SUMURI + NW3C

TRAINING CATALOG

TRANSFORMING TRAINING INTO INVESTIGATION

TRAINING@SUMURI.COM

NW3C

Since 1978, NW3C has empowered criminal justice professionals worldwide by providing expert training and technical assistance focusing on economic and high-tech crime, criminal intelligence, and legal strategies.

SUMURI

SUMURI provides the forensic community with unique and relevant digital forensic solutions while adhering to their core values of honor, integrity, loyalty, positive attitude, dedication and most important above all – altruism.

COURSES FEATURE:

- Delivery in English with 7 hours of instruction per day
- Optional pre-tests and post-tests to measure learning
- One-on-one interaction between students and instructors
- We come to you virtually or in-person
- Certificates of completion jointly sealed by NW3C and SUMURI

VIRTUAL LAB: These courses include a virtual lab environment with interactive exercises for each student to complete.

MULTI-DAY OPTION: Some courses offer the option of an added delivery day to allow for a slower and more in-depth delivery of technical material.

COURSE PAIRINGS: These courses have recommendations on other topics that can be combined modularly to create a longer learning experience based on specific interests and missions.

ALL COURSES ARE TAUGHT BY IADLEST INTERNATIONALLY CERTIFIED INSTRUCTORS

IICI is the premier distinction for instructors providing training in the international arena

Table of Contents

CI 102

Virtual Lab

3 Days

32 Students Max

This course pairs well with:

DF100 Basic Digital Forensic Analysis: Seizure

CI240 Intermediate Cyber Investigations: Virtual Currency

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 online social media platforms, best practices for building an 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.

Key concepts covered in this course include:

- Internet basics
- Popular sites
- The dark web
- Tor

Student Testimonials

"This training has helped me conduct online research on crimes including murder, capital murder, sexual coercion, and other crimes." -Waco, Texas

"This class has been useful in locating suspect information and is a critical part of my daily investigative techniques." -Missoula, Montana

CI 202

Virtual Lab

3 or 4 Days

32 Students Max

This course pairs well with:

IA102 Introduction to Link Analysis

IA300 Advanced Criminal Intelligence: Tradecraft and Analysis

Intermediate Cyber Investigations: Online Open Source Investigations

This course equips participants with the knowledge and expertise essential for proficiently conducting online investigations. Participants will delve into the intricate world of open source information, mastering specialized techniques, tools, and methodologies crucial for uncovering digital evidence related to criminal activities. Participants will learn how to collect and document uncovered information, effectively manage cases, and validate data.

Key concepts covered in this course include:

- Exploring social media platforms
- Preparing, collecting, and validating open source information
- Online investigation fundamentals

Student Testimonials

"Enrolling in this course has been a transformative experience in my journey as an investigator. With a primary focus on combating Child Sexual Abuse Material (CSAM), this course provides a comprehensive understanding of the intricacies involved in conducting online investigations."
-Anonymous

CI 203

Virtual Lab

2 or 3 Days

32 Students Max

This course pairs well with:

CI202 Intermediate Cyber Investigations: Online Open Source Investigations

CI240 Intermediate Cyber Investigations: Virtual Currency

Intermediate Cyber Investigations: Dark Web Investigations

This course will provide the skills necessary for criminal justice professionals to conduct online investigations using darknets including Tor, Tails, Freenet, and I2P. Topics will include operational security for conducting dark web investigations, how to setup up a research/undercover computer using virtual machines and Android phone emulators, setting up software for Tor, Tails, Freenet and I2P, researching dark markets, and understanding how to conduct undercover purchases of items for investigations. Basic cryptocurrency will also be included to facilitate purchases along with open source Intelligence techniques that are necessary to pivot from the dark web to the clear web for identification of targets.

Key concepts covered in this course include:

- Darknets
- Dark web
- Tor
- Virtual machines
- Cryptocurrency basics

Student Testimonials

"This course has not only expanded my skill set but has also empowered me with the confidence to tackle complex online investigations with precision and efficiency. I am truly grateful for the invaluable insights gained and highly recommend this course to any criminal justice professional looking to enhance their capabilities in the digital age." -Phoenix, Arizona

CI 240

Virtual Lab

3 Days

32 Students Max

This course pairs well with:

FC099 Basic Level Spreadsheeting Skills

CI202 Intermediate Cyber Investigations: Online Open Source Investigations

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 of 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. Hands-on exercises include: opening a bitcoin wallet, bitcoin transactions, investigating the blockchain, and identifying services using free/open source explorers.

Key concepts covered in this course include:

- Virtual currency basics
- Blockchain
- Cryptocurrencies in detail
- Investigative techniques
- Stablecoins
- Decentralized finance (DeFi)
- Non-fungible tokens (NFT)

Student Testimonials

"Relying exclusively on skills I learned in this course, I was able to identify the subject's wallet addresses and manually track the individual transactions the subject was conducting with the fraudulently received funds through the blockchain and corroborate text discussions with actual transactions." -New York, New York

IA 102

Interactive Exercises

1 Day

32 Students Max

This course pairs well with:

CI202 Intermediate Cyber Investigations: Online Open Source Investigations

CI203 Intermediate Cyber Investigations: Dark Web Investigations

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.

Key concepts covered in this course include:

- Basic knowledge of link and association analysis
- Process of social network analysis
- Visual mapping and mathematical components

Student Testimonials

"With information learned in this course, I created a link matrix in order to attempt to identify any particular person, vehicle, or house which may be significant in a homicide investigation." -Yuma, Arizona

"I had a case involving parcels with suspected cocaine and a large number of individuals. With the knowledge gained from the Introduction to Link Analysis course, I was able to create a link chart to aid in the ongoing investigation. It was extremely useful during surveillance and when briefing teams on the case." -Doylestown, Pennsylvania

IA 105

Interactive Exercises

3 or 4 Days

32 Students Max

This course pairs well with:

IA102 Introduction to Link Analysis

Intelligence Writing and Briefing

This course covers basic intelligence writing and briefing principles as well as methods for effective and clear intelligence sharing. Topics include creative and critical thinking, critical reading skills, source evaluation, privacy and civil rights, intelligence writing style and structure, and generating and presenting intelligence briefings. With guidance from experienced experts, students gain hands-on experience by working through data sets based on real cases to produce intelligence products. Instructors and peers provide feedback on briefings and reports produced and presented in class.

Key concepts covered in this course include:

- Foundational skills
- Information sources
- Analytical reports
- Privacy considerations
- Briefings

Student Testimonials

"After completing this class, I took the information I learned and immediately applied it to the creation and formatting of intelligence products as well as to the organizing and classifying of information and intelligence. Since applying what I learned in the class, the police departments have found the intelligence products impressive, credible, and useful. They have arrested and charged individuals involved in criminal activity at the events, or have completed other enforcement actions that positively impact the safety of the venues and communities in general." -Waukegan, Illinois

IA 300

Interactive Exercises

3 Days

32 Students Max

This course pairs well with:

CI202 Intermediate Cyber Investigations: Online Open Source Investigations

CI203 Intermediate Cyber Investigations: Dark Web Investigations

Advanced Criminal Intelligence: Tradecraft and Analysis

This course is dedicated to studying the fundamentals of quantitative and qualitative data analysis and how to formulate 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 also explore several common investigative objectives, including the discovery of associations between people and entities, the correlation between unlawful activity and suspects, behavioral affinities, and predictions. The course will introduce the Enterprise Theory of Crime and how to use 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.

Key concepts covered in this course include:

- Data management techniques
- Network analysis
- Enterprise Theory of Crime

Student Testimonials

"Overall I really enjoyed the course. Great combination of practical application, history/historical context, philosophy, logic (and how these disciplines apply to our fields), real-life examples and relevant facts pertaining to crime in our society today, resources and useful skills that we can directly apply the the work that we do. I found the instructors to be incredibly kind, caring, helpful, personable, approachable, good at explaining, patient, and they seemed to truly care about our learning." -Anonymous

CI 350

Interactive Exercises

3 Days

32 Students Max

This course pairs well with:

CI202 Intermediate Cyber Investigations: Online Open Source Investigations

CI240 Intermediate Cyber Investigations: Virtual Currency

The Internet: Investigations and Intelligence

The course gives students an up-to-date understanding of how social networking sites work and how members act and interact. Students will learn what information is available on various sites and how to integrate that information into criminal investigations and criminal intelligence analysis.

- The role of OSINT in predicting and interdicting spree killings - case studies and analysis
- OSINT and criminal investigations
- Metadata exploitation in criminal investigations
- OSINT collection tools
- EXIF tags and geolocation of devices for investigations and operational security
- Case studies in metadata vulnerability exploitation and facial recognition
- Online undercover operations
- Counterintelligence concerns for law enforcement
- Law enforcement interaction with Internet service providers
- Emerging technologies used to hide on the Internet
- Proxies, VPNs, Tor, Onion Routers, Deepnet, and Darknet
- Dark market investigative tactics, techniques, and procedures

NOTICE: Course contains graphic content including profanity, and sexual and violent images.

Student Testimonials

"This is the best training I've attended in my six years as a digital evidence analyst. What really differentiated it from the other trainings I've taken was it's ability to blend theory and on the ground case work. The training covered not only what data is out there but how to get it via legal demand and how to use it in an actual case." -Queens, NY

CS 235

Virtual Lab

4 Days

32 Students Max

This course pairs well with:

DF205 Intermediate Digital Forensic Analysis: SQLite Primer

DF340 Advanced Digital Forensic Analysis: Linux

Basic Network Intrusion Investigations

This course covers the skills and techniques involved in responding to a network security incident. The course focuses on the identification, extraction, and detailed examination of artifacts associated with network and intrusions. Memory analysis, host machine forensics, network traffic and log analysis, malware analysis, and virtual machine sandboxing are covered through lecture, discussion, and hands-on exercises. Additional topics include key cybersecurity concepts and issues, as well as the various classifications and types of network attacks.

Key concepts covered in this course include:

- Introduction to cybersecurity
- Network traffic analysis
- Network attacks
- Investigative techniques
- Hands-on experience

Student Testimonials

"Whether you're a seasoned cybersecurity professional looking to refine your skills or a novice eager to dive into the world of incident response, this course is a must. I can confidently say that it has equipped me with the knowledge and expertise needed to tackle any network security challenge head-on." -Martinsburg, West Virginia

DF 100

Interactive Exercises

1 Day

32 Students Max

This course pairs well with:

CI102 Basic Cyber Investigations: Dark Web & OSINT

CI202 Intermediate Cyber Investigations: Online Open Source Investigations

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.

Key concepts covered in this course include:

- Preparation for incident response
- Identification of relevant sources of digital evidence
- Proper collection of digital evidence
- Legal and valid preservation of digital evidence

Student Testimonials

"This course helped me to be more aware of the different types of storage devices that are available, and how to obtain the information from these devices." -Wellington, Ohio

"This class helped me with a case involving a female who was laundering money through her bank account for a "crypto coin" company. After seizing her cell phone, laptop, and computer, I was able to identify several banks she was using to launder money and she was charges accordingly. I was also able to get the account information for the other individual which returned as a dummy account." -Casper, Wyoming

DF 101

Virtual Lab

3 or 4 Days

32 Students Max

This course pairs well with:

DF202 Intermediate Digital Forensic Analysis: Windows File Systems

DF310 Advanced Digital Forensic Analysis: Windows Analysis

Basic Digital Forensic Analysis: Windows Acquisition

This course provides the fundamental knowledge and skills required to acquire forensic backup images of commonly encountered forms of digital evidence (Microsoft® Windows® based computers and external storage devices) in a forensically-sound manner. Presentations and hands-on practical exercises cover 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.

Key concepts covered in this course include:

- Storage media
- Forensic acquisition process and methods
- Tool validation
- Hardware and software write blockers
- Forensic backup image formats

Student Testimonials

"My training with NW3C was instrumental in my promotion to Digital Evidence Examiner. I am confident that I would not have been prepared for the promotional process without the instruction of NW3C." -Raleigh, North Carolina

"The knowledge I have gained from NW3C courses about digital forensics has been helpful in understanding and comfort level when working on various video capture and storage devices (whether they are DVRs/NVRs or PC-based surveillance systems). This course has made me more comfortable working with PC-based surveillance (CCTV) systems." - Indianapolis, Indiana

DF 201

Virtual Lab

4 Days

32 Students Max

This course pairs well with:

DF101 Basic Digital Forensic Analysis: Windows Acquisition

DF202 Intermediate Digital Forensic Analysis: Windows File Systems

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 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.

Key concepts covered in this course include:

- Digital forensic process
- Validation
- Effective tool usage
- Reporting

Student Testimonials

"The training received from NW3C has helped tremendously in these cases by providing us with insight in how to better utilize the tools we have to find relevant evidence in each of the cases." -Salem, Oregon

DF 202

Virtual Lab

3 Days

32 Students Max

This course pairs well with:

DF101 Basic Digital Forensic Analysis: Windows Acquisition

DF310 Advanced Digital Forensic Analysis: Windows

Intermediate Digital Forensic Analysis: Windows File Systems

This course introduces investigators and digital forensics professionals in law enforcement to the file systems utilized by Microsoft Windows®. The course provides knowledge and skills that will assist students in many facets of their examination of digital evidence located in FAT32, exFAT, and NTFS formatted media. The concepts covered for each of the file systems will include a detailed look into the structure of the file systems and a look into the process that occurs when files or folders are saved, deleted, and restored. Detailed hands-on exercises will give students the knowledge and skills to articulate key findings to investigators, prosecutors, judges, and juries.

Key concepts covered in this course include:

- Computer communication and formatting
- File system structure and layout
- Saving files
- Deleting files
- Restoring files

Student Testimonials

"This training helped prepare me for reviewing results of digital forensic exams and for other training in forensics tools. I used this training in a case that resulted in an arrest for a drug-related offense and an investigation into fraud involving the same suspect is ongoing." -St. Paul, Minnesota

DF 203

Virtual Lab

3 Days

32 Students Max

This course pairs well with:

DF340 Advanced Digital Forensic Analysis: Linux

Intermediate Digital Forensic Analysis: Forensic Tools for Video Analysis

This course provides training on digital forensics for video, specifically targeting common file formats rather than proprietary video encodings or delivery methods. It aims to equip investigators with automated tools to answer critical questions about the video's origins and authenticity. This training is designed to support investigations by providing the necessary expertise to handle the complexities of video evidence in the digital age, where authenticity and source identification are paramount.

Key concepts covered in this course include:

- Tool and result verification
- Metadata and structural parsing
- Image classification
- Structural signatures and classification
- Deepfake detection and analysis
- Reporting results

Student Testimonials

"Whether you're a seasoned investigator or new to the field, this training is invaluable. It empowers you with the expertise needed to handle video evidence in the digital age, where authenticity is paramount. I can confidently say that this course has enhanced my capabilities as an investigator, and I feel better equipped to support investigations in an increasingly digital world." -Anonymous

DF 205

Virtual Lab

1 Day

32 Students Max

This course pairs well with:

DF330 Advanced Digital Forensic Analysis: iOS & Android

FC099 Basic Level Spreadsheeting Skills

Intermediate Digital Forensic Analysis: SQLite Primer

Mobile devices dominate the intake lists and desks of most digital forensic 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.

Key concepts covered in this course include:

- What is SQLite and how to identify and analyze logically
- Recognizing relevant locations of valuable data within SQLite database
- Develop skills needed for crafting custom SQLite queries
- Recognize and decode a variety of common timestamp formats
- Perform SQLite analysis with automation

Student Testimonials

"The SQL class has opened up a new level of comfort when investigating Mobile devices. I have been able to confidently confirm the data that automated tools have produced. Recently, I conducted digital forensic exam on a cell phone regarding child pornography. There was no relevant evidence located by the automated tool. I then proceeded to explore different databases, and eventually located child exploitation material and other relevant evidence. This training also helped in a similar manner on a school threat investigation." -Williamsville, Illinois

DF 310

Virtual Lab

4 Days

32 Students Max

This course pairs well with:

DF101 Basic Digital Forensic Analysis: Windows Acquisition

DF202 Intermediate Digital Forensic Analysis: Windows File Systems

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 jump lists. This course uses a mixture of lecture, discussion, demonstration, and hands-on exercises.

Key concepts covered in this course include:

- The registry
- Shellbags
- Mounted devices
- Change journal
- Prefetch

Student Testimonials

"Recently we received three child pornography investigations from the National Center for Missing and Exploited Children NCMEC. These examinations were somewhat more difficult and I used the skills I learned in this class to successfully extract artifacts which substantially increased the successful extraction of evidence. All three cases have been submitted and all suspects charged." -Richfield, MN

"The knowledge I have gained from the courses assist me daily in investigations. I have used the information gained on dozens of cases. Several leading to arrests and convictions. This course help me increase my understanding, as I am working in my computer forensic software." -Oakland, CA

DF 330

Virtual Lab

4 Days

32 Students Max

This course pairs well with:

DF100 Basic Digital Forensic Analysis: Seizure

DF205 Intermediate Digital Forensic Analysis: SQLite Primer

Advanced Digital Forensic Analysis: iOS & Android

This course provides the advanced knowledge and skills necessary to analyze data on iOS® devices, as well as various Android™ devices. Students use forensically-sound techniques to analyze potential evidence. Students will learn current techniques and procedures to better understand the mobile device evidence which they are encountering. Topics include holistic application analysis and a detailed explanation of default folder structures. The forensic artifacts covered include device information, call history, messages, web browser history, Wi-Fi, and Bluetooth artifacts. Students will use a variety of free and/or open-source utilities to gain a verbose view of these digital artifacts.

Key concepts covered in this course include:

- Holistic data analysis
- In-depth SQLite analysis
- Advanced analysis techniques

Student Testimonials

"The class has assisted me in viewing more database related information versus just what the tool will parse out." -Michigan

"In general, this class provided me with the knowledge and skills to better understand the file structure of iOS and Android operating systems and improved my forensic analysis abilities when processing digital evidence." -Roseburg, Oregon

DF 340

Virtual Lab

2 Days

32 Students Max

This course pairs well with:

DF203 Intermediate Digital Forensic Analysis: Forensic Tools for Video Analysis

DF205 Intermediate Digital Forensic Analysis: SQLite Primer

Advanced Digital Forensic Analysis: Linux

This advanced course will provide instruction and practical exercises to give the vital skills and necessary resources to investigate crimes involving Linux-based operating systems. The topics included will leverage free and open-source tools for the acquisition of information from the Linux operating system, its analysis, and reporting. It will also cover a variety of distributions commonly encountered, including volatile memory distributions such as Tails and Whonix, along with installed distributions including Qubes, Ubuntu, Fedora, and Kali.

Key concepts covered in this course include:

- Analysis of SQLite databases from Linux-based operating systems
- Triage techniques
- Analysis of command line history and application usage

Student Testimonials

"I am immensely grateful for the opportunity to take part in this advanced course. It has not only deepened my expertise in investigating crimes involving Linux-based operating systems but has also equipped me with the confidence and skills needed to excel in this specialized field of forensic investigation." -Anonymous

FC 099

Virtual Lab

1 Day

32 Students Max

This course pairs well with:

FC200 Intermediate Level Spreadsheeting Skills

Basic Level Spreadsheeting Skills

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

Key concepts covered in this course include:

- Work with multiple worksheets within a workbook
- Hide, unhide, and protect worksheets
- Adjust rows and columns
- Use copy and paste options
- Find, select, and sort data

Student Testimonials

"Taking Basic Level Spreadsheeting Skills class has augmented my data analytics skills and helped me to combine effectiveness with efficiency in financial analysis. It is pertinent for investigators to be more knowledgeable or at least know as much as the criminals being investigated in order to deduce, separate fraud from errors, and render unbiased opinions or judgments." -New York, New York

"Spreadsheets are always a part of my investigations. This class showed me more efficient ways to accomplish basic tasks from the ribbon rather than always going to more complicated routes. This has saved me time and frustration, and I tell you that in itself is priceless!" -Portland, Oregon

FC 200

Virtual Lab

2 Days

32 Students Max

This course pairs well with:

FC099 Basic Level Spreadsheeting Skills

Intermediate Level Spreadsheeting Skills

This intermediate spreadsheeting course uses Microsoft® Excel to assess and organize data in an electronic format. The class is designed for students 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.

Key concepts covered in this course include:

- Relative, absolute, and mixed cell referencing
- Text, date, and time-based functions and formulas
- How to nest functions
- Management of delimited data
- VLOOKUP and XLOOKUP
- Dynamic arrays

Student Testimonials

"The skills learned in this course have streamlined the way that I review complex data sets which in turn freed up time to pursue other investigative avenues in all cases in my purview." -Jackson, Mississippi

"Attended this class to see what content NW3C teaches at an intermediate level. Several tips and tricks provided that have proven useful to increase my efficiency. I particularly liked the layout of the provided guides being within Excel vs. Word or a PowerPoint." -Phoenix, Arizona

FC 105

Interactive Exercises

2 Days

32 Students Max

This course pairs well with:

FC201 Financial Records Investigative Skills

FC203 Financial Investigations: Beyond the Basics

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.

Key concepts covered in this course include:

- Introduction to analysis
- Financial records
- Financial profiling
- Hands-on experience

Student Testimonials

"Information from this class ensured I adopted a methodical and measured approach to analyzing the financial records in an investigation thereby being able to demonstrate that the funds used by the suspect had been obtained illegally through fraud. This provided prima facie evidence of their culpability." -Tampa, Florida

"I use the training provided in this course within all of my case work. I work on a variety of different types of cases from elder abuse to embezzlement to murder cases." -Anonymous

FC 201

Interactive Exercises

3 Days

32 Students Max

This course pairs well with:

FC105 Financial Records Examination & Analysis

FC203 Financial Investigations: Beyond the Basics

Financial Records Investigative Skills

This course builds on the concepts introduced in FC105 (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.

Key concepts covered in this course include:

- Money laundering
- Spreadsheeting skills
- Working with financial data
- Hands-on experience

Student Testimonials

"The skills I learned were invaluable in keeping track of the hundreds of invoices and identifying the same delivery dates. Also, due to the complexity of this case, flow chart skills were also necessary to keep track of all the subjects, vehicles, and locations." -Tacoma, Washington

"This class helped me to more accurately identify sources where evidence could be located and ultimately was. It prepared me how to approach my investigations by helping me to think more broadly than I previously did." -Indianapolis, Indiana

FC 203

Interactive Exercises

3 Days

32 Students Max

This course pairs well with:

IA300 Advanced Criminal Intelligence: Tradecraft and Analysis

FC204 Combating Transnational Crime & Terrorism Financing

Financial Investigations: Beyond the Basics

This three-day course covers the fundamentals of financial investigations and incorporates some of the more advanced processes that elevate an investigation. During this course, students will learn about investigative processes, practical tools, and sources of information necessary to plan and conduct financial investigations. The course begins with a description of the basic composition of elements within illicit financial networks and how they work to compromise legitimate business and financial sectors. Course material will describe government, regulatory, and investigative actions within the United States, and by international partners to detect and investigate illicit actors and networks. The course also includes considerations for investigation planning and promoting creative thinking.

Key concepts covered in this course include:

- Illicit network vulnerabilities
- Movement of money and messaging
- Bank Secrecy Act
- Value flow
- Fronts, shells, and shelf business
- Investigation preparation

Student Testimonials

"I was able to learn new terms and ideas for conducting investigations. I frequently write warrants to banks and this class improved my ability to gather information the first time. " -Lawrence, Kansas

"This class provided me with the investigative processes, practical tools, and sources of information needed to enhance my data security, privacy, and technology accountability investigations. " -Newark, New Jersey

FC 204

Interactive Exercises

3 Days

32 Students Max

This course pairs well with:

FC203 Financial Investigations: Beyond the Basics

IA300 Advanced Criminal Intelligence: Tradecraft and Analysis

Combating Transnational Crime & Terrorism Financing

An effective financial investigation can disrupt terrorism organizations and interrupt, deter, or even stop operational terrorism activities before they can begin. In this three-day course, students develop an understanding of how financial systems are used to support terrorism 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 such as Society for Worldwide Interbank Financial Telecommunications (SWIFT) messaging, and records used in banking and money services businesses.

Key concepts covered in this course include:

- Illicit finance
- Money laundering and trade-based money laundering
- Value transfer methods
- Critical thinking in case planning

Student Testimonials

"I was able to use the concepts learned in this course, apply associations based on 13 separate suspect interviews and arrests to develop links of suspects associations, some assets, and locations of catalytic converter sales. This visualization made it easier for the task force to determine which nodes had the most connections with others, resulting in concentrating resources to those suspects first. As a result, one spin off investigation has provided evidence of other crimes committed which will be referred to the proper jurisdictions." -Anonymous

TRAINING@SUMURI.COM