High-Tech Crime

Financial Crime

Intelligence Analysis

Legal Issues

Classroom & Online Instruction

Tools & Resources
In the last five years, NW3C has trained nearly 40,000 students in all 50 states. In-person training features student-centered, hands-on practical exercises.

Each year, NW3C provides hundreds of hours of technical assistance to law enforcement, regulatory agencies, and prosecutorial agencies that investigate economic and high-tech crime.

Since 2014, NW3C has offered high-quality, on-demand training around the clock, via a robust in-house online learning platform that has reached over 98,000 students.

NW3C 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 webinars are a convenient way to learn more about new and emerging topics related to the investigation and prosecution of economic and high-tech crime. Many webinars feature nationally and internationally recognized subject matter experts.

NW3C creates, maintains, updates, and distributes valuable forensic tools to law enforcement professionals free of charge. Resources like the Law Enforcement Cyber Center (LECC) provide news and information.

NW3C designs and delivers specialized training for prosecutors and judges, giving them the skills to litigate and adjudicate cases involving economic and high-tech crime.

This project was supported by Grant NO. 2018-MU-BX-K001 awarded by the Bureau of Justice Assistance. The Bureau of Justice assistance is a component of the Department of Justice’s Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI101</td>
<td>BCI-DF</td>
<td>Basic Cyber Investigations: Digital Footprints</td>
</tr>
<tr>
<td>CI102</td>
<td>BCI-DW/OSINT</td>
<td>Basic Cyber Investigations: Dark Web &amp; Open Source Intelligence</td>
</tr>
<tr>
<td>CI103</td>
<td>BCI-ADID</td>
<td>Basic Cyber Investigations: Advertising Identifiers</td>
</tr>
<tr>
<td>CI130</td>
<td>BCI-CRA</td>
<td>Basic Cyber Investigations: Cellular Records Analysis</td>
</tr>
<tr>
<td>CI240</td>
<td>ICI-VC</td>
<td>Intermediate Cyber Investigations: Virtual Currency</td>
</tr>
<tr>
<td>DF100</td>
<td>BDFA-SEIZURE</td>
<td>Basic Digital Forensic Analysis: Seizure</td>
</tr>
<tr>
<td>DF101</td>
<td>BDFA-WIN-ACQ</td>
<td>Basic Digital Forensic Analysis: Windows® Acquisition</td>
</tr>
<tr>
<td>DF201</td>
<td>IDFA-AFT</td>
<td>Intermediate Digital Forensic Analysis: Automated Forensic Tools</td>
</tr>
<tr>
<td>DF205</td>
<td>IDFA-SQLITE</td>
<td>Intermediate Digital Forensic Analysis: SQLite Primer</td>
</tr>
<tr>
<td>DF310</td>
<td>ADFA-WIN</td>
<td>Advanced Digital Forensic Analysis: Windows®</td>
</tr>
<tr>
<td>DF320</td>
<td>ADFA-MAC</td>
<td>Advanced Digital Forensic Analysis: macOS®</td>
</tr>
<tr>
<td>DF330</td>
<td>ADFA-MOBILE I</td>
<td>Advanced Digital Forensic Analysis: iOS® &amp; Android®</td>
</tr>
<tr>
<td>FT Series</td>
<td></td>
<td>Digital Forensics: Fast Track</td>
</tr>
<tr>
<td>FC099</td>
<td>BLSS</td>
<td>Basic Level Spreadsheeting Skills</td>
</tr>
<tr>
<td>FC101</td>
<td>FIPS</td>
<td>Financial Investigations Practical Skills</td>
</tr>
<tr>
<td>FC102</td>
<td>FIT</td>
<td>Financial Investigations Triage</td>
</tr>
<tr>
<td>FC105</td>
<td>FREA</td>
<td>Financial Records Examination and Analysis</td>
</tr>
<tr>
<td>FC110</td>
<td>FCAS</td>
<td>Financial Crimes Against Seniors</td>
</tr>
<tr>
<td>FC111</td>
<td>FCSS</td>
<td>Financial Crimes Against Seniors Seminar</td>
</tr>
<tr>
<td>FC122</td>
<td>IPTT</td>
<td>Intellectual Property Theft Training</td>
</tr>
</tbody>
</table>
FINANCIAL RECORDS INVESTIGATIVE SKILLS 12
MONEY LAUNDERING & COMMINGLING 13
FOUNDATIONS OF INTELLIGENCE ANALYSIS TRAINING 13
INTRODUCTION TO LINK ANALYSIS 13
INTELLIGENCE WRITING AND BRIEFING 14
DIGITAL EVIDENCE BASICS & THE CLOUD ACT 14
MOBILE EVIDENCE FOR PROSECUTORS 14
INTRODUCTION TO PREVIEWING 15
UNDERSTANDING DIGITAL FOOTPRINTS 15
INTRODUCTION TO CELL PHONE INVESTIGATIONS 15
VIRTUAL CURRENCY 16
APPLE® INTRODUCTION 16
CYBERSTALKING 16
THE DARK WEB: AN INTRODUCTION 17
INTRODUCTION TO SOCIAL MEDIA AND NETWORKING 17
FIRST RESPONDERS & DIGITAL EVIDENCE 17
SEARCH WARRANTS & DIGITAL EVIDENCE 18
SEARCHING WITHOUT A WARRANT 18
ONLINE UNDERCOVER 18
POST-SEIZURE EVIDENTIARY CONCERNS 19
MOBILE DIGITAL DEVICES & GPS 19
INVESTIGATING INCIDENTS INVOLVING UAVS 19
INTRODUCTION TO COMPUTER NETWORKS 20
ENCRIPTION 20
HOW COMPUTERS WORK AND STORE DATA 20
BASIC DIGITAL FORENSIC ANALYSIS: SEIZURE 21
OVERVIEW OF WHITE COLLAR CRIME 21
FINANCIAL INVESTIGATION BASICS 21
INTRODUCTION TO MORTGAGE FRAUD 22
INTELLECTUAL PROPERTY THEFT: TIME TO MAKE A DIFFERENCE 22
HUMAN TRAFFICKING AWARENESS FOR LAW ENFORCEMENT OFFICERS 22
THE BANK SECRECY ACT: WHAT LAW ENFORCEMENT NEEDS TO KNOW 23
VICTIM-CENTERED SOLUTIONS TO ELDER EXPLOITATION 23
INTRODUCTION TO INTELLIGENCE 23
BASIC ANALYST SKILLS AND REQUIREMENTS 24
POLICIES AND GUIDANCE FOR INTELLIGENCE ANALYSTS EXERCISE 24
PROSECUTING THE DARK WEB 24
SEARCH WARRANTS & DIGITAL EVIDENCE 25
SEARCHING WITHOUT A WARRANT 25
## TOOLS & RESOURCES

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT160 LCCI-WB</td>
<td>LEGAL CHALLENGES TO CRIMINAL INVESTIGATION</td>
<td>25</td>
</tr>
<tr>
<td>PT220 PT-WB</td>
<td>INTRODUCING DIGITAL EVIDENCE IN COURT</td>
<td>26</td>
</tr>
<tr>
<td>RESOURCES</td>
<td>WEBINARS</td>
<td>26</td>
</tr>
<tr>
<td>RESOURCES</td>
<td>MOBILE FRIENDLY PRODUCTS</td>
<td>26</td>
</tr>
<tr>
<td>RESOURCES</td>
<td>PUBLICATIONS</td>
<td>27</td>
</tr>
<tr>
<td>RESOURCES</td>
<td>INTELLECTUAL PROPERTY (IP) WEBSITE</td>
<td>27</td>
</tr>
<tr>
<td>RESOURCES</td>
<td>CYBER S.W.A.T.™</td>
<td>27</td>
</tr>
<tr>
<td>RESOURCES</td>
<td>LAW ENFORCEMENT CYBER CENTER</td>
<td>28</td>
</tr>
<tr>
<td>FORENSIC TOOLS</td>
<td>NW3C UTILITY SUITE™</td>
<td>29</td>
</tr>
<tr>
<td>FORENSIC TOOLS</td>
<td>PERPHOUND™</td>
<td>30</td>
</tr>
<tr>
<td>FORENSIC TOOLS</td>
<td>PHOTOHUNTER™</td>
<td>30</td>
</tr>
<tr>
<td>FORENSIC TOOLS</td>
<td>REPORT GENERATOR™</td>
<td>30</td>
</tr>
</tbody>
</table>
CI 101
CYBER INVESTIGATIONS

Quick Info

1 DAY
CLASSROOM
LIVE ONLINE

BASIC CYBER INVESTIGATIONS: DIGITAL FOOTPRINTS

This course introduces learners to 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, and the consequences of oversharing personal information, along with steps to take after becoming a target of doxing.

CI 102
CYBER INVESTIGATIONS

Quick Info

3 DAY
CLASSROOM
LIVE ONLINE

BCI-DW/OSINT
BASIC CYBER INVESTIGATIONS: DARK WEB & OPEN SOURCE INTELLIGENCE

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. Instructors demonstrate both open source and commercially available investigative tools for evidence collection and recovery of forensic artifacts associated with online social networking and online social media. Automated tools to crawl websites and preserve online evidence are also demonstrated.

CI 103
CYBER INVESTIGATIONS

Quick Info

1 DAY
CLASSROOM
LIVE ONLINE

BCI-ADID
BASIC CYBER INVESTIGATIONS: ADVERTISING IDENTIFIERS

This course teaches law enforcement investigators and analysts methods for handling cases where device location information may be of importance. Topics include 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.
BCI-CRA
BASIC CYBER INVESTIGATIONS: CELLULAR RECORDS ANALYSIS

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. No special hardware or software is required.

ICI-VC
INTERMEDIATE CYBER INVESTIGATIONS: VIRTUAL CURRENCY

This course provides students with the fundamental knowledge and skills they need 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 (Bitcoin®, Ethereum®, and Monero) 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.

BDFA-SEIZURE
BASIC DIGITAL FORENSIC ANALYSIS: SEIZURE

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.
BDFA-WIN-ACQ

BASIC DIGITAL FORENSIC ANALYSIS: WINDOWS ACQUISITION

This course provides the fundamental knowledge and skills required to acquire forensic backup images of commonly encountered forms of digital evidence (Microsoft® Windows® based computers and external storage devices) in a forensically sound manner. Presentations and hands-on practical exercises cover storage media and how data is stored, the forensic acquisition process, tool validation, hardware and software write blockers, forensic backup image formats, and multiple forensic acquisition methods. Students will use third party tools, both free and commercial, that are currently used by practitioners in the field. Key concepts covered in this course include storage media, forensic acquisition process and methods, tool validation, hardware and software write blockers, and forensic backup image formats.

IDFA-AFT

INTERMEDIATE DIGITAL FORENSIC ANALYSIS: AUTOMATED FORENSIC TOOLS

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 Forensics 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.

IDFA-SQLITE

INTERMEDIATE DIGITAL FORENSIC ANALYSIS: SQLITE PRIMER

Mobile devices dominate the intake list and the desks of most digital forensics’ analysts globally. As devices are becoming more secure, with an increase in security; the need for detailed analysis is increasing as well. 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. Rather than hope our forensic tools support the newest applications or be tethered to how a certain utility parses data, we can arm ourselves with the skills and techniques needed to conquer the analysis of nearly any application.
<table>
<thead>
<tr>
<th>Course Code</th>
<th>Course Title</th>
<th>Quick Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>DF 310</td>
<td>ADFA-WIN</td>
<td>ADVANCED DIGITAL FORENSIC ANALYSIS: WINDOWS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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. This course uses a mixture of lecture, discussion, demonstration, and hands-on exercises.</td>
</tr>
<tr>
<td></td>
<td>DF 320</td>
<td>ADFA-Mac</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ADVANCED DIGITAL FORENSIC ANALYSIS: macOS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This course teaches students to identify and collect volatile data, acquire forensically-sound images of Apple® 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®.</td>
</tr>
<tr>
<td></td>
<td>DF 330</td>
<td>ADFA-MOBILE I</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ADVANCED DIGITAL FORENSIC ANALYSIS: iOS &amp; ANDROID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This course provides the fundamental knowledge and skills necessary to preserve, acquire, and analyze data on iOS® devices, (iPod Touch®, iPhone®, and iPad®) as well as 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.</td>
</tr>
</tbody>
</table>
The Digital Forensics Fast Track program was developed to assist agencies in establishing or replenishing a cadre of digital forensic examiners in a short period of time. Multiple weeks of instruction are delivered at intervals of three to six weeks, allowing the students time to apply what they have learned before returning for more advanced training.

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

This course provides hands-on investigative training at a basic level. 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.
FIT
FINANCIAL INVESTIGATIONS TRIAGE
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, interviewing witnesses and suspects, and investigative strategies for different types of financial crimes.

FREA
FINANCIAL RECORDS EXAMINATION AND ANALYSIS
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: spreadsheet data outputs, graphic representations, and written/oral presentations.

FCAS
FINANCIAL CRIMES AGAINST SENIORS
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. Students work together to conduct a mock investigation into a hypothetical case.
FCSS
FINANCIAL CRIMES AGAINST SENIORS SEMINAR

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. Detailed examination of a case study from initial complaint to prosecution reinforces and illustrates the course content. 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.

IPTT
INTELLECTUAL PROPERTY THEFT TRAINING

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.

FRIS
FINANCIAL RECORDS INVESTIGATIVE SKILLS

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.
**MLC**

**MONEY LAUNDERING & COMMINGLING**

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. The course instruction will use examples of real-life cases to provide an interactive session for students.

**FIAT**

**FOUNDATIONS OF INTELLIGENCE ANALYSIS TRAINING**

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. The course was developed by a consortium that included NW3C, the Law Enforcement Intelligence Unit (LEIU), the International Association of Law Enforcement Intelligence Analysts (IALEIA), and the Regional Information Sharing System (RISS). This course incorporates blended learning through online training modules—IA 098 Introduction to Intelligence, IA 099 Basic Analyst Skills and Requirements, and IA 100 Policies and Guidance for Intelligence Analysts. This course has been certified by DHS/FEMA as course number WV-001-PREV.

**ILA**

**INTRODUCTION TO LINK ANALYSIS**

This course provides in-depth instruction on Association and Social Network Analysis. The first part of this course explains the purpose and process of association analysis and how to create an association matrix. Students will also learn how to build and present a link chart using standard symbols and terms. The second part of this course explains what social network analysis is with focus on types of centrality, network structure, and the application of the Target Centric approach.
## IWAB
### INTELLIGENCE WRITING AND BRIEFING
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. An instructor and peer-feedback process is applied to the reports and briefings produced in class.

This course was originally developed in partnership with the U.S. Department of Homeland Security (DHS), the Federal Emergency Management Agency (FEMA), under the National Training and Education Division (NTED).

## DEB
### DIGITAL EVIDENCE BASICS & THE CLOUD ACT
This course provides the technical and legal information prosecutors need to see in cases involving digital evidence through the entire criminal justice process, including seizure, extraction, admissibility, and verdict. Topics include digital evidence commonly seized during the execution of a search warrant, digital evidence stored remotely by third-party service providers, and the processes investigators use to obtain this evidence (such as the interrogation of digital devices). There is a strong focus on case law and other legal issues surrounding the collection and custody of digital evidence, as well as its use at trial. The course also examines new legislation like the CLOUD Act, which is reforming the digital evidence landscape just as rapidly as the ever-changing case law.

## MEP
### MOBILE EVIDENCE FOR PROSECUTORS
This course walks prosecutors through the mobile forensic process, providing crucial information that can help them work effectively with investigators and forensic examiners. The course is designed around the legal issues involved with mobile forensics: from seizure of a device, to admissibility of evidence obtained from a forensic examination, to effective testimony, to challenges commonly raised by defense counsel. Team taught by a mobile forensic examiner and an experienced prosecutor, the course weaves technical and legal concepts together (including state-specific case law) in a format specifically designed for the needs of prosecutors.
ITP-WB
INTRODUCTION TO PREVIEWING
This interactive online course provides an overview of the basic concepts behind secure previewing of digital devices in a forensically-sound manner. Students become familiar with both on-site and off-site secure previewing and learn to identify the two states in which a preview can be conducted (live-box and dead-box previewing). At the completion of the course, students will be able to recognize the recommended collection order of volatile data (the order of volatility).

UDF-WB
UNDERSTANDING DIGITAL FOOTPRINTS
This online course introduces learners to 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, and the consequences of oversharing personal information, as well as steps to take after becoming a target of doxing.

ICPI-WB
INTRODUCTION TO CELL PHONE INVESTIGATIONS
This online course provides an overview of the two phases of a cell phone investigation: the preservation, extraction, and analysis of data within the phone, and the acquisition and analysis of data external to the phone (call detail records and other information). Students become familiar with several forensic tools currently in use in the field, including NW3C’s PerpHound™, a specialized tool that assists in plotting historical cell site locations. Other topics include cell phone components, cellular network components, and mobile device identification.
VC-WB
VIRTUAL CURRENCY

This online course covers basic information and concepts that serve as an introduction to virtual currencies and their relationship to other types of currency. It covers various types of virtual currency, including the difference between decentralized and centralized currencies, with a strong focus on Bitcoin® what it is, how it is stored, and Bitcoin-specific investigative tips and techniques.

AI-WB
APPLE INTRODUCTION

This online course provides the fundamental knowledge necessary to identify different types of Apple® hardware and to use the macOS® operating system. Students learn what hardware devices are currently available from Apple including laptops, desktops, wireless hardware, and mobile devices. Students are also introduced to the macOS graphical user interface and its four major components: Desktop, Finder, Menu Bar, and Dock.

CS-WB
CYBERSTALKING

This online course provides information on what constitutes cyberstalking in a legal context and information on handling cyberstalking complaints. Common elements of cyberstalking cases, potential tools and platforms used by cyberstalkers, and behavioral indicators are also covered in this course. Developed with a victim-centered approach, this course provides information on establishing a relationship with victims to maximize their safety and further investigative efforts. The course concludes with guidance on developing an investigative checklist and additional resources available to law enforcement.
DARK-WB
THE DARK WEB: AN INTRODUCTION

This online course introduces the dark web and some of the most popular tools to access the darknet, including Tor, Freenet, and Invisible Internet Project (I2P). Basic topics include what Tor is, how it works, and who uses it; as well as dark markets in Tor Hidden Service Servers (also known as .onion servers) and other hidden services. The course concludes with brief case studies covering some of the largest dark-market seizures in history.

ISMN-WB
INTRODUCTION TO SOCIAL MEDIA AND NETWORKING

This course introduces learners to the digital space known as social media. It presents basic terminology used to describe how social media and networking services are accessed, statistical data on users and mobile devices, and a variety of popular services. This course also identifies and explains law enforcement uses of social media and networking services, the value of open source intelligence (OSINT), and important considerations such as social media policies, ethics, and privacy issues associated with social media and networking services.

LC1-WB
FIRST RESPONDERS & DIGITAL EVIDENCE

This online course provides basic information for first responders who may encounter digital evidence in the course of their duties. Topics include the definition of digital evidence, where it can be found, the importance of getting digital devices to a forensics expert, and the ways in which digital evidence can be compromised. This course also addresses the issue of when a warrant is required to seize and/or search digital devices.

This course is part of the training series Legal Concerns for Digital Evidence Responders. It can be completed as a stand-alone course or in combination with the other courses.
**LC2-WB**

**SEARCH WARRANTS & DIGITAL EVIDENCE**

This online course provides information on obtaining and executing search warrants in cases involving digital evidence, with a focus on the similarities and differences between these and other search warrants. The course covers establishing probable cause, particularity, scope, and nexus; the use of outside experts; and out-of-state warrants for remote evidence.

This course is part of the training series Legal Concerns for Digital Evidence Responders. It can be completed as a stand-alone course or in combination with the other courses.

---

**LC3-WB**

**SEARCHING WITHOUT A WARRANT**

This online course provides legal information on situations involving digital evidence in which the Fourth Amendment does not apply. Topics include reasonable expectation of privacy in a digital context, private searches, reasonable government searches, and searches with consent.

This course is part of the training series Legal Concerns for Digital Evidence Responders. It can be completed as a stand-alone course or in combination with the other courses.

---

**LC5-WB**

**ONLINE UNDERCOVER**

This online course provides a legal overview of what investigators are and are not permitted to do while conducting online undercover investigations. Topics include terms of service, entrapment and outrageous government misconduct, and wiretapping law as it relates to the recording and documenting of online activities. This course also covers defense strategies commonly used to counter online undercover investigations.

This course is part of the training series Legal Concerns for Digital Evidence Responders. It can be completed as a stand-alone course or in combination with the other courses.
LC6-WB
POST-SEIZURE EVIDENTIARY CONCERNS

In contrast to the other courses in this series, which deal primarily with the acquisition of digital evidence, this online course addresses legal issues that appear relatively late in the investigative and judicial process. Topics include the Fifth Amendment as it applies to passwords and login credentials, determining the ownership of files on digital devices, and the admissibility of online evidence.

This course is part of the training series Legal Concerns for Digital Evidence Responders. It can be completed as a stand-alone course or in combination with the other courses.

LC7-WB
MOBILE DIGITAL DEVICES & GPS

This online course addresses the legal issues surrounding mobile digital devices including cell phones and GPS devices. Topics include seizing and searching mobile devices, the process of obtaining both historical and current location information from cellular service providers, and legal process needed to install a GPS unit on a suspect's vehicle.

This course is part of the training series Legal Concerns for Digital Evidence Responders. It can be completed as a stand-alone course or in combination with the other courses.

UAV-WB
INVESTIGATING INCIDENTS INVOLVING UAVS

This online course introduces the history of UAVs and the ways they are commonly used, both legitimately and in relation to a crime, and focuses on the ways law enforcement can gather and analyze evidence involving drones. Topics include gathering evidence both internal and external to the drone, as well as methods for manually processing flight logs and displaying data on Google Earth™.
ICN-WB

INTRODUCTION TO COMPUTER NETWORKS

This online course introduces fundamental concepts and terminology related to computer networks. Topics include the importance of computer networks, types of computer networks, common network components, network topologies and media, the OSI and TCP/IP models of communication, and IP addressing. The course also addresses law enforcement’s role in cybersecurity within the current landscape of digital crime.

ENC2-WB

ENCRYPTION

This online course covers the purpose of encryption and the process of encrypting data, as well as clarifying the distinctions between encryption and other operations like password protection and encoding. It explores the confusion, diffusion, and secret key encryption methods. Topics include detecting encryption (including recognition of some of the most popular types of encryption software), as well as proper procedures for law enforcement professionals who detect that encryption may be present on a device. Additionally, this course provides an overview of some of the best and most common encryption detection software tools.

HDS-WB

HOW COMPUTERS WORK AND STORE DATA

The first module of this online course covers fundamentals such as recognizing computer components and their functions, accessing computer firmware, and the startup and shutdown processes. The second module covers how a hard disk drive works, how data is converted into digital information, how to calculate the storage capacity of a device, partitioning and how that is used for storage, and how a solid state drive functions.
**BDFA-Seizure-WB**

**BASIC DIGITAL FORENSIC ANALYSIS: SEIZURE**

This online course introduces the information and techniques law enforcement personnel need to safely and methodically collect and preserve digital evidence in a forensically-sound manner at a crime scene. 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.

---

**WCC-WB**

**OVERVIEW OF WHITE COLLAR CRIME**

This online course presents awareness-level information on a variety of topics related to white collar crime. The course covers basic definitions and terminology, common types of white collar crime, and the effects of white collar crime on society. Students learn to recognize and respond to common internet scams, provide assistance to victims of white collar crime, and recognize warning signs and red flags of criminal behavior. This course emphasizes law enforcement’s role in preventing and responding to white collar crime, and includes additional resources for combating this widespread problem.

---

**FIB-WB**

**FINANCIAL INVESTIGATION BASICS**

This course provides fundamental knowledge on financial investigation and data analysis. The investigation portion of the course will cover common consumer scams, how to identify suspects and their financial accounts and best processes for obtaining suspect’s records. The analysis portion of the course will cover the process of acquiring data, discuss methods for entering data, and provide strategies for finding patterns in data sets.
MORF-WB
INTRODUCTION TO MORTGAGE FRAUD

This online course presents awareness-level information on mortgage fraud. The course covers basic definitions and terminology, common types of mortgage fraud schemes, components of fraud, roles in the mortgage process, and legal explanations. Students also learn to recognize fraud indicators associated with a variety of schemes and opportunities to commit fraud throughout the mortgage process. A sample mortgage loan application and other forms used in the process are available to download within this course.

IPT-WB
INTELLECTUAL PROPERTY THEFT: TIME TO MAKE A DIFFERENCE

This online course presents awareness-level information on intellectual property (IP) theft. Students will be presented with a high-level approach to understanding the scope and trends of IP, general tips on identifying counterfeit products, informational videos, and more. The National Intellectual Property Rights Coordination Center will be discussed at the end of this training with an emphasis on information sharing.

HTA-WB
HUMAN TRAFFICKING AWARENESS FOR LAW ENFORCEMENT OFFICERS

This online course provides law enforcement personnel with an overview of the various elements involved in the crime of human trafficking. It covers the major types, scope, and extent of human trafficking. Additionally, it discusses resources for law enforcement who encounter human trafficking. Topics include physical and behavioral indicators of human trafficking, trafficked victims’ rights, the elements of a human trafficking operation, and information about several federal and private organizations making efforts to combat human trafficking.
BSA-WB
THE BANK SECRECY ACT: WHAT LAW ENFORCEMENT NEEDS TO KNOW

This online course presents awareness-level information on the Bank Secrecy Act (BSA) and how it is used to aid law enforcement investigations into terrorism and criminal activity. Students are introduced to the BSA, the USA PATRIOT Act, and definitions of commonly-used terms. This course also explains the various documents and forms filed by financial institutions under the BSA. The Financial Crimes Enforcement Network (FinCEN) is discussed with an emphasis on services and resources provided to law enforcement. Proper application of BSA forms is reinforced through scenario-based exercises at the end of this course.

VCS-WB
VICTIM-CENTERED SOLUTIONS TO ELDER EXPLOITATION

This online course is a series of ten victim-centered, interactive web-based training modules covering trauma informed promising practices for detecting and responding to elder financial exploitation. Each module will focus on one victim of elder financial exploitation, and address how Adult Protective Services (APS) workers, financial industry professionals, law enforcement, and other responders detect, respond to, and support victims.

IINT-WB
INTRODUCTION TO INTELLIGENCE

This online course introduces students to the basics of law enforcement intelligence. Developed for criminal justice practitioners, entry level analysts, and those pursuing a career in intelligence analysis, this course provides a historical background, explanation of the purpose and models of intelligence, the intelligence cycle, and legal issues and ethics.
BASR-WB
BASIC ANALYST SKILLS AND REQUIREMENTS

This online course introduces students to the basic skills and requirements of today’s law enforcement intelligence analysts. Developed for criminal justice practitioners, entry level analysts, and those pursuing a career in intelligence analysis, this course highlights core competencies, provides instruction on various thinking models, and inference development. Both written and spoken products of intelligence such as reports and briefings will also be discussed.

PGIAE-WB
POLICIES AND GUIDANCE FOR INTELLIGENCE ANALYSTS EXERCISE

This independent reading exercise provides students with policy and guidance documents critical to the role of an intelligence analyst. The documents in this exercise include: 28 CFR Part 23 and a Guide to Criminal Intelligence Policies, Analyst Professional Development Roadmap, National Criminal Intelligence Sharing Plan, and Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities.

PDW-WB
PROSECUTING THE DARK WEB

This online course introduces prosecutors to the challenges they may face in prosecuting cases involving the dark web. It is designed around a case study that moves through the entire prosecutorial process, from charging decisions through sentencing. Topics include how the dark web works, an introduction to Tor and similar tools, and an overview of key terms related to investigations in the dark web. The course provides a framework for the prosecution of a case involving the dark web, including a specific timeline showing what steps to take and when. Relevant, up-to-date case law is included to assist in future prosecutorial efforts.
PT2-WB
SEARCH WARRANTS & DIGITAL EVIDENCE
This online course provides information on obtaining and executing search warrants in cases involving digital evidence, with a focus on the similarities and differences between these and other search warrants. The course covers establishing probable cause, particularity, scope, and nexus; the use of outside experts; and out-of-state warrants for remote evidence.

PT3-WB
SEARCHING WITHOUT A WARRANT
This online course provides legal information on situations involving digital evidence in which the Fourth Amendment does not apply. Topics include reasonable expectation of privacy in a digital context, private searches, reasonable government searches, and searches with consent.

LCCI-WB
LEGAL CHALLENGES TO CRIMINAL INVESTIGATIONS
This online course provides information regarding the legal principles involving the rights of defendants and witnesses. This course covers several topics pertaining to criminal investigations including admissible evidence, exculpatory evidence, and the exclusionary rule. There is a strong focus on the Fourth, Fifth, and Sixth Amendments to the U.S. Constitution.
PT-WB
INTRODUCING DIGITAL EVIDENCE IN COURT

This course focuses on the modern challenges with introducing digital evidence in court. In this course, we cover both Brady and admissibility requirements and explain what steps need to be taken to ensure digital evidence can be introduced and effectively used at trial. Takeaways from the course include best practices for visual presentations and a mock exam template.

WEBINARS

NW3C webinars are a convenient way to learn more about new and emerging topics related to the investigation and prosecution of economic and high-tech crime. Through a combination of live and on-demand webinars, criminal justice professionals can gain and enhance their knowledge and skills without a large time commitment or the need to travel to a training site.

MOBILE FRIENDLY PRODUCTS

A continually updated group of products and tools designed for your phone or tablet. Apple® iOS® and Android™ compatible; also accessible via desktop or laptop computer.

Interactive resources on topics related to cyber and economic crime. Recent topics include Bitcoin® and other cryptocurrencies and intellectual property theft, with a focus on counterfeit goods.

Need-to-know information on emerging apps and other cyber investigative trends.
PUBLICATIONS

Download these informative products from the NW3C website:

- **Cyber Alerts**: General and investigative information on new and emerging apps, gaming platforms, and online communities that pose a specific threat and/or are of investigative interest to law enforcement.

- **White Papers**: In an effort to provide information about trends related to white collar crime, NW3C periodically produces briefs and white papers for general and law enforcement audiences.

INTELLECTUAL PROPERTY (IP) WEBSITE

The purpose of this site is to provide a common place for Intellectual Property Enforcement Program (IPEP) Grantees and Law Enforcement to find training, resources, and technical assistance that will aid in their intellectual property theft investigations. This site also contains legal resources for prosecutors and judges and citizen resources for the general public.

This site is managed by the National White Collar Crime Center (NW3C) and funded by the Bureau of Justice Assistance (BJA).

For more information, visit: www.iptheft.org

CYBER S.W.A.T.

Cyber S.W.A.T.™ is an innovative program that helps teens learn to navigate their online communities safely by pairing School Resource Officers with a team of Cyber S.W.A.T. peer mentors. Ten schools are participating in the Cyber S.W.A.T. program during the 2019-2020 school year. Cyber S.W.A.T. was developed through a collaboration with The Safe Surfin’ Foundation and NW3C.

For more information about bringing Cyber S.W.A.T to your school, visit www.teamcyberswat.org.
The Law Enforcement Cyber Center (LECC) is an online toolkit designed to meet the specific and practical needs of chiefs, investigators, line officers, digital forensic examiners, technical support staff, and other practitioners. LECC enhances the awareness, expands the education, and builds the capacity of justice and public safety professionals towards the global goal of combating high-tech crimes.

Under the direction to the Bureau of Justice Assistance, NW3C works in close collaboration with the International Association of Chiefs of Police (IACP) and the Police Executive Research Forum (PERF) to manage and support the LECC.

Those visiting the LECC can:

- Find model policies, guides, and white papers to help agencies detect, prevent, and investigate high-tech crime.
- Search upcoming online and in-person training courses, conferences, and other events in a single database.
- See a curated news feed of the ever-evolving world of technology and digital evidence.

For more information, visit: iacpcybercenter.org
NW3C UTILITY SUITE

The NW3C Utility Suite™ is a collection of software products that are distributed free of charge to law enforcement. The included utilities and their descriptions are listed below.

USN Journal Converter:

Convert the output from either “Fsutil” or “USNDump” into a standard spreadsheet format for easier analysis.

Recycle Bin Parser:

Quickly analyze the metadata and files found within the Windows® Recycle Bin.

Quick Hashing Utility:

Quickly hash a file, a string, or hex values. The supported hash algorithms are: MD5, SHA1, SHA256, SHA384, SHA512, REPMD160, CRC32 (Hex), and CRC32((Decimal)

Batch Hashing Utility:

Quickly hash the contents of a directory (selected directories can also be processed recursively). Once processed, the hashed values can be saved to a spreadsheet for later analysis. The supported hash algorithms are: MD5, SHA1, SHA256, SHA384, SHA512, RIPEMD, CRC32 (Hex), and CRC32 (Decimal).

Hex Viewer:

View a file in a standard hexadecimal/ASCII format, search for specific values, and copy/paste any hexadecimal or ASCII value(s).

Date/Time Utility:

Quickly convert between various date/time formats: Standard date/time format, Unix, Mac® Absolute Time, Windows® File Time, HFS+File Time, PRTime, Webkit, and more. Convert custom date/time formats by entering a custom epoch value.
PERPHOUND

PerpHound™ aids in the processing and plotting of call detail records, and allows the user to view and plot images and their associated EXIF information.

PHOTOHUNTER

PhotoHunter™ allows the user to view and plot images and their associated EXIF information.

REPORT GENERATOR

Report Generator™ allows the user to generate an HTML-based report from separate data files.