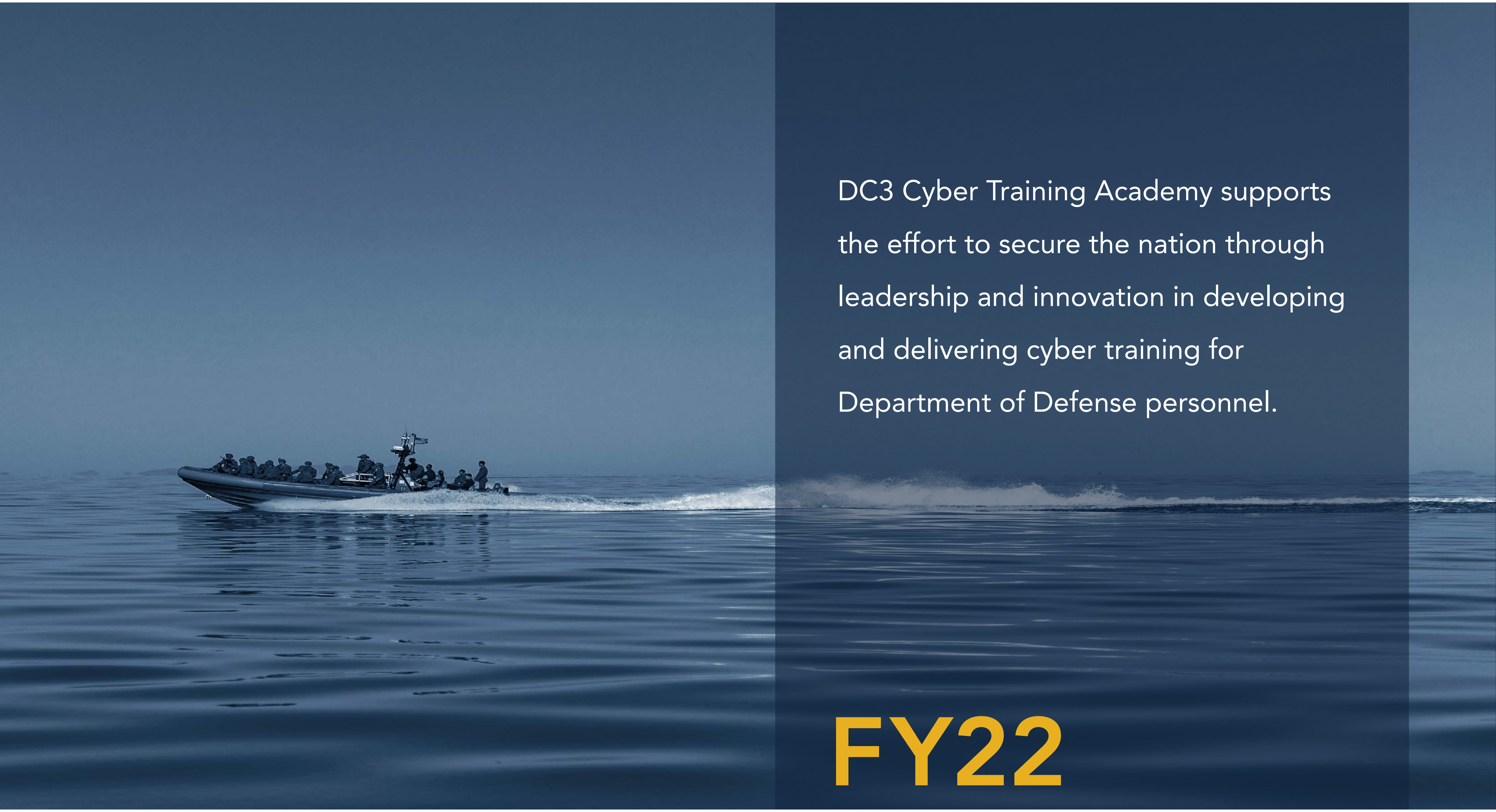
DC3 Cyber Training Academy



DC3 Cyber Training Academy supports the effort to secure the nation through leadership and innovation in developing and delivering cyber training for Department of Defense personnel.

FY22

COURSE CATALOG

About

Established in 1998, the Academy has its headquarters and main in-residence training facility in Hanover, Maryland. A rigorous Academy curriculum provides Department of Defense personnel with the relevant knowledge and cutting-edge skills they need to meet mission goals. Students can access courses three ways: instructor-led virtual training, online asynchronous, or through mobile training units in a variety of locations in the United States and abroad.

The Academy operates under the DoD Reform Initiative Directive 27.

MISSION

To provide cyber training to individuals and Department of Defense (DOD) elements that must ensure Defense information systems are secure from unauthorized use, counterintelligence, and criminal and fraudulent activities.

What We Offer

The Academy provides training in more than a dozen courses—ranging from computer basics to network intrusions and cyber analysis—designed to meet the evolving needs of students. In addition, the Academy offers training in modern cybersecurity tools such as OpenVAS and Network Mapper.

Students who pass these courses receive course completion certificates. In addition, the Academy offers three DOD certifications, widely recognized as validations of competency in digital forensic skills, to students who pass the following combinations of courses:

Digital Media Collector (DMC)
INCH, CIRC

Digital Forensic Examiner (DFE)
INCH, CIRC, WFE-E

Cyber Crime Investigator (CCI)
INCH, CIRC, WFE-E, FIWE

Icon Key

🕒 Duration

☑ Prerequisites

🏅 Accreditation

Accreditations

The Academy has earned national recognition for its excellence in cyber training from these organizations.

American Council on Education (ACE)
ACE provides college credit recommendations for a select number of Academy courses.

Council on Occupational Education (COE)
COE is the Academy's main accreditor, assuring quality and integrity in career and technical education.

International Accreditors for Continuing Education and Training (IACET)
The Academy, which IACET has recognized for its excellence in institutional practices, is an Authorized Provider of IACET Continuing Education Units (CEUs).

DC3 Cyber Training Academy Contact Information

learn.dcita.edu
443-733-1990
CTA.Registrar@dcita.edu

CORE

CF100
Cyber Fundamentals 100

NP | OL

CF200
Cyber Fundamentals 200

NP | OL

CY101
Cyber 101

NP | OL

ICI
Introduction to Cyber Investigations

ACE | NP | OL

INCH
Introduction to Networks and Computer Hardware

ACE | IACET | ILV | NP | OL | RES

MCIU
Managing Cyber Investigation Units

NP | OL

NIB
Network Intrusions Basics

NP | OL

NMAP
Network Mapper

OL

OPV
OpenVAS

NP | OL

INTERMEDIATE

CAC
Cyber Analyst Course

ILV | RES

CIRC
Cyber Incident Response Course

ACE | IACET | RES

FIWE
Forensics and Intrusions in a Windows Environment

ACE | IACET | ILV | RES

LA
Log Analysis

ACE | IACET | OL | RES

LXE
Linux Essentials

NP | OL | RES

NTC
Network Traffic Collection

ILV | RES

TEDA
Technology Evidence in Domestic Abuse

NP | OL

WFE-E
Windows Forensic Examinations - EnCase

ILV | OL | RES

NP No Prerequisites
RES In Residence **ILV** Instructor-led Virtual **OL** Online
ACE American Council on Education Credit Recommendation
IACET Eligible for IACET Continuing Education Units

Digital Media Collector (DMC) — INCH > CIRC
Digital Forensic Examiner (DFE) — INCH > CIRC > WFE-E
Cyber Crime Investigator (CCI) — INCH > CIRC > WFE-E > FIWE (with CI/LE badge)

CAC
Cyber Analyst Course

INTERMEDIATE

This course presents analytical methodologies and information sources applicable to a cyber environment. 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.

Course Objectives

- Review multiple reports containing relevant artifacts using basic cyber analysis techniques
- Analyze electronic artifacts in existing forensic and information reports
- Analyze basic data contained in text-based and binary logs
- Develop charts to visualize relevant data
- Develop information from internet-based resources while maintaining anonymity
- Classify network intrusions and malicious code types
- Investigate network traffic and explain network monitoring concepts

In Residence 80 hours over 10 days
Instructor-led Virtual 80 hours over 10 days

INCH

None

Back to top

CF100

Cyber Fundamentals 100

CORE

This course introduces students to hardware and software basics, operating systems, network architecture, and internet applications. It is the first installment of a two-part curriculum providing foundational cyber knowledge to Defense Criminal Investigative Organizations' (DCIOs) cyberspace workforce elements and Department of Defense (DOD) personnel, whose duties include protecting DOD information systems from unauthorized and/or illegal access.

Course Objectives

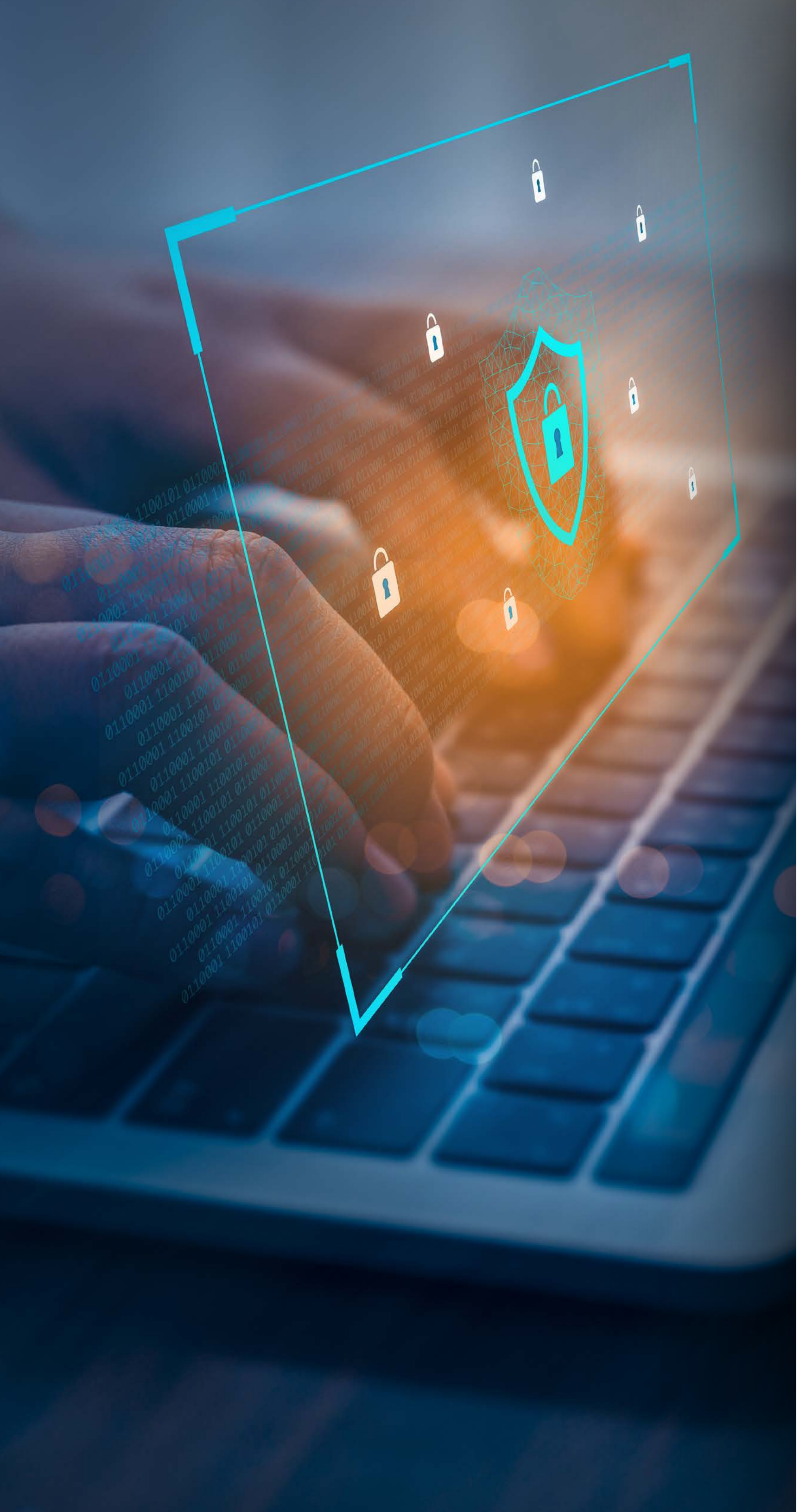
- Disassemble a personal computer (PC) virtually and assemble it to an operational status to demonstrate both conceptual and procedural knowledge of physical computer components and architectures
- Differentiate between the basic features, functions, and requirements of common operating systems
- Select the type of data transmissions for the appropriate networking protocol to establish a computer network
- Summarize basic internet applications and potential vectors of intrusion

Online 80 hours over 3 weeks

None

None

Back to top



CF200

Cyber Fundamentals 200

CORE

This course serves as the second installment of a two-part curriculum to provide foundational cyber knowledge to Defense Criminal Investigative Organizations' (DCIOs) cyberspace workforce elements and Department of Defense (DOD) personnel whose duties include the protection of DOD information systems from unauthorized and/or illegal access.

Course Objectives

- Differentiate between the basic administrative concepts, structure, and internal processes of Windows and Linux operating systems
- Select the type of data transmissions for the appropriate networking protocol to manage an established network
- Determine the best cybersecurity defense practices to meet common security standards

🕒 **Online** 80 hours over 3 weeks

None

None

Back to top

CIRC
Cyber Incident Response Course

INTERMEDIATE

This course builds on Introduction to Networks and Computer Hardware (INCH). CIRC prepares cyber crime first-responder students for digital investigations. The course provides scenarios for students to apply response protocols in a practical environment. Using trusted forensic tools, students identify and extract digital evidence from target devices. Students then document evidence using lawful, professional techniques.

Course Objectives

- Prepare for a cyber incident response and perform the role of a first responder
- Prepare accurate documentation of a cyber investigation to include all actions taken
- Examine where digital data resides in a variety of digital devices
- Explain forensic imaging principles
- Collect volatile and non-volatile data
- Demonstrate how to handle digital media effectively upon responding to an incident
- Generate hash values for collected data and forensic images

In Residence 40 hours over 5 days

INCH

ACE Recommended Course 3 Semester Hours Lower-Division
IACET CEU-eligible 4.0 CEUs

Back to top

CY101
Cyber 101

CORE

This course provides fundamental cyber knowledge to Department of Defense employees and contractors who may have limited to no cyber knowledge and skills within the Intelligence (Cyber) or Cyber Enabler workforces.

Course Objectives

- Choose the correct location of the devices within a computer network
- Implement one layer (such as malware) of the appropriate operational security (OPSEC) policy
- Categorize types of attack methods, targets, and vulnerabilities
- Select the appropriate national and international laws, regulations, policies, and ethics that relate to cybersecurity
- Select risk management strategies that minimize risk, implement controls, and accept residual risk

Online 40 hours over 2 weeks

None

None

Back to top

FIWE

Forensics and Intrusions in a Windows Environment

INTERMEDIATE

This course for network investigations is a scenario-based training in how to conduct a full investigation of a network intrusion. Students conduct several forensic examinations, analyzing log data and network traffic, preparing an executive summary, creating an event timeline, and performing malware analysis. These skills prepare students to perform a variety of network investigations.

Course Objectives

- Explain how to conduct a lawful network investigation
- Generate a detailed and accurate account of a network intrusion
- Analyze network-based evidence
- Analyze host-based evidence

In Residence 80 hours over 10 days
Instructor-led Virtual 80 hours over 10 days

NIB and WFE-E

ACE Recommended Course 5 Semester Hours Upper-Division
IACET CEU-eligible 4.0 CEUs

Back to top

ICI

Introduction to Cyber Investigations

CORE

This course prepares students to perform or support the role of case agent for basic cyber investigations. 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.

Note: Students must have unrestricted internet access to complete this course.

Course Objectives

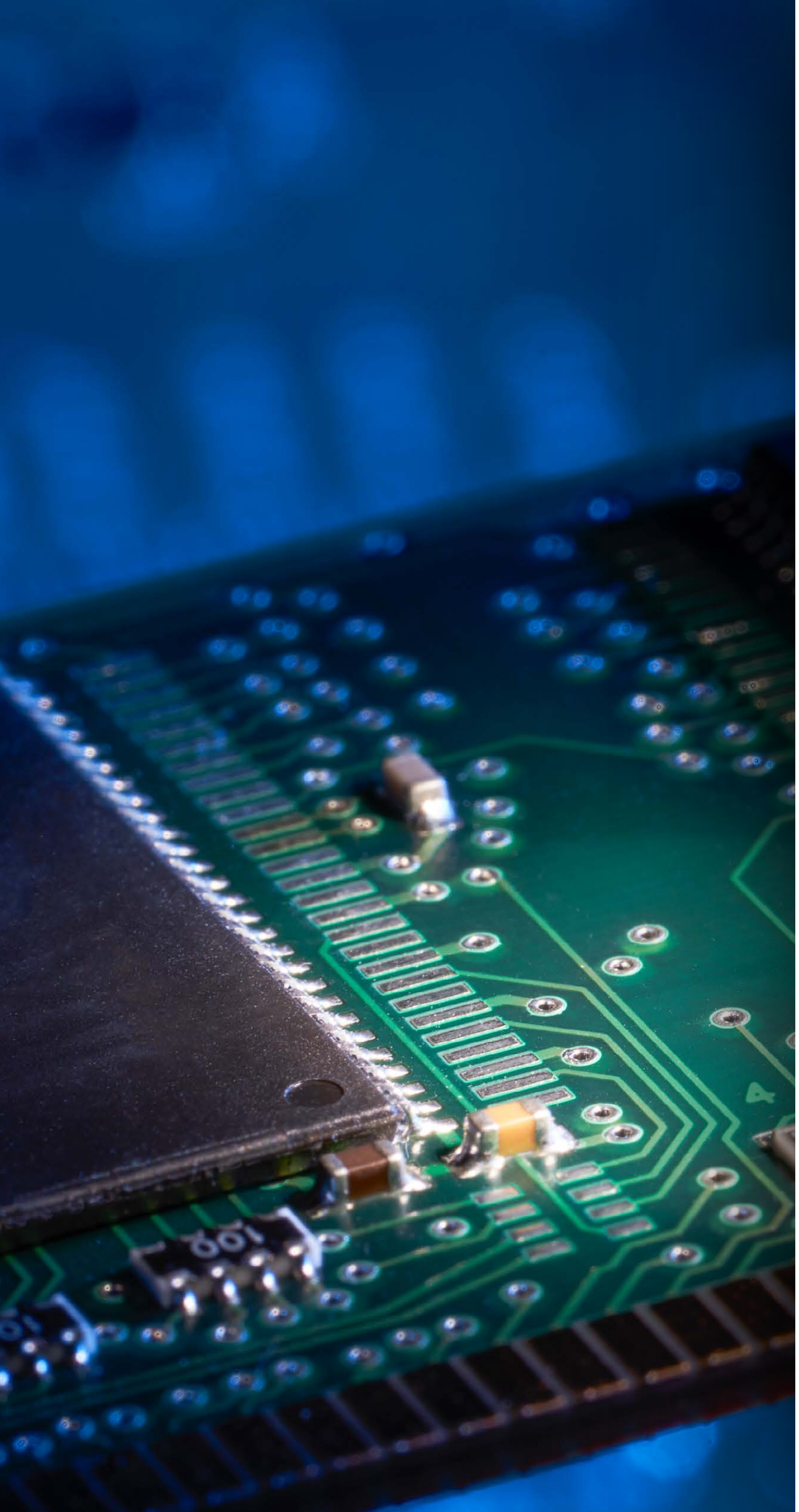
- Explain and define the scope and nature of cyber investigations
- Perform the collection and analysis of evidence in cyber investigations
- Prepare a subpoena and explain the legal fundamentals of cyber investigations
- Explain the role of cyber forensic laboratories in investigations
- Explain the different investigation methods among the military, civilians, corporate entities, and other countries and the available resources for each

Online 40 hours over 5 weeks

None

ACE Recommended Course 3 Semester Hours Lower-Division

Back to top



INCH

Introduction to Networks and Computer Hardware

CORE

This course teaches computer basics, network theory, and input/output device identification and function. Students explore common operating system functionality, focusing on the use of the command line in Microsoft Windows. The course material and practical exercises also introduce troubleshooting, as well as security and safety terminology and techniques.

Course Objectives

- Identify hardware components in a computer system
- Explain the functions of computer hardware where data is stored, including hard drives, removable media, random-access memory, and the central processing unit
- Employ operating system tools to manage disks, partitions, and file systems
- Perform domain management and administrative tasks using Windows Server Active Directory and Group Policy tools
- Explain basic theory, technologies, and components that facilitate network data transmission
- Configure a system to be able to communicate on a network
- Perform basic computer troubleshooting
- Perform basic computer tasks using Windows
- Explain methods to implement basic computer and network security

In Residence 40 hours over 5 days
Online 40 hours over 4 weeks
Instructor-led Virtual 40 hours over 5 days

None

ACE Recommended Course 3 Semester Hours Lower-Division
IACET CEU-eligible 4.0 CEUs

Back to top

LA
Log Analysis

INTERMEDIATE

This course provides a comprehensive understanding of log analysis techniques. Students learn how to process logs from Microsoft Windows and Linux operating systems, firewalls, intrusion detection systems, and web and email servers. Students also learn how to assemble evidence found in logs to assist in tasks ranging from building a case to recognizing an intrusion.

Course Objectives

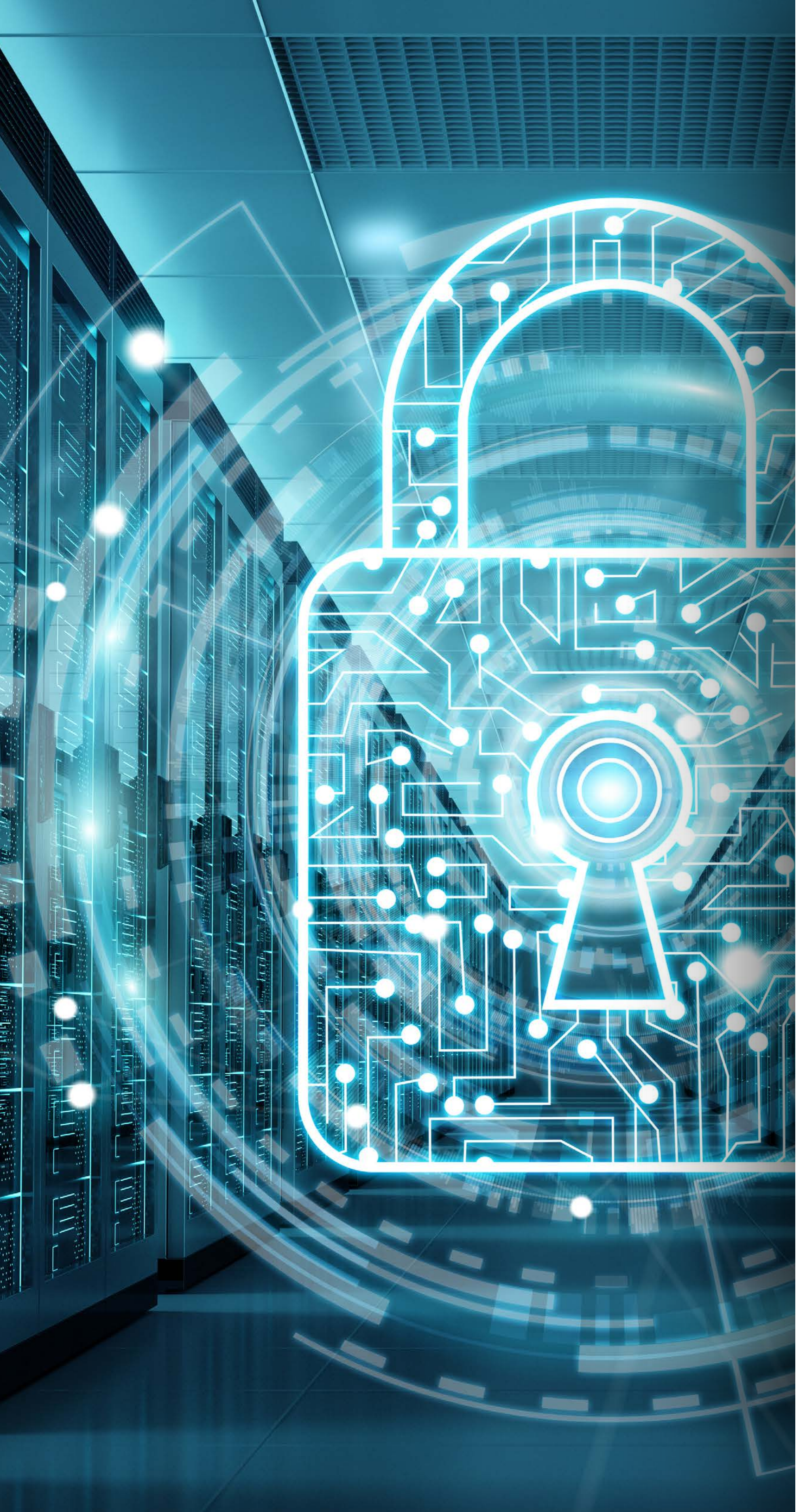
- Explain log analysis methodology
- Explain the benefits of log analysis in an intrusion investigation
- Analyze and evaluate log files
- Perform the extraction of information from log files
- Arrange log file data

In Residence 50 hours over 5 days
Online 50 hours over 5 weeks

NIB

ACE Recommended Course 5 Semester Hours Upper-Division
IACET CEU-eligible 4.0 CEUs

Back to top



LXE

Linux Essentials

INTERMEDIATE

This course teaches the core techniques and concepts of Linux system management and administration. 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.

Course Objectives

All course learning objectives are as defined by the Linux Professional Institute (LPI) for their Linux Essentials exam.

🕒 **In Residence** 40 hours over 5 days
Online 40 hours over 4 weeks

None

None

Back to top

MCIU

Managing Cyber Investigation Units

CORE

This course prepares students to take on or support the role of manager of a cyber investigation unit (CIU). Students learn how to establish a CIU on an organizational level and how to oversee operational policies. They also explore requirements for personnel and facilities. The course includes instruction on the importance of training to maintain consistent lab quality.

Course Objectives

- Explain organizational needs specific to establishing a CIU
- Give examples of budgetary expenditures and concerns specific to cyber investigations
- Explain personality traits and skill sets to be considered for the recruitment and retention of CIU personnel

Online 30 hours over 3 weeks

None

None

Back to top

NIB

Network Intrusions Basics

CORE

This course provides core knowledge needed to perform a network investigation. Students learn the language of intrusions and explore network fundamentals, including network architecture. The concepts presented in this course prepare students for additional network investigations courses.

Course Objectives

- Classify network intrusion elements
- Give examples of artifacts related to network intrusions
- Explain the basics of networking and network architecture

Online 10 hours; self-paced

None

None

Back to top

NMAP

Network Mapper

CORE

This course provides instruction in using Network Mapper (Nmap) to manage vulnerabilities, verify baseline configuration compliance, and identify risk among communication protocols, data services, and associated ports. 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.

Course Objectives

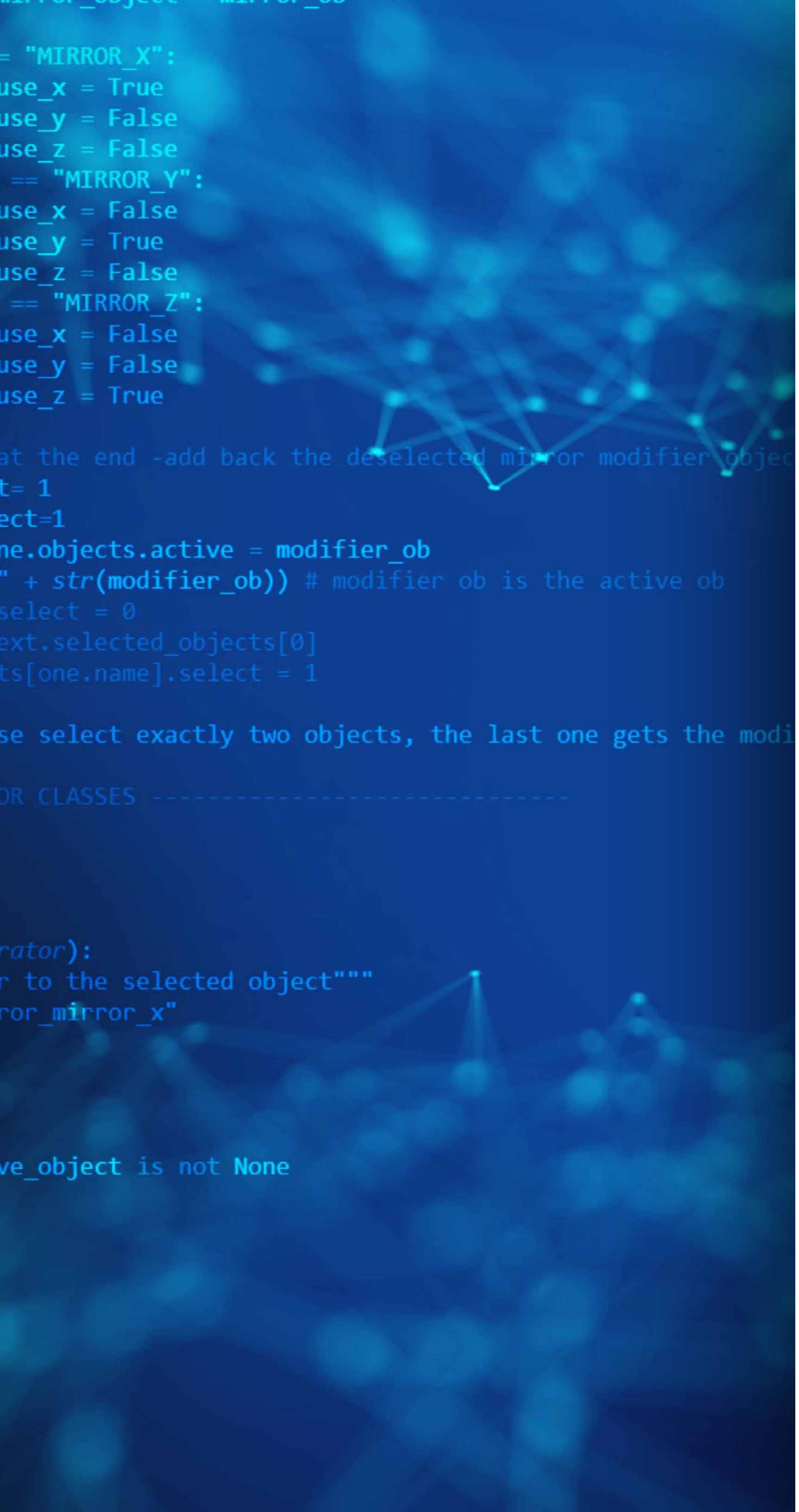
- Install Nmap in a Windows and Linux environment
- Determine what hosts, ports, and services are available on a network
- Determine what operating systems, applications, and devices are running on a network

Online 8 hours

INCH

None

Back to top



NTC
Network Traffic Collection

INTERMEDIATE

This course prepares students to strategically place a monitoring sensor on a network to capture traffic to and from a specific host. 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.

Course Objectives

- Explain basic theory, technologies, and components that facilitate network data transmission
- Examine network traffic and previously captured data
- Perform a logical and physical assessment of a network to identify potential witness devices and the data they contain
- Assess a network and configure and place a network monitoring sensor
- Configure network data acquisition tools
- Use common internet research utilities
- Explain a network monitoring system in a wireless environment
- Analyze network traffic and system artifacts to identify probing and intrusion techniques

In Residence 40 hours over 5 days
Instructor-led Virtual 40 hours over 5 days

CIRC

None

Back to top

OPV

OpenVAS

CORE

This course provides instruction in using OpenVAS software to run vulnerability scans, generate reports, and analyze the results. Students install OpenVAS using the command line and operate the Greenbone Security Assistant interface to navigate and customize the software. Practical exercises train students on OpenVAS terminology and techniques.

Course Objectives

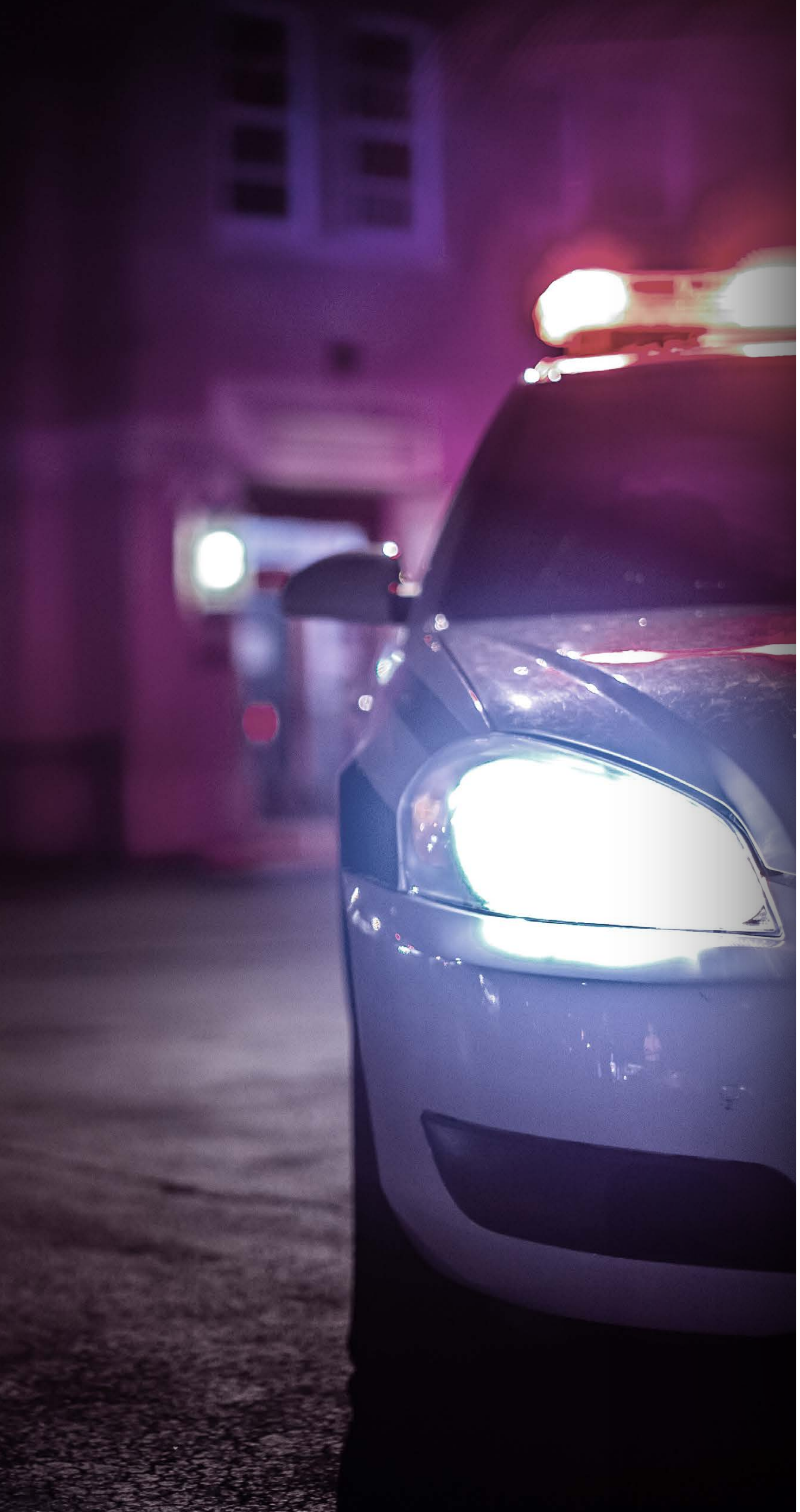
- Install OpenVAS software successfully in a Linux environment
- Run an OpenVAS "quick start" vulnerability scan utilizing the Greenbone Security Assistant interface
- Configure the target, parameters, and breadth of an OpenVAS custom vulnerability scan based on a scenario
- Assess the vulnerability risks to a system and possible remediation based on the results of an OpenVAS report generated from a custom vulnerability scan

Online 8 hours

None

None

Back to top



TEDA

Technology Evidence in Domestic Abuse

INTERMEDIATE

This course provides an overview of the role that technology can play in domestic abuse and in domestic violence cases for military first responders. The course introduces critical concepts on the intersection of technology and domestic abuse, such as how abuse manifests, underlying dynamics of abuse, signs of escalation, relevant UCMJ articles and DoD policies, as well as industry standards for the collection of digital evidence.

Course Objectives

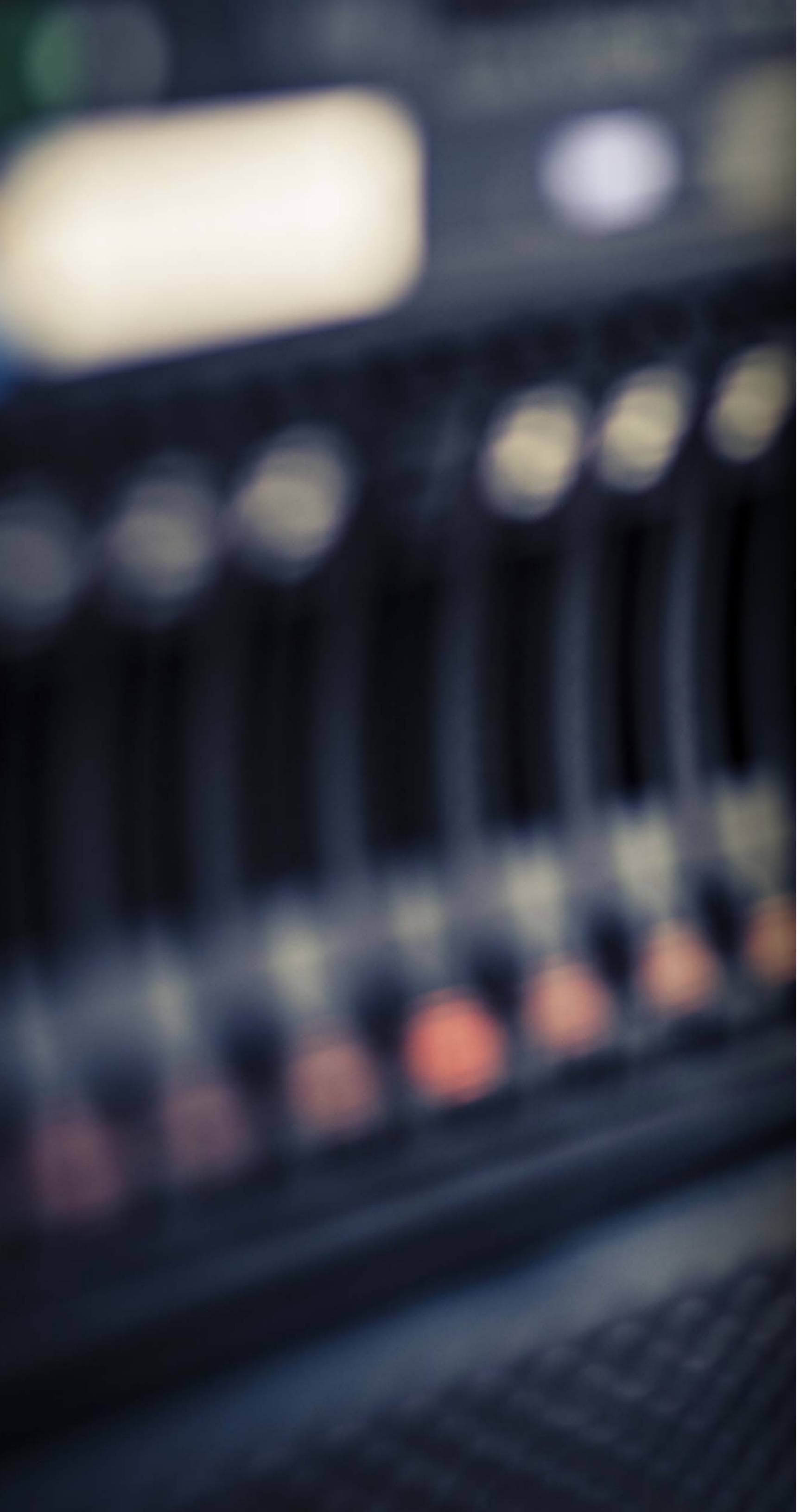
- Describe the fundamentals of domestic abuse and provide examples of abuse tactics through technology (for example, a threatening text; spoofing; hacking into IoT devices or victim email, social media accounts)
- Categorize abuser behaviors, including with technology, that indicate increased risk of escalation and violence (for example, cyberstalking)
- Select the applicable military law and DoD policy concerning abuse
- Evaluate a situation and perform necessary actions in accordance with best practices

Online 90 minutes

None

None

Back to top



WFE-E

Windows Forensic Examinations - EnCase

INTERMEDIATE

This course builds on the Cyber Incident Response Course (CIRC). WFE-E presents a comprehensive forensic examination process, including technical procedures and reporting. Students use the EnCase forensic tool to conduct thorough examinations of Windows systems.

Course Objectives

- Conduct a forensic examination of a Windows operating system image in a lawful manner
- List the recommended specifications for a forensic workstation
- Demonstrate the basic functions, configurations, outputs, tools, and settings of EnCase
- Examine a forensic image from a Windows computer using basic forensic processes and automated tools in EnCase
- Use Password Recovery Toolkit (PRTK) to defeat protected files
- Produce examiner’s notes

In Residence 40 hours over 5 days
Online 40 hours over 4 weeks
Instructor-led Virtual 40 hours over 5 days

CIRC

IACET CEU-eligible 4.0 CEUs

Back to top

DC3 Cyber Training Academy Student Grievance Process

For all non-school-related issues:
Students should use their military chain of command through their service's detachment leadership.

For all schoolhouse-related issues:
Students should follow the process described below: Most student complaints/grievances can be resolved informally by discussing the matter with the instructor. If a student's complaint cannot be resolved informally by working with the instructor, the student may submit a written description of the issue, along with supporting documentation (if applicable) to the CTA Registrar (CTA.Registrar@dcita.edu).

DC3 Cyber Training Academy will examine the submission, consult with the DC3 CTA Cyber Training Operations Lead, and provide an appropriate response and a written description of the resolution.

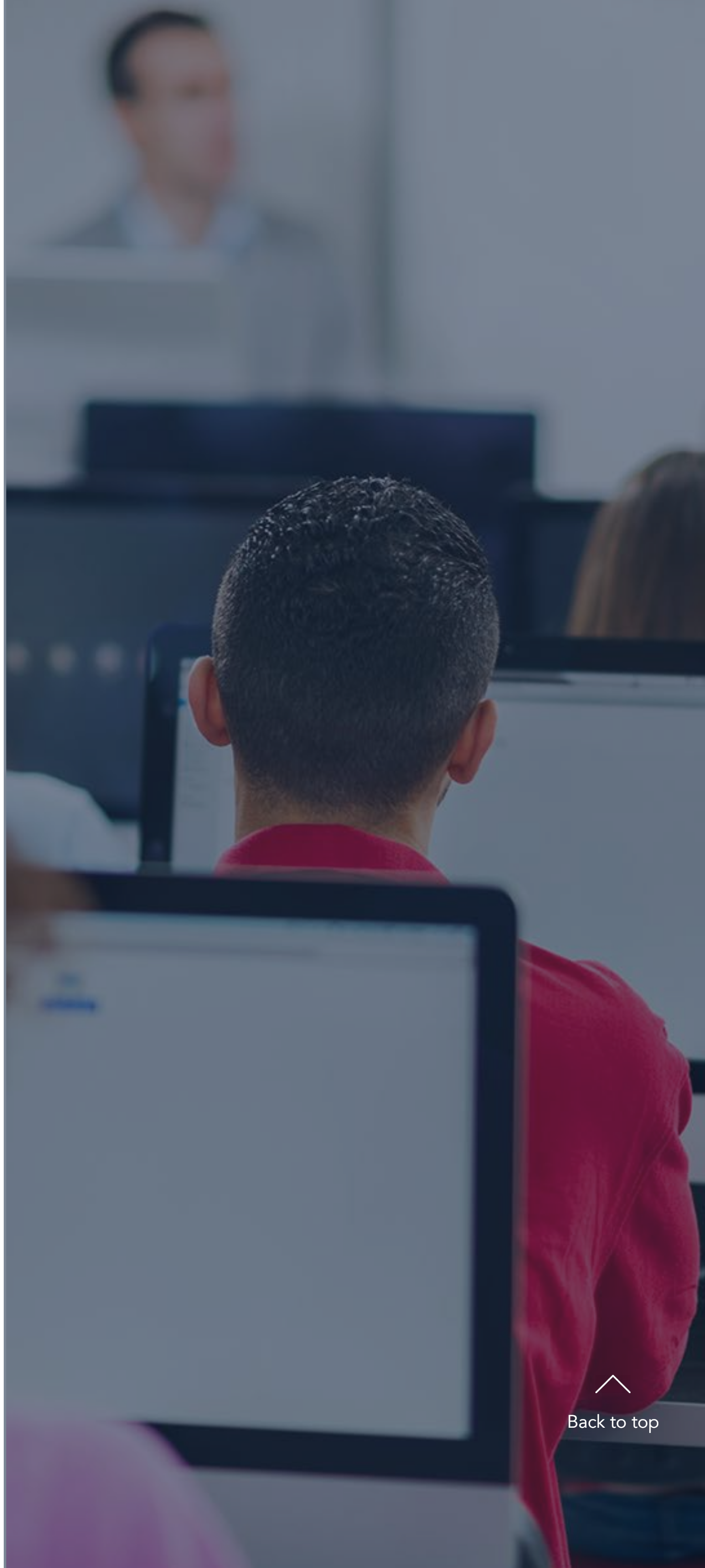
If the response is not satisfactory to the student, the student may petition the DC3 Cyber Training Academy Director for review and/or possible investigation.

The DC3 Cyber Training Academy Director would then examine the submission and provide an appropriate response and a written description of the resolution. All decisions by the DC3 Cyber Training Academy Director are final.

While the appeals and grievance decisions of the Academy are final, students may inform our accrediting agency, the Council on Occupational Education (COE), at the address below if they feel their issues are not satisfactorily resolved:

Council on Occupational Education (COE)
7840 Roswell Road
Building 300, Suite 325
Atlanta, GA 30350
Telephone: (800) 917-2081

For information on the Academy's behavior and conduct standards, please review the Standards of Behavior and Conduct standard operating procedure.



Back to top

DC3 Cyber Training Academy

CONTACT

learn.dcita.edu

443-733-1990

CTA.Registrar@dcita.edu

ADDRESS

DC3 Cyber Training Academy
7740 Milestone Parkway, Suite 400
Hanover, MD 21076