

Universidad Simón Bolívar Departamento de Computación y Tecnología de la Información Redes de Computadores (CI-4835)

TALLER DE TRABAJO EN CASA#2

RECURSOS REQUERIDOS: Para la ejecución de esta práctica el estudiante deberá disponer un PC ejecutando Wireshark®. Recuerde además que desde Windows® y a través de una aplicación portable de 32 bits, puede instalar y ejecutar Wireshark desde un dispositivo USB (wiki.wireshark.org/WiresharkPortable). Si usa un teléfono inteligente con Android®, se sugiere disponer de TCPDUMP para la captura de datos (www.androidtcpdump.com).

LAPSO DE ENTREGA: Expira el miércoles 1 de Noviembre a las 00:00am

MODALIDAD: Trabajo en grupos de 2 personas.

ACTIVIDADES A REALIZAR:

Parte 1: Captura de datos. Realice algunas conexiones de tráfico de datos desde un dispositivo electrónico con conexión a la Internet y capture datos que contengan al menos 30 segundos secuenciales de tráfico. Repita la operación a la misma hora y trate de replicar las mismas interacciones y servicios, por al menos 3 días consecutivos. Cada una de las capturas deberá quedar grabada en un archivo distinto bajo el formato "cap". Utilice las opciones (Statistics | Protocol Hierarchy) para identificar un sumario de protocolos y aplicaciones durante las capturas similar al de la Figura 0. Documente su proceso.

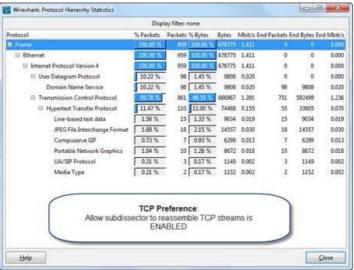


Figura 0: Protocolos y aplicaciones en una traza de captura

Parte 2: Identificando las demoras de tiempo entre paquetes. Realice alguna operación de descarga de archivo(s) de algún sitio en la red público y a bajo condiciones que le parezcan de alta competición en solicitudes. Configure la aplicación de monitorización del tráfico de la red, para que muestre el transcurso del tiempo desde la llegada del primer paquete. Para ello puede usar las opciones de: (View | Time Display Format | Seconds since Previous Displayed Packet). Una posible muestra de cómo lucen ordenados los paquetes por una columna de retrasos de tiempo se muestra en la Figura 1.

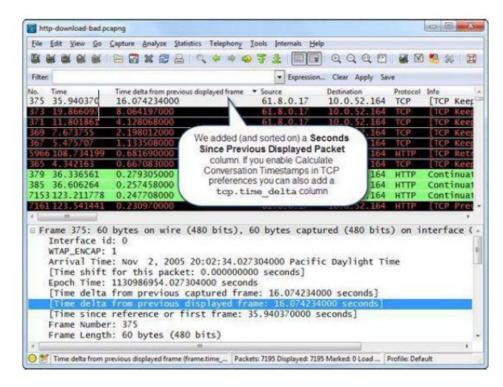


Figura 1: Tráfico ordenado por la columna de Tiempo Delta

La Figura 1 ilustra que después de procesar el paquete 365, los paquetes secuenciales del 367 al 375 llegan con retrasos de 1,2,4, y 8 segundos. Se observa de ese modo un incremento de retrasos con tendencia exponencial. Se desea que usted pruebe varias veces y con mayor lapso de duración, para que pueda identificar algún patrón notable de retrasos o un patrón de regularidad entre el tiempo de procesamiento de captura de cada paquete. Documente su hallazgo.

<u>Parte 3: Mayor conversación lógica.</u> Con base a los archivos obtenidos en la Parte 1, y usando las opciones (Statistics | Conversations) determine las entidades lógicas que más se comunicaron. Documente su hallazgo y preséntelo en modo semejante al que indica la Figura 2.

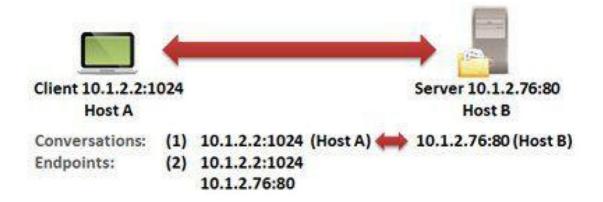


Figura 2: Conversación con mayor intercambio de tráfico en la red

<u>Parte 4: Informe de resultados.</u> Con base a los resultados obtenidos en las parte 1,2 y 3, elabore en grupo, un informe técnico de resultados de las experiencias y entréguelo a su profesor para ser evaluado. Explique allí la disposición y estructura de sus equipos y sistemas, su configuración y el procedimiento seguido. Si deduce alguna conclusión o si consulta algún material bibliográfico, agregue ello en secciones específicas.

MTS / Oct 2017