

Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

Student:

Vidhi Kadakia

Email:

jinsukrishna108@gmail.com

Time on Task:

3 hours, 20 minutes

Progress:

100%

Report Generated: Sunday, November 30, 2025 at 4:16 PM

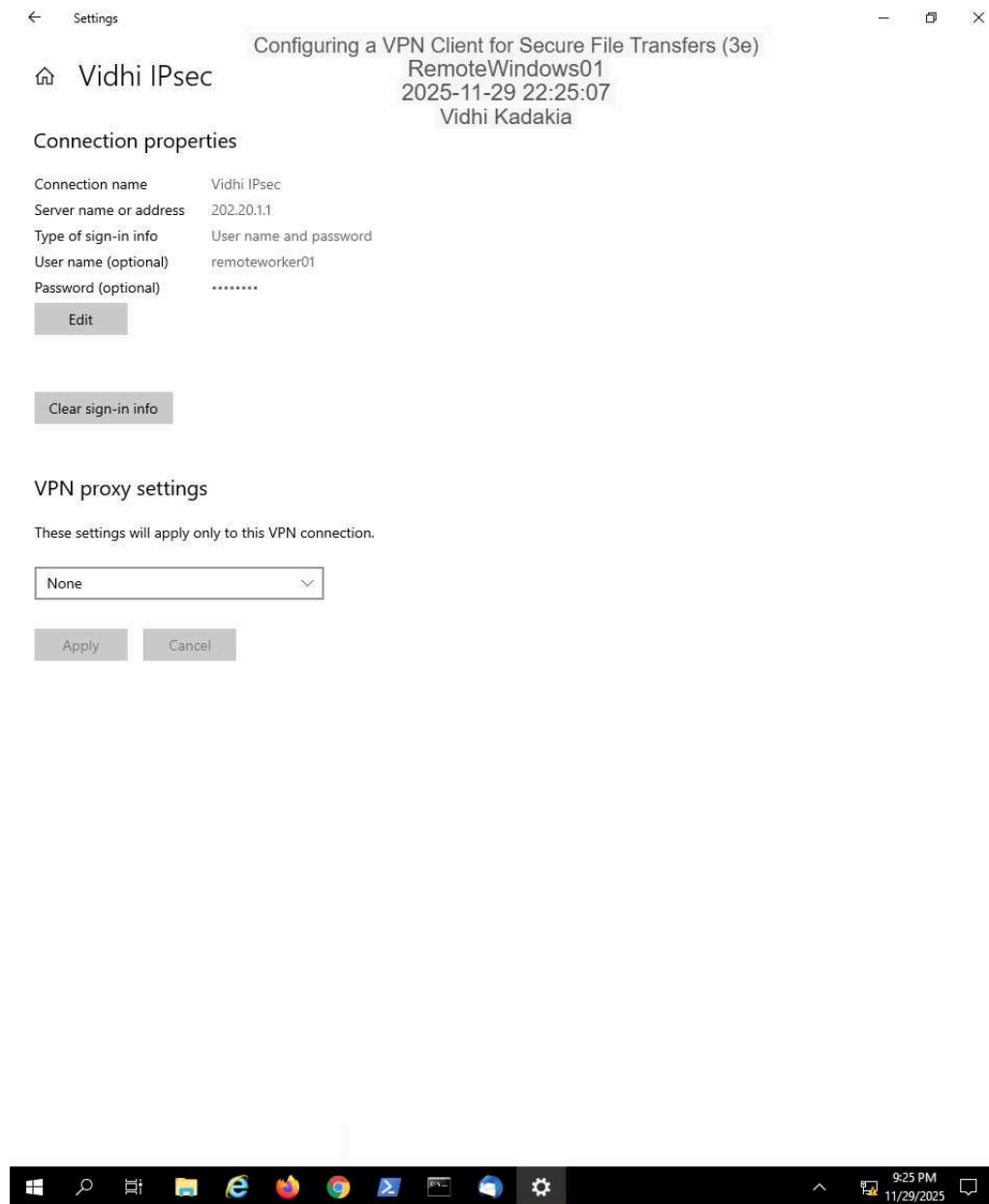
Section 1: Hands-On Demonstration

Part 1: Configure a Windows VPN Client

30. **Make a screen capture** showing the **VPN connection properties**.

Configuring a VPN Client for Secure File Transfers (3e)

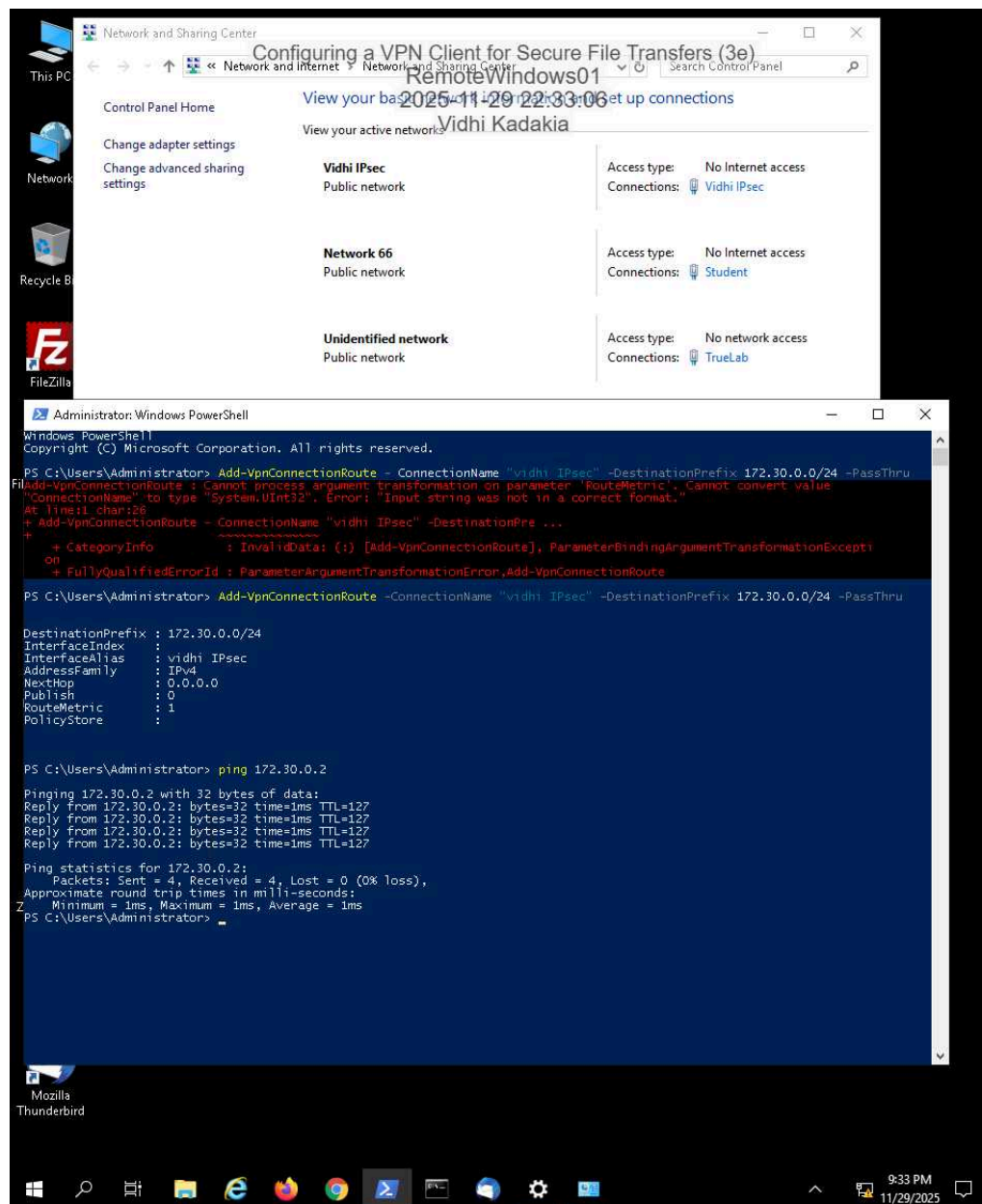
Network Security, Firewalls, and VPNs, Third Edition - Lab 09



54. Make a screen capture showing the successful ping response.

Configuring a VPN Client for Secure File Transfers (3e)

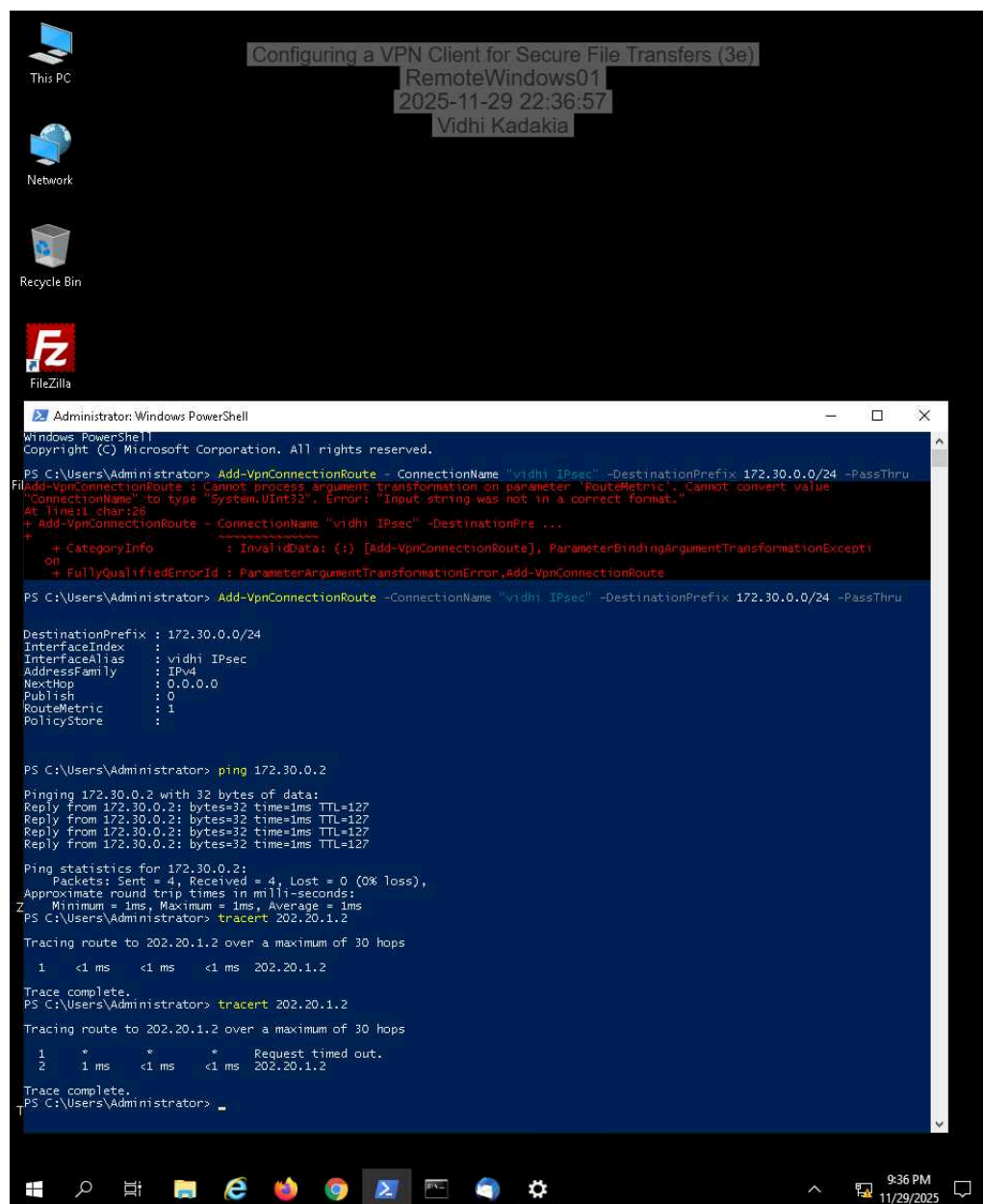
Network Security, Firewalls, and VPNs, Third Edition - Lab 09



72. Make a screen capture showing your new tracert results.

Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

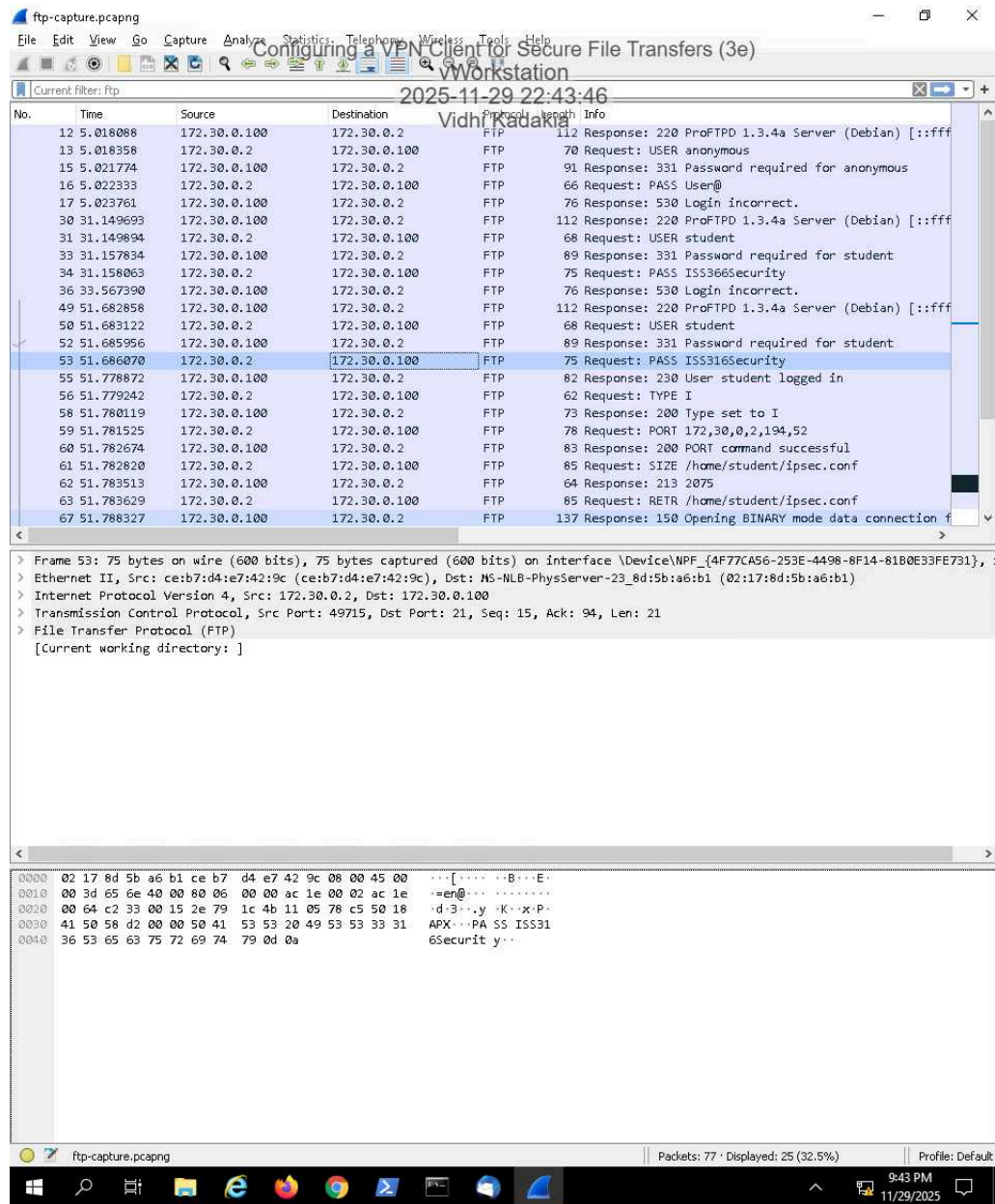


Part 2: Compare Secure and Non-Secure File Transfers in Wireshark

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

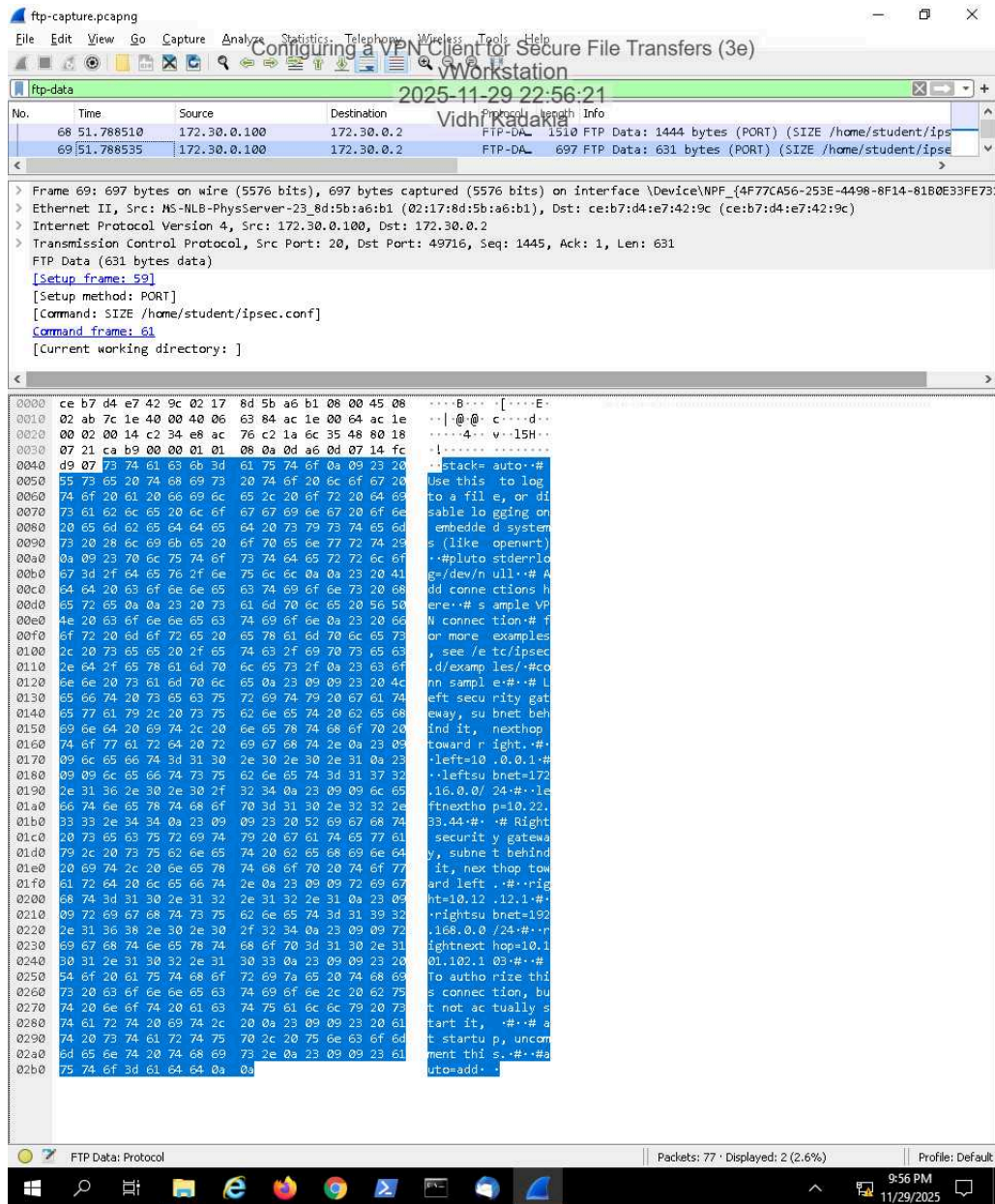
12. **Make a screen capture** showing the **packet that carries the correct password**.



Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

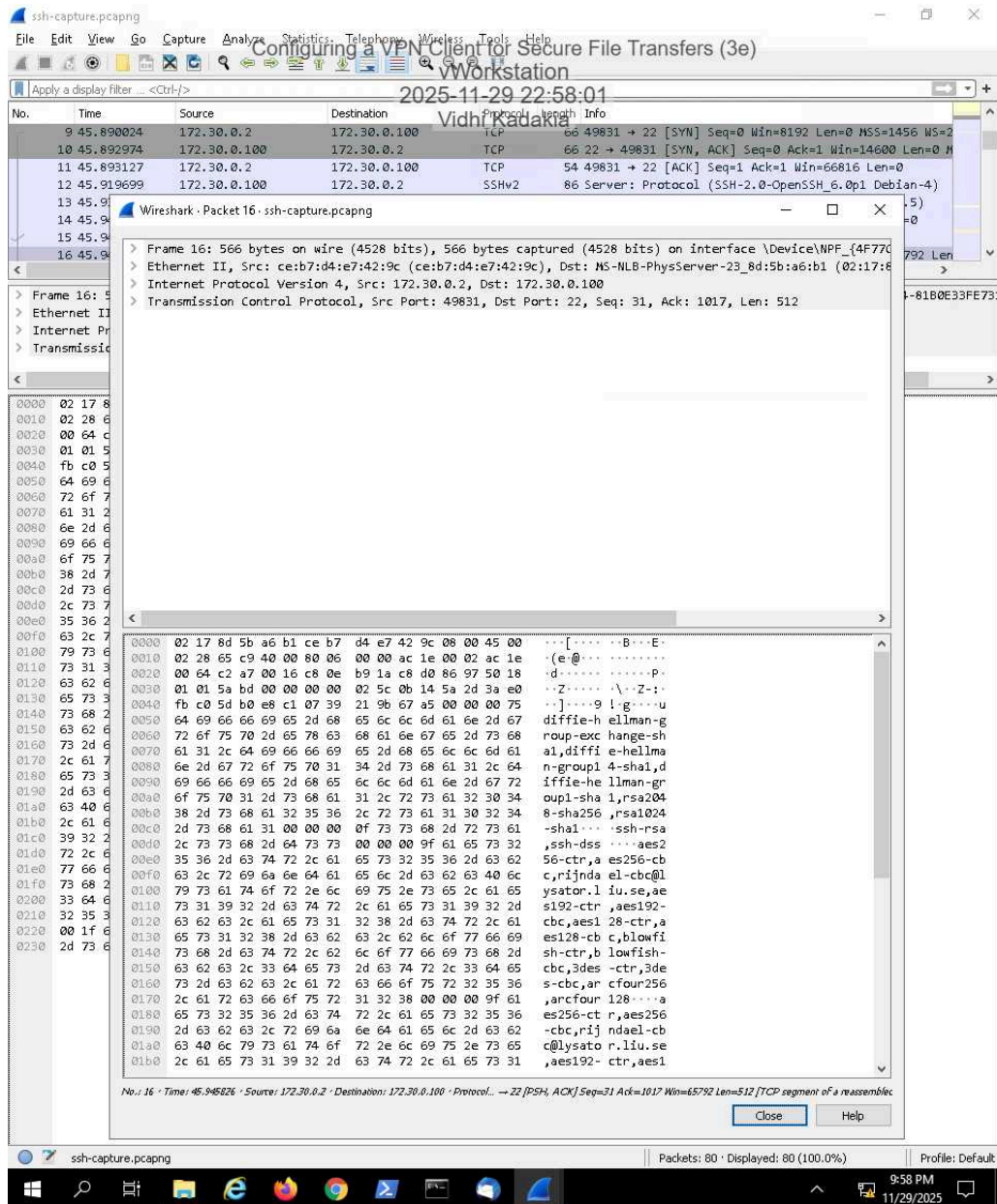
28. Make a screen capture showing the Wireshark window and the packet bytes pane for Packet 69.



Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

44. Make a screen capture showing the packet details pane for packet 16.



Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

49. Make a screen capture showing the last SSHv2 packet in the SSH file transfer.

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a packet capture titled "ssh-capture.pcapng". The packet list pane on the left shows a list of captured packets, with packet 79 selected. The packet details pane on the right shows the structure of packet 79, which is an SSHv2 packet. The packet bytes pane at the bottom shows the raw data of the selected packet in hexadecimal and ASCII.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
72	79.069299	172.30.0.2	172.30.0.100	SSHv2	122	Client: Encrypted packet (len=68)
73	79.070187	172.30.0.100	172.30.0.2	SSHv2	1510	Server: Encrypted packet (len=1456)
74	79.070211	172.30.0.100	172.30.0.2	SSHv2	730	Server: Encrypted packet (len=676)
76	79.073321	172.30.0.2	172.30.0.100	SSHv2	122	Client: Encrypted packet (len=68)
77	79.073880	172.30.0.100	172.30.0.2	SSHv2	138	Server: Encrypted packet (len=84)
78	79.075923	172.30.0.2	172.30.0.100	SSHv2	122	Client: Encrypted packet (len=68)
79	79.076514	172.30.0.100	172.30.0.2	SSHv2	122	Server: Encrypted packet (len=68)

Packet Details (Frame 79):

- Frame 79: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface \Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731}.
- Ethernet II, Src: NS-NLB-PhysServer-23_8d:5b:a6:b1 (02:17:8d:5b:a6:b1), Dst: ce:b7:d4:e7:42:9c (ce:b7:d4:e7:42:9c).
- Internet Protocol Version 4, Src: 172.30.0.100, Dst: 172.30.0.2.
- Transmission Control Protocol, Src Port: 22, Dst Port: 49831, Seq: 7493, Ack: 2699, Len: 68.
- SSH Protocol.

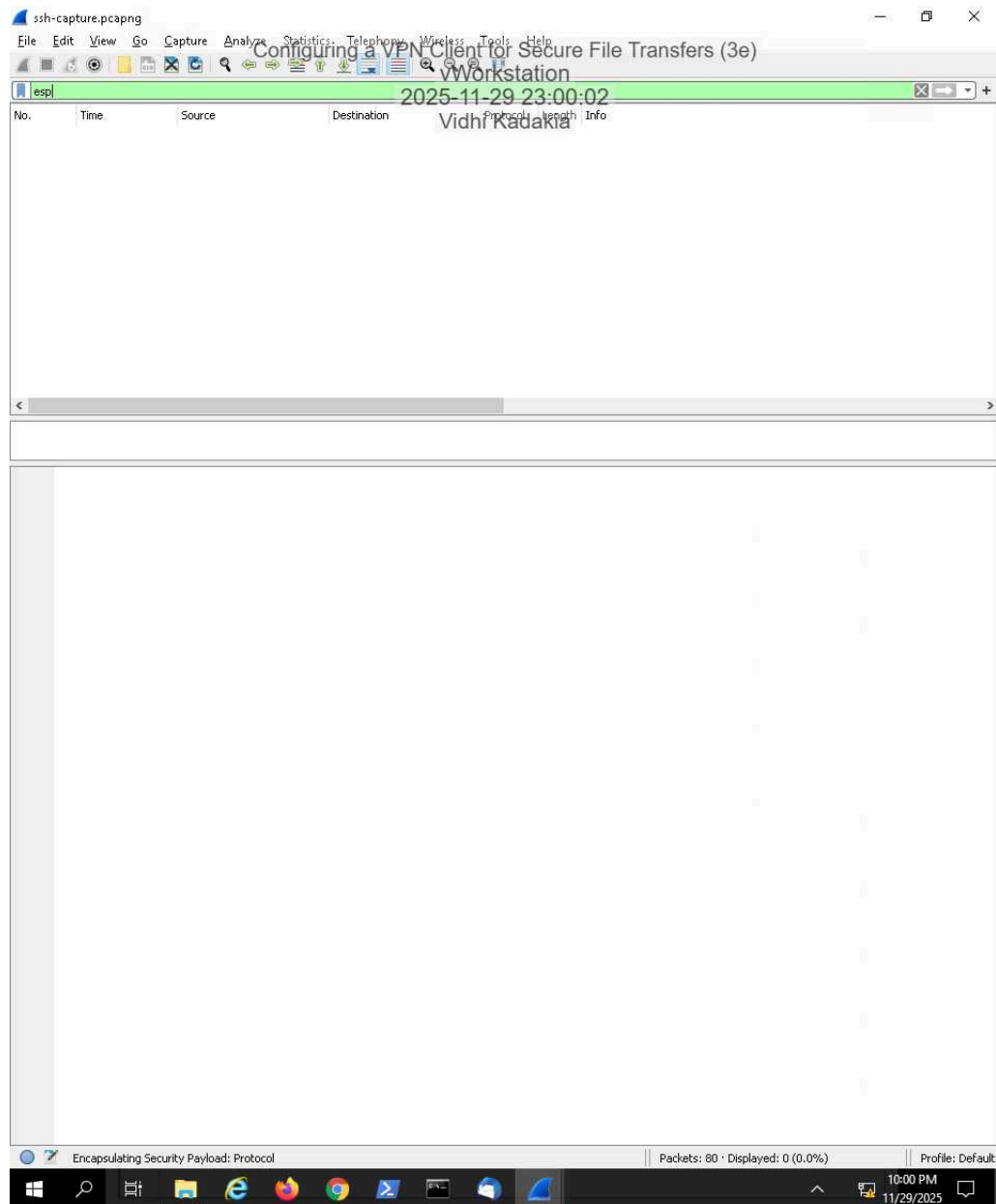
Packet Bytes:

```
0000  ce b7 d4 e7 42 9c 02 17 8d 5b a6 b1 08 00 45 08  ...B...[....E...
0010  00 6c c3 c9 40 00 40 06 1e 18 ac 1e 00 64 ac 1e  1..@...d...
0020  00 02 00 16 c2 a7 c8 d0 9f e3 c8 0e c3 86 50 18  ....P...
0030  08 b3 5f fa 00 00 88 48 12 81 ee c4 db 56 76 ba  ...H...Sv...
0040  e9 1d c7 9d fd a1 2e c8 9b 96 89 0d c3 33 bd 3e  ....3>...
0050  fd 1f 9c 0c 08 eb 96 87 0f 39 5a 0e 02 77 fe 64  ...9Z..w.d...
0060  c6 ad 74 38 c3 dc 25 96 9c 43 46 39 63 73 8a 98  ..t8..%..CF9cs...
0070  b2 9d 3a 20 85 1a 76 43 59 97  ...vC Y...
```


Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

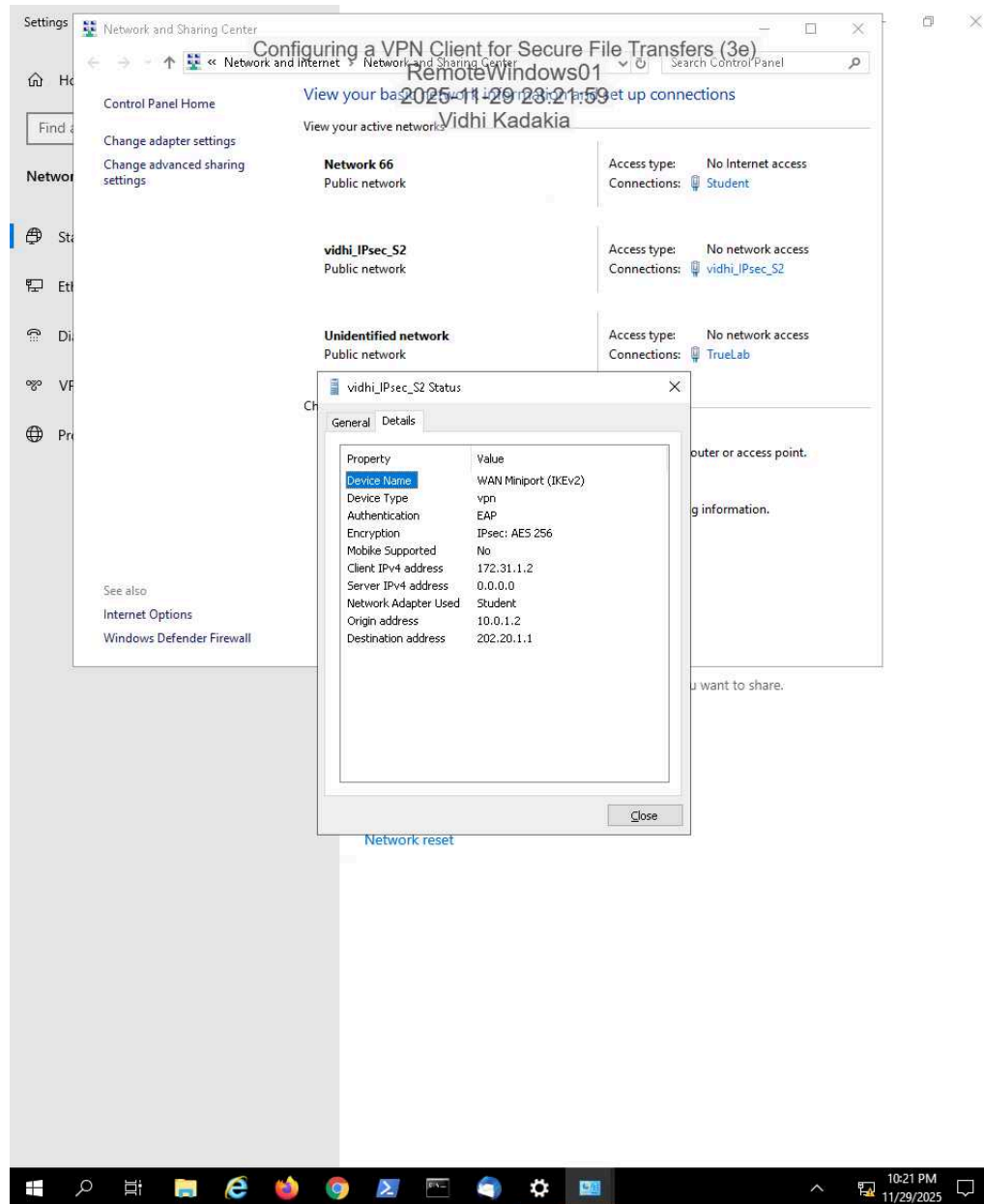
51. Make a screen capture showing the **last packets in the ESP exchange**.



Section 2: Applied Learning

Part 1: Configure a Windows VPN Client

19. Make a screen capture showing the IPsec VPN connection encrypted with AES 256.



23. **Make a screen capture** showing your **successful tracert** to the remote machine.



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt displays the following text:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> tracert 172.30.0.2

Tracing route to VWORKSTATION [172.30.0.2]
over a maximum of 30 hops:

  1  *      *      *      Request timed out.
  2  1 ms   <1 ms <1 ms VWORKSTATION [172.30.0.2]

Trace complete.
PS C:\Users\Administrator>
```

The window has a dark blue background. The taskbar at the bottom shows various application icons and the system clock indicating 10:22 PM on 11/29/2025.

Part 2: Compare Secure and Non-Secure File Transfers in Wireshark

Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

7. Make a screen capture showing the IKE_SA_INIT and IKE_AUTH packets.

The image shows a Windows desktop with a VMware Workstation window titled "Configuring a VPN Client for Secure File Transfers (3e)". Inside the VM, a Wireshark packet capture is displayed. The capture is filtered for "is:ikeip" and shows a list of 16 packets. The first packet (No. 2) is an IKE_SA_INIT Initiator Request from 10.0.1.2 to 202.20.1.1. The subsequent packets are IKE_SA_INIT Responder Responses and IKE_AUTH packets (Initiator Requests and Responder Responses) for various IKE_AUTH NIDs (01, 02, 03, 04, 05). The packet details pane shows the selected packet (No. 2) with its Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Internet Security Association and Key Management Protocol (ISAKMP) headers. The packet bytes pane shows the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Length	Info
2	9.065639	10.0.1.2	202.20.1.1	ISAKMP	674	IKE_SA_INIT MID=00 Initiator Request
3	9.083863	202.20.1.1	10.0.1.2	ISAKMP	523	IKE_SA_INIT MID=00 Responder Response
4	9.093750	10.0.1.2	202.20.1.1	ISAKMP	626	IKE_AUTH MID=01 Initiator Request (fragment 1/3)
5	9.093796	10.0.1.2	202.20.1.1	ISAKMP	626	IKE_AUTH MID=01 Initiator Request (fragment 2/3)
6	9.093812	10.0.1.2	202.20.1.1	ISAKMP	162	IKE_AUTH MID=01 Initiator Request (fragment 3/3)
7	9.099740	202.20.1.1	10.0.1.2	ISAKMP	1282	IKE_AUTH MID=01 Responder Response (fragment 1/2)
8	9.099775	202.20.1.1	10.0.1.2	ISAKMP	482	IKE_AUTH MID=01 Responder Response (fragment 2/2)
9	9.135283	10.0.1.2	202.20.1.1	ISAKMP	142	IKE_AUTH MID=02 Initiator Request
10	9.137369	202.20.1.1	10.0.1.2	ISAKMP	158	IKE_AUTH MID=02 Responder Response
11	9.138822	10.0.1.2	202.20.1.1	ISAKMP	190	IKE_AUTH MID=03 Initiator Request
12	9.140310	202.20.1.1	10.0.1.2	ISAKMP	190	IKE_AUTH MID=03 Responder Response
13	9.140661	10.0.1.2	202.20.1.1	ISAKMP	126	IKE_AUTH MID=04 Initiator Request
14	9.141637	202.20.1.1	10.0.1.2	ISAKMP	126	IKE_AUTH MID=04 Responder Response
15	9.149409	10.0.1.2	202.20.1.1	ISAKMP	158	IKE_AUTH MID=05 Initiator Request
16	9.156626	202.20.1.1	10.0.1.2	ISAKMP	302	IKE_AUTH MID=05 Responder Response

Frame 2: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits) on interface \Device\NPF_{D52CDBBA-4A0A-4ABA-981C-E72E7E6C6C6C} Ethernet II, Src: VMware_00:00:00:00:00:00 (00:50:56:ae:3d:7a), Dst: VMware_00:00:00:00:00:00 (00:50:56:ae:10:f1) Internet Protocol Version 4, Src: 10.0.1.2, Dst: 202.20.1.1 User Datagram Protocol, Src Port: 500, Dst Port: 500 Internet Security Association and Key Management Protocol

0000 00 50 56 ae 10 f1 00 50 56 ae 3d 7a 08 00 45 00 ..PV...P V...z...E...
0010 02 94 e6 70 00 00 80 11 7b d1 0a 00 01 02 ca 14 ...p...{...
0020 01 01 01 f4 01 f4 02 80 70 4f df a9 8b 8a 8c 5epO...^...
0030 c2 ad 80 00 00 00 00 00 00 00 21 20 22 08 00 001...
0040 00 00 00 02 78 22 00 00 88 02 00 00 2c 01 01x...
0050 00 03 00 00 0c 01 00 00 0c 0e 01 00 03 00
0060 00 06 03 00 00 02 03 00 06 02 00 00 02 00 00
0070 00 06 04 00 00 0e 02 00 2c 02 01 00 04 03 00
0080 00 0c 01 00 00 0c 60 0e 01 00 03 00 00 08 03 00
0090 00 0c 03 00 00 08 02 00 05 00 00 00 08 04 00
00a0 00 0e 00 00 00 2c 03 01 00 04 03 00 00 0c 01 00
00b0 00 0c 80 0e 01 00 03 00 00 08 03 00 00 0d 03 00
00c0 00 06 02 00 06 00 00 00 08 04 00 0e 28 00
00d0 01 08 00 0e 00 00 72 3c 95 cd 79 34 16 8f c5 d5<...y4...

Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

22. Make a screen capture showing the filtered FTP packets in your capture file.

The screenshot shows a Wireshark capture of FTP traffic. The packet list is filtered by 'ftp' and shows 36 packets. The selected packet (No. 36) is a response from 172.30.0.2 to 172.40.0.2. The packet details pane shows the raw data and hex representation of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
6	13.522568	172.40.0.20	172.30.0.2	FTP	78	Request: 230 VSFTPD 3.03 Server
7	13.527355	172.30.0.2	172.40.0.20	FTP	68	Response: 230 UTF8 ON
9	13.527777	172.40.0.20	172.30.0.2	FTP	80	Request: 200 Always in UTF8 mode.
12	17.641343	172.30.0.2	172.40.0.20	FTP	68	Request: USER student
14	17.642115	172.40.0.20	172.30.0.2	FTP	88	Response: 331 Please specify the password.
17	22.934081	172.30.0.2	172.40.0.20	FTP	68	Request: PASS student
19	22.957228	172.40.0.20	172.30.0.2	FTP	77	Response: 230 Login successful.
21	30.050056	172.30.0.2	172.40.0.20	FTP	77	Request: PORT 172,30,0,2,195,4
22	30.050895	172.40.0.20	172.30.0.2	FTP	105	Response: 200 PORT command successful. Consider using PASV.
23	30.060669	172.30.0.2	172.40.0.20	FTP	69	Request: RETR file.txt
27	30.061968	172.40.0.20	172.30.0.2	FTP	120	Response: 150 Opening BINARY mode data connection for file.txt (73 bytes).
31	30.064987	172.40.0.20	172.30.0.2	FTP	78	Response: 226 Transfer complete.
35	41.461501	172.30.0.2	172.40.0.20	FTP	60	Request: QUIT
36	41.462290	172.40.0.20	172.30.0.2	FTP	68	Response: 221 Goodbye.

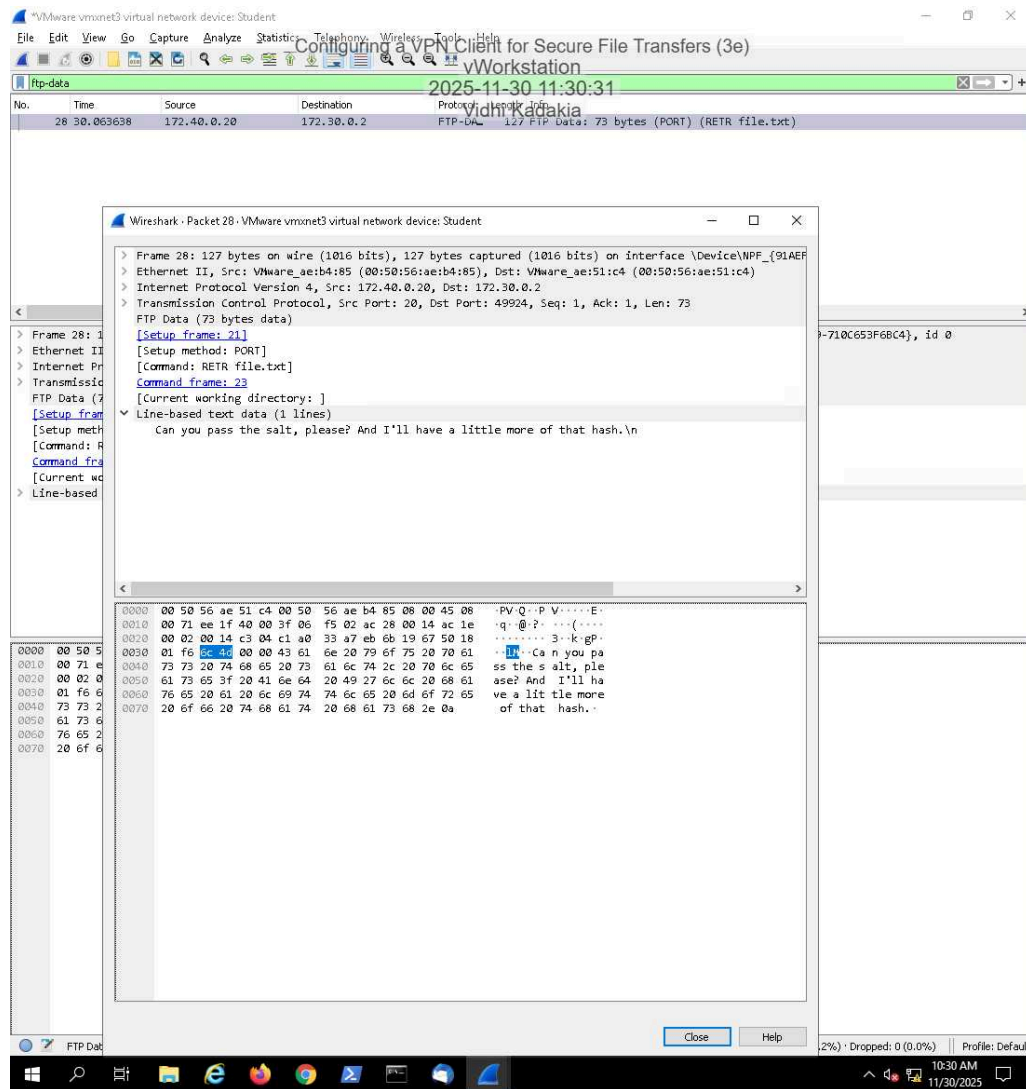
Frame 36: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface \Device\NPF{91AEFD1F-6258-4122-8A69-710C653F6BC4}, id 0

0000 00 50 56 ae 51 c4 00 50 56 ae b4 85 08 00 45 00 -PV Q P V.....E
0010 00 36 4e 9c 40 00 3f 05 94 c9 ac 28 00 14 ac 1e -6N @ ? - - - (- - -
0020 00 02 00 15 c2 f8 76 18 37 0b eb fa ab 5c 50 18 - - - - - v - 7 - - - - \ P -
0030 01 f6 5f 0b 00 00 32 32 31 20 47 6f 6f 64 62 79 - - - - - 22 1 Goodbye
0040 65 2e 0d 0a e . . .

Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

24. Make a screen capture showing the contents of the file.txt file in the packet bytes pane.



Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

27. Make a screen capture showing the filtered SSH packets in your capture file.

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, and Help. The title bar reads "Configuring a VPN Client for Secure File Transfers (3e)". The main window is titled "ssh" and shows a list of captured packets filtered for the SSH protocol. The list includes columns for No., Time, Source, Destination, Protocol, and Length. The packets are numbered 51 through 79, all originating from 172.40.0.2 and destined for 172.30.0.2. The protocols listed are SSHv2, and the lengths range from 64 to 1110 bytes. The packet list is expanded to show details for packet 55, which is an SSHv2 packet from 172.40.0.2 to 172.30.0.2. The details pane shows the following information:

- Frame 55: 1110 bytes on wire (8880 bits), 1110 bytes captured (8880 bits) on interface \Device\NPF_{91AEFD1F-6258-4122-8A69-710C653F6BC4}, id 0
- Ethernet II, Src: VMware_ae:b4:85 (00:50:56:ae:b4:85), Dst: VMware_ae:51:c4 (00:50:56:ae:51:c4)
- Destination: VMware_ae:51:c4 (00:50:56:ae:51:c4)
- Source: VMware_ae:b4:85 (00:50:56:ae:b4:85)
- Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 172.40.0.20, Dst: 172.30.0.2
- Transmission Control Protocol, Src Port: 22, Dst Port: 49965, Seq: 33, Ack: 1197, Len: 1056
- SSH Protocol
- SSH Version 2 (encryption:aes256-ctr mac: hmac-sha2-256 compression:none)
- [Direction: server-to-client]

The packet bytes pane at the bottom shows the raw data of the packet, including the SSHv2 protocol header and the encrypted payload. The status bar at the bottom indicates "Packets: 83 - Displayed: 19 (22.9%) - Dropped: 0 (0.0%) | Profile: Default".

Section 3: Challenge and Analysis

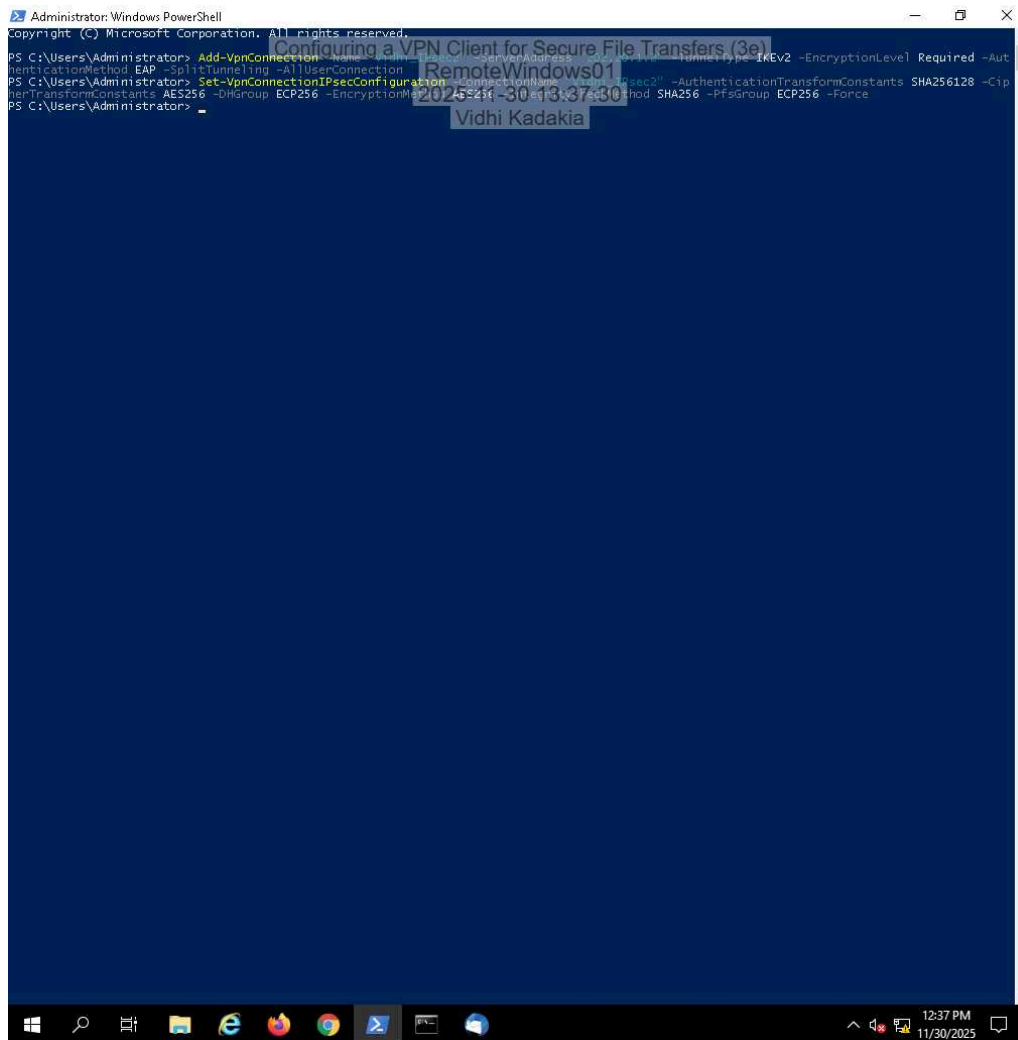
Part 1: Create a New VPN Connection using PowerShell

Document the command you used to add your VPN connection.

```
Add-VpnConnection -Name "Vidhi_IPsec2" -ServerAddress "202.20.1.2" -TunnelType IKEv2  
-EncryptionLevel Required -AuthenticationMethod EAP -SplitTunneling -AllUserConnection
```

Part 2: Implement a Custom IPsec Policy

Make a screen capture showing the successfully executed `Set-VpnConnectionIPsecConfiguration` command in PowerShell.



Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

Part 3: Verify Your VPN Implementation using Wireshark

Make a screen capture showing the **CREATE_CHILD_SA** exchange.

VMware vmxnet3 virtual network device: Student

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Configuring a VPN Client for Secure File Transfers (3e)

RemoteWindows01

2025-11-30 14:05:54

Vidhi Kadakia

No.	isakmp	Source	Destination	Protocol	Length	Info
3	0.650241	202.20.1.1	10.0.1.2	ISAKMP	126	INFORMATIONAL MID=26 Responder Request
4	0.650532	10.0.1.2	202.20.1.1	ISAKMP	126	INFORMATIONAL MID=26 Initiator Response
21	14.242944	10.0.1.2	202.20.1.1	ISAKMP	126	INFORMATIONAL MID=06 Initiator Request
22	14.245956	202.20.1.1	10.0.1.2	ISAKMP	126	INFORMATIONAL MID=06 Responder Response
27	14.258913	10.0.1.2	202.20.1.1	ISAKMP	126	INFORMATIONAL MID=07 Initiator Request
28	14.260554	202.20.1.1	10.0.1.2	ISAKMP	126	INFORMATIONAL MID=07 Responder Response
34	15.678946	10.0.1.2	202.20.1.1	ISAKMP	674	IKE_SA_INIT MID=00 Initiator Request
35	15.696226	202.20.1.1	10.0.1.2	ISAKMP	523	IKE_SA_INIT MID=00 Responder Response
36	15.706983	10.0.1.2	202.20.1.1	ISAKMP	626	IKE_AUTH MID=01 Initiator Request (fragment 1/3)
37	15.707021	10.0.1.2	202.20.1.1	ISAKMP	626	IKE_AUTH MID=01 Initiator Request (fragment 2/3)
38	15.707039	10.0.1.2	202.20.1.1	ISAKMP	210	IKE_AUTH MID=01 Initiator Request (fragment 3/3)
39	15.712443	202.20.1.1	10.0.1.2	ISAKMP	1282	IKE_AUTH MID=01 Responder Response (fragment 1/2)
40	15.712521	202.20.1.1	10.0.1.2	ISAKMP	482	IKE_AUTH MID=01 Responder Response (fragment 2/2)
41	15.717329	10.0.1.2	202.20.1.1	ISAKMP	142	IKE_AUTH MID=02 Initiator Request
42	15.718000	202.20.1.1	10.0.1.2	ISAKMP	158	IKE_AUTH MID=02 Responder Response
43	15.719870	10.0.1.2	202.20.1.1	ISAKMP	190	IKE_AUTH MID=03 Initiator Request
44	15.720965	202.20.1.1	10.0.1.2	ISAKMP	190	IKE_AUTH MID=03 Responder Response
45	15.738215	10.0.1.2	202.20.1.1	ISAKMP	126	IKE_AUTH MID=04 Initiator Request
46	15.739487	202.20.1.1	10.0.1.2	ISAKMP	126	IKE_AUTH MID=04 Responder Response
47	15.742509	10.0.1.2	202.20.1.1	ISAKMP	158	IKE_AUTH MID=05 Initiator Request
48	15.747750	202.20.1.1	10.0.1.2	ISAKMP	302	IKE_AUTH MID=05 Responder Response

> Frame 3: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{D52CDBBA-4A0A-4ABA-981C-E72EF...}

> Ethernet II, Src: VMware_ae:58:77 (00:50:56:ae:58:77), Dst: VMware_ae:9a:ca (00:50:56:ae:9a:ca)

> Internet Protocol Version 4, Src: 202.20.1.1, Dst: 10.0.1.2

> User Datagram Protocol, Src Port: 4500, Dst Port: 4500

> UDP Encapsulation of IPsec Packets

> Internet Security Association and Key Management Protocol

0000 00 50 56 ae 9a ca 00 50 56 ae 58 77 08 00 45 00 PV...P V Xw...E-

0010 00 70 43 e9 00 00 3f 11 61 7d ca 14 01 01 0a 00 pC...? a).....

0020 01 02 11 94 11 94 00 5c db e3 00 00 00 00 eb d4 \

0030 76 b7 5e e8 6e 9a 22 33 20 38 b4 7b 8a 6b 2e 20 v...n."3 8 {k.

0040 25 00 00 00 00 1a 00 00 00 50 00 00 00 34 6d e5 %.....P...4m.

0050 d9 8a e3 8d b6 dd 11 b5 18 32 8f 32 df 93 25 002.2...%

0060 cb 4d 33 5b 4d ad b2 c9 5d 89 2e 08 cc fa e3 34 N3[M...]....4

0070 b9 3a a8 0f dc 0a 71 5d 47 28 2a d4 29 d9 .:....q] G(*).

Internet Security Association and Key Management Protocol: Protocol

Packets: 86 · Displayed: 21 (24.4%) · Dropped: 0 (0.0%) | Profile: Default

1:05 PM 11/30/2025

Configuring a VPN Client for Secure File Transfers (3e)

Network Security, Firewalls, and VPNs, Third Edition - Lab 09

Make a screen capture showing the selected Diffie-Hellman transform.

VMware vmxnet3 virtual network device: Student

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Configuring a VPN Client for Secure File Transfers (3e)

RemoteWindows01

2025-11-30 14:05:59

Vidhi Kadakia

No.	isakmp	Source	Destination	Protocol	Length	Info
3	0.650241	202.20.1.1	10.0.1.2	ISAKMP	126	INFORMATIONAL MID=26 Responder Request
4	0.650532	10.0.1.2	202.20.1.1	ISAKMP	126	INFORMATIONAL MID=26 Initiator Response
21	14.242944	10.0.1.2	202.20.1.1	ISAKMP	126	INFORMATIONAL MID=06 Initiator Request
22	14.245956	202.20.1.1	10.0.1.2	ISAKMP	126	INFORMATIONAL MID=06 Responder Response
27	14.258913	10.0.1.2	202.20.1.1	ISAKMP	126	INFORMATIONAL MID=07 Initiator Request
28	14.260554	202.20.1.1	10.0.1.2	ISAKMP	126	INFORMATIONAL MID=07 Responder Response
34	15.678946	10.0.1.2	202.20.1.1	ISAKMP	674	IKE_SA_INIT MID=00 Initiator Request
35	15.696226	202.20.1.1	10.0.1.2	ISAKMP	523	IKE_SA_INIT MID=00 Responder Response
36	15.706983	10.0.1.2	202.20.1.1	ISAKMP	626	IKE_AUTH MID=01 Initiator Request (fragment 1/3)
37	15.707021	10.0.1.2	202.20.1.1	ISAKMP	626	IKE_AUTH MID=01 Initiator Request (fragment 2/3)
38	15.707039	10.0.1.2	202.20.1.1	ISAKMP	210	IKE_AUTH MID=01 Initiator Request (fragment 3/3)
39	15.712443	202.20.1.1	10.0.1.2	ISAKMP	1282	IKE_AUTH MID=01 Responder Response (fragment 1/2)
40	15.712521	202.20.1.1	10.0.1.2	ISAKMP	482	IKE_AUTH MID=01 Responder Response (fragment 2/2)
41	15.717329	10.0.1.2	202.20.1.1	ISAKMP	142	IKE_AUTH MID=02 Initiator Request
42	15.718000	202.20.1.1	10.0.1.2	ISAKMP	158	IKE_AUTH MID=02 Responder Response
43	15.719870	10.0.1.2	202.20.1.1	ISAKMP	190	IKE_AUTH MID=03 Initiator Request
44	15.720965	202.20.1.1	10.0.1.2	ISAKMP	190	IKE_AUTH MID=03 Responder Response
45	15.738215	10.0.1.2	202.20.1.1	ISAKMP	126	IKE_AUTH MID=04 Initiator Request
46	15.739487	202.20.1.1	10.0.1.2	ISAKMP	126	IKE_AUTH MID=04 Responder Response
47	15.742509	10.0.1.2	202.20.1.1	ISAKMP	158	IKE_AUTH MID=05 Initiator Request
48	15.747750	202.20.1.1	10.0.1.2	ISAKMP	302	IKE_AUTH MID=05 Responder Response

> Frame 3: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{D52CDBBA-4A0A-4ABA-981C-E72EF}

> Ethernet II, Src: VMware_ae:58:77 (00:50:56:ae:58:77), Dst: VMware_ae:9a:ca (00:50:56:ae:9a:ca)

> Internet Protocol Version 4, Src: 202.20.1.1, Dst: 10.0.1.2

> User Datagram Protocol, Src Port: 4500, Dst Port: 4500

> UDP Encapsulation of IPsec Packets

> Internet Security Association and Key Management Protocol

0000 00 50 56 ae 9a ca 00 50 56 ae 58 77 08 00 45 00 PV...P V Xw...E

0010 00 70 43 e9 00 00 3f 11 61 7d ca 14 01 01 0a 00 pC...? a).....

0020 01 02 11 94 11 94 00 5c db e3 00 00 00 00 eb d4 \

0030 76 b7 5e e8 6e 9a 22 33 20 38 b4 7b 8a 6b 2e 20 v^..n"3 8- {k.

0040 25 00 00 00 00 1a 00 00 00 50 00 00 00 34 6d e5 %.....P...4m.

0050 d9 8a e3 8d b6 dd 11 b5 18 32 8f 32 df 93 25 00 2.2.%

0060 cb 4d 33 5b 4d ad b2 c9 5d 89 2e 08 cc fa e3 34 N3[H...].4

0070 b9 3a a8 0f dc 0a 71 5d 47 28 2a d4 29 d9 .:....q] G(*). .

Internet Security Association and Key Management Protocol: Protocol

Packets: 86 · Displayed: 21 (24.4%) · Dropped: 0 (0.0%) | Profile: Default

1:05 PM 11/30/2025