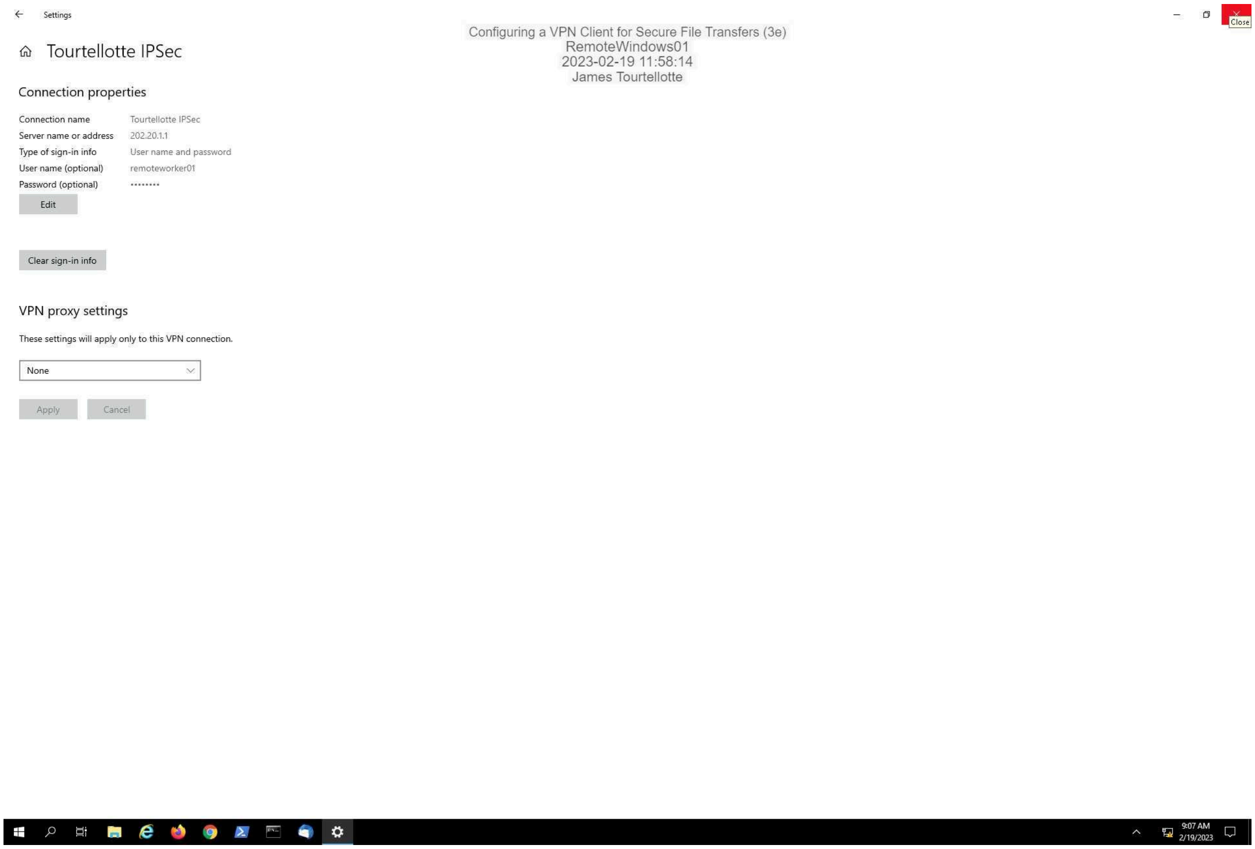
James Everett Tourtellotte IV
ITN 263
2/27/2023

New Lab 09: Configuring a VPN Client for Secure File Transfer

Lab #9 Screen Captures

Screen Capture 1, Section 1:



Configuring a VPN Client for Secure File Transfers (3e)
RemoteWindows01
2023-02-19 11:58:14
James Tourtellotte

Tourtellotte IPSec

Connection properties

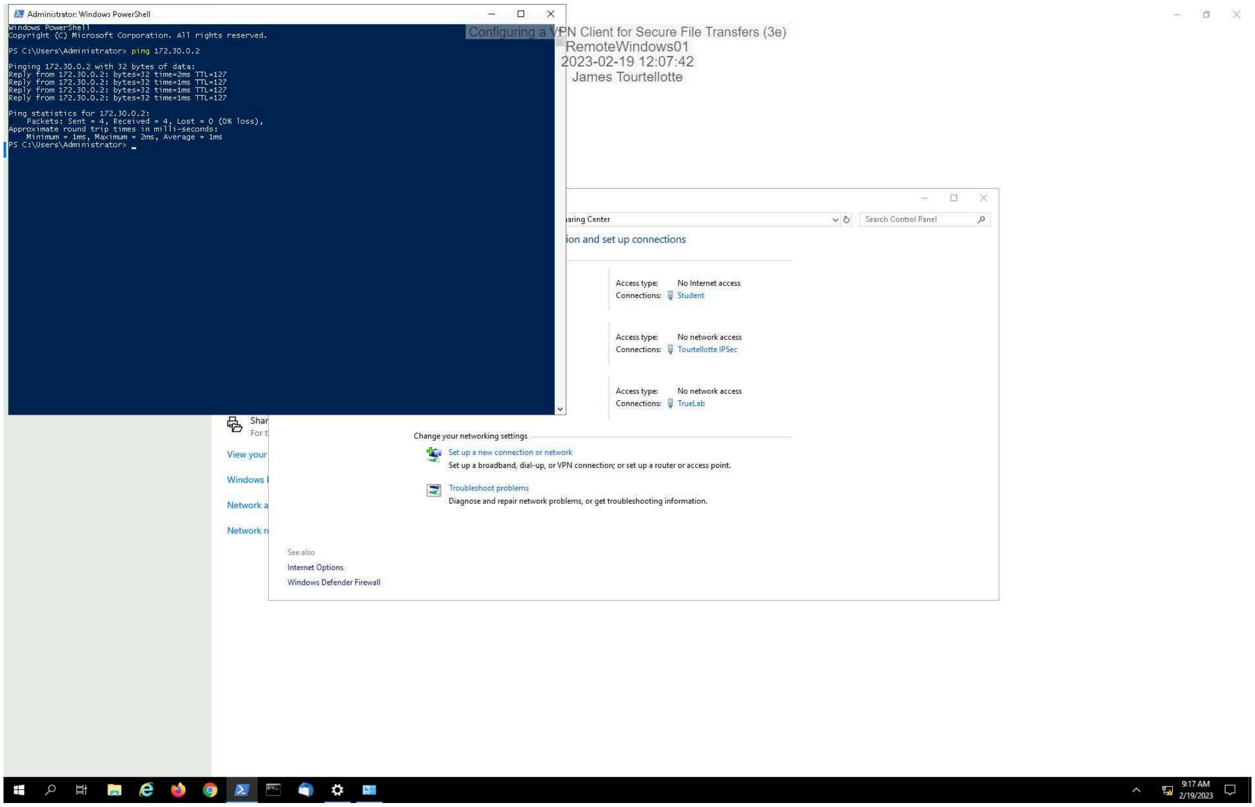
Connection name: Tourtellotte IPSec
Server name or address: 202.20.1.1
Type of sign-in info: User name and password
User name (optional): remoteworker01
Password (optional): ••••••••

VPN proxy settings

These settings will apply only to this VPN connection.

None

Screen Capture 2, Section 1:



Administrator: Windows PowerShell

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

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=2ms 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 = 2ms, Average = 1ms
PS C:\Users\Administrator> _
```

Configuring a VPN Client for Secure File Transfers (3e)
RemoteWindows01
2023-02-19 12:07:42
James Tourtellotte

Access type: No Internet access
Connections: Student

Access type: No network access
Connections: Tourtellotte IPSec

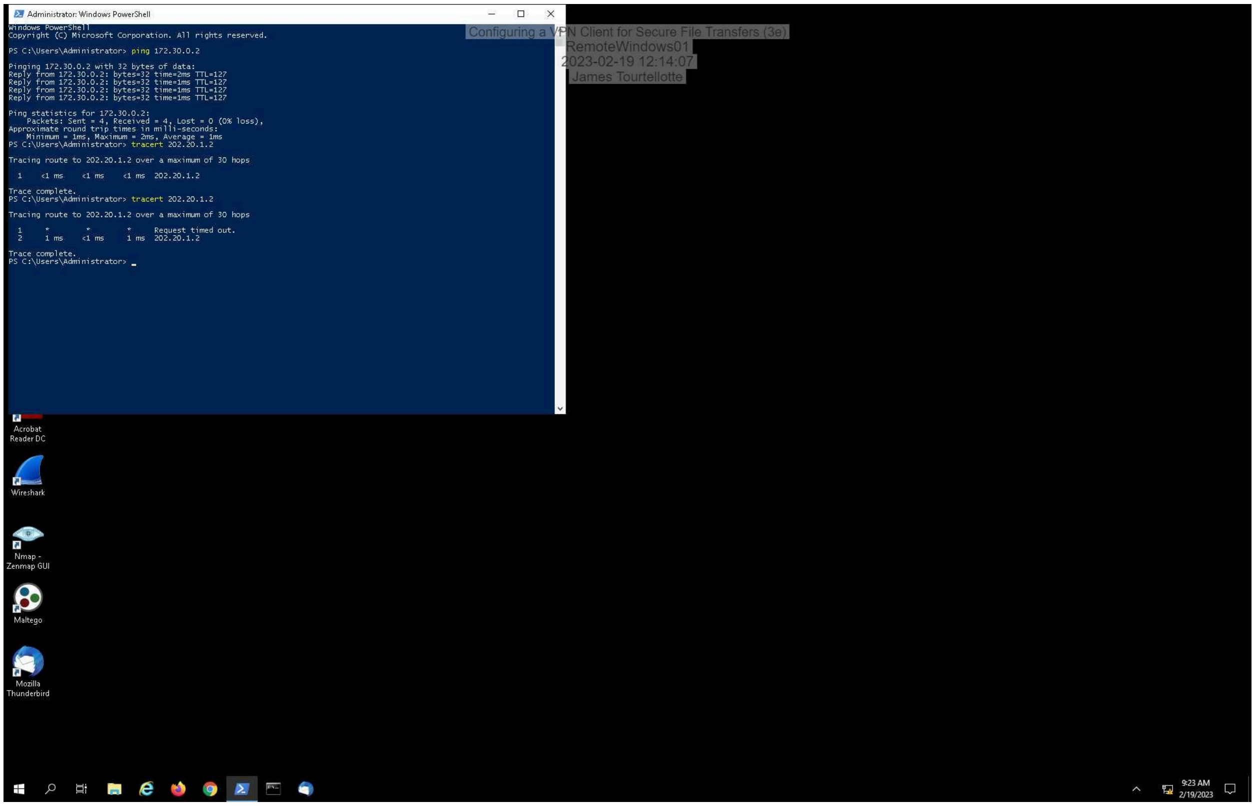
Access type: No network access
Connections: TrueLab

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

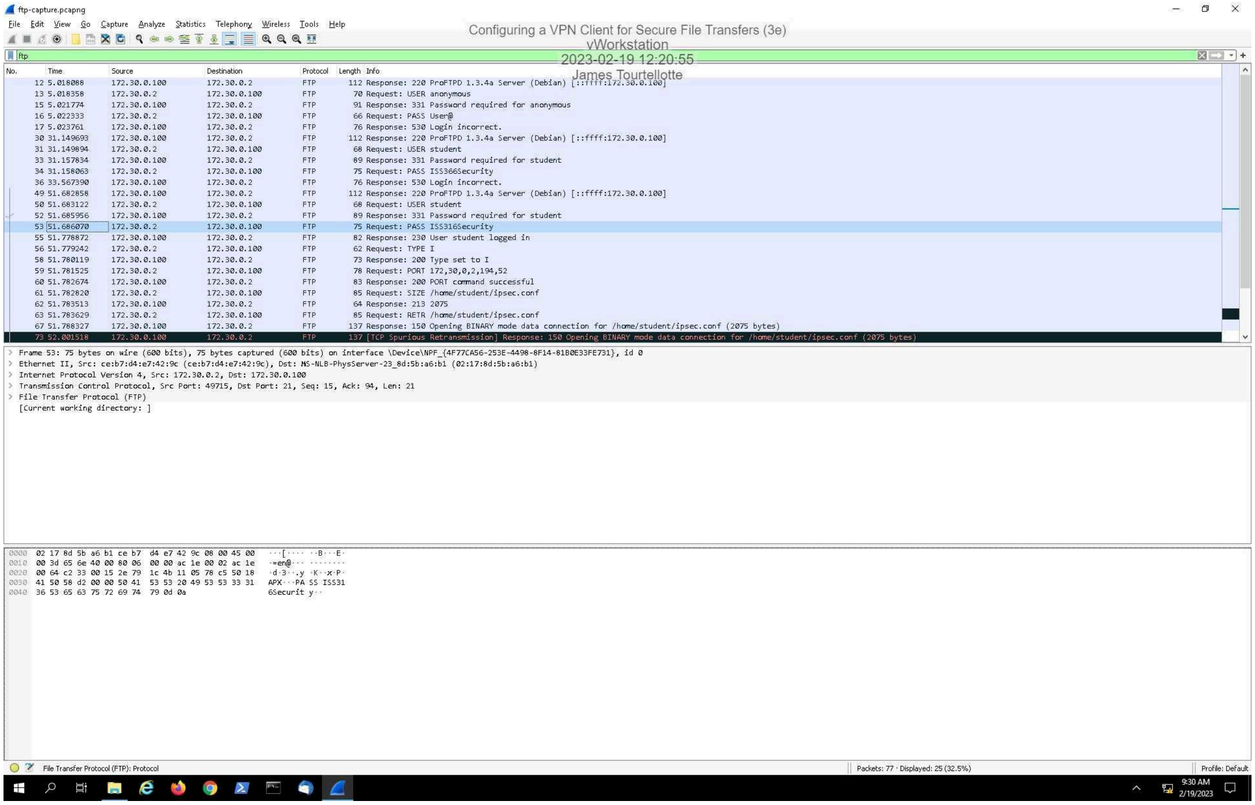
Screen Capture 3, Section 1:



Configuring a VPN Client for Secure File Transfers (3e)
RemoteWindows01
2023-02-19 12:14:07
James Tourtellotte

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

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=2ms 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 = 2ms, 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> _
```

Screen Capture 4, Section 1:


ftp-capture.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ftp
File Transfer Protocol (FTP): Protocol
Packets: 77 · Displayed: 25 (32.5%)
Profile: Default
9:30 AM
2/19/2023

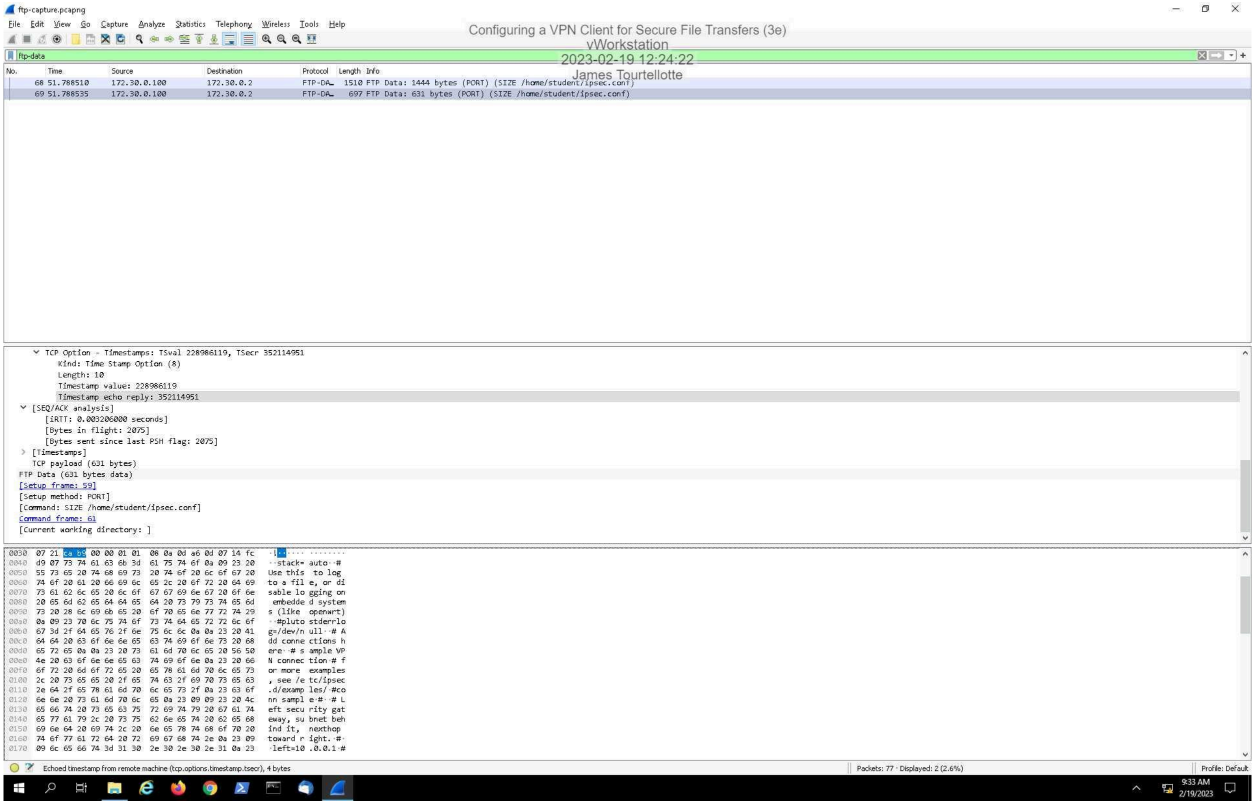
Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-19 12:20:55
James Tourtellotte

```
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)
  73 52.001518  172.30.0.100  172.30.0.2    FTP       137 [TCP Spurious Retransmission] 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·
0010  00 3d 65 6e 40 00 80 06  00 00 ac 1e 00 02 ac 1e   ·=en@··· ········
0020  00 64 c2 33 00 15 2e 79  1c 4b 11 05 78 c5 50 18   ·d·3··.y ·K··x·P·
0030  41 50 58 d2 00 00 50 41  53 53 20 49 53 53 33 31   APX···PA SS ISS31
0040  36 53 65 63 75 72 69 74  79 0d 0a                  6Securit y··
```

Screen Capture 5, Section 1:



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

Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-19 12:24:22
James Tourtellotte

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)
```

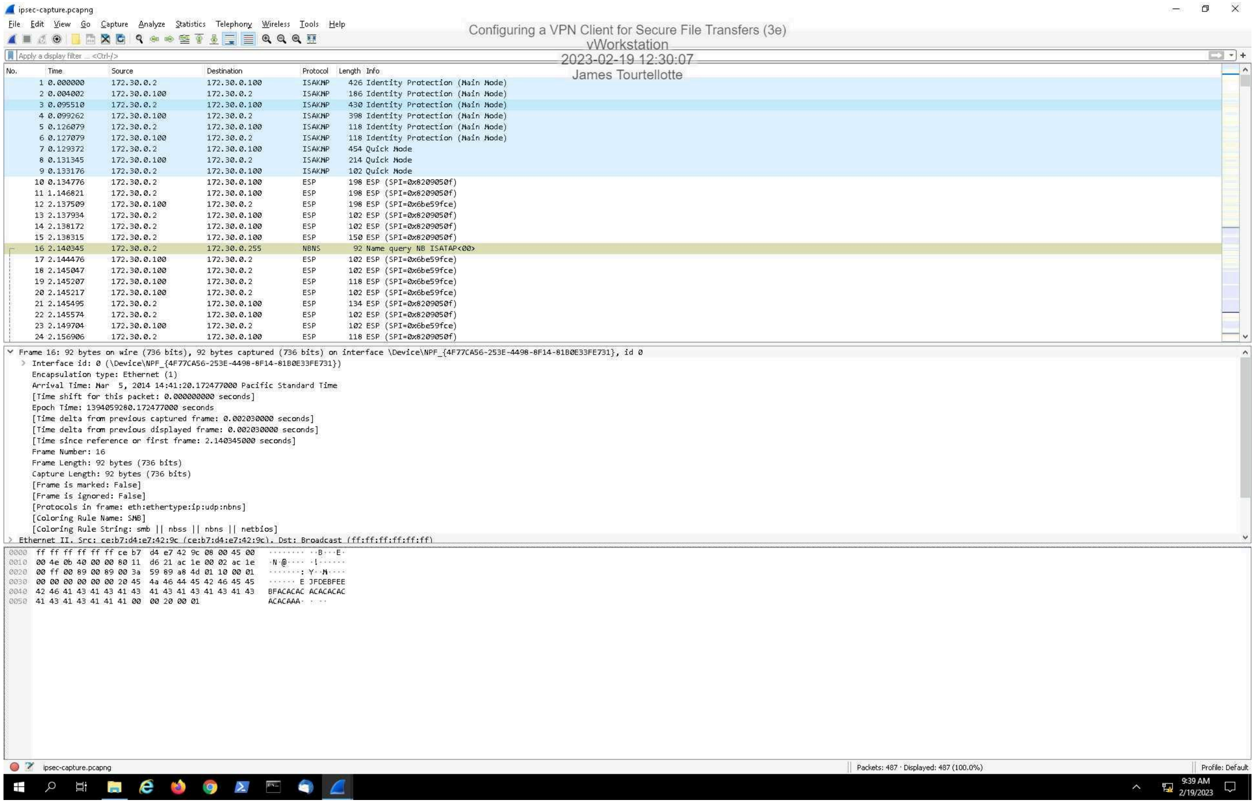
```
    ˅ TCP Option - Timestamps: TSval 228986119, TSecr 352114951
          Kind: Time Stamp Option (8)
          Length: 10
          Timestamp value: 228986119
          Timestamp echo reply: 352114951
  ˅ [SEQ/ACK analysis]
      [iRTT: 0.003206000 seconds]
      [Bytes in flight: 2075]
      [Bytes 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: ]
```

```
0030  07 21 ca b9 00 00 01 01  08 0a 0d a6 0d 07 14 fc   ·!······ ········
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
00e0  4e 20 63 6f 6e 6e 65 63  74 69 6f 6e 0a 23 20 66   N connec tion·# f
00f0  6f 72 20 6d 6f 72 65 20  65 78 61 6d 70 6c 65 73   or more  examples
0100  2c 20 73 65 65 20 2f 65  74 63 2f 69 70 73 65 63   , see /e tc/ipsec
0110  2e 64 2f 65 78 61 6d 70  6c 65 73 2f 0a 23 63 6f   .d/examp les/·#co
0120  6e 6e 20 73 61 6d 70 6c  65 0a 23 09 09 23 20 4c   nn sampl e·#··# L
0130  65 66 74 20 73 65 63 75  72 69 74 79 20 67 61 74   eft secu rity gat
0140  65 77 61 79 2c 20 73 75  62 6e 65 74 20 62 65 68   eway, su bnet beh
0150  69 6e 64 20 69 74 2c 20  6e 65 78 74 68 6f 70 20   ind it,  nexthop 
0160  74 6f 77 61 72 64 20 72  69 67 68 74 2e 0a 23 09   toward r ight.·#·
0170  09 6c 65 66 74 3d 31 30  2e 30 2e 30 2e 31 0a 23   ·left=10 .0.0.1·#
```

Echoed timestamp from remote machine (tcp.options.timestamp.tsecr), 4 bytes

Packets: 77 · Displayed: 2 (2.6%)

Screen Capture 6, Section 1:


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

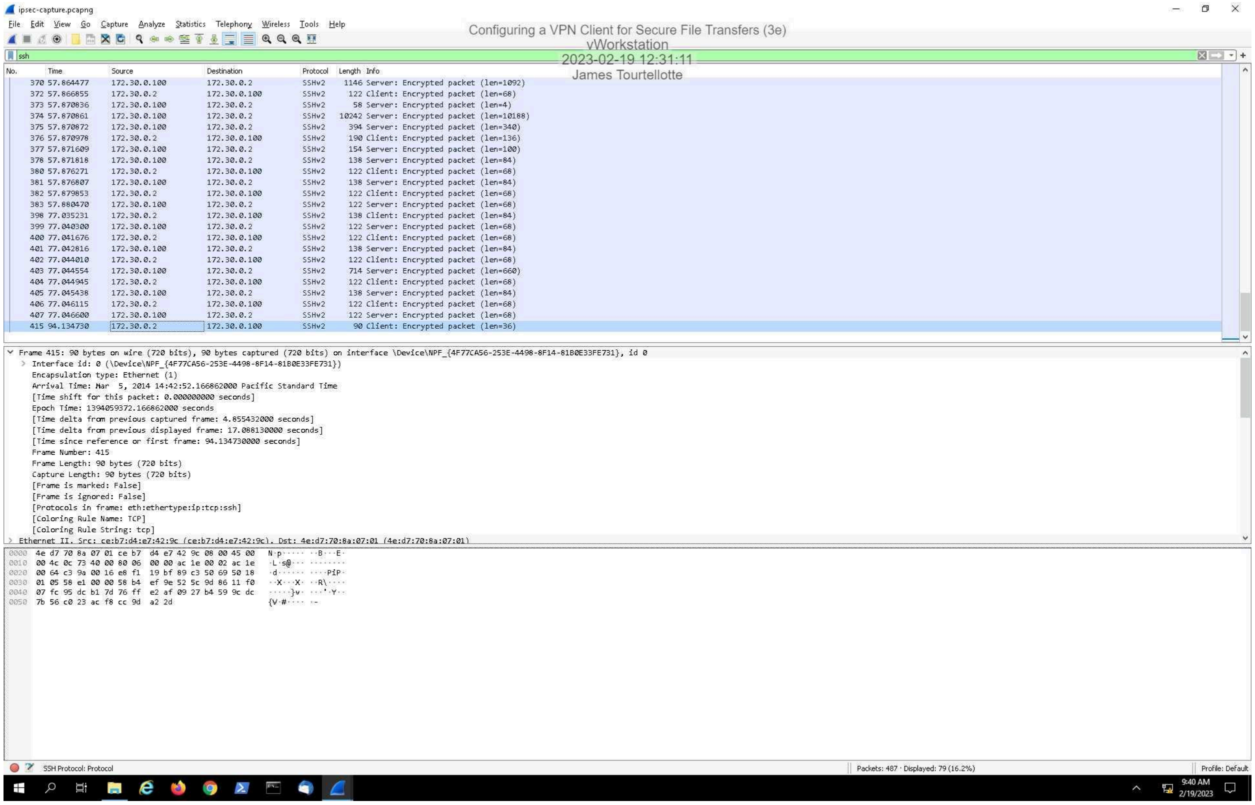
Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-19 12:30:07
James Tourtellotte

```
No.   Time      Source        Destination   Protocol Length Info
    1 0.000000  172.30.0.2    172.30.0.100  ISAKMP    426 Identity Protection (Main Mode)
    2 0.004002  172.30.0.100  172.30.0.2    ISAKMP    186 Identity Protection (Main Mode)
    3 0.095510  172.30.0.2    172.30.0.100  ISAKMP    430 Identity Protection (Main Mode)
    4 0.099262  172.30.0.100  172.30.0.2    ISAKMP    398 Identity Protection (Main Mode)
    5 0.126079  172.30.0.2    172.30.0.100  ISAKMP    118 Identity Protection (Main Mode)
    6 0.127079  172.30.0.100  172.30.0.2    ISAKMP    118 Identity Protection (Main Mode)
    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)
   22 2.145574  172.30.0.2    172.30.0.100  ESP       102 ESP (SPI=0x8209050f)
   23 2.149704  172.30.0.100  172.30.0.2    ESP       102 ESP (SPI=0x6be59fce)
   24 2.156906  172.30.0.2    172.30.0.100  ESP       118 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
  > Interface id: 0 (\Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  5, 2014 14:41:20.172477000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1394059280.172477000 seconds
    [Time delta from previous captured frame: 0.002030000 seconds]
    [Time delta from previous displayed frame: 0.002030000 seconds]
    [Time since reference or first frame: 2.140345000 seconds]
    Frame Number: 16
    Frame Length: 92 bytes (736 bits)
    Capture Length: 92 bytes (736 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:nbns]
    [Coloring Rule Name: SMB]
    [Coloring Rule String: smb || nbss || nbns || netbios]
> Ethernet II, Src: ce:b7:d4:e7:42:9c (ce:b7:d4:e7:42:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
```

```
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· · ··
```

Screen Capture 7, Section 1:


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

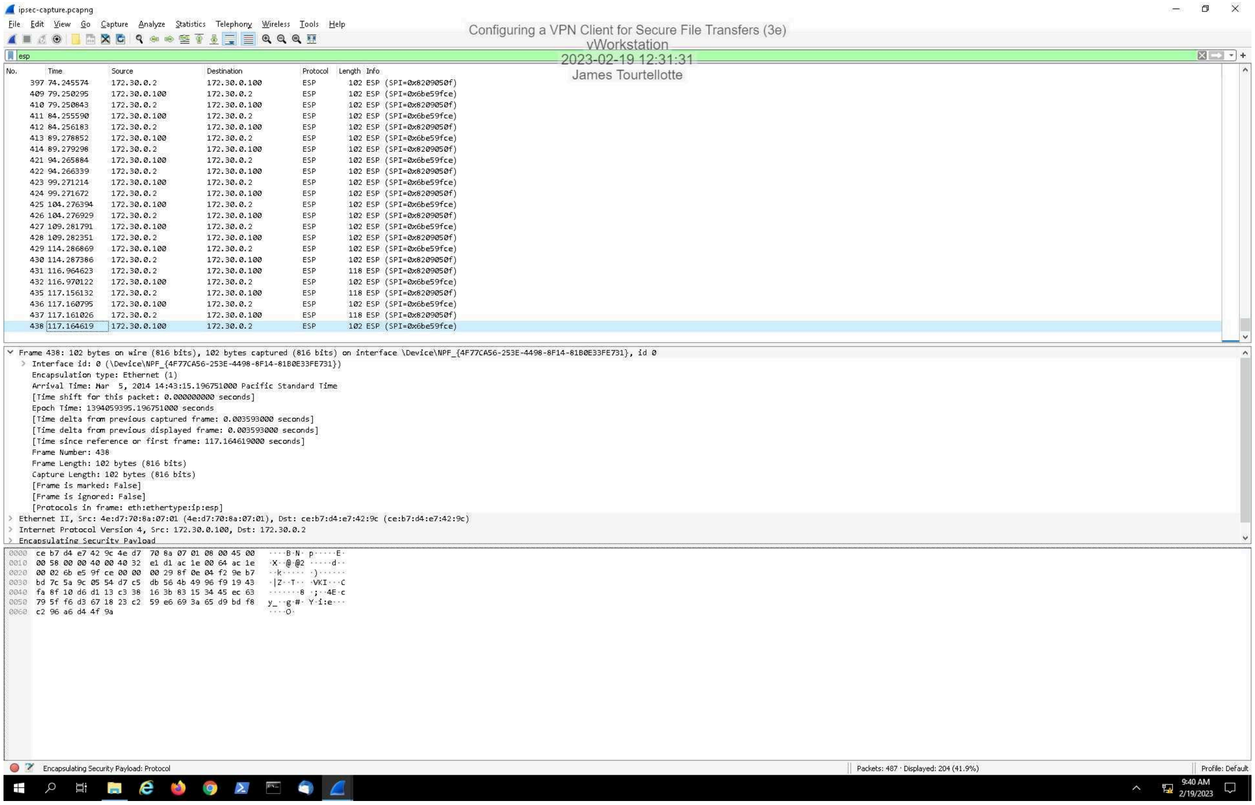
Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-19 12:31:11
James Tourtellotte

```
No.   Time       Source        Destination   Protocol Length Info
  370 57.864477  172.30.0.100  172.30.0.2    SSHv2    1146 Server: Encrypted packet (len=1092)
  372 57.866855  172.30.0.2    172.30.0.100  SSHv2     122 Client: Encrypted packet (len=68)
  373 57.870836  172.30.0.100  172.30.0.2    SSHv2      58 Server: Encrypted packet (len=4)
  374 57.870861  172.30.0.100  172.30.0.2    SSHv2   10242 Server: Encrypted packet (len=10188)
  375 57.870872  172.30.0.100  172.30.0.2    SSHv2     394 Server: Encrypted packet (len=340)
  376 57.870978  172.30.0.2    172.30.0.100  SSHv2     190 Client: Encrypted packet (len=136)
  377 57.871609  172.30.0.100  172.30.0.2    SSHv2     154 Server: Encrypted packet (len=100)
  378 57.871818  172.30.0.100  172.30.0.2    SSHv2     138 Server: Encrypted packet (len=84)
  380 57.876271  172.30.0.2    172.30.0.100  SSHv2     122 Client: Encrypted packet (len=68)
  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)
```

```
Frame 415: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface \Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731}, id 0
  > Interface id: 0 (\Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  5, 2014 14:42:52.166862000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1394059372.166862000 seconds
    [Time delta from previous captured frame: 4.855432000 seconds]
    [Time delta from previous displayed frame: 17.088130000 seconds]
    [Time since reference or first frame: 94.134730000 seconds]
    Frame Number: 415
    Frame Length: 90 bytes (720 bits)
    Capture Length: 90 bytes (720 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:tcp:ssh]
    [Coloring Rule Name: TCP]
    [Coloring Rule String: tcp]
> Ethernet II, Src: ce:b7:d4:e7:42:9c (ce:b7:d4:e7:42:9c), Dst: 4e:d7:70:8a:07:01 (4e:d7:70:8a:07:01)
```

```
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·#···· ·-
```

Screen Capture 8, Section 1:



Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-19 12:31:31
James Tourtellotte

esp

```
No.     Time        Source          Destination     Protocol  Length  Info
    397 74.245574   172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    409 79.250295   172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    410 79.250843   172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    411 84.255590   172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    412 84.256183   172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    413 89.278852   172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    414 89.279298   172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    421 94.265884   172.30.0.100    172.30.0.2      ESP        102 ESP (SPI=0x6be59fce)
    422 94.266339   172.30.0.2      172.30.0.100    ESP        102 ESP (SPI=0x8209050f)
    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)
```

```
v Frame 438: 102 bytes on wire (816 bits), 102 bytes captured (816 bits) on interface \Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731}, id 0
  > Interface id: 0 (\Device\NPF_{4F77CA56-253E-4498-8F14-81B0E33FE731})
    Encapsulation type: Ethernet (1)
    Arrival Time: Mar  5, 2014 14:43:15.196751000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1394059395.196751000 seconds
    [Time delta from previous captured frame: 0.003593000 seconds]
    [Time delta from previous displayed frame: 0.003593000 seconds]
    [Time since reference or first frame: 117.164619000 seconds]
    Frame Number: 438
    Frame Length: 102 bytes (816 bits)
    Capture Length: 102 bytes (816 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:esp]
> 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
```

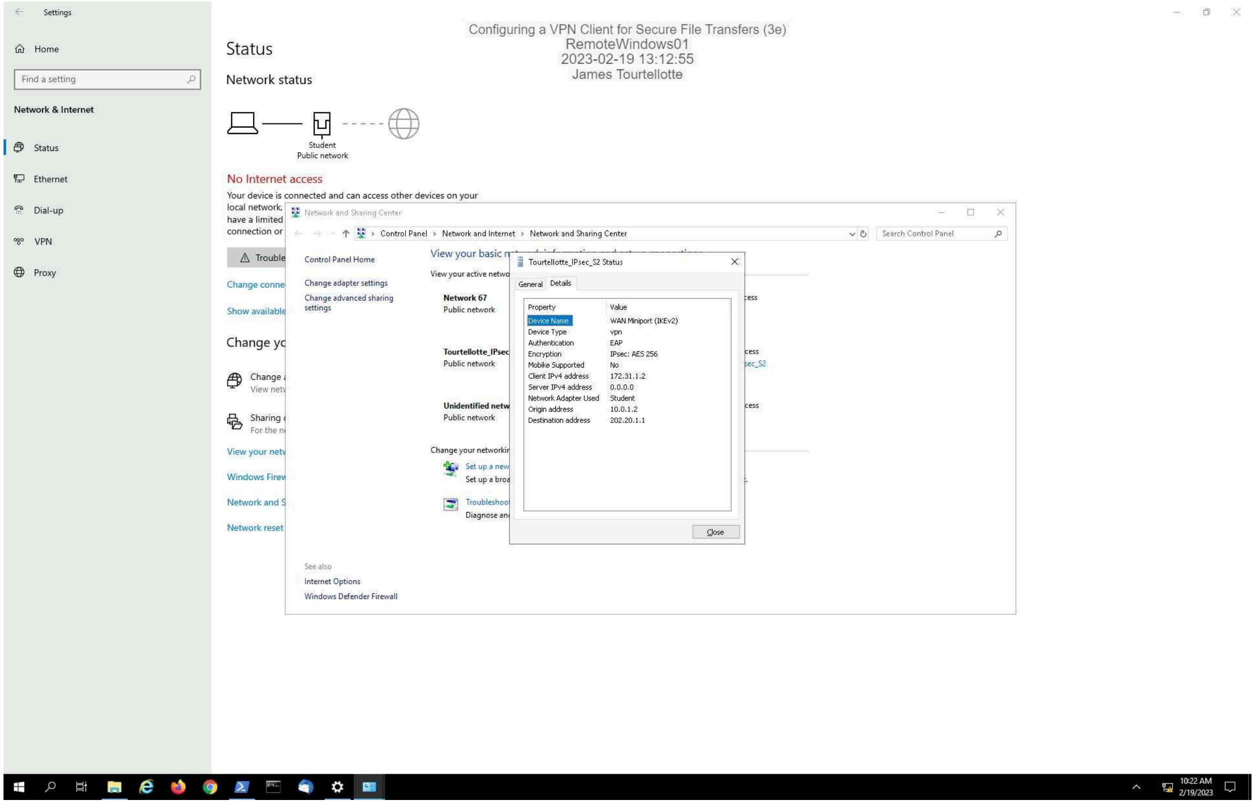
```
0000  ce b7 d4 e7 42 9c 4e d7  70 8a 07 01 08 00 45 00   ····B·N· p·····E·
0010  00 58 00 00 40 00 40 32  e1 d1 ac 1e 00 64 ac 1e   ·X··@·@2 ·····d··
0020  00 02 6b e5 9f ce 00 00  00 29 8f 0e 04 f2 9e b7   ··k····· ·)······
0030  bd 7c 5a 9c 05 54 d7 c5  db 56 4b 49 96 f9 19 43   ·|Z··T·· ·VKI···C
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

Screen Capture 1, Section 2:



Configuring a VPN Client for Secure File Transfers (3e)
RemoteWindows01
2023-02-19 13:12:55
James Tourtellotte

Status

Network status

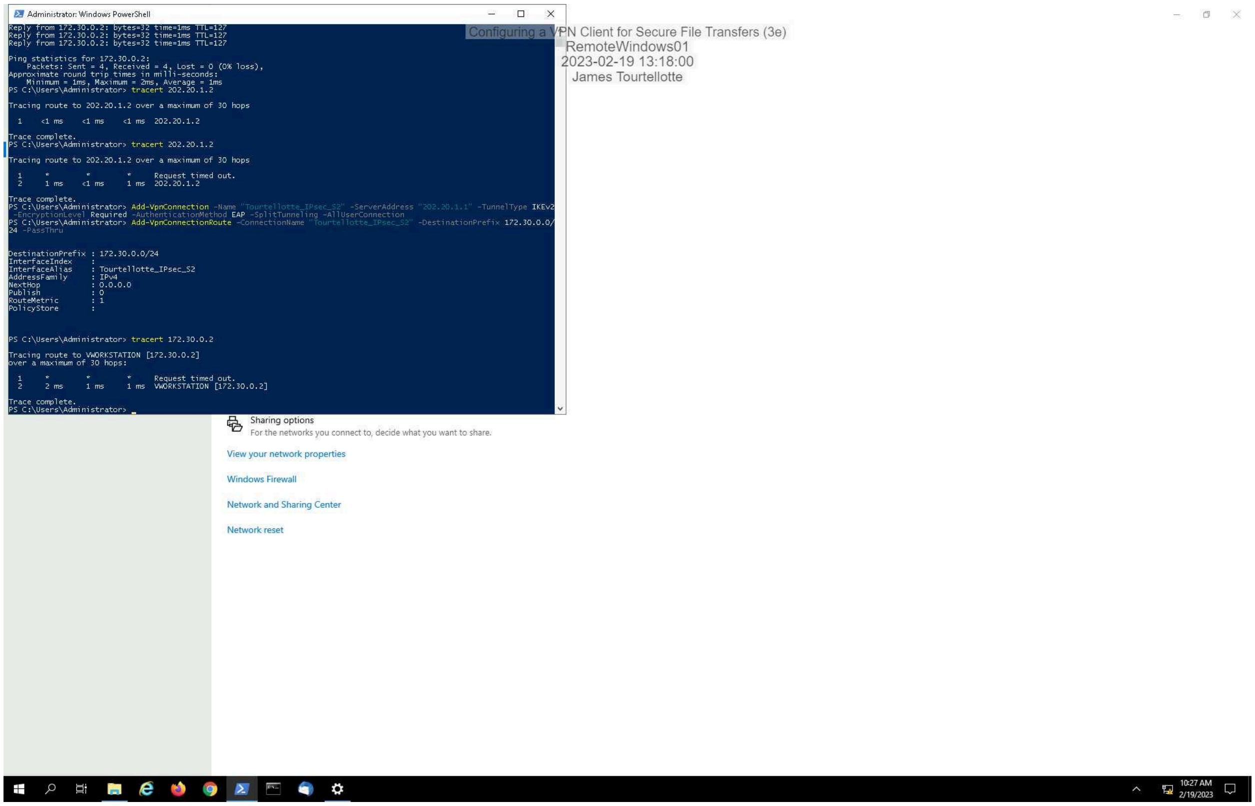
No Internet access

Your device is connected and can access other devices on your local network, have a limited connection or

Tourtellotte_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	172.31.1.2
Server IPv4 address	0.0.0.0
Network Adapter Used	Student
Origin address	10.0.1.2
Destination address	202.20.1.1

Screen Capture 2, Section 2:

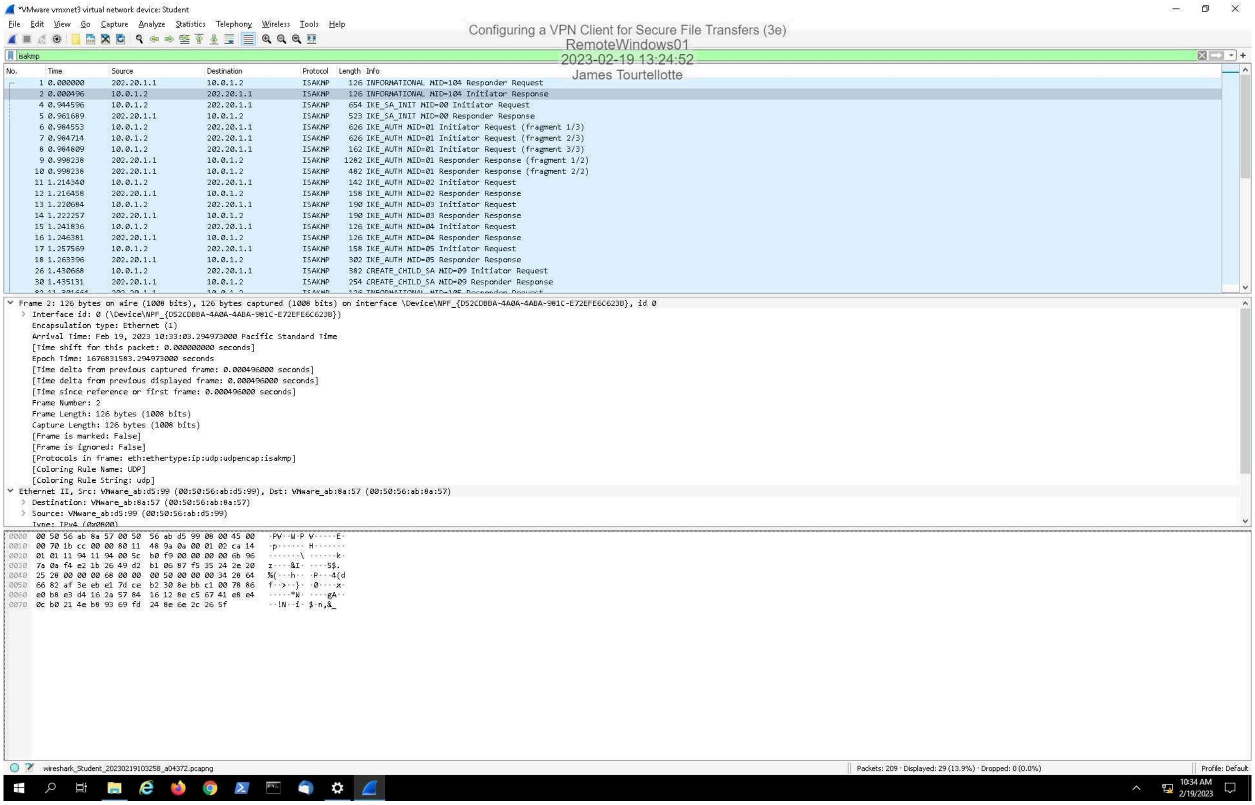


Configuring a VPN Client for Secure File Transfers (3e)
RemoteWindows01
2023-02-19 13:18:00
James Tourtellotte

```
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 = 2ms, 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> Add-VpnConnection -Name "Tourtellotte_IPsec_S2" -ServerAddress "202.20.1.1" -TunnelType IKEv2
 -EncryptionLevel Required -AuthenticationMethod EAP -SplitTunneling -AllUserConnection
PS C:\Users\Administrator> Add-VpnConnectionRoute -ConnectionName "Tourtellotte_IPsec_S2" -DestinationPrefix 172.30.0.0/
24 -PassThru


DestinationPrefix : 172.30.0.0/24
InterfaceIndex    :
InterfaceAlias    : Tourtellotte_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     2 ms     1 ms     1 ms  VWORKSTATION [172.30.0.2]

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

Sharing options
For the networks you connect to, decide what you want to share.
View your network properties
Windows Firewall
Network and Sharing Center
Network reset
10:27 AM
2/19/2023

Screen Capture 3, Section 2:


*VMware vmxnet3 virtual network device: Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
isakmp

Configuring a VPN Client for Secure File Transfers (3e)
RemoteWindows01
2023-02-19 13:24:52
James Tourtellotte

```
No.   Time       Source       Destination  Protocol Length Info
    1 0.000000   202.20.1.1   10.0.1.2     ISAKMP    126 INFORMATIONAL MID=104 Responder Request
    2 0.000496   10.0.1.2     202.20.1.1   ISAKMP    126 INFORMATIONAL MID=104 Initiator Response
    4 0.944596   10.0.1.2     202.20.1.1   ISAKMP    654 IKE_SA_INIT MID=00 Initiator Request
    5 0.961689   202.20.1.1   10.0.1.2     ISAKMP    523 IKE_SA_INIT MID=00 Responder Response
    6 0.984553   10.0.1.2     202.20.1.1   ISAKMP    626 IKE_AUTH MID=01 Initiator Request (fragment 1/3)
    7 0.984714   10.0.1.2     202.20.1.1   ISAKMP    626 IKE_AUTH MID=01 Initiator Request (fragment 2/3)
    8 0.984809   10.0.1.2     202.20.1.1   ISAKMP    162 IKE_AUTH MID=01 Initiator Request (fragment 3/3)
    9 0.998238   202.20.1.1   10.0.1.2     ISAKMP   1282 IKE_AUTH MID=01 Responder Response (fragment 1/2)
   10 0.998238   202.20.1.1   10.0.1.2     ISAKMP    482 IKE_AUTH MID=01 Responder Response (fragment 2/2)
   11 1.214340   10.0.1.2     202.20.1.1   ISAKMP    142 IKE_AUTH MID=02 Initiator Request
   12 1.216458   202.20.1.1   10.0.1.2     ISAKMP    158 IKE_AUTH MID=02 Responder Response
   13 1.220684   10.0.1.2     202.20.1.1   ISAKMP    190 IKE_AUTH MID=03 Initiator Request
   14 1.222257   202.20.1.1   10.0.1.2     ISAKMP    190 IKE_AUTH MID=03 Responder Response
   15 1.241836   10.0.1.2     202.20.1.1   ISAKMP    126 IKE_AUTH MID=04 Initiator Request
   16 1.246381   202.20.1.1   10.0.1.2     ISAKMP    126 IKE_AUTH MID=04 Responder Response
   17 1.257569   10.0.1.2     202.20.1.1   ISAKMP    158 IKE_AUTH MID=05 Initiator Request
   18 1.263396   202.20.1.1   10.0.1.2     ISAKMP    302 IKE_AUTH MID=05 Responder Response
   26 1.430668   10.0.1.2     202.20.1.1   ISAKMP    382 CREATE_CHILD_SA MID=09 Initiator Request
   30 1.435131   202.20.1.1   10.0.1.2     ISAKMP    254 CREATE_CHILD_SA MID=09 Responder Response
```

```
v Frame 2: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface \Device\NPF_{D52CDBBA-4A0A-4ABA-981C-E72EFE6C623B}, id 0
  > Interface id: 0 (\Device\NPF_{D52CDBBA-4A0A-4ABA-981C-E72EFE6C623B})
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 19, 2023 10:33:03.294973000 Pacific Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1676831583.294973000 seconds
    [Time delta from previous captured frame: 0.000496000 seconds]
    [Time delta from previous displayed frame: 0.000496000 seconds]
    [Time since reference or first frame: 0.000496000 seconds]
    Frame Number: 2
    Frame Length: 126 bytes (1008 bits)
    Capture Length: 126 bytes (1008 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:udpencap:isakmp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: VMware_ab:d5:99 (00:50:56:ab:d5:99), Dst: VMware_ab:8a:57 (00:50:56:ab:8a:57)
  > Destination: VMware_ab:8a:57 (00:50:56:ab:8a:57)
  > Source: VMware_ab:d5:99 (00:50:56:ab:d5:99)
    Type: IPv4 (0x0800)
```

```
0000  00 50 56 ab 8a 57 00 50  56 ab d5 99 08 00 45 00   ·PV··W·P V·····E·
0010  00 70 1b cc 00 00 80 11  48 9a 0a 00 01 02 ca 14   ·p······ H·······
0020  01 01 11 94 11 94 00 5c  b0 f9 00 00 00 00 6b 96   ·······\ ······k·
0030  7a 0a f4 e2 1b 26 49 d2  b1 06 87 f5 35 24 2e 20   z····&I· ····5$. 
0040  25 28 00 00 00 68 00 00  00 50 00 00 00 34 28 64   %(···h·· ·P···4(d
0050  66 82 af 3e eb e1 7d ce  b2 30 8e bb c1 00 78 86   f··>··}· ·0····x·
0060  e0 b8 e3 d4 16 2a 57 84  16 12 8e c5 67 41 e8 e4   ·····*W· ····gA··
0070  0c b0 21 4e b8 93 69 fd  24 8e 6e 2c 26 5f         ··!N··i· $·n,&_
```

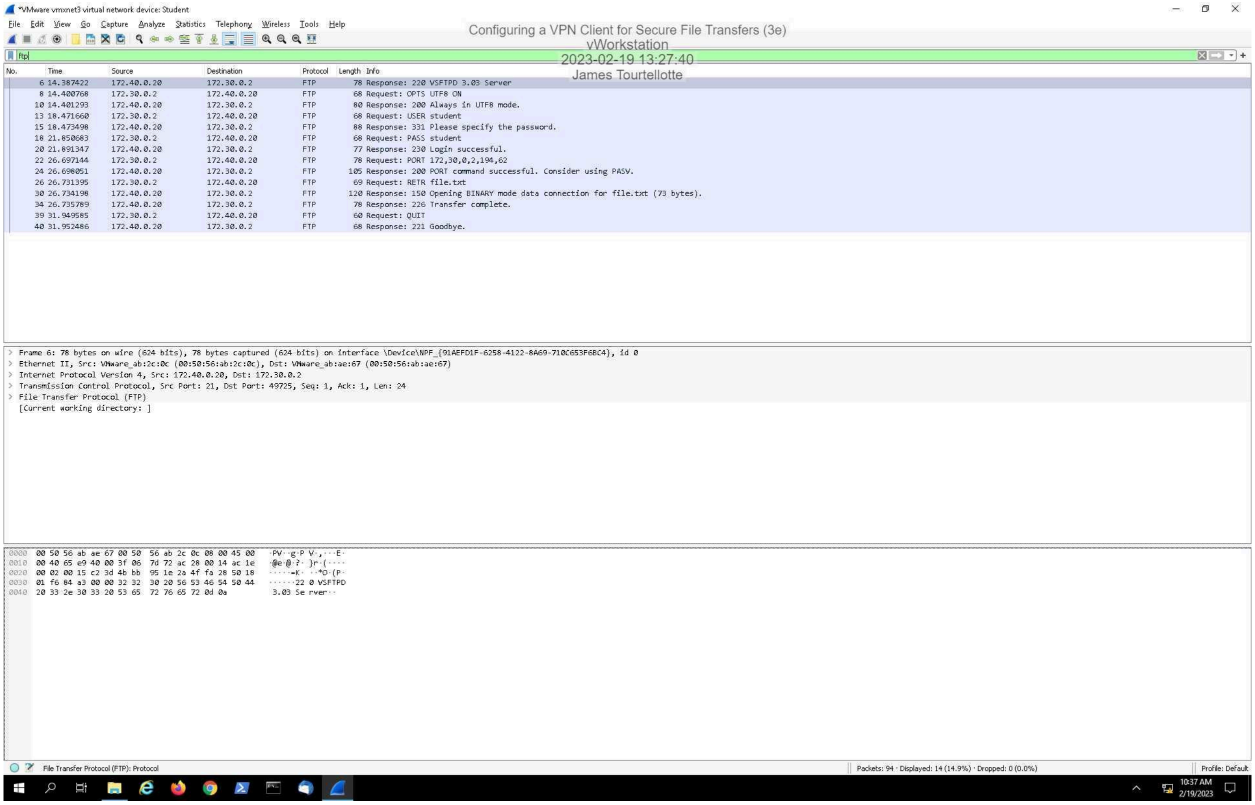
wireshark_Student_20230219103258_a04372.pcapng

Packets: 209 · Displayed: 29 (13.9%) · Dropped: 0 (0.0%)

Profile: Default

10:34 AM
2/19/2023

Screen Capture 4, Section 2:


*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
2023-02-19 13:27:40
James Tourtellotte

ftp

```
No.   Time       Source       Destination  Protocol Length Info
    6 14.387422  172.40.0.20  172.30.0.2   FTP        78 Response: 220 VSFTPD 3.03 Server
    8 14.400768  172.30.0.2   172.40.0.20  FTP        68 Request: OPTS UTF8 ON
   10 14.401293  172.40.0.20  172.30.0.2   FTP        80 Response: 200 Always in UTF8 mode.
   13 18.471660  172.30.0.2   172.40.0.20  FTP        68 Request: USER student
   15 18.473498  172.40.0.20  172.30.0.2   FTP        88 Response: 331 Please specify the password.
   18 21.850683  172.30.0.2   172.40.0.20  FTP        68 Request: PASS student
   20 21.891347  172.40.0.20  172.30.0.2   FTP        77 Response: 230 Login successful.
   22 26.697144  172.30.0.2   172.40.0.20  FTP        78 Request: PORT 172,30,0,2,194,62
   24 26.698051  172.40.0.20  172.30.0.2   FTP       105 Response: 200 PORT command successful. Consider using PASV.
   26 26.731395  172.30.0.2   172.40.0.20  FTP        69 Request: RETR file.txt
   30 26.734198  172.40.0.20  172.30.0.2   FTP       120 Response: 150 Opening BINARY mode data connection for file.txt (73 bytes).
   34 26.735789  172.40.0.20  172.30.0.2   FTP        78 Response: 226 Transfer complete.
   39 31.949585  172.30.0.2   172.40.0.20  FTP        60 Request: QUIT
   40 31.952486  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:2c:0c (00:50:56:ab:2c:0c), Dst: VMware_ab:ae:67 (00:50:56:ab:ae:67)
> Internet Protocol Version 4, Src: 172.40.0.20, Dst: 172.30.0.2
> Transmission Control Protocol, Src Port: 21, Dst Port: 49725, Seq: 1, Ack: 1, Len: 24
> File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  00 50 56 ab ae 67 00 50  56 ab 2c 0c 08 00 45 00   ·PV··g·P V·,···E·
0010  00 40 65 e9 40 00 3f 06  7d 72 ac 28 00 14 ac 1e   ·@e·@·?· }r·(····
0020  00 02 00 15 c2 3d 4b bb  95 1e 2a 4f fa 28 50 18   ·····=K· ··*O·(P·
0030  01 f6 84 a3 00 00 32 32  30 20 56 53 46 54 50 44   ······22 0 VSFTPD
0040  20 33 2e 30 33 20 53 65  72 76 65 72 0d 0a          3.03 Se rver··
```

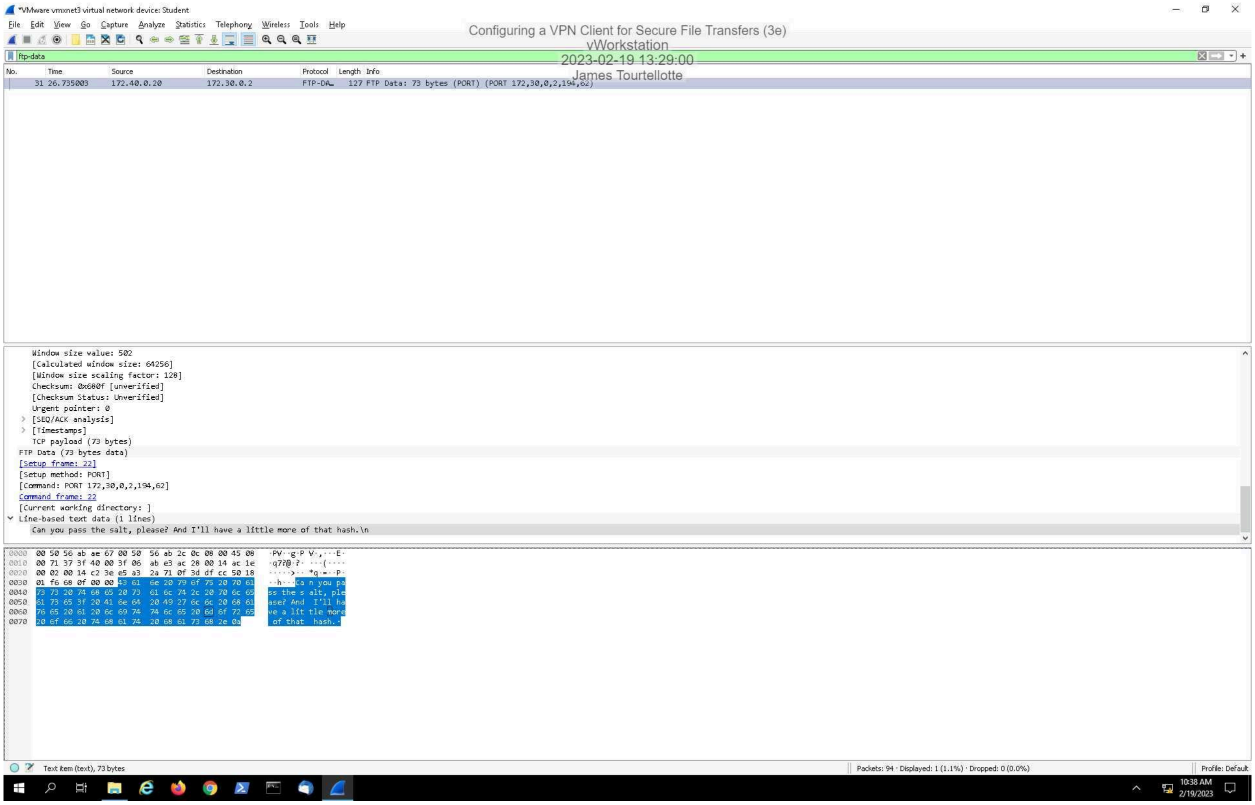
File Transfer Protocol (FTP): Protocol

Packets: 94 · Displayed: 14 (14.9%) · Dropped: 0 (0.0%)

Profile: Default

10:37 AM
2/19/2023

Screen Capture 5, Section 2:



*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
2023-02-19 13:29:00
James Tourtellotte

ftp-data

```
No.     Time       Source        Destination   Protocol  Length Info
     31 26.735003  172.40.0.20   172.30.0.2    FTP-DA…      127 FTP Data: 73 bytes (PORT) (PORT 172,30,0,2,194,62)
```

```
      Window size value: 502
      [Calculated window size: 64256]
      [Window size scaling factor: 128]
      Checksum: 0x680f [unverified]
      [Checksum Status: Unverified]
      Urgent pointer: 0
    > [SEQ/ACK analysis]
    > [Timestamps]
      TCP payload (73 bytes)
   FTP Data (73 bytes data)
   [Setup frame: 22]
   [Setup method: PORT]
   [Command: PORT 172,30,0,2,194,62]
   Command frame: 22
   [Current working directory: ]
 v Line-based text data (1 lines)
      Can you pass the salt, please? And I'll have a little more of that hash.\n
```

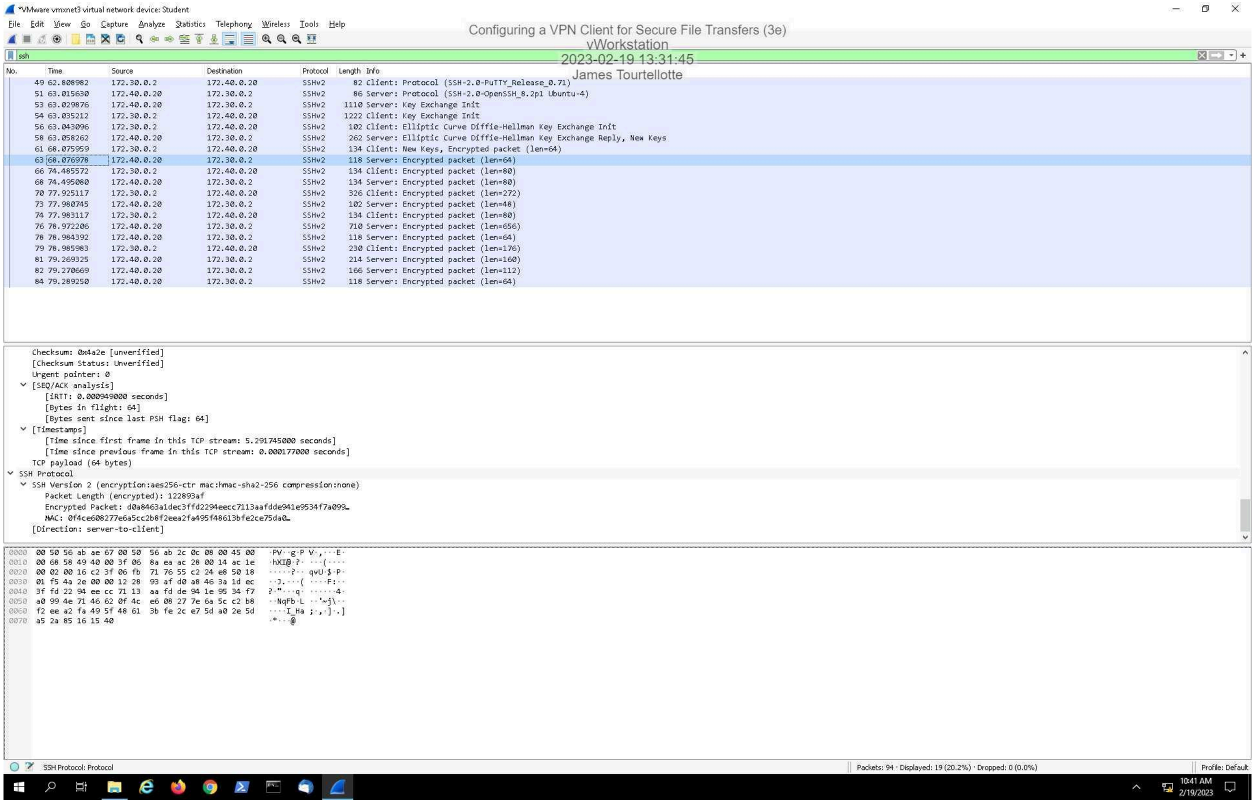
```
0000  00 50 56 ab ae 67 00 50  56 ab 2c 0c 08 00 45 08   ·PV··g·P V·,···E·
0010  00 71 37 3f 40 00 3f 06  ab e3 ac 28 00 14 ac 1e   ·q7?@·?· ···(····
0020  00 02 00 14 c2 3e e5 a3  2a 71 0f 3d df cc 50 18   ·····>·· *q·=··P·
0030  01 f6 68 0f 00 00 43 61  6e 20 79 6f 75 20 70 61   ··h···Ca n you 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.·
```

Text item (text), 73 bytes

Packets: 94 · Displayed: 1 (1.1%) · Dropped: 0 (0.0%)

Profile: Default

Screen Capture 6, section 2:


*VMware vmxnet3 virtual network device: Student
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ssh

Configuring a VPN Client for Secure File Transfers (3e)
vWorkstation
2023-02-19 13:31:45
James Tourtellotte

```
No.     Time         Source         Destination    Protocol  Length Info
     49 62.808982    172.30.0.2     172.40.0.20    SSHv2       82 Client: Protocol (SSH-2.0-PuTTY_Release_0.71)
     51 63.015630    172.40.0.20    172.30.0.2     SSHv2       86 Server: Protocol (SSH-2.0-OpenSSH_8.2p1 Ubuntu-4)
     53 63.029876    172.40.0.20    172.30.0.2     SSHv2     1110 Server: Key Exchange Init
     54 63.035212    172.30.0.2     172.40.0.20    SSHv2     1222 Client: Key Exchange Init
     56 63.043096    172.30.0.2     172.40.0.20    SSHv2      102 Client: Elliptic Curve Diffie-Hellman Key Exchange Init
     58 63.058262    172.40.0.20    172.30.0.2     SSHv2      262 Server: Elliptic Curve Diffie-Hellman Key Exchange Reply, New Keys
     61 68.075959    172.30.0.2     172.40.0.20    SSHv2      134 Client: New Keys, Encrypted packet (len=64)
     63 68.076978    172.40.0.20    172.30.0.2     SSHv2      118 Server: Encrypted packet (len=64)
     66 74.485572    172.30.0.2     172.40.0.20    SSHv2      134 Client: Encrypted packet (len=80)
     68 74.495080    172.40.0.20    172.30.0.2     SSHv2      134 Server: Encrypted packet (len=80)
     70 77.925117    172.30.0.2     172.40.0.20    SSHv2      326 Client: Encrypted packet (len=272)
     73 77.980745    172.40.0.20    172.30.0.2     SSHv2      102 Server: Encrypted packet (len=48)
     74 77.983117    172.30.0.2     172.40.0.20    SSHv2      134 Client: Encrypted packet (len=80)
     76 78.972206    172.40.0.20    172.30.0.2     SSHv2      710 Server: Encrypted packet (len=656)
     78 78.984392    172.40.0.20    172.30.0.2     SSHv2      118 Server: Encrypted packet (len=64)
     79 78.985983    172.30.0.2     172.40.0.20    SSHv2      230 Client: Encrypted packet (len=176)
     81 79.269325    172.40.0.20    172.30.0.2     SSHv2      214 Server: Encrypted packet (len=160)
     82 79.270669    172.40.0.20    172.30.0.2     SSHv2      166 Server: Encrypted packet (len=112)
     84 79.289250    172.40.0.20    172.30.0.2     SSHv2      118 Server: Encrypted packet (len=64)
```

```
    Checksum: 0x4a2e [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  ˅ [SEQ/ACK analysis]
      [iRTT: 0.000949000 seconds]
      [Bytes in flight: 64]
      [Bytes sent since last PSH flag: 64]
  ˅ [Timestamps]
      [Time since first frame in this TCP stream: 5.291745000 seconds]
      [Time since previous frame in this TCP stream: 0.000177000 seconds]
    TCP payload (64 bytes)
˅ SSH Protocol
  ˅ SSH Version 2 (encryption:aes256-ctr mac:hmac-sha2-256 compression:none)
      Packet Length (encrypted): 122893af
      Encrypted Packet: d0a8463a1dec3ffd2294eecc7113aafdde941e9534f7a099…
      MAC: 0f4ce608277e6a5cc2b8f2eea2fa495f48613bfe2ce75da0…
    [Direction: server-to-client]
```

```
0000  00 50 56 ab ae 67 00 50  56 ab 2c 0c 08 00 45 00   ·PV··g·P V·,···E·
0010  00 68 58 49 40 00 3f 06  8a ea ac 28 00 14 ac 1e   ·hXI@·?· ···(····
0020  00 02 00 16 c2 3f 06 fb  71 76 55 c2 24 e8 50 18   ·····?·· qvU·$·P·
0030  01 f5 4a 2e 00 00 12 28  93 af d0 a8 46 3a 1d ec   ··J.···( ····F:··
0040  3f fd 22 94 ee cc 71 13  aa fd de 94 1e 95 34 f7   ?·"···q· ······4·
0050  a0 99 4e 71 46 62 0f 4c  e6 08 27 7e 6a 5c c2 b8   ··NqFb·L ··'~j\··
0060  f2 ee a2 fa 49 5f 48 61  3b fe 2c e7 5d a0 2e 5d   ····I_Ha ;·,·]·.]
0070  a5 2a 85 16 15 40                                  ·*···@
```

SSH Protocol: Protocol

Packets: 94 · Displayed: 19 (20.2%) · Dropped: 0 (0.0%)

Profile: Default

10:41 AM
2/19/2023