# Forensic Investigation of the Dark Web and Cryptocurrency on iOS

Degree programme : MAS Digital Forensics & Cyber Investigation

The dark web and cryptocurrency have given cybercriminals a layer of protection by anonymizing their network traffic and transactions. This paper aims to provide artifacts of the usage of the dark web and cryptocurrency on iOS. We conducted a logical acquisition on an un-jailbroken device and a file system acquisition on a jailbroken device. The entire TOR browsing scenario and all transactions done with Metamask on the device were found with the file system acquisition.

## Introduction

Interpol defines cybercrime as “a fast-growing area of crime, more and more criminals are exploiting the speed, convenience, and anonymity of the Internet to commit a diverse range of criminal activities that know no borders, either physical or virtual” (Erdal Ozkaya, Inside the Dark Web, 2019). On the internet, the deep web and especially the dark web are where most criminal activities occur. To access the dark web, the most popular software used is the Tor Browser, which is an extended version of the Mozilla Firefox browser. As the dark web is highly encrypted, by its multi-layered encryption, tracing back actions to the user is extremely complex. Additionally, cryptocurrency is the main payment method used on the dark web. Investigating the dark web and cryptocurrencies is thus essential in the fight against cybercrime, however, such investigations demand lots of resources and in some cases remain impossible. Nevertheless, finding traces of TOR, and therefore illegal dark web onion sites, as well as illegal cryptocurrency transactions can be found at an individual level by conducting digital forensics analysis on the seized suspect devices.

## Objectives:

In our research, we wanted to provide admissible court incriminating artifacts of usage of the dark web and cryptocurrency on iOS, respectively the Onion Browser and Metamask applications. The following questions were asked:

- What artifacts can be extracted and where are they located?
- What differences in artifacts can we extract from a logical acquisition on an un-jailbroken iOS device and from a file system acquisition on a jailbroken iOS device?

## Methods:

We used the digital forensic tool, Belkasoft X for both, the logical and file system acquisition and analysis.

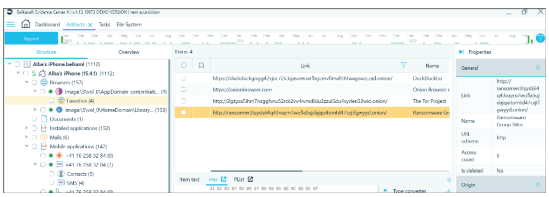
We used an un-jailbroken iOS X device version 15.4.1, and a jailbroken iOS 6 device version 12.5.1, using the Checkr1an jailbreak on the Checkm8 bootROM exploit.

## Results:

We were able to conclude that there were different artifacts acquired during the file system acquisition on the jailbroken iOS device which were not present during the logical acquisition. Additionally, we were able to demonstrate that a logical acquisition of an un-jailbroken iOS device provides some results, but limited results. However, a file system acquisition on a jailbroken device will provide more artifacts; in our research, we could see the entire browsing history of the Onion Browser and the full incoming and outgoing transactions history for Metamask.

## Discussion:

We wanted to focus on iOS, as there hasn’t been a lot of research conducted. However, the growing use of mobile devices is skyrocketing. To our knowledge, jailbreaking recent iOS devices with newer versions installed is impossible to perform as of date, therefore more research should be done in this regard. Moreover, our research focused on the Onion Browser and the Metamask applications, but many Tor and digital wallet applications exist on iOS devices, as such each application could be different and may provide different artifacts.



Belkasoft X - TOR Bookmarked Onions Links

Catalina Falo
cfalo@protonmail.com

Flamur Ramiqi