# JAMK University of Applied Sciences

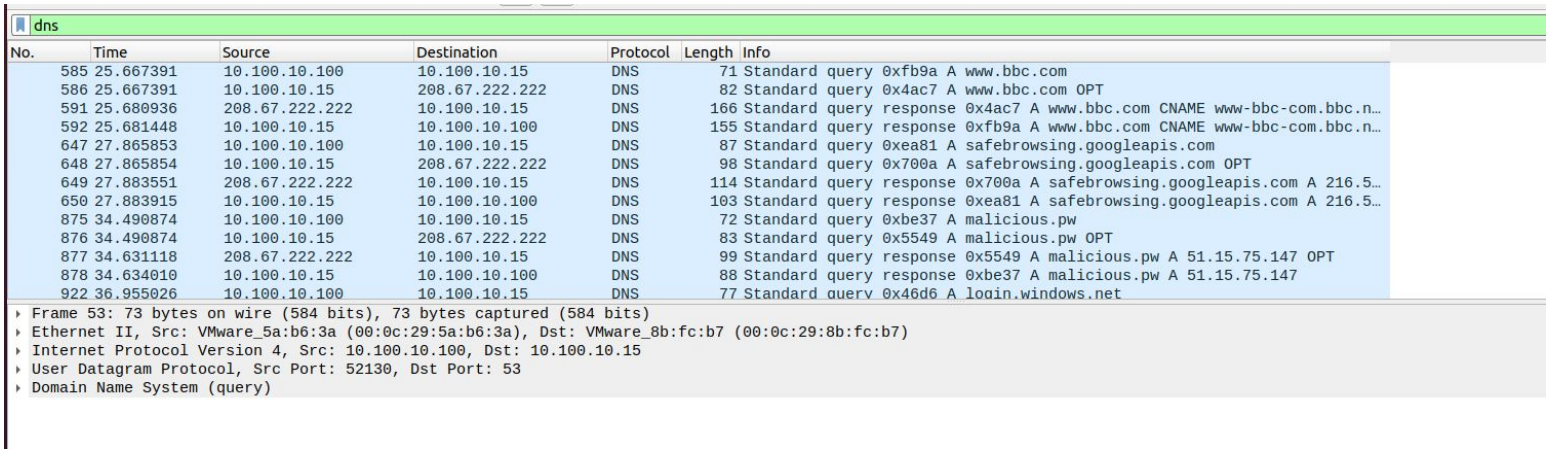
Data Security Testing

# Laboratory 1
# Network audit File

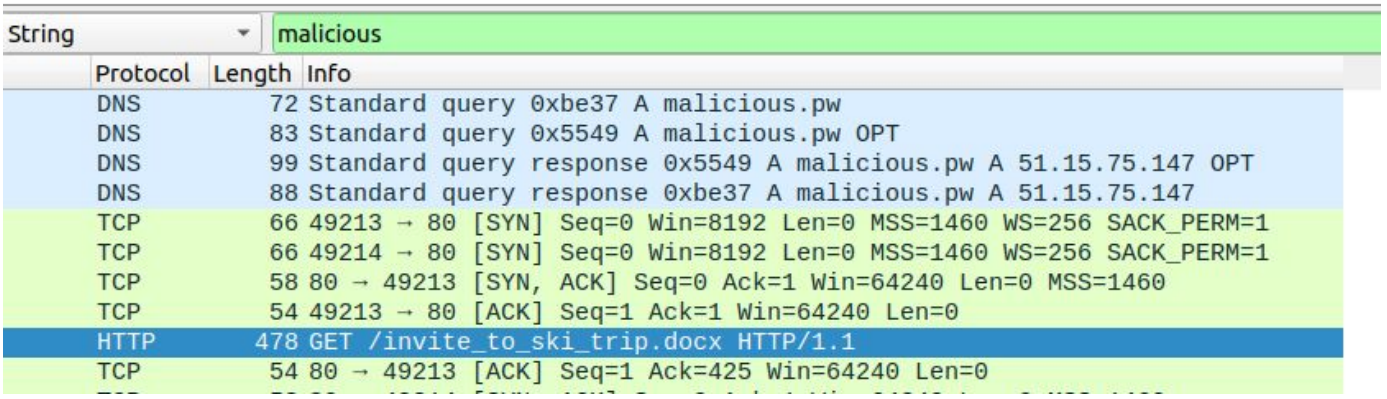
Teacher: Markku Vajaranta
Autor of Assignment: Adam Pawełek
Group: TTKS0700-3001
Jamk number: AA4917

# Assignment 1

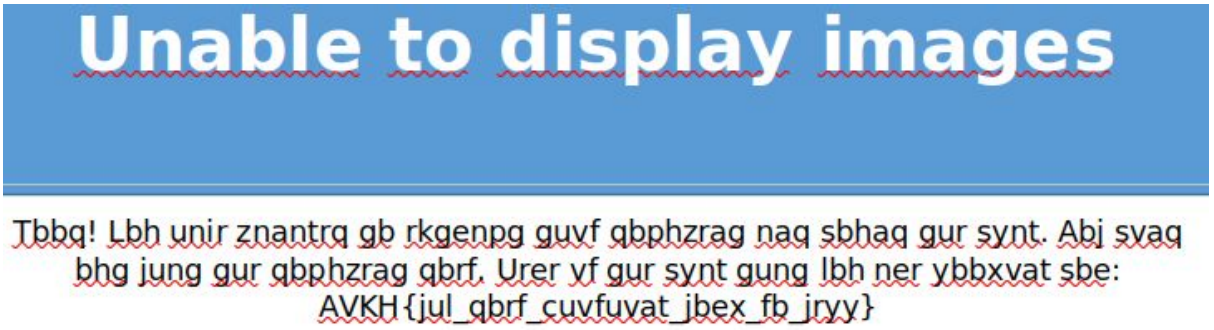
I started my search in Wireshark with a dns filter. This was what Wireshark returned as a result.




I found out that some of dns protocols come from malicious sites.
After I used filter with word “malicious” I saw that the first GET HTTP request was file invite_to_ski_trip.docx



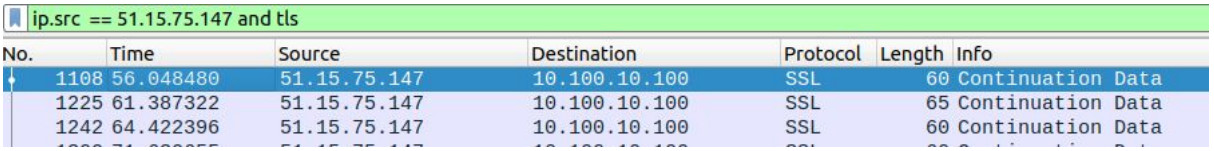

Then I opened the invite_to_ski_trip.docx and saw the text with the similar format to the nixu flag after decrypt it with Caesar cipher (ROT 13) I found the flag which was: NIXU{why_does_phishing_work_so_well}



Good! You have managed to extract this document and found the flag. Now find out what the document does. Here is the flag that you are looking for:
NIXU{why_does_phishing_work_so_well}

# Assignment 2

First I tried to find tls connection  between 51.15.75.147 (malicious source) and infected computer.




After Follow TCP  stream showed the data how the infected program works.


Then when I was scrolling down through the data I found that program type cleartext.txt (the same name as in the HINT) and displayed data looks like a NIXU flag. I decrypted it with ROT (1). The second flag is : NIXU{wh4t_1s_th1s_cl34rt3xt_tr1ck3ry}