Dark Web Investigator

A Real World Look at Investigations in the Dark Web

This course is designed for investigator to understand where to start their Darknet investigations and how to operate in this new environment. Investigators engaged in online investigations of any kind and those using open source (OSINT) analytics, will benefit greatly from this course. Crime analysts, National security investigators, crimes against children investigators, and drug investigators will especially benefit.

This is an advanced level course presented from an investigators point of view. Those with a non-technical background will also benefit from the material presented.

The content of this unique course is not offered anywhere else. The course material is supported by real world examples and incidents. This is not a general lecture course. This course will provide the student with the understanding of how to accomplish effective investigations of Darknet sites and users. The course will allow investigators to step up their investigative skills to meet the new challenges offered by the anonymity of the Darknet.

The course will be a presentation and demonstration of the techniques.

Primary Learning Modules

The Darknet/Dark Web, what it is and what it is not

Understanding what the Darknet really is can be a challenge. The technology behind the Darknet is not a single program or location. This session will explore what the Darknet is and how it differs from the Deep web.

To Tor or not to Tor

Setting up and using Tor may be easy. but finding what you want on the Tor network can be a challenge. This session will look at the Tor network how it works and methods for using it during an investigation.

Tor and its use in an investigation

Attendees will set up and access The Onion Router (Tor). They will learn how the network hides its users and makes investigating users a challenge. This session will look at the Tor network work and methods for using it successfully during an investigation.

Course Type
Specialized

Course Length

Course Code
TS - DW

Cryptocurrency as misused by Criminals

This session will provide investigators with the ability to understand and deal with cryptocurrencies during investigations. Attendees will have a clear understanding of how the use of Bitcoins are affecting investigations. They will learn to how to track the funds through various cryptocurrencies. Attendees will understand how wallets work, where evidence in the cryptocurrency system resides, how the blockchain works and investigators can track transactions through the system.

Going Undercover on the Darknet

Darknet investigations require the use of a persona like any other investigation. It also requires that you understand the equipment you are using, and practice online officer safety techniques specialized for online/Darknet investigations. This session will look at the requirements and investigator have equipment and persona background specializing in Darknet investigations.

Darkweb legend building

Non attributable profile and legend building, tradecraft, and dark web officer safety techniques.

Dark web investigative techniques

Students will learn the covert (non-attribution) and non-identifying search methods for the dark web, including: Deep searching and analysis, alternative tool and site searching, footprint reduction and incognito browsing, non-identifying profile creation using virtual phones and emails to allow registration.

Technology and techniques to locate a suspect on the Darknet

Anonymous networks are intentionally designed to hide users. Are there legally available methods which we can implement to identify anonymous users on the Internet? The answer is definitely yes. The attendees will learn techniques to locate targets online through the use of various code. The attendees will actually build tools to assist in an investigation. The potential legal issues when implementing these techniques will also be discussed.

Meta data use on the Internet in Images and documents

This module exposes the investigator to the use of Meta Data in files. How tracking duplicates, the sources uploading, revealing Exif data in images and other identifiers used to establish device location, source and tracking.

Target Attribution

Technology can often let us track a device to a physical location. However, placing a target actually behind the keyboard of a computer or cell device is a challenge for most prosecutors and investigators. This block will provide attendees with the investigative clues there may be to prove ownership and use of a computer or device.

Using web bugs and other technology to locate a suspect

How can we locate targets online through the use of various code. How can it be done and what skills does the investigator need? What are the potential legal issues?

Advanced Darknet/Dark Web Investigations, identifying the anonymous user

Are there legally available methods which we can implement to identify anonymous users on the Internet? The answer is definitely yes. This session will discuss the techniques available to the investigator to identify users of anonymization on the Internet.

PREREQUISITES

To get the most out of this class, you should have minimal experience of forensic examinations.

CLASS MATERIALS AND SOFTWARE

- Electronic copy of the course material.

- Step-by-step instructions for all exercises.

- Handouts and cheat-sheets for quick reference to detailed information sources.

- Course Thumb drive with associated software and resource material.