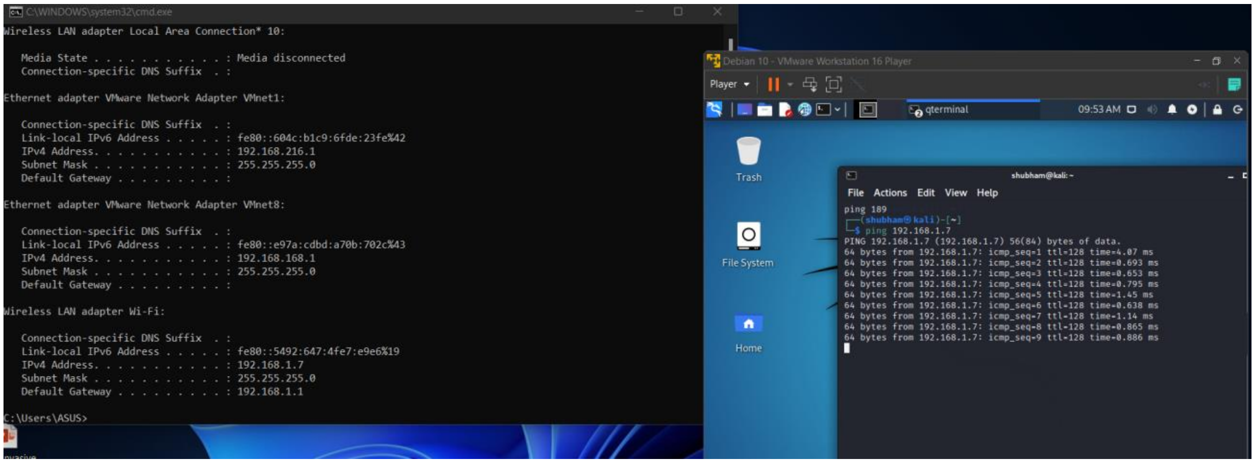
11) Show Windows and Kali can communicate


C:\WINDOWS\system32\cmd.exe
Debian 10 - VMware Workstation 16 Player
Player
qterminal
09:53 AM
Trash
File System
Home
shubham@kali: ~
File Actions Edit View Help

```
Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::604c:b1c9:6fde:23fe%42
   IPv4 Address. . . . . . . . . . . : 192.168.216.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e97a:cdbd:a70b:702c%43
   IPv4 Address. . . . . . . . . . . : 192.168.168.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5492:647:4fe7:e9e6%19
   IPv4 Address. . . . . . . . . . . : 192.168.1.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Users\ASUS>
```

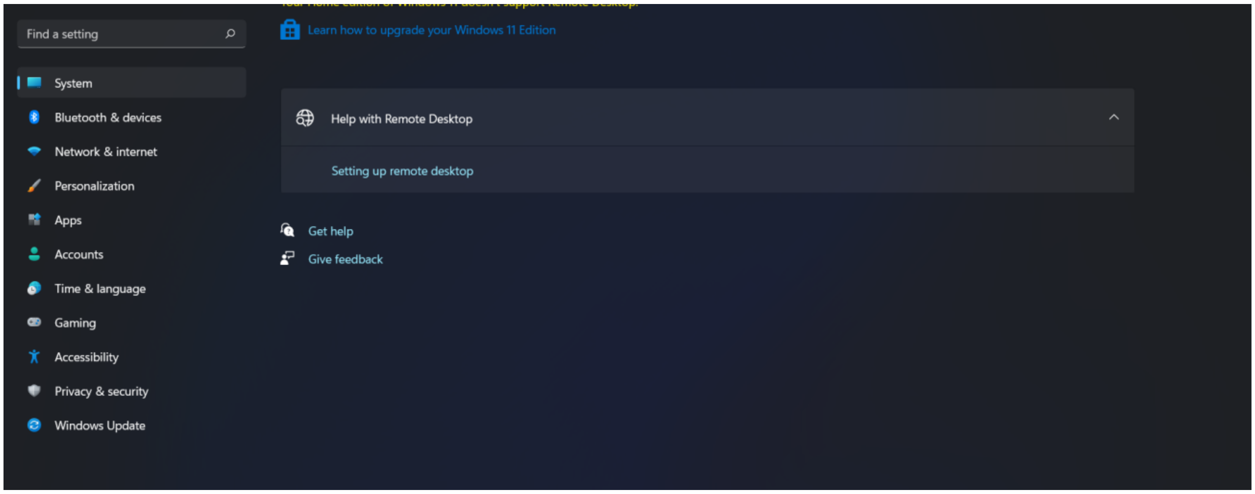
```
ping 189
┌──(shubham㉿kali)-[~]
└─$ ping 192.168.1.7
PING 192.168.1.7 (192.168.1.7) 56(84) bytes of data.
64 bytes from 192.168.1.7: icmp_seq=1 ttl=128 time=4.07 ms
64 bytes from 192.168.1.7: icmp_seq=2 ttl=128 time=0.693 ms
64 bytes from 192.168.1.7: icmp_seq=3 ttl=128 time=0.653 ms
64 bytes from 192.168.1.7: icmp_seq=4 ttl=128 time=0.795 ms
64 bytes from 192.168.1.7: icmp_seq=5 ttl=128 time=1.45 ms
64 bytes from 192.168.1.7: icmp_seq=6 ttl=128 time=0.638 ms
64 bytes from 192.168.1.7: icmp_seq=7 ttl=128 time=1.14 ms
64 bytes from 192.168.1.7: icmp_seq=8 ttl=128 time=0.865 ms
64 bytes from 192.168.1.7: icmp_seq=9 ttl=128 time=0.886 ms
```

Ping windows ip on Kali VM

12) How to open RDP and new ports on windows VM

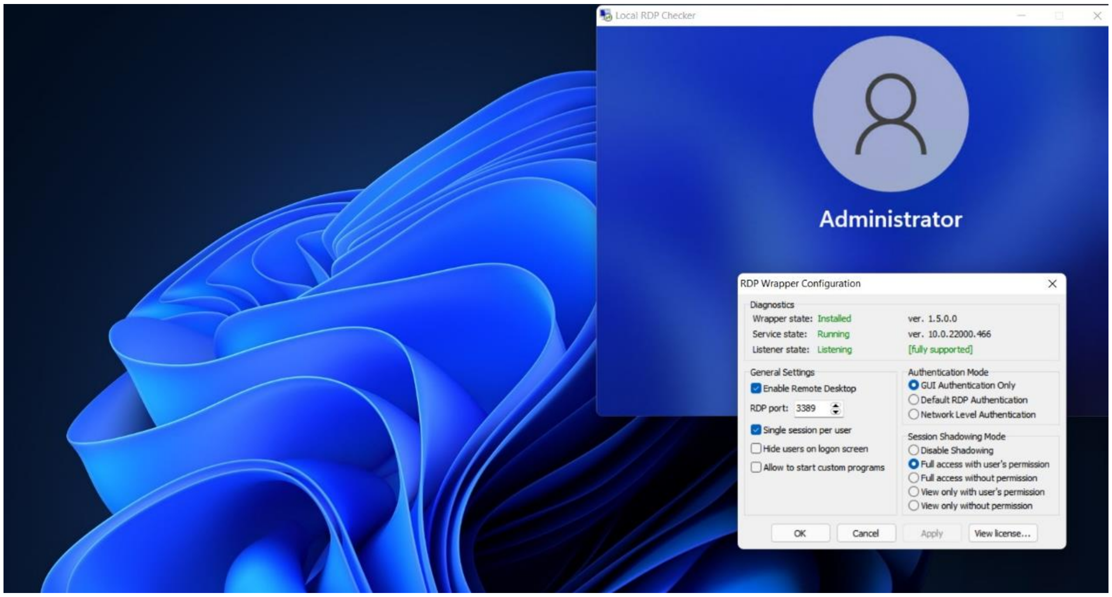
RDP PORT(3399):

If windows Pro then it can be turned on simply from Settings-> RDP Connection



Your Home edition of Windows 11 doesn't support Remote Desktop.

Else we need to install [Releases · stascorp/rdpwrap (github.com)](https://github.com/stascorp/rdpwrap/releases) for Windows Home



RDP Wrapper Configuration

Diagnostics

Wrapper state: Installed ver. 1.5.0.0

Service state: Running ver. 10.0.22000.466

Listener state: Listening [fully supported]

General Settings

☑ Enable Remote Desktop

RDP port: 3389

☑ Single session per user

☐ Hide users on logon screen

☐ Allow to start custom programs

Authentication Mode

● GUI Authentication Only

○ Default RDP Authentication

○ Network Level Authentication

Session Shadowing Mode

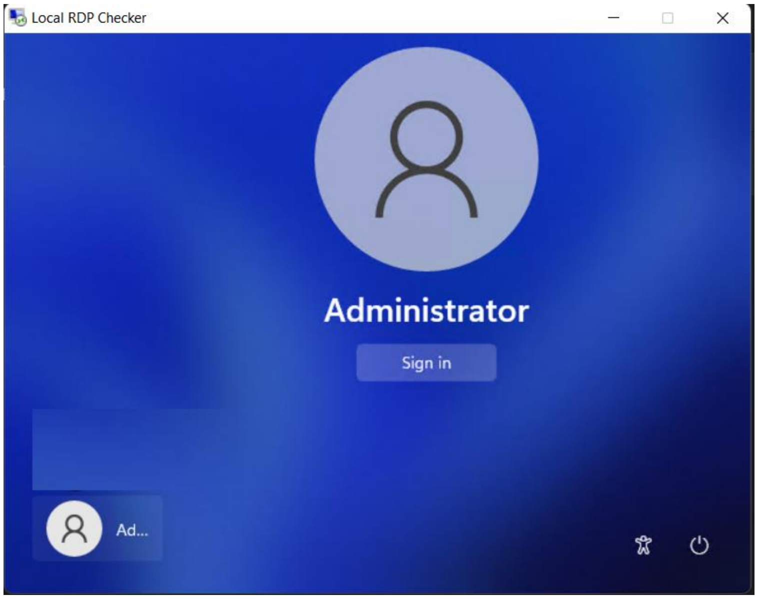
○ Disable Shadowing

● Full access with user's permission

○ Full access without permission

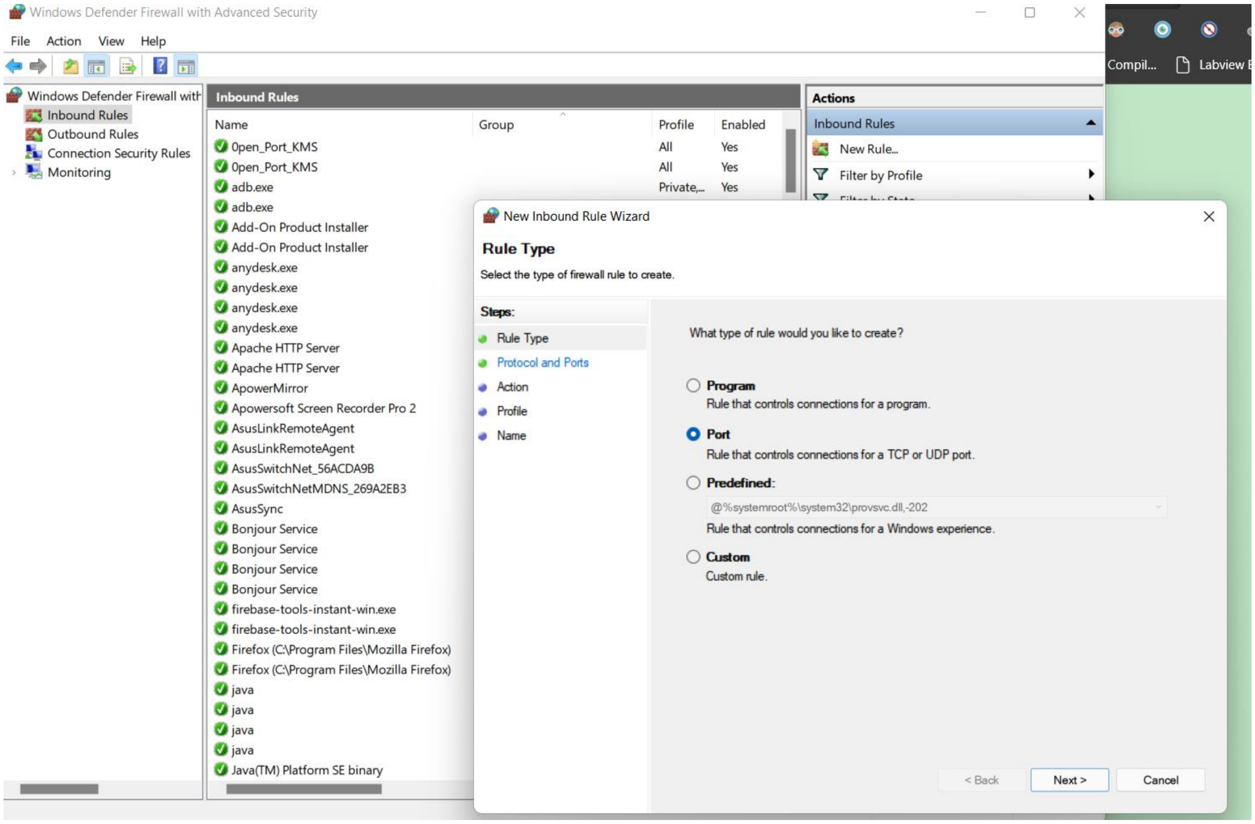
○ View only with user's permission

○ View only without permission



RDP: If its Kali linux we can use xrdp to setup RDP

New ports: using firewall and clicking new on inbound rules



Inbound Rules

Name	Group	Profile	Enabled
✓ 0pen_Port_KMS		All	Yes
✓ 0pen_Port_KMS		All	Yes
✓ adb.exe		Private,...	Yes
✓ adb.exe			
✓ Add-On Product Installer			
✓ Add-On Product Installer			
✓ anydesk.exe			
✓ anydesk.exe			
✓ anydesk.exe			
✓ anydesk.exe			
✓ Apache HTTP Server			
✓ Apache HTTP Server			
✓ ApowerMirror			
✓ Apowersoft Screen Recorder Pro 2			
✓ AsusLinkRemoteAgent			
✓ AsusLinkRemoteAgent			
✓ AsusSwitchNet_56ACDA9B			
✓ AsusSwitchNetMDNS_269A2EB3			
✓ AsusSync			
✓ Bonjour Service			
✓ Bonjour Service			
✓ Bonjour Service			
✓ Bonjour Service			
✓ firebase-tools-instant-win.exe			
✓ firebase-tools-instant-win.exe			
✓ Firefox (C:\Program Files\Mozilla Firefox)			
✓ Firefox (C:\Program Files\Mozilla Firefox)			
✓ java			
✓ java			
✓ java			
✓ java			
✓ Java(TM) Platform SE binary			

New Inbound Rule Wizard

Rule Type

Select the type of firewall rule to create.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

What type of rule would you like to create?

○ **Program**
Rule that controls connections for a program.

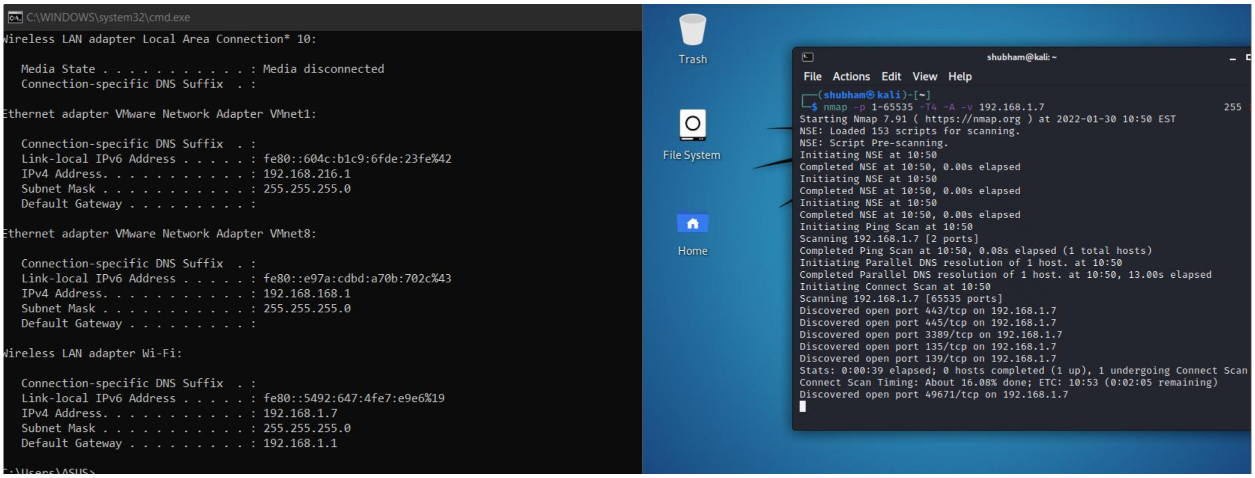
● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
@%systemroot%\system32\provsvc.dll,-202
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

< Back | Next > | Cancel

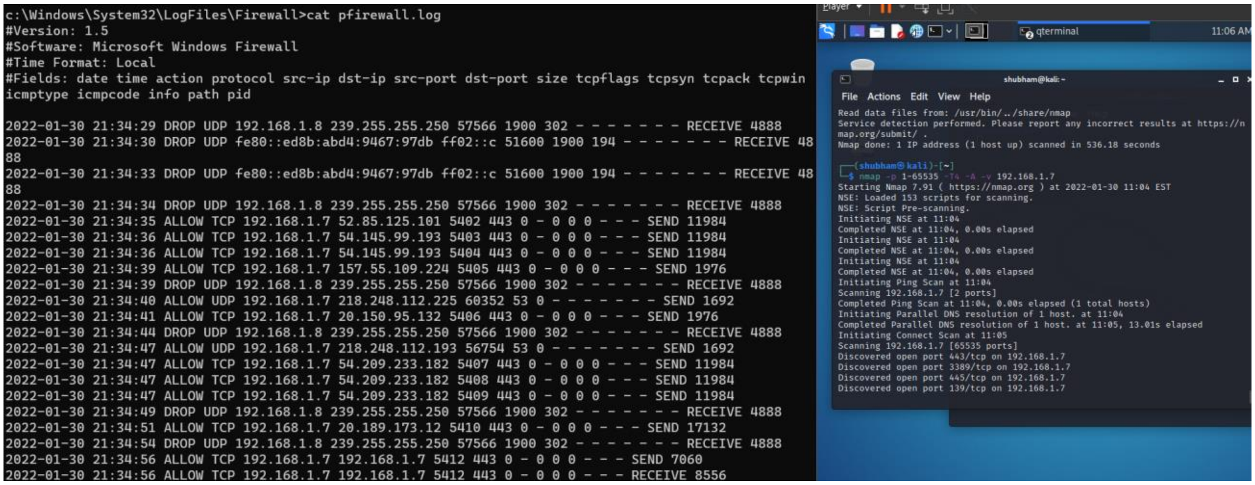
13) Nmap to scan ports on Windows VM



```
Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter VMware Network Adapter VMnet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::604c:b1c9:6fde:23fe%42
   IPv4 Address. . . . . . . . . . . : 192.168.216.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter VMware Network Adapter VMnet8:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::e97a:cdbd:a70b:702c%43
   IPv4 Address. . . . . . . . . . . : 192.168.168.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::5492:647:4fe7:e9e6%19
   IPv4 Address. . . . . . . . . . . : 192.168.1.7
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

C:\Users\ASUS>
```

```
┌──(shubham㉿kali)-[~]
└─$ nmap -p 1-65535 -T4 -A -v 192.168.1.7                                255
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-30 10:50 EST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:50
Completed NSE at 10:50, 0.00s elapsed
Initiating NSE at 10:50
Completed NSE at 10:50, 0.00s elapsed
Initiating NSE at 10:50
Completed NSE at 10:50, 0.00s elapsed
Initiating Ping Scan at 10:50
Scanning 192.168.1.7 [2 ports]
Completed Ping Scan at 10:50, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:50
Completed Parallel DNS resolution of 1 host. at 10:50, 13.00s elapsed
Initiating Connect Scan at 10:50
Scanning 192.168.1.7 [65535 ports]
Discovered open port 443/tcp on 192.168.1.7
Discovered open port 445/tcp on 192.168.1.7
Discovered open port 3389/tcp on 192.168.1.7
Discovered open port 135/tcp on 192.168.1.7
Discovered open port 139/tcp on 192.168.1.7
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 16.08% done; ETC: 10:53 (0:02:05 remaining)
Discovered open port 49671/tcp on 192.168.1.7
```

14) Firewall logs port scan shows Received Packets

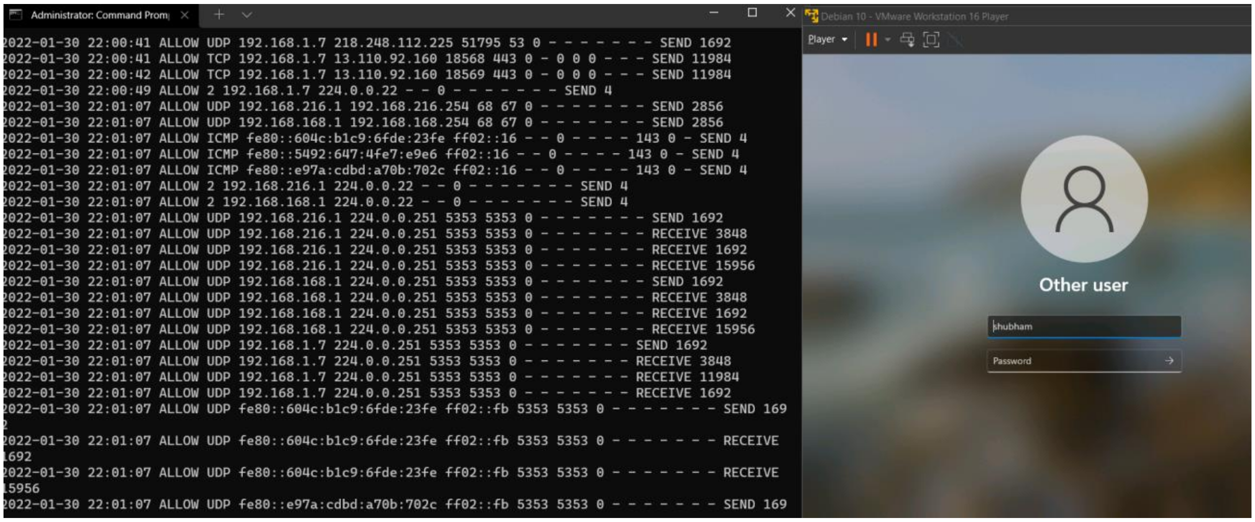


```
c:\Windows\System32\LogFiles\Firewall>cat pfirewall.log
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin
icmptype icmpcode info path pid

2022-01-30 21:34:29 DROP UDP 192.168.1.8 239.255.255.250 57566 1900 302 - - - - - - - RECEIVE 4888
2022-01-30 21:34:30 DROP UDP fe80::ed8b:abd4:9467:97db ff02::c 51600 1900 194 - - - - - - - RECEIVE 48
88
2022-01-30 21:34:33 DROP UDP fe80::ed8b:abd4:9467:97db ff02::c 51600 1900 194 - - - - - - - RECEIVE 48
88
2022-01-30 21:34:34 DROP UDP 192.168.1.8 239.255.255.250 57566 1900 302 - - - - - - - RECEIVE 4888
2022-01-30 21:34:35 ALLOW TCP 192.168.1.7 52.85.125.101 5402 443 0 - 0 0 0 - - - SEND 11984
2022-01-30 21:34:36 ALLOW TCP 192.168.1.7 54.145.99.193 5403 443 0 - 0 0 0 - - - SEND 11984
2022-01-30 21:34:36 ALLOW TCP 192.168.1.7 54.145.99.193 5404 443 0 - 0 0 0 - - - SEND 11984
2022-01-30 21:34:39 ALLOW TCP 192.168.1.7 157.55.109.224 5405 443 0 - 0 0 0 - - - SEND 1976
2022-01-30 21:34:39 DROP UDP 192.168.1.8 239.255.255.250 57566 1900 302 - - - - - - - RECEIVE 4888
2022-01-30 21:34:40 ALLOW UDP 192.168.1.7 218.248.112.225 60352 53 0 - - - - - - - SEND 1692
2022-01-30 21:34:41 ALLOW TCP 192.168.1.7 20.150.95.132 5406 443 0 - 0 0 0 - - - SEND 1976
2022-01-30 21:34:44 DROP UDP 192.168.1.8 239.255.255.250 57566 1900 302 - - - - - - - RECEIVE 4888
2022-01-30 21:34:47 ALLOW UDP 192.168.1.7 218.248.112.193 56754 53 0 - - - - - - - SEND 1692
2022-01-30 21:34:47 ALLOW TCP 192.168.1.7 54.209.233.182 5407 443 0 - 0 0 0 - - - SEND 11984
2022-01-30 21:34:47 ALLOW TCP 192.168.1.7 54.209.233.182 5408 443 0 - 0 0 0 - - - SEND 11984
2022-01-30 21:34:47 ALLOW TCP 192.168.1.7 54.209.233.182 5409 443 0 - 0 0 0 - - - SEND 11984
2022-01-30 21:34:49 DROP UDP 192.168.1.8 239.255.255.250 57566 1900 302 - - - - - - - RECEIVE 4888
2022-01-30 21:34:51 ALLOW TCP 192.168.1.7 20.189.173.12 5410 443 0 - 0 0 0 - - - SEND 17132
2022-01-30 21:34:54 DROP UDP 192.168.1.8 239.255.255.250 57566 1900 302 - - - - - - - RECEIVE 4888
2022-01-30 21:34:56 ALLOW TCP 192.168.1.7 192.168.1.7 5412 443 0 - 0 0 0 - - - SEND 7060
2022-01-30 21:34:56 ALLOW TCP 192.168.1.7 192.168.1.7 5412 443 0 - 0 0 0 - - - RECEIVE 8556
```

```
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 536.18 seconds

┌──(shubham㉿kali)-[~]
└─$ nmap -p 1-65535 -T4 -A -v 192.168.1.7
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-30 11:04 EST
NSE: Loaded 153 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:04
Completed NSE at 11:04, 0.00s elapsed
Initiating NSE at 11:04
Completed NSE at 11:04, 0.00s elapsed
Initiating NSE at 11:04
Completed NSE at 11:04, 0.00s elapsed
Initiating Ping Scan at 11:04
Scanning 192.168.1.7 [2 ports]
Completed Ping Scan at 11:04, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:04
Completed Parallel DNS resolution of 1 host. at 11:05, 13.01s elapsed
Initiating Connect Scan at 11:05
Scanning 192.168.1.7 [65535 ports]
Discovered open port 443/tcp on 192.168.1.7
Discovered open port 3389/tcp on 192.168.1.7
Discovered open port 445/tcp on 192.168.1.7
Discovered open port 139/tcp on 192.168.1.7
```

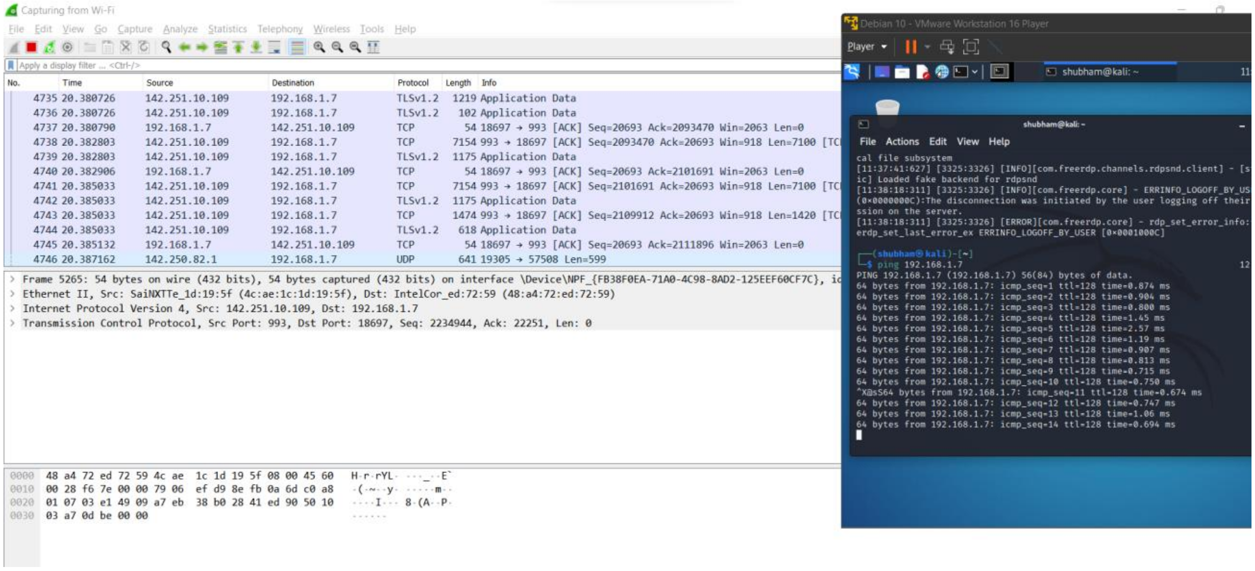
15) Firewall Logs Session connection

Using xfreerdp we can connect to windows VM from Kali VM


Administrator: Command Prom
Debian 10 - VMware Workstation 16 Player
Player
Other user
shubham
Password

```
2022-01-30 22:00:41 ALLOW UDP 192.168.1.7 218.248.112.225 51795 53 0 - - - - - - - SEND 1692
2022-01-30 22:00:41 ALLOW TCP 192.168.1.7 13.110.92.160 18568 443 0 - 0 0 0 - - - SEND 11984
2022-01-30 22:00:42 ALLOW TCP 192.168.1.7 13.110.92.160 18569 443 0 - 0 0 0 - - - SEND 11984
2022-01-30 22:00:49 ALLOW 2 192.168.1.7 224.0.0.22 - - 0 - - - - - - - SEND 4
2022-01-30 22:01:07 ALLOW UDP 192.168.216.1 192.168.216.254 68 67 0 - - - - - - - SEND 2856
2022-01-30 22:01:07 ALLOW UDP 192.168.168.1 192.168.168.254 68 67 0 - - - - - - - SEND 2856
2022-01-30 22:01:07 ALLOW ICMP fe80::604c:b1c9:6fde:23fe ff02::16 - - 0 - - - - 143 0 - SEND 4
2022-01-30 22:01:07 ALLOW ICMP fe80::5492:647:4fe7:e9e6 ff02::16 - - 0 - - - - 143 0 - SEND 4
2022-01-30 22:01:07 ALLOW ICMP fe80::e97a:cdbd:a70b:702c ff02::16 - - 0 - - - - 143 0 - SEND 4
2022-01-30 22:01:07 ALLOW 2 192.168.216.1 224.0.0.22 - - 0 - - - - - - - SEND 4
2022-01-30 22:01:07 ALLOW 2 192.168.168.1 224.0.0.22 - - 0 - - - - - - - SEND 4
2022-01-30 22:01:07 ALLOW UDP 192.168.216.1 224.0.0.251 5353 5353 0 - - - - - - - SEND 1692
2022-01-30 22:01:07 ALLOW UDP 192.168.216.1 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 3848
2022-01-30 22:01:07 ALLOW UDP 192.168.216.1 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 1692
2022-01-30 22:01:07 ALLOW UDP 192.168.216.1 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 15956
2022-01-30 22:01:07 ALLOW UDP 192.168.168.1 224.0.0.251 5353 5353 0 - - - - - - - SEND 1692
2022-01-30 22:01:07 ALLOW UDP 192.168.168.1 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 3848
2022-01-30 22:01:07 ALLOW UDP 192.168.168.1 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 1692
2022-01-30 22:01:07 ALLOW UDP 192.168.168.1 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 15956
2022-01-30 22:01:07 ALLOW UDP 192.168.1.7 224.0.0.251 5353 5353 0 - - - - - - - SEND 1692
2022-01-30 22:01:07 ALLOW UDP 192.168.1.7 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 3848
2022-01-30 22:01:07 ALLOW UDP 192.168.1.7 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 11984
2022-01-30 22:01:07 ALLOW UDP 192.168.1.7 224.0.0.251 5353 5353 0 - - - - - - - RECEIVE 1692
2022-01-30 22:01:07 ALLOW UDP fe80::604c:b1c9:6fde:23fe ff02::fb 5353 5353 0 - - - - - - - SEND 169
2
2022-01-30 22:01:07 ALLOW UDP fe80::604c:b1c9:6fde:23fe ff02::fb 5353 5353 0 - - - - - - - RECEIVE
1692
2022-01-30 22:01:07 ALLOW UDP fe80::604c:b1c9:6fde:23fe ff02::fb 5353 5353 0 - - - - - - - RECEIVE
15956
2022-01-30 22:01:07 ALLOW UDP fe80::e97a:cdbd:a70b:702c ff02::fb 5353 5353 0 - - - - - - - SEND 169
```

16) Wireshark on windows VM


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source          Destination     Protocol Length Info
4735 20.380726   142.251.10.109  192.168.1.7     TLSv1.2  1219 Application Data
4736 20.380726   142.251.10.109  192.168.1.7     TLSv1.2   102 Application Data
4737 20.380790   192.168.1.7     142.251.10.109  TCP        54 18697 → 993 [ACK] Seq=20693 Ack=2093470 Win=2063 Len=0
4738 20.382803   142.251.10.109  192.168.1.7     TCP      7154 993 → 18697 [ACK] Seq=2093470 Ack=20693 Win=918 Len=7100 [TC
4739 20.382803   142.251.10.109  192.168.1.7     TLSv1.2  1175 Application Data
4740 20.382906   192.168.1.7     142.251.10.109  TCP        54 18697 → 993 [ACK] Seq=20693 Ack=2101691 Win=2063 Len=0
4741 20.385033   142.251.10.109  192.168.1.7     TCP      7154 993 → 18697 [ACK] Seq=2101691 Ack=20693 Win=918 Len=7100 [TC
4742 20.385033   142.251.10.109  192.168.1.7     TLSv1.2  1175 Application Data
4743 20.385033   142.251.10.109  192.168.1.7     TCP      1474 993 → 18697 [ACK] Seq=2109912 Ack=20693 Win=918 Len=1420 [TC
4744 20.385033   142.251.10.109  192.168.1.7     TLSv1.2   618 Application Data
4745 20.385132   192.168.1.7     142.251.10.109  TCP        54 18697 → 993 [ACK] Seq=20693 Ack=2111896 Win=2063 Len=0
4746 20.387162   142.250.82.1    192.168.1.7     UDP       641 19305 → 57508 Len=599
```

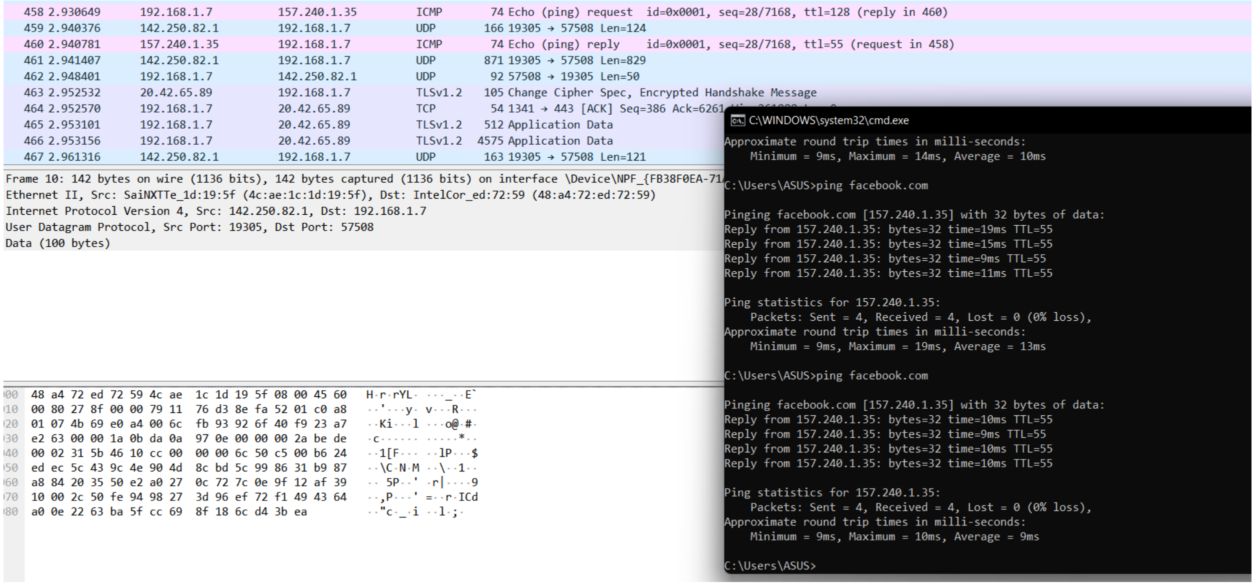
```
> Frame 5265: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{FB38F0EA-71A0-4C98-8AD2-125EEF60CF7C}, id
> Ethernet II, Src: SaiNXTTe_1d:19:5f (4c:ae:1c:1d:19:5f), Dst: IntelCor_ed:72:59 (48:a4:72:ed:72:59)
> Internet Protocol Version 4, Src: 142.251.10.109, Dst: 192.168.1.7
> Transmission Control Protocol, Src Port: 993, Dst Port: 18697, Seq: 2234944, Ack: 22251, Len: 0
```

```
0000  48 a4 72 ed 72 59 4c ae  1c 1d 19 5f 08 00 45 60   H·r·rYL· ···_··E`
0010  00 28 f6 7e 00 00 79 06  ef d9 8e fb 0a 6d c0 a8   ·(·~··y· ·····m··
0020  01 07 03 e1 49 09 a7 eb  38 b0 28 41 ed 90 50 10   ····I··· 8·(A··P·
0030  03 a7 0d be 00 00                                  ······
```

Debian 10 - VMware Workstation 16 Player
Player
shubham@kali: ~
shubham@kali: ~
File Actions Edit View Help

```
cal file subsystem
[11:37:41:627] [3325:3326] [INFO][com.freerdp.channels.rdpsnd.client] - [s
ic] Loaded fake backend for rdpsnd
[11:38:18:311] [3325:3326] [INFO][com.freerdp.core] - ERRINFO_LOGOFF_BY_US
(0×0000000C):The disconnection was initiated by the user logging off their
ssion on the server.
[11:38:18:311] [3325:3326] [ERROR][com.freerdp.core] - rdp_set_error_info:
erdp_set_last_error_ex ERRINFO_LOGOFF_BY_USER [0×0001000C]

┌──(shubham㉿kali)-[~]
└─$ ping 192.168.1.7
PING 192.168.1.7 (192.168.1.7) 56(84) bytes of data.
64 bytes from 192.168.1.7: icmp_seq=1 ttl=128 time=0.874 ms
64 bytes from 192.168.1.7: icmp_seq=2 ttl=128 time=0.904 ms
64 bytes from 192.168.1.7: icmp_seq=3 ttl=128 time=0.800 ms
64 bytes from 192.168.1.7: icmp_seq=4 ttl=128 time=1.45 ms
64 bytes from 192.168.1.7: icmp_seq=5 ttl=128 time=2.57 ms
64 bytes from 192.168.1.7: icmp_seq=6 ttl=128 time=1.19 ms
64 bytes from 192.168.1.7: icmp_seq=7 ttl=128 time=0.907 ms
64 bytes from 192.168.1.7: icmp_seq=8 ttl=128 time=0.813 ms
64 bytes from 192.168.1.7: icmp_seq=9 ttl=128 time=0.715 ms
64 bytes from 192.168.1.7: icmp_seq=10 ttl=128 time=0.750 ms
^X@sS64 bytes from 192.168.1.7: icmp_seq=11 ttl=128 time=0.674 ms
64 bytes from 192.168.1.7: icmp_seq=12 ttl=128 time=0.747 ms
64 bytes from 192.168.1.7: icmp_seq=13 ttl=128 time=1.06 ms
64 bytes from 192.168.1.7: icmp_seq=14 ttl=128 time=0.694 ms
```

17) PING Wireshark



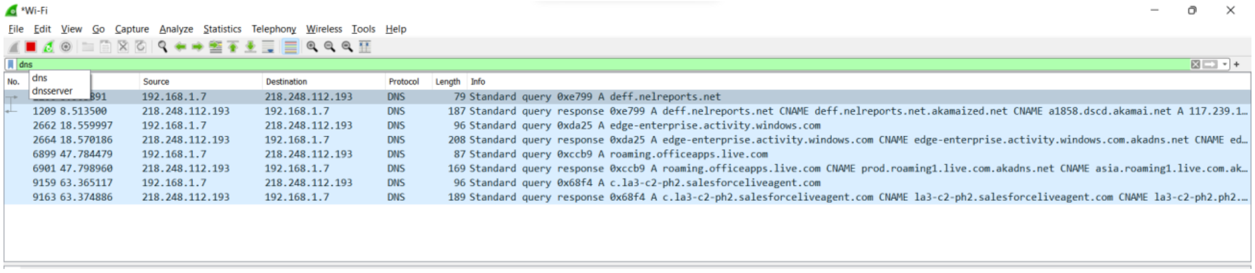
```
458 2.930649   192.168.1.7    157.240.1.35   ICMP      74 Echo (ping) request  id=0x0001, seq=28/7168, ttl=128 (reply in 460)
459 2.940376   142.250.82.1   192.168.1.7    UDP      166 19305 → 57508 Len=124
460 2.940781   157.240.1.35   192.168.1.7    ICMP      74 Echo (ping) reply    id=0x0001, seq=28/7168, ttl=55 (request in 458)
461 2.941407   142.250.82.1   192.168.1.7    UDP      871 19305 → 57508 Len=829
462 2.948401   192.168.1.7    142.250.82.1   UDP       92 57508 → 19305 Len=50
463 2.952532   20.42.65.89    192.168.1.7    TLSv1.2  105 Change Cipher Spec, Encrypted Handshake Message
464 2.952570   192.168.1.7    20.42.65.89    TCP       54 1341 → 443 [ACK] Seq=386 Ack=6261
465 2.953101   192.168.1.7    20.42.65.89    TLSv1.2  512 Application Data
466 2.953156   192.168.1.7    20.42.65.89    TLSv1.2 4575 Application Data
467 2.961316   142.250.82.1   192.168.1.7    UDP      163 19305 → 57508 Len=121
```

```
Frame 10: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{FB38F0EA-71
Ethernet II, Src: SaiNXTTe_1d:19:5f (4c:ae:1c:1d:19:5f), Dst: IntelCor_ed:72:59 (48:a4:72:ed:72:59)
Internet Protocol Version 4, Src: 142.250.82.1, Dst: 192.168.1.7
User Datagram Protocol, Src Port: 19305, Dst Port: 57508
Data (100 bytes)
```

```
00  48 a4 72 ed 72 59 4c ae  1c 1d 19 5f 08 00 45 60   H·r·rYL· ···_··E`
10  00 80 27 8f 00 00 79 11  76 d3 8e fa 52 01 c0 a8   ··'···y· v···R···
20  01 07 4b 69 e0 a4 00 6c  fb 93 92 6f 40 f9 23 a7   ··Ki···l ···o@·#·
30  e2 63 00 00 1a 0b da 0a  97 0e 00 00 00 2a be de   ·c······ ·····*··
40  00 02 31 5b 46 10 cc 00  00 00 6c 50 c5 00 b6 24   ··1[F··· ··lP···$
50  ed ec 5c 43 9c 4e 90 4d  8c bd 5c 99 86 31 b9 87   ··\C·N·M ··\··1··
60  a8 84 20 35 50 e2 a0 27  0c 72 7c 0e 9f 12 af 39   ·· 5P··' ·r|····9
70  10 00 2c 50 fe 94 98 27  3d 96 ef 72 f1 49 43 64   ··,P···' =··r·ICd
80  a0 0e 22 63 ba 5f cc 69  8f 18 6c d4 3b ea         ··"c·_·i ··l·;·
```

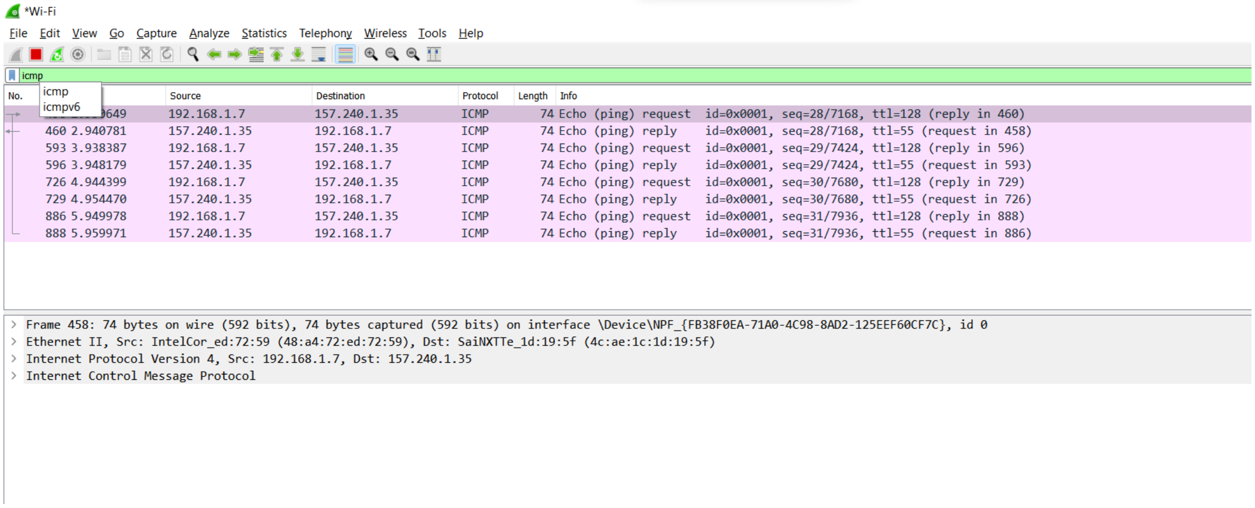
```
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 14ms, Average = 10ms

C:\Users\ASUS>ping facebook.com

Pinging facebook.com [157.240.1.35] with 32 bytes of data:
Reply from 157.240.1.35: bytes=32 time=19ms TTL=55
Reply from 157.240.1.35: bytes=32 time=15ms TTL=55
Reply from 157.240.1.35: bytes=32 time=9ms TTL=55
Reply from 157.240.1.35: bytes=32 time=11ms TTL=55

Ping statistics for 157.240.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 19ms, Average = 13ms

C:\Users\ASUS>ping facebook.com

Pinging facebook.com [157.240.1.35] with 32 bytes of data:
Reply from 157.240.1.35: bytes=32 time=10ms TTL=55
Reply from 157.240.1.35: bytes=32 time=9ms TTL=55
Reply from 157.240.1.35: bytes=32 time=10ms TTL=55
Reply from 157.240.1.35: bytes=32 time=10ms TTL=55

Ping statistics for 157.240.1.35:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 10ms, Average = 9ms

C:\Users\ASUS>
```

18) DNS


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver

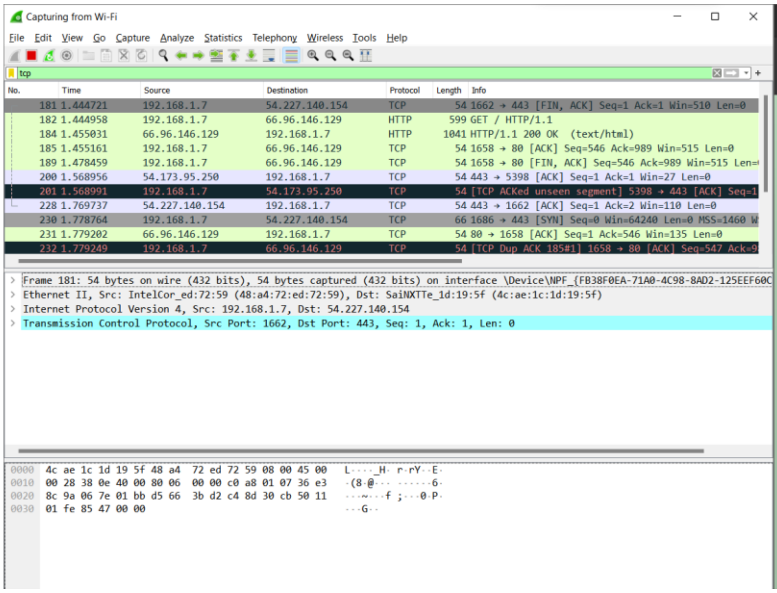
```
No.   Time        Source           Destination      Protocol Length Info
      …391        192.168.1.7      218.248.112.193  DNS       79 Standard query 0xe799 A deff.nelreports.net
1209  8.513500    218.248.112.193  192.168.1.7      DNS      187 Standard query response 0xe799 A deff.nelreports.net CNAME deff.nelreports.net.akamaized.net CNAME a1858.dscd.akamai.net A 117.239.1…
2662  18.559997   192.168.1.7      218.248.112.193  DNS       96 Standard query 0xda25 A edge-enterprise.activity.windows.com
2664  18.570186   218.248.112.193  192.168.1.7      DNS      208 Standard query response 0xda25 A edge-enterprise.activity.windows.com CNAME edge-enterprise.activity.windows.com.akadns.net CNAME ed…
6899  47.784479   192.168.1.7      218.248.112.193  DNS       87 Standard query 0xccb9 A roaming.officeapps.live.com
6901  47.798960   218.248.112.193  192.168.1.7      DNS      169 Standard query response 0xccb9 A roaming.officeapps.live.com CNAME prod.roaming1.live.com.akadns.net CNAME asia.roaming1.live.com.ak…
9159  63.365117   192.168.1.7      218.248.112.193  DNS       96 Standard query 0x68f4 A c.la3-c2-ph2.salesforceliveagent.com
9163  63.374886   218.248.112.193  192.168.1.7      DNS      189 Standard query response 0x68f4 A c.la3-c2-ph2.salesforceliveagent.com CNAME la3-c2-ph2.salesforceliveagent.com CNAME la3-c2-ph2.ph2…
```

19) ICMP

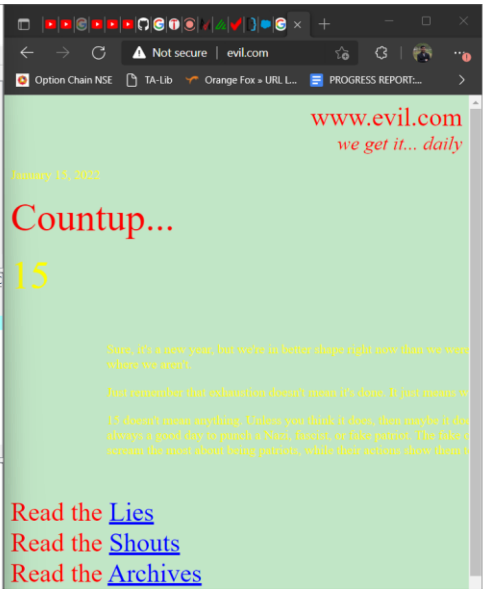

*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6

```
No.      Time         Source          Destination     Protocol  Length Info
      0649            192.168.1.7     157.240.1.35    ICMP          74 Echo (ping) request  id=0x0001, seq=28/7168, ttl=128 (reply in 460)
  460 2.940781        157.240.1.35    192.168.1.7     ICMP          74 Echo (ping) reply    id=0x0001, seq=28/7168, ttl=55 (request in 458)
  593 3.938387        192.168.1.7     157.240.1.35    ICMP          74 Echo (ping) request  id=0x0001, seq=29/7424, ttl=128 (reply in 596)
  596 3.948179        157.240.1.35    192.168.1.7     ICMP          74 Echo (ping) reply    id=0x0001, seq=29/7424, ttl=55 (request in 593)
  726 4.944399        192.168.1.7     157.240.1.35    ICMP          74 Echo (ping) request  id=0x0001, seq=30/7680, ttl=128 (reply in 729)
  729 4.954470        157.240.1.35    192.168.1.7     ICMP          74 Echo (ping) reply    id=0x0001, seq=30/7680, ttl=55 (request in 726)
  886 5.949978        192.168.1.7     157.240.1.35    ICMP          74 Echo (ping) request  id=0x0001, seq=31/7936, ttl=128 (reply in 888)
  888 5.959971        157.240.1.35    192.168.1.7     ICMP          74 Echo (ping) reply    id=0x0001, seq=31/7936, ttl=55 (request in 886)

> Frame 458: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{FB38F0EA-71A0-4C98-8AD2-125EEF60CF7C}, id 0
> Ethernet II, Src: IntelCor_ed:72:59 (48:a4:72:ed:72:59), Dst: SaiNXTTe_1d:19:5f (4c:ae:1c:1d:19:5f)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 157.240.1.35
> Internet Control Message Protocol
```

20) Website hello


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp

```
No.      Time        Source          Destination      Protocol  Length Info
  181 1.444721       192.168.1.7     54.227.140.154   TCP           54 1662 → 443 [FIN, ACK] Seq=1 Ack=1 Win=510 Len=0
  182 1.444958       192.168.1.7     66.96.146.129    HTTP         599 GET / HTTP/1.1
  184 1.455031       66.96.146.129   192.168.1.7      HTTP        1041 HTTP/1.1 200 OK  (text/html)
  185 1.455161       192.168.1.7     66.96.146.129    TCP           54 1658 → 80 [ACK] Seq=546 Ack=989 Win=515 Len=0
  189 1.478459       192.168.1.7     66.96.146.129    TCP           54 1658 → 80 [FIN, ACK] Seq=546 Ack=989 Win=515 Len=
  200 1.568956       54.173.95.250   192.168.1.7      TCP           54 443 → 5398 [ACK] Seq=1 Ack=1 Win=27 Len=0
  201 1.568991       192.168.1.7     54.173.95.250    TCP           54 [TCP ACKed unseen segment] 5398 → 443 [ACK] Seq=1
  228 1.769737       54.227.140.154  192.168.1.7      TCP           54 443 → 1662 [ACK] Seq=1 Ack=2 Win=110 Len=0
  230 1.778764       192.168.1.7     54.227.140.154   TCP           66 1686 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 W
  231 1.779202       66.96.146.129   192.168.1.7      TCP           54 80 → 1658 [ACK] Seq=1 Ack=546 Win=135 Len=0
  232 1.779249       192.168.1.7     66.96.146.129    TCP           54 [TCP Dup ACK 185#1] 1658 → 80 [ACK] Seq=547 Ack=9

> Frame 181: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{FB38F0EA-71A0-4C98-8AD2-125EEF60C
> Ethernet II, Src: IntelCor_ed:72:59 (48:a4:72:ed:72:59), Dst: SaiNXTTe_1d:19:5f (4c:ae:1c:1d:19:5f)
> Internet Protocol Version 4, Src: 192.168.1.7, Dst: 54.227.140.154
> Transmission Control Protocol, Src Port: 1662, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

0000  4c ae 1c 1d 19 5f 48 a4  72 ed 72 59 08 00 45 00   L····_H· r·rY··E·
0010  00 28 38 0e 40 00 80 06  00 00 c0 a8 01 07 36 e3   ·(8·@··· ······6·
0020  8c 9a 06 7e 01 bb d5 66  3b d2 c4 8d 30 cb 50 11   ···~···f ;···0·P·
0030  01 fe 85 47 00 00                                  ···G··
```



www.evil.com
we get it... daily

January 15, 2022

Countup...

15

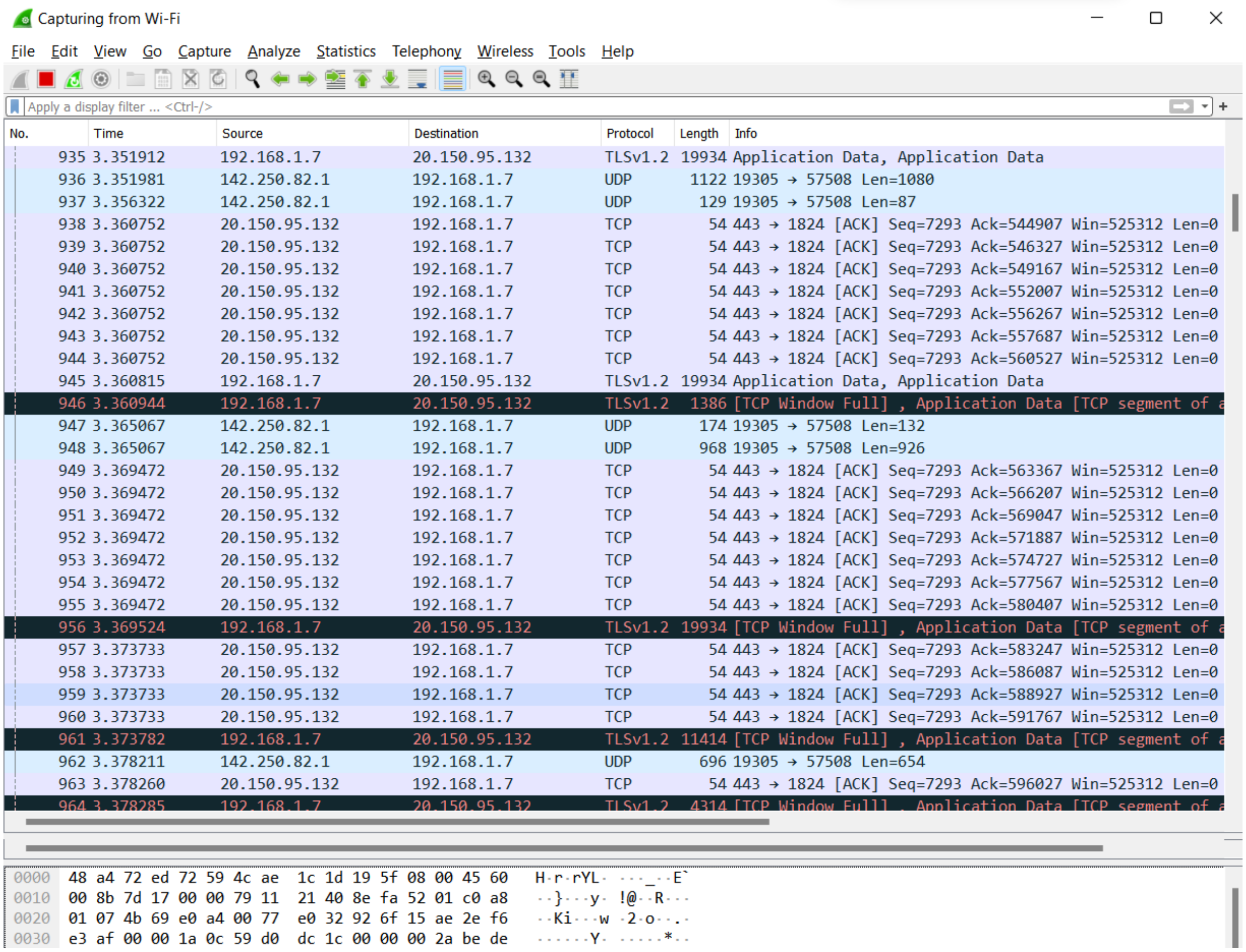
Sure, it's a new year, but we're in better shape right now than we were where we aren't.

Just remember that exhaustion doesn't mean it's done. It just means w

15 doesn't mean anything. Unless you think it does, then maybe it doe always a good day to punch a Nazi, fascist, or fake patriot. The fake c scream the most about being patriots, while their actions show them t

Read the Lies
Read the Shouts
Read the Archives

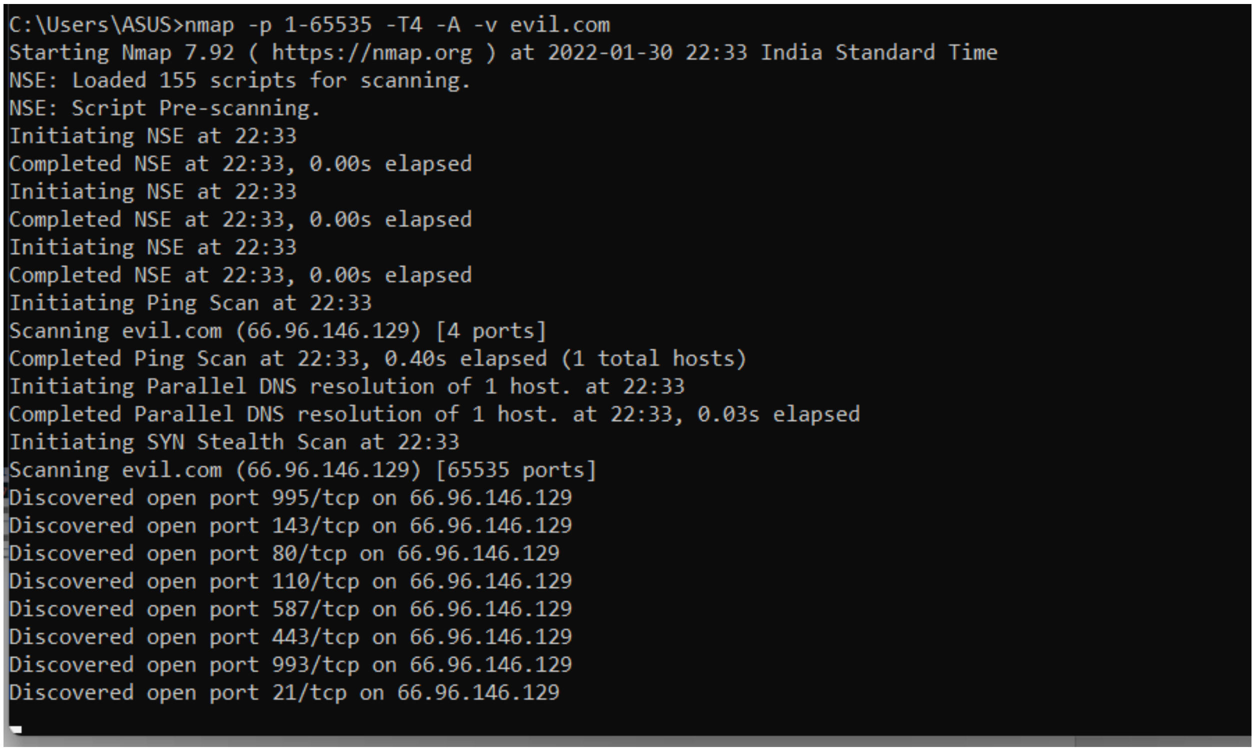
21) Website server ports shown in wireshark


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

```
No.    Time       Source          Destination     Protocol  Length Info
   935 3.351912   192.168.1.7     20.150.95.132   TLSv1.2  19934 Application Data, Application Data
   936 3.351981   142.250.82.1    192.168.1.7     UDP       1122 19305 → 57508 Len=1080
   937 3.356322   142.250.82.1    192.168.1.7     UDP        129 19305 → 57508 Len=87
   938 3.360752   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=544907 Win=525312 Len=0
   939 3.360752   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=546327 Win=525312 Len=0
   940 3.360752   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=549167 Win=525312 Len=0
   941 3.360752   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=552007 Win=525312 Len=0
   942 3.360752   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=556267 Win=525312 Len=0
   943 3.360752   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=557687 Win=525312 Len=0
   944 3.360752   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=560527 Win=525312 Len=0
   945 3.360815   192.168.1.7     20.150.95.132   TLSv1.2  19934 Application Data, Application Data
   946 3.360944   192.168.1.7     20.150.95.132   TLSv1.2   1386 [TCP Window Full] , Application Data [TCP segment of a
   947 3.365067   142.250.82.1    192.168.1.7     UDP        174 19305 → 57508 Len=132
   948 3.365067   142.250.82.1    192.168.1.7     UDP        968 19305 → 57508 Len=926
   949 3.369472   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=563367 Win=525312 Len=0
   950 3.369472   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=566207 Win=525312 Len=0
   951 3.369472   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=569047 Win=525312 Len=0
   952 3.369472   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=571887 Win=525312 Len=0
   953 3.369472   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=574727 Win=525312 Len=0
   954 3.369472   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=577567 Win=525312 Len=0
   955 3.369472   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=580407 Win=525312 Len=0
   956 3.369524   192.168.1.7     20.150.95.132   TLSv1.2  19934 [TCP Window Full] , Application Data [TCP segment of a
   957 3.373733   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=583247 Win=525312 Len=0
   958 3.373733   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=586087 Win=525312 Len=0
   959 3.373733   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=588927 Win=525312 Len=0
   960 3.373733   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=591767 Win=525312 Len=0
   961 3.373782   192.168.1.7     20.150.95.132   TLSv1.2  11414 [TCP Window Full] , Application Data [TCP segment of a
   962 3.378211   142.250.82.1    192.168.1.7     UDP        696 19305 → 57508 Len=654
   963 3.378260   20.150.95.132   192.168.1.7     TCP         54 443 → 1824 [ACK] Seq=7293 Ack=596027 Win=525312 Len=0
   964 3.378285   192.168.1.7     20.150.95.132   TLSv1.2   4314 [TCP Window Full] , Application Data [TCP segment of a
```

```
0000  48 a4 72 ed 72 59 4c ae  1c 1d 19 5f 08 00 45 60   H·r·rYL· ···_··E`
0010  00 8b 7d 17 00 00 79 11  21 40 8e fa 52 01 c0 a8   ··}···y· !@··R···
0020  01 07 4b 69 e0 a4 00 77  e0 32 92 6f 15 ae 2e f6   ··Ki···w ·2·o··.·
0030  e3 af 00 00 1a 0c 59 d0  dc 1c 00 00 00 2a be de   ······Y· ·····*··
```

Or using nmap



```
C:\Users\ASUS>nmap -p 1-65535 -T4 -A -v evil.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-30 22:33 India Standard Time
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
Initiating NSE at 22:33
Completed NSE at 22:33, 0.00s elapsed
Initiating Ping Scan at 22:33
Scanning evil.com (66.96.146.129) [4 ports]
Completed Ping Scan at 22:33, 0.40s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:33
Completed Parallel DNS resolution of 1 host. at 22:33, 0.03s elapsed
Initiating SYN Stealth Scan at 22:33
Scanning evil.com (66.96.146.129) [65535 ports]
Discovered open port 995/tcp on 66.96.146.129
Discovered open port 143/tcp on 66.96.146.129
Discovered open port 80/tcp on 66.96.146.129
Discovered open port 110/tcp on 66.96.146.129
Discovered open port 587/tcp on 66.96.146.129
Discovered open port 443/tcp on 66.96.146.129
Discovered open port 993/tcp on 66.96.146.129
Discovered open port 21/tcp on 66.96.146.129
```