LIVE Digital Forensics

(Customized Course)

DAY ONE START

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
  - UAE: Cybercrime law No. 2
  - 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. Defeating Hacker hiding techniques

- Unallocated space
- File fragmentation
- Obfuscating strings

LAB TWO: String Searching for information

- Attributes
- File signatures
- File segmentation
- File combining

LAB THREE: File Hiding and Combining

- File binding and wrappers

LAB FOUR: File Wrappers

- Alternate data streams

LAB FIVE: Alternate Data Streams

- Registry
- Object linking and embedding (OLE)
- Office documents
- File manipulations
  - Extensions
  - Headers

LAB SIX: File manipulation

DAY ONE LAB: Forensic Challenge

DAY TWO START

V. Application of Steganography to defeat forensic examinations

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

LAB SEVEN: Steganography

VI. 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 EIGHT: TCP/IP analysis

VII. 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 NINE: Analyzing basic attacks

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

LAB TEN: Analyzing a sophisticated attack

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

LAB ELEVEN: Analysis of Web Attacks

DAY TWO LAB: Forensic Challenge Two

DAY THREE START

VIII. 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

LAB TWELVE: Email Forensics

IX. 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 THIRTEEN: Web Forensics

X. Applying Internet Forensics to catch the crafty hackers

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

XI. 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

XII. Encryption and password hashing primer

- Encryption techniques
  - Algorithms

        - Stream
        - Block
        - Identifying

LAB FOURTEEN: 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 FIFTEEN: Password Cracking

XIII. Introduction to "LIVE" Forensics

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

LAB SIXTEEN: Capturing Volatile Information

DAY THREE LAB: Forensic Challenge Three

DAY FOUR START

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

- Analyzing volatile data
    - Network connections
    - Ports
    - Processes
    - Memory of processes
    - Open files and handles
    - Routing tables
    - Kernel modules
    - Mounts
- Analyzing non-volatile data
    - System version
    - Time and date stamps
    - Logs
    - History files
- Rootkits

LAB SEVENTEEN: Linux "LIVE"

XV. 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
- Analyzing non-volatile data
    - System version
    - Time and date stamp
    - Registry data
    - Login history
    - Auditing policy
    - Examining the event viewer
    - Logs and using logparser
        - Using logparser
        - Developing powerful queries
            - Basic
            - Advanced

LAB EIGHTEEN: Windows "LIVE"

XVI. Advanced Windows Forensics: Performing low-level internal analysis to identify advanced memory corruptions

- Windows internals
  - System architecture
  - Memory management
  - Cache management
  - Dumps analysis
  - Tools
    - Filemon
    - Regmon
    - Process explorer
    - Process explode
    - Dependency walker
- Win32 rootkits
  - Traditional
    - Trojaned files and processes
  - Hooking
    - Man in the middle attack against the descriptor table
  - DKOM
    - Unlinking processes direct in memory

LAB NINETEEN: Windows Rootkits

DAY FOUR LAB: Forensic Challenge Four