Install WireShark, T Shark, or a similarNprogram. newer versions of WireShark may differ slightly from the installation screenshots in the slides.

-Packet captures are here: [https://umd.box.com/s/g9zo7lelfm5si4p53sfdwvunz52odgo1 (Links to an external site.)](https://umd.box.com/s/g9zo7lelfm5si4p53sfdwvunz52odgo1)

-Provide a screenshot and written explanation of what is happening for each question number below.

1. Inside the example1.pcap packet capture is a copy of obiwan.exe, extract it using the methods demonstrated in the class lecture on Network forensics. Provide a screenshot of how you extracted it, with your name somewhere very visible in the screenshot.

2.Run obiwan.exe on a Windows system (It is NOT malware, but if you want to be Super safe build a VM and run it in there) Provide a screenshot of Obiwan.exe running.

3.Start a packet capture with Wireshark/tcpdump on the system you are running obiwan.exe. Provide a screenshot of the traffic or capture of obiwan.exe running, with your name visible somewhere in the screenshot.

4. Review the network traffic from Obiwan.exe. Provide a written detailed description to what computer activity(s) obiwan.exe performs?

Provide a screenshot with your answer for #4 but the written description is most important to get full credit.

Submit the assignment in the exampled report format (In theAnnouncements section).