

### REDES INGENIERÍA DE SISTEMAS

**Laboratorio 1 – Protocolos de la capa de Transporte y Aplicación**

### DOCENTES

### Edwin Ferney Castillo – [efcastillo@unicauca.edu.co](mailto:efcastillo@unicauca.edu.co)

### POPAYÁN 2024-1

### Contenido

**1 Contenido**

1. [Objetivos 3](#_bookmark0)
2. [Introducción 3](#_bookmark1)
3. [Reflexión inicial 4](#_bookmark2)
4. [Actividades a Realizar 5](#_bookmark3)
   1. [Actividad 1: Configuración de la computadora host del módulo para capturar protocolos](#_bookmark4) [de la capa de aplicación. 5](#_bookmark4)
   2. [Actividad 2: Captura y análisis de la comunicación HTTP entre la computadora host del](#_bookmark5) [módulo y un servidor Web. 6](#_bookmark5)
   3. [Actividad 3. Captura y análisis de la comunicación FTP entre la computadora host del](#_bookmark6) [módulo y un servidor Web. 9](#_bookmark6)
   4. [Actividad 4. Reflexión 14](#_bookmark7)
   5. [Actividad 5. Captura y análisis de la comunicación utilizando el cliente FTP Filezilla 14](#_bookmark8)
   6. [Actividad 6. Analizar los paquetes DNS (UDP) capturados 14](#_bookmark9)
5. [Entregables 16](#_bookmark10)
   1. [Informe 16](#_bookmark11)
   2. [Trazas de captura de Wireshark 17](#_bookmark12)
6. [Rúbrica de Evaluación: 17](#_bookmark13)
7. [Anexos 17](#_bookmark14)
8. [Material de Referencia 17](#_bookmark15)
9. [Referencias 17](#_bookmark16)

*Guía realizada por el docente Edwin Ferney Castillo (efcastillo@unicauca.edu.co)*

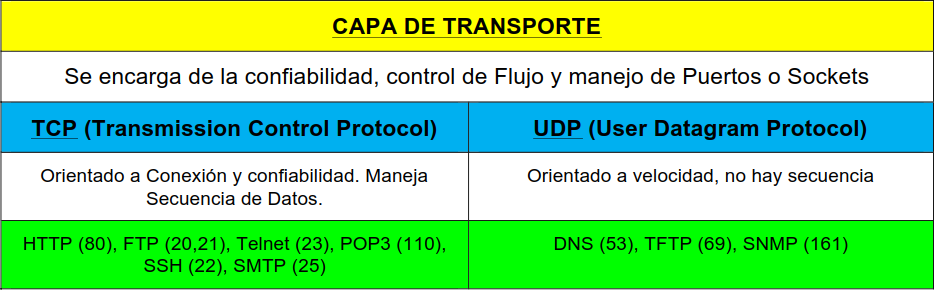
# Objetivos

Al completar esta práctica de laboratorio, usted podrá:

* Configurar la computadora host para capturar protocolos de la capa de aplicación.
* Capturar y analizar la comunicación HTTP entre la computadora host del módulo y un servidor Web.
* Capturar y analizar la comunicación FTP entre la computadora host del módulo y un servidor FTP.
* Observar los canales TCP para establecer y administrar la comunicación con conexiones HTTP y FTP.

# Introducción

La función principal de la capa de transporte es mantener un registro de las conversaciones de múltiples aplicaciones en el mismo host. Sin embargo, cada aplicación tiene determinados requisitos para sus datos y, por lo tanto, se han desarrollado diferentes protocolos de transporte para que cumplan con estos requisitos (ver tabla 1).



### Tabla 1. Características capa de transporte

Los protocolos de la capa de aplicación definen la comunicación entre servicios de red, como un servidor Web y un cliente y un servidor FTP y un cliente. Los clientes inician la comunicación con el servidor adecuado y el servidor responde al cliente. Para cada servicio de red existe un servidor determinado que escucha, en un puerto determinado, las conexiones del cliente. Puede haber diversos servidores en el mismo dispositivo final. Un usuario puede abrir diferentes aplicaciones del cliente para el mismo servidor, pero cada cliente se comunica, en forma exclusiva, con una sesión establecida entre el cliente y el servidor.

Los protocolos de la capa de aplicación se basan en los protocolos TCP/IP de menor nivel, como TCP o UDP. Esta práctica utiliza el analizador de protocolos **Wireshark1** para examinar **dos** protocolos populares de la capa de aplicación, HTTP y FTP, y la manera en que los protocolos de la capa de transporte, TCP y UDP, administran el canal de comunicación. También se examinan las solicitudes más comunes de los clientes y las correspondientes respuestas del servidor.

# Reflexión inicial

Los **protocolos de red** describen las funciones que se producen durante las comunicaciones de red. Los protocolos generalmente no describen cómo cumplir una función en particular. El protocolo describe solamente qué funciones se requieren de una regla de comunicación en particular, pero no cómo realizarlas, por ende, la implementación de un protocolo en particular es independiente de la tecnología.

En esta práctica de laboratorio se utilizarán las aplicaciones del cliente para conectarse a los servicios de red del servidor de la Universidad del Cauca. El estudiante monitorea la comunicación con Wireshark y analiza los paquetes capturados.

Se utiliza un explorador Web (Internet Explorer, Edge Explorer, Firefox o Google Chrome) para conectarse al servicio de red del servidor. El servidor de la Universidad del Cauca tiene varios servicios de red previamente configurados, como el HTTP, que esperan responder las solicitudes del cliente.

También se utilizará el explorador Web para examinar el protocolo FTP y el cliente de línea de comando FTP. El ejercicio demostrará que, aunque los clientes pueden diferir, la comunicación subyacente con el servidor sigue siendo la misma.

1 Wireshark provee la capacidad de capturar y mostrar todo el tráfico de red que entra y sale de la PC en la cual está instalado, a través de una **interfaz de red**. <https://www.wireshark.org/>

# Actividades a Realizar

## Actividad 1: Configuración de la computadora host del módulo para capturar protocolos de la capa de aplicación.

Nota importante: Para desarrollar la práctica de laboratorio se requiere conexión a internet.

### Paso 1. Descargar e instalar Wireshark

Si el software Wireshark no está instalado en la computadora host del módulo (anfitrión), puede descargarse desde la página oficial <https://www.wireshark.org/>. Vea la Figura 1. El URL de descarga es: <https://www.wireshark.org/#download>

|  |
| --- |
|  |
| **Figura 1. Página de descarga Wireshark** |

* + 1. Haga clic con el botón derecho del mouse sobre el nombre del archivo wireshark, teniendo en cuenta si su equipo es de 32 o 64 bits. Luego, guarde el archivo en la computadora host del módulo.
    2. Cuando el archivo se haya descargado, haga doble clic en el nombre del archivo e instale Wireshark con las configuraciones predeterminadas.
    3. Para entender más como funciona Wireshark puede utilizar el siguiente enlace: <https://www.youtube.com/watch?v=XYo5ADPrTYE>

### Paso 2. Iniciar Wireshark y configurar la interfaz de captura.

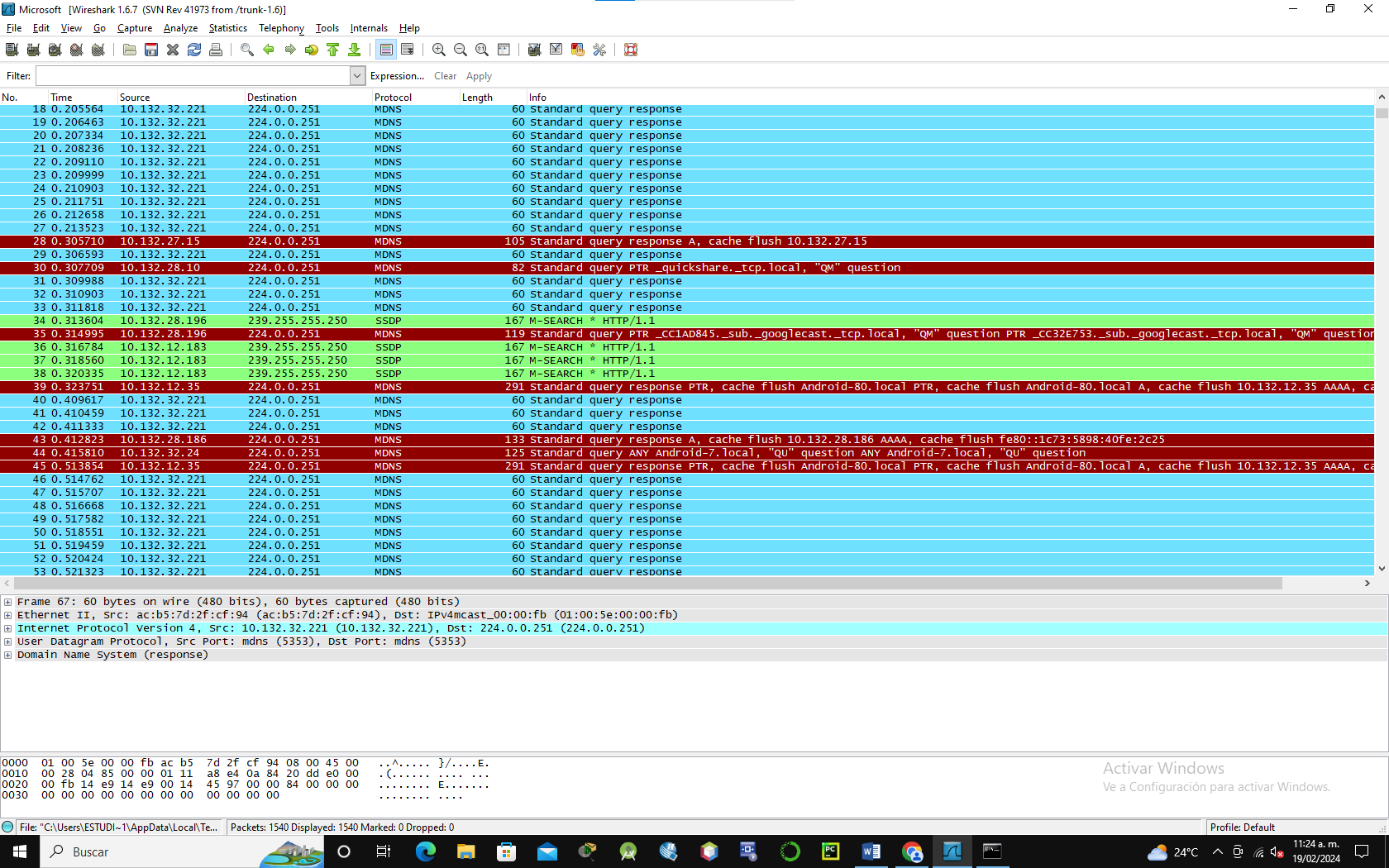
1. Inicie Wireshark desde Inicio > Todos los programas > Wireshark > Wireshark.
2. Cuando se muestra la ventana que se abre, establece la interfaz de captura correcta. La interfaz correcta es la interfaz con acceso a internet (Ethernet o wifi). Vea la Figura 2.

|  |
| --- |
|  |
| **Figura 2: Ventana de captura de interfaz de Wireshark** |

Wireshark puede iniciarse haciendo clic en el botón Inicio de la interfaz. Después, la interfaz se utiliza como predeterminada y no se necesita cambiar.

Wireshark debe comenzar a registrar datos.

1. Detenga Wireshark por ahora. Wireshark se utilizará en las siguientes actividades.



## Actividad 2: Captura y análisis de la comunicación HTTP entre la computadora host del módulo y un servidor Web.

HTTP es un protocolo de capa de aplicación que depende de los protocolos de menor nivel, como TCP, para establecer y administrar el canal de comunicación. Esta parte de la práctica de laboratorio demostrará cómo las sesiones entre múltiples clientes Web y el servidor Web se mantienen separadas.

### Paso 1. Iniciar las capturas de Wireshark.

Inicie una captura de Wireshark. Wireshark mostrará capturas basadas en el tipo de paquete. Para ello puede basarse en el video expuesto en la actividad anterior.

### Paso 2. Verificar direcciones IP del cliente y el servidor.

Para realizar esta tarea, utilice las utilidades de red vista en clase.

### Dirección IP cliente

### 

### 

### Dirección IP del servidor (Univirtual - Universidad del Cauca)

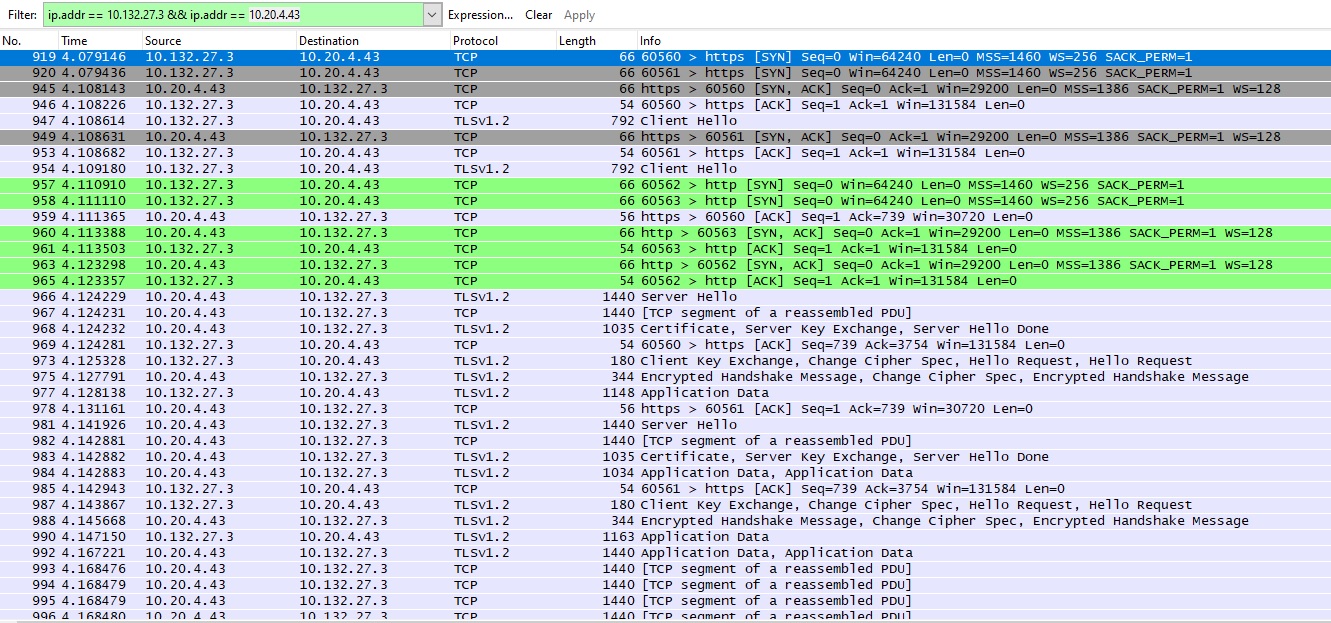
### 

### 

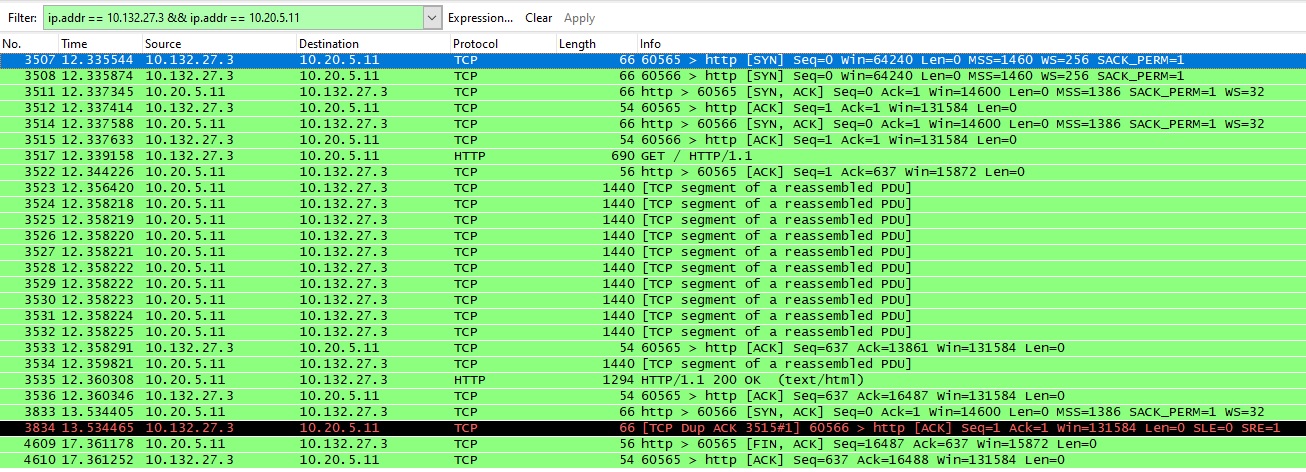
### http://192.168.128.2/redes/public/login

### Paso 3. Iniciar el explorador Web del host del módulo.

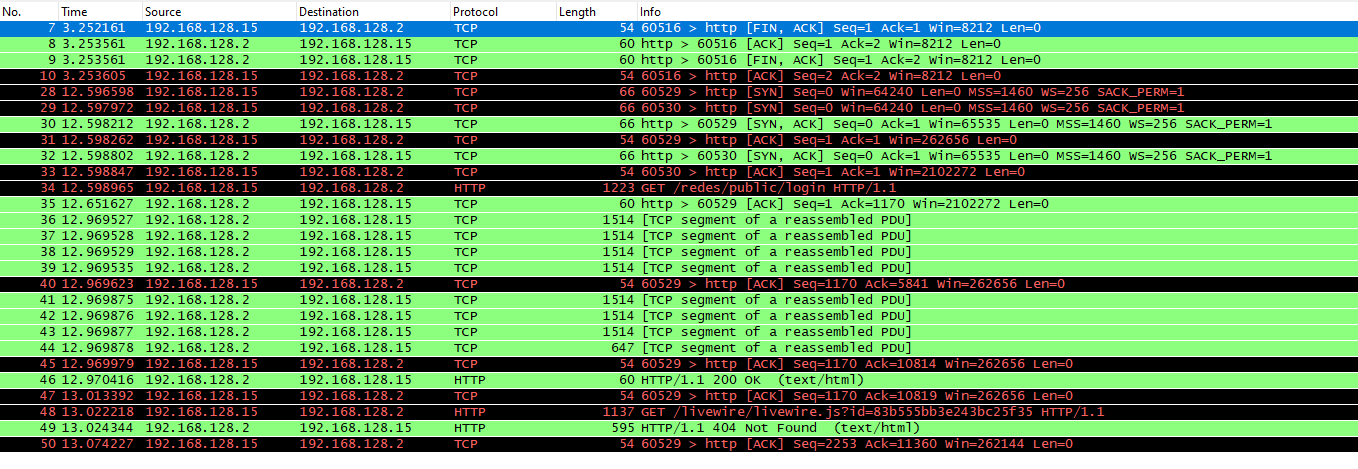
* + 1. Inicie las capturas de Wireshark.
    2. Con un explorador Web, de su elección, conéctese al URL <https://univirtual.unicauca.edu.co/>.
    3. Haga clic en el botón Actualizar del explorador Web. No debe haber cambios en la pantalla del cliente Web.



* + 1. Abra un segundo explorador Web y conéctese al URL <http://biblio.unicauca.edu.co/>. En la pantalla aparece una página Web diferente. No cierre ningún explorador hasta que la captura de Wireshark se detenga.



* + 1. Abra un tercer explorador Web y conéctese al servidor web local proporcionado por el docente encargado (ejemplo, http://ip\_del\_servidor/redes/public/login). En la pantalla aparece una página Web diferente.



* + 1. No cierre ningún explorador hasta que la captura de Wireshark se detenga.

### Paso 4. Detener las capturas de Wireshark y analizar los datos capturados.

1. Detenga las capturas de Wireshark.
2. Cierre los exploradores Web.

**Nota importante**: Se recomienda solo abrir en el explorador seleccionado las tres (3) URLs de la práctica con el fin de facilitar el análisis de los datos capturados.

Se muestran los datos Wireshark resultantes. En el paso 3, se crearon al menos cuatro (4) sesiones HTTP. Identifique cada una de estas sesiones con ayuda de Wireshark. Explicar y dejar evidencia.

Analice los datos HTTP capturados. Utilice los resultados de captura de Wireshark para responder las siguientes preguntas:

* 1. Complete la siguiente tabla con la información presentada en la sesión HTTP, hacer los mismo para el acceso a los tres servicios web:

|  |  |
| --- | --- |
| **Dirección IP del explorador Web (cliente)** |  |
| **Dirección IP del servidor Web** |  |
| **Protocolo de la capa de transporte (UDP/TCP)** |  |
| **Número de puerto del explorador Web** |  |
| **Número de puerto del servidor Web** |  |

* 1. ¿Qué computadora inició la sesión HTTP y cómo lo hizo?, responder la pregunta teniendo en cuenta la información teórica de los capítulos 1-4 del curso.
  2. En TCP se establecen las conexiones usando el protocolo de acuerdo a **tres vías** (three-way handshake), utilice los resultados de las capturas para evidenciar este proceso. Explique en detalle cada vía en cada caso (soporte la explicación con capturas de pantalla de la vía correspondiente).
  3. ¿Qué computadora señaló inicialmente un fin a la sesión HTTP y cómo lo hizo?, explicar y dejar evidencia.
  4. Resalte la primera línea del protocolo HTTP, una solicitud GET (Obtener) del explorador Web. Vaya a la segunda ventana de Wireshark (doble clic a la línea en mención) para examinar los protocolos en capas. Si es necesario, expanda los campos.
  5. ¿Qué protocolo se lleva (encapsulado) dentro del segmento TCP?, dejar evidencia.
  6. Expanda el último registro de protocolo y cualquier subcampo. Ésta es la información real enviada al servidor Web. Complete la siguiente tabla utilizando la información del protocolo.

|  |  |
| --- | --- |
| **Versión del protocolo** |  |
| **Método de solicitud** |  |
| **Solicitud URI** |  |
| **Idioma** |  |

Es importante mencionar que la solicitud URI es la ruta para el documento solicitado. En el primer explorador, la ruta es el directorio raíz del servidor Web. Aunque no se solicitó ninguna página, algunos servidores Web están configurados para mostrar un archivo predeterminado, si está disponible.

El servidor Web responde con el próximo paquete HTTP (**text/html**). Una respuesta para el explorador Web es posible porque el servidor Web (1) comprende el tipo de solicitud y (2) tiene que devolver un archivo.

**Nota importante**: Los crackers a veces envían solicitudes desconocidas o dañadas a servidores Web para intentar detener el servidor o poder acceder a la línea de comando del servidor. Además, una solicitud para una página Web desconocida da como resultado un mensaje de error.

* 1. Resalte la respuesta del servidor Web y luego vaya a la segunda ventana (la del medio). Abra todos los subcampos de HTTP colapsados. Observe la información que devuelve el servidor. En esta respuesta, sólo hay unas pocas líneas de texto (las respuestas del servidor Web pueden contener miles o millones de bytes). El explorador Web comprende los datos de la ventana del explorador y los formatea correctamente.
  2. ¿Cuál es la respuesta del servidor Web para la solicitud GET del cliente Web?, explicar y dejar evidencia.
  3. ¿Qué significa esta respuesta?
  4. Desplácese hacia abajo de la ventana superior de Wireshark hasta que se muestre la segunda sesión de HTTP, *actualizada*. El significado de la acción de actualización se encuentra en la respuesta del servidor, 304 **Not Modified** (304 No modificado), localice esta línea en Wireshark.

Con un paquete simple devuelto para la solicitud inicial de GET y para la actualización, el ancho de banda utilizada es mínimo. Sin embargo, para una respuesta inicial que contenga millones de bytes, un simple paquete de respuesta puede generar un significativo ahorro de ancho de banda.

Debido a que esta página Web ha sido guardada en la caché del cliente Web, la solicitud GET contenía las siguientes instrucciones adicionales para el servidor Web.



Localice esta información en Wireshark y dejar la respectiva evidencia.

## Actividad 3. Captura y análisis de la comunicación FTP entre la computadora host del módulo y un servidor Web.

El protocolo de la capa de aplicación FTP ha recibido una revisión significativa desde que apareció por primera vez en RFC 114, en 1971. La versión 5.1 de FTP se define en RFC 959, de octubre de 1985.

En esta actividad, la utilidad de línea de comando FTP se utiliza para descargar datos desde un servidor FTP.

### Paso 1. Iniciar las capturas de Wireshark.

Si es necesario, consulte la Actividad 1, Paso 2, para abrir Wireshark.

### Paso 2: Iniciar el cliente FTP de la línea de comandos host del módulo.

1. Inicie una sesión FTP de una computadora host del módulo con el servidor FTP, usando la utilidad del cliente FTP de Windows. Para ello, abra la terminal de Windows y escriba **ftp** seguido de la tecla *Intro* Para autenticar, utilice la identificación de usuario **anonymous** (anónima). Como respuesta a la petición de contraseña, presione <Intro>.

**> ftp ftp.unicauca.edu.co** Conectado a odin.unicauca.edu.co. 220 (vsFTPd 3.0.3)

200 Always in UTF8 mode.

Usuario (odin.unicauca.edu.co:(none)): **anonymous**

331 Please specify the password. Contraseña: **<INTRO>**

230 Login successful.

1. Si presenta problemas de conectividad con el servidor FTP de la Universidad del Cauca utilice el siguiente servidor FTP: [ftp.cdc.gov](ftp://ftp.cdc.gov/)
2. El indicador del cliente FTP es ftp>. Esto significa que el cliente FTP espera un comando para enviar al servidor FTP. Para ver una lista de los comandos del cliente FTP, escriba help <INTRO> (ayuda, <aceptar>):

ftp> **help**

Los comandos se pueden abreviar. Comandos:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ! | delete | literal | prompt | send |
| ? | debug | ls | put | status |
| append | dir | mdelete | pwd | trace |
| ascii | disconnect | mdir | quit | type |
| bell | get | mget | quote | user |
| binary | glob | mkdir | recv | verbose |
| bye | hash | mls | remotehelp |  |
| cd  close | help  lcd | mput  open | rename  rmdir |  |

Desafortunadamente, la gran cantidad de comandos del cliente FTP dificulta el uso de la utilidad de la línea de comandos para un principiante. Sólo usaremos unos pocos comandos para la evaluación de Wireshark.

1. Escriba el comando ***dir*** para mostrar los contenidos actuales del directorio:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| drwxr-xr-x | 23 0 | 0 | 4096 Mar 21 | 2017 Documentos\_Publicos |
| drwxr-xr-x | 7 0 | 0 | 4096 Sep 09 | 2012 Facultades |
| drwxr-xr-x | 19 0 | 0 | 4096 Feb 06 | 2019 cuentas |
| drwxr-xr-x | 12 0 | 0 | 4096 May 09 | 2018 windows |

El cliente FTP es un directorio raíz del servidor FTP. Éste no es el directorio raíz real del servidor; sólo el punto más importante al que puede acceder el usuario **anonymous**. El usuario **anonymous** ha sido ubicado en una **root**, prohibiendo el acceso fuera del directorio actual.

ftp> **dir**

200 PORT command successful. Consider using PASV. 150 Here comes the directory listing.

226 Directory send OK.

ftp: 278 bytes recibidos en 0.01segundos 21.38a KB/s.

1. Sin embargo, los subdirectorios se pueden recorrer y los archivos se pueden transferir a la computadora host del módulo. Vaya al directorio **windows/Documentos**/, descargue un archivo y salga.

ftp> **cd windows/Documentos/**

250 Directory successfully changed.

ftp> **dir**

200 PORT command successful. Consider using PASV. 150 Here comes the directory listing.

226 Directory send OK.

ftp: 381 bytes recibidos en 0.03segundos 15.24a KB/s.

ftp> **get "Liberar\_espacio\_Outlook.pdf"**

200 PORT command successful. Consider using PASV.

|  |  |  |  |
| --- | --- | --- | --- |
| -rwxr-xr-x | 1 0 | 0 | 1819369 Oct 25 2013 Liberar\_espacio\_Outlook.pdf |
| -rw-r--r-- | 1 0 | 0 | 559576 Sep 26 2013 Liberar\_espacio\_Outlook\_express.pdf |
| -rwxr-xr-x | 1 0 | 0 | 1838214 Oct 25 2013 Manual\_liberacion\_espacio\_Outlook\_2007.pdf |
| -rwxr-xr-x | 1 0 | 0 | 1819369 Oct 25 2013 Manual\_liberacion\_espacio\_Outlook\_2013.pdf |

150 Opening BINARY mode data connection for Liberar\_espacio\_Outlook.pdf (1819369 bytes).

226 Transfer complete.

ftp: 1819369 bytes recibidos en 3.95segundos 461.07a KB/s.

ftp> **quit**

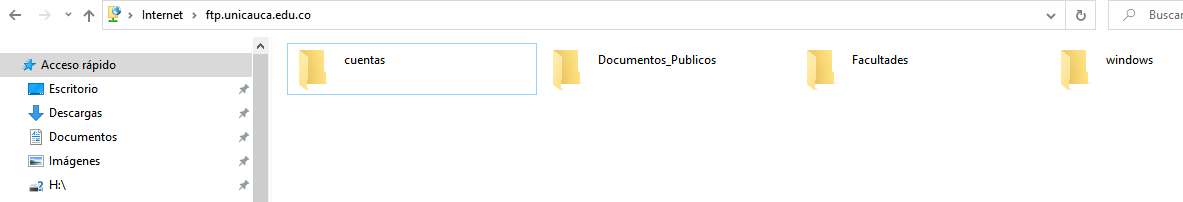
221 Goodbye.

1. Cierre la ventana de la línea de comandos con el comando exit (salir).
2. Detenga las capturas de Wireshark y guárdelas como

### FTP\_Command\_Line\_Client.

### Paso 3: Iniciar el explorador Web del host del módulo.

1. Inicie nuevamente las capturas Wireshark.
2. Abra un explorador del sistema, como lo muestra la Figura 3, y escriba el URL <ftp://ftp.unicauca.edu.co/>. Se abre una ventana del explorador que muestra los directorios disponibles. Además, el explorador se registró en el servidor FTP como usuario **anonymous**, como se muestra en la parte inferior de la captura de la pantalla.



### Figura 3. Explorador Web utilizado como un cliente FTP

1. Utilizando el explorador, vaya por los directorios hasta la ruta URL **windows/Documentos**/. Haga doble clic en el archivo Liberar\_espacio\_Outlook.pdf y guarde el archivo.
2. Al finalizar, cierre el explorador Web.
3. Detenga las capturas de Wireshark y guárdalas como **FTP\_Web\_Browser\_Client**.

### Paso 4: Detener las capturas de Wireshark y analizar los datos capturados.

1. Si aún no está abierta, abra la captura de Wireshark **FTP\_Web\_Browser\_Client**.
2. En la ventana superior de Wireshark, seleccione la captura FTP que es la primera transmisión del protocolo FTP. Respuesta: 220. Mostrar la Captura de Wireshark de una sesión FTP con un explorador Web.
3. Vaya a la ventana de Wireshark del medio y expanda el protocolo FTP. FTP se comunica usando códigos, como HTTP. Responder:
   1. ¿Cuál es la respuesta 220 del servidor FTP?
   2. Cuando el servidor FTP emitió una Respuesta: 331. Especifique la contraseña. ¿Cuál fue la respuesta del explorador Web?
   3. ¿Qué número de puerto utiliza el cliente FTP para conectarse al puerto 21 del servidor FTP?
   4. Cuando se transfieren datos, o con listados simples de directorios, se abre un nuevo puerto. Esto se llama modo de transferencia. El modo de transferencia puede ser activo o pasivo.

En modo activo, el servidor abre una sesión TCP para el cliente FTP y transfiere datos por ese puerto. El número de puerto de origen del servidor FTP es 20 y el número de puerto del cliente FTP es un número mayor a 1023. Sin embargo, en el modo pasivo, el cliente abre un nuevo puerto para el servidor para la transferencia de datos. Ambos números de puerto son mayores a 1023.

¿Cuál es el número de puerto de Datos FTP utilizado por el servidor FTP?

1. Abra la captura de Wireshark **FTP\_Command\_Line\_Client** y observe la comunicación FTP. Cuál es la semejanza entre los clientes línea de comando y browser.

### Paso 5: Modos de transferencia FTP activo y pasivo

Investigar la diferencia entre los Modos de transferencia FTP activo y pasivo.

## Actividad 4. Reflexión

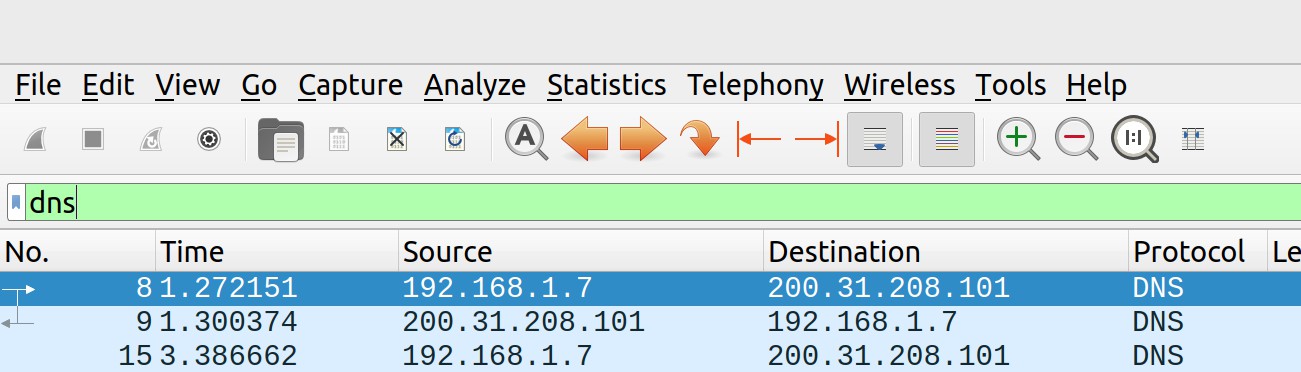
Explicar y evidenciar como los protocolos HTTP y FTP finalizan una sesión.

## Actividad 5. Captura y análisis de la comunicación utilizando el cliente FTP Filezilla

Habilite la captura de Wireshark, utilice FTP Filezilla2, uno de los clientes FTP multiplataforma más conocidos y utilizados en la actualidad. Para ello debe descargar e instalar Filezilla en su forma predeterminada (ver material de apoyo). Para esta actividad debe conectarse al servidor FTP de la Universidad del Cauca y capturar los datos respectivos. Observe y analice el comportamiento de los protocolos mencionados durante la práctica. Contrastar con las actividades anteriores.

## Actividad 6. Analizar los paquetes DNS (UDP) capturados

1. Habilite la captura de Wireshark, luego abra un explorador Web y escriba [www.google.com](http://www.google.com/) (o la url de su preferencia) y presione Enter para continuar.
2. Haga clic en Stop (Detener) para detener la captura de Wireshark cuando vea la página de inicio de Google.
3. En la ventana principal de Wireshark, escriba ***dns*** en el área de entrada de la barra de herramientas Filter (Filtrar). Haga clic en Apply (Aplicar) o presione Entrar.



### Figura 4. Filtro Wireshark

2 https://filezilla-project.org/

**Nota**: si no ve resultados después de aplicar el filtro DNS, cierre el explorador Web y, en la ventana del símbolo del sistema (**cmd**), escribe ***ipconfig /flushdns*** para eliminar todos los resultados anteriores del DNS. Reinicie la captura de Wireshark y repita las instrucciones anteriores. Si el problema no se resuelve, en la ventana del símbolo del sistema, puede escribir **nslookup** [www.google.com](http://www.google.com/) como alternativa para el explorador Web.

1. En el panel de la lista de paquetes (sección superior) de la ventana principal, ubique el paquete que incluye “**standard query**” (consulta estándar) y “A [www.google.com](http://www.google.com/)”.
2. Examine UDP (datagrama) mediante una consulta DNS para [www.google.com](http://www.google.com/) según lo capturado por Wireshark.
3. Amplíe el protocolo de datagramas de usuario en el panel de detalles del paquete haciendo clic en el signo más (+). Observe que hay solo cuatro campos. Identifique y explique cada uno de dichos campos. Dejar evidencia del resultado obtenido.
4. ¿Cuál es la longitud del datagrama (bytes)? ¿Cuántos bytes pertenecen a la cabecera y cuantos pertenecen a la consulta DNS? Dejar evidencia y justificar
5. Observe el datagrama de respuesta (DNS→Cliente) y responda:
   * ¿Observe la cantidad de bytes y comparelo con el tamaño del datagrama de la consulta, cual es más grande? Dejar evidencia
   * ¿Cuál fue el comportamiento de los números de puerto? Observe que hay solo cuatro campos. Identifique y explique cada uno de dichos campos. Dejar evidencia del resultado obtenido.
   * ¿Cuáles son los beneficios de utilizar UDP en lugar de TCP como protocolo de transporte para servicios o protocolos como DNS o DHCP o por ejemplo streaming de audio y video?
   * ¿Cuáles son los beneficios de utilizar TCP en lugar de UDP como protocolo de transporte para protocolos de mail (POP3, SMTP), conexiones remotas (Telnet, SSH) y/o transferencia de archivos (FTP)?
6. ¿Cuáles son los beneficios de utilizar UDP en lugar de TCP como protocolo de transporte para servicios o protocolos como DNS o DHCP o por ejemplo streaming de audio y video?
7. ¿Cuáles son los beneficios de utilizar TCP en lugar de UDP como protocolo de transporte para protocolos de mail (POP3, SMTP), conexiones remotas (Telnet, SSH) y/o transferencia de archivos (FTP)?

### Material de apoyo:

Pueden basarse en los siguientes enlaces:

* <https://www.webempresa.com/blog/ftp-y-uso-de-filezilla.html>

* <https://raiolanetworks.es/blog/manual-filezilla-cliente-ftp/>

* <https://www.youtube.com/watch?v=szdiWw_CWKE>

# Entregables:

## Informe

El informe debe contener las siguientes secciones:

### Introducción

1. **Bitácora de configuración e instalación de los servicios**: desarrollo de las actividades
2. **Archivos y capturas de pantalla de la señalización Wireshark** (En caso de ser necesario)
3. **Experiencias de la práctica**: problemas encontrados durante la práctica y sus soluciones. Además de otras consideraciones que les parecieron interesantes o les llamaron la atención durante la práctica
4. **Enlace del video**: en el video deben aparecer los dos integrantes (usar cámara) y el video debe iniciar con un Slide con la información personal de los estudiantes y el tema a tratar

### Conclusiones

### Referencias

## Trazas de captura de Wireshark

# Rúbrica de Evaluación:

|  |  |
| --- | --- |
| **%** | **RESUMEN** |
| 30% | Informe |
| 70% | Sustentación Individual (Crear video y subirlo a YouTube) |

# Anexos

# Material de Referencia

# Referencias

**1** https://[www.netacad.com/es](http://www.netacad.com/es)