SANS

The Most Trusted Name in Hands-on Information & Software Security Training & Professional Certification

Community SANS in East Africa

NAIROBI • October 4–8 2010

FOR408: Computer Forensics Essentials

"This course provided the right mix of methodology and technical material to understand the basic of forensics. Good explanation of evidentiary data and the specifics of evidence."

– J.T. LAZO, FEDERAL RESERVE BOARD

K-90

Community SANS

FOR408: Computer Forensics Essentials

5-DAY COURSE • 6 CPE CREDITS PER DAY • LAPTOP REQUIRED

who should attend

››› Information technology professionals who wish to learn the core concepts in computer forensics investigations

››› Incident Response Team Members who are responding to security incidents and need to utilize computer forensics to help solve their cases

››› Law enforcement officers, federal agents, or detectives who desire to become a subject matter expert on computer forensics for Windows based operating systems

››› Information security managers who need to understand digital forensics in order to understand information security implications and potential litigation related issues or manage investigative teams

››› Information technology lawyers and paralegals who desire to have a formal education in digital forensic investigations

››› Anyone interested in computer forensic investigations with a background in information systems, information security, and computers

sampling of topics

- Digital Forensics Essentials
- Windows File System Basics
- Fundamental Forensic Methodology
- Evidence Acquisition Tools and Techniques
- Law Enforcement Bag and Tag
- Evidence Integrity
- Presentation and Reporting of Evidence and Analysis
- Windows XP, VISTA, and Windows 7 Investigation and Analysis
- Windows In-Depth Registry Forensics
- Tracking User Activity
- And Much More...

course overview

This course focuses on the critical knowledge that a computer forensics investigator must know to investigate computer crime incidents successfully. You will learn how computer forensics analysts focus on collecting and analyzing data from computer systems to track user-based activity that could be used internally or in civil/criminal litigation. This course covers the fundamental steps of the in-depth computer forensics methodology so that each student will have the complete qualifications to work as a computer forensics investigator in the field helping solve and fight crime. In addition to in-depth technical digital forensics, knowledge on Windows Digital Forensics (Windows XP through Windows 7 and Server 2008) you will be exposed to well known computer forensics tools so such as FTK, Registry Analyzers, FTK Imager, Prefetch Analyzers, and much more.

course description

DAY 1: DIGITAL FORENSICS AND E-DISCOVERY FUNDAMENTALS

Focus: Investigations begin with a firm knowledge in proper evidence acquisition and analysis. Digital Forensics is more than just using a tool that automatically recovers data. You must focus on the facts to seek the truth. Digital Forensics requires analytical skills. Today you will learn how the professionals accomplish digital forensics.

DAY 2: EVIDENCE ACQUISITION AND ANALYSIS

Focus: You will learn proper evidence acquisition, integrity, and handling skills of logical, physical, and system memory utilizing the Tableau T35es writer. Moving quickly from acquisition, you will begin your investigation using cutting-edge tools that the pros use.

DAY 3: CORE WINDOWS FORENSICS PART I - EMAIL AND REGISTRY ANALYSIS

Focus: Beginning with host, server, and webmail forensics the investigator will learn how to recover and analyze the most world's most popular form of communication. Following this, the next focus centers on Windows XP, Vista, and Windows 7 Registry Analysis and USB Device Forensics.

DAY 4: CORE WINDOWS FORENSICS PART II - ARTIFACT AND BROWSER FORENSICS

Focus: Hundreds of files are created by actions of the suspect. Learn how to examine key files such as link files, the windows prefetch, pagefile/system memory, and more. Internet Explorer and Firefox Browser Digital Forensics is covered in detail. Learn how to examine exactly what an individual did while surfing via their web-browser. The results will give you pause the next time you use the web.

DAY 5: DIGITAL FORENSIC CHALLENGE AND MOCK TRIAL

Focus: Windows Vista/7 Based Digital Forensic Challenge. There has been a murder-suicide and you have been called in to investigate the system. This day is a capstone for every artifact discussed in the class. You will use this day to solidly your skills that you have learned over the past week.

training venue

Nairobi Safari Club - Lillian Towers
Koinange Street / University Way Nairobi, Kenya
Tel: +254-20-2821000 • Fax: +254-20-2215137
info@nairobisafariclub.com | http://www.nairobisafariclub.com

about the instructor

ISMAEL VALENZUELA
— INSTRUCTOR —

Since he founded one of the first IT Security consultancies in Spain, Ismael Valenzuela has participated as a security professional in numerous international projects across EMEA, India and Australia in the last 10 years. He currently works as Global IT Security Manager for iSOFT Group Ltd., one of the world's largest providers of healthcare IT solutions with presence in more than 40 countries. Ismael's expertise includes security assessments, penetration testing, risk analysis, ISO 27001 implementation, security architecture design and review, IDS/IPS technology, traffic analysis, log correlation, incident handling and digital forensics analysis.

Ismael also serves on the GIAC Advisory Board, and is an international instructor for the British Standard Institute (BSi). He holds a bachelor's degree in computer science from the University of Malaga (Spain), is certified in Business Administration, and holds several professional certifications including GCFA, GPEN, GWAPT, GCIA, CISSP, ITIL, CISM and IRCA 27001 Lead Auditor from Bureau Veritas UK.

registration information

DETAIL & REGISTRATION: **http://www.sans.org/info/60388**

TUITION: **FOR408: Computer Forensics Essentials**

FEE IF PAID BY 25 AUGUST - $4200 • FEE IF PAID BY 8 SEPTEMBER - $4300 • FEE IF PAID AFTER 8 SEPTEMBER - $4500

SANS CONTACT: Barbara Basalgete, Director SANS EMEA: **+44 20 3384 3473** | **bbasalgete@sans.org**

K-NINETY CONTACT: Preston Odera, CEO: **+254 722 771478** | **preston.odera@gmail.com**

about the Community SANS program in EMEA

The Community SANS format in EMEA (Europe, Middle East and Africa Region) offers the most popular SANS courses in your local community and in your local language. The classroom setting is small with fewer than 25 students. The instructors are pulled from the best of the local mentor program or qualified security experts who have passed SANS rigorous screening process called "the murder boards". The course material is delivered over consecutive days, and the course content is the same as ones provided at a larger training event. In addition to the excellent courseware, not only will you be able to use the skills that you learned as soon as you return to the office, but you will be able to continue to network with colleagues in your community that you meet at the training.

SANS has partnered with K-Ninety East Africa Ltd. to bring the FOR408 course for the first time to East Africa. K-Ninety will be promoting the event locally.

about SANS

SANS is the most trusted and by far the largest source for training and certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center. The SANS (SysAdmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. A range of individuals from auditors and network administrators, to chief information security officers are sharing the lessons they learn and are jointly finding solutions to the challenges they face. At the heart of SANS are the many security practitioners in varied global organizations from corporations to universities working together to help the entire information security community.

http://www.sans.org

about K-Ninety East Africa Ltd.

K-Ninety East Africa Ltd. (K-90) is a consulting company dealing in training, conferences, e-learning solutions, bandwidth optimization solutions, IS audit, forensics audit, information systems security, and computer audit solution.

http://k-90ea.com