|  |  |
| --- | --- |
| **ELEMENT** | **CONTENT** |
| DEPARTMENT | CIS |
| AUTHOR (S) | Jack Skoda |
| COURSE NUMBER | **CIS 4310** |
| COURSE TITLE | **Computer Forensics** |
| SHORT TITLE | Comp Forensics |
| COURSE LEVEL | 4000 |
| DATE CREATED |  |
| CHECKED/CHANGED | 2/28/2017 |
| PREREQUISITES | CIS 2151, 2230 |
| COREQUISITES |  |
| RESTRICTIONS |  |
| SPECIAL FEES | No |
| CREDITS | 3 |
| HOURS | 3 hours of lecture per week |
| SEMESTER | Fall |
| COURSE DESCRIPTION | This class is an introduction to digital forensic methods, practices, technology, and legal concerns. The student considers issues of incident response and handling, data collection, chain of evidence, data analysis, cryptanalysis, steganography, and report writing. |
| SUGGESTED TEXTS | *Incident Response and Digital Forensics*; Kevin Mandia |
| OPTIONAL TEXTS | *File System Forensics Analysis*; Brian Carrier |
| COURSE OUTCOMES | The successful student will be able to:   1. Respond to a computer security incident 2. Conduct a computer security investigation 3. Analyze computer evidence |
| COURSE CONTENT | 1. Legal considerations of digital forensics    1. Relevant state laws    2. Relevant federal laws    3. International cyber law    4. Policy 2. Incident response    1. What is incident response?    2. Planning for IR    3. Handling the incident    4. Case study of current incident 3. Data Collection    1. Chain of custody for evidence    2. Handling digital evidence    3. Crime scene processing    4. Collecting evidence from Windows (aka live response)    5. Collecting evidence from Linux (aka live response)    6. Collecting network evidence 4. Cryptanalysis    1. History of cryptanalysis    2. Frequency analysis    3. Brute force attacks    4. Side channel attacks 5. Steganography and data hiding    1. Methods for hiding data in Windows    2. Methods for hiding data in Linux    3. Stego tools    4. Stego detection tools 6. Presenting evidence    1. Writing forensic reports    2. Presenting forensic evidence |
| LAB/STUDIO OUTCOMES |  |
| LAB/STUDIO CONTENT |  |
| LECTURE CAPACITY | 32 |
| LAB CAPACITY |  |
| GRADED OR P/NP | Graded |
| EVALUATION | Participation, quizzes, exams, homework |
| DELIVERY METHOD | HYB |
| ROOM REQUIREMENTS |  |
| AUTHOR’S NOTES |  |