



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

IIC2333 — Sistemas Operativos y Redes

Tarea 3 – Respuesta Pregunta a

1. Según el user-agent registrado: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/69.0.3497.100 Safari/537.36, en mi caso **Chrome/69.0.3497.100**.
2. Se transfieren en **TCP**.
3. Para cada uno de los accesos, fue 200. Nota: navegador estaba en modo incógnito.
4. La dirección fue **http://192.168.1.9:3000/comando/ultra/secreto/germy.jpg**
5. Fueron paquetes con formato TCP de tipo **audio/mpeg**. Son múltiples porque el archivo debe dividirse de cierta manera para poder transferirse.
6.
 - (a) */register*: 456 bytes captured.
 - (b) */*: 768 bytes captured.
 - (c) */*: 847 bytes captured.
 - (d) */big.txt*: 775 bytes captured.
 - (e) *http://192.168.1.9:3000/comando/ultra/secreto/win98.mp3*: 779 bytes captured.
 - (f) */meme*: 772 bytes captured.
 - (g) */power*: 773 bytes captured.
7.
 - (a) */register*: 15 GETs de los distintos recursos, contando el GET inicial.
 - (b) */*: 16 GETs de los distintos recursos, contando el GET inicial.
 - (c) */*: 1 GET, porque el contenido ya estaba en cache, sin embargo no aparecieron los requests con estado 200 (cache) o 304 en la captura.
 - (d) */big.txt*: 1 GET, solo 1 recurso.
 - (e) *http://192.168.1.9:3000/comando/ultra/secreto/win98.mp3*: 1 GET, solo un recurso.
 - (f) */meme*: 3 GET incluyendo el inicial, porque hay 2 imágenes, lo que significa 2 GETs.
 - (g) */power*: 1 GET, solo 1 recurso.
8. Las imagenes se descargan de manera paralela, puesto que no se espera a que el servidor responda para hacer el request de la otra imagen.
9. Se utiliza el método **HTTP GET** porque es un listado en donde no se modifica nada en el lado del servidor, aparte de ser más liviano que un POST por ejemplo, que también pudiese haber sido usado, pero no estaría bien utilizado de acuerdo a los estandares. En el caso de */power* no mucho, pero en el caso de */register* sí, puesto que los parametros de GET estarían expuestos en la URL, para que otros pudiesen verlos si es que están observando la red.



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

IIC2333 — Sistemas Operativos y Redes

Tarea 3 – Respuesta Pregunta b

- /register: 80 segmentos.
 - /: 86 segmentos.
 - /: 14 segmentos (70 en cache).
 - /big.txt:
 - http://192.168.1.9:3000/comando/ultra/secreto/win98.mp3:
 - /meme: 115 segmentos.
 - /power: 5 segmentos.
- /register: [2, 26] segmentos.
 - /: [2, 23] segmentos.
 - /: [14,14] segmentos.
 - /big.txt:
 - http://192.168.1.9:3000/comando/ultra/secreto/win98.mp3:
 - /meme: [4, 56] segmentos.
 - /power: [5,5] segmentos.
- Duplicates: 130, con el filtro *tcp.analysis.duplicate_ack*.
 - Damaged: 50, con *_ws.expert.severity == error*
 - Lost: 9, con el filtro *tcp.analysis.lost_segment*
- Se puede apreciar un handshake en la siguiente secuencia:

No.	Time	Source	Destination	Protocol	Length	Info
501	19.287753	192.168.1.142	192.168.1.9	TCP	78	60724 → 3000 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TSval=195865153 TSecr=0 SACK_PERM=1
502	19.288389	192.168.1.9	192.168.1.142	TCP	78	3000 → 60724 [SYN, ACK, ECN] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=32 TSval=1012413193 TSecr=195865153 SACK_PERM=1
503	19.288365	192.168.1.142	192.168.1.9	TCP	66	60724 → 3000 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=195865153 TSecr=1012413193

A esto se le llama *three-way (or 3-step) handshake*. Primero se manda un SYN al server, en donde Seq=0, luego el server responde con Seq=0 y Ack=1, lo que significa que recibió la llamada del cliente, luego el cliente manda al server Seq=1 y Ack=1, finalizando el handshake.



PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE
ESCUELA DE INGENIERÍA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACIÓN

IIC2333 — Sistemas Operativos y Redes

Tarea 3 – Respuesta Pregunta c

1. La lista está en el archivo *list.csv*.
2. Podría pasar si es que se le hace ping a una IP en esa subnet que no existe, por lo que no tendrá información relacionada. Cuando tráfico llega al router para esa IP, un paquete ARP es difundido en la 2da capa, si no hay respuesta, la dirección IP aparece como unresolved y si hay una respuesta, entonces se mapea la IP con la MAC correspondiente en la tabla ARP.

3. Le hice ping a **192.168.1.117**, lo que arrojó:

```
26546 817.109546 Apple_9b:8a:79 Sony_ba:04:92 ARP 42 192.168.1.142 is at 68:5b:35:9b:8a:79
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Apple_9b:8a:79 (68:5b:35:9b:8a:79)
  Sender IP address: 192.168.1.142
  Target MAC address: Sony_ba:04:92 (54:53:ed:ba:04:92)
  Target IP address: 192.168.1.117
```

Por lo que la MAC del target fue **54:53:ed:ba:04:92**.