



## FY25 February 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.*

---

#### **A+ (A+)**

A+ course is the industry standard for launching IT careers. In this bootcamp-style course, students install, configure, optimize, troubleshoot, repair, upgrade, and perform preventive maintenance on personal computers, digital devices, and operating systems. A+ is designed for individuals with basic computer user skills who are interested in obtaining a job as an entry-level IT technician. It is also designed for students seeking the CompTIA A+ certification who want to prepare for the CompTIA's A+ Core 1 (220-11001) and Core 2 (220-11002) certification exams. Students must make their own arrangements to take the exam at any CompTIA testing center. Vouchers are not included with this course.

**Delivery:** In-residence

**Duration:** 40 hours of training over 1 week

**CompTIA CEU-eligible**

**Prerequisite:** None

**Scheduled offering:**

[A+-2502 \(10-14 FEB\)](#)

---

#### **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-2503 \(3-14 FEB\)](#)

---



## FY25 February Offerings

### **CompTIA advanced Security Practitioner (CASP+)**

The CompTIA CASP+ bootcamp runs for 40 hours over 5 days and covers technical skills in security architecture and senior security engineering in traditional, cloud, and hybrid environments, governance, risk, and compliance skills, assessing an enterprise's cybersecurity readiness, and leading technical teams to implement enterprise-wide cybersecurity solutions. The DC3 Cyber Training Academy does not provide exam vouchers for CompTIA courses. Students must obtain their own vouchers and make their own arrangements to take the exam at any CompTIA testing location.

**Delivery:** In-residence

**Duration:** 40 hours of training over 1 week

**Prerequisite:** None

**Scheduled offering:**

[CASP+-2501-2501 \(10-14 FEB\)](#)

---

### **Cryptocurrency Activities (CCA)**

Cryptocurrency Activities (CCA) is a 40-hour in-residence training course designed for law enforcement and counterintelligence professionals and provides students with an understanding of cryptocurrency fundamentals and the skills necessary to conduct investigations into cryptocurrency transactions. The course immerses students in scenario-based exercises that allow them to practice and reinforce what they have learned while using trusted resources. CCA culminates with a graded Final Exam.

**Delivery:** In-residence

**Duration:** 40 hours of training over 1 week

**Prerequisite:** None

**Scheduled offering:**

[CCA-2503 \(24-28 FEB\)](#)

---



## FY25 February Offerings

### **Cyber Fundamentals 200 (CF200)**

CF200 is an 80-hour course that serves as the second installment of a two-part curriculum to provide foundational cyber knowledge to cyberspace workforce elements and Department of Defense (DOD) personnel, whose duties include the protection of DOD information systems from unauthorized and/or illegal access. The course comprises three units with multiple lessons; each unit culminates in a unit milestone exam and the 2 course ends with a Capstone Exam. There is a test-out option available to permit qualified personnel to bypass the course.

**Delivery:** Online asynchronous (Self-paced/no instructor)

**Duration:** 80 hours of training over 3 weeks

**Prerequisite:** None

**Scheduled offering:**

CF200-2504-OL (3-21 FEB)

---

### **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-2504 (24 FEB – 7 MAR)

---



## FY25 February Offerings

### **Cyber 101 (CY101)**

Cyber 101 (CY101) is a 40-hour course that is designed to provide fundamental cyber knowledge to students interested in developing cyber competency or who are in roles where they support cyber operations (such as CPTs, MDTs). CY101 is a requirement for any personnel identified in DoDD 8140 as a “cyber enabler.” The course consists of five units containing modules and lessons, unit Milestone Exams, and a final, graded Capstone Exam.

**Delivery:** Online asynchronous (Self-paced/no instructor)

**Duration:** 40 hours of training over 3 weeks

**Prerequisite:** None

**Scheduled Offering:**

CY101-2504-OL (3-21 FEB)

CY101-2505B-OL (18 FEB – 7 MAR)

---

### **Cybersecurity Analyst (CySA+)**

Cybersecurity Analyst (CySA+) is a bootcamp-style course that teaches incident detection, prevention, and response through continuous security monitoring for success in a high-stakes analysis. Students learn processes in security operations, vulnerability management, incident response and management, and how to apply best practices for reporting and communication. Vouchers are not included.

**Delivery:** In-residence

**Duration:** 40 hours of training over 1 week

**Prerequisite:** None

**Scheduled Offering:**

CySA+-2504 (3-7 FEB)

---



## FY25 February Offerings

### **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-2505 (3-7 FEB)

DWA-2506 (24-28 FEB)

---

### **Forensics and Intrusions in a Windows Environment (FIWE)**

Forensics and Intrusions in a Windows Environment (FIWE) is an 80-hour scenario-based training course developing students' skills in conducting a full investigation of a network intrusion. FIWE is designed for Defense Criminal Investigative Organizations (DCIOs), DoD intrusion analysts, network operators, and investigators. Students conduct forensic examinations of victim devices, analyze log data and network traffic data, create an event timeline, perform malware analysis, and prepare narrative reports of their findings. These skills prepare students to perform a variety of network investigations. FIWE contains three modules and culminates with a graded Final Exam.

**Delivery:** In-residence

**Duration:** 80 hours of training over 2 weeks

**Prerequisite:** NIB and WFE-E

*IACT CEU-eligible, ACE Recommendation*

**Scheduled Offering:**

FIWE-2503 (24 FEB – 7 MAR)

---



## FY25 February Offerings

### **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-2503-OL](#) (24 FEB – 27 MAR)

---

### **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-2507-OL](#) (3-27 FEB)

[INCH-2508-OL](#) (3-27 FEB)

---



## FY25 February Offerings

### **Log Analysis (LA)**

LA is a 50-hour course that provides a comprehensive understanding of log analysis techniques. LA is designed for cyber investigators or analysts interested in furthering their skills in determining the how, when, and where of a network intrusion through log file analysis and investigation. Students learn how to process logs from Windows and Linux operating systems, firewalls, intrusion detection systems, and web and email servers. Students learn how to assemble evidence found in logs to assist in tasks ranging from building a case to recognizing an intrusion. LA contains three modules comprising multiple lessons and culminates with a final, graded exam.

**Delivery:** Online

**Duration:** 50 hours of training over 5 weeks

**Prerequisite:** None

**Scheduled offering:**

[LA-2504-OL](#) (24 FEB – 27 MAR)

---

### **Linux Essentials (LXE)**

Linux Essentials (LXE) is a 40-hour course that teaches core concepts and techniques of Linux system management and administration. LXE is designed for students who want to develop greater understanding of Linux or who conduct investigative and security activities associated with Linux environments. Students acquire intermediate Linux skills used in cyber investigation studies and real-world investigative and security tasks. The course prepares students to carry out functions and tasks relevant to any standard Linux environment. LXE contains nine lessons and culminates with a final, graded exam.

**Delivery:** Online

**Duration:** 40 hours of training over 4 weeks

**Prerequisite:** None

**Scheduled offerings:**

[LXE-2503-OL](#) (3-27 FEB)

---



## FY25 February Offerings

### **Network Mapper (NMAP)**

Network Mapper (NMAP) is an 8-hour course that provides instruction in using the Network Mapper tool to manage vulnerabilities, verify baseline configuration compliance, and identify risk among communication protocols, data services, and associated ports. NMAP is designed for work roles assigned to the specific task of exploring networks to isolate vulnerabilities and applying programs that protect exploitable ports from attacks. Students learn how to conduct reconnaissance on adversary networks. The course provides functional information and focuses on useful, real-life examples that students can immediately apply. NMAP contains five modules and culminates with a Final Exam.

**Delivery:** Online

**Duration:** 8 hours of training over 5 days

**Prerequisite:** INCH

**Scheduled Offering:**

NMAP-2503-OL (18-24 FEB)

---

### **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-2503 (10-14 FEB)

---



## FY25 February Offerings

### **Penetration Testing (PenTest+)**

Penetration Testing (PenTest+) is a bootcamp-style course that covers all penetration testing stages and teaches vulnerability management. Students learn planning and scoping, information gathering and vulnerability scanning, how to apply best practices for reporting and communication, updated approaches to attacks and exploits, code analysis, and uses of various tools. Vouchers are not included.

**Delivery:** In-residence

**Duration:** 40 hours of training over 1 week

**Prerequisite:** None

**Scheduled Offering:**

PenTest+-2502 (10-14 FEB)

---

### **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-2504 (24 FEB – 7 MAR)

---