

College Based On-line 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 on-line 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 XGov.Org). The below left graphic depicts a student audio/video computer desktop. Skype audio is augmented by the multimedia PowerPoint presentation running in Internet Explorer.

Our college based real world computer forensics training is designed



for busy professionals. Training occurs during the 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 on Monday, Wednesday and Friday evenings from 7-9 p.m., Central time. Other courses occur during the same time frame on Tuesdays and Thursdays.

On-line Forensics Examiner Instructor

Pictured in casual attire suitable to his current semi-retirement in rural Tennessee, 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 seven regionally accredited universities or colleges in the Midwest and South.



Prerequisites and Resources

Student Background

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

Twelve week examiner students should minimally have prior experience in loading Microsoft Windows operating systems and applications as well as copying/moving/linking files using Windows Explorer. 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. Students should additionally be able to re-size, delete and create logical partitions. 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.

Communications Computer - Notebook, desktop or tower computer running Microsoft Internet Explorer 6+ and Skype 4+ is recommended. Use of non-Microsoft Windows XP, Vista or Windows 7 personal computers may preclude optimum use of the web based Power Point presentations. 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 on-line laboratory sessions, simultaneous use of a separate forensic exercise computer is recommended, albeit not required. The exercise computer must be minimally equipped with a DVD-ROM bootable drive. The exercise computer should minimally be configured with a Pentium IV or equivalent processor, 512MB of RAM (Random Access Memory) and 20GB of free hard disk capacity on a single drive. 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 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). CodeWeavers Crossover, a commercial implementation of Wine, will also be used to run Windows applications under Linux.

The use of virtualization software on the communications computer in lieu of a physical exercise computer may be an option for some. Students electing to run OpenSuSE Linux inside of Windows on the communications computer in lieu of a separate exercise computer should do so with the following understandings: classroom instruction is oriented to the use of a separate exercise computer and assistance in the use of virtualized systems is limited; a separate forensics (exercise) computer is required to accomplish computer forensics for hire at the conclusion of the course; SuSE Linux running in a virtualized session within the communications computer must be able to directly access a 243MB FAT16 exercise partition; and virtualization use mandates the availability of increased hard disk, memory and processor resources on the communications computer.

Exercise Software - Required preliminary and comprehensive forensic exercise images are available in Norton Ghost GHO, Safeback, WinHex and Active@ DiskImage (Version 2 for DOS) formats. If used, Norton Ghost should be 2001, 2002 or 2003; Ghost 10 is the last version to include Ghost 2003. Possession of a specialist or forensics licensed version of WinHex disk editor is recommended, especially for those intending to do forensics after the course. A personal license copy will support most course requirements. The WinHex disk editor is available for purchase or evaluation download at www.WinHex.com.

12-Week Examiner Course Resources

Students are provided illustrated loose-leaf study notebook inserts, a SuSE 11.x 32bit DVDROM and CompuForensics DOS bootable CD-ROM with NTFS and FAT support (contains software supporting DOS, Windows and Linux based 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 higher official. Successful completion also results in the award of 7.5 continuing education units. Some students may have the option of using the participating universities laboratory computers; in such instances, university laboratory fees are likely to apply. As in conventional classroom instruction, registration and tuition is handled by the hosting university.

The Forensics Examiner course syllabus includes essential and most popular components of previously offered on-campus 6-day Examiner

Basic and 5-day Examiner Advanced courses. **You save \$2995.**

Examiner 75-hour Course - \$995

1st Week - System Preparation

Using VOIP & CompuPic Video Site
Floppy/Zip Media & Key Disk Preparation
Exercise Computer Compatibility

2nd Week - Searches & Legal Issues

Preparing for a Computer Search
On-site Computer Search Guidelines
On-site UNIX & Linux System Searches
Certification, Licensing & Legal Issues

3rd Week - Linux Installation & Use

SuSE Open Linux 11.x Installation
Understanding the Linux File System
KDE GUI Information & YaST Navigation
Linux Desktop Configuration
CodeWeavers 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 Utilities

Access Data's Forensic Toolkit (FTK)
Maresware Analysis Tools Laboratory
Erased File Restoration Laboratory
Quick View Plus Laboratory
Windows Screen Capture/Editing

6th Week - OS Basics & Forensic Hardware

Microcomputer Fundamentals
DOS to Windows 7 Analysis Fundamentals
Windows File Control System Fundamentals
Local & Wide Area Network Fundamentals
Deployment Kit & Workstation Configuration
External Storage Alternatives

7th Week - Hidden Data & Encryption

Hidden Data & Steganography
Steganography Laboratory
WinHex Disk Editor Laboratory
Password Encryption/Decryption

8th Week - Linux Analysis of Windows

Linux System Command Line Laboratory
Linux System GUI Application Laboratory
Linux GUI Analysis Tools Laboratory
Other Non-Linux OS Analysis Tools
Documentation Laboratory
Internet Activity Reconstruction

9th Week - Additional Forensic Resources

Examiner CD-ROM Content Review
Shell Scripts & Compiling Source Code
Linux Screen Capture & Graphics Editing
In-depth Analysis Considerations
Forensic Unit Personnel Staffing
Marketing & Business Considerations

10th Week - Comprehensive Exercise

Comprehensive Exercise Partition Preparation
Exercise Image Restoration & Documentation
Forensic Case Analysis
Discussion of Exercise Findings

11th Week - Technical Investigative Report

Technical Report/Courtroom Testimony Overview
Evidence Receipt & Image Restoration Paragraphs
Witness & Suspect Interview Paragraphs
Forensic Disk Analysis Paragraphs

12th Week - Internet Investigations

Introduction to the Internet
Internet Sources of Information
Hacker Profile Analysis
E-mail Header Analysis
Pedophile/Stalker Analysis
Predication/Synopsis & Attachments

Legal Issues 40 Hour Course - \$795

The Forensics Examiner Legal Issues Course is taught on Tuesday and Thursday evenings from 7:00-9:00 p.m. Central. The course is taught by retired federal agents with decades of criminal investigative experience and hundreds of hours of courtroom experience. The courtroom laboratory instructor is also a practicing attorney in Texas. Voice Over Internet Protocol (VOIP) audio conferencing will utilize GoToMeeting. Lecture and video visual effects will be supported by an on-line Power Point presentation website which requires use of Internet Explorer 6 or later. The National Institute of Justice Mock Trial DVD (among issued materials) and other Department of Justice resources are employed.

1st Block - Introduction & Legal Concepts

Using VOIP & CompuPic Video Site
American Legal System Dark Realities
Constitutional Law - Fourth Amendment
Rule 41, Federal Rules of Criminal Seizure

2nd Block - Warrants & Consent Searches

Searches Without a Warrant
Probable Cause & Search Affidavits
Warrant Based Searches
Private/Government Workplace Searches

3rd Block - Linux/Windows Installation

Major Federal Statutes
State & Local Statutes
Court Legal Precedence
State Forensic Examiner Licensing

4th Block - Courtroom Testimony

Forensic Examiner Ethics
Admissability of Evidence
Expert Testimony
Verbal & Non-verbal Witness Tactics

5th Block - Courtroom Laboratory

Pretrial Hearings
Initial Expert Testimony
Cross Examination
Peer Review

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.