 64-bit
Kali2017.1.rinkuamarayilmohanc08067
Windows 7 x64
Scenario 1 (2).pcapng
Wireshark · Follow TCP Stream (tcp.stream eq 5) · Scenario 1 (2).pcapng
Show data as
Raw
Stream
5
To direct input to this VM, click inside or press Ctrl+G.
1°C
Cloudy
ENG
US

```
tcp.stream eq 5

No.   Time
1108  34603437.468
1109  34603437.739
1110  34603437.739
1111  34603437.739
1112  34603438.026
1113  34603438.107
1114  34603438.107
1115  34603438.277
1116  34603438.277
1117  34603438.337
1118  34603438.337
1119  34603438.497
1120  34603438.497
1121  34603438.837
1122  34603438.837
1123  34603439.157
1124  34603439.157
1125  34603439.517
1126  34603439.517
1127  34603439.897
1128  34603439.897
1129  34603440.267

Frame 1111: 136 byt
0000  00 04 02 00 00

0 client pkts, 230 server pkts, 0 turns.
46.161.20.66:80 → 12.183.1.55:44385 (296kB)
```

We can see the virus file in the raw format.

Save the file as dump 1.

Now open the file in HxD editor



HxD - [C:\Users\rinku\Desktop\software\dump1]

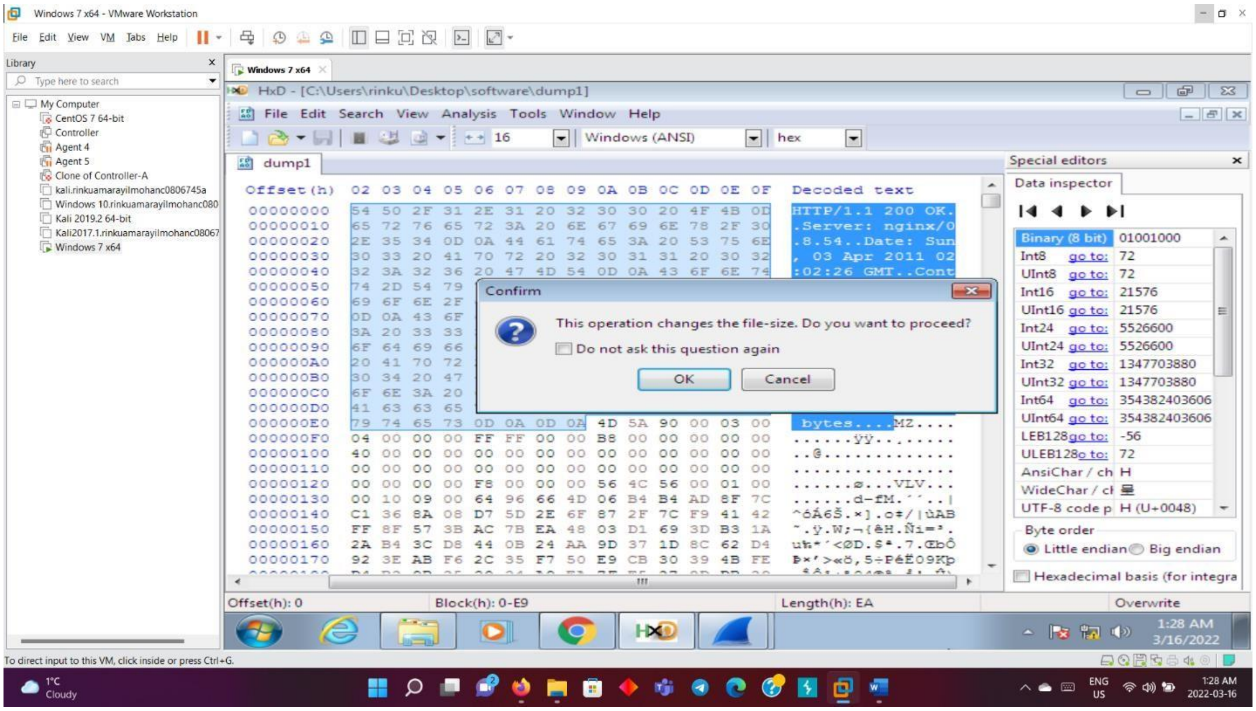
```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D  HTTP/1.1 200
00000010  0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 2F 30  .Server: ngi
00000020  2E 38 2E 35 34 0D 0A 44 61 74 65 3A 20 53 75 6E  .8.54..Date:
00000030  2C 20 30 33 20 41 70 72 20 32 30 31 31 20 30 32  , 03 Apr 201
00000040  3A 30 32 3A 32 36 20 47 4D 54 0D 0A 43 6F 6E 74  :02:26 GMT..
00000050  65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63  ent-Type: ap
00000060  61 74 69 6F 6E 2F 6F 63 74 65 74 2D 73 74 72 65  ation/octet-
00000070  61 6D 0D 0A 43 6F 6E 74 65 6E 74 2D 4C 65 6E 67  am..Content-
00000080  74 68 3A 20 33 33 31 37 37 36 0D 0A 4C 61 73 74  th: 331776..
00000090  2D 4D 6F 64 69 66 69 65 64 3A 20 53 75 6E 2C 20  -Modified: S
000000A0  30 33 20 41 70 72 20 32 30 31 31 20 30 32 3A 30  03 Apr 2011
000000B0  30 3A 30 34 20 47 4D 54 0D 0A 43 6F 6E 6E 65 63  0:04 GMT..Co
000000C0  74 69 6F 6E 3A 20 6B 65 65 70 2D 61 6C 69 76 65  tion: keep-a
000000D0  0D 0A 41 63 63 65 70 74 2D 52 61 6E 67 65 73 3A  ..Accept-Ran
000000E0  20 62 79 74 65 73 0D 0A 0D 0A 4D 5A 90 00 03 00   bytes....MZ
000000F0  00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00  ......ÿÿ....
00000100  00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00  ..@.........
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ............
00000120  00 00 00 00 00 00 F8 00 00 00 56 4C 56 00 01 00  ......ø...VL
00000130  00 00 00 10 09 00 64 96 66 4D 06 B4 B4 AD 8F 7C  ......d-fM.´
00000140  5E F3 C1 36 8A 08 D7 5D 2E 6F 87 2F 7C F9 41 42  ^óÁ6Š.×].o‡/
00000150  98 02 FF 8F 57 3B AC 7B EA 48 03 D1 69 3D B3 1A  ˜.ÿ.W;¬{êH.Ñ
00000160  75 89 2A B4 3C D8 44 0B 24 AA 9D 37 1D 8C 62 D4  u‰*´<ØD.$ª.7
00000170  DE D7 92 3E AB F6 2C 35 F7 50 E9 CB 30 39 4B FE  Þ×'>«ö,5÷PéË
```

Offset(h): 0 | Overwrite

Data inspector	
Binary (8 bit)	01001000
Int8	72
UInt8	72
Int16	21576
UInt16	21576
Int24	5526600
UInt24	5526600
Int32	1347703880
UInt32	1347703880
Int64	354382403606
UInt64	354382403606
LEB128	-56
ULEB128	72
AnsiChar / ch	H
WideChar / ch	䡈
UTF-8 code p	H (U+0048)

Byte order: ● Little endian ○ Big endian

□ Hexadecimal basis (for integra



HxD - [C:\Users\rinku\Desktop\software\dump1]

```
Offset(h) 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D  HTTP/1.1 200 OK.
00000010  65 72 76 65 72 3A 20 6E 67 69 6E 78 2F 30  .Server: nginx/0
00000020  2E 35 34 0D 0A 44 61 74 65 3A 20 53 75 6E  .8.54..Date: Sun
00000030  30 33 20 41 70 72 20 32 30 31 31 20 30 32  , 03 Apr 2011 02
00000040  32 3A 32 36 20 47 4D 54 0D 0A 43 6F 6E 74  :02:26 GMT..Cont
00000050  74 2D 54 79
00000060  69 6F 6E 2F
00000070  0D 0A 43 6F
00000080  3A 20 33 33
00000090  6F 64 69 66
000000A0  20 41 70 72
000000B0  30 34 20 47
000000C0  6F 6E 3A 20
000000D0  41 63 63 65
000000E0  79 74 65 73 0D 0A 0D 0A 4D 5A 90 00 03 00   bytes....MZ....
000000F0  04 00 00 00 FF FF 00 00 B8 00 00 00 00 00  ......ÿÿ......
00000100  40 00 00 00 00 00 00 00 00 00 00 00 00 00  ..@...........
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..............
00000120  00 00 00 00 F8 00 00 00 56 4C 56 00 01 00  ......ø...VLV...
00000130  00 10 09 00 64 96 66 4D 06 B4 B4 AD 8F 7C  ......d-fM.´´..|
00000140  C1 36 8A 08 D7 5D 2E 6F 87 2F 7C F9 41 42  ^óÁ6Š.×].o‡/|ùAB
00000150  FF 8F 57 3B AC 7B EA 48 03 D1 69 3D B3 1A  ˜.ÿ.W;¬{êH.Ñi=³.
00000160  2A B4 3C D8 44 0B 24 AA 9D 37 1D 8C 62 D4  u‰*´<ØD.$ª.7.ŒbÔ
00000170  92 3E AB F6 2C 35 F7 50 E9 CB 30 39 4B FE  Þ×'>«ö,5÷PéË09Kþ
```

Confirm

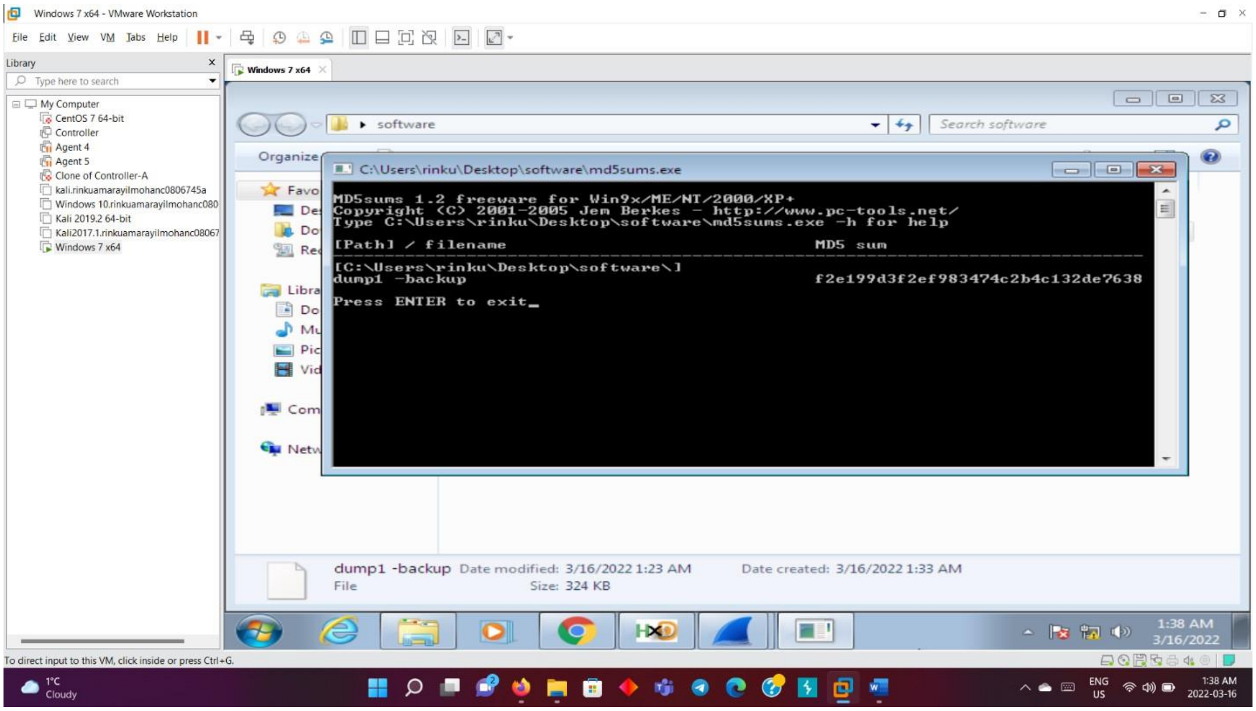
This operation changes the file-size. Do you want to proceed?

□ Do not ask this question again

OK | Cancel

Offset(h): 0 | Block(h): 0-E9 | Length(h): EA | Overwrite

Now select the header file and right click and delete it.


Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Controller
Agent 4
Agent 5
Clone of Controller-A
kali.rinkuamarayilmohanc0806745a
Windows 10.rinkuamarayilmohanc080
Kali 2019.2 64-bit
Kali2017.1.rinkuamarayilmohanc08067
Windows 7 x64
software
Search software
dump1 -backup Date modified: 3/16/2022 1:23 AM Date created: 3/16/2022 1:33 AM
File Size: 324 KB
1:38 AM
3/16/2022
To direct input to this VM, click inside or press Ctrl+G.

C:\Users\rinku\Desktop\software\md5sums.exe

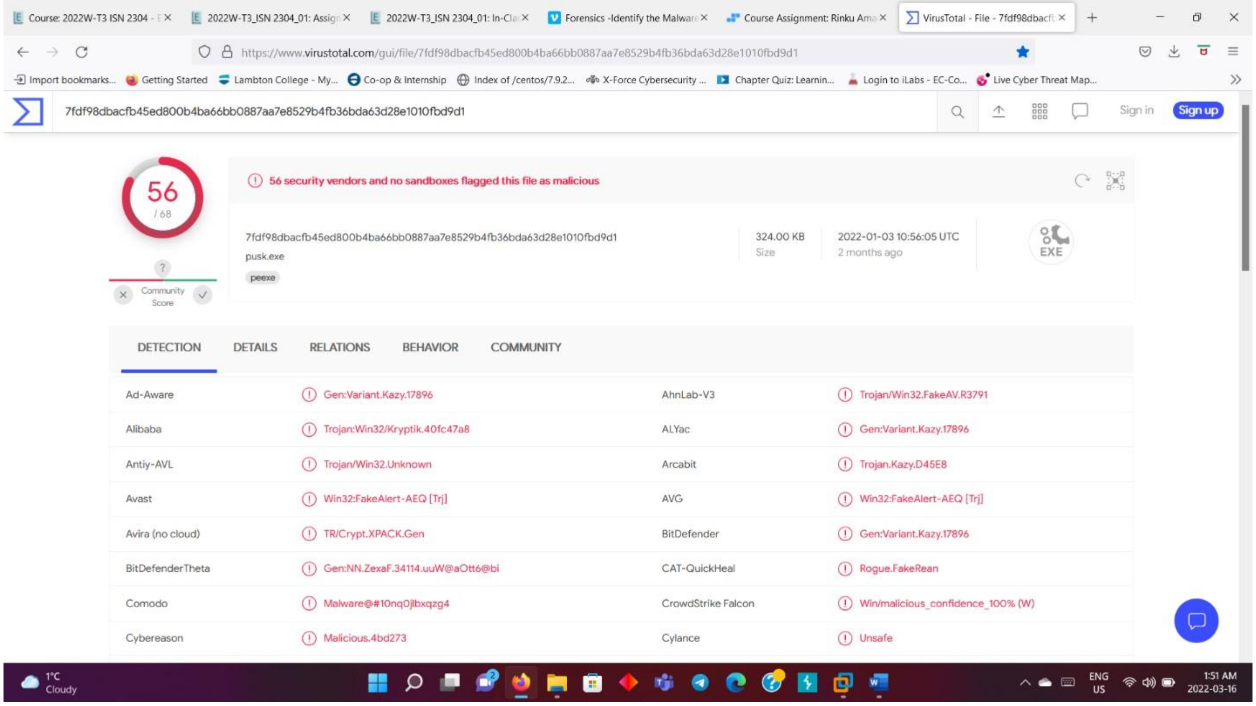
```
MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type C:\Users\rinku\Desktop\software\md5sums.exe -h for help

[Path] / filename                                         MD5 sum
-----------------------------------------------------------------------------
[C:\Users\rinku\Desktop\software\]
dump1 -backup                                             f2e199d3f2ef983474c2b4c132de7638

Press ENTER to exit_
```

Now drag and drop the dump 1 file to md5sums, so we get the window open as shown in the screenshot above.

We can see the MD5 sum value

Now go to the host machine and launch a browser and search for virustotal.com website and paste the md5sum value and search.

We get the below details as shown in the screenshot.


Course: 2022W-T3 ISN 2304
2022W-T3_ISN 2304_01: Assign
2022W-T3_ISN 2304_01: In-Cla
Forensics -Identify the Malware
Course Assignment: Rinku Ama
VirusTotal - File - 7fdf98dbacfb
https://www.virustotal.com/gui/file/7fdf98dbacfb45ed800b4ba66bb0887aa7e8529b4fb36bda63d28e1010fbd9d1
Import bookmarks... Getting Started Lambton College - My... Co-op & Internship Index of /centos/7.9.2... X-Force Cybersecurity ... Chapter Quiz: Learnin... Login to iLabs - EC-Co... Live Cyber Threat Map...
7fdf98dbacfb45ed800b4ba66bb0887aa7e8529b4fb36bda63d28e1010fbd9d1
Sign in
Sign up
56
/ 68
Community Score
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY
1:51 AM
2022-03-16

56 security vendors and no sandboxes flagged this file as malicious

7fdf98dbacfb45ed800b4ba66bb0887aa7e8529b4fb36bda63d28e1010fbd9d1
pusk.exe
peexe

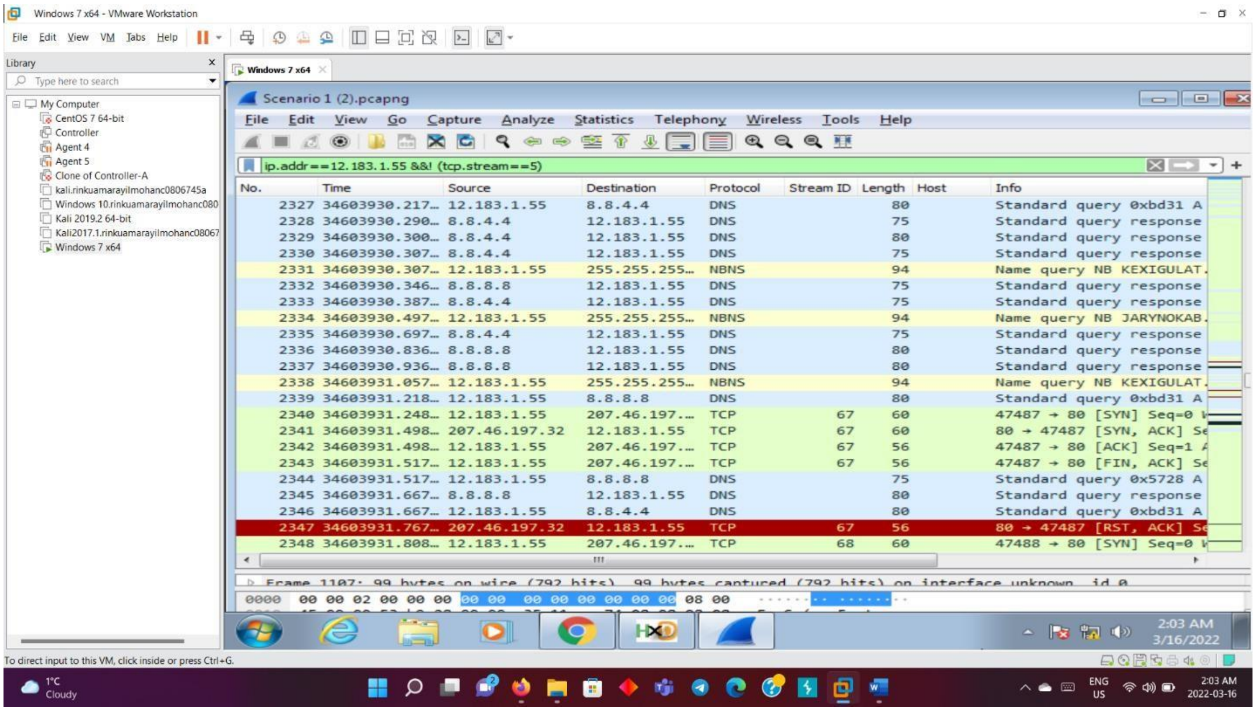
324.00 KB
Size

2022-01-03 10:56:05 UTC
2 months ago

Ad-Aware	Gen:Variant.Kazy.17896	AhnLab-V3	Trojan/Win32.FakeAV.R3791
Alibaba	Trojan:Win32/Kryptik.40fc47a8	ALYac	Gen:Variant.Kazy.17896
Antiy-AVL	Trojan/Win32.Unknown	Arcabit	Trojan.Kazy.D45E8
Avast	Win32:FakeAlert-AEQ [Trj]	AVG	Win32:FakeAlert-AEQ [Trj]
Avira (no cloud)	TR/Crypt.XPACK.Gen	BitDefender	Gen:Variant.Kazy.17896
BitDefenderTheta	Gen:NN.ZexaF.34114.uuW@aOtt6@bi	CAT-QuickHeal	Rogue.FakeRean
Comodo	Malware@#10nq0jlbxqzg4	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.4bd273	Cylance	Unsafe

We can see 56 security vendors, the list of companies that detected this virus.

Now we go get back to wireshark and enter the query : ip.addr==12.183.1.55 &&! (tcp.stream==5)



Scenario 1 (2).pcapng

```
ip.addr==12.183.1.55 &&! (tcp.stream==5)
```

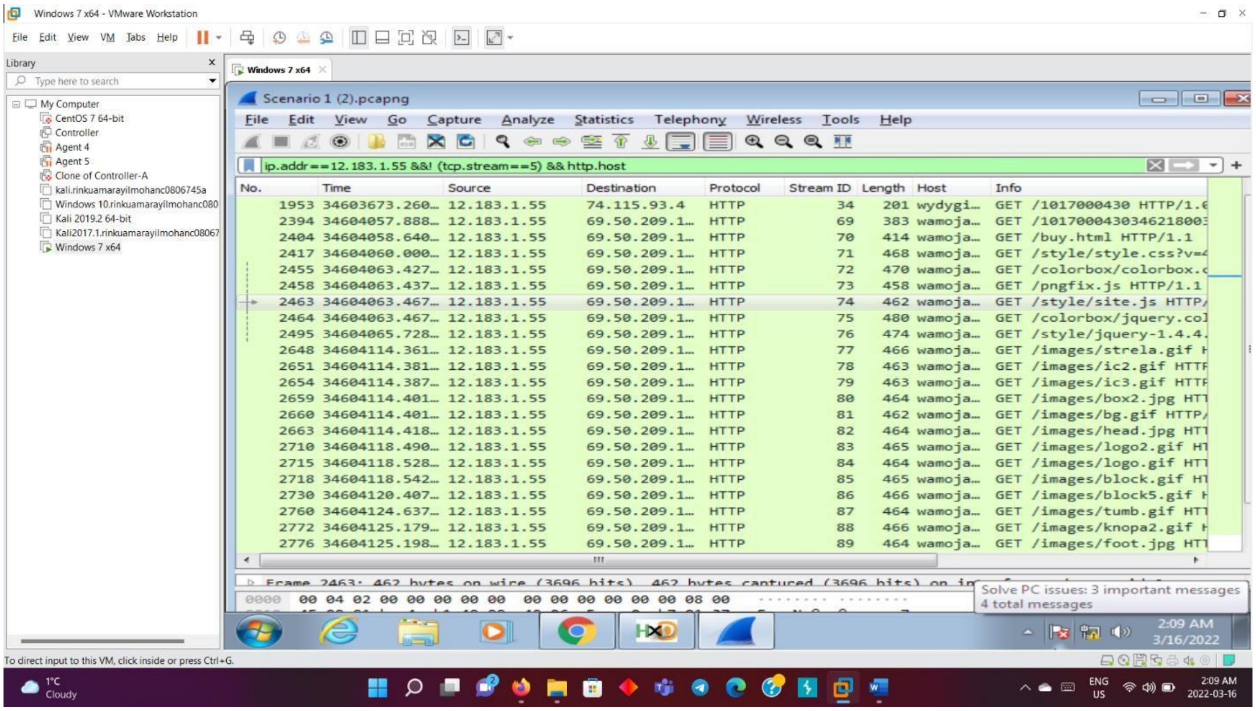
No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
2327	34603930.217…	12.183.1.55	8.8.4.4	DNS		80		Standard query 0xbd31 A
2328	34603930.290…	8.8.4.4	12.183.1.55	DNS		75		Standard query response
2329	34603930.300…	8.8.4.4	12.183.1.55	DNS		80		Standard query response
2330	34603930.307…	8.8.4.4	12.183.1.55	DNS		75		Standard query response
2331	34603930.307…	12.183.1.55	255.255.255…	NBNS		94		Name query NB KEXIGULAT.
2332	34603930.346…	8.8.8.8	12.183.1.55	DNS		75		Standard query response
2333	34603930.387…	8.8.4.4	12.183.1.55	DNS		75		Standard query response
2334	34603930.497…	12.183.1.55	255.255.255…	NBNS		94		Name query NB JARYNOKAB.
2335	34603930.697…	8.8.4.4	12.183.1.55	DNS		75		Standard query response
2336	34603930.836…	8.8.8.8	12.183.1.55	DNS		80		Standard query response
2337	34603930.936…	8.8.8.8	12.183.1.55	DNS		80		Standard query response
2338	34603931.057…	12.183.1.55	255.255.255…	NBNS		94		Name query NB KEXIGULAT.
2339	34603931.218…	12.183.1.55	8.8.8.8	DNS		80		Standard query 0xbd31 A
2340	34603931.248…	12.183.1.55	207.46.197.…	TCP	67	60		47487 → 80 [SYN] Seq=0 W
2341	34603931.498…	207.46.197.32	12.183.1.55	TCP	67	60		80 → 47487 [SYN, ACK] Se
2342	34603931.498…	12.183.1.55	207.46.197.…	TCP	67	56		47487 → 80 [ACK] Seq=1 A
2343	34603931.517…	12.183.1.55	207.46.197.…	TCP	67	56		47487 → 80 [FIN, ACK] Se
2344	34603931.517…	12.183.1.55	8.8.8.8	DNS		75		Standard query 0x5728 A
2345	34603931.667…	8.8.8.8	12.183.1.55	DNS		80		Standard query response
2346	34603931.667…	12.183.1.55	8.8.4.4	DNS		80		Standard query 0xbd31 A
2347	34603931.767…	207.46.197.32	12.183.1.55	TCP	67	56		80 → 47487 [RST, ACK] Se
2348	34603931.808…	12.183.1.55	207.46.197.…	TCP	68	60		47488 → 80 [SYN] Seq=0 W

```
Frame 1107: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface unknown, id 0
0000  00 00 02 00 00 00 00 00  00 00 00 00 00 00 08 00
```

Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Controller
Agent 4
Agent 5
Clone of Controller-A
kali.rinkuamarayilmohanc0806745a
Windows 10.rinkuamarayilmohanc080
Kali 2019.2 64-bit
Kali2017.1.rinkuamarayilmohanc08067
Windows 7 x64
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
2:03 AM
3/16/2022
To direct input to this VM, click inside or press Ctrl+G.
1°C
Cloudy
ENG
US
2:03 AM
2022-03-16

We get the above details.

query : ip.addr==12.183.1.55 &&! (tcp.stream==5) && http.host



Scenario 1 (2).pcapng

```
ip.addr==12.183.1.55 &&! (tcp.stream==5) && http.host
```

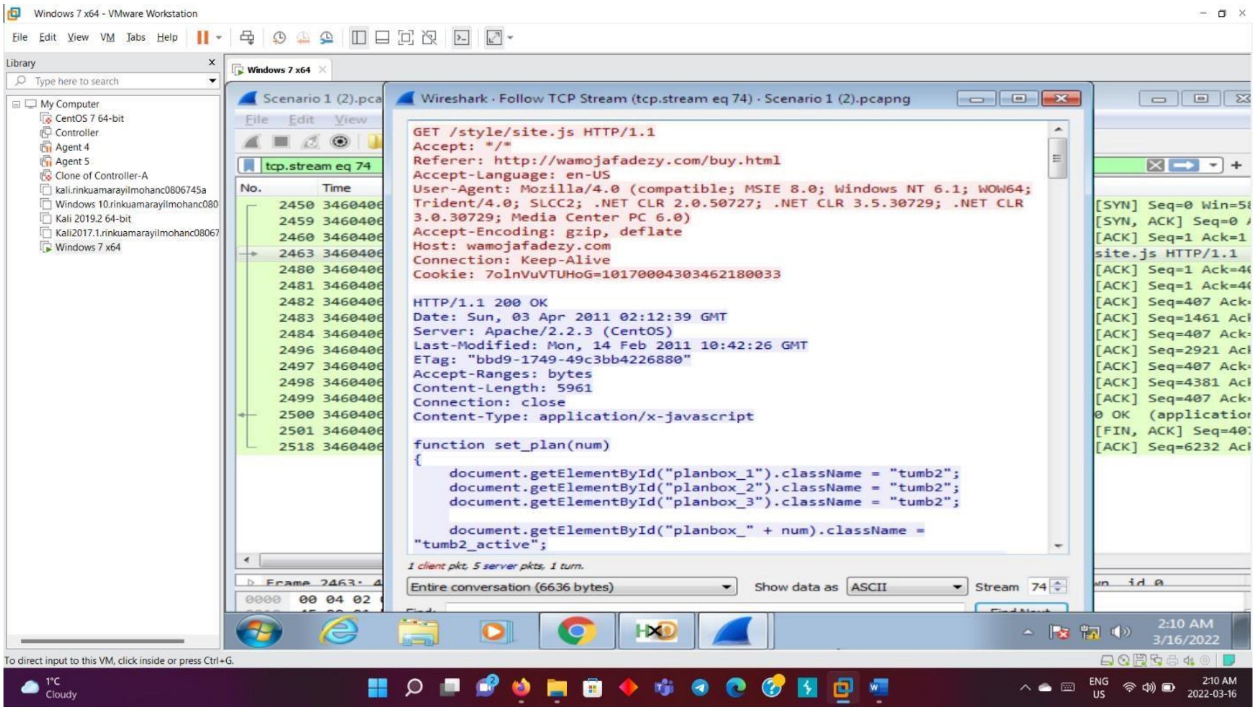
No.	Time	Source	Destination	Protocol	Stream ID	Length	Host	Info
1953	34603673.260…	12.183.1.55	74.115.93.4	HTTP	34	201	wydygi…	GET /1017000430 HTTP/1.(
2394	34604057.888…	12.183.1.55	69.50.209.1…	HTTP	69	383	wamoja…	GET /10170004303462180003
2404	34604058.640…	12.183.1.55	69.50.209.1…	HTTP	70	414	wamoja…	GET /buy.html HTTP/1.1
2417	34604060.000…	12.183.1.55	69.50.209.1…	HTTP	71	468	wamoja…	GET /style/style.css?v=4
2455	34604063.427…	12.183.1.55	69.50.209.1…	HTTP	72	470	wamoja…	GET /colorbox/colorbox.c
2458	34604063.437…	12.183.1.55	69.50.209.1…	HTTP	73	458	wamoja…	GET /pngfix.js HTTP/1.1
2463	34604063.467…	12.183.1.55	69.50.209.1…	HTTP	74	462	wamoja…	GET /style/site.js HTTP/
2464	34604063.467…	12.183.1.55	69.50.209.1…	HTTP	75	480	wamoja…	GET /colorbox/jquery.col
2495	34604065.728…	12.183.1.55	69.50.209.1…	HTTP	76	474	wamoja…	GET /style/jquery-1.4.4.
2648	34604114.361…	12.183.1.55	69.50.209.1…	HTTP	77	466	wamoja…	GET /images/strela.gif H
2651	34604114.381…	12.183.1.55	69.50.209.1…	HTTP	78	463	wamoja…	GET /images/ic2.gif HTTP
2654	34604114.387…	12.183.1.55	69.50.209.1…	HTTP	79	463	wamoja…	GET /images/ic3.gif HTTP
2659	34604114.401…	12.183.1.55	69.50.209.1…	HTTP	80	464	wamoja…	GET /images/box2.jpg HTT
2660	34604114.401…	12.183.1.55	69.50.209.1…	HTTP	81	462	wamoja…	GET /images/bg.gif HTTP/
2663	34604114.418…	12.183.1.55	69.50.209.1…	HTTP	82	464	wamoja…	GET /images/head.jpg HTT
2710	34604118.490…	12.183.1.55	69.50.209.1…	HTTP	83	465	wamoja…	GET /images/logo2.gif HT
2715	34604118.528…	12.183.1.55	69.50.209.1…	HTTP	84	464	wamoja…	GET /images/logo.gif HTT
2718	34604118.542…	12.183.1.55	69.50.209.1…	HTTP	85	465	wamoja…	GET /images/block.gif HT
2730	34604120.407…	12.183.1.55	69.50.209.1…	HTTP	86	466	wamoja…	GET /images/block5.gif H
2760	34604124.637…	12.183.1.55	69.50.209.1…	HTTP	87	464	wamoja…	GET /images/tumb.gif HTT
2772	34604125.179…	12.183.1.55	69.50.209.1…	HTTP	88	466	wamoja…	GET /images/knopa2.gif H
2776	34604125.198…	12.183.1.55	69.50.209.1…	HTTP	89	464	wamoja…	GET /images/foot.jpg HTT

```
Frame 2463: 462 bytes on wire (3696 bits), 462 bytes captured (3696 bits) on in
0000  00 04 02 00 00 00 00 00  00 00 00 00 00 00 08 00
```

Solve PC issues: 3 important messages
4 total messages

Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Controller
Agent 4
Agent 5
Clone of Controller-A
kali.rinkuamarayilmohanc0806745a
Windows 10.rinkuamarayilmohanc080
Kali 2019.2 64-bit
Kali2017.1.rinkuamarayilmohanc08067
Windows 7 x64
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
2:09 AM
3/16/2022
To direct input to this VM, click inside or press Ctrl+G.
1°C
Cloudy
ENG
US
2:09 AM
2022-03-16

We can see all the http connections.



Windows 7 x64 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
CentOS 7 64-bit
Controller
Agent 4
Agent 5
Clone of Controller-A
kali.rinkuamarayilmohanc0806745a
Windows 10.rinkuamarayilmohanc080
Kali 2019.2 64-bit
Kali2017.1.rinkuamarayilmohanc08067
Windows 7 x64
Scenario 1 (2).pca
Wireshark · Follow TCP Stream (tcp.stream eq 74) · Scenario 1 (2).pcapng
To direct input to this VM, click inside or press Ctrl+G.
2:10 AM
3/16/2022
1°C
Cloudy
ENG
US
2:10 AM
2022-03-16

tcp.stream eq 74

```
No.    Time
2450 3460406                    [SYN] Seq=0 Win=5
2459 3460406                    [SYN, ACK] Seq=0 
2460 3460406                    [ACK] Seq=1 Ack=1
2463 3460406                    site.js HTTP/1.1
2480 3460406                    [ACK] Seq=1 Ack=4
2481 3460406                    [ACK] Seq=1 Ack=4
2482 3460406                    [ACK] Seq=407 Ack
2483 3460406                    [ACK] Seq=1461 Ac
2484 3460406                    [ACK] Seq=407 Ack
2496 3460406                    [ACK] Seq=2921 Ac
2497 3460406                    [ACK] Seq=407 Ack
2498 3460406                    [ACK] Seq=4381 Ac
2499 3460406                    [ACK] Seq=407 Ack
2500 3460406                    0 OK  (applicatio
2501 3460406                    [FIN, ACK] Seq=40
2518 3460406                    [ACK] Seq=6232 Ac
```

```
GET /style/site.js HTTP/1.1
Accept: */*
Referer: http://wamojafadezy.com/buy.html
Accept-Language: en-US
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR
3.0.30729; Media Center PC 6.0)
Accept-Encoding: gzip, deflate
Host: wamojafadezy.com
Connection: Keep-Alive
Cookie: 7olnVuVTUHoG=10170004303462180033

HTTP/1.1 200 OK
Date: Sun, 03 Apr 2011 02:12:39 GMT
Server: Apache/2.2.3 (CentOS)
Last-Modified: Mon, 14 Feb 2011 10:42:26 GMT
ETag: "bbd9-1749-49c3bb4226880"
Accept-Ranges: bytes
Content-Length: 5961
Connection: close
Content-Type: application/x-javascript

function set_plan(num)
{
    document.getElementById("planbox_1").className = "tumb2";
    document.getElementById("planbox_2").className = "tumb2";
    document.getElementById("planbox_3").className = "tumb2";

    document.getElementById("planbox_" + num).className =
"tumb2_active";
```

1 client pkt, 5 server pkts, 1 turn.

Entire conversation (6636 bytes) Show data as ASCII Stream 74

We can cross check if the link is secure by right clicking the link and select follow and tcp.stream.

When we see User-agent, then we can confirm that it was requested by the agent. Not all links can be malicious

Conclusion

Using Wireshark, we were able to locate the malware and the information stored in it by analyzing the data packet stream. Hex Editor and MD5Sum generator were also useful in confirming the detected file’s integrity.

Summary

We started with Wireshark to try and locate the malware. We were able to get the victim IP address from Wireshark's packet capture logs, upon using the IP address to create appropriate filter queries we were able to successfully locate the malware and the IP address it was communicating with using victims' system. After capturing the malware, we used Hex Editor to remove the header data in the malware binary and then calculated the MD5 hash for rest of the data using MD5Sum. This generated hash was then used by an online tool, Virus Total which uses multiple security vendors to confirm the file is indeed infected.

Achievement

In this assignment we were able to successfully analyze data packets in a network, identify malwares present and differentiate malicious traffic from actual traffic. We were able to utilize Wireshark to not only identify but extract details about the malware. We learnt about editing binary files using Hex Editor and how to confirm malware presence in a captured binary using Virus Total.

Reference

1. https://vimeo.com/617511540
2. https://drive.google.com/drive/folders/1Ffv50PIHWIlZg4zjmk0W7vLvRHzcZ01I?usp=sharing 3. https://drive.google.com/drive/folders/19BcrG1-57OMdlylRyPi_35kpCffFyQYv?usp=sharing

Name of students who has not participated in the assignment.
Student name:
Student name:
Student name:
Student name:
Student name:

All students have participated in this assignment