



Advanced Forensic Techniques  
March 8, 2008  
9:00 am - 6:00 pm

Georgetown University  
Clarendon Campus

### Syllabus

Chris McGrath, CPA

#### Course Description/Objectives:

This class concentrates on advance tools to detect fraud. The emphasis will be on computer assisted forensic techniques. Statistical techniques, data quality integrity and computer recovery methodologies will be reviewed.

#### Course Textbook/Materials:

No textbook is required; course materials to be provided.

#### Class Schedule (subject to change depending upon the progress of the class):

##### Part One

1. Introduction
  - a. History of computer forensics
  - b. Evidence, Warrants, 4<sup>th</sup> Amendment, and Commonwealth v. Copenhefer
  - c. Computer evidence
  - d. Activities of an investigator
  - e. Class discussion – manager surfing restricted websites
  - f. Basic Process
2. Crime Scene Investigating
  - a. Preservation
  - b. Collection
  - c. Analysis
  - d. Legal evidence
3. The Business Environment
  - a. Taking a step back
  - b. The risk of doing business
  - c. Basic processes and business
  - d. The business need

- e. Computer Assurance vs. Crime Scene Investigation
- 4. Business and IT
  - a. Risk, threats and controls
  - b. The computerized business
    - i. Business elements
    - ii. Business model
    - iii. Barings
  - c. Looking at data
  - d. Case 1 – Travel reimbursements
  - e. Business cycles
- 5. Expenditure cycle
  - a. Attributes of integrity
  - b. How to test?
  - c. Case 2 – You are the new controller

#### Part Two

- 1. Computer forensic case
  - a. Database forensics
  - b. Computer evidence
- 2. Chain of custody
  - a. Disk evidence
  - b. What is evidence?
  - c. E-Discovery
  - d. Best evidence rule
- 3. Obtaining evidence
  - a. Getting evidence
  - b. Where is the evidence?
- 4. Recent trends
  - a. Emails: Federal Rules of Civil Procedure
  - b. Tools
    - i. Encase
    - ii. F.R.E.D.
    - iii. Common tools
- 5. Analysis
  - a. Logs
  - b. Metadata
  - c. Steganography (example)
- 6. More evidence
  - a. Emails
  - b. Frying a hard disk
  - c. Company secrets
- 7. Best practices

Contact information: Chris McGrath, CPA (410) 979-7223