1. How many packets exist in the capture?

220  
<https://gyazo.com/927ce2fae15677c47e6385cb5aae267d>  
<https://gyazo.com/9aaff07e36054145586492188de6cf20>

1. At what time did the packet capture occur?

March 16, 2013 @ 2:10pm

<https://gyazo.com/d5a8cb710a1c2ade41eef67e348372fb>

1. What is the timespan, in seconds, of the traffic? (How many seconds of traffic were captured?)

From the above gif:  
~~395 sec~~ 396 between the start of the first session and the ~~start~~ end of the final session… ~~(I couldn’t find a display for session end times, so it may have been longer?)~~

<https://gyazo.com/1f4a35400d3e979f005af4b6c90034e6>

1. Is there any traffic other than TCP sessions?

no

<https://gyazo.com/59602e2806ebe1b87d2dbc9c4ba64e78>

1. How many TCP sessions exist in the packet capture?

13

<https://gyazo.com/352ef5827a4831db4d196fffb88d146f>

1. How many sessions involve the IP address 203.0.113.15?

3

<https://gyazo.com/a51fb6fcb72b8de865387a1f1750b40d>

1. How many bytes of non-TCP traffic exist in the traffic?

0  
I was pretty sure just from the above answers, but just to double check I opened up wireshark for this one

<https://gyazo.com/5f1dbd8cf43eac1d198c466e84767873>

1. Using Argus, determine how many bytes were transferred between 203.0.113.15 and 172.16.0.37.

Argus is not installed, and I couldn’t install it, but I tried adding up all bytes between them as displayed on networkminer: I came to 17,372‬ bytes exchanged between the two (requests+responses)

<https://gyazo.com/8072a20136d428d1e3f393838006a3ce>  
<https://gyazo.com/438ae4037e96e78a202a4e55d6526e72>

1. Using tshark, determine how many bytes were transferred between 203.0.113.15 and 172.16.0.37.

20488 bytes

I used a chunky command for this… I’m assuming the difference Is due to tshark counting the packet wrappers themselves in the byte count, and networkminer only counted content.

https://i.gyazo.com/c6abecc69c2ca5403900318f6cefa653.png

The output is also saved in a file on the desktop called tmp.txt, looks something like this but longer:

<https://i.gyazo.com/a2678c17e3f8b05af93c55d1bcb3e0ef.png>

1. What website was the user trying to access in the port 80 session on IP 199.59.150.7 (hint: use

tshark)?  
Twitter.com  
<https://gyazo.com/1cad319876e4902c93c3d086be5a82a7>

Bonus: How did the server on IP/port 199.59.150.7:80 respond?

Moved permanently

<https://gyazo.com/6dd57b688c07a9c4457bdfd724769da3>