Objective

The primary objective was to secure the file transfer process using TLS, ensuring that the data exchanged between the client and server is encrypted and protected from potential eavesdropping or interception.

Methodology

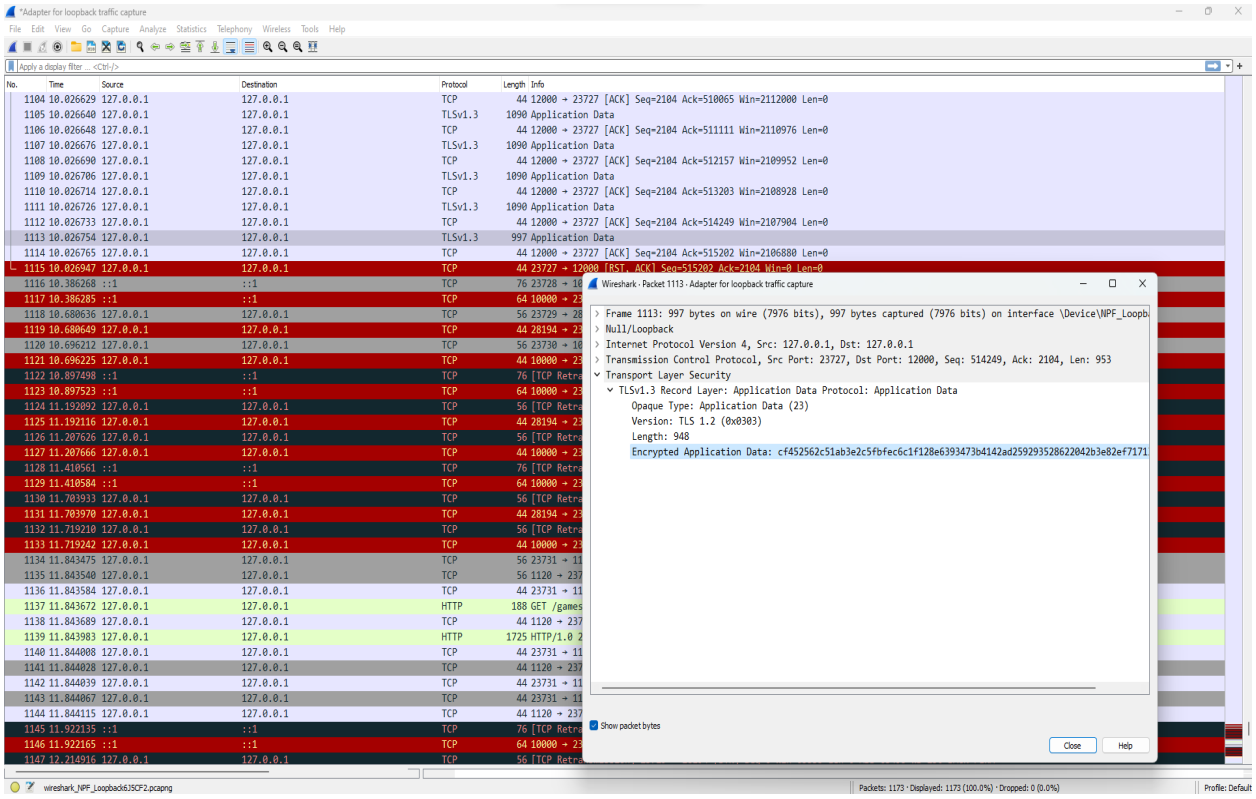
The application was tested by running the TLS-enabled server and client scripts, with the client sending files to the server. Wireshark, a network protocol analyzer, was used to capture and analyze the network traffic during this file transfer process.

Wireshark Capture Analysis

- **Capture Details**: The Wireshark capture revealed TLSv1.3 traffic between the localhost IP (`127.0.0.1`), confirming that the communication was restricted to the local machine, as expected in a testing environment.

- **TLS Encryption Verification**: The capture line `1113 10.026754 127.0.0.1 127.0.0.1 TLSv1.3 997 Application Data` is significant. It indicates that the data being transferred was encapsulated within TLSv1.3 protocol, signifying encrypted communication. The fact that the data content is not visible in the capture (as opposed to plaintext transmission) further supports that the TLS encryption was active and functioning as intended.

- **TCP Protocol Mechanics**: Additional lines in the capture, such as TCP acknowledgments (`ACK`), are part of the standard TCP communication protocol, showcasing the underlying transport mechanism over which TLS operates.



Role of Digital Certificates

- Identity Verification: Certificates serve as a means of verifying the identity of entities in a network, similar to a digital ID. In the context of our TLS application, the certificate helps the client to verify the server's identity.
- Public Key Distribution: Certificates contain the public key of the entity, allowing others to encrypt messages that only the private key holder can decrypt.

Conclusion

The analysis of the Wireshark capture provides strong evidence that the file transfer application successfully implemented TLS for secure communication. The presence of TLSv1.3 Application Data entries in the network traffic capture confirms that the data being transferred between the client and server was encrypted, fulfilling the core objective of enhancing the application's security.

This implementation and its verification via Wireshark highlight the effectiveness of TLS in securing data transfer in network applications, an essential aspect in the field of network security and data privacy.