Práctica/Laboratorio de TCP

Para la captura dada analizar con el siguiente cuestionario utilizando una herramienta como wireshark.

1. Cuántos intentos de conexiones TCP hay en la captura?
2. Cuales son la fuente y el destino (IP:port) para c/u?
3. Cuántos conexiones TCP exitosas hay en la captura? Cómo se identifican las exitosas de las no exitosas, que flags se encuentran en estas?

   Dada la primera exitosa responder:

4. Quién inicia la conexión, quien sería el servidor y quién el cliente? Qué flags se ven activados? En que segmentos se ve el 3-way hand-shake?
5. Qué ISNs se intercambian?
6. Qué opciones se negocian. Qué significa c/u? Cuál es el MTU negociado?
7. Quién es el que envía la mayor cantidad de datos (IP:port)?
8. Identificar primer segmento de datos (origen, destino, tiempo, número de fila y número de secuencia TCP).
   a) Cuántos datos lleva?
   b) Cúando es confirmado (tiempo, número de fila y número de secuencia TCP)?
   c) La confirmación, qué cantidad de bytes confirma ?
9. Control de Flujo:
   a) Se activa en algún momento el mecanismo de control de lujo?
   b) Indicar donde (tiempo, número de fila y número de secuencia TCP) y a que se debe?
   c) Cuánto tiempo parece durar?
   d) Cuál es el numero de ventana que desactiva el mismo?
   e) Qué otros datos se pueden obtener?

10. Control de Congestión:
    a) Se encuentra en la red indicios de congestión?
    b) Cómo se detectan?, Indicar un número de segmento perdido.
    c) En que momento se ve la primera retransmisión (tiempo y número en el analizador)?
    d) Cuántos segmentos se re-transmiten?
11. Quién inicia el cierre de la conexión? Qué flags se utilizan? En que segmentos se ve esta (tiempo, número de fila y número de secuencia TCP) ?
12. El RTT entre que valores oscila?
13. El BW digital alcanzado, cual parece ser?
14. Qué otros datos puede obtener de la captura sobre el flujo analizado?