P3 Report

Introduction

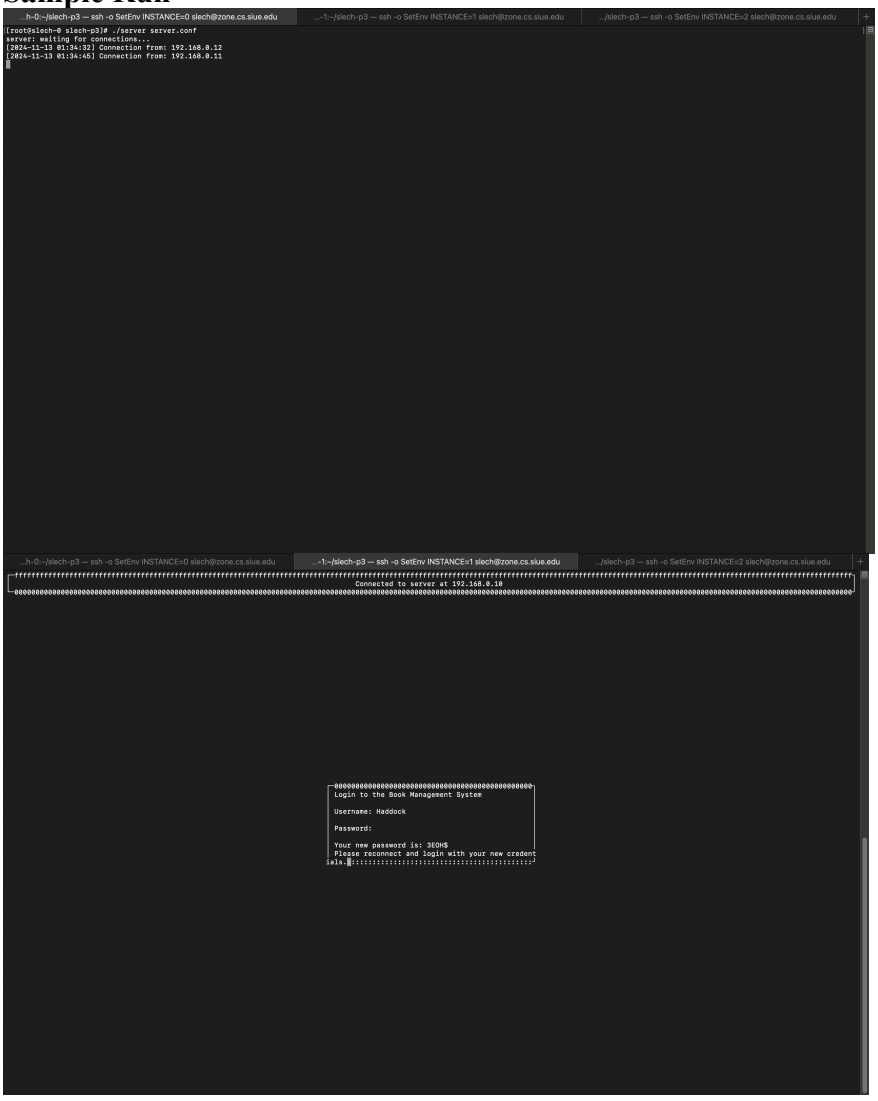
The primary objective of this project was to deepen my understanding of cybersecurity principles and secure network programming. A significant focus was placed on establishing encrypted communications between the client and server using SSL/TLS protocols, thereby ensuring data confidentiality and integrity. Additionally, I sought to develop robust user authentication mechanisms, including password hashing, salting, and secure storage, to protect user credentials effectively. Another key goal was to create an intuitive and secure text-based user interface (TUI) using the ncurses library, facilitating seamless interactions between users and the system. Prior to embarking on P3, I possessed some understanding of secure programming practices, including input validation, error handling, and basic encryption techniques. However, my practical experience with integrating OpenSSL for secure communications and managing cryptographic operations was limited. Through this project, I anticipated gaining advanced knowledge of cryptographic algorithms, specifically AES-256-CBC for data encryption and SHA-512 for hashing, as well as enhancing my skills in implementing secure password management and comprehensive security measures to safeguard data transmitted between client and server.

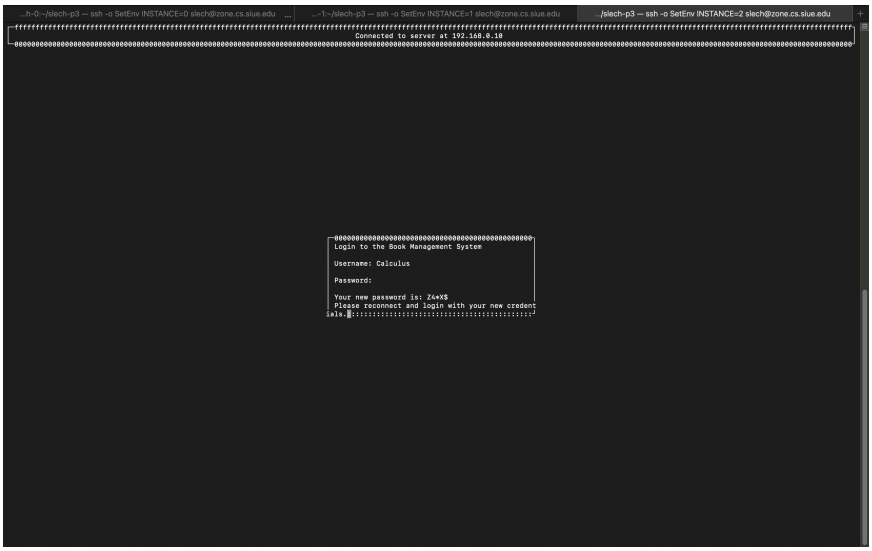
Design

The system is architected on a client-server model, where the server manages a book database, and clients interact with the server to perform various operations such as searching, managing, and recommending books. Communication between the client and server is secured using SSL/TLS protocols to ensure that all data transmitted is encrypted and protected against eavesdropping and tampering. One of the key design choices was the implementation of secure communication using OpenSSL. By utilizing OpenSSL, I established encrypted channels between the client and server, ensuring that all data transmitted remains confidential and integral. I selected strong cipher suites like TLS_AES_256_GCM_SHA384 and TLS_CHACHA20_POLY1305_SHA256 to enhance security. Additionally, certificate management was implemented to authenticate the server to the client, thereby preventing man-in-the-middle attacks. For user authentication, a robust mechanism was developed involving password hashing and salting. User passwords are hashed using the SHA-512 algorithm combined with unique salts before being stored in the .book_shadow file. This approach ensures that even if the password storage is compromised, the actual passwords remain protected. Furthermore, passwords are encrypted using AES-256-CBC before being transmitted over the network, adding an extra layer of security against potential interception. The client application features a text-based user interface (TUI) developed using the ncurses library. This choice was made to create an interactive and user-friendly interface that allows users to navigate through various operational modes (SEARCH, MANAGE, RECOMMEND) seamlessly. The TUI facilitates smooth user interactions, making the system accessible and easy to use. A significant challenge encountered during the design phase was integrating OpenSSL effectively. Configuring OpenSSL correctly for both client and server required meticulous attention to detail, especially in setting up cipher suites and managing certificates. Additionally, managing and interpreting OpenSSL errors necessitated comprehensive error-checking mechanisms to ensure smooth encryption and decryption processes. Another challenge was implementing secure

password handling, which involved generating secure passwords and salts that met complexity requirements while maintaining randomness. Developing reliable encryption and decryption functions to securely transmit passwords between client and server also posed some challenges.

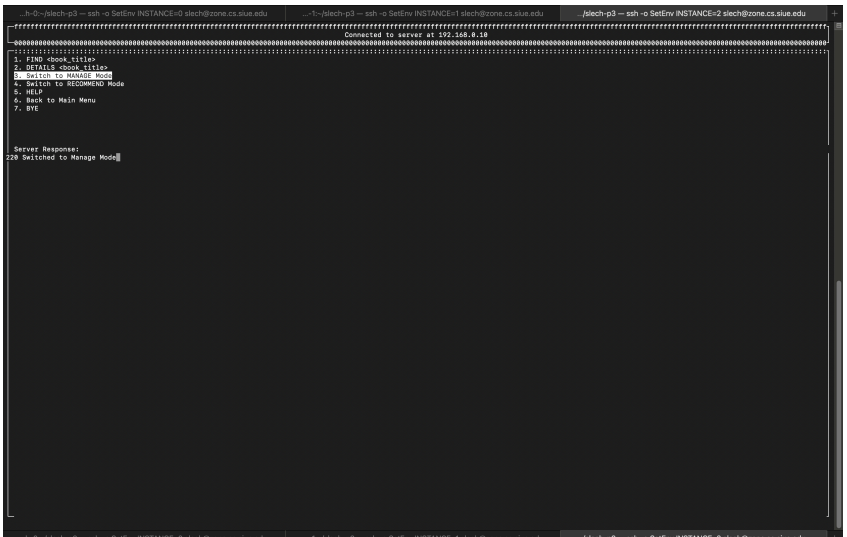
Sample Run





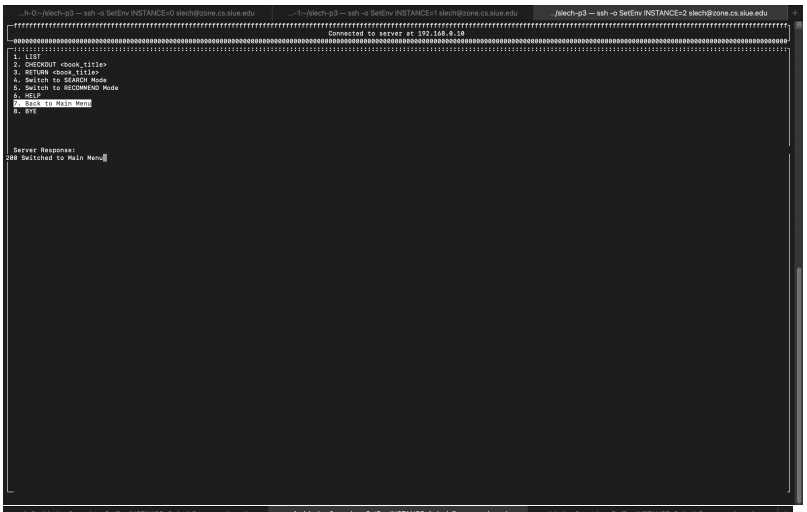
Initial connections from multiple clients and registering. Afterwards must reconnect on same clients and relogin with new password. In These examples when logging in I used USER -> Haddock and PASS -> Stew1!, USER -> Calculus and PASS -> St3w!!

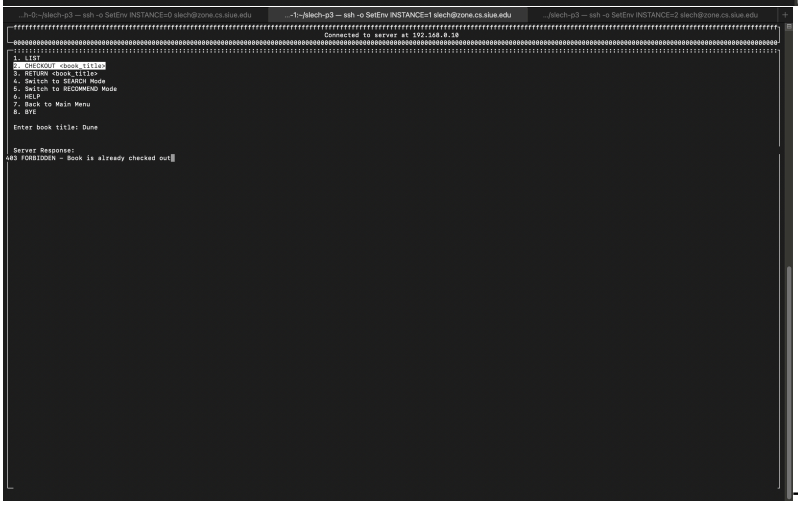
Navigate TUI with arrow keys press return/enter


../slech-p3 — ssh -o SetEnv INSTANCE=2 slech@zone.cs.siue.edu
Connected to server at 192.168.0.10
1. FIND <book_title>
2. DETAILS <book_title>
3. Switch to MANAGE Mode
4. Switch to RECOMMEND Mode
5. HELP
6. Back to Main Menu
7. BYE
Server Response:
220 Switched to Manage Mode

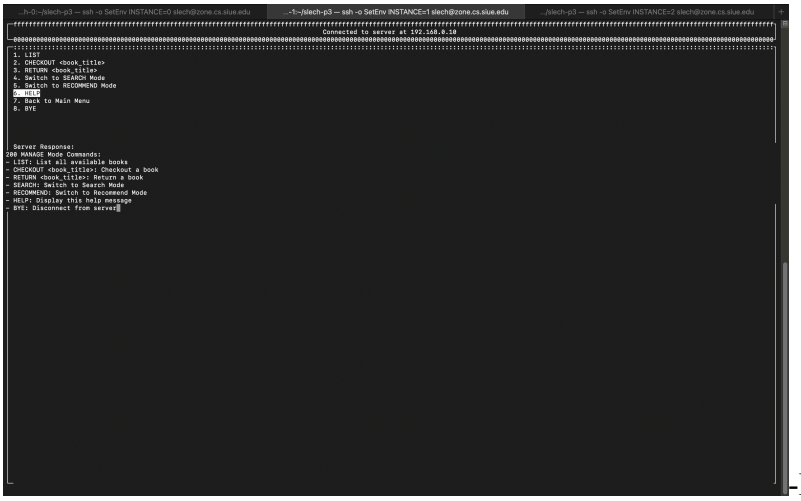

../slech-p3 — ssh -o SetEnv INSTANCE=2 slech@zone.cs.siue.edu
Connected to server at 192.168.0.10
1. LIST
2. CHECKOUT <book_title>
3. RETURN <book_title>
4. Switch to SEARCH Mode
5. Switch to RECOMMEND Mode
6. HELP
7. Back to Main Menu
8. BYE
Server Response:
260 <data> list of available books:
Title: Dune, Author: Frank Herbert, Genre: Science Fiction, Available: Yes, Rating: 5
Title: The Martian, Author: Andy Weir, Genre: Science Fiction, Available: Yes, Rating: 5
Title: Harry Potter and the Sorcerer's Stone, Author: J.K. Rowling, Genre: Fantasy, Available: Yes, Rating: 2
Title: And Then There Were None, Author: Agatha Christie, Genre: Mystery, Available: Yes, Rating: 1
Title: The Girl with the Dragon Tattoo, Author: Stieg Larsson, Genre: Mystery, Available: Yes, Rating: 2


../slech-p3 — ssh -o SetEnv INSTANCE=2 slech@zone.cs.siue.edu
Connected to server at 192.168.0.10
1. LIST
2. CHECKOUT <book_title>
3. RETURN <book_title>
4. Switch to SEARCH Mode
5. Switch to RECOMMEND Mode
6. HELP
7. Back to Main Menu
8. BYE
Enter book title: Harry Potter
Server Response:
250 <data> Book checked out

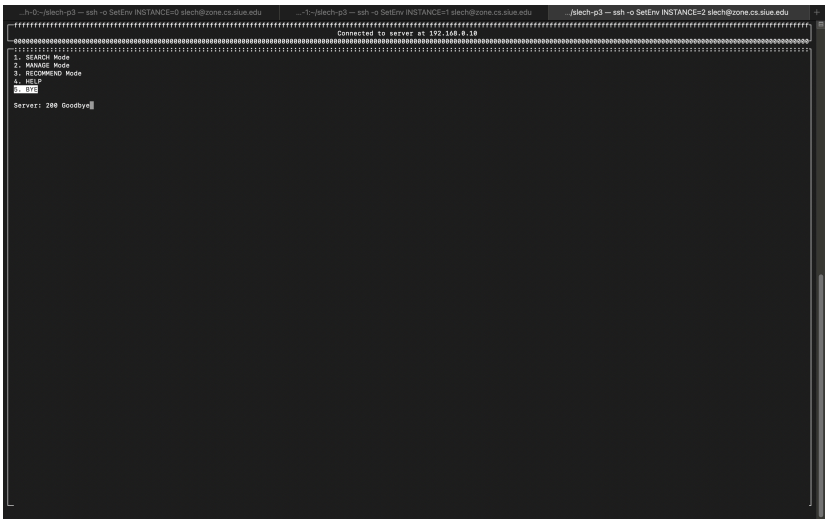


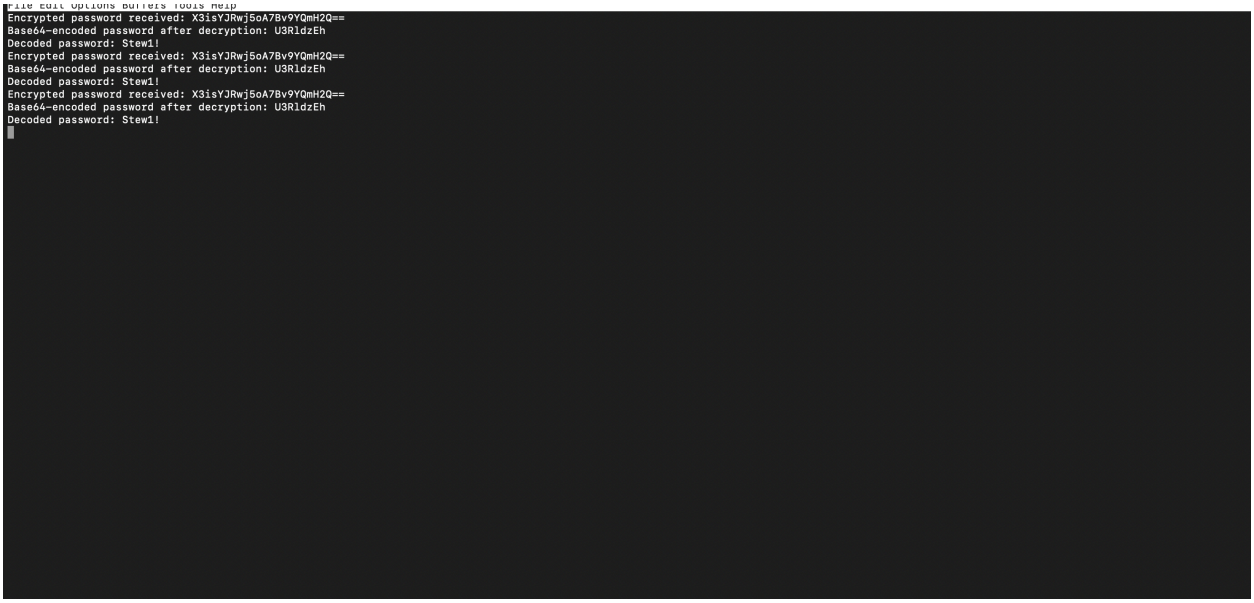


-Concurrency



-Help Mode specific

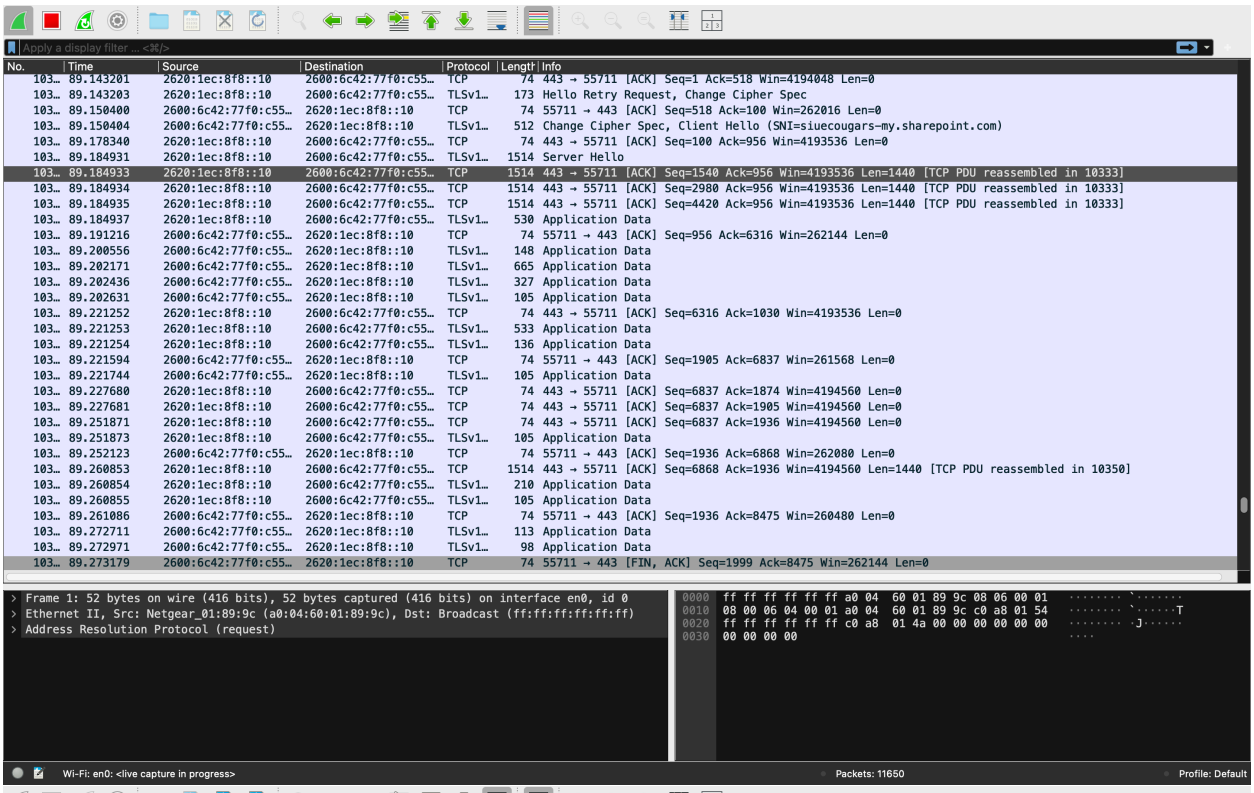


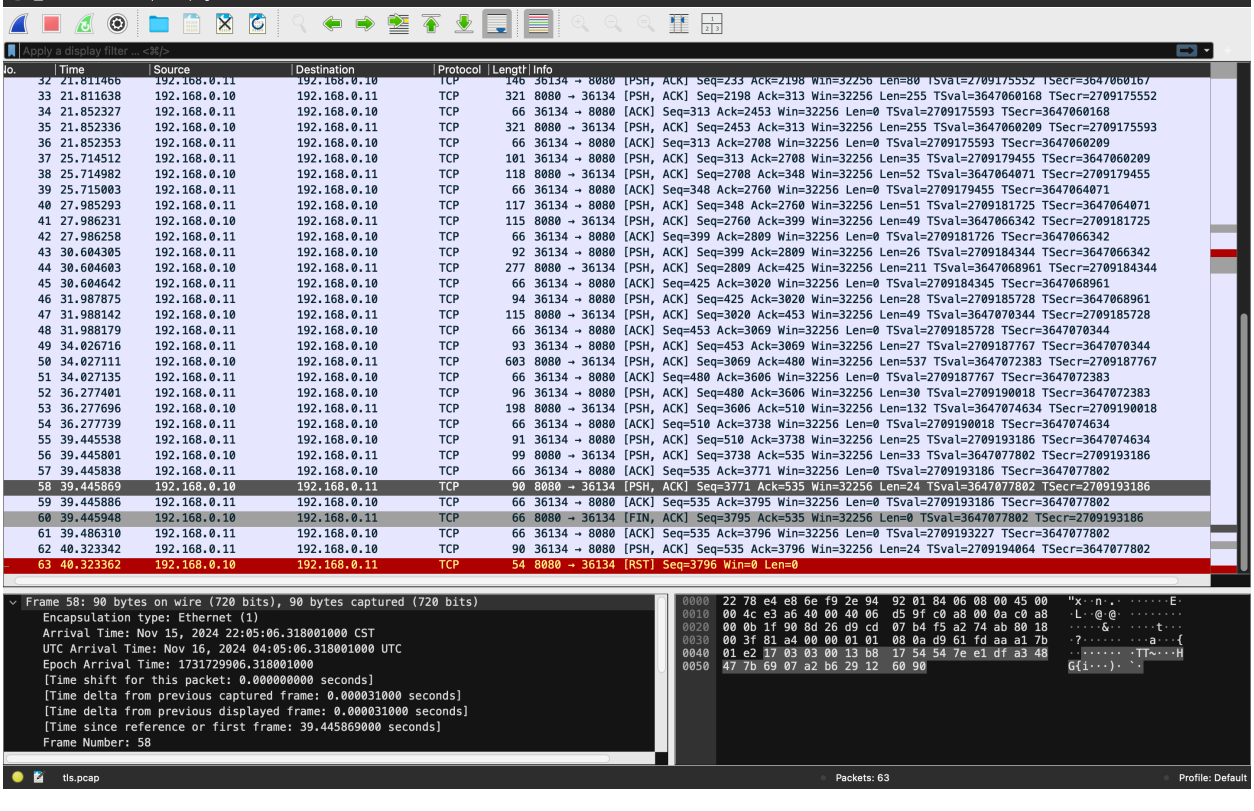


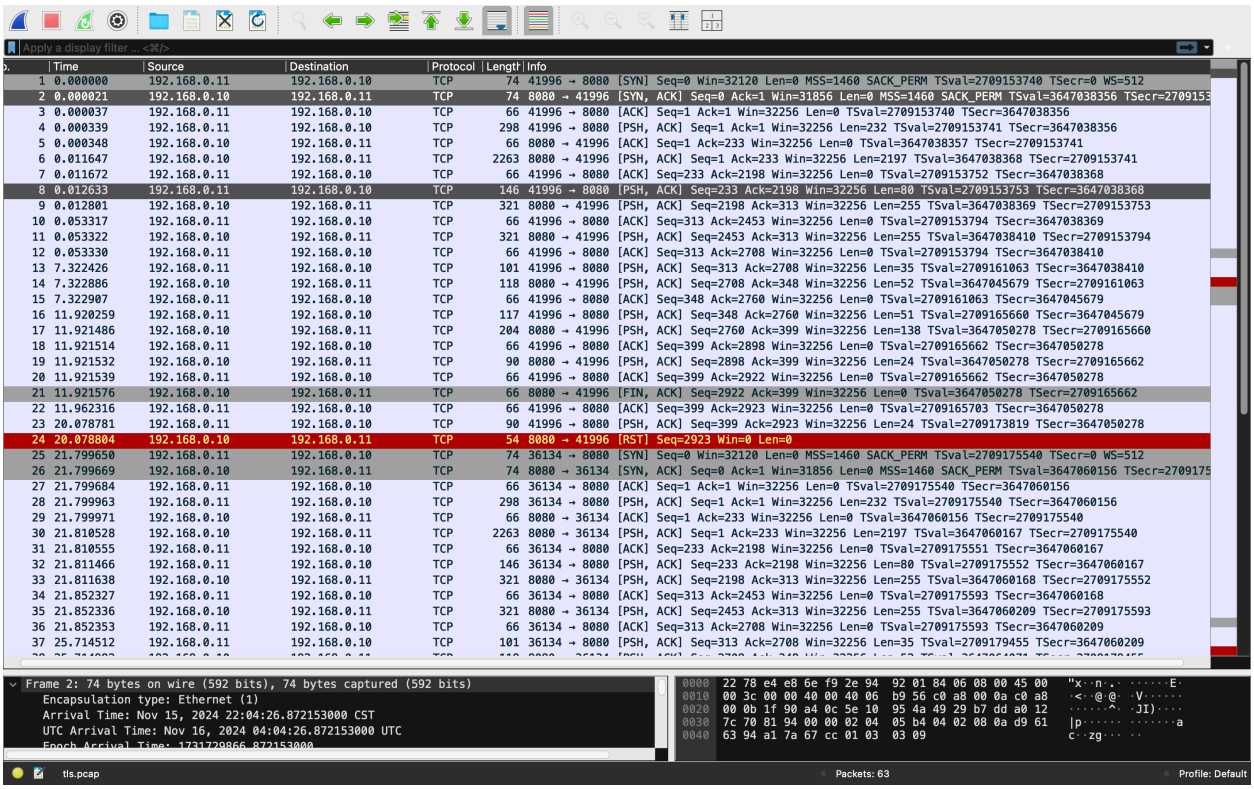
Proof of base64 encoding in debug logs made by server and client

Proof of Secure Communication

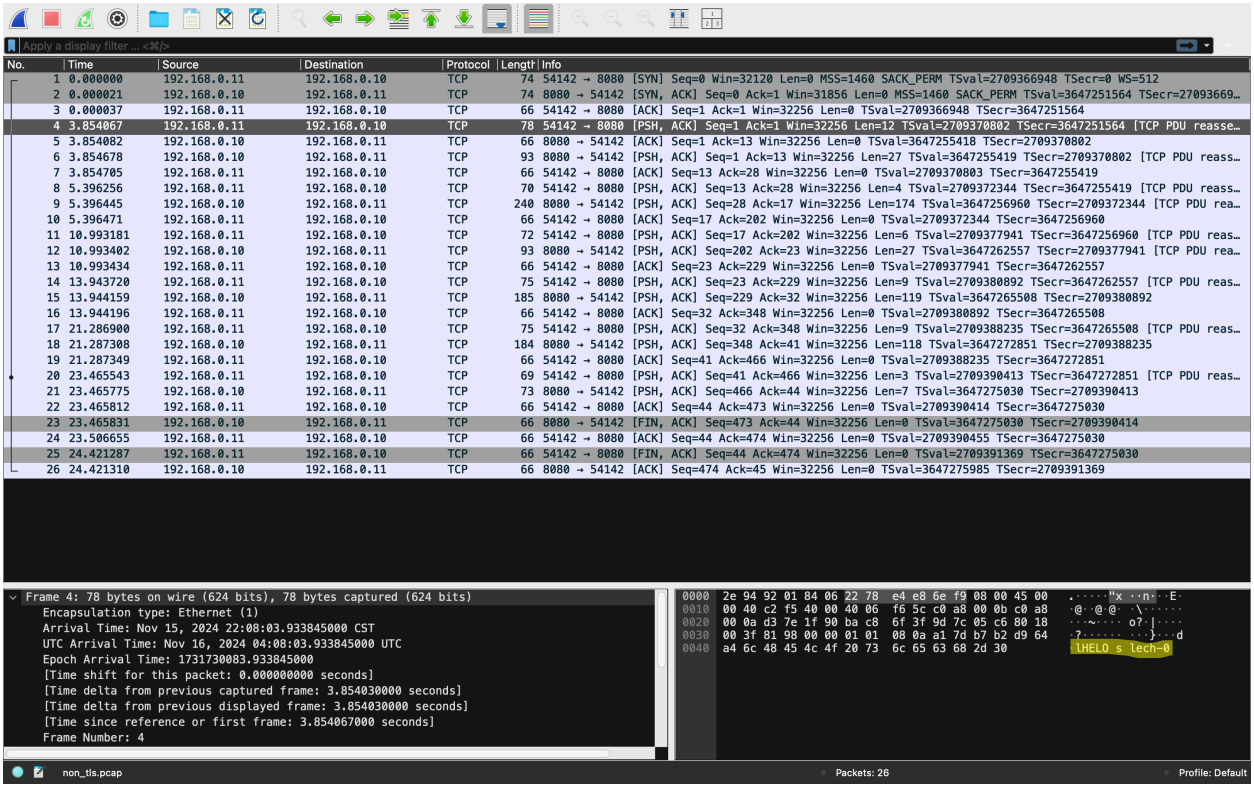
TLS CAPTURE

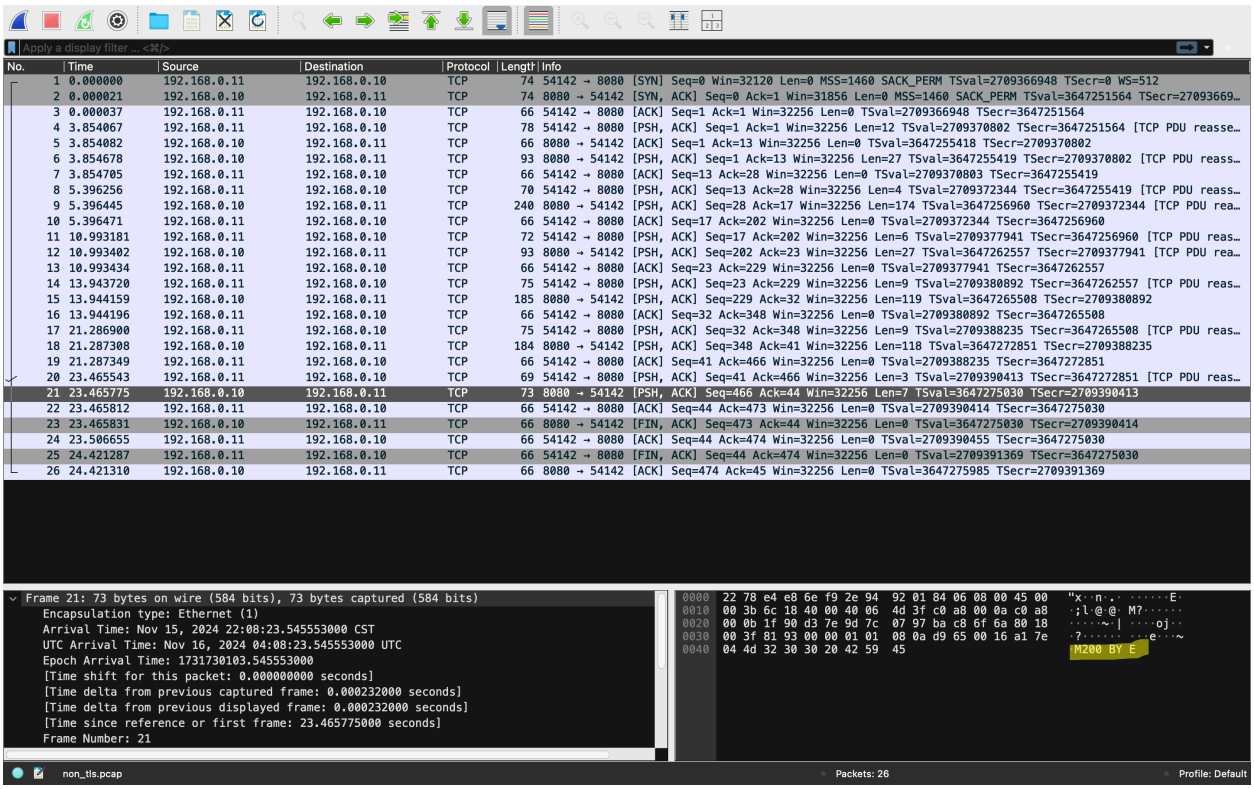

Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
103… 89.143201 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 74 443 → 55711 [ACK] Seq=1 Ack=518 Win=4194048 Len=0
103… 89.143203 2620:1ec:8f8::10 2600:6c42:77f0:c55… TLSv1… 173 Hello Retry Request, Change Cipher Spec
103… 89.150400 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TCP 74 55711 → 443 [ACK] Seq=518 Ack=100 Win=262016 Len=0
103… 89.150404 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TLSv1… 512 Change Cipher Spec, Client Hello (SNI=siuecougars-my.sharepoint.com)
103… 89.178340 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 74 443 → 55711 [ACK] Seq=100 Ack=956 Win=4193536 Len=0
103… 89.184931 2620:1ec:8f8::10 2600:6c42:77f0:c55… TLSv1… 1514 Server Hello
103… 89.184933 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 1514 443 → 55711 [ACK] Seq=1540 Ack=956 Win=4193536 Len=1440 [TCP PDU reassembled in 10333]
103… 89.184934 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 1514 443 → 55711 [ACK] Seq=2980 Ack=956 Win=4193536 Len=1440 [TCP PDU reassembled in 10333]
103… 89.184935 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 1514 443 → 55711 [ACK] Seq=4420 Ack=956 Win=4193536 Len=1440 [TCP PDU reassembled in 10333]
103… 89.184937 2620:1ec:8f8::10 2600:6c42:77f0:c55… TLSv1… 530 Application Data
103… 89.191216 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TCP 74 55711 → 443 [ACK] Seq=956 Ack=6316 Win=262144 Len=0
103… 89.200556 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TLSv1… 148 Application Data
103… 89.202171 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TLSv1… 665 Application Data
103… 89.202436 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TLSv1… 327 Application Data
103… 89.202631 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TLSv1… 105 Application Data
103… 89.221252 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 74 443 → 55711 [ACK] Seq=6316 Ack=1030 Win=4193536 Len=0
103… 89.221253 2620:1ec:8f8::10 2600:6c42:77f0:c55… TLSv1… 533 Application Data
103… 89.221254 2620:1ec:8f8::10 2600:6c42:77f0:c55… TLSv1… 136 Application Data
103… 89.221594 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TCP 74 55711 → 443 [ACK] Seq=1905 Ack=6837 Win=261568 Len=0
103… 89.221744 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TLSv1… 105 Application Data
103… 89.227680 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 74 443 → 55711 [ACK] Seq=6837 Ack=1874 Win=4194560 Len=0
103… 89.227681 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 74 443 → 55711 [ACK] Seq=6837 Ack=1905 Win=4194560 Len=0
103… 89.251871 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 74 443 → 55711 [ACK] Seq=6837 Ack=1936 Win=4194560 Len=0
103… 89.251873 2620:1ec:8f8::10 2600:6c42:77f0:c55… TLSv1… 105 Application Data
103… 89.252123 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TCP 74 55711 → 443 [ACK] Seq=1936 Ack=6868 Win=262080 Len=0
103… 89.260853 2620:1ec:8f8::10 2600:6c42:77f0:c55… TCP 1514 443 → 55711 [ACK] Seq=6868 Ack=1936 Win=4194560 Len=1440 [TCP PDU reassembled in 10350]
103… 89.260854 2620:1ec:8f8::10 2600:6c42:77f0:c55… TLSv1… 210 Application Data
103… 89.260855 2620:1ec:8f8::10 2600:6c42:77f0:c55… TLSv1… 105 Application Data
103… 89.261086 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TCP 74 55711 → 443 [ACK] Seq=1936 Ack=8475 Win=260480 Len=0
103… 89.272711 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TLSv1… 113 Application Data
103… 89.272971 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TLSv1… 98 Application Data
103… 89.273179 2600:6c42:77f0:c55… 2620:1ec:8f8::10 TCP 74 55711 → 443 [FIN, ACK] Seq=1999 Ack=8475 Win=262144 Len=0
Frame 1: 52 bytes on wire (416 bits), 52 bytes captured (416 bits) on interface en0, id 0
Ethernet II, Src: Netgear_01:89:9c (a0:04:60:01:89:9c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (request)
0000 ff ff ff ff ff ff a0 04 60 01 89 9c 08 06 00 01 .... `.......
0010 08 00 06 04 00 01 a0 04 60 01 89 9c c0 a8 01 54 .... `......T
0020 ff ff ff ff ff ff c0 a8 01 4a 00 00 00 00 00 00 .... .J......
0030 00 00 00 00 ....
Wi-Fi: en0: <live capture in progress>
Packets: 11650
Profile: Default


Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
32 21.811466 192.168.0.11 192.168.0.10 TCP 146 36134 → 8080 [PSH, ACK] Seq=233 Ack=2198 Win=32256 Len=80 TSval=2709175552 TSecr=3647060167
33 21.811638 192.168.0.10 192.168.0.11 TCP 321 8080 → 36134 [PSH, ACK] Seq=2198 Ack=313 Win=32256 Len=255 TSval=3647060168 TSecr=2709175552
34 21.852327 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=313 Ack=2453 Win=32256 Len=0 TSval=2709175593 TSecr=3647060168
35 21.852336 192.168.0.10 192.168.0.11 TCP 321 8080 → 36134 [PSH, ACK] Seq=2453 Ack=313 Win=32256 Len=255 TSval=3647060209 TSecr=2709175593
36 21.852353 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=313 Ack=2708 Win=32256 Len=0 TSval=2709175593 TSecr=3647060209
37 25.714512 192.168.0.11 192.168.0.10 TCP 101 36134 → 8080 [PSH, ACK] Seq=313 Ack=2708 Win=32256 Len=35 TSval=2709179455 TSecr=3647060209
38 25.714982 192.168.0.10 192.168.0.11 TCP 118 8080 → 36134 [PSH, ACK] Seq=2708 Ack=348 Win=32256 Len=52 TSval=3647064071 TSecr=2709179455
39 25.715003 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=348 Ack=2760 Win=32256 Len=0 TSval=2709179455 TSecr=3647064071
40 27.985293 192.168.0.11 192.168.0.10 TCP 117 36134 → 8080 [PSH, ACK] Seq=348 Ack=2760 Win=32256 Len=51 TSval=2709181725 TSecr=3647064071
41 27.986231 192.168.0.10 192.168.0.11 TCP 115 8080 → 36134 [PSH, ACK] Seq=2760 Ack=399 Win=32256 Len=49 TSval=3647066342 TSecr=2709181725
42 27.986258 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=399 Ack=2809 Win=32256 Len=0 TSval=2709181726 TSecr=3647066342
43 30.604305 192.168.0.11 192.168.0.10 TCP 92 36134 → 8080 [PSH, ACK] Seq=399 Ack=2809 Win=32256 Len=26 TSval=2709184344 TSecr=3647066342
44 30.604603 192.168.0.10 192.168.0.11 TCP 277 8080 → 36134 [PSH, ACK] Seq=2809 Ack=425 Win=32256 Len=211 TSval=3647068961 TSecr=2709184344
45 30.604642 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=425 Ack=3020 Win=32256 Len=0 TSval=2709184345 TSecr=3647068961
46 31.987875 192.168.0.11 192.168.0.10 TCP 94 36134 → 8080 [PSH, ACK] Seq=425 Ack=3020 Win=32256 Len=28 TSval=2709185728 TSecr=3647068961
47 31.988142 192.168.0.10 192.168.0.11 TCP 115 8080 → 36134 [PSH, ACK] Seq=3020 Ack=453 Win=32256 Len=49 TSval=3647070344 TSecr=2709185728
48 31.988179 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=453 Ack=3069 Win=32256 Len=0 TSval=2709185728 TSecr=3647070344
49 34.026716 192.168.0.11 192.168.0.10 TCP 93 36134 → 8080 [PSH, ACK] Seq=453 Ack=3069 Win=32256 Len=27 TSval=2709187767 TSecr=3647070344
50 34.027111 192.168.0.10 192.168.0.11 TCP 603 8080 → 36134 [PSH, ACK] Seq=3069 Ack=480 Win=32256 Len=537 TSval=3647072383 TSecr=2709187767
51 34.027135 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=480 Ack=3606 Win=32256 Len=0 TSval=2709187767 TSecr=3647072383
52 36.277401 192.168.0.11 192.168.0.10 TCP 96 36134 → 8080 [PSH, ACK] Seq=480 Ack=3606 Win=32256 Len=30 TSval=2709190018 TSecr=3647072383
53 36.277696 192.168.0.10 192.168.0.11 TCP 198 8080 → 36134 [PSH, ACK] Seq=3606 Ack=510 Win=32256 Len=132 TSval=3647074634 TSecr=2709190018
54 36.277739 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=510 Ack=3738 Win=32256 Len=0 TSval=2709190018 TSecr=3647074634
55 39.445538 192.168.0.11 192.168.0.10 TCP 91 36134 → 8080 [PSH, ACK] Seq=510 Ack=3738 Win=32256 Len=25 TSval=2709193186 TSecr=3647074634
56 39.445801 192.168.0.10 192.168.0.11 TCP 99 8080 → 36134 [PSH, ACK] Seq=3738 Ack=535 Win=32256 Len=33 TSval=3647077802 TSecr=2709193186
57 39.445838 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=535 Ack=3771 Win=32256 Len=0 TSval=2709193186 TSecr=3647077802
58 39.445869 192.168.0.10 192.168.0.11 TCP 90 8080 → 36134 [PSH, ACK] Seq=3771 Ack=535 Win=32256 Len=24 TSval=3647077802 TSecr=2709193186
59 39.445886 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=535 Ack=3795 Win=32256 Len=0 TSval=2709193186 TSecr=3647077802
60 39.445948 192.168.0.10 192.168.0.11 TCP 66 8080 → 36134 [FIN, ACK] Seq=3795 Ack=535 Win=32256 Len=0 TSval=3647077802 TSecr=2709193186
61 39.486310 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=535 Ack=3796 Win=32256 Len=0 TSval=2709193227 TSecr=3647077802
62 40.323342 192.168.0.11 192.168.0.10 TCP 90 36134 → 8080 [PSH, ACK] Seq=535 Ack=3796 Win=32256 Len=24 TSval=2709194064 TSecr=3647077802
63 40.323362 192.168.0.10 192.168.0.11 TCP 54 8080 → 36134 [RST] Seq=3796 Win=0 Len=0
Frame 58: 90 bytes on wire (720 bits), 90 bytes captured (720 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Nov 15, 2024 22:05:06.318001000 CST
UTC Arrival Time: Nov 16, 2024 04:05:06.318001000 UTC
Epoch Arrival Time: 1731729906.318001000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000031000 seconds]
[Time delta from previous displayed frame: 0.000031000 seconds]
[Time since reference or first frame: 39.445869000 seconds]
Frame Number: 58
0000 22 78 e4 e8 6e f9 2e 94 92 01 84 06 08 00 45 00 "x··n·.· ·····E·
0010 00 4c e3 a6 40 00 40 06 d5 9f c0 a8 00 0a c0 a8 ·L··@·@· ········
0020 00 0b 1f 90 8d 26 d9 cd 07 b4 f5 a2 74 ab 80 18 ·····&·· ····t···
0030 00 3f 81 a4 00 00 01 01 08 0a d9 61 fd aa a1 7b ·?····· ···a···{
0040 01 e2 17 03 03 00 13 b8 17 54 54 7e e1 df a3 48 ·····TT~···H
0050 47 7b 69 07 a2 b6 29 12 60 90 G{i···)· `·
tls.pcap
Packets: 63
Profile: Default


Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.11 192.168.0.10 TCP 74 41996 → 8080 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2709153740 TSecr=0 WS=512
2 0.000021 192.168.0.10 192.168.0.11 TCP 74 8080 → 41996 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=3647038356 TSecr=2709153
3 0.000037 192.168.0.11 192.168.0.10 TCP 66 41996 → 8080 [ACK] Seq=1 Ack=1 Win=32256 Len=0 TSval=2709153740 TSecr=3647038356
4 0.000339 192.168.0.11 192.168.0.10 TCP 298 41996 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=32256 Len=232 TSval=2709153741 TSecr=3647038356
5 0.000348 192.168.0.10 192.168.0.11 TCP 66 8080 → 41996 [ACK] Seq=1 Ack=233 Win=32256 Len=0 TSval=3647038357 TSecr=2709153741
6 0.011647 192.168.0.10 192.168.0.11 TCP 2263 8080 → 41996 [PSH, ACK] Seq=1 Ack=233 Win=32256 Len=2197 TSval=3647038368 TSecr=2709153741
7 0.011672 192.168.0.11 192.168.0.10 TCP 66 41996 → 8080 [ACK] Seq=233 Ack=2198 Win=32256 Len=0 TSval=2709153752 TSecr=3647038368
8 0.012633 192.168.0.11 192.168.0.10 TCP 146 41996 → 8080 [PSH, ACK] Seq=233 Ack=2198 Win=32256 Len=80 TSval=2709153753 TSecr=3647038368
9 0.012801 192.168.0.10 192.168.0.11 TCP 321 8080 → 41996 [PSH, ACK] Seq=2198 Ack=313 Win=32256 Len=255 TSval=3647038369 TSecr=2709153753
10 0.053317 192.168.0.11 192.168.0.10 TCP 66 41996 → 8080 [ACK] Seq=313 Ack=2453 Win=32256 Len=0 TSval=2709153794 TSecr=3647038369
11 0.053322 192.168.0.10 192.168.0.11 TCP 321 8080 → 41996 [PSH, ACK] Seq=2453 Ack=313 Win=32256 Len=255 TSval=3647038410 TSecr=2709153794
12 0.053330 192.168.0.11 192.168.0.10 TCP 66 41996 → 8080 [ACK] Seq=313 Ack=2708 Win=32256 Len=0 TSval=2709153794 TSecr=3647038410
13 7.322426 192.168.0.11 192.168.0.10 TCP 101 41996 → 8080 [PSH, ACK] Seq=313 Ack=2708 Win=32256 Len=35 TSval=2709161063 TSecr=3647038410
14 7.322886 192.168.0.10 192.168.0.11 TCP 118 8080 → 41996 [PSH, ACK] Seq=2708 Ack=348 Win=32256 Len=52 TSval=3647045679 TSecr=2709161063
15 7.322907 192.168.0.11 192.168.0.10 TCP 66 41996 → 8080 [ACK] Seq=348 Ack=2760 Win=32256 Len=0 TSval=2709161063 TSecr=3647045679
16 11.920259 192.168.0.11 192.168.0.10 TCP 117 41996 → 8080 [PSH, ACK] Seq=348 Ack=2760 Win=32256 Len=51 TSval=2709165660 TSecr=3647045679
17 11.921486 192.168.0.10 192.168.0.11 TCP 204 8080 → 41996 [PSH, ACK] Seq=2760 Ack=399 Win=32256 Len=138 TSval=3647050278 TSecr=2709165660
18 11.921514 192.168.0.11 192.168.0.10 TCP 66 41996 → 8080 [ACK] Seq=399 Ack=2898 Win=32256 Len=0 TSval=2709165662 TSecr=3647050278
19 11.921532 192.168.0.10 192.168.0.11 TCP 90 8080 → 41996 [PSH, ACK] Seq=2898 Ack=399 Win=32256 Len=24 TSval=3647050278 TSecr=2709165662
20 11.921539 192.168.0.11 192.168.0.10 TCP 66 41996 → 8080 [ACK] Seq=399 Ack=2922 Win=32256 Len=0 TSval=2709165662 TSecr=3647050278
21 11.921576 192.168.0.10 192.168.0.11 TCP 66 8080 → 41996 [FIN, ACK] Seq=2922 Ack=399 Win=32256 Len=0 TSval=3647050278 TSecr=2709165662
22 11.962316 192.168.0.11 192.168.0.10 TCP 66 41996 → 8080 [ACK] Seq=399 Ack=2923 Win=32256 Len=0 TSval=2709165703 TSecr=3647050278
23 20.078781 192.168.0.11 192.168.0.10 TCP 90 41996 → 8080 [PSH, ACK] Seq=399 Ack=2923 Win=32256 Len=24 TSval=2709173819 TSecr=3647050278
24 20.078804 192.168.0.10 192.168.0.11 TCP 54 8080 → 41996 [RST] Seq=2923 Win=0 Len=0
25 21.799650 192.168.0.11 192.168.0.10 TCP 74 36134 → 8080 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2709175540 TSecr=0 WS=512
26 21.799669 192.168.0.10 192.168.0.11 TCP 74 8080 → 36134 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=3647060156 TSecr=2709175
27 21.799684 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=1 Ack=1 Win=32256 Len=0 TSval=2709175540 TSecr=3647060156
28 21.799963 192.168.0.11 192.168.0.10 TCP 298 36134 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=32256 Len=232 TSval=2709175540 TSecr=3647060156
29 21.799971 192.168.0.10 192.168.0.11 TCP 66 8080 → 36134 [ACK] Seq=1 Ack=233 Win=32256 Len=0 TSval=3647060156 TSecr=2709175540
30 21.810528 192.168.0.10 192.168.0.11 TCP 2263 8080 → 36134 [PSH, ACK] Seq=1 Ack=233 Win=32256 Len=2197 TSval=3647060167 TSecr=2709175540
31 21.810555 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=233 Ack=2198 Win=32256 Len=0 TSval=2709175551 TSecr=3647060167
32 21.811466 192.168.0.11 192.168.0.10 TCP 146 36134 → 8080 [PSH, ACK] Seq=233 Ack=2198 Win=32256 Len=80 TSval=2709175552 TSecr=3647060167
33 21.811638 192.168.0.10 192.168.0.11 TCP 321 8080 → 36134 [PSH, ACK] Seq=2198 Ack=313 Win=32256 Len=255 TSval=3647060168 TSecr=2709175552
34 21.852327 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=313 Ack=2453 Win=32256 Len=0 TSval=2709175593 TSecr=3647060168
35 21.852336 192.168.0.10 192.168.0.11 TCP 321 8080 → 36134 [PSH, ACK] Seq=2453 Ack=313 Win=32256 Len=255 TSval=3647060209 TSecr=2709175593
36 21.852353 192.168.0.11 192.168.0.10 TCP 66 36134 → 8080 [ACK] Seq=313 Ack=2708 Win=32256 Len=0 TSval=2709175593 TSecr=3647060209
37 25.714512 192.168.0.11 192.168.0.10 TCP 101 36134 → 8080 [PSH, ACK] Seq=313 Ack=2708 Win=32256 Len=35 TSval=2709179455 TSecr=3647060209
Frame 2: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Nov 15, 2024 22:04:26.872153000 CST
UTC Arrival Time: Nov 16, 2024 04:04:26.872153000 UTC
0000 22 78 e4 e8 6e f9 2e 94 92 01 84 06 08 00 45 00 "x··n·.· ·····E·
0010 00 3c 00 00 40 00 40 06 b9 56 c0 a8 00 0a c0 a8 ·<··@·@· ·V····
0020 00 0b 1f 90 a4 0c 5e 10 95 4a 49 29 b7 dd a0 12 ·····^· ·JI)····
0030 7c 70 81 94 00 00 02 04 05 b4 04 02 08 0a d9 61 |p····· ·····a
0040 63 94 a1 7a 67 cc 01 03 03 09 c··zg··· ··
tls.pcap
Packets: 63
Profile: Default

Without TLS


Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
1 0.000000 192.168.0.11 192.168.0.10 TCP 74 54142 → 8080 [SYN] Seq=0 Win=32120 Len=0 MSS=1460 SACK_PERM TSval=2709366948 TSecr=0 WS=512
2 0.000021 192.168.0.10 192.168.0.11 TCP 74 8080 → 54142 [SYN, ACK] Seq=0 Ack=1 Win=31856 Len=0 MSS=1460 SACK_PERM TSval=3647251564 TSecr=27093669…
3 0.000037 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [ACK] Seq=1 Ack=1 Win=32256 Len=0 TSval=2709366948 TSecr=3647251564
4 3.854067 192.168.0.11 192.168.0.10 TCP 78 54142 → 8080 [PSH, ACK] Seq=1 Ack=1 Win=32256 Len=12 TSval=2709370802 TSecr=3647251564 [TCP PDU reasse…
5 3.854082 192.168.0.10 192.168.0.11 TCP 66 8080 → 54142 [ACK] Seq=1 Ack=13 Win=32256 Len=0 TSval=3647255418 TSecr=2709370802
6 3.854678 192.168.0.10 192.168.0.11 TCP 93 8080 → 54142 [PSH, ACK] Seq=1 Ack=13 Win=32256 Len=27 TSval=3647255419 TSecr=2709370802 [TCP PDU reass…
7 3.854705 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [ACK] Seq=13 Ack=28 Win=32256 Len=0 TSval=2709370803 TSecr=3647255419
8 5.396256 192.168.0.11 192.168.0.10 TCP 70 54142 → 8080 [PSH, ACK] Seq=13 Ack=28 Win=32256 Len=4 TSval=2709372344 TSecr=3647255419 [TCP PDU reass…
9 5.396445 192.168.0.10 192.168.0.11 TCP 240 8080 → 54142 [PSH, ACK] Seq=28 Ack=17 Win=32256 Len=174 TSval=3647256960 TSecr=2709372344 [TCP PDU rea…
10 5.396471 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [ACK] Seq=17 Ack=202 Win=32256 Len=0 TSval=2709372344 TSecr=3647256960
11 10.993181 192.168.0.11 192.168.0.10 TCP 72 54142 → 8080 [PSH, ACK] Seq=17 Ack=202 Win=32256 Len=6 TSval=2709377941 TSecr=3647256960 [TCP PDU reas…
12 10.993402 192.168.0.10 192.168.0.11 TCP 93 8080 → 54142 [PSH, ACK] Seq=202 Ack=23 Win=32256 Len=27 TSval=3647262557 TSecr=2709377941 [TCP PDU rea…
13 10.993434 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [ACK] Seq=23 Ack=229 Win=32256 Len=0 TSval=2709377941 TSecr=3647262557
14 13.943720 192.168.0.11 192.168.0.10 TCP 75 54142 → 8080 [PSH, ACK] Seq=23 Ack=229 Win=32256 Len=9 TSval=2709380892 TSecr=3647262557 [TCP PDU reas…
15 13.944159 192.168.0.10 192.168.0.11 TCP 185 8080 → 54142 [PSH, ACK] Seq=229 Ack=32 Win=32256 Len=119 TSval=3647265508 TSecr=2709380892
16 13.944196 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [ACK] Seq=32 Ack=348 Win=32256 Len=0 TSval=2709380892 TSecr=3647265508
17 21.286900 192.168.0.11 192.168.0.10 TCP 75 54142 → 8080 [PSH, ACK] Seq=32 Ack=348 Win=32256 Len=9 TSval=2709388235 TSecr=3647265508 [TCP PDU reas…
18 21.287308 192.168.0.10 192.168.0.11 TCP 184 8080 → 54142 [PSH, ACK] Seq=348 Ack=41 Win=32256 Len=118 TSval=3647272851 TSecr=2709388235
19 21.287349 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [ACK] Seq=41 Ack=466 Win=32256 Len=0 TSval=2709388235 TSecr=3647272851
20 23.465543 192.168.0.11 192.168.0.10 TCP 69 54142 → 8080 [PSH, ACK] Seq=41 Ack=466 Win=32256 Len=3 TSval=2709390413 TSecr=3647272851 [TCP PDU reas…
21 23.465775 192.168.0.10 192.168.0.11 TCP 73 8080 → 54142 [PSH, ACK] Seq=466 Ack=44 Win=32256 Len=7 TSval=3647275030 TSecr=2709390413
22 23.465812 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [ACK] Seq=44 Ack=473 Win=32256 Len=0 TSval=2709390414 TSecr=3647275030
23 23.465831 192.168.0.10 192.168.0.11 TCP 66 8080 → 54142 [FIN, ACK] Seq=473 Ack=44 Win=32256 Len=0 TSval=3647275030 TSecr=2709390414
24 23.506655 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [ACK] Seq=44 Ack=474 Win=32256 Len=0 TSval=2709390455 TSecr=3647275030
25 24.421287 192.168.0.11 192.168.0.10 TCP 66 54142 → 8080 [FIN, ACK] Seq=44 Ack=474 Win=32256 Len=0 TSval=2709391369 TSecr=3647275030
26 24.421310 192.168.0.10 192.168.0.11 TCP 66 8080 → 54142 [ACK] Seq=474 Ack=45 Win=32256 Len=0 TSval=3647275985 TSecr=2709391369
Frame 4: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
Encapsulation type: Ethernet (1)
Arrival Time: Nov 15, 2024 22:08:03.933845000 CST
UTC Arrival Time: Nov 16, 2024 04:08:03.933845000 UTC
Epoch Arrival Time: 1731730083.933845000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 3.854030000 seconds]
[Time delta from previous displayed frame: 3.854030000 seconds]
[Time since reference or first frame: 3.854067000 seconds]
Frame Number: 4
0000 2e 94 92 01 84 06 22 78 e4 e8 6e f9 08 00 45 00 ·····"x ··n···E·
0010 00 40 c2 f5 40 00 40 06 f6 5c c0 a8 00 0b c0 a8 ·@··@·@· ·\····
0020 00 0a d3 7e 1f 90 ba c8 6f 3f 9d 7c 05 c6 80 18 ···~···· o?·|····
0030 00 3f 81 98 00 00 01 01 08 0a a1 7d b7 b2 d9 64 ·?····· ···}···d
0040 a4 6c 48 45 4c 4f 20 73 6c 65 63 68 2d 30 ·lHELO s lech-0
non_tls.pcap
Packets: 26
Profile: Default



Secure communication within the system is achieved through multiple layers of encryption and authentication mechanisms. Data transmitted between the client and server is encrypted using the AES-256-CBC cipher, ensuring that even if intercepted, the data remains unintelligible without the proper decryption key. User passwords are hashed using the SHA-512 algorithm combined with unique salts before being stored, which adds an additional layer of security, making it computationally infeasible to reverse-engineer the original passwords from their hashes.
To facilitate safe transmission of sensitive data, such as encrypted passwords, base64 encoding is employed. This encoding ensures that binary data is safely transmitted over protocols that may not handle binary data gracefully. Moreover, the client verifies the server's SSL certificate against a trusted certificate authority to authenticate the server and prevent man-in-the-middle attacks. The .book_shadow file, which stores user credentials, is secured with file permissions set to owner read/write only preventing unauthorized access and ensuring that sensitive information remains protected.

Summary

Throughout the project, several key milestones were successfully achieved. A secure client-server communication channel was established using SSL/TLS protocols, ensuring that all data transmitted between the client and server is encrypted and secure. A robust user authentication mechanism was implemented, incorporating hashed and salted passwords to enhance the security of user credentials with base64 encoding is employed. The development of an interactive text-based user interface using ncurses provided a user-friendly platform for seamless interactions and navigation through various operational modes. The server was also equipped to handle

multiple concurrent client connections efficiently using process forking and signal handling, ensuring scalability and performance.

Conclusion

This project provided a comprehensive exploration into secure network programming and cybersecurity practices. By developing a secure book management system, I gained valuable insights into implementing encryption protocols, managing user authentication securely, and designing user-friendly interfaces. The successful establishment of encrypted communication channels and robust authentication mechanisms demonstrated the practical application of theoretical cybersecurity concepts.