

Forensic Computer Examiner Certification Training

222 hours

Course Overview/Description

This is a rewarding but challenging program. To better prepare you to take the course, we have included three required short online courses: Basic CompTIA A+, Network+ and Security+ Certification Prep courses at no extra charge. The forensic computer examiner field has grown tremendously in the past few years. For many years, law enforcement officers have been the primary forensic computer examiners, however, as criminal defense attorneys, and later civil attorneys, encountered the law-enforcement examiners, the need for qualified civilian forensic computer examiners grew. Currently, there is a huge demand for certified, qualified forensic computer examiners. Some trained examiners have started their own businesses, some work for large companies, such as Deloitte and Touche, and others work for law-enforcement agencies.

This comprehensive online program prepares individuals for a career in this emerging field. Through this training, students learn to retrieve evidence and prepare reports, based on that evidence, which will stand up in a court of law. A section on the ethics of computer forensics and on the preparation and analysis of investigation results is also included.

This program is hands-on and emphasizes “learning by doing.” The primary certification for civilian forensic computer examiners is the Certified Computer Examiner (CCE®) certification. The online Forensic Computer Examiner program is an authorized CCE training course and thoroughly prepares students to take the CCE certification exam.

Obtaining a quality forensic computer-examiner education is the best way to prepare for the profession. This online, self-paced program prepares students for CCE certification. Students will be paired with an instructor for one-on-one assistance.

Course Objectives

After successful completion of the Forensic Computer Examiner online program, students will:

- Understand what makes an examiner a good examiner.
- Be able to explain to clients why trained forensic examiners should be used.
- Understand what a forensic examiner may expect to encounter during an examination.
- Understand software licensing and how it affects forensic examiners.
- Understand forensic ethical standards as they apply to forensic examiners.
- Understand basic forensic examination procedures.
- Be able to prepare and verify forensically sterile examination media.

- Understand the importance and methodology of note taking and reports.
- Understand basic PC hardware identification.
- Have a basic understanding of the legal privacy issues relating to the examination of magnetic media.
- Understand when a legal opinion may be necessary to prevent privacy issues from interfering with the examination or causing a valid lawsuit.
- Have a basic understanding of how to properly acquire, collect, or seize magnetic media.
- Understand how to properly establish and maintain the physical "chain of custody" of media and evidence.
- Make exact forensic copies of original floppy-diskette media.
- Understand the logical structures of DOS and Windows 95/98
- Understand where the creation and modification dates and times are stored in a directory entry.
- Understand the significance of the creation and modification dates and times.
- Understand how to recover data from unallocated space.
- Understand and explain how files are created.
- Understand and explain what happens when a file is deleted.
- Understand, explain and manually recover DOS legal single and multiple cluster deleted files.
- Understand, explain and manually recover DOS legal multiple cluster fragmented deleted files.
- Understand how to determine the Last Accessed Date and the Modification Date and Time, their significance and when they are modified.
- Understand how Windows long file names are stored, what happens when they are deleted and how to restore long file names.
- Understand how sub-directories are stored, what happens when they are deleted and how to recover deleted sub-directories.
- Understand what happens when a diskette or hard-disk drive is formatted and how to recover files, sub-directories, and data from formatted disks.
- Understand the NTFS partition table, boot record, and root directory.
- Understand Bitmaps.
- Understand the MFT.
- Understand NTFS Headers and Attributes.
- Understand Resident and Non-resident files.
- Understand Run lists, etc.
- Understand Alternate data streams.
- Understand NTFS File storage.
- Understand the various dates and times stored in attributes.
- Understand File deletion and recovery.
- Understand Directory storage.
- Understand Tracing files/directories.
- Understand the NTFS registry "hive."
- Understand Examining NTFS drives.
- Understand the basic imaging methods and how to make "exact copies" of media.

- Understand the significance of, location of and how to recover data from swap files, temporary files, Internet cache files, Internet cookies, mail files and Internet sites visited.
- Understand basic Internet issues such as, doing a basic "whois."
- Understand how to preserve the original media.
- Understand how to prevent inadvertent writes.
- Understand how to prevent virus introduction and how to prevent activation of "booby traps."
- Understand how to safely handle media.
- Understand how to find and document normal data and graphical files.
- Understand how people commonly try to hide data.
- Understand how to find and document data in unallocated space.
- Understand how to find hidden data.
- Understand password protection schemes and how to lock and unlock many passwords.
- Understand how to access MS Word metadata.
- Understand the basic use of automated forensic suites (FTK).
- Understand basic data formats and types.
- Understand how to conduct basic data-format conversions.
- Understand the basic issues in examining CDR media.
- Understand how to present recovered and evidence data to the client in a useful format.
- Understand how to manage data.
- Understand how to present data in court or other proceedings in a clear and understandable manner.
- Have conducted an examination of a hard disk drive that covers the full range of forensic issues found in this training course.
- Be fully prepared to sit for the CCE Certification testing through the International Society of Forensic Computer Examiners.

Course Outline

- **Basic CompTIA A+ Certification Prep**
 - a. Lesson 1: The path of the tech
 - b. Lesson 2: The visible PC
 - c. Lesson 3: Introduction to CPUs
 - d. Lesson 4: Modern CPUs
 - e. Lesson 5: RAM Fundamentals
 - f. Lesson 6: RAM today
 - g. Lesson 7: BIOS/CMOS
 - h. Lesson 8: Expansion bus fundamentals
 - i. Lesson 9: Modern Expansion bus types
 - j. Lesson 10: Motherboards and cases
 - k. Lesson 11: Power supplies and electricity
 - l. Lesson 12: Input/output devices

- **CompTIA Network+ Certification Prep**
 - a. Lesson 1: Bus topologies and ethernet
 - b. Lesson 2: Star topologies and ethernet
 - c. Lesson 3: Ring topologies and token ring
 - d. Lesson 4: The OSI model
 - e. Lesson 5: The protocol suites
 - f. Lesson 6: TCP/IP in detail
 - g. Lesson 7: Network operating systems
 - h. Lesson 8: Network server hardware
 - i. Lesson 9: Connectivity hardware
 - j. Lesson 10: Remote connection technology
 - k. Lesson 11: Remote access
 - l. Lesson 12: Maintaining and troubleshooting networks

- **CompTIA Security+ Certification Prep**
 - a. Lesson 1: Basic goals, tools and techniques of computer security
 - b. Lesson 2: Unauthorized access control
 - c. Lesson 3: Attack methods
 - d. Lesson 4: Tools and techniques to protect servers
 - e. Lesson 5: Securing wireless networks, mobile devices, directory services, and remote access
 - f. Lesson 6: Encryption
 - g. Lesson 7: PKI, Certificate Authorities, digital certificates, trust models
 - h. Lesson 8: Protecting data from would-be attackers and spies within an organization
 - i. Lesson 9: Techniques to make the “bad guys” job tougher and techniques to catch them
 - j. Lesson 10: Hardening a network against attack, scanning for vulnerabilities and patching a network
 - k. Lesson 11: Availability of network resources
 - l. Lesson 12: Policies and procedures, forensics and security training - keys to security management

- **Forensic Computer Examiner Module 1 - Introduction to Computer Forensics**
 - a. Recommended Machine Configuration
 - b. What makes a good computer forensic examiner?
 - c. Computer Forensics vs. E Discovery
 - d. Dealing with clients or employers
 - i. Work Product
 - ii. Client Contracts
 - iii. Legal and Privacy Issues
 - e. Software Licensing
 - f. Ethical Conduct Issues

- g. Cases that may include digital evidence
- h. Forensic Examination Procedures
- i. Determining Scope of Examinations
- j. Hardware and Imaging Issues
- k. Floppy Diskette, USB and Optical Media Examination
- l. Limited Examinations
- m. Forensically Sterile Examination Media
- n. Examination Documentation and Reports
- o. ASCII Table
- p. General Overview of Boot Process and Operating Systems
- q. Floppy Diskette Sides, FD Tracks, Hard Disk Drives
- r. BIOS History
- s. Networked Computers
- t. Media Acquisition
- u. Acquisition Documentation
- v. Chain of Custody

- **Forensic Computer Examiner Module 2 - Imaging and Introduction to SMART**

- a. Imaging Theory and Process
- b. Imaging Methods
- c. Write Blocking
- d. Imaging Flash Drives
- e. SMART Introduction
- f. Wiping, Hashing, Validation, Image Restoration, Cloning, Unallocated Space
- g. Drive Partitioning
- h. One (1) Student Lab Practical Exercise

- **Forensic Computer Examiner Module 3 - File Signatures, Data Formats & Unallocated Space**

- a. File Identification
- b. File Headers
- c. General File Types
- d. File Viewers
- e. Examination of Compressed Files
- f. Data Carving - Using Simple Carver
- g. One (1) Student Lab Practical Exercise

- **Forensic Computer Examiner Module 4 - FAT File System**

- a. Logical structures of DOS, Windows 95, Windows 98
- b. Master Boot Record

- c. File Allocation Table
 - i. 16 Bit FAT
 - ii. 32 Bit FAT
 - d. Directory Entries
 - e. Clusters
 - f. Unallocated Space
 - g. Sub-Directories
 - h. FORMAT
 - i. Six (6) Student Lab Practical Exercises
- **Forensic Computer Examiner Module 5 - NTFS**
 - a. Introduction and Overview
 - b. Basic Terms
 - c. Basic Boot Record Information
 - d. Time Stamps
 - e. Root Directory
 - f. Recycle Bin
 - g. File Creation
 - h. File Deletion
 - i. Examining NTFS Drives
 - j. Two (2) Student Lab Practical Exercises
- **Forensic Computer Examiner Module 6 - Registry & Artifacts**
 - a. Creating an Examination Boot Disk
 - b. Data Recovery
 - c. Windows Swap and Page Files
 - d. Forensic Analysis of the Windows Registry
 - e. Internet Cache Files, Cookies and Internet Sites
 - f. Microsoft Outlook
 - g. MSMAIL
 - h. Logical Structures
 - i. Tracking User Specific Computer Use
 - j. Internet Explorer Cache Index
 - k. VISTA
 - l. Basic Mail Issues
 - m. Basic Internet Issues

- n. Common Situations Encountered during Examinations
 - o. Password Protection and Defeating Passwords
 - p. Compound Documents
 - q. Examining CDR Media
 - r. FTK
 - s. Three (3) Student Lab Practical Exercises
- **Forensic Computer Examiner Module 7 - Forensic Policy, Case Writing, Legal Process & Forensic Tool Kits**
 - a. Use of Policy and Checklists in Forensic Practice
 - b. Data Presentation to Client
 - c. Case Report Writing
 - d. Legal Process
 - e. Expert Admission
 - f. Going to Court
 - g. Use of Forensic Tools and Software
 - h. One (1) Student Lab Practical Exercise - Hard drive examination

Prerequisites/Audience

Students will be required to take three short, online information assurance courses prior to beginning the Forensic Computer Examiner coursework.

Basic CompTIA A+ Certification Prep
CompTIA Network+ Certification Prep
CompTia Security+ Certification Prep

Basic computer skills are essential, including the ability to work outside the Windows GUI interface. This is due to much of the forensic examiner's job utilizing data that cannot easily be accessed from within Windows. Being comfortable working within the DOS environment will be very helpful in this field.

A good measure of a potential student's readiness for this course would be to have the ability to successfully complete the A+ certification through Microsoft. Note that this is by no means a prerequisite. However, the basic knowledge needed for being successful enrolling within our training typically requires that a student be at this level of experience.

A forensic computer examiner will be required to work with the hardware of a computer on many occasions. The ability or desire to remove and replace hard-disk drives from computers and change



jumper settings is required. These topics are briefly covered within our course. However, it is expected that a student have this familiarity prior to enrolling.

Students must also have no criminal record. This includes any felony conviction where the individual could have or received a sentence of one or more years imprisonment. This also includes any criminal history of sexually related offenses as many digital examinations include these topics which could easily discredit an examiner if found to have a history.

Note: Students who plan to pursue the Certified Computer Examiner (CCE®) credential must have attended a course through an ISFCE Authorized Training Center (such as this), have documented experience in forensic computer examinations, OR be able to produce a well documented self study.

PC Requirements/Materials Included

Minimum Computer Requirements:

- PC with latest updates and BIOS (Mac computers may not be used)
- Windows 98SE, 2000 or XP Operating System (Vista & Windows 7 as well as all 64-bit processors are not yet supported)
- Internet access
- 1 GB (or more) memory
- 2 GB or larger hard disk drive for examination purposes
- 2 open USB 2.0 ports

Recommended Configuration:

- PC with latest updates and BIOS
- Windows 2000 or XP Operating System (Vista & Windows 7 as well as all 64-bit processors are not yet supported)
- Internet access - High speed Internet access is recommended.
- 2 GB (or more) memory
- 15 GB or larger hard disk drive for examination purposes
- Integrated PS/2 ports (Not USB Keyboard or Mouse)
- 4 open USB 2.0 ports
- 1 open Firewire / IEEE 1394 port
- Read / Write Blocking device such as the 'FireFly Read/Write' device made by Digital Intelligence

Students may use either a desktop or a laptop computer.

The material used in this course is based on the concept of teaching computer forensics from a vendor neutral perspective. This course teaches the low level mechanics of commonly

encountered file systems. If a student can gain a solid understanding of one file system and how it functions at a low level then that student will be prepared to learn other file systems as well.

This course material will teach low level mechanics and functions of both the FAT file system and the New Technology File System (NTFS). Although the FAT file system is not available on new computers, it is the default file system on floppy diskettes and USB devices. Many computer forensic incidents involve USB devices and will continue to involve these devices for years to come. Consequently, students studying to become successful forensic computer examiners must understand the FAT file.

Windows 98 and earlier versions are based on the FAT file system. A computer formatted with Windows 2000, XP, and Vista versions will typically be formatted with the NTFS file system.

The completion of several practical exercises is a requirement of this course. Some might include floppy diskettes. Although the floppy diskette is no longer commonly encountered in the field, it is the exercise that is significant and any action taken on a floppy diskette can be replicated on a hard drive.

The Forensic Computer Examiner program will train you to not only thoroughly examine digital media, but also clearly document, control, prepare and present examination results.

This program includes instruction on conducting thorough examinations, identifying where and how data is stored, recovering and interpreting data and drawing appropriate conclusions based on the data.

A sound understanding of the FAT and NTFS file systems is critical to forensic examination. These file systems are important because they are the base of Windows operating systems, portable flash media, storage devices and other digital media in use everywhere today. USB drives, mobile phones, laptops, desktops and cameras are examples of common equipment that use these systems. FAT file system logical structures are utilized by DOS and Windows 9.x. NTFS logical structures are utilized by Windows NT, 2000, XP and Vista.

Students will be provided a package of forensic industry-standard software bundled with this course. Each registered student will receive:

- SMART - www.ASRData.com
- Simple Carver - www.SimpleCarver.com
- Password Kit - www.LostPassword.com
- Forensic Tool Kit (Demo version) - www.AccessData.com
- Numerous other free and shareware tools!

Instructor Bio

John Mellon is the primary author of this computer forensic examination course. He is a retired US Customs Senior Special Agent with 28 years investigative experience and over 17 years experience in computers. He is an IACIS certified forensic computer examiner.

Mr. Mellon had Initial experience with the CP-M operating system in 1986. He had initial computer forensic training in 1991 by the International Association of Computer Investigative Specialists (IACIS). He has been an active member of IACIS and is a member of the Board of Directors.

He is the past chairman of the IACIS DOS Seizure Certification Committee. He is the past chairman of the IACIS DOS/Windows Processing Certification Committee. He is the past chairman of the Certification Committee and the past Chairman of the IACIS Board of Directors.

Mr. Mellon has been a lead instructor at IACIS training conferences. He has been involved in the training of hundreds of law enforcement officers world-wide in computer forensics since 1994.

He has taught numerous highly technical subjects including DOS and Windows 95/98 file systems, architecture and the boot process, DOS and Windows 95/98 examination techniques and procedures, recovery of deleted files, recovery of Windows long file names, date and time stamp alterations, recovering formatted disks, the process and problems in making forensic copies of media, file type identification and the use of file viewing applications during examinations, the theory of archived files and compressed disks, examining archived and compressed disks and files, data format conversion, basic Novell theory and the methods for seizing and examining Novell networks, examination of Windows swap and related files and the new IACIS Examination Standards and Forensic Code of Ethics.

He developed and implemented the IACIS Forensic Examination Standards, the IACIS Code of Ethics, the advanced Windows Processing Certification, the past IACIS Certified Forensic Computer Examiner (CFCE) problems containing numerous technical issues. These problems must be completed to attain the CFCE certification from IACIS. He continues to instruct civilians and law enforcement officers world-wide in computer forensic examinations.

Mr. Mellon was the first computer forensic examiner for US Customs in Miami, Florida. In that connection he set up the forensic examination program in Miami in 1991 and forensically examined many computers between 1991 and 1993.

He started Key Computer Service in 1993 and has continued to forensically examine computers for US Customs, DEA, local police agencies, attorneys, private companies and individuals.

He has been cited as a computer forensic expert witness in courts and in affidavits in US District Court, Miami, Florida and in Atlanta, Georgia.

John Fretts retired from the Bureau of Alcohol, Tobacco, Firearms and Explosives in 2005, after a distinguished thirty-year career with the Department of Justice, Bureau of Alcohol, Tobacco & Firearms. Mr. Fretts began his ATF career as a Special Agent in the Washington, DC Field Division where he led numerous Federal investigations into violations of Federal firearms and explosive laws. In 1991, Mr. Fretts was promoted to the position of Project Manager at ATF Headquarters.

In 1994, Mr. Fretts transferred to Connecticut with his appointment as Supervisor of ATF's Hartford Field Office. While in Connecticut, Mr. Fretts nurtured his technical interests, developing skills as a specialist in computer forensic investigations. He successfully completed the CIS 2000 Program, at the Federal Law Enforcement Training Center, in Brunswick, Georgia. He was also certified by the International Association of Computer Investigative Specialists as a Certified Forensic Computer Examiner (CFCE) in 2004. Because of his management experience and knowledge of computer investigations, John was named Regional Supervisor of ATF Computer Forensic Operations for the northeast United States. While with the ATF, Mr. Fretts testified in Federal Court and is qualified to appear as an expert in Computer Forensics and Data Recovery.

Upon retirement from Federal service, Mr. Fretts accepted a position as Director of Investigations with Security Services of Connecticut (SSC), a regional firm specializing in a full range of investigative services, specializing in computer forensics.

Mr. Fretts had oversight of SSC's computer forensic operation and was regularly called upon to lecture on the topic of computer forensics and data recovery as it relates to fraud and computer misuse. In his presentations to corporate clients and at trade shows, Mr. Fretts has an uncanny ability to explain the most complex aspects of computer forensics to those with the least understanding of the subject. With his law enforcement background, Mr. Fretts was adept at explaining the necessity to respond rapidly to an incident involving fraud or criminal activity involving computers and the need to preserve electronic evidence.

In August of 2007, Mr. Fretts resigned from his position with SSC to concentrate his time and skills on computer forensics investigation and education. Mr. Fretts is a member of the University of New Haven, Criminal Justice curriculum, Student Advisory Board. He is a veteran of the United States Army, and has a Bachelors degree in Criminal Justice.

Steve Wisenburg is a 14-year veteran of the City of Atlanta Police Department. He has been a Detective since 1999, where he started investigations in the physical abuse and sexual abuse of children. These investigations lead to child porn investigations as well as other exploited children on the Internet investigation. He is now assigned to the Cybercrime Unit where he is a full time computer forensic examiner.

Mr. Wisenburg is the current president of the Atlanta Chapter of the High Technology Investigation Association (HTCIA). He holds the Certified Computer Examiner (CCE) certification. He also is one of the founding directors of the Cybercrime Summit, a training conference held in Metro Atlanta each year. Mr. Wisenburg has attended several training classes including the following:

Computer forensics Boot Camp, Practical Data Forensics using Linux, Access Data Forensic Boot Camp, EnCase Intermediate analysis and reporting, Basic Data Recovery and Analysis, Advanced Data recovery and analysis ILook, Maresware Software Training, etc.

Dave Good has served the U.S Dept. of Treasury and the U.S. Dept. of Justice for the past 18 years. He has over 21 years experience in the management, design and implementation of



mainframe systems, local area networks, and virtual private networks.

Mr. Good's experience includes:

- Electronic Data Systems, Camphill PA, Philadelphia PA, Seattle WA, Dallas TX,
- Washington D.C. 1984 - 1988 Computer Operations, Network Operations
- Network Solutions, Herndon VA, 1988 - 1989 Network Operations
- Automation Research Systems, Alexandria VA, 1989 - 1992 Local Area Network
- Installation and Management
- Washington D.C. 1992 - Present Local Area Network Installation and Management,
- Enterprise Systems Architecture Program Management Computer Forensics

Mr. Good completed the first seat based Enterprise Systems Architecture for the Federal Government where 300 sites were outfitted with new desktops, laptops, servers, and implemented the conversion of a packet switched network to a frame relay network for all sites.

He is currently serving as a Digital Investigator and Program Manager of the Computer Forensics Branch for a National Law Enforcement Agency.

He has been cited as a computer forensic expert witness in US District Court, Charlotte, NC.

Mr. Good is a active member of the National Technical Investigators Association, The High Technology Crime Investigation Association, and the International Society of Forensic Computer Examiners.

Mr. Good holds the following certifications:

- Novell Master Certified Network Engineer (MCNE)
- CCE
- Comptia A+
- Comptia Net+
- Comptia IT Project+

Phil Harrold was employed by the Odessa, Texas Police Department from 1979-1988. His assignments included patrol, narcotics and crimes against property. From 1989 until 2000 Mr. Harrold was employed by the Monroe County, Florida Sheriff's Office. His assignments with that agency included patrol, general investigations, homicide investigations and he was a bomb technician.

Mr. Harrold has been employed from 2000 to the present by the State Attorney's Office, 16th Judicial Circuit, and State of Florida as an Investigator. He specializes in computer related investigations and performs forensic examinations for local, state and federal agencies.



Mr. Harrold's education includes:

- 1982-AAS in Law Enforcement from Odessa College
- 1985-Bachelor of Arts in Criminal Justice from the University of Texas of the Permian Basin
- 1997-Master of Science Degree in Management from Troy State University
- Mr. Harrold's specialized training includes:
- US Army/FBI Hazardous Devices School, Redstone Arsenal Alabama
- US Army/FBI Weapons of Mass Destruction School
- IACIS Basic
- Computer Crime Investigation
- Basic Data Recovery and Analysis
- Advanced Analysis of Microsoft NTFS
- Advanced Analysis of Email
- Microsoft Access
- On-line investigations
- Access Data-Intermediate Forensic Boot Camp
- Homicide Investigation
- Hostage Negotiation
- Multi-Disciplinary Investigation of Computer Facilitated Child Sexual Exploitation
- Racketeering Investigations

Mr. Harrold's certifications include:

- Certified Computer Examiner (CCE)
- Electronic Evidence Collection Specialist (IACIS)

Mr. Harrold's professional affiliations include:

- International Association of Computer Investigative Specialists
- High Technology Crime Investigation Association
- High Tech Crime Consortium
- International Society of Forensic Computer Examiners

Keith Barger is a Director in KPMG's Forensic practice in Houston, Texas. Keith specializes in electronic data discovery and investigative services in support of civil litigation and provides advisory services regarding technology related matters.

Keith joined KPMG in 2006 after six years as a Special Agent and Digital Forensics Western Regional Coordinator with the Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).



Keith has extensive experience in digital forensic investigations, forensic methodologies, computer evidence recovery, and data analysis. Keith has investigated and provided oversight for domestic investigations violating Federal, State, and local laws. These investigations often included testimonies before grand juries, inquests, trials, and other hearings.

Keith is responsible for the National direction and oversight with regards to KPMG's Hold Order Management System. He leads a national team responsible for the collection of litigation preservation requests on behalf of KPMG and its clients and collaborates with others on his team in the identification of custodians, automation of the collection process and the production of litigation requests to relevant parties.

Additionally he is responsible for the assessment and review of network infrastructures and related record management systems recommending improvements and overseeing the implementation of those improvements.

William (Bill) D. Taylor is a Computer Investigative Specialist/ Special Agent with a federal law enforcement agency in Nashville, Tennessee. He has served as a full time forensic computer examiner since 1994.

Mr. Taylor is a Certified Forensic Computer Examiner (International Association of Computer Investigative Specialists), a Certified Fraud Examiner, (Association of Certified Fraud Examiners) and holds an Associate Degree in Forensic Computer Science.

In addition he holds both Baccalaureate and Master's Degrees in Criminal Justice and is a graduate of the FBI National Academy. Mr. Taylor has over 24 years investigative law enforcement experience at the state local and federal level. He served on the IACIS Board of Directors for six years, Vice-President for 1 year and as President and CEO for nearly 3 years.