

COURSE TITLE: Cybercrime Investigation I

COURSE NUMBER: IA-533

CREDIT HOURS: 3

PREREQUISITE: Computer Literacy Course

Text: Casey, E. (2001). *Digital Evidence and Computer Crime, Forensic Science, and Computers and the Internet*, Academic Press.

Additional Readings:

Bequai, A. (1998). A guide to cyber-crime investigations, computers & security. *North-Holland*, 17(7), 579.

Keegan, C. (2002). Cyber-Terrorism Risk, Financial Executive, *Finance Executive*, 18 (8), 35-7

Keyes, D.& Rapp, M., (1999). How vulnerable is the industry to electronic intrusion? *Electric Perspectives*, 24(5) 60-2.

Catalogue Description

Intensive hands on investigation of computer related crime designed for the profession as an electronic crime investigator. Course prepares students to become effective cyber crime investigators. Students will identify, evaluate, classify, and demonstrate proficiency in investigating computer related crimes. Students subject to background investigation prior to admittance.

Course Objectives: At the conclusion this course, students will be able to:

1. Recognize and describe the functions of internal hardware components of computers.
2. Apply techniques in analysis of sequences in electronic crime.
3. Comprehend motivational factors in deviant behavior of computer criminals.

4. Analyze historical concepts of operating systems.
5. Understand how data is transferred from input devices to electronic media.
6. Analyze the differences in operating systems when performing investigations.
7. Understand network applications for investigations.
8. Evaluate search warrant requirements for computer network centers.
9. Synthesize the procedures of how to structure a cyber crime investigation.
10. Analyze the processes an investigator should follow when searching for evidence on a network.
11. Demonstrate procedures for doing e-mail tracking for use as evidence.
12. Analyze the operation of wireless networks, layering, RF concepts, Ethernets and microchips to assist the investigator in the processing of digital evidence.

Topical Outline – INDT-557 Cyber Crime Investigation I

- I. Historic Analysis of Computer Related Crime
 - a. State and Federal Laws as they pertain to establishing expert witness status.
- II. Importance of historical knowledge of Computer Operating Systems
 - a. Evolution of computer hardware IDE / EIDE / ATA Interface
 - b. Switch settings on Hard Drives, Modems, Printers, Memory, RAM
 - c. DOS Commands MD, CD, DIR, COPY, CHKDSK, DEL, TYPE, RENAME, PATH, ATTRIB
 - d. DOS' Edit Program, Redirection, Wildcards,
- IV. Evaluation of Computer Data (Bits and Bytes)
 - a. From bits and bytes to ASCII
 - b. The ANSI/ASCII standard – what are bits, nibbles, bytes, characters, words, and beyond.
 - c. DISKEDIT in hex mode.
- V. Understand Logical and Physical Characteristics of Hard and Floppy Drives
 - a. Cylinders, Heads, and Sectors
 - b. Verification of the total data capacity of a seized hard drive.
 - c. The difference between Physical and Logical drives.
 - d. Using FDISK to partition a drive

- e. DOS Format – What changes it does and does not make.
 - f. Sectors, clusters, File Allocation Tables (FAT) and system areas
 - g. Un-formatting – Recovery techniques
 - h. Drive Letter Assignment
- VII. Evaluation of the DOS File System and where data could be hidden.
- a. Sectors, Clusters, System Area
 - b. Subdirectory clusters
 - c. Storage issues with respect to size, date and time
 - d. Tracing out the chain of a file
 - e. The problem with slack space
 - f. Understanding the dot and dot-dot pointer.
- VIII. Recovering Erased Files
- a. Deleting files – What changes and what does not
 - b. What it takes to manually unerase a file using Norton's DISKEDIT program
 - c. Automatic unerase using the unerase utility
 - d. Long File Names/Recycle Bin
- IX. Creating Controlled – Boot Floppies, Boot Sequence
- a. Power on sequence
 - b. How to examine CMOS settings – Hard drive parameters, Power-on passwords, drive sequence
 - c. Boot record
 - d. DOS 7 modifications
 - e. Creating an autoexec.bat file
 - f. Hard drive write blockers and other utilities
- X. Motivational Factors in deviant behavior of computer criminals
- a. Financial
 - b. Spite Revenge
 - c. Pedophilia
 - d. E-Bay Fraud
- XII. Process Analysis and Seizure Considerations – Preserving Computer Based Evidence
- a. Pre-Raid considerations
 - b. Raid Kit items: tools, hardware, tape, labels, camera and film
 - c. Securing and processing an electronic crime scene
 - d. Safeguarding evidence
 - e. Evidence analysis considerations
 - f. Duplicate image versus file-by-file copy
 - g. Hardware and software considerations – validation of tools
 - h. Working with SAFEBACK and removable media
 - i. Imaging floppy disks
- XIII. Automated Search Techniques

- a. Identifying Files
 - b. Headers and Extensions
 - c. Keyword concepts
 - d. Working with automated tools and Disk Edit
- XIV. Network Investigations
- a. Network Topologies
 - b. Conducting the Network Investigation
 - c. Dealing with the Network Administrator
 - d. Wireless
- XV. Investigative Framework Methods
- a. Introduction to TCP/IP
 - b. E-Mail Headers
 - c. USENET, News,
 - d. Traceroute
 - e. Ping
 - f. NEOTRACE
 - g. NSLOOKUP
 - h. Host, Message Digest, File Signatures, Cyclic Redundancy Checks
 - i. Break-in-Intrusion Logs
 - j. Kernel Hacking, Root Kits
- XVI. What is Fraud?
- a. An intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right
 - b. Deceit
 - c. Trickery
 - d. Cheating
- XVII. What is an Investigation?
- a. An Investigation is a Search for the Truth
 - b. The Investigator
 - c. The Investigation
 - d. Unbiased
 - e. Truthful
 - f. Integrity
- XVIII. LARCENY
- a. Unlawful taking
 - b. Personal Property
 - c. Intent
 - d. Permanently Deprive
- XIX. Embezzlement
- a. Common Methods

- b. Limited only by imagination.
- c. Cash is received and the employee merely pockets it without making a record of the transaction.

XX Types of Embezzlement

- a. Point of Sale
- b. Payroll Frauds
- c. Kickbacks
- d. Pad expense accounts.
- e. Failure to return property
- f. Inventory theft
- g. Lapping
- h. Real-estate?

XXI. Computer/Internet Related Embezzlement

- a) Do traces of all IP address discovered
- b) 2703f Preservation Letter
- c) Pin register on Suspect's telephone
- d) Search Warrant on ISP's
- e) Forensic on both Complainant's & Suspect's PCU (documents, internet history, e-mail, diary etc...)

XXI. Interviewing/Interrogating Suspect

- a. Interview Suspect at home if possible (not in custody)
- b. Inquire about financial institution/situation
- c. Show empathy
- d. Ask the suspect why did he/she took the money

XXII. If Confession is Obtained

- a. Ask when (time line) and why?
- b. Method of Embezzlement (could be another incident or different crime they are confessing to)
- c. Amount taken
- d. Account for all the money that was taken
- e. Any co-conspirators?
- f. Use search warrants to "freeze" defendant's accounts

XXII. Fraudulent Checks

- a. Definitions
- b. Check: a written order directing a financial institution to pay money as instructed
- c. Counterfeit check: Fraudulent Checks
- d. Uttering & Publishing MCL750.249

XXIII. Fraudulent Checks

- a. Non-criminal
- b. Post dated checks (extension of credit)

- c. Checks returned unpaid for rent (except first payment checks)
- d. Bad checks where partial payment has been accepted
- e. Unpaid checks for legal reason, i.e. Tax levy, court ordered seizure, garnishments

XXIV. Methods of Committing Check Fraud

- a. Theft and forgery of a legitimate check
- b. Issuance of genuine checks to fictitious entities
- c. Alteration of legitimate checks
- d. Duplication or counterfeit copies of checks
- e. Check-Kiting

XXV. CRIMINALS USE COMPUTERS TO COMMIT FRAUD

- a. Fraudulent Checks
- b. Fraudulent Checks
- c. Obtain Original Document
- d. Process for fingerprints
- e. Handwriting analysis (after suspect is arrested)
- f. Needed as Evidence in Court
- g. Fraudulent Checks
- h. Investigative Techniques
- i. Merchants

GRADING REQUIREMENTS

- 1) Quiz 1..... 15%
- 2) Quiz 2..... 15%
- 3) Research Paper..... 30%
 - a. See Attachment for Research Paper Guidelines
- 4) Final Examination..... 40%

100-91 = A
 81 – 90 = B
 71 – 80 = C
 65 – 70 = D
 65 and below = F

All examinations are practical exams involving case studies and recovery of information from electronic media.

Bibliography

- Albanese, J. S. & Pursley, R. D. (1993). *Crime in America: some existing and emerging issues* Upper Saddle River NJ: Prentice Hall.
- Altschuler, B. & Sgroi, C. (1996). *Understanding law in a changing society*. Upper Saddle River NJ: Prentice Hall.
- Ashley, P., and Vandenwauver, M. (1999). *Practical intranet security*, Kluwer Academic Publishers.
- Bequai, A. (1998). A guide to cyber-crime investigations, computers & security. *North-Holland*, 17(7), 579.
- Bequai, A. (1999). Cyber-crime the US experience, computers & security. *North-Holland*, 18(1), 16.
- Bequai, A. (2001). Organized crime goes cyber, computers & security. *North-Holland*, 20(6), 475,
- Caloyannides, M. A. (2001). *Computer forensics and privacy*, Artech House.
- Casey, E, (2000). *Digital evidence and computer crime*, Academic Press.
- CERT (Computer Emergency Response Team) at <http://www.cert.org>, a reporting center at the Software Engineering Institute (SEI) of Carnegie Mellon University.
- Chordas, L. (2001). Cyber-crime fighters with list of top 10 computer viruses. *Best's Review*, 102(8), 107.
- Clark, F., Diliberto, K., and Geberth V. J. (1999) *Investigating computer crime*, CRC Press.
- Computer and Network Security Reference Index* at <http://www.vtcif.telstra.com.au/info/security.html>
- Conly, C. H. (1993). [Organizing for computer crime investigation and prosecution](#), Amazon.com
- Cromwell, P. F. & Dunham, R. F. (1997). *Crime and justice in America: realities and future prospects*. Upper Saddle River NJ: Prentice Hall.
- Croydon, H. (2002). Making sense of cyber-exposures. *National Underwriter*, 106(24) 26, 28-9
- Denning, D.E. & Denning, P.J., *Internet besieged – countering cyberspace scofflaws*, Addison-Wesley.

- Escamilla, J. (1998). *Intrusion detection – network security beyond the firewall*, Wiley & Sons, Inc.
- Falconer, T. (1995). Cyber crooks., *CA Magazine*, 128, 12-17
- Gabrys, E. (2002). The international dimensions of cyber-crime, part 2: A look at the council of europe's cyber-crime convention and the need for an international regime to fight cyber-crime. *Information Systems Security*, 11(5) 24-32
- Garfinkel, S. (1997). *Web security & commerce*, O'Reilly & Associates, Inc.
- Garfinkel, S.(1998). The FBI's cyber crime crackdown, technology review. *Technology Review*. 105(9) 67-8, 70, 72, 74.
- Garfinkel, S., and Spafford G. (1996). *Practice UNIX and internet security*, O' Reilly.
- Goch, L. (2002). Demands for coverage increase as cyber-terrorism risk is realized. *Best's Review*, 102 (9), 59.
- Gripman, D. L. (1997). The doors are locked but the thieves and vandals are still getting in: A proposal in tort to alleviate corporate America's cyber-crime problem, *Software law journal*, 16(1) 167.
- Howard, L. S. (2002). Insurers scramble for cover in chaotic property remarket., *National Underwriter (Property & Casualty/Risk & Benefits Management Edition)*, 106 (7), 12-13
- Icove, D. J., Seger, K. and, VonStorch, W., (1995). Computer crime: a crimefighters handbook, O'Reilly and Associates
- InfoSec and InfoWar Portal maintained at <http://www.infowar.com>.
- Johnsson, J. (2001). Insurers hedging cyber-crime risk, prepare to pay more for computer crime coverage, *Crain's Chicago Business*, 24(50) 1, 32
- Keegan, C. (2002). Cyber-Terrorism Risk, Financial Executive, *Finance Executive*, 18 (8), 35-7
- Keyes, D.& Rapp, M., (1999). How vulnerable is the industry to electronic intrusion? *Electric Perspectives*, 24(5) 60-2.
- Kruse, W. G. & Heiser, J. G. (2001). *Computer forensics: incident response essentials*, Addison Wesley.
- Larson, E. & Stephens, B. (2000). Web Servers, Security, & Maintenance, Prentice-Hall,
- Liddle, A. J. (2000). Survey: corporate, government computer crime and related costs rising, *Nation's Restaurant News*, 34(22) 54.
- Linux links at <http://topology.org/soft/linux.html>

- Maiwald, E. (2001). *Network security: A beginner's guide*, Osborne, McGraw-Hill.
- Marcella, A.J. & Greenfield, R.S. (2002). *Cyber forensics*, CRC Press, Auerbach Publications.
- Microsoft Windows 2000 Security: Technical Reference, Microsoft Press, 2000
- Nemeth, E., Anyder, G., Seebass, S., and Hein, T.R. (2001). *unix system administration handbook*, (3rd ed). Prentice-Hall.
- Network Security Library maintained at <http://secinf.net>.
- Newville, L. L. (2001). Cyber crime and the courts - investigating and supervising the information age offender, *Federal probation*. 65(2) 11.
- Northcutt, S., Cooper, M., Fearnow, M., and Frederick, K. (2001). *Intrusion signature and analysis*, New Riders.
- Parker, D. B. (1999). Fighting Cyber Crime: Good and Bad Control Objectives, *Computer Security Journal*. 15(1) 11.
- PC Guide at <http://www.pcguides.com/topic.html>
- Pounder, C. (2001). The council of Europe cyber-crime convention, computers & security. *North-Holland*, 20(5) 380.
- Pounder, C. (2002). Cyber crime: the backdrop to the council of Europe convention Internet crimes. *Time*, 155(14) 50-1.
- Radcliff, D. (2000). The cyber-mod squad sets out after crackers., Secret Service's Electronic Crimes Task Force, *Computerworld* 34(25) 44-5.
- Radcliff, D. M. (2002). Cybersleuthing solves the case., *Computerworld*, 36(3) 36-7.
- Richardson, P. (2001). The code of silence, computer crime is rising in Chicago area but firms reluctant to say so, *Crain's Chicago Business*, 24(37) 15, 18-20.
- Roberts, S. (2002). Companies' exposure to cyber terror growing, *Business Insurance* 36 (48)10, 16, 18.
- Rosenblatt, K. S. (1995), [High-technology crime: investigating cases involving Computers](#), KSK Publications.
- Schiffman, M. (2001). *Hacker's challenge*, Osborne/McGraw-Hill.
- Sinrod, E. J. & Reilly, W. P. (2000). Cyber-Crimes: A practical approach to the application of federal computer crime laws, *Santa Clara Computer and High-Technology Law Journal*, 16(2), 177.

- Skoudis, E. (2002). *Counter hack*, Prentice Hall.
- Strebe, M., Perkins, C., and Moncur, M.G. (1999). *NT 4 network security*, (2nd ed.) SYBEX Inc.
- Taylor, C., (2001). HR versus the cyber-criminals, *People Management* 7(18)11.
- Thomas, R. and Seanor, J. (1997). *Computer crime law for the investigator*, O'Reilly and Associates.
- Trembly, A. C. (1999). Cyber crime means billions in losses, *National Underwriter (Life & Health/Financial Services Edition)*103(27) 37.
- Trembly, A. C. (2002). Cyber Attacks Bleed U.S. Companies, *National Underwriter (Property & Casualty/Risk & Benefits Management Edition)* 106(28) 22-3.
- Trembly, A. C. (2002). In The Battle To Protect Computer Systems, Our Shields Are Failing Badly. *National Underwriter (Life & Health/Financial Services Edition)* 106(15) 36, 39.
- Trembly, A. C. (2002). Instant messaging leaves firms exposed., *National Underwriter (Property & Casualty/Risk & Benefits Management Edition)* 106(9) 28-29.
- Trembly, A. C., (2002). Cyber crime means billions in losses., *National Underwriter (Property & Casualty/Risk & Benefits Management Edition)* 103(26) 19
- Veysey, S. (2000). Many U.K. companies lack cyber cover: survey., *Business Insurance* 34(25)24-5.
- Waller, D. C. (1995). Onward cyber soldiers, *Time*,146 38-44
- Webber, J. (2001). Combating cyber-crime: at what costs? *Law/technology*,34(2) 26.
- Wright, S. W., Campus cops try to fill role as cyber superheros., *Black Issues in Higher Education*,17(13)64-5.