

Objetivos:

- Familiarizarse con el software para rastreo de paquetes Wireshark
- Identificar detalles de paquetes
- Identificar detalles de DNS
- Comprender el funcionamiento de servidores DNS locales,
- Entender el almacenamiento en caché de DNS, los registros y mensajes de DNS y el campo TYPE en el registro de DNS.

Entrega:

- Fecha: Jueves 24 de Febrero / 2022 (E-Aulas 23:59)
- Modalidad: Por grupos
- Metodología: Observar y aprender haciendo (Hands-on)

Contexto:

Una vez realizado el primer Hands-On conociendo Wireshark en el laboratorio de introducción, la idea es utilizar la herramienta para investigar los protocolos en funcionamiento. En este taller exploraremos varios aspectos del protocolo HTTP: la interacción básica GET/RESPONSE, formatos de mensajes HTTP, recuperación de archivos HTML grandes, recuperación de archivos HTML con objetos incrustados, autenticación y seguridad HTTP.

En este Hands-on, también analizaremos más de cerca el lado del cliente de DNS. Recuerde que la función del cliente en el DNS es relativamente simple: un cliente envía una consulta a su servidor DNS local y recibe una respuesta. Desde el punto de vista del cliente, muchas cosas pueden suceder "a sus espaldas", invisibles para un cliente DNS, ya que los servidores DNS jerárquicos se comunican entre sí para resolver de forma recursiva o iterativa la consulta de DNS del cliente. Sin embargo, desde el punto de vista del cliente DNS, el protocolo es bastante simple: se formula una consulta al servidor DNS local y se recibe una respuesta de ese servidor.

Actividades:

Actividad 1: Interacción GET/RESPONSE de archivos más grandes y objetos embebidos

Actividad 2: Autenticación HTTP

Actividad 3: NSLOOKUP

Actividad 4: DNS y almacenamiento caché y seguimiento de DNS con Wireshark

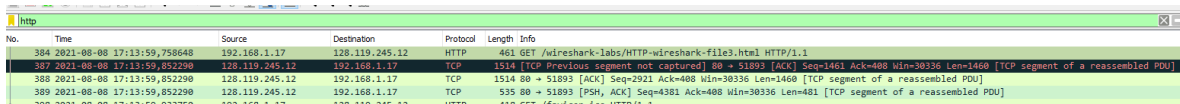
Actividad 5: nslookup y Wireshark

Actividad 1: Interacción GET/RESPONSE de archivos más grandes y objetos embebidos

En esta actividad el objetivo es explorar qué sucede cuando descargamos un archivo HTML largo. Para eso siga las siguientes indicaciones:

1. Inicie su navegador web y asegúrese de que la memoria caché de su navegador esté borrada.
2. Inicie el rastreador de paquetes de Wireshark
3. Ingrese la siguiente URL en su navegador
<http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file3.html>
4. Su navegador debería mostrar la Declaración de Derechos de EE. UU. (Bastante extensa)
5. Detenga la captura de paquetes de Wireshark y filtre paquetes HTTP.

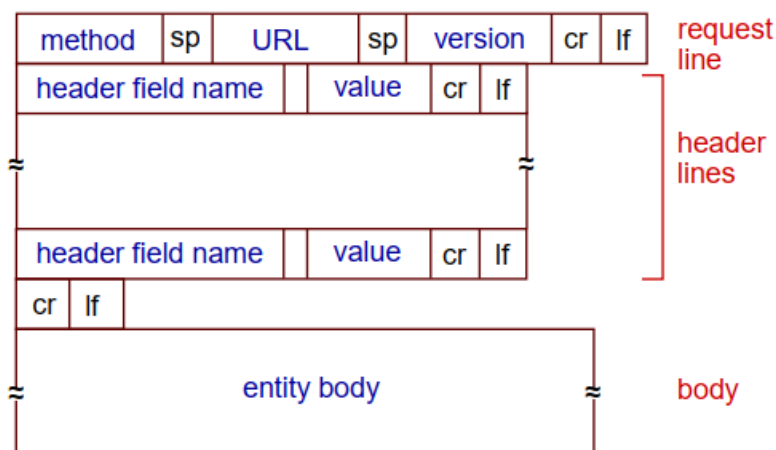
En la ventana de lista de paquetes, debería ver su mensaje HTTP GET, seguido de una respuesta TCP de múltiples paquetes a su solicitud HTTP GET:



No.	Time	Source	Destination	Protocol	Length	Info
384	2021-08-08 17:13:59.758648	192.168.1.17	128.119.245.12	HTTP	461	GET /wireshark-labs/HTTP-wireshark-file3.html HTTP/1.1
387	2021-08-08 17:13:59.852290	128.119.245.12	192.168.1.17	TCP	1514	[TCP Previous segment not captured] 80 → 51893 [ACK] Seq=1461 Ack=488 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
388	2021-08-08 17:13:59.852290	128.119.245.12	192.168.1.17	TCP	1514	80 → 51893 [ACK] Seq=2921 Ack=488 Win=30336 Len=1460 [TCP segment of a reassembled PDU]
389	2021-08-08 17:13:59.852290	128.119.245.12	192.168.1.17	TCP	535	80 → 51893 [PSH, ACK] Seq=4381 Ack=488 Win=30336 Len=481 [TCP segment of a reassembled PDU]

Recuerde que el mensaje de respuesta HTTP consta de una línea de estado, seguida de líneas de encabezado, seguidas de una línea en blanco, seguida del cuerpo de la entidad. En el caso de nuestro HTTP GET, el cuerpo de la entidad en la respuesta es el archivo HTML solicitado completo. (Capa de Aplicación Parte 1 - HTTP)

HTTP request message: Formato general



Basado en: Jim Kurose, Keith Ross Pearson, 2020 Slides

En este caso, el archivo HTML es bastante largo, y con 4500 bytes es demasiado grande para caber en un paquete TCP. El único mensaje de respuesta HTTP se divide en varias partes mediante TCP, y cada parte está contenida en un segmento TCP separado. En versiones recientes de Wireshark, Wireshark indica cada segmento TCP como un paquete separado, y el hecho de que la única

Redes de Computadores 2022-1
Hands-on 2: HTTP Authentication + DNS

Profesor: David F. Celeita R.

respuesta HTTP se fragmentó en varios paquetes TCP se indica mediante el "segmento TCP de una PDU reensamblada" en la columna Información de la pantalla de Wireshark.

Preguntas:

- A. ¿Cuántos mensajes de solicitud HTTP GET envió su navegador?
- B. ¿Qué número de paquete de la traza contiene el mensaje GET para el archivo "la Declaración de Derechos"?
- C. ¿Qué número de paquete en el rastreo contiene el código de estado y la frase asociados con la respuesta a la solicitud HTTP GET?
- D. ¿Cuál es el código de estado y la frase en la respuesta?
- E. ¿Cuántos segmentos TCP que contienen datos fueron necesarios para llevar la única respuesta HTTP y el texto de la "Declaración de Derechos"?

Actividad 2: Autenticación HTTP

Por último, intentemos visitar un sitio web que esté protegido con contraseña y examinemos la secuencia de mensajes HTTP intercambiados por dicho sitio. La URL es:

http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html

Está protegido con contraseña:

El nombre de usuario: wireshark-students

Contraseña: network

Así que accedamos a este sitio "seguro" protegido por contraseña:

1. Leer la descripción de esquemas de autenticación HTTP:
[http://frontier.userland.com/stories/storyReader\\$2159](http://frontier.userland.com/stories/storyReader$2159)
2. Asegúrese de que la memoria caché de su navegador esté borrada, como se mencionó anteriormente, y cierre su navegador. Luego, inicie su navegador nuevamente.
3. Inicie el rastreador de paquetes de Wireshark
4. Ingrese la siguiente URL en su navegador
http://gaia.cs.umass.edu/wireshark-labs/protected_pages/HTTP-wireshark-file5.html
5. Escriba el nombre de usuario y la contraseña solicitados en el cuadro emergente.
6. Detenga la captura de paquetes de Wireshark y filtre paquetes HTTP.

Preguntas:

- A. ¿Cuál es la respuesta del servidor (código de estado y frase) en respuesta al mensaje HTTP GET inicial de su navegador?
- B. Cuando su navegador envía el mensaje HTTP GET por segunda vez, ¿qué campo nuevo se incluye en el mensaje HTTP GET?

El nombre de usuario y la contraseña están codificados en la cadena de caracteres (d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5l) después del encabezado "Authorization: Basic" en el mensaje HTTP GET del cliente. Si bien puede parecer que su nombre de usuario y contraseña están encriptados, simplemente están codificados en un formato conocido como formato Base64.

¡El nombre de usuario y la contraseña no están encriptados!

Interceptación de usuario y contraseña:

Ingresa a: <http://www.motobit.com/util/base64-decoder-encoder.asp>

Seleccione "Decode" e ingrese la cadena codificada en base64: d2lyZXNoYXJrLXN0dWRlbnRz

Así, usted ha traducido de la codificación Base64 a la codificación ASCII y, por lo tanto, debería ver su nombre de usuario:

The Form.SizeLimit is 10000000bytes. Please, do not post more data using this form.

Source data from the Base64 string:
wireshark-students:network

Type (or copy-paste) some text to a textbox below. The text can be a Base64 string to decode or any string to encode to a Base64.
d2lyZXNoYXJrLXN0dWRlbnRzOm5ldHdvcm5=

or select a file to convert to a Base64 string.
Examinar... No se ha seleccionado ningún archivo. Convert the source data

What to do with the source data:
☐ encode the source data to a Base64 string (base64 encoding)
Maximum characters per line: 76
☒ decode the data from a Base64 string (base64 decoding)

Para ver la contraseña, ingrese el resto de la cadena: Om5ldHdvcm5 = y presione decodificar.

Conclusión:

Dado que cualquiera puede descargar una herramienta como Wireshark y realizar un sniffer de paquetes que pasan por su adaptador de red, y cualquiera puede traducir de Base64 a ASCII, como lo acabamos de hacer, debe quedar claro para usted que **las contraseñas simples en sitios puramente WWW no son seguros a menos que se tomen medidas adicionales.**

En el módulo de seguridad de nuestro curso, exploraremos alternativas para hacer que el acceso a la WWW sea más seguro. Sin embargo, es evidente que necesitaremos algo que vaya más allá del marco de autenticación HTTP básico.

Actividad 3: NSLOOKUP

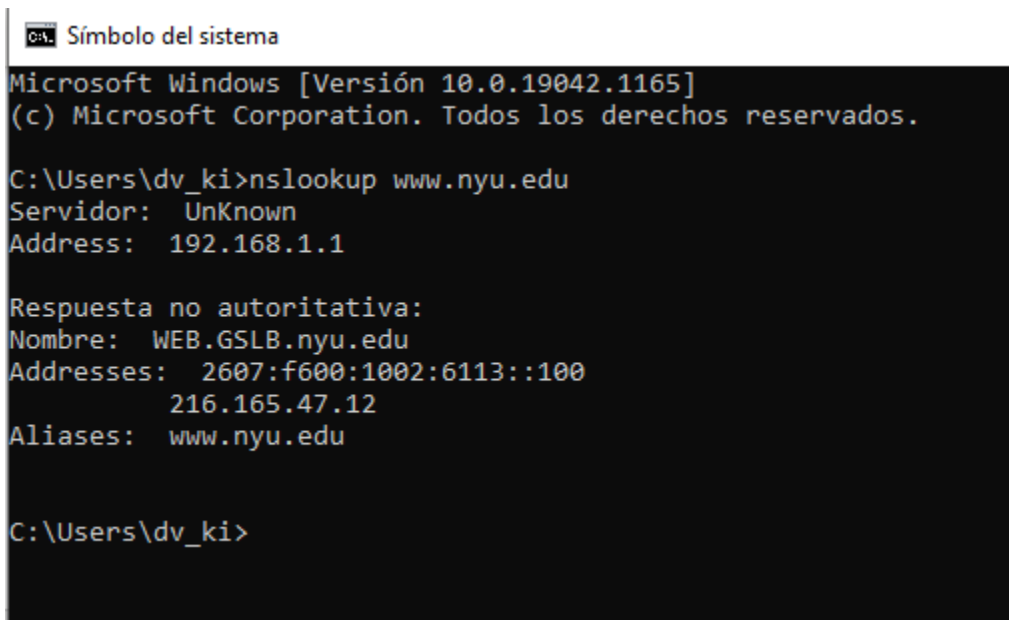
Comencemos nuestra investigación del DNS examinando el comando nslookup, que invocará los servicios DNS subyacentes para implementar su funcionalidad. El comando nslookup está disponible en la mayoría de los sistemas operativos Microsoft, Apple IOS y Linux. Para ejecutar nslookup, simplemente escriba el comando nslookup en la línea de comandos en una ventana de DOS, ventana de terminal Mac IOS o shell de Linux.

En su operación más básica, nslookup permite que el host que ejecuta nslookup consulte cualquier servidor DNS especificado para obtener un registro DNS. El servidor DNS consultado puede ser un servidor DNS raíz, un servidor DNS de dominio de nivel superior (Top-Level Domain TLD), un servidor DNS autorizado o un servidor DNS intermedio.

Por ejemplo, **nslookup** se puede utilizar para recuperar un registro DNS "Tipo = A" que asigna un nombre de host (por ejemplo, www.nyu.edu) a su dirección IP. Para realizar esta tarea, nslookup envía una consulta DNS al servidor DNS especificado (o al servidor DNS local predeterminado para el host en el que se ejecuta nslookup, si no se especifica un servidor DNS específico), recibe una respuesta DNS de ese servidor DNS y muestra el resultado.

Ejecución del comando – Ejemplo 1:

Ejecute el comando nslookup consultando www.nyu.edu:



```
CA: Símbolo del sistema
Microsoft Windows [Versión 10.0.19042.1165]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\dv_ki>nslookup www.nyu.edu
Servidor: UnKnown
Address: 192.168.1.1

Respuesta no autoritativa:
Nombre: WEB.GSLB.nyu.edu
Addresses: 2607:f600:1002:6113::100
           216.165.47.12
Aliases: www.nyu.edu

C:\Users\dv_ki>
```

1. Abrir CMD o terminal de su OS
2. Ejecutar el comando nslookup consultando www.nyu.edu

En el caso anterior, el comando `nslookup` recibe un argumento, un nombre de host (`www.nyu.edu`). En palabras, este comando dice "por favor envíeme la dirección IP del host `www.nyu.edu`". Como se muestra en la captura de pantalla, la respuesta de este comando proporciona dos datos:

1. El nombre y la dirección IP del servidor DNS que proporciona la respuesta; en este caso, el servidor DNS local de su ISP o los servidores de la Universidad del Rosario.
2. La respuesta en sí, que es el nombre de host canónico y la dirección IP de `www.nyu.edu`. Es posible que haya notado que hay dos pares de direcciones proporcionadas para `www.nyu.edu`. La primera (`216.165.47.12`) es una dirección IPv4 en la notación decimal con puntos de aspecto familiar; la segunda (`2607: f600: 1002: 6113 :: 100`) es una dirección IPv6 más larga y complicada.

Nota: IPv4 e IPv6 serán temas que abordaremos después de capa de transporte. Por ahora, nos enfocaremos en la dirección más sencilla (IPv4)

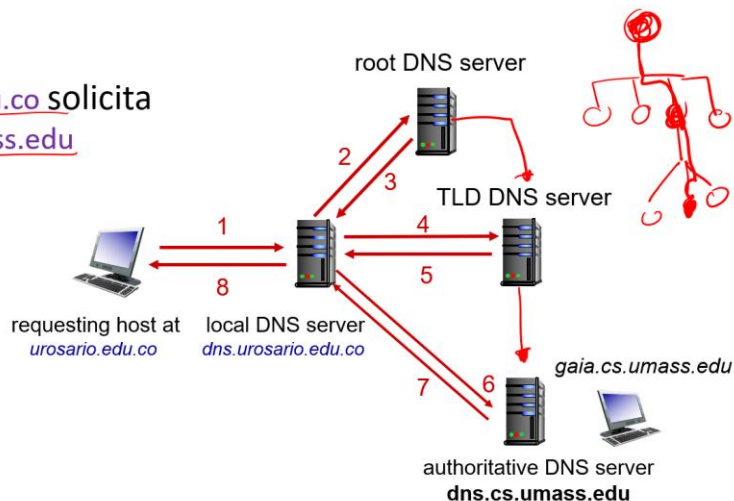
Aunque la respuesta provino del servidor DNS local (con dirección IP `192.168.1.1`) en una red domiciliaria, es muy posible que este servidor DNS local contactara iterativamente con otros servidores DNS para obtener la respuesta (recordar esquemas de consulta en la presentación de capa de aplicación – parte 2 DNS):

Resolución de nombres DNS: consulta iterada

Ejemplo: host en `urosario.edu.co` solicita la dirección IP de `gaia.cs.umass.edu`

Consulta iterada:

- El servidor contactado responde con el nombre del servidor para contactar
- "No sé este nombre, pero pregúntale a este servidor"

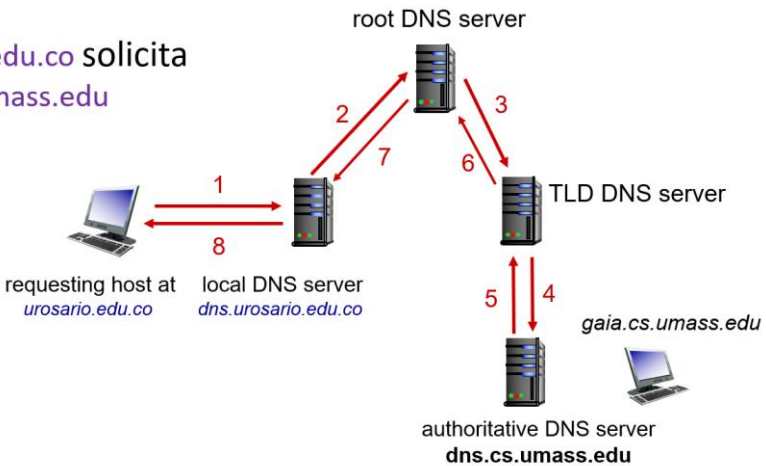


Resolución de nombres DNS: consulta recursiva

Ejemplo: host en urosario.edu.co solicita la dirección IP de gaia.cs.umass.edu

Consulta recursiva:

- pone la carga de la resolución de nombres en el servidor de nombres contactado
- carga pesada en los niveles superiores de jerarquía (?)



Además de usar nslookup para consultar un registro DNS "Tipo = A", también podemos usar nslookup para consultar un registro "TYPE = NS", que devuelve el nombre de host (y su dirección IP) de un servidor DNS autorizado, que sabe cómo obtener las direcciones IP de los hosts en el dominio del servidor autorizado.

Ejecución del comando – Ejemplo 2:

```
C:\> Símbolo del sistema

Microsoft Windows [Versión 10.0.19042.1165]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\dv_ki>nslookup -type=NS nyu.edu
Servidor: UnKnown
Address: 192.168.1.1

Respuesta no autoritativa:
nyu.edu nameserver = ns1.nyu.net
nyu.edu nameserver = ns4.nyu.edu
nyu.edu nameserver = ns2.nyu.org

C:\Users\dv_ki>
```

Nota: Cuando no se usa la opción `-type`, nslookup usa el valor predeterminado, que es consultar registros de tipo A.

En el segundo ejemplo se ha invocado nslookup con la opción `"-type = NS"` y el dominio `"nyu.edu"`. Esto hace que nslookup envíe una consulta para un registro de tipo NS al servidor DNS local

Redes de Computadores 2022-1

Hands-on 2: HTTP Authentication + DNS

Profesor: David F. Celeita R.

predeterminado. En palabras, la consulta dice, "por favor envíeme los nombres de host del DNS autorizado para nyu.edu".

La respuesta, que se muestra en la captura de pantalla anterior, primero indica el servidor DNS que proporciona la respuesta (nuevamente depende del ISP o si pertenece a la red de la Universidad) junto con tres servidores de nombres DNS NYU. Cada uno de estos servidores es de hecho un servidor DNS autorizado para los hosts en el campus de la universidad NYU. Sin embargo, nslookup también indica que la respuesta es "no autorizada", lo que significa que esta respuesta provino de la caché de algún servidor en lugar de un servidor DNS autorizado de la NYU.

Opciones adicionales del comando nslookup:

nslookup tiene una serie de opciones adicionales además de "-type = NS" que es posible que desee explorar.

Vínculo: <https://www.cloudns.net/blog/10-most-used-nslookup-commands/>

Instrucciones y preguntas:

1. Ejecute nslookup para obtener la dirección IP del servidor web del Instituto Indio de Tecnología en Bombay, India: www.iitb.ac.in. ¿Cuál es la dirección IP de www.iitb.ac.in?
2. ¿Cuál es la dirección IP del servidor DNS que proporcionó la respuesta a su comando nslookup en la pregunta 1 anterior?
3. ¿La respuesta a su comando nslookup en la pregunta 1 anterior provino de un servidor autorizado o no autorizado?
4. Utilice el comando nslookup para determinar el nombre del servidor de nombres autorizado para el dominio iit.ac.in. ¿Cuál es ese nombre? (Si hay más de un servidor autorizado, ¿cuál es el nombre del primer servidor autorizado devuelto por nslookup)? Si tuviera que encontrar la dirección IP de ese servidor de nombres autorizado, ¿cómo lo haría?
5. Repita el ejercicio consultando www.urosario.edu.co

Para ambas consultas adjunte las impresiones de pantalla de la respuesta a los comandos.

Actividad 4: DNS y almacenamiento caché y seguimiento de DNS con Wireshark

A partir de la descripción de la resolución de consultas de DNS iterativa y recursiva (presentadas en la actividad 1), podría pensar que se debe contactar al servidor DNS local cada vez que una aplicación necesita traducir de un nombre de host a una dirección IP. Sin embargo en la práctica no siempre es cierto.

La mayoría de los hosts (por ejemplo, su computadora personal) mantienen un caché de registros DNS recuperados recientemente (a veces llamado caché de resolución de DNS), al igual que muchos navegadores web mantienen un caché de objetos recuperados recientemente por HTTP. Cuando un host necesita invocar los servicios DNS, ese host primero verificará si el registro DNS necesario reside en la caché de DNS de este host; si se encuentra el registro, el anfitrión ni siquiera se molestará en contactar al servidor DNS local y en su lugar utilizará este registro DNS en caché. Un registro DNS en una caché de resolución eventualmente se agotará y se eliminará de la caché de resolución, al igual que los registros almacenados en caché en un servidor DNS local expirarán.

También puede borrar explícitamente los registros en su caché de DNS. No hay nada de malo en hacerlo, solo significará que su computadora deberá invocar el servicio DNS distribuido la próxima vez que necesite usar el servicio de resolución de nombres DNS, ya que no encontrará registros en la caché.

Para borrar la caché DNS de su computador personal:

- Windows: `ipconfig /flushdns`
- Linux: `sudo systemd-resolve --flush-caches`
- Mac: `sudo killall -HUP mDNSResponder`

Ahora que estamos familiarizados con `nslookup` y con la limpieza de la caché de resolución de DNS, vamos a continuar con la 3ra actividad de este Hands-on. Primero capturemos los mensajes DNS que son generados por la actividad de navegación web normal.

Instrucciones:

1. Borre la caché de DNS en su host, como se describe en la actividad 3.
2. Abra su navegador web y borre la memoria caché de su navegador.
3. Abra Wireshark e ingrese `ip.addr == <your_IP_address>` en el filtro de pantalla, donde `<your_IP_address>` es la dirección IPv4 de su computadora. Con este filtro, Wireshark solo mostrará los paquetes que se originen o estén destinados a su host.
4. Inicie la captura de paquetes en Wireshark.
5. Con su navegador, visite la página web: http://gaia.cs.umass.edu/kurose_ross/
6. Detenga la captura de paquetes.

Preguntas:

1. Busque el primer mensaje de consulta de DNS que resuelve el nombre `gaia.cs.umass.edu`. ¿Cuál es el número de paquete en el seguimiento del mensaje de consulta de DNS? ¿Este mensaje de consulta se envía a través de UDP o TCP?

2. Ahora localice la respuesta DNS correspondiente a la consulta DNS inicial. ¿Cuál es el número de paquete en el seguimiento del mensaje de respuesta de DNS? ¿Se recibe este mensaje de respuesta a través de UDP o TCP?
3. ¿Cuál es el puerto de destino para el mensaje de consulta de DNS? ¿Cuál es el puerto de origen del mensaje de respuesta de DNS?
4. ¿A qué dirección IP se envía el mensaje de consulta de DNS?
5. Examine el mensaje de consulta de DNS. ¿Cuántas "preguntas" contiene este mensaje DNS? ¿Cuántas "respuestas" contiene?
6. Examine el mensaje de respuesta de DNS al mensaje de consulta inicial. ¿Cuántas "preguntas" contiene este mensaje DNS? ¿Cuántas "respuestas" contiene?
7. La página web del archivo base http://gaia.cs.umass.edu/kurose_ross/ hace referencia al objeto de imagen http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E_2.jpg que, al igual que la base página web, está en gaia.cs.umass.edu. ¿Cuál es el número de paquete en el seguimiento de la solicitud HTTP GET inicial para el archivo base http://gaia.cs.umass.edu/kurose_ross/?
8. ¿Cuál es el número de paquete en el seguimiento de la consulta DNS realizada para resolver gaia.cs.umass.edu de modo que esta solicitud HTTP inicial pueda enviarse a la dirección IP gaia.cs.umass.edu?
9. ¿Cuál es el número de paquete en el seguimiento de la respuesta DNS recibida?
10. ¿Cuál es el número de paquete en el seguimiento de la solicitud HTTP GET para el objeto de imagen http://gaia.cs.umass.edu/kurose_ross/header_graphic_book_8E2.jpg ?
11. ¿Cuál es el número de paquete en la consulta DNS realizada para resolver gaia.cs.umass.edu para que esta segunda solicitud HTTP pueda enviarse a la dirección IP gaia.cs.umass.edu?
12. Analice cómo el almacenamiento en caché de DNS afecta la respuesta a esta última pregunta.

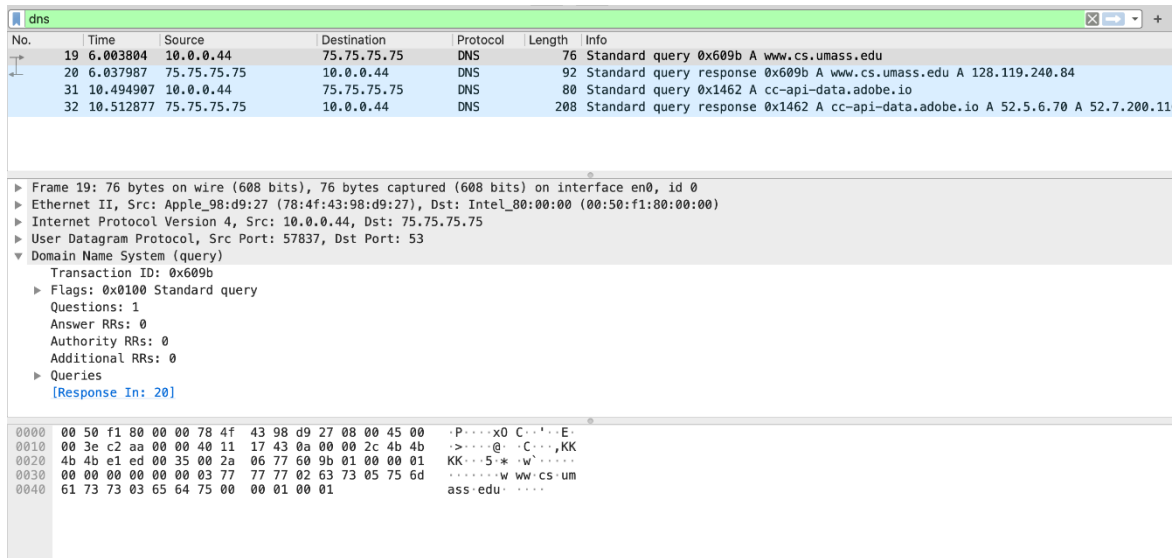
Nota: Organice las respuestas de números de paquetes en una tabla.

Actividad 5: nslookup y Wireshark

Instrucciones parte A:

1. Inicie la captura de paquetes en Wireshark.
2. Haga un nslookup en www.cs.umass.edu
3. Detenga la captura de paquetes.

Debería obtener un rastro similar al siguiente en su ventana de Wireshark. Veamos la primera consulta de tipo A (que es el paquete número 19 en la figura a continuación, y se indica con la "A" en la columna de información para ese paquete).



Preguntas:

1. ¿Cuál es el puerto de destino para el mensaje de consulta de DNS? ¿Cuál es el puerto de origen del mensaje de respuesta de DNS?
2. ¿A qué dirección IP se envía el mensaje de consulta de DNS? ¿Es esta la dirección IP de su servidor DNS local predeterminado?
3. Examine el mensaje de consulta de DNS. ¿Qué "tipo" de consulta de DNS es? ¿El mensaje de consulta contiene alguna "respuesta"?
4. Examine el mensaje de respuesta de DNS al mensaje de consulta. ¿Cuántas "preguntas" contiene este mensaje de respuesta de DNS? ¿Cuántas "respuestas"?

Instrucciones parte B:

Utilice nslookup para emitir un comando que devolverá un registro DNS de tipo NS, ingrese el siguiente comando:

```
nslookup -type = NS umass.edu
```

Al mismo tiempo capture paquetes con Wireshark, y una vez realizada la consulta DNS detenga la captura.

Preguntas:

1. ¿A qué dirección IP se envía el mensaje de consulta de DNS? ¿Es esta la dirección IP de su servidor DNS local predeterminado?
2. Examine el mensaje de consulta de DNS. ¿Cuántas preguntas tiene la consulta? ¿El mensaje de consulta contiene alguna "respuesta"?
3. Examine el mensaje de respuesta de DNS. ¿Cuántas respuestas tiene la respuesta? ¿Qué información contienen las respuestas? ¿Cuántos registros de recursos adicionales se devuelven? ¿Qué información adicional se incluye en estos registros de recursos adicionales?

Entregables: Una carpeta con los siguientes elementos:

Un solo Reporte PDF de todas las actividades incluyendo impresión de pantalla por cada ítem y respuestas a cada pregunta.

Archivos de **capturas de Wireshark** por cada actividad respectivamente.

Actividad 1: Interacción GET/RESPONSE de archivos más grandes y objetos embebidos (20%)

Actividad 2: Autenticación HTTP (20%)

Actividad 3: NSLOOKUP (20%)

Actividad 4: DNS y almacenamiento caché y seguimiento de DNS con Wireshark (20%)

Actividad 5: nslookup y Wireshark (20%)