NATIA 2026: Annual Training, Certification, & Technology Exhibition

Course Descriptions and Schedule

NATIA 2026
July 26 - 30
Columbus, OH

NATIA 2026 Course Catalog | Revised March 16, 2026

Please note: The Course Catalog offerings, schedule and room assignments may be subject to change. Please check the NATIA 2026 Event App onsite for the most up-to-date information.

50 Shades of Infrared

Law enforcement uses infrared light in many different ways. Most common is illumination for low light cameras. There are other uses of infrared, such as target identification. This workshop will explore some of the properties of infrared light and how they can be useful in law enforcement applications. Students will receive an inexpensive night vision device for testing projects. Students will build an infrared "throwy" for temporarily illuminating areas with IR light. Then students will build an IR "Firefly" that can be used for target identification in areas of darkness. In all, students will build 3 different IR projects for use in the field. Basic soldering skills are desirable, however this course is a simple course where soldering may also be learned. The course will also cover some simple electronic parts identification and explanation of their functions.

Included with Registration

Date	Time	Room
Wednesday, July 29	10:00 AM – 12:30 PM	B132

A Comparison and Discussion of Australian Technical Surveillance Team Methodology

Over the course of a two-hour, syndicate-style presentation, this course will demonstrate the techniques and processes used by many Australian technical units to manage and record the administrative, operational, equipment and location specific aspects of an operation. The session will include a comparison of an Australian three-person technical installation team with equivalent teams operating in other countries. Attendees will be guided step by step through the Australian approach, from the initial approach to a hostile premises, through entry, clearance, installation and exit. The instructor will explain how the entire operation is formally documented through official notes and established unit process. At the conclusion of the presentation, each student will be provided a set of generic documents that they can take back to their agency and adapt for their own use.

Included with Registration

Date	Time	Room
Monday, July 27	3:30 PM – 5:30 PM	A222
Thursday, July 30	1:00 PM – 3:00 PM	A220

AC Electrical Safety Familiarization

This is a hands-on workshop that is an introduction to working with electricity when installing covert devices and how to do it safely. You will learn how to recognize power sources and where to connect to them to make your devices operational. Students will receive a basic tool kit to take back to their agency. **(Continued next page)**

AC Electrical Safety Familiarization (Continued)

Pre-Registration Required – Additional Fee: $200

Date	Time	Room
Monday, July 27	8:00 AM – 12:30 PM	B233

AI For Law Enforcement

This four-hour, hands-on workshop introduces law enforcement professionals to practical, responsible uses of artificial intelligence in investigations and daily operations. The course focuses on field-ready applications that help accelerate research, improve evidence review, streamline report writing, and enhance case analysis while remaining compliant with legal standards and agency policy. Participants learn how to use widely available AI tools to support investigative work, with an emphasis on effective prompting, recognizing inaccuracies, and maintaining human oversight. Instruction includes AI-assisted analysis of case files and evidence, pattern and data correlation, report drafting and refinement, and efficient review of audio and video evidence. The course also introduces secure, offline AI solutions that allow agencies to use AI while keeping sensitive data on premises.

Included with Registration

Date	Time	Room
Monday, July 27	1:00 PM – 5:30 PM	B231
Wednesday, July 29	8:00 AM – 12:30 PM	B231

Advanced Mesh Networks-Airborne Mesh and TAK

This advanced course instructs students on the design and deployment of airborne mesh networks using fixed-wing aircraft integrated within the Team Awareness Kit (TAK) ecosystem, with an emphasis on extending secure communications and real-time situational awareness in complex operational environments. Participants learn network architecture and planning, antenna configuration, spectrum management, payload integration, and seamless TAK connectivity, along with techniques for transporting live ISR video across a mesh network while managing bandwidth, minimizing latency, and securely streaming to TAK users without compromising command-and-control data. The course further contrasts rapid-deployment local configurations—typically built around fixed sites and wired backbones—with broader statewide systems that must address end-user connectivity, austere environments, and limited infrastructure, providing practical exercises that develop the capability to build scalable, resilient airborne mesh networks supporting multi-agency operations, disaster response, and large-scale public safety missions.

Included with Registration

(Continued next page)

Advanced Mesh Networks-Airborne Mesh and TAK (Continued)

Date	Time	Room
Tuesday, July 28	10:30 AM – 12:30 PM	B130
Wednesday, July 29	8:00 AM – 10:00 AM	A215

Antennas and Feedlines-The Wires Behind the Wireless

An introduction to antennas, Radio Frequency (RF) feedlines, and antenna testing.

Included with Registration

Date	Time	Room
Tuesday, July 28	8:00 AM – 10:00 AM	A222
Wednesday, July 29	10:30 AM – 12:30 PM	A222

Application of Non-Linear Junction Detectors During Search Warrants

Students will learn the theory and application of Non-Linear Junction Detection (NLJD) and how to effectively implement a NLJD in the execution of a search warrant. NLJD's can be an effective tool in the detection of illicit listening devices or other illicit storage media.

Included with Registration

Date	Time	Room
Tuesday, July 28	10:30 AM – 12:30 PM	A211

Basic Surface Mount Soldering

Students will learn the basics of surface mount soldering for repairs and building circuit boards. Students will receive a surface mount soldering station and all tools needed to accomplish surface mount soldering. Students will build a solder practice board and a remote switch board.

Scheduling Note: This is a two-day class (eight hours) taking place on both Wednesday and Thursday.

Pre-Registration Required – Additional Fee: $550

Date	Time	Room
Wednesday, July 29 ***and***	8:00 AM – 12:30 PM	A210
Thursday, July 30	8:00 AM – 12:00 PM	A210

Beginner 3D Printing for Law Enforcement Applications: Bambu Labs P2S w/ AMS

This beginner-level course introduces law enforcement professionals with little or no prior experience to the practical use of 3D printing for operational support. Participants will learn to safely operate and maintain the Bambu Labs P2S 3D printer with the Automatic Material System (AMS) while gaining hands-on experience with Bambu Studio (Bambu Slicer) to produce reliable, functional components for field use. The course covers essential 3D printing concepts such as materials, layer height, infill, supports, and print orientation, along with configuring slicer profiles for strength, durability, and precision. Students will also explore filament selection (PLA, PETG, ABS, TPU) for different operational environments and common law enforcement applications such as mounting brackets and equipment accessories. Through practical exercises, attendees will learn how slicing settings affect structural integrity, how to modify supports for complex prints, and how to tune infill and wall structures for mission-specific durability. By the end of the session, participants will be able to independently prepare and slice print files, produce functional components tailored to agency needs, and diagnose common printing issues. Equipment provided includes a Bambu Labs P2S printer with AMS, two spools of filament, digital calipers, and a basic 3D printing toolkit.

A Windows-based laptop with administrator rights and a mouse or trackball is required to fully participate in the course.

Scheduling Note: This is a two-day class (eight hours) taking place on both Monday and Tuesday.

Pre-Registration Required – Additional Fee: $1,100

Date	Time	Room
Monday, July 27 ***and***	1:00 PM – 5:30 PM	A210
Tuesday, July 28	8:00 AM – 12:30 PM	A210

Beyond the Write Blocker: Non-Traditional Evidence Capture

This is a 4-hour course with each hour dedicated to a specific topic, with 4 scenarios that all support Preserve - Authenticate - Defend.

- Hour 1: DVR/NVR acquisition. Post export preservation, authentication, and defense of solution chosen.
- Hour 2: Hardware Encrypted Devices that have a Video Port. Imaging and preservation requirements and methods. Authentication of original and subsequent captures and reasoning of the process. **(Continued next page)**

Beyond the Write Blocker: Non-Traditional Evidence Capture (Continued)

- Hour 3: MTP Data Acquisition. Why this method may be necessary.
- Hour 4: Using OCR and Autopsy to post process. OR Capstone Exercises for proper preservation, authentication and defense.

A laptop with administrative privileges, Windows 11 and available USB ports is required for this course, in addition to a 32GP USB thumb drive that must be supplied by the student.

Included with Registration

Date	Time	Room
Thursday, July 30	8:00 AM – 3:00 PM	B130

Blue Force Tracking with TAK: ATAK/iTAK/WinTAK Workshop

The Team Awareness Kit (TAK) is a geospatial, situation awareness platform originally developed for and used by the Department of Defense, which is now available to civilians. This course will familiarize you with the setup and use of the various TAK clients (ATAK, iTAK, WinTAK, WebTAK) to help support Public Safety operations.

Students "Bring Your Own Device" (phone/tablet/laptop) with Wi-Fi.

Included with Registration

Date	Time	Room
Monday, July 27	1:00 PM – 5:30 PM	A211
Thursday, July 30	8:00 AM – 12:30 PM	A224

Build a Battery Pack Using a Spot Welder

Students will learn how to build a battery pack and how to calculate the number of cells to attain the voltage and current required. A spot welder and hand tools are included in the course fee.

Pre-Registration Required – Additional Fee: $195

Date	Time	Room
Wednesday, July 29	8:00 AM – 12:30 PM	A230
Thursday, July 30	8:00 AM – 12:30 PM	A230

Building Cameras Part 3: Modifying Cobra & LED Street Lights

This course will outline how to fabricate Cobra-style streetlights for installing small dome cameras, like the Canon VB-S30D, for surveillance pole camera use. This presentation will cover both the older style Cobra lights as well as the modern LED lights. A listing of needed equipment, tools, and instructions for fabricating the light housings will be provided. Configuring the equipment will not be included in this class, as that was covered in "Part 2", presented at the NATIA 2025 Training Event. Presentation slides will be available on the eShow App.

Included with Registration

Date	Time	Room
Tuesday, July 28	10:30 AM – 12:30 AM	A222
Wednesday, July 29	10:30 AM – 12:30 AM	A224

CTI Exam

Administration of the Certified Technical Investigator Exam

Pre- Registration Required (Onsite Registrations Accepted) – Exam Fee: $150

Date	Time	Room
Tuesday, July 28	1:00 PM – 3:00 PM	A224

CTI Exam Review

Review the CTI course material to help those who would like to challenge the CTI Exam.

Included with Registration

Date	Time	Room
Tuesday, July 28	8:00 AM – 12:30 PM	A224

Close Access Essentials

This course introduces law enforcement personnel to the full-spectrum methodology, mindset, and capabilities of modern red teams and physical adversaries targeting protected facilities. Participants examine how attackers conduct open-source intelligence gathering, on-site reconnaissance, social engineering, and access control exploitation to defeat badges, security systems, and procedures that agencies often assume are robust. Through case-based discussion, students confront their own assumptions about what an adversary "looks like," **(Continued next page)**

Close Access Essentials (Continued)

explore how stereotypes undermine situational awareness, and learn why well-meaning insiders routinely grant access to hostile actors and clandestine technical devices.

Included with Registration

Date	Time	Room
Wednesday, July 29	10:30 AM – 12:30 PM	A215
Thursday, July 30	8:00 AM – 10:00 AM	A215

Connecting the Dots: Improvements in AI/ML for Technical Investigations

Connecting the Dots: Improvements in AI/ML for Technical Investigations is a forward-focused course for investigators, analysts, and technical professionals seeking to operationalize recent advances in artificial intelligence and machine learning within digital and network investigations. The program examines how emerging AI/ML methodologies are reshaping technical casework—ranging from behavioral signal detection within encrypted IP traffic to next-generation automatic speech recognition (ASR) models that surpass traditional transcription tools. Participants will learn how to transform raw, high-volume data into actionable intelligence by identifying human-driven patterns, correlating disparate data sources, and extracting meaningful insights from complex datasets. The course emphasizes both conceptual understanding and practical implementation strategies, equipping attendees with structured frameworks to deploy AI-driven capabilities effectively in operational environments.

Included with Registration

Date	Time	Room
Tuesday, July 28	8:00 AM – 10:00 AM	B130

Covert Audio Surveillance: Standards, Fundamentals, and Operational Practice

This session delivers a technical and operational deep dive into modern audio surveillance, emphasizing the need for reliable, interoperable, and legally defensible systems in today's high-stakes investigative environments. Designed for both experienced covert audio operators and those newer to the discipline, the course reinforces foundational audio capture principles while addressing the increasing complexity of digital systems, vendor claims, and emerging threats to audio authenticity. Participants review core concepts such as microphone placement, signal-to-noise ratios, and intelligibility, and learn how recognized standards and forensic best practices support admissibility and operational reliability. **(Continued next page)**

Covert Audio Surveillance: Standards, Fundamentals, and Operational Practice (Continued)
The session also provides practical guidance on evaluating audio technologies, preserving evidence integrity through proper metadata and chain-of-custody procedures, and mitigating risks posed by AI-generated audio, deepfakes, and transmission limitations. Attendees leave with actionable knowledge to improve audio quality, ensure system interoperability, and maintain effective, defensible audio surveillance operations under judicial and technical scrutiny.

Included with Registration

Date	Time	Room
Monday, July 27	3:30 PM – 5:30 PM	A216
Wednesday, July 29	8:00 AM – 10:00 AM	A213

Covert Electrical Power Interception: Governance, Safety, and Utility-Asset Coordination for Technical Surveillance

This session equips technical investigators and supervisors with the governance, safety, and operational frameworks required to lawfully obtain covert mains power for surveillance devices. Drawing on formal agreements endorsed by electricity and network regulators, attendees will learn how law enforcement can expand the scope of electrical work under supervision and compliance controls. The presentation covers risk management, PPE standards, energized-environment protocols, and approved interception methods with emphasis on verification steps to protect law enforcement agencies from breaches of regulatory compliance. A dedicated segment addresses confidential utility-infrastructure coordination, explaining how WA Police enable lawful installations on network providers' infrastructure. This includes request/approval pathways, WHS site control, confidentiality obligations, branding constraints, and incident reporting. The session is strictly neutral and non-commercial; all techniques are presented to standards and internal governance, not to promote products. Attendees will leave with actionable insights to strengthen operational safety, compliance, and interoperability in technical surveillance deployments.

Included with Registration

Date	Time	Room
Monday, July 27	1:00 PM – 3:00 PM	A222
Thursday, July 30	8:00 AM – 10:00 AM	A222

Cyber Crime Challenges for the Law Enforcement Community

Review of current cyber crime trends, particularly as currently being accelerated by AI (Artificial Intelligence) and steps Law Enforcement officers can take both professionally and personally to be aware and prepared.

Included with Registration

Date	Time	Room
Tuesday, July 28	10:30 AM – 12:30 PM	A216
Thursday, July 30	1:00 PM – 3:00 PM	A216

DIY PoleCam Lab - Version 3.0

Students will build and program a covert aerial mounted camera, that can be mounted on a pole, street furniture, or a rooftop for a fraction of the cost of buying a turn-key system. Students will construct the box, assemble the 3D-printed mounting solution, and then program the camera, modem and relays to work as a complete solution.
The system will include:

- Weatherproofed covert housing
- 18 X Optical zoom - PTZ camera
- Cat 12 – Modem
- Independent Cell based LTE-M Reset
- 4 independent relays
- Low voltage, Low or High temp notification
- Automatic Fan activation
- Ruggedized power connectors
- Pole mount kit
- Optional Front and Side panels for different looks

Pre-Registration Required – Additional Fee: $4,550

Date	Time	Room
Monday, July 27	1:00 PM – 5:30 PM	B215

Defeating Encryption: Lawful Access Strategies and Case Management Essentials

Encryption remains one of the most significant barriers to obtaining critical evidence in modern investigations. This lecture examines the role of lawful access in overcoming these challenges at various stages of an investigation. Topics include Covert Access and Intercept Team (CAIT) techniques such as lawful hacking, traditional Part VI (Title III) telephony interception, social engineering, and agent plays for acquiring PINs and passwords. We will also explore the role of legal tools like production and assistance orders for recovering passwords and PINs, and discuss how backroom teams can implement simple policy changes to ensure known and suspected credentials are captured, summarized, and made accessible to key stakeholders throughout the life of a project. This session emphasizes theory, workflow integration, and strategic planning rather than hands-on technical execution.

Included with Registration

Date	Time	Room
Tuesday, July 28	8:00 AM – 10:00 AM	A220
Thursday, July 30	8:00 AM – 10:00 AM	A220

Ditch the Cell Plan: Track Anything, Anywhere for Pennies a Year

What if you could track your car, your dog, your kid's backpack, or a shipping container halfway across the country, live, with no cellular plan, no monthly subscription, and a battery that lasts over a year? That's not a pitch, it's LoRa. In this two-hour lecture, we'll pull back the curtain on the long-range radio technology and the Helium Network that make it possible to get real-time GPS tracking for just pennies a year. You'll see how a device the size of a credit card can send its location for miles without ever touching a cell tower, and how the Helium Network crowdsourced an entire wireless infrastructure by paying everyday people in crypto to run hot spots. No technical background required, just bring your curiosity and prepare to rethink what wireless can do.

Included with Registration

Date	Time	Room
Thursday, July 30	8:00 AM – 10:00 AM	A213

Drone as First Responder: Creating a DFR Program in Your Agency

A true Drone as First Responder (DFR) program is fundamentally a technical and logistical system designed for pre-arrival situational awareness, leveraging Unmanned Aircraft Systems (UAS) for immediate intelligence gathering. The core technical architecture involves pre-positioned, often automated, launch infrastructure, such as Drone-in-a-Box (DIAB) systems, deployed on strategic fixed sites like rooftops or fire stations. This fixed-site model, unlike patrol-led UAS, ensures a rapid 1-3 minute response time upon a 911 dispatch by allowing a dedicated, centralized Remote Pilot (Teleoperator) in a Real-Time Operations Center to immediately launch the drone. Critical to this functionality is robust connectivity, utilizing high-speed internet and public safety cellular bands like FirstNet or 4.9 GHz, to maintain a stable, live, high-resolution visual and/or thermal video feed that is instantly streamed to dispatchers and responding ground units.

Included with Registration

Date	Time	Room
Monday, July 27	1:00 PM – 3:00 PM	A220
Wednesday, July 29	8:00 AM – 10:00 AM	A220

Effective Password Recovery with Hashcat: Tools, Techniques, and Trends

Enhance your ability to access encrypted devices, files, and networks by learning how to effectively leverage Hashcat, the leading open-source password recovery tool. This workshop covers practical cracking strategies, password psychology and trends, as well as bypass techniques investigators can apply in the field. We'll finish with an overview of password-cracking hardware options, both on-premise and cloud-based, followed by an interactive Q&A session.

A laptop that can be connected to the internet is required for this class.

Included with Registration

Date	Time	Room
Monday, July 27	1:00 PM – 5:30 PM	A226
Wednesday, July 29	8:00 AM – 12:30 PM	A226

Flexible Magnetic Mount Build

Students will build a pair of flexible magnetic mounts for vehicle tracking. The mounts are attached to a rubber pad allowing for the magnets to adhere to curved, or odd shaped steel on the underbody of a vehicle. The mounts are used instead of the hard, metallic plate that is usually attached to the GPS unit. The mounts are also great solution for mounting an external battery pack.

Flexible Magnetic Mount Build (Continued)

Pre-Registration Required – Additional Fee: $140

Date	Time	Room
Thursday, July 30	1:00 PM – 3:00 PM	A216

Flip My Flipper Zero

Flipper Zero is a versatile, pocket-sized device that empowers individuals to explore and interact with the world of wireless technologies. Through hands-on exercises and practical demonstrations, learners will gain understanding of the Flipper Zero's capabilities. There is a multitude of potential applications in various fields, including cybersecurity, IoT, and law enforcement! This workshop will familiarize you with the basic components and functionalities of the Flipper Zero. Explore hands on techniques for capturing, analyzing, and modifying wireless signals, and on how to utilize the Flipper Zero for security testing, Wi-Fi deauth and Fun! Learn fundamental concepts of wireless communication protocols such as RFID, NFC, Bluetooth, and Infrared. Flipper Zero will be provided to each student.

A laptop with administrative rights is required for this class.

Pre-Registration Required – Additional Fee: $325

Date	Time	Room
Tuesday, July 28	8:00 AM – 12:30 PM	A226
Thursday, July 30	8:00 AM – 12:30 PM	A226

From Surveillance to Entry: How Criminals Prepare for Residential Burglaries

Criminals increasingly use low-tech to high-tech surveillance before committing residential burglaries, and officers can benefit from understanding these indicators: 1. Criminal pre-surveillance behaviors. 2. Technology used by burglars. 3. Indicators that homeowners and Officers might miss. 4. Evidence handling and legal considerations. 5. Prevention messaging for community policing.

Included with Registration

Date	Time	Room
Wednesday, July 29	8:00 AM – 10:00 AM	A211

Fundamental Electronics and Using a Multi-Meter

This in-depth workshop is focused on the application of electronic laws in solving electrical problems associated with surveillance equipment. This information is directly applicable to technical surveillance equipment installation, troubleshooting, and repair. Students will be given basic instruction on basic electrical principles and electronic components. The workshop includes hands on exercises utilizing the techniques and theories discussed in conjunction with a digital multimeter to establish troubleshooting techniques. It will explain basic electronic principles (Voltage, current, resistance); Review the metric system; Discuss electrical laws and how they apply to troubleshooting (ohm's and Kirchoff's); Parallel vs series circuits; Switches (mechanical, electrical, and electronic); Basic troubleshooting techniques; Applying techniques in the real world with multimeter as diagnostic tool. A multi-meter will be issued to each student to take back to their agency.

Pre-Registration Required – Additional Fee: $50

Date	Time	Room
Monday, July 27	1:00 PM – 5:30 PM	B235
Wednesday, July 29	8:00 AM – 12:30 PM	B235

High Reliability Soldering

This course will give students confidence in making a high reliable solder connection. Students will learn the theory of soldering and the importance of component preparation. Each student will be given a state-of-the-art soldering station and the necessary tools to take back to their agency. The soldering station is compatible with North American (type B) and European (Europlug) electrical source via USB cable. Ample time will be devoted to populating a printed circuit board with electronic components and de-soldering the components from the circuit board. No previous soldering experience is necessary.

Pre-Registration Required – Additional Fee: $145

Date	Time	Room
Monday, July 27	1:00 PM – 5:30 PM	B230
Tuesday, July 28	8:00 AM – 12:30 PM	B230

How to Get the Equipment You Want

Unravel the mysteries of procurement in this practical, nuts-and-bolts course. Topics include communicating with vendors, purchasing personnel, and command staff; product research, red flags, and best practices; grants, budgets, and creative funding sources; your expectations, rights, and responsibilities when you buy. Course content is applicable to supervisors as well as officers new to the process. The instructor brings over 20 years' experience selling technology to law enforcement agencies. **(Continued next page)**

How to Get the Equipment You Want (Continued)

Included with Registration

Date	Time	Room
Tuesday, July 28	8:00 AM – 10:00 AM	A213
Wednesday, July 29	10:30 AM – 12:30 PM	A216

IP Addresses as Digital Fingerprints

IP addresses are often the digital fingerprints that lead investigators to critical breakthroughs. In this webinar, we'll examine the pivotal role IP data plays in modern criminal investigations and show how combining technical knowledge with investigative tools can accelerate case success. Join us to:

- Acquire and resolve IP addresses to their original source with precision
- Combine public OSINT and private, lawfully obtained IP data for stronger case development
- Detect and interpret the use of VPNs, proxies, and NATs in obfuscating criminal activity
- Identify key providers that store IP data and understand how to legally obtain it
- Effectively deconflict to streamline efforts and avoid overlap across teams and jurisdictions

Whether you're targeting online predators, drug networks, fraud operations, or violent offenders, this session will arm you with the digital tracing skills necessary to connect virtual breadcrumbs to real-world arrests

Included with Registration

Date	Time	Room
Wednesday, July 29	8:00 AM – 10:00 AM	A222

IP Networking for Beginners

None of us signed up for law enforcement careers thinking we'd become network engineers, yet here we are. This class is designed for those who are new to IP networking or need a refresher. Students will learn basic concepts and methods to successfully configure cameras, encoders, and routers. We'll also cover some advanced topics, such as port forwarding and dynamic domain name services.

Included with Registration

Date	Time	Room
Monday, July 27	1:00 PM – 3:00 PM	A216
Monday, July 27	8:00 AM – 10:00 AM	A216

Interdiction – Device Concealment and Detection in Transport, Packages, Places and People

The carriage of contraband, be it human, drugs, stolen goods, or illegal imports are often tagged with trackers and/or devices capable of being tracked. Bluetooth, Wi-Fi, and mesh are all RF technologies that can trigger an alert to reveal a package, vehicle, container, or human which requires further investigation as a result of the detection of unusual or suspected RF activity. This workshop will demonstrate best practice tradecraft around how to identify sources of RF which will lead a higher level of detection and disruption of criminal behavior.

Included with Registration

Date	Time	Room
Monday, July 27	1:00 PM – 3:00 PM	B130

Jammer Detection - The Adversary You Need to be Looking For

Jamming is routinely used as a mechanism to obfuscate movement, conceal criminality and to hide under an umbrella of radio silence. Jamming of GPS and other common radio channels is a sure sign of suspicious activity. The ability to detect jamming activity can help significantly in fighting a wide range of crime types including high value auto theft, truck cargo theft, movement of drugs or people and illegal garages “chop shops” - either from the ground or from the air. The ability to detect, map and defeat jamming activity removes a criminal’s cloak of invisibility. This workshop will demonstrate the tradecraft around Jammer detection at a local and regional level and demonstrate how to locate the origin of the jamming.

Included with Registration

Date	Time	Room
Monday, July 27	3:30 PM – 5:30 PM	B130

Leveraging Ever-Expanding LPR Networks to Strengthen Criminal Investigations

This presentation examines the rapid and exponential growth of License Plate Recognition (LPR) systems and their expanding role in modern law enforcement investigations. Attendees will explore how agencies gain access to both government-owned and commercial LPR systems and develop an understanding of how Artificial Intelligence (AI) is significantly enhancing LPR capabilities to improve public safety, investigative efficiency, and real-time situational awareness. **(Continued next page)**

Leveraging Ever-Expanding LPR Networks to Strengthen Criminal Investigations (Continued)
The session will explain how today's AI-driven LPR systems extend well beyond basic license plate capture by providing valuable contextual data such as vehicle make, model, color, travel patterns, and behavioral indicators. These advancements enable investigators to develop stronger leads, identify suspect vehicles more quickly, and reconstruct vehicle movements with greater accuracy.

In addition, the presentation will highlight LPR best practices, advanced query strategies, and effective hotlist management, while examining how LPR technology supports call detail records (CDR) and broader digital evidence analysis. The session will also include real-world operational examples demonstrating the crime-fighting power of LPR technology and its role in strengthening investigations.

Included with Registration

Date	Time	Room
Monday, July 27	3:30 PM – 5:30 PM	A224
Wednesday, July 29	8:00 AM – 10:00 AM	A216

More Than a Sector to Me: Timing Advance and Site Characteristics in Cell Site Analysis

Traditional cell site analysis often stops at identifying the serving tower and sector, but modern investigations demand far more precision. This seminar takes participants beyond the basics and into the deeper layers of cellular network behavior that can meaningfully refine device location assessments. Attendees will learn what Timing Advance (TA) is, how it is generated within LTE and 5G networks, and how to properly interpret TA values to estimate a device's distance from a serving site. Through practical examples, the session will demonstrate how TA can corroborate or challenge assumptions made from simple traditional usage mapping.

The seminar also explores how to integrate TA with traditional cell site and azimuth analysis to build a more accurate picture of user equipment (UE) movement and location. Participants will examine key site-specific characteristics that can reveal additional clues about where a UE could have been located, especially in the absence of TA data.

Included with Registration

Date	Time	Room
Monday, July 27	1:00 PM – 3:00 PM	A224
Wednesday, July 29	8:00 AM – 10:00 AM	A224

OSINT in Tactical Investigations

This course examines the internet as a critical investigative resource, emphasizing the importance of identifying actionable intelligence rather than focusing solely on individuals. **(Continued next page)**

OSINT in Tactical Investigations (Continued)

Participants learn how online research can reveal valuable information such as personal identification, movements, business relationships, family associations, addresses, telephone numbers, and other investigative leads. The course also highlights how accurate and methodical searches on social media platforms can assist in identifying suspects, witnesses, and associated networks. Instruction includes effective search engine techniques, real-time search pattern manipulation, and the use of open-source intelligence (OSINT) from both surface and deep web resources. Participants are introduced to the capabilities and limitations of artificial intelligence and facial recognition, including methods for detecting AI-generated images and using image analysis tools responsibly. Additional topics cover username analysis across platforms and proven strategies for navigating social networking sites to uncover reliable, actionable intelligence that supports successful investigations.

Included with Registration

Date	Time	Room
Tuesday, July 28	10:30 AM – 12:30 PM	A213
Wednesday, July 29	10:30 AM – 12:00 PM	A213

Streetlight Power Taps for Surveillance Equipment

Course will provide students with knowledge and hands on practical experience to assemble devices to access power from streetlight poles to power surveillance equipment. Students will leave with a street light photo cell voltage tester, 110v-3pin photo cell plug in power tap, 110v- 7 pin photocell plug in power tap, 110-12v Mesh network bypass solution, and a street light pole hand hole adapter to safely power ground pedestal style props. Students will also take home various hand tools used during the class for future builds at their home agencies.

Pre-Registration Required – Additional Fee: $375

Date	Time	Room
Tuesday, July 28	8:00 AM – 12:30 PM	B132
Monday, July 27	1:00 PM – 5:30 PM	B132

TEMPEST Concerns (Detection & Mitigation) and In-Place Monitoring Systems (IPMS)

The first module will consist of focusing on protecting electromagnetic radiation emitted from electronic devices. The second module will focus on systems designed to continuously monitor the condition or performance of a specific environment, structure, or process without requiring removal or interruption.

Included with Registration

TEMPEST Concerns (Detection & Mitigation) and In-Place Monitoring Systems (IPMS) (Continued)

Date	Time	Room
Tuesday, July 28	8:00 AM – 10:00 AM	A211

TPSM - Tire Pressure Sensor Monitoring to Surveil, Detect and Record

Tire pressure sensor monitoring will enable exploitation of mobile device security. Cars, trucks and motorbikes all have unique identifiers which could be identified, recorded and tracked in order to geolocate vehicles and by implication persons of interest. This workshop will demonstrate best practice around how to utilize this disruptive technology and analyze the data generated by vehicle tires and in order to track and lifestyle a vehicle, trigger watchlists and provide actionable intelligence.

Included with Registration

Date	Time	Room
Thursday, July 30	8:00 AM – 10:00 AM	A211

Tactical Indoor UAS Ops

This comprehensive indoor drone training program is delivered as a 16-hour course conducted over four consecutive days during the Training Event. The class meets Monday through Thursday for four hours each day. During the first two instructional blocks, students are introduced to foundational UAS concepts, including basic terminology, remote control operations, flight maneuvers, and indoor safety procedures. In the remaining sessions, students transition to hands-on application, practicing structured flight techniques, maneuvering patterns, and scenario-based operations in a controlled indoor environment. Each participant will receive a DJI Neo configured with a tactical setup that can be taken back and implemented within their agency. Realistic training scenarios will serve to complete an indoor NIST Basic Course Evaluation.

Scheduling Note: This is an intensive four-day (16 hour) class taking place during all training hours Monday, Tuesday, Wednesday and Thursday.

Pre-Registration Required – Additional Fee: $1,300

Date	Time	Room
Monday, July 27 ***and***	1:00 PM – 5:30 PM	B131
Tuesday, July 28 ***and***	8:00 AM – 12:30 PM	
Wednesday, July 29 ***and***	8:00 AM – 12:30 PM	
Thursday, July 30	8:00 AM – 12:00 PM	

Technical Installations in a High Voltage Environment Refresher Training for Supervisors and Installers

This four-hour High Voltage Installation Safety Refresher provides OSHA-recommended annual training and supports OSHA's emphasis on a continual process of improving workplace safety and health in high-voltage environments. The course reinforces required OSHA training topics while focusing on the prevention of serious electrical injuries and the application of safe work practices.

Instruction includes updates to 29 CFR 1910.269; identification and prevention of electrical hazards; electrical safe work practices and safety principles; guidelines for personnel qualification; site surveys, job briefings, and work planning requirements; bucket truck operations; traffic control and environmental considerations; and both management and personal responsibilities.

This course is intended for qualified employees who have successfully completed NATIA's Technical Installations in a High Voltage Environment course, as well as their supervisors and managers. It is also appropriate for other NATIA members seeking an overview of high-voltage safety requirements, training obligations, and inherent risks prior to committing their organization and personnel to this type of work.

Pre-Registration Required – Additional Fee: $100

Date	Time	Room
Tuesday, July 28	8:00 AM – 12:30 PM	A213

Test Table

Have you ever been on the internet and saw a tool or item that was advertised as a labor saver or short cut to making your job easier? Have you then looked at the price and decided to skip it because you didn't want to spend your money on it, and your department did not have funding? Welcome to the Test Table.

NATIA is hosting a room this year with new tools and ideas that are out there that maybe you haven't seen or have and want to try. At the Test Table you will be able to pick them up, hold them and use them and see if they are really something that you can use in your shop back home.

Those that come into the Test Table will be asked to drop a business card off in a raffle box. On Thursday morning, all the major tools/items will be raffled off to those who came in and tried the items out. Maybe you won't have to spend your money on that tool after all. Additionally, we will be bringing back NATIA's ham radio station, N1TIA, that will be in operation during this time.

Included with Registration

(Continued next page)

Test Table (Continued)

Date	Time	Room
Tuesday, July 28	8:00 AM – 12:30 PM	A233
Wednesday, July 29	8:00 AM – 12:30 PM	A233
Thursday, July 30	8:00 AM – 10:00 AM	A233

Timing Advance - Understanding How it Works and How to Explain Anomalies

This course provides a technical examination of Timing Advance (TA)—a data point widely relied upon by law enforcement agencies across the United States, yet frequently misunderstood. The session explains what Timing Advance is, how it is generated by cellular networks, and how service providers supply it within cellular records. Attendees will learn how TA should be properly interpreted, including operational use cases, the meaning and limitations of TA bands, and how accuracy can vary based on network architecture and environmental factors. Instruction also addresses Timing Advance in 5G environments, including Standalone (SA) deployments, FR1 and FR2 frequency ranges, and the impact of subcarrier spacing on TA calculations. The course further evaluates the reliability of TA data and reviews benchmarking projects designed to measure its real-world accuracy. Participants will leave with a clearer technical understanding of Timing Advance, its evidentiary value, and its investigative limitations.

Included with Registration

Date	Time	Room
Wednesday, July 29	10:30 AM – 12:30 PM	A112

UAS Exploitation and Intelligence Triage: From Recovery to Intelligence Reporting

This course will cover post mitigation or discovery of downed drone actions, starting with safety. Scene documentation, drone descriptives, handling to preserve DNA and fingerprints. Acquisition/Extraction methods, data parsing, categorizing, and carving (hands-on). Steps on converting drone data to human friendly maps, charts, and expository reports that answer investigative needs or intelligence collection requirements.

Students will receive a Drone Forensic Intelligence System Tool (Drone FIST) and instructions on how to use this tool (source code provided). This tool is a product created within NCIS.

Each student will need to provide a laptop with administrative rights and at least two USB port, running Windows 11, 32 GB of Ram, i7, 500 GB hard drive. Additionally, a 32GB USB thumb drive is required.

Included with Registration

UAS Exploitation and Intelligence Triage: From Recovery to Intelligence Reporting (Continued)

Date	Time	Room
Wednesday, July 29	8:00 AM – 12:30 PM	B130

Volt/Amp Distribution Box Build for Surveillance Platforms

Students will learn why the use of this device is a labor saver when putting together a battery-operated surveillance platform. Each student will assemble a small box with a volt and amp meter that will be in between the power source (battery) and the devices to be powered for the surveillance set up. The device will indicate the voltage and current required for any equipment connected to it in order to determine the ampere hour capacity of the battery needed to run the equipment. The components of the box will be discussed so that students will have a good understanding of what the device is capable of. Input and output of the device is protected by a diode to prevent damage to any equipment or power supply if voltage polarity is reversed. The use of the diode, meter, connectors etc. will be explained with a power point and then the device will be built using a step-by-step power point. As the device is being built, the meter is tested to assure connections are correct and at the conclusion of the build, each student will test the completed device with 4 different current loads to appreciate the usefulness of the device. Parameters of the device are 4.5vdc to 30vdc at 10 amp maximum. The class is designed for beginner through advanced tech so no one is left behind.

Pre-Registration Required – Additional Fee: $50

Date	Time	Room
Thursday, July 30	8:00 AM – 10:00 AM	B132
Thursday, July 30	1:00 PM – 3:00 PM	B132

WIFI Pineapple Pager Basics

Students will learn the basics of using the Hak5 WIFI Pineapple Pager in a law enforcement context. Labs will cover equipment updates, maintenance, WIFI device jamming for high-risk warrant execution, new payload installation, device recon and discovery, Wigle.net for recon. Device familiarization, firmware updates, factory reset and recovery options, WIFI Basics, Community payload resources (Github/Discord Links), uploading custom payloads from flash drive, 30 minutes of physical recon in the surrounding area, 30 minutes of analysis and extracting intel from the data. Targeted Device discovery, deauthing WIFI devices. Students will receive 1 WIFI Pineapple Pager, cabling, and a USB flash drive containing scripts and updates.

A laptop with admin privileges is required for this class

Pre-Registration Required – Additional Fee: $375

(Continued next page)

WIFI Pineapple Pager Basics (Continued)

Date	Time	Room
Tuesday, July 28	8:00 AM – 12:30 PM	B231
Thursday, July 30	8:00 AM – 12:30 PM	B231

Your Phone is Screaming Your Name: Using Wi-Fi Probe Requests to Detect and Track Surveillance

Chasing Your Tail – Next Generation (CYT-NG): Wireless Device Persistence Analysis for Surveillance and Counter-Surveillance is a technical and operational course examining how Wi-Fi probe requests—continuously broadcast by wireless devices—create persistent digital signatures that can be detected, analyzed, and correlated across time and location. Participants are introduced to CYT-NG, an open-source Python tool designed to determine whether a device is following you across multiple locations or whether you are successfully tracking a target device. The course covers hardware selection, Kismet configuration, and full system deployment, while demonstrating overlapping time-window analysis to generate device persistence scores and identify recurring devices of investigative interest. Instruction includes GPS correlation and clustering algorithms to distinguish random proximity from sustained co-movement, as well as integration with the Wiggle API to geolocate probed SSIDs that may reveal associated residences, workplaces, hotels, or other significant locations.

Attendees will also learn to produce professional outputs including Markdown and HTML reports, KML files, Google Earth visualizations, movement paths, threat-level indicators, and activity heatmaps. Through a guided setup process using a Linux laptop, monitor-mode Wi-Fi adapter, and Bluetooth GPS receiver, participants will leave with a comprehensive implementation guide and the knowledge required to independently deploy and operate the system in real-world surveillance and counter-surveillance environments.

Included with Registration

Date	Time	Room
Tuesday, July 28	10:30 AM – 12:30 PM	A220