LAB : **Practical Network Security**

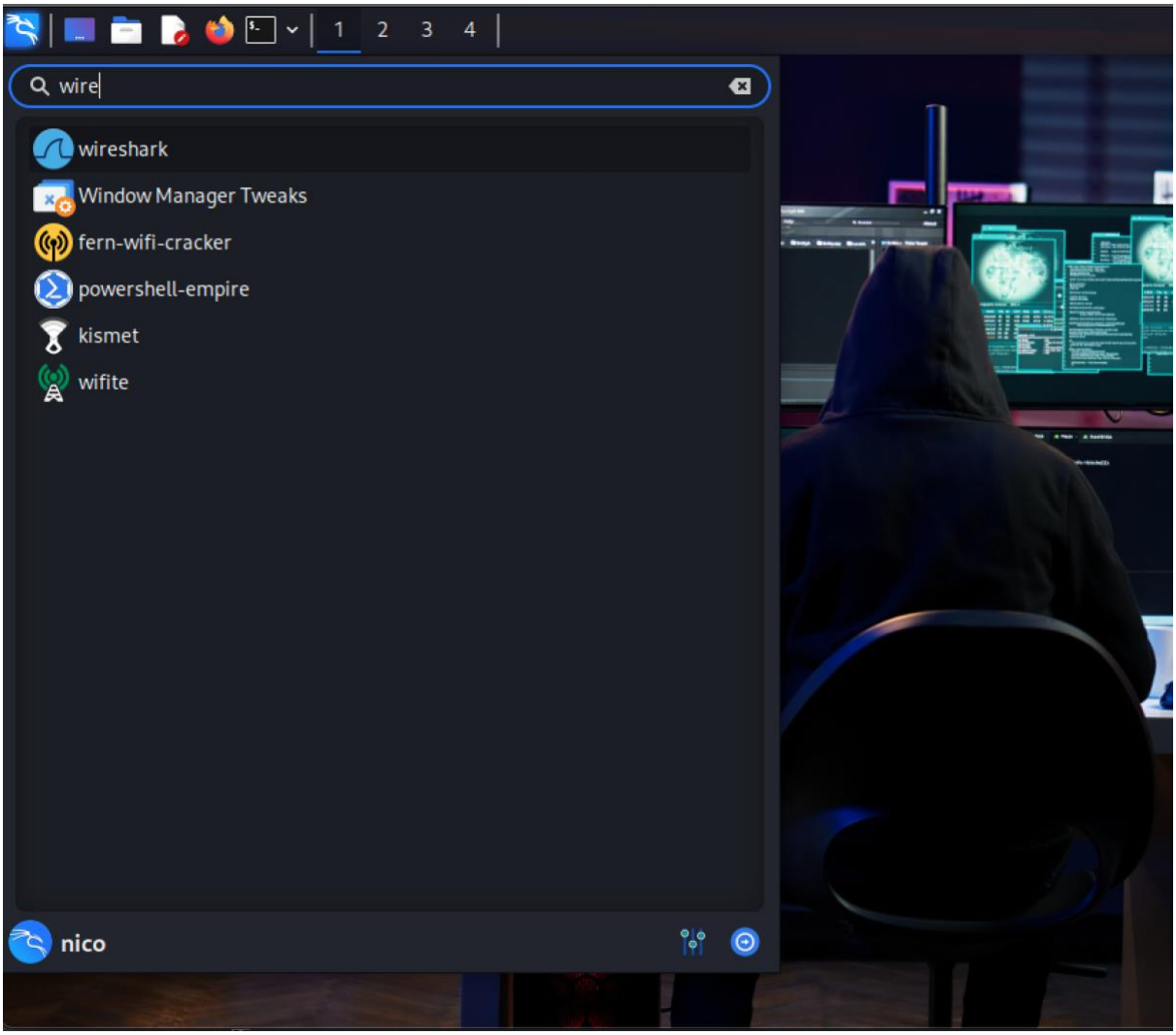
Senin, 24 November 2025

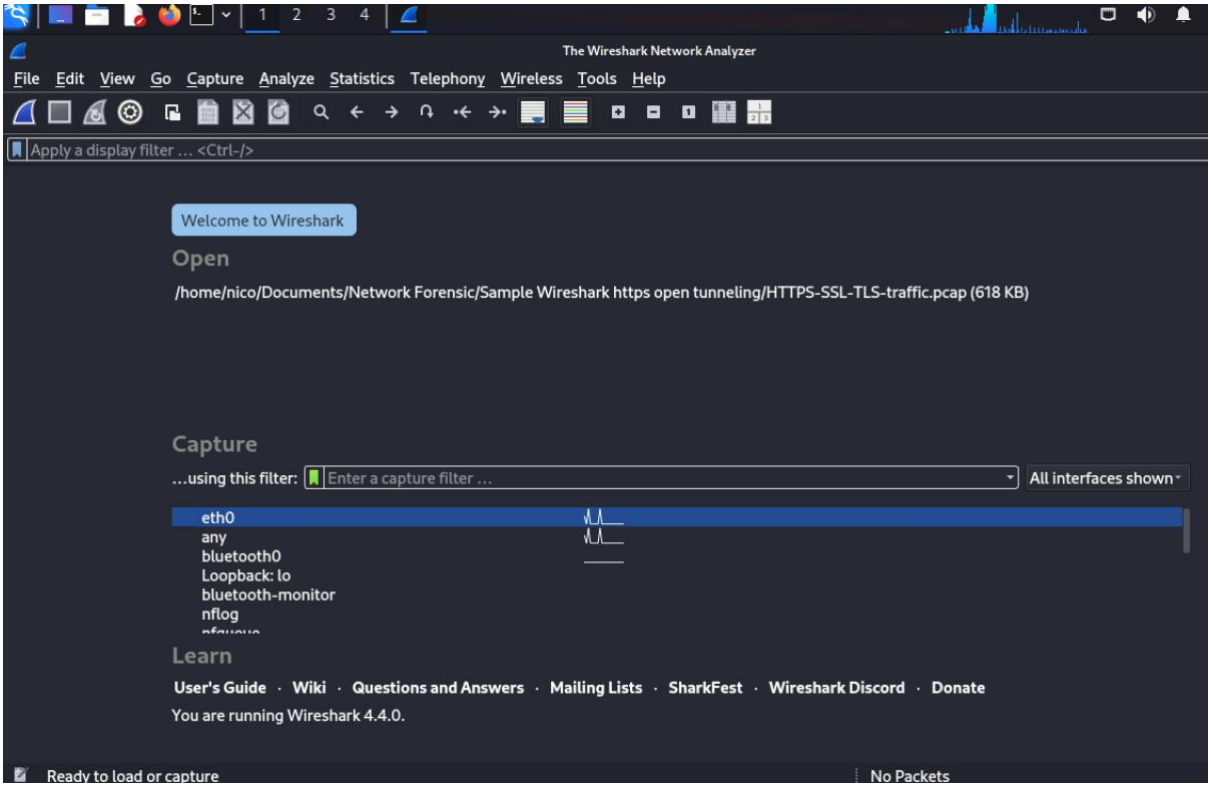
Tujuan : Investigate suspicious activity

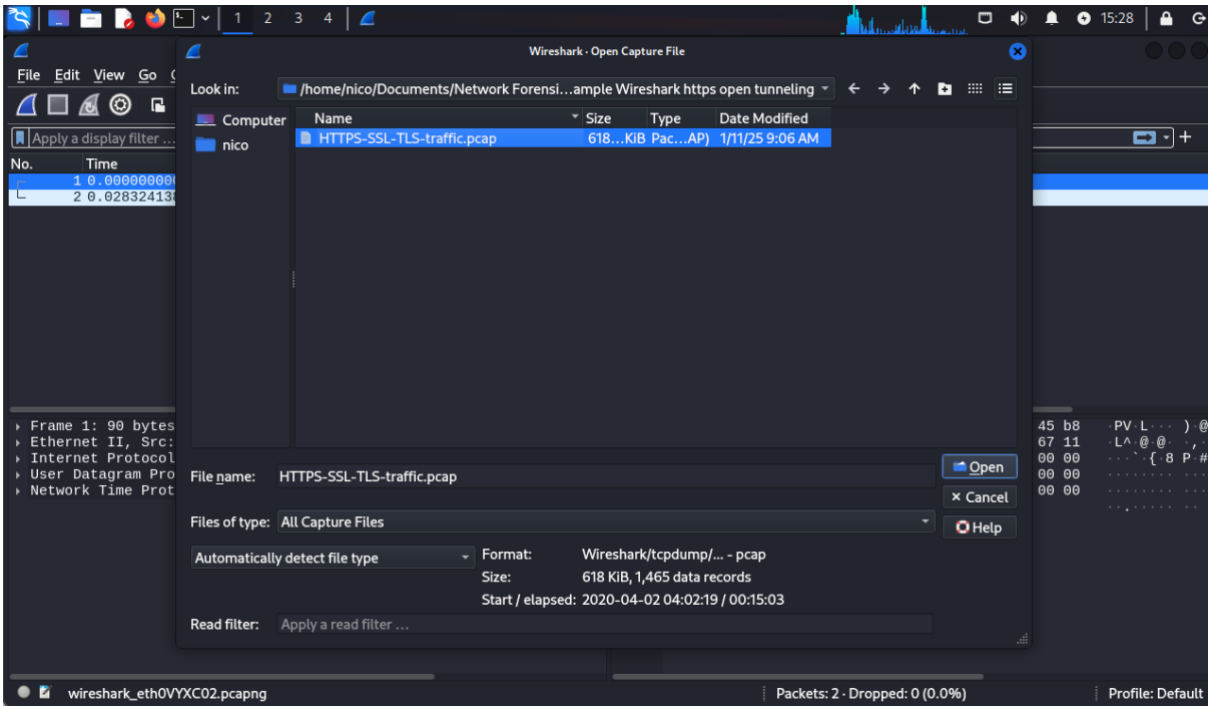
- **Review packet captures (.pcap) – Menganalisa Trafik Paket di Jaringan**
- **See encrypted traffic (HTTPS) – Melihat Paket HTTP Enkripsi**
- **Decrypt traffic using Key – Mendekripsi Paket Http yang terenkripsi**
- **Cek Malware C2C Server di Virustotal.**

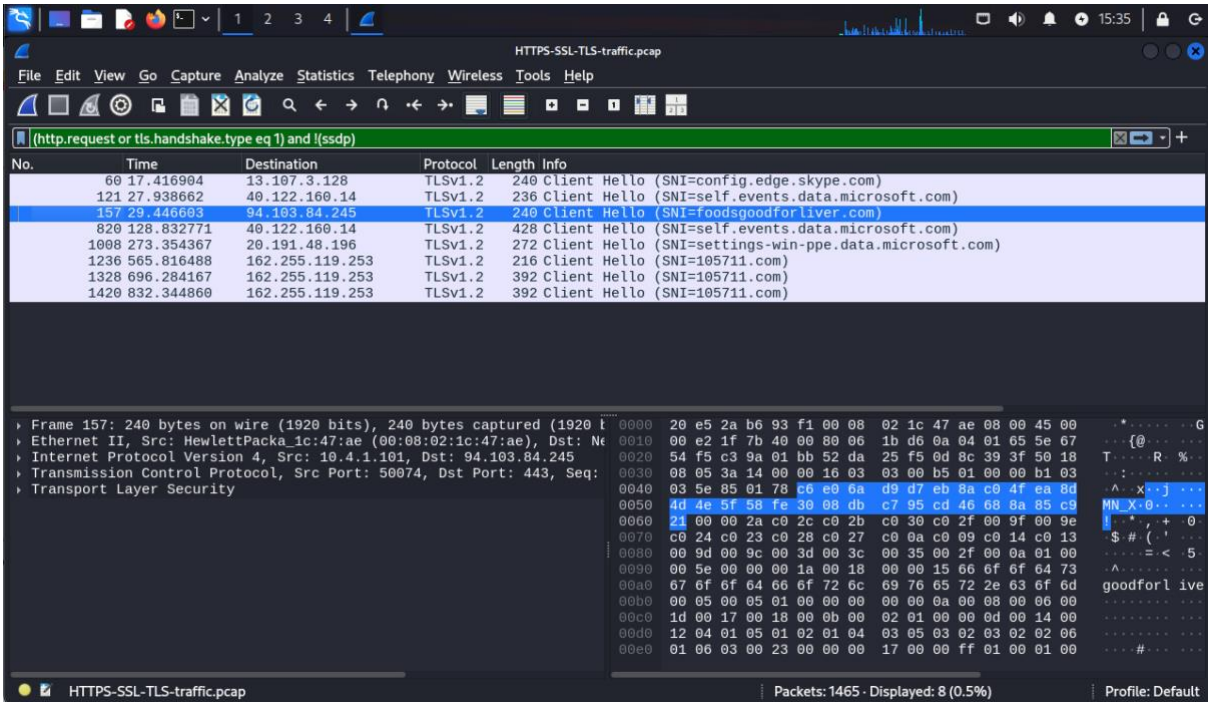
1. Https traffic without the key Log File.

Open HTTPS-SSL-TLS-traffic.pcap in wireshark 4.4.0 Kalilinux



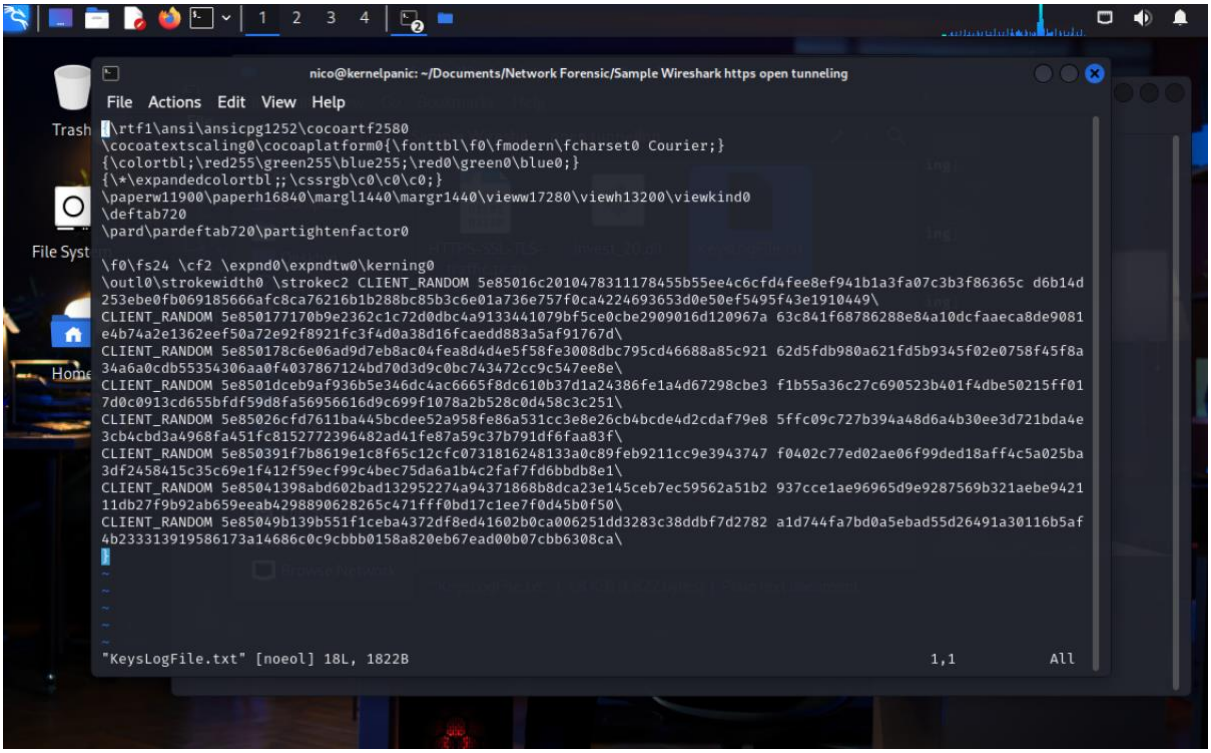

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Open
/home/nico/Documents/Network Forensic/Sample Wireshark https open tunneling/HTTPS-SSL-TLS-traffic.pcap (618 KB)
Capture
...using this filter: Enter a capture filter ...
All interfaces shown
eth0
any
bluetooth0
Loopback: lo
bluetooth-monitor
nflog
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate
You are running Wireshark 4.4.0.
Ready to load or capture
No Packets


Wireshark · Open Capture File
Look in: /home/nico/Documents/Network Forensi...ample Wireshark https open tunneling
Computer
nico
Name
Size
Type
Date Modified
HTTPS-SSL-TLS-traffic.pcap
618...KiB
Pac...AP)
1/11/25 9:06 AM
File name: HTTPS-SSL-TLS-traffic.pcap
Open
Cancel
Help
Files of type: All Capture Files
Automatically detect file type
Format: Wireshark/tcpdump/... - pcap
Size: 618 KiB, 1,465 data records
Start / elapsed: 2020-04-02 04:02:19 / 00:15:03
Read filter: Apply a read filter ...
wireshark_eth0VYXC02.pcapng
Packets: 2 · Dropped: 0 (0.0%)
Profile: Default

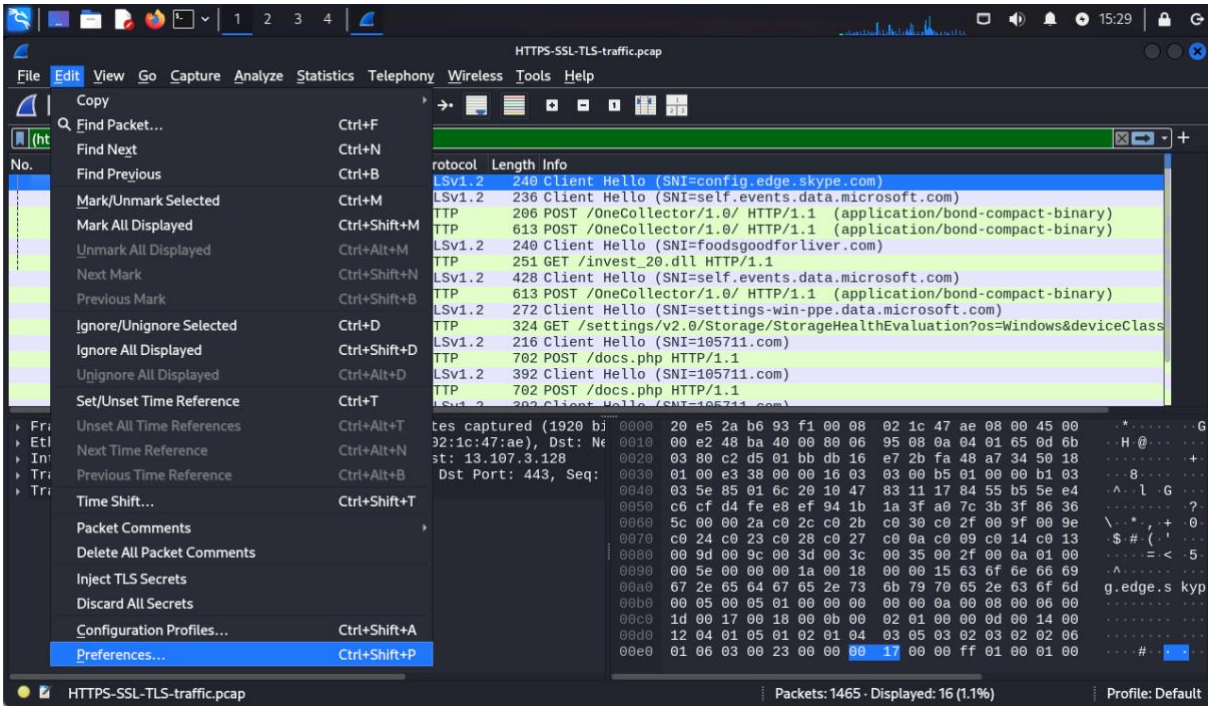


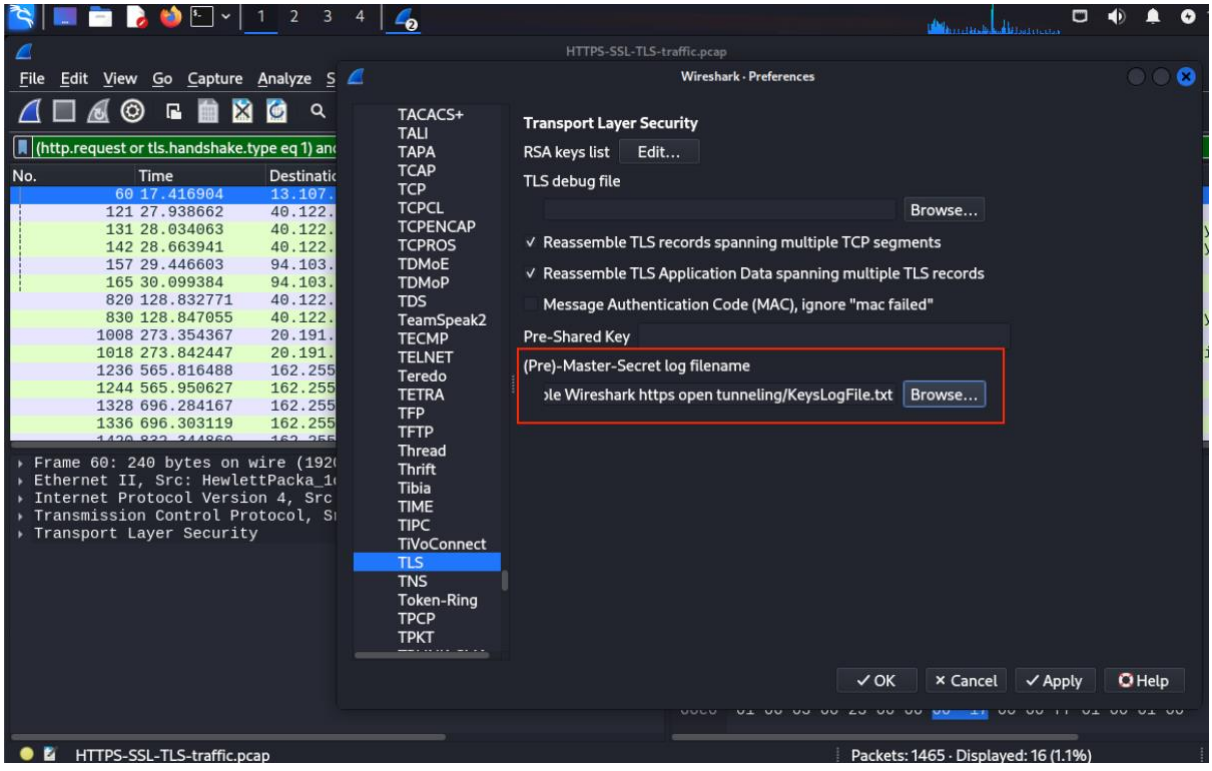
This show connection https Tlsv1.2 length info only show client hello no header and client hello (encrypt communication)

2. To open encrypt communication we using key log file .

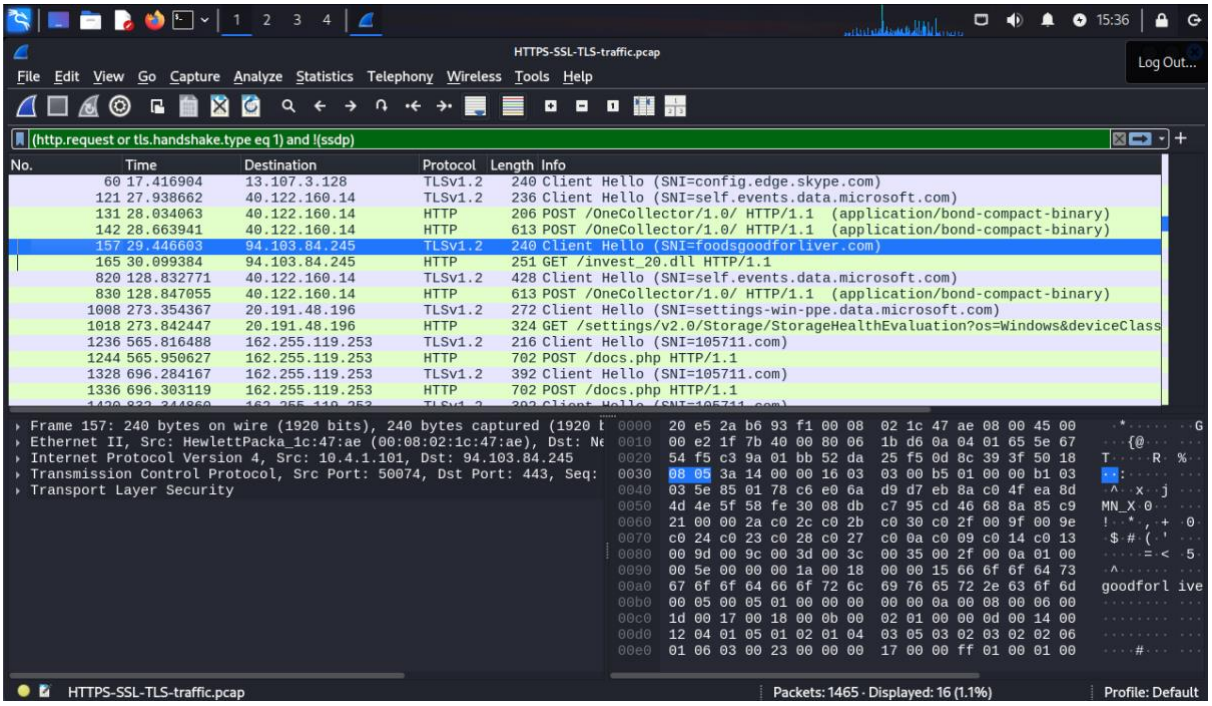


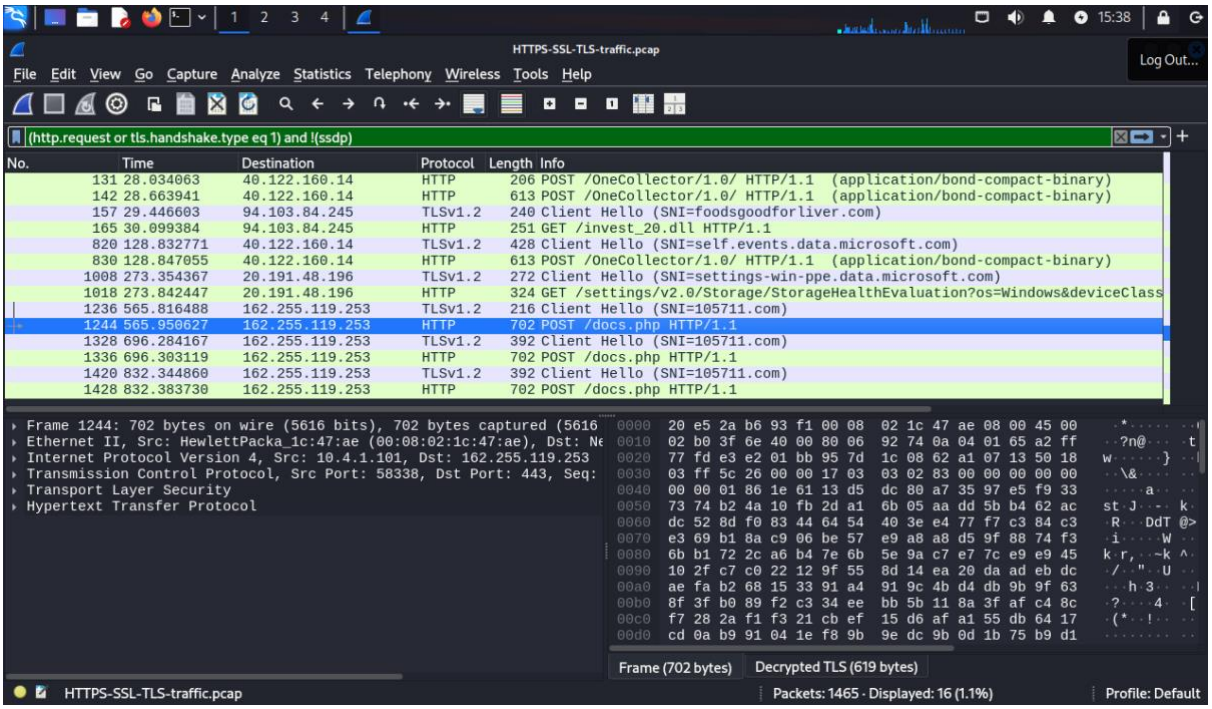
3. Loading the Key Log File into wireshark.





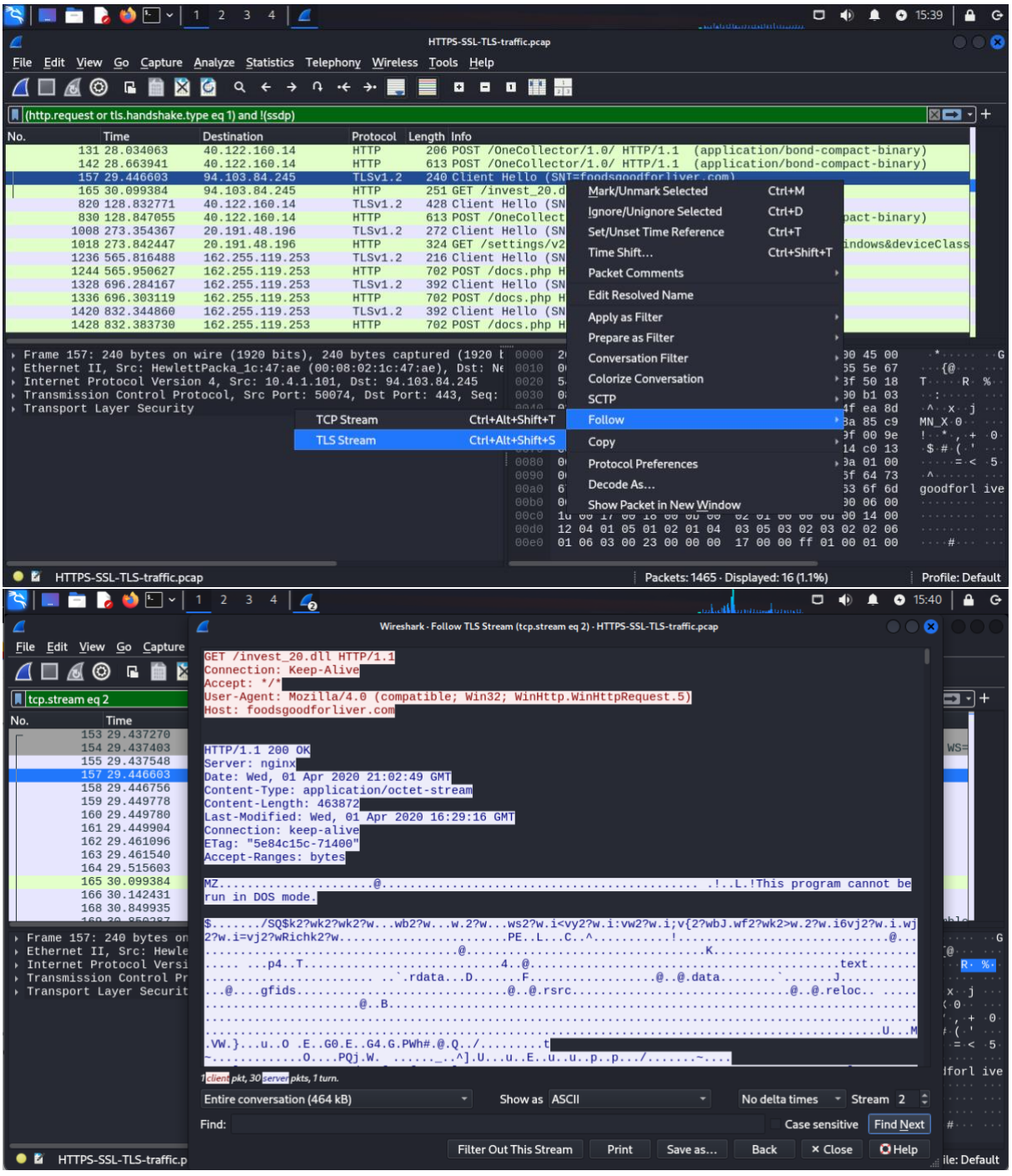
4. After add KeyLog File, https traffic with the key log file shown this :



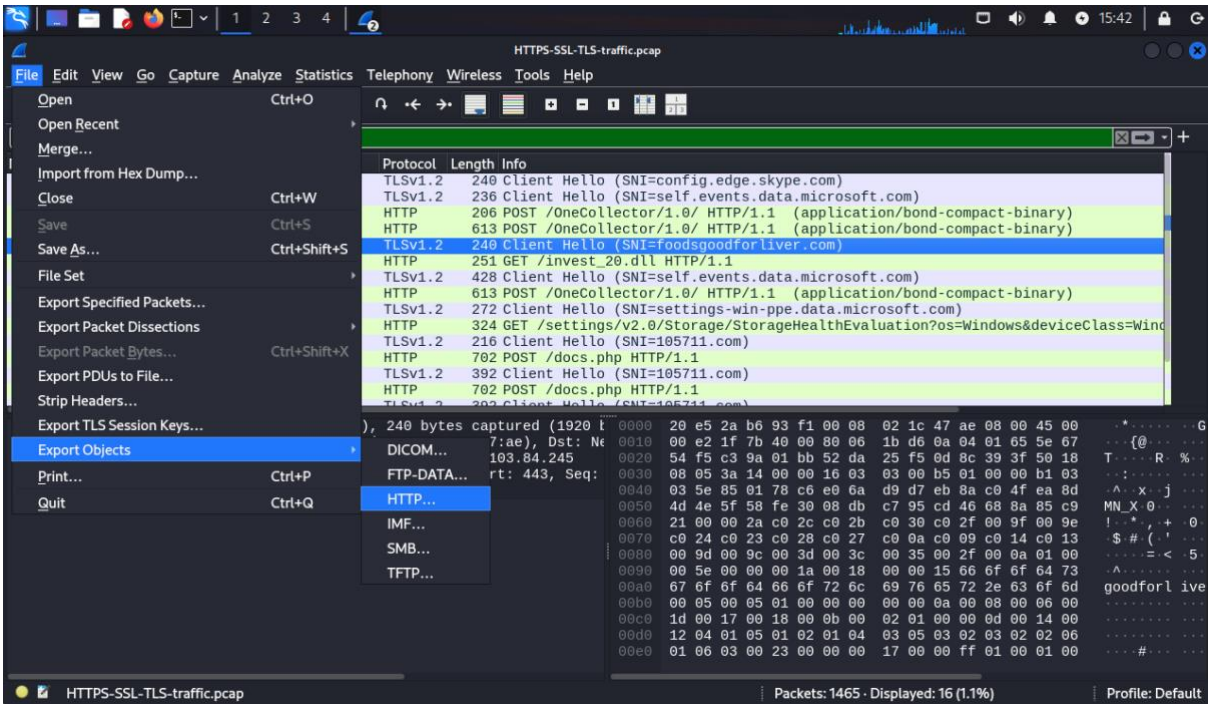


we now see http request is clear text such as foodgoodliver.com get file /invest_20.dll. and 105711.com – post /docs.php.
The GET request to foodgoodliver.com returned a DLL file for dridex. The POST request to 105711.com are command control (C2) traffic form Dridex-infected windows host.

5. We can review the trafiic by following TLS Stream.

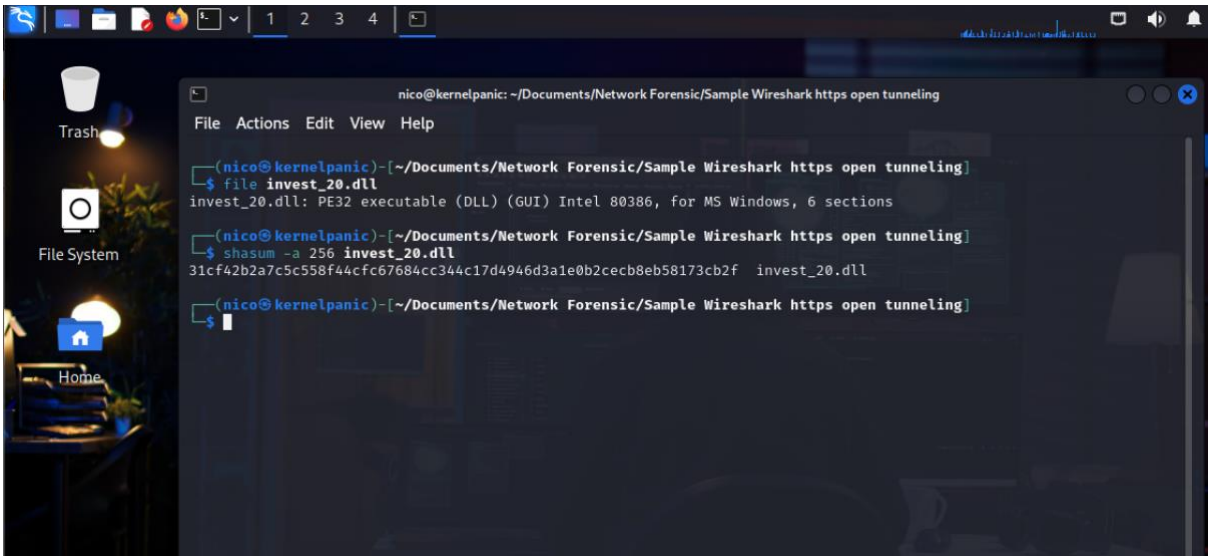


6. Export File From Traffic foodsgoodforliver.com. (Malware).



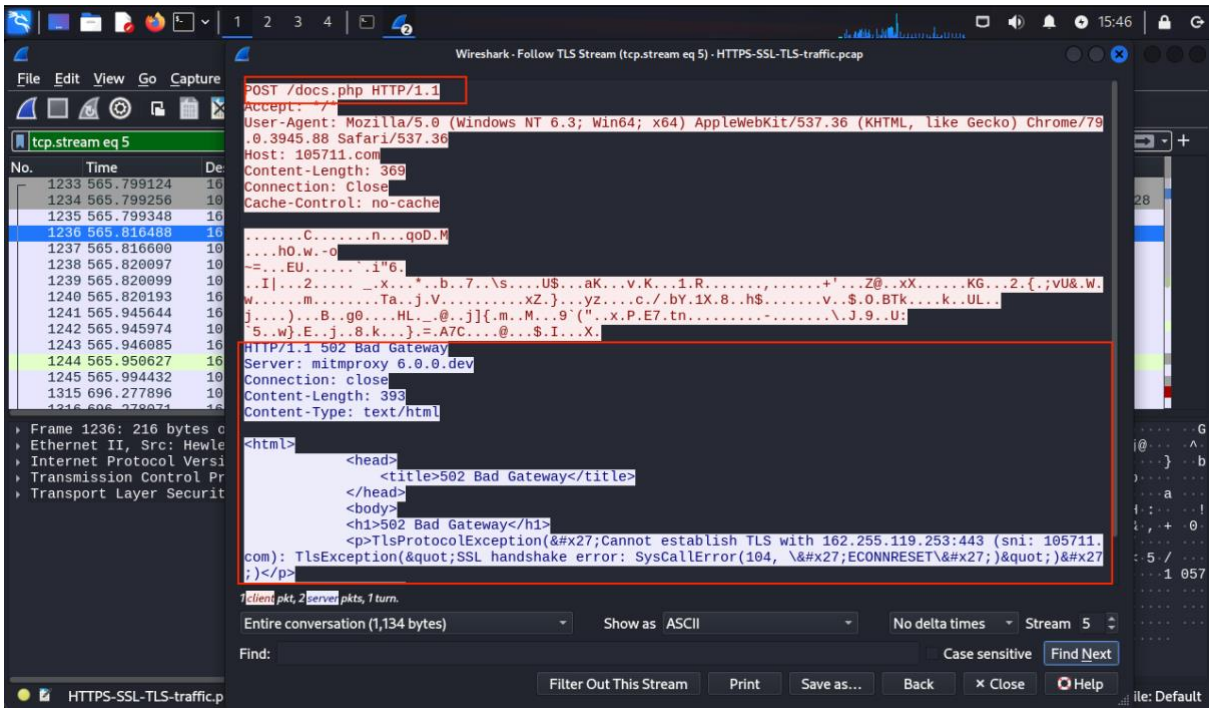
File -> Export Objects -> HTTP , file name is : invest20.dll

7. Check hash of the file.



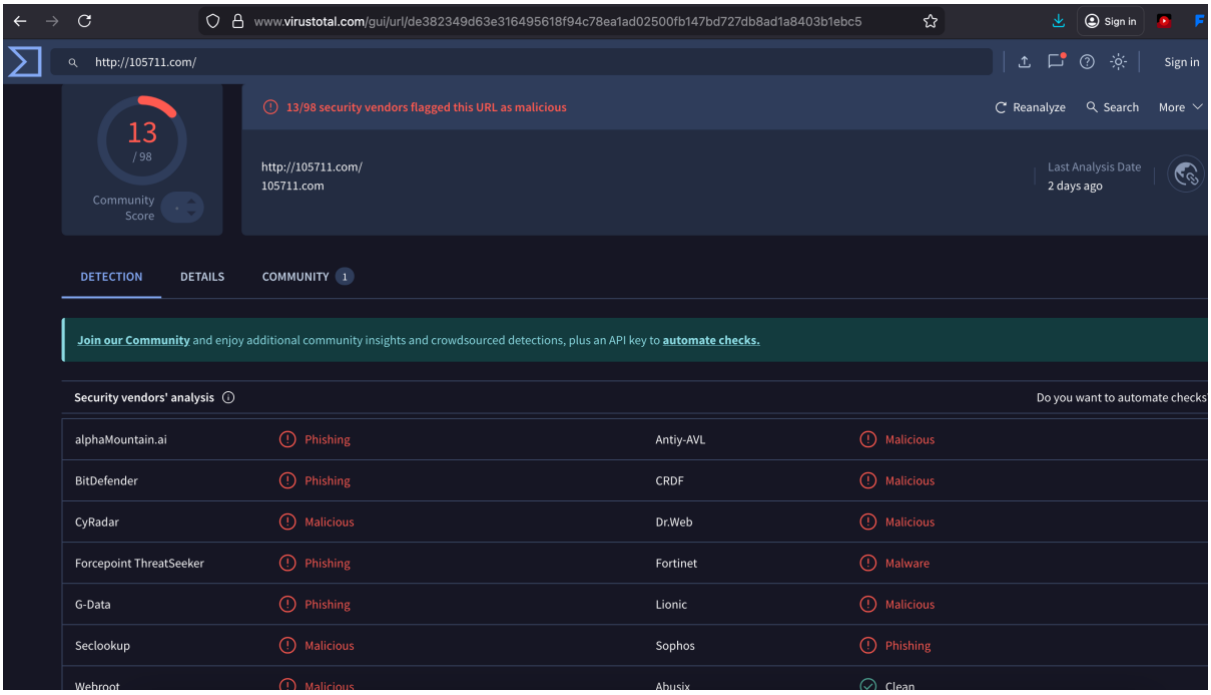
The SHA256 hash of this malware is :
31cf42b2a7c5c558f44cfc67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f

8. Investigate HTTP stream from malicious POST request.



We can review C2 traffic from Dridex infection. Stream from one of the POST requests to 105711.com

9. **Cek Virus Total**



Terdapat server C2 ke arah malware,