Jackson Warren

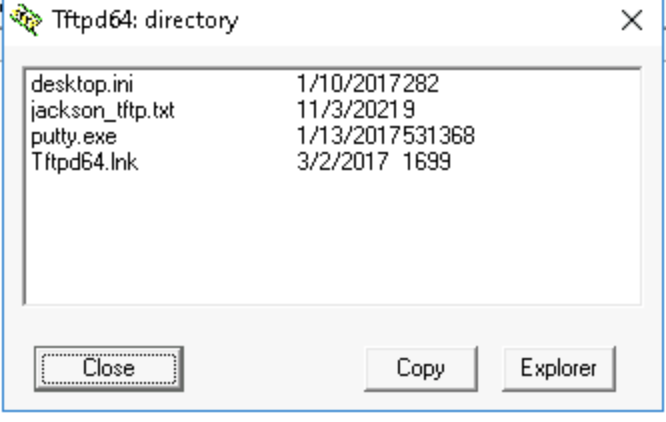
Jeremy Bergen

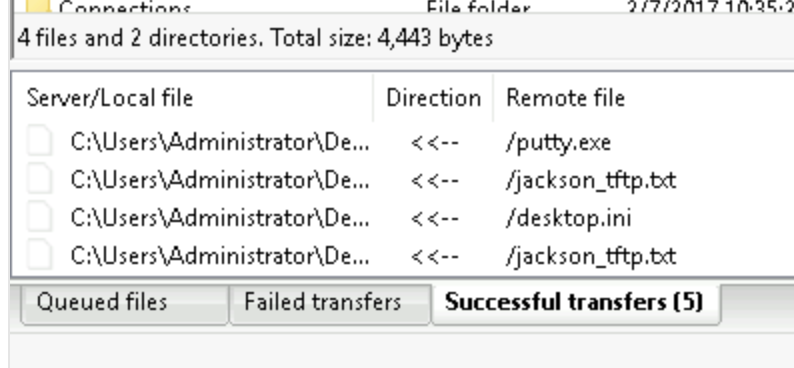
CSCI 370

11/15/21

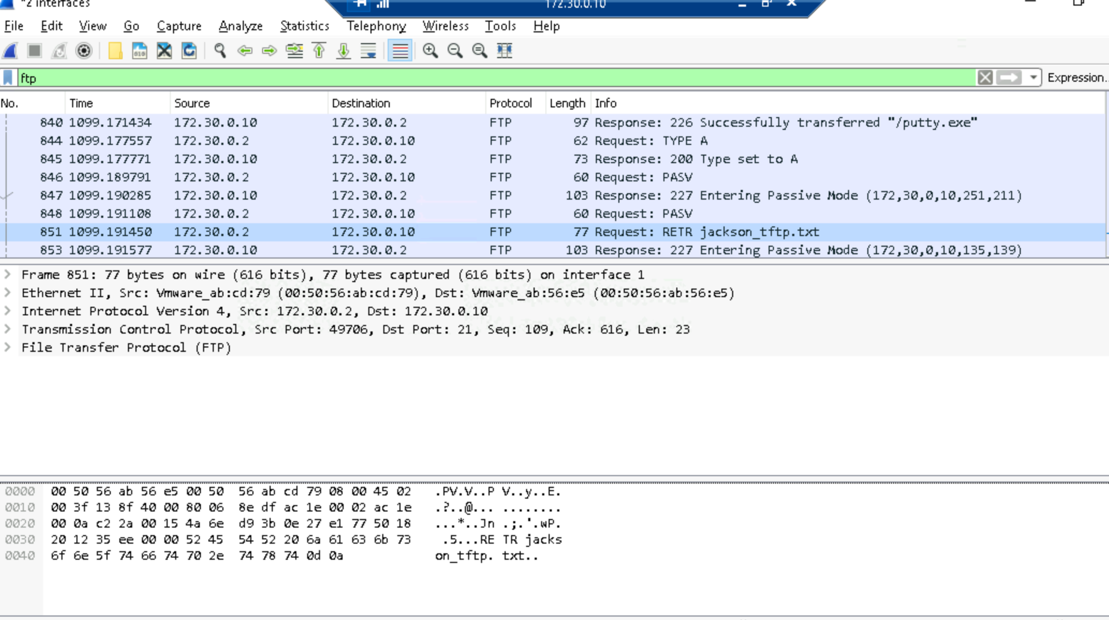
Week 11: Lab 10

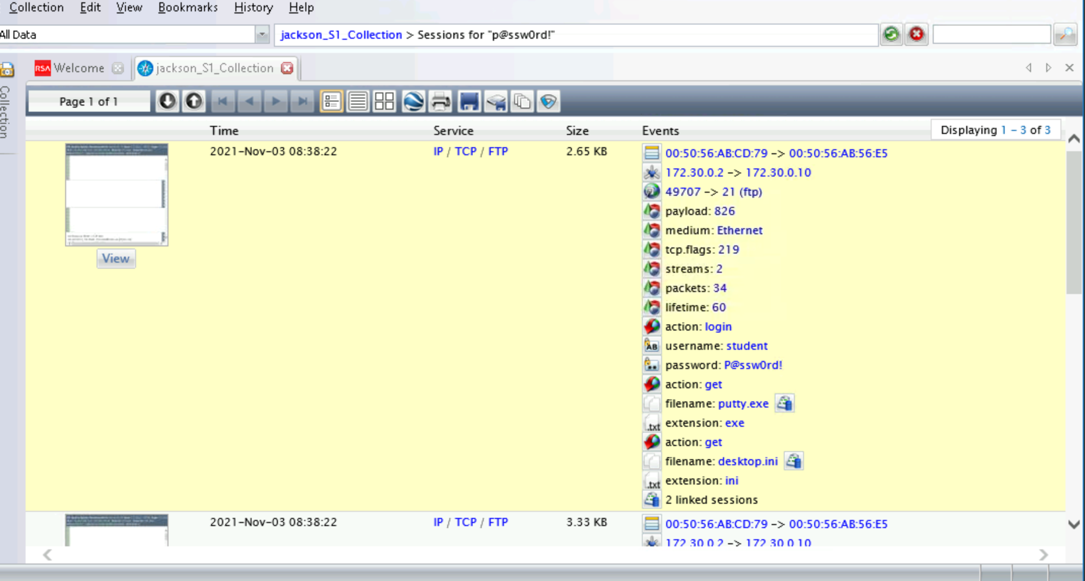
Section 1:



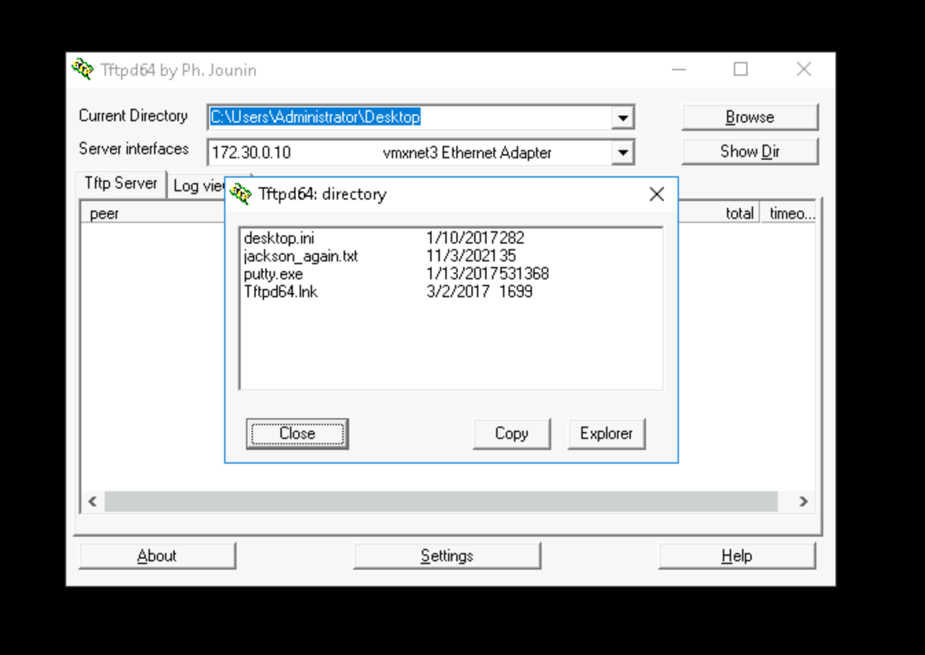


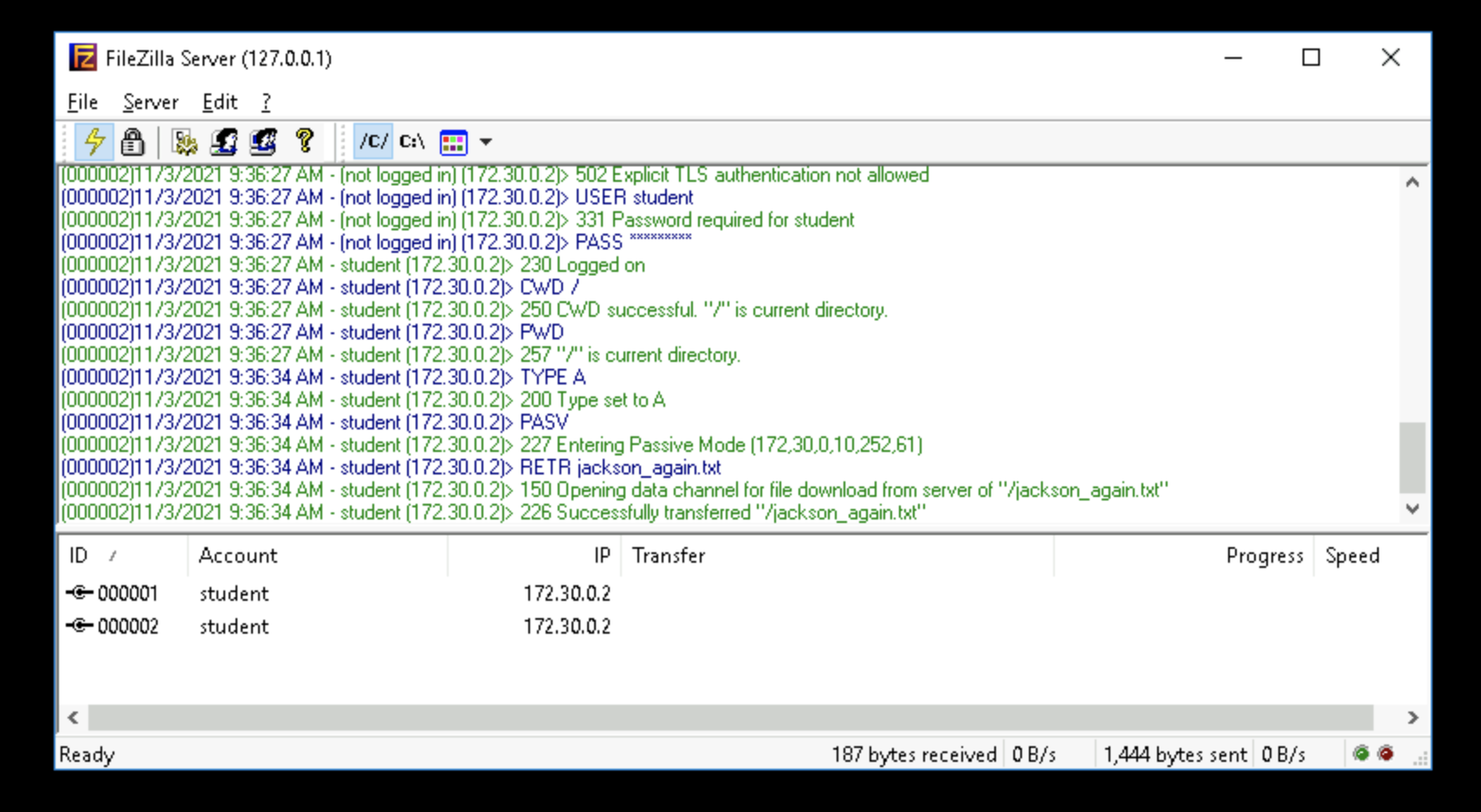
Accidently downloaded another folder too

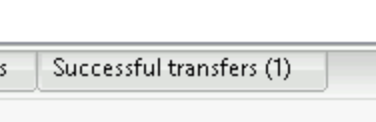




Section 2:





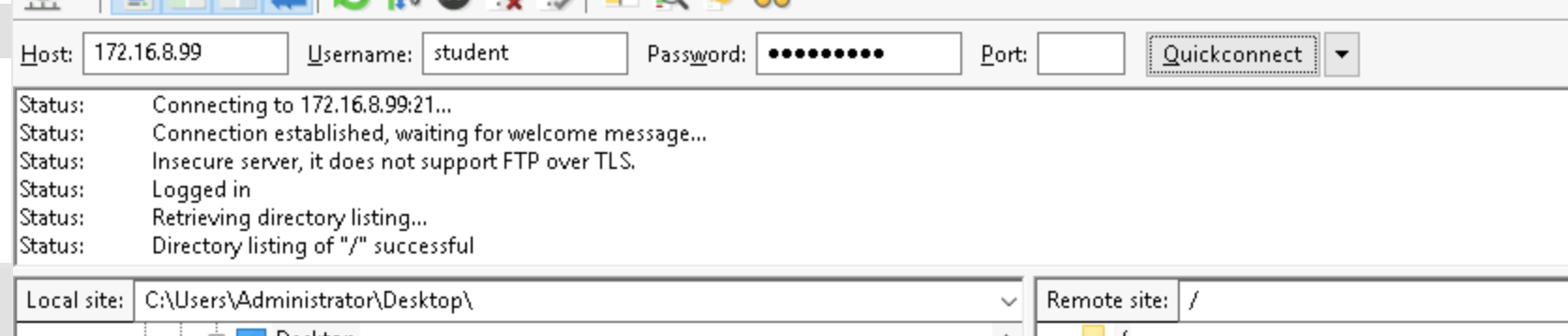
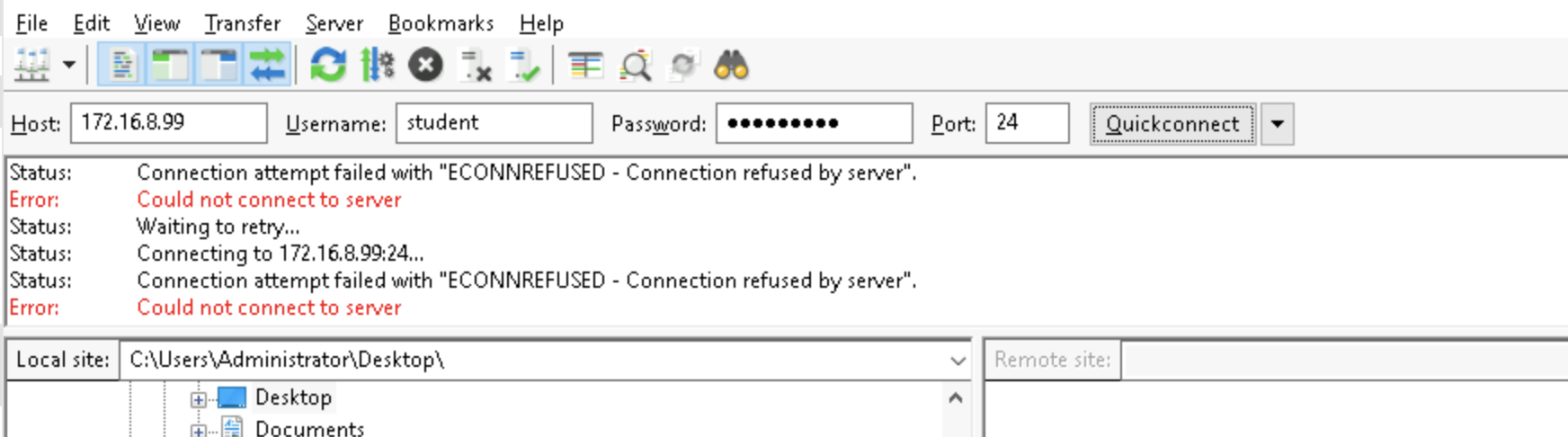
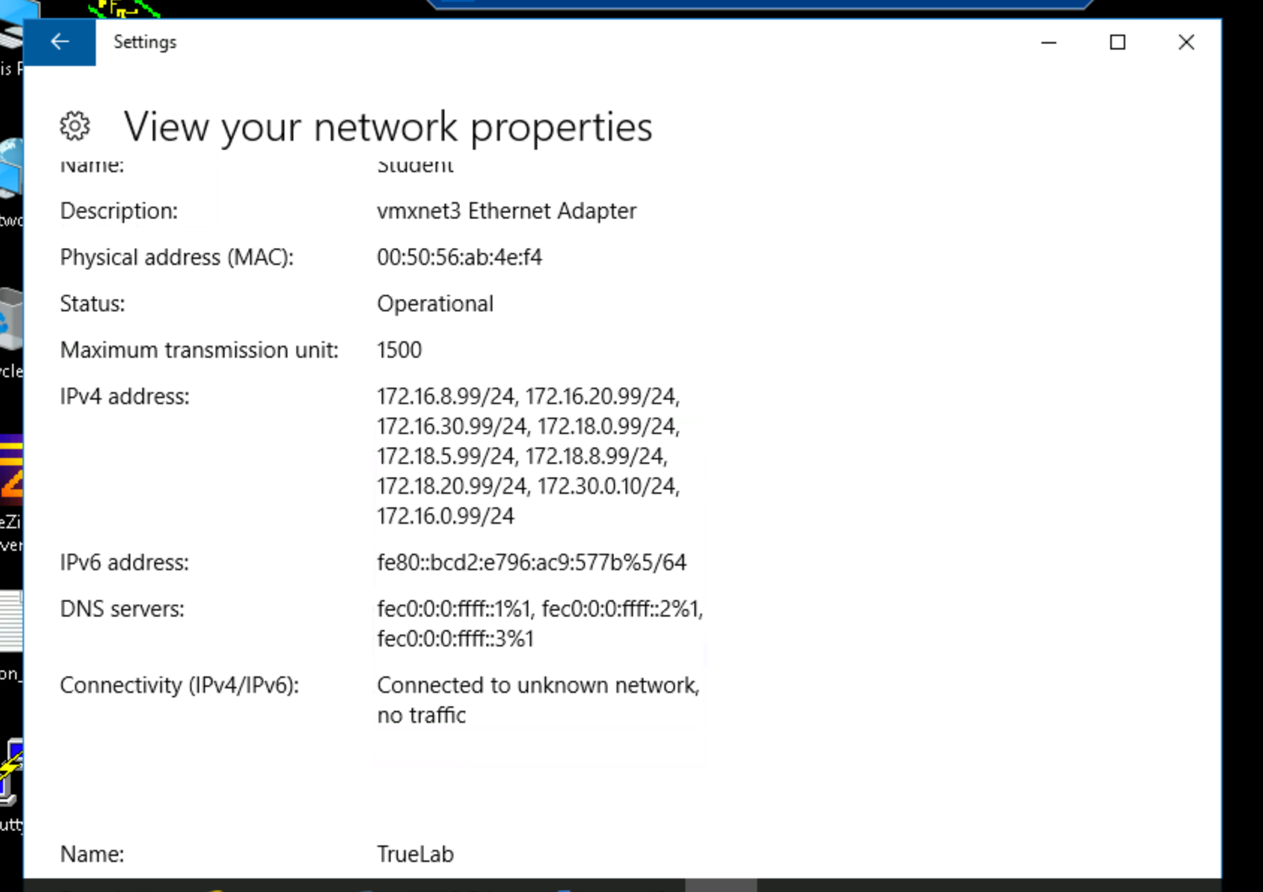


Ok, so. I have made a fatal error. I forgot to click the little shark fin for the entire last part and therefore, my data was not being stored on WireShark. I could go back and redo it but I feel like I already know what I’d be looking for from the last part… So, just imagine pictures of me viewing the cisco passwords and some “Oooo’s” and “Ahhhhh’s” when not being able to when it’s SSH, and reading my text file that says “I like big numbers and I cannot lie”.

I have now realized this will of course also screw up part 3 of Section 2 since I won’t have the WireShark code to analyze using the RSA software. So, imagine me now having a screen shot showing the details of the text file.

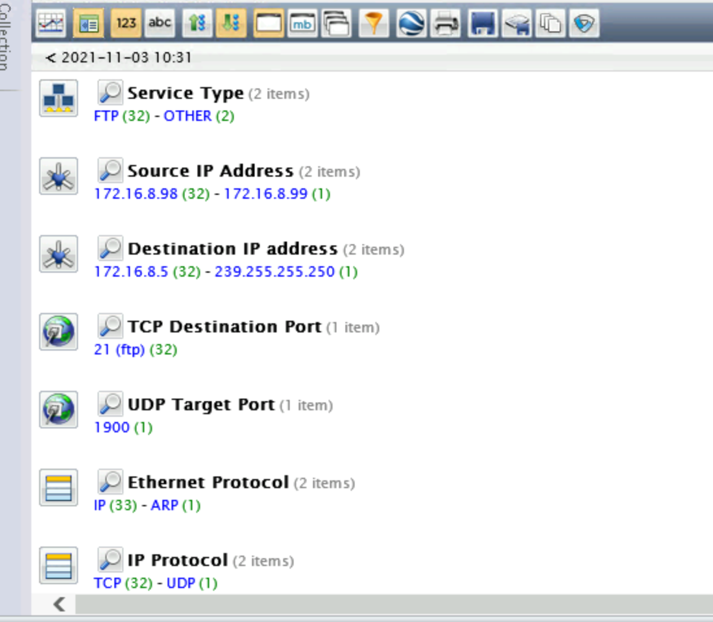
Section 3:

Part 1: The only IP addresses I saw were the ones involved in our lab. This includes: 172.30.0.20, 172.16.8.5, and 172.16.20.5. I did not notice anything out of the ordinary.

Part 2: 

Oh, look at that, it worked! After I used port 21 again. I was thinking that maybe the /24 was port but it was not.

Part 3:



I believe the way you’d detect someone trying to access you through RSA is recognizing a large amount of Source IP Addresses, which would be someone sending us a lot of traffic from a single IP. We realize that a single IP is spamming us with requests and therefore may be attacking us trying to brute force our password. With way way more attempts, I think this would be much more obvious too when you see thousands of requests from a single IP. We can then also click on those requests and further analyze this, looking at the requests they were making to confirm these suspicions.