PRODUCTS & SERVICES GUIDE

NW3C offers a variety of products that prepare criminal justice personnel to successfully investigate and prosecute cases related to high-tech and economic crime.

CLASSROOM TRAINING
LIVE ONLINE TRAINING
ONLINE TRAINING
WEBINARS
TECHNICAL ASSISTANCE
INVESTIGATIVE TOOLS
RESOURCES

year / 2023 / nw3c / products

Version 2.0 | Updated January 2023

IN PERSON CLASSROOM

In the last five years, NW3C has trained nearly 25,000 students in all 50 states. In-person training features student-centered, hands-on practical exercises.

VIRTUAL CLASSROOM

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.

SELF PACED

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 125,000 students.

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.

TECHNICAL ASSISTANCE

NW3C provides technical assistance to law enforcement and regulatory agencies in the areas of Cybercrime, Financial Crime, Intelligence Analysis, and Intellectual Property Theft. Technical assistance examples include guidance on analyzing financial records, handling electronic evidence (smartphones, computers, etc.), and identifying counterfeit goods.

TOOLS AND RESOURCES

NW3C offers a variety of resources that will assist law enforcement officers and prosecutors in the investigation and prosecution of cyber and financial crime.

PROSECUTORS AND JUDGES

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. 15PBJA-21-GK-02799-ECON 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 CLASSROOM AND VIRTUAL CLASSROOM COURSES

SELF PACED COURSES

TOOLS & RESOURCES

CI 101
CYBER INVESTIGATIONS

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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 online social media, and the consequences of oversharing personal information, along with steps to take after becoming a target of doxing or identity theft/ fraud.

IADLEST Certified This course has been certified by IADLEST as part of the National Certification Program.

CI 102
CYBER INVESTIGATIONS

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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

2 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

BCI-ADID

BASIC CYBER INVESTIGATIONS: ADVERTISING IDENTIFIERS

This course was designed for law enforcement investigators, examiners, and analysts in situations where device location information may be important. Class concepts include exploring user attributes, advertising identifiers in detail, important legal considerations and processes, overall investigative processes, and tools available to law enforcement. Students will use a commercially available investigative tool for querying an advertising identifier data set and displaying signal locations.

CI 130
CYBER INVESTIGATIONS

Quick Info

2 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

CI 140
CYBER INVESTIGATIONS

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

MCIU

MANAGING A CYBERCRIME UNIT

The Managing a Cybercrime Investigation Unit curriculum provides students with information they need to collaboratively create and manage a functional and successful cybercrime unit within their jurisdiction. This course offers information on how to establish a unit, how to staff your unit, how to create and maintain a budget that works for your unit, and offers insight on the forensic process and laboratory workflows.

CI 240
CYBER INVESTIGATIONS

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

ICI-VC

INTERMEDIATE CYBER INVESTIGATIONS: VIRTUAL CURRENCY

This course provides students with the fundamental knowledge they need to investigate crimes involving virtual currency. Instructors explain foundational concepts like the characteristics of money, virtual currency, and cryptocurrency. Blockchain technology, proof of work, and proof of stake are covered and students learn how industry-leading cryptocurrencies (Bitcoin®, Ethereum®, and Monero) work. Finally, students learn investigative techniques for tracking and documenting transactions, and best practices for seizing and securing cryptocurrency. Hands-on exercises include: opening a bitcoin wallet, bitcoin transactions, investigating the blockchain, and identifying services using free/open-source explorers.

DF 100
DIGITAL FORENSICS

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program

DF 101
DIGITAL FORENSICS

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

BDFA-WIN-ACQ

BASIC DIGITAL FORENSIC ANALYSIS: WINDOWS AQUISITION

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 topics on 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.

DF 201
DIGITAL FORENSICS

Quick Info

4 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

DF 202
DIGITAL FORENSICS

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

IDFA-WIN-FS

INTERMEDIATE DIGITAL FORENSIC ANALYSIS: WINDOWS FILE SYSTEM

This course teaches students to prepare and store a digital storage device using the three main Windows® operating system file formats. These operating systems include FAT32, exFAT, and NTFS. Students will explore the layouts and steps for partitioning a hard drive and how partitioning and formatting prepares the drive for storage of data. In addition, the steps that occur when a file is saved in each of the formats will be explored in detail. Students will hand recover data files that have been deleted by reversing the process of deletion. This course covers the Recycle Bin of the current NTFS in Windows®.

DF 205
DIGITAL FORENSICS

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

DF 310
DIGITAL FORENSICS

Quick Info

4 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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 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.

DF 320
DIGITAL FORENSICS

Quick Info

4 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

ADFA-Mac

ADVANCED DIGITAL FORENSIC ANALYSIS: macOS

This course teaches students to identify various artifacts typically located in property lists and SQLite databases on macOS®-based computers. It also teaches students how to perform forensic analysis. Key concepts covered in this course include processing basics, SQLite databases, SQLite queries, and native system-related artifacts. Students will use hands-on practical experience writing basic SQLite queries and learn to analyze operating system artifacts. The forensic artifacts covered in this course include user login passwords, FaceTime®, messages, mail, contacts, calendars, reminders, notes, photos, Safari®, Google Chrome™, and Mozilla Firefox®.

DF 330
DIGITAL FORENSICS

Quick Info

4 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

FC 099
FINANCIAL CRIME

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

BLSS

BASIC LEVEL SPREADSHEETING SKILLS

This course provides foundational spreadsheeting knowledge and skills by combining live demonstrations and hands-on exercises using Microsoft® Excel. The class is designed for learners who are brand new to spreadsheeting or need a refresher. Topics include an overview of the user interface, formatting, freeze panes, autofill, worksheet headers, print headers, and footers. The course also introduces filtering, sorting, conditional formatting, sparklines, base-level charting, and writing a basic formula.

FC 101
FINANCIAL CRIME

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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. This includes 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.

FC 102
FINANCIAL CRIME

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

TTFI

TOOLS AND TECHNIQUES FOR FINANCIAL INVESTIGATIONS

This course provides a basic overview of emerging issues in financial crime. Students learn to ask critical questions, gather documentation, and analyze information for leads at the onset of a financial crime investigation. Topics include working with financial records (both individual and business), money laundering, and tools to use during an investigation.

FC 105
FINANCIAL CRIME

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

FC 110
FINANCIAL CRIME

Quick Info

2 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

FC 111
FINANCIAL CRIME

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

FC 120
FINANCIAL CRIME

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

RTEF

RESPONDING TO TRANSNATIONAL ELDER FRAUD

This course provides law enforcement with an introduction to collaboratively assisting older adult victims of transnational elder fraud. Students will be provided with background information on transnational elder fraud and common scams used by perpetrators of transnational elder fraud. Students will learn tips for interviewing older adults and how to respond to victims using trauma informed techniques. Additionally, students will learn to navigate resources designed for victims of transnational elder fraud so that they can better serve their communities as well as resources designed for law enforcement that can lead to more successful investigations.

FC 122

FINANCIAL CRIME

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

FC 130

FINANCIAL CRIME

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

TIF

TARGETING INVESTMENT FRAUD

This course provides investigators and prosecutors with the knowledge and tools they need to respond to the growing problem of investment fraud. Topics include what constitutes a security, using the Howey Test to determine if a particular offering is a security, identifying investment fraud schemes, and investigative strategies for working with victims and perpetrators. The course also covers fraud prevention strategies, and students are provided with additional resources for both prevention and investigation.

FC 200

FINANCIAL CRIME

Quick Info

2 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

ILSS

INTERMEDIATE LEVEL SPREADSHEETING SKILLS: ASSESSING AND ORGANIZING DATA

This intermediate spreadsheeting course uses Microsoft® Excel to assess and organize data in an electronic format. The class is designed for learners who have experience using Excel and who want to increase their spreadsheeting knowledge and skills. Topics include text functions, absolute referencing, date and time functions, flash fill, handling formula errors, VLOOKUP, dynamic arrays, and data validation. The course combines live demonstrations, instructor-led exercises, and independent student exercises.

FC 201
FINANCIAL CRIME

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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, 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.

FC 203
FINANCIAL CRIME

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

FIBB

FINANCIAL INVESTIGATIONS: BEYOND THE BASICS

This course covers the fundamentals of financial investigations and incorporates some of the more advanced processes that elevate an investigation. Students will learn investigative processes, practical tools, and sources of information necessary to plan and conduct financial investigations. It provides a description of the basic composition of elements within illicit financial networks and how they work to compromise legitimate business and financial sectors. Material will describe government, regulatory, and investigative actions within the United States, and by international partners to detect and investigate illicit actors and networks. This course includes considerations for investigation planning and promotion of creative thinking.

FC 204
FINANCIAL CRIME

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

CTCTF

COMBATING TRANSNATIONAL CRIME & TERRORISM FINANCING

This course helps students develop an understanding of how financial systems are used to support terror activities and transnational criminal organizations. Students will work with tools and methods to investigate the manipulation of financial, communication, and business systems used for illicit purposes. Students will learn how to work with suspicious activity reports, crucial financial records, and records used in banking and money services businesses. They will also learn how to gather information and evidence on other means of value transfer methods associated with money laundering, the black-market peso and forms of trade-based money laundering, hawala and other alternate remittance systems, and virtual assets (cryptocurrency).

IA 101
INTELLIGENCE ANALYSIS

Quick Info

4 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

FIAT

FOUNDATIONS OF INTELLIGENCE ANALYSIS TRAINING

This course addresses the critical need for well-trained intelligence analysts to interpret growing amounts of information. It 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). It 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.

IA 102
INTELLIGENCE ANALYSIS

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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.

IA 103
INTELLIGENCE ANALYSIS

Quick Info

1 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

ISIA

INTRODUCTION TO STRATEGIC INTELLIGENCE ANALYSIS

This course introduces analysts to the historical context of strategic analysis through broader concepts of thinking and analyzing more strategic aspects. A key component of modern analytical investigations is the ability to collect and analyze multiple data sets and information sources to generate a holistic product. Introduction to Strategic Intelligence Analysis (ISIA) expands on the basic principles of strategic analysis explored in the Foundations of Intelligence Analysis Training (FIAT) while building a framework for real-world application and broader occupational contexts.

IA 105
INTELLIGENCE ANALYSIS

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

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).

IA 300
INTELLIGENCE ANALYSIS

Quick Info

3 DAY

IN PERSON CLASSROOM

VIRTUAL CLASSROOM

ACITA

ADVANCED CRIMINAL INTELLIGENCE: TRADECRAFT AND ANALYSIS

This course studies the fundamentals of data analysis and how to form arguments in support of criminal investigations and intelligence. Students will learn about data management techniques and a disciplined process to clean and standardize data in preparation for analysis. The course will explore common investigative objectives including the discovery of associations between people and entities, the correlation between unlawful activity and suspects, behavioral affinities, and predictions. It introduces the Enterprise Theory of Crime and the use of network analysis to formulate conclusions about the structure of criminal organizations, their players and roles, the identification of facilitators, charting of financial arrangements, and connections to unlawful activity.

PT 101
INTELLIGENCE ANALYSIS

Quick Info

1 DAY

VIRTUAL CLASSROOM

IN PERSON CLASSROOM

ICCP

INTRODUCTION TO CYBERCRIME UNITS FOR PROSECUTORS

Cybercrime and digital evidence affect almost every aspect of criminal prosecutions. This includes the mode of crime, investigation, grand jury, trial, and sentencing. A prosecutor's office needs to have an expert who possesses this unique knowledge to prosecute typical cybercrime cases and act as a point person for the office. The purpose of this course is to help students learn how to become that office expert. The course will provide the student with a solid base of knowledge for setting up and running a cybercrime unit, discuss best practices for the unit, and provide resources for reference. Regardless of the size of the unit, this course will provide the necessary tools for establishing its effectiveness.

CI 091
CYBER INVESTIGATIONS

Quick Info

1/2 HOUR

SELF PACED

ITP2-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).

IADLEST Certified This course has been certified by IADLEST as part of the National Certification Program.

CI 099
CYBER INVESTIGATIONS

Quick Info

11/2 HOUR

SELF PACED

IOT-WB

INTRODUCTION TO THE INTERNET OF THINGS

This course provides an overview of how the Internet of Things (IoT) and associated devices can help law enforcement with their investigations. It will familiarize learners with what IoT is, how it works, common devices, and how it can be leveraged for gathering evidence.

IADLEST Certified This course has been certified by IADLEST as part of the National Certification Program.

CI 101
CYBER INVESTIGATIONS

Quick Info

1/2 HOUR

SELF PACED

UDF2-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.

IADLEST Certified This course has been certified by IADLEST as part of the National Certification Program.

CI 103
CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF PACED

ICPI2-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.

IADLEST Certified This course has been certified by IADLEST as part of the National Certification Program.

CI 104
CYBER INVESTIGATIONS

Quick Info

1/2 HOUR

SELF PACED

VC2-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. The course describes different types of virtual currencies and covers the main differences between decentralized and centralized currencies. Focusing on Bitcoin® , students will learn what Bitcoin is, how it is stored, and what are some investigative tips for law enforcement.

IADLEST Certified This course has been certified by IADLEST as part of the National Certification Program.

CI 105
CYBER INVESTIGATIONS

Quick Info

2 HOUR

SELF PACED

PL-WB

PRESERVATION LETTERS: THEIR VITAL ROLE IN INVESTIGATIONS

With the rise of electronic evidence and the likelihood that the crimes you're investigating are conducted with or supported by the use of mobile devices, the Internet, or cloud-based applications, preservation letters provide a means to prevent the destruction of electronic records and buy an investigator time to retrieve and analyze potential evidence. This course focuses on the basics of preservation letters - what they are, their purpose, language to include, how to locate contact information, and how to submit them.

IADLEST Certified This course has been certified by IADLEST as part of the National Certification Program.

CI 106

CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF PACED

ITR-WB

RANSOMWARE: AN INTRODUCTION

According to the FBI's Internet Crime Complaint Center (IC3), ransomware attacks lead to several billion dollars lost each year. Law enforcement officers should know how to respond to and protect their agencies and communities from these attacks. This interactive module teaches participants how to recognize and respond to a ransomware attack and discusses how ransomware can affect devices and networks and how to prevent ransomware attacks.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

CI 107

CYBER INVESTIGATIONS

Quick Info

1 1/2 HOUR

SELF PACED

DISM-WB

DEEPFAKES: AN INTRODUCTION TO SYNTHETIC MEDIA

This course introduces learners to the colloquially used term deepfakes and the technology that makes this type of synthetic media possible. Deepfakes and artificial intelligence (AI) are increasingly used by cybercriminals to avoid biometric security, steal identities, and facilitate financial crime. This course covers how artificial intelligence is used to create deepfakes, common uses of synthetic media, and how to recognize deepfakes.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

CI 108

CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF PACED

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.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

CI 111
CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF PACED

DARK2-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.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

CI 131
CYBER INVESTIGATIONS

Quick Info

1 1/2 HOUR

SELF PACED

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. It identifies 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.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

CI 132
CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF PACED

ASET-WB

ADVANCED SEARCH ENGINE TECHNIQUES

This course focuses on practical online search techniques. Students will learn about using the advanced features of popular search engines, accessing cached versions of websites, searching with images, and common signs of fake and manipulated images. This course is part of the Open Source Intelligence Modules. It can be completed as a stand-alone course or in combination with the other courses.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

CI 133
CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF PACED

DWS-WB

DEEP WEB SEARCHING

This course covers a variety of tools and techniques to conduct deep web searches that go beyond common search engines like Google. The course highlights tools for discovering information about people and companies both domestically and internationally. It also includes tools for discovering and manipulating device information such as IP addresses. This course is part of the Open Source Intelligence Modules. It can be completed as a stand-alone course or in combination with the other courses.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

CI 134
CYBER INVESTIGATIONS

Quick Info

1 1/2 HOUR

SELF PACED

SMS-WB

SOCIAL MEDIA SEARCHING

This course focuses on gathering information from social media sites. Students will learn about popular social media platforms, tools that can help them discover information on social media, and ways to capture and save online media. This course is part of the Open Source Intelligence Modules. It can be completed as a stand-alone course or in combination with the other courses.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

CI 151
CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF PACED

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.

CI 152
CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF-PACED

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.

CI 155
CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF-PACED

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.

CI 156
CYBER INVESTIGATIONS

Quick Info

1 HOUR

SELF-PACED

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.

CI 157
CYBER INVESTIGATIONS

Quick Info

1/2 HOUR

SELF PACED

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.

CI 220
CYBER INVESTIGATIONS

Quick Info

1 1/2 HOUR

SELF PACED

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™.

CS 100
CYBER SECURITY

Quick Info

3 HOUR

SELF PACED

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.

CS 103

CYBER SECURITY

Quick Info

2 HOUR

SELF PACED

DT-WB

DIGITAL TRUST

Trust is an essential component for reducing friction between people, organizations, government, and other entities. When trust is high, people are more willing to cooperate, require less assurances for doing so, and are less skeptical of the outcomes. This course will provide an overview of factors that contribute to public trust in law enforcement's use of current and emerging digital technologies. It will analyze the benefits and risks associated with them, as well as the laws and ethics that should guide their use.

This course has been certified by IADLEST as part of the National Certification Program.

DF 091

DIGITAL FORENSICS

Quick Info

1 HOUR

SELF PACED

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.

This course has been certified by IADLEST as part of the National Certification Program.

DF 099

DIGITAL FORENSICS

Quick Info

3 HOUR

SELF PACED

HDS2-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.

This course has been certified by IADLEST as part of the National Certification Program.

DF 102
DIGITAL FORENSICS

Quick Info

8 HOUR

SELF PACED

ISDE-WB

IDENTIFYING AND SEIZING ELECTRONIC EVIDENCE

Identifying and Seizing Digital Evidence provides a comprehensive overview of the issues surrounding digital media in relation to criminal investigations. Topics covered in this training include preparing to respond to a digital crime scene, identifying potential sources of digital evidence, and properly collecting items of evidentiary value to be used in court proceedings. The roles of the first responder, investigator, digital forensic examiner, prosecutor, and defense counsel are differentiated and explored. Legal concerns in conducting a search for digital evidence are also addressed.

FC 100
FINANCIAL CRIME

Quick Info

2 HOUR

SELF PACED

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.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

FC 104
FINANCIAL CRIME

Quick Info

1 HOUR

SELF PACED

FIB-WB

FINANCIAL INVESTIGATIONS 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.

FC 106
FINANCIAL CRIME

Quick Info

2 HOUR

SELF PACED

RTEF-WB

RESPONDING TO TRANSNATIONAL ELDER FRAUD

This course provides law enforcement with an introduction to collaboratively assisting older adult victims of transnational elder fraud. Students will be provided with background information on transnational elder fraud and common scams used by perpetrators of transnational elder fraud. Students will learn tips for interviewing older adults and how to respond to victims using trauma-informed techniques. Additionally, students will learn to navigate resources designed for victims of transnational elder fraud so that they can better serve their communities as well as resources designed for law enforcement that can lead to more successful investigations.

FC 115
FINANCIAL CRIME

Quick Info

1 1/2 HOUR

SELF PACED

MORF2-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.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

FC 123
FINANCIAL CRIME

Quick Info

1 HOUR

SELF PACED

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.

FC 141
FINANCIAL CRIME

Quick Info

1 HOUR

SELF PACED

HTA2-WB

HUMAN TRAFFICKING AWARENESS FOR LAW ENFORCEMENT OFFICERS

This course, available in English and Spanish, provides law enforcement personnel with an overview of various elements involved in the crime of human trafficking. It covers the major types, scope, and extent of human trafficking. 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.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

FC 151
FINANCIAL CRIME

Quick Info

1 HOUR

SELF PACED

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.

FC 160
FINANCIAL CRIME

Quick Info

1 HOUR

SELF PACED

EAGLE2-WB

THE ELDER ABUSE GUIDE FOR LAW ENFORCEMENT

This course covers the main features of the free tool, Elder Abuse Guide for Law Enforcement (EAGLE), and introduces types of elder abuse. This course provides information on how to navigate through the EAGLE portal and how to identify EAGLE-provided aids for evidence and processing. Topics include an introductory understanding of elder abuse, financial abuse, physical abuse, and neglect.

IADLEST Certified

This course has been certified by IADLEST as part of the National Certification Program.

FC 175
FINANCIAL CRIME

Quick Info

2 HOUR

SELF PACED

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.

IA 100
INTELLIGENCE ANALYSIS

Quick Info

4 HOUR

SELF PACED

IIA-WB

INTRODUCTION TO INTELLIGENCE ANALYSIS

This interactive online training provides an overview of the basic concepts behind intelligence analysis. Topics covered in this 4-part training include the history of intelligence analysis and how it relates to the current environment, the purposes of intelligence analysis, the common models of intelligence analysis, and the necessary skills and personal traits for success in intelligence analysis. The course will also cover differences between intelligence and information., the law enforcement intelligence cycle, the target-centric approach, and the differences between the two.

PT 100
PROSECUTORS

Quick Info

1 HOUR

SELF PACED

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.

WI 100
WELLNESS

Quick Info

1 HOUR

SELF PACED

SRLE-WB

STRESS AND RESILIENCE IN LAW ENFORCEMENT

This course will provide insight and information on the topic of wellness and mental health, focusing on stress and resilience in everyday policing. At the conclusion of this course, you will understand how stress affects the brain, alters behaviors and feelings, and tools to build resilience. It is imperative that law enforcement officers understand that to take care of others you must take care of yourself first. Wellness and mental health training is not an option, but a requirement to ensure you can sustain a healthy career and personal life.

IADLEST Certified This course has been certified by IADLEST as part of the National Certification Program.

OC
OFFICER CYBERSAFETY

5-10 MINUTES

SELF PACED

OFFICER CYBERSAFETY TRAINING: SECURING APPS, BROWSERS, AND DEVICES

Law enforcement officers, other criminal justice practitioners, and their families are at high risk for doxing. It is important to ensure that apps, browsers, and devices are set in a way that minimizes the risk of compromise. Each Officer Cybersafety microlearning module takes no more than 10 minutes to complete. You can follow along with the step-by-step security instructions by having the app, browser, or device available during the training.

W

WEBINARS

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. NW3C webinars are typically offered a few times a week and range between 60 to 90 minutes in length. Each webinar ends with a Q&A session giving attendees the opportunity to interact and ask questions.

In addition to the many webinar topics, NW3C hosts Asked & Answered webinars. These webinars are structured as Q&A sessions and give participants the opportunity to ask a panel of experts questions on topics such as high-tech crime and intelligence analysis.

NW3C also partners with financial institutions, tool vendors, and subject matter experts in the field to provide webinars to law enforcement with the most current investigative techniques and tools.

A certificate of training is issued for both live and on-demand webinars for those viewing them in their entirety.

R
RESOURCES

TECHNICAL ASSISTANCE

NW3C provides technical assistance to law enforcement and regulatory agencies in the areas of Cybercrime, Financial Crime, Intelligence Analysis, and Intellectual Property Theft. Technical assistance examples include guidance on analyzing financial records, handling electronic evidence (smartphones, computers, etc.), and identifying counterfeit goods.

The technical assistance request is only intended to be used by U.S. Criminal Justice Practitioners. Requests submitted by the general public and others will not be processed.

R
RESOURCES

INVESTIGATIVE RESOURCES

NW3C offers a variety of resources that will assist law enforcement officers and prosecutors in the investigation and prosecution of cyber and financial crime. The investigative resources can be found on the NW3C website and includes law enforcement tools, legal templates, intellectual property theft resources, information security guides, law enforcement guides, and cryptocurrency resources. Access to these resources requires a web-user account for the NW3C website.

R
RESOURCES

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 NW3C and funded by the Bureau of Justice Assistance (BJA).

For more information, visit: www.iptheft.org

R
RESOURCES

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. 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.

CYBER SWAT

R
RESOURCES

TRAFFICK STOP

With support from the Office for Victims of Crime (OVC), Office of Justice Programs, U.S. Department of Justice, NW3C has developed the TraffickSTOP program—a human trafficking identification and prevention curriculum for high school students. NW3C has partnered with the International Association of Chiefs of Police and the National Association of School Resource Officers to develop a toolkit with curriculum, materials, and resources that will be implemented in select pilot schools during the 2021-2022 school year and additional schools in the 2022-2023 school year. Law enforcement representatives will be trained to deliver this curriculum in the selected schools.

For more information about bringing TRAFFICK STOP to your school, visit traffickingstop.org

TRAFFICK STOP

R

RESOURCES

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 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, REPEMD160, 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.

FT
FORENSIC TOOLS

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.

www.nw3c.org

VA

Corporate Headquarters

National White Collar Crime Center
4901 Dickens Road, Suite 110
Richmond, VA 23230

(804) 273-6932

WV

Training and Research Facility

National White Collar Crime Center
5000 NASA Blvd., Suite 2100
Fairmont, WV 26554

(304) 367-1994

training@nw3c.org