Application Layer Security Lab

CYBR3010

Cybersecurity Foundations

Arr Domingo

Student ID: 200458099

November 30, 2025

Instructor: Sam El-Awour

Table of Contents

1 Introduction

This document is about the security of application layer, specifically the configuration of SSL (Secure Socket Layer) inspection, also known as TLS (Transport Layer Security) interception. This is a feature in the next-generation firewall that allows the firewall to intercept the SSL/TLS encrypted internet communication, such as HTTPS, between client and server. The interception would allow the FortiGate firewall to examine and manage the traffic in the network by acting as a "man in the middle", decrypting the traffic, inspecting it using security profiles, and then re-encrypting it before forwarding the traffic. Moreover, this document will show the process of injecting SSL certificate in Windows client virtual machine, as well as decrypting SSL/TLS traffic in Wireshark.

2 Network Diagram

This is a detailed network setup with a focus on one windows client virtual machine (VM 2), virtual switch, and a virtual firewall. The windows client virtual machine (VM 2) is configured to have SSL/TLS certificate, and the virtual FortiGate firewall is configured to implement SSL/TLS inspection and manage/examine SSL/TLS traffic in the network.

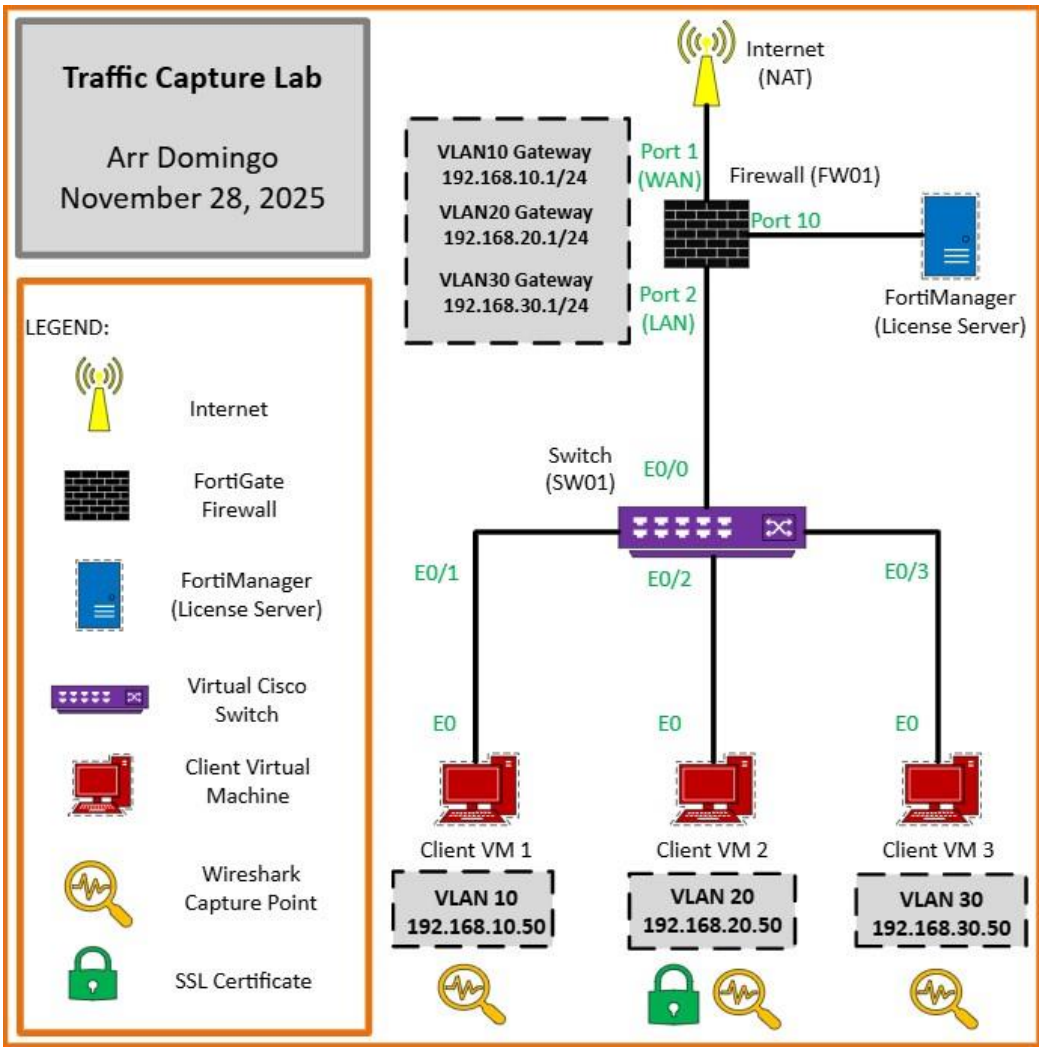

Figure 1. Network diagram of Application Layer Security.

3 Implementation of SSL inspection in the firewall

In simple terms, SSL Inspection or TLS Interception is a man-in-the-middle executed to filter out malicious content. This interceptor sits in between the client and server, inspecting all the traffic passing through it, and finally deciding whether the traffic/content is allowed or not.

3.1 Before implementing SSL inspection for Windows client VM2

- Open the browser and search something on the internet (yahoo.com, etc).
- Click on the lock icon to see what SSL certificates being signed.
- Click “Connection secure” then click “More information”. In here, it will show the security feature that is verified by DigiCert Inc, which means website is trusted.

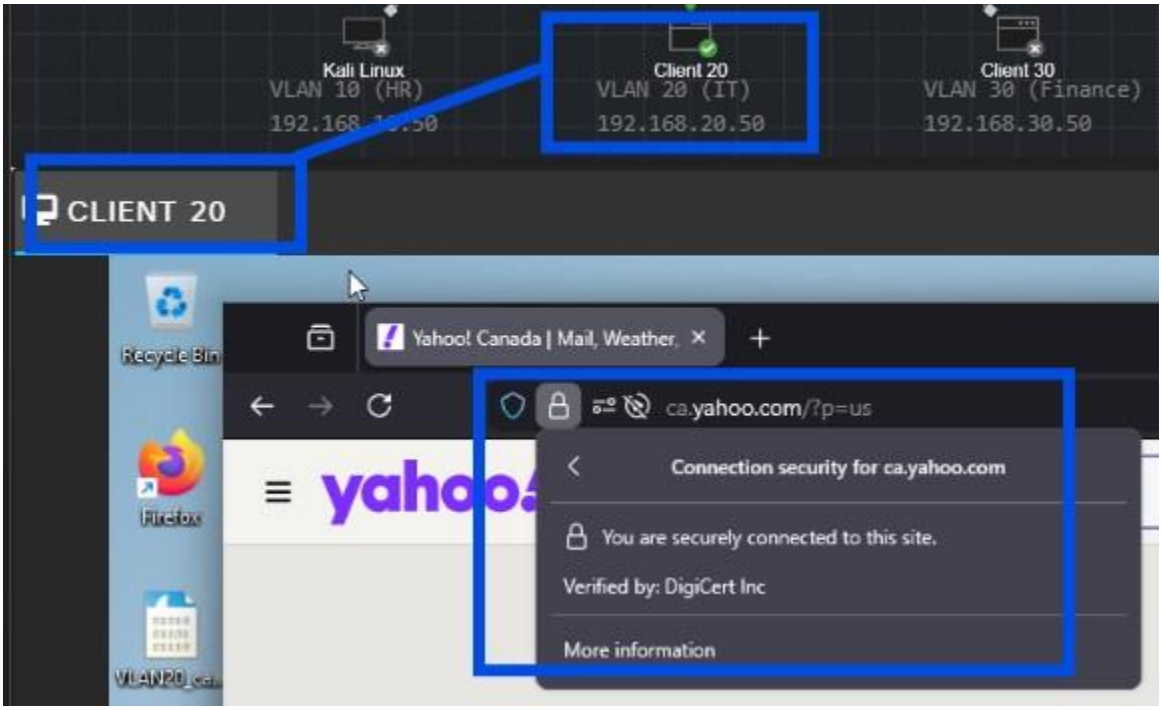

Figure 2. DigiCert Inc is digital certificates that secure websites and online transactions, manage identities for devices, and enable secure document signing.

- To check valid trusted certificate issuer in Windows, click Windows logo and search “Manage user certificates”.

- Click “Trusted Root Certification Authorities” and click "Certificates”. This will show lists of all the certificate issuer trusted by Windows which means browser would accept this certificate and make the connection secure.

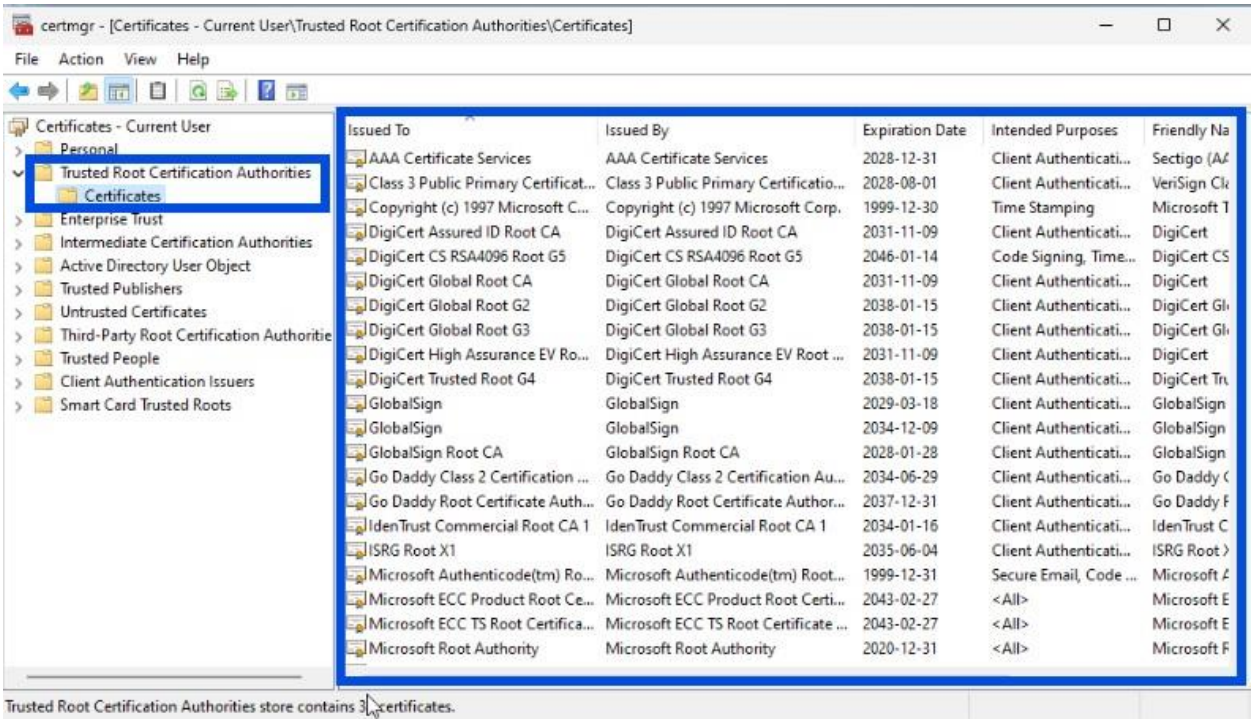

Figure 3. Certificate issuer trusted by Windows.

- At this point, the FortiGate firewall has no visibility in the traffic.

3.2 Set up SSL inspection in the firewall for VM2

- In CML, start the firewall (FW01) as well as all other devices.
- Right click the firewall (FW01) and choose “Console”. You know firewall is done booting when you are able to see the serial number and the firewall login.
- Type “cisco” in the “Firewall login” and “Password”.
- Wait until you see “Welcome”.

- Type “get system interface physical port1” to get information about port 1 that is connected to the internet. Open the IP address in another browser.
- On the browser, click “Advanced”.
- Click “Proceed to 192.168.202.146(unsafe)”.
- Type “cisco” as the Username and Password, then click “Login”.
- Click "Login Read-Write".
- Click "Yes".
- Click "Begin".
- In the Dashboard Setup, choose the default which is "Optimal" and press "OK".
- Firewall (FW01) dashboard will open up.
- In the FortiGate firewall (FW01) dashboard, click “Policy & Objects”.
- Click “Firewall Policy”.
- Base from the previous configuration, click “Edit” to the policy related to VM 2 which is “IT(VLAN20)”.
- Enable “AntiVirus” and on “SSL inspection”, choose “deep-inspection”.

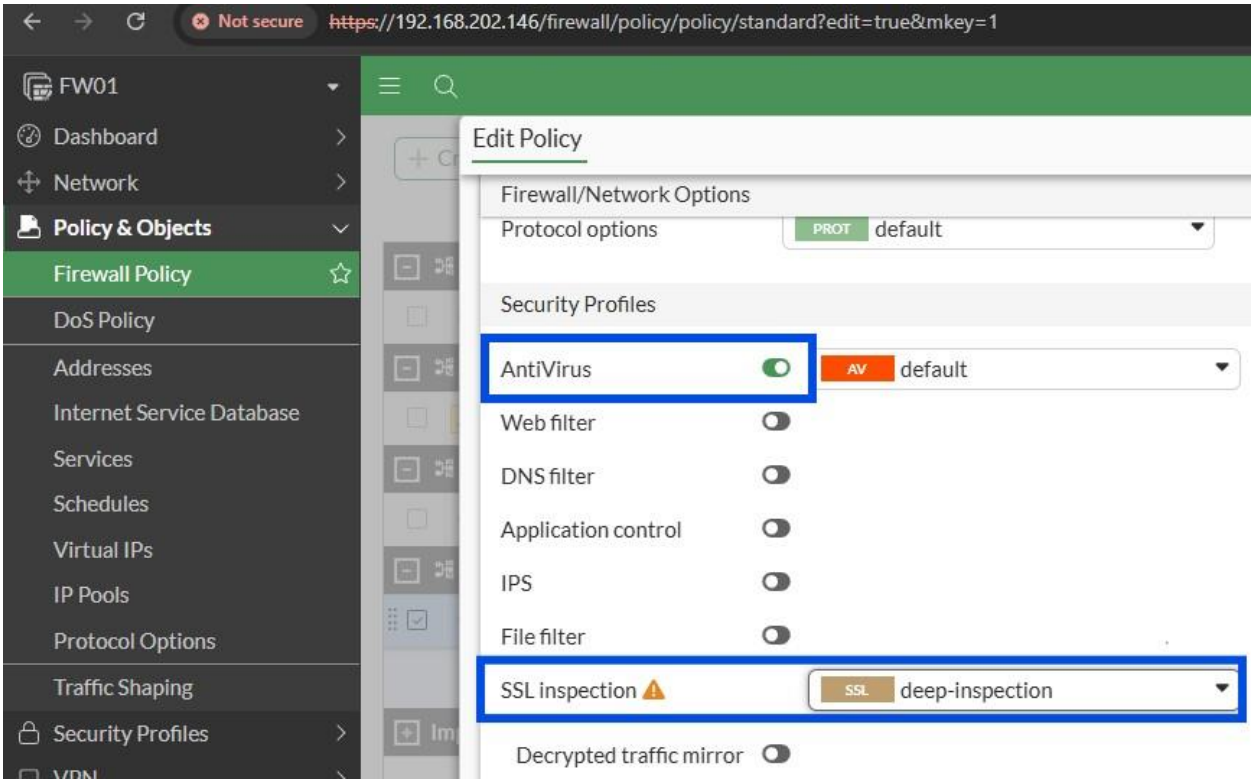

Figure 4. Enable antivirus and set SSL inspection to deep-inspection.

- Click OK.
- Confirmation will appear which means end users will see certificate warnings. Hit OK.

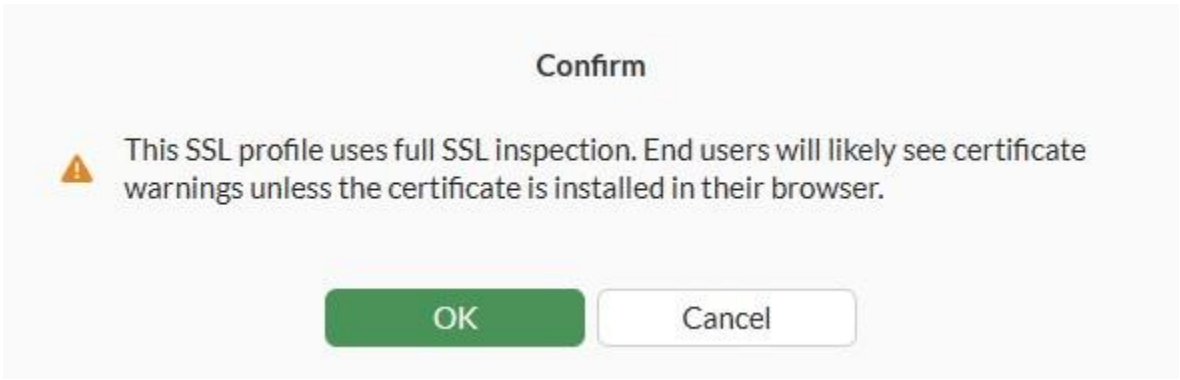

Figure 5. Confirmation message after SSL configuration.

3.3. After implementing SSL inspection for Windows client VM2

- Go back to the CML and close the previous browser. Open new browser.
- Go to yahoo.com. Warning will appear.

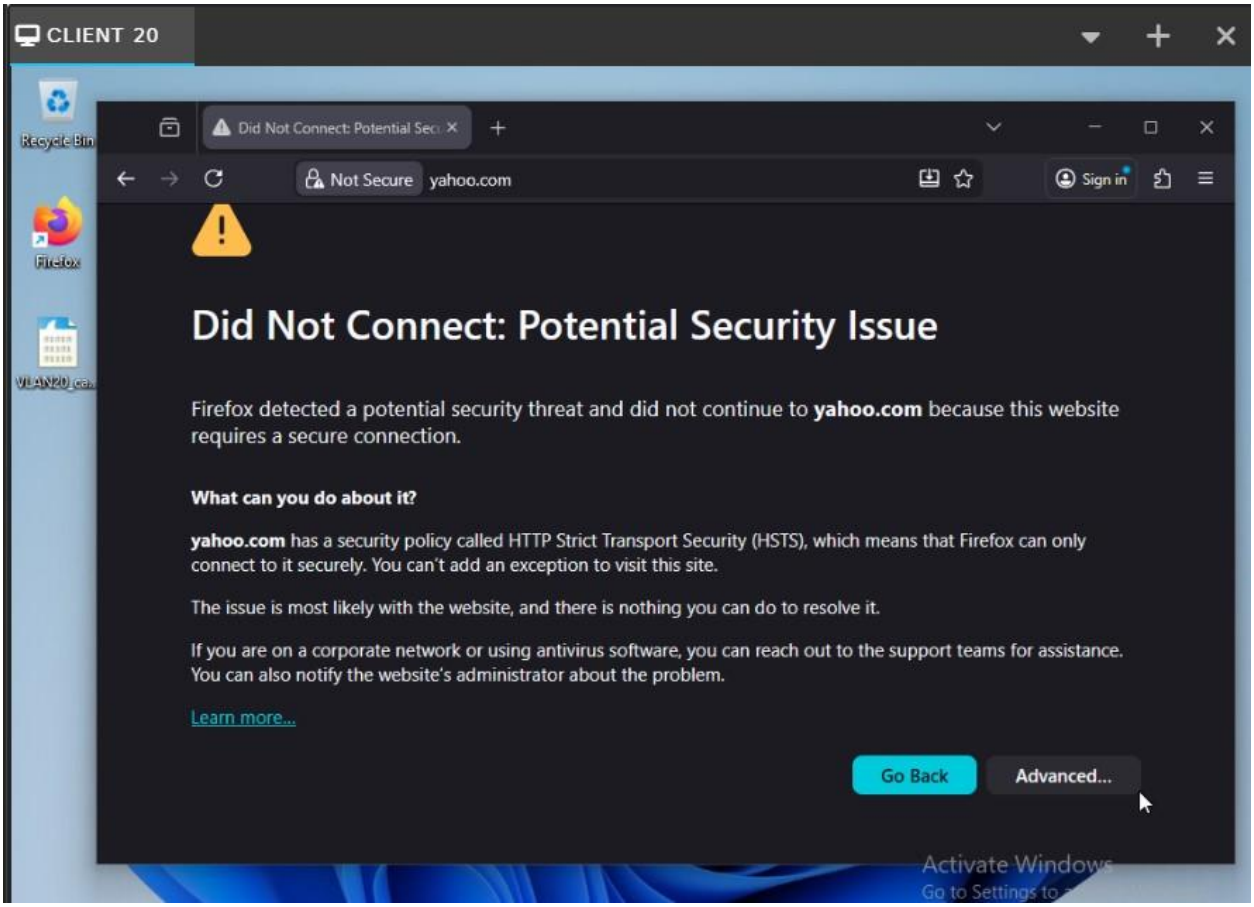

Figure 6. Warning message after the implementation of SSL inspection in FortiGate firewall. This means that browser does not trust the security certificate presented by FortiGate. To fix this, the FortiGate's CA (Certificate Authority) must be injected in VM 2 windows client and add to their trusted root certificate authorities store.

4 Injection of SSL Certificate to the client (VM2)

SSL certificate is a digital certificate that authenticates a website's identity and enables an encrypted connection. The purpose of using SSL certificate is to establish a secure and encrypted connection between a web server and a browser. It uses encryption algorithms to scramble data in transit, which prevents hackers from reading it as it is sent over the connection.

4.1 Before the injection of SSL certificate to Windows client (VM2)

- Every time you search a website in a browser, there will always be a warning message.

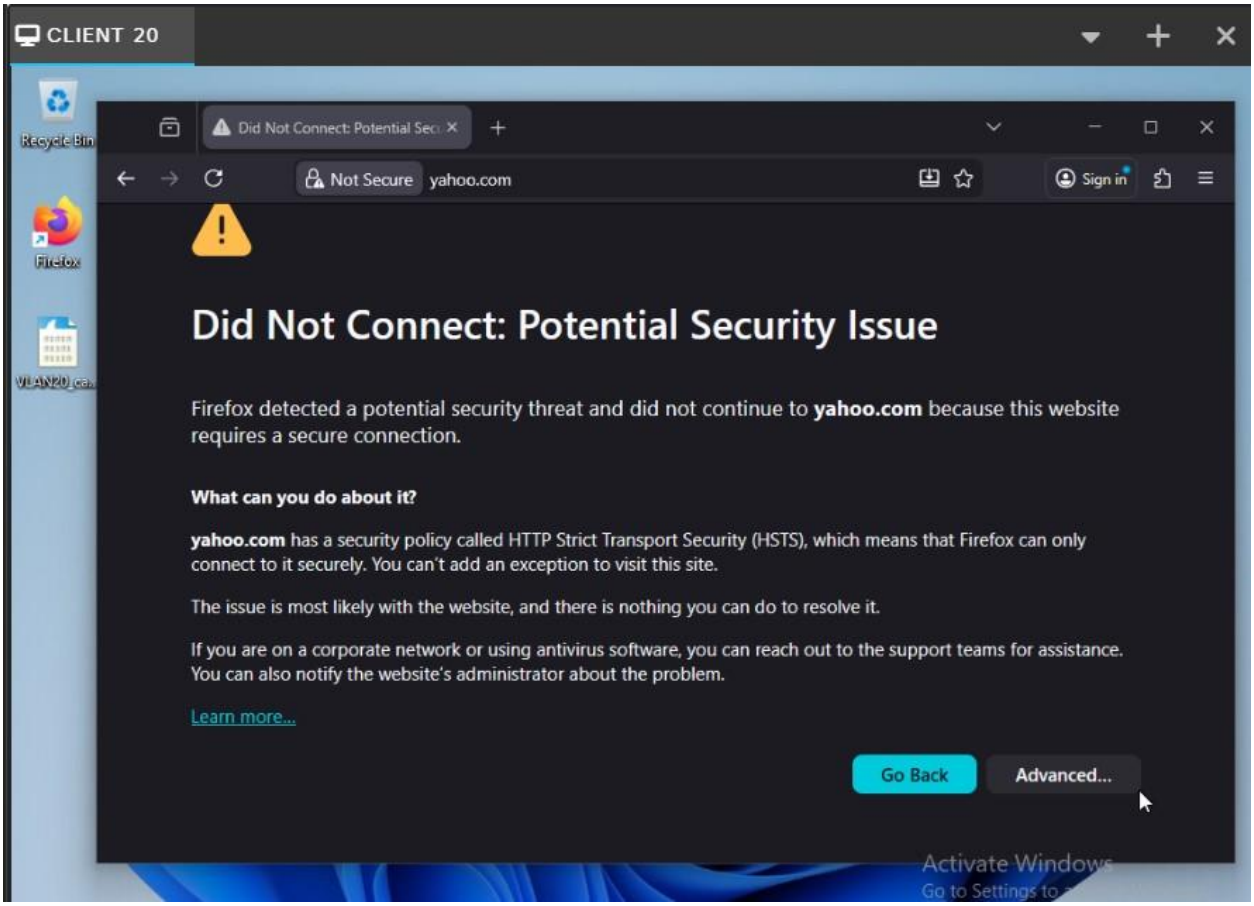

Figure 7. Warning message before the injection of SSL certificate.

- To eliminate this warning message, take the SSL certificate from the firewall and inject it into the trusted certificate in VM 2 Windows client virtual machine.

4.2 Process to inject SSL certificate to Windows client (VM2)

- First is to download the certificate from the firewall. To download the certificate, go to CMD and run “ipconfig” command to check “Default Gateway”.
- Paste the default gateway which is 192.168.20.1 in browser tab. Notice that it doesn’t go through.
- To resolve this, go to FortiGate firewall, click “Network” and click “Interfaces”.
- Click the + sign beside “LAN (port2)” and double-click the VLAN20.
- Under “Administrative Access”, check the “HTTPS”.

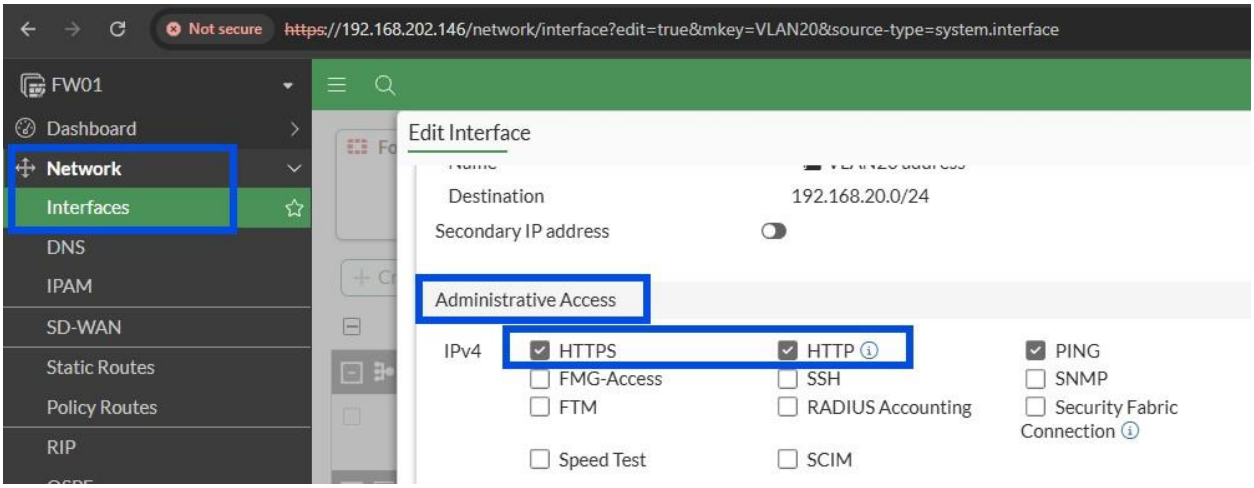

Figure 8. Allow HTTPS and HTTP in VLAN20.

- Click OK.
- By now, you can open FortiGate firewall with the self-signed certificate in the browser of VLAN20.

- Go to “Security Profiles”, click “SSL/SSH Inspection”, then double-click “SSL deep-inspection”.

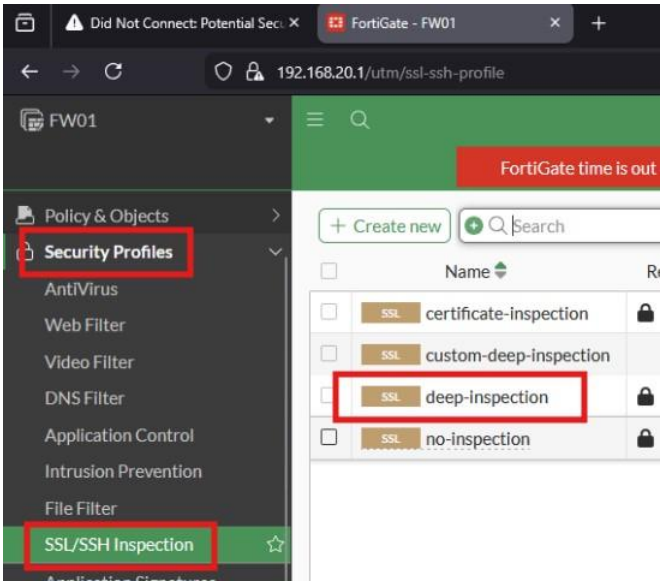

Figure 9. Process to check SSL deep-inspection details.

- Where you see “CA certificate”, this will tell you the firewall certificate which is “Fortinet_CA_SSL”. Click “Download”. (Note that in real world, firewall certificate will normally be downloaded within a certificate server like windows domain controller.)

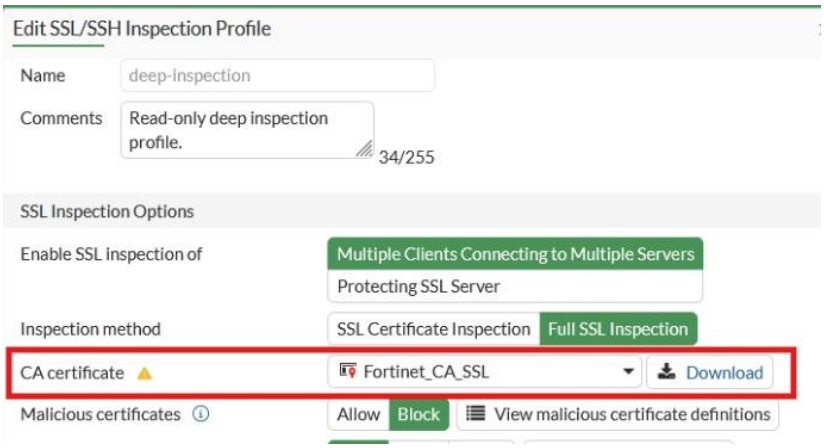

Figure 10. Downloading SSL certificate in FortiGate firewall.

- Open the downloaded SSL certificate.
- Click “Install Certificate”.
- Choose “Local Machine” then click “Next”.
- Choose “Place all certificates in the following store”, then click browse and choose “Trusted Root Certification Authorities”. Finally, click OK.
- Click Next.
- Click Finish. Successful message will pop-up.

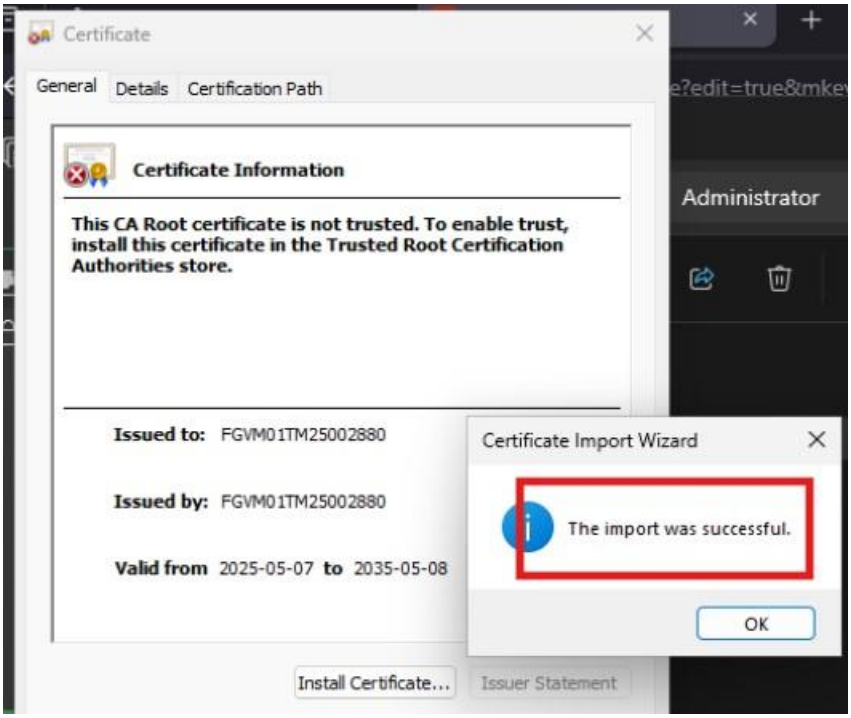

Figure 11. Successful installation of SSL certificate.

- Click OK.

4.3 After the injection of SSL certificate to Windows client (VM2)

- To verify, open the browser once again and search yahoo.com. By this time, you can now access the website with no certificate warning. This means that connection is now trusted.

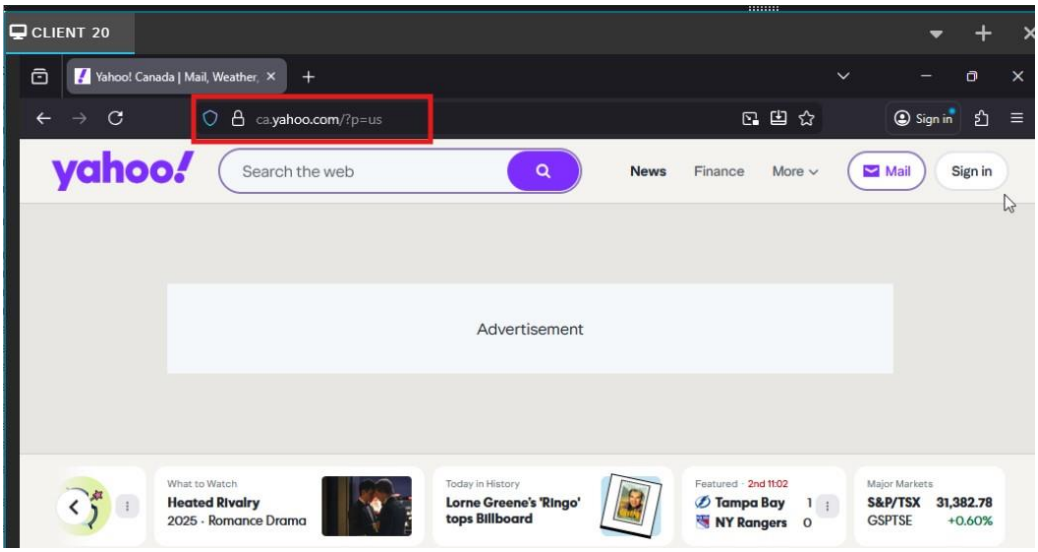

Figure 12. No more warning message.

5 Wireshark capture for decrypting SSL/TLS traffic

SSL/TLS decryption is the process of intercepting and decrypting encrypted internet traffic to inspect its contents for security threats like malware or phishing attacks. It involves using methods like a private key to unscramble the data, making it visible to security tools so they can identify and block malicious activity that might be hidden within encrypted sessions.

To decrypt SSL traffic in Wireshark, you need a key log file, which contains the session keys, generated by a client application during a capture. The process involves setting an

environment variable to generate the log file, capturing the traffic, and then configuring Wireshark to use that log file and provide the path to the log file.

5.1 Create key log file

- Generate the key log file by typing “environment” in Windows search bar.
- Click the “Edit the system environment variables”.
- “System Properties” window will appear. Click “Environment Variables” button.

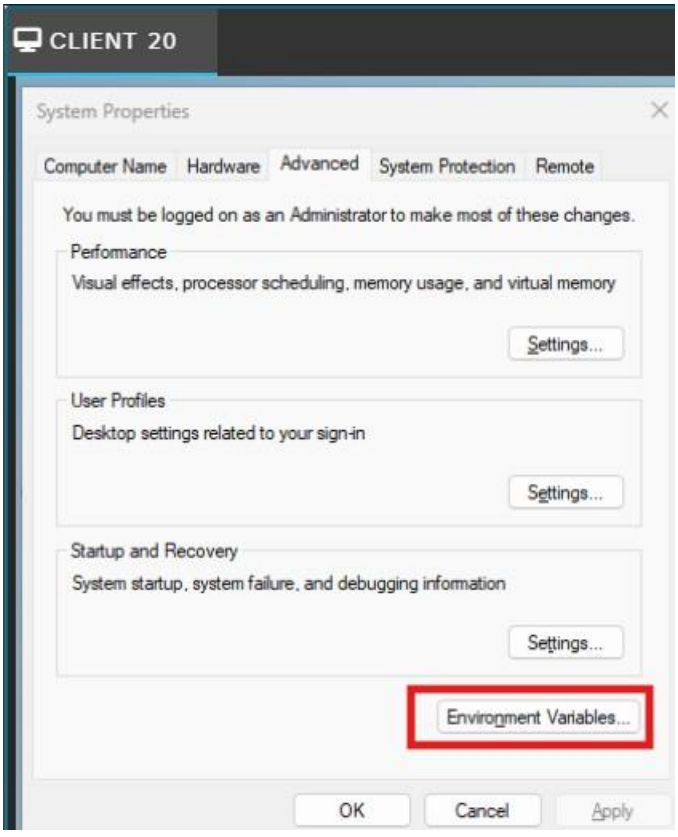

Figure 13. Navigating environment variables.

- Click “New” under “User variables for Administrator”.

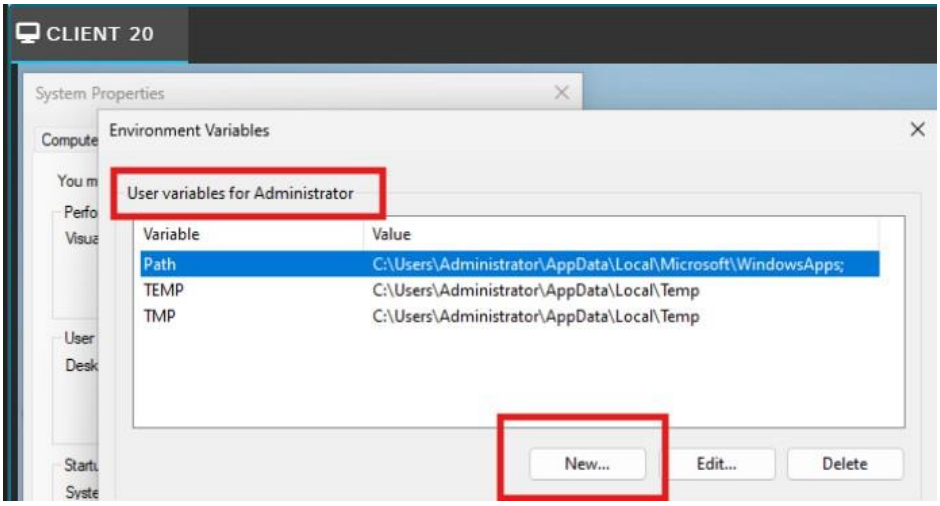

Figure 14. Adding new environment variables.

- Set "Variable name" to “SSLKEYLOGFILE”.
- Set "Variable value" to the absolute path where you want the key log file to be saved (C:\Users\Administrator\Desktop\sslkeylog.log). Note that variable will automatically log the session keys for all subsequent traffic.
- Click "OK" on all open dialogs.
- SSLKEYLOGFILE variable is now created.

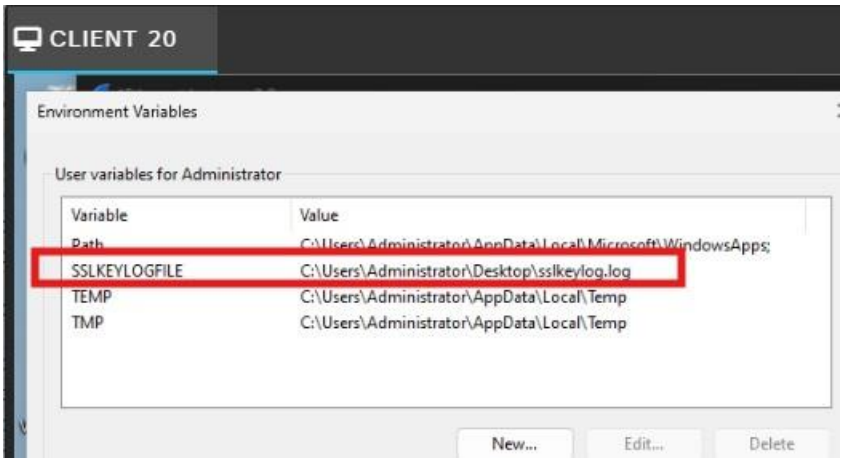

Figure 15. SSLKEYLOGFILE variable.

- Open Wireshark and start a new capture on the appropriate interface.
- Open the browser and search multiple websites or services you want to capture. The keys will be logged in the specified file.
- Stop the capture in Wireshark when done loading the website.

5.2 Before decrypting SSL/TLS traffic

- Analyze the traffic in Wireshark. Up to you if you want to use the filter function but the idea is to look for packet with info from client ("Client Hello").
- Right-click on the packet with info "Client Hello", go to "Follow", and click "TLS Stream".

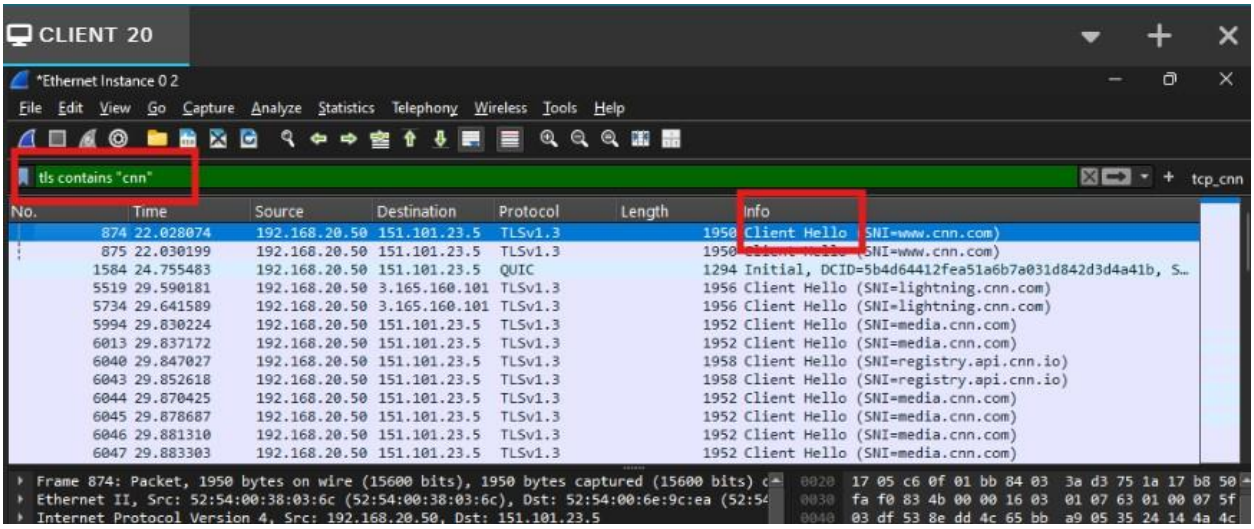

Figure 16. Start of analyzing Wireshark traffic.

- Below are the screenshots of SSL/TLS packets and their details.

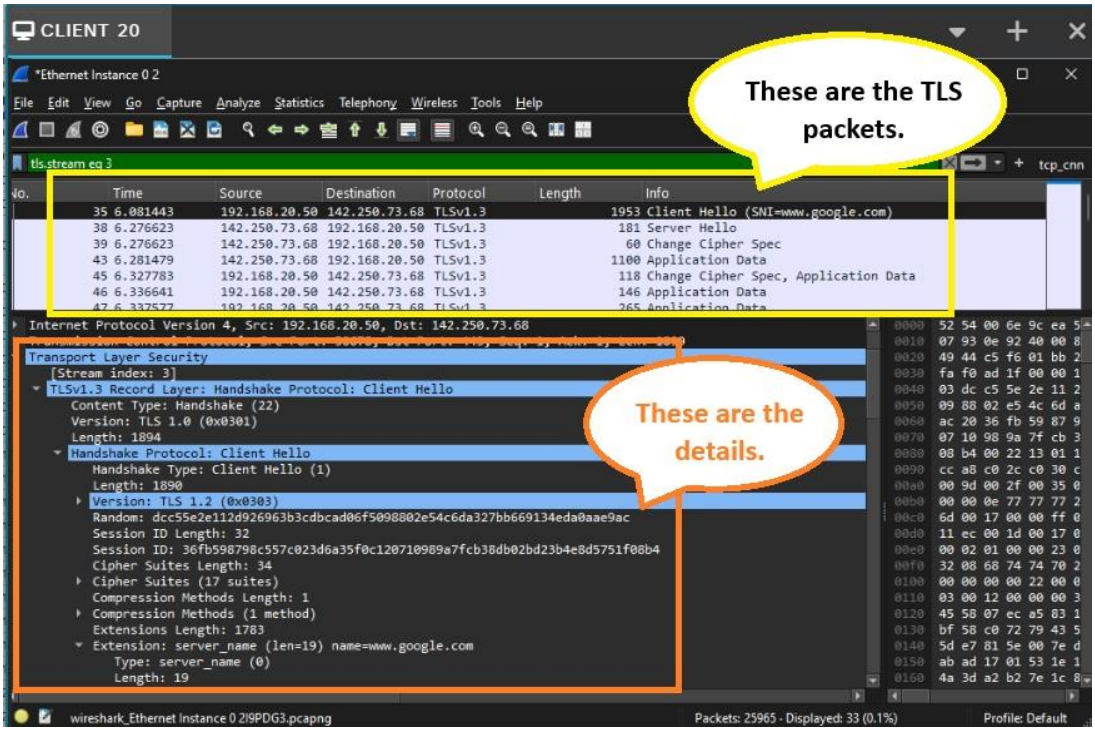

Figure 17. SSL/TLS packet details.

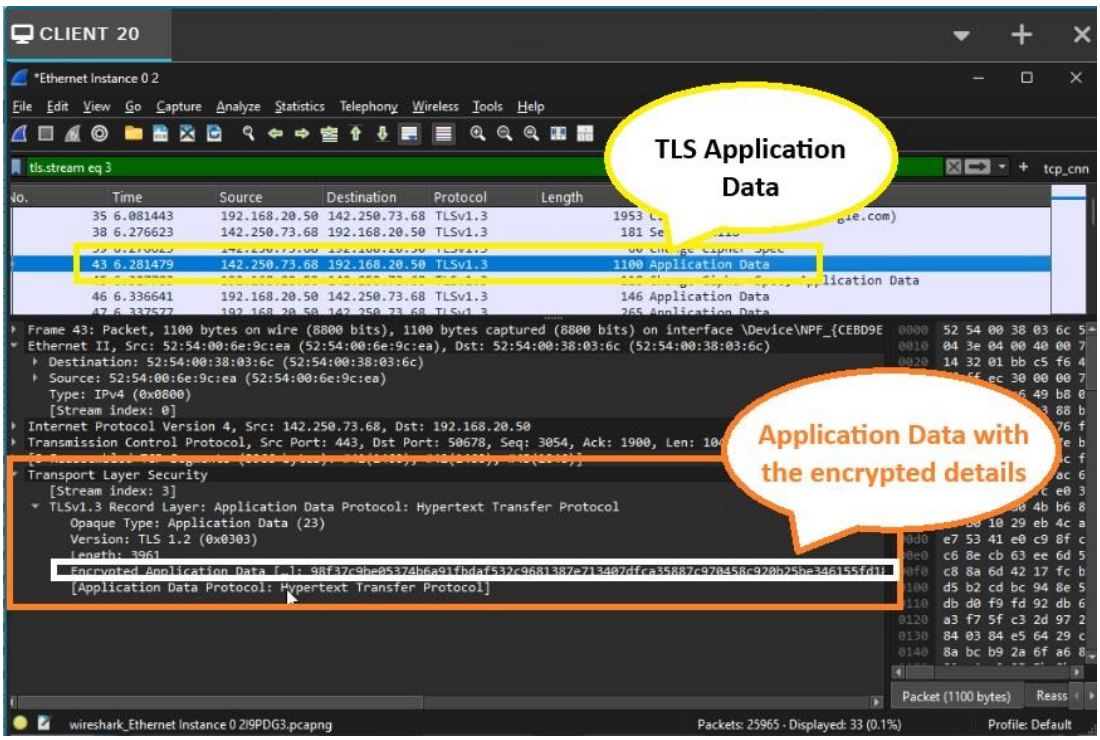

Figure 18. Encrypted application data.

5.3 Process of decrypting SSL/TLS traffic

- In Wireshark, go to “Edit” then click “Preferences”.
- Expand “Protocols”, scroll down and select “TLS”.
- In the "(Pre)-Master-Secret log filename" field, click Browse and select the sslkeylog.log file you created earlier.

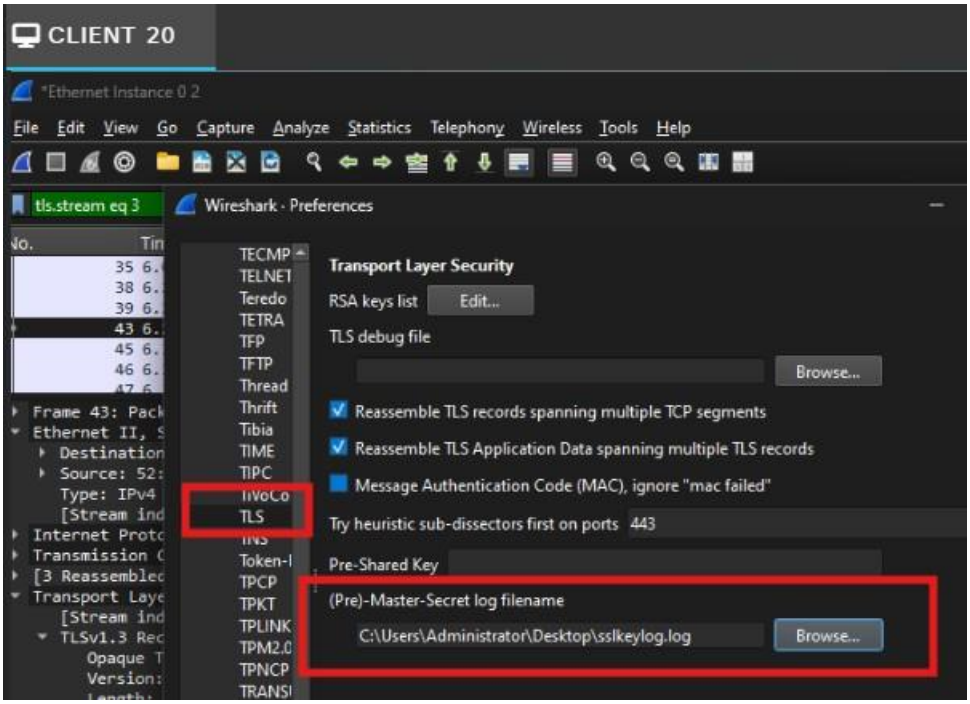

Figure 19. Browse key log file to decrypt SSL traffic.

- Click OK to apply the changes.

5.4 After decrypting SSL/TLS traffic

- Once decrypted, Wireshark will display HTTP2 protocols, HTTP GET/POST requests, Host header, and Content-type. Below is the screenshot.

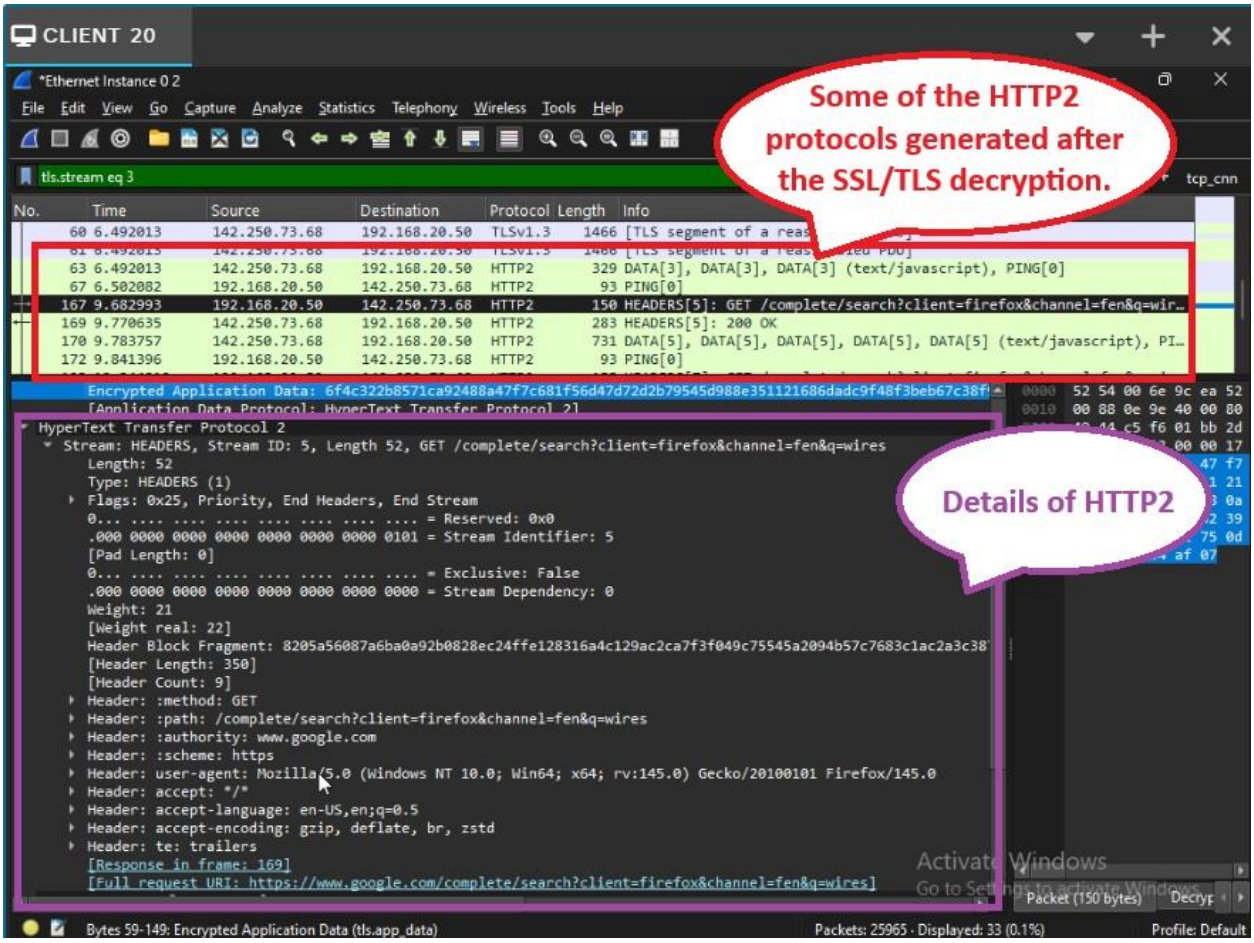

Figure 20. HTTP2 capture after decrypting SSL/TLS traffic.

6 Question and Answer

6.1 Explain the process of SSL/TLS interception and include how certificates are handled and the role of root certificate authorities in maintaining trust.

SSL (Secure Sockets Layer) refers to a protocol for encryption to keep user data secure, authenticate communications that take place on the websites, and stop attackers from

tampering with internet communications. TLS (Transport Layer Security) is the successor technology to SSL which was replaced in 2015 after it was compromised by several vulnerabilities. Most people use the common term SSL because it's more widely known.

SSL/TLS interception works by allowing a firewall to temporarily act as a man-in-the-middle (MITM) in encrypted web traffic so it can apply security checks.

1. The client tries to connect to a secure website.
2. The firewall stops the request and creates two separate TLS sessions:
    - One between the client - firewall
    - One between the firewall - real server
3. To keep the browser from warning the user, the firewall re-signs the website's certificate using its own internal CA (Certificate Authorities) certificate.
4. If the client trusts that CA, the browser accepts the connection as valid.
5. The firewall decrypts the traffic, scans it for threats, then re-encrypts it and sends it on.

Root Certificate Authorities is a trusted CA (Certificate Authorities) required so the browser does not display security warnings. When the firewall's CA certificate is added to the client machine, it becomes trusted where browser treats the firewall like any legitimate CA.

6.2 What technical challenges can occur during SSL/TLS inspection (e.g., certificate pinning, encrypted SNI)? Propose potential solutions for these issues.

These are technical challenges that occur during SSL/TLS inspection:

- Certificate Pinning

Some apps embed the server's certificate or public key. If the certificate changes because of inspection, the app rejects the connection. The solution is to bypass the inspection for pinned services (e.g. banking apps, updates).

- Encrypted SNI (Server Name Indication)

When SNI is encrypted, the firewall can't identify the domain being requested, making filtering harder. The solution would be to use domain-category based rules, or DNS filtering.

- Performance Overhead

Decrypting and re-encrypting traffic is CPU-intensive. The solution is to use hardware capable of SSL acceleration, limit inspection to high-risk categories, and avoid decrypting streaming/video sites.

6.3 How does SSL/TLS inspection intersect with data privacy laws and compliance requirements such as GDPR, HIPAA, or PIPEDA? Provide examples of scenarios where SSL inspection might be restricted or prohibited.

SSL/TLS inspection has important legal and privacy implications because it allows a firewall to decrypt and view data that users expect to remain private. As soon as an organization performs SSL inspection, it becomes responsible for protecting any personal or sensitive

information that passes through the device. Different laws regulate how this decrypted data may be handled such as GDPR (EU), HIPAA (US healthcare), and PIPEDA (Canada) limit how organizations can access and process personal or sensitive information. For example, decrypting traffic may require user consent, strict access controls, and justification that the inspection is necessary. In many cases, certain types of encrypted traffic must not be inspected at all. Common examples include banking websites, healthcare portals containing patient data, and personal services like webmail or social media. These types of traffic are often excluded or bypassed during SSL inspection to avoid violating privacy regulations or exposing confidential information.

References

A Lock, Two Keys and Strong Identity. (n.d.). Retrieved from digicert: https://www.digicert.com/tls-ssl/tls-ssl-certificates

CyberSec. (n.d.). *FortiGate SSL Deep Inspection – Basic Behavior Explained*. Retrieved from Youtube: https://www.youtube.com/watch?v=t2HDzenmNWc&t=32s

Hacksi. (n.d.). *How to DECRYPT HTTPS Traffic with Wireshark*. Retrieved from Youtube: https://www.youtube.com/watch?v=eeikugGyilg

How does SSL work? | SSL certificates and TLS. (n.d.). Retrieved from Cloudflare: https://www.cloudflare.com/learning/ssl/how-does-ssl-work/

Thakkar, J. (2018, August 3). *What is SSL Inspection? How does it work?* Retrieved from HashedOut: https://www.thesslstore.com/blog/ssl-inspection/

What is an SSL certificate – Definition and Explanation. (n.d.). Retrieved from kaspersky: https://www.kaspersky.com/resource-center/definitions/what-is-a-ssl-certificate

What Is SSL Inspection? (n.d.). Retrieved from Zscaler: https://www.zscaler.com/resources/security-terms-glossary/what-is-ssl-inspection