NW3C provides a nationwide support system for law enforcement and regulatory agencies tasked with the prevention, investigation, and prosecution of economic and high-tech crime. For over 40 years, NW3C’s comprehensive training and technical assistance programs have helped law enforcement professionals master the principles, concepts, and skills they need to fight these and related crimes.

NW3C’s work is funded primarily by grants through congressional appropriations from the Bureau of Justice Assistance (BJA) and other federal agencies. NW3C’s BJA-supported training is available to state, local, tribal, and territorial law enforcement personnel.
Phone  877-628-7674

Email  training@nw3c.org or onlinelearning@nw3c.org

Web  www.nw3c.org

Facebook  NationalWhiteCollarCrimeCenter

NW3C Offices
Wilton Park West
4905 Dickens Road
Suite 106
Richmond, VA 23230

5000 NASA Blvd.
Suite 2400
Fairmont, WV 26554
In the last five years, NW3C has trained more than 67,000 students in all 50 states. Our in-person training features student-centered, hands-on practical exercises.

Every year, NW3C provides hundreds of hours of technical assistance to law enforcement agencies investigating economic and high-tech crimes.

Since 2014, NW3C has made high-quality training available around the clock via a robust in-house online learning platform that reaches thousands of students every month.

NW3C’s webinars are a convenient way to learn more about new and emerging topics related to the investigation and prosecution of high-tech and economic crime.

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

NW3C reaches out to prosecutors and judges with specialized training to ensure that cases involving economic and high-tech crimes are handled effectively and treated fairly in the courtroom.

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.
## In-person courses

<table>
<thead>
<tr>
<th>Code</th>
<th>Course Code</th>
<th>Course Description</th>
<th>Credits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CI101</td>
<td>BCI-DF</td>
<td>Basic Cyber Investigations: Digital Footprints</td>
<td>6</td>
</tr>
<tr>
<td>CI102</td>
<td>BCI-DW/OSINT</td>
<td>Basic Cyber Investigations: Dark Web &amp; Open Source Intelligence</td>
<td>6</td>
</tr>
<tr>
<td>CI130</td>
<td>BCI-CRA</td>
<td>Basic Cyber Investigations: Cellular Records Analysis</td>
<td>6</td>
</tr>
<tr>
<td>CI240</td>
<td>ICI-VC</td>
<td>Intermediate Cyber Investigations: Virtual Currency</td>
<td>7</td>
</tr>
<tr>
<td>DF100</td>
<td>BDFA-Seizure</td>
<td>Basic Digital Forensic Analysis: Seizure</td>
<td>7</td>
</tr>
<tr>
<td>DF102</td>
<td>BDFA-Previewing</td>
<td>Basic Digital Forensic Analysis: Previewing</td>
<td>7</td>
</tr>
<tr>
<td>DF103</td>
<td>BDFA-Acquisition</td>
<td>Basic Digital Forensic Analysis: Acquisition</td>
<td>8</td>
</tr>
<tr>
<td>DF201</td>
<td>IDFA-AFT</td>
<td>Intermediate Digital Forensic Analysis: Automated Forensic Tools</td>
<td>8</td>
</tr>
<tr>
<td>DF310</td>
<td>ADFA-Win</td>
<td>Advanced Digital Forensic Analysis: Windows</td>
<td>8</td>
</tr>
<tr>
<td>DF320</td>
<td>ADFA-Mac</td>
<td>Advanced Digital Forensic Analysis: macOS</td>
<td>9</td>
</tr>
<tr>
<td>DF330</td>
<td>ADFA-Mobile I</td>
<td>Advanced Digital Forensic Analysis: iOS &amp; Android</td>
<td>9</td>
</tr>
<tr>
<td>DF340</td>
<td>ADFA-Mobile II</td>
<td>Advanced Digital Forensic Analysis: Advanced Mobile Acquisition</td>
<td>9</td>
</tr>
<tr>
<td>FTSeries</td>
<td></td>
<td>Digital Forensics Fast Track</td>
<td>10</td>
</tr>
<tr>
<td>FC101</td>
<td>FIPS</td>
<td>Financial Investigations Practical Skills</td>
<td>10</td>
</tr>
<tr>
<td>FC102</td>
<td>FIT</td>
<td>Financial Investigations Triage</td>
<td>10</td>
</tr>
<tr>
<td>FC105</td>
<td>FREA</td>
<td>Financial Records Examination &amp; Analysis</td>
<td>11</td>
</tr>
<tr>
<td>FC110</td>
<td>FCAS</td>
<td>Financial Crimes Against Seniors</td>
<td>11</td>
</tr>
<tr>
<td>FC111</td>
<td>FCSS</td>
<td>Financial Crimes Against Seniors Seminar</td>
<td>11</td>
</tr>
<tr>
<td>FC122</td>
<td>IPTT</td>
<td>Intellectual Property Theft Training</td>
<td>12</td>
</tr>
<tr>
<td>FC201</td>
<td>FRIS</td>
<td>Financial Records Investigative Skills</td>
<td>12</td>
</tr>
<tr>
<td>IA101</td>
<td>FIAT</td>
<td>Foundations of Intelligence Analysis Training</td>
<td>12</td>
</tr>
<tr>
<td>IA105</td>
<td>IWAB</td>
<td>Intelligence Writing &amp; Briefing</td>
<td>13</td>
</tr>
<tr>
<td>ID</td>
<td>Course</td>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>------</td>
<td>--------------</td>
<td>------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>CI091</td>
<td>ITP-WB</td>
<td>Introduction to Previewing</td>
<td>13</td>
</tr>
<tr>
<td>CI099</td>
<td>BCS-WB</td>
<td>Basic Computer Skills for Law Enforcement</td>
<td>13</td>
</tr>
<tr>
<td>CI100</td>
<td>ISEE-WB</td>
<td>Identifying &amp; Seizing Electronic Evidence</td>
<td>14</td>
</tr>
<tr>
<td>CI101</td>
<td>UDF-WB</td>
<td>Understanding Digital Footprints</td>
<td>14</td>
</tr>
<tr>
<td>CI103</td>
<td>ICPI-WB</td>
<td>Introduction to Cell Phone Investigations</td>
<td>14</td>
</tr>
<tr>
<td>CI104</td>
<td>VC-WB</td>
<td>Virtual Currency</td>
<td>15</td>
</tr>
<tr>
<td>CI106</td>
<td>AI-WB</td>
<td>Apple Introduction</td>
<td>15</td>
</tr>
<tr>
<td>CI110</td>
<td>Dark-WB</td>
<td>The Dark Web</td>
<td>15</td>
</tr>
<tr>
<td>CI131</td>
<td>SMB-WB</td>
<td>Social Media Basics</td>
<td>16</td>
</tr>
<tr>
<td>CI151</td>
<td>LC1-WB</td>
<td>First Responders &amp; Digital Evidence</td>
<td>16</td>
</tr>
<tr>
<td>CI152</td>
<td>LC2-WB</td>
<td>Search Warrants &amp; Digital Evidence</td>
<td>16</td>
</tr>
<tr>
<td>CI153</td>
<td>LC3-WB</td>
<td>Searching Without a Warrant</td>
<td>17</td>
</tr>
<tr>
<td>CI155</td>
<td>LC5-WB</td>
<td>Online Undercover</td>
<td>17</td>
</tr>
<tr>
<td>CI156</td>
<td>LC6-WB</td>
<td>Post-Seizure Evidentiary Concerns</td>
<td>17</td>
</tr>
<tr>
<td>CI157</td>
<td>LC7-WB</td>
<td>Mobile Digital Devices &amp; GPS</td>
<td>18</td>
</tr>
<tr>
<td>CI210</td>
<td>GCSI-WB</td>
<td>GPS Interrogation</td>
<td>18</td>
</tr>
<tr>
<td>CS100</td>
<td>ICN-WB</td>
<td>Introduction to Computer Networks</td>
<td>18</td>
</tr>
<tr>
<td>DF091</td>
<td>ENC2-WB</td>
<td>Encryption</td>
<td>19</td>
</tr>
<tr>
<td>DF099</td>
<td>HDS-WB</td>
<td>How Computers Work &amp; Store Data</td>
<td>19</td>
</tr>
<tr>
<td>DF100</td>
<td>BDFA-Seizure-WB</td>
<td>Basic Digital Forensic Analysis: Seizure</td>
<td>19</td>
</tr>
<tr>
<td>FC100</td>
<td>WCC-WB</td>
<td>Overview of White Collar Crime</td>
<td>20</td>
</tr>
<tr>
<td>FC115</td>
<td>MORF-WB</td>
<td>Introduction to Mortgage Fraud</td>
<td>20</td>
</tr>
<tr>
<td>Code</td>
<td>Title</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------------------------------------------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>FC123</td>
<td>Intellectual Property Theft: Time to Make a Difference</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>FC141</td>
<td>Human Trafficking Awareness for Law Enforcement Officers</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>FC142</td>
<td>Human Trafficking Awareness for West Virginia</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>FC151</td>
<td>Law Enforcement Officers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FC151</td>
<td>The Bank Secrecy Act: What Law Enforcement Needs to Know</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>PT110</td>
<td>Prosecuting the Dark Web</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>PT152</td>
<td>Search Warrants &amp; Digital Evidence</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>PT153</td>
<td>Searching Without a Warrant</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>PT160</td>
<td>Legal Challenges to Criminal Investigations</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>PT201</td>
<td>Digital Evidence Basics &amp; the CLOUD Act</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>PT230</td>
<td>Mobile Forensics for Prosecutors</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>PIRF-WB</td>
<td>Prosecuting Insurance Fraud Resource</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Training Presentations for Judges</td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>

### Prosecutors and judges

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>PT110</td>
<td>Prosecuting the Dark Web</td>
<td>22</td>
</tr>
<tr>
<td>PT152</td>
<td>Search Warrants &amp; Digital Evidence</td>
<td>22</td>
</tr>
<tr>
<td>PT153</td>
<td>Searching Without a Warrant</td>
<td>22</td>
</tr>
<tr>
<td>PT160</td>
<td>Legal Challenges to Criminal Investigations</td>
<td>23</td>
</tr>
<tr>
<td>PT201</td>
<td>Digital Evidence Basics &amp; the CLOUD Act</td>
<td>23</td>
</tr>
<tr>
<td>PT230</td>
<td>Mobile Forensics for Prosecutors</td>
<td>23</td>
</tr>
<tr>
<td>PIRF-WB</td>
<td>Prosecuting Insurance Fraud Resource</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>Training Presentations for Judges</td>
<td>24</td>
</tr>
</tbody>
</table>

### Tools and resources

<table>
<thead>
<tr>
<th>Code</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Webinars</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Mobile-friendly Products</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Multimedia</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Publications</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Law Enforcement Cyber Center</td>
<td>26</td>
</tr>
<tr>
<td></td>
<td>Forensic Tools</td>
<td>27</td>
</tr>
</tbody>
</table>
CI101  BCI-DF  
**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 social media, and the consequences of oversharing personal information; as well as steps to take after becoming a target of doxing.

CI102  BCI-DW/OSINT  
**Basic Cyber Investigations:  Dark Web & Open Source Intelligence**

This course provides expert guidance in the skills law enforcement officers need to conduct successful online investigations. Topics include IP addresses and domains, an overview of currently popular social media platforms, best practices for building an online undercover profile, foundational knowledge related to the dark web, and the use of the dark web as an investigative tool. Instructors demonstrate both open-source and commercially-available investigative tools for social engineering, information gathering, and artifacts related to social media; as well as automated utilities to capture information and crawl websites.

CI130  BCI-CRA  
**Basic Cyber Investigations:  Cellular Records Analysis**

This course is for officers, investigators, and analysts who encounter cell phone evidence that includes information external to the phone. Class concepts include instruction on how to request, read, and analyze call detail records from cellular providers; and how to plot cellular site locations to determine the approximate position of a suspect during a given period. No special hardware or software is required. However, this course focuses heavily on analysis; as such, a strong working knowledge of Microsoft Excel is highly recommended. Students are provided with a free copy of NW3C’s PerpHound™ tool, which assists in the plotting of call detail record locations.
DF102  B DFA Previewing
Basic Digital Forensic Analysis: Previewing

This course provides the fundamental knowledge and skills necessary to preview the most commonly-encountered forms of digital evidence. The course covers Windows-based and macOS-based computers, mobile devices, and removable storage media. In a combination of lecture, discussion, and practical exercises; instructors introduce the previewing process, legal considerations, live previewing, and dead-box previewing. Students gain hands-on experience with free and commercial third-party previewing tools that are in current use by practitioners in the field.

DF100  B DFA 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. Topics include recognizing potential sources of digital evidence; planning and executing a digital evidence-based seizure; and the preservation, packaging, documentation, and transfer of digital evidence.

CI240  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 like 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.
DF103 ADFA-Win
Advanced Digital Forensic Analysis: Windows

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 the various artifacts found in each of the Registry hive files. Students also examine Event Logs, Volume Shadow Copies, link files, and thumbnails. This course uses a mixture of lecture, discussion, demonstration, and hands-on exercises.
DF320 ADFA-Mac
Advanced Digital Forensic Analysis: macOS

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.

DF330 ADFA-Mobile I
Advanced Digital Forensic Analysis: iOS & Android

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.

DF340 ADFA-Mobile II
Advanced Digital Forensic Analysis: Advanced Mobile Acquisition

This course equips digital forensics professionals with the skills, utilities, and methods necessary to acquire data from otherwise-inaccessible devices. Students learn the advanced acquisition hierarchy and when to elevate the method of acquisition—from advanced custom recovery usage to bypass passcodes, to device encryption and other security measures, and ultimately to the acquisition of a physical forensic backup of the device. Hands-on instruction and practice includes EDL methods, jailbreaking, soft rooting, hard rooting, custom recovery usage, and exploit porting; concluding with a capstone analysis block on proper methods for handling acquired data.
FT-Series

Digital Forensics Fast Track

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 3 to 6 weeks, allowing the students time to apply what they have learned before returning for more advanced training. The classes build upon each other, and earlier classes in the fast track serve as prerequisites for later classes.

FC101 FIPS

Financial Investigations Practical Skills

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.

FC102 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, red flags in financial cases, money laundering, investigative strategies for different types of financial crimes, visual aids, and commingled funds.
FC105  FREA
Financial Records Examination & 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.

FC110  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.

FC111  FCSS
Financial Crimes Against Seniors Seminar
This 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.
IA101  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, Law Enforcement Intelligence Unit (LEIU), the International Association of Law Enforcement Intelligence Analysis (IALEIA), and the Regional Information Sharing System (RISS).

This course has been certified by DHS/FEMA as course number WV-001-PREV.
IA105  IWAB

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

CI091  ITP-WB

Introduction to Previewing
This interactive online module provides an overview of the basic concepts behind secure previewing of digital devices. 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”).

This course serves as a prerequisite for BDFA-Previewing but can also be completed as a stand-alone course.

CI099  BCS-WB

Basic Computer Skills for Law Enforcement
This course covers the fundamental skills involved with operating a computer using the Windows 7 or Windows 8 operating systems. Topics include components of computer hardware, Windows File Explorer, file management in Windows, and program installation.

The course consists of six sequential instructional modules. After completing each module, students should proceed to the next.
CI100 ISEE-WB
**Identifying & Seizing Electronic Evidence**
This course introduces the information and techniques law enforcement personnel need to safely and methodically collect and preserve electronic evidence at a crime scene. Topics include recognizing potential sources of electronic evidence; planning and executing a digital evidence-based seizure; and the preservation, packaging, documentation, and transfer of digital evidence.

CI100 (ISEE-WB) is a Department of Homeland Security Approved Course.

CI101 UDF-WB
**Understanding 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 social media, and the consequences of oversharing personal information; as well as steps to take after becoming a target of doxing.

CI103 ICPI-WB
**Introduction to Cell Phone Investigations**
This 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, as well as 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.
CI104 VC-WB Virtual Currency
This 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.

CI106 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.

This course serves as a prerequisite for ADFA-Mac but can also be completed as a stand-alone course.

CI110 Dark-WB The Dark Web
This course introduces the dark web and some of the most popular darknets, including the Tor Project, Freenet, and Invisible Internet Project (I2P). Basic topics include what Tor is, how it works, and who uses it; as well as dark markets within Tor, and the hidden services they provide. The course concludes with brief case studies covering some of the largest dark market seizures in history.
CI131 SMB-WB
Social Media Basics

This course introduces learners to the world of social media, including fundamental concepts, trends, and benefits for law enforcement organizations. This course examines how the most popular social media platforms like Facebook and Instagram work, and how people tend to use them. This course also introduces other social media platforms and apps, such as Snapchat and Periscope. There is a strong focus on social media as a tool for law enforcement, including designating a social media officer and establishing an agency social media policy for official and personal use.

CI151 LC1-WB
First Responders & Digital Evidence

This 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.

CI152 LC2-WB
Search Warrants & Digital Evidence

This 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.
CI153 LC3-WB
Searching Without a Warrant

This 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.

CI155 LC5-WB
Online Undercover

This 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.

CI156 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 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.
This 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.
DF091  ENCT2-WB  Encryption

This course provides an introduction to data encryption, covering the purpose of encryption as well as the process of encrypting data, and 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. The course also provides an overview of some of the best and most common encryption detection software tools. This course serves as a prerequisite for several classroom courses and can also be completed as a stand-alone course.

DF099  HDS-WB  How Computers Work & Store Data

The first module of this 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 hard drive functions.

This course serves as a prerequisite for BDFA-Acquisition but can also be completed as a stand-alone course.

DF100  BDFA-Seizure-WB  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. Topics include recognizing potential sources of digital evidence; planning and executing a digital evidence-based seizure; and the preservation, packaging, documentation, and transfer of digital evidence.

Coming soon
FC123  IPT-WB

**Intellectual Property Theft: Time to Make a Difference**

This 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.

FC115  MORF-WB

**Introduction to Mortgage Fraud**

This 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.

FC100  WCC-WB

**Overview of White Collar Crime**

This 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.
FC141 HTA-WB
Human Trafficking Awareness for Law Enforcement Officers

This course provides law enforcement personnel with an overview of the various elements involved in the crime of human trafficking, with a focus on the situation in West Virginia. The course covers West Virginia’s human trafficking law, the major types of human trafficking, the scope and extent of human trafficking, and 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. This course is approved for 1 hour of annual in-service training for West Virginia Law Enforcement.

FC142 HTAWV-WB
Human Trafficking Awareness for West Virginia Law Enforcement Officers

This course provides law enforcement personnel with an overview of the various elements involved in the crime of human trafficking, with a focus on the situation in West Virginia. The course covers West Virginia’s human trafficking law, the major types of human trafficking, the scope and extent of human trafficking, and 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. This course is approved for 1 hour of annual in-service training for West Virginia Law Enforcement.

FC151 BSA-WB
The Bank Secrecy Act: What Law Enforcement Needs to Know

This 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.
PT110 PDW-WB
Prosecuting the Dark Web
This 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 other popular darknets, 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.

PT152 PT2-WB
Search Warrants & Digital Evidence
This 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.

PT153 PT3-WB
Searching Without a Warrant
This 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.
PT160 LCCI-WB
Legal Challenges to Criminal Investigations

This course provides information regarding the legal principles involving the rights of defendants and witnesses. This course will cover a number of 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.

PT201 DEB
Digital Evidence Basics & the CLOUD Act

This course provides the technical and legal information prosecutors need to see cases involving digital evidence through the entire criminal justice process, from seizure and extraction to admissibility to 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.

PT230 MFP
Mobile Forensics 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.
Prosecuting Insurance Fraud Resource

This resource provides information about investigating and prosecuting insurance crime in the Property and Casualty (P&C) arena. P&C insurance crime involves auto, homeowners’, and commercial policies; and spans a wide range of property- and medically-related fraud. This resource includes examples of insurance fraud; indicators and red flags of fraud; investigative guides and aids; and contact information for regional, state, and local resources for investigators and prosecutors.

This resource is presented in partnership with the National Insurance Crime Bureau.

Training Presentations for Judges

Prosecutors and defense attorneys know that almost every criminal investigation today involves some digital evidence—or the potential for it. This means that in order to fairly adjudicate today’s cases, judges in all jurisdictions must be up to speed on the latest technological developments and case law. NW3C reaches out to judges via 90-minute presentations that can be delivered at professional conferences, as stand-alone lectures, or in a webinar format.
Webinars
NW3C’s webinars are a convenient way to learn more about new and emerging topics related to the investigation and prosecution of high-tech and economic crime. With live and on-demand webinars, criminal justice professionals can gain 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.

Multimedia
Stay up-to-date with streaming audio and video.

Cyber Shorts | Need-to-know information on emerging topics, presented in engaging videos suitable for agency roll call.

Podcasts | Law enforcement-specific commentary and advice from experts on topics relating to the investigation and prosecution of white collar crime, with a special focus on intellectual property theft.
Publications

Download these informative products from NW3C’s 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.

Law Enforcement Cyber Center

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 of 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.

- Model policies, guides, and white papers to help your agency detect, prevent, and investigate high-tech crime.
- Search for upcoming online and in-person training classes, conferences, and other events in a single database.
- A curated news feed on the ever-evolving world of technology and digital evidence.
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.

Current version: v1.0.2

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, RIPEMD160, 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, RIPEMD160, 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.

SQLite Extraction Utility:
Export the data stored within a SQLite table to a spreadsheet.
**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.
*Current version: v4.0.3*

**PhotoHunter**
PhotoHunter allows the user to view and plot images and their associated EXIF information.
*Current version: v1.0.3*

**Report Generator**
Report Generator allows the user to generate an HTML-based report from separate data files.
*Current version: v2.0.1*
NW3C’s BJA-supported training is available to state, local, tribal, and territorial law enforcement personnel.

www.nw3c.org

887-628-7674

training@nw3c.org

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.

© 2018. NW3C, Inc. d/b/a the National White Collar Crime Center. All rights reserved.