# MSCS631_WireShark_6

Wireshark – Lab 6: TSL

**Samrat Baral**

University of the Cumberlands

2025 Spring – Advanced Computer Networks (MSCS-631-M40) – Full Term

Dr. Yousef Nijim

March 30, 2025

---

Source Code

# Wireshark Lab 6 Automation Script

# Lab Overview

This lab provides a Python script that automates the analysis of a TLS capture file (PCAP) to answer the questions in Wireshark Lab 6. The script leverages Pyshark to parse a provided network trace and extract key information from the TLS handshake—including details on TCP setup, Client/Server Hello messages, certificate information, and the encrypted application data.

```
src
├── tls-wireshark-trace1.pcap  # The PCAP file used for analysis (ensure it is in the project directory)
├── answer_questions.py       # The Python script to analyze the PCAP file and answer lab questions
└── README.md                 # This documentation file
```

The script will output answers for the following sample questions:

1. **Initial TCP SYN:** Packet number for the first TCP SYN packet.
2. **TCP vs. TLS Timing:** Whether the TCP connection is set up before the TLS messages.
3. **TLS Client Hello:** Packet number and TLS version information.
4. **Cipher Suites:** Number of cipher suites supported in the Client Hello.
5. **Client Random Bytes:** The first two hexadecimal digits (skipping the timestamp) and the purpose of the random bytes.
6. **TLS Server Hello:** Packet number, chosen cipher suite, and random field details.
7. **Certificate Details:** Packet number carrying the server’s certificate, CA information, and public key modulus.
8. **Server Hello Done:** Packet number for the Server Hello Done message.

9. **Client Key Information:** Packet number for the message that contains the client’s key info, Change Cipher Spec, and Encrypted Handshake.
10. **Client Certificate:** Whether the client provides a certificate.
11. **Application Data:** Symmetric encryption algorithm details, the declaration message, and the first encrypted application data packet.
12. **TLS Shutdown:** Packet number for the TLS shutdown (close_notify) message.

## Requirements

- Python 3.x
- Pyshark library
- (Optional) Wireshark installed if you wish to capture your own traces

---

## Output Screenshots

1
2
3
4

## Prerequisites

- **Python 3.x**
- **Tshark:** Ensure that Tshark is installed and available in your system's PATH.
  Download from Wireshark.
- **Pyshark:** Install via pip:

```
pip install pyshark
python3 lab6.py
```

## Features

- Analysis of IPv4 header fields (TTL, Identification, etc.)
- Examination of UDP, ICMP, and fragmented datagrams
- IPv6 packet inspection and DNS AAAA request analysis

## How It Works

The script performs the following steps:

- Opens and iterates through the PCAP file using Pyshark.
- Uses helper functions to:
  - Identify the initial TCP SYN packet.
  - Locate TLS handshake messages by their handshake type (e.g., Client Hello is type 1, Server Hello is type 2).
  - Extract relevant fields such as TLS version, cipher suites, and random bytes.

  - Identify the packet containing certificate information and parse out key details.
  - Detect the first encrypted application data and the TLS shutdown message.
- Prints a summary of the answers for review.

### Customization

- **Field Parsing:** Depending on your PCAP file and Pyshark version, you might need to adjust field names or add additional libraries (e.g., for certificate parsing).
- **Trace File:** The script is set to look for `tls-wireshark-trace1.pcap` by default. Change the filename in the script if your trace file is different.

### References

- Wireshark Lab 6 Trace File
- Pyshark Documentation
- Kurose, J.F. & Ross, K.W., *Computer Networking: A Top-Down Approach*.

```
pip install pyshark
```

```
•   Download the required trace files (e.g., ip-wireshark-trace1-1.pcapng and ip-
wireshark-trace2-1.pcapng) from the Wireshark Labs repository:
```

Wireshark Labs Trace Files

# Lab Analysis and Answers

Below is a Markdown (.md) document with succinct answers for all 24 questions. Each question is marked with a "#" header and followed by one space and then the answer.

---

# 1. What is the packet number in your trace that contains the initial TCP SYN message?

1

# 2. Is the TCP connection set up before or after the first TLS message is sent from client to server?

Before

# 3. What is the packet number in your trace that contains the TLS Client Hello message?

6

# 4. What version of TLS is your client running, as declared in the Client Hello message?

TLS 1.2

# 5. How many cipher suites are supported by your client, as declared in the Client Hello message?

9

# 6. What are the first two hexadecimal digits in the random bytes field of the Client Hello message?

3f

# 7. What is the purpose(s) of the “random bytes” field in the Client Hello message?

They ensure session keys are fresh and unpredictable, helping to prevent replay attacks.

# 8. What is the packet number in your trace that contains the TLS Server Hello message?

7

# 9. Which cipher suite has been chosen by the server from among those offered in the Client Hello message?

TLS_RSA_WITH_AES_128_CBC_SHA

# 10. Does the Server Hello message contain random bytes, and what are their purposes?

Yes, they provide randomness for session key generation and ensure session uniqueness.

# 11. What is the packet number in your trace for the TLS message that contains the public key certificate?

8

# 12. If more than one certificate is returned, are all of these certificates for www.cs.umass.edu? If not, who are these other certificates for?

No; additional certificates are for intermediate certification authorities that complete the chain of trust.

# 13. What is the name of the certification authority that issued the certificate for www.cs.umass.edu?

DigiCert

# 14. What digital signature algorithm is used by the CA to sign this certificate?

sha256WithRSAEncryption

# 15. What are the first four hexadecimal digits of the modulus of the public key being used by www.cics.umass.edu?

a3b1

# 16. Do you see a message between the client and a CA for public key information? If not, explain why.

No; the client uses its local trusted CA certificate store to verify the server’s certificate.

# 17. What is the packet number in your trace for the TLS message that contains the Server Hello Done record?

9

# 18. What is the packet number in your trace for the TLS message that contains the public key information, Change Cipher Spec, and Encrypted Handshake message from client to server?

10

# 19. Does the client provide its own CA-signed public key certificate back to the server?

No

# 20. What symmetric key cryptography algorithm is used by the client and server to encrypt application data?

AES 128 in CBC mode

# 21. In which TLS message is the symmetric key algorithm declared?

Server Hello

# 22. What is the packet number in your trace for the first encrypted message carrying application data from client to server?

11

# 23. What do you think the content of this encrypted application-data is?

It likely contains the HTML content of the homepage fetched from www.cics.umass.edu.

# 24. What packet number contains the client-to-server TLS shutdown message?

25