Redes Informáticas
Laboratorio No. 5

Integrantes: Ana Díaz
Richard González
John Villareal
Carlos Robles
Adrián Concepción

En los grupos de laboratorio, conteste cada una de las situaciones:

1. Verifique quienes son los ISP en nuestro país.
   A. InterFast Panamá
   B. Ovnicom
   C. C. MásMóvil
   D. D. Tigo / Cable onda

2. Enumere seis tecnologías de acceso. Clasifíquelas como de acceso residencial, acceso empresarial o acceso inalámbrico de área extensa.
   - FTTH / FTTP — Fibra hasta el hogar (Fiber-to-the-Home / Fiber-to-thePremises)
     Clasificación: Acceso residencial (también empresarial cuando se ofrecen SLA/pares dedicados).
   - HFC / Cable coaxial (Hybrid Fiber-Coaxial) Clasificación: Acceso residencial (también comercial en algunos casos). DSL (ADSL/VDSL) sobre par de cobre.
     Clasificación: Acceso residencial (zonas con infraestructura de cobre, menor rendimiento).
   - FWA — Fixed Wireless Access (4G LTE / 5G para hogar / CPE)
     Clasificación: Acceso inalámbrico de área extensa (puede ser residencial o empresarial según el servicio).
   - WISP / Wireless punto a punto / microondas (proveedores locales)
     Clasificación: Acceso inalámbrico de área extensa (muy usado en zonas rurales y montañosas).
   - Satélite (VSAT; constelaciones LEO tipo Starlink / OneWeb)
     Clasificación: Acceso inalámbrico de área extensa (ideal en lugares sin infraestructura terrestre).

3. Enumere las tecnologías de acceso residencial disponibles en nuestra provincia. Para cada tipo de acceso, detalle la velocidad de descarga ofrecida, la velocidad de carga y el precio mensual.
   A) Fibra óptica (FTTH) — proveedores: Tigo,Claro,Digicel, otros
      Velocidades típicas anunciadas: 100 Mbps — 1,000 Mbps (1 Gbps) descarga.
      Velocidad de subida: desde 10–15 Mbps en planes intermedios; planes superiores y promociones ofrecen simétricos (100/100 hasta 1000/1000).

Tigo anuncia hasta 750–1000 Mbps y Claro promociona hasta 1,000 Mbps simétricos en sus materiales.

Precio mensual (rango observado en el mercado panameño/urbano): aproximadamente $25–$90 USD/mes para planes residenciales (100–500 Mbps típicos); planes de 1 Gbps o bundles pueden estar por encima de $60–$120 según promoción y TV incluida.

Fuentes locales muestran paquetes urbanos competitivos (ej.: guías y comparadores).

B) Cable coaxial HFC (antes Cable Onda,ahora parte de algunos paquetes comerciales)
Velocidades típicas: 50–500 Mbps de bajada (según paquete y overbooking).
Subida: usualmente asimétrica (ej. 10–30 Mbps).
Precio: similar al rango fibra para niveles medios; promociones varían ampliamente ($30–$90+). (nota: muchos operadores están migrando HFC a FTTH).

C) FixedWireless para hogar (FWA — 4G/5G Home) — operadores móviles (Tigo,Claro,Digicel)
Velocidades: en áreas urbanas típicamente 50–200 Mbps en 4G/5G; en mejores ubicaciones 200–500 Mbps (5G FWA). Mapas de cobertura móvil muestran buena cobertura 4G/5G en David.
Subida: variable, típicamente 10–50 Mbps según tecnología.
Precio mensual: paquetes de “Internet hogar inalámbrico” suelen estar en $20–$60 USD/mes según datos incluidos y velocidad.

D) WISPs locales / Internetinalámbrico punto-a-multipunto (Planet Telecom y otros operadores regionales)
Velocidades ofrecidas (ejemplos locales): varía mucho; hay planes muy bajos para zonas remotas (1–5 Mbps) y paquetes mejores en áreas semiurbanas (10–50 Mbps). Planet Telecom publica paquetes y cobertura para muchas localidades de Chiriquí. Ejemplo histórico de tarifas publicadas por Planet Telecom (tarifas antiguas/indicativas): 1 Mb $85/mes, 3 Mb $99/mes — esas cifras muestran cómo el acceso inalámbrico rural puede ser más caro por Mbps; precios reales actuales pueden ser distintos tras actualización.
Subida: muchas veces asimétrica y menor que la bajada (ej. 50% de bajada).
Precio: suele ser más alto por Mbps en áreas remotas; rangos muy amplios — desde $30 por paquetes modestos hasta $150+ en enlaces dedicados o zonas muy aisladas.

E) ADSL/VDSL (par de cobre) — todavía presente en algunas zonas
Velocidades: 1–20/30 Mbps típicos para ADSL/VDSL.
Subida: baja (1–5 Mbps).
Precio: generalmente barato pero cada vez menos ofrecido donde hay fibra; típicamente por debajo de $30/mes si aún está comercializado.

F) Satélite / VSAT / Starlink (opciones para áreas sin cobertura)
Velocidades: Starlink y VSAT comerciales pueden ofrecer 25–200+ Mbps con mayor latencia; Starlink típicamente 50–200 Mbps en muchas ubicaciones.
Subida: variable (10–40 Mbps típicos).
Precio: más alto que tierra: instalación + equipo (antena/terminal) y $70– $150+/mes según proveedor y plan. (datos generales de mercado y guías de expatriados en Panamá).

4. Describa las tecnologías de acceso inalámbrico a Internet más populares hoy día. Compárelas e indique sus diferencias.
   A. 4G LTE / LTE-Advanced (FWA)
      Qué es: accesos fijos que usan la red móvil 4G con un CPE (router) en la casa.
      Pros: despliegue rápido, buena cobertura urbana y periurbana, coste de instalación bajo.
      Contras: velocidades y latencia dependen de congestión celular y distancia a la BTS; asimetría y límites de datos en algunos planes.
   B. 5G FWA (FixedWireless Access sobre 5G)
      Qué es: usa 5G para llevar banda ancha fija a hogares (CPE 5G).
      Pros: puede acercarse o competir con fibra en velocidad (200–1000 Mbps), despliegue más barato que tirar fibra.
      Contras: cobertura inicialmente limitada a núcleos urbanos; rendimiento muy dependiente de espectro y densidad de estaciones.
   C. WISP (PMP en bandas licenciadas/no lic.) — microondas / enlaces punto-a-multipunto.
      Qué es: proveedores locales que instalan torres y antenas direccionales para llevar Internet a poblaciones rurales o colinas.
      Pros: acceso donde no llega fibra, relativamente rápido de desplegar para zonas montañosas (útil en Chiriquí).
      Contras: sensibilidad al trazado (obstáculos), variabilidad por clima, menor simetría y a veces precios por Mbps mayores. Planet Telecom es ejemplo local.
   D. Satélite (GEO/V-SAT y constelaciones LEO tipo Starlink)
      Qué es: enlace vía satélite para cubrir lugares sin infraestructura terrestre.
      Pros: cobertura casi global; LEO (Starlink) ofrece latencias y velocidades mejores que satélite GEO tradicional.
      Contras: coste de equipo e instalación, latencia variable (GEO mucho mayor), precio mensual generalmente alto.

Capture pantallas con la ejecución de este.

Segunda Parte: Aprendizaje del manejo del analizador Wireshark

Wireshark es un programa que, ejecutado en un sistema final, es capaz de capturar todo el tráfico de red recibido o enviado por dicho sistema. Es una herramienta de gran utilidad, pues no sólo captura el tráfico sino que además es capaz de analizarlo, mostrando al usuario información detallada de los protocolos de cada uno de los niveles (desde el nivel de enlace de datos hasta el nivel de aplicación). Es por ello que recibe el nombre de analizador de protocolos. Es una herramienta muy completa y compleja, por lo que vamos a centrarnos en el manejo básico de la interfaz de la misma y a la vez utilizar algunos comandos y opciones fundamentales para el trabajo habitual con esta herramienta.

Arranque el analizador de protocolos Wireshark

1. Wireshark es capaz de utilizar los servicios de DNS para, en sus diversas ventanas, mostrarnos siempre nombres de host y dominio, en lugar de mostrarnos las direcciones IP equivalentes, en el formato numérico xxx.xxx.xxx.xxx habitual. Esa característica nos será de mucha utilidad en esta práctica. Entre en "Edit" → "Preferences", pulse "Name Resolution" en el panel de la izquierda, active la opción "Resolve Network (IP) addresses". Wireshark también es capaz de mostrarnos, en lugar de los números de puerto TCP y UDP, el nombre del protocolo que usa habitualmente dicho número de puerto.

2. En esta práctica concreta no nos interesa habilitar esta funcionalidad de Wireshark. Entre en "Edit" →"Preferences", pulse "Name Resolution" en el panel de la izquierda, desactive la opción "Resolve Transport Name" y pulse "OK" para cerrar la ventana y que tengan efecto los cambios.

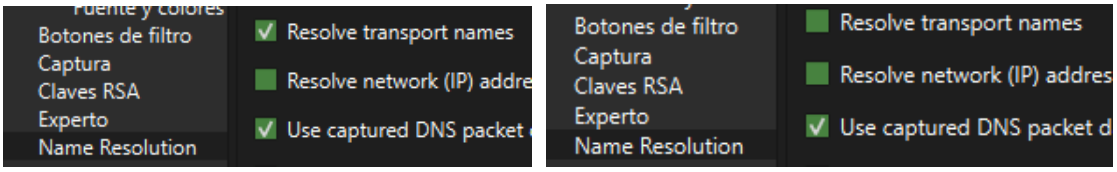


Figura 1: Configuración de la visualización de los nombres de dominio

3. Haga que Wireshark comience a capturar el tráfico que entra y sale de su conexión de red

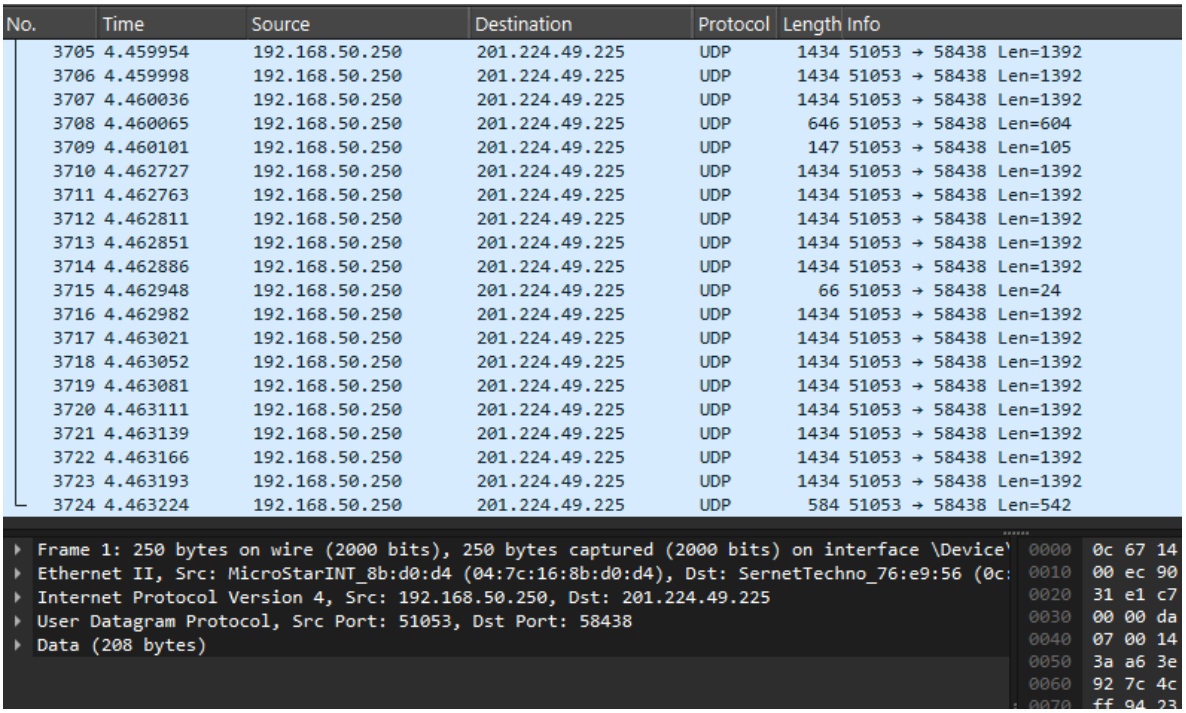
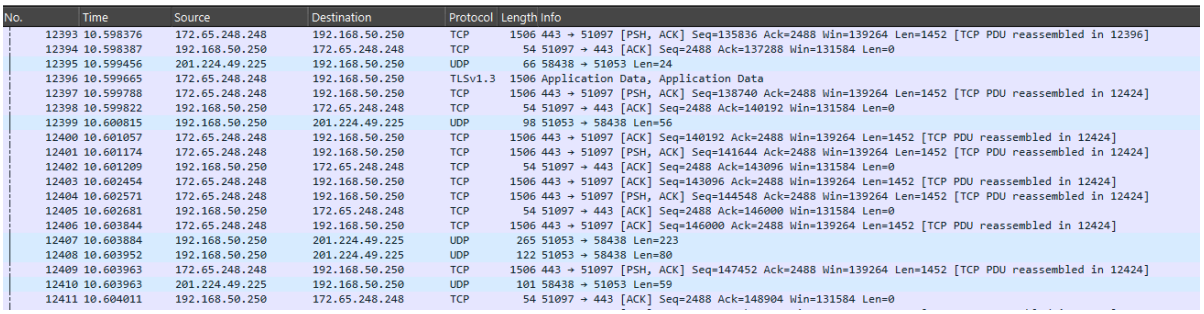


Figura 2: Análisis inicial en Wireshark

4. Genere tráfico de red abriendo el navegador y visitando alguna página web.



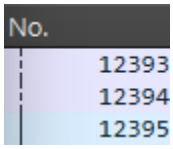
No.	Time	Source	Destination	Protocol	Length	Info
12393	10.598376	172.65.248.248	192.168.50.250	TCP	1506	443 → 51097 [PSH, ACK] Seq=135836 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12396]
12394	10.598387	192.168.50.250	172.65.248.248	TCP	54	51097 → 443 [ACK] Seq=2488 Ack=137288 Win=131584 Len=0
12395	10.599456	201.224.49.225	192.168.50.250	UDP	66	58438 → 51053 Len=24
12396	10.599665	172.65.248.248	192.168.50.250	TLSv1.3	1506	Application Data, Application Data
12397	10.599788	172.65.248.248	192.168.50.250	TCP	1506	443 → 51097 [PSH, ACK] Seq=138740 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12424]
12398	10.599822	192.168.50.250	172.65.248.248	TCP	54	51097 → 443 [ACK] Seq=2488 Ack=140192 Win=131584 Len=0
12399	10.600815	192.168.50.250	201.224.49.225	UDP	98	51053 → 58438 Len=56
12400	10.601057	172.65.248.248	192.168.50.250	TCP	1506	443 → 51097 [ACK] Seq=140192 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12424]
12401	10.601174	172.65.248.248	192.168.50.250	TCP	1506	443 → 51097 [PSH, ACK] Seq=141644 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12424]
12402	10.601209	192.168.50.250	172.65.248.248	TCP	54	51097 → 443 [ACK] Seq=2488 Ack=143096 Win=131584 Len=0
12403	10.602454	172.65.248.248	192.168.50.250	TCP	1506	443 → 51097 [ACK] Seq=143096 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12424]
12404	10.602571	172.65.248.248	192.168.50.250	TCP	1506	443 → 51097 [PSH, ACK] Seq=144548 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12424]
12405	10.602681	192.168.50.250	172.65.248.248	TCP	54	51097 → 443 [ACK] Seq=2488 Ack=146000 Win=131584 Len=0
12406	10.603844	172.65.248.248	192.168.50.250	TCP	1506	443 → 51097 [ACK] Seq=146000 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12424]
12407	10.603884	192.168.50.250	201.224.49.225	UDP	265	51053 → 58438 Len=223
12408	10.603952	192.168.50.250	201.224.49.225	UDP	122	51053 → 58438 Len=80
12409	10.603963	172.65.248.248	192.168.50.250	TCP	1506	443 → 51097 [PSH, ACK] Seq=147452 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12424]
12410	10.603963	201.224.49.225	192.168.50.250	UDP	101	58438 → 51053 Len=59
12411	10.604011	192.168.50.250	172.65.248.248	TCP	54	51097 → 443 [ACK] Seq=2488 Ack=148904 Win=131584 Len=0

Figura 3: Tráfico en la red después de haber entrado a una página web

5. Podrá ver que Wireshark le muestra en el panel superior de su ventana principal las tramas que ha capturado, fruto del tráfico de datos entre el cliente y el servidor web. Detenga la captura de tráfico cuando observe que la carga de la página anterior ha terminado.

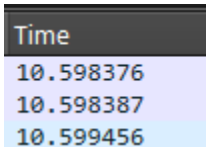
6. Como ya sabe de la primera práctica, en el listado de tramas podemos ver mucha información de cada trama, organizada en columnas, las que aparecen por defecto son:

a) La primera columna se llama "No." y nos muestra el número de orden en el que se han ido capturando las tramas, de la 1 a la N.



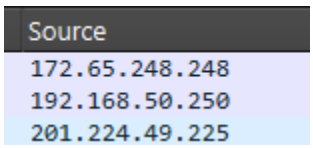
No.
12393
12394
12395

b) La segunda columna se llama "Time" y en ella Wireshark nos muestra, en segundos, información temporal del instante en que fue capturada esa trama. Por defecto este tiempo se mide desde el instante en que se capturó la primera trama, por lo que en la trama número 1 es 0.000000.



Time
10.598376
10.598387
10.599456

c) La columna "Source" muestra información del equipo que envió la trama (o el que envió alguna PDU encapsulada en dicha trama, depende de cómo hayamos configurado Wireshark).



Source
172.65.248.248
192.168.50.250
201.224.49.225

d) La columna "Destination" es análoga a la anterior, mostrándonos información del equipo destino.

Destination
192.168.50.250
172.65.248.248
192.168.50.250

f)) La columna "Protocol" muestra información de protocolo de más alto nivel encapsulado en esa trama y que Wireshark es capaz de analizar.

Destination
192.168.50.250
172.65.248.248
192.168.50.250

g) La columna "Length" muestra el número de bytes de la trama. En la última sesión de laboratorio se verá qué campos de la trama (E_PDU) incluye.

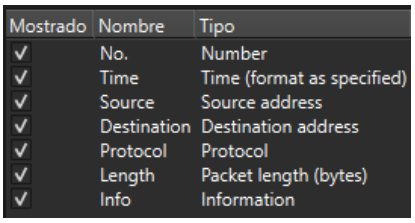
Length
1506
54
66

h) La columna "info" muestra información resumida del protocolo de más alto nivel que Wireshark es capaz de analizar en esa trama.

Length	Info
1506	443 → 51097 [PSH, ACK] Seq=135836 Ack=2488 Win=139264 Len=1452 [TCP PDU reassembled in 12396]
54	51097 → 443 [ACK] Seq=2488 Ack=137288 Win=131584 Len=0
66	58438 → 51053 Len=24

7. Es posible quitar y añadir columnas de información al listado de tramas, para adaptarlo a nuestras necesidades en cada momento. En esta práctica será necesario añadir dos nuevas columnas que nos presenten información de los puertos de origen y de destino de las T_PDU de los protocolos TCP y UDP. Con esto podremos identificar el número de puerto usado para identificar al proceso de aplicación cliente y servidor en una trama que encapsule protocolos hasta el nivel de aplicación. Para hacerlo debe seguir estas instrucciones:

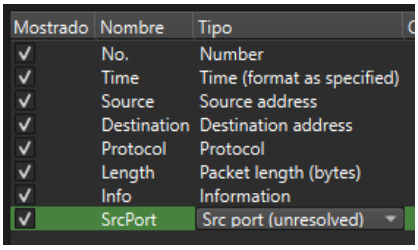
a) Entre en "Edit" → "Preferences", y pulse en la rama "Columns" (dentro de "User Interface" en el panel de la izquierda).



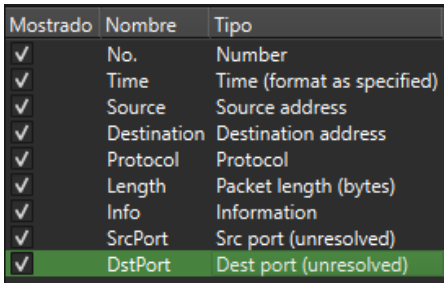
b) Pulse el botón "Add" una vez para añadir una nueva columna.

c) Haga "clic" en el texto "New column" que ha aparecido, y editelo escribiendo como título de la nueva columna el texto "SrcPort" y pulsando "Intro" en el teclado.

d) En el campo "Field Type" debe seleccionar de la lista desplegable el valor "Src Port (unresolved).

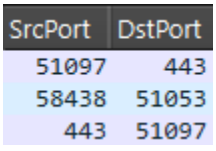


e) Repita los pasos b), c) y d) para crear otra columna con título "DstPort" y que tenga "Dest Port (unresolved)" de "Field Type".



f) Pulse "OK" para cerrar la ventana "Preferences".

g) Observe que en el listado de tramas aparecen las dos nuevas columnas, en la parte de la derecha (si no puede verla ve desplácese hacia la derecha). Utilice el ratón para reordenar las columnas y colocar las dos nuevas delante de la columna “Info” o bien ajuste el ancho de la columna "Info" para que se muestren todas ellas en pantalla sin tener que de desplazarse.



SrcPort	DstPort
51097	443
58438	51053
443	51097

8. Como ya sabe, la ventana principal de Wireshark está dividida en tres paneles. Ya hemos repasado el panel superior, el listado de tramas. Los otros dos paneles están muy relacionados con el panel superior, pues nos muestran información de la trama que hayamos seleccionado en el listado de tramas.

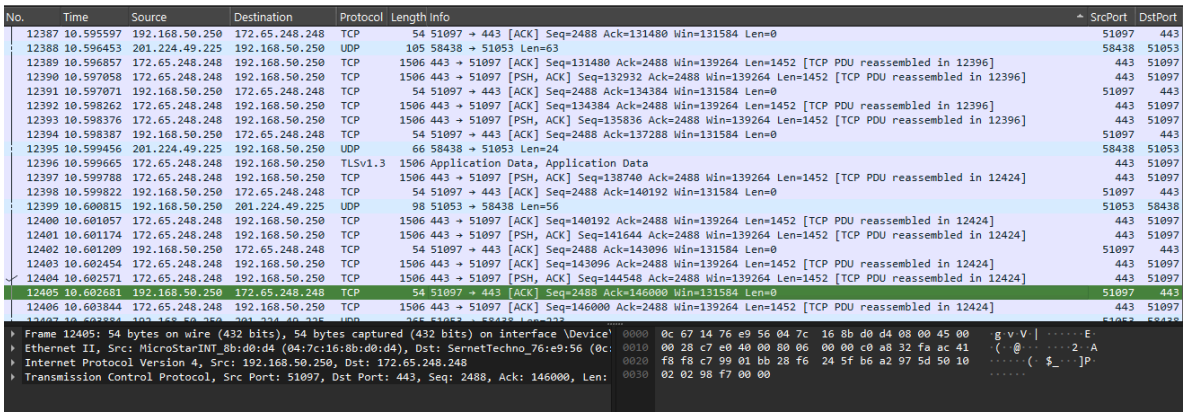
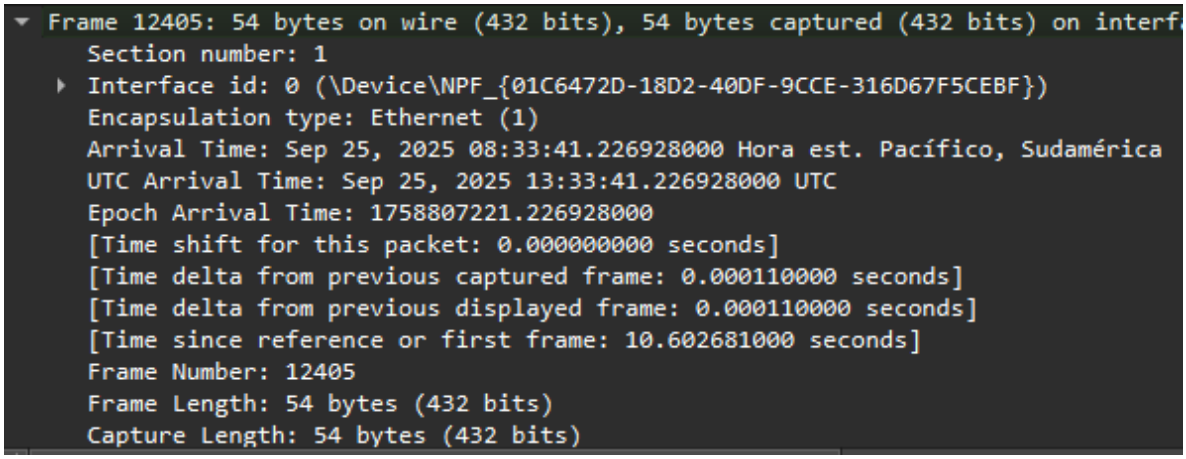


Figura 4: Vista de los 3 paneles de Wireshark

9. El panel central, "detalles de la trama", muestra diversa información de la trama y de su contenido, de forma ordenada y estructurada por niveles. En primer lugar se muestra información de la trama completa y luego se va mostrando información de cada uno de los niveles, empezando desde el nivel de enlace, a continuación red, transporte y aplicación (si es que aparecen todos, cosa que no siempre ocurre). En cada línea hay un "+" a la izquierda para desplegar la información del protocolo asociada a cada nivel (una vez interpretada por la herramienta). No toda la información que aparece de un determinado protocolo forma realmente parte de dicho protocolo. A veces Wireshark añade información que ha determinado como resultado de un análisis que ha realizado a nivel global, en cuyo caso esta información aparece entre corchetes [ ].



Por otro lado, tampoco todo lo que aparece detrás de un "+" es necesariamente un protocolo. Por ejemplo, Wireshark es capaz de analizar diferentes formatos de ficheros como GIF, PNG, JPG, etc. y los muestra a la derecha de un "+". Seleccione con el ratón una trama que en la columna "protocol" muestre HTTP y fíjese en los nombres de los protocolos que aparecen en el panel central.

Espere a que acabe la carga y detenga la captura en Wireshark . Nótese que pulsando F5 en Firefox también se recarga la página actual como si se pulsase sobre el icono de la flecha enroscada.

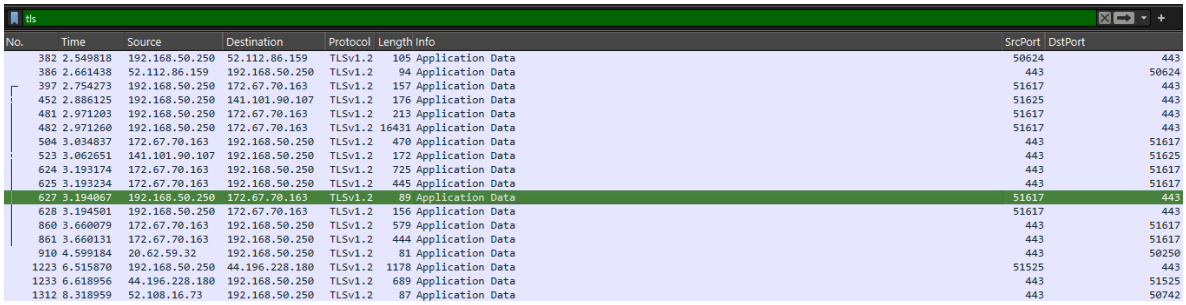


Figura 5: Protocolo tls, equivalente a https, utilizado en la mayoría de navegadores modernos

10. El panel inferior, "bytes de la trama", muestra un volcado en hexadecimal y en ASCII del contenido de la trama seleccionada. Los datos en hexadecimal (en la parte izquierda) se presentan en filas de 16 bytes, junto con una primera columna que indica la posición relativa (dentro de la trama) del primer octeto de la fila. Si en el panel central se hace "clic" en alguno de los niveles (o en algún campo dentro de estos) se resaltan con fondo oscuro en el panel inferior los bytes asociados a aquello sobre lo que hemos hecho "clic". Al revés también funciona, pulsando sobre bytes del panel inferior y viendo en el panel central cómo se selecciona el campo de información correspondiente. Haga "clic" en "detalles de trama" en "Hipertext Transfer Protocol" para seleccionar el protocolo HTTP. ¿Qué información aparece en ASCII en "bytes de tramas"? Pulse sobre el "+" que aparece al lado de "Hipertext Transfer Protocol" en "detalles de trama", observará el contenido de la HTTP_PDU. Haga "clic" varias veces en diferentes líneas de cabecera y observe como se ve en ASCII esa información. ¿Cómo se muestra en ASCII los códigos de control '\r' y '\n"?

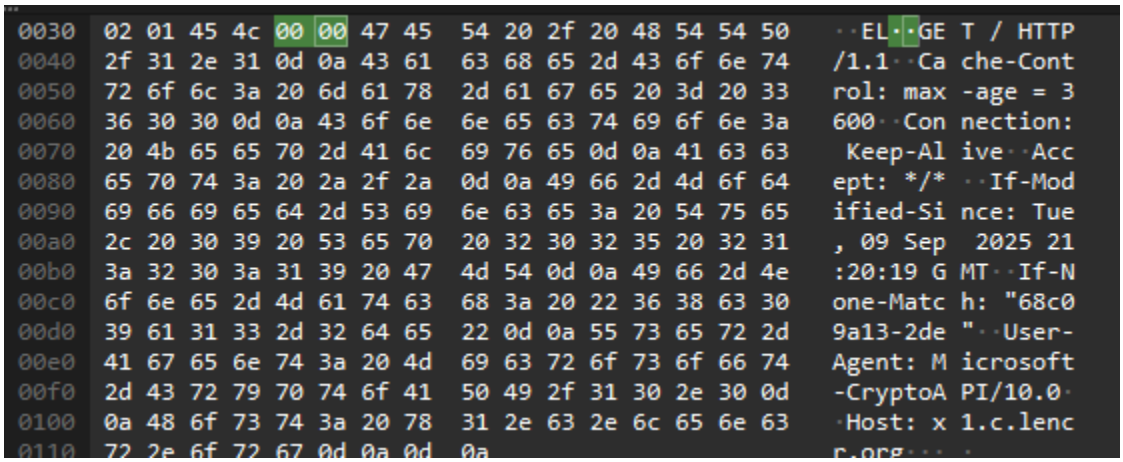


Figura 6: los códigos de control se muestran como puntos

11. Como sabe, el contenido mostrado en el listado de tramas puede ser guardado en un archivo (entrando en File → Save o haciendo clic en), el cual puede ser cargado en cualquier otro momento (entrando en File → Open o haciendo clic en). Esto le puede ser de gran utilidad si le faltase tiempo para completar esta práctica, pues podría llevarse la captura a su casa y acabar allí la parte del estudio experimental que no haya podido terminar.

Respecto a las marcas de tiempo, mostradas en la columna "Time" del listado de tramas, la primera trama tiene por defecto la marca 0.000000 segundos y el resto de marcas van incrementándose respecto a esta.

No obstante, es posible establecer una marca de referencia en cualquier trama de forma que sea el "cero" para todas las tramas a continuación de ella, que verán su marca de tiempo modificado considerando esa referencia, lo cual es útil para medir tiempos entre tramas desde una primera que será la que tomemos como "referencia". Para ello seleccionamos la trama que queremos marcar como referencia con clicderecho y elegimos "Set Time Reference (Toggle)", apareciendo *REF* en esa trama y modificándose el tiempo de las tramas siguientes. Si repetimos la operación se quita la referencia de esa trama. Tenga en cuenta que puede haber varias "referencias locales" en el listado de tramas.

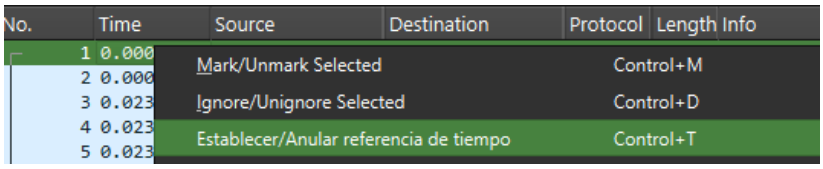
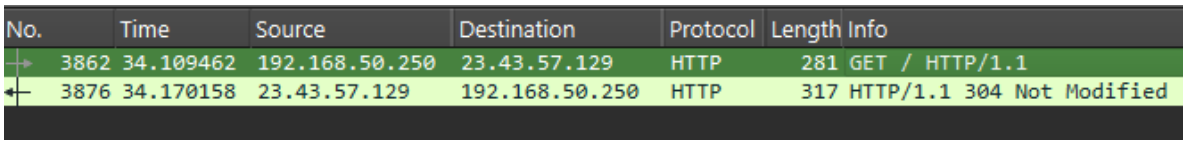


Figura 7: Estableciendo referencia de tiempo

12. Fíjese que en el listado de tramas hay varias tramas que contienen PDUs del protocolo HTTP (fíjese en el valor de la columna "Protocol"). Concretamente, debe encontrar una

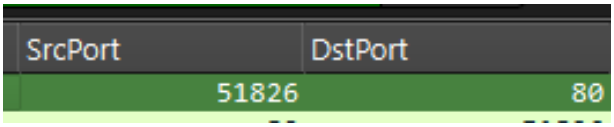
trama que muestre en la columna "Info" que contiene una petición GET del protocolo HTTP.



No.	Time	Source	Destination	Protocol	Length	Info
3862	34.109462	192.168.50.250	23.43.57.129	HTTP	281	GET / HTTP/1.1
3876	34.170158	23.43.57.129	192.168.50.250	HTTP	317	HTTP/1.1 304 Not Modified

Figura 8: Petición GET en el protocolo HTTP

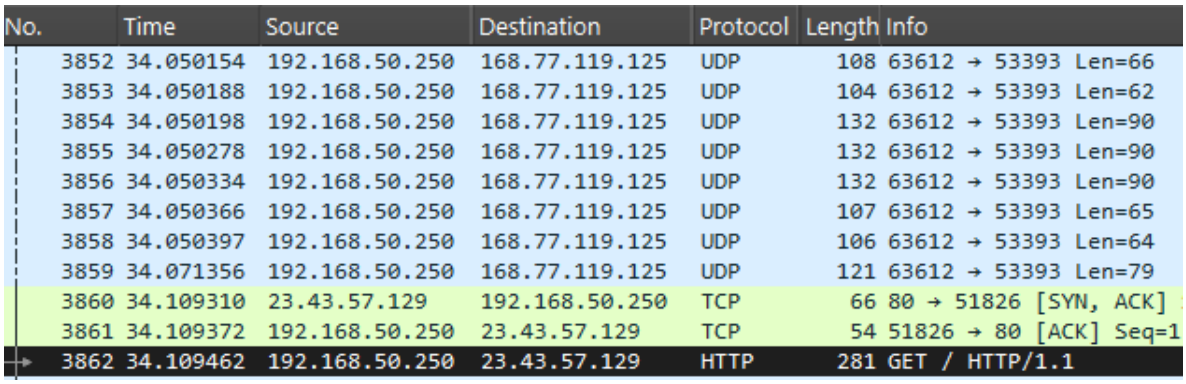
13. La petición GET la ha emitido el proceso cliente, que está asociado a un determinado puerto en el host origen ("source host"). Gracias a la columna SrcPort (puerto fuente o puerto origen) podemos averiguar con facilidad el número de puerto asociado al proceso cliente.



SrcPort	DstPort
51826	80

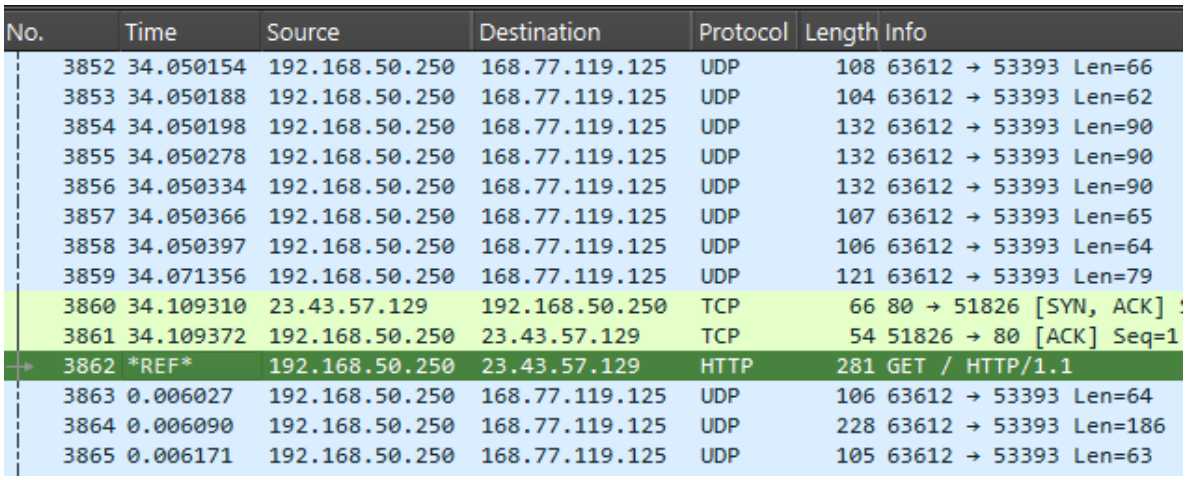
14. Compruebe que el valor numérico de la columna DstPort de la trama que encapsula el GET es el valor habitual usado por un proceso servidor del protocolo HTTP. Anótelo.

15. Ahora vamos a hacer que la trama con el GET pase a ser la "referencia temporal" con respecto a la cual medir los tiempos de captura de las tramas capturadas detrás de ella. Para ello seleccione dicha trama haciendo "clic" sobre ella con el botón derecho del ratón y seleccione en el menú contextual que le aparece la opción "Set Time Reference (Toggle)". Fíjese que ahora esa trama no tiene marca de tiempo en la columna "Time" sino que aparece el texto *REF*. Es posible anular esta operación repitiendo los mismos pasos que hemos dado sobre esa trama.



No.	Time	Source	Destination	Protocol	Length	Info
3852	34.050154	192.168.50.250	168.77.119.125	UDP	108	63612 → 53393 Len=66
3853	34.050188	192.168.50.250	168.77.119.125	UDP	104	63612 → 53393 Len=62
3854	34.050198	192.168.50.250	168.77.119.125	UDP	132	63612 → 53393 Len=90
3855	34.050278	192.168.50.250	168.77.119.125	UDP	132	63612 → 53393 Len=90
3856	34.050334	192.168.50.250	168.77.119.125	UDP	132	63612 → 53393 Len=90
3857	34.050366	192.168.50.250	168.77.119.125	UDP	107	63612 → 53393 Len=65
3858	34.050397	192.168.50.250	168.77.119.125	UDP	106	63612 → 53393 Len=64
3859	34.071356	192.168.50.250	168.77.119.125	UDP	121	63612 → 53393 Len=79
3860	34.109310	23.43.57.129	192.168.50.250	TCP	66	80 → 51826 [SYN, ACK]
3861	34.109372	192.168.50.250	23.43.57.129	TCP	54	51826 → 80 [ACK] Seq=1
3862	34.109462	192.168.50.250	23.43.57.129	HTTP	281	GET / HTTP/1.1

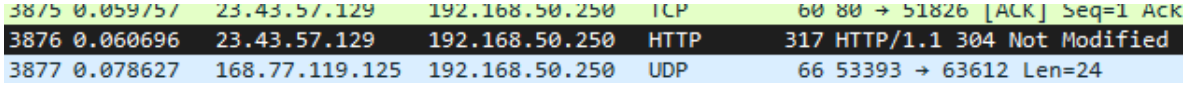
Figura 9: Antes de asignar la referencia de tiempo



No.	Time	Source	Destination	Protocol	Length	Info
3852	34.050154	192.168.50.250	168.77.119.125	UDP	108	63612 → 53393 Len=66
3853	34.050188	192.168.50.250	168.77.119.125	UDP	104	63612 → 53393 Len=62
3854	34.050198	192.168.50.250	168.77.119.125	UDP	132	63612 → 53393 Len=90
3855	34.050278	192.168.50.250	168.77.119.125	UDP	132	63612 → 53393 Len=90
3856	34.050334	192.168.50.250	168.77.119.125	UDP	132	63612 → 53393 Len=90
3857	34.050366	192.168.50.250	168.77.119.125	UDP	107	63612 → 53393 Len=65
3858	34.050397	192.168.50.250	168.77.119.125	UDP	106	63612 → 53393 Len=64
3859	34.071356	192.168.50.250	168.77.119.125	UDP	121	63612 → 53393 Len=79
3860	34.109310	23.43.57.129	192.168.50.250	TCP	66	80 → 51826 [SYN, ACK]
3861	34.109372	192.168.50.250	23.43.57.129	TCP	54	51826 → 80 [ACK] Seq=1
3862	*REF*	192.168.50.250	23.43.57.129	HTTP	281	GET / HTTP/1.1
3863	0.006027	192.168.50.250	168.77.119.125	UDP	106	63612 → 53393 Len=64
3864	0.006090	192.168.50.250	168.77.119.125	UDP	228	63612 → 53393 Len=186
3865	0.006171	192.168.50.250	168.77.119.125	UDP	105	63612 → 53393 Len=63

Figura 10: Después de asignar la referencia de tiempo

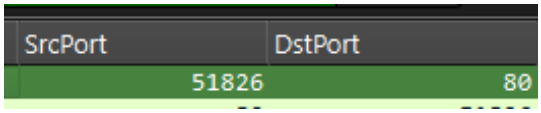
16. Localice, detrás de la trama del GET, una trama que encapsule la respuesta HTTP a dicho GET. En la columna "Info" de la respuesta debe aparecer la línea de estado "HTTP/1.1 200 OK" o bien la línea de estado "HTTP/1.1 304 Not modified", dependiendo de las circunstancias en que se generó el GET con Mozilla Firefox.



3875	0.059757	23.43.57.129	192.168.50.250	TCP	60	80 → 51826 [ACK] Seq=1 Ack
3876	0.060696	23.43.57.129	192.168.50.250	HTTP	317	HTTP/1.1 304 Not Modified
3877	0.078627	168.77.119.125	192.168.50.250	UDP	66	53393 → 63612 Len=24

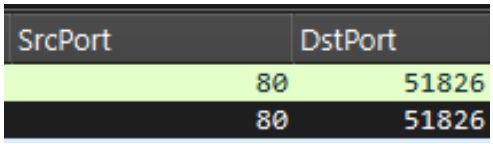
Figura 11: Respuesta del Get

17. Compruebe que en la respuesta se usan los mismos puertos que en la solicitud, pero puerto origen es ahora puerto destino y viceversa.



SrcPort	DstPort
51826	80

Figura 12: Puertos del GET



SrcPort	DstPort
80	51826
80	51826

Figura 13: Puertos de la respuesta

18. Compruebe que ocurre lo mismo con los valores de las columnas "Source" y "Destination".

No.	Time	Source	Destination	Protocol	Length	Info
3862	*REF*	192.168.50.250	23.43.57.129	HTTP	281	GET / HTTP/1.1
3876	0.060696	23.43.57.129	192.168.50.250	HTTP	317	HTTP/1.1 304 Not Modified

Figura 14: Comprobación de los valores de Source y Destination

19. Como hemos hecho que la trama del GET sea la referencia temporal de todas las tramas que le siguen, es muy fácil medir el tiempo transcurrido entre la emisión del GET y la recepción de la respuesta.

20. ¿Cuánto vale el RTT entre su PC y alguna página web?

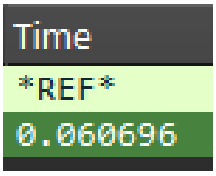
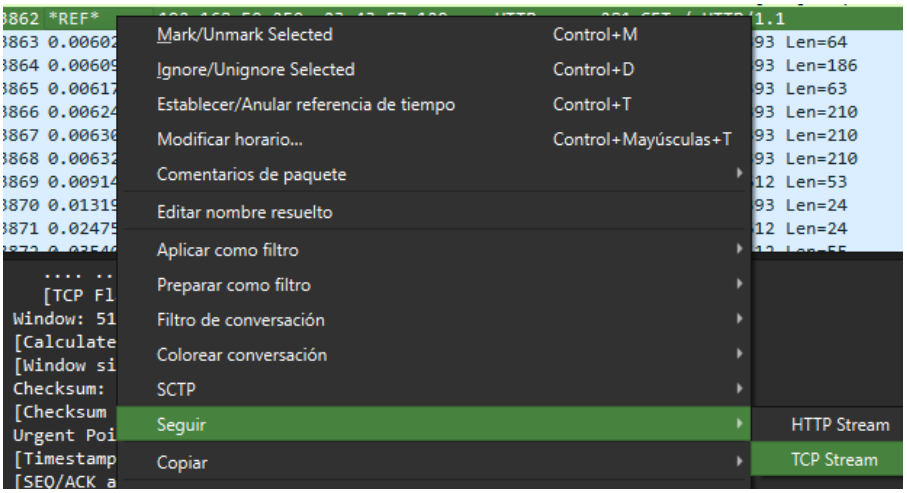


Figura 15: Tiempo de respuesta entre la pc y la página web

21. Wireshark es capaz de, a partir de una trama cualquiera que contenga una T_PDU del protocolo TCP (o UDP), localizar todas las demás T_PDU que se transmitieron en la misma conexión TCP que ella (o en el caso de UDP, las T_PDU entre el mismo cliente y servidor usando una determinada pareja de puertos UDP). Gracias a eso puede mostrarnos el flujo de bytes transmitidos a través de esa conexión TCP por los procesos cliente y servidor (o el intercambio de A_PDUs en el caso de UDP). Seleccione la trama del GET haciendo "clic" sobre ella con el botón derecho del ratón y seleccione en el menú contextual que le aparece la herramienta "Follow TCP Stream". (Nota: Para UDP sería "Follow UDP Stream")



22. En la ventana "Follow TCP Stream" podemos ver en color rosa los bytes enviados por el proceso cliente y de color morado los bytes enviado por el proceso servidor. Si el cliente y el servidor mantienen un diálogo "largo" a través de una misma conexión (como en las conexiones HTTP persistentes) podría verse como se van alternando los mensajes del cliente y del servidor.