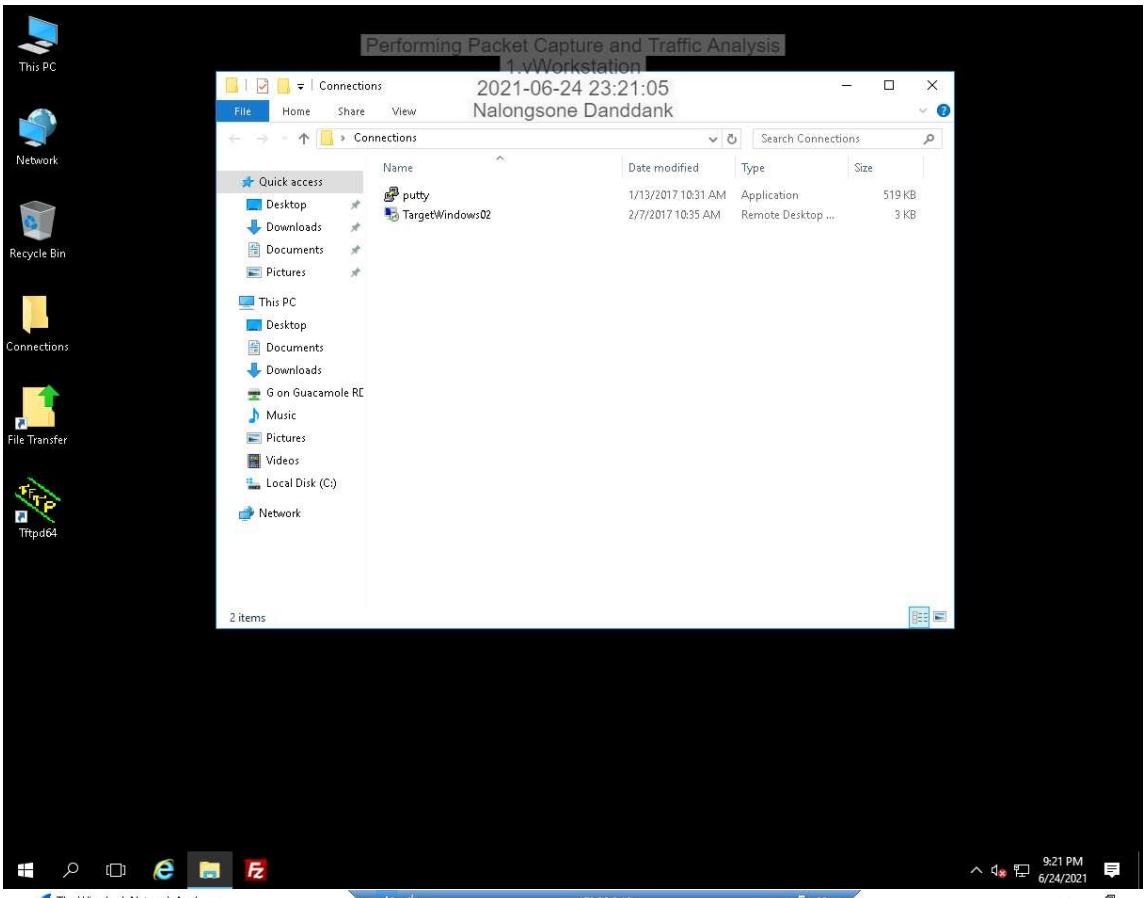
Nalongsone Danddank Student ID : 14958950 StarID: jf3893pd
Email: nalongsone.danddank@my.metrostate.edu\

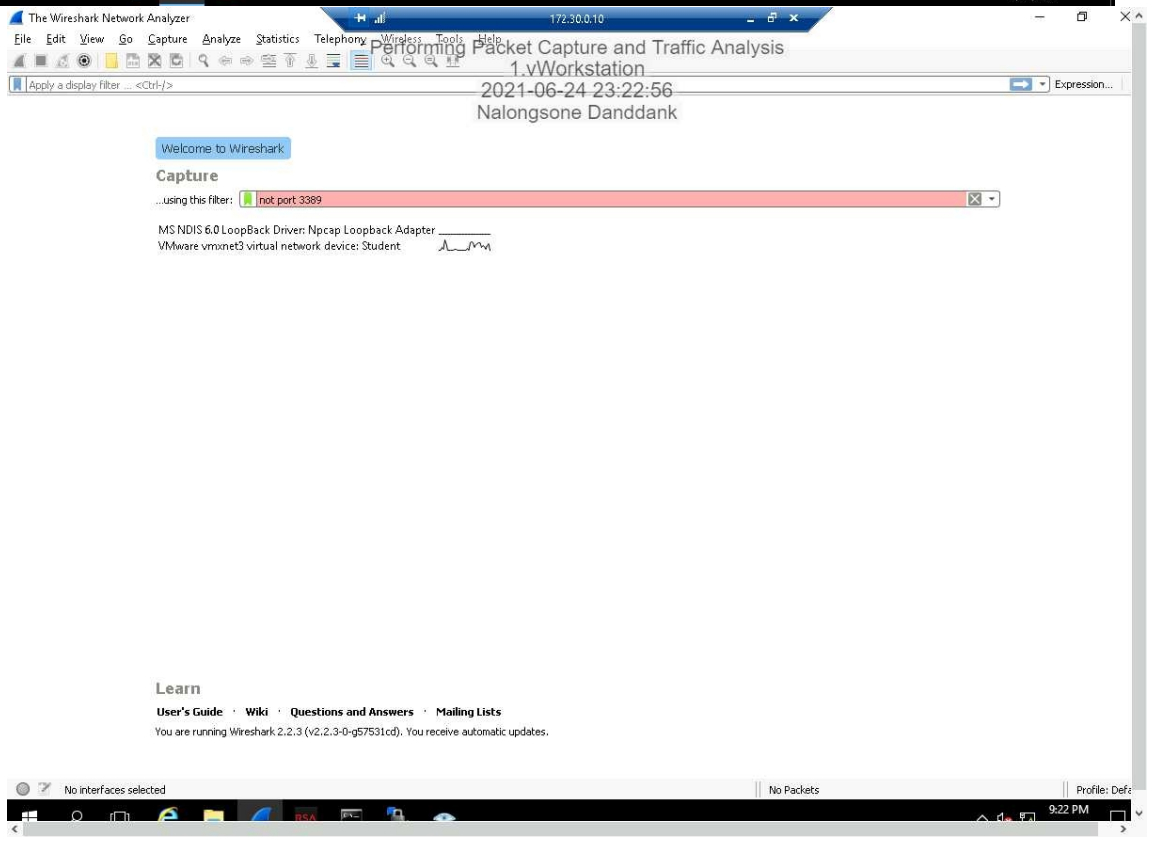
ICS382/CYBR332-51 —Computer Security

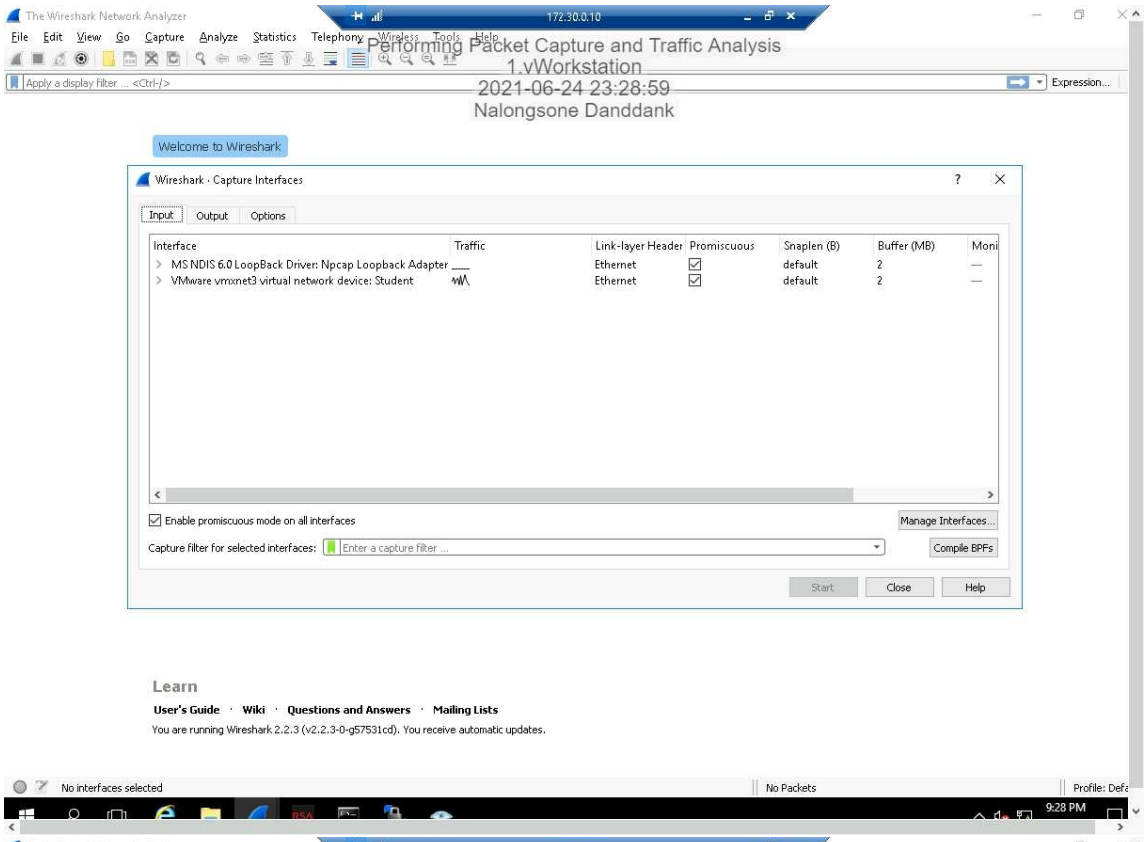
Lab #5 Report

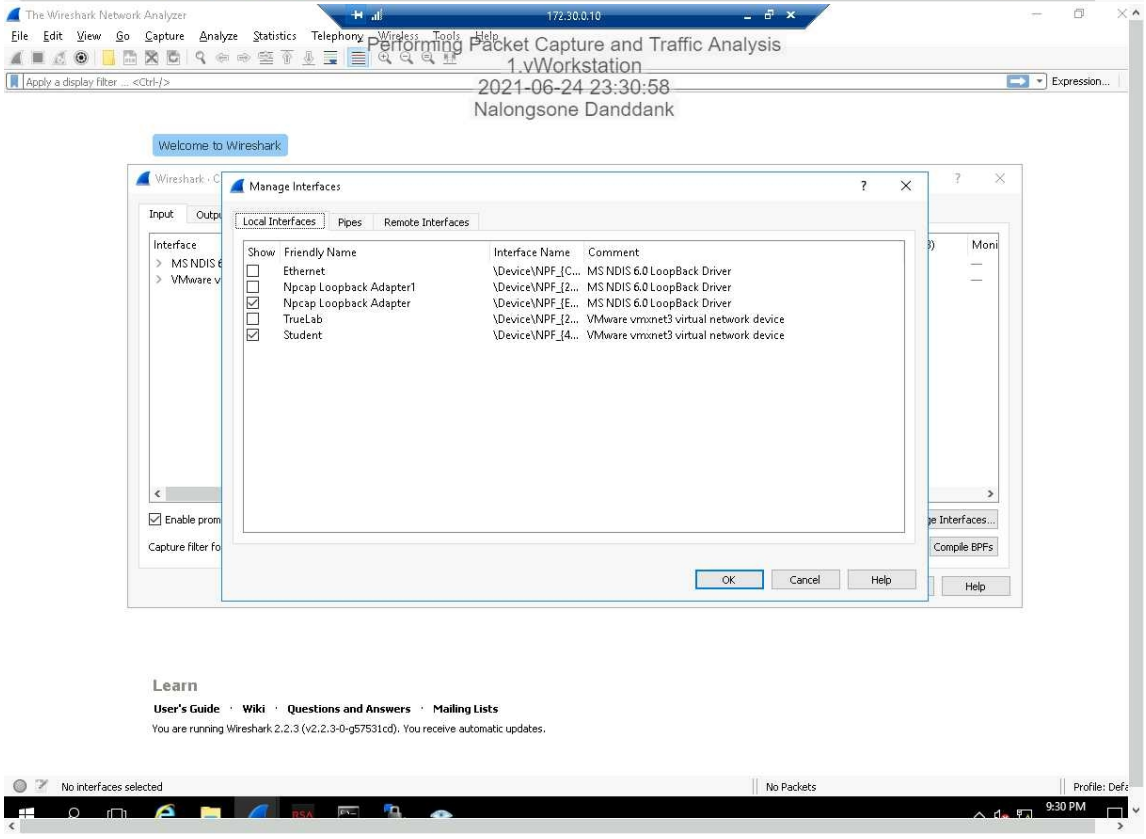
Performing Packet Capture and Traffic Analysis

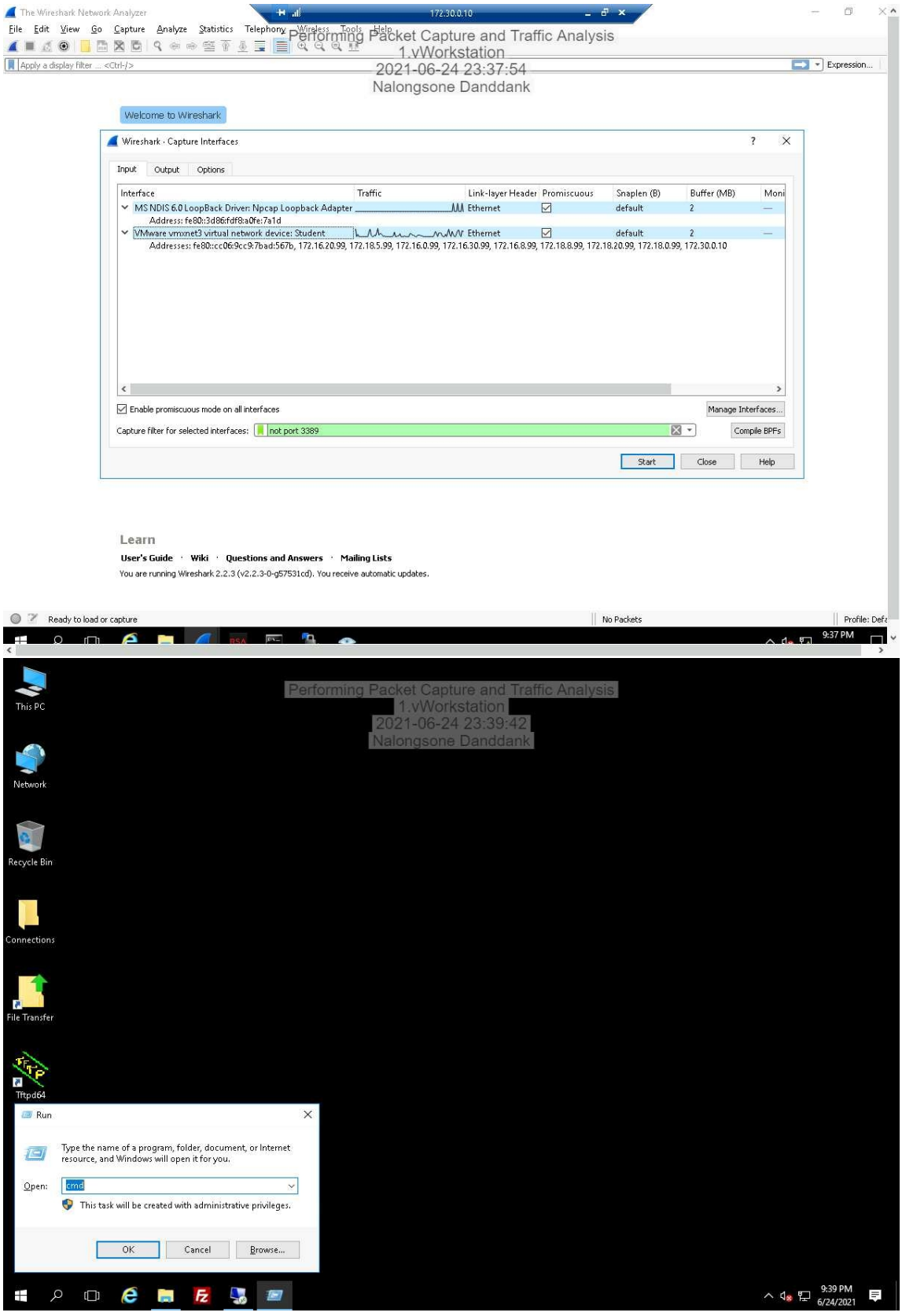
Part 1: Generate Network Traffic.

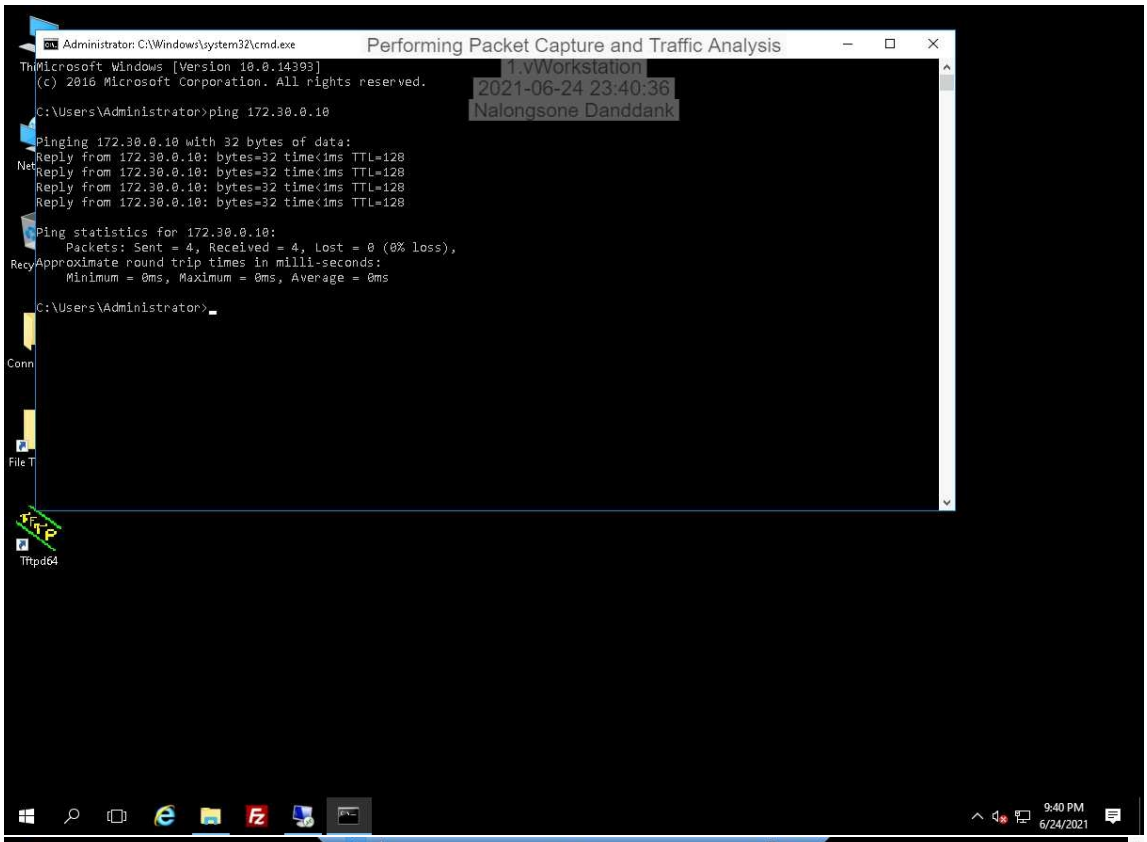


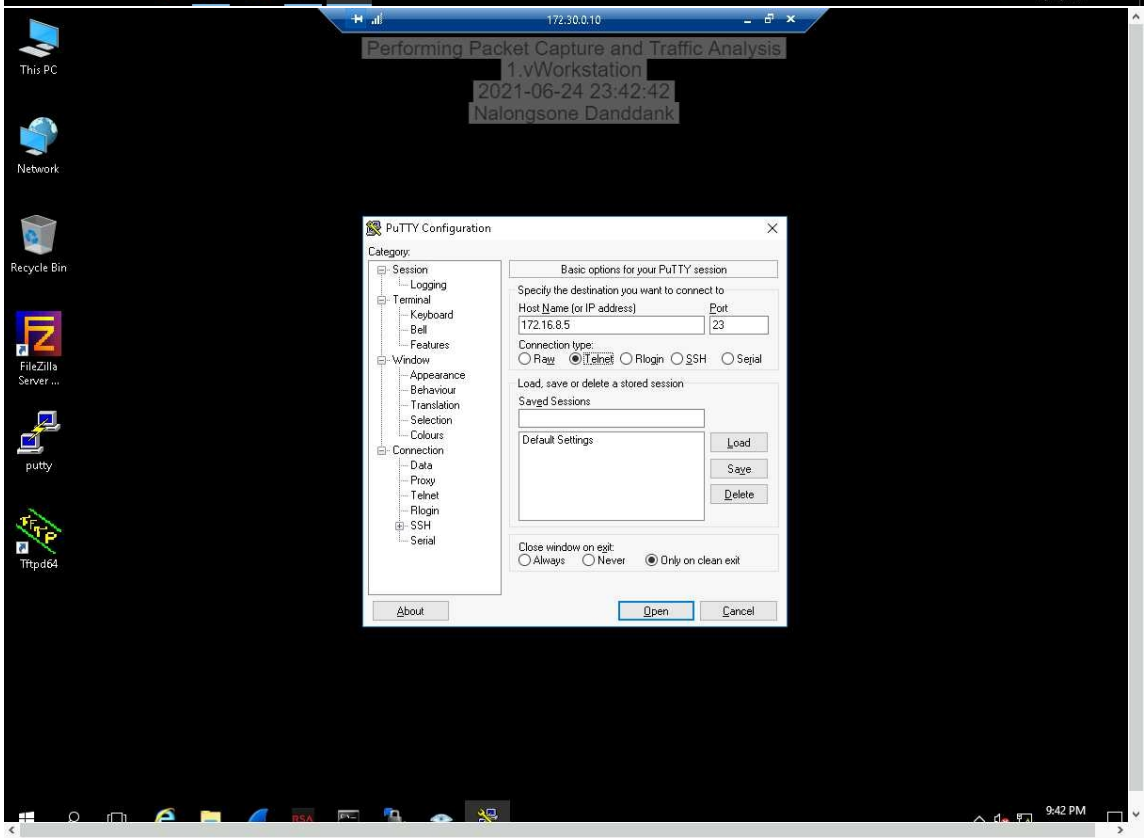


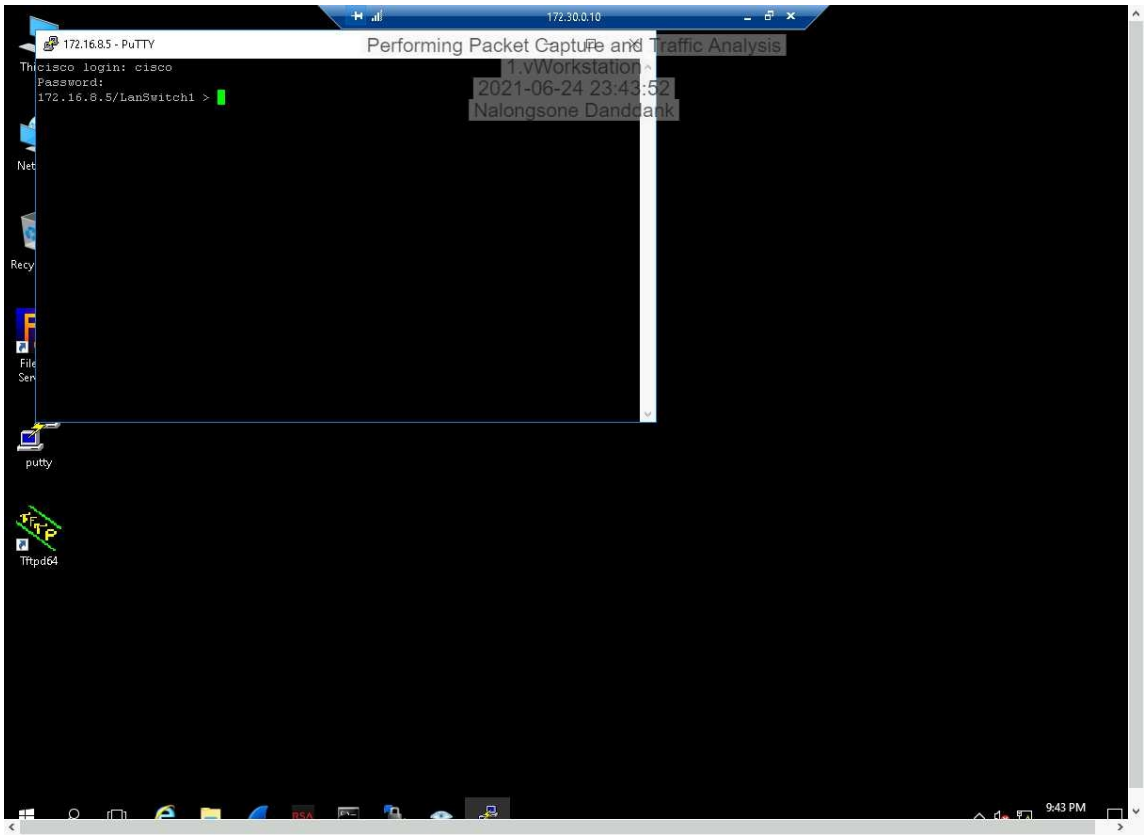

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:28:59
Nalongsone Danddank
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Wireshark · Capture Interfaces
Input Output Options
Interface Traffic Link-layer Header Promiscuous Snaplen (B) Buffer (MB) Moni
MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter Ethernet default 2
VMware vmxnet3 virtual network device: Student Ethernet default 2
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces: Enter a capture filter ...
Compile BPFs
Start Close Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.2.3 (v2.2.3-0-g57531cd). You receive automatic updates.
No interfaces selected
No Packets
Profile: Defa
9:28 PM

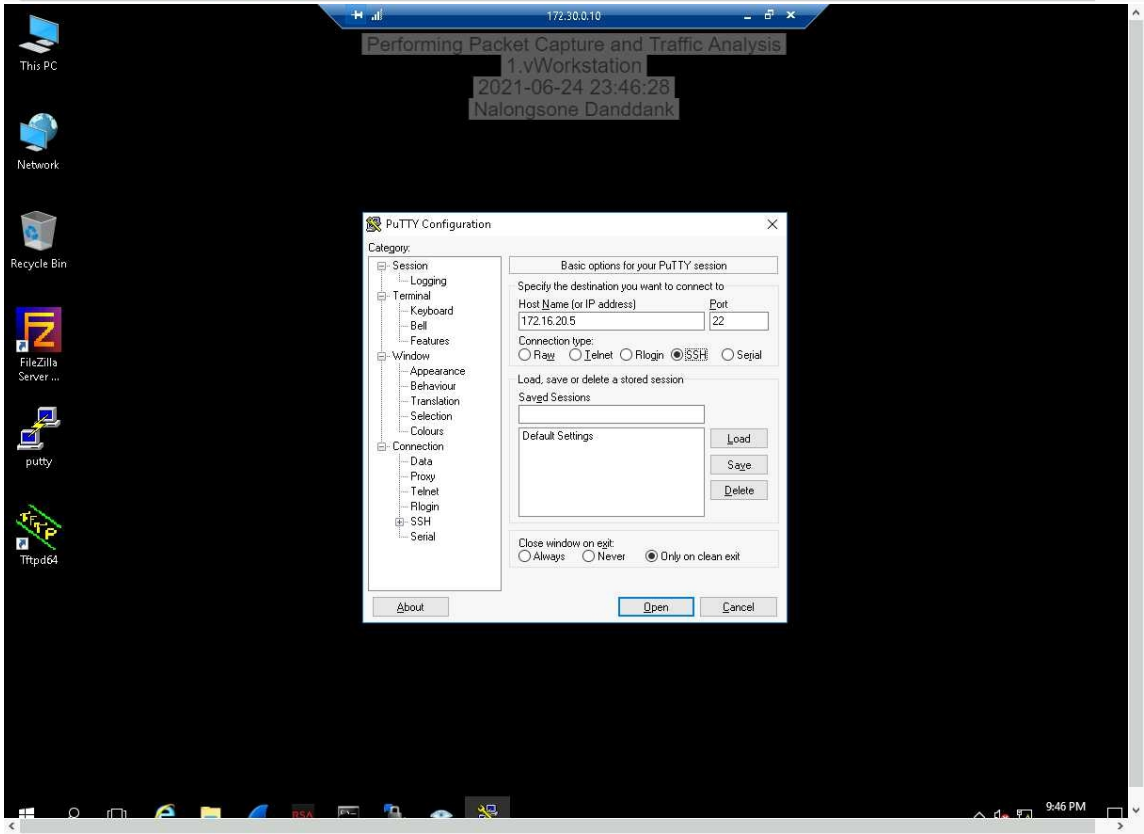

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:30:58
Nalongsone Danddank
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Manage Interfaces
Local Interfaces Pipes Remote Interfaces
Show Friendly Name Interface Name Comment
Ethernet \Device\NPF_{C... MS NDIS 6.0 LoopBack Driver
Npcap Loopback Adapter1 \Device\NPF_{2... MS NDIS 6.0 LoopBack Driver
Npcap Loopback Adapter \Device\NPF_{E... MS NDIS 6.0 LoopBack Driver
TrueLab \Device\NPF_{2... VMware vmxnet3 virtual network device
Student \Device\NPF_{4... VMware vmxnet3 virtual network device
OK Cancel Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.2.3 (v2.2.3-0-g57531cd). You receive automatic updates.
No interfaces selected
No Packets
Profile: Defa
9:30 PM

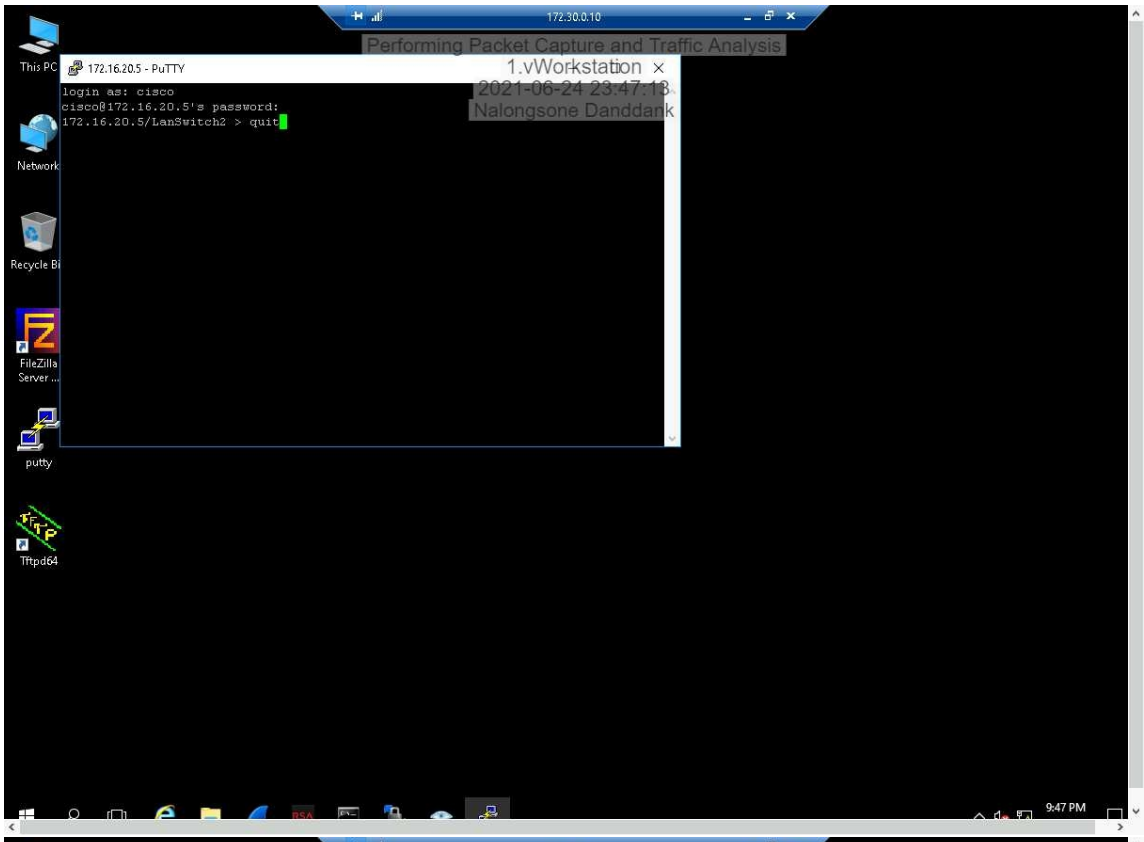

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:37:54
Nalongsone Danddank
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
Welcome to Wireshark
Wireshark · Capture Interfaces
Input Output Options
Interface Traffic Link-layer Header Promiscuous Snaplen (B) Buffer (MB) Moni
MS NDIS 6.0 LoopBack Driver: Npcap Loopback Adapter Ethernet default 2
Address: fe80::3d86:fdf8:a0fe:7a1d
VMware vmxnet3 virtual network device: Student Ethernet default 2
Addresses: fe80::cc06:9cc9:7bad:567b, 172.16.20.99, 172.18.5.99, 172.16.0.99, 172.16.30.99, 172.16.8.99, 172.18.8.99, 172.18.20.99, 172.18.0.99, 172.30.0.10
Enable promiscuous mode on all interfaces
Manage Interfaces...
Capture filter for selected interfaces: not port 3389
Compile BPFs
Start Close Help
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
You are running Wireshark 2.2.3 (v2.2.3-0-g57531cd). You receive automatic updates.
Ready to load or capture
No Packets
Profile: Defa
9:37 PM
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:39:42
Nalongsone Danddank
This PC
Network
Recycle Bin
Connections
File Transfer
Tftpd64
Run
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open: cmd
This task will be created with administrative privileges.
OK Cancel Browse...
9:39 PM
6/24/2021

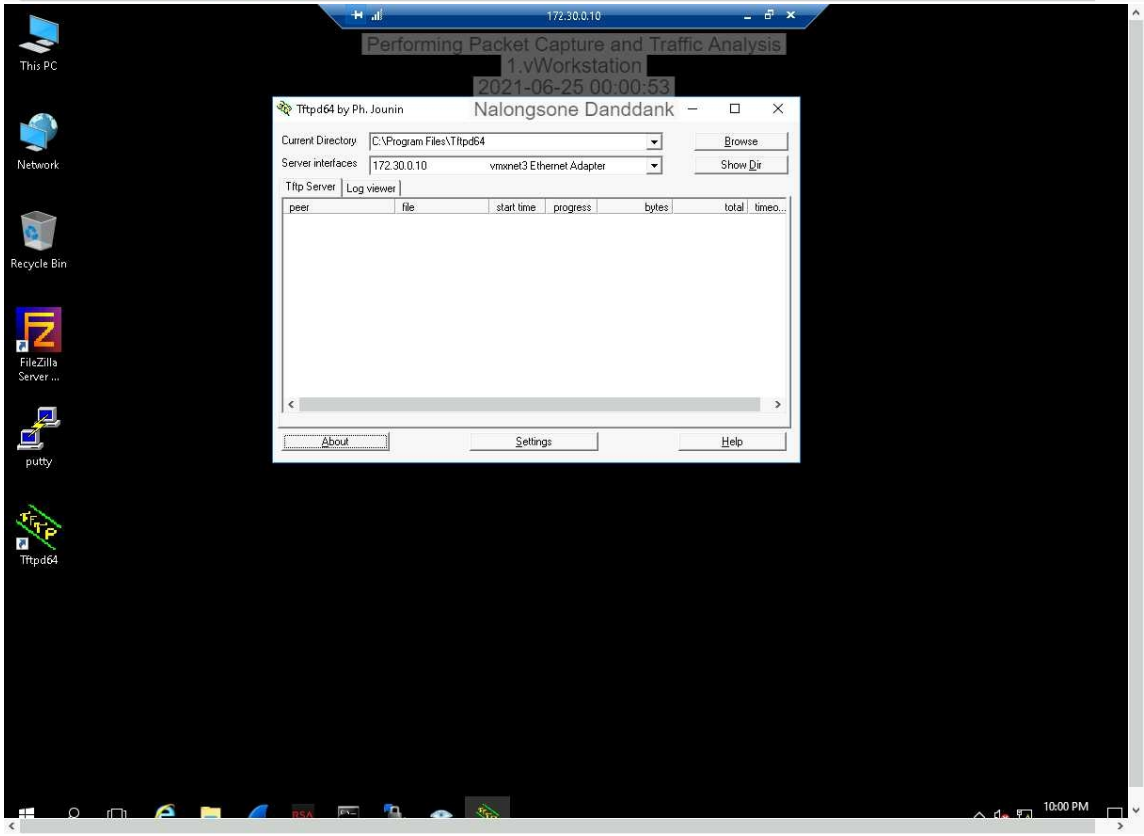

Administrator: C:\Windows\system32\cmd.exe
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:40:36
Nalongsone Danddank
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>ping 172.30.0.10
Pinging 172.30.0.10 with 32 bytes of data:
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Reply from 172.30.0.10: bytes=32 time<1ms TTL=128
Ping statistics for 172.30.0.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\Users\Administrator>
Tftpd64
9:40 PM
6/24/2021

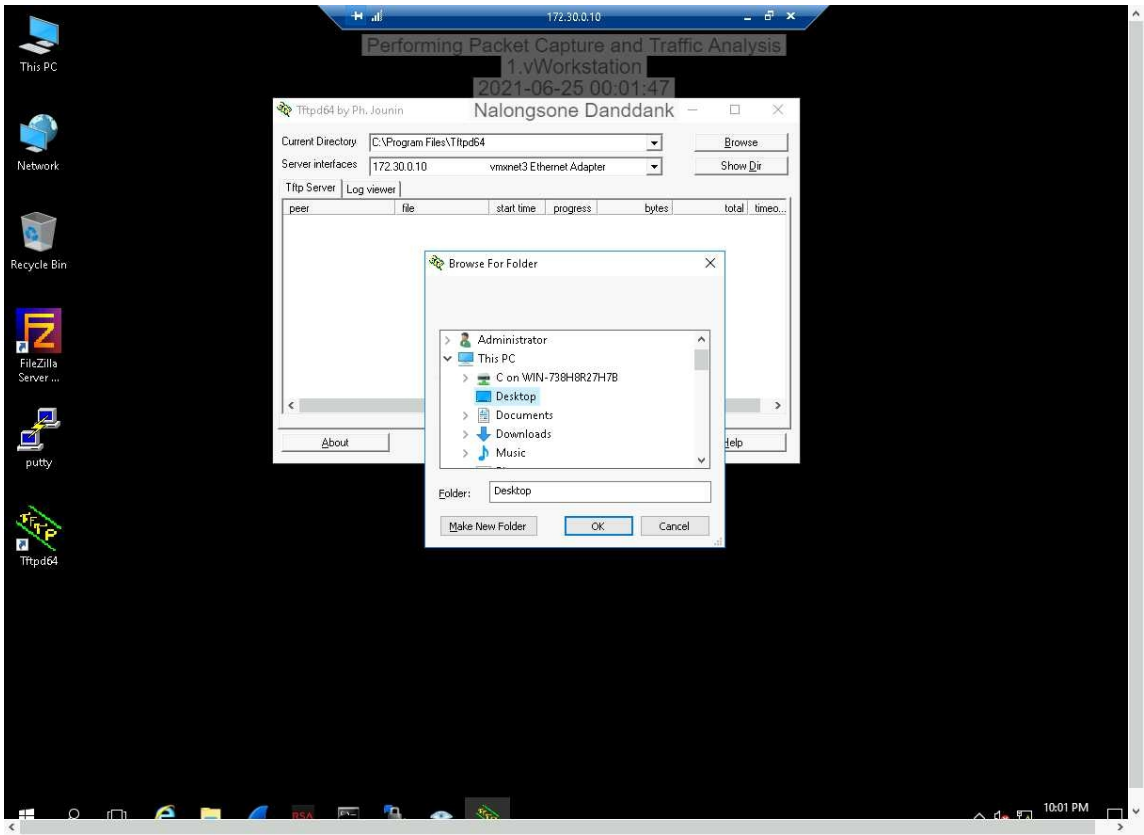

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:42:42
Nalongsone Danddank
This PC
Network
Recycle Bin
FileZilla Server ...
putty
Tftpd64
PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
172.16.8.5
23
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel
9:42 PM

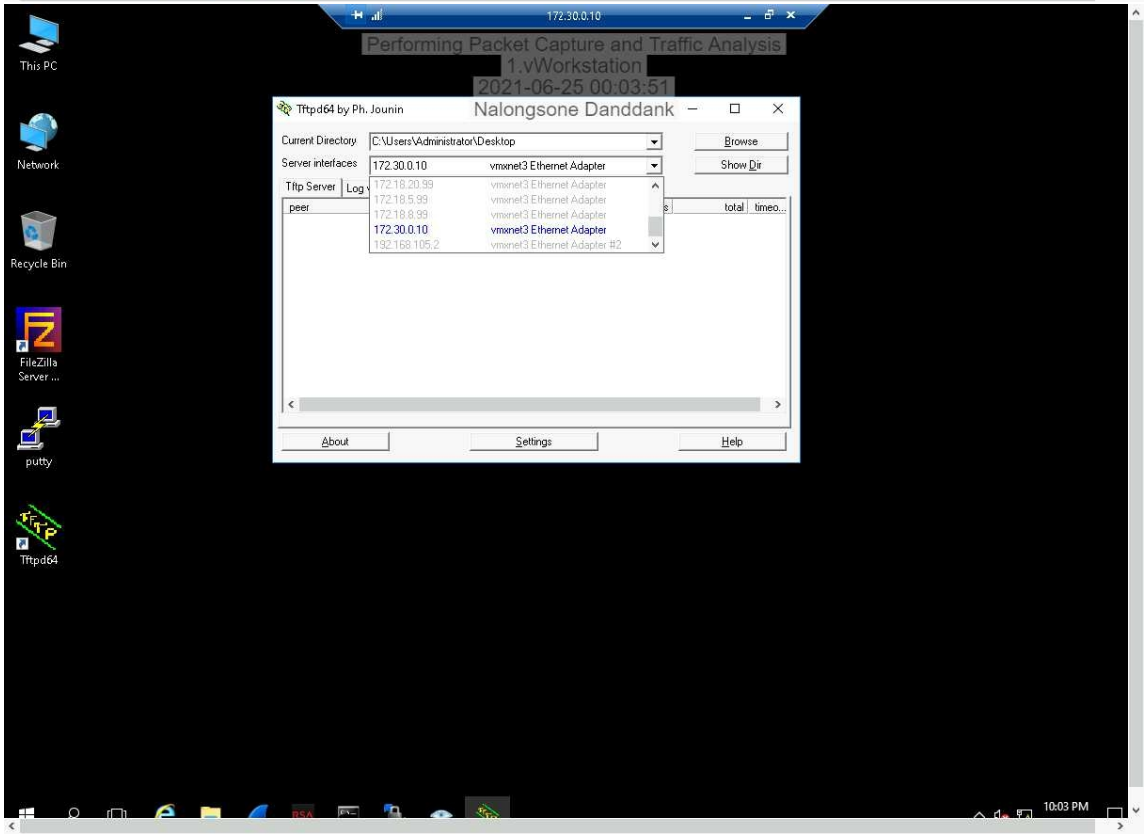

172.30.0.10
172.16.8.5 - PuTTY
cisco login: cisco
Password:
172.16.8.5/LanSwitch1 >
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:43:52
Nalongsone Danddank
putty
Tftpd64
9:43 PM

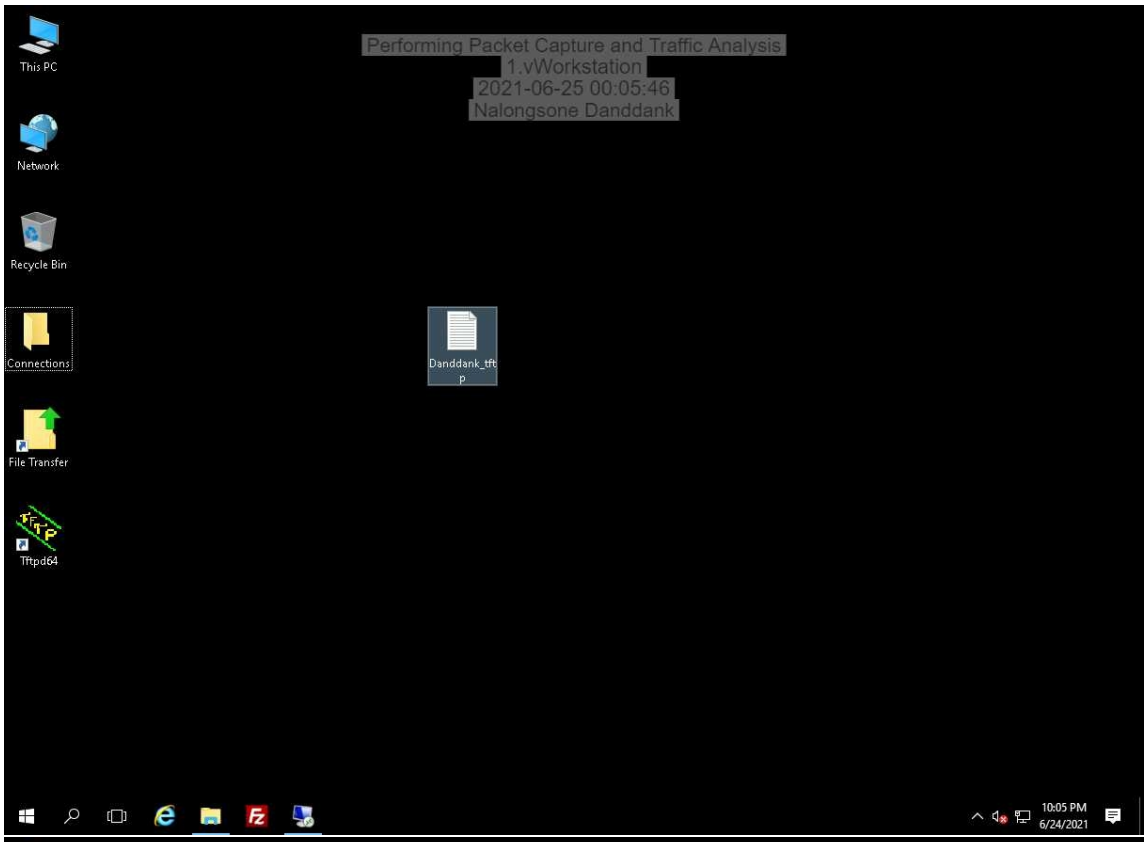

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:46:28
Nalongsone Danddank
This PC
Network
Recycle Bin
FileZilla Server ...
putty
Tftpd64
PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Specify the destination you want to connect to
Host Name (or IP address)
Port
172.16.20.5
22
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel
9:46 PM

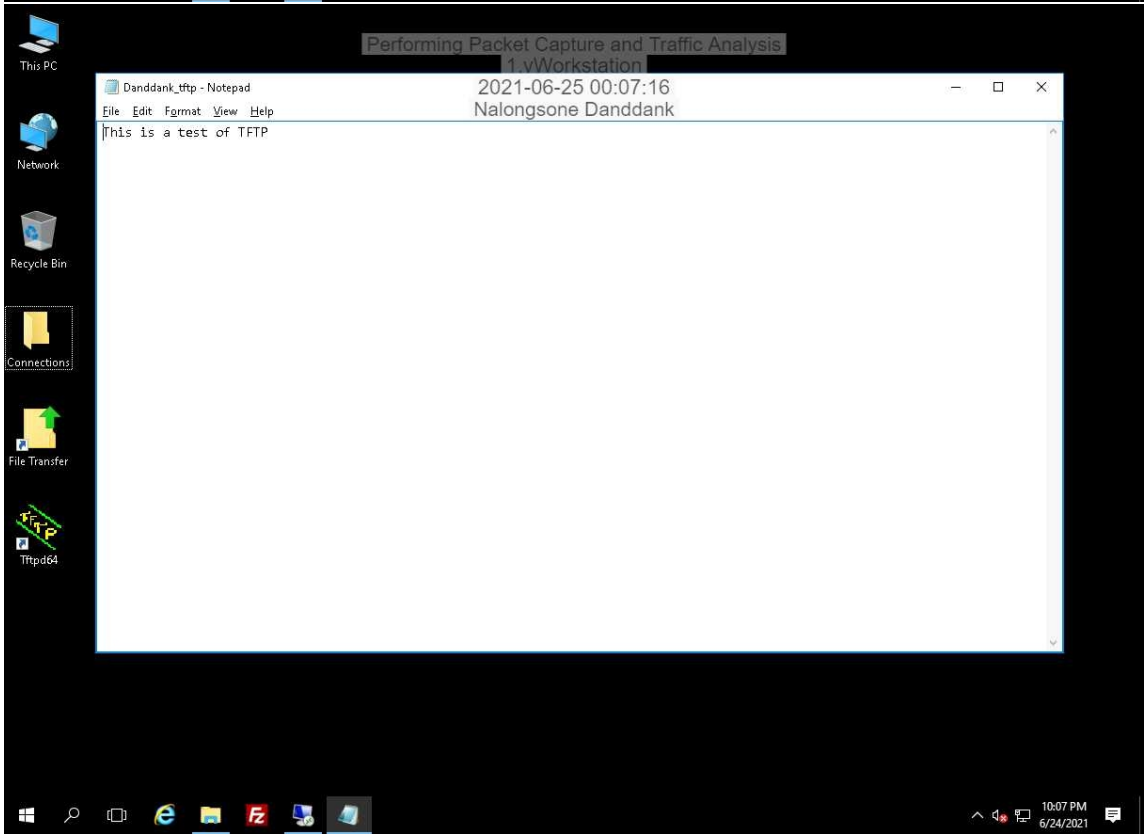

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-24 23:47:13
Nalongsone Danddank
172.16.20.5 - PuTTY
login as: cisco
cisco@172.16.20.5's password:
172.16.20.5/LanSwitch2 > quit
This PC
Network
Recycle Bi
FileZilla Server ...
putty
Tftpd64
9:47 PM

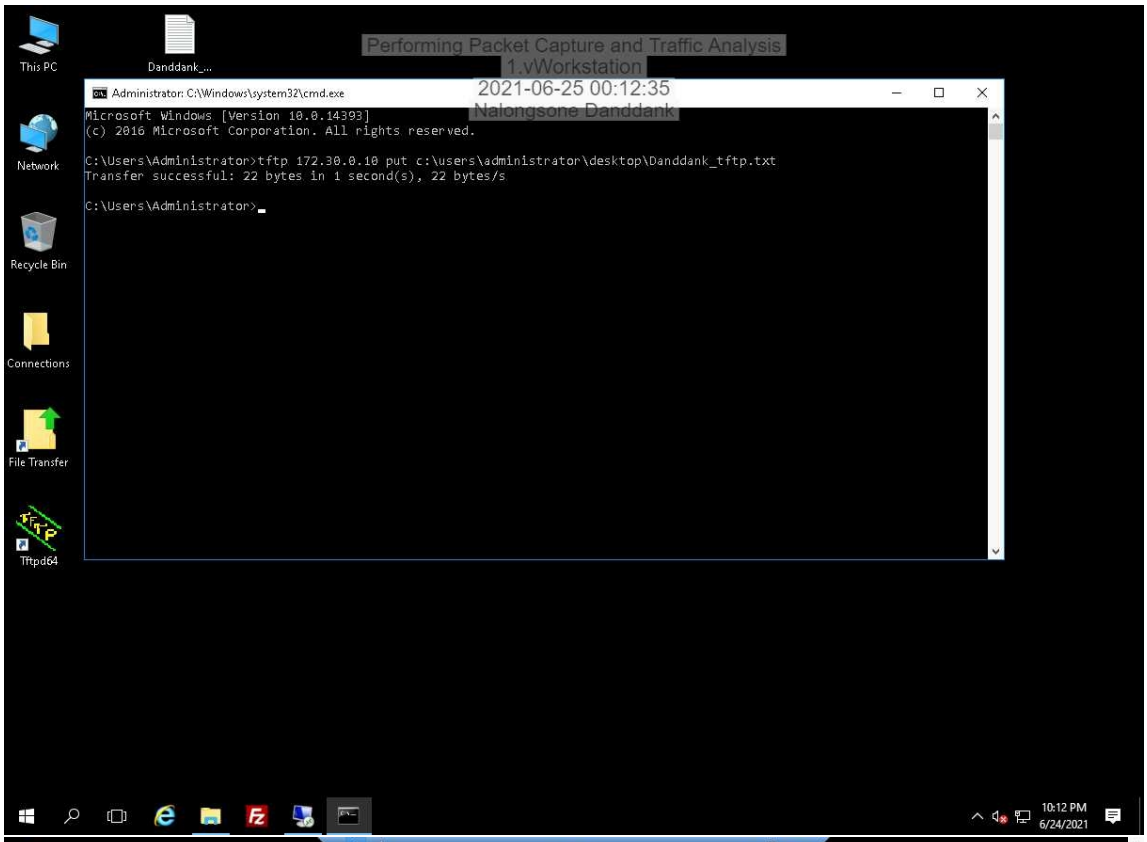

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:00:53
Nalongsone Danddank
Tftpd64 by Ph. Jounin
Current Directory
C:\Program Files\Tftpd64
Browse
Server interfaces
172.30.0.10
vmxnet3 Ethernet Adapter
Show Dir
Tftp Server
Log viewer
peer
file
start time
progress
bytes
total
timeo...
About
Settings
Help
This PC
Network
Recycle Bin
FileZilla Server ...
putty
Tftpd64
10:00 PM

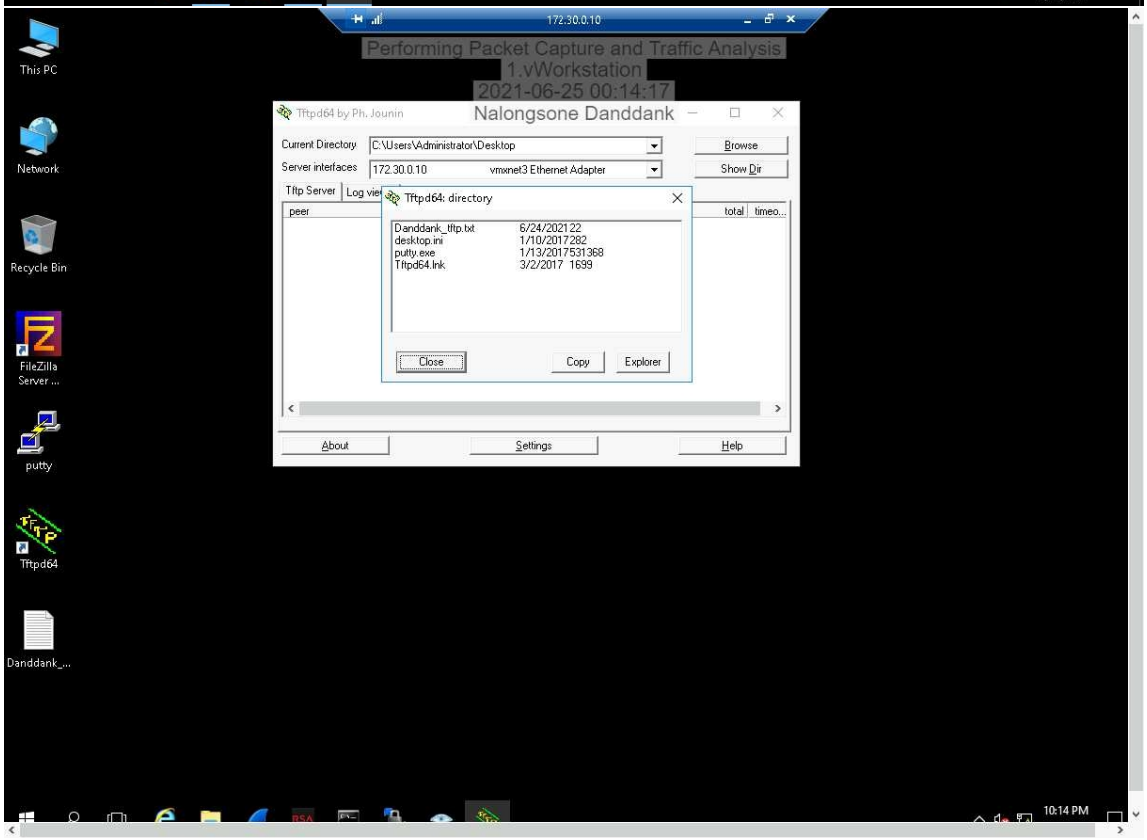

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:01:47
Tftpd64 by Ph. Jounin
Nalongsone Danddank
Current Directory C:\Program Files\Tftpd64
Server interfaces 172.30.0.10 vmxnet3 Ethernet Adapter
Browse
Show Dir
Tftp Server
Log viewer
peer
file
start time
progress
bytes
total
timeo...
About
Help
Browse For Folder
Administrator
This PC
C on WIN-738H8R27H7B
Desktop
Documents
Downloads
Music
Folder: Desktop
Make New Folder
OK
Cancel
This PC
Network
Recycle Bin
FileZilla Server ...
putty
Tftpd64
10:01 PM

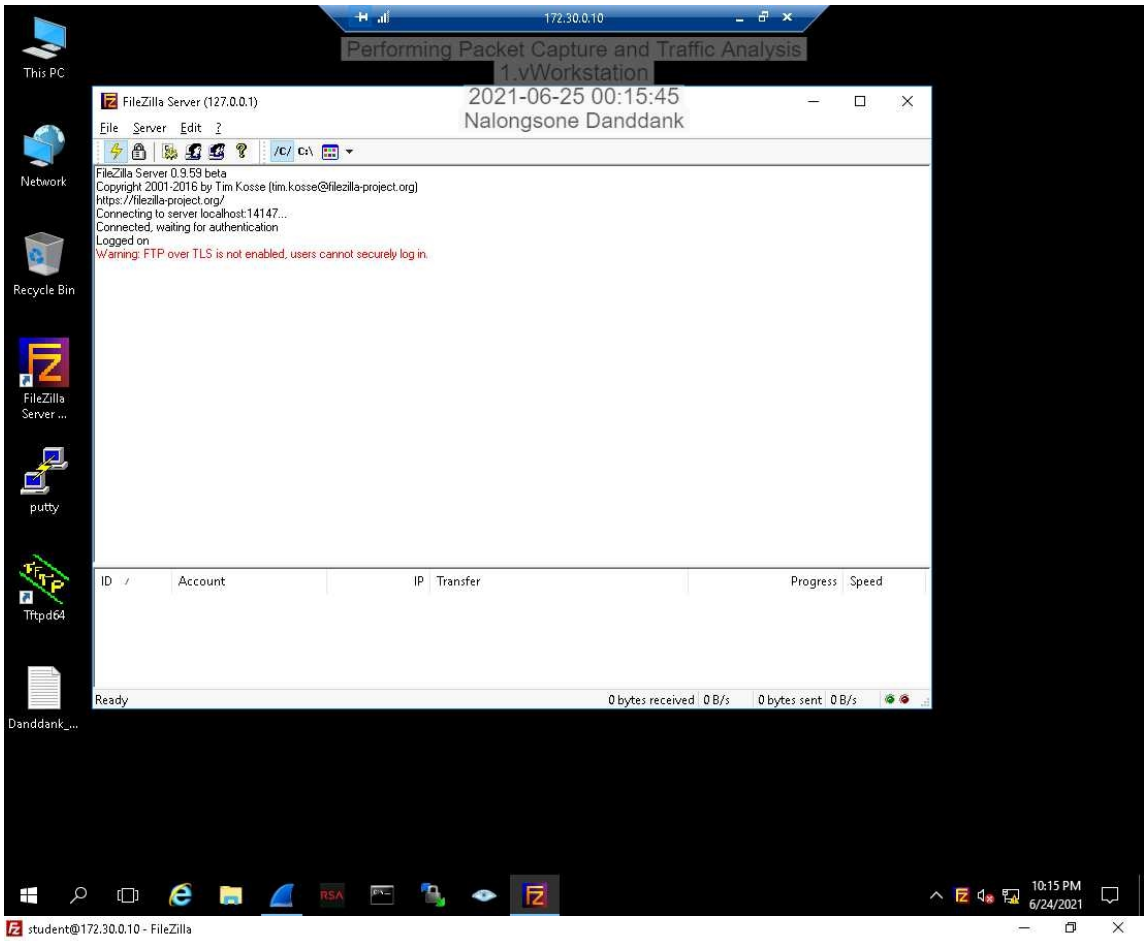

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:03:51
Tftpd64 by Ph. Jounin
Nalongsone Danddank
Current Directory C:\Users\Administrator\Desktop
Server interfaces 172.30.0.10 vmxnet3 Ethernet Adapter
Browse
Show Dir
Tftp Server
peer
total
timeo...
172.18.20.99 vmxnet3 Ethernet Adapter
172.18.5.99 vmxnet3 Ethernet Adapter
172.18.8.99 vmxnet3 Ethernet Adapter
172.30.0.10 vmxnet3 Ethernet Adapter
192.168.105.2 vmxnet3 Ethernet Adapter #2
About
Settings
Help
This PC
Network
Recycle Bin
FileZilla Server ...
putty
Tftpd64
10:03 PM

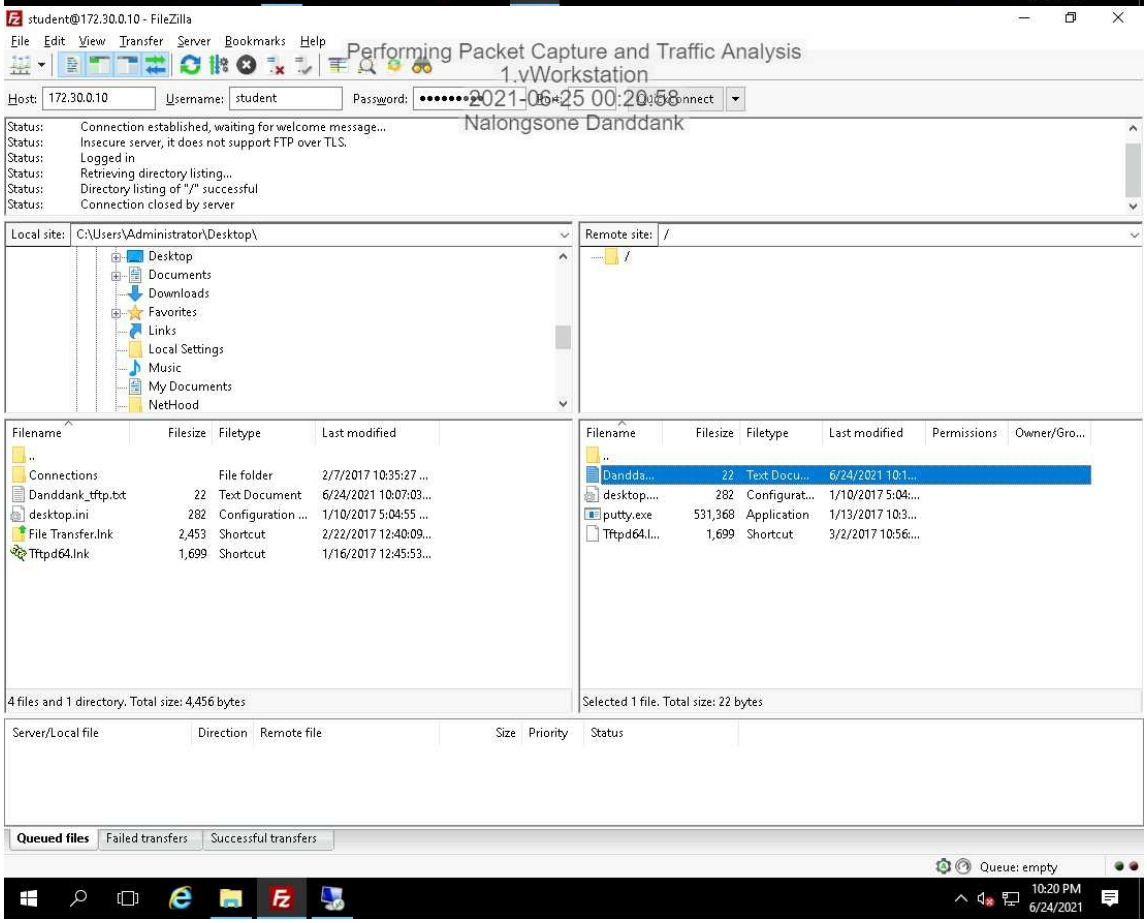

Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:05:46
Nalongsone Danddank
This PC
Network
Recycle Bin
Connections
File Transfer
Tftpd64
Danddank_tftp
10:05 PM
6/24/2021

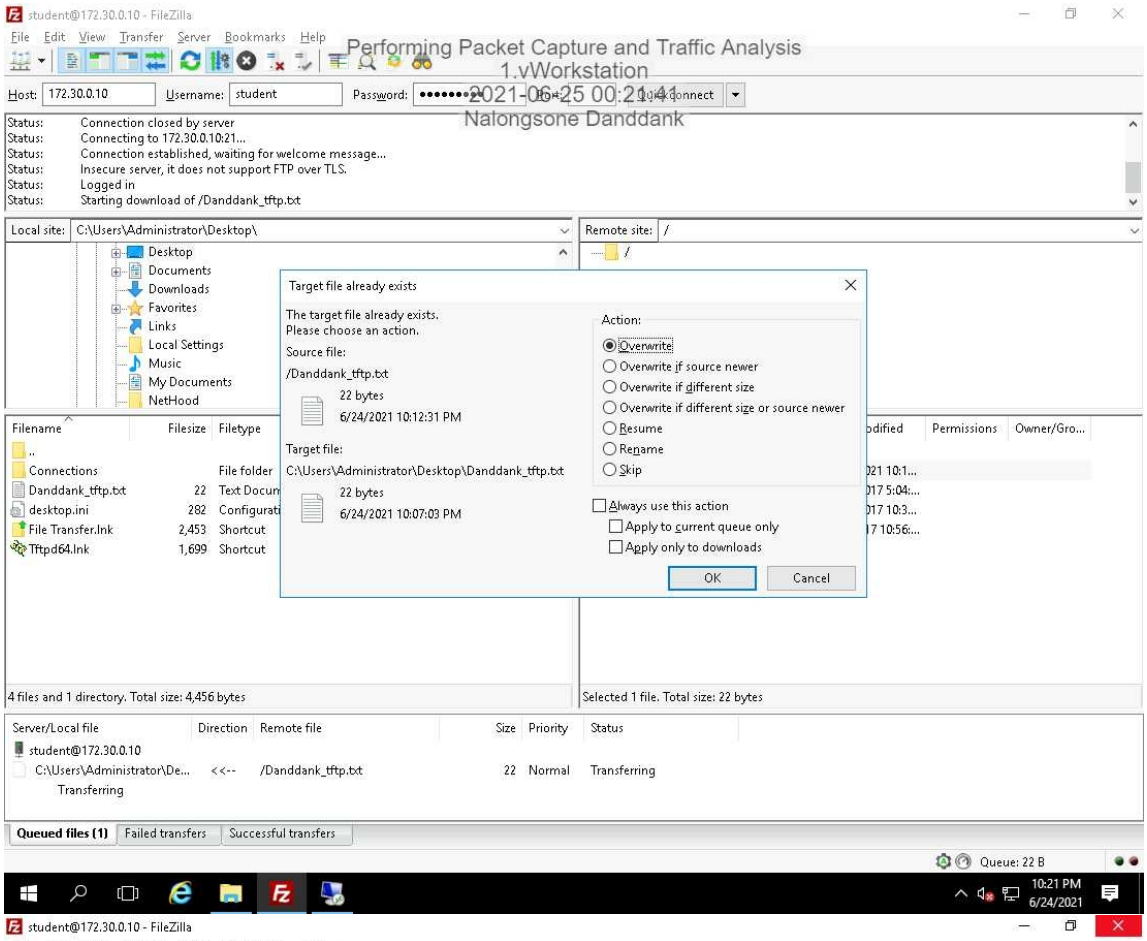

Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:07:16
Nalongsone Danddank
Danddank_tftp - Notepad
File Edit Format View Help
This is a test of TFTP
This PC
Network
Recycle Bin
Connections
File Transfer
Tftpd64
10:07 PM
6/24/2021

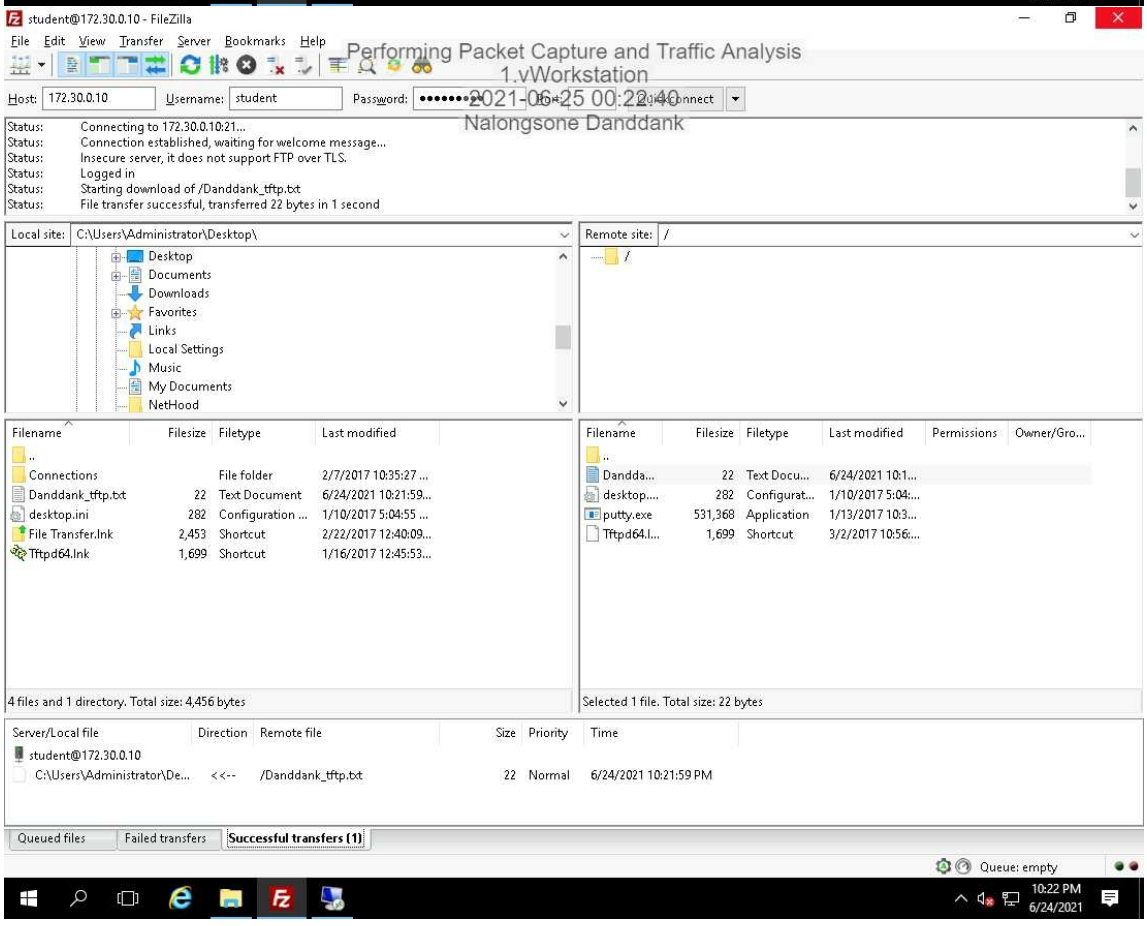

Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:12:35
Nalongsone Danddank
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>tftp 172.30.0.10 put c:\users\administrator\desktop\Danddank_tftp.txt
Transfer successful: 22 bytes in 1 second(s), 22 bytes/s
C:\Users\Administrator>
This PC
Danddank_...
Network
Recycle Bin
Connections
File Transfer
Tftpd64
10:12 PM
6/24/2021

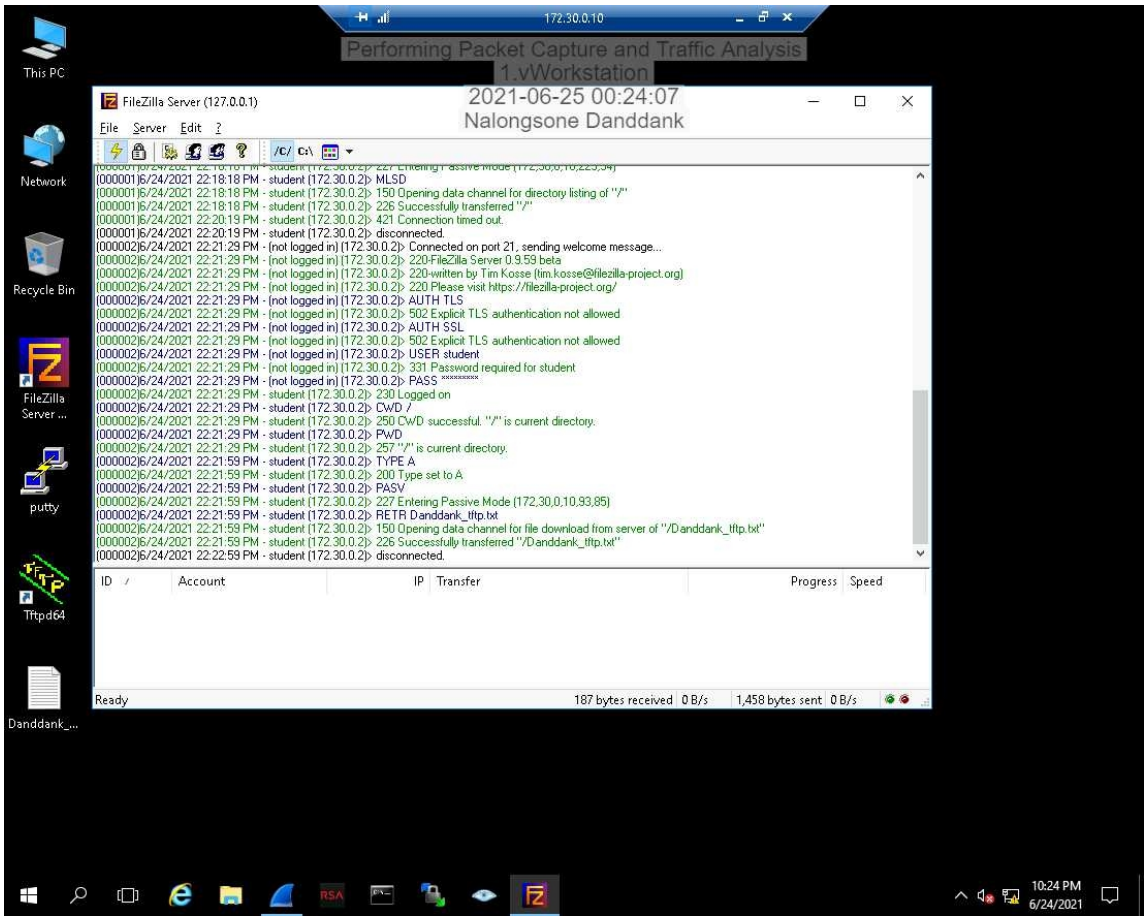

172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:14:17
Nalongsone Danddank
Tftpd64 by Ph. Jounin
Current Directory
C:\Users\Administrator\Desktop
Browse
Server interfaces
172.30.0.10
vmxnet3 Ethernet Adapter
Show Dir
Tftp Server
peer
total
timeo...
Tftpd64: directory
Danddank_tftp.txt 6/24/2021 22
desktop.ini 1/10/2017 282
putty.exe 1/13/2017 531368
Tftpd64.lnk 3/2/2017 1699
Close
Copy
Explorer
About
Settings
Help
This PC
Network
Recycle Bin
FileZilla Server ...
putty
Tftpd64
Danddank_...
10:14 PM


172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:15:45
Nalongsone Danddank
FileZilla Server (127.0.0.1)
File Server Edit ?
FileZilla Server 0.9.59 beta
Copyright 2001-2016 by Tim Kosse (tim.kosse@filezilla-project.org)
https://filezilla-project.org/
Connecting to server localhost:14147...
Connected, waiting for authentication
Logged on
Warning: FTP over TLS is not enabled, users cannot securely log in.
ID / Account IP Transfer Progress Speed
Ready
0 bytes received 0 B/s
0 bytes sent 0 B/s
This PC
Network
Recycle Bin
FileZilla Server ...
putty
Tftpd64
Danddank_...
10:15 PM
6/24/2021

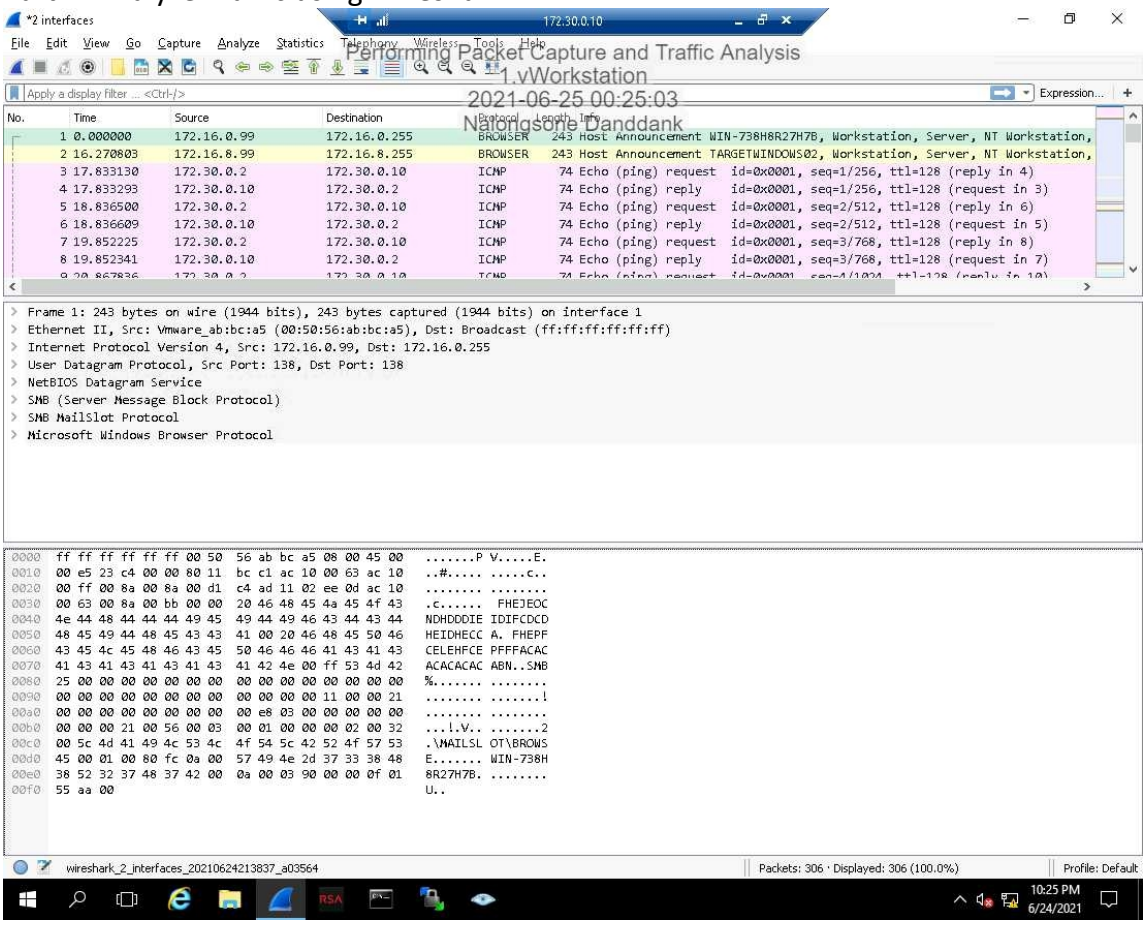

student@172.30.0.10 - FileZilla
File Edit View Transfer Server Bookmarks Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:20:58
Nalongsone Danddank
Host: 172.30.0.10 Username: student Password: Quickconnect
Status: Connection established, waiting for welcome message...
Status: Insecure server, it does not support FTP over TLS.
Status: Logged in
Status: Retrieving directory listing...
Status: Directory listing of "/" successful
Status: Connection closed by server
Local site: C:\Users\Administrator\Desktop\
Remote site: /
Desktop
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
Filename Filesize Filetype Last modified
Connections File folder 2/7/2017 10:35:27 ...
Danddank_tftp.txt 22 Text Document 6/24/2021 10:07:03...
desktop.ini 282 Configuration ... 1/10/2017 5:04:55 ...
File Transfer.lnk 2,453 Shortcut 2/22/2017 12:40:09...
Tftpd64.lnk 1,699 Shortcut 1/16/2017 12:45:53...
Filename Filesize Filetype Last modified Permissions Owner/Gro...
Dandda... 22 Text Docu... 6/24/2021 10:1...
desktop.... 282 Configurat... 1/10/2017 5:04:...
putty.exe 531,368 Application 1/13/2017 10:3...
Tftpd64.l... 1,699 Shortcut 3/2/2017 10:56:...
4 files and 1 directory. Total size: 4,456 bytes
Selected 1 file. Total size: 22 bytes
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers
Queue: empty
10:20 PM
6/24/2021

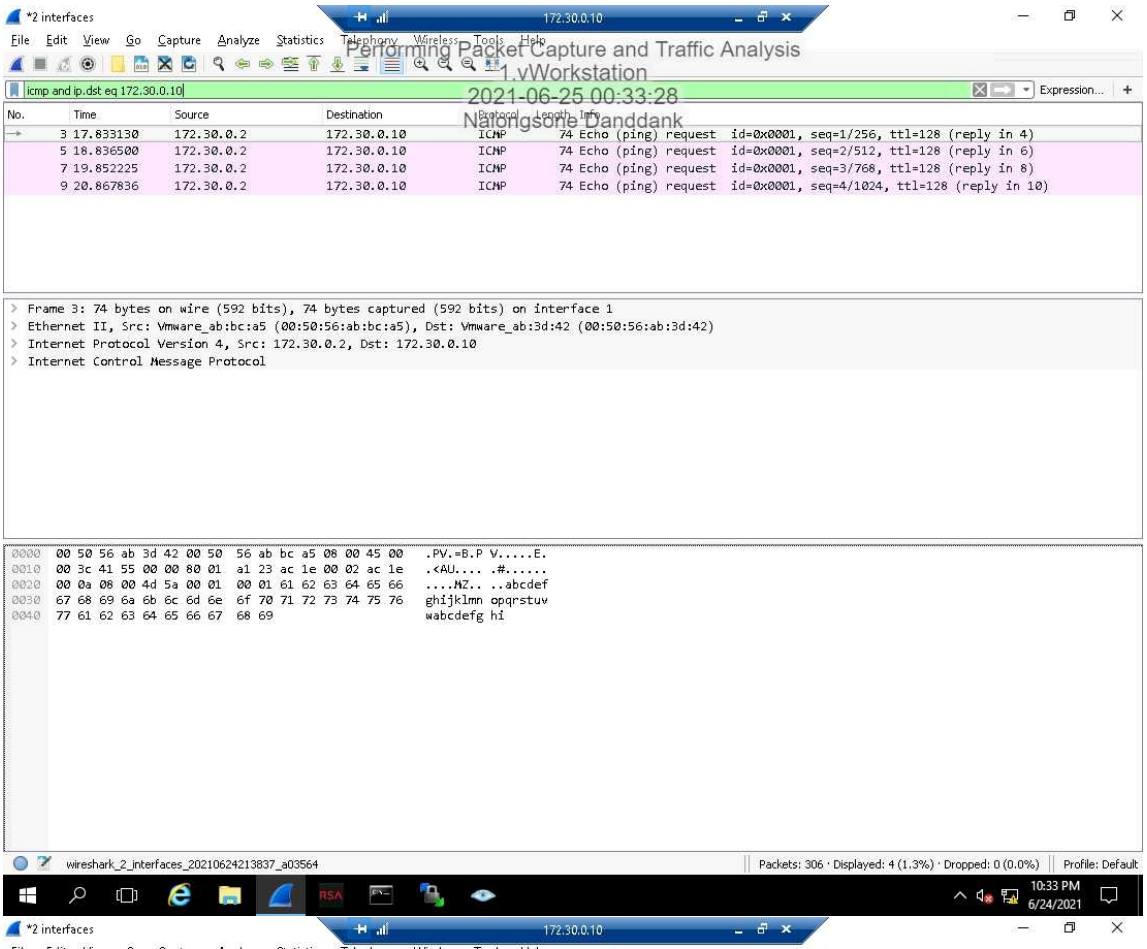

student@172.30.0.10 - FileZilla
File Edit View Transfer Server Bookmarks Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:21:44
Nalongsone Danddank
Host: 172.30.0.10 Username: student Password: Quickconnect
Status: Connection closed by server
Status: Connecting to 172.30.0.10:21...
Status: Connection established, waiting for welcome message...
Status: Insecure server, it does not support FTP over TLS.
Status: Logged in
Status: Starting download of /Danddank_tftp.txt
Local site: C:\Users\Administrator\Desktop\
Remote site: /
Desktop
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
Target file already exists
The target file already exists.
Please choose an action.
Source file:
/Danddank_tftp.txt
22 bytes
6/24/2021 10:12:31 PM
Target file:
C:\Users\Administrator\Desktop\Danddank_tftp.txt
22 bytes
6/24/2021 10:07:09 PM
Action:
Overwrite
Overwrite if source newer
Overwrite if different size
Overwrite if different size or source newer
Resume
Rename
Skip
Always use this action
Apply to current queue only
Apply only to downloads
OK
Cancel
Filename Filesize Filetype
Connections File folder
Danddank_tftp.txt 22 Text Docu
desktop.ini 282 Configurati
File Transfer.lnk 2,453 Shortcut
Tftpd64.lnk 1,699 Shortcut
4 files and 1 directory. Total size: 4,456 bytes
Selected 1 file. Total size: 22 bytes
Server/Local file Direction Remote file Size Priority Status
student@172.30.0.10
C:\Users\Administrator\De... <<-- /Danddank_tftp.txt 22 Normal Transferring
Transferring
Queued files (1) Failed transfers Successful transfers
Queue: 22 B
10:21 PM
6/24/2021

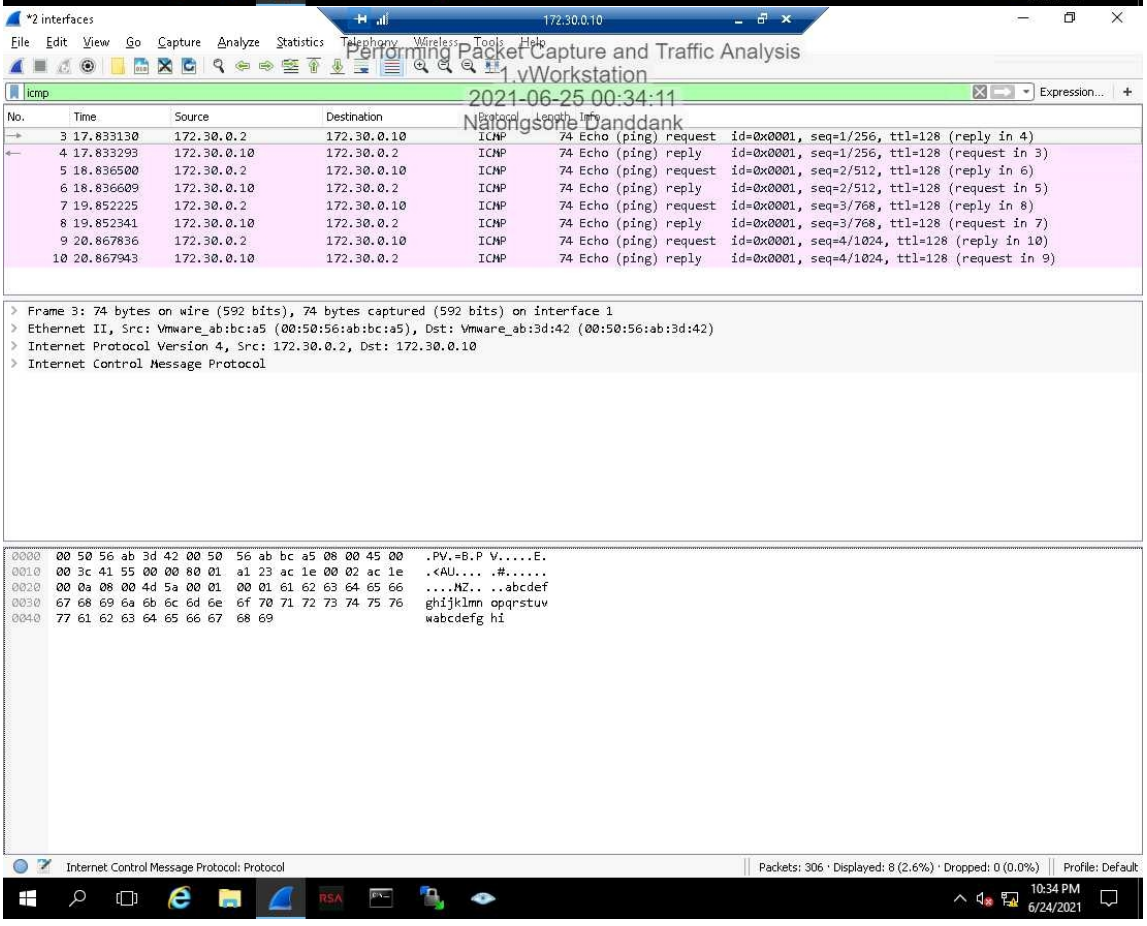

student@172.30.0.10 - FileZilla
File Edit View Transfer Server Bookmarks Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:22:40
Nalongsone Danddank
Host: 172.30.0.10 Username: student Password: Quickconnect
Status: Connecting to 172.30.0.10:21...
Status: Connection established, waiting for welcome message...
Status: Insecure server, it does not support FTP over TLS.
Status: Logged in
Status: Starting download of /Danddank_tftp.txt
Status: File transfer successful, transferred 22 bytes in 1 second
Local site: C:\Users\Administrator\Desktop\
Remote site: /
Desktop
Documents
Downloads
Favorites
Links
Local Settings
Music
My Documents
NetHood
Filename Filesize Filetype Last modified
Connections File folder 2/7/2017 10:35:27 ...
Danddank_tftp.txt 22 Text Document 6/24/2021 10:21:59...
desktop.ini 282 Configuration ... 1/10/2017 5:04:55 ...
File Transfer.lnk 2,453 Shortcut 2/22/2017 12:40:09...
Tftpd64.lnk 1,699 Shortcut 1/16/2017 12:45:53...
Filename Filesize Filetype Last modified Permissions Owner/Gro...
Dandda... 22 Text Docu... 6/24/2021 10:1...
desktop.... 282 Configurat... 1/10/2017 5:04:...
putty.exe 531,368 Application 1/13/2017 10:3...
Tftpd64.l... 1,699 Shortcut 3/2/2017 10:56:...
4 files and 1 directory. Total size: 4,456 bytes
Selected 1 file. Total size: 22 bytes
Server/Local file Direction Remote file Size Priority Time
student@172.30.0.10
C:\Users\Administrator\De... <<-- /Danddank_tftp.txt 22 Normal 6/24/2021 10:21:59 PM
Queued files Failed transfers Successful transfers (1)
Queue: empty
10:22 PM
6/24/2021

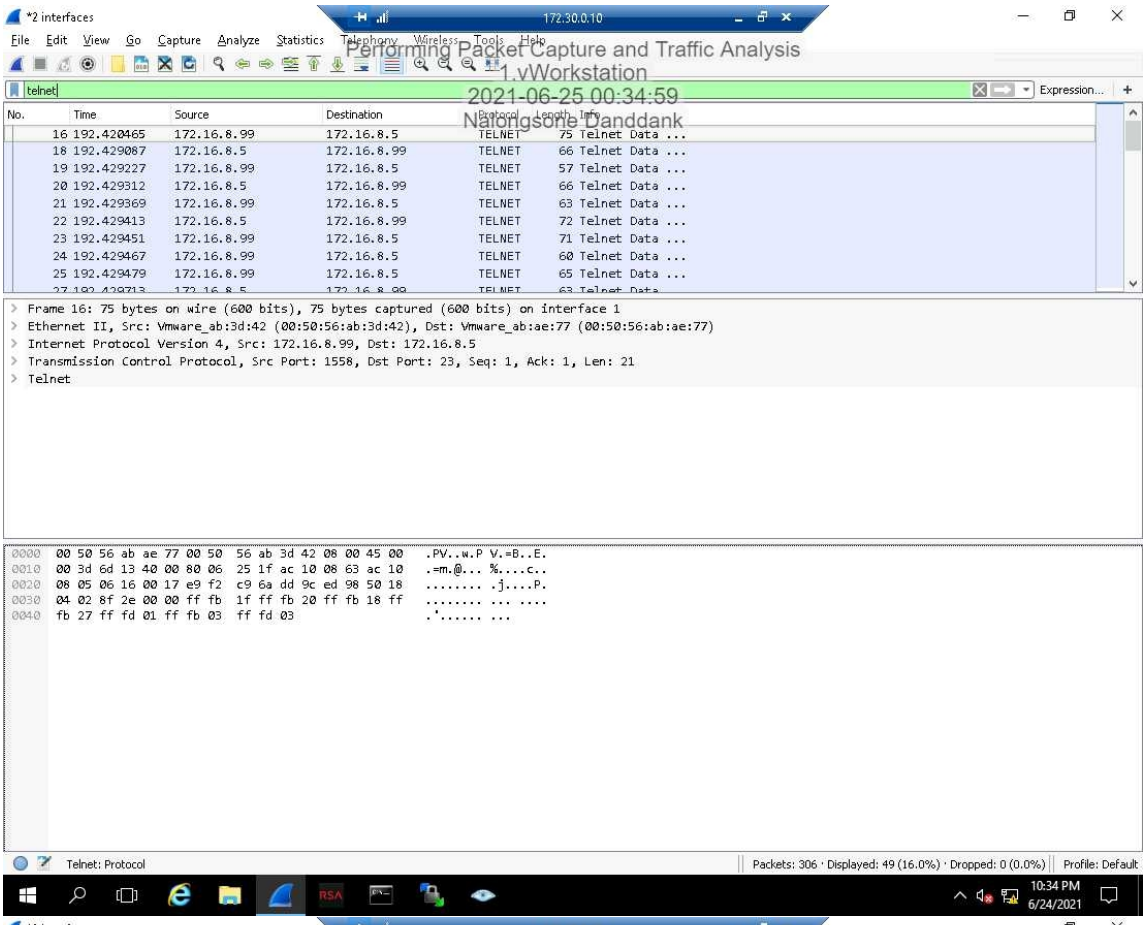


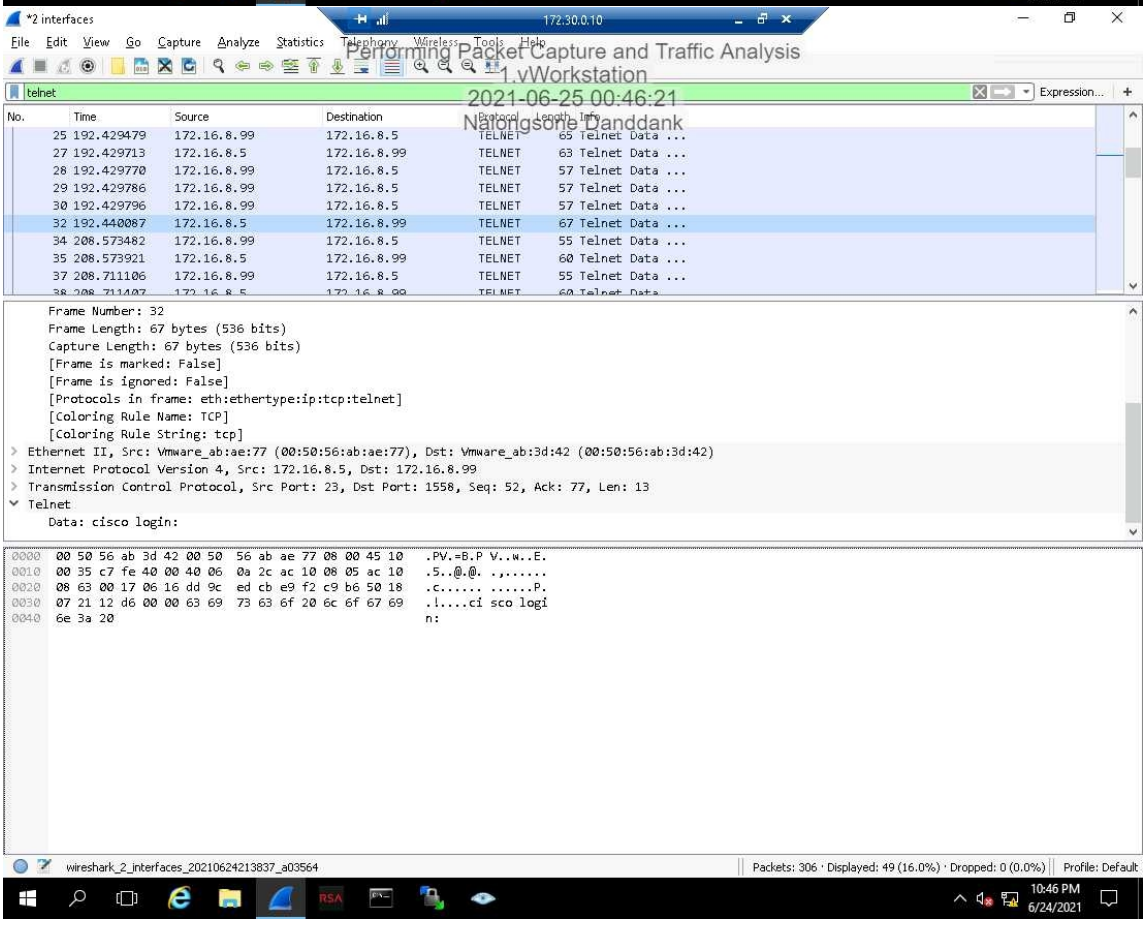
Part 2: Analyze Traffic using Wireshark.

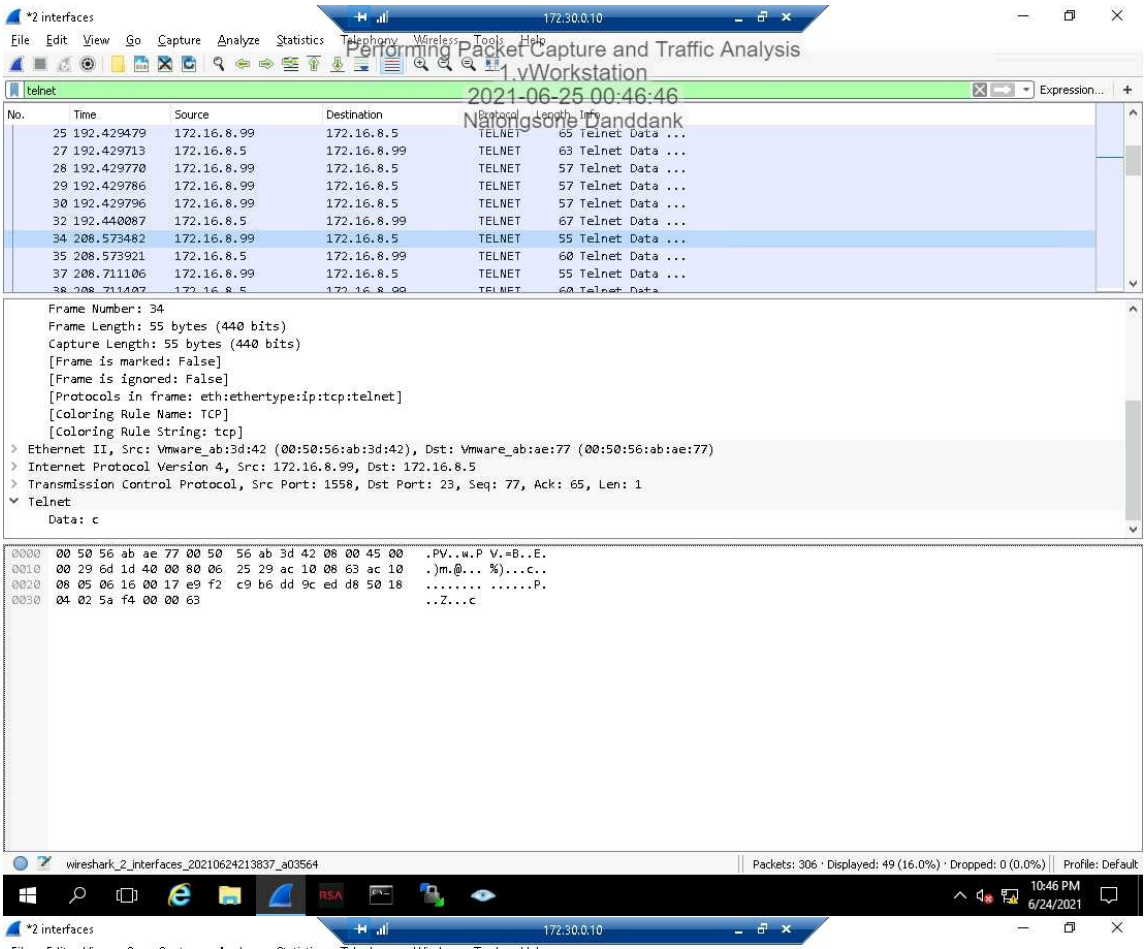


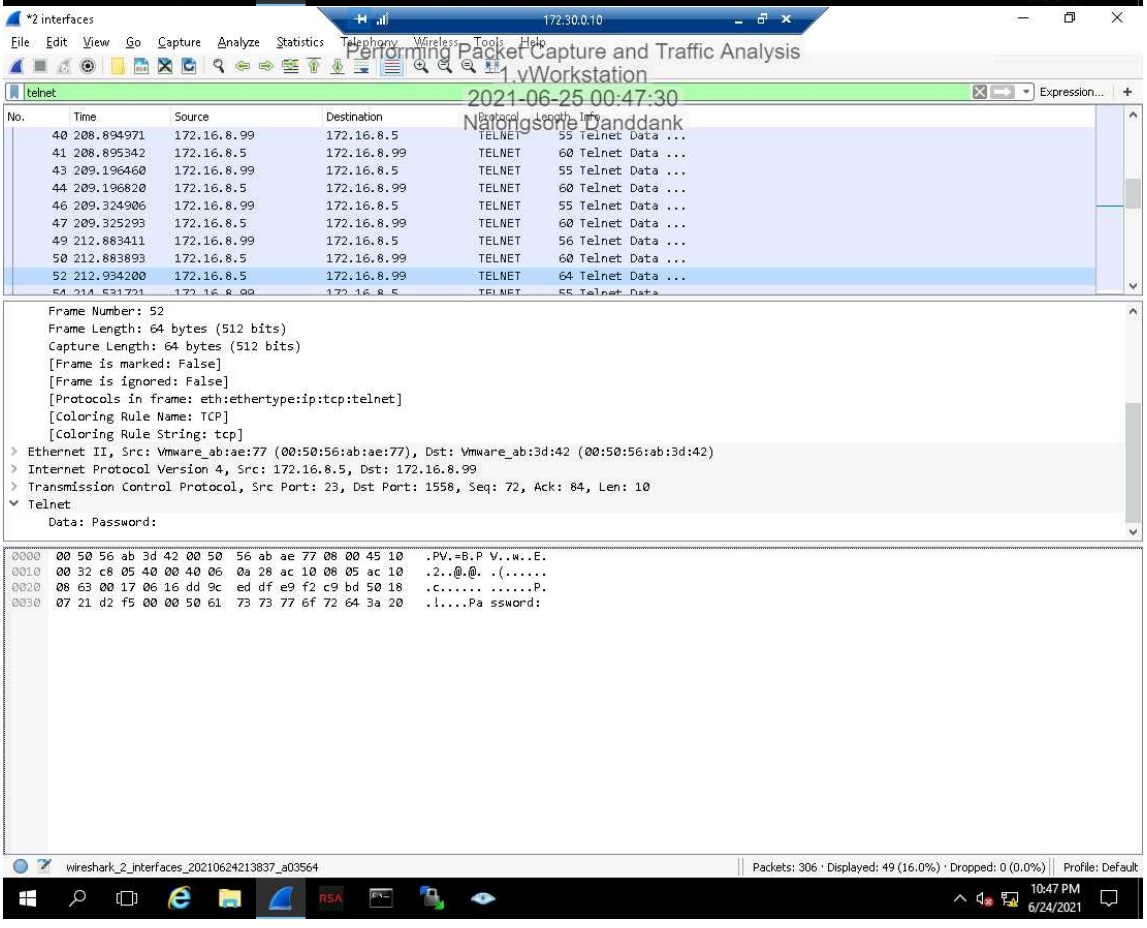

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:33:28
Nalorlgsone Danddank
icmp and ip.dst eq 172.30.0.10
Expression...
No. Time Source Destination Protocol Length Info
3 17.833130 172.30.0.2 172.30.0.10 ICMP 74 Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 4)
5 18.836500 172.30.0.2 172.30.0.10 ICMP 74 Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 6)
7 19.852225 172.30.0.2 172.30.0.10 ICMP 74 Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 8)
9 20.867836 172.30.0.2 172.30.0.10 ICMP 74 Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 10)
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 1
Ethernet II, Src: Vmware_ab:bc:a5 (00:50:56:ab:bc:a5), Dst: Vmware_ab:3d:42 (00:50:56:ab:3d:42)
Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.10
Internet Control Message Protocol
0000 00 50 56 ab 3d 42 00 50 56 ab bc a5 08 00 45 00 .PV.=B.P V.....E.
0010 00 3c 41 55 00 00 80 01 a1 23 ac 1e 00 02 ac 1e .<AU.... .#.....
0020 00 0a 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 ....MZ.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
wireshark_2_interfaces_20210624213837_a03564
Packets: 306 · Displayed: 4 (1.3%) · Dropped: 0 (0.0%)
Profile: Default
10:33 PM
6/24/2021

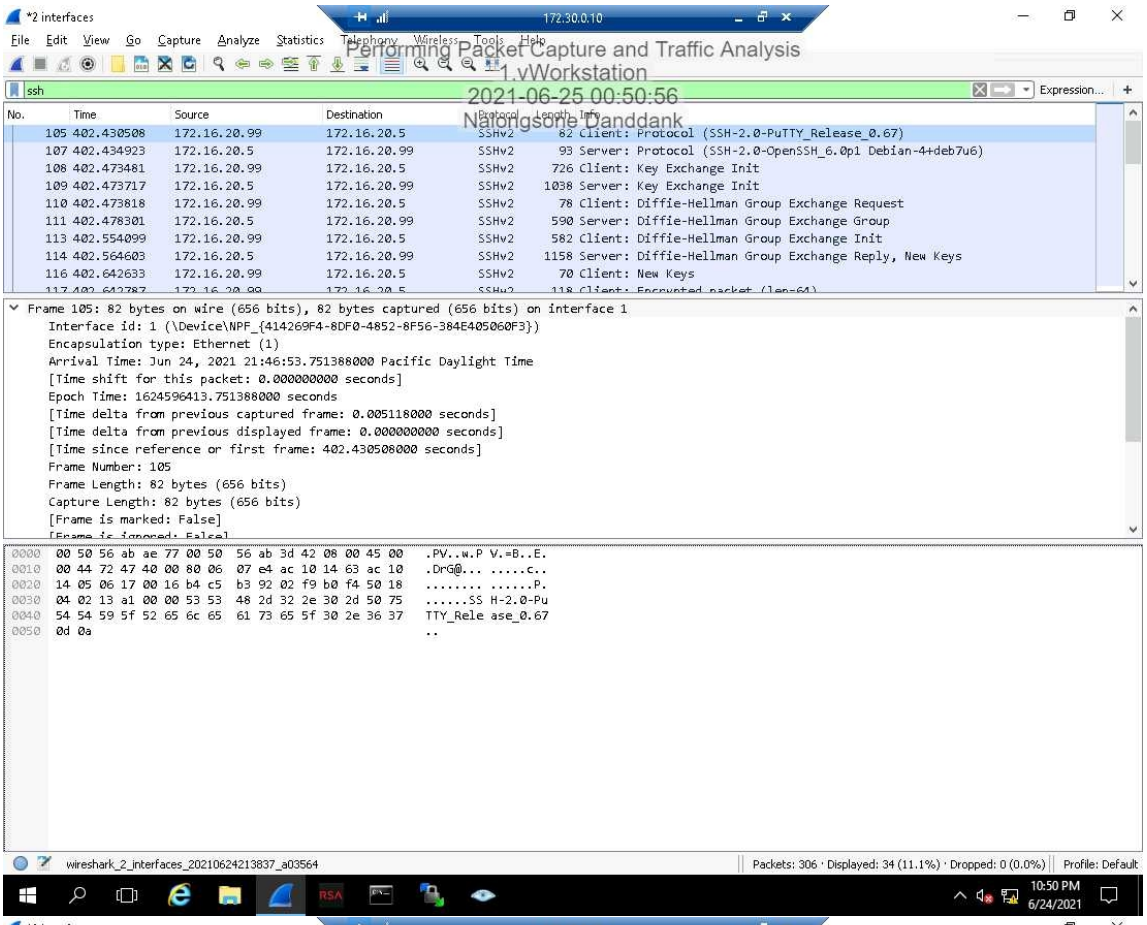

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:34:11
Nalorlgsone Danddank
icmp
Expression...
No. Time Source Destination Protocol Length Info
3 17.833130 172.30.0.2 172.30.0.10 ICMP 74 Echo (ping) request id=0x0001, seq=1/256, ttl=128 (reply in 4)
4 17.833293 172.30.0.10 172.30.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=1/256, ttl=128 (request in 3)
5 18.836500 172.30.0.2 172.30.0.10 ICMP 74 Echo (ping) request id=0x0001, seq=2/512, ttl=128 (reply in 6)
6 18.836609 172.30.0.10 172.30.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=2/512, ttl=128 (request in 5)
7 19.852225 172.30.0.2 172.30.0.10 ICMP 74 Echo (ping) request id=0x0001, seq=3/768, ttl=128 (reply in 8)
8 19.852341 172.30.0.10 172.30.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=3/768, ttl=128 (request in 7)
9 20.867836 172.30.0.2 172.30.0.10 ICMP 74 Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (reply in 10)
10 20.867943 172.30.0.10 172.30.0.2 ICMP 74 Echo (ping) reply id=0x0001, seq=4/1024, ttl=128 (request in 9)
Frame 3: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 1
Ethernet II, Src: Vmware_ab:bc:a5 (00:50:56:ab:bc:a5), Dst: Vmware_ab:3d:42 (00:50:56:ab:3d:42)
Internet Protocol Version 4, Src: 172.30.0.2, Dst: 172.30.0.10
Internet Control Message Protocol
0000 00 50 56 ab 3d 42 00 50 56 ab bc a5 08 00 45 00 .PV.=B.P V.....E.
0010 00 3c 41 55 00 00 80 01 a1 23 ac 1e 00 02 ac 1e .<AU.... .#.....
0020 00 0a 08 00 4d 5a 00 01 00 01 61 62 63 64 65 66 ....MZ.. ..abcdef
0030 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 ghijklmn opqrstuv
0040 77 61 62 63 64 65 66 67 68 69 wabcdefg hi
Internet Control Message Protocol: Protocol
Packets: 306 · Displayed: 8 (2.6%) · Dropped: 0 (0.0%)
Profile: Default
10:34 PM
6/24/2021

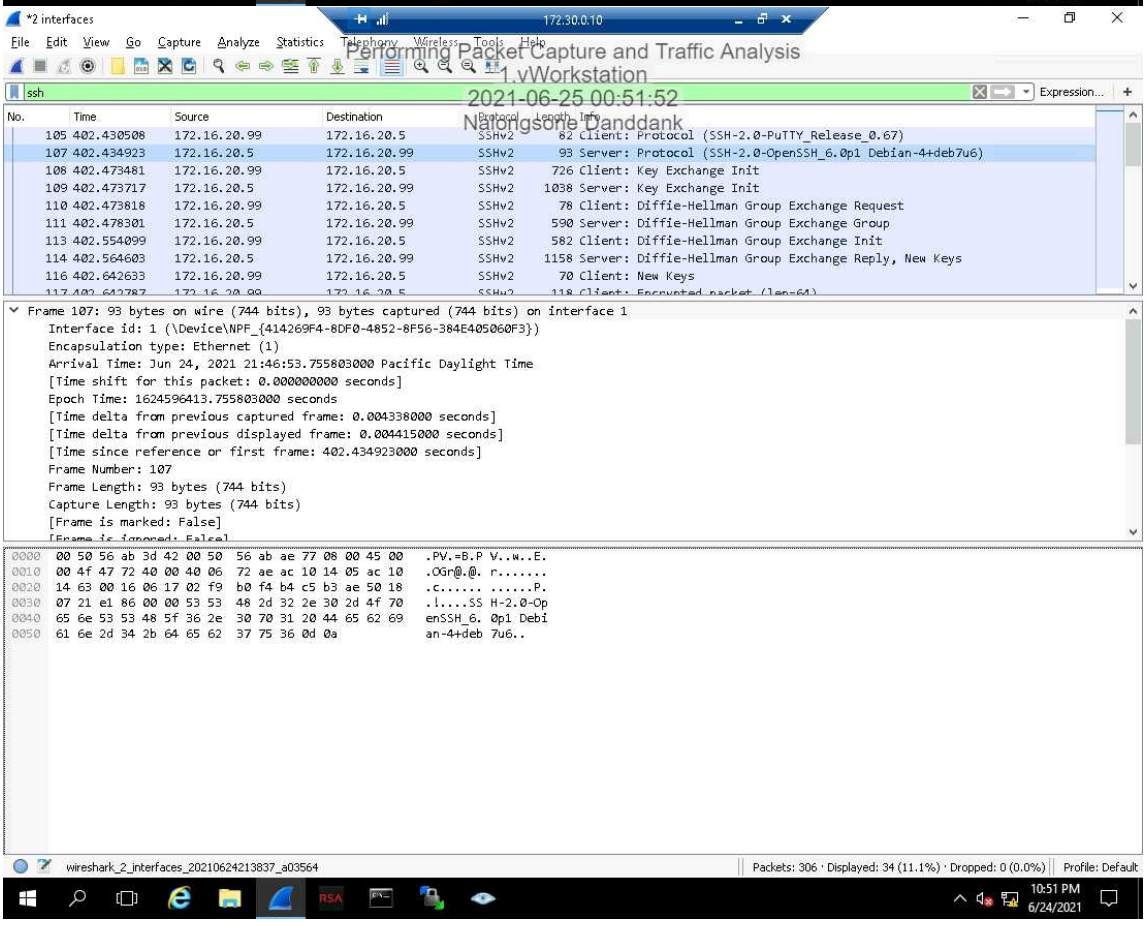

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:34:59
Nalongsone Danddank
telnet
Expression...
No. Time Source Destination Protocol Length Info
16 192.420465 172.16.8.99 172.16.8.5 TELNET 75 Telnet Data ...
18 192.429087 172.16.8.5 172.16.8.99 TELNET 66 Telnet Data ...
19 192.429227 172.16.8.99 172.16.8.5 TELNET 57 Telnet Data ...
20 192.429312 172.16.8.5 172.16.8.99 TELNET 66 Telnet Data ...
21 192.429369 172.16.8.99 172.16.8.5 TELNET 63 Telnet Data ...
22 192.429413 172.16.8.5 172.16.8.99 TELNET 72 Telnet Data ...
23 192.429451 172.16.8.99 172.16.8.5 TELNET 71 Telnet Data ...
24 192.429467 172.16.8.99 172.16.8.5 TELNET 60 Telnet Data ...
25 192.429479 172.16.8.99 172.16.8.5 TELNET 65 Telnet Data ...
Frame 16: 75 bytes on wire (600 bits), 75 bytes captured (600 bits) on interface 1
Ethernet II, Src: Vmware_ab:3d:42 (00:50:56:ab:3d:42), Dst: Vmware_ab:ae:77 (00:50:56:ab:ae:77)
Internet Protocol Version 4, Src: 172.16.8.99, Dst: 172.16.8.5
Transmission Control Protocol, Src Port: 1558, Dst Port: 23, Seq: 1, Ack: 1, Len: 21
Telnet
0000 00 50 56 ab ae 77 00 50 56 ab 3d 42 08 00 45 00 .PV..w.P V.=B..E.
0010 00 3d 6d 13 40 00 80 06 25 1f ac 10 08 63 ac 10 .=m.@... %....c..
0020 08 05 06 16 00 17 e9 f2 c9 6a dd 9c ed 98 50 18 .... .j....P.
0030 04 02 8f 2e 00 00 ff fb 1f ff fb 20 ff fb 18 ff ....
0040 fb 27 ff fd 01 ff fb 03 ff fd 03 .'...... ...
Telnet: Protocol
Packets: 306 · Displayed: 49 (16.0%) · Dropped: 0 (0.0%)
Profile: Default
10:34 PM
6/24/2021

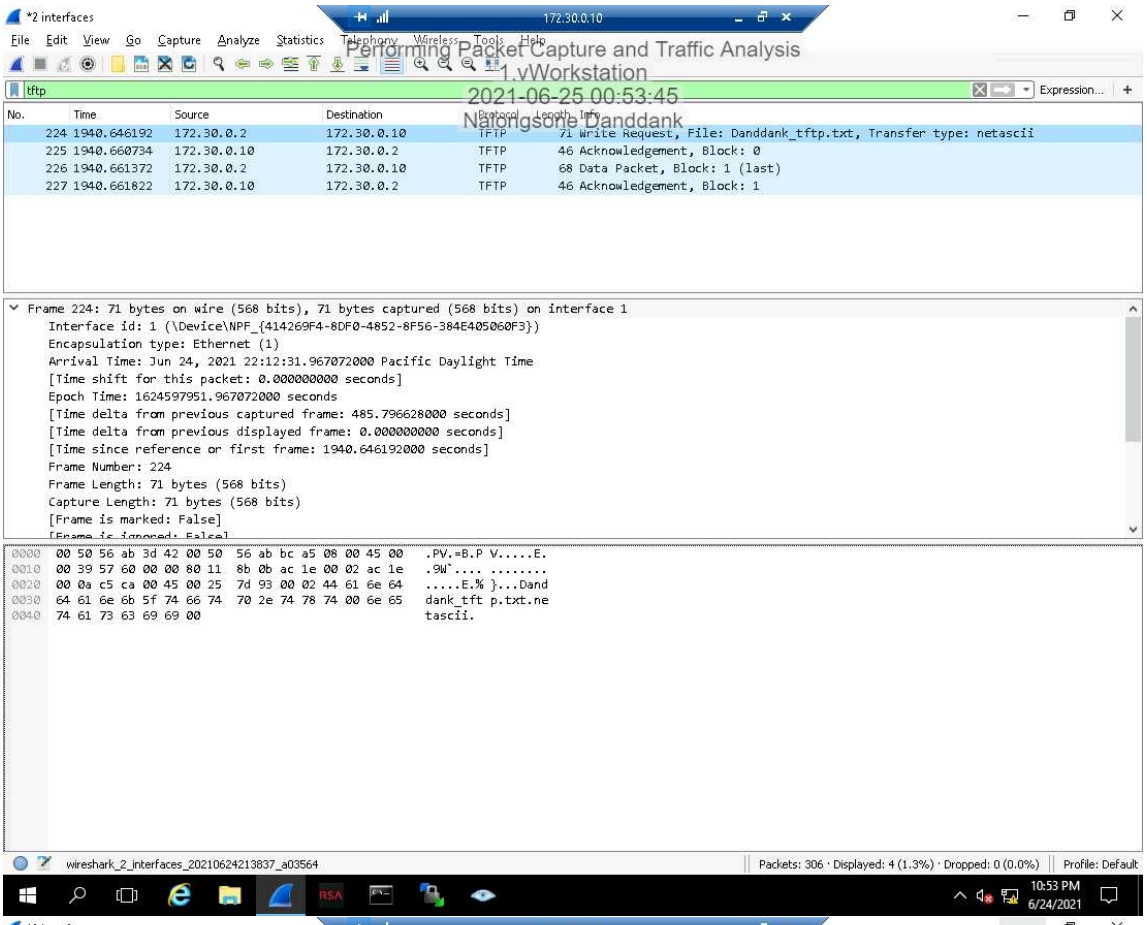

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:46:21
Nalongsone Danddank
telnet
Expression...
No. Time Source Destination Protocol Length Info
25 192.429479 172.16.8.99 172.16.8.5 TELNET 65 Telnet Data ...
27 192.429713 172.16.8.5 172.16.8.99 TELNET 63 Telnet Data ...
28 192.429770 172.16.8.99 172.16.8.5 TELNET 57 Telnet Data ...
29 192.429786 172.16.8.99 172.16.8.5 TELNET 57 Telnet Data ...
30 192.429796 172.16.8.99 172.16.8.5 TELNET 57 Telnet Data ...
32 192.440087 172.16.8.5 172.16.8.99 TELNET 67 Telnet Data ...
34 208.573482 172.16.8.99 172.16.8.5 TELNET 55 Telnet Data ...
35 208.573921 172.16.8.5 172.16.8.99 TELNET 60 Telnet Data ...
37 208.711106 172.16.8.99 172.16.8.5 TELNET 55 Telnet Data ...
Frame Number: 32
Frame Length: 67 bytes (536 bits)
Capture Length: 67 bytes (536 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:telnet]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Vmware_ab:ae:77 (00:50:56:ab:ae:77), Dst: Vmware_ab:3d:42 (00:50:56:ab:3d:42)
Internet Protocol Version 4, Src: 172.16.8.5, Dst: 172.16.8.99
Transmission Control Protocol, Src Port: 23, Dst Port: 1558, Seq: 52, Ack: 77, Len: 13
Telnet
Data: cisco login:
0000 00 50 56 ab 3d 42 00 50 56 ab ae 77 08 00 45 10 .PV.=B.P V..w..E.
0010 00 35 c7 fe 40 00 40 06 0a 2c ac 10 08 05 ac 10 .5..@.@. .,......
0020 08 63 00 17 06 16 dd 9c ed cb e9 f2 c9 b6 50 18 .c...... ......P.
0030 07 21 12 d6 00 00 63 69 73 63 6f 20 6c 6f 67 69 .!....ci sco logi
0040 6e 3a 20 n:
wireshark_2_interfaces_20210624213837_a03564
Packets: 306 · Displayed: 49 (16.0%) · Dropped: 0 (0.0%)
Profile: Default
10:46 PM
6/24/2021

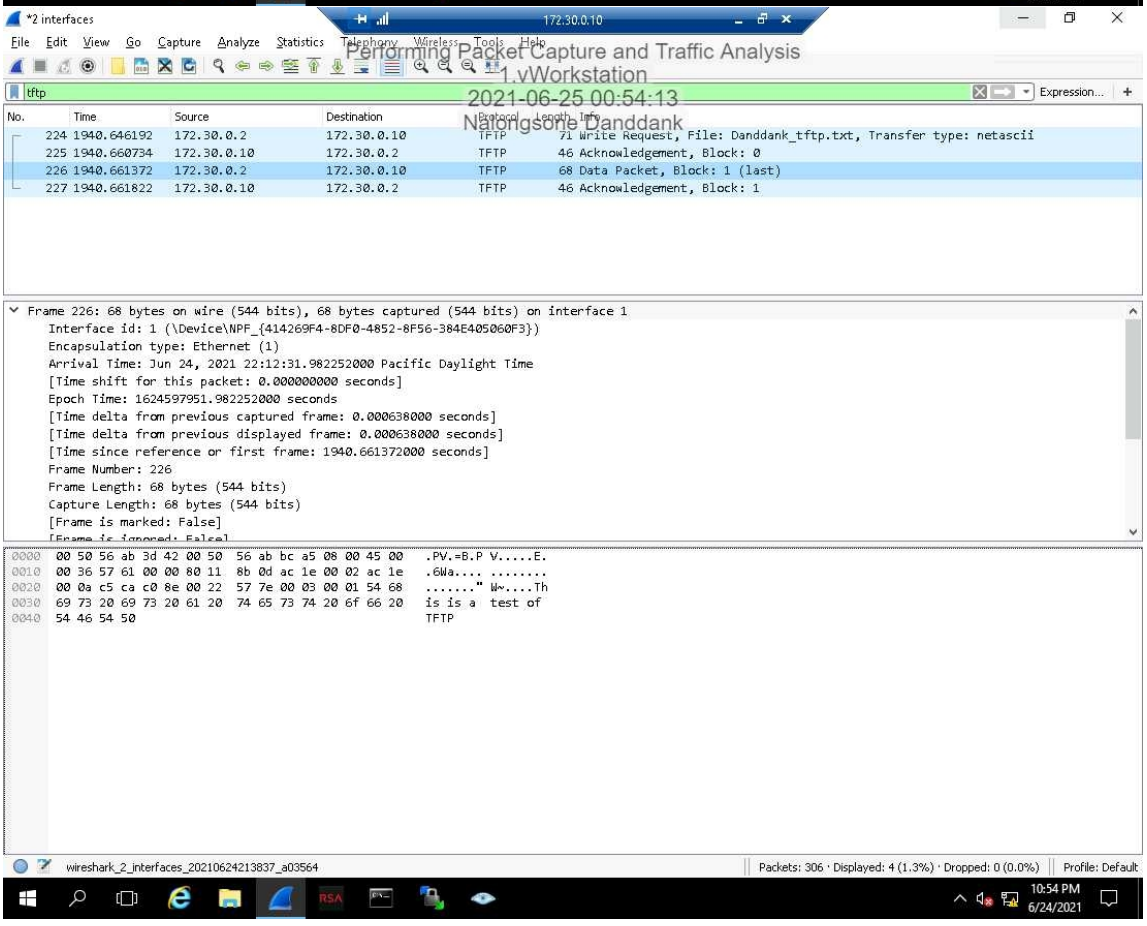

*2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:46:46
Nalongsone Danddank
telnet
Expression...
No. Time Source Destination Protocol Length Info
25 192.429479 172.16.8.99 172.16.8.5 TELNET 65 Telnet Data ...
27 192.429713 172.16.8.5 172.16.8.99 TELNET 63 Telnet Data ...
28 192.429770 172.16.8.99 172.16.8.5 TELNET 57 Telnet Data ...
29 192.429786 172.16.8.99 172.16.8.5 TELNET 57 Telnet Data ...
30 192.429796 172.16.8.99 172.16.8.5 TELNET 57 Telnet Data ...
32 192.440087 172.16.8.5 172.16.8.99 TELNET 67 Telnet Data ...
34 208.573482 172.16.8.99 172.16.8.5 TELNET 55 Telnet Data ...
35 208.573921 172.16.8.5 172.16.8.99 TELNET 60 Telnet Data ...
37 208.711106 172.16.8.99 172.16.8.5 TELNET 55 Telnet Data ...
Frame Number: 34
Frame Length: 55 bytes (440 bits)
Capture Length: 55 bytes (440 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:telnet]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Vmware_ab:3d:42 (00:50:56:ab:3d:42), Dst: Vmware_ab:ae:77 (00:50:56:ab:ae:77)
Internet Protocol Version 4, Src: 172.16.8.99, Dst: 172.16.8.5
Transmission Control Protocol, Src Port: 1558, Dst Port: 23, Seq: 77, Ack: 65, Len: 1
Telnet
Data: c
0000 00 50 56 ab ae 77 00 50 56 ab 3d 42 08 00 45 00 .PV..w.P V.=B..E.
0010 00 29 6d 1d 40 00 80 06 25 29 ac 10 08 63 ac 10 .)m.@... %)...c..
0020 08 05 06 16 00 17 e9 f2 c9 b6 dd 9c ed d8 50 18 ....P.
0030 04 02 5a f4 00 00 63 ..Z...c
wireshark_2_interfaces_20210624213837_a03564
Packets: 306 · Displayed: 49 (16.0%) · Dropped: 0 (0.0%)
Profile: Default
10:46 PM
6/24/2021

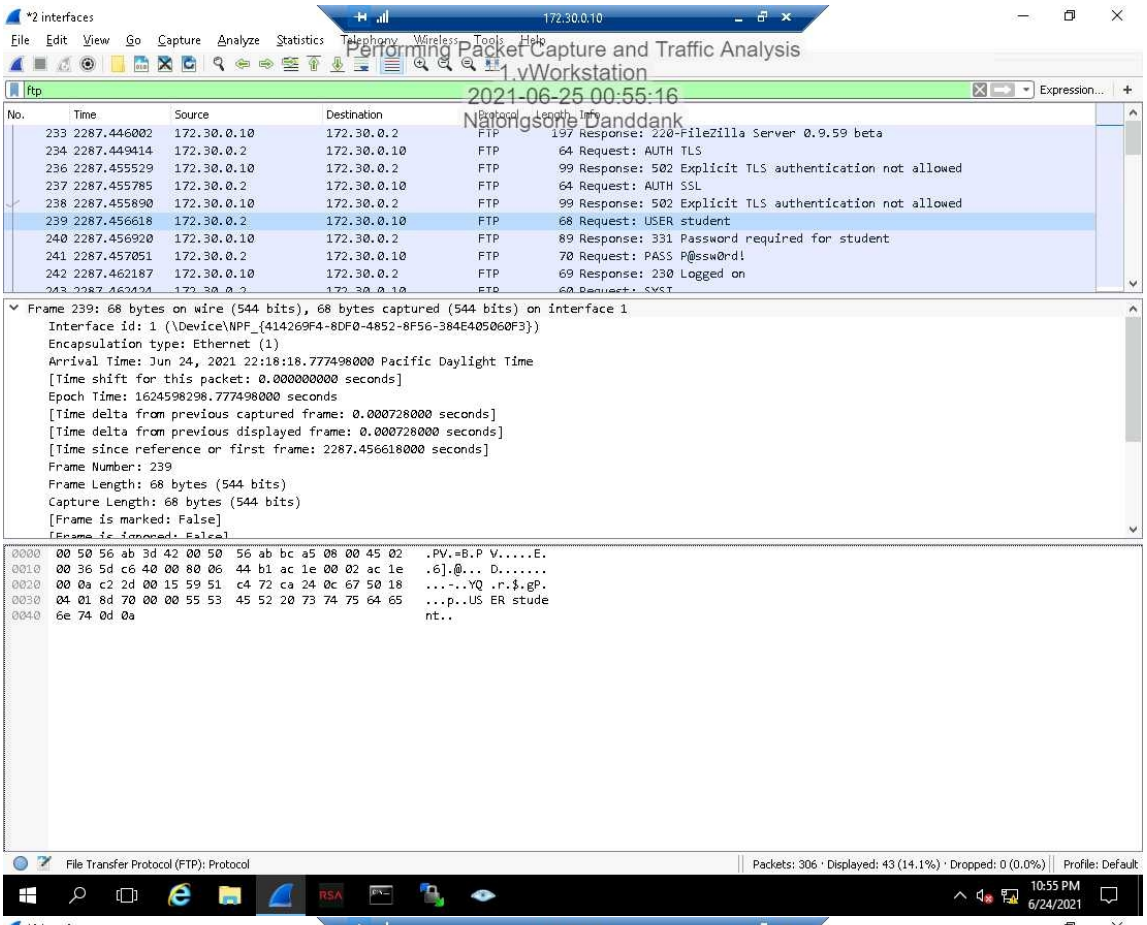

*2 interfaces
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
172.30.0.10
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:47:30
Nalongsone Danddank
telnet
Expression...
No. Time Source Destination Protocol Length Info
40 208.894971 172.16.8.99 172.16.8.5 TELNET 55 Telnet Data ...
41 208.895342 172.16.8.5 172.16.8.99 TELNET 60 Telnet Data ...
43 209.196460 172.16.8.99 172.16.8.5 TELNET 55 Telnet Data ...
44 209.196820 172.16.8.5 172.16.8.99 TELNET 60 Telnet Data ...
46 209.324906 172.16.8.99 172.16.8.5 TELNET 55 Telnet Data ...
47 209.325293 172.16.8.5 172.16.8.99 TELNET 60 Telnet Data ...
49 212.883411 172.16.8.99 172.16.8.5 TELNET 56 Telnet Data ...
50 212.883893 172.16.8.5 172.16.8.99 TELNET 60 Telnet Data ...
52 212.934200 172.16.8.5 172.16.8.99 TELNET 64 Telnet Data ...
Frame Number: 52
Frame Length: 64 bytes (512 bits)
Capture Length: 64 bytes (512 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:tcp:telnet]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Vmware_ab:ae:77 (00:50:56:ab:ae:77), Dst: Vmware_ab:3d:42 (00:50:56:ab:3d:42)
Internet Protocol Version 4, Src: 172.16.8.5, Dst: 172.16.8.99
Transmission Control Protocol, Src Port: 23, Dst Port: 1558, Seq: 72, Ack: 84, Len: 10
Telnet
Data: Password:
0000 00 50 56 ab 3d 42 00 50 56 ab ae 77 08 00 45 10 .PV.=B.P V..w..E.
0010 00 32 c8 05 40 00 40 06 0a 28 ac 10 08 05 ac 10 .2..@.@. .(......
0020 08 63 00 17 06 16 dd 9c ed df e9 f2 c9 bd 50 18 .c..... ......P.
0030 07 21 d2 f5 00 00 50 61 73 73 77 6f 72 64 3a 20 .!....Pa ssword:
wireshark_2_interfaces_20210624213837_a03564
Packets: 306 · Displayed: 49 (16.0%) · Dropped: 0 (0.0%)
Profile: Default
10:47 PM
6/24/2021

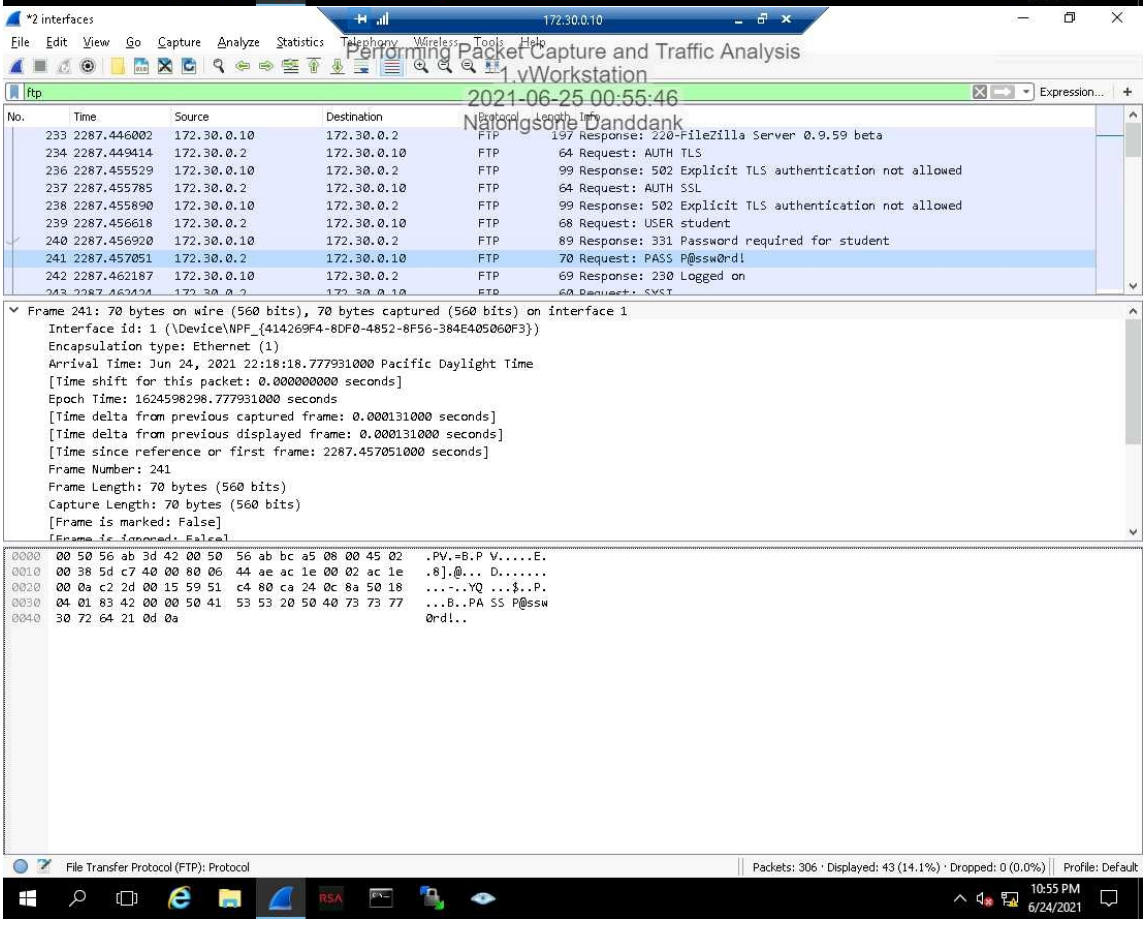

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:50:56
Natorgsone Danddank
ssh
Expression...
No. Time Source Destination Protocol Length Info
105 402.430508 172.16.20.99 172.16.20.5 SSHv2 82 Client: Protocol (SSH-2.0-PuTTY_Release_0.67)
107 402.434923 172.16.20.5 172.16.20.99 SSHv2 93 Server: Protocol (SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u6)
108 402.473481 172.16.20.99 172.16.20.5 SSHv2 726 Client: Key Exchange Init
109 402.473717 172.16.20.5 172.16.20.99 SSHv2 1038 Server: Key Exchange Init
110 402.473818 172.16.20.99 172.16.20.5 SSHv2 78 Client: Diffie-Hellman Group Exchange Request
111 402.478301 172.16.20.5 172.16.20.99 SSHv2 590 Server: Diffie-Hellman Group Exchange Group
113 402.554099 172.16.20.99 172.16.20.5 SSHv2 582 Client: Diffie-Hellman Group Exchange Init
114 402.564603 172.16.20.5 172.16.20.99 SSHv2 1158 Server: Diffie-Hellman Group Exchange Reply, New Keys
116 402.642633 172.16.20.99 172.16.20.5 SSHv2 70 Client: New Keys
Frame 105: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface 1
Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 24, 2021 21:46:53.751388000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1624596413.751388000 seconds
[Time delta from previous captured frame: 0.005118000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 402.430508000 seconds]
Frame Number: 105
Frame Length: 82 bytes (656 bits)
Capture Length: 82 bytes (656 bits)
[Frame is marked: False]
0000 00 50 56 ab ae 77 00 50 56 ab 3d 42 08 00 45 00 .PV..w.P V.=B..E.
0010 00 44 72 47 40 00 80 06 07 e4 ac 10 14 63 ac 10 .DrG@... .....c..
0020 14 05 06 17 00 16 b4 c5 b3 92 02 f9 b0 f4 50 18 .... P.
0030 04 02 13 a1 00 00 53 53 48 2d 32 2e 30 2d 50 75 ..... SS H-2.0-Pu
0040 54 54 59 5f 52 65 6c 65 61 73 65 5f 30 2e 36 37 TTY_Rele ase_0.67
0050 0d 0a ..
wireshark_2_interfaces_20210624213837_a03564
Packets: 306 · Displayed: 34 (11.1%) · Dropped: 0 (0.0%)
Profile: Default
10:50 PM
6/24/2021

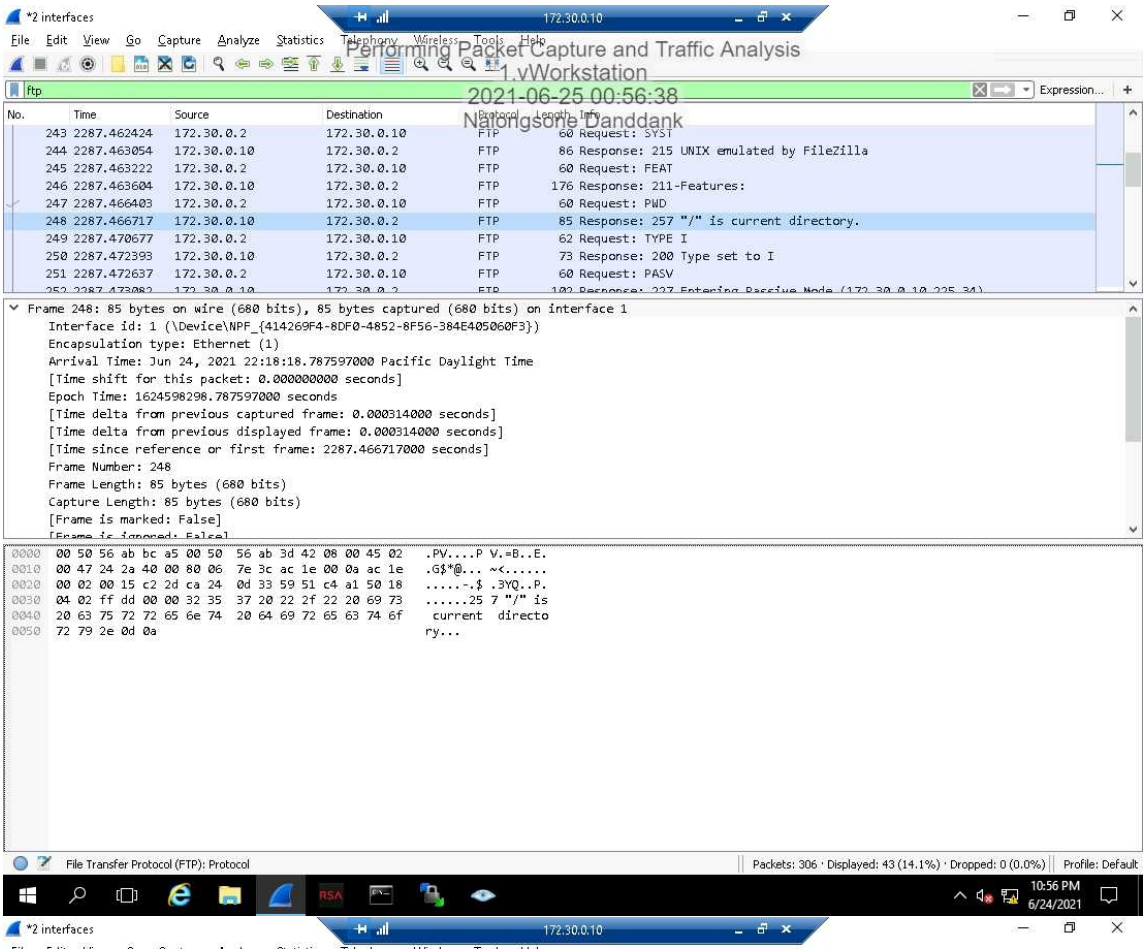

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:51:52
Natorgsone Danddank
ssh
Expression...
No. Time Source Destination Protocol Length Info
105 402.430508 172.16.20.99 172.16.20.5 SSHv2 82 Client: Protocol (SSH-2.0-PuTTY_Release_0.67)
107 402.434923 172.16.20.5 172.16.20.99 SSHv2 93 Server: Protocol (SSH-2.0-OpenSSH_6.0p1 Debian-4+deb7u6)
108 402.473481 172.16.20.99 172.16.20.5 SSHv2 726 Client: Key Exchange Init
109 402.473717 172.16.20.5 172.16.20.99 SSHv2 1038 Server: Key Exchange Init
110 402.473818 172.16.20.99 172.16.20.5 SSHv2 78 Client: Diffie-Hellman Group Exchange Request
111 402.478301 172.16.20.5 172.16.20.99 SSHv2 590 Server: Diffie-Hellman Group Exchange Group
113 402.554099 172.16.20.99 172.16.20.5 SSHv2 582 Client: Diffie-Hellman Group Exchange Init
114 402.564603 172.16.20.5 172.16.20.99 SSHv2 1158 Server: Diffie-Hellman Group Exchange Reply, New Keys
116 402.642633 172.16.20.99 172.16.20.5 SSHv2 70 Client: New Keys
Frame 107: 93 bytes on wire (744 bits), 93 bytes captured (744 bits) on interface 1
Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 24, 2021 21:46:53.755803000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1624596413.755803000 seconds
[Time delta from previous captured frame: 0.004338000 seconds]
[Time delta from previous displayed frame: 0.004415000 seconds]
[Time since reference or first frame: 402.434923000 seconds]
Frame Number: 107
Frame Length: 93 bytes (744 bits)
Capture Length: 93 bytes (744 bits)
[Frame is marked: False]
0000 00 50 56 ab 3d 42 00 50 56 ab ae 77 08 00 45 00 .PV.=B.P V..w..E.
0010 00 4f 47 72 40 00 40 06 72 ae ac 10 14 05 ac 10 .OGr@.@. r.......
0020 14 63 00 16 06 17 02 f9 b0 f4 b4 c5 b3 ae 50 18 .c..... ..... P.
0030 07 21 e1 86 00 00 53 53 48 2d 32 2e 30 2d 4f 70 .!....SS H-2.0-Op
0040 65 6e 53 53 48 5f 36 2e 30 70 31 20 44 65 62 69 enSSH_6. 0p1 Debi
0050 61 6e 2d 34 2b 64 65 62 37 75 36 0d 0a an-4+deb 7u6..
wireshark_2_interfaces_20210624213837_a03564
Packets: 306 · Displayed: 34 (11.1%) · Dropped: 0 (0.0%)
Profile: Default
10:51 PM
6/24/2021

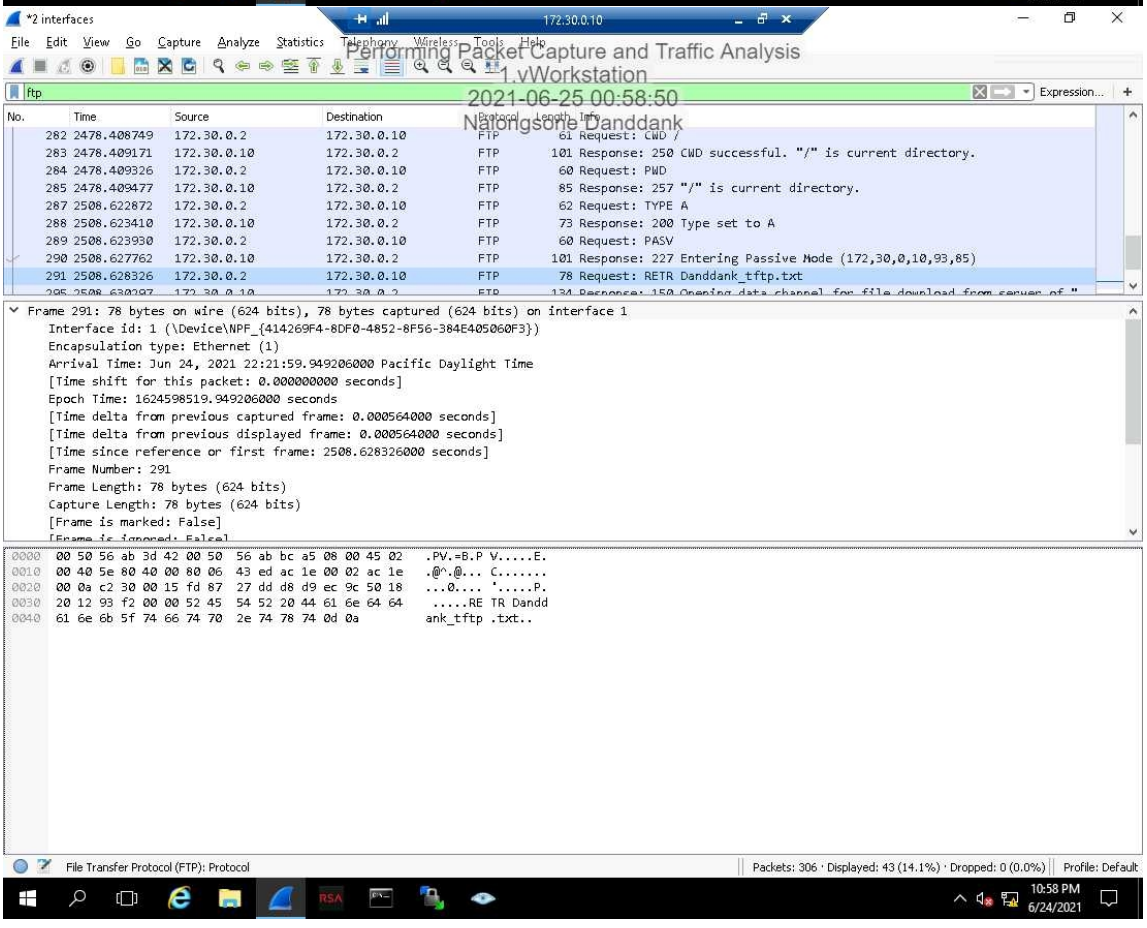

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:53:45
Nalongsone Danddank
tftp
Expression...
No. Time Source Destination Protocol Length Info
224 1940.646192 172.30.0.2 172.30.0.10 TFTP 71 Write Request, File: Danddank_tftp.txt, Transfer type: netascii
225 1940.660734 172.30.0.10 172.30.0.2 TFTP 46 Acknowledgement, Block: 0
226 1940.661372 172.30.0.2 172.30.0.10 TFTP 68 Data Packet, Block: 1 (last)
227 1940.661822 172.30.0.10 172.30.0.2 TFTP 46 Acknowledgement, Block: 1
Frame 224: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface 1
Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 24, 2021 22:12:31.967072000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1624597951.967072000 seconds
[Time delta from previous captured frame: 485.796628000 seconds]
[Time delta from previous displayed frame: 0.000000000 seconds]
[Time since reference or first frame: 1940.646192000 seconds]
Frame Number: 224
Frame Length: 71 bytes (568 bits)
Capture Length: 71 bytes (568 bits)
[Frame is marked: False]
0000 00 50 56 ab 3d 42 00 50 56 ab bc a5 08 00 45 00 .PV.=B.P V.....E.
0010 00 39 57 60 00 00 80 11 8b 0b ac 1e 00 02 ac 1e .9W`.... ....
0020 00 0a c5 ca 00 45 00 25 7d 93 00 02 44 61 6e 64 .....E.% }...Dand
0030 64 61 6e 6b 5f 74 66 74 70 2e 74 78 74 00 6e 65 dank_tft p.txt.ne
0040 74 61 73 63 69 69 00 tascii.
wireshark_2_interfaces_20210624213837_a03564
Packets: 306 · Displayed: 4 (1.3%) · Dropped: 0 (0.0%)
Profile: Default
10:53 PM
6/24/2021

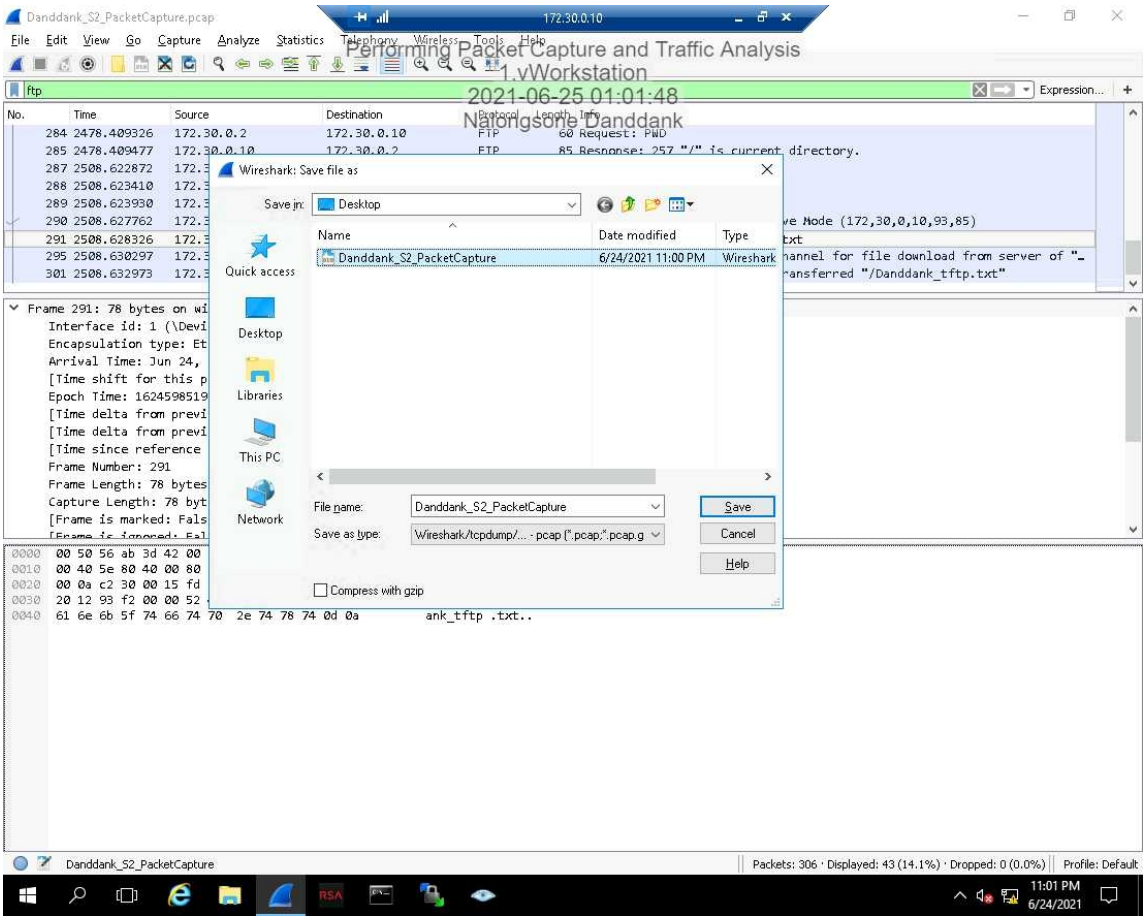

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:54:13
Nalongsone Danddank
tftp
Expression...
No. Time Source Destination Protocol Length Info
224 1940.646192 172.30.0.2 172.30.0.10 TFTP 71 Write Request, File: Danddank_tftp.txt, Transfer type: netascii
225 1940.660734 172.30.0.10 172.30.0.2 TFTP 46 Acknowledgement, Block: 0
226 1940.661372 172.30.0.2 172.30.0.10 TFTP 68 Data Packet, Block: 1 (last)
227 1940.661822 172.30.0.10 172.30.0.2 TFTP 46 Acknowledgement, Block: 1
Frame 226: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 1
Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 24, 2021 22:12:31.982252000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1624597951.982252000 seconds
[Time delta from previous captured frame: 0.000638000 seconds]
[Time delta from previous displayed frame: 0.000638000 seconds]
[Time since reference or first frame: 1940.661372000 seconds]
Frame Number: 226
Frame Length: 68 bytes (544 bits)
Capture Length: 68 bytes (544 bits)
[Frame is marked: False]
0000 00 50 56 ab 3d 42 00 50 56 ab bc a5 08 00 45 00 .PV.=B.P V.....E.
0010 00 36 57 61 00 00 80 11 8b 0d ac 1e 00 02 ac 1e .6Wa.... ....
0020 00 0a c5 ca c0 8e 00 22 57 7e 00 03 00 01 54 68 .... W~....Th
0030 69 73 20 69 73 20 61 20 74 65 73 74 20 6f 66 20 is is a test of
0040 54 46 54 50 TFTP
wireshark_2_interfaces_20210624213837_a03564
Packets: 306 · Displayed: 4 (1.3%) · Dropped: 0 (0.0%)
Profile: Default
10:54 PM
6/24/2021


*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:55:16
Natorigsone Danddank
ftp
Expression...
No. Time Source Destination Protocol Length Info
233 2287.446002 172.30.0.10 172.30.0.2 FTP 197 Response: 220-FileZilla Server 0.9.59 beta
234 2287.449414 172.30.0.2 172.30.0.10 FTP 64 Request: AUTH TLS
236 2287.455529 172.30.0.10 172.30.0.2 FTP 99 Response: 502 Explicit TLS authentication not allowed
237 2287.455785 172.30.0.2 172.30.0.10 FTP 64 Request: AUTH SSL
238 2287.455890 172.30.0.10 172.30.0.2 FTP 99 Response: 502 Explicit TLS authentication not allowed
239 2287.456618 172.30.0.2 172.30.0.10 FTP 68 Request: USER student
240 2287.456920 172.30.0.10 172.30.0.2 FTP 89 Response: 331 Password required for student
241 2287.457051 172.30.0.2 172.30.0.10 FTP 70 Request: PASS P@ssw0rd!
242 2287.462187 172.30.0.10 172.30.0.2 FTP 69 Response: 230 Logged on
Frame 239: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface 1
Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 24, 2021 22:18:18.777498000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1624598298.777498000 seconds
[Time delta from previous captured frame: 0.000728000 seconds]
[Time delta from previous displayed frame: 0.000728000 seconds]
[Time since reference or first frame: 2287.456618000 seconds]
Frame Number: 239
Frame Length: 68 bytes (544 bits)
Capture Length: 68 bytes (544 bits)
[Frame is marked: False]
0000 00 50 56 ab 3d 42 00 50 56 ab bc a5 08 00 45 02 .PV.=B.P V.....E.
0010 00 36 5d c6 40 00 80 06 44 b1 ac 1e 00 02 ac 1e .6].@... D.......
0020 00 0a c2 2d 00 15 59 51 c4 72 ca 24 0c 67 50 18 ...-..YQ .r.$.gP.
0030 04 01 8d 70 00 00 55 53 45 52 20 73 74 75 64 65 ...p..US ER stude
0040 6e 74 0d 0a nt..
File Transfer Protocol (FTP): Protocol
Packets: 306 · Displayed: 43 (14.1%) · Dropped: 0 (0.0%)
Profile: Default
10:55 PM
6/24/2021

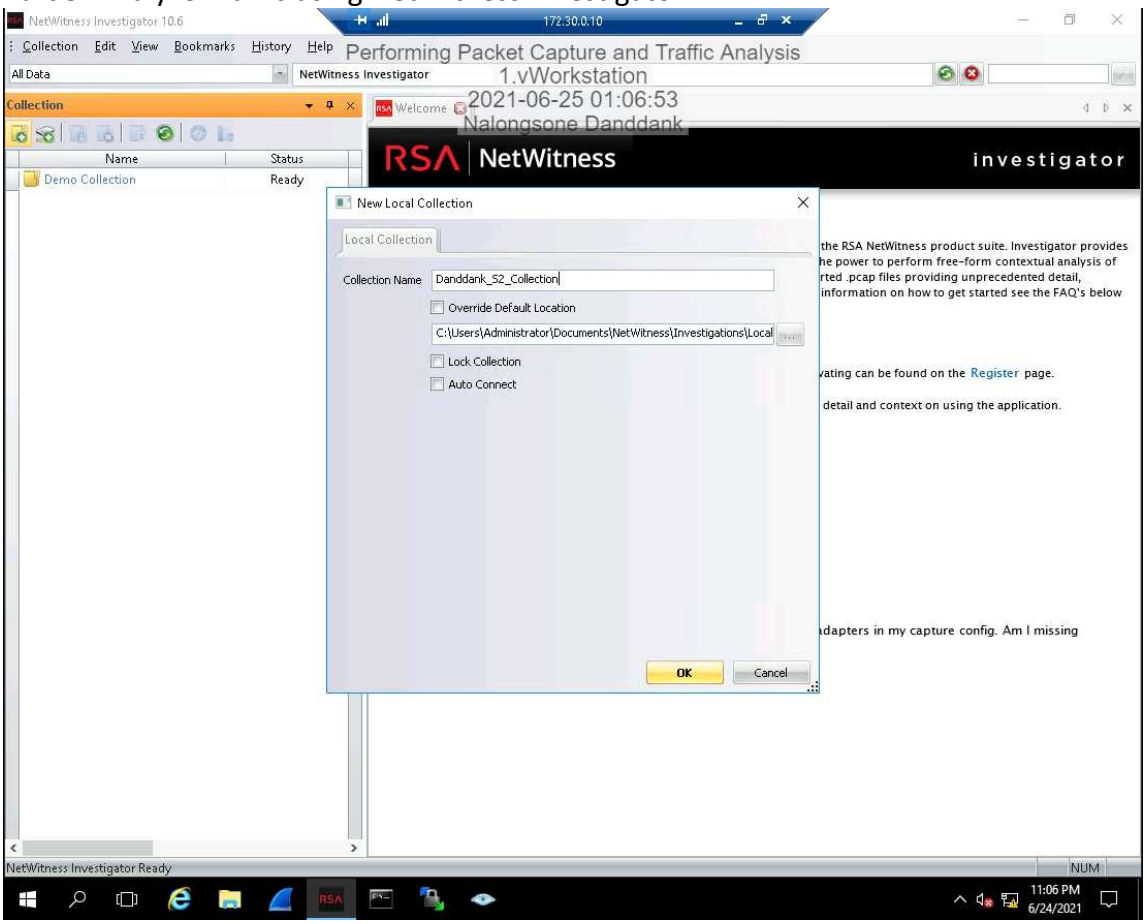

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:55:46
Natorigsone Danddank
ftp
Expression...
No. Time Source Destination Protocol Length Info
233 2287.446002 172.30.0.10 172.30.0.2 FTP 197 Response: 220-FileZilla Server 0.9.59 beta
234 2287.449414 172.30.0.2 172.30.0.10 FTP 64 Request: AUTH TLS
236 2287.455529 172.30.0.10 172.30.0.2 FTP 99 Response: 502 Explicit TLS authentication not allowed
237 2287.455785 172.30.0.2 172.30.0.10 FTP 64 Request: AUTH SSL
238 2287.455890 172.30.0.10 172.30.0.2 FTP 99 Response: 502 Explicit TLS authentication not allowed
239 2287.456618 172.30.0.2 172.30.0.10 FTP 68 Request: USER student
240 2287.456920 172.30.0.10 172.30.0.2 FTP 89 Response: 331 Password required for student
241 2287.457051 172.30.0.2 172.30.0.10 FTP 70 Request: PASS P@ssw0rd!
242 2287.462187 172.30.0.10 172.30.0.2 FTP 69 Response: 230 Logged on
Frame 241: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface 1
Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 24, 2021 22:18:18.777931000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1624598298.777931000 seconds
[Time delta from previous captured frame: 0.000131000 seconds]
[Time delta from previous displayed frame: 0.000131000 seconds]
[Time since reference or first frame: 2287.457051000 seconds]
Frame Number: 241
Frame Length: 70 bytes (560 bits)
Capture Length: 70 bytes (560 bits)
[Frame is marked: False]
0000 00 50 56 ab 3d 42 00 50 56 ab bc a5 08 00 45 02 .PV.=B.P V.....E.
0010 00 38 5d c7 40 00 80 06 44 ae ac 1e 00 02 ac 1e .8].@... D.......
0020 00 0a c2 2d 00 15 59 51 c4 80 ca 24 0c 8a 50 18 ...-..YQ ...$..P.
0030 04 01 83 42 00 00 50 41 53 53 20 50 40 73 73 77 ...B..PA SS P@ssw
0040 30 72 64 21 0d 0a 0rd!..
File Transfer Protocol (FTP): Protocol
Packets: 306 · Displayed: 43 (14.1%) · Dropped: 0 (0.0%)
Profile: Default
10:55 PM
6/24/2021

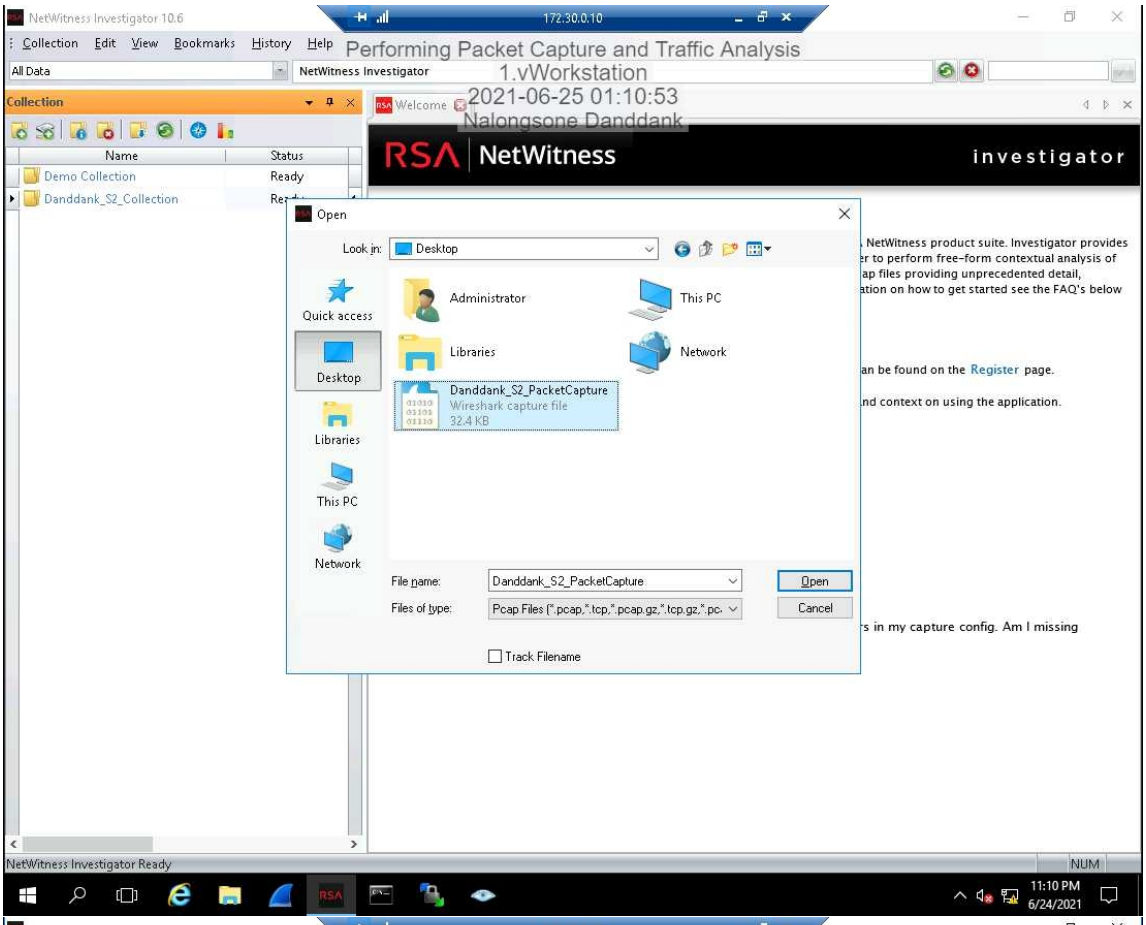

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:56:38
Nalorigsone Danddank
ftp
Expression...
No. Time Source Destination Protocol Length Info
243 2287.462424 172.30.0.2 172.30.0.10 FTP 60 Request: SYST
244 2287.463054 172.30.0.10 172.30.0.2 FTP 86 Response: 215 UNIX emulated by FileZilla
245 2287.463222 172.30.0.2 172.30.0.10 FTP 60 Request: FEAT
246 2287.463604 172.30.0.10 172.30.0.2 FTP 176 Response: 211-Features:
247 2287.466403 172.30.0.2 172.30.0.10 FTP 60 Request: PWD
248 2287.466717 172.30.0.10 172.30.0.2 FTP 85 Response: 257 "/" is current directory.
249 2287.470677 172.30.0.2 172.30.0.10 FTP 62 Request: TYPE I
250 2287.472393 172.30.0.10 172.30.0.2 FTP 73 Response: 200 Type set to I
251 2287.472637 172.30.0.2 172.30.0.10 FTP 60 Request: PASV
Frame 248: 85 bytes on wire (680 bits), 85 bytes captured (680 bits) on interface 1
Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 24, 2021 22:18:18.787597000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1624598298.787597000 seconds
[Time delta from previous captured frame: 0.000314000 seconds]
[Time delta from previous displayed frame: 0.000314000 seconds]
[Time since reference or first frame: 2287.466717000 seconds]
Frame Number: 248
Frame Length: 85 bytes (680 bits)
Capture Length: 85 bytes (680 bits)
[Frame is marked: False]
0000 00 50 56 ab bc a5 00 50 56 ab 3d 42 08 00 45 02 .PV....P V.=B..E.
0010 00 47 24 2a 40 00 80 06 7e 3c ac 1e 00 0a ac 1e .G$*@... ~<......
0020 00 02 00 15 c2 2d ca 24 0d 33 59 51 c4 a1 50 18 .....-.$ .3YQ..P.
0030 04 02 ff dd 00 00 32 35 37 20 22 2f 22 20 69 73 ......25 7 "/" is
0040 20 63 75 72 72 65 6e 74 20 64 69 72 65 63 74 6f current directo
0050 72 79 2e 0d 0a ry...
File Transfer Protocol (FTP): Protocol
Packets: 306 · Displayed: 43 (14.1%) · Dropped: 0 (0.0%)
Profile: Default
10:56 PM
6/24/2021

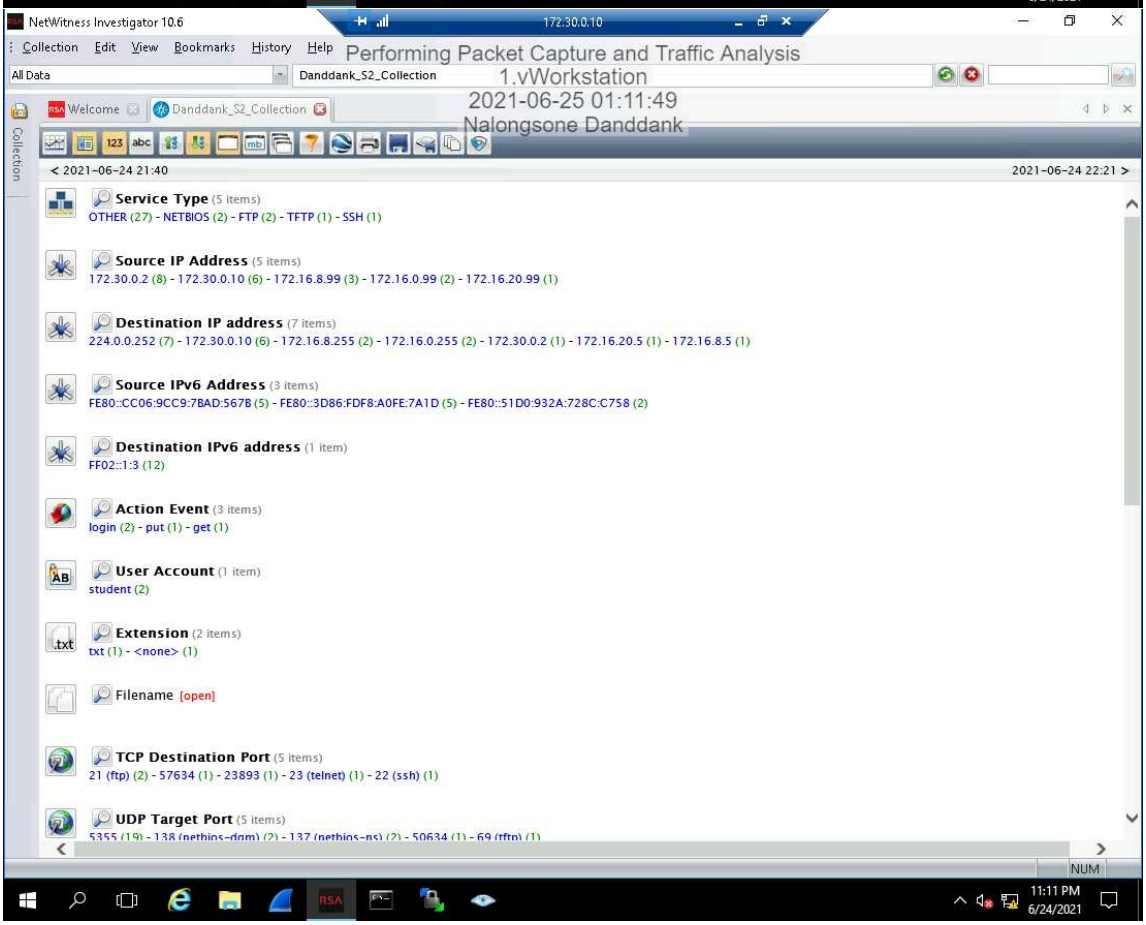

*2 interfaces
172.30.0.10
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 00:58:50
Nalorigsone Danddank
ftp
Expression...
No. Time Source Destination Protocol Length Info
282 2478.408749 172.30.0.2 172.30.0.10 FTP 61 Request: CWD /
283 2478.409171 172.30.0.10 172.30.0.2 FTP 101 Response: 250 CWD successful. "/" is current directory.
284 2478.409326 172.30.0.2 172.30.0.10 FTP 60 Request: PWD
285 2478.409477 172.30.0.10 172.30.0.2 FTP 85 Response: 257 "/" is current directory.
287 2508.622872 172.30.0.2 172.30.0.10 FTP 62 Request: TYPE A
288 2508.623410 172.30.0.10 172.30.0.2 FTP 73 Response: 200 Type set to A
289 2508.623930 172.30.0.2 172.30.0.10 FTP 60 Request: PASV
290 2508.627762 172.30.0.10 172.30.0.2 FTP 101 Response: 227 Entering Passive Mode (172,30,0,10,93,85)
291 2508.628326 172.30.0.2 172.30.0.10 FTP 78 Request: RETR Danddank_tftp.txt
Frame 291: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 1
Interface id: 1 (\Device\NPF_{414269F4-8DF0-4852-8F56-384E405060F3})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 24, 2021 22:21:59.949206000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1624598519.949206000 seconds
[Time delta from previous captured frame: 0.000564000 seconds]
[Time delta from previous displayed frame: 0.000564000 seconds]
[Time since reference or first frame: 2508.628326000 seconds]
Frame Number: 291
Frame Length: 78 bytes (624 bits)
Capture Length: 78 bytes (624 bits)
[Frame is marked: False]
0000 00 50 56 ab 3d 42 00 50 56 ab bc a5 08 00 45 02 .PV.=B.P V.....E.
0010 00 40 5e 80 40 00 80 06 43 ed ac 1e 00 02 ac 1e .@^.@... C.......
0020 00 0a c2 30 00 15 fd 87 27 dd d8 d9 ec 9c 50 18 ...0.... '.....P.
0030 20 12 93 f2 00 00 52 45 54 52 20 44 61 6e 64 64 ......RE TR Dandd
0040 61 6e 6b 5f 74 66 74 70 2e 74 78 74 0d 0a ank_tftp .txt..
File Transfer Protocol (FTP): Protocol
Packets: 306 · Displayed: 43 (14.1%) · Dropped: 0 (0.0%)
Profile: Default
10:58 PM
6/24/2021

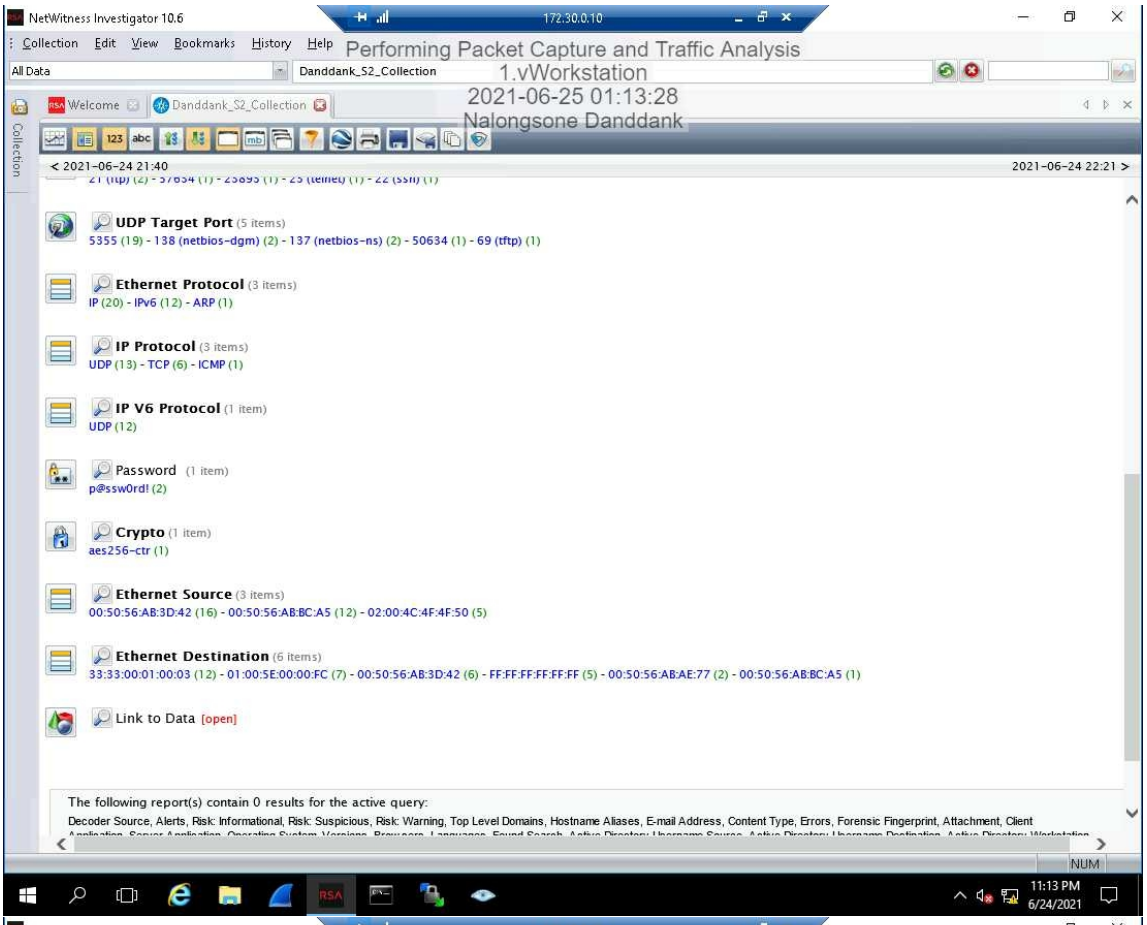


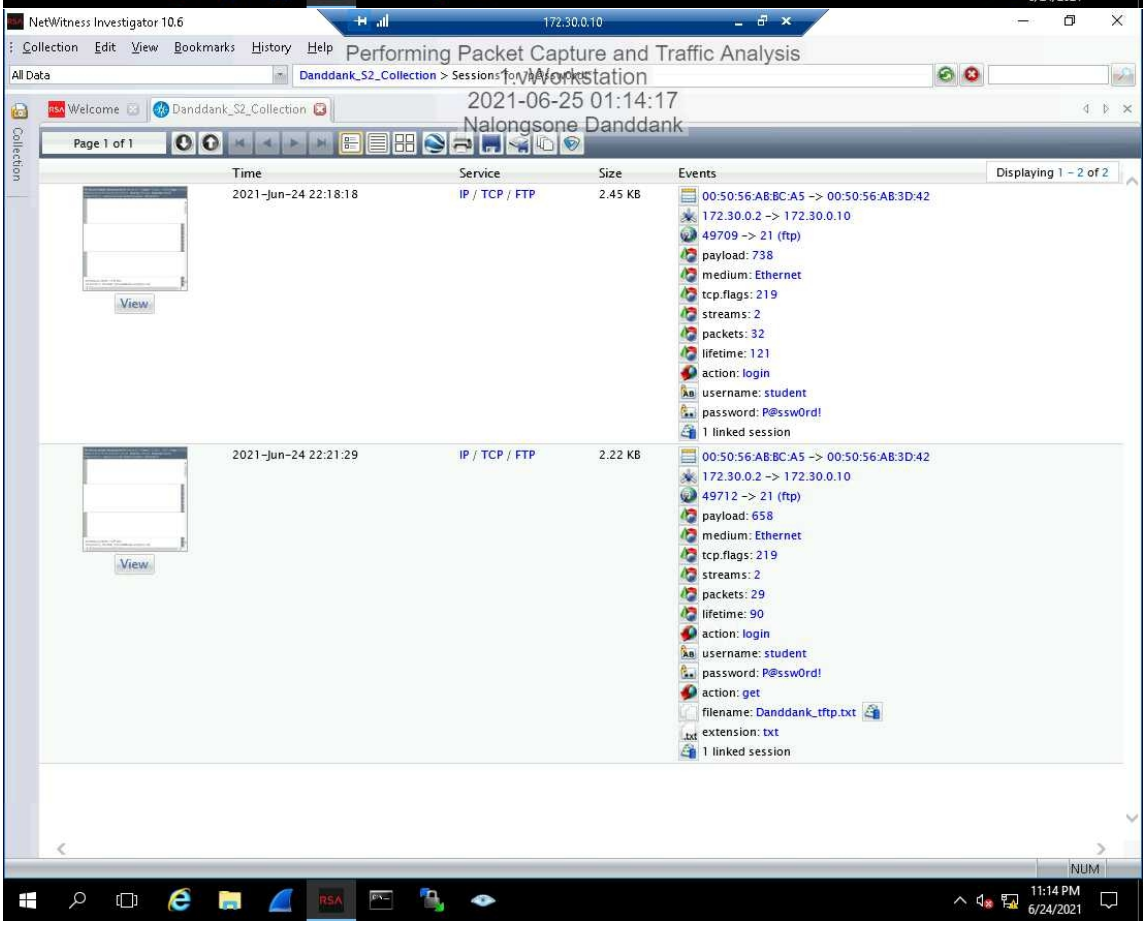
Part 3: Analyze Traffic using NetWitness Investigator.

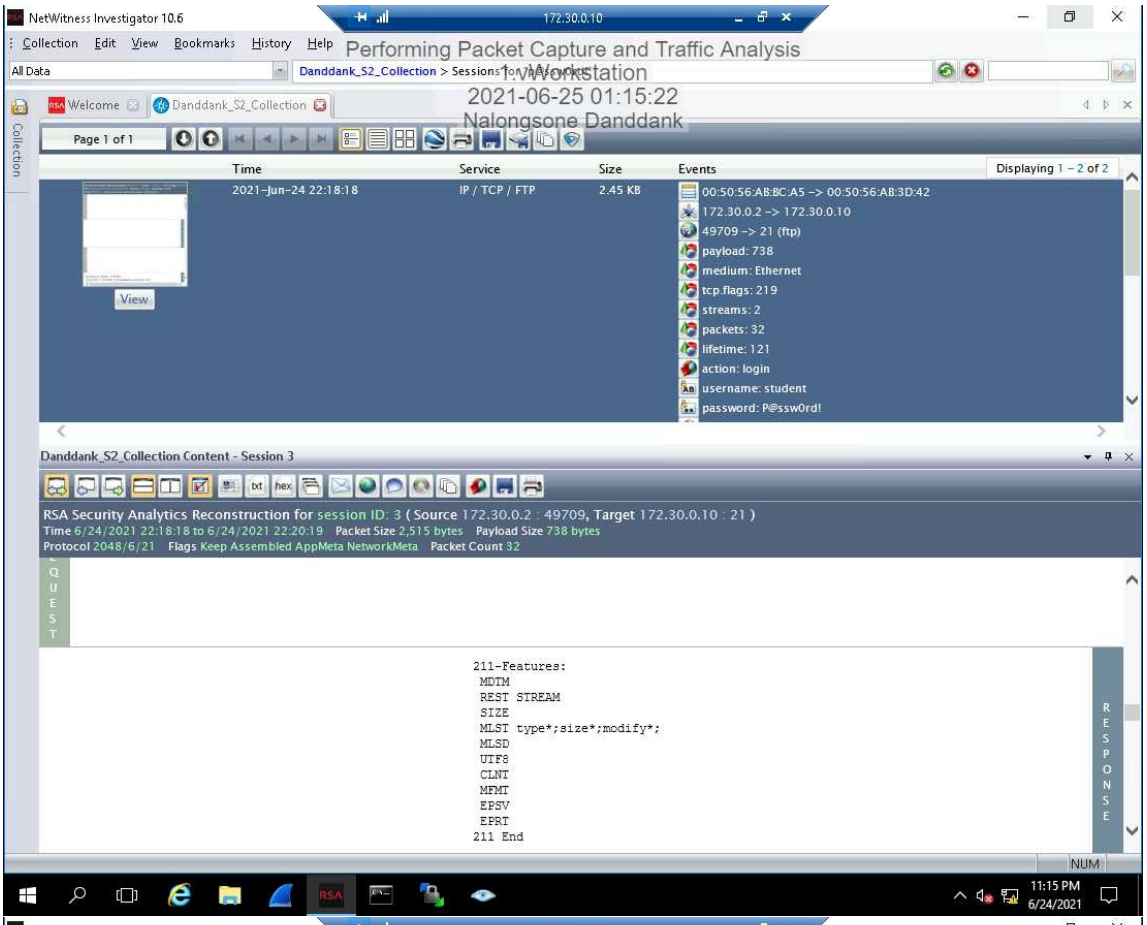


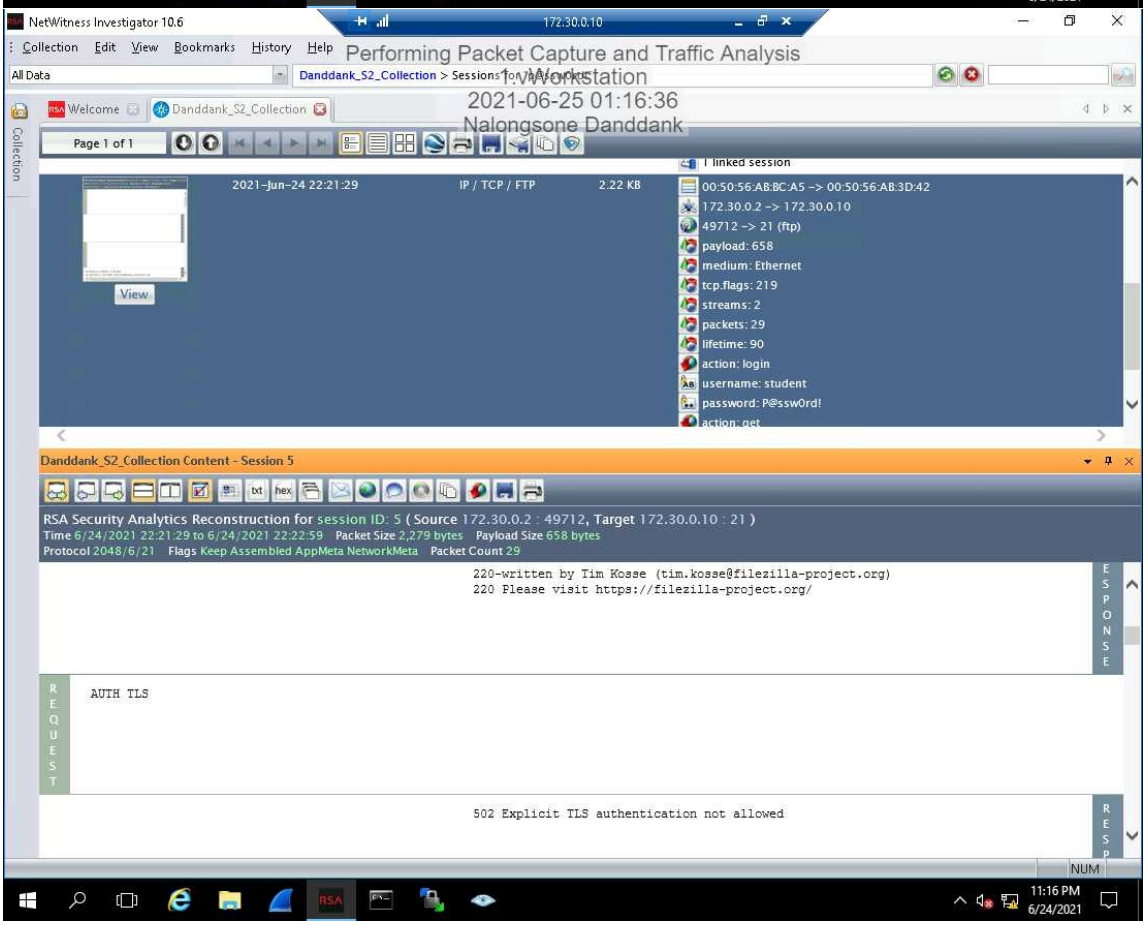

NetWitness Investigator 10.6
172.30.0.10
Collection Edit View Bookmarks History Help
Performing Packet Capture and Traffic Analysis
All Data
NetWitness Investigator
1.vWorkstation
2021-06-25 01:10:53
Nalongsone Danddank
Collection
Welcome
Name
Status
Demo Collection
Ready
Danddank_S2_Collection
RSA NetWitness investigator
Open
Look in: Desktop
Quick access
Desktop
Libraries
This PC
Network
Administrator
This PC
Libraries
Network
Danddank_S2_PacketCapture
Wireshark capture file
32.4 KB
File name: Danddank_S2_PacketCapture
Files of type: Pcap Files (*.pcap,*.tcp,*.pcap.gz,*.tcp.gz,*.pc
Open
Cancel
Track Filename
NetWitness product suite. Investigator provides
to perform free-form contextual analysis of
ap files providing unprecedented detail,
ation on how to get started see the FAQ's below
an be found on the Register page.
nd context on using the application.
s in my capture config. Am I missing
NetWitness Investigator Ready
NUM
11:10 PM
6/24/2021

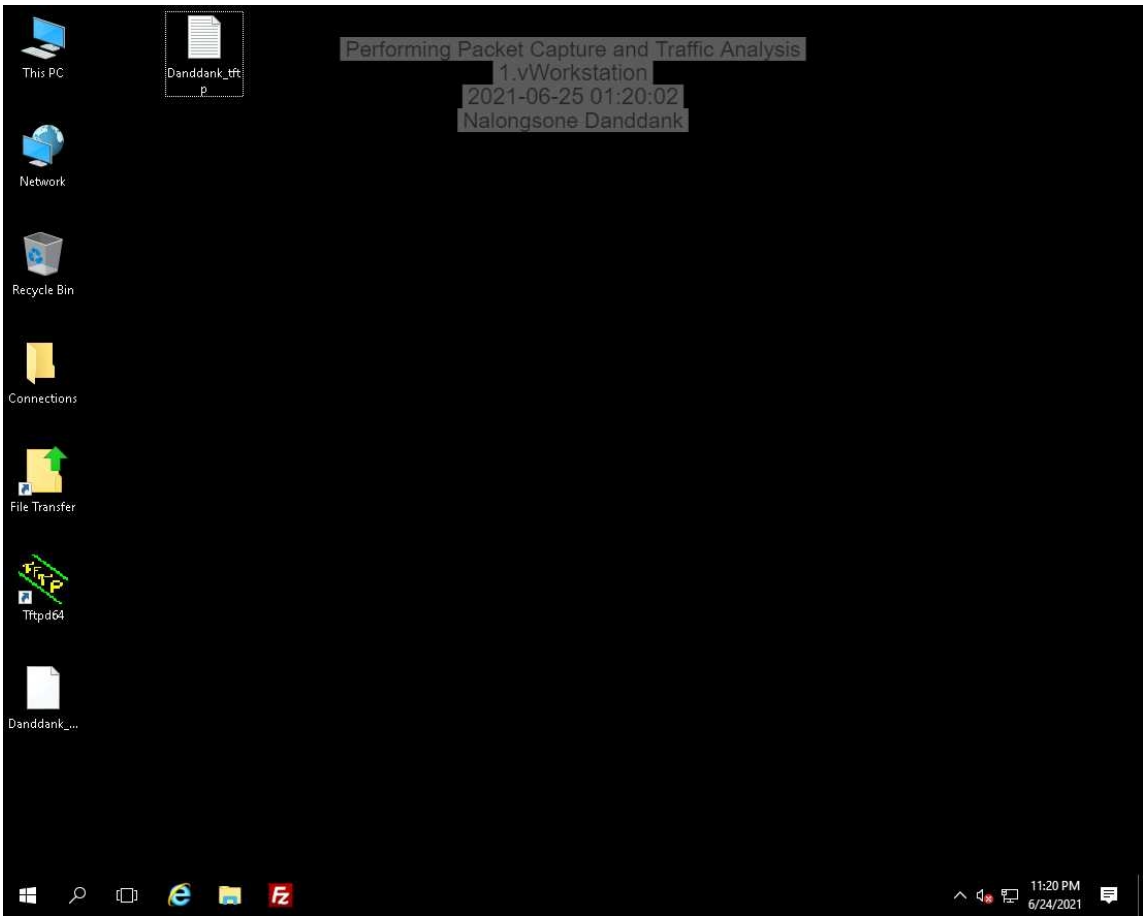

NetWitness Investigator 10.6
172.30.0.10
Collection Edit View Bookmarks History Help
Performing Packet Capture and Traffic Analysis
All Data
Danddank_S2_Collection
1.vWorkstation
2021-06-25 01:11:49
Nalongsone Danddank
Welcome
Danddank_S2_Collection
< 2021-06-24 21:40
2021-06-24 22:21 >
Service Type (5 items)
OTHER (27) - NETBIOS (2) - FTP (2) - TFTP (1) - SSH (1)
Source IP Address (5 items)
172.30.0.2 (8) - 172.30.0.10 (6) - 172.16.8.99 (3) - 172.16.0.99 (2) - 172.16.20.99 (1)
Destination IP address (7 items)
224.0.0.252 (7) - 172.30.0.10 (6) - 172.16.8.255 (2) - 172.16.0.255 (2) - 172.30.0.2 (1) - 172.16.20.5 (1) - 172.16.8.5 (1)
Source IPv6 Address (3 items)
FE80::CC06:9CC9:7BAD:567B (5) - FE80::3D86:FDF8:A0FE:7A1D (5) - FE80::51D0:932A:728C:C758 (2)
Destination IPv6 address (1 item)
FF02::1:3 (12)
Action Event (3 items)
login (2) - put (1) - get (1)
User Account (1 item)
student (2)
Extension (2 items)
txt (1) - <none> (1)
Filename [open]
TCP Destination Port (5 items)
21 (ftp) (2) - 57634 (1) - 23893 (1) - 23 (telnet) (1) - 22 (ssh) (1)
UDP Target Port (5 items)
NUM
11:11 PM
6/24/2021


NetWitness Investigator 10.6
172.30.0.10
Collection Edit View Bookmarks History Help
Performing Packet Capture and Traffic Analysis
All Data
Danddank_S2_Collection
1.vWorkstation
2021-06-25 01:13:28
Nalongsone Danddank
Welcome
Danddank_S2_Collection
< 2021-06-24 21:40
2021-06-24 22:21 >
UDP Target Port (5 items)
5355 (19) - 138 (netbios-dgm) (2) - 137 (netbios-ns) (2) - 50634 (1) - 69 (tftp) (1)
Ethernet Protocol (3 items)
IP (20) - IPv6 (12) - ARP (1)
IP Protocol (3 items)
UDP (13) - TCP (6) - ICMP (1)
IP V6 Protocol (1 item)
UDP (12)
Password (1 item)
p@ssw0rd! (2)
Crypto (1 item)
aes256-ctr (1)
Ethernet Source (3 items)
00:50:56:AB:3D:42 (16) - 00:50:56:AB:BC:A5 (12) - 02:00:4C:4F:4F:50 (5)
Ethernet Destination (6 items)
33:33:00:01:00:03 (12) - 01:00:5E:00:00:FC (7) - 00:50:56:AB:3D:42 (6) - FF:FF:FF:FF:FF:FF (5) - 00:50:56:AB:AE:77 (2) - 00:50:56:AB:BC:A5 (1)
Link to Data [open]
The following report(s) contain 0 results for the active query:
Decoder Source, Alerts, Risk: Informational, Risk: Suspicious, Risk: Warning, Top Level Domains, Hostname Aliases, E-mail Address, Content Type, Errors, Forensic Fingerprint, Attachment, Client
NUM
11:13 PM
6/24/2021


NetWitness Investigator 10.6
172.30.0.10
Collection Edit View Bookmarks History Help
Performing Packet Capture and Traffic Analysis
All Data
Danddank_S2_Collection > Sessions for
1.vWorkstation
2021-06-25 01:14:17
Nalongsone Danddank
Welcome
Danddank_S2_Collection
Page 1 of 1
Displaying 1 - 2 of 2
Time
Service
Size
Events
2021-Jun-24 22:18:18
IP / TCP / FTP
2.45 KB
00:50:56:AB:BC:A5 -> 00:50:56:AB:3D:42
172.30.0.2 -> 172.30.0.10
49709 -> 21 (ftp)
payload: 738
medium: Ethernet
tcp.flags: 219
streams: 2
packets: 32
lifetime: 121
action: login
username: student
password: P@ssw0rd!
1 linked session
View
2021-Jun-24 22:21:29
IP / TCP / FTP
2.22 KB
00:50:56:AB:BC:A5 -> 00:50:56:AB:3D:42
172.30.0.2 -> 172.30.0.10
49712 -> 21 (ftp)
payload: 658
medium: Ethernet
tcp.flags: 219
streams: 2
packets: 29
lifetime: 90
action: login
username: student
password: P@ssw0rd!
action: get
filename: Danddank_tftp.txt
extension: txt
1 linked session
View
NUM
11:14 PM
6/24/2021


NetWitness Investigator 10.6
172.30.0.10
Collection Edit View Bookmarks History Help
Performing Packet Capture and Traffic Analysis
1 Workstation
2021-06-25 01:15:22
Nalongsone Danddank
All Data
Danddank_S2_Collection > Sessions for 'Workstation'
Welcome
Danddank_S2_Collection
Page 1 of 1
Time
Service
Size
Events
Displaying 1 - 2 of 2
2021-Jun-24 22:18:18
IP / TCP / FTP
2.45 KB
View
00:50:56:AB:BC:A5 -> 00:50:56:AB:3D:42
172.30.0.2 -> 172.30.0.10
49709 -> 21 (ftp)
payload: 738
medium: Ethernet
tcp.flags: 219
streams: 2
packets: 32
lifetime: 121
action: login
username: student
password: P@ssw0rd!
Danddank_S2_Collection Content - Session 3
RSA Security Analytics Reconstruction for session ID: 3 (Source 172.30.0.2 : 49709, Target 172.30.0.10 : 21)
Time 6/24/2021 22:18:18 to 6/24/2021 22:20:19 Packet Size 2,515 bytes Payload Size 738 bytes
Protocol 2048/6/21 Flags Keep Assembled AppMeta NetworkMeta Packet Count 32
QUEST
211-Features:
MDTM
REST STREAM
SIZE
MLST type*;size*;modify*;
MLSD
UTF8
CLNT
MFMT
EPSV
EPRT
211 End
RESPONSE
NUM
11:15 PM
6/24/2021


NetWitness Investigator 10.6
172.30.0.10
Collection Edit View Bookmarks History Help
Performing Packet Capture and Traffic Analysis
1 Workstation
2021-06-25 01:16:36
Nalongsone Danddank
All Data
Danddank_S2_Collection > Sessions for 'Workstation'
Welcome
Danddank_S2_Collection
Page 1 of 1
1 linked session
2021-Jun-24 22:21:29
IP / TCP / FTP
2.22 KB
View
00:50:56:AB:BC:A5 -> 00:50:56:AB:3D:42
172.30.0.2 -> 172.30.0.10
49712 -> 21 (ftp)
payload: 658
medium: Ethernet
tcp.flags: 219
streams: 2
packets: 29
lifetime: 90
action: login
username: student
password: P@ssw0rd!
action: get
Danddank_S2_Collection Content - Session 5
RSA Security Analytics Reconstruction for session ID: 5 (Source 172.30.0.2 : 49712, Target 172.30.0.10 : 21)
Time 6/24/2021 22:21:29 to 6/24/2021 22:22:59 Packet Size 2,279 bytes Payload Size 658 bytes
Protocol 2048/6/21 Flags Keep Assembled AppMeta NetworkMeta Packet Count 29
220-written by Tim Kosse (tim.kosse@filezilla-project.org)
220 Please visit https://filezilla-project.org/
RESPONSE
REQUEST
AUTH TLS
502 Explicit TLS authentication not allowed
NUM
11:16 PM
6/24/2021


This PC
Danddank_tftp
Performing Packet Capture and Traffic Analysis
1.vWorkstation
2021-06-25 01:20:02
Nalongsone Danddank
Network
Recycle Bin
Connections
File Transfer
Tftpd64
Danddank_...
11:20 PM
6/24/2021

End.