Cyber Crime Technology (CCT)

CCT 8240. ACE Prep Part 1. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
This class is part 1 of the AccessData Certified Examiner (A.C.E) certification training.

CCT 8241. ACE Prep Part 2. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
This class is Part 2 of the A.C.E. certification training.

CCT 8242. Accelerated ACE Prep. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The Accelerated AccessData Certified Examiner class provides the knowledge and skills necessary to install, configure and effectively use FTK Imager, Forensic Toolkit, Password Recovery Toolkit, Registry Viewer. Participants will also use AccessData products to conduct forensic investigations on various systems and locate forensic artifacts. This course operates under a shorter time frame to allow a more expeditious complete of the ACE certification.

CCT 8251. Internet Forensics 1. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8251 course is intended to build on the knowledge acquired by students in the digital forensics program. Part 1 of this 3 part course focuses on the recovery of digital artifacts left behind during the use of common web browsers and other internet enabled applications. The course will teach students how to recover, interpret, and report internet evidence.
Prerequisites: Take CCT 240 or CCT 241

CCT 8252. Internet Forensics 2. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8252 course is intended to build on the knowledge acquired by students in the digital forensics program. Part 2 of this 3 part course focuses on the discovery and documentation of digital artifacts left behind during the use of today's popular internet enabled applications. The course will teach students how to recover, interpret, and report internet evidence.
Prerequisites: Take CCT 8251 with a minimum grade of S

CCT 8253. Internet Forensics 3. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8253 course is intended to build on the knowledge acquired by students in the digital forensics program. Part 3 of this 3 part course focuses on the discovery and documentation of digital artifacts left behind during the use of today's popular web browsers and internet enabled applications. The course will give students the ability to practice recovering, interpreting, and reporting of internet evidence.
Prerequisites: Take CCT 8252 with a minimum grade of S

CCT 8261. Mobile Device Forensics 1. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8261 course is part one of the Mobile Devices course series intended to build on the knowledge acquired by students throughout the digital forensics program. The series focuses on the discovery and documentation of digital artifacts from today's mobile devices. The course series will teach students how to recover, interpret, and report evidence.

CCT 8262. Mobile Device Forensics 2. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8262 course is part two of the Mobile Devices course series intended to build on the knowledge acquired by students throughout the digital forensics program. The series focuses on the discovery and documentation of digital artifacts from today's mobile devices. The course series will teach students how to recover, interpret, and report evidence.

CCT 8263. Mobile Device Forensics 3. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8263 course is part three of the Mobile Devices course series intended to build on the knowledge acquired by students throughout the digital forensics program. The series focuses on the discovery and documentation of digital artifacts from today's mobile devices. The course series will teach students how to recover, interpret, and report evidence.

CCT 8271. Mac Forensics Module 1. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
This course is the first of a three-part series of Macintosh forensics. This first module introduces the Apple Mac OS X user interface and operating/file system function. Topics include OS X interface basics such as using Finder, creating user accounts, using File Vault and installing/uninstalling applications. GPT disk structure and date and time acquisition will be covered along with the extensible firmware interface.

CCT 8272. Mac Forensics Module 2. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
This course is the second of a three-part series on Macintosh forensics. This second module introduces the steps taken to image a Mac from static to live Linux CD acquisitions. This module also covers finding evidence in the directory structure in addition to recovering user logon passwords. Specific Mac application artifacts will be covered from Safari, iChat and Apple Mail.

CCT 8273. Mac Forensics Module 3. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
This course is the third of a three-part series on Macintosh forensics. This final module ties together the knowledge obtained from the prior classes in a practical assessment.

CCT 8274. Applied Decryption and Advanced Password Recovery I. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8274 course is the first of a three part series of Applied Decryption and Advanced Password Recovery. This first module introduces the theory of applied decryption. Topics include the history of encryption, the complexity of algorithms, and advanced concepts such as hashing, salting, and encryption enhancing features. We will cover all of the basic and advanced password encryption and hashing algorithms as well as learn about the people responsible for developing them.

CCT 8275. Applied Decryption and Advanced Password Recovery II. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8275 course is the second of a three part series of Applied Decryption and Advanced Password Recovery. This module introduces the tools necessary in applied decryption. Topics include the difference between dictionary attacks, brute-force attacks, and rainbow tables. The use of advanced decryption tools such as PRTK, Passware, Aircrack, and SSLStrip.
CCT 8276. Applied Decryption and Advanced Password Recovery III. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8276 course is the third of a three part series of Applied Decryption and Advanced Password Recovery. This module combines the theory and the practical application of applied decryption. Topics include decrypting password hashes, decrypting salted password hashes, decrypting wireless encryption, and decrypting common network encryption.

CCT 8277. Distributed Processing Module 1. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
Distributed Processing Module 1 is the first of a 3 part sequence that allows users to leverage the processing power of multiple computers to process and index massive volumes of digital evidence faster than any other solution available today. When analyzing digital evidence, investigators must process the captured data to break out compound files and index documents and email, so they can be searched effectively. Distributed Processing can leverage up to four processing workers, one on the local examiner computer and three distributed computers. This allows them process terabytes of computer evidence in a fraction of the time it would take normally.

CCT 8278. Distributed Processing Module 2. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
Distributed Processing Module 2 is the second of a three part sequence that allows users to leverage the processing power of multiple computers to process and index massive volumes of digital evidence faster than any other solution available today. When analyzing digital evidence, investigators must process the captured data to break out compound files and index documents and email, so they can be searched effectively. Distributed Processing can leverage up to four processing workers, one on the local examiner computer and three distributed computers. This allows them process terabytes of computer evidence in a fraction of the time it would take normally.

CCT 8279. Distributed Processing Module 3. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
Distributed Processing Module 3 is the third of a three part sequence that allows users to leverage the processing power of multiple computers to process and index massive volumes of digital evidence faster than any other solution available today. When analyzing digital evidence, investigators must process the captured data to break out compound files and index documents and email, so they can be searched effectively. Distributed Processing can leverage up to four processing workers, one on the local examiner computer and three distributed computers. This allows them process terabytes of computer evidence in a fraction of the time it would take normally.

CCT 8280. Data Recovery Techniques. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The accelerated CCT8280 course introduces the unique skills and methodologies necessary to assist in the investigation and prosecution of cyber crimes. Topics include hardware and software issues, recovering erased files, overcoming encryption, advanced imaging, transient data, internet issues and testimony considerations.

CCT 8299. Combined Distributed Processing Module 1. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
Distributed Processing allows users to leverage the processing power of multiple computers to process and index massive volumes of digital evidence faster than any other solution available today. When analyzing digital evidence, investigators must process the captured data to break out compound files and index documents and email, so they can be searched effectively. Distributed Processing can leverage up to four processing workers, one on the local examiner computer and three distributed computers. This allows them to process terabytes of computer evidence in a fraction of the time it would take normally.

CCT 8371. Registry Forensics 1. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8371 course is the first of a three-part series on Windows Registry Forensics. This first module introduces the Windows Registry in various versions of Microsoft Windows systems. Topics include static and dynamic registry files, registry hives and structure and operating system specific implementations. Students will utilize registry specific tools to view registry files in the file system.

CCT 8372. Registry Forensics 2. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8372 course is the second of a three-part series on Windows Registry Forensics. This second module introduces specific evidentiary artifacts located in the Windows Registry and how to obtain registry files from a static or live acquisition. This module covers the artifacts located within the five key registry files of Window XP and subsequent Microsoft operating system as well as the two key registry files of the Windows 9x operating systems.
Prerequisites: Take CCT 8371 with a minimum grade of S

CCT 8373. Registry Forensics 3. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
The CCT8373 course is the third of a three-part series on Windows Registry Forensics. This final module ties together the knowledge obtained from the prior classes in a practical assessment.
Prerequisites: Take CCT 8373 with a minimum grade of S

CCT 8400. Access Data Forensics. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
This course explores the installation, configuration and operational use of the Forensic Tool Kit 5.X software family. Upon completion of this course, the student should be able to competently perform the Access Data Certified Professional examination. Suggested prior experience or training: Basic Digital Forensics Training and 1 year experience in a Digital Forensics environment. CompTIA A+ or equivalent computer hardware and software skills. Suggested prior coursework from CPCC: CTI-130 OS and Device foundations CCT-121 Computer Crime Investigations Class Contact Hours: 60 hours; 30 hours seated "in person" instruction and 30 hours online self-paced content. Course Text: Supplied by Division Title: Access Data Forensics; Academic Edition Training Manual.

CCT 8410. En case Digital Forensics. 0.0 Hours. Class-440.0. Clinical-0.0. Lab-0.0. Work-0.0
This course explores the operational use of the En case 8.xx software product. Upon completion of this course, the student should be able to competitively perform a basic forensics examination using En case.