

## COURSE OUTLINE

COURSE TITLE: COMPUTER FORENSICS II

COURSE NUMBER: Ia-558

CREDIT HOURS: 3 Graduate

PREPREGUISITE: IA – 533 Computer Forensics I

### CATALOG DESCRIPTION

Comprehension of network forensic investigations and application of investigative framework methodologies. Students will apply Linux for forensic analysis, and Access Data Forensic Tool Kit. Evaluation of Steganography tools and field acquisition of electronic media will be presented.

### COURSE OBJECTIVES

At the conclusion of this course, the student will be able to:

1. Analyze network hardware involved in intrusion detection.
2. Comprehend the variables in network search warrant requirements.
3. Apply the necessary methodologies to conduct a computer forensic examination.
4. Application of Linux operating system for forensic analysis of seized media.
5. Evaluate password recovery tools (PRTK) and Distributed Network Attack Software.
6. Analyze hidden information from pictures and digital audio files utilizing Steganography software.
7. Describe field acquisition problems and solutions of image acquisition issues in hardware and software.

## COURSE OUTLINE

- I. Forensic Network Investigations
  - a. Network Computer Components
  - b. Working with Network Administrators
  - c. Search Warrant Issues Related to Network Centers
  
- II. Investigative Framework Methods
  - a. Cybercrime Methodologies
  - b. Structure of Cybercrime Investigations
  - c. Case Management – Pursue or Drop
  
- III. Linux for Forensic Analysis
  - a. Introduction of Linux Operating Systems
  - b. Various Types of Linux
  - c. Unix Networks
  - d. Linux Forensic Tools
  
- IV. Access Data – Password Recovery Tool Kit Software
  - a. Password Recovery Issues / Investigations
  - b. Profile of the Suspect / Password Database
  - c. Password Recovery Toolkit
  - d. Distributed Network Attack Software
  
- V. Steganography
  - a. Explanation and Usages
  - b. How Steganography Applies to Computer Forensics
  
- VI. Field Acquisition Kit and Methodology
  - a. Field Acquisitions of Electronic Media
  - b. Hardware Requirements
  - c. Methodology of Field Acquisitions

## 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

## **Bibliography**

- Bick, J. (2000). *101 things you need to know about internet law*, Three Rivers Press.
- Casey, E. (2000). *Digital evidence computer crime: forensic science. computer and the internet*, Academic Press.
- Casey, E. (2001). *Handbook of computer crimes investigation: forensic tools & technology*, Academic Press.
- Cavazos, E., & Morin, G. (1996). *Cyber-space and the law: your rights and duties in the on-line world*, Massachusetts Institute of Technology.
- Caloyannides, Michael. (2001). *Computer forensics and privacy (artech house computer security series*, Sequoia Publishing, Inc.
- Defleur, Margaret. (2002). *Computer-assisted investigative reporting: development and methodology*, Lawrence Erlbaum Associates.
- Furnell, S. (2002). *Cybercrime: vandalizing the information society*, Pearson Education Limited.
- Ferguson, N., & Schneier, B. (2001). *Practical cryptography*, John Wiley & Sons Publishing.
- Glover, T., Young, M., (2000). *Pocket PCRef: hardware and software for the computer forensic community (10<sup>th</sup> Ed.)*, Sequoia Publishing, Inc.
- Harvey, G. (1998). *DOS for dummies: quick reference 3<sup>rd</sup> edition*, IDG Books Worldwide, Inc.
- Kovacich, G. L., Kovacich, G., & Boni, W. (1999). *High technology crime investigator's handbook*, Butterworth-Heinemann.
- Kruse II, W., & Heiser, J. (2002). *Computer forensics: incident response essentials*, Lucent Technologies.
- Loader, Brian. (2000). *Cybercrime: security and surveillance in the information age*.

Routledge.

Mandia, K., & Prosser, C. (2001). *Incident response: investigation computer crime*, McGraw-Hill Companies.

Marcella, A., & Greenfield, R. (2002). *Cyber forensics: a field manual for collecting, examining, and preserving evidence of computer crimes*, Auerbach Publications.

McClure, S., Scambray, J., & Kurtz, G. (2001). *Hacking exposed: network security secrets & solutions (3<sup>rd</sup> ed.)*, McGraw Hills Companies.

Meadhra, M., Rampling, B., & Correll, R. (2000). *Windows 2000 professional bible*, Hungry Minds Inc.

Mena, Jesus. (2003). *Investigative data mining for security and criminal detection, first edition*. Butterworth-Heinemann.

Middleton, Bruce. (2002). *Cyber crime investigator's field guide*, Auerbach Publications.

Minsasi, M. (2002). *The complete pc upgrade and maintenance guide: (with CD- ROM)*, Sybex Publishing.

Minasi, M., York, D., & Hunt, C. (2000). *Linux for windows NT/2000 administrators: the secret decoder ring*, Sybex Publishing.

Mueller, S., (2001). *Upgrading and repairing PC's (13<sup>th</sup> edition)*, Que Publishing, Inc.

Murray, K. (2003). *Faster smarter microsoft office X*. Microsoft Corporation.

Negus, C. (2002). *Red hat linux 8 bible*, Wiley Publishing, Inc.

Phillips, Amelia. (2003). *Guide to computer forensics investigation*. Course Technology.

Piper, F., & Murphy, S. (2002). *Cryptography: a very short introduction*, Oxford University Press.

- Richards, J. (2002). *Transnational criminal organizations, cybercrime, and money laundering: a handbook for law enforcement officers, auditor (2<sup>nd</sup> edition)*, CRC Press.
- Rosch, W. (2003). *The Winn L. Rosch hardware bible 6<sup>th</sup> edition*, Que Publisher, Inc.
- Russell, D., & Gangemi, G., (1991). *Computer security basics*, O'Reilly & Associates, Inc.
- Sammes, T., Jenkinson, B., & Sammes, A. (2000). *Forensic computing: a practitioners guide (practitioner series)*, Springer Verlag.
- Schweitzer, D. (2003). *Incident response: computer forensics toolkit*, Hungry Minds, Inc.
- Shinder, D., & Tittel, E. (2002) *Scene of the cybercrime: computer forensics handbook*, Syngress Publishing, Inc.
- Simpson, A. (2001). *Windows XP bible*, Hungry Minds, Inc.
- Smith, F., & Bace, R. (2002). *A guide to forensic testimony: the art and practice of preserving testimony as an expert technical witness*, Addison Wesley Professional.
- Stephenson, P. (2000). *Investigating computer-related crime*, CRC Press.
- U.S. Government. (2003). *21st century guide to cybercrime: the computer crime section of the justice department and the national infrastructure protection center - hacking, intellectual property crimes, policy, cases, guidance, laws, documents, economic espionage, privacy issues, internet and web crimes, cyberethics, threat assessments, intrusion targets (core federal information series CD-ROM)*. Progressive Management.
- U.S. Government. (2003). *2003 guide to computer and internet crimes and cybercrime: hacking, intellectual property crimes, policy, cases, guidance, laws, documents, web crimes, targets (core federal information series CD-ROM)*. Progressive Management.

Vacca, J., & Erbschloe, M. (2002). *Computer forensics: computer crime scene investigation (with CD-ROM)*, Charles River Media.

Welsh, M., Laufman, L., Dalheimer, M., & Dawson, T. (2002). *Running linux, fourth edition*, O'Reilly & Associates.

Wilding, Edward. (1997). *Computer evidence: a forensic investigations handbook*. Sweet & Maxwell, Ltd.

Zaenglein, N. (2000). *Secret software: making the most of computer resources for data protection, information recovery, forensic examination, crime investigation and more*, Paladin Press.