LOS ANGELES POLICE DEPARTMENT
INTELLIGENCE AND CRIME ANALYSIS, LEVEL 1
Expanded Course Outline (8-Hours)
1850-32013

Instructors:

Curtis Davis, Police Officer III/CCIA - POST ID B95-K95
Rebecca Nagy, Crime Intelligence Analyst II/CCIA - POST ID C08-M40
Christine Jackson, Detective II/CCIA (Course Coordinator) - POST ID A82-L60

Instructional Goal – This course will provide students with a Practical Application of Open Source to support Situational Awareness, and Tactical and Strategic Analytical Support. Students will understand the use of Open Sources (including social media) across the spectrum of information, intelligence, investigative, and evidence. This course will provide analysts, investigators, and related personnel performing an analytical function in their current assignment, at least eight hours of continuing analytic-based education annually through a combination of in-class and online courses. This is minimally required to maintain currency and professional standing in the field.

Performance Objectives - Using lecture and learning activities including case studies and hands-on scenarios, the student will:

❑ Develop the basic components of communication skills and techniques;

❑ Demonstrate a minimum standard of strategic communication skills with every technique and exercise presented;

❑ Develop an understanding of the laws and Department policies involving persons who access department systems, open source databases, and other means to obtain information on publicly accessible systems;

❑ Demonstrate ability to provide investigative leads to detectives and other concerned personnel by searching publicly available information, web-based internal departmental databases, and external law enforcement databases and third-party data sources;

❑ Demonstrate ability to conduct intelligence analysis, such as link analysis, reporting, and briefing using information provided by internal and external databases, and analytical programs to connect individuals and organizations involved in criminal activity;

❑ Develop knowledge to adhere to Department policy and legal restrictions pertaining to confidentiality, access, use, and dissemination of law enforcement related information and work product to ensure integrity of information;

❑ Demonstrate the use of analytical ability, technology application, and oral Communication to successfully complete hands-on exercises.

LOS ANGELES POLICE DEPARTMENT
INTELLIGENCE AND CRIME ANALYSIS, LEVEL 1
Expanded Course Outline (8-Hours)
1850-32013

I. Basic Open Source - Information to Evidence **0800-0830 (30 Min)**

a. Course Overview
    i. Facility description
        1. Restrooms and breaks
        2. Computer usage
b. Welcome and Introductions
    i. Instructors and Course Facilitators
        1. Background and Experience
    ii. Student Introductions
        1. Current assignment
        2. Identify experience
    iii. Itinerary review
c. Class Activity – Group Exercise

II. Information to Intelligence **0830-1000 (90 Min)**

a. Basic Overview
    i. Criminal Intelligence
        1. Information
            a. What is it?
        2. Intelligence Principles
            a. SIGINT, GEOINT, MASINT, HUMINT, OSINT

b. Intelligence Cycle
    i. Purpose
        1. Actionable Intelligence
        2. Process
    ii. Direction/Tasking
        1. Obtaining of the information, and the delivery of the information to the "end-user"
        2. Requirements and Collection Planning
    iii. Evaluation and Collation of Intelligence information
        1. Information must be properly evaluated before it can be acted upon.
        2. Raw data shall be organized and formatted so the analyst can retrieve; sort; identify patterns, anomalies, and gaps in; and store the data.
            a. An inventory of the data is the quickest way to see gaps and identify further collection efforts.
    iv. Data integration and analysis
        1. Best results can only be achieved when the analyst and investigator work together in partnership
        2. The results of analysis are hypotheses, conclusions, and recommendations for action.
        3. Deconfliction
    v. Re-Evaluation and Dissemination
            a. Putting intelligence and information together in an organized way so that the difficult task of extracting meaning from the assembled information is made easier.
            b. Intelligence is of no value unless it is shared. Analytic products may be developed to support internal or multiagency needs and short-term or long-term goals.

c. Information technology is very much key to intelligence sharing

2. Provide it to multiple consumers across the same relevant teams so that you don't have a single point of failure, but also aren't sending it to teams that lack the need to know.

3. Privacy

a. Who – "need to know?"

b. Why - "would they receive info?"

c. When – "to disseminate info"

d. Analysts must be able to apply their agency's policies, guidelines, and operating procedures to information and intelligence sharing

c. Tactical Intelligence Analysis

i. Intelligence provides the knowledge on which to base decisions and select appropriate targets for investigation

ii. use of criminal intelligence analysis is appropriate to support investigations, surveillance operations and the prosecution of cases

d. Strategic Intelligence Analysis

i. Concept of collecting and utilizing information to support decision making

ii. products of intelligence analysis can assist in developing strategic plans to tackle current problems and prepare for future anticipated ones.

iii. law enforcement agencies need forward looking, assertive, and comprehensive strategies to counteract the threat of organized crime groups.

e. Real-time Situational Awareness

i. Raw information to start (Public Safety Interest – All-hazards)

ii. Typically, a specific incident or event and can be actionable

iii. Compressed Operational Tempo

1. Actional value (resource allocation tools)

2. Assess and decision making

a. Info/intel moved up thru the ranks

f. Assess Knowledge – Written Quiz

III. Legal Guidelines: 1000-1130 (90 Min)

a. Introduction
    i. Civil Rights, Civil Liberties, Privacy
        1. Learning Activity
    ii. California Constitution
    iii. Privacy Guidelines and Good Faith
b. History of Policing Intelligence in Law Enforcement
    i. Timeline
    ii. Dossier System
    iii. Lessons-Learned – Case Studies
c. Ethics
    i. Definitions of privacy, civil rights, and civil liberties
    ii. Noble Cause Corruption
    iii. Intelligence Abuses
    iv. P.L.A.N – Proportional, Legal, Accountable, Necessary
d. 1st Amendment
    i. Protects
        1. Advocacy of violence or lawbreaking, depending on context, may be protected speech under the First Amendment.
        2. First Amendment protects political hyperbole and sharp attacks that do not rise to the level of a true threat.
        3. Speech may lose its protection when it is used to intimidate others.
e. De Facto Standards
    i. Policies, Protocols and Guidelines
        1. Berkeley Protocol, LEIU, 28 CFR Part 23
            a. Articulate that the use of resources will be consistent with applicable laws, regulations, and agency policies and procedures.
            b. Specify the documentation, storage, and retention requirements

ii. 28 CFR Part 23

1. The purpose for which information is collected, retained, used, and shared and the way it is done may impact individual privacy, civil rights, and civil liberties.
    a. Relevant legal concerns include issues surrounding: Privacy, civil rights, and civil liberties protections.
    b. Security of information
    c. Operational security practices for storage and retention of law enforcement intelligence and information.
    d. remaining cognizant of the potential consequences of oversharing personal information online;
        i. explore existing methods of maintaining good OPSEC.
2. Caution to not include in any retention system information which has been obtained in violation of any applicable federal, state, or local law.
    a. Indiscriminate data hoarding is not only likely breaching US privacy legislation, it also compromises the ethics of investigations.

iii. LEIU Guidelines

1. Applied – Collection, Timeline, Purpose
2. OSINT guidelines
    a. Define authorization to use open source platforms or tools
    b. information obtained from open source resources will undergo evaluation to determine credibility and reliability

f. Critical Thinking

i. Critical vs. Creative

ii. Intelligence – Avoidance of Politicization

iii. Learning Activity

g. Articulation

i. Criminal Nexus vs. Situational Awareness

ii. Threat Classification

h. Assess Knowledge - Written Quiz

IV. Recommended Best Practices: 1230-1330 (60 Min)

a. OSINF vs. OSINT

i. OSINF

1. Definition, Collection and Examples
2. Quantity vs Quality

ii. Open Source Intelligence (OSINT) was developed as an intelligence discipline to identify and understand threats using publicly available information.

1. Used for Counter-Terrorism, directing Mis-information, National Cybersecurity, and Transportation Security. Today it's used by attorneys, thinktanks, researchers, academia, media, and other members of the public
2. Effective open source investigation requires case-by-case implementation to ensure good outcomes.
3. Targeted collection of specific data and the application of processes and technology to better refine your search.
4. Avoid risk of exposing your identity or accidentally informing an individual that they are under investigation by leaving a digital footprint.
5. Failure to implement best practices therefore not only compromises the investigation but can also leave unaddressed threats off the table.

b. Capture

iii. Capture the data and record

1. Where it was found (URL)
2. Log date and time saved.
3. Where possible full-content capture may assist in attribution or identification

iv. Content can easily be altered or removed from the internet, who can find that key evidence has disappeared when presenting findings, undermining a case.

v. How you need to use the information, and how it might need to be used in the future?

c. Redaction- Privacy

vi. Personal Identifying Information (PII)

1. Federal Rule of Civil Procedure 5.2 and Local Rule 5.2-1.

d. Protect

vii. Stored in a secured area restricted to authorized personnel

e. Purge

viii. Purge Criteria

1. Utility
2. Timeliness and Appropriateness
3. Accuracy and completeness

ix. Review and Purge time Schedule

x. Manner of Destruction

b. Digital Evidence

i. Ensure evidence is secure, keep track of all sources, including screenshots and timestamps of important findings.

1. Archive evidence properly
2. Encrypt storage for data protection

ii. Cross-check and connect records obtained via legal process with open source data

1. Business records obtained from service providers
2. Records from forensic extractions of computers, tablets, and phones

iii. Software tools to collect/automate evidence gathering

f. Classification for Law Enforcement

i. Law Enforcement Sensitive (LES)

V. Sources of Information **1330-1530 (120 Min)**

a. Open Source Intelligence Techniques
    i. Organizing and Assessing
    ii. Setup an Effective Crime Analysis Toolbox
        1. Hardware sources
            a. Unattributable/Firewall
            b. Internet throughput
            c. Computer equipment
        2. Software
            a. Setup desktop workspace and applications
            b. Tabs, Bookmarks, Browser Extensions, Taskbar
        3. Intel Cycle – Planning, Direction and Tasking
    iii. Live Demo – Learning Exercise/Hands-on
b. Sources of Information – Collection/Processing
    i. Building Blocks – Intel, Investigation, Evidence
        1. Determine where you are (stage) and what you need
    ii. News, Government, Legal and other public data sources
        1. Media, print newspapers, magazines, radio, and television.
        2. Online publications, blogs, discussion groups.
        3. Public government data; source comes from an official source they are publicly accessible. Professional and academic publications.
    iii. Search Engines (Google/Bing/Wayback)
        1. Can be used to initiate an investigation, discover data or new sources.
        2. Google's advanced search queries 'dorking'
            a. Search string: "jane" "smith" -site:twitter.com: Expected Result: Look for an exact match to the first and last name but in different combinations, and exclude Twitter from the results.
            b. People Search process: Decide how to organize/collate data, don't break the law, identify formal names, identify titles and honorifics, Identify the target's social media profiles.

iv. Social Media

1. Twitter, Facebook, Instagram, YouTube, and other social media websites. This source also outpaces a variety of other sources due to its timeliness and ease of access.
2. If search goes beyond mere identification, then social activity across social platforms, discussion sites, blogs, and forums will weigh heavily in your investigation.

    a. Usernames can hold meaning to the individual, and as a result provide useful information when expanding investigations to different social platforms.

3. Social media has been the most effective medium for gathering information on individuals, sources can include social networking sites, professional networking sites, video sharing or vlog sites.

4. There are four components to turning social media data into actionable intelligence:

    a. Classify the threat

    b. Determine its severity

    c. Eliminate false positives

    d. Add context

v. Data Brokers (paid/free)

1. People search websites, i.e. spokeo.com and beenverified.com, can also be used to quickly search for people using a real name, username, email, or phone number.

2. May be necessary to search multiple sites to get all the data you need about a person.

vi. Use of services such as Who.is or ICANN Lookup to find basic domain registration information for IP addresses.

vii. Live Demo – Learning Exercise/Hands-on

c. Production/Dissemination – Tools to present to end-user

d. Redaction/Encryption

i. Live Demo – Learning Exercise/Hands-on

VI. Understand the Spectrum (How it comes together): 1530-1700 (90 Min)

a. Social Listening (Raw information)

   i. Monitoring in real time

   ii. To probe posts for information on public safety interest such as potential threats and breaking news.

b. Targeting a Threat

   i. Utilize OSINT to perform overview of threat.

      1. Technical, procedural and analytical tools to scope one's threat.

c. Intelligence/Investigation

   i. Effective intelligence begins by addressing the following questions:

      1. What do we need to know?
      2. Why do we need to know it?
      3. Who might have the information we need?
      4. How should we perform the research?
      5. What will we do with the results?
      6. Does the effort justify the cost?

d. Assess Knowledge – Hands-on activities

   i. OSINT Search (Group Exercise) – Investigative product

   ii. Situational Awareness Exercise – Report for dissemination