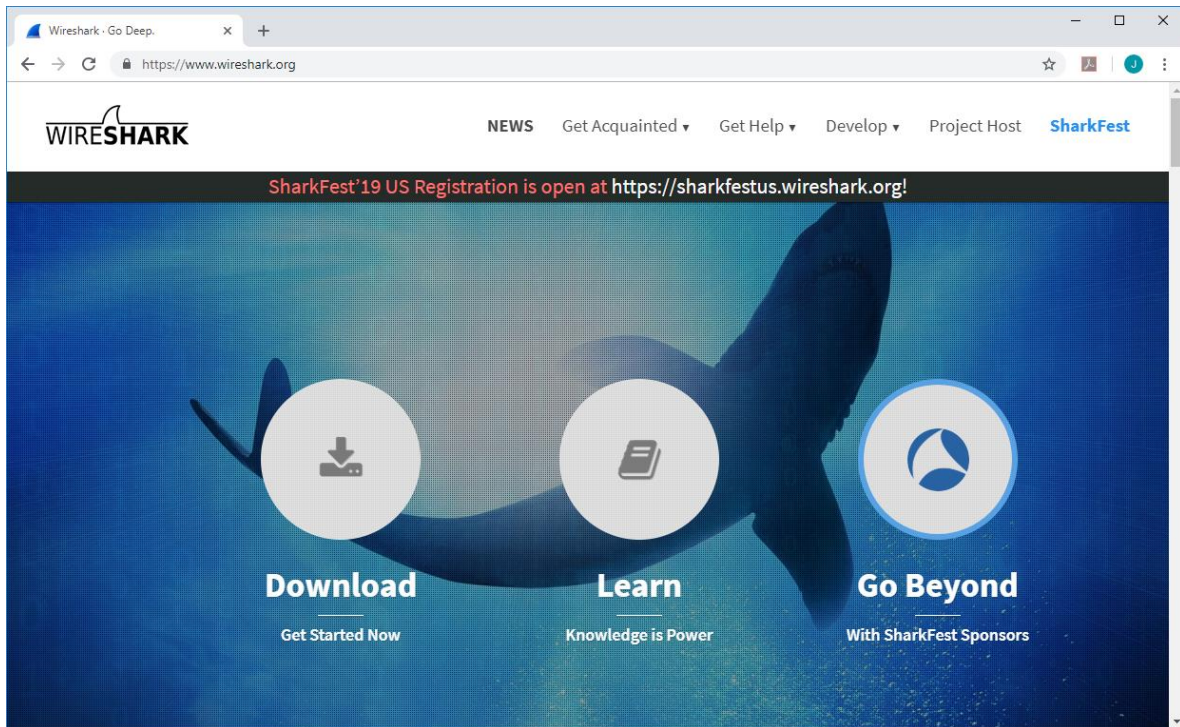
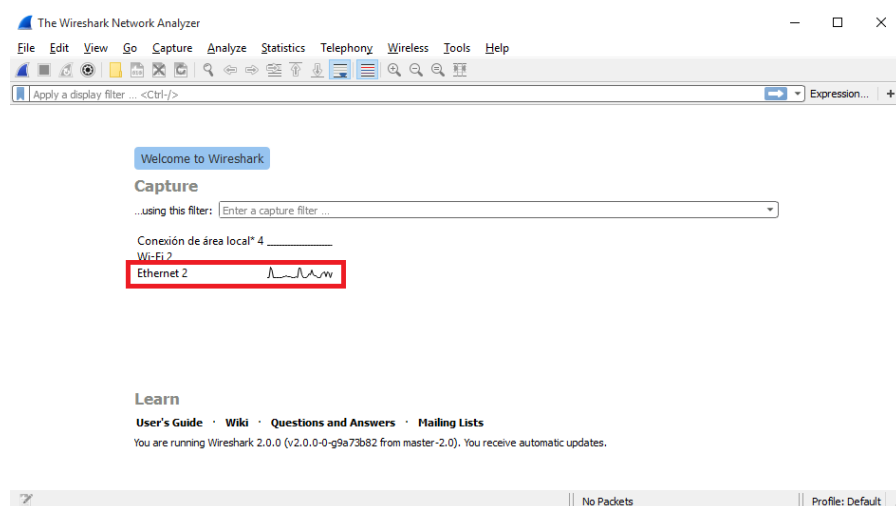


PRACTICA 1 GRUPAL USO DE WIRESHARK

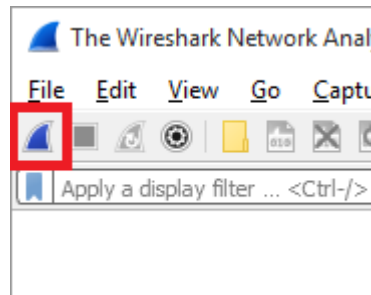
1. Descarga e instala la última versión de Wireshark, disponible en <https://www.wireshark.org/>



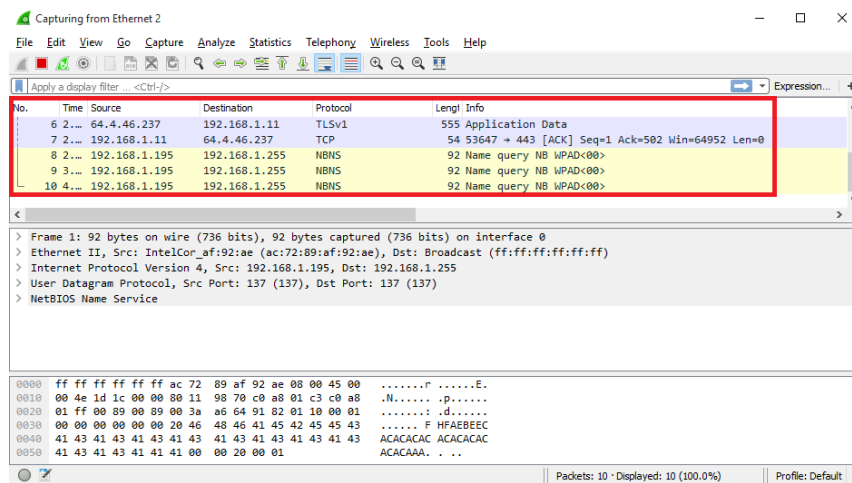
2. Ejecuta Wireshark y haz clic en la interfaz de red que muestre actividad:



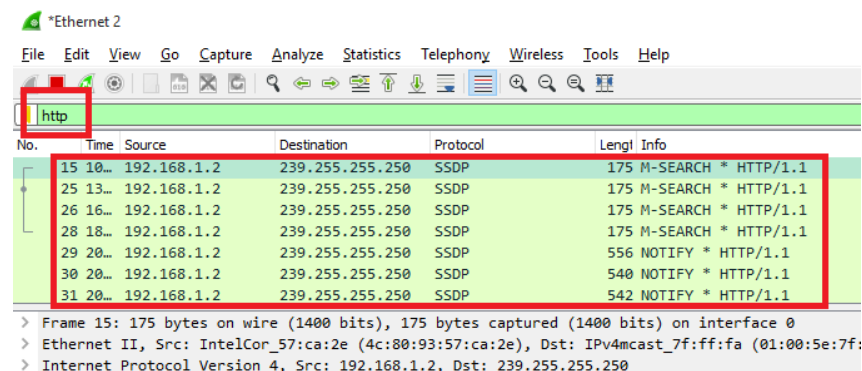
3. Haz clic en el ícono “Start capturing packets” que se encuentra en la esquina superior izquierda:



4. El programa comenzará a mostrar el tráfico de red que está pasando por la interfaz seleccionada:



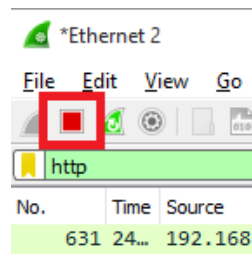
5. Escribe la palabra *http* en el campo “Apply a display filter”. Esto hará que Wireshark muestre únicamente el tráfico relacionado con el protocolo HTTP:



6. Abre un navegador web e ingresa a la página <http://collider.com/rick-and-morty-season-4-images/>



7. Una vez que el navegador termine de cargar la página, detén el monitoreo de Wireshark, haciendo clic en el botón Stop:



8. En Wireshark, identifica el tráfico relacionado al request del recurso (URI) que abrió el navegador:

No.	Time	Source	Destination	Protocol	Length	Info
48	2.114231	192.168.101.31	151.101.0.249	HTTP	612	GET /rick-and-morty-season-4-images/ HTTP/1.1
274	2.459671	192.168.101.31	201.174.231.185	HTTP	385	GET /p?c1=2&c2=18120612&ns_type=hidden&ns_st_sv=6
304	2.484626	201.174.231.185	192.168.101.31	HTTP	363	HTTP/1.1 200 OK (GIF89a)

9. Inspecciona el contenido del mensaje de dicho request:

```

Hypertext Transfer Protocol
> GET /game/switch/the-legend-of-zelda-breath-of-the-wild HTTP/1.1\r\n
Host: www.metacritic.com\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
Upgrade-Insecure-Requests: 1\r\n
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\n
Referer: https://www.google.com.mx/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
[truncated]Cookie: CBS_INTERNAL=0; trctestcookie=ok; ctk=NTk5YjMzZTM5ZmI0NDcwZWMSYyYwMTZjZWISMQ%3D\r\n
[Full request URI: http://www.metacritic.com/game/switch/the-legend-of-zelda-breath-of-the-wild]
[HTTP request 1/2]
[Response in frame: 3454]
[Next request in frame: 4858]

```

0000	2c dd 95 ca fe 3c a0 48 1c d3 f0 d1 08 00 45 00	,....<.HE.
0010	05 45 33 d7 40 00 80 06 20 17 c0 a8 01 53 c0 21	.E3.@... ..S.!
0020	1f a8 f5 5f 00 50 f9 6a a5 63 f3 88 fd d5 50 18	...P.j .C....P.
0030	01 03 01 43 00 00 34 2e 31 35 30 33 33 34 33 35	...C..4. 15033435
0040	39 30 2e 31 35 31 35 31 39 37 38 39 33 2e 31 35	90.15151 97893.15

Frame (1363 bytes) Reassembled TCP (2721 bytes)

10. Observa que el request se fragmentó en 4:

```

Hypertext Transfer Protocol
> GET /rick-and-morty-season-4-images/ HTTP/1.1\r\n
Host: collider.com\r\n
Connection: keep-alive\r\n
Cache-Control: max-age=0\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,i
Referer: https://www.google.com/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: es-ES,es;q=0.9,en;q=0.8\r\n
[truncated]Cookie: FUUID=1d14f062-8f83-4831-b1b5-1f5ace66ba17; _sp_ses.26
If-Modified-Since: Tue, 16 Jul 2019 18:16:46\r\n
\r\n
[Full request URI: http://collider.com/rick-and-morty-season-4-images/]
[HTTP request 1/4]
[Response in frame: 392]
[Next request in frame: 691]

```

Observe que el siguiente fragmento del request está en el frame 691

11. Identifica el otro fragmento del request, en base al “Next request fragment” y analízcelos.

12. Haga lo mismo para el mensaje de response y sus fragmentos. El mensaje de response correspondiente está indicado en el frame 3454 (Response in frame):

```

v Hypertext Transfer Protocol
  > GET /tv/ HTTP/1.1\r\n
    Host: collider.com\r\n
    Connection: keep-alive\r\n
    Accept: */*\r\n
    X-Requested-With: XMLHttpRequest\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64;
    Referer: http://collider.com/rick-and-morty-sea
    Accept-Encoding: gzip, deflate\r\n
    Accept-Language: es-ES,es;q=0.9,en;q=0.8\r\n
  > [truncated]Cookie: FUUID=1d14f062-8f83-4831-b1b
    If-Modified-Since: Tue, 13 Aug 2019 08:16:19\r\n
    \r\n
    [Full request URI: http://collider.com/tv/]
    [HTTP request 4/4]
    [Prev request in frame: 821]
    [Response in frame: 858]
  
```

Por lo tanto, el mensaje de response es:

840	3.696087	192.168.101.31	151.101.0.249	HTTP	490 GET /tv/ HTTP/1.1
858	3.738454	151.101.0.249	192.168.101.31	HTTP	377 HTTP/1.1 200 OK (text/html)
865	3.823974	192.168.101.31	35.232.218.165	HTTP	976 GET /i?stm=1565712354754&e=se&se

```

v Hypertext Transfer Protocol
  > HTTP/1.1 200 OK\r\n
    Content-Type: text/html; charset=UTF-8\r\n
    Server: Apache/2.4.25 (Debian)\r\n
    X-Powered-By: PHP/7.3.7\r\n
    Link: <http://collider.com/wp-json/>; rel="https://api.w.org/"\r\n
    Last-Modified: Tue, 13 Aug 2019 08:16:19\r\n
    Content-Encoding: gzip\r\n
    Cache-Control: public, max-age=900\r\n
    X-Obj-Url: /tv/\r\n
    X-Obj-Host: collider.com\r\n
    X-Obj-Device: desktop\r\n
  > Content-Length: 11359\r\n
    Accept-Ranges: bytes\r\n
    Date: Tue, 13 Aug 2019 16:05:46 GMT\r\n
    Via: 1.1 varnish\r\n
    Age: 2938\r\n
    Connection: keep-alive\r\n
    X-Served-By: cache-dfw18625-DFW\r\n
    X-Cache: HIT\r\n
    X-Cache-Hits: 8\r\n
    X-Timer: S1565712347.579377,VS0,VE0\r\n
    Vary: Accept-Encoding, User-Agent, X-Browser, X-Galleries\r\n
    \r\n
    [HTTP response 4/4]
    [Time since request: 0.042367000 seconds]
    [Prev request in frame: 821]
    [Prev response in frame: 826]
    [Request in frame: 840]
    Content-encoded entity body (gzip): 11359 bytes -> 47858 bytes
    File Data: 47858 bytes
  > Line-based text data: text/html (983 lines)
  
```

