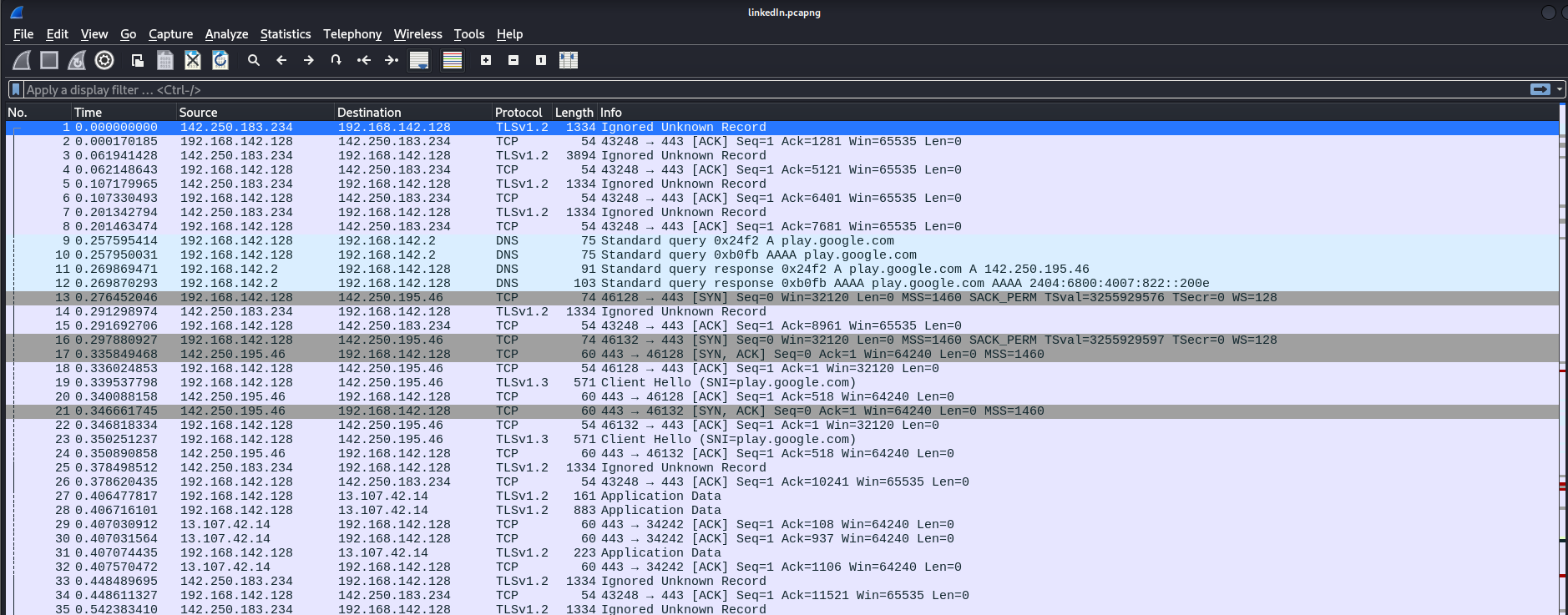
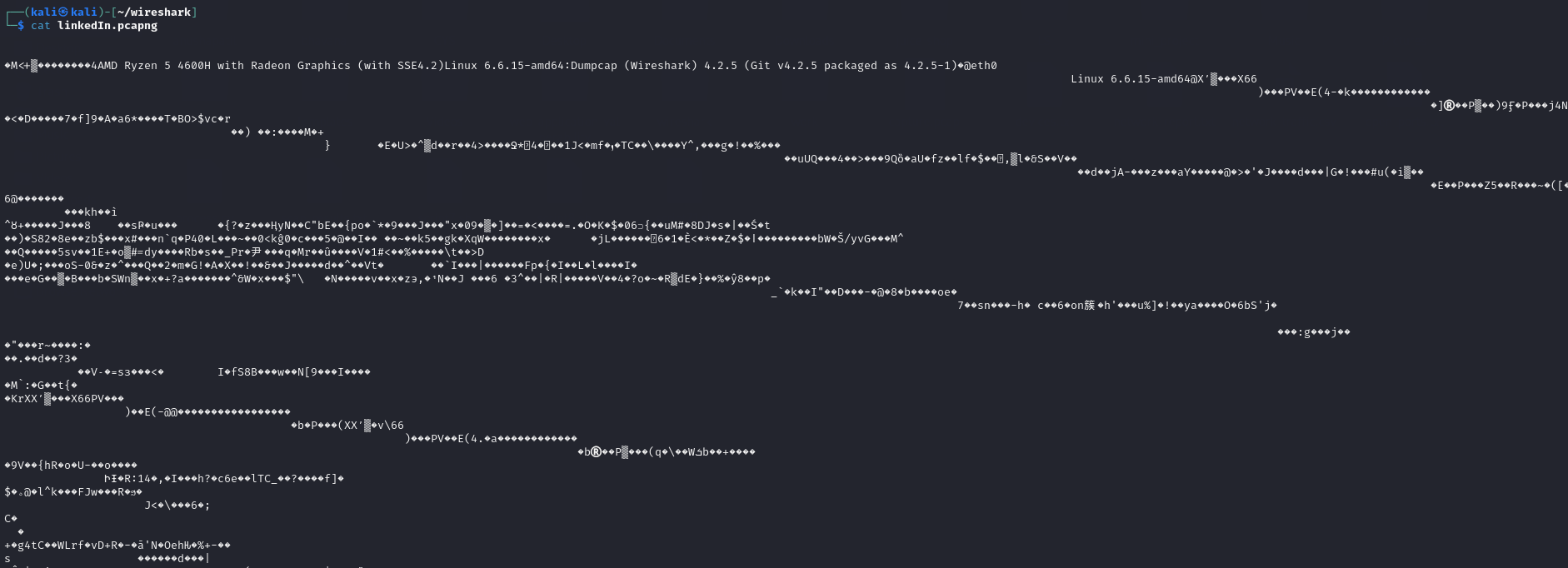
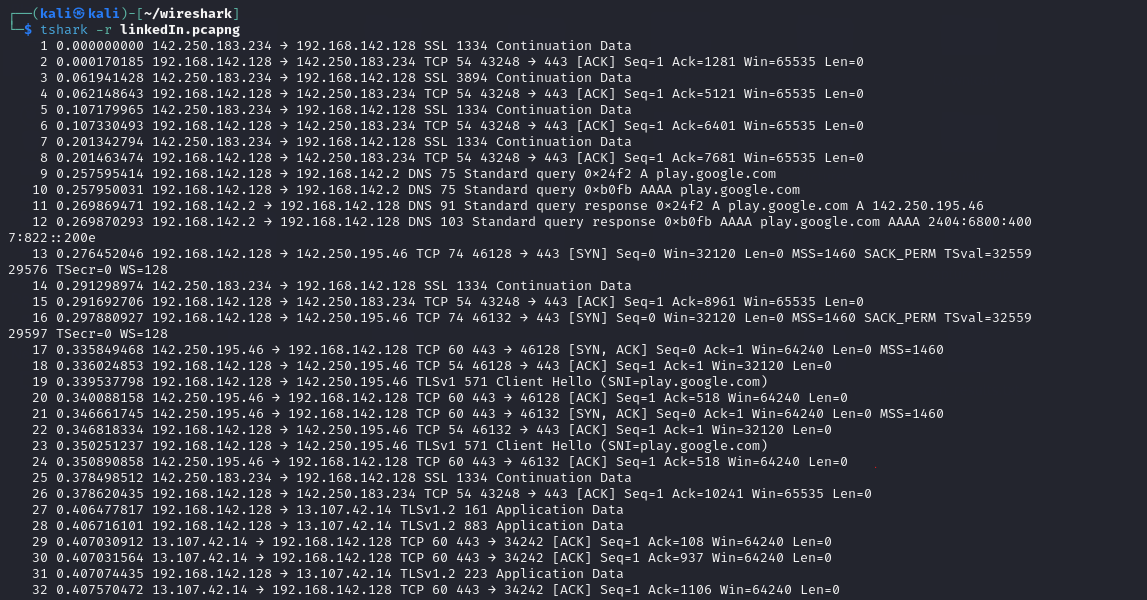
Wireshark Capture of [www.linkedin.com](http://www.linkedin.com)



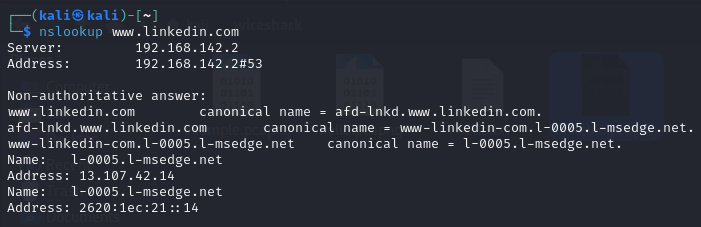
Normal wireshark file is stored in the .pcapng extention



Command to open .pcapng file in human readable form

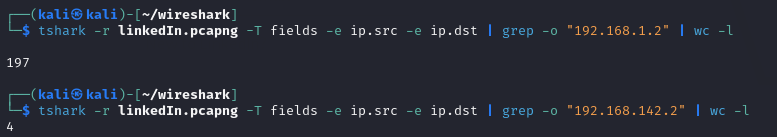


IP address of [www.linkein.com](http://www.linkein.com)



Using grep

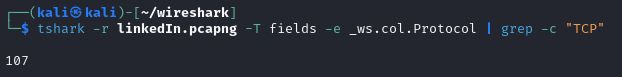
1. How many packets contains a specific IP address



1. Packets contain keyword “google”



1. Number of packets containing TCP protocol

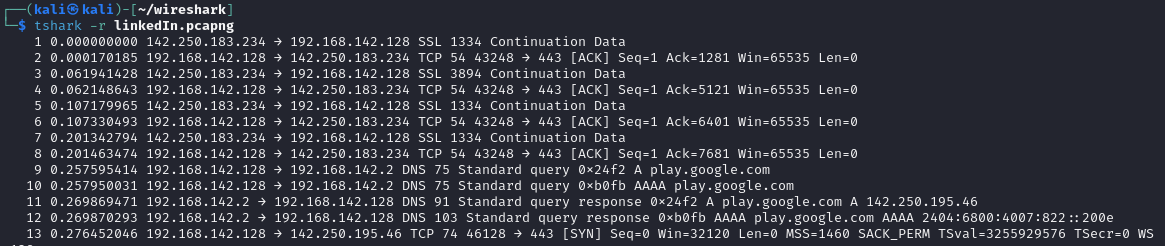


Using sed

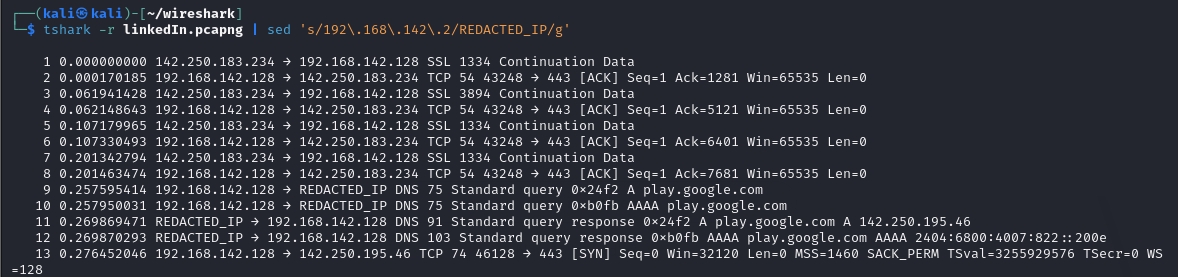
1. Replacing all occurences of a IP address with the RADACTED\_IP

REDACTED\_IP is a placeholder term used to mask or hide the actual IP address, 192.168.1.1. The purpose of using REDACTED\_IP is to anonymize sensitive or private information, like internal IP addresses, while still preserving the structure of the output

Before the command

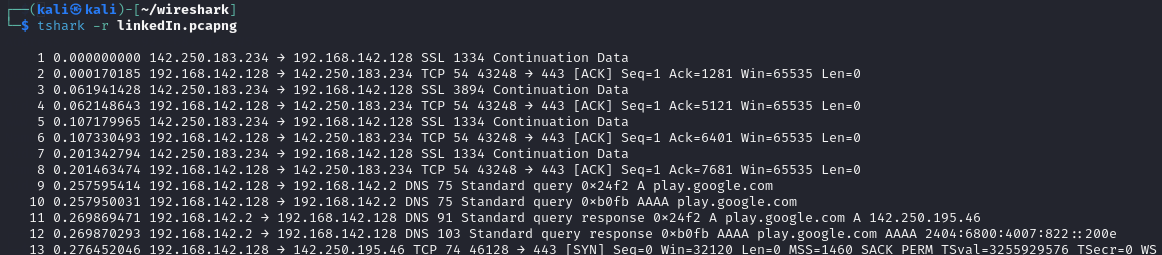


After the command

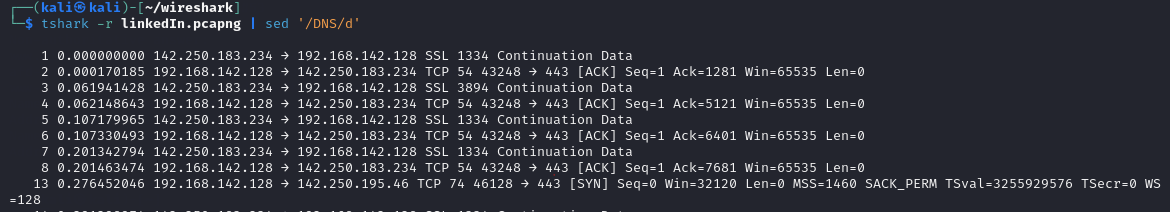


1. Removing all line with the protocol “DNS”

Before deleting DNS

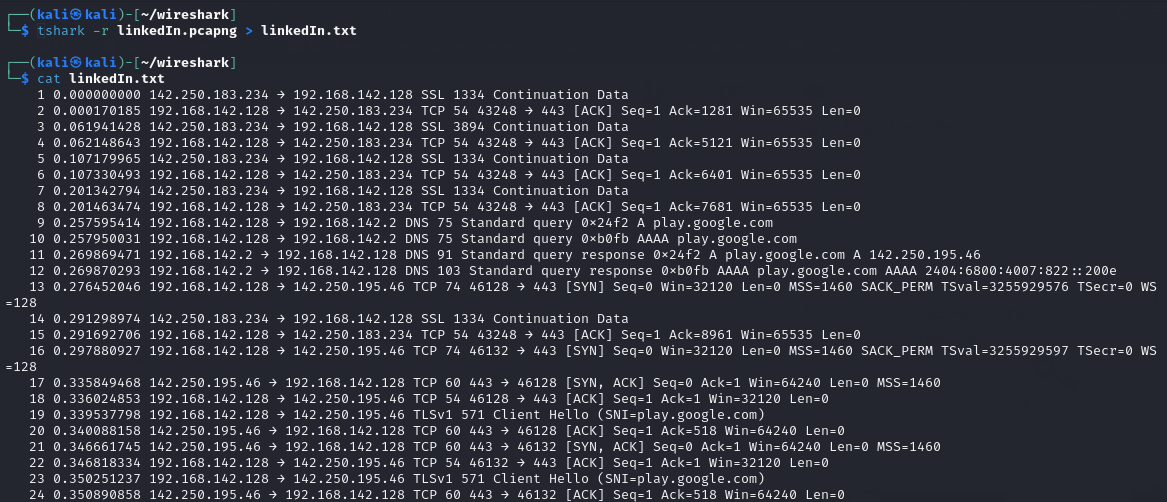


After deleting DNS

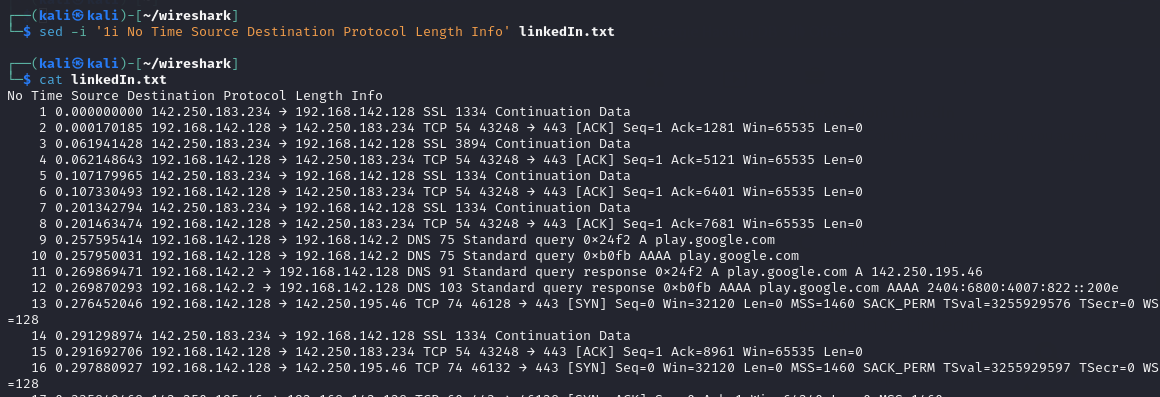


1. Adding header

Redirecting linkedIn.pcapng to linkedIn.txt

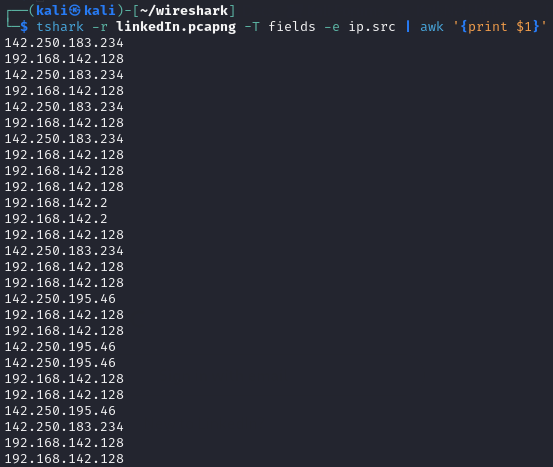


Adding header

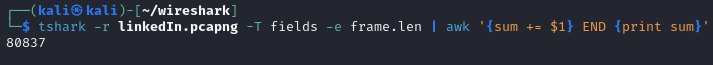


Using awk

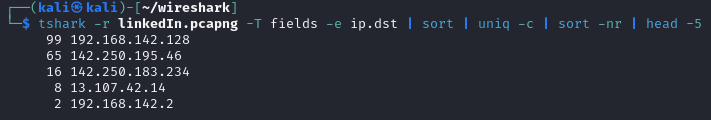
1. Print only source IP



1. Total number of bytes transferred



1. Top 5 destination IP : output contains the number of packet sent and the IP address

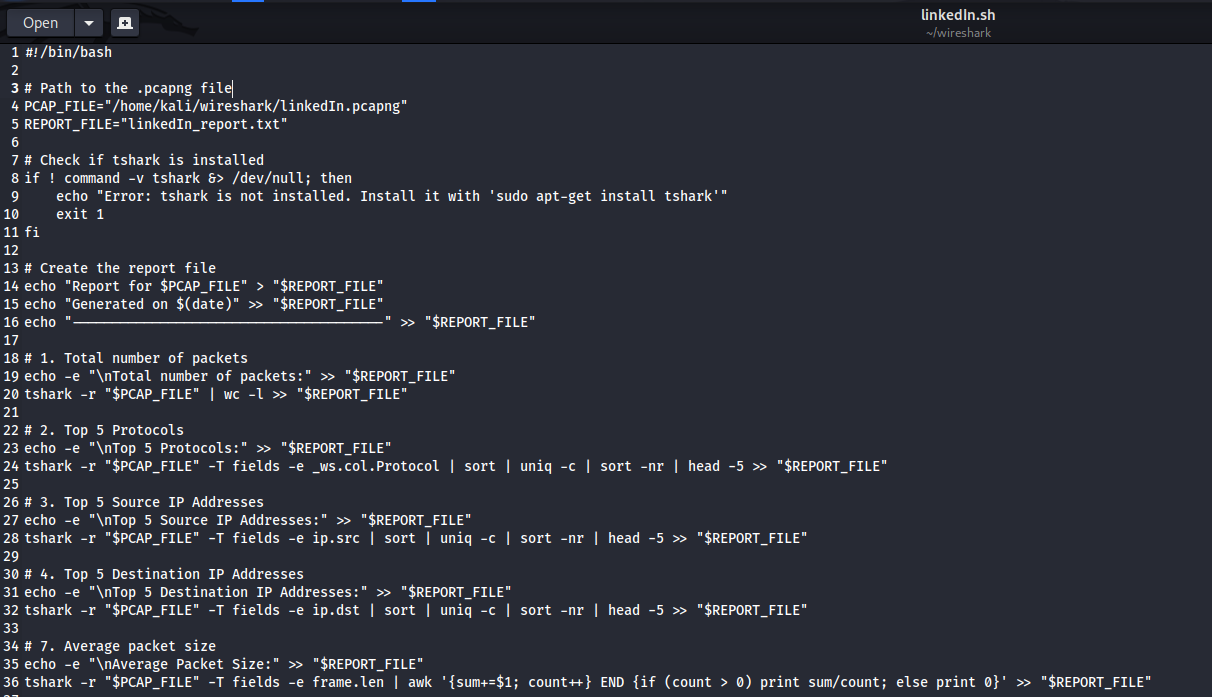


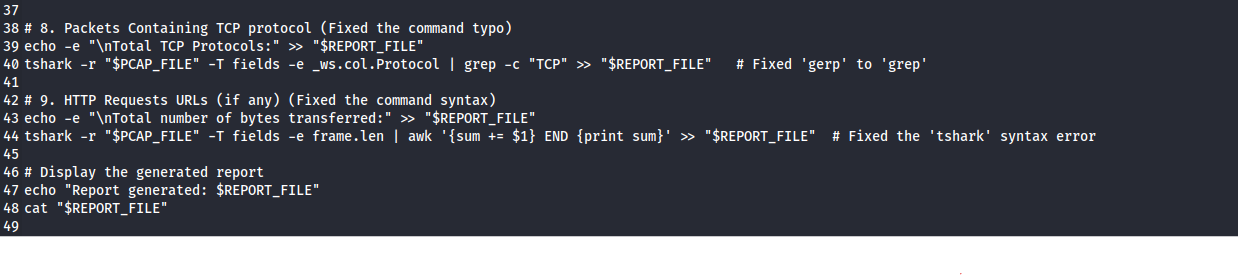
1. Average packet size



SCRIPT FOR REPORT GENERATION

Script





Output

