DC3 Cyber Training Academy

FY25 October Offerings

Enroll Now

Click on the "Enroll Now" link to view the online catalog and to register for classes. Please contact the DC3 Cyber Training Academy Registrar with any questions.

Cyber Analyst Course (CAC)

The Cyber Analyst Course (CAC) is an 80-hour course that presents analytical methodologies and information sources applicable to a cyber environment. CAC is designed for Defense Criminal Investigative Organizations (DCIOs), cyber-intrusions investigators, information assurance professionals, and prospective lab examiners. Topics include interpreting analysis and forensic reports, internet research, computer system and network analysis, log analysis, data-hiding techniques, and intrusion identification. The course also covers using specialized analytical software and writing analysis reports. CAC contains six modules and culminates with a Final Knowledge Exam and a Final Performance Exam.

Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: INCH
Scheduled offering:
CAC-2501 (28 OCT – 8 NOV)

Cyber Incident Response Course (CIRC)

The Cyber Incident Response Course (CIRC) is an 80-hour course that prepares students in cyber incident response and evidence collection. In this course, students are provided various scenarios to understand and develop response protocols in a real-world environment. Using trusted forensic tools, students identify and extract digital evidence from various devices such as computers, cell phones and small form factor digital storage devices. Students are taught how to properly document evidence using lawful, professional techniques to ensure the legal admissibility of the seized evidence. CIRC contains three units with quizzes and a course Capstone Exercise.

Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: INCH
IACET CEU-eligible, ACE Recommendation
Scheduled Offering:
CIRC-2501 (28 OCT – 8 NOV)

Dark Web Activities (DWA)

Dark Web Activities (DWA) introduces key concepts and tools for navigating and using the web, with a focus on identifying and tracking illegal activities and documenting findings. It distinguishes between the deep web and dark web, explaining their unique features and components. The course covers the essential technologies and tools used for accessing and navigating the dark web, as well as techniques for tracking illegal activities such as cyber crime, drug trafficking, and fraud.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
DWA-2501 (28 OCT – 8 NOV)

Introduction to Cyber Investigations (ICI)

Introduction to Cyber Investigations (ICI) is a 40-hour course that prepares students to perform or support the role of a case agent responsible for a basic cyber investigation. ICI is designed for Defense Criminal Investigative Organizations (DCIOs), cyber-intrusions investigators, information assurance professionals, and prospective lab examiners. Students learn basic technical concepts and the legal framework that guides the conduct of cyber investigations. Students also study special aspects of cyber case management (including online evidence collection) and subjects of cyber investigations. ICI contains five modules with module assignments and exercises and culminates with a final, graded exam.

Delivery: Online
Duration: 40 hours of training over 5 weeks
Prerequisite: None
ACE Recommendation
Scheduled Offering:
ICI-2501-OL (28 OCT – 28 NOV)

DC3 Cyber Training Academy

FY25 October Offerings

Introduction to Networks and Computer Hardware (INCH) OL/ILV

INCH is a 40-hour course that teaches computer basics, network theory, and input/output device identification and function. INCH is designed for personnel working in or interested in pursuing a career in fields such as computer intrusion investigations, information assurance, and digital evidence examinations. Students explore common operating system functionality and the use of the command line in Microsoft Windows. The course material and practical exercises introduce troubleshooting, as well as security and safety terminology and techniques. INCH contains 10 modules and culminates with a Capstone Exam.

Delivery: Online or Instructor-Led Virtual
Duration: Online is 40 hours of training over 4 weeks
Instructor-Led Virtual is 40 hours of training over 5 days
Prerequisite: None
IACET CEU-eligible, ACE Recommendation
Scheduled offerings:
INCH-2501-OL (28 OCT – 21 NOV)
INCH-2502-OL (28 OCT – 21 NOV)

Introduction to Networks and Computer Hardware In-Residence (INCH-RES)

INCH-RES is a 40-hour course that teaches computer basics, network theory, and input/output device identification and function. INCH-RES is designed for personnel working in or interested in pursuing a career in fields such as computer intrusion investigations, information assurance, and digital evidence examination. Students explore common operating system functionality and the use of the command line in Microsoft Windows. The course material and practical exercises introduce troubleshooting, security, and safety terminology and techniques, complete with the physical disassembly and reassembly of a computer. INCH-RES contains 10 modules and culminates in Capstone Exam. A test-out option is available to permit qualified personnel to bypass the course.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
IACET CEU-eligible, ACE Recommendation
Scheduled offering:
INCH-RES-2501 (21-25 OCT)

Please note that INCH Test Out options are available.

Linux+ (Linux+)

The Computing Technology Industry Association's (CompTIA) Linux+ proves you have the skills administrators need to secure the enterprise, power the cloud, and keep systems running. This bootcamp-style course covers an evolving job role that focuses more on how Linux powers the cloud. Students will review cutting edge technologies that help automate and orchestrate business processes, including infrastructure as code and containers. Vouchers are not included.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
Linux+-2501 (28 OCT – 1 NOV)

Mac Forensics (MACF)

The Mac Forensics (MACF) course focuses on conducting digital investigations of Macintosh operating systems (macOS) and iPhone operating systems (iOS) in a forensically sound manner. It builds on the foundation of the Forensics Intrusions in a Windows Environment course and introduces best practices and relevant technical aspects of macOS forensic examinations and incident response. It includes scenarios that build upon each other so students can practice what they learn using trusted forensic tools

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offerings:
MACF-2501 (21-25 OCT)

Network + (NET+)

NET+ is a bootcamp-style course that builds on your existing user-level knowledge and experience with computer operating systems and networks so you can master the fundamental skills and concepts needed for success in any networking career. Students are taught to describe the major networking technologies and systems of modern networks and configure, manage, and troubleshoot modern networks. Students must make their own arrangements to take the exam at any CompTIA testing center. Vouchers are not included.
Delivery: In-residence
Duration: Approximately 40 hours over 1 week
Prerequisite: None
Scheduled offering:
NET+-2501 (21-25 OCT)

Network Traffic Collection (NTC)

NTC is a 40-hour course that prepares students to strategically place monitoring sensors in a network to capture traffic to and from a specific host. NTC is designed for Department of Defense (DOD), cyber-intrusions investigators, information assurance professionals, prospective lab examiners, and military intelligence and 5 counterintelligence personnel. Students examine how to evaluate a network, both physically and logically, to determine proper sensor placement. Students also study how to filter network traffic to comply with wiretap authority, hide the presence of the monitoring workstation on the network, and evaluate captured traffic for the proper content. NTC contains five modules and culminates with a final, graded exam.
Delivery: In-residence
Duration: Approximately 40 hours over 1 week
Prerequisite: None
Scheduled offering:
NTC-2501 (21-25 OCT)

Windows Forensic Examinations (WFE)

WFE provides training that enables professionals to conduct digital analysis of Windows systems in a forensically reliable manner. Building on the foundation of the Cyber Incident Response Course (CIRC), this course introduces best practices and relevant technical aspects of Windows forensic examinations. The course immerses students in mini-scenarios that escalate in difficulty, allowing them to practice and reinforce what they have learned while using trusted forensic tools, and provides a longform practice that prepares students for the Capstone Exam.

Delivery: In-residence
Duration: 80 hours of training over 2 weeks in-residence
Prerequisite: CIRC
Scheduled offering:
WFE-2501 (21 OCT – 1 NOV)