A06 – Wireshark

**10 points**  
Turn in a Word or PDF document to the D2L Dropbox

**Overview**

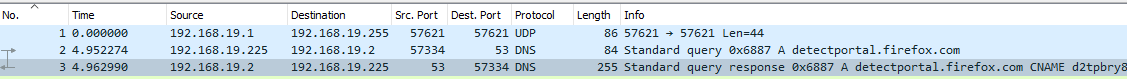
In this lab, you will use Wireshark to search through a traffic capture and derive conclusions about the packets that are captured. A pcap file is attached in D2L and to this document that contains the specific traffic capture for the lab. You can verify that you have the correct file by going to Statistics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

The packet capture can also be downloaded at this link: <http://weluc.com/lab06.pcap>

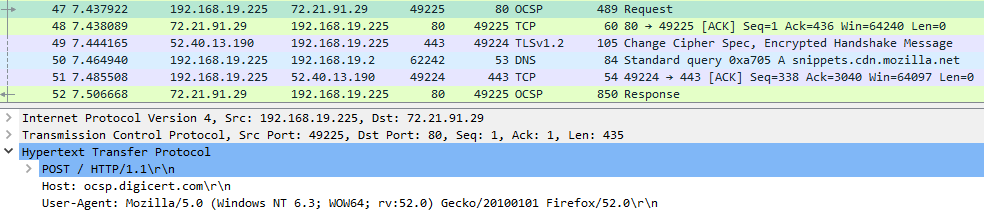
## Deliverable

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

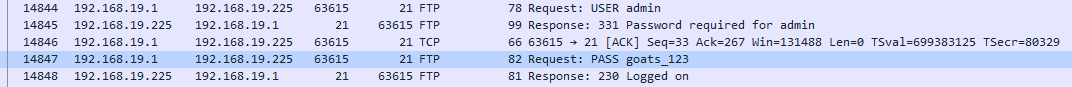
1. What is the IP address of the client in the capture?

The client 192.168.19.225 is the main actor in this pcap. First request it appears in is a dns request to 192…2  


1. What is the operating system of the client in the capture?

Packet #47 posts a certificate verification request to a web-based certificate Authority, and it reports it’s OS in the User-Agent Field to be Windows  


1. What is the username/password to the FTP server?

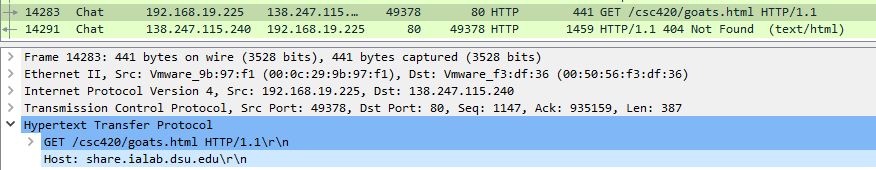
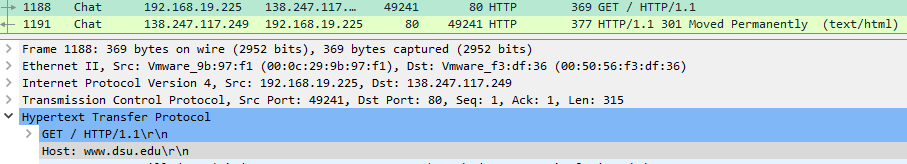
Username: admin Password: goads\_123  


1. 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.

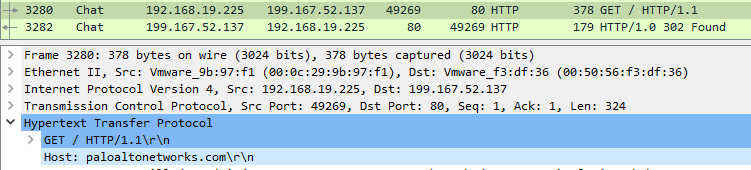


1. There was an error browsing a particular website. What was the URL and the error?

The request was for “share.ialab.dsu.edu/csc420/goats.html” and it returned a 404 error… There was another 404 error just prior - when trying to open the “/favicon.ico” file under the same domain

  
I also found an Error#301 “Moved Permanently” when trying to visit dsu.edu  


1. The user visited 3 websites, what were they (remember, other sites may have had requests, what sites did the user specifically go to)?  
   share.ialab.dsu.edu, paloaltonetworks.com, and dsu.edu (two of said requests are pictured in the previous question)



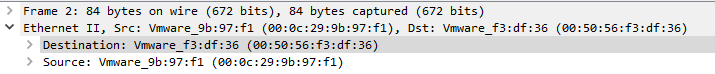
1. There was a DNS request for an MX record; what was it?

Request for dsu.edu  


1. A request is made to “something”. msftncsi.com -> what is this for?

This is Windows’ way of measuring / determining network connectivity status  
<https://www.techrepublic.com/blog/data-center/what-do-microsoft-and-ncsi-have-in-common/>

1. What “hardware” was the machine involved in this capture running on?

Vmware   


1. There’s a file transferred over HTTP called “success.txt”. Where is it from, what are its contents, and what is its purpose?

This is a file that Firefox will request on startup to detect if it is trapped in a captive portal, the file is hosted on the web under their domain “detectportal.firefox.com.” if it gets a success, then it is not in a captive portal and has internet access. If it fails to retrieve the file then it is either in a captive portal, or does not have internet connectivity.