1.Obtinere certificat de la google.com

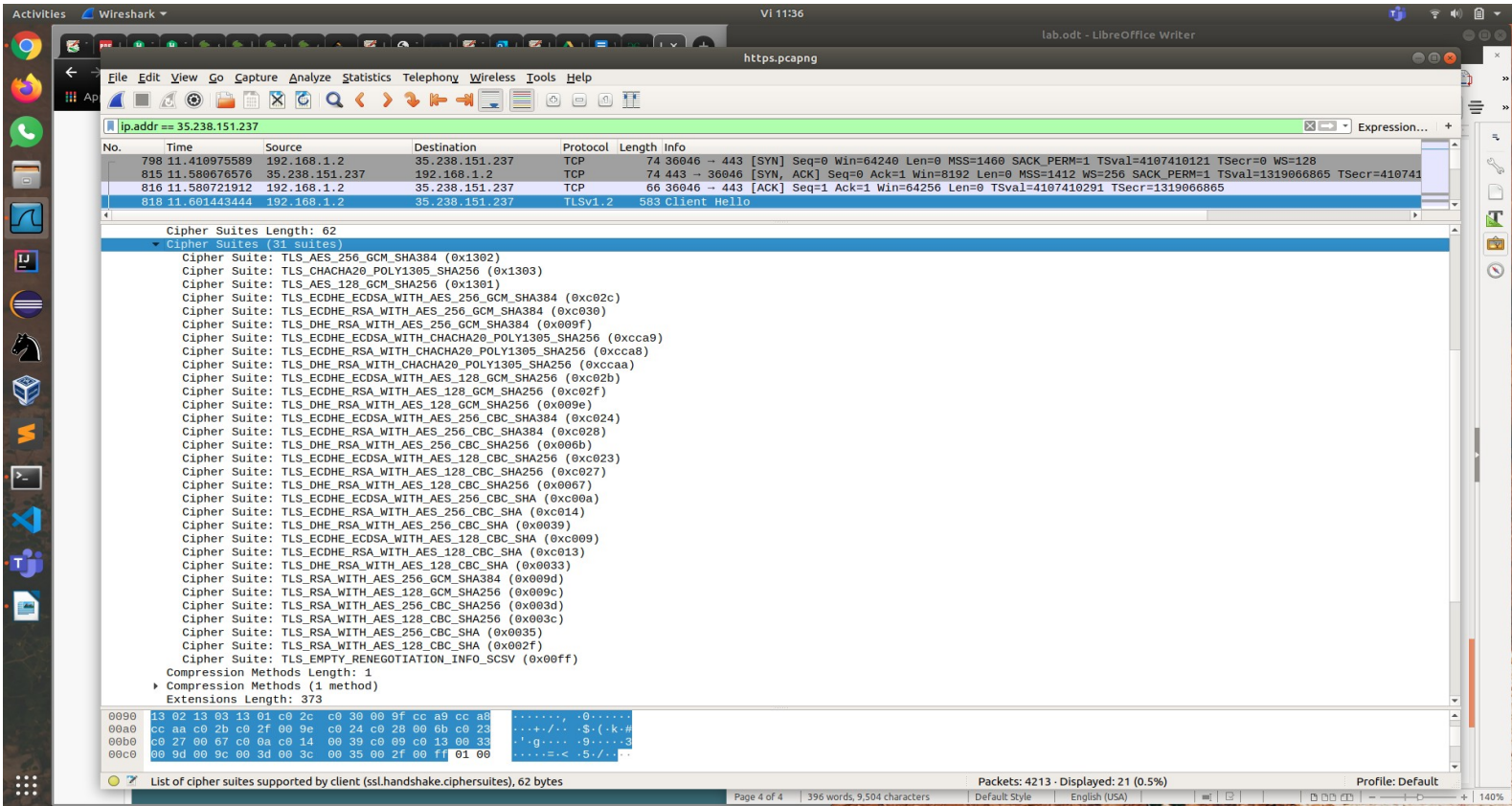
comenzi:
sudo openssl s_client -servername google.com -showcerts -connect google.com:443 >> file.crt
sudo openssl x509 -in file.crt -text

-tipul cifrului folosit:
New, TLSv1.3, Cipher is TLS_AES_256_GCM_SHA384
-entitatea care a eliberat certificatul: **Issuer: C = US, O = Google Trust Services, CN = GTS CA 1O1**
-intervalul de timp in care certificatul e valid:
Validity
Not Before: Apr 15 20:16:47 2020 GMT
Not After : Jul 8 20:16:47 2020 GMT
-cheia publica:
Public-Key: (256 bit)
pub:
04:8e:a4:03:0d:0c:a7:1d:52:28:80:ba:89:51:b9:
45:7a:7a:60:33:a5:ab:25:a4:05:c8:32:d9:b6:5c:
2b:ba:05:a7:6d:2d:e1:66:36:48:30:da:5b:27:28:
08:45:60:83:90:67:3b:51:ef:d0:e2:85:81:9b:49:
c3:50:56:d8:a9

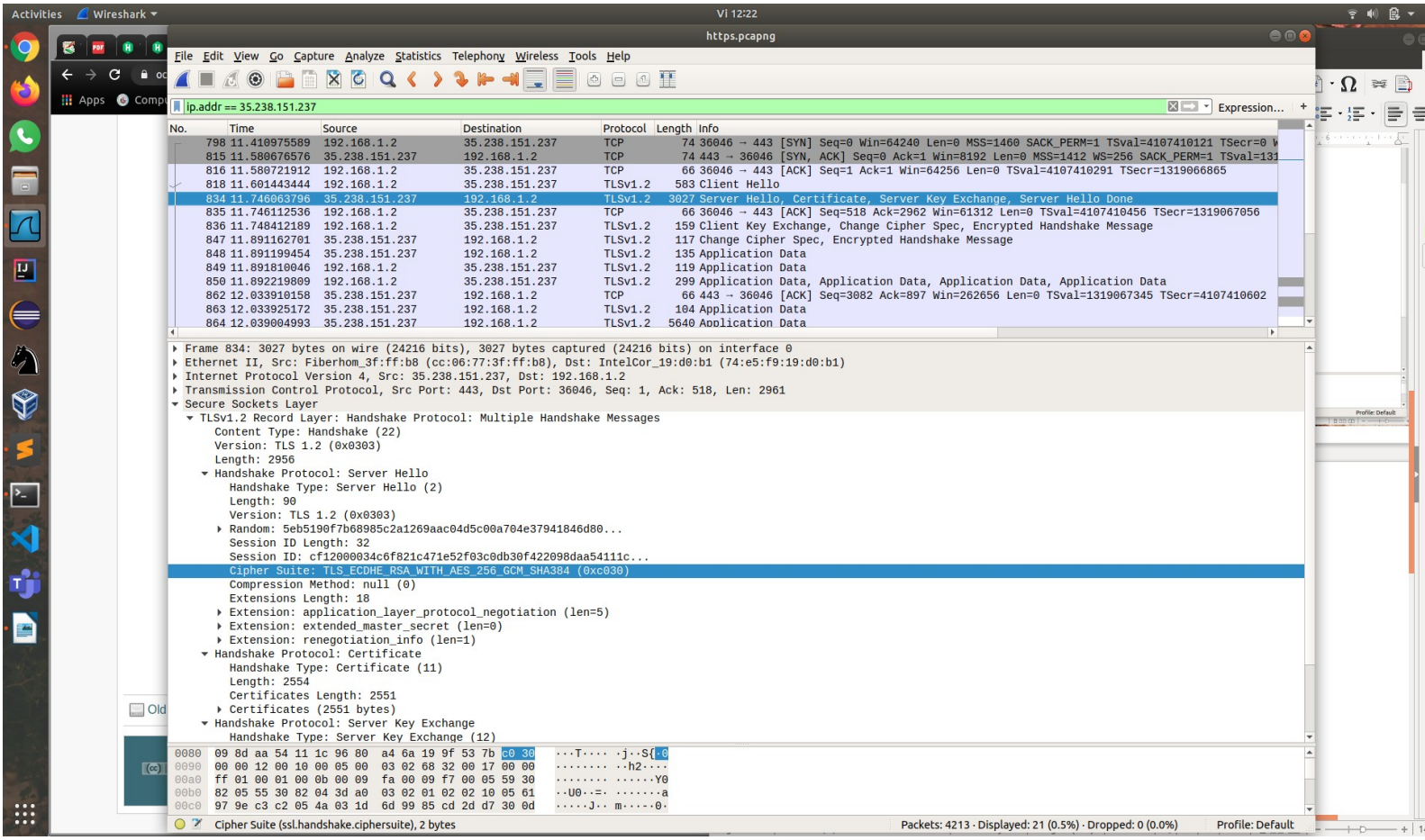
2. Am atasat http.pcapng. (comanda folosita:
curl -vvv http://login.onlineplanservice.com/Login.aspx?ReturnUrl=%2f)
Informatiile disponibile in captura de trafic arata ca http surprinde si ce se trasmite de la server, si ce se transmite de la client. La https nu se mai poate vedea mesajul de la http deoarece este encriptat. (la https sunt mai multe mesaje decat la http).

3. Comanda folosita: **curl -vvv https://login.onlineplanservice.com/Login.aspx?ReturnUrl=%2f**

Informatii identificate din wireshark:
-versiunea de tls folosita: **TLS 1.2**
-suitele de cifruri (cipher suits) suportate de client:



-suita aleasa de server:
Identificata prin campul ‘**Cipher Suite**’ in captura de mai jos.



Am atasat captura **https.pcapng.**

4. Am atasat captura ssh.pcapng.
Comandafolosita. *ssh* *andreea.horovei@fep.grid.pub.ro*.