NW3C now offers live online training! Live online training is 100% instructor-led and allows you to learn remotely in an interactive virtual environment. Students will learn in-depth material during lectures, hands-on exercises, and breakout sessions. Get the same benefits of a traditional classroom setting while learning virtually!

+ nw3c.org/live-online
Basic Cyber Investigations: Digital Footprints

BCDF | 1 day  This course introduces the concept of digital footprints and best practices in protecting personally identifiable information (PII). Topics include limiting an individual's digital footprint, protecting privacy on online social media, the consequences of oversharing PII, and steps to take after becoming a target of doxing.

Basic Cyber Investigations: Dark Web & Open Source Intelligence

BCDW/OSINT | 3 day  This course provides expert guidance in the skills that law enforcement officers need to conduct successful online investigations. Topics include IP addresses and domains, an overview of currently popular online social media platforms, best practices for building an online undercover profile, foundational knowledge related to the dark web, and recovery of forensic evidence from the dark web.

Basic Cyber Investigations: Advertising Identifiers

BCI-ADID | 1 day  This course covers device identifiers (IDs) in general, advertising IDs in detail, important legal considerations, overall investigative process, and tools available to law enforcement. Students will use commercially available investigative tools for querying databases of advertising IDs and displaying their recorded broadcast locations.

Basic Cyber Investigations: Cellular Records Analysis

BCI-CRA | 2 day  This course is designed for officers, investigators, and analysts who encounter cell phone evidence retained by cellular carriers. Class concepts include instruction on how to preserve, request, interpret, analyze, and present call detail records from cellular providers, and how to plot cellular site locations to determine the approximate position of a device during a given period.

Intermediate Cyber Investigations: Virtual Currency

ICI-VC | 2 day  This course provides students with the fundamental knowledge and skills needed to investigate crimes involving virtual currency. Instructors explain foundational concepts including the characteristics of money, virtual currency, and cryptocurrency. Blockchain technology, proof work, and proof of stake are covered, and students learn how industry-leading cryptocurrencies work and how they differ from each other. Finally, students learn investigative techniques for tracking and documenting transactions and best practices for seizing and securing cryptocurrency.

Basic Digital Forensic Analysis: Seizure

BDA-SEizure | 1 day  This course introduces the information and techniques law enforcement personnel need to safely and methodically collect and preserve digital evidence at a crime scene in a forensically-sound manner. Topics include recognizing potential sources of digital evidence; planning and executing a digital evidence-based seizure; and the preservation, collection, documentation, and transfer of digital evidence.

Basic Digital Forensic Analysis

BDA | 2 day  This course provides the fundamental knowledge and skills required to preview and acquire images from some of the most commonly encountered forms of digital evidence in a forensically-sound manner. This course covers digital storage media and how data is stored, firmware interfaces, the forensic previewing process, live and dead-box previewing, the forensic acquisition process, tool validation, hardware and software write blockers, forensic image formats, and multiple forensic acquisition methods.

Intermediate Digital Forensic Analysis: Automated Forensic Tools

IDFA-AFT | 4 day  This course provides students with the fundamental knowledge and skills necessary to perform a limited digital forensic examination, validate hardware and software tools, and effectively use digital forensic suites and specialized tools. The course begins with a detailed explanation of the digital forensic examination process, including documentation, case management, evidence handling, validation, and virtualization. Students learn to use today’s leading commercial and open source digital forensic suites: Magnet AXIOM™, X-Ways Forensics, and Autopsy®. Instruction on each suite will include an interface overview, configuration, hashing, file signature analysis, keyword searching, data carving, bookmarking, and report creation.
Intermediate Digital Forensic Analysis—SQLite Primer

**IDFA-SQLITE | 4 day**  Mobile devices dominate the intake list and the desks of most digital PRIMER forensics’ analysts globally. SQLite is a self-contained, serverless database engine. It is found on nearly every operating system and dominates iOS®, Android®, and macOS® as one of the most prevalent and relevant data storage mechanisms. With an increase in device security, learn to arm yourself with the skills and techniques needed to conquer the analysis of nearly any application.

Advanced Digital Forensic Analysis: Windows

**ADFA-Win | 4 day**  This course covers the identification and extraction of artifacts associated with the Microsoft® Windows® operating system. Topics include the Change Journal, Bitlocker®, and a detailed examination of various artifacts found in each of the Registry hive files. Students also examine event logs, Volume Shadow Copies, link files, and jump lists.

Advanced Digital Forensic Analysis: macOS

**ADFA-Mac | 4 day**  This course teaches students to identify and collect volatile data, acquire forensically-sound images of Macintosh® computers, and perform forensic analysis of macOS® operating system and application artifacts. Students gain hands-on experience scripting and using automated tools to conduct a simulated live triage, and use multiple methods to acquire forensically-sound images of Apple Macintosh computers. Topics include how the macOS default file system stores data, what happens when files are sent to the macOS Trash, where operating system and application artifacts are stored, and how they can be analyzed. Forensic artifacts covered include password recovery, recently-opened files and applications, encryption handling, Mail, Safari®, Messages, Facetime®, Photos, Chrome™, and Firefox®.

Advanced Digital Forensic Analysis: iOS & Android

**ADFA-Mobile | 4 day**  This course provides the fundamental knowledge and skills necessary to preserve, acquire, and analyze data on iOS® devices and various Android™ devices. Students use forensically-sound tools and techniques to acquire and analyze potential evidence. Topics include identifying potential threats to data stored on devices, available imaging options, accessing locked devices, and the default folder structure. The forensic artifacts covered include device information, call history, voicemail, messages, web browser history, contacts, and photos.

Basic Level Spreadsheetsing Skills

**BLSS | 1 day**  This course provides foundational spreadsheetsing knowledge and skills to enhance workplace productivity. The course covers basic navigation of Microsoft® Excel by combining live demonstrations and hands-on exercises.

Financial Investigations Practical Skills

**FIPS | 3 day**  Students develop the practical skills, insight, and knowledge necessary to manage a successful financial investigation from start to finish, including the acquisition and examination of financial records, interview skills, and case management and organization. Additional topics include forgery and embezzlement, financial exploitation of the elderly, working with spreadsheets, financial profiling, and state-specific statutes and legal issues.

Financial Investigations Triage

**FIT | 1 day**  This course provides an overview of the actions investigators can take at the outset of a financial crime investigation. Students learn to ask critical questions, gather documentation, and analyze information for leads. Topics include obtaining and working with financial records, red flags in financial cases, money laundering, and investigative strategies for different types of financial crimes.

Financial Records Examination & Analysis

**FREA | 3 day**  This course covers the acquisition, examination, and analysis of many types of financial records, including bank statements and checks, wire transfer records, and business records. Topics include recognizing and investigating common indicators of fraud, using spreadsheets to facilitate analysis and pattern recognition, and financial profiling. There is a strong focus on presenting financial evidence in multiple modalities including spreadsheet data outputs, graphic representations, and written/oral presentations.
**FC110**  
**Financial Crimes Against Seniors**  
*FCAS | 2 day*  
This course promotes a multi-agency approach to the problem of financial exploitation of senior citizens. Bringing together law enforcement personnel and adult protective services investigators, the course enhances students’ investigative skills and interviewing techniques while facilitating networking and cooperation that can extend out of the classroom and into real cases. Topics include recognizing elder abuse, working with victims, identifying perpetrators, and resources for investigation and community awareness.

**FC111**  
**Financial Crimes Against Seniors Seminar**  
*FCSS | 1 day*  
This basic overview course promotes a multi-agency approach to the problem of financial exploitation of senior citizens. Topics include working with senior victims, examining documents like bank records and power of attorney, and resources for investigation and community awareness. With a dual focus on financial abuse by trusted persons and common scams aimed at seniors, the course introduces senior-specific investigative skills while facilitating networking and cooperation that can extend out of the classroom and into real cases.

**FC122**  
**Intellectual Property Theft Training**  
*IPTT | 1 day*  
This course introduces the problem of intellectual property (IP) theft and provides tools, techniques, and resources for investigating and prosecuting these crimes. A combination of lecture, discussion, and interactive exercises illustrates the potential dangers and economic repercussions of counterfeit products, as well as best practices and techniques for investigating IP theft. Students are provided with relevant statutes, sample organizational documents for IP investigations, and additional resources for investigators and prosecutors.

**FC201**  
**Financial Records Investigative Skills**  
*FRIS | 3 day*  
This course builds on the concepts introduced in FC 101 (FIPS) and FC 105 (FREA), introducing investigators and prosecutors to emerging issues in financial crime. Topics include money laundering, analyzing large financial data sets, conducting effective interviews, and managing large amounts of financial evidence. This course consists of a mix of lecture, discussion, and hands-on exercises. Students conduct a mock investigation that includes interviews, data analysis, and the construction of an electronic case file.

**FC210**  
**Money Laundering & Commingling**  
*MLC | 1/2 day*  
This course provides basic to intermediate knowledge of the money laundering process and the commingling of funds. The course will provide an understanding of the ingenuity criminals use to move and hide funds while concealing their identity.

**IA101**  
**Foundations of Intelligence Analysis Training**  
*FIAT | 4 day*  
This course addresses the critical need for well-trained intelligence analysts to interpret growing amounts of information. This introductory course covers the history and purpose of intelligence analysis, the intelligence cycle, analytical thinking skills, and the importance of strategic analysis. This course has been certified by DHS/FEMA as course number WV-001-PREV.

**IA102**  
**Introduction to Link Analysis**  
*ILA | 1 day*  
This course provides in-depth instruction on association and social network analysis. This course explains the purpose and process of association analysis, how to create an association matrix, and what social network analysis is with focus on types of centrality, network structure, and the application of the Target Centric approach. Students will also learn how to build and present a link chart using standard symbols and terms.

**IA105**  
**Intelligence Writing and Briefing**  
*IWAB | 3 day*  
This course covers basic intelligence writing and briefing principles as well as methods to facilitate increased intelligence sharing. Topics include creative/critical thinking and critical reading skills, source evaluation, privacy and civil rights, intelligence product writing structure and style, and creating and presenting intelligence briefings.