Wireshark Exercise Part-2

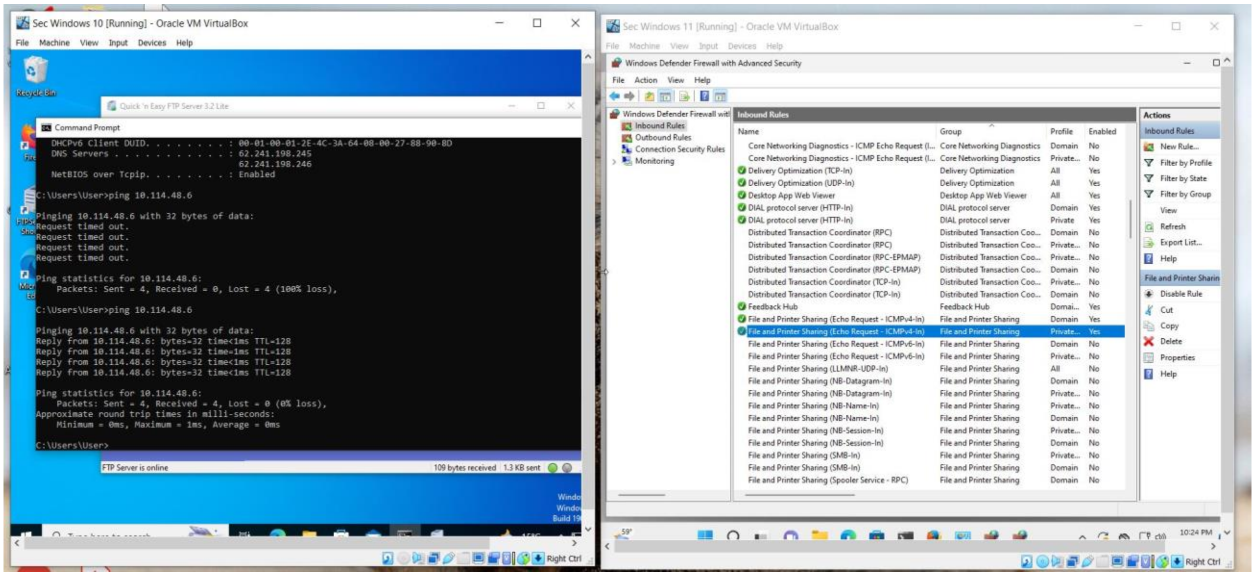
For this exercise, three virtual machines have been prepared. Th first one is Kali Linux, from where Wireshark has been run. The other two virtual machines are Windows 10 and Windows 11. In windows 10, Firewall, Defender and updates have been disabled. Echo request-ICMPv4-In rule has been enabled. Quick n Easy FTP server 3.2 has been installed in windows 10. In Windows 11 Mozilla Firefox has been installed. All three machines are on 10.114.48.0 network. IP addresses assigned for these three machines are-

Kali Linux- 10.114.48.4

Windows 10- 10.114.48.5

Windows 11 – 10.114.48.6

All three machines can ping/communicate each other. These are shown in following screenshots-



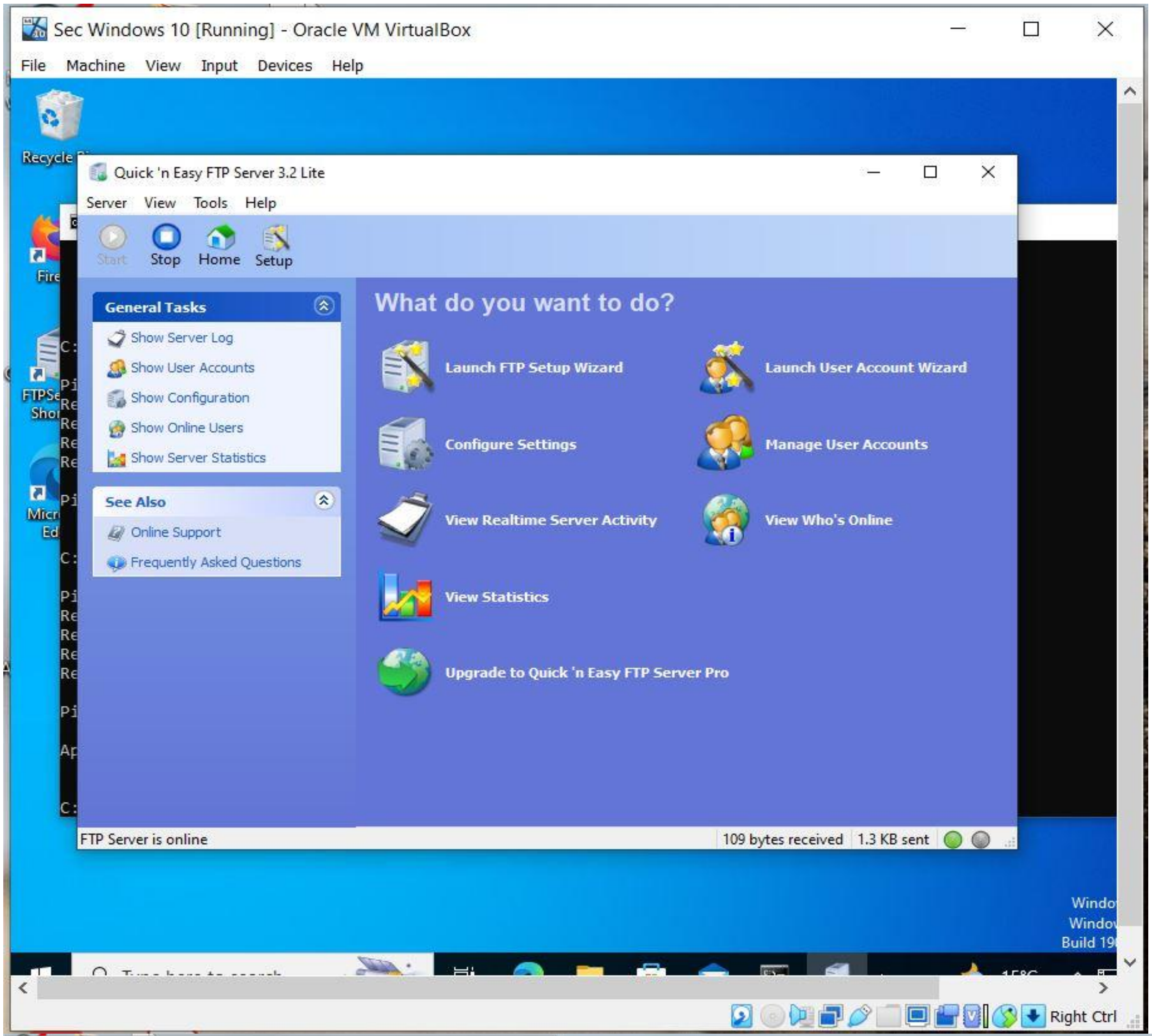
Sec Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Quick 'n Easy FTP Server 3.2 Lite
Command Prompt

```
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-4C-3A-64-08-00-27-88-90-8D
   DNS Servers . . . . . . . . . . . : 62.241.198.245
                                       62.241.198.246
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\User>ping 10.114.48.6

Pinging 10.114.48.6 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.114.48.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\User>ping 10.114.48.6

Pinging 10.114.48.6 with 32 bytes of data:
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128
Reply from 10.114.48.6: bytes=32 time=1ms TTL=128
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128

Ping statistics for 10.114.48.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
```

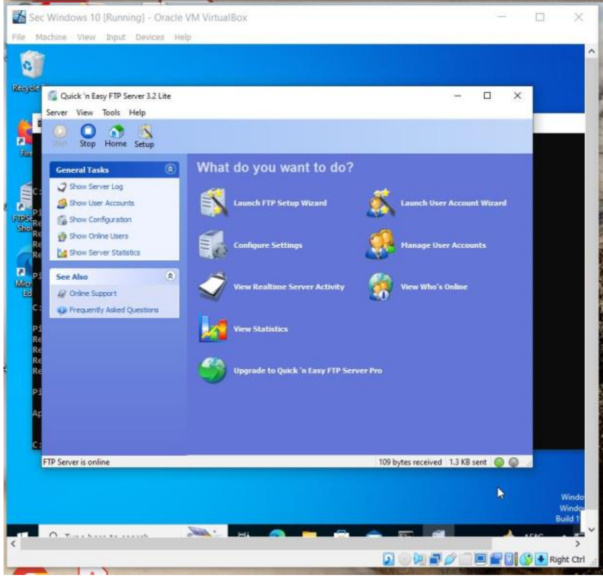
FTP Server is online | 109 bytes received | 1.3 KB sent

Inbound Rules

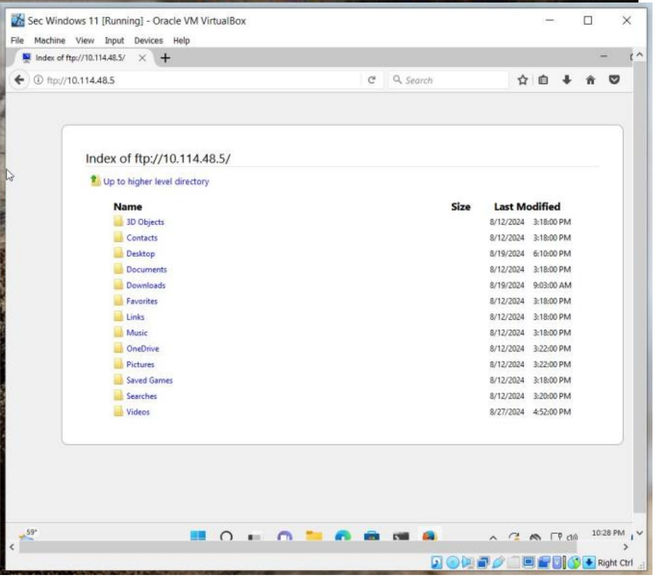
Name	Group	Profile	Enabled
Core Networking Diagnostics - ICMP Echo Request (I...	Core Networking Diagnostics	Domain	No
Core Networking Diagnostics - ICMP Echo Request (I...	Core Networking Diagnostics	Private...	No
✓ Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes
✓ Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes
✓ Desktop App Web Viewer	Desktop App Web Viewer	All	Yes
✓ DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes
✓ DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (RPC-EPMAP)	Distributed Transaction Coo...	Domain	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Private...	No
Distributed Transaction Coordinator (TCP-In)	Distributed Transaction Coo...	Domain	No
✓ Feedback Hub	Feedback Hub	Domai...	Yes
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Domain	Yes
✓ File and Printer Sharing (Echo Request - ICMPv4-In)	File and Printer Sharing	Private...	Yes
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Echo Request - ICMPv6-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Private...	No
File and Printer Sharing (SMB-In)	File and Printer Sharing	Domain	No
File and Printer Sharing (Spooler Service - RPC)	File and Printer Sharing	Domain	No



FTP Server is online | 109 bytes received | 1.3 KB sent


Sec Windows 10 [Running] - Oracle VM VirtualBox
Quick 'n Easy FTP Server 3.2 Lite
What do you want to do?
Right Ctrl

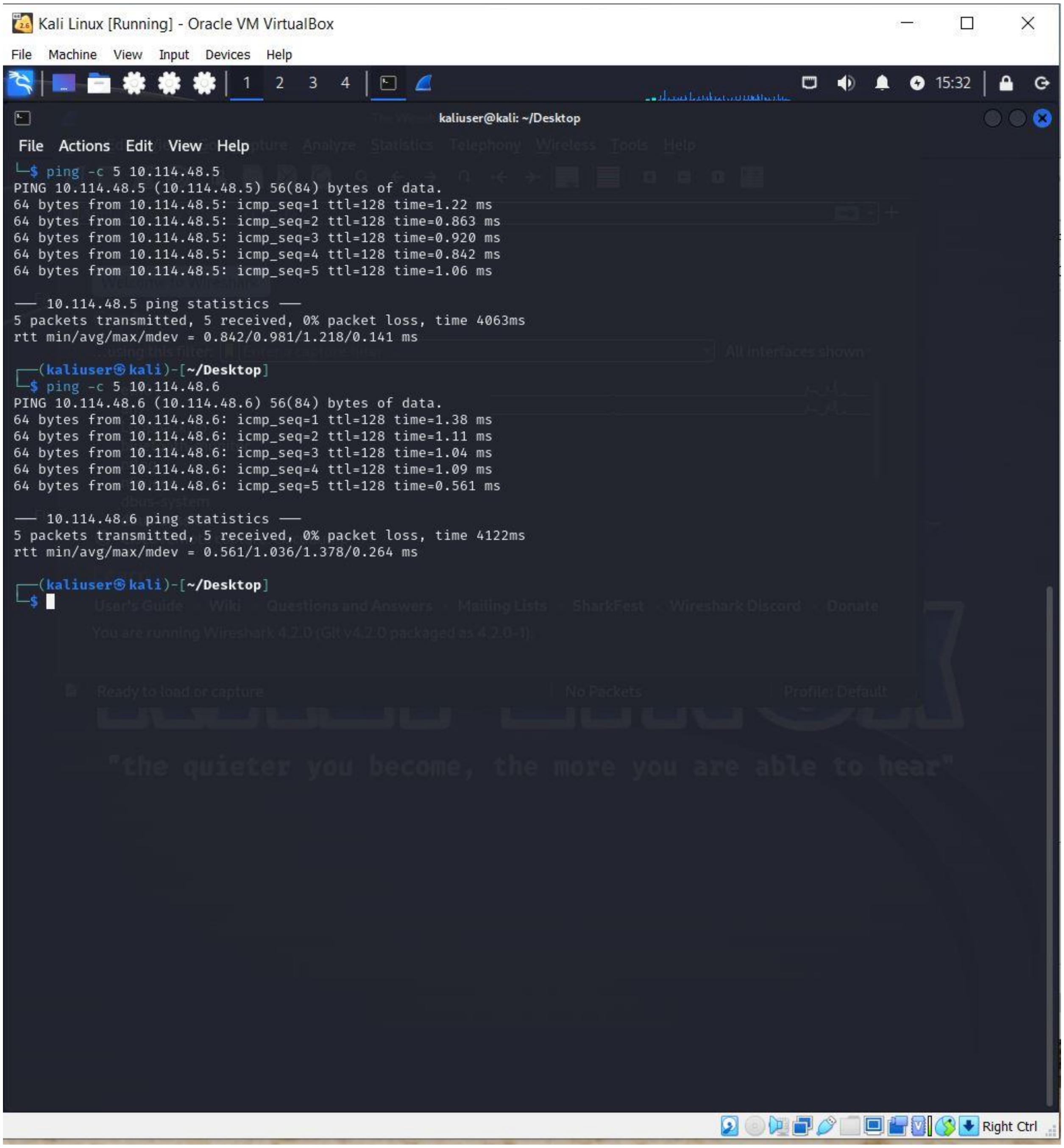
FTP Server is online | 109 bytes received | 1.3 KB sent


Sec Windows 11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of ftp://10.114.48.5/
ftp://10.114.48.5
Search
Right Ctrl

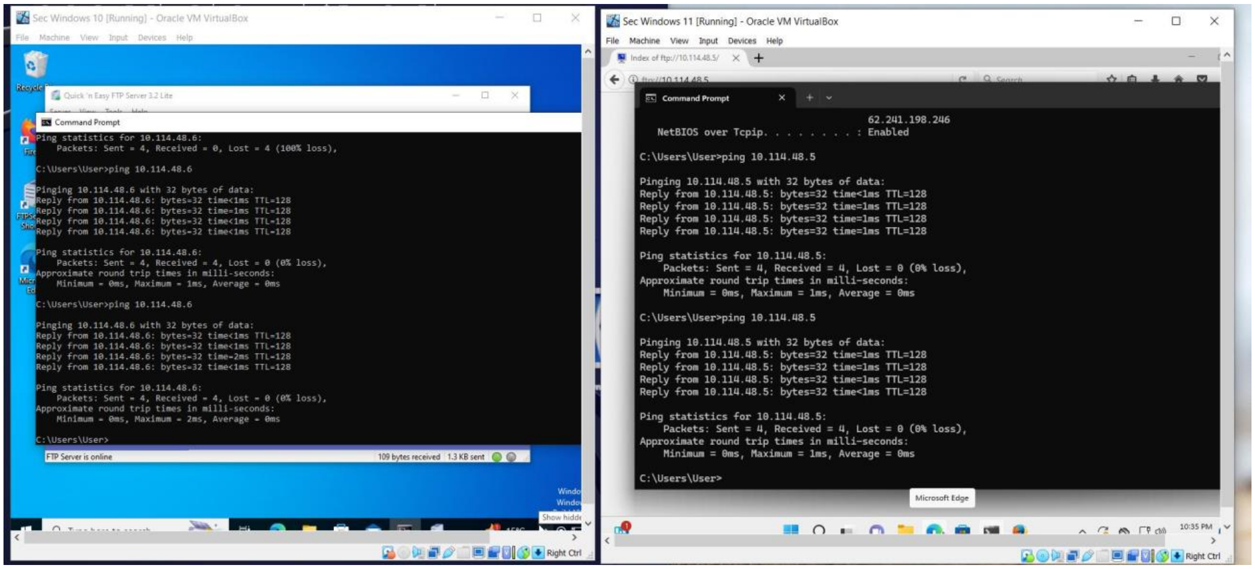
Index of ftp://10.114.48.5/

Up to higher level directory

Name	Size	Last Modified
3D Objects		8/12/2024 3:18:00 PM
Contacts		8/12/2024 3:18:00 PM
Desktop		8/19/2024 6:10:00 PM
Documents		8/12/2024 3:18:00 PM
Downloads		8/19/2024 9:03:00 AM
Favorites		8/12/2024 3:18:00 PM
Links		8/12/2024 3:18:00 PM
Music		8/12/2024 3:18:00 PM
OneDrive		8/12/2024 3:22:00 PM
Pictures		8/12/2024 3:22:00 PM
Saved Games		8/12/2024 3:18:00 PM
Searches		8/12/2024 3:20:00 PM
Videos		8/27/2024 4:52:00 PM


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
15:32
kaliuser@kali: ~/Desktop
File Actions Edit View Help
Right Ctrl

```
└─$ ping -c 5 10.114.48.5
PING 10.114.48.5 (10.114.48.5) 56(84) bytes of data.
64 bytes from 10.114.48.5: icmp_seq=1 ttl=128 time=1.22 ms
64 bytes from 10.114.48.5: icmp_seq=2 ttl=128 time=0.863 ms
64 bytes from 10.114.48.5: icmp_seq=3 ttl=128 time=0.920 ms
64 bytes from 10.114.48.5: icmp_seq=4 ttl=128 time=0.842 ms
64 bytes from 10.114.48.5: icmp_seq=5 ttl=128 time=1.06 ms

--- 10.114.48.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4063ms
rtt min/avg/max/mdev = 0.842/0.981/1.218/0.141 ms

┌──(kaliuser㉿kali)-[~/Desktop]
└─$ ping -c 5 10.114.48.6
PING 10.114.48.6 (10.114.48.6) 56(84) bytes of data.
64 bytes from 10.114.48.6: icmp_seq=1 ttl=128 time=1.38 ms
64 bytes from 10.114.48.6: icmp_seq=2 ttl=128 time=1.11 ms
64 bytes from 10.114.48.6: icmp_seq=3 ttl=128 time=1.04 ms
64 bytes from 10.114.48.6: icmp_seq=4 ttl=128 time=1.09 ms
64 bytes from 10.114.48.6: icmp_seq=5 ttl=128 time=0.561 ms

--- 10.114.48.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4122ms
rtt min/avg/max/mdev = 0.561/1.036/1.378/0.264 ms

┌──(kaliuser㉿kali)-[~/Desktop]
└─$ 
```

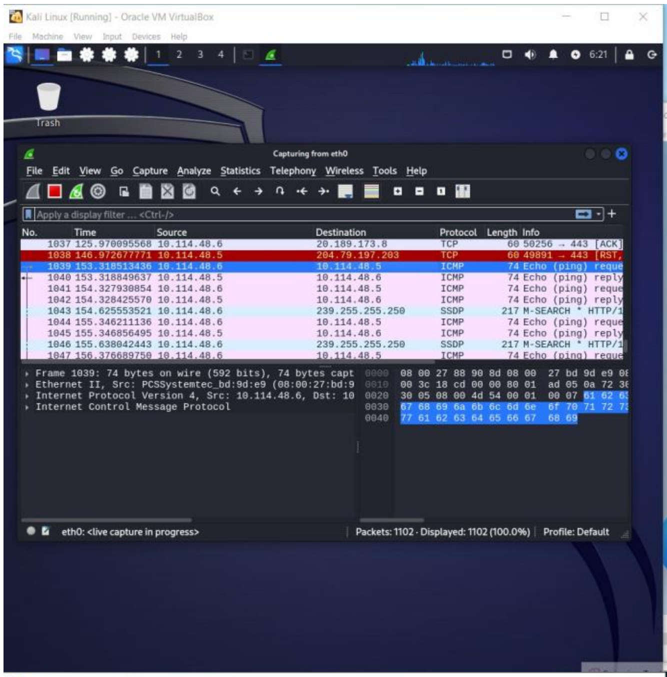

Sec Windows 10 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Quick 'n Easy FTP Server 3.2 Lite
Command Prompt
FTP Server is online
109 bytes received
1.3 KB sent
Right Ctrl
Sec Windows 11 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Index of ftp://10.114.48.5/
Command Prompt
Microsoft Edge
10:35 PM
Right Ctrl

```
Ping statistics for 10.114.48.6:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\User>ping 10.114.48.6

Pinging 10.114.48.6 with 32 bytes of data:
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128
Reply from 10.114.48.6: bytes=32 time=1ms TTL=128
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128

Ping statistics for 10.114.48.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>ping 10.114.48.6

Pinging 10.114.48.6 with 32 bytes of data:
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128
Reply from 10.114.48.6: bytes=32 time=2ms TTL=128
Reply from 10.114.48.6: bytes=32 time<1ms TTL=128

Ping statistics for 10.114.48.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Users\User>
```

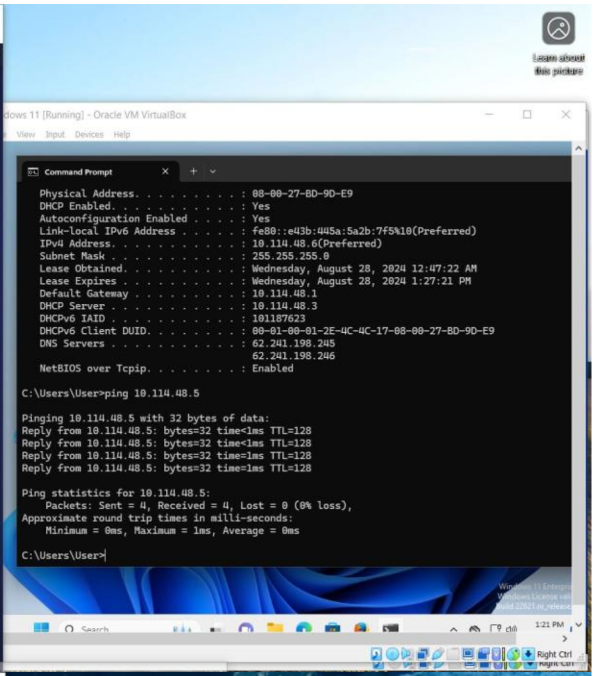
```
                                       62.241.198.246
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\User>ping 10.114.48.5

Pinging 10.114.48.5 with 32 bytes of data:
Reply from 10.114.48.5: bytes=32 time<1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128

Ping statistics for 10.114.48.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>ping 10.114.48.5

Pinging 10.114.48.5 with 32 bytes of data:
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128
Reply from 10.114.48.5: bytes=32 time<1ms TTL=128

Ping statistics for 10.114.48.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
```

Wireshirk Pcap Analysis

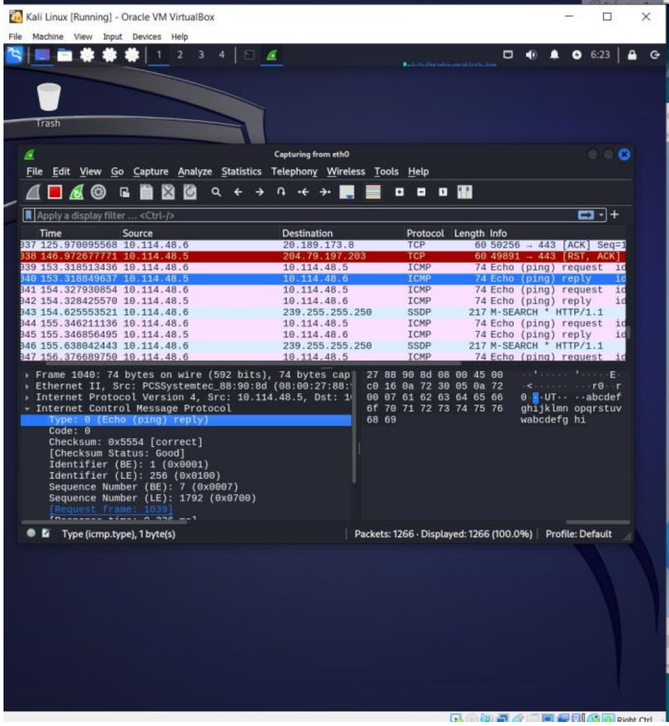
To experiment with wireshark, packet capture has been pressed to run and captured packets have been started to be visible for analysis. From Windows 10 and Windows 11 command prompt, both devices have been pinged, which became visible in Pcap after filtering as icmp packets. Useful information such as source and destination IPs have been seen. Also, FTP data traffics have been seen when Windows 11 started to connect FTP server in Windows 10. Wireshark also has shown unencrypted data such as username and password. These are shown in screenshots below:


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
6:21
Trash
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

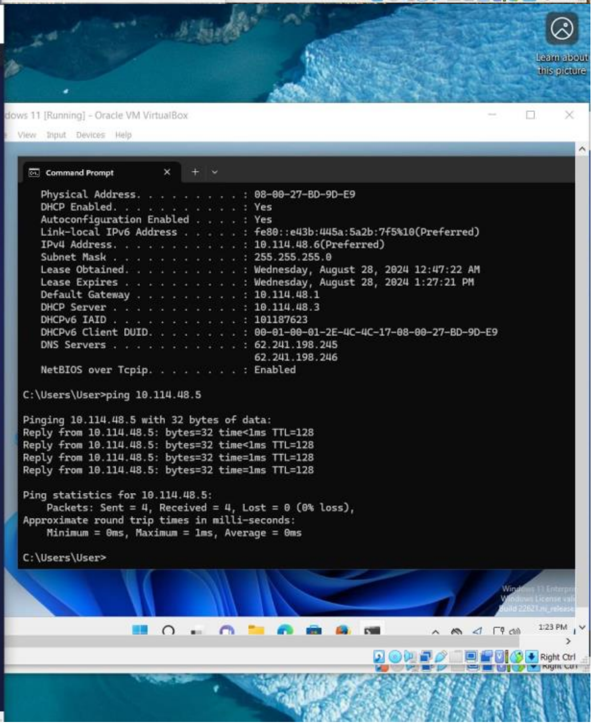
```
No.   Time           Source        Destination      Protocol Length Info
 1037 125.970095568 10.114.48.6   20.189.173.8     TCP       60 50256 → 443 [ACK]
 1038 146.972677771 10.114.48.5   204.79.197.203   TCP       60 49891 → 443 [RST,
 1039 153.318513436 10.114.48.6   10.114.48.5      ICMP      74 Echo (ping) reque
 1040 153.318849637 10.114.48.5   10.114.48.6      ICMP      74 Echo (ping) reply
 1041 154.327930854 10.114.48.6   10.114.48.5      ICMP      74 Echo (ping) reque
 1042 154.328425570 10.114.48.5   10.114.48.6      ICMP      74 Echo (ping) reply
 1043 154.625553521 10.114.48.6   239.255.255.250  SSDP     217 M-SEARCH * HTTP/1
 1044 155.346211136 10.114.48.6   10.114.48.5      ICMP      74 Echo (ping) reque
 1045 155.346856495 10.114.48.5   10.114.48.6      ICMP      74 Echo (ping) reply
 1046 155.638042443 10.114.48.6   239.255.255.250  SSDP     217 M-SEARCH * HTTP/1
 1047 156.376689750 10.114.48.6   10.114.48.5      ICMP      74 Echo (ping) reque

› Frame 1039: 74 bytes on wire (592 bits), 74 bytes capt   0000  08 00 27 88 90 8d 08 00  27 bd 9d e9 08
› Ethernet II, Src: PCSSystemtec_bd:9d:e9 (08:00:27:bd:9   0010  00 3c 18 cd 00 00 80 01  ad 05 0a 72 36
› Internet Protocol Version 4, Src: 10.114.48.6, Dst: 10   0020  30 05 08 00 4d 54 00 01  00 07 61 62 63
› Internet Control Message Protocol                        0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73
                                                           0040  77 61 62 63 64 65 66 67  68 69

eth0: <live capture in progress>    Packets: 1102 · Displayed: 1102 (100.0%)    Profile: Default
```



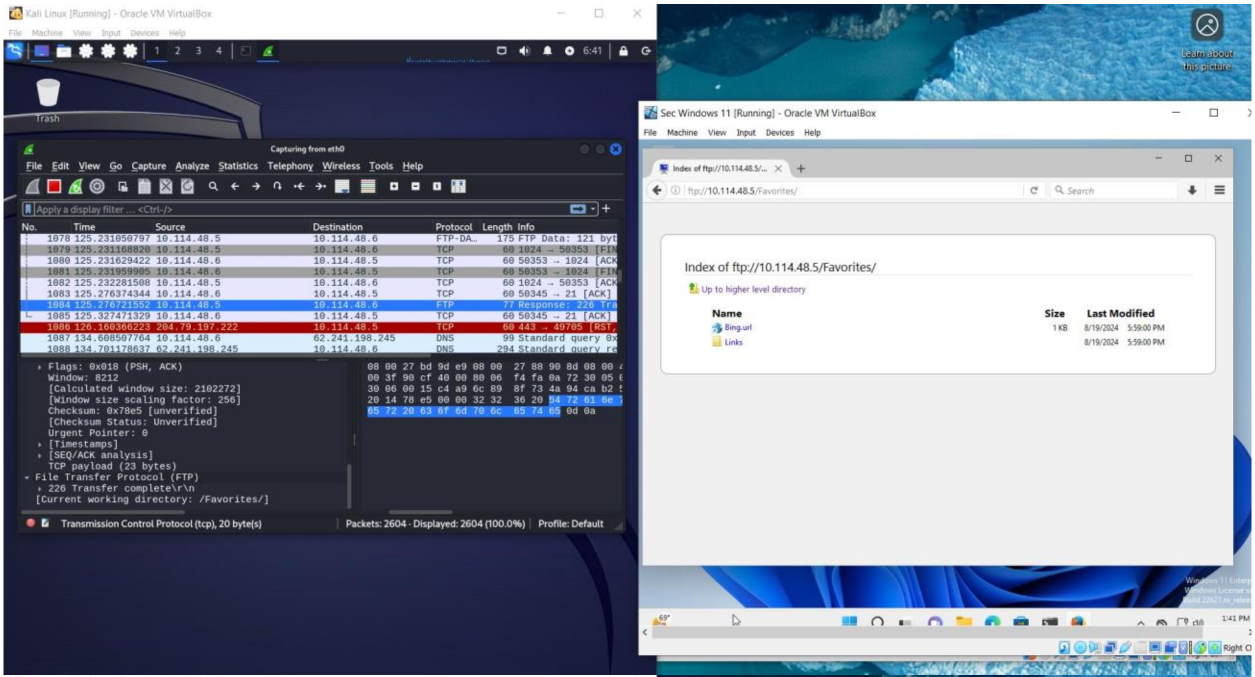
```
   Physical Address. . . . . . . . . : 08-00-27-BD-9D-E9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e43b:445a:5a2b:7f5%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.114.48.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 28, 2024 12:47:22 AM
   Lease Expires . . . . . . . . . . : Wednesday, August 28, 2024 1:27:21 PM
   Default Gateway . . . . . . . . . : 10.114.48.1
   DHCP Server . . . . . . . . . . . : 10.114.48.3
   DHCPv6 IAID . . . . . . . . . . . : 101187623
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-4C-4C-17-08-00-27-BD-9D-E9
   DNS Servers . . . . . . . . . . . : 62.241.198.245
                                       62.241.198.246
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\User>ping 10.114.48.5

Pinging 10.114.48.5 with 32 bytes of data:
Reply from 10.114.48.5: bytes=32 time<1ms TTL=128
Reply from 10.114.48.5: bytes=32 time<1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128

Ping statistics for 10.114.48.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
```


Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
6:23
Trash
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Right Ctrl

```
    Time          Source        Destination      Protocol Length Info
)37 125.970095568 10.114.48.6   20.189.173.8     TCP       60 50256 → 443 [ACK] Seq=1
)38 146.972677771 10.114.48.5   204.79.197.203   TCP       60 49891 → 443 [RST, ACK]
)39 153.318513436 10.114.48.6   10.114.48.5      ICMP      74 Echo (ping) request  id
)40 153.318849637 10.114.48.5   10.114.48.6      ICMP      74 Echo (ping) reply    id
)41 154.327930854 10.114.48.6   10.114.48.5      ICMP      74 Echo (ping) request  id
)42 154.328425570 10.114.48.5   10.114.48.6      ICMP      74 Echo (ping) reply    id
)43 154.625553521 10.114.48.6   239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
)44 155.346211136 10.114.48.6   10.114.48.5      ICMP      74 Echo (ping) request  id
)45 155.346856495 10.114.48.5   10.114.48.6      ICMP      74 Echo (ping) reply    id
)46 155.638042443 10.114.48.6   239.255.255.250  SSDP     217 M-SEARCH * HTTP/1.1
)47 156.376689750 10.114.48.6   10.114.48.5      ICMP      74 Echo (ping) request  id

› Frame 1040: 74 bytes on wire (592 bits), 74 bytes cap   27 88 90 8d 08 00 45 00   ··'·····'····E
› Ethernet II, Src: PCSSystemtec_88:90:8d (08:00:27:88:   c0 16 0a 72 30 05 0a 72   ·<·······r0··r
› Internet Protocol Version 4, Src: 10.114.48.5, Dst: 1   00 07 61 62 63 64 65 66   0 · ·UT·· ··abcdef
⌄ Internet Control Message Protocol                       6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
     Type: 0 (Echo (ping) reply)                          68 69                     wabcdefg hi
     Code: 0
     Checksum: 0x5554 [correct]
     [Checksum Status: Good]
     Identifier (BE): 1 (0x0001)
     Identifier (LE): 256 (0x0100)
     Sequence Number (BE): 7 (0x0007)
     Sequence Number (LE): 1792 (0x0700)
     [Request frame: 1039]

Type (icmp.type), 1 byte(s)    Packets: 1266 · Displayed: 1266 (100.0%)    Profile: Default
```



```
   Physical Address. . . . . . . . . : 08-00-27-BD-9D-E9
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::e43b:445a:5a2b:7f5%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.114.48.6(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, August 28, 2024 12:47:22 AM
   Lease Expires . . . . . . . . . . : Wednesday, August 28, 2024 1:27:21 PM
   Default Gateway . . . . . . . . . : 10.114.48.1
   DHCP Server . . . . . . . . . . . : 10.114.48.3
   DHCPv6 IAID . . . . . . . . . . . : 101187623
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2E-4C-4C-17-08-00-27-BD-9D-E9
   DNS Servers . . . . . . . . . . . : 62.241.198.245
                                       62.241.198.246
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Users\User>ping 10.114.48.5

Pinging 10.114.48.5 with 32 bytes of data:
Reply from 10.114.48.5: bytes=32 time<1ms TTL=128
Reply from 10.114.48.5: bytes=32 time<1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128
Reply from 10.114.48.5: bytes=32 time=1ms TTL=128

Ping statistics for 10.114.48.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\User>
```



Kali Linux [Running] - Oracle VM VirtualBox

Capturing from eth0

```
No.   Time            Source          Destination     Protocol  Length Info
1078 125.231050797 10.114.48.5      10.114.48.6      FTP-DA…     175 FTP Data: 121 byt
1079 125.231168820 10.114.48.5      10.114.48.6      TCP          60 1024 → 50353 [FIN
1080 125.231629422 10.114.48.6      10.114.48.5      TCP          60 50353 → 1024 [ACK
1081 125.231959905 10.114.48.6      10.114.48.5      TCP          60 50353 → 1024 [FIN
1082 125.232281508 10.114.48.5      10.114.48.6      TCP          60 1024 → 50353 [ACK
1083 125.276374344 10.114.48.6      10.114.48.5      TCP          60 50345 → 21 [ACK]
1084 125.276721552 10.114.48.5      10.114.48.6      FTP          77 Response: 226 Tra
1085 125.327471329 10.114.48.6      10.114.48.5      TCP          60 50345 → 21 [ACK]
1086 126.160366223 204.79.197.222   10.114.48.5      TCP          60 443 → 49705 [RST,
1087 134.608507764 10.114.48.6      62.241.198.245   DNS          99 Standard query 0x
1088 134.701178637 62.241.198.245   10.114.48.6      DNS         294 Standard query re
```

```
  Flags: 0x018 (PSH, ACK)
  Window: 8212
  [Calculated window size: 2102272]
  [Window size scaling factor: 256]
  Checksum: 0x78e5 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  [Timestamps]
  [SEQ/ACK analysis]
  TCP payload (23 bytes)
File Transfer Protocol (FTP)
  226 Transfer complete\r\n
[Current working directory: /Favorites/]
```

```
08 00 27 bd 9d e9 08 00  27 88 90 8d 08 00
00 3f 90 cf 40 00 80 06  f4 fa 0a 72 30 05
30 06 00 15 c4 a9 6c 89  8f 73 4a 94 ca b2
20 14 78 e5 00 00 32 32  36 20 54 72 61 6e
65 72 20 63 6f 6d 70 6c  65 74 65 0d 0a
```

Transmission Control Protocol (tcp), 20 byte(s) | Packets: 2604 · Displayed: 2604 (100.0%) | Profile: Default

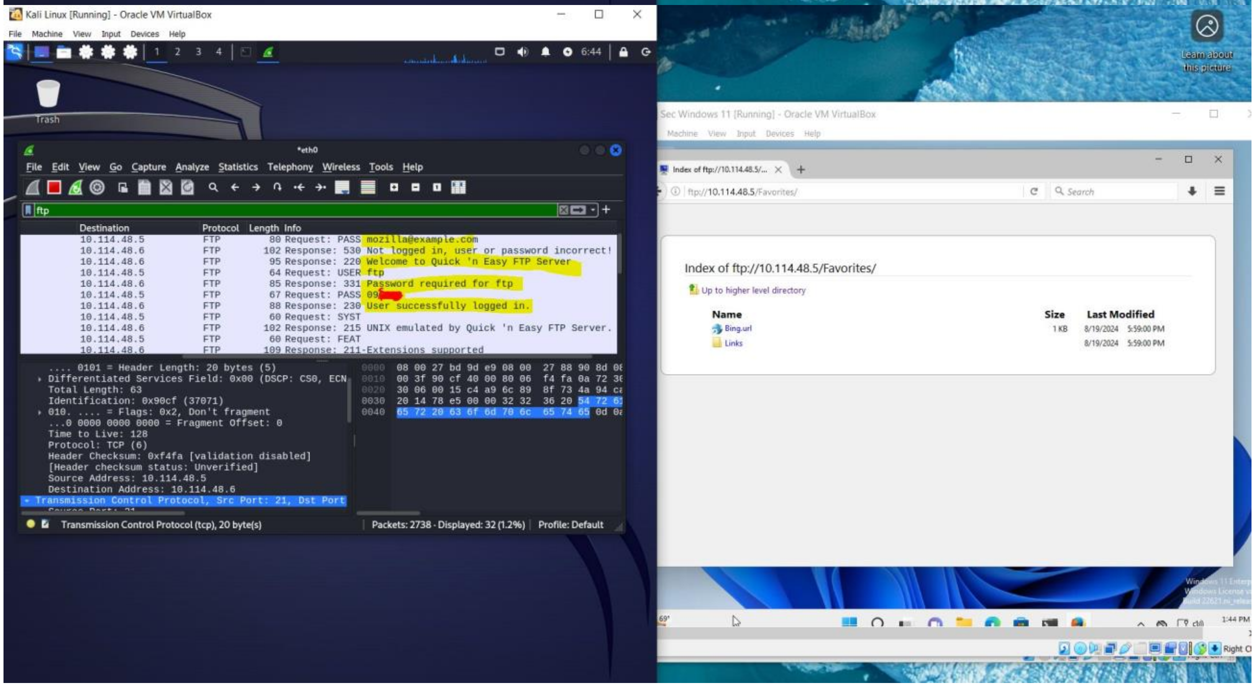
Sec Windows 11 [Running] - Oracle VM VirtualBox

Index of ftp://10.114.48.5/Favorites/

Up to higher level directory

Name	Size	Last Modified
Bing.url	1 KB	8/19/2024 5:59:00 PM
Links		8/19/2024 5:59:00 PM

Trash
File Machine View Input Devices Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Index of ftp://10.114.48.5/...
ftp://10.114.48.5/Favorites/
Search
Learn about this picture
6:41
1:41 PM



Kali Linux [Running] - Oracle VM VirtualBox

*eth0

ftp

```
Destination     Protocol  Length Info
10.114.48.5     FTP          80 Request: PASS mozilla@example.com
10.114.48.6     FTP         102 Response: 530 Not logged in, user or password incorrect!
10.114.48.6     FTP          95 Response: 220 Welcome to Quick 'n Easy FTP Server
10.114.48.5     FTP          64 Request: USER ftp
10.114.48.6     FTP          85 Response: 331 Password required for ftp
10.114.48.5     FTP          67 Request: PASS 09[redacted]
10.114.48.6     FTP          88 Response: 230 User successfully logged in.
10.114.48.5     FTP          60 Request: SYST
10.114.48.6     FTP         102 Response: 215 UNIX emulated by Quick 'n Easy FTP Server.
10.114.48.5     FTP          60 Request: FEAT
10.114.48.6     FTP         109 Response: 211-Extensions supported
```

```
  .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN
  Total Length: 63
  Identification: 0x90cf (37071)
  010. .... = Flags: 0x2, Don't fragment
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 128
  Protocol: TCP (6)
  Header Checksum: 0xf4fa [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.114.48.5
  Destination Address: 10.114.48.6
Transmission Control Protocol, Src Port: 21, Dst Port
```

```
0000  08 00 27 bd 9d e9 08 00  27 88 90 8d 08
0010  00 3f 90 cf 40 00 80 06  f4 fa 0a 72 30
0020  30 06 00 15 c4 a9 6c 89  8f 73 4a 94 ca
0030  20 14 78 e5 00 00 32 32  36 20 54 72 61
0040  65 72 20 63 6f 6d 70 6c  65 74 65 0d 0a
```

Transmission Control Protocol (tcp), 20 byte(s) | Packets: 2738 · Displayed: 32 (1.2%) | Profile: Default

Sec Windows 11 [Running] - Oracle VM VirtualBox

Index of ftp://10.114.48.5/Favorites/

Up to higher level directory

Name	Size	Last Modified
Bing.url	1 KB	8/19/2024 5:59:00 PM
Links		8/19/2024 5:59:00 PM

Trash
File Machine View Input Devices Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Index of ftp://10.114.48.5/...
ftp://10.114.48.5/Favorites/
Search
Learn about this picture
6:44
1:44 PM