# 18-003 The Dark Web

Los Angeles County Sheriff's Department

**FIELD OPERATIONS DIRECTIVE**

## THE DARK WEB

Technology and methodology as it relates to the internet is constantly evolving. In order to maximize the effectiveness of this directive and ensure the highest level of security, this directive should be reviewed regularly and adjusted to reflect a contemporary and relevant approach. Fraud and Cyber Crimes Bureau (FCCB) is designated as the unit for operational needs, policy updates, and best practices updates.

## PURPOSE

The purpose of this directive is to ensure a safe, secure, and efficient environment when conducting investigations on the dark web.

## DARK WEB DEFINITION

The dark web is a part of the world wide web which is accessed via the public internet, but is not indexed by normal Internet search engines. The dark web consists of "dark nets," which is actively hidden information from the rest of the web. It contains websites, peer-to-peer networks, email, file sharing protocols, and other communications where specific, specialized software, such as The Onion Router (TOR) and Invisible Internet Project (I2P), are required to gain access or maintain a presence. In other words, these websites or file locations are not indexed by mainstream search engines (Bing, Google, Ask, etc.). One way dark web content can be identified is by the domain extension ".onion" or "I2P," which is used to maintain a website presence on the dark web.

## DARK WEB SPECIAL INVESTIGATIONS CENTER

FCCB will maintain a centralized, secure, and isolated computer infrastructure for the purposes of conducting obfuscated dark web investigations, outside of, and exclusive from, the Sheriff's Data Network (SDN). This location shall be the **ONLY** location where dark web content is accessed. The following approval process is required prior to any Department member using the Dark Web Special Investigations Network:

- Approval from the FCCB Dark Web Special Investigations Center Manager;
- Submission of a list of Dark Web areas of, or locations of, suspected criminal interest;
- Explanation of reasonable suspicion; and
- The requesting investigator shall ensure his or her immediate supervisor concurs with the request.

## DARK WEB INVESTIGATIONS

A dark web investigation is defined as any time a Department member accesses the dark web for the purposes of furthering an investigation, conducting follow-up, surveillance, or gathering of intelligence.

If a Department member, through the course of their investigation, develops articulable facts which lead the investigator to believe evidence resides on the dark web, that investigator may access the dark web, with approval as noted above.

Examples of specific and reasonable suspicion include specific “onion” dark web addresses obtained through search warrants, informants, suspect and witness interviews, and other law enforcement reports or resources.

## MANAGEMENT OF DARK WEB INVESTIGATIVE SESSIONS

FCCB shall ensure specialized staff are trained and available to manage and conduct oversight during any access of the dark web.

All dark web sessions shall be conducted in the Dark Web Special Investigations Center. All live sessions should be recorded in their entirety and stored for a minimum of five years at FCCB or alternate location at the direction of the FCCB Dark Web Special Investigations Center Manager.

The dark web session shall be limited to dark web access and under no circumstances shall Department members access any Department email, personal email, personal accounts, law enforcement accounts, or any other information on the internet that may potentially compromise the investigators anonymity or network anonymity.

Removable digital media such as flash drives, optical media, portable hard drives, or any other media capable of copying or transferring digital information shall not be brought into the Dark Web Special Investigations Center.

Any information, digital or otherwise, obtained from the dark web shall not be removed from the Dark Web Special Investigations Center without the approval of the on-duty FCCB Dark Web Special Investigations Center Manager, as appointed by the captain of FCCB.

If information located on the dark web is of evidentiary value, the information shall be saved on a new clean flash drive or one that has been properly conditioned to remove any contaminating information. Once saved, the flash drive shall be marked as “Hazardous, Possible Malware”, and booked into evidence at the Cyber Investigations Center. Any evidence obtained from the dark web shall not be transferred onto or accessed via the SDN in any manner. The investigator shall defer to the FCCB Dark Web Special Investigations Center Manager for best practices in preserving a copy or printout of dark web data, if necessary for evidentiary purposes.

FCCB shall maintain a user log that will document all dark web sessions. The log will include the investigator’s name and employee number, current unit of assignment, file number (if applicable), date, time, session length, and name of FCCB monitor. The log will be retained by FCCB for one year.

FCCB personnel tasked with managing the Dark Web Center shall maintain the level of training necessary to safely and securely configure a reliable network infrastructure and maintain the necessary anonymity online. They shall also direct users on how to securely conduct their investigation.

Questions regarding the content of this Field Operations Directive may be directed to Fraud and Cyber Crimes Bureau, at (562) 946-7201.