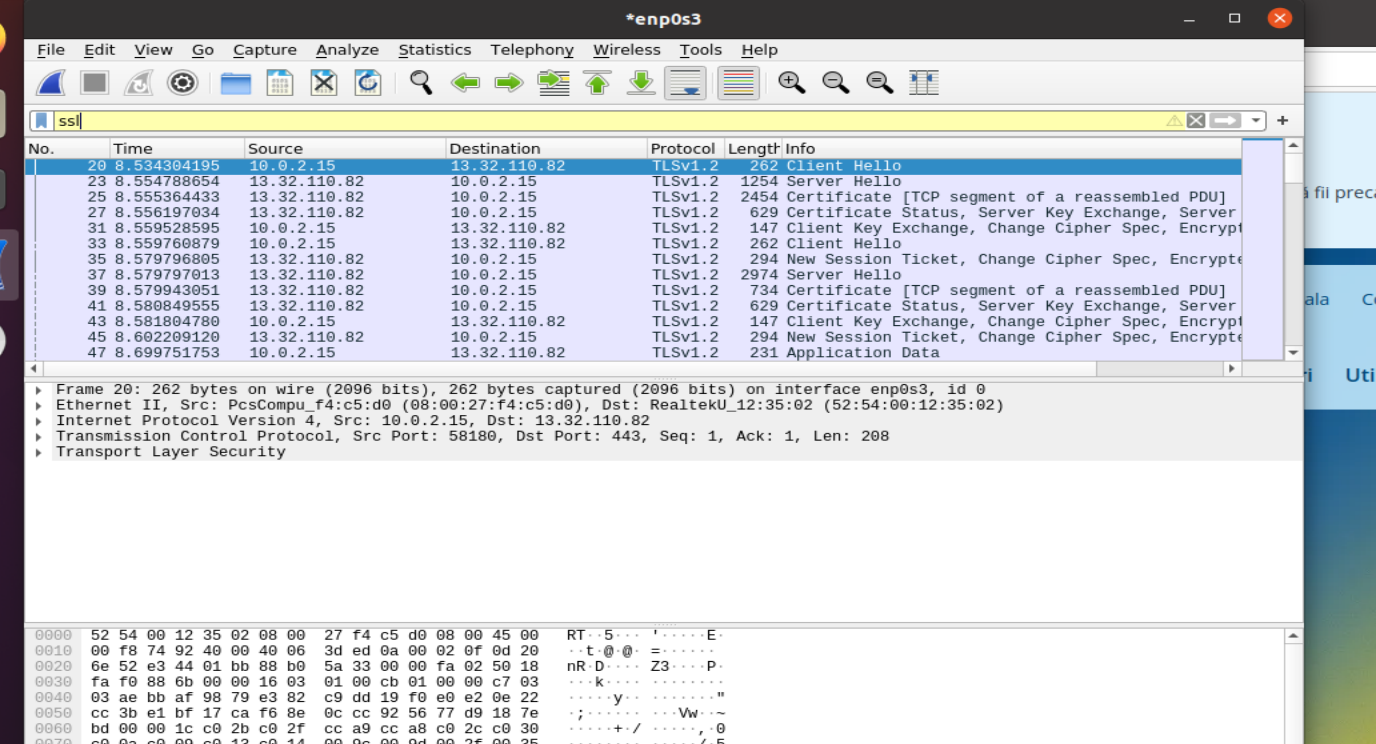
Laborator 8

Parvan Andrei Leonard

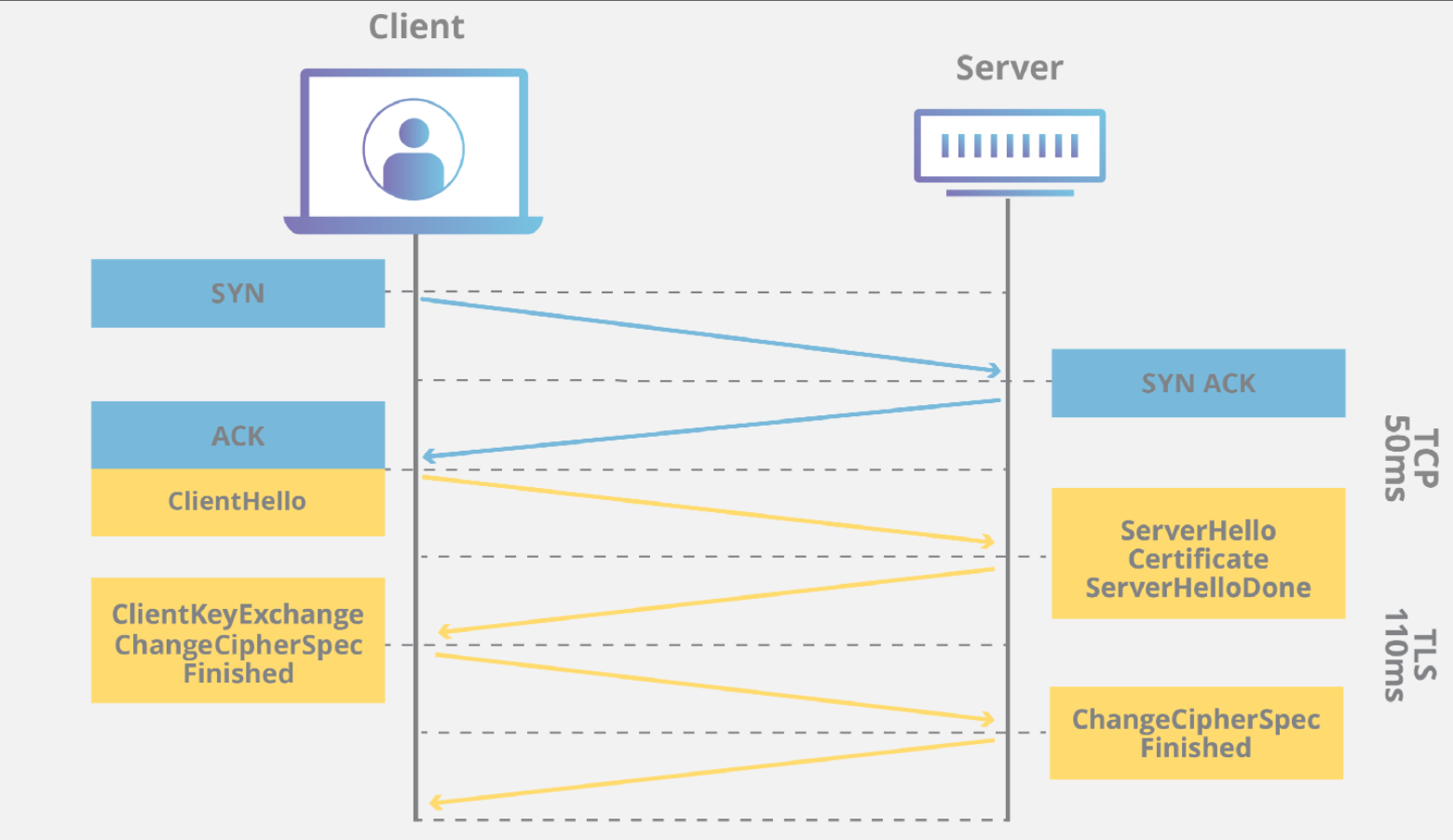
Capturarea pachetelor dintr-o sesiune SSL (1p) Primul pas este capturarea pachetelor dintr-o sesiune SSL. Pentru a realiza acest pas accesaţi un site de e-commerce sau e-banking ce utilizează criptarea (eventual demaraţi procesul de achiziţie al unui produs). După capturarea pachetelor cu Wireshark, trebuie să setaţi un filtru astfel încât să fie afişate doar cadrele Ethernet care conţin înregistrări SSL (o înregistrare SSL este acelaşi lucru cu un mesaj SSL) trimise şi recepţionate de gazda la care lucraţi. Pentru limitarea numărului pe pachete capturate de Wireshark se recomanda setarea filtrului „tcp.port == 443” în fereastra de opţiuni captură (Puteti aplica si filtrul “ssl”). Ar trebui să obţineţi ceva similar Figurii 1. Precizaţi URL-ul folosit pentru interceptarea traficului. Filtraţi pachetele afişate astfel încât acestea să se limiteze la o singură conexiune TCP peste care rulează SSL (de la segmentul TCP SYN şi până la segmentul TCP FIN-ACK); salvaţi într-un fişier (NumePrenume\_SSL1.pcap) doar pachetele afişate. Acest fişier trebuie inclus în arhivă corespunzătoare acestui laborator, întrucât va constitui baza pentru răspunsurile la întrebările din secţiunea 2.

URL: <https://www.bcr.ro/ro/persoane-fizice>



Pentru fiecare din primele 8 cadre Ethernet, specificaţi sursa cadrului (client sau server), determinaţi numărul de înregistrări SSL incluse în acel cadru şi listaţi tipurile de înregistrări SSL care sunt incluse în cadru. Desenaţi o diagramă care să pună în evidenţă schimburile de înregistrări; folosiţi o săgeată pentru fiecare înregistrare SSL.

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. Cadru | Sursa | Nr. Inregistrari | Tip inregistrari |
| 1 | 10.0.2.15 | 1 | Client Hello |
| 2 | 13.32.110.82 | 1 | Server Hello |
| 3 | 13.32.110.82 | 1 | Certificate [TCP segment of a reassembled PDU] |
| 4 | 13.32.110.82 | 3 | Certificate Status, Server Key Exchange, Server Hello Done |
| 5 | 10.0.2.15 | 3 | Client Key Exchange, Change Cipher Spec, Ecrypted Handshake |
| 6 | 10.0.2.15 | 1 | Client Hello |
| 7 | 13.32.110.82 | 3 | New Session Ticket, Change Cipher Spec, Ecrypted Handshake |
| 8 | 13.32.110.82 | 1 | Server Hello |



Fiecare înregistrare SSL începe cu aceleaşi trei câmpuri (având valori posibil diferite). Unul din aceste câmpuri este Tip conţinut (eng. Content Type) şi are dimensiunea de un octet. Listaţi toate cele trei câmpuri şi precizaţi dimensiunea lor.

Content type – 1 octet

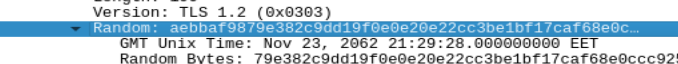
Version – 2 octeti

Length – 2 octeti

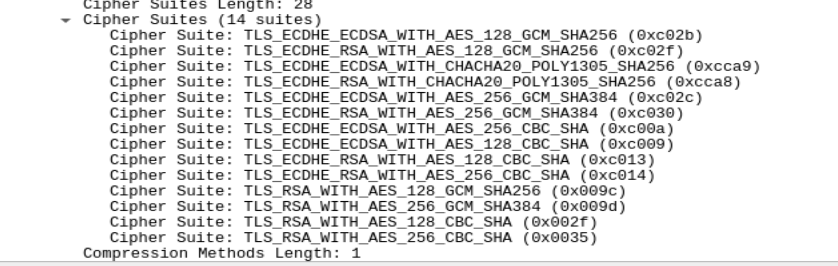
3. Expandaţi înregistrarea ClientHello. (Dacă captura voastră conţine mai multe înregistrări ClientHello, expandaţi cadrul care o conţine pe prima) Care este valoarea câmpului Content Type.

Content type: Handshake

4. Conţine înregistrarea ClientHello un număr unic? Dacă da, care este valoarea acestui număr în notaţie hexazecimală.

Da. 

5. Suita de cifruri suportate de client este anunţată prin înregistrarea ClientHello? Dacă da, în prima suită listată, care sunt algoritmii cu cheie publică, algoritmii cu cheie simetrică şi algoritmii de dispersie? Precizaţi acronimul şi denumirea completă pentru 10 suite de cifruri listate.

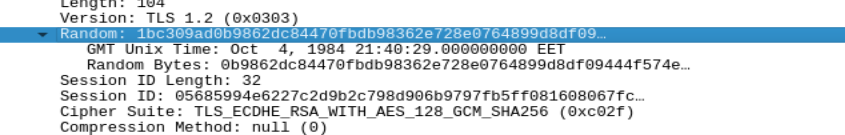


|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nr. | Nume | Algoritm cheie publica | Algoritm cu cheie simetrica | Algoritm dispersie |
| 1 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | AES\_128 | GCM | SHA256 |
| 2 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 | AES\_128 | GCM | SHA256 |
| 3 | TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305\_SHA256 | CHACHA20 | POLY1305 | SHA256 |
| 4 | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384 | AES\_256 | CBC | SHA284 |
| 5 | TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384 | AES\_256 | CBC | SHA384 |
| 6 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA | AES\_128 | CBC | SHA |
| 7 | TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256 | AES\_128 | GCM | SHA256 |
| 8 | TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384 | AES\_256 | GCM | SHA384 |
| 9 | TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA | AES\_128 | CBC | SHA |
| 10 | TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA | AES\_256 | CBC | SHA |

6. Identificaţi înregistrarea ServerHello corespunzătoare înregistrării ClientHello analizate anterior. Este specificată alegerea unei suită de cifruri? Care sunt algoritmii din suita de cifruri aleasă?



7. Include această înregistrare un număr unic? Dacă da, care este dimensiunea acestuia? Care este scopul numerelor unice la client şi la server în cadrul protocolului SSL.



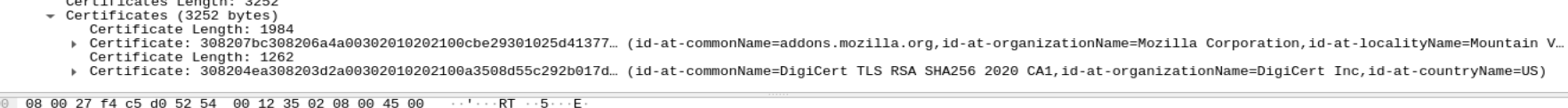
32 biti, session highjack.

8. Include această înregistrare un identificator de sesiune? Care este scopul identificatorului de sesiune?



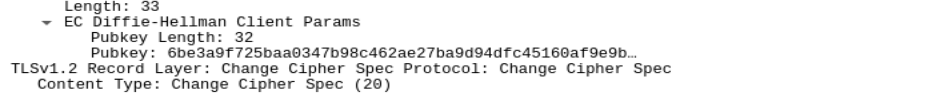
Sa iti refaca sesiunea in caz ca s-a pierdut.

9. Include această înregistrare un certificat, sau certificatul este inclus într-o înregistrare separată. Certificatul încape într-un singur cadru Ethernet?



Certificatul este inclus intr-o inregistrare separata. Nu incape intr-un singur cadru fiind ca este prea mare.

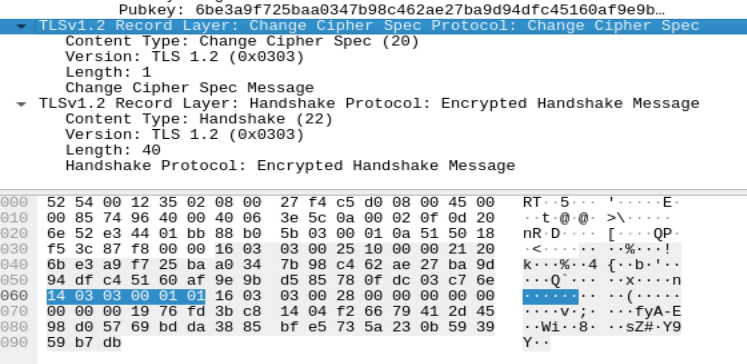
10. Identificaţi Client Key Exchange. Conţine această înregistrare o pre-cheie primară? Pentru ce este utilizată aceasta? Este această cheie criptată? Daca da, cum? Cât de lungă este cheia criptată?



Folosesc cheia asimetrica ca sa trimita cheia simetrica, este criptata, Se foloseste cipher ales din server hello, este folosita pentru a calcula master secret. Acesta contine cheia simetrica. Lungimea este de 32 de biti.

11. Care este scopul înregistrării Change Cipher Spec? Câţi octeţi are înregistrarea în captura voastră?

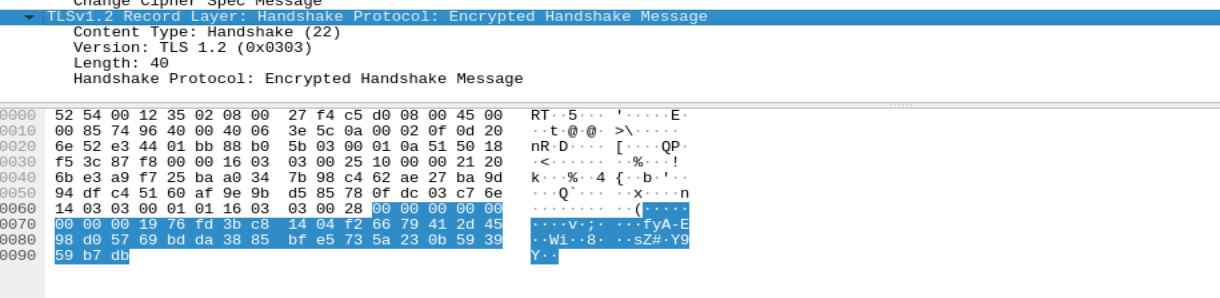
Are 6 biti.

****

Sa notifice ambele parti ca poate incepe comunicarea pe cheie simetrica asa cum s-a stabilit.

12. În înregistrarea Encrypted Handshake (rom. înţelegere criptată), ce anume este criptat şi cum?

Se foloseste pentru prevenirea manipularii datelor in stadiul schimbarii de suite de cifruri.



13. Trimite şi serverul o înregistrare de tip schimbă cifrul şi o înregistrare de tip înţelegere criptată către client? Cum diferă aceste înregistrări de cele trimise de client?

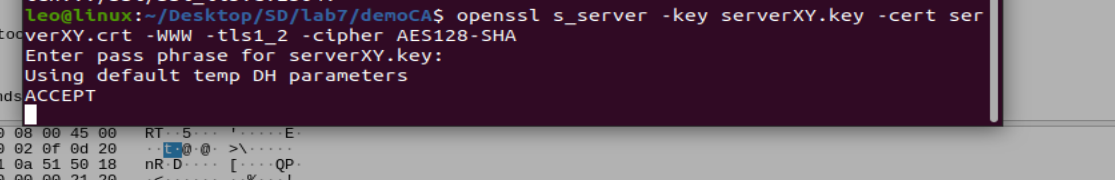
Da. Nu sunt diferite. Daca nu sunt la fel inseamna ceva nu este in regula.

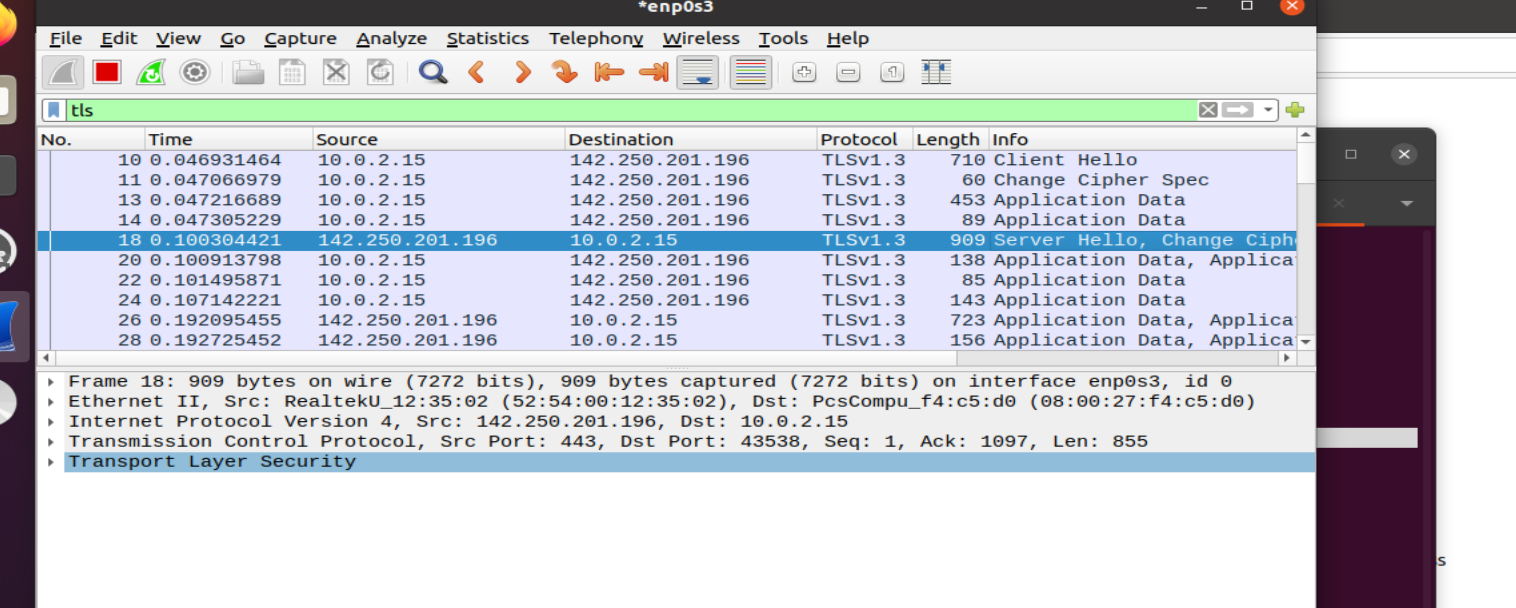
14. Cum sunt criptate datele de nivel aplicaţie? Înregistrările ce conţin date aplicaţie includ şi un câmp MAC?

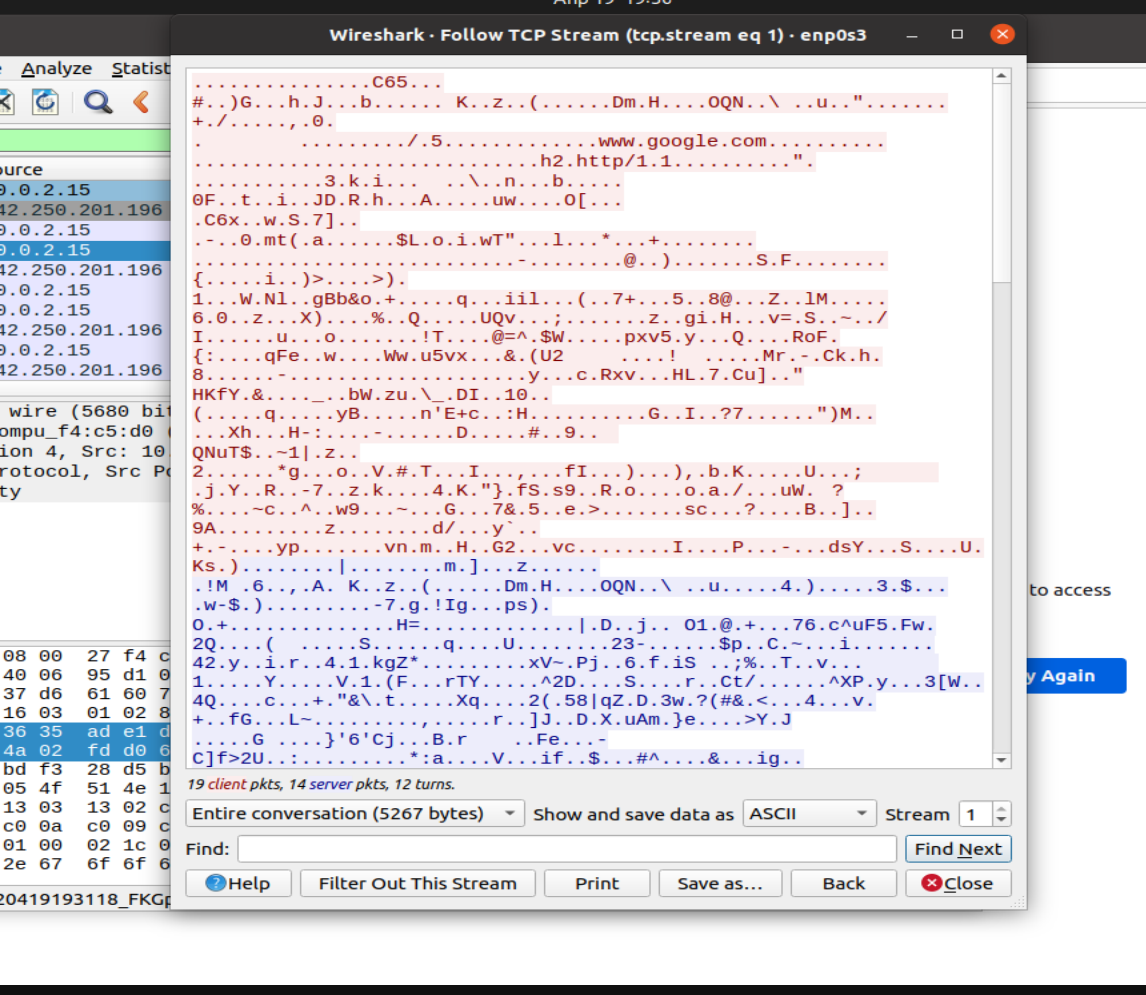
Cu cheia simetrica.

5. Decriptarea traficului de pe conexiunile SSL:

5.1



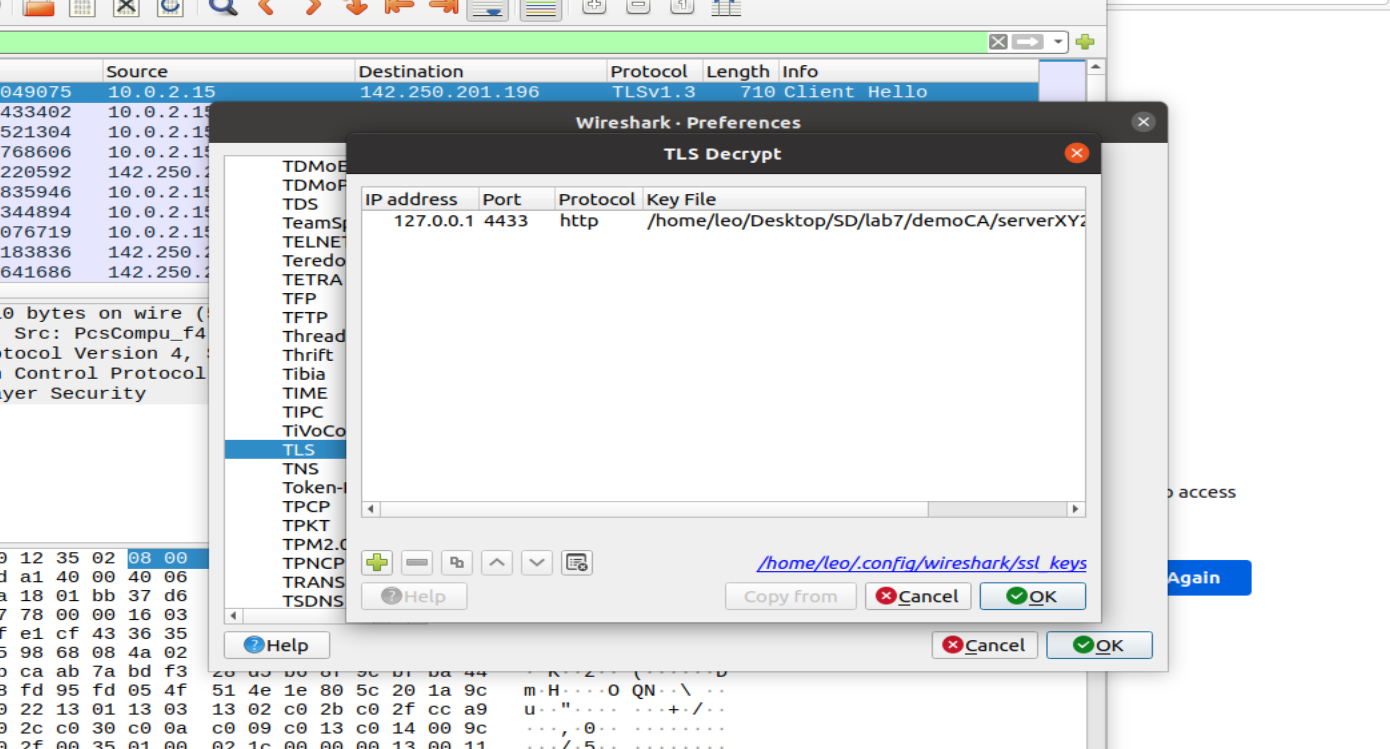


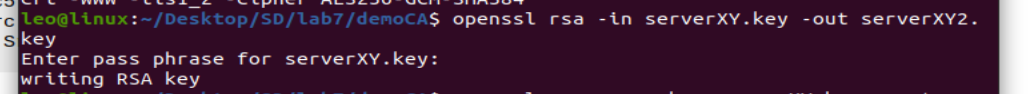


Scop: specifica ce suituri de cipher sa folosesca si ce versiune sa foloseasca tls1\_2 e cel mai safe.

Dupa ce dai comanda la 5.2 daca nu se vede fluxul de date se incarca asa cum este

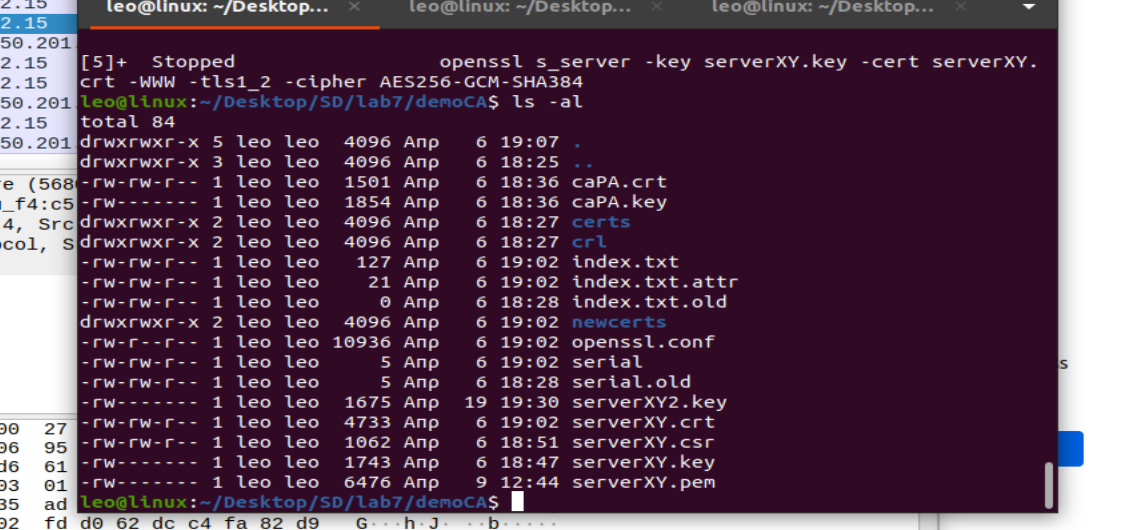
5.2





5.3

Ls -al



Chmod