Security 508

System Forensics, Investigation & Response

Week 1

Agenda

- Introductions
- How to Get the Most Out of This Course
- GIAC Certification Overview

About the Class

- 10 Class Meetings
  - Tuesday, 6:30pm to 8:30pm
  - Last class on March 25th

- Questions
  - Via email
  - Via Phone appointment

About the Class (2)

- Class Time
  - Overview of the material
  - Questions and discussion
  - Demos, tools, additional resources
  - Exercises and challenges with the lab

About the Class (3)

- Actively participate to get the most out of the class
- Share experiences
- Ask and answer questions
- Prepare for the exams
- Evaluations - Offer comments, suggestions, feedback

Study Plan

- Read assigned material ***prior*** to each meeting
- Listen to MP3 live conference audio files
- Review material and highlight
- Take practice tests
- Ask questions
- Have fun!

SANS Live Conference MP3 Audio Files

- You have access to SANS live conference MP3 Audio Files in your Portal Account.
- These files are available for 4 months, not just the 10 weeks of the course.
- Download the MP3 files so you can review them again, once the class is over.
- Listen to the audio files as often as possible.

Course Schedule

- Week 1 – Introduction & Certification Overview
- Week 2 – Essentials
- Week 3 – IR & Volatile Evidence Gathering
- Week 4 – Hard Drive Evidence Acquisition
- Week 5 – File System Forensic Analysis, and Automated Toolkits

Course Schedule (cont.)

- Week 6 – Windows Imaging, and & Volatile Evidence Gathering
- Week 7 – Windows Media & Artifact Analysis, and Windows Challenge
- Week 8 – Computer Investigative Law
- Week 9 – Advanced Forensics & Forensic Challenge
- Week 10 – Wrap Up & Forensic Challenge

SANS Code of Ethics

- You will respect the SANS' right to this intellectual property
  - Some students think they can attend this course and then share the course materials with their colleagues
  - Some will even try to sell books on eBay
- The entire contents of this course are the property of the SANS Institute.

  "User may not copy, reproduce, distribute, display, modify or create derivative works based upon all or any portion of this publication, in any medium whether printed, electronic or otherwise."
- You will not plagiarize other people's work (for optional Gold certification technical paper assignment)

SANS Copyright Policy

- SANS Copyrighted Information
  - DO NOT distribute any of the SANS training materials to anyone else. This is licensed to you and you only!
  - All online materials are copyrighted. Do not distribute. Copyright information is in all the different areas of SANS, please review.
  - You CAN provide links to the public material on the SANS website, to direct others to where they can read the information.

Intellectual Property

- Some students think they can attend this course and then share the course materials with their colleagues
- Some will even try to sell books on eBay

You May Not Teach Someone Else This Material

- User may not do any of the items listed on the previous slide for any reason, and "especially not for the purposes of teaching any computer or electronic security courses to any third party."

Online Study Materials

SANS Local Mentor Program provides:

- SANS live conference MP3 Audio Files
- Course Syllabus