ASM Educational Center (ASM) Est. 1992

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | Phone: 301-984-7400 | Fax: 301-984-7401
Web: www.asmed.com | E-mail: info@asmed.com

Cyber Crime Forensics Outline
(Customized Course)

DAY ONE

I. Introduction to Forensics

- Computer Forensics defines
- Traditional forensics
- "Live" system forensics
- Establishing a Forensic Methodology
    - Repeatable process

LAB ONE : Forensic Analysis: What were up against

II. Legal aspects of a Forensic Investigation

- Computer crime law
    - 1029 and 1030
    - RIPA
    - Others
- Investigating the scene
    - Preservation of evidence
    - Maintaining the chain of custody

III. Planning a Response to a potential incident

- Search and seizure laws
- What can and cannot you take
- Laws of digital evidence
    - Hearsay
        - Exceptions to the hearsay law
    - Digital evidence references
        - International Journal of Digital Evidence
        - Chief Police Officers Guide
    - Interviewing techniques
        - Characteristics of deception
    - Incident response life-cycle

IV. Performing Traditional or disk-based forensics to extract evidence

- Hard drive interfaces
    - SCSI, IDE. SATA,
    - Fibre Channel
- Acquiring an image
        - dd

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | Phone: 301-984-7400 | Fax: 301-984-7401
Web: www.asmed.com | E-mail: info@asmed.com

- power of netcat
- EnCase
- Forensics Toolkit
- Paraben

LAB TWO: Netcat and image creation

- integrity verification
  - MD5
  - SHA-1
  - SHA-256
  - SHA-512

LAB THREE: Maintaining image integrity

- Write blockers
  - Hardware
  - Software

DAY ONE LAB: Forensic Challenge

DAY TWO

V. Examining Internals of the Operating System Boot Process

- Windows
- Linux
- Unix
- Mac

VI. Dissecting Internals of the Hard Drive

- Cylinder structure
- Power on routine
- System Area
- Bad block tables
  - P-list
  - G-list
- Heads
  - R/W
  - GMR
- Platter structures

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

VII. Exploring Hard drive recovery techniques

- Replacing the heads
- Platter swaps
- Swapping PCBs

VIII. Analyzing Volumes for Forensic Evidence

- PC partitions
  - DOS
  - Apple
  - Removable media
- Server partitions
  - BSD
  - Solaris
- Others
  - RAID
    Spanned disks

LAB FOUR: Recovering deleted partitions

IX. Analyzing File Systems

- File system defined
- Categories
- FAT analysis
  - File system and content
- FAT structure
  - Boot sector
  - FAT32
  - Naming conventions

LAB FIVE: FAT File System

- NTFS
  - Basic disks
  - Dynamic discs
  - Comparison of basic and dynamic
  - MFT
  - Handling small files
  - Recovery techniques
    - Legacy
    - Current

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

LAB SIX: NTFS File System

- Ext2 and Ext3
  - Concepts and analysis
  - Structure
    - Superblock
    - Group descriptor tables
    - Symbolic link
- UFS1 and UFS2
  - Concepts and analysis
  - Structure
    - Superblock
    - Inodes

DAY TWO LAB: Forensic Challenge Two

DAY THREE

X. Defeating Hacker hiding techniques

- Unallocated space
- File fragmentation
- Obfuscating strings

LAB SEVEN: String Searching for information

- Attributes
- File signatures
- File segmentation
- File combining

LAB EIGHT: File Hiding and Combining

- File binding and wrappers

LAB NINE: File Wrappers

- Alternate data streams

LAB TEN: Alternate Data Streams

- Registry
- Object linking and embedding (OLE)

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | Phone: 301-984-7400 | Fax: 301-984-7401
Web: www.asmed.com | E-mail: info@asmed.com

- Office documents
- File manipulations
    - Extensions
    - Headers

LAB ELEVEN: File manipulation

XI. Application of Steganography to defeat forensic examinations

- Defining
- History
- Types
- Steganography vs Watermarking
- Steganalysis
- Detecting Steg
- Future of Steganography

LAB TWELVE: Steganography

XII. Capturing traffic on the "wire" and Implementing Network Forensics

- TCP/IP fundamentals
- TCP/IP internals
- Layer by layer forensics
- Collecting data
    - Raw protocol analysis
        - Tcpdump
        - Windump
    - Full protocol analysis
        - Wireshark
            - Working with filters
            - Session re-assembly

LAB THIRTEEN: TCP/IP analysis

DAY THREE LAB: Forensic Challenge Three

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

DAY FOUR

XIII. Intrusion Analysis of Network Traffic on Windows and Linux

- Identifying normal vs abnormal traffic
- Determining cause of abnormal traffic
  - Error
  - Malicious
- Recognizing common patterns of network attacks
- Identifying the OS from the network traffic
  - Passive fingerprinting characteristics
    - Nuances of the TCP/IP stack

LAB FOURTEEN: Analyzing basic attacks

- Components of a sophisticated attack
  - Deception techniques
  - Protocol camouflage
  - Encryption and tunnels

LAB FIFTEEN: Analyzing a sophisticated attack

- Components of advanced attacks
- Protocol encapsulation
  - More than one layer 7
- Web attacks
  - Services
  - SQL
  - XSS
  - Access controls

LAB SIXTEEN: Analysis of Web Attacks

XIV. Email Forensics: Investigating Email to trace a path to the perpetrator

- Client side investigations
- Server side investigations
- Analyzing headers
- Validating the path
- Recovering deleted emails
- Recovering email attachments
- Forensic analysis of online email systems

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

LAB SEVENTEEN: Email Forensics

XV. Web Activity Forensics: Reconstruction of Internet traffic after deliberate deletion

- Reconstructing browsing activity
- Analyzing cookies
- Examining temporary files and storage locations
- Registry artifacts
- Reconstructing cleared histories and private data
  - Index.dat
  - History.dat

LAB EIGHTEEN: Web Forensics

XVI. Applying Internet Forensics to catch the crafty hackers

- Understanding DNS
- Records of interest
- Analyzing DNS activity at the packet level
- Authoritative vs non-authoritative

XVII. Recovering Protected Storage information to identify illicit activity

- Locating stored data
  - Pass View
- Formats of storage
- Auto completion
- Registry data
- Recovering protected storage data in IE 7
  - Pass View 1.7

DAY FOUR LAB: Forensic Challenge Four

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

DAY FIVE

XVIII. Encryption and password hashing primer

- Encryption techniques
  - Algorithms
    - Stream
    - Block
    - Identifying

LAB NINETEEN: Identifying algorithms

- Cracking
  - Fallacy of
  - Definition of a "cryptographic" crack
- Hashing
  - Algorithms
    - UNIX/Linux
    - Windows
      - LM
      - NTLM
      - NTLMv2
  - Cracking
    - Dictionary
    - Hybrid
    - Brute force
    - Rainbow

LAB TWENTY: Password Cracking

XIX. Introduction to "LIVE" Forensics

- Volatile data
- Non-volatile data
- Process and memory analysis

LAB TWENTY ONE: Capturing Volatile Information

XX. Understanding Unix/Linux "LIVE" Forensics to recover memory based evidence

- Analyzing volatile data
  - Network connections
  - Ports
  - Processes
  - Memory of processes

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | Phone: 301-984-7400 | Fax: 301-984-7401
Web: www.asmed.com | E-mail: info@asmed.com

- Open files and handles
- Routing tables
- Kernel modules
- Mounts

- Analyzing non-volatile data
  - System version
  - Time and date stamps
  - Logs
  - History files
- Rootkits

LAB TWENTY TWO: Linux ”LIVE”

XXI. Processing Windows “LIVE” Forensics information to discover malware

- Analyzing volatile data
  - Network connections
  - Ports
  - Processes
  - Memory of processes
  - Open files and handles
  - Routing tables
  - System memory

LAB TWENTY THREE: Windows “LIVE”

XXII. Staying current

- Staying current
  - Reference white papers and sites
  - Classic books
  - Forums and newsletters
  - Conferences