Wireshark

In this lab, you will use Wireshark to search through a traffic capture and derive conclusions about the packets that are captured. A pcap file is attached in D2L that contains the specific traffic capture for the lab. You can verify that you have the correct file by going to Statistics > Capture File Properties and verifying that there are 16133 packets captured.

Answer the following questions below with both the answer AND a screenshot showing your search and how you got your results.

1. What is the IP address of the client in the capture?
2. What is the operating system of the client in the capture?
3. What is the username/password to the FTP server?
4. Take a screenshot of one of the jpg files that were transferred over FTP (this was not shown in class, you will need to research this). Take a screenshot of the actual image, not just the packets.
5. There was an error browsing a particular website. What was the URL and the error?
6. The user visited 3 websites, what were they (remember, other sites may have had requests, what sites did the user specifically go to)?
7. There was a DNS request for an MX record; what was it?
8. A request is made to “something”. msftncsi.com -> what is this for?
9. What “hardware” was the machine involved in this capture running on?
10. There’s a file transferred over HTTP called “success.txt”. Where is it from, what are its contents, and what is its purpose?