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.

Advanced Malware Analysis (AMA)

Advanced Malware Analysis (AMA) is designed to provide students with the fundamental principles of dissecting and reverse engineering complex malware. In this 80-hour course, students will inspect malware via disassembly tools and other static analysis methods to identify capabilities, indicators of compromise, and attacker infrastructure. Using both attacker and defender perspectives, students will learn to overcome the advanced techniques used to circumvent reverse engineering.

Delivery: In-residence
Duration: 80 hours of training over 2 weeks
Prerequisite: None
Scheduled offering:
AMA-2501 (18-29 AUG)

Basic Malware Analysis (BMA)

Basic Malware Analysis (BMA) is a 40-hour course designed to provide students with a foundational understanding of malicious software and its forms, traits, author motivations, and impacts. Students will be introduced to common techniques and tools for both dynamic and static analysis and will develop a basic understanding of the process for uncovering the functionality of malware samples. Students also learn how to establish a network-isolated malware analysis lab, and how to interpret analytical reports resulting from static and dynamic analysis of malware. The BMA course contains six modules with corresponding module exams and culminates in a graded Final Exam.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
BMA-2504 (11-15 AUG)

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: Instructor-Led Virtual (ILV)
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
CCA-2507-ILV (4-8 AUG)

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: Instructor-Led Virtual (ILV)
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
DWA-2509-ILV (25-29 AUG)

DC3 Cyber Training Academy

FY25 August Offerings

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
IACET CEU-eligible, ACE Recommendation
Scheduled Offering:
FIWE-2504B (18-29 AUG)

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-2507-OL (18 AUG – 18 SEPT)

DC3 Cyber Training Academy

FY25 August Offerings

Introduction to Networks and Computer Hardware (INCH)

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
Duration: 40 hours of training over 4 weeks
Prerequisite: None
IACET CEU-eligible, ACE Recommendation
Scheduled offerings:
INCH-2521-OL (18 AUG – 11 SEPT)
INCH-2522-OL (18 AUG – 11 SEPT)

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-2508-OL (18 AUG – 18 SEPT)

DC3 Cyber Training Academy

FY25 August Offerings

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 graded Final Exam.

Delivery: Online
Duration: 40 hours of training over 4 weeks
Prerequisite: None
Scheduled offerings:
LXE-2510-OL (18 AUG – 11 SEPT)

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: Instructor-Led Virtual (ILV)
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
MACF-2506 (4-8 AUG)

DC3 Cyber Training Academy

FY25 August 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-2506-OL (11-15 AUG)

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: Instructor-Led Virtual (ILV)
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled offering:
NTC-2506-ILV (11-15 AUG)

Online Undercover Activities (OUA)

Online Undercover Activities (OUA) is a 40-hour scenario-based training course that will develop professionals' skills in conducting a full online undercover operation. The course provides both theory and practical training, enabling students to develop and plan an online undercover operation, create personas, manage digital footprints, engage in simulated dark web marketplaces and forums, and report their findings and activities. OUA contains six modules and culminates in a final, graded exam.

Delivery: In-residence
Duration: 40 hours of training over 1 week
Prerequisite: None
Scheduled Offering:
OUA-2503 (11-15 AUG)

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
IACET CEU-eligible, ACE Recommendation
Scheduled offering:
WFE-2507B (4-15 AUG)
