Computer Forensics Essentials: In International Contexts

Spring Semester 2015
INFO 5571
CRD 24722

Instructors: Corey Schou, Ph.D. & Larry Leibrock, Ph.D.
Emails: Schou@iri.isu.edu & Leiblarr@isu.edu or larry.leibrock@gmail.com
Office: TBA  Phone: 907-599-0251
Skype: leiblarr@skype.com or Googlehangout (Gchat) larry.leibrock@gmail.com
Office hours: Monday 0800 - 0900 (or by appointment)
Class Times and Meetings: Monday 1500 to 1745 - Classroom TBA
Teaching Assistant: TBA

Learners and Overarching Course Objectives
This is a clinical course that provides learners at both the undergraduate and graduate levels, with an introduction and practical, hands-on experience in conducting Digital Forensic Science. Prospective learners will come from Idaho State University - Computer Science, Informatics and Political Science disciplines. International students are welcomed to enroll in this course. Special attention will be directed on international policies dealing with data privacy, rules of evidence and nation-state concerns about proper access and use of data derived from surveillance and digital data capture. International standards and prevailing data security issues will be a feature of this course.

Interdisciplinary Focus
This broadly construed, interdisciplinary pedagogy includes; Socratic-styled questioning, directed out-of-class readings, case-discussions, learner-centered inquiry, exercising critical thinking techniques, hands-on practice for thoughtful and rigorous examination focused on these topics;

1) Data privacy laws and compliance with international, nation-state and local government investigative requirements
2) Appropriate engagement/authorization and posed statement-of-work requirements
3) Proper acquisition of items of evidentiary interest,
4) Authentication of entire corpus, items, artifacts, extracts,
5) Classification and Identification forensics processes
6) Comparisons and Attribution forensics processes,
7) Forensics Analytical verification techniques,
8) Developing fact-based observations,
9) Developing sufficient reporting,
10) Defending reports, evidentiary artifacts and forensics findings,
11) Development of inter-disciplinary skills in understanding and properly utilizing digital forensics terms-of-art.

Learner Outcomes
There are two interdependent learning outcomes in this course.

1. Given a lawful and ethical search task, using a basic forensics toolkit, successfully acquire, investigate, safeguard one questioned digital artifact, prepare a sufficient report and defend the report to a notional trier-of-fact, in accord with prevailing forensics procedures and tradecraft.

2. Achieve, understand and critically develop the sufficient level of; computer forensics techniques, skills, knowledge, legal and ethical experiences in order to successfully deal with the prevailing industry-standard

Acknowledgement - Larry Leibrock, as a learner among learners wishes, to acknowledge and thank my pervious instructors, students and the wide range of forensics investigations, in giving me the foundational and wonderful opportunity to both practice and teach in the exciting area of digital forensics. I am privileged and thankful to have this exemplary opportunity.

For this course, the terms and basic conceptualizations of digital and computer forensics are used interchangeably. There are extant distinctions but they are not material to this course.

Copyright© Asserted by Larry Leibrock
certification examination - Certified Forensics Professional (CCFP)® administered by the ISC²® and agree to the ISC² code of ethics. https://www.isc2.org

Vehicle for Learners
A comprehensive range of ethical concerns, national and international laws, technical and managerial topics will be critically presented assessed, providing students with both theoretical and decisional insights into the professional forensics discipline. Students will have an opportunity to work with X-Ways, Winhex® EnCase®, Access Data FTK® and other forensic programs, which will offer practical hands-on experience with currently utilized forensic equipment and other forensic software tools. A range of US and international data control topics concerning data privacy, surveillance, electronic evidence in litigation, data retention, data destruction, litigation, internal investigations, regulatory compliance and system incident response will also be critically explored within the context of digital forensics case-discussions.

Adult learners, as a highly valued source of future knowledge-workers, who will assume extensive responsibilities in technical, managerial or policy making leadership positions - in the emerging and digitally interconnected world, an understanding of computer forensics is important. Skilled computer science students, information assurance specialists and political-science trained policy makers will require a deepening knowledge, skills and training with digital forensics, in order to make knowledgeable decisions, insightful judgments, mitigate a variety of risks and facilitate compliance with our data laws regulations and societal needs.

The posed course accomplishes these aforementioned needs by:

- Assessing the roles of digital forensics practices in international and nation - public and private investigations,
- Discovering the specific areas of media representation, media forms, network interactions and software-hardware-user interactions,
- Introducing the prevailing, over-arching digital forensic science concepts and terms-of-art,
- Probing the potential risk/benefits, limitations and uncertainties concerning digital forensics practices,
- Providing active learning, collaborative teams to conduct “hands on” exercises to practice case investigations.
- Stimulating some potential utility and cautionary awareness of ethical issues raised by the use of digital forensics
- Utilizing current exam preparation materials to rigorously prepare for and successfully complete the Certified Cyber Forensics Professional Certification® exam.

Required Course Materials

- TEACHING NOTE: Information Assurance & Digital Security -Making Good Use of Socratic Methods & Questioning in Dealing with A Complex Case© Available in ISU Course Moodle
- One (1) bound composition book or laboratory notebook 100 pages 9.75 inch by 7.5 inch
- A Digital signing Certificate issued by the Instructor

Required Computer Hardware

- In order to complete this course you are required to have day-to-day use have a functional Windows® 7 or 8 personal computer. This computer must have internet access to ISU and Moodle services. You must have these
two items (1) a CD drive-capable of read/writes and burning ISO media and (2) at least 1 X 500 GB (minimum capacity - you can get larger one if your want) USB ancillary drive. You must bring the computer, and USB Drive, with power supplies to each class meeting.

Recommended Materials and Useful References for Forensics Professional Development (Not Required for this Course)

- A magnifier lens
- A metallic ruler
- A pair of mechanics gloves
- A static electricity “monkey” strap
- An inexpensive computer tool kit
- An inexpensive digital camera
- *Cybercrime Case Presentation, Shavers, 2013, ISBN 978-0-12-409504-5*
- Sharpie® Fine Tip pens
- *Windows Forensics Analysis Toolkit Windows 8, Carvey ISBN 978-0-12-417157-2*

**Learning Modality**

Explicitly stated - this course will not use of the prevailing professor lecture method. Class discussions will employ the Socratic questioning model. We will make continual and disciplined use of the *Question - Elicit - Demonstrate - Assess* clinical teaching method. Learners are expected to complete readings, prepare assignments and come to class prepared to engage in case-discussions.
Note about the Professor and Attributions
I am a former employee of the US Intelligence Community, I am now retired from US government service. In this retired status, the US Intelligence community does not review, provide information or gives any direction to either the content or delivery of this University course, whatsoever. Note, that I am entirely responsible for the creation, pedagogy, content and conduct of our discussions and assignments. Any opinions, perspectives, analyses that I present in the course of our learning activities are mine alone and should not be attributed to the US Intelligence Community or any respective US government agency.

Attributions
I purpose to make use of the Chatham House Rule for all of our classroom and computer-mediated discussions. The Chatham House Rule reads as follows:

When a meeting, or any part thereof, is held under the Chatham House Rule, all participants are free to speak or to use the information exchanged, but neither the identity, affiliation nor attributions made by any speaker(s), nor that of any other participant, may be revealed.

Attribution at: http://www.chathamhouse.org/about/chatham-house-rule/#sthash.q6jSYp2l.dpuf

I ask for your assent to make use of this rule in this course.

Day-to-Day Communications
Emails. Moodle site and chat group sessions should be reviewed on a daily basis, keep in mind that comments, changes clarification, and news are updated on a regular basis.

Individual Assignments
There are a number (< 12) homework assignments, designed to help reinforce the concepts, make attributions of terms-of-art and forensics material, that has been covered or will be covered in the assignments, case projects and discussions. Assignment completions are indicative of your professional discipline and your commitment to active learning. Completion of these assignments are crucial to your success in this class and your potential entry into the profession of digital forensics. Homework assignments should always be submitted on the due date via Moodle. Late assignments are not accepted and will receive a zero score for that assignment. Any questions, reduced to email to the instructor, pertaining to your assigned grade, must be addressed within 1 week, (7 elapsed days) after you receive the questioned grade.

Exams
There will be a one midterm exam assigned during the semester. All exams represent individual work, this is an ISU honor code matter. There are no make-up for any exam except under very extreme and exceptional circumstances. The final but ungraded exam will be administered before the spring semester 2015 finals week. All students in the course will be required to register with (ISC)² for the CCFP exam and take the 125 question (multiple choice) (6 domains of CCFP exam. The exam which will be administered under proctor controls at a special facility in Salt Lake, City, Utah. ISU will provide bus transportation to the proctored exam site. For all who achieve the passing metric for the CCFP and complete the necessary (ISC)² paperwork, Dr. Schou will then provide the official endorsement for your candidacy to become an associate of the (ISC)². This is a very important milestone in your career.

Forensics Tiger Team Projects
To gain collaborative skills, knowledge and forensics practices, learners will be assigned to work in self-managed tiger teams. Assignments will be made during week 2, based on the overarching need to develop and support diversity,
concerning differing life experiences, prior skills, career goals, level and types of education. Learners are to collaboratively collaborate and actively work in these self-managed tiger teams. This is to remain constant over the duration of the course, to research, conduct forensics investigations, write and present forensics reports concerning the set of assigned digital forensics investigations. Tiger teams will self-monitor and self-assess individual contributions to the tiger team effort. Further details for this grading rubric will be described in detail in our class meeting.

Forensic Lab
The forensic lab is located

Course Conduct
You are required to observe the rules of academic integrity and classroom conduct established by the University. Cheating will not be tolerated. Students found cheating will receive a grade of F for the course and may be subject to further disciplinary action. The University Integrity policies are posted on the course website and should be reviewed carefully.

Assignments and Grading
Explicitly stated, the grading rubric for this course is 50% based on individual work and 50% based on work done in small forensics teams (Tiger Teams). The following table arrays the course grading rubric and the points for individual and small group work.

<table>
<thead>
<tr>
<th>Assignments</th>
<th>Maximum Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homework Assignments (&lt;12) (Individual Work)</td>
<td>30</td>
</tr>
<tr>
<td>Forensics Tiger Team Projects (&lt;4) (Group Work)</td>
<td>40</td>
</tr>
<tr>
<td>Tiger Team Self-Assessment of each (individual work) on team</td>
<td>10</td>
</tr>
<tr>
<td>Midterm Examination (Individual Work)</td>
<td>20</td>
</tr>
<tr>
<td>Final Exam - CCFP to be completed before Final Grade</td>
<td>Required</td>
</tr>
<tr>
<td>Total Potential Points for Undergraduates</td>
<td>100</td>
</tr>
<tr>
<td>Graduate Project (Critical Assessment of a Forensics Tool or Forensics Book Review-(5-12 PAGES) - selected in conference with the instructor(s)</td>
<td>100</td>
</tr>
<tr>
<td>Total Potential Points for Graduates</td>
<td>200</td>
</tr>
</tbody>
</table>

Undergraduate Grade Rubric
The rubric for undergraduate course grade of A is 90 points and above, A- is 80 points and above, B+ is 75 points and above, B is 70 points and above, B- is 60 points and above, C+ is 55 points and above, C is 50 points and above, C- is 40 points and above, D is 30 points and above and a grade of F is earned if you receive fewer than 30 points. Depending on the overall class performance, I reserve the right to adjust the scale. My decision to adjust the scale will only be made at the end of the semester once all of the course grades are in.

Graduate Grade Rubric
The rubric for graduate course grade of A is 190 points and above, A- is 180 points and above, B+ is 175 points and above, B is 170 points and above, B- is 160 points and above, C+ is 155 points and above, C is 150 points and above, C- is 140 points and above, D is 130 points and above and a grade of F is earned if you receive fewer than 130 points. Depending on the overall class performance, I reserve the right to adjust the scale. My decision to adjust the scale will only be made at the end of the semester once all of the course grades are in.

Incomplete Grades
According to University Regulations, a grade of Incomplete can only be given if the student is currently passing the course and circumstances prevent them from completing the semester. Incomplete grades will not be given once the student has taken the mid-term exam.

**Weather Emergencies**
In the event of weather difficulties the course meeting will occur on the ISU Moodle site

**Tentative Course Schedule:**

<table>
<thead>
<tr>
<th>Session</th>
<th>Case</th>
<th>Topics</th>
<th>Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/12</td>
<td></td>
<td>Course Introduction, Computer Forensics and Investigations as a Profession</td>
<td>Syllabus, Chapters 1, 2 and 3</td>
</tr>
<tr>
<td>1/19</td>
<td>1</td>
<td><strong>No Class - Federal Holiday</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>1/26</td>
<td>2</td>
<td>Experts and Computer Forensics</td>
<td>Chapters 4, 5 and 6 CCFP</td>
</tr>
<tr>
<td>2/2</td>
<td>3</td>
<td>The Prevailing Investigative Process</td>
<td>Chapters 7, 8, 9 and 10 CCFP</td>
</tr>
<tr>
<td>2/9</td>
<td>4</td>
<td>Evidence and Evidence Management - Custodial Attributes</td>
<td>Chapters 11, 12, 13 and 14 CCFP</td>
</tr>
<tr>
<td>2/16</td>
<td></td>
<td><strong>No Class - Federal Holiday</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>2/23</td>
<td>5</td>
<td>Forensics Theory, Principles and Methods</td>
<td>Chapters, 15, 16, 17 and 18 CCFP</td>
</tr>
<tr>
<td>3/2</td>
<td>6</td>
<td>Media, Operating Systems and Networks</td>
<td>Chapters 19, 20 and 21 CCFP</td>
</tr>
<tr>
<td>3/9</td>
<td>7</td>
<td>Mobile, Embedded and Multimedia Forensics</td>
<td>Chapters 22, 23, and 24 CCFP</td>
</tr>
<tr>
<td>3/16</td>
<td>8</td>
<td>Virtual Machines, Tools and Techniques (OUT OF CLASS MID-TERM EXAM)</td>
<td>Chapter 25 and 26 CCFP</td>
</tr>
<tr>
<td>3/23</td>
<td></td>
<td><strong>Spring Break</strong></td>
<td>N/A</td>
</tr>
<tr>
<td>3/30</td>
<td>9</td>
<td>Anti-Forensics, Software Forensics</td>
<td>Chapter 27 and 28 CCFP</td>
</tr>
<tr>
<td>4/6</td>
<td>10</td>
<td>Email, Messaging and Databases</td>
<td>Chapter 29 and 30 CCFP</td>
</tr>
<tr>
<td>4/13</td>
<td>11</td>
<td>Malware and the Cloud</td>
<td>Chapter 31 and 32 CCFP</td>
</tr>
<tr>
<td>4/20</td>
<td>12</td>
<td>Social Networks and Big Data</td>
<td>Chapter 33 and 34 CCFP</td>
</tr>
<tr>
<td>4/25</td>
<td>13</td>
<td>3 Hour Review and Test Preparation</td>
<td></td>
</tr>
<tr>
<td>4/27</td>
<td>14</td>
<td>Control Systems, Critical Infrastructure, Gaming and Virtual Reality</td>
<td>Chapters 35, 36 and 37 CCFP</td>
</tr>
<tr>
<td>5/1</td>
<td>15</td>
<td>CCFP Review FRIDAY AFTERNOON - EVENING (3 HOURS)</td>
<td>CCFP</td>
</tr>
<tr>
<td>5/2</td>
<td></td>
<td><strong>TRAVEL TO CCFP Exam in Salt Lake City SATURDAY AFTERNOON</strong></td>
<td></td>
</tr>
<tr>
<td>5/5</td>
<td></td>
<td>Graduate Papers Due</td>
<td></td>
</tr>
</tbody>
</table>