

CGS 5132, Spring 2007

S. Lang Syllabus for CGS 5132, Computer Forensics II January 8, 2007

Instructor: Dr. S. Lang 207 Harris Center, (407) 823-2474, lang@cs.ucf.edu	Instructor's Office Hours: <ul style="list-style-type: none">• Tuesday: 3 to 4 pm; and Thursday: 2 to 4 pm (in Rm. 207 of Harris Center)• Wednesday: 6 to 9 pm (by appt., Rm. 315 of NCFS)
---	--

(Optional) Texts:

[*Digital Evidence and Computer Crime*](#), Second Edition, by E. Casey, Academic Press, March 2004, ISBN 0-12-163104-4.

[*Hacking Exposed*](#), 5th Edition (Paperback), by Stuart McClure, Joel Scambray, George Kurtz (Paperback), McGraw-Hill Osborne, 2005, ISBN-10: 0072260815.

[*Incident Response and Computer Forensics*](#), Second Edition, by K. Mandia, C. Prorise, and M. Pepe, Osborne/McGraw-Hill, March 2003, ISBN 0-07-222696-X.

Objectives:

- Learn the concepts of
 - computer system security models
 - cryptography
 - fundamentals of computer networking and the layered protocol architectures
 - detection and prevention of intrusion and attack
 - digital evidence collection and evaluation
 - legal issues involved in network forensic analysis.
- Use documented cyber crimes and intrusion records as case studies
- Emphasize both the conceptual models and the hands-on experience of using tools with the Internet and the Web browsers as the underlying media.

Topics:

Security models	user identification and authentication, access control lists.
Cryptography	cryptographic algorithms, key management, password protection
Computer networks	TCP, UDP, IP protocols of the Internet
The Web	HTTP, DNS, Email and SMTP, telnet, ftp
Taxonomy of Computer Attacks	system flaws (buffer overflows, out-of-band data, CGI coding), insecure OS, poor configurations, communication vulnerabilities, attacks on network communications (denial-of-service, Emails, packet sniffing, TCP hijacking, routing attacks, sequence number guessing)
Intrusion Detection and Prevention	system logs, audit trails, monitoring, firewalls, vulnerability scanning, Intrusion Detection System (IDS) tools on UNIX and Windows NT systems.
Forensic Analysis	statistical and pattern matching techniques, case studies of documented attacks and analyses, legal issues (securing and documenting the attacks, digital evidence collection and evaluation, reporting and help).
Presentation and projects	evaluation of presentations and projects

Prerequisites:

Undergraduate degree in CS or a closely related field, or Computer Forensics I, or permission of the course instructor.

Grading Policy:

- Homework assignments (50%)
- Online tests (30%)
- Presentation or term project (20%)

Course Websites:



<http://www.cs.ucf.edu/courses/cgs5132/spr2007>



<http://webct.ucf.edu/webct/public/home.pl>

Online References

- (1) Internet Resources for Computer Forensics at <http://faculty.ncwc.edu/toconnor/426/426links.htm>, a part of Professor O'Connor's criminal justice megalinks at <http://faculty.ncwc.edu/toconnor/default.htm>.
- (2) The Electronic Evidence Information Center: <http://www.e-evidence.info/>
- (3) Computer Forensics, Cybercrime, and Steganography Resources: <http://www.forensics.nl>
- (4) The Computer Technology Documentation Project: <http://www.comptechdoc.org/index.html>
- (5) Forensic Science Resources: http://www.tncrimlaw.com/forensic/f_crimescene.html
- (6) Forensic Evidence Master Index: <http://www.forensic-evidence.com/site/MasterIndex.html>
- (7) *CERT* (Computer Emergency Response Team) at <http://www.cert.org>, a reporting center at the Software Engineering Institute (SEI) of Carnegie Mellon University, for Internet security problems.
- (8) *Network Security Library* maintained at <http://secinf.net>, which provides links to online publications related UNIX, Windows, WWW, firewalls, security.
- (9) *Security Resources* of security related organizations and agencies, publications, tools, ethics and law, at <http://www.tnn.com/tnn/resources/security.htm>, a part of Guy's list of Internet Resources at <http://www.tnn.com/tnn/resources/guylist.htm>.
- (10) TUCOFS - The Ultimate Collection of Forensic Software at <http://www.tucofs.com/tucofs.htm> covering lots of links.
- (11) Linux links at <http://www.topology.org/soft/linux.html>, <http://loll.sourceforge.net/linux/links/>, each have lots of links.
- (12) Wayne's Forensics and Incident Response Resources page at <http://www.windowsnetworking.com/kbase/WindowsTips/WindowsXP/AdminTips/Security/WaynesForensicsandIncidentResponseResources.html>.
- (13) Craig D. Ball's page on helping lawyers master technology, at <http://www.craigball.com/>.
- (14) Ken Withers's page with links to resources on computer-based disclosure and discovery in civil litigation, at <http://www.kenwithers.com>.
- (15) Legal and business publications from Pike & Fisher on digital discovery and e-evidence at http://www.pf.com/law_internet_digitaldisc.asp.