

DarkNet Investigations for Law Enforcement



Days: 2

Audience: The course is strictly restricted to government officials, Department of Defense, and law enforcement as it contains new and innovative methodology and techniques.

Crime analysts, National security investigators, crimes against children investigators, drug investigators, and prosecutors will especially benefit.

Description: This 2-day course is designed for government and police investigators, 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, drug investigators, and prosecutors 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 course is strictly restricted to government officials, Department of Defense, and law enforcement as it contains new and innovative methodology and techniques.

The course will be a presentation and demonstration of the techniques. LANTEC will provide student computers for all hands-on activities. Students will receive: Electronic copy of the course material, step-by-step instructions for all exercises, handouts and cheat-sheets for quick reference to detailed information sources and a Course Thumb drive with associated software and resource material and up to \$2000.00 worth of investigative software.

OUTLINE:

DAY 1

I. THE DARKNET/DARKWEB - WHAT IT IS AND WHAT IT IS NOT

- Understanding what the Darknet really 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 Deepweb.

II. TO TOR OR NOT TO TOR

- Setting up and using Tor may in itself 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.

DarkNet Investigations for

Law Enforcement

III. DARKNET OFFICE SAFETY

- 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 an investigator has for equipment and persona background specializing in Darknet investigations.

IV. CASE EXAMPLES

- The block will discuss case examples of real world Darknet investigations, the successes and the failures.

V. BUILD A TOR HIDDEN SERVICE

- In this block the student will actually build their own Tor Hidden Service site. This will demonstrate the backend of the Tor Hidden Services and how they actually function.

DAY 2

VI. CRYPTOCURRENCY AND ITS USE IN THE DARKNET

- New to investigations involving bitcoin? Need to understand how to track the funds through various cryptocurrencies? How do wallets work and is there any evidence I can use when I find one? This session will provide you with the ability to understand and deal with Bitcoin and other cryptocurrencies during your investigations.

VII. I2P INVESTIGATIONS

- This block discusses I2P as a Darknet tool and how to investigate cases involving this tool.

VIII. FREENET INVESTIGATIONS

- This block discusses Freenet as a Darknet tool and how to investigate cases involving this tool.

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.