# 

LAB 1

Data Security Testing

Jere Pesonen – TTV18S1

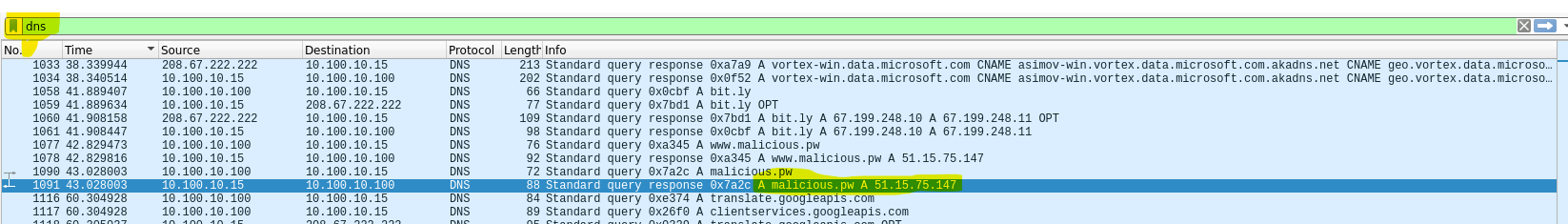
M3227@student.jamk.fi

10-2020

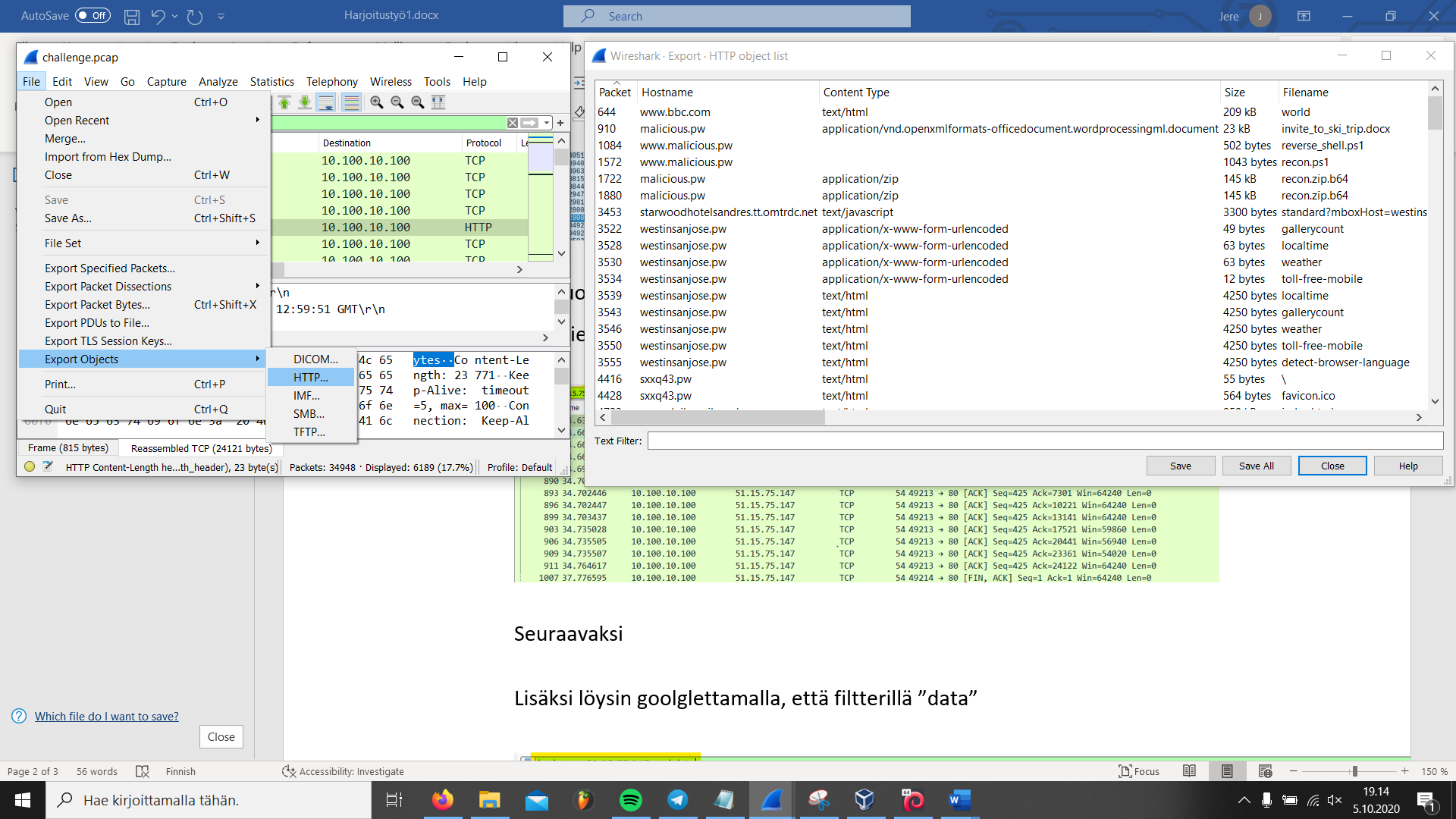
Tieto – ja viestintätekniikka

Tekniikan ja liikenteen ala

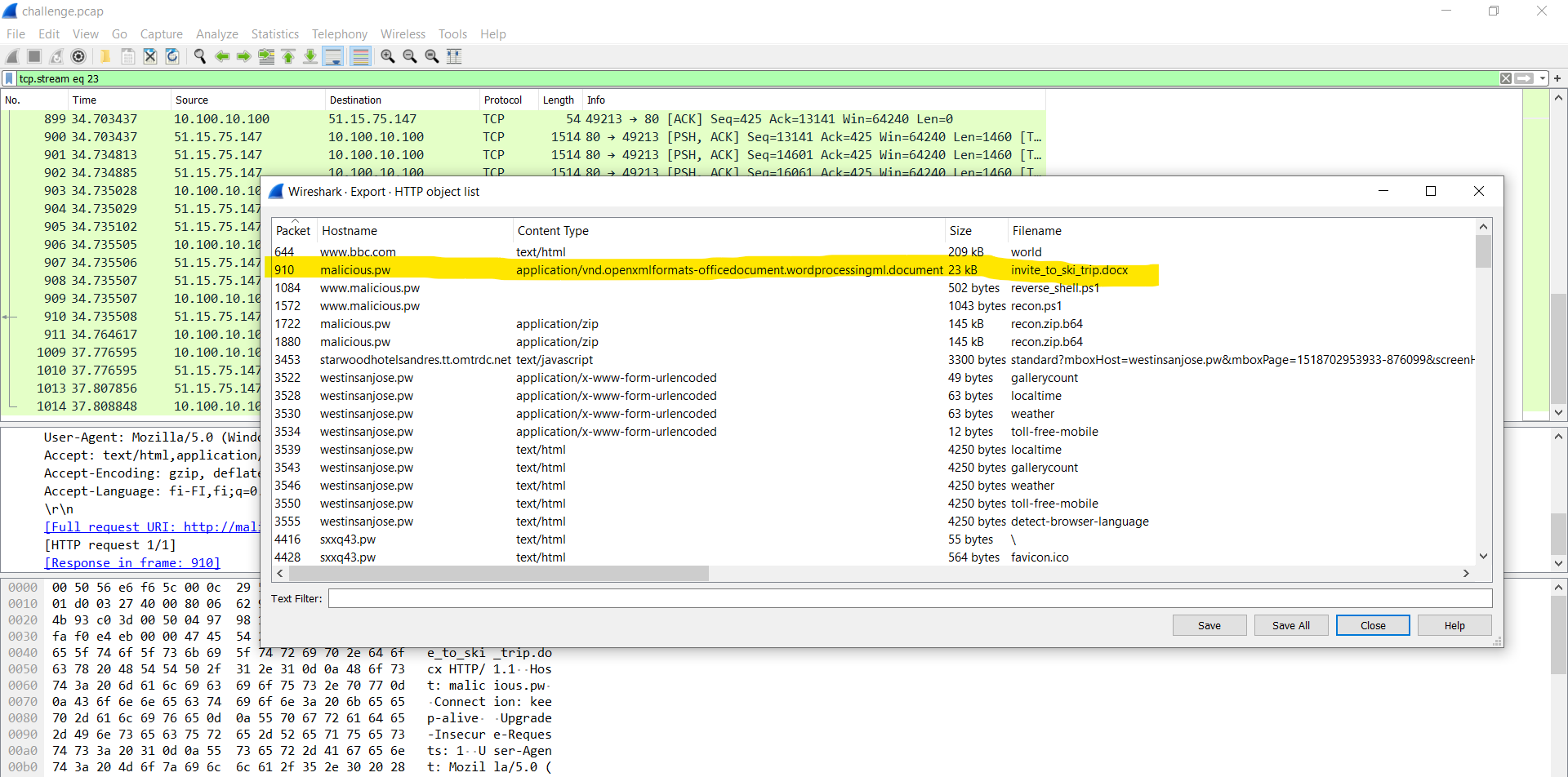
Phishcap – Part1

I started with the tip and filtered traffic with ”dns”. There were query for malicious.pw, which indeed sounded suspicious. Sites ip was 51.15.75.147.

I filtered traffic with destination to that ip and found interesting GET request, for docx file ”invite\_to\_ski\_trip”.

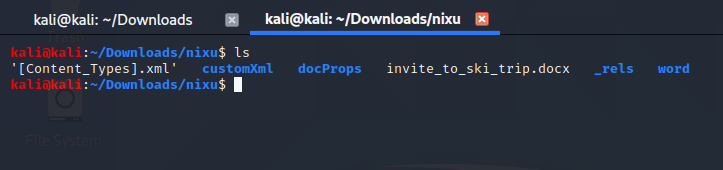


With ip source filter i found the file itself. I downloaded the docx file from to my kali virtul machine, from file/export objects/http. Packet 910



the flag can be found at the word document, but i desided not to open it, but unzip and find the flag from xml files.

on kali i unzipped docx file and got:



the content of the word document itself can be found at word/document.xml.

I copied the content of document.xml file to browser tool which pretty prints xml. And first flag was found.

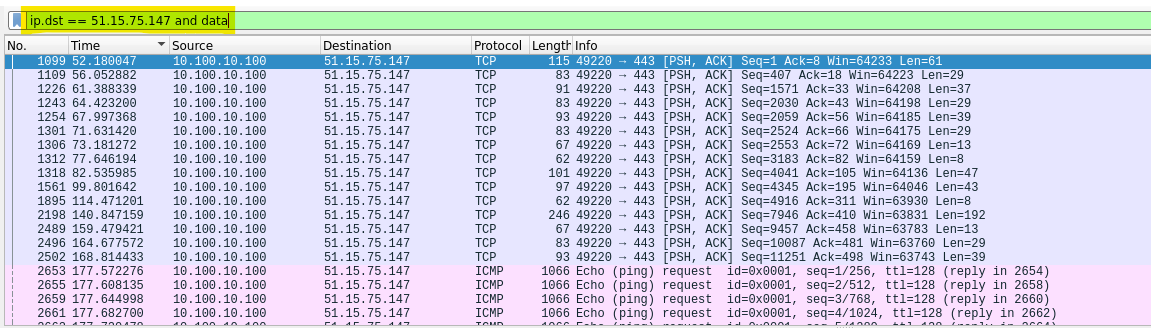


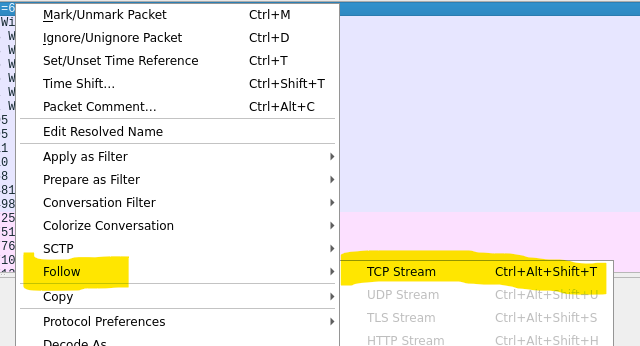
it was encrypted with ceasar cipher with rotation of 13 (or rot13).

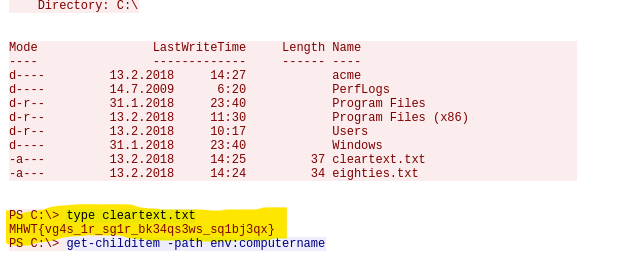
Flag = NIXU{why\_does\_phishing\_work\_so\_well}

Phishcap – Part2

Second flag i found with a little accident. I just added ”data” to search parameters, and followed tcp stream. then i scrolled down tcp stream for a while, and file cleartext.txt was opened, and it cointained encrypted flag.







Flag was encrypted the same as the first one

Flag: NIXU{wh4t\_1s\_th1s\_cl34rt3xt\_tr1ck3ry}

There were also GET request for ”reverse\_shell.ps1” file between the packets. I think hacker planted reverse shell script to target computer through ”invite\_to\_ski\_trip.docx” . So the tcp stream is hacker reading target computers files through ssl.