(812) 606-9222
Charles.L.Cohen@gmail.com
Skype: CTC-LLC

# Online Social Networking
# And
# Criminal Investigations
## (Two Day Course)

INSTRUCTOR: CHARLES COHEN, Cohen Training & Consulting, LLC.

The way people choose to communicate, the technologies that facilitate that communication, and the companies that the control the companies have rapidly evolved. Criminal investigators and analysts need to also evolve.

There are over 1,000 English language social networking sites on the Internet. Facebook **alone** has over 1.95 billion profiles. While this is the best known site in the United States, several others are dominant in other countries and cultures. VK is the most popular in Russia, while QQ rules in China.

There are 350 million images and 175 million status updates loaded on Facebook every day. It is the world's largest holder of images of faces tied to identity. Even as this is true, people worldwide are moving away from Web-based online social networks in favor of app-based online social networks such as WhatsApp, Snapchat, KIK, Whisper, Instagram, Vine, Periscope, and many others.

Too often, investigators and analysts overlook or underutilize these valuable resources. Social networking sites are virtual communities. As in any large community, criminal organizations, fraud, violet crime, and victimization exist. Investigators need to understand these communities along with the tools, tricks, and techniques to prevent, track, and solve crimes.

Current trends include social networks based around live streaming video, like OovoO and TinyChat, and mobile social networks like, Snapchat, YikYak, and Vibe. These emergent technologies lead to risks and opportunities for law enforcement professionals that never previously existed. Current and future undercover officers must now face a world in which facial recognition and Internet caching make it possible to locate an online image posted years or decades before. The meshing of geolocation, social networking, and mobile devices allow officers to employ new investigative techniques not previously available.

This two day (16 hour) course is designed for criminal intelligence analysts, special agents, and other investigators. Students with any level of familiarity with the Internet and computers, from beginning to advanced, will find this course beneficial.

The program gives students an up-to-date understanding of how social networking sites work and how members act and interact. Student will learn what information is available on various sites and how to integrate that information into criminal investigations and criminal intelligence analysis.

**Modules:**

- The role of Online Social Media OSINT in Predicting and Interdicting Spree Killings: Case Studies and Analysis
- OSINT and Criminal Investigations
- Metadata Exploitation in Criminal Investigations
- Open Source Intelligence (OSINT) Collection Tools: Creating an Inexpensive OSINT Toolbox
- EXIF Tags and Geolocation of Devices for Investigations and Operational Security
- Case Studies in Metadata Vulnerability Exploitation and Facial Recognition
- Online Undercover Operations: Observation and Infiltration
- Counterintelligence Concerns for Law Enforcement: How to Keep Yourself and Your Family Safe Online
- Law Enforcement Interaction with Internet Service Providers: Data Retention and the Service of Legal Process
- What Investigators Need to Know about Emerging Technologies Used to Hide on the Internet

**By the end of the course, students will:**

- Have a clear understanding how criminals exploit social communities through case studies and live online examples.
- Learn how to efficiently do automated subject link analysis using social networking data.
- Be familiar with the operation of the largest sites, to include: Twitter, Facebook, Youtube, Ask.fm, Snapchat, Foursquare, and Tumblr.
- Learn various ways of concealing the location from which the Internet is accessed when using online social networks.
- Understand how criminal organizations use online social networks to interact, identify victims, and conceal their identity.
- Receive extensive information on the two leading trends in online social networks—microblogging and mobilization.
    - Become acquainted with the latest mobile social networking technology and platforms, including geolocation.
- Explore the phenomena of virtual worlds and massively multi-player games, and understand how criminals recruit, communicate, and launder money in these environments.
    - Understand how immersive social networks, such as Second Life and Sony's Home are exploited by criminals and how these sites can be used to gather criminal intelligence.
    - See how Linden Dollars, Project Entropia Dollars (PED), WoW Gold, and other non-sovereign currencies are used to launder money and obfuscate financial transitions.
- Know what information is available from social networking sites through the service of legal process, and how to make that service.
    - Thoroughly explore the implications of 18 USC 2703, the Communications Assistance for Law Enforcement Act (CALEA), and the Electronic Communications Privacy Act (ECPA), and how these federal laws impact in investigative and intelligence operations.
- Learn about the risk to law enforcement officers, especially undercover investigators, posed by online social networking, social media, and viral videos.
- Practice preserving the publicly viewable portions of a suspect social networking profile and flash

video in a forensically sound manner.

- Learn how to, and practice, using proxies, bulletproof servers, onion routers, and other means to conceal online identity.
- Learn how to obtain free open-source information on suspects and intelligence targets using the Internet.
- Learn how to interpret email headers, identify ownership of Web sites, and locate Internet Service Providers.
- Learn how to identify real-life intelligence targets by participating in the virtual world of social networking.
- Understand the unique challenges and opportunities associated with specialty networking sites, like Grou.ps and Gigatribe.
- Become acquainted with the latest mobile social networking technology and platforms, including geotagged photographs, Life360, and mobile VoIP.

- See examples of how older online technologies, such as forums, bulletin board systems, and chat rooms are still exploited by criminal offenders.
    - Explore how criminals, from trans-national drug organizations to extremist groups, use Internet Relay Chat, Usenet, and fserve to exchange interact and exchange information.

Students receive course material, including legal process contact information, preservation letters, boilerplate compliance documents, and resource guides.

**NOTICE: Course contains graphic content including profanity, and sexual and violent images.**