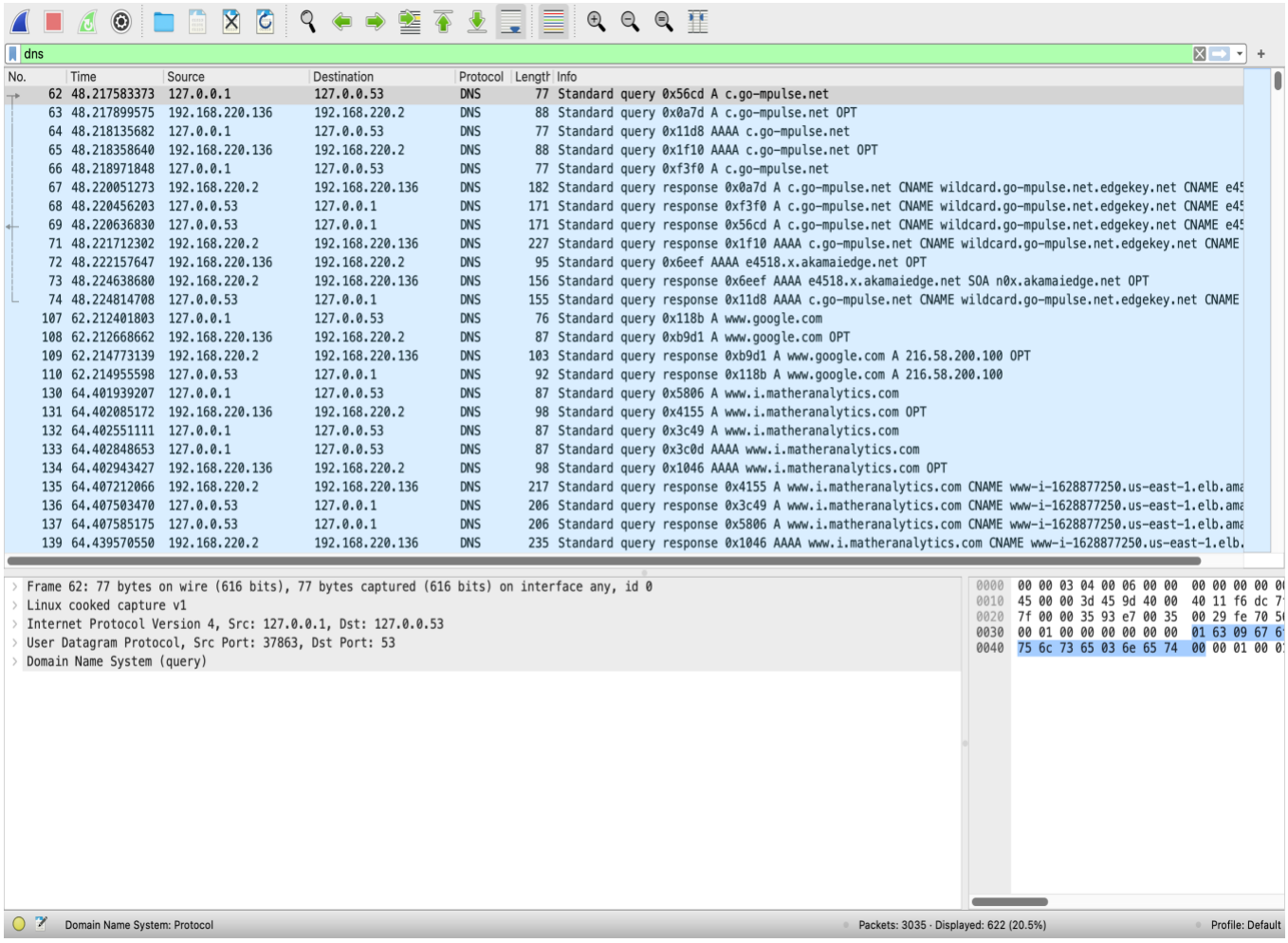
greenthom – 300536064

Lab 3 – CYBR171

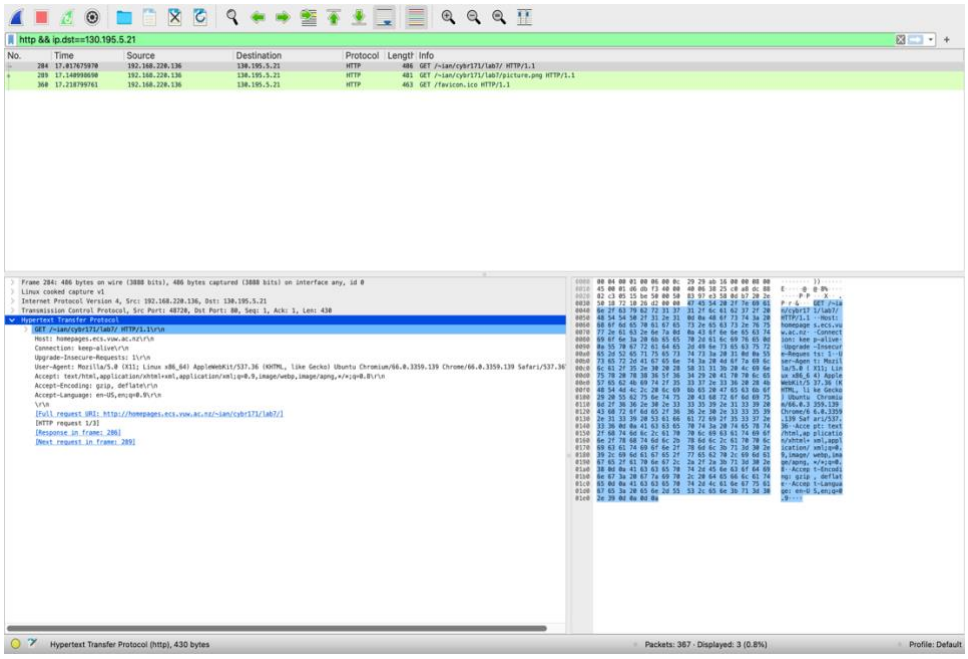
Task 2: Finding Domain Name Lookups

Applied filter for DNS traffic. Can see where human addresses become IP addresses, even if it has HTTPS encryption.

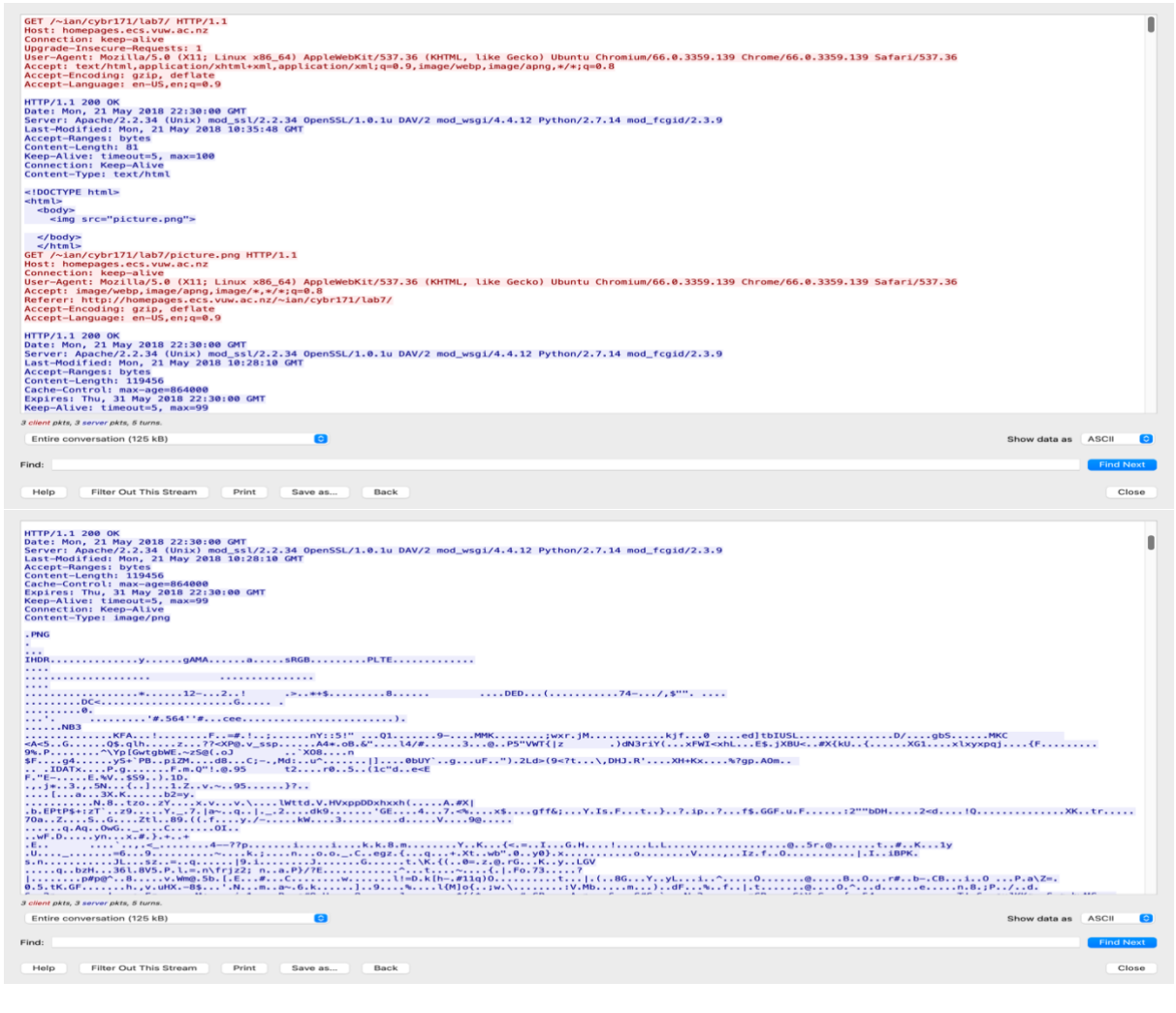


Task 3: Finding Web Traffic and inspecting it

See results for destination IP. Used command: “http && ip.dst == 130.195.5.21”

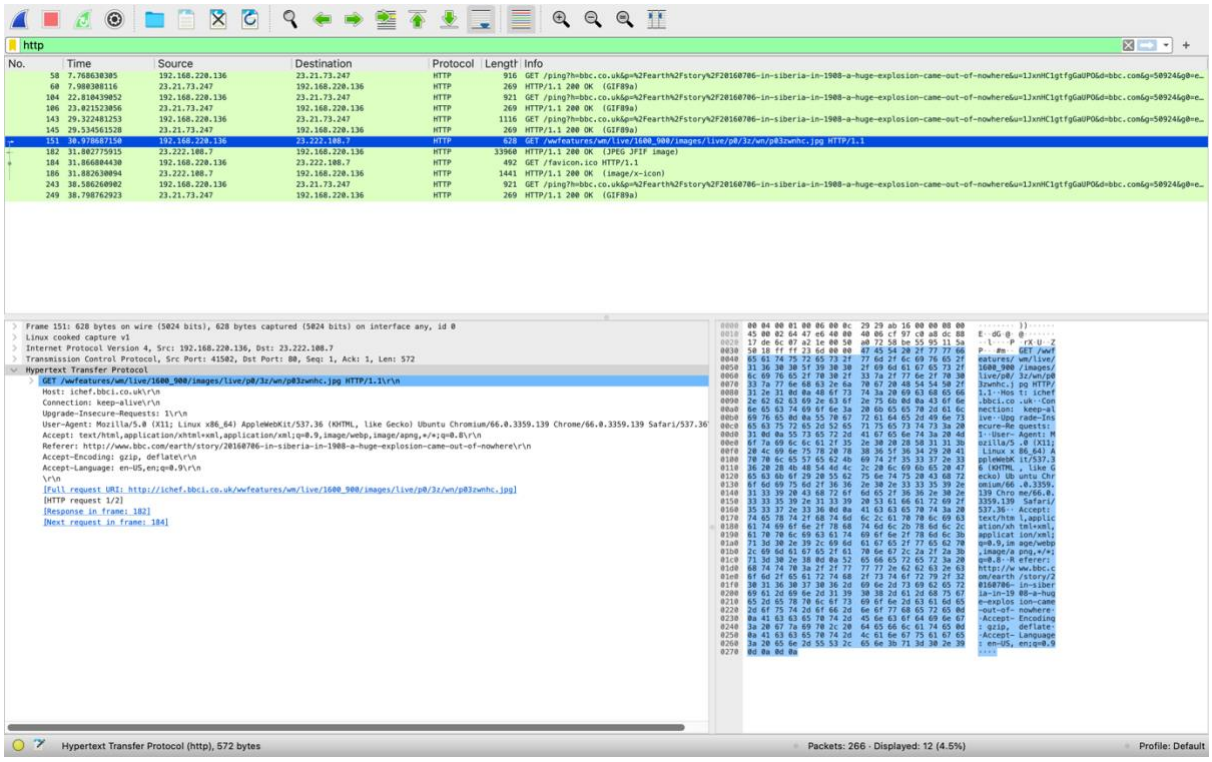


Here we can see the result of following HTTP stream-unencrypted and we can see the HTTP stream between the client and web server:

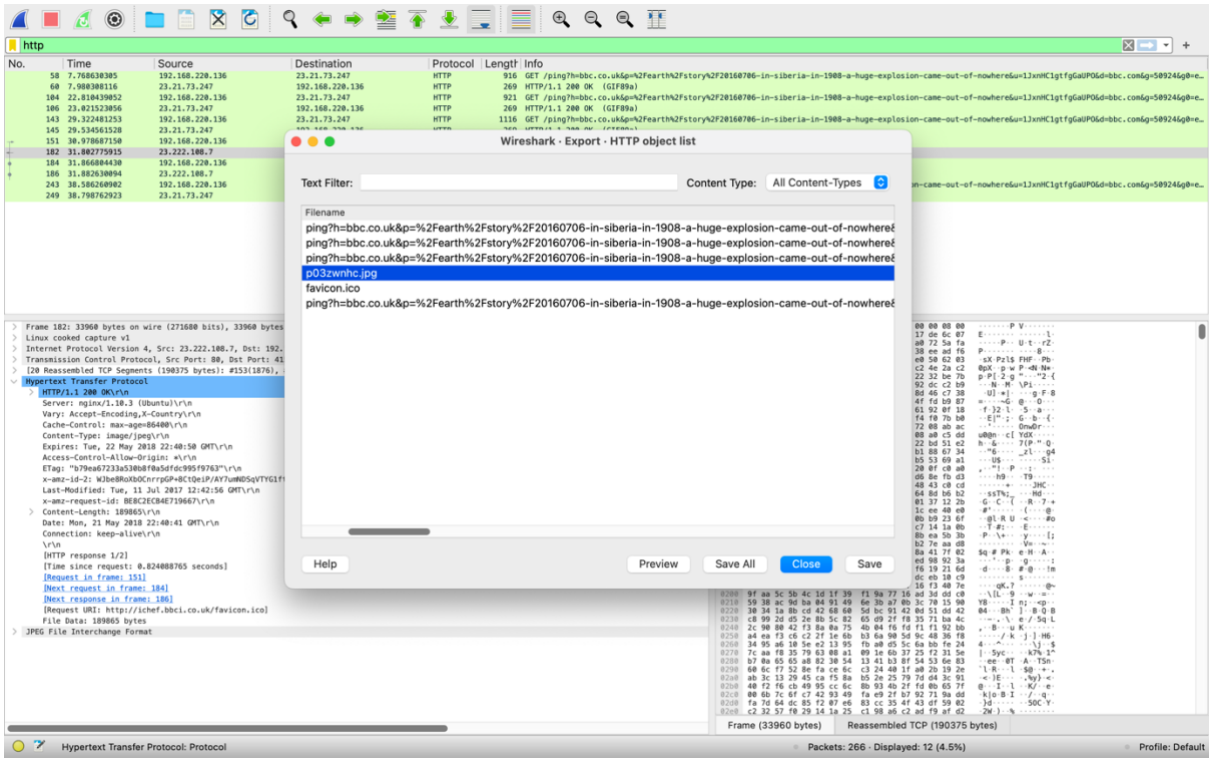


Task 4: Extracting HTTP objects from a stream:

Export HTTP Object: Can see JPG to extract by looking through HTTP



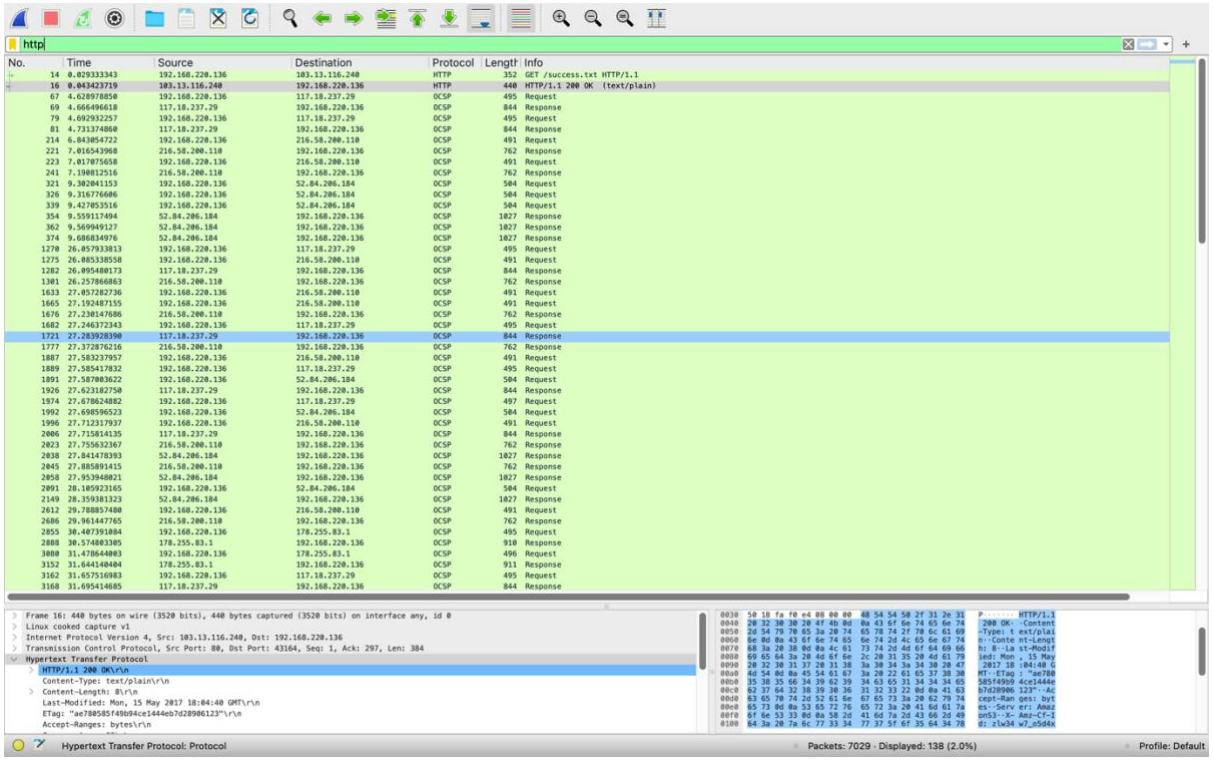
Export HTTP objects to create HTTP objects list – Preview: p03zwnhc.jpg



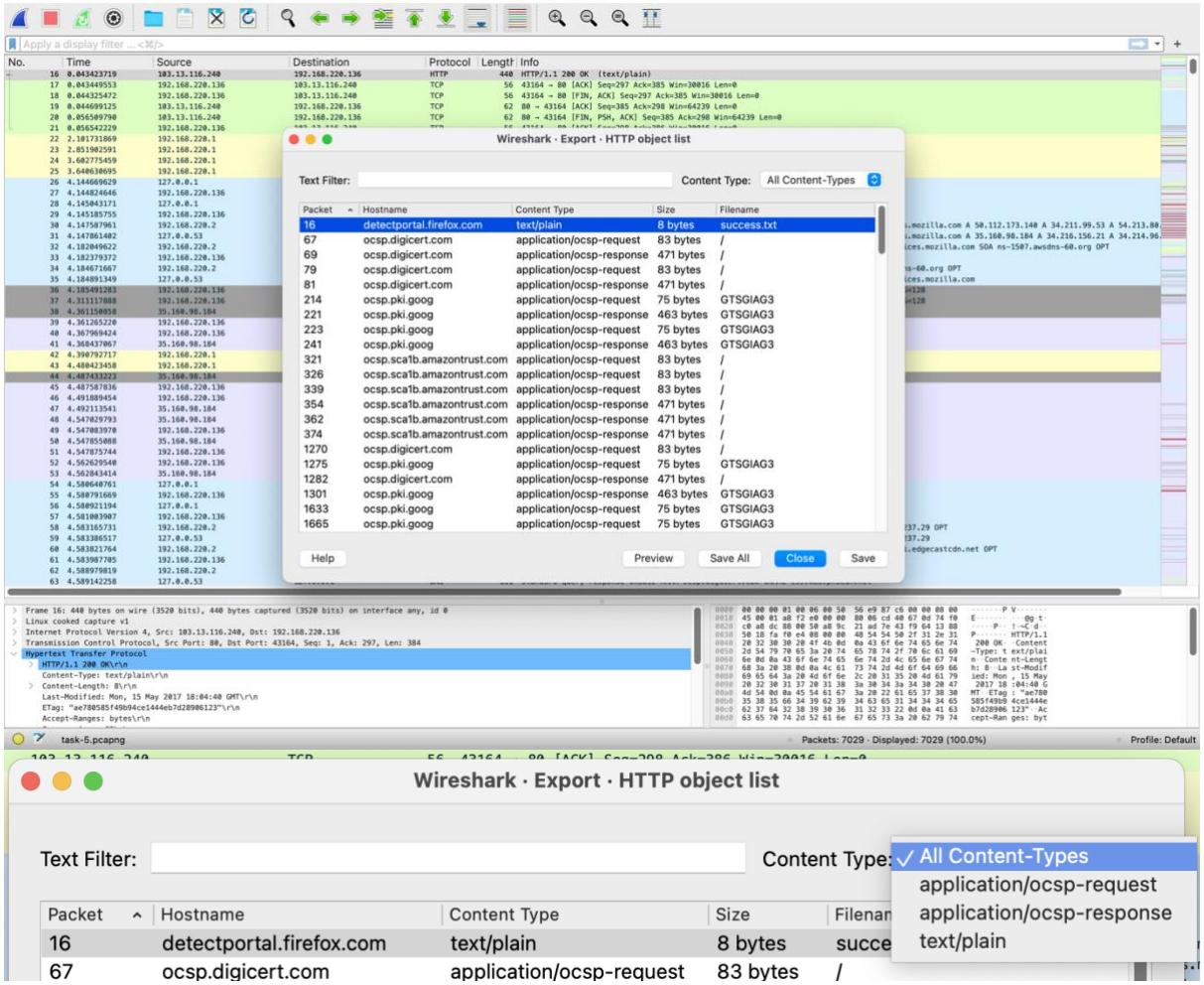
Preview of HTTP object p03zwnhc.jpg:

Task 5: HTTPS to the rescue

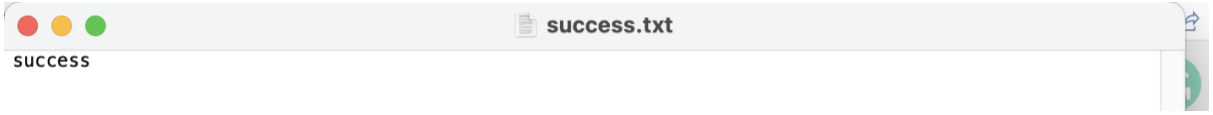
Looked through HTTP:



Attempting to export http objects:



As we can see that not much can be displayed which is likely to the objects are https encrypted compared to the objects in task number 4 where we could see all objects (e.g. jpg) as well as filenames. However here we can see there is only ocsp-requests and responses which are not readable and cannot be previewed(same thing!) apart from one .txt file (success). Here is the success.txt file.



Looking through https through entering command ‘tcp.port == 443’ , the number for the https traffic is encrypted and therefore we cannot identify much information as we already knew from trying to export the objects.