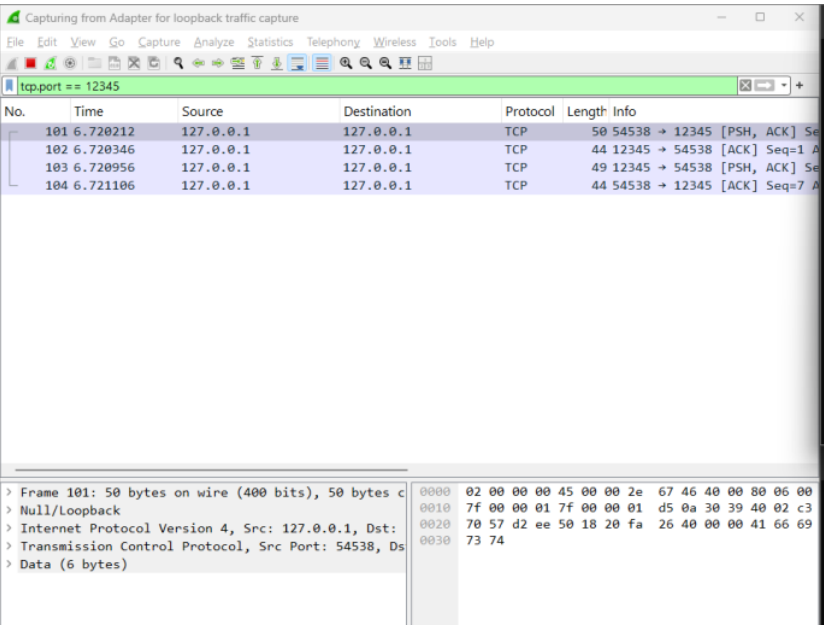
Name: Gehad Khaled Elsamadisy

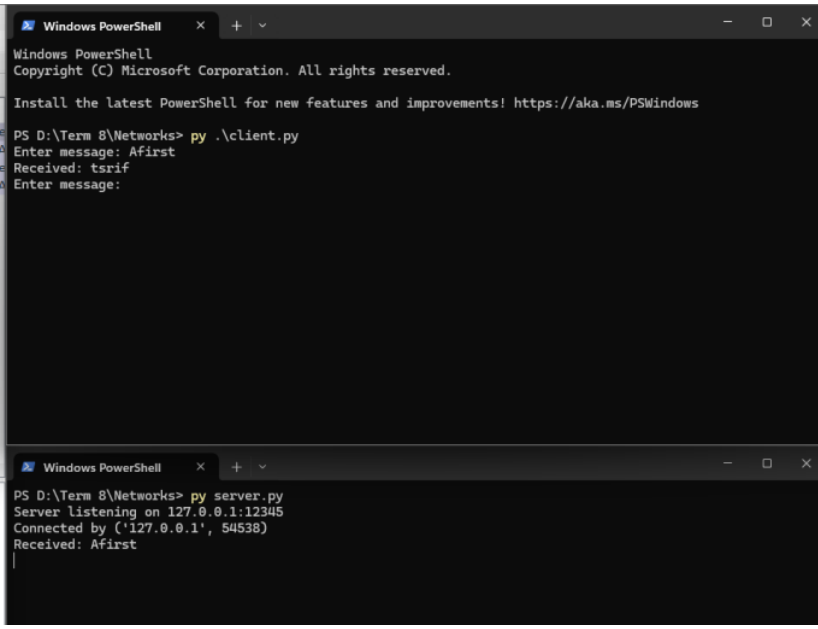
ID : 7980

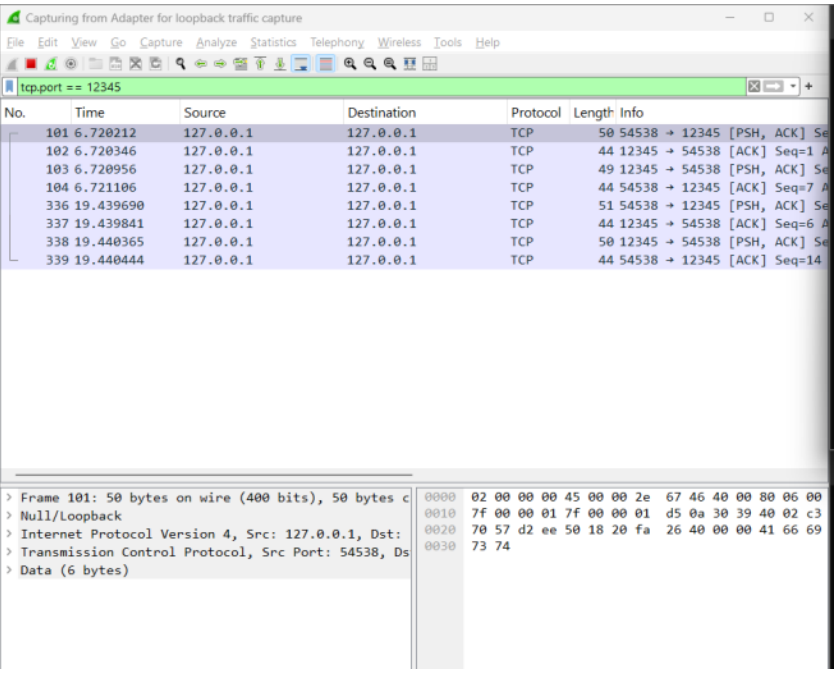
Group 2 section 2

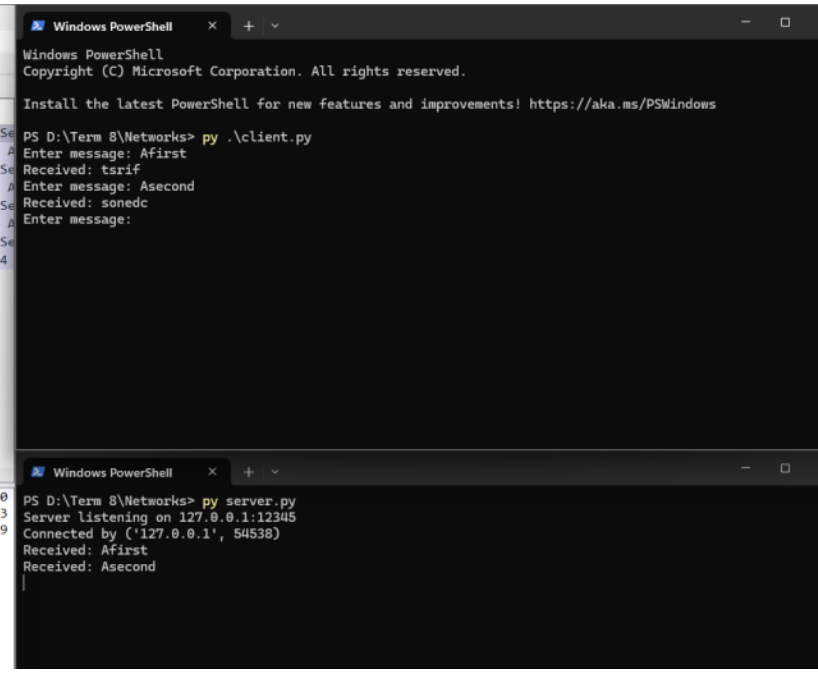
- Assigned Port number : 12345
- Run the server and client simultaneously
- If first letter is A: order will be descending.
- If first letter is C: order will be ascending.
- If first letter is D: make all letters CAPITAL
- Here are some tests:

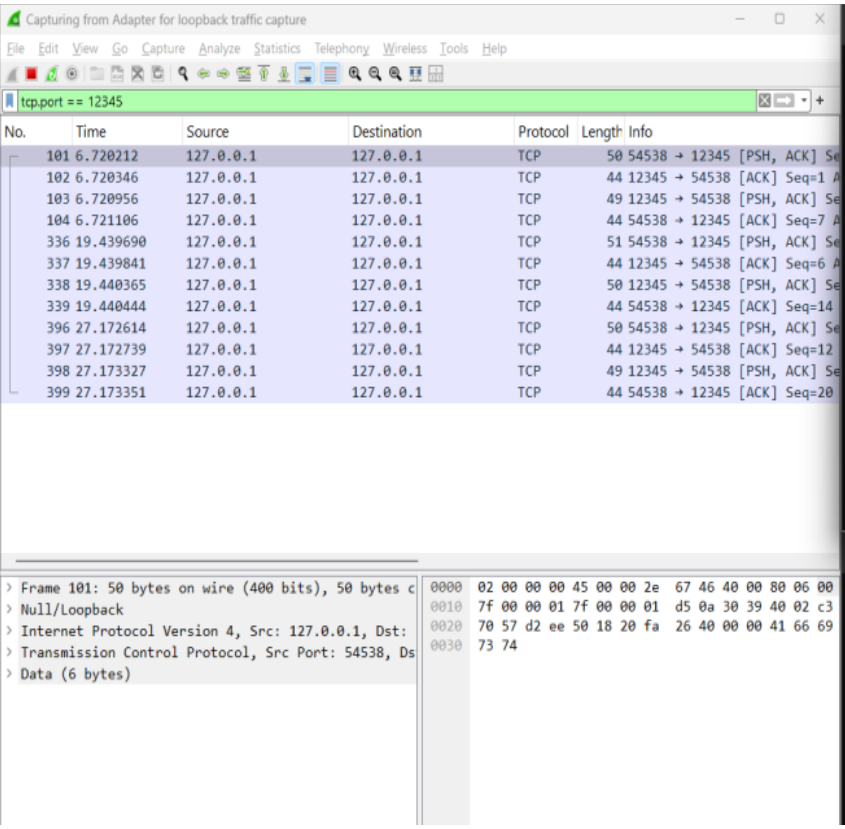
- Opened wireshark and searched for the port 12345, sent some messages and watched the results in wireshark

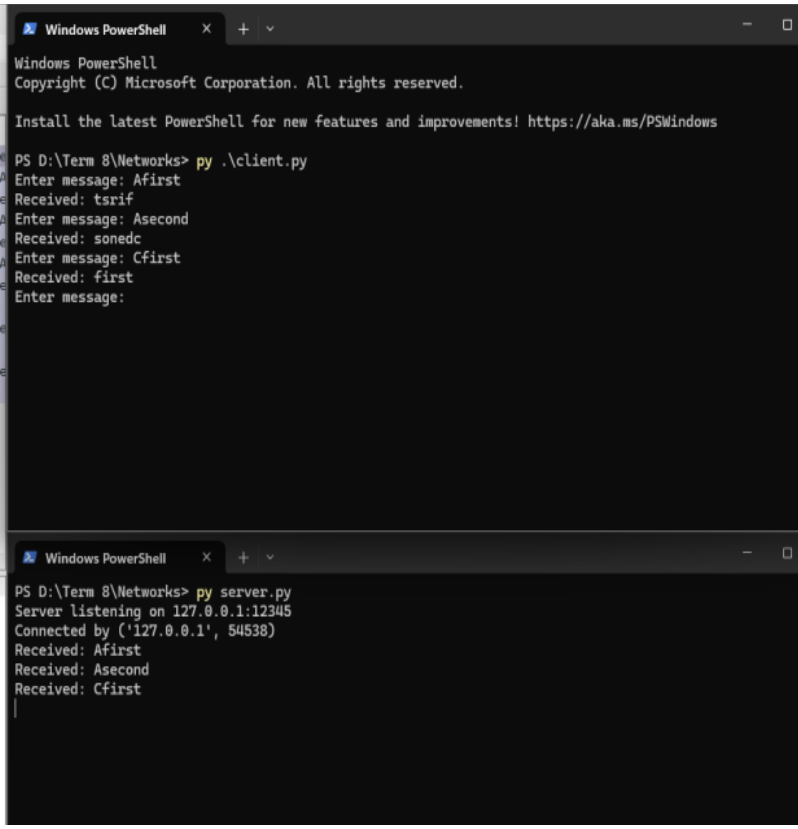

Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 12345
No. Time Source Destination Protocol Length Info
101 6.720212 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK] Se
102 6.720346 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1 A
103 6.720956 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK] Se
104 6.721106 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=7 A
Frame 101: 50 bytes on wire (400 bits), 50 bytes c
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 54538, Ds
Data (6 bytes)
0000 02 00 00 00 45 00 00 2e 67 46 40 00 80 06 00
0010 7f 00 00 01 7f 00 00 01 d5 0a 30 39 40 02 c3
0020 70 57 d2 ee 50 18 20 fa 26 40 00 00 41 66 69
0030 73 74

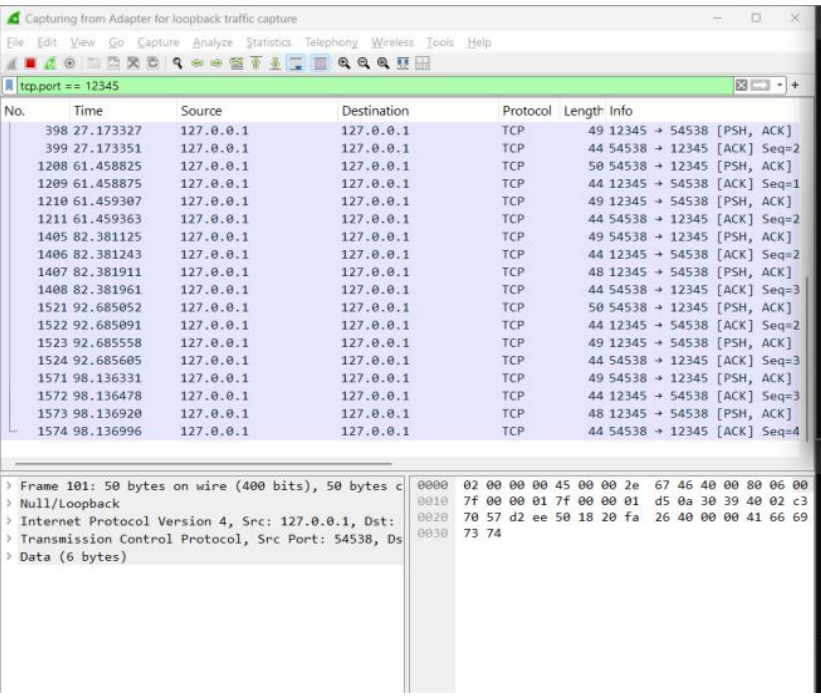

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\Term 8\Networks> py .\client.py
Enter message: Afirst
Received: tsrif
Enter message:
Windows PowerShell
PS D:\Term 8\Networks> py server.py
Server listening on 127.0.0.1:12345
Connected by ('127.0.0.1', 54538)
Received: Afirst

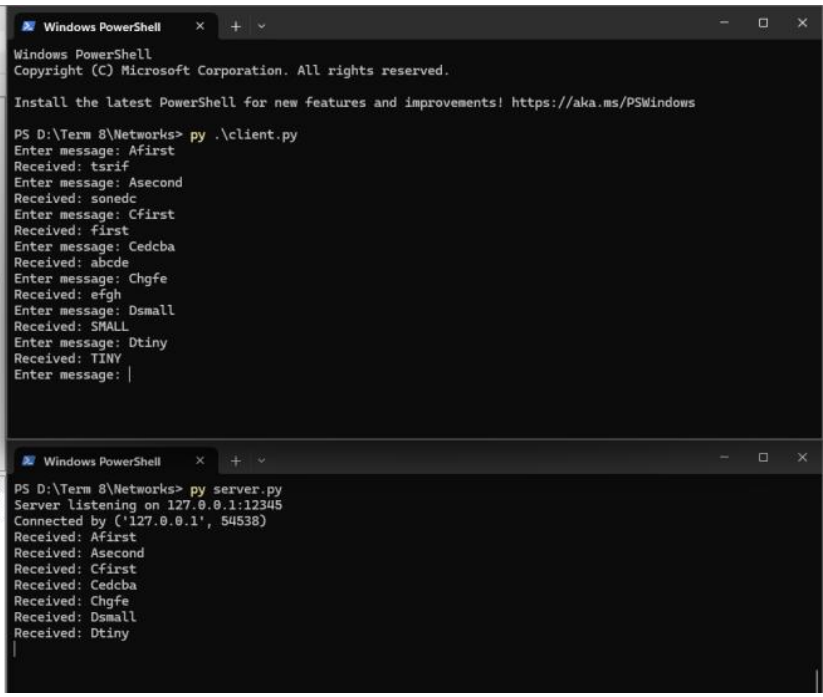

Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 12345
No. Time Source Destination Protocol Length Info
101 6.720212 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK] Se
102 6.720346 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1 A
103 6.720956 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK] Se
104 6.721106 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=7 A
336 19.439690 127.0.0.1 127.0.0.1 TCP 51 54538 → 12345 [PSH, ACK] Se
337 19.439841 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=6 A
338 19.440365 127.0.0.1 127.0.0.1 TCP 50 12345 → 54538 [PSH, ACK] Se
339 19.440444 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=14
Frame 101: 50 bytes on wire (400 bits), 50 bytes c
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 54538, Ds
Data (6 bytes)
0000 02 00 00 00 45 00 00 2e 67 46 40 00 80 06 00
0010 7f 00 00 01 7f 00 00 01 d5 0a 30 39 40 02 c3
0020 70 57 d2 ee 50 18 20 fa 26 40 00 00 41 66 69
0030 73 74

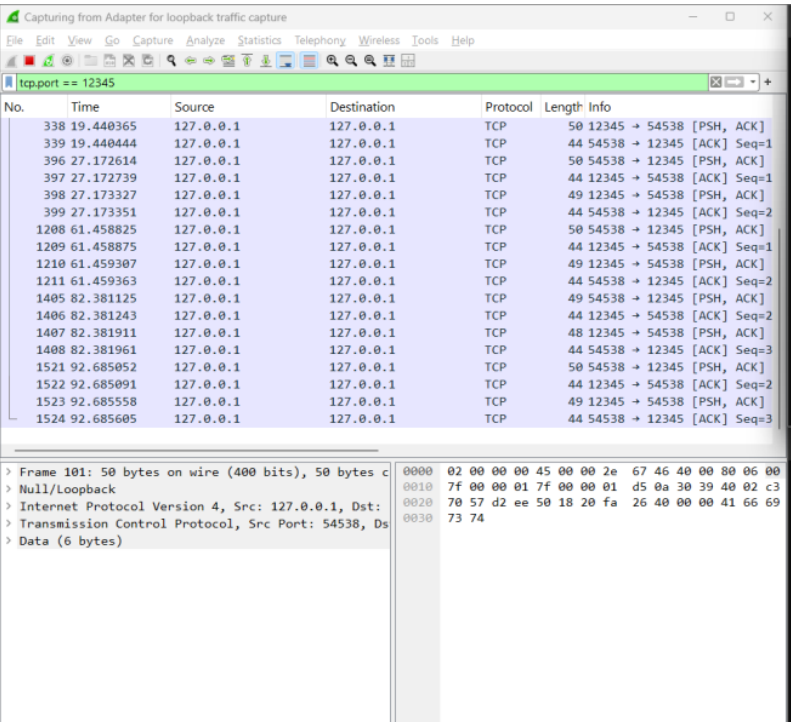

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\Term 8\Networks> py .\client.py
Enter message: Afirst
Received: tsrif
Enter message: Asecond
Received: sonedc
Enter message:
Windows PowerShell
PS D:\Term 8\Networks> py server.py
Server listening on 127.0.0.1:12345
Connected by ('127.0.0.1', 54538)
Received: Afirst
Received: Asecond

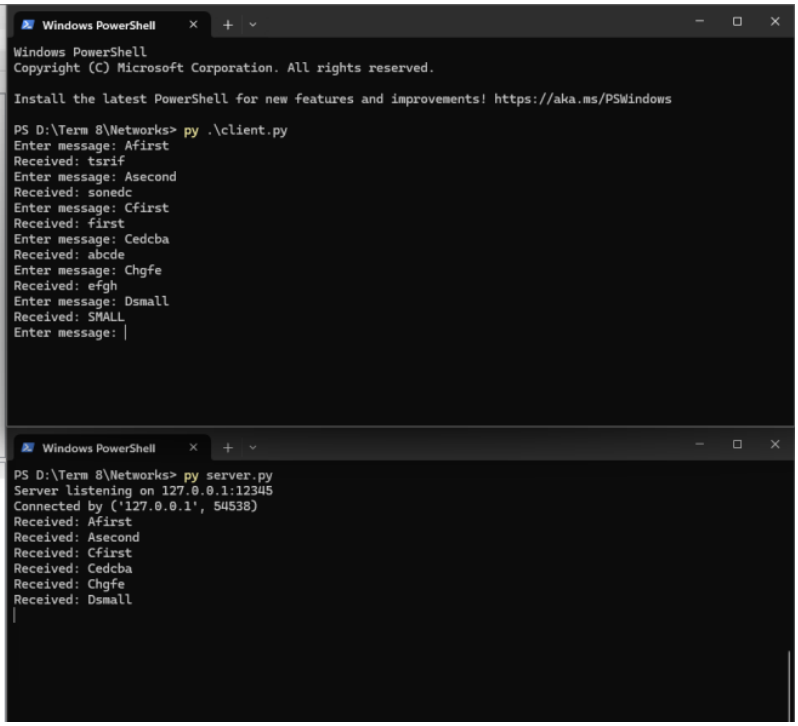

Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 12345
No. Time Source Destination Protocol Length Info
101 6.720212 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
102 6.720346 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1
103 6.720956 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
104 6.721106 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=7
336 19.439690 127.0.0.1 127.0.0.1 TCP 51 54538 → 12345 [PSH, ACK]
337 19.439841 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=6
338 19.440365 127.0.0.1 127.0.0.1 TCP 50 12345 → 54538 [PSH, ACK]
339 19.440444 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=14
396 27.172614 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
397 27.172739 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=12
398 27.173327 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
399 27.173351 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=20
Frame 101: 50 bytes on wire (400 bits), 50 bytes c
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 54538, Ds
Data (6 bytes)
0000 02 00 00 00 45 00 00 2e 67 46 40 00 80 06 00
0010 7f 00 00 01 7f 00 00 01 d5 0a 30 39 40 02 c3
0020 70 57 d2 ee 50 18 20 fa 26 40 00 00 41 66 69
0030 73 74

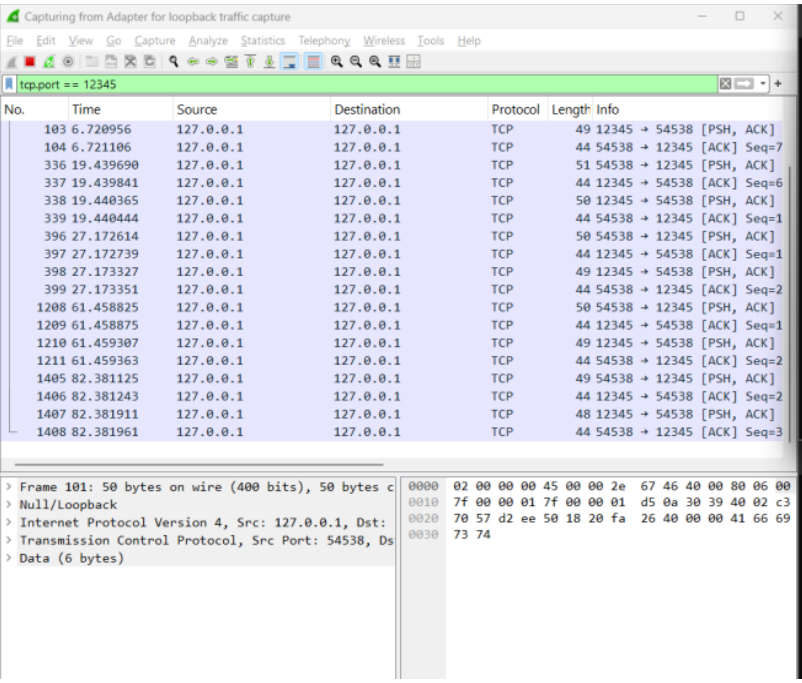

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\Term 8\Networks> py .\client.py
Enter message: Afirst
Received: tsrif
Enter message: Asecond
Received: sonedc
Enter message: Cfirst
Received: first
Enter message:
Windows PowerShell
PS D:\Term 8\Networks> py server.py
Server listening on 127.0.0.1:12345
Connected by ('127.0.0.1', 54538)
Received: Afirst
Received: Asecond
Received: Cfirst

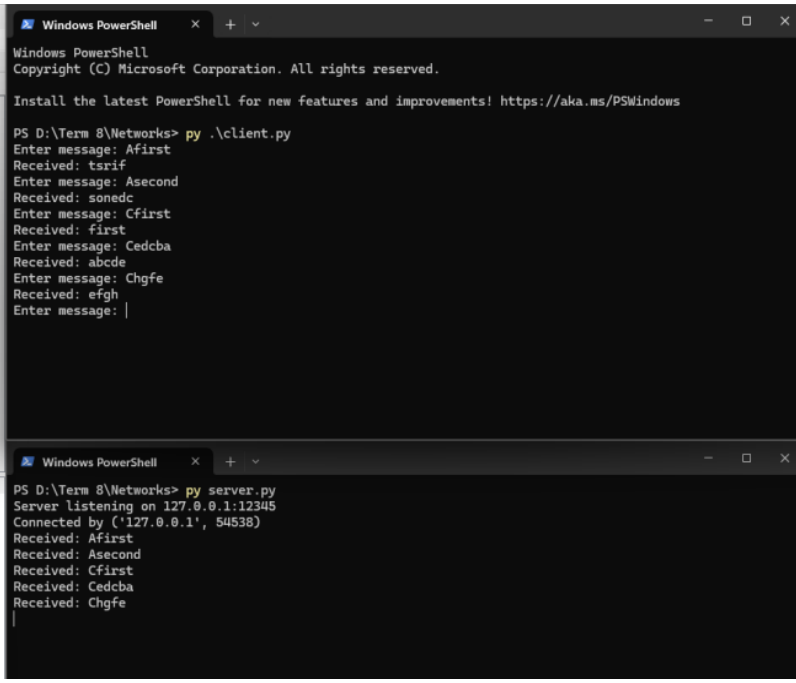

Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 12345
No. Time Source Destination Protocol Length Info
398 27.173327 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
399 27.173351 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=2
1208 61.458825 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
1209 61.458875 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1
1210 61.459307 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
1211 61.459363 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=2
1405 82.381125 127.0.0.1 127.0.0.1 TCP 49 54538 → 12345 [PSH, ACK]
1406 82.381243 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=2
1407 82.381911 127.0.0.1 127.0.0.1 TCP 48 12345 → 54538 [PSH, ACK]
1408 82.381961 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=3
1521 92.685052 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
1522 92.685091 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=2
1523 92.685558 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
1524 92.685605 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=3
1571 98.136331 127.0.0.1 127.0.0.1 TCP 49 54538 → 12345 [PSH, ACK]
1572 98.136478 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=3
1573 98.136920 127.0.0.1 127.0.0.1 TCP 48 12345 → 54538 [PSH, ACK]
1574 98.136996 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=4
Frame 101: 50 bytes on wire (400 bits), 50 bytes c
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 54538, Ds
Data (6 bytes)
0000 02 00 00 00 45 00 00 2e 67 46 40 00 80 06 00
0010 7f 00 00 01 7f 00 00 01 d5 0a 30 39 40 02 c3
0020 70 57 d2 ee 50 18 20 fa 26 40 00 00 41 66 69
0030 73 74

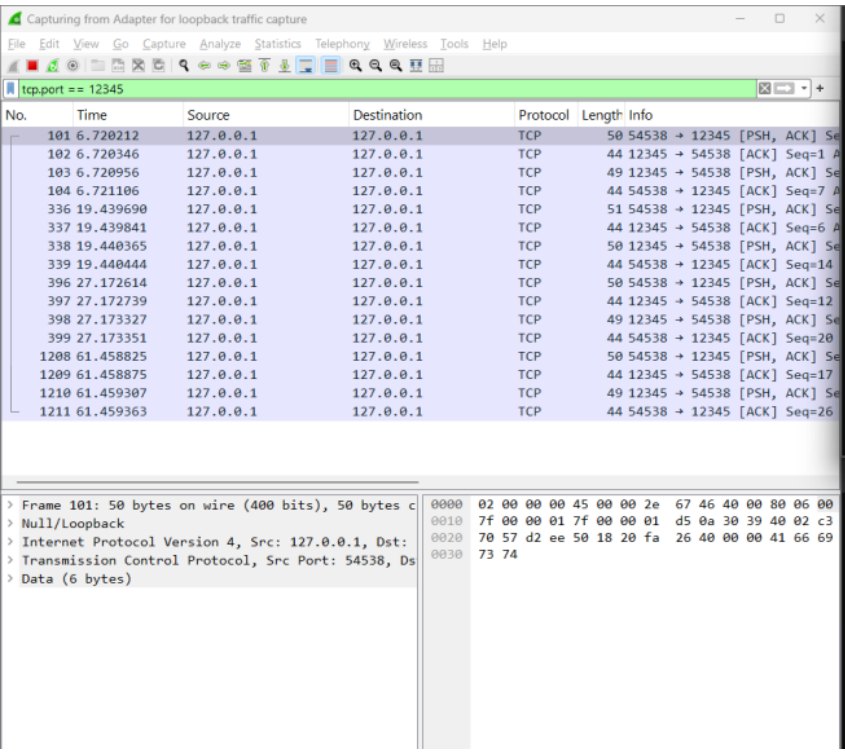

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\Term 8\Networks> py .\client.py
Enter message: Afirst
Received: tsrif
Enter message: Asecond
Received: sonedc
Enter message: Cfirst
Received: first
Enter message: Cedcba
Received: abcde
Enter message: Chgfe
Received: efgh
Enter message: Dsmall
Received: SMALL
Enter message: Dtiny
Received: TINY
Enter message:
Windows PowerShell
PS D:\Term 8\Networks> py server.py
Server listening on 127.0.0.1:12345
Connected by ('127.0.0.1', 54538)
Received: Afirst
Received: Asecond
Received: Cfirst
Received: Cedcba
Received: Chgfe
Received: Dsmall
Received: Dtiny

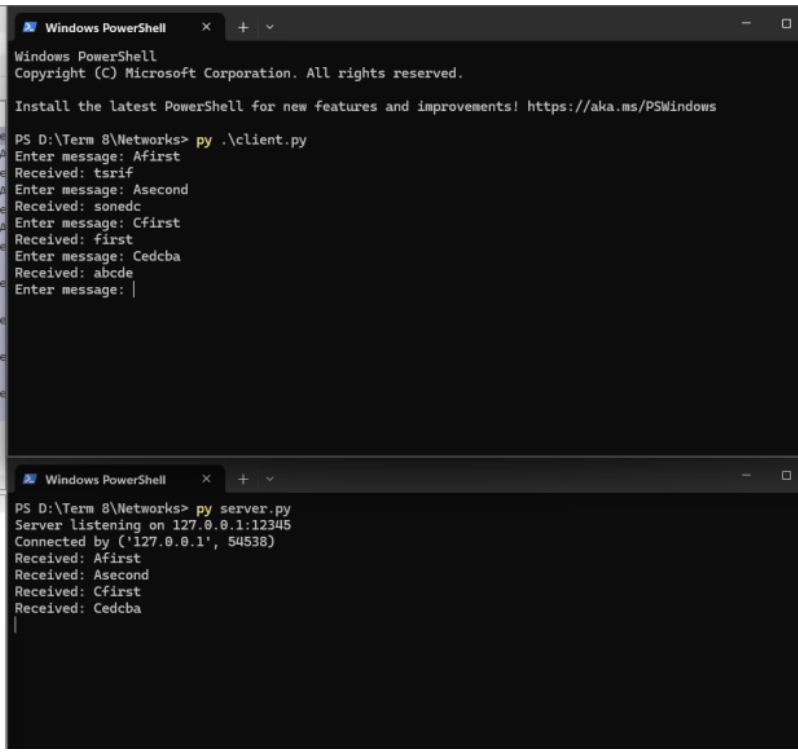

Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 12345
No. Time Source Destination Protocol Length Info
338 19.440365 127.0.0.1 127.0.0.1 TCP 50 12345 → 54538 [PSH, ACK]
339 19.440444 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=1
396 27.172614 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
397 27.172739 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1
398 27.173327 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
399 27.173351 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=2
1208 61.458825 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
1209 61.458875 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1
1210 61.459307 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
1211 61.459363 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=2
1405 82.381125 127.0.0.1 127.0.0.1 TCP 49 54538 → 12345 [PSH, ACK]
1406 82.381243 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=2
1407 82.381911 127.0.0.1 127.0.0.1 TCP 48 12345 → 54538 [PSH, ACK]
1408 82.381961 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=3
1521 92.685052 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
1522 92.685091 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=2
1523 92.685558 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
1524 92.685605 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=3
Frame 101: 50 bytes on wire (400 bits), 50 bytes c
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 54538, Ds
Data (6 bytes)
0000 02 00 00 00 45 00 00 2e 67 46 40 00 80 06 00
0010 7f 00 00 01 7f 00 00 01 d5 0a 30 39 40 02 c3
0020 70 57 d2 ee 50 18 20 fa 26 40 00 00 41 66 69
0030 73 74

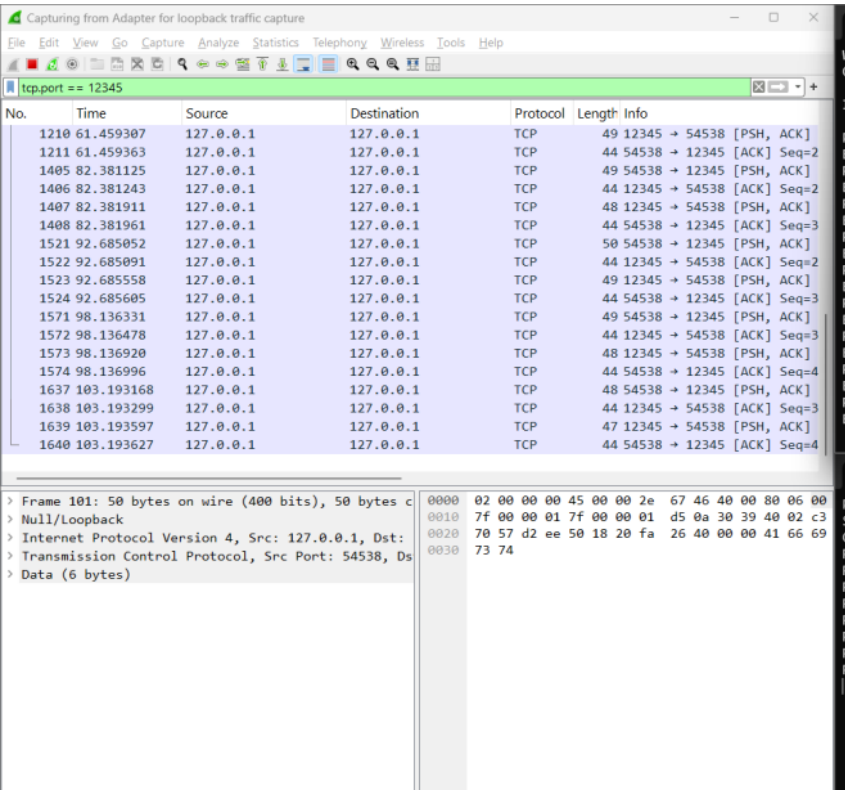

Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\Term 8\Networks> py .\client.py
Enter message: Afirst
Received: tsrif
Enter message: Asecond
Received: sonedc
Enter message: Cfirst
Received: first
Enter message: Cedcba
Received: abcde
Enter message: Chgfe
Received: efgh
Enter message: Dsmall
Received: SMALL
Enter message:
Windows PowerShell
PS D:\Term 8\Networks> py server.py
Server listening on 127.0.0.1:12345
Connected by ('127.0.0.1', 54538)
Received: Afirst
Received: Asecond
Received: Cfirst
Received: Cedcba
Received: Chgfe
Received: Dsmall

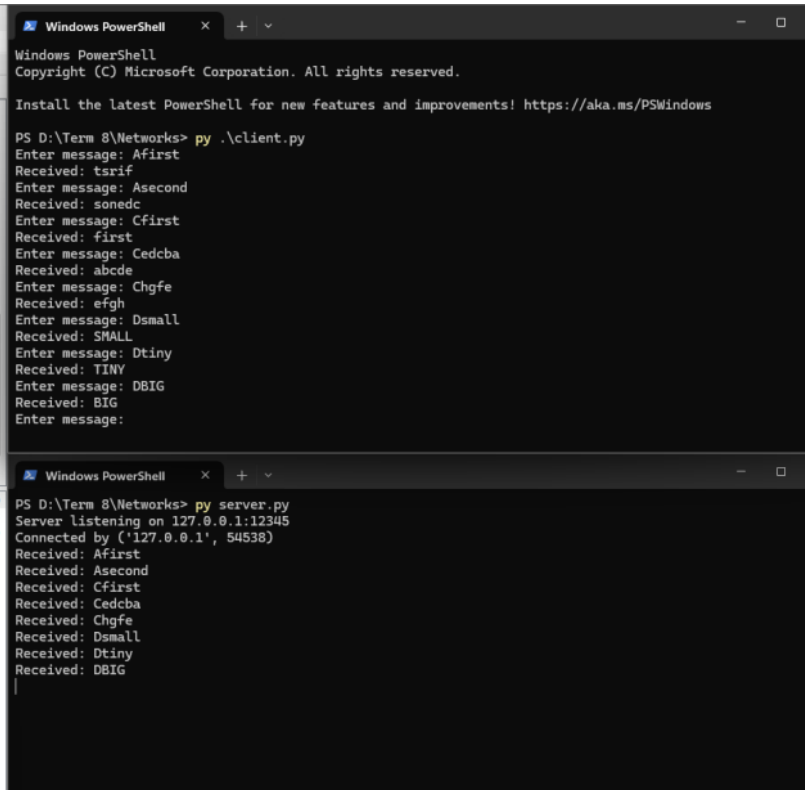

Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 12345
No. Time Source Destination Protocol Length Info
103 6.720956 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
104 6.721106 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=7
336 19.439690 127.0.0.1 127.0.0.1 TCP 51 54538 → 12345 [PSH, ACK]
337 19.439841 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=6
338 19.440365 127.0.0.1 127.0.0.1 TCP 50 12345 → 54538 [PSH, ACK]
339 19.440444 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=1
396 27.172614 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
397 27.172739 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1
398 27.173327 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
399 27.173351 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=2
1208 61.458825 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
1209 61.458875 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1
1210 61.459307 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
1211 61.459363 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=2
1405 82.381125 127.0.0.1 127.0.0.1 TCP 49 54538 → 12345 [PSH, ACK]
1406 82.381243 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=2
1407 82.381911 127.0.0.1 127.0.0.1 TCP 48 12345 → 54538 [PSH, ACK]
1408 82.381961 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=3
Frame 101: 50 bytes on wire (400 bits), 50 bytes c
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 54538, Ds
Data (6 bytes)
0000 02 00 00 00 45 00 00 2e 67 46 40 00 80 06 00
0010 7f 00 00 01 7f 00 00 01 d5 0a 30 39 40 02 c3
0020 70 57 d2 ee 50 18 20 fa 26 40 00 00 41 66 69
0030 73 74


Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\Term 8\Networks> py .\client.py
Enter message: Afirst
Received: tsrif
Enter message: Asecond
Received: sonedc
Enter message: Cfirst
Received: first
Enter message: Cedcba
Received: abcde
Enter message: Chgfe
Received: efgh
Enter message:
Windows PowerShell
PS D:\Term 8\Networks> py server.py
Server listening on 127.0.0.1:12345
Connected by ('127.0.0.1', 54538)
Received: Afirst
Received: Asecond
Received: Cfirst
Received: Cedcba
Received: Chgfe


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 12345
No. Time Source Destination Protocol Length Info
101 6.720212 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
102 6.720346 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=1
103 6.720956 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
104 6.721106 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=7
336 19.439690 127.0.0.1 127.0.0.1 TCP 51 54538 → 12345 [PSH, ACK]
337 19.439841 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=6
338 19.440365 127.0.0.1 127.0.0.1 TCP 50 12345 → 54538 [PSH, ACK]
339 19.440444 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=14
396 27.172614 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
397 27.172739 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=12
398 27.173327 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
399 27.173351 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=20
1208 61.458825 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
1209 61.458875 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=17
1210 61.459307 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
1211 61.459363 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=26
Frame 101: 50 bytes on wire (400 bits), 50 bytes c
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 54538, Ds
Data (6 bytes)
0000 02 00 00 00 45 00 00 2e 67 46 40 00 80 06 00
0010 7f 00 00 01 7f 00 00 01 d5 0a 30 39 40 02 c3
0020 70 57 d2 ee 50 18 20 fa 26 40 00 00 41 66 69
0030 73 74


Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\Term 8\Networks> py .\client.py
Enter message: Afirst
Received: tsrif
Enter message: Asecond
Received: sonedc
Enter message: Cfirst
Received: first
Enter message: Cedcba
Received: abcde
Enter message:
Windows PowerShell
PS D:\Term 8\Networks> py server.py
Server listening on 127.0.0.1:12345
Connected by ('127.0.0.1', 54538)
Received: Afirst
Received: Asecond
Received: Cfirst
Received: Cedcba


Capturing from Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 12345
No. Time Source Destination Protocol Length Info
1210 61.459307 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
1211 61.459363 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=2
1405 82.381125 127.0.0.1 127.0.0.1 TCP 49 54538 → 12345 [PSH, ACK]
1406 82.381243 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=2
1407 82.381911 127.0.0.1 127.0.0.1 TCP 48 12345 → 54538 [PSH, ACK]
1408 82.381961 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=3
1521 92.685052 127.0.0.1 127.0.0.1 TCP 50 54538 → 12345 [PSH, ACK]
1522 92.685091 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=2
1523 92.685558 127.0.0.1 127.0.0.1 TCP 49 12345 → 54538 [PSH, ACK]
1524 92.685605 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=3
1571 98.136331 127.0.0.1 127.0.0.1 TCP 49 54538 → 12345 [PSH, ACK]
1572 98.136478 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=3
1573 98.136920 127.0.0.1 127.0.0.1 TCP 48 12345 → 54538 [PSH, ACK]
1574 98.136996 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=4
1637 103.193168 127.0.0.1 127.0.0.1 TCP 48 54538 → 12345 [PSH, ACK]
1638 103.193299 127.0.0.1 127.0.0.1 TCP 44 12345 → 54538 [ACK] Seq=3
1639 103.193597 127.0.0.1 127.0.0.1 TCP 47 12345 → 54538 [PSH, ACK]
1640 103.193627 127.0.0.1 127.0.0.1 TCP 44 54538 → 12345 [ACK] Seq=4
Frame 101: 50 bytes on wire (400 bits), 50 bytes c
Null/Loopback
Internet Protocol Version 4, Src: 127.0.0.1, Dst:
Transmission Control Protocol, Src Port: 54538, Ds
Data (6 bytes)
0000 02 00 00 00 45 00 00 2e 67 46 40 00 80 06 00
0010 7f 00 00 01 7f 00 00 01 d5 0a 30 39 40 02 c3
0020 70 57 d2 ee 50 18 20 fa 26 40 00 00 41 66 69
0030 73 74


Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS D:\Term 8\Networks> py .\client.py
Enter message: Afirst
Received: tsrif
Enter message: Asecond
Received: sonedc
Enter message: Cfirst
Received: first
Enter message: Cedcba
Received: abcde
Enter message: Chgfe
Received: efgh
Enter message: Dsmall
Received: SMALL
Enter message: Dtiny
Received: TINY
Enter message: DBIG
Received: BIG
Enter message:
Windows PowerShell
PS D:\Term 8\Networks> py server.py
Server listening on 127.0.0.1:12345
Connected by ('127.0.0.1', 54538)
Received: Afirst
Received: Asecond
Received: Cfirst
Received: Cedcba
Received: Chgfe
Received: Dsmall
Received: Dtiny
Received: DBIG