Investigating Social Networks (CSNI)

Global forensic training

Level
Intermediate

Length
Four days (28 hours)

Training Track
Investigators

Delivery mode
Instructor-Led

Course description

The Cellebrite Social Network Investigations (CSNI) course is a 4-day program designed for technically savvy investigators, digital evidence analysts, and forensic practitioners. This course provides students with an introduction to social media investigations to include pre-seizure actions and basic investigative techniques. Students will learn how to create undercover accounts and use open source intelligence to gather information from publicly available information from social networks such as Facebook, Twitter, Periscope, and more.

Using real life application and comprehensive instruction on legal processes (subpoenas, orders, warrants), students will learn how to identify and contact suspects. To complete the workflow, students will learn how to seize devices for extraction and how to work with the data that is returned from forensic examinations. Students will also learn methods to deconflict their cases from other law enforcement officers. As the course progresses, students will be exposed to tools and techniques to collect social media evidence from devices and cloud data sources (UFED Touch and Cloud Analyzer). Students will earn a CSNI certificate documenting satisfactory completion of a knowledge exam with a score of 80% or better.

Course objectives

Upon successful completion of this course, the student will be able to:

- Identify social media platforms
- Preserve social media evidence
- Create and operate undercover accounts
- Locate open source intelligence
- Identify difference levels of user data
- Draft subpoenas, orders, and search warrants

Module	Description and objectives
Introduction	• Course introduction and administration • Course materials • Instructor introductions • Participant introductions • Cellebrite overview
Social Media Basics	• Definitions of social media • Popular social media networks and applications • Popular online ad services • Usefulness of social media networks
Undercover Accounts	• Introduction into resources, and tools used for undercover social media investigations. • Creating and properly documenting an undercover email address • Guidelines for using undercover photos
Avoiding Entrapment	• Definitions of entrapment and predisposition • Identifying ongoing patterns of conduct • Proper undercover pace and tone • Examples of entrapment
Undercover Device Evidence (UFED-Cloud Analyzer Component)	• Necessity of proper evidence extraction • Identifying evidence unique to the device • Identifying evidence that may exist on offsite servers • Benefits of using Cloud Analzer to supplement a device extraction
Open Source Intelligence	• Manual web based searches • Third party search engines • Email and Cellular queries • Darkweb and TOR
Consentual Account Reviews	• Necessity of proper evidence extraction • Identifying evidence unique to the device vs server • UFED overview • Benefits of using Cloud Analzer to supplement a device extraction

Module	Description and objectives
Social Media Data & Legal Process	• The Electronic Communications Privacy Act (ECPA) • Categories of stored data and provider retention rates • User notificiation policies by Internet Service Providers (ISPs) • Law Enforcement Portals and legal process submission
Basic Subscriber Data	• Definition of subscriber data • Use and drafting of subpoenas • Requirements and authority of subpoenas • Practical exercise issuing a proper subpoena
Transactional Data	• Definition of transactional data • Use and drafting of court orders • Requirements and authority of court orders • Examples of assorted court orders
Content and Communications	• Definition of content and communications • Use and drafting of social network or cloud search warrants • Requirements and authority of search warrants • Examples of assorted social network and cloud search warrants
Investigations Involving Exigency & Children	• Definition and examples of exigency • Obtaining social media data under exigent circumstances • The National Center for Missing and Exploited Children • Resources for intelligence and analytical assistance during emergencies
Final Exam/ Practical	The CSNI examination is a timed examination consisting of 25 randomly selected knowledge questions related to: • Identify social media platforms • Preserve social media evidence • Create and operate undercover accounts • Locate open source intelligence • Identify difference levels of user data • Draft subpoenas, orders, and search warrants

Important notice: Restricted to law enforcment and prosecutors only.

Get skilled. Get certified.

Every day around the world, digital data is impacting investigations. Making it intelligent and actionable is what Cellebrite does best. The Cellebrite Academy reflects our commitment to digital forensics excellence; training forensics examiners, analysts, investigators and prosecutors around the world to achieve a higher standard of professional competency and success.

Learn more at cellebritelearningcenter.com

Cellebrite Digital intelligence for a safer world

Rev. CSNI 12-18 (EN)