1. What are the two most common destination ports for this IP, by total bytes transferred?

443: 1.788MB

80: 914KB

<https://gyazo.com/8caa9160a43adc642dbf2356f50cffb6>

1. What destination connection did 192.168.19.255 talk to most, in terms of bytes?

23.0.60.207

<https://gyazo.com/c4e8574f4d05b975a07dd306abfe6cdb>

1. Can you figure out what this IP is?

Something to do with Akamai Tech. Inc. ?  
<https://gyazo.com/7b96100aa6a3204775cca2d18b68326c>

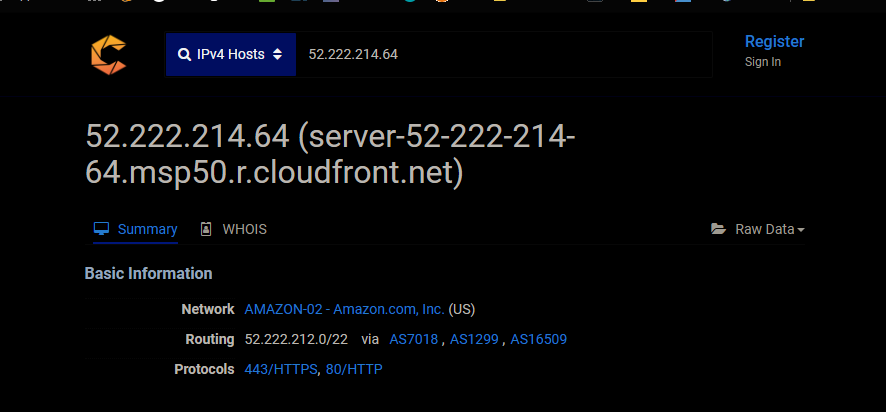
3. What destination IP did 192.168.19.225 talk to most, in terms of number of

connections?

52.222.214.64

<https://gyazo.com/9305aff78ebb57b4e9a90ef07d6f0a7f>

1. Can you figure out what this IP is?

Amazon?  
  
<https://gyazo.com/b3adbe2f8480383783d4169a9d71d937>

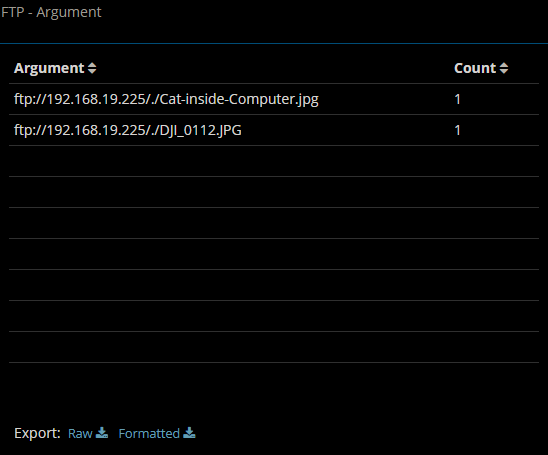
1. How many DNS requests did 192.168.19.225 make? What server was it using?

192.168.19.2  
<https://gyazo.com/5260404b7fba30630314bec911cdb7a6>

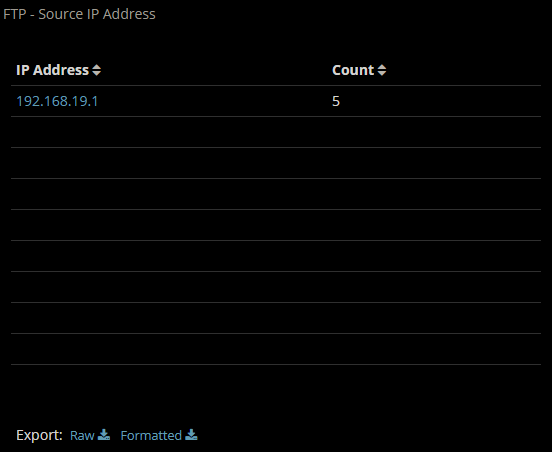
5. What domain did 192.168.19.225 request most often?  
cs9.wac.phicdn.net

<https://gyazo.com/02cd153f8945c35971f5ab517a2076eb>

6. What username was used to log in to the FTP server?  
  
<https://gyazo.com/2a3549c5d35deb45e591033bc928f82c>

7. What two file names were downloaded from the FTP server?  
Cat-inside-Computer.jpgand DJI\_0112.JPG  
  
<https://gyazo.com/77b9aa8169dc21d0c32bfb390d895ee3>

8. What system was browsing to the FTP server? That is, what IP address is the client at?

192.168.19.1  
  
<https://gyazo.com/6c43b4fe28add78a9759ce56f2abd009>

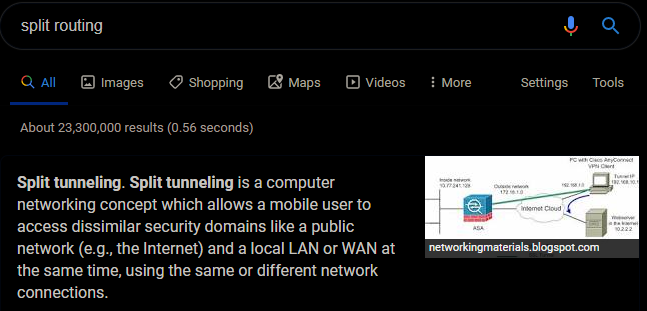
9. When browsing to a website, 192.168.19.225 got an HTTP 301 Moved Permanently

response. Which IP address provided this response?

I’m having some difficulty viewing the related widget.   
Gif demonstrating my issue:   
<https://gyazo.com/aeedf79da629e2f76a4233f5e3b80285>  
there seems to be some confusion within the program, because on inspection it *does* have the data, there was a ‘moved permanently response, but it just doesn’t display it…

10. Bro found quite a bit of traffic that it categorized as weird. What were they? Conduct a

bit of research – would you say this this traffic is weird? Would you say it is malicious? Explain the various types found.

Split routing: seems normal, someone leaves their phone set to both WIFI-ON and Mobile-Data-ON  
  
<https://gyazo.com/edb287b95117b7ffa3093d2db3e92909>

Data\_before\_established: seems like it goes hand in hand with split routing, a connection established over the alternate network (their mobile network) suddenly starts recieving data over our wifi network.

inappropriate\_fin: results from split routing as well, when BRO doesn’t see half of the FIN exchange

above\_hole\_data\_without\_any\_acks: seems like a record of connections that have been dropped due to apparent packet loss? It seems that if too much data is received after a break in the ack sequence, the connection is just dropped. from what I could gather here: <https://docs.zeek.org/en/stable/scripts/base/init-bare.bro.html?highlight=above_hole#id-tcp_max_above_hole_without_any_acks>

I didn’t find many specifics on bad\_udp\_checksum, or bad\_IP\_checksum… on a tangent I found something about the bad ICMP and TCP checksums being generalized as suspicious/bad traffic, and recommending blocking the ip addresses… I am going to assume the same is true of these two, but I still am unsure about what the bad checksum indicates… would it suggest someone is using something like a burp? (I would assume burp and similar software would adjust the checksum to match any edited data.)

Similarly, not much came up from ip\_hdr\_len\_zero, but just from the name I can understand why it would be suspicious traffic.