Networking Lab 0 Encapsulation and Wireshark

Wireshark is an open source network analyzer. It copies the network traffic through your computer's Network Interface Card (NIC) and displays the traffic for analysis. In this lab, we will use it to show how data is encapsulated according to the TCP/IP or OSI 7 Layer Model.

Read

Read Wireshark_Intro_v7.0.pdf and follow the procedures it gives, to learn install and open Wireshark.

Read or Listen to CyberAces Module 2 Networking, Session 1 Intro and Layer 1 (https://tutorials.cyberaces.org/tutorials/view/2-1.html)

Encapsulation

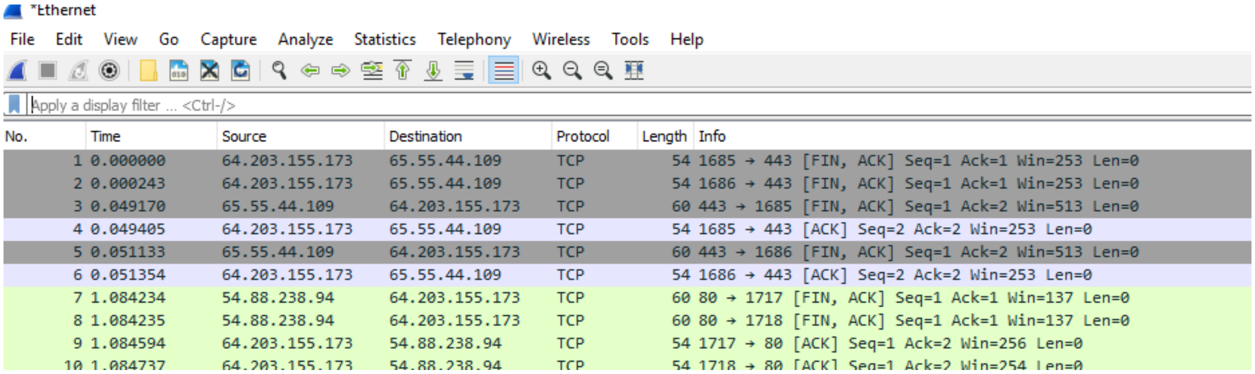
First, let's get a packet to analyze. Start a capture in Wireshark. You will see that your computer is receiving a lot of traffic (and generating some) without you doing anything on your computer. This background traffic is mostly comprised of broadcasts from other computers announcing their existence and advertising services. At this point, we are not interested in the broadcast traffic, but it demonstrates our first problem. There is *a lot* of traffic, and we will have to work to separate traffic of interest from all the noise.

Wireshark uses two primary filtering methods: Capture Filters and Display Filters. Capture Filters filter the traffic as it is being recorded, which reduces the amount of data that Wireshark saves. Traffic that does not pass the filter is not kept in Wireshark and cannot be displayed. Display filters do not affect what is being recorded, but only what is shown on the display. For the time being, we will just use Display Filters.

Find the packet we want with Wireshark Display Filters

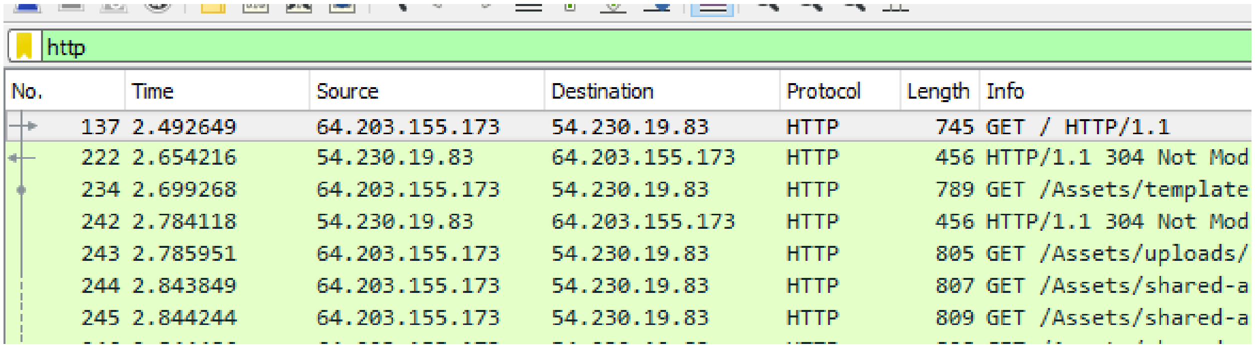
We will start by looking at an HTTP request for a web page. It should look like "GET / HTTP1.1". It says we are looking for a web page (GET) at the root, or beginning (/), of the site, and we are using HTTP version 1.1.

1. Open Wireshark and a web browser, if they are not open already.
2. Start a new packet capture in Wireshark.
3. In your web browser, open a site that you like that uses http, not https. If you are having trouble finding an http site, http://www.bu.edu/ will work.
4. Stop the packet capture when the site finishes loading. If you look at the Wireshark screen, you will see that is full of stuff that does not interest you.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	64.203.155.173	65.55.44.109	TCP	54	1685 → 443 [FIN, ACK] Seq=1 Ack=1 Win=253 Len=0
2	0.000243	64.203.155.173	65.55.44.109	TCP	54	1686 → 443 [FIN, ACK] Seq=1 Ack=1 Win=253 Len=0
3	0.049170	65.55.44.109	64.203.155.173	TCP	60	443 → 1685 [FIN, ACK] Seq=1 Ack=2 Win=513 Len=0
4	0.049405	64.203.155.173	65.55.44.109	TCP	54	1685 → 443 [ACK] Seq=2 Ack=2 Win=253 Len=0
5	0.051133	65.55.44.109	64.203.155.173	TCP	60	443 → 1686 [FIN, ACK] Seq=1 Ack=2 Win=513 Len=0
6	0.051354	64.203.155.173	65.55.44.109	TCP	54	1686 → 443 [ACK] Seq=2 Ack=2 Win=253 Len=0
7	1.084234	54.88.238.94	64.203.155.173	TCP	60	80 → 1717 [FIN, ACK] Seq=1 Ack=1 Win=137 Len=0
8	1.084235	54.88.238.94	64.203.155.173	TCP	60	80 → 1718 [FIN, ACK] Seq=1 Ack=1 Win=137 Len=0
9	1.084594	64.203.155.173	54.88.238.94	TCP	54	1717 → 80 [ACK] Seq=1 Ack=2 Win=256 Len=0
10	1.084737	64.203.155.173	54.88.238.94	TCP	54	1718 → 80 [ACK] Seq=1 Ack=2 Win=254 Len=0

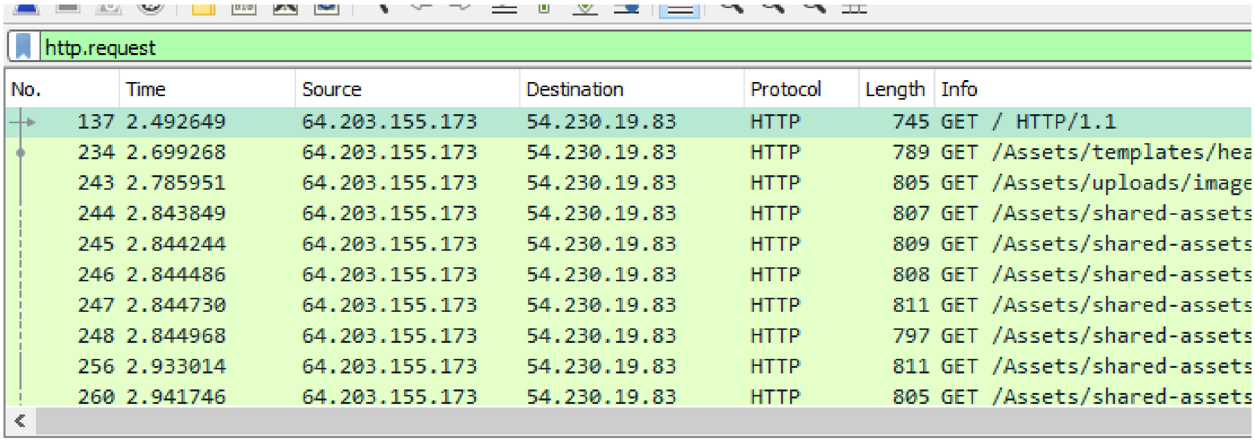
5. Type http in the display filter window. This is better, as the request is probably at the top of the list.



http

```
No.   Time        Source           Destination      Protocol  Length Info
  137 2.492649    64.203.155.173   54.230.19.83     HTTP        745 GET / HTTP/1.1
  222 2.654216    54.230.19.83     64.203.155.173   HTTP        456 HTTP/1.1 304 Not Mod
  234 2.699268    64.203.155.173   54.230.19.83     HTTP        789 GET /Assets/template
  242 2.784118    54.230.19.83     64.203.155.173   HTTP        456 HTTP/1.1 304 Not Mod
  243 2.785951    64.203.155.173   54.230.19.83     HTTP        805 GET /Assets/uploads/
  244 2.843849    64.203.155.173   54.230.19.83     HTTP        807 GET /Assets/shared-a
  245 2.844244    64.203.155.173   54.230.19.83     HTTP        809 GET /Assets/shared-a
```

6. Just to show that display filters can be more specific, change http to http.request in the display filter window. I have found the http.request filter to be very helpful when I am trying to track the sequence of web pages that led a user to malware.

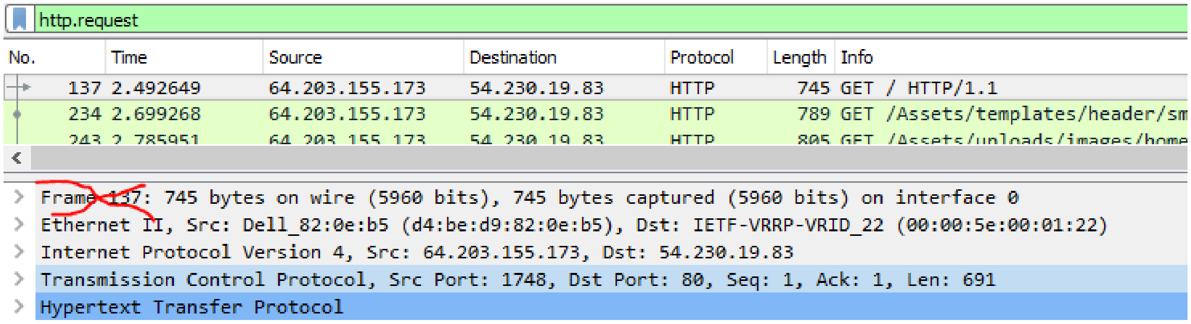


http.request

```
No.   Time        Source           Destination      Protocol  Length Info
  137 2.492649    64.203.155.173   54.230.19.83     HTTP        745 GET / HTTP/1.1
  234 2.699268    64.203.155.173   54.230.19.83     HTTP        789 GET /Assets/templates/hea
  243 2.785951    64.203.155.173   54.230.19.83     HTTP        805 GET /Assets/uploads/image
  244 2.843849    64.203.155.173   54.230.19.83     HTTP        807 GET /Assets/shared-assets
  245 2.844244    64.203.155.173   54.230.19.83     HTTP        809 GET /Assets/shared-assets
  246 2.844486    64.203.155.173   54.230.19.83     HTTP        808 GET /Assets/shared-assets
  247 2.844730    64.203.155.173   54.230.19.83     HTTP        811 GET /Assets/shared-assets
  248 2.844968    64.203.155.173   54.230.19.83     HTTP        797 GET /Assets/shared-assets
  256 2.933014    64.203.155.173   54.230.19.83     HTTP        811 GET /Assets/shared-assets
  260 2.941746    64.203.155.173   54.230.19.83     HTTP        805 GET /Assets/shared-assets
```

Use the Wireshark Details Panel to see encapsulation

1. Highlight the GET / HTTP1.1 packet and look at the Details Pane. Compare what you see with the Encapsulation picture on slide 5 and 7 of CyberAces_Module2-Networking-IntroAndLayer1.pdf. Ignore Layer 5 (Session) and Layer 6 (Presentation), as they are seldom/never used. Note that the section called Frame on the Wireshark Details Pane is data added by Wireshark for bookkeeping. It is not part of the packet.



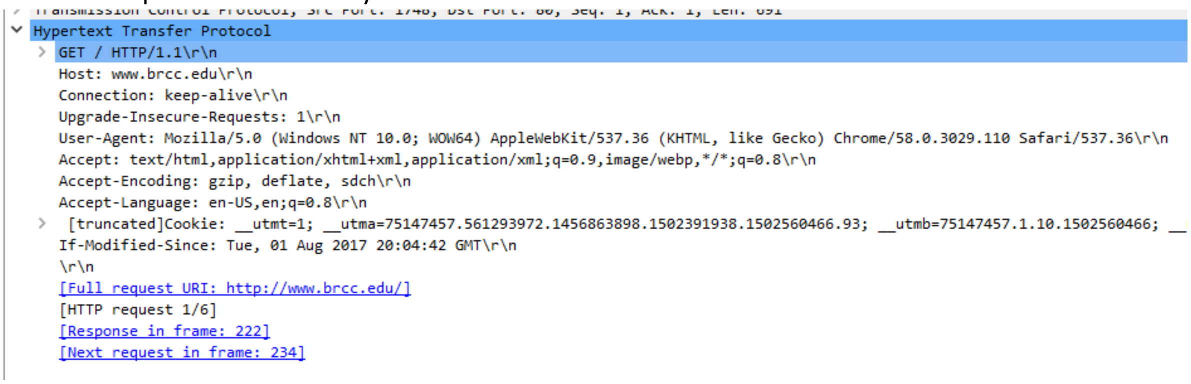
http.request

```
No.   Time        Source           Destination      Protocol  Length Info
  137 2.492649    64.203.155.173   54.230.19.83     HTTP        745 GET / HTTP/1.1
  234 2.699268    64.203.155.173   54.230.19.83     HTTP        789 GET /Assets/templates/header/sm
  243 2.785951    64.203.155.173   54.230.19.83     HTTP        805 GET /Assets/uploads/images/home
```

```
> Frame ~~137~~: 745 bytes on wire (5960 bits), 745 bytes captured (5960 bits) on interface 0
> Ethernet II, Src: Dell_82:0e:b5 (d4:be:d9:82:0e:b5), Dst: IETF-VRRP-VRID_22 (00:00:5e:00:01:22)
> Internet Protocol Version 4, Src: 64.203.155.173, Dst: 54.230.19.83
> Transmission Control Protocol, Src Port: 1748, Dst Port: 80, Seq: 1, Ack: 1, Len: 691
> Hypertext Transfer Protocol
```

The section labeled Ethernet II is layer 2 (data link), Internet Protocol Version 4 is layer 3 (network), Transmission Control Protocol is Layer 4 (transport) , and Hypertext Transfer Protocol is layer 7 (application.)

2. Click the Hypertext Transfer Protocol (where the abbreviation “http” comes from) to open it. The is the Application Layer of your packet, the data that was sent to the web server. You will probably see that a great deal of information went along with your request. For example, your browser tells the server what browser and operating system you are using, your language, what file types it can accept, etc. It makes your browsing experience better, but also helps web sites track you.



```
Transmission Control Protocol, Src Port: 1748, Dst Port: 80, Seq: 1, Ack: 1, Len: 691
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: www.brcc.edu\r\n
  Connection: keep-alive\r\n
  Upgrade-Insecure-Requests: 1\r\n
  User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
  Accept-Encoding: gzip, deflate, sdch\r\n
  Accept-Language: en-US,en;q=0.8\r\n
   [truncated]Cookie: __utmt=1; __utma=75147457.561293972.1456863898.1502391938.1502560466.93; __utmb=75147457.1.10.1502560466; __
  If-Modified-Since: Tue, 01 Aug 2017 20:04:42 GMT\r\n
  \r\n
  [Full request URI: http://www.brcc.edu/]
  [HTTP request 1/6]
  [Response in frame: 222]
  [Next request in frame: 234]
```

3. What you see above is the Data section, that is shown in a yellow box on the encapsulation slide (CyberAces_Module2-Networking-IntroAndLayer1_20150129 slide 6.) Find the sections in your Wireshark display that correspond to the remaining layers, Transport, Network, and Data Link (Physical is your cable, NIC, etc, so it won’t appear in Wireshark.) It shouldn’t be hard, as they are in order.

Hand In

Fill in some of the information from your packet below the drawing. For the Data Link layer, just put the source and destination MAC addresses (look like xx:xx:xx:xx:xx:xx). For the Network layer, put the source and destination IP addresses (xxx.xxx.xxx.xxx), and for the Transport layer put the source and destination port numbers. For the Application layer data, GET / HTTP1.1 is fine.

Layer	2: Data Link	3: Network	4: Transport	7: Application
Address	Src, Dst MAC	Src, Dst IP Addr	Src, Dst Port	Data
Your PDU				