

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

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

Student:

Stephen Asamoah

Email:

stephen.asamoah@howardcc.edu

Time on Task:

3 hours, 55 minutes

Progress:

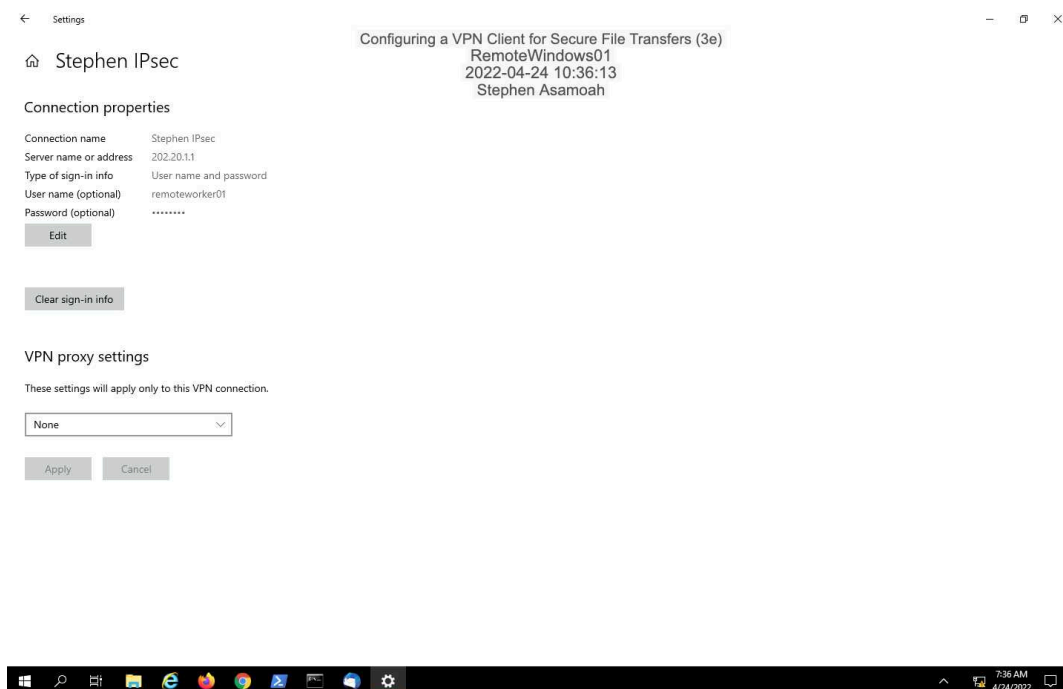
100%

Report Generated: Sunday, April 24, 2022 at 2:15 PM

Section 1: Hands-On Demonstration

Part 1: Configure a Windows VPN Client

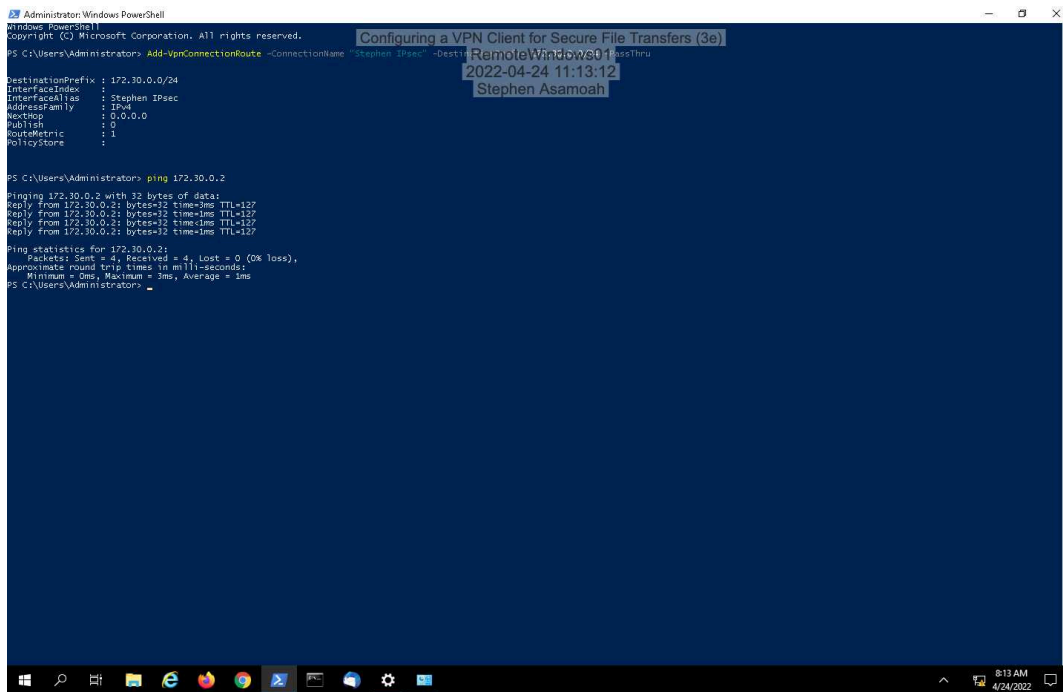
30. **Make a screen capture** showing the **VPN connection properties**.



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.



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

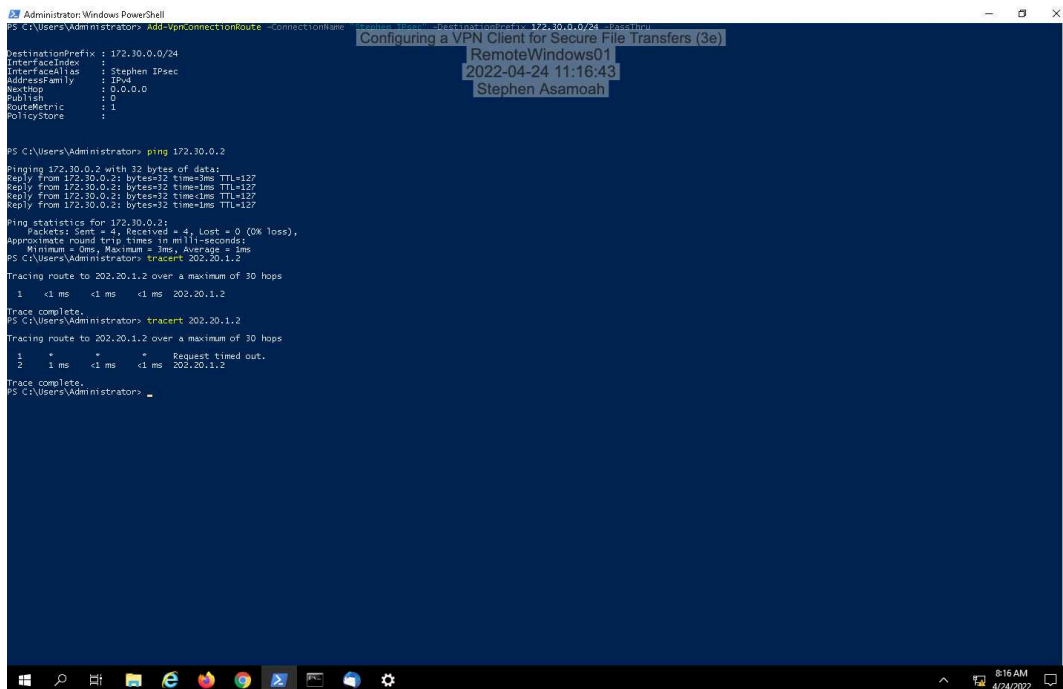
PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "Stephen IPsec" -DestinationPrefix 172.30.0.0/24 -InterfaceIndex 1 -AddressFamily IPsec -NextHop 0.0.0.0 -Publish 0 -RouteMetric 1 -PolicyStore

PS C:\Users\Administrator> ping 172.30.0.2

Pinging 172.30.0.2 with 32 bytes of data:
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127

Ping statistics for 172.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 1ms
PS C:\Users\Administrator>
```

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



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

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "Stephen IPsec" -DestinationPrefix 172.30.0.0/24 -InterfaceIndex 1 -AddressFamily IPsec -NextHop 0.0.0.0 -Publish 0 -RouteMetric 1 -PolicyStore

PS C:\Users\Administrator> ping 172.30.0.2

Pinging 172.30.0.2 with 32 bytes of data:
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127
Reply from 172.30.0.2: bytes=32 time=1ms TTL=127

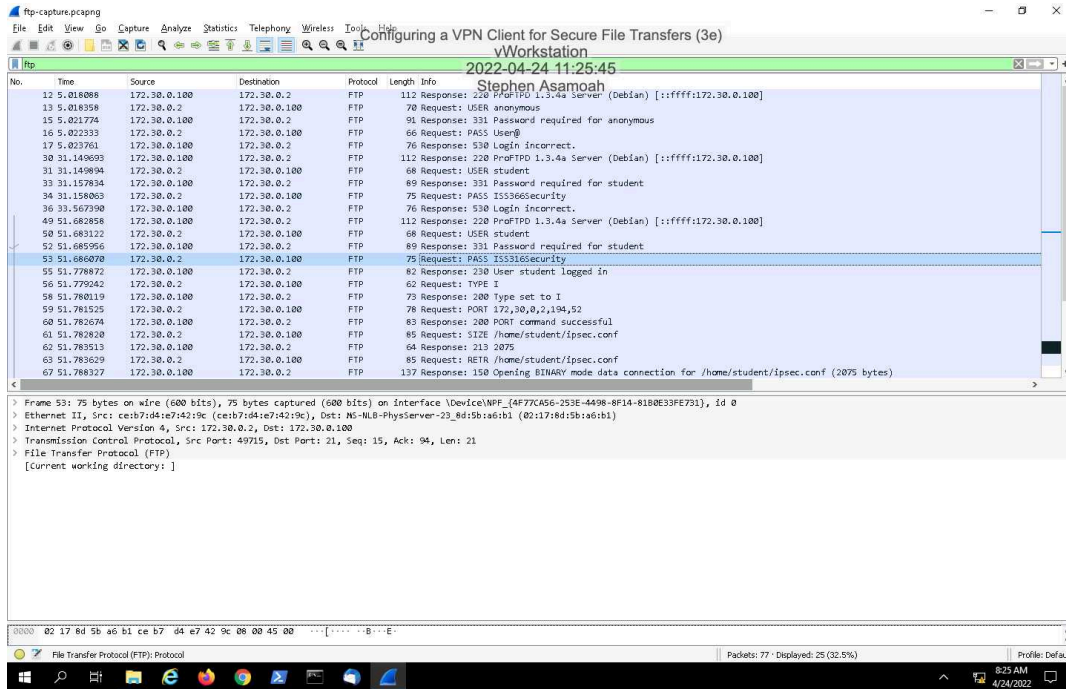
Ping statistics for 172.30.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 1ms
PS C:\Users\Administrator> tracert 202.20.1.2

Tracing route to 202.20.1.2 over a maximum of 30 hops:
  0  <1 ms  <1 ms  <1 ms  202.20.1.2
Trace complete.
PS C:\Users\Administrator> tracert 202.20.1.2

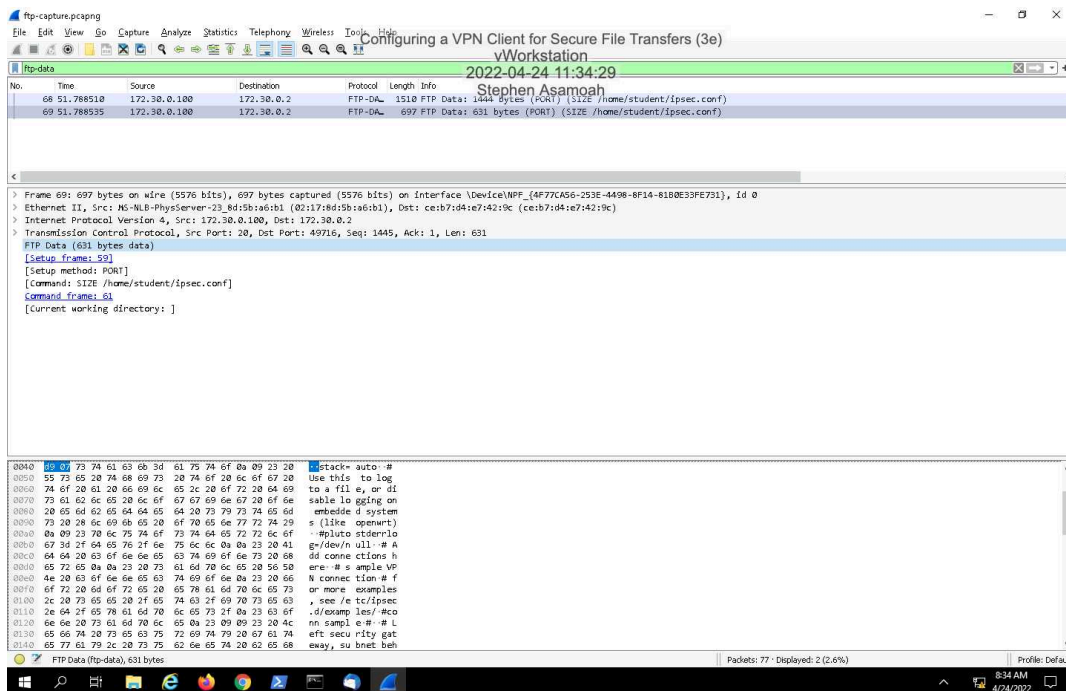
Tracing route to 202.20.1.2 over a maximum of 30 hops:
  0  *      *      *      Request timed out.
  1  1 ms  <1 ms  <1 ms  202.20.1.2
Trace complete.
PS C:\Users\Administrator>
```

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

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



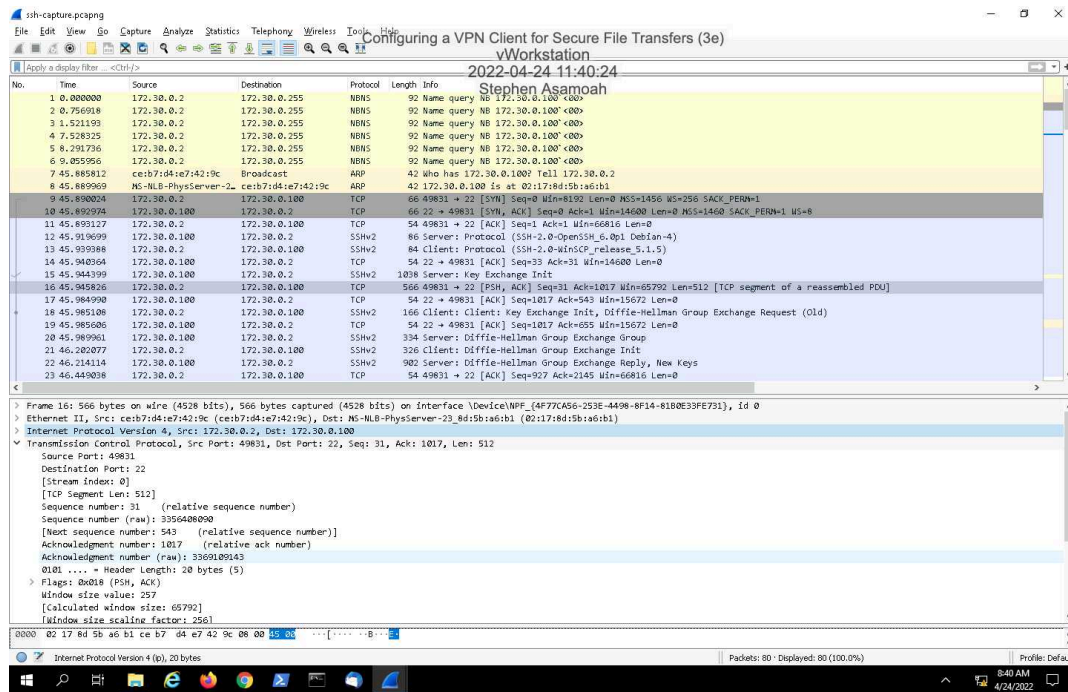
28. Make a screen capture showing the Wireshark window and the packet bytes pane for Packet 69.



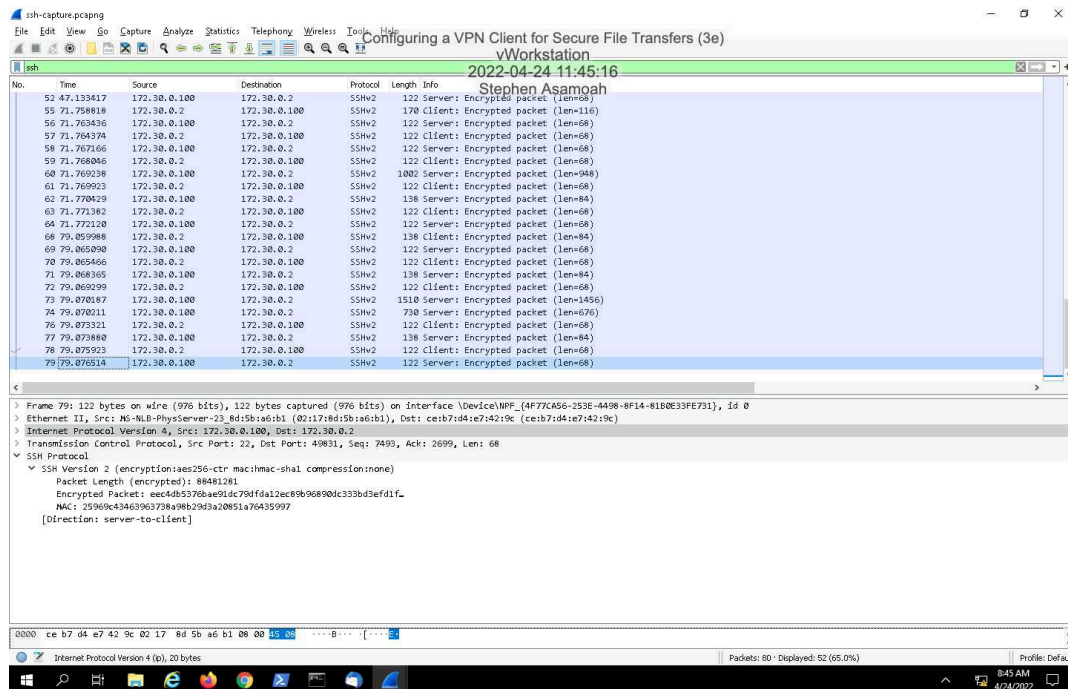
Configuring a VPN Client for Secure File Transfers (3e)

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

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



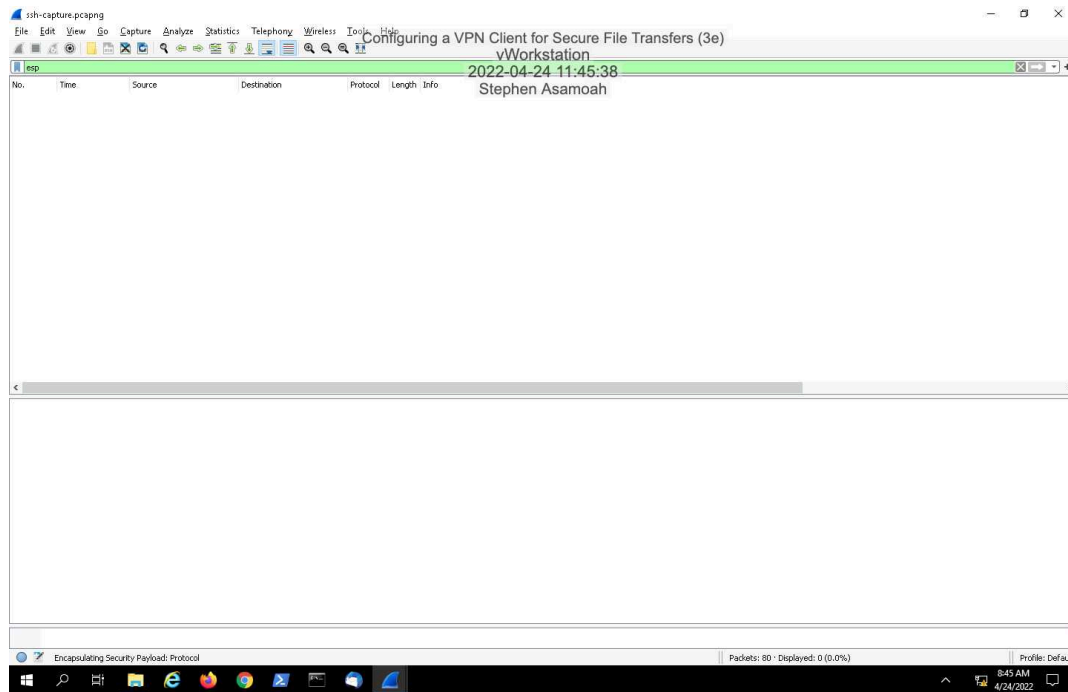
49. Make a screen capture showing the last SSHv2 packet in the SSH file transfer.



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

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

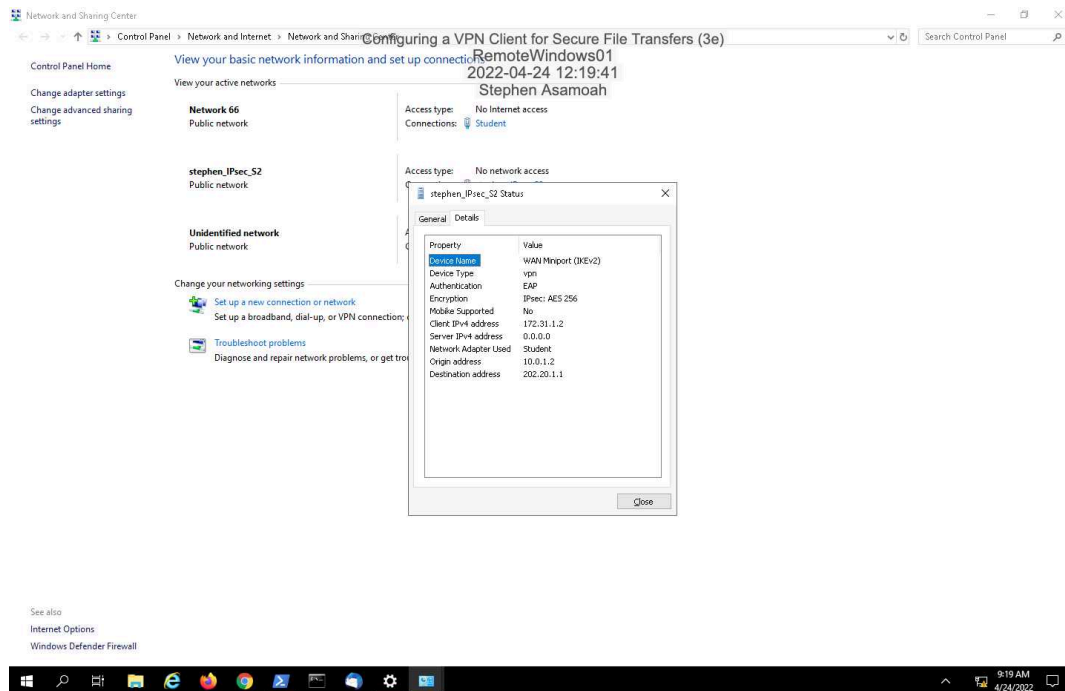
51. Make a screen capture showing the **last packets in the ESP exchange**.



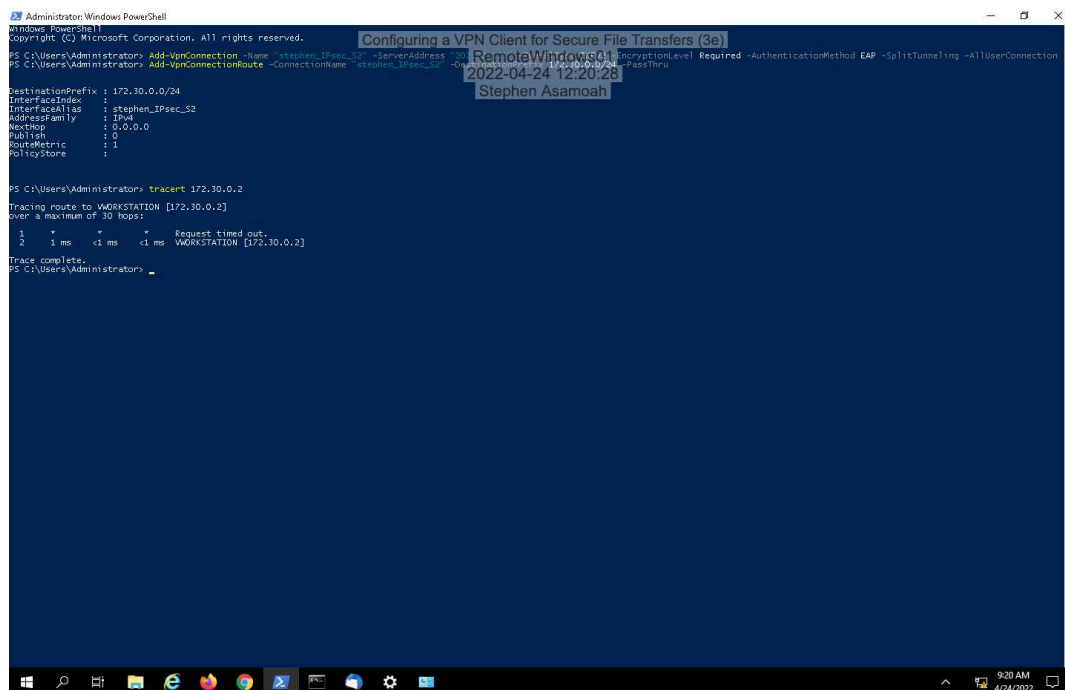
Section 2: Applied Learning

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.

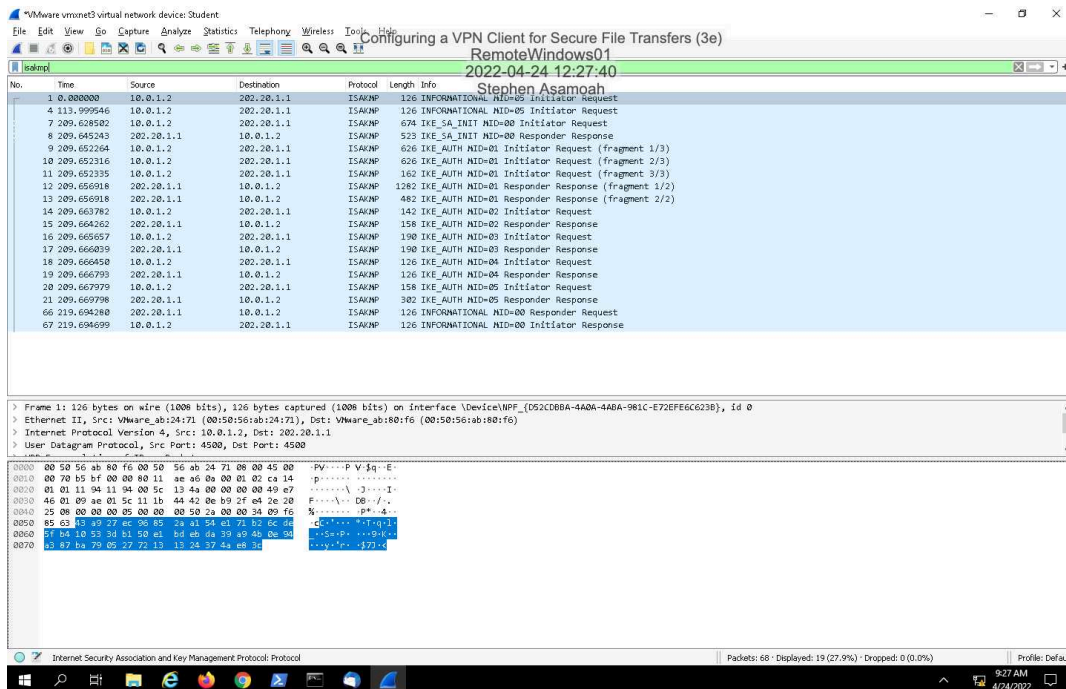


Configuring a VPN Client for Secure File Transfers (3e)

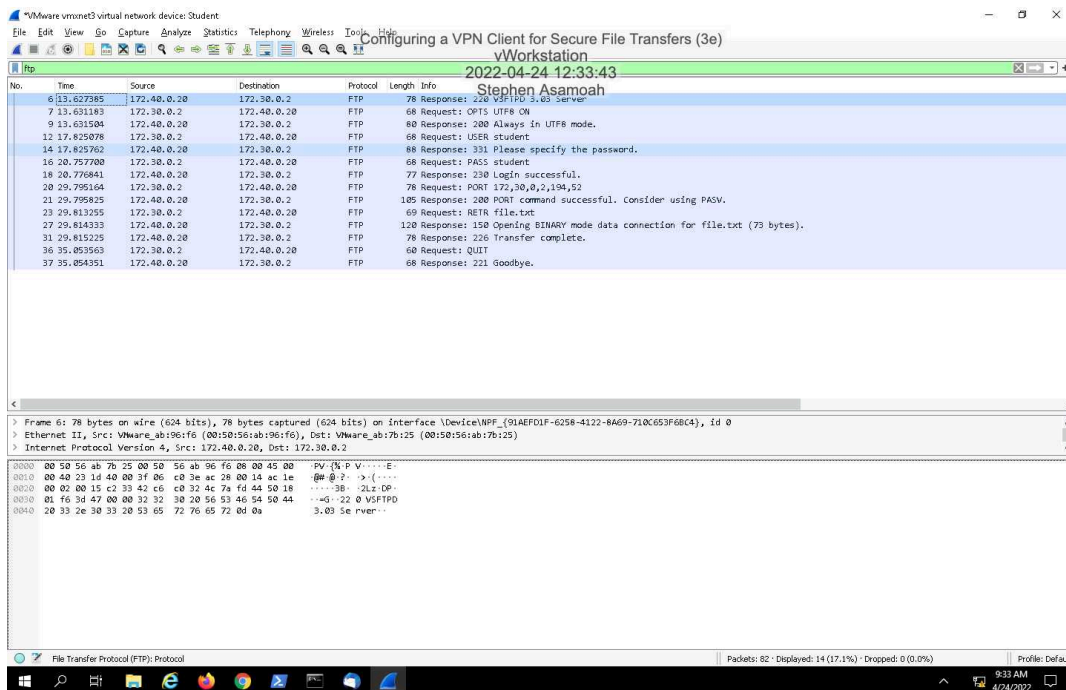
Network Security, Firewalls, and VPNs, Third Edition - Lab 09

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

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



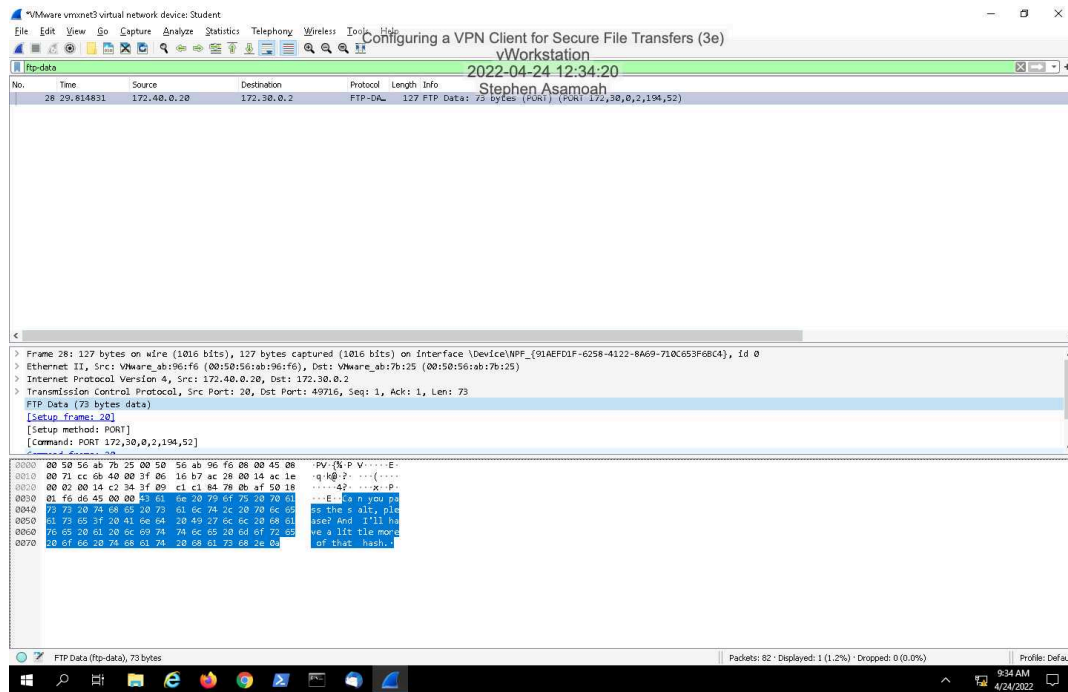
22. Make a screen capture showing the filtered FTP packets in your capture file.



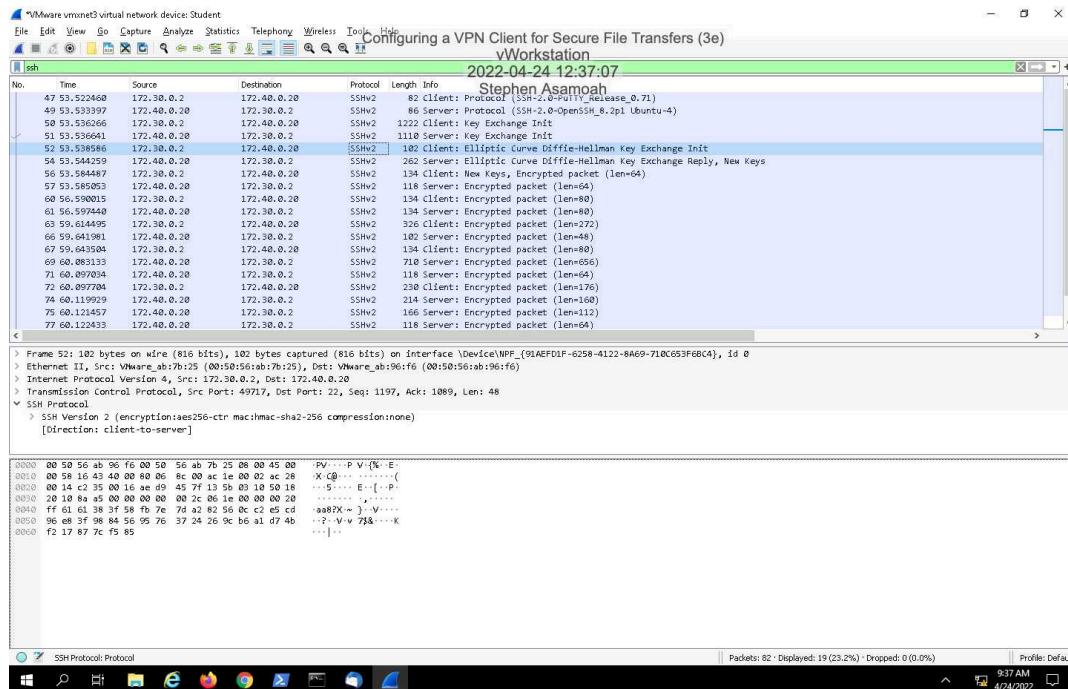
Configuring a VPN Client for Secure File Transfers (3e)

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.



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



Section 3: Challenge and Analysis

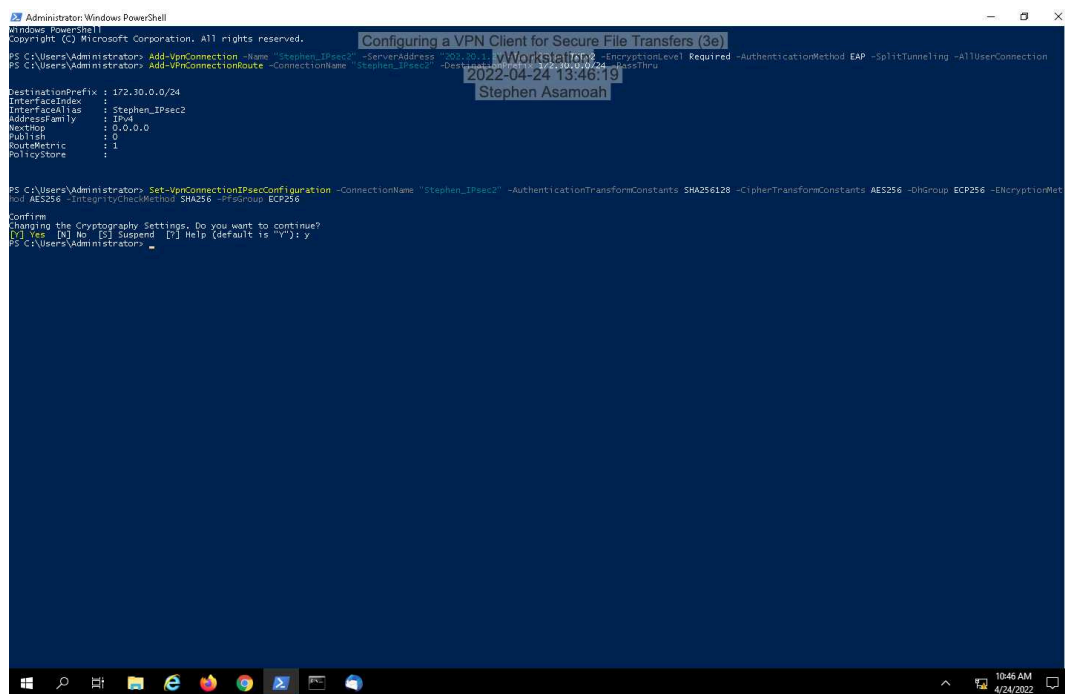
Part 1: Create a New VPN Connection using PowerShell

Document the command you used to add your VPN connection.

VPN Config: Add-VpnConnection -Name "Stephen_IPsec2" -ServerAddress '202.20.1.2' -TunnelType IKEv2 -EncryptionLevel Required -AuthenticationMethod EAP -SplitTunneling -AllUserConnection
Adding VPN: Add-VpnConnectionRoute -ConnectionName "Stephen_IPsec2" -DestinationPrefix 172.30.0.0/24 -PassThru

Part 2: Implement a Custom IPsec Policy

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



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command prompt shows the following commands and output:

```
PS C:\Users\Administrator> Add-VpnConnection -Name "Stephen_IPsec2" -ServerAddress '202.20.1.2' -TunnelType IKEv2 -EncryptionLevel Required -AuthenticationMethod EAP -SplitTunneling -AllUserConnection
PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "Stephen_IPsec2" -DestinationPrefix 172.30.0.0/24 -PassThru

DestinationPrefix : 172.30.0.0/24
InterfaceIndex    : 
InterfaceAlias    : Stephen_IPsec2
AddressFamily     : IPv4
NextHop           : 0.0.0.0
Publish           : 0
RouteMetric       : 1
PolicyStore       : 

PS C:\Users\Administrator> Set-VpnConnectionIPsecConfiguration -ConnectionName "Stephen_IPsec2" -AuthenticationTransformConstants SHA256128 -CipherTransformConstants AES256 -DhGroup ECP256 -EncryptionMet
oid AES256 -IntegrityCheckMethod SHA256 -PfsGroup ECP256

Confirm
Changing the Cryptography Settings. Do you want to continue?
[Y] Yes [N] No [S] Suspend [D] Help (default is "Y"): y
PS C:\Users\Administrator>
```

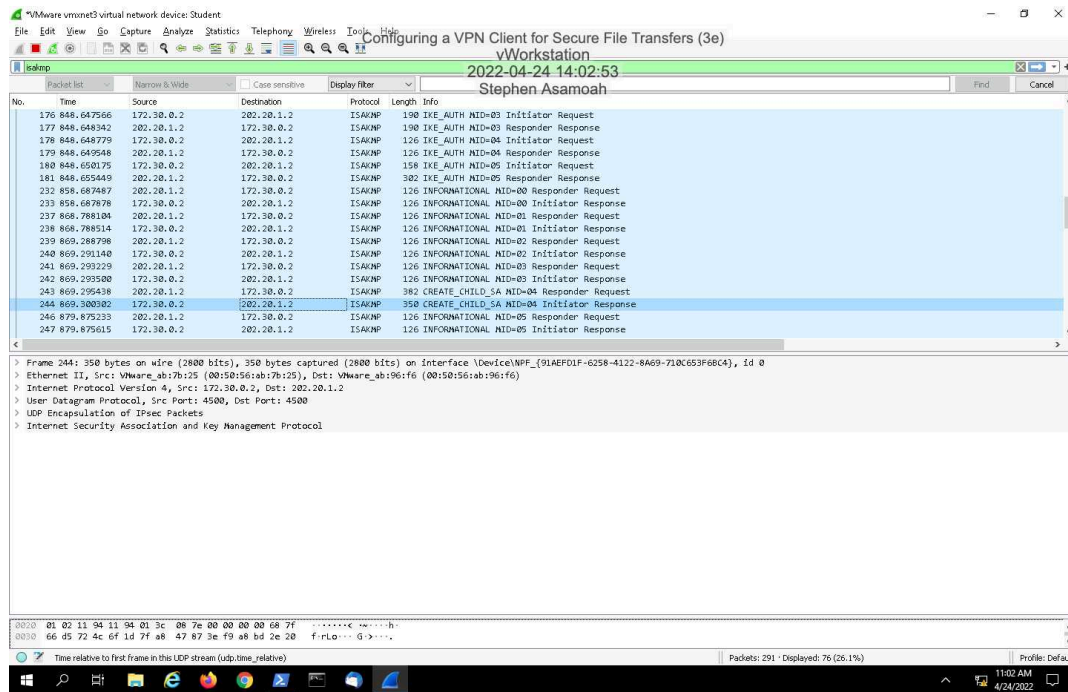
The screenshot also shows a watermark "vWorkstation" and a timestamp "2022-04-24 10:46:19" over the command prompt. The taskbar at the bottom shows the system clock as 10:46 AM on 4/24/2022.

Part 3: Verify Your VPN Implementation using Wireshark

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

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

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



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

