COURSE OUTLINE

JUST365 / CITA365 Digital Forensic Analysis

Prepared By: Robert Edwards and William Mein
Revised By: Robert House

SCHOOL OF SCIENCE, HEALTH, AND PUBLIC SERVICE
and
CANINO SCHOOL OF ENGINEERING TECHNOLOGY
MARCH 2013
A. **TITLE:** Digital Forensic Analysis

B. **COURSE NUMBER:** CSIT365/CSIT365

C. **CREDIT HOURS:** 3

D. **WRITING INTENSIVE COURSE (OPTIONAL):** No

E. **COURSE LENGTH:** 15 Weeks

F. **SEMESTER(S) OFFERED:** Spring

G. **HOURS OF LECTURE, LABORATORY, RECITATION, TUTORIAL ACTIVITY:** Two hours lecture, two hours laboratory per week

H. **CATALOGUE DESCRIPTION:** This course is designed to prepare the student to complete forensic analysis of digital media and to understand the process and technical challenges of internet investigations. The course looks specifically at how to obtain evidence from digital media, how to process network messages and logs while preserving the evidentiary chain, and how to adhere to the legal requirements of the search and seizure of digital media and related equipment and information.

I. **PRE-REQUISITES/CO-REQUISITES:**
   a. Prerequisites
      - CITA171 Operating System Fundamentals or
      - Permission of the instructor.
   b. Co-requisites: None.

J. **GOALS (STUDENT LEARNING OUTCOMES):**

   Upon completion of the course, the student will be able to:

<table>
<thead>
<tr>
<th>Course Objective</th>
<th>Institutional SLO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Describe the role of computer forensics.</td>
<td>3. Professional Competence</td>
</tr>
<tr>
<td>2. Demonstrate an ability to apply computer forensics to investigations.</td>
<td>2. Critical Thinking</td>
</tr>
<tr>
<td>3. Demonstrate the ability to perform a computer forensic analysis using computer and network-based tools.</td>
<td>2. Critical Thinking</td>
</tr>
<tr>
<td>4. Analyze case studies involving collaborative investigation techniques.</td>
<td>3. Professional Competence</td>
</tr>
<tr>
<td>5. Describe the concepts of how data are stored on digital devices.</td>
<td>2. Critical Thinking</td>
</tr>
<tr>
<td>6. Describe the process of computer forensic analysis.</td>
<td>3. Professional Competence</td>
</tr>
<tr>
<td>7. Apply current knowledge and techniques to the analysis of digital devices.</td>
<td>2. Critical Thinking</td>
</tr>
<tr>
<td>8. Construct a comprehensive report of forensic analysis.</td>
<td>1. Communication</td>
</tr>
<tr>
<td></td>
<td>3. Professional Competence</td>
</tr>
</tbody>
</table>
K. **TEXTS:**

*System Forensics, Investigation and Response.* John Vacca and K. Rudolph. (Jones and Bartlett, 2011).

*Laboratory Manual to Accompany System Forensics, Investigation and Response.* (Jones and Bartlett, 2013).

Virtual Lab access – available with the textbook bundle listed above.

L. **REFERENCES:**

M. **EQUIPMENT:** Computer and Internet access.

N. **GRADING METHOD:** A-F

O. **MEASUREMENT CRITERIA/METHODS:**

- Participation
- Reports
- Lab Assignments
- Tests

P. **DETAILED TOPICAL OUTLINE:**

1. The System Forensics Landscape
   - System Forensics Fundamentals
   - Overview of Computer Crime
   - Challenges of System Forensics
   - Forensics Methods and Labs
2. Technical Overview: System Forensics Tools, Techniques, and Methods
   - System Forensics Technologies
   - Controlling a Forensic Investigation
   - Collecting, Seizing, and Protecting Evidence
   - Investigating Information-Hiding Techniques
   - Recovering Data
   - Investigating and Scrutinizing E-mail
   - Performing Network and Internet Analysis
   - Searching Memory in Real Time with Live Systems Forensics
3. Emerging Technologies, Future Direction, and Resources
   - Incident/Intrusion Response
   - Future Directions

Q. **LABORATORY OUTLINE:**

Assignments using the *JBL Virtual Security Cloud Labs* which provides a "virtual sandbox" for students to practice coursework on an actual IT infrastructure.

1. Perform a Byte-Level Computer Audit
2. Apply the Daubert Standard on the Workstation Domain
3. Create a Forensic System Case File for Analyzing Forensic Evidence
4. Uncover New Digital Evidence Using Bootable Utilities
5. Automate Digital Evidence Discovery Using Paraben's D3 Commander
6. Extract Artifacts from an Image File
7. Decode an FTP Protocol Session and Perform Forensic Analysis
8. Automate Image Evaluations and Identify Suspicious or Modified Files
9. Craft an Evidentiary Report for a Digital Forensic Case
10. Perform an Incident Response Investigation for a Suspicious Logon