# Digital Forensics - Project Report

Eugen Saraci
eugen.saraci@studenti.unipd.it

January 9, 2019

# Chapter 1

# Introduction

*This work is mainly based off the research papers [1] and [2], the goal is to replicate and possibly improve some of the resulsts achieved in the cited papers.*

## 1.1 Introduction

### 1.1.1 Traffic Analysis

In the last years the expansion of SSL/TLS has made it harder for attackers to sniff passwords or clear text information through packet sniffing or, more in general, through network traffic analysis. The main reason for this is that SSL/TLS provides a cryptographically secure payload encryption, which means that even though packets can still be easily captured, no useful information can be inferred from the payload content without having the encryption keys. It is worth mentioning that the endpoints of the communication (i.e. source and destination IP adresses) are transmitted in clear text for routing purposes; by performing a DNS lookup of the addresses and attacker could easily infer what site a user is visiting. While we can still try to hide these information by using a VPN (or a proxy server), for many users this issue does not represent a relevant privacy problem, therefore no countermeasures are usually adopted in non privacy-critical environments.

### 1.1.2 Inferring user actions

In this work we show that by using a combination of machine learning algorithms we can correclty infer user actions through encrypted traffic analysis. It needs to be noticed that we totally ignore the payload contents, while we focus more on a structure we call *flow*, which is a vectorial representation of the packets exchanged between the source and the destination.

# Bibliography

[1] Mauro Conti, Luigi V. Mancini, Riccardo Spolaor, and Nino Vincenzo Verde. 2015. Can't You Hear Me Knocking: Identification of User Actions on Android Apps via Traffic Analysis. In Proceedings of the 5th ACM Conference on Data and Application Security and Privacy (CODASPY '15). ACM, New York, NY, USA, 297-304. DOI: https://doi.org/10.1145/2699026.2699119

[2] Conti, M., Mancini, L. V., Spolaor, R., & Verde, N. V. (2016). Analyzing android encrypted network traffic to identify user actions. IEEE Transactions on Information Forensics and Security, 11(1), 114-125.