Tel. +39 02 365738
info@overneteducation.it
www.overneteducation.it

# OEC253

# OSINT - Investigazioni nel dark web e su crittovalute

Durata: 2 gg

## Descrizione

Il corso ha lo scopo di fornire una panoramica, teorica e pratica, del mondo delle reti anonime e delle crittovalute.
Gli aspetti tecnici sono propedeutici alla comprensione della parte pratica ed investigativa, in modo da avere un approccio più consapevole agli argomenti illustrati.
La conoscenza dei contenuti del corso è destinata a coloro che devono svolgere indagini e analisi nel mondo del Dark Web e delle valute virtuali.

## A chi è rivolto?

- analisti forensi
- analisti antifrode
- Forze dell'Ordine e Forze Armate
- giornalisti

## Prerequisiti

Buona conoscenza del

- sistema operativo Windows / Tsurugi Linux
- browser Firefox e Chrome

Conoscenza di base di

- rete internet

## Contenuti

Giorno 1

Anonimato in rete e best practices

- Cenni su indirizzi IP pubblici e funzionamento client/server di Internet
- Proxy, VPN e differenze
- Servizi privacy oriented
- Best practices.

Utilizzo di Linux (distro consigliata Tsurugi)

- Presentazione della distro
- Comandi base del terminale Linux (directory, permessi, installazione)
- Cenni sul networking (interfacce di rete, modifica IP locale e MAC address, configurare una VPN)
- Cenni su distro particolari (Kali, BackBox, Tails, Whonix, Kodachi, ecc).

Cenni sulle reti anonime

- I2P
- Zeronet
- Freenet
- Openbazar

La rete TOR

- Il protocollo TOR
- La navigazione in TOR
- La ricerca di siti e risorse (motori di ricerca, forum dedicati, raccolte).

Creazione di un hidden service

- Installazione di LAMP2
- Basi di HTML
- Creazione di coppia di chiavi e test della pagina.

I black market

- Principali categorie
- Principali black market per categoria
- Iscrizione e best practices (evitare tracciamento e portali SCAM)
- Simulazione di acquisto da vari market
- Metodi di spedizione e tecniche di ricezione
- Utilizzo dati storici per fini investigativi.

Creazione di un browser investigativo

- Creare un profilo Firefox o utilizzare la versione portable in ambiente Windows
- Utilizzo di Firefox per navigare in TOR
- Modifiche suggerite per la pagina “about:config” di Firefox
- Add-on suggeriti per analisi e raccolta di dati

Giorno 2

Le comunicazioni

- App e servizi utilizzati
- La chiave PGP
- Creazione, utilizzo e test di comunicazioni cifrate con PGP
- Analisi di una chiave PGP (strumenti software e online)
- Soluzioni software per utilizzo della chiave PGP (Windows e Linux)

I pagamenti

- Cenni sulle crittovalute
- Presentazione delle principali monete utilizzate
- Dove e come procurarsi monete virtuali

Utilizzo dei Bitcoin

- Principali wallet e tipologie
- Creazione di un wallet con Electrum
- Importazione di un wallet esistente (da seed e da chiave privata)
- Effettuazione di transazioni con Electrum
- Altre funzionalità di Electrum

Analisi dei pagamenti effettuati con crittovalute

- Presentazione di diversi blockchain explorer
- Analisi del funzionamento delle transazioni
- Utilizzo dei blockchain explorer per clustering (base)
- Servizi di monitoraggio per indirizzi Bitcoin
- Mixer e cambiavalute