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

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

Student:	Email:
Roman Cassman	rcassman0001@kctcs.edu

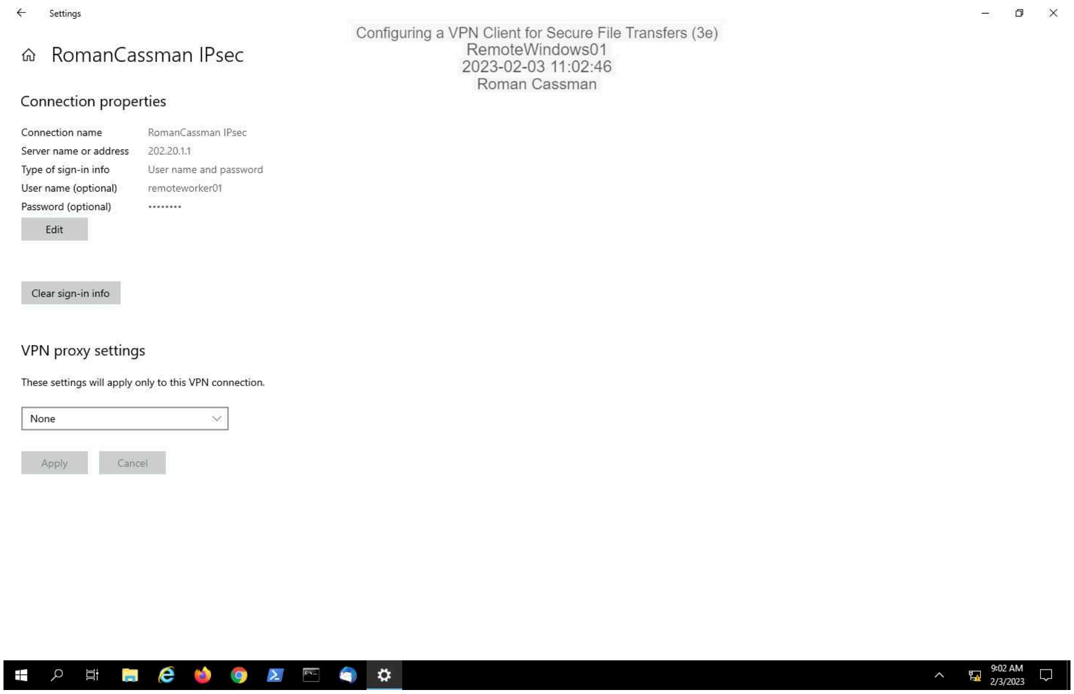
Time on Task:	Progress:
10 hours, 0 minutes	77%

Report Generated: Friday, February 3, 2023 at 3:40 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)
RemoteWindows01
2023-02-03 11:02:46
Roman Cassman

RomanCassman IPsec

Connection properties

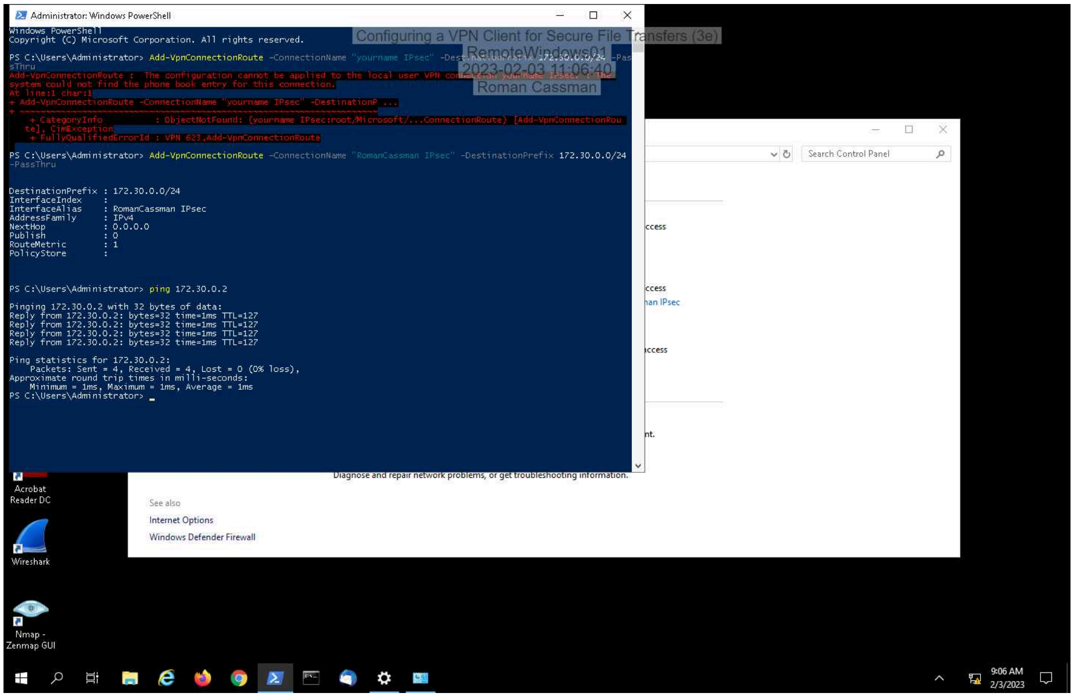
Connection name: RomanCassman IPsec
Server name or address: 202.20.1.1
Type of sign-in info: User name and password
User name (optional): remoteworker01
Password (optional): ••••••••

VPN proxy settings

These settings will apply only to this VPN connection.

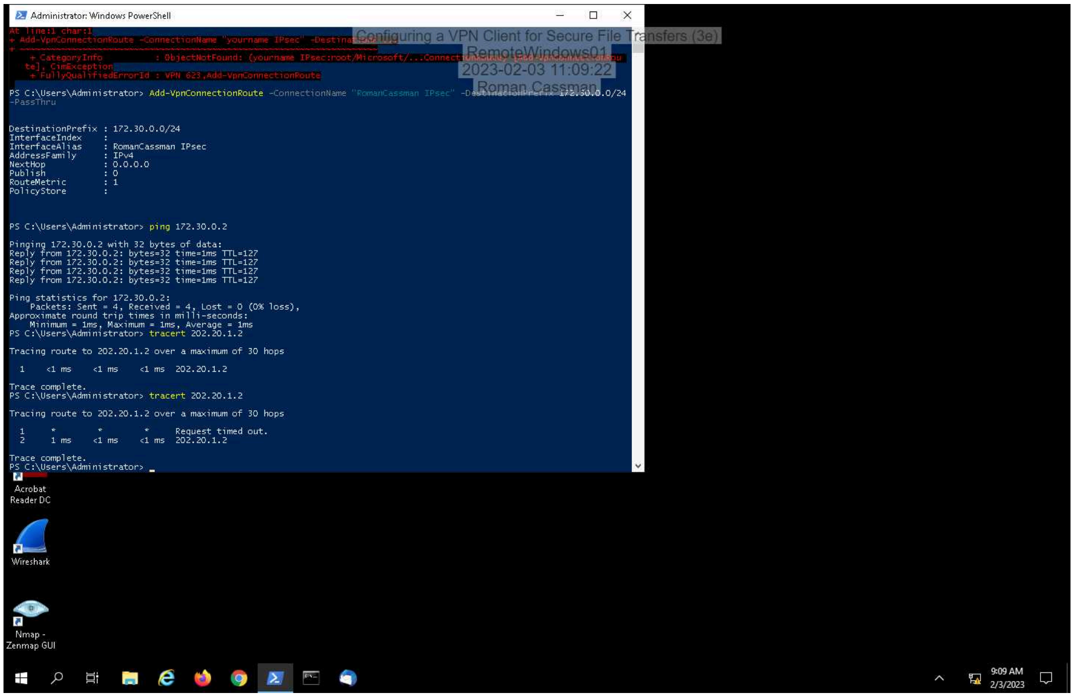
None

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


Administrator: Windows PowerShell
Configuring a VPN Client for Secure File Transfers (3e)
RemoteWindows01
2023-02-03 11:06:40
Roman Cassman
Search Control Panel
ccess
ccess
an IPsec
ccess
nt.
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Defender Firewall
Acrobat Reader DC
Wireshark
Nmap - Zenmap GUI
9:06 AM
2/3/2023

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

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "yourname IPsec" -DestinationPrefix 172.30.0.0/24 -Pas
sThru
Add-VpnConnectionRoute :  The configuration cannot be applied to the local user VPN connection yourname IPsec. : The
system could not find the phone book entry for this connection.
At line:1 char:1
+ Add-VpnConnectionRoute -ConnectionName "yourname IPsec" -DestinationP ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (yourname IPsec:root/Microsoft/...ConnectionRoute) [Add-VpnConnectionRou
   te], CimException
    + FullyQualifiedErrorId : VPN 623,Add-VpnConnectionRoute

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "RomanCassman IPsec" -DestinationPrefix 172.30.0.0/24
-PassThru


DestinationPrefix : 172.30.0.0/24
InterfaceIndex    :
InterfaceAlias    : RomanCassman IPsec
AddressFamily     : IPv4
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 = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Users\Administrator> _
```

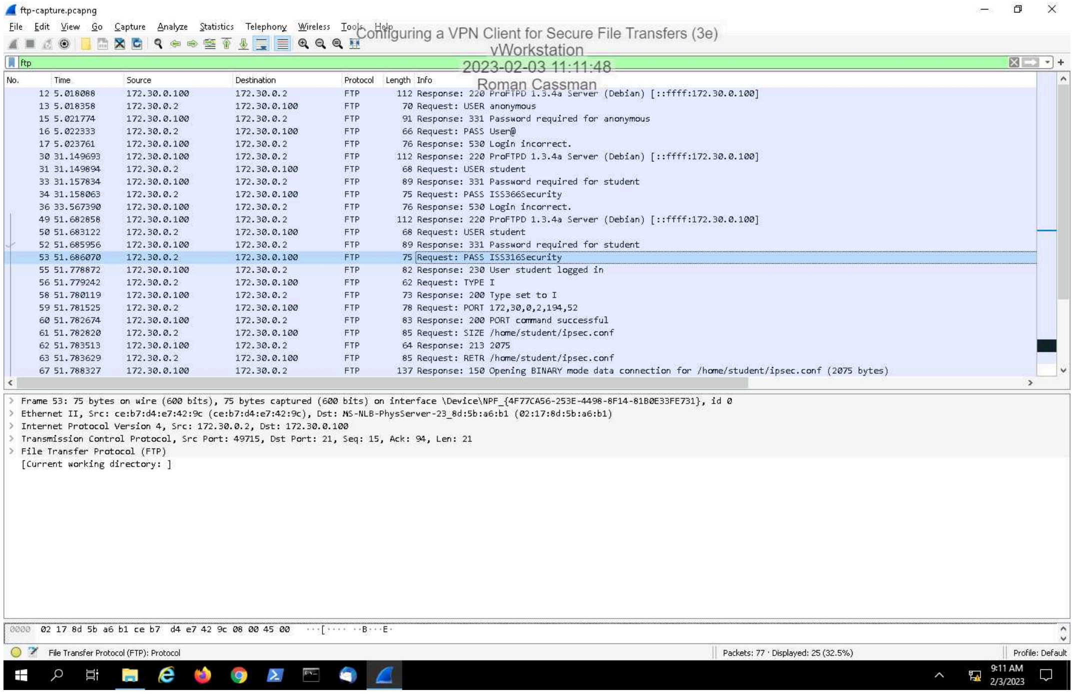
72. **Make a screen capture** showing your **new tracert results**.



```
At line:1 char:1
+ Add-VpnConnectionRoute -ConnectionName "yourname IPsec" -DestinationP ...
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (yourname IPsec:root/Microsoft/...ConnectionRoute) [Add-VpnConnectionRou
   te], CimException
    + FullyQualifiedErrorId : VPN 623,Add-VpnConnectionRoute

PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "RomanCassman IPsec" -DestinationPrefix 172.30.0.0/24
-PassThru


DestinationPrefix : 172.30.0.0/24
InterfaceIndex    :
InterfaceAlias    : RomanCassman IPsec
AddressFamily     : IPv4
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 = 1ms, 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

  1    <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

  1     *        *        *     Request timed out.
  2     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**.


ftp-capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-03 11:11:48
Roman Cassman
9:11 AM
2/3/2023

Display filter: ftp

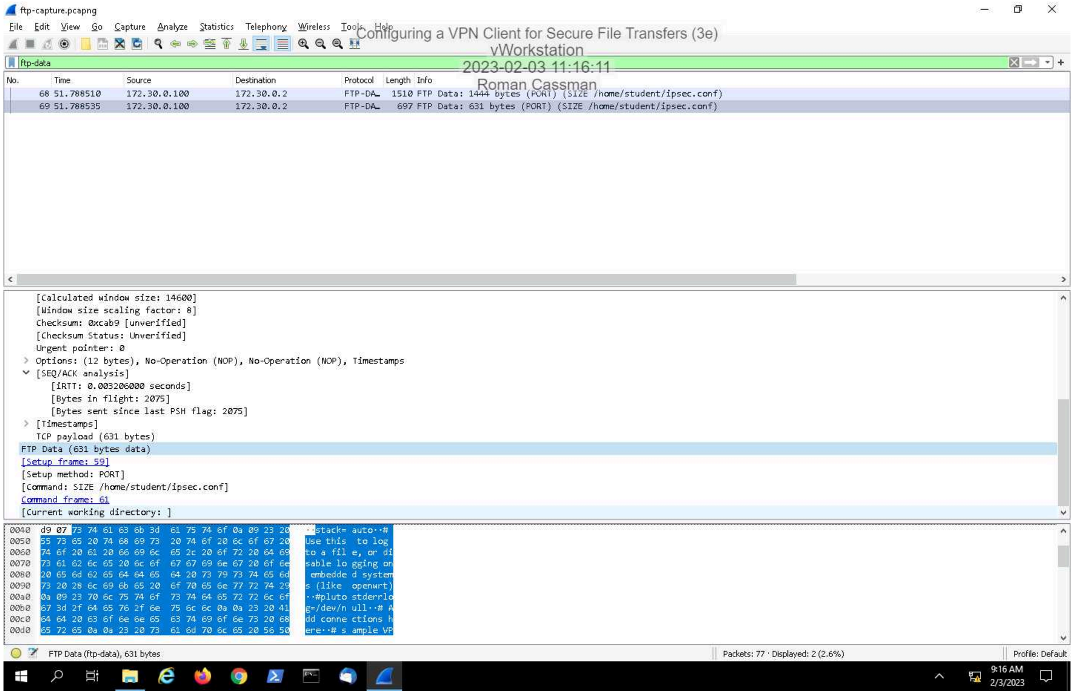
```
No.   Time        Source         Destination    Protocol  Length  Info
   12 5.018088    172.30.0.100   172.30.0.2     FTP        112 Response: 220 ProFTPD 1.3.4a Server (Debian) [::ffff:172.30.0.100]
   13 5.018358    172.30.0.2     172.30.0.100   FTP         70 Request: USER anonymous
   15 5.021774    172.30.0.100   172.30.0.2     FTP         91 Response: 331 Password required for anonymous
   16 5.022333    172.30.0.2     172.30.0.100   FTP         66 Request: PASS User@
   17 5.023761    172.30.0.100   172.30.0.2     FTP         76 Response: 530 Login incorrect.
   30 31.149693   172.30.0.100   172.30.0.2     FTP        112 Response: 220 ProFTPD 1.3.4a Server (Debian) [::ffff:172.30.0.100]
   31 31.149894   172.30.0.2     172.30.0.100   FTP         68 Request: USER student
   33 31.157834   172.30.0.100   172.30.0.2     FTP         89 Response: 331 Password required for student
   34 31.158063   172.30.0.2     172.30.0.100   FTP         75 Request: PASS ISS366Security
   36 33.567390   172.30.0.100   172.30.0.2     FTP         76 Response: 530 Login incorrect.
   49 51.682858   172.30.0.100   172.30.0.2     FTP        112 Response: 220 ProFTPD 1.3.4a Server (Debian) [::ffff:172.30.0.100]
   50 51.683122   172.30.0.2     172.30.0.100   FTP         68 Request: USER student
   52 51.685956   172.30.0.100   172.30.0.2     FTP         89 Response: 331 Password required for student
   53 51.686070   172.30.0.2     172.30.0.100   FTP         75 Request: PASS ISS316Security
   55 51.778872   172.30.0.100   172.30.0.2     FTP         82 Response: 230 User student logged in
   56 51.779242   172.30.0.2     172.30.0.100   FTP         62 Request: TYPE I
   58 51.780119   172.30.0.100   172.30.0.2     FTP         73 Response: 200 Type set to I
   59 51.781525   172.30.0.2     172.30.0.100   FTP         78 Request: PORT 172,30,0,2,194,52
   60 51.782674   172.30.0.100   172.30.0.2     FTP         83 Response: 200 PORT command successful
   61 51.782820   172.30.0.2     172.30.0.100   FTP         85 Request: SIZE /home/student/ipsec.conf
   62 51.783513   172.30.0.100   172.30.0.2     FTP         64 Response: 213 2075
   63 51.783629   172.30.0.2     172.30.0.100   FTP         85 Request: RETR /home/student/ipsec.conf
   67 51.788327   172.30.0.100   172.30.0.2     FTP        137 Response: 150 Opening BINARY mode data connection for /home/student/ipsec.conf (2075 bytes)
```

```
> Frame 53: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface \Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731}, id 0
> Ethernet II, Src: ce:b7:d4:e7:42:9c (ce:b7:d4:e7:42:9c), Dst: MS-NLB-PhysServer-23_8d:5b:a6:b1 (02:17:8d:5b:a6:b1)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.100
> Transmission Control Protocol, Src Port: 49715, Dst Port: 21, Seq: 15, Ack: 94, Len: 21
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  02 17 8d 5b a6 b1 ce b7  d4 e7 42 9c 08 00 45 00   ···[···· ··B···E·
```

File Transfer Protocol (FTP): Protocol | Packets: 77 · Displayed: 25 (32.5%) | Profile: Default

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


ftp-capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-03 11:16:11
Roman Cassman
9:16 AM
2/3/2023

Display filter: ftp-data

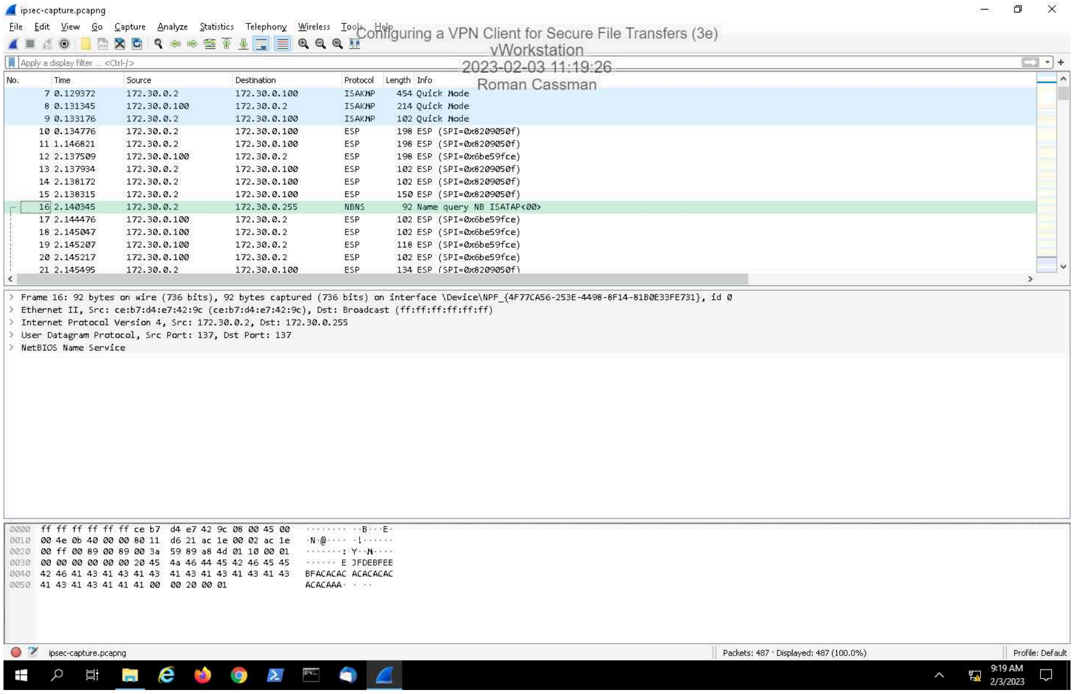
```
No.   Time        Source         Destination    Protocol  Length  Info
   68 51.788510   172.30.0.100   172.30.0.2     FTP-DA…    1510 FTP Data: 1444 bytes (PORT) (SIZE /home/student/ipsec.conf)
   69 51.788535   172.30.0.100   172.30.0.2     FTP-DA…     697 FTP Data: 631 bytes (PORT) (SIZE /home/student/ipsec.conf)
```

```
    [Calculated window size: 14600]
    [Window size scaling factor: 8]
    Checksum: 0xcab9 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
  v [SEQ/ACK analysis]
      [iRTT: 0.003206000 seconds]
      [Bytes in flight: 2075]
      [Bytes sent since last PSH flag: 2075]
  > [Timestamps]
    TCP payload (631 bytes)
FTP Data (631 bytes data)
[Setup frame: 59]
[Setup method: PORT]
[Command: SIZE /home/student/ipsec.conf]
Command frame: 61
[Current working directory: ]
```

```
0040  d9 07 73 74 61 63 6b 3d  61 75 74 6f 0a 09 23 20   ··stack= auto··# 
0050  55 73 65 20 74 68 69 73  20 74 6f 20 6c 6f 67 20   Use this  to log 
0060  74 6f 20 61 20 66 69 6c  65 2c 20 6f 72 20 64 69   to a fil e, or di
0070  73 61 62 6c 65 20 6c 6f  67 67 69 6e 67 20 6f 6e   sable lo gging on
0080  20 65 6d 62 65 64 64 65  64 20 73 79 73 74 65 6d    embedde d system
0090  73 20 28 6c 69 6b 65 20  6f 70 65 6e 77 72 74 29   s (like  openwrt)
00a0  0a 09 23 70 6c 75 74 6f  73 74 64 65 72 72 6c 6f   ··#pluto stderrlo
00b0  67 3d 2f 64 65 76 2f 6e  75 6c 6c 0a 0a 23 20 41   g=/dev/n ull··# A
00c0  64 64 20 63 6f 6e 6e 65  63 74 69 6f 6e 73 20 68   dd conne ctions h
00d0  65 72 65 0a 0a 23 20 73  61 6d 70 6c 65 20 56 50   ere··# s ample VP
```

FTP Data (ftp-data), 631 bytes | Packets: 77 · Displayed: 2 (2.6%) | Profile: Default

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


ipsec-capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-03 11:19:26
Roman Cassman

```
No.  Time       Source        Destination   Protocol Length Info
   7 0.129372   172.30.0.2    172.30.0.100  ISAKMP    454 Quick Mode
   8 0.131345   172.30.0.100  172.30.0.2    ISAKMP    214 Quick Mode
   9 0.133176   172.30.0.2    172.30.0.100  ISAKMP    102 Quick Mode
  10 0.134776   172.30.0.2    172.30.0.100  ESP       198 ESP (SPI=0x8209050f)
  11 1.146821   172.30.0.2    172.30.0.100  ESP       198 ESP (SPI=0x8209050f)
  12 2.137509   172.30.0.100  172.30.0.2    ESP       198 ESP (SPI=0x6be59fce)
  13 2.137934   172.30.0.2    172.30.0.100  ESP       102 ESP (SPI=0x8209050f)
  14 2.138172   172.30.0.2    172.30.0.100  ESP       102 ESP (SPI=0x8209050f)
  15 2.138315   172.30.0.2    172.30.0.100  ESP       150 ESP (SPI=0x8209050f)
  16 2.140345   172.30.0.2    172.30.0.255  NBNS       92 Name query NB ISATAP<00>
  17 2.144476   172.30.0.100  172.30.0.2    ESP       102 ESP (SPI=0x6be59fce)
  18 2.145047   172.30.0.100  172.30.0.2    ESP       102 ESP (SPI=0x6be59fce)
  19 2.145207   172.30.0.100  172.30.0.2    ESP       118 ESP (SPI=0x6be59fce)
  20 2.145217   172.30.0.100  172.30.0.2    ESP       102 ESP (SPI=0x6be59fce)
  21 2.145495   172.30.0.2    172.30.0.100  ESP       134 ESP (SPI=0x8209050f)
```

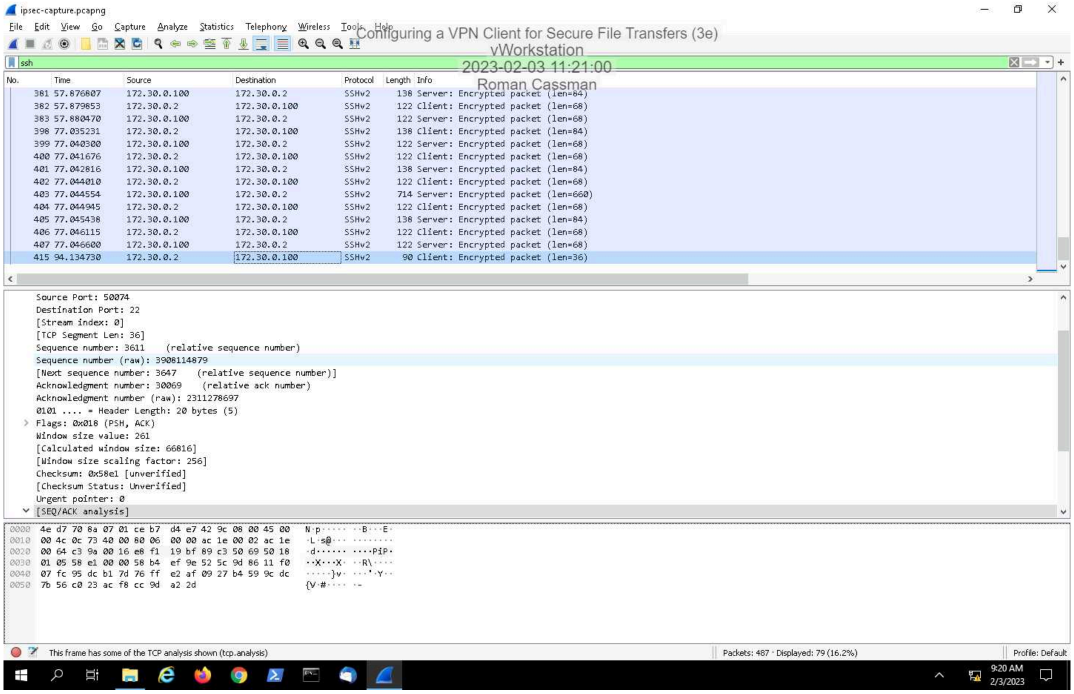
```
> Frame 16: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731}, id 0
> Ethernet II, Src: ce:b7:d4:e7:42:9c (ce:b7:d4:e7:42:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff ce b7  d4 e7 42 9c 08 00 45 00   ········ ··B···E·
0010  00 4e 0b 40 00 00 80 11  d6 21 ac 1e 00 02 ac 1e   ·N·@···· ·!······
0020  00 ff 00 89 00 89 00 3a  59 89 a8 4d 01 10 00 01   ·······: Y··M····
0030  00 00 00 00 00 00 20 45  4a 46 44 45 42 46 45 45   ······ E JFDEBFEE
0040  42 46 41 43 41 43 41 43  41 43 41 43 41 43 41 43   BFACACAC ACACACAC
0050  41 43 41 43 41 41 41 00  00 20 00 01               ACACAAA· ····
```

ipsec-capture.pcapng | Packets: 487 · Displayed: 487 (100.0%) | Profile: Default

9:19 AM
2/3/2023

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


ipsec-capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh

Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-03 11:21:00
Roman Cassman

```
No.  Time        Source        Destination   Protocol Length Info
 381 57.876807   172.30.0.100  172.30.0.2    SSHv2     138 Server: Encrypted packet (len=84)
 382 57.879853   172.30.0.2    172.30.0.100  SSHv2     122 Client: Encrypted packet (len=68)
 383 57.880470   172.30.0.100  172.30.0.2    SSHv2     122 Server: Encrypted packet (len=68)
 398 77.035231   172.30.0.2    172.30.0.100  SSHv2     138 Client: Encrypted packet (len=84)
 399 77.040300   172.30.0.100  172.30.0.2    SSHv2     122 Server: Encrypted packet (len=68)
 400 77.041676   172.30.0.2    172.30.0.100  SSHv2     122 Client: Encrypted packet (len=68)
 401 77.042816   172.30.0.100  172.30.0.2    SSHv2     138 Server: Encrypted packet (len=84)
 402 77.044010   172.30.0.2    172.30.0.100  SSHv2     122 Client: Encrypted packet (len=68)
 403 77.044554   172.30.0.100  172.30.0.2    SSHv2     714 Server: Encrypted packet (len=660)
 404 77.044945   172.30.0.2    172.30.0.100  SSHv2     122 Client: Encrypted packet (len=68)
 405 77.045438   172.30.0.100  172.30.0.2    SSHv2     138 Server: Encrypted packet (len=84)
 406 77.046115   172.30.0.2    172.30.0.100  SSHv2     122 Client: Encrypted packet (len=68)
 407 77.046600   172.30.0.100  172.30.0.2    SSHv2     122 Server: Encrypted packet (len=68)
 415 94.134730   172.30.0.2    172.30.0.100  SSHv2      90 Client: Encrypted packet (len=36)
```

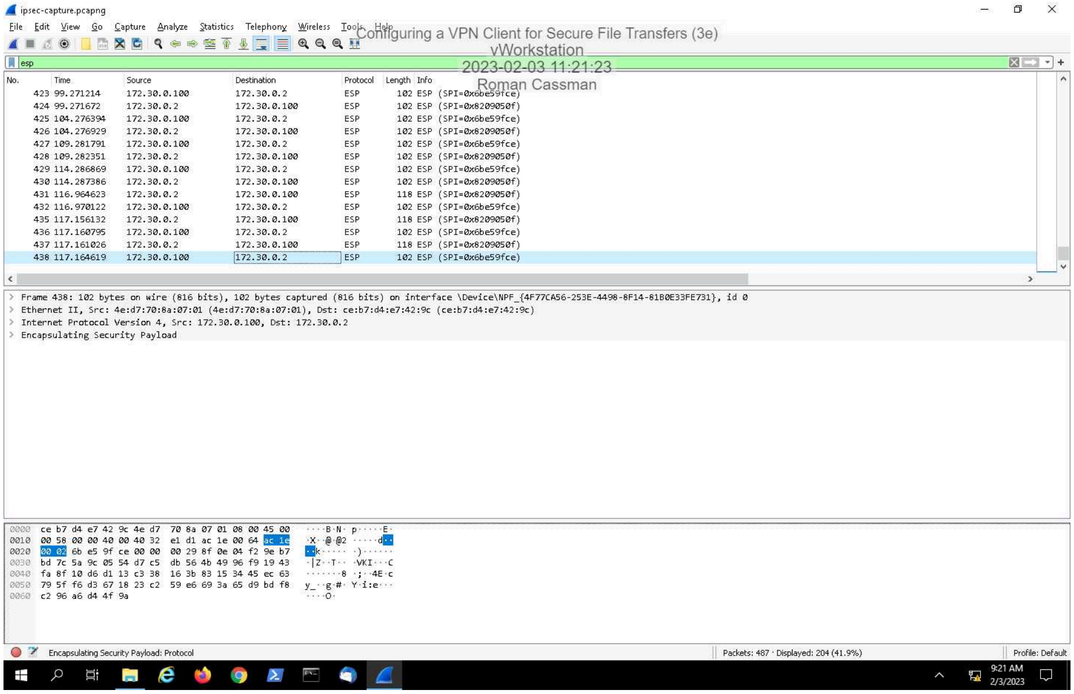
```
    Source Port: 50074
    Destination Port: 22
    [Stream index: 0]
    [TCP Segment Len: 36]
    Sequence number: 3611    (relative sequence number)
    Sequence number (raw): 3908114879
    [Next sequence number: 3647    (relative sequence number)]
    Acknowledgment number: 30069    (relative ack number)
    Acknowledgment number (raw): 2311278697
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 261
    [Calculated window size: 66816]
    [Window size scaling factor: 256]
    Checksum: 0x58e1 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  v [SEQ/ACK analysis]
```

```
0000  4e d7 70 8a 07 01 ce b7  d4 e7 42 9c 08 00 45 00   N·p····· ··B···E·
0010  00 4c 0c 73 40 00 80 06  00 00 ac 1e 00 02 ac 1e   ·L·s@··· ········
0020  00 64 c3 9a 00 16 e8 f1  19 bf 89 c3 50 69 50 18   ·d······ ····PiP·
0030  01 05 58 e1 00 00 58 b4  ef 9e 52 5c 9d 86 11 f0   ··X···X· ··R\····
0040  07 fc 95 dc b1 7d 76 ff  e2 af 09 27 b4 59 9c dc   ·····}v· ···'·Y··
0050  7b 56 c0 23 ac f8 cc 9d  a2 2d                     {V·#···· ·-
```

This frame has some of the TCP analysis shown (tcp.analysis) | Packets: 487 · Displayed: 79 (16.2%) | Profile: Default

9:20 AM
2/3/2023

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



ipsec-capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-03 11:21:23
Roman Cassman

esp

```
No.     Time        Source          Destination     Protocol  Length Info
    423 99.271214   172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    424 99.271672   172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    425 104.276394  172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    426 104.276929  172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    427 109.281791  172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    428 109.282351  172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    429 114.286869  172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    430 114.287386  172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    431 116.964623  172.30.0.2      172.30.0.100    ESP        118 ESP (SPI=0x8209050f)
    432 116.970122  172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    435 117.156132  172.30.0.2      172.30.0.100    ESP        118 ESP (SPI=0x8209050f)
    436 117.160795  172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    437 117.161026  172.30.0.2      172.30.0.100    ESP        118 ESP (SPI=0x8209050f)
    438 117.164619  172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
```

```
> Frame 438: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731}, id 0
> Ethernet II, Src: 4e:d7:70:8a:07:01 (4e:d7:70:8a:07:01), 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
> Encapsulating Security Payload
```

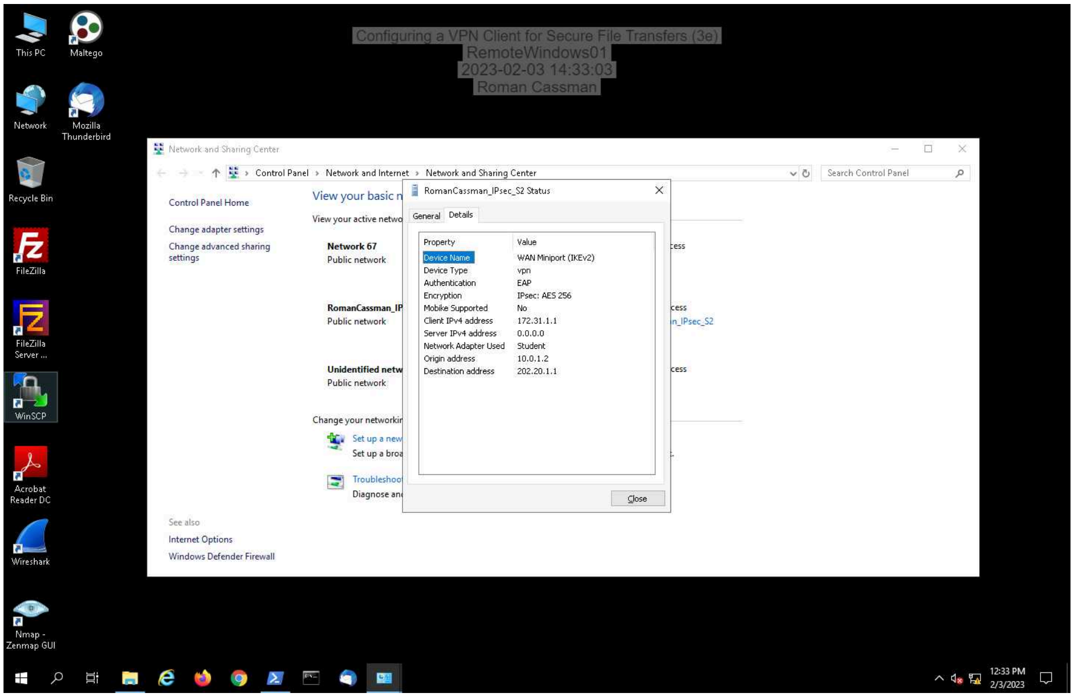
```
0000  ce b7 d4 e7 42 9c 4e d7  70 8a 07 01 08 00 45 00   ····B·N· p·····E·
0010  00 58 00 00 40 00 40 32  e1 d1 ac 1e 00 64 ac 1e   ·X··@·@2 ·····d··
0020  00 02 6b e5 9f ce 00 00  00 29 8f 0e 04 f2 9e b7   ··k····· ·)······
0030  bd 7c 5a 9c 05 54 d7 c5  db 56 4b 49 96 f9 19 43   ·|Z··T·· ·VKI···C
0040  fa 8f 10 d6 d1 13 c3 38  16 3b 83 15 34 45 ec 63   ·······8 ·;··4E·c
0050  79 5f f6 d3 67 18 23 c2  59 e6 69 3a 65 d9 bd f8   y_··g·#· Y·i:e···
0060  c2 96 a6 d4 4f 9a                                  ····O·
```

Encapsulating Security Payload: Protocol | Packets: 487 · Displayed: 204 (41.9%) | Profile: Default

Section 2: Applied Learning

Part 1: Configure a Windows VPN Client

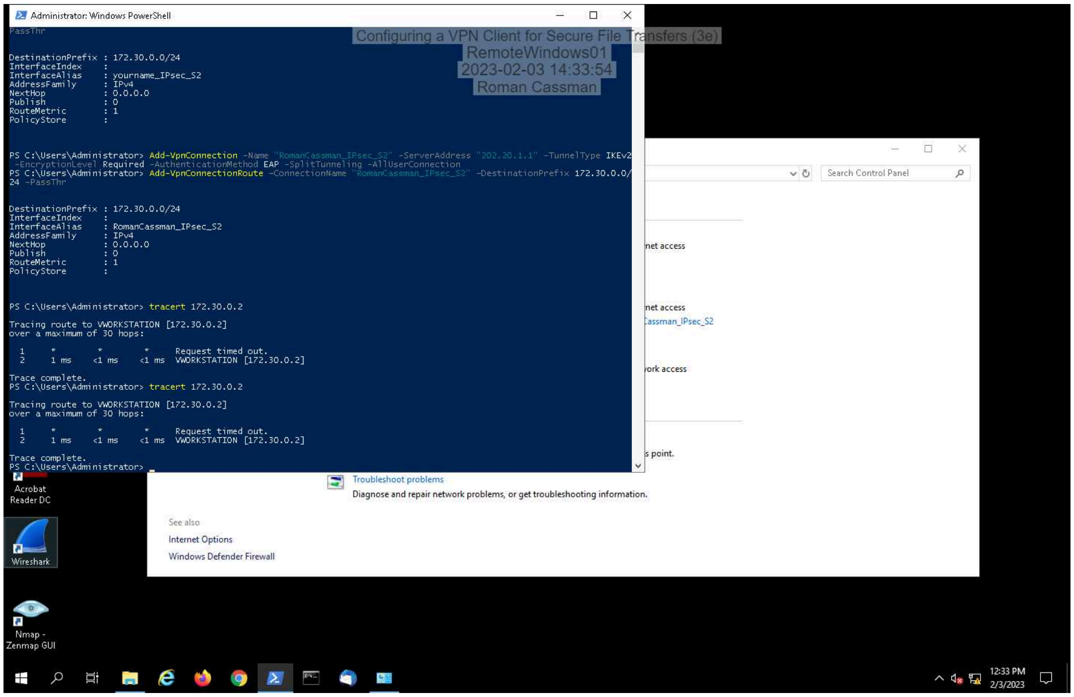
19. **Make a screen capture** showing the **IPsec VPN connection encrypted with AES 256**.



RomanCassman_IPsec_S2 Status

Property	Value
Device Name	WAN Miniport (IKEv2)
Device Type	vpn
Authentication	EAP
Encryption	IPsec: AES 256
Mobike Supported	No
Client IPv4 address	172.31.1.1
Server IPv4 address	0.0.0.0
Network Adapter Used	Student
Origin address	10.0.1.2
Destination address	202.20.1.1

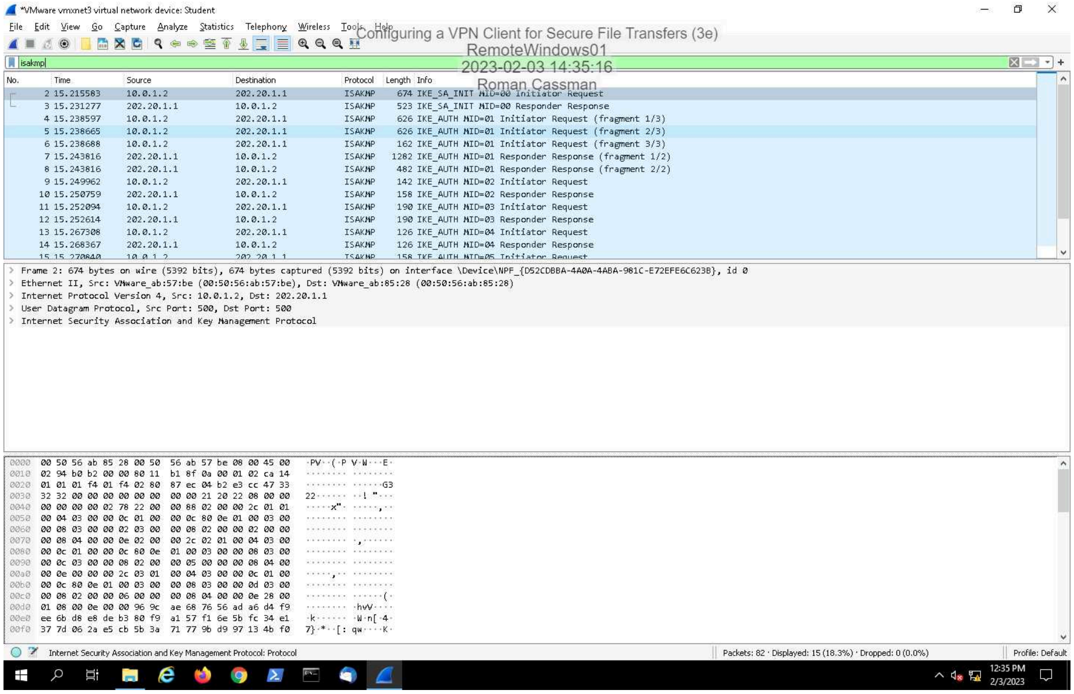
23. **Make a screen capture** showing your **successful tracert to the remote machine**.


Administrator: Windows PowerShell
Configuring a VPN Client for Secure File Transfers (3e)
RemoteWindows01
2023-02-03 14:33:54
Roman Cassman
Search Control Panel
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Defender Firewall
12:33 PM
2/3/2023

```
PassThr

DestinationPrefix : 172.30.0.0/24
InterfaceIndex    :
InterfaceAlias    : yourname_IPsec_S2
AddressFamily     : IPv4
NextHop           : 0.0.0.0
Publish           : 0
RouteMetric       : 1
PolicyStore       :


PS C:\Users\Administrator> Add-VpnConnection -Name "RomanCassman_IPsec_S2" -ServerAddress "202.20.1.1" -TunnelType IKEv2
 -EncryptionLevel Required -AuthenticationMethod EAP -SplitTunneling -AllUserConnection
PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "RomanCassman_IPsec_S2" -DestinationPrefix 172.30.0.0/
24 -PassThr


DestinationPrefix : 172.30.0.0/24
InterfaceIndex    :
InterfaceAlias    : RomanCassman_IPsec_S2
AddressFamily     : IPv4
NextHop           : 0.0.0.0
Publish           : 0
RouteMetric       : 1
PolicyStore       :


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> 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> _
```

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**.


*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
2023-02-03 14:35:16
Roman Cassman
12:35 PM
2/3/2023

Filter: isakmp

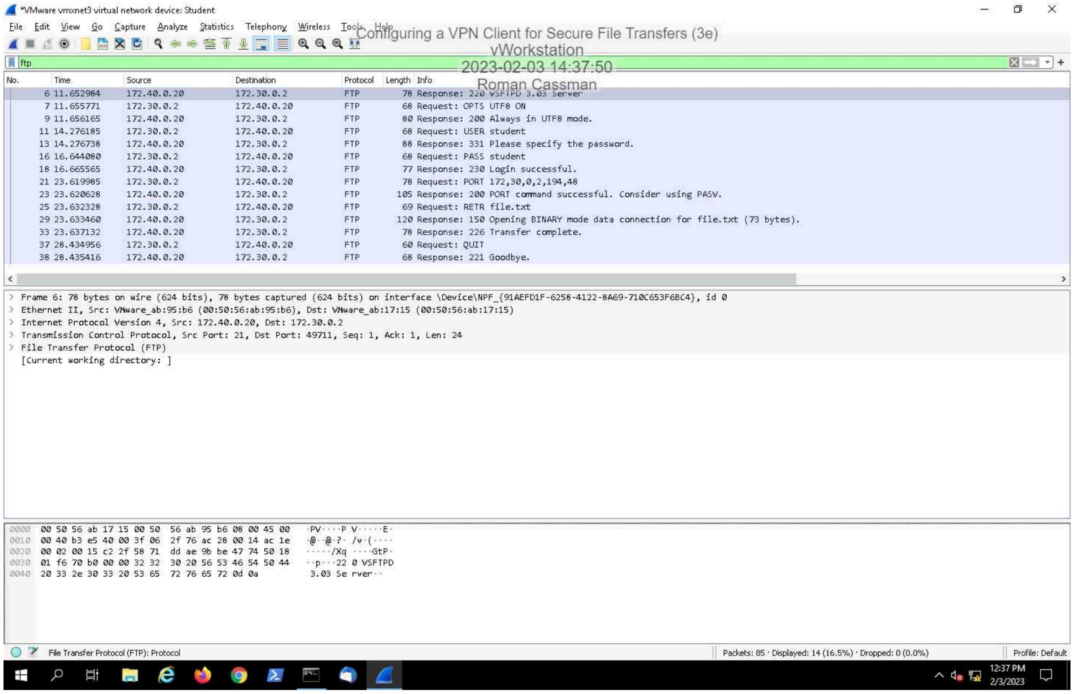
```
No.   Time       Source       Destination  Protocol Length Info
    2 15.215583  10.0.1.2     202.20.1.1   ISAKMP    674 IKE_SA_INIT MID=00 Initiator Request
    3 15.231277  202.20.1.1   10.0.1.2     ISAKMP    523 IKE_SA_INIT MID=00 Responder Response
    4 15.238597  10.0.1.2     202.20.1.1   ISAKMP    626 IKE_AUTH MID=01 Initiator Request (fragment 1/3)
    5 15.238665  10.0.1.2     202.20.1.1   ISAKMP    626 IKE_AUTH MID=01 Initiator Request (fragment 2/3)
    6 15.238688  10.0.1.2     202.20.1.1   ISAKMP    162 IKE_AUTH MID=01 Initiator Request (fragment 3/3)
    7 15.243816  202.20.1.1   10.0.1.2     ISAKMP   1282 IKE_AUTH MID=01 Responder Response (fragment 1/2)
    8 15.243816  202.20.1.1   10.0.1.2     ISAKMP    482 IKE_AUTH MID=01 Responder Response (fragment 2/2)
    9 15.249962  10.0.1.2     202.20.1.1   ISAKMP    142 IKE_AUTH MID=02 Initiator Request
   10 15.250759  202.20.1.1   10.0.1.2     ISAKMP    158 IKE_AUTH MID=02 Responder Response
   11 15.252094  10.0.1.2     202.20.1.1   ISAKMP    190 IKE_AUTH MID=03 Initiator Request
   12 15.252614  202.20.1.1   10.0.1.2     ISAKMP    190 IKE_AUTH MID=03 Responder Response
   13 15.267308  10.0.1.2     202.20.1.1   ISAKMP    126 IKE_AUTH MID=04 Initiator Request
   14 15.268367  202.20.1.1   10.0.1.2     ISAKMP    126 IKE_AUTH MID=04 Responder Response
   15 15.270840  10.0.1.2     202.20.1.1   ISAKMP    158 IKE_AUTH MID=05 Initiator Request
```

```
> Frame 2: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits) on interface \Device\NPF_{D52CDBBA-4A0A-4ABA-981C-E72EFE6C623B}, id 0
> Ethernet II, Src: VMware_ab:57:be (00:50:56:ab:57:be), Dst: VMware_ab:85:28 (00:50:56:ab:85:28)
> 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 ab 85 28 00 50  56 ab 57 be 08 00 45 00   ·PV··(·P V·W···E·
0010  02 94 b0 b2 00 00 80 11  b1 8f 0a 00 01 02 ca 14   ········ ········
0020  01 01 01 f4 01 f4 02 80  87 ec 04 b2 e3 cc 47 33   ········ ······G3
0030  32 32 00 00 00 00 00 00  00 00 21 20 22 08 00 00   22······ ··! "···
0040  00 00 00 00 02 78 22 00  00 88 02 00 00 2c 01 01   ·····x"· ·····,··
0050  00 04 03 00 00 0c 01 00  00 0c 80 0e 01 00 03 00   ········ ········
0060  00 08 03 00 00 02 03 00  00 08 02 00 00 02 00 00   ········ ········
0070  00 08 04 00 00 0e 02 00  00 2c 02 01 00 04 03 00   ········ ·,······
0080  00 0c 01 00 00 0c 80 0e  01 00 03 00 00 08 03 00   ········ ········
0090  00 0c 03 00 00 08 02 00  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 08 02 00 00 06 00 00  00 08 04 00 00 0e 28 00   ········ ······(·
00d0  01 08 00 0e 00 00 96 9c  ae 68 76 56 ad a6 d4 f9   ········ ·hvV····
00e0  ee 6b d8 e8 de b3 80 f9  a1 57 f1 6e 5b fc 34 e1   ·k······ ·W·n[·4·
00f0  37 7d 06 2a e5 cb 5b 3a  71 77 9b d9 97 13 4b f0   7}·*··[: qw····K·
```

Internet Security Association and Key Management Protocol: Protocol | Packets: 82 · Displayed: 15 (18.3%) · Dropped: 0 (0.0%) | Profile: Default

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


*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)
vWorkstation
2023-02-03 14:37:50
Roman Cassman
12:37 PM
2/3/2023

Filter: ftp

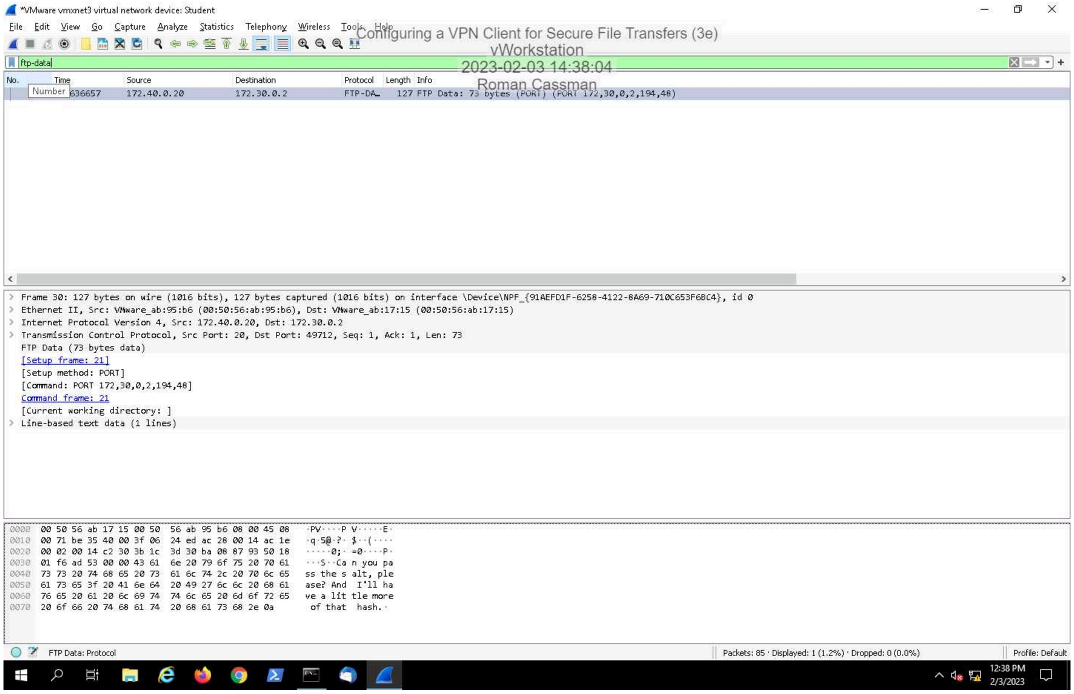
```
No.   Time       Source       Destination  Protocol Length Info
    6 11.652984  172.40.0.20  172.30.0.2   FTP       78 Response: 220 VSFTPD 3.03 Server
    7 11.655771  172.30.0.2   172.40.0.20  FTP       68 Request: OPTS UTF8 ON
    9 11.656165  172.40.0.20  172.30.0.2   FTP       80 Response: 200 Always in UTF8 mode.
   11 14.276185  172.30.0.2   172.40.0.20  FTP       68 Request: USER student
   13 14.276738  172.40.0.20  172.30.0.2   FTP       88 Response: 331 Please specify the password.
   16 16.644080  172.30.0.2   172.40.0.20  FTP       68 Request: PASS student
   18 16.665565  172.40.0.20  172.30.0.2   FTP       77 Response: 230 Login successful.
   21 23.619985  172.30.0.2   172.40.0.20  FTP       78 Request: PORT 172,30,0,2,194,48
   23 23.620628  172.40.0.20  172.30.0.2   FTP      105 Response: 200 PORT command successful. Consider using PASV.
   25 23.632328  172.30.0.2   172.40.0.20  FTP       69 Request: RETR file.txt
   29 23.633460  172.40.0.20  172.30.0.2   FTP      120 Response: 150 Opening BINARY mode data connection for file.txt (73 bytes).
   33 23.637132  172.40.0.20  172.30.0.2   FTP       78 Response: 226 Transfer complete.
   37 28.434956  172.30.0.2   172.40.0.20  FTP       60 Request: QUIT
   38 28.435416  172.40.0.20  172.30.0.2   FTP       68 Response: 221 Goodbye.
```

```
> Frame 6: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{91AEFD1F-6258-4122-8A69-710C653F6BC4}, id 0
> Ethernet II, Src: VMware_ab:95:b6 (00:50:56:ab:95:b6), Dst: VMware_ab:17:15 (00:50:56:ab:17:15)
> Internet Protocol Version 4, Src: 172.40.0.20, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 49711, Seq: 1, Ack: 1, Len: 24
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 50 56 ab 17 15 00 50  56 ab 95 b6 08 00 45 00   ·PV····P V·····E·
0010  00 40 b3 e5 40 00 3f 06  2f 76 ac 28 00 14 ac 1e   ·@··@·?· /v·(····
0020  00 02 00 15 c2 2f 58 71  dd ae 9b be 47 74 50 18   ·····/Xq ····GtP·
0030  01 f6 70 b0 00 00 32 32  30 20 56 53 46 54 50 44   ··p···22 0 VSFTPD
0040  20 33 2e 30 33 20 53 65  72 76 65 72 0d 0a          3.03 Se rver··
```

File Transfer Protocol (FTP): Protocol | Packets: 85 · Displayed: 14 (16.5%) · Dropped: 0 (0.0%) | Profile: Default

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


*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)
vWorkstation
2023-02-03 14:38:04
Roman Cassman
Number
FTP Data: Protocol
Profile: Default
12:38 PM
2/3/2023

ftp-data

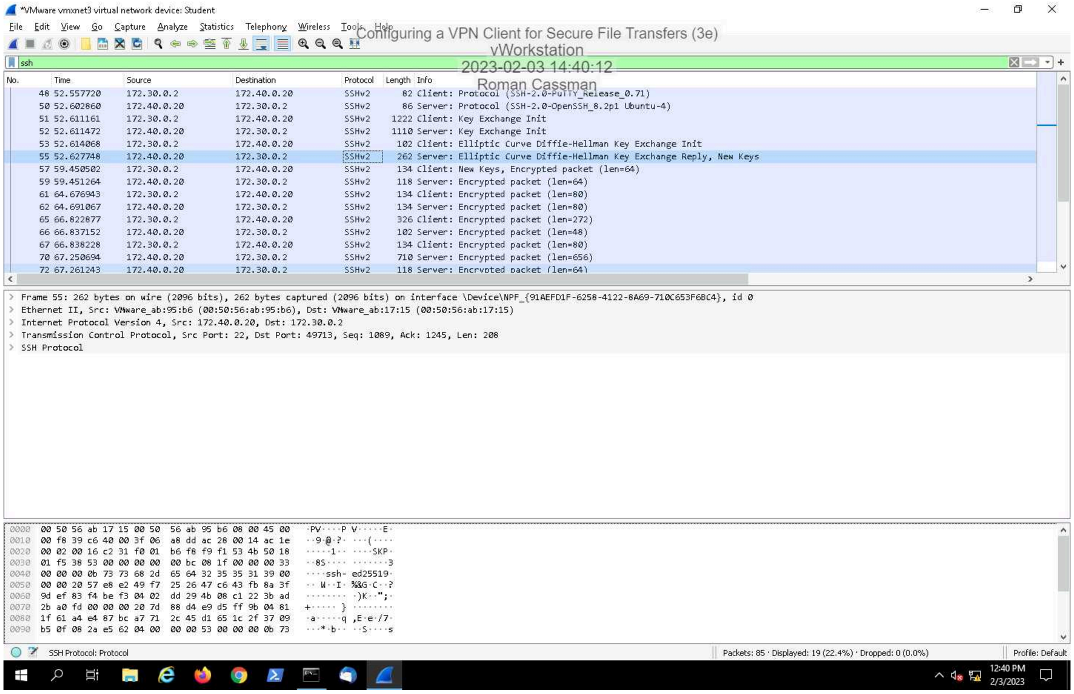
```
No.     Time          Source        Destination   Protocol  Length Info
        636657        172.40.0.20   172.30.0.2    FTP-DA…      127 FTP Data: 73 bytes (PORT) (PORT 172,30,0,2,194,48)
```

```
> Frame 30: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on interface \Device\NPF_{91AEFD1F-6258-4122-8A69-710C653F6BC4}, id 0
> Ethernet II, Src: VMware_ab:95:b6 (00:50:56:ab:95:b6), Dst: VMware_ab:17:15 (00:50:56:ab:17:15)
> Internet Protocol Version 4, Src: 172.40.0.20, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 20, Dst Port: 49712, Seq: 1, Ack: 1, Len: 73
  FTP Data (73 bytes data)
  [Setup frame: 21]
  [Setup method: PORT]
  [Command: PORT 172,30,0,2,194,48]
  Command frame: 21
  [Current working directory: ]
> Line-based text data (1 lines)
```

```
0000  00 50 56 ab 17 15 00 50  56 ab 95 b6 08 00 45 08   ·PV····P V·····E·
0010  00 71 be 35 40 00 3f 06  24 ed ac 28 00 14 ac 1e   ·q·5@·?· $··(····
0020  00 02 00 14 c2 30 3b 1c  3d 30 ba 08 87 93 50 18   ·····0;· =0····P·
0030  01 f6 ad 53 00 00 43 61  6e 20 79 6f 75 20 70 61   ···S··Ca n you pa
0040  73 73 20 74 68 65 20 73  61 6c 74 2c 20 70 6c 65   ss the s alt, ple
0050  61 73 65 3f 20 41 6e 64  20 49 27 6c 6c 20 68 61   ase? And  I'll ha
0060  76 65 20 61 20 6c 69 74  74 6c 65 20 6d 6f 72 65   ve a lit tle more
0070  20 6f 66 20 74 68 61 74  20 68 61 73 68 2e 0a       of that  hash.·
```

Packets: 85 · Displayed: 1 (1.2%) · Dropped: 0 (0.0%)

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


*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)
vWorkstation
2023-02-03 14:40:12
Roman Cassman
SSH Protocol: Protocol
Profile: Default
12:40 PM
2/3/2023

ssh

```
No.  Time       Source        Destination   Protocol  Length Info
  48 52.557720  172.30.0.2    172.40.0.20   SSHv2         82 Client: Protocol (SSH-2.0-PuTTY_Release_0.71)
  50 52.602860  172.40.0.20   172.30.0.2    SSHv2         86 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4)
  51 52.611161  172.30.0.2    172.40.0.20   SSHv2       1222 Client: Key Exchange Init
  52 52.611472  172.40.0.20   172.30.0.2    SSHv2       1110 Server: Key Exchange Init
  53 52.614068  172.30.0.2    172.40.0.20   SSHv2        102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
  55 52.627748  172.40.0.20   172.30.0.2    SSHv2        262 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
  57 59.450502  172.30.0.2    172.40.0.20   SSHv2        134 Client: New Keys, Encrypted packet (len=64)
  59 59.451264  172.40.0.20   172.30.0.2    SSHv2        118 Server: Encrypted packet (len=64)
  61 64.676943  172.30.0.2    172.40.0.20   SSHv2        134 Client: Encrypted packet (len=80)
  62 64.691067  172.40.0.20   172.30.0.2    SSHv2        134 Server: Encrypted packet (len=80)
  65 66.822877  172.30.0.2    172.40.0.20   SSHv2        326 Client: Encrypted packet (len=272)
  66 66.837152  172.40.0.20   172.30.0.2    SSHv2        102 Server: Encrypted packet (len=48)
  67 66.838228  172.30.0.2    172.40.0.20   SSHv2        134 Client: Encrypted packet (len=80)
  70 67.250694  172.40.0.20   172.30.0.2    SSHv2        710 Server: Encrypted packet (len=656)
  72 67.261243  172.40.0.20   172.30.0.2    SSHv2        118 Server: Encrypted packet (len=64)
```

```
> Frame 55: 262 bytes on wire (2096 bits), 262 bytes captured (2096 bits) on interface \Device\NPF_{91AEFD1F-6258-4122-8A69-710C653F6BC4}, id 0
> Ethernet II, Src: VMware_ab:95:b6 (00:50:56:ab:95:b6), Dst: VMware_ab:17:15 (00:50:56:ab:17:15)
> Internet Protocol Version 4, Src: 172.40.0.20, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 22, Dst Port: 49713, Seq: 1089, Ack: 1245, Len: 208
> SSH Protocol
```

```
0000  00 50 56 ab 17 15 00 50  56 ab 95 b6 08 00 45 00   ·PV····P V·····E·
0010  00 f8 39 c6 40 00 3f 06  a8 dd ac 28 00 14 ac 1e   ··9·@·?· ···(····
0020  00 02 00 16 c2 31 f0 01  b6 f8 f9 f1 53 4b 50 18   ·····1·· ····SKP·
0030  01 f5 38 53 00 00 00 00  00 bc 08 1f 00 00 00 33   ··8S···· ·······3
0040  00 00 00 0b 73 73 68 2d  65 64 32 35 35 31 39 00   ····ssh- ed25519·
0050  00 00 20 57 e8 e2 49 f7  25 26 47 c6 43 fb 8a 3f   ·· W··I· %&G·C··?
0060  9d ef 83 f4 be f3 04 02  dd 29 4b 08 c1 22 3b ad   ········ ·)K··";·
0070  2b a0 fd 00 00 00 20 7d  88 d4 e9 d5 ff 9b 04 81   +····· } ········
0080  1f 61 a4 e4 87 bc a7 71  2c 45 d1 65 1c 2f 37 09   ·a·····q ,E·e·/7·
0090  b5 0f 08 2a e5 62 04 00  00 00 53 00 00 00 0b 73   ···*·b·· ··S····s
```

Packets: 85 · Displayed: 19 (22.4%) · Dropped: 0 (0.0%)

Section 3: Challenge and Analysis

Part 1: Create a New VPN Connection using PowerShell

Document the **command you used to add your VPN connection**.

Incomplete

Part 2: Implement a Custom IPsec Policy

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

Incomplete

Part 3: Verify Your VPN Implementation using Wireshark

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

Incomplete

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

Incomplete