College Based Online Training

CompuForensics, in association with fully accredited state universities and colleges, offers the government and private sectors a highly cost effective approach to upgrading the technical skills of their investigative, intelligence and support personnel. As a pioneer in federal law enforcement computer forensics and Internet crime investigations with over a quarter century of federal law enforcement experience, culminating in the development and management of a national agency computer forensics program, the lead forensics instructor brings an insightful approach second to none.

'Live' - Not Just A Correspondence Course

Unlike traditional correspondence courses, our online training is live. That is, an instructor is available during each block of instruction via Skype teleconferencing software. Lectures and laboratories are augmented by Power Point multimedia presentations hosted by password protected high speed XML web sites (CompuPic.Net or alternate web site). The below left graphic depicts a student audio/video computer desktop. Skype audio is augmented by the multimedia Power Point presentation running in Internet Explorer.

Our college based real world computer forensics training is designed

for busy professionals. Training occurs during the afternoon or evening with an option for telephonic participation when unforeseen circumstances mandate. Class size is limited to afford increased interaction between the instructor and students.

Continental US and Canadian Examiner students have the option of using any cellular or hard wired telephone when unavoidably away from their audio/video communications computer. Long distance telephone calls are initiated via Skype by the instructor.

Instructor audio is saved for later use with multimedia web sites by students who missed live sessions. Said participation does not, however, count toward the 70% attendance required for successful course completion.

The 12-week Computer Forensics Examiner classes occur Monday through Thursday. Afternoon classes are held from noon to 2:10 p.m. and evening classes from 6-8:10 p.m.; all times are US Central. The 3 -week Mac Analysis Using Linux classes occur Monday through Thursday from 6-8:00 p.m. Central. The 12-week course is eligible for both WIA and VA grants as well as substantial computer forensics hardware and software educational discounts.

Online Forensics Examiner Instructor

The instructor possesses professional training and experience second to none. Possessing bachelor and masters university degrees, the instructor additionally attended special agent academies for the Department of the Treasury, US Customs Service, Naval Criminal Investigative Service and USAF Office of Special Investigations. Applicable technical training was principally hosted by the Treasury Department and Central Intelligence Agency. A former field grade intelligence officer with the USAF and US Army, he is a decorated Vietnam air combat veteran. Retiring at age 53 with a quarter century of federal law enforcement experience, he served as field agent, agent supervisor and headquarters staff, including service as a national program manager for computer forensics. In addition to well over a decade of US Government computer forensics experience, he has taught computer forensics since 1999 at universities.

Real World Computer Forensics Training

Prerequisites and Resources

Student Background

All online students should be fluent in English. All lectures, laboratories and videos are provided solely in English. The online format does not lend itself well to those with hearing or sight disabilities.

Twelve week examiner students should minimally have prior experience in loading the Microsoft Windows XP operating system and applications, copying/moving/linking files using Windows Explorer, and be familiar with the use of classic menu options under XP. Prior use of basic Command Prompt utilities such as format, change directory, rename, delete and copy is also required. A+ or comparable computer hardware background is minimally desirable. Prior experience with Linux or computer forensics is not required.

12-Week Examiner Computer System Requirements

Audio Headset - Use of an ear phone with an integrated microphone is required to avoid background noise and echo effects. Suitable head phones with integrated microphones are widely available for as little as $20. Student microphones should be muted when not used for talking.

Audio/Video Computer - A laptop, desktop or tower computer running Skype is recommended. Our new Flash implemented Power Point presentation interface should be compatible with all major browsers. Skype teleconferencing software is available for Windows, Macintosh and Linux operating systems. Download a free copy of Skype from www.Skype.com. GoToMeeting may replace Skype in some instances.

Exercise Computer - Since the Examiner course involves some rebooting during online laboratory sessions, simultaneous use of a separate forensic exercise computer is recommended. The exercise computer should be minimally equipped with a DVD-ROM bootable drive. The exercise computer should minimally be configured with a Pentium IV or equivalent processor running at 1.6 GHz or faster, 512 megabytes of RAM (Random Access Memory) and 30 gigabytes of free hard disk capacity. Use of RAID or unusually large drives is not recommended. While the exercise computer can be a notebook, use of a desktop or tower with at least one available removable drive bay is preferred for those intending to use their exercise computer to do computer forensics analysis at the conclusion of the course. The exercise computer should contain Windows XP (Vista or Windows 7 can be used with the understanding that some Windows

forensic utilities may not be fully supported). OpenSuSE 11.1 Linux will be installed during the initial weeks of the course. Code Weavers Crossover will be used to run Windows applications under Linux. Use of a virtual exercise computer on the Audio/Video Computer in lieu of a separate exercise computer is authorized with the understanding that limited support for virtual operating environments is provided. VMWare Workstation and Player, as well as Oracle's Virtual Box, have been used successfully by students.

Exercise Software - Required preliminary and comprehensive forensic exercise images are available in Norton Ghost, Safeback 3.0, WinHex and Active Disk Image formats. If used, Norton Ghost should be 2001, 2002 or 2003; Ghost 10 is the last version to include Ghost 2003. Possession of a personal or higher licensed version of WinHex disk editor is recommended for the course; the specialist or higher license is recommended for those intending to do forensics after the course. A personal license copy (about $50 US) will support most WinHex instruction requirements. The trial ware version of WinHex can be used with the understanding that several of the WinHex exercises will not be supported. Students should additionally possess a bootable Knoppix 5.1.1 CD-ROM; download links for Knoppix 5.1.1 and OpenSuSE 11.1 are available at CompuForensics.com.

12-Week Examiner Course Resources

Students are provided a NIJ Mock Trial DVD and CompuForensics bootable CD-ROM by US Mail. The NIJ DVD is also provided students in the Court/Legal issues sub-course, which is a part of the 100-hour 12 week Examiner course. The bootable CD-ROM contains software and instructional material relating to the analysis of Windows computers.

Students having attended at least 70% of scheduled classes and satisfactorily completing a case based comprehensive exercise are issued a college certificate of completion signed by a college dean or comparable official. Successful completion also results in the award of 10 continuing education units. Some students may have the option of using the participating school's laboratory computers; in such instances, school laboratory fees are likely to apply. As in conventional classroom instruction, registration and tuition is handled by the hosting university or college.

The online forensics examiner course syllabus includes essential and most popular components of previously offered 6-day Examiner Basic and 5-day Examiner Advanced courses. Although a few hours longer than the replaced Basic and Advanced courses combined, course tuition is a

quarter that of replaced on-campus courses; **$2995 Savings**.

Examiner 100-hour Course - $995

1st Week - System Preparation & Overview
Using VOIP & CompuPic Video Site
Exercise Computer Compatibility
Forensic Workstation(s) Configuration
Preliminary & In Depth Analysis
Examiner CD-ROM Content Review

2nd Week - Searches & Business Issues
Preparing for a Computer Search
On-site Computer Search Guidelines
On-site UNIX & Linux System Searches
Forensic Staffing & Employment
Marketing & Business Considerations
Peer Certification & Licensing Issues

3rd Week - Linux/Windows Installation
OpenSuSE 11.1 Installation
Linux Distributions & File Control Systems
KDE GUI Information & YaST Navigation
Linux Desktop Configuration
Code Weavers CrossOver

4th Week - Evidence Handling & Disk Imaging
Computer Evidence Handling & Documentation
Restored Evidence Drive Preparation
System Backup Imaging Laboratory
Exercise Image Restoration Laboratory
Safeback, WinHex & Linux DD Imaging

5th Week - DOS/Windows Forensic Utilities
DOS Analysis Tools Laboratory
Access Data's Forensic Tool Kit & Laboratory
Xways' WinHex Disk Editor & Laboratory
Quick View Plus Laboratory

6th Week - Computer Hardware & OS Basics
Microcomputer Fundamentals
Floppies, Disk Platters & External Storage
DOS to Windows 8 Analysis Fundamentals
Local & Wide Area Network Fundamentals

7th Week - Hidden Data & Encryption
Hidden Data & Steganography
Steganography Laboratory
Encryption Laboratory
Decryption Laboratory
Erased File Recovery Laboratory

8th Week - Linux Analysis of Windows
Linux OS Command Line & GUI Laboratory
Target System Documentation Laboratory
Internet Activity Reconstruction
Shell Scripts & Compiling Source Code
Linux Screen Capture & Graphics Editing

9th Week - Comprehensive Exercise
Comprehensive Exercise Partition Preparation
Exercise Image Restoration & Documentation
Court Exhibit Preparation Techniques
Realistic Criminal Case Analysis
Discussion of Exercise Findings

10th Week - Technical Investigative Report
Technical Investigative Report Overview
Predication/Synopsis & Attachments
Evidence Receipt & Image Restoration Paragraphs
Witness & Suspect Interview Paragraphs
Forensic Disk Analysis Paragraphs

11th Week - Internet Investigations
Internet, UseNet & Internet Relay Chat
Internet Sources of Information
Hacker Profile Analysis
E-mail Header Analysis
Child Pornography Investigations
Pedophile/Stalker Analysis

12th Week - Court/Legal Issues
Fourth Amendment - Search & Seizure
Federal Rules of Criminal/Civil Procedure
Court Legal Precedence
Preliminary Hearings & Disclosure
Courtroom Demeanor & Expert Testimony

Real World Computer Forensics Training

Consult www.CompuForensics.com for locations and class dates.
© CompuForensics 1999-2012

Court/Legal Issues 8.5 Hour Course $135

The twelfth and final week of the 100-hour examiner course is also available as a separate course. No prerequisites are required for this sub-course, which is held during the last week of the scheduled Examiner afternoon and evening courses. Classes are held Monday through Thursday. Afternoon classes meet from noon to 2:10 p.m. Evening classes meet from 6:00 to 8:10 p.m. All times are US Central; daylight saving time may apply. Students receive the NIJ Mock Trial DVD by US Mail. A web cam is recommended for use during the last day of class.

Fourth Amendment - Search & Seizure
Federal Rules of Criminal/Civil Procedure
Court Legal Precedence
Preliminary Hearings & Disclosure
Courtroom Demeanor & Expert Testimony

Mac Analysis Using Linux $349

The 100-hour 12-week live on-line Computer Forensics Examiner course provides computer professionals with the training needed to begin performing Windows computer forensics; Linux and Windows, including WinHex and FTK, are employed. The newly introduced 24-hour 3-week live on-line Mac Analysis Using Linux course expands forensic examiner skills to include Apple computers. Both courses require A+ or comparable computer literacy. Those enrolling in the Mac forensics course should have additionally taken or plan to take the 12-week examiner course (or comparable training); the 12-week course includes forensic instruction applicable to both Windows and Mac platforms, including 8.5 hours of legal and courtroom instruction needed for licensing in some states.

Topics
Introduction/Overview
Mac Forensics Platform
Mac Forensics Software
Mac Hardware Systems
Mac Operating Systems
HFS & HFS Plus File Systems
Mac System Field Analysis
Forensic Disk Imaging Lab
Raw Image Restoration Lab
Image Documentation Lab
WiebeTech Ultra Dock Lab
GUI Utilities Lab
Command Line Utilities Lab
Mac File Recovery Lab
Mac Encryption/Decryption
Comprehensive Exercise
Exercise Findings/Exhibits

For information, contact CompuForensics by e-mail at info@ugov.net or call 931-287-9009.

For Enrollment and Tuition, contact participating universities and colleges. A current campus listing can be found at www.CompuForensics.com.