University of Rhode Island

CSF412

Spring 2015 Syllabus

Teaching Staff: Daniel Dickerman (dickermand@cs.uri.edu)

Teaching Assistant: Mark Gadoury (mgads1130@my.uri.edu)

Course Meets: Online Jan 21 – May 12, 2015

Course Web Page: https://sakai.uri.edu/portal

Goals:

• Continue learn about the field of Computer Forensics, by building on those topics learned in CSF410

• Learn in-depth details about the Windows Operating Systems and the forensic artifacts available to the Forensic Examiner

• Learn about tools and techniques for finding, recovering and interpreting Windows artifacts

• Gain hands–on experience using Computer Forensic tools

Course Materials:

Textbook:


Software:

• WinHex Specialist (Note: if you did not already purchase this during a prerequisite course, you must purchase at this time. Contact the teaching staff for information about discounted academic pricing)

• Other Forensic and special purpose software provided through Sakai

Course Work:

For this course, you should expect to complete between 15 - 20 hours worth of coursework each week.

Weekly Readings and Lectures

• Readings - Readings will be assigned every week, and are linked off of the course webpage in either PDF, DOC or HTML format. Students are expected to do all readings, ask questions about them on the discussion board if necessary, participate in discussions about the readings, and be able to answer quiz and final exam questions about the readings.
• **Video Lecture** – There are lectures by Professor Dickerman and other URI Computer Science faculty each week, describing computer forensics procedures and demonstrating computer forensic techniques and technology. The lectures are provided as digital video (MOV format) and are available for downloading or streaming off the Internet from the Lectures pages of the course website. Approximately two hours of lecture are assigned every week. Students are expected to view all lectures, ask questions about them on the discussion board if necessary, participate in discussions about the lectures, and be able to answer quiz and final exam questions about the lectures.

**Graded Assignments**

• **Mandatory Discussions** - (indicated by [Mandatory] in the discussion topic title). Because this is an online course, the Mandatory discussions will form an integral part of your participation grade. Mandatory discussions will be posted by Graduate students as part of their assigned research topics. Each Graduate student must post two Mandatory discussion questions over the duration of the course. The Graduate students will post their first Mandatory post between Friday, Feb 20th – Sunday, Feb 22nd by 11:59pm and their second discussion between Friday, Mar 27th – Sunday, Mar 29th by 11:59 pm. **As a CSF412 student, you will not be required to initiate mandatory discussions.**

To receive full credit for your participation in our discussions; you need to make at least two posts that add substance to the conversation during each of the two periods. You must contribute at least one post in two different discussions initiated by the Graduate students twice during the semester. These two posts must be created by the following Friday at midnight when the discussion closes.

**Late posts will not be graded.** Missed graded discussions can only be made-up in exceptional circumstances, such as death in the family or documented illness.

Mandatory topics will be originated by the Professor, TA, URI staff, or by a student designated by the teaching staff. Your posts should demonstrate you understand the materials assigned. Your responses might integrate multiple views and/or motivate other students to respond. You should provide evidence that you are reading the assigned materials and the other students' postings and bring out interesting interpretations. Don't just demonstrate that you know the facts, but show that you are able to analyze them and handle conceptual ideas. Posts that only state, "I agree" or "That is an interesting idea" are OK in the forum, but they will not receive credit. Feel free to contribute from your personal experiences or your own research or interests.

*The participation grade is based on that a student needs to actively participate in the class discussion board by: 1) adding substantive responses and counter responses to the mandatory discussion questions that showed thought, research, and understanding of the topic being discussed; 2) assisting other students with help/guidance; and/or 3) contributing to the class by posting online resources relating to topics from the course.*

All discussion is considered confidential within the course –content posted on the course discussion board is not to be shared with people outside of the course. All class discussion should be on the class discussion board, direct student-to-student contact is not allowed unless approved by the instructor.

• **Weekly Quizzes** - There will be a quiz each week. The quiz will be based on all reading and lecture material. Quizzes will be done using a web-based timed quiz mechanism.
Quizzes will be available for three days (typically Thursday through Saturday) of the week that the topic is being covered - **you must take the required quiz at some time during its availability time.** A quiz not taken during the availability time for that quiz will be graded as a zero. Your single lowest required quiz grade of the semester will be dropped.

- **Weekly Forensics Exercises** - There are weekly forensic exercises where students are required to perform various forensic tasks. Material required for the exercises are provided via download.

Neatness and adherence to the form specified in exercise descriptions is expected and constitutes part of the grade for each assignment. All practical work will be graded based on the standard of work that should be produced by a professional in the field. All answers should be as detailed and thorough as possible or points will be deducted.

Most exercises will require the use of software provided as part of the course, or a trial version that you will need to download from external web sites that will be specified. Some exercises will require the use of virtual machines, using configurations that will be provided in the course materials. Some exercises may require access to a computer that you can take apart (see Hardware and Software Requirements below). Some exercises require you to turn in photos of system components acquired by you using by a digital camera (or scanning non-digital photos).

**LATE PENALTY FOR EXERCISES:** Most exercise reports are due as an upload to the course website within one week of being assigned. Exercise reports submitted after the due date will receive a 5% late penalty per day, not including weekends or holidays. No exercise reports will be accepted later than 4 days past the due date. In addition, teaching staff will not be available to offer assistance on an exercise past its due date. Exercises will be posted each Friday and will be due the following Friday unless otherwise specified.

- **Final Exam** - There will be a final exam during the final week of the course. The exam will be cumulative and will require you to put into practice everything you have learned in this course.

### Additional Course Information

#### Course Questions and Announcements

The course discussion forums serve not only as a graded discussion forum (**Mandatory** topics), but also as a way for the instructors to make course announcements (**Info** topics) and for students to post questions about the course readings, lectures and assignments (**Question** topics).

- **Info** (indicated by [Info] in the discussion topic title). - These discussion topics are typically posted by the Professor or TA to clarify or update some information on the course, an assignment, or some other relevant topic of interest.

- **Questions** (indicated by [Question] in the discussion topic title). - These discussion topics are typically posted by students seeking help from other students and/or from the staff about some aspect of the course or about computer forensics in general. Participation in these discussion topics is optional and not required, although particularly helpful responses to the questions of others can help your class participation grade. However, again, participation in Question discussions is not required.

### Typical Weekly Schedule:

**Our typical assignment week runs from Friday to Friday.**
Friday

- New readings, lectures, and assignments posted for the week.

Following Week

- Quiz (available Thursday-Saturday) on the readings and lectures that were assigned the previous Friday.
- Assignments due by midnight (US Eastern time) on Friday.

Discussion Board Use & Teaching Staff Availability:

- Any question related to troubleshooting or not understanding homework assignments should be directed to the discussion board (not to TA email – unless the question will somehow reveal an answer). The teaching staff will check the discussion board periodically Mondays through noon on Friday. No teaching staff assistance will be provided on the discussion board after noon on Friday. However, we encourage you to continue to use the discussion board for help from each other.
- You should contact the teaching staff via email with questions related to grading issues or homework questions that cannot be posted to the discussion board. You should not contact the teaching staff via email with general question related to troubleshooting or not understanding homework assignments.
- If you would like to schedule an online or in-person appointment to meet with teaching staff you may do so by contacting them via email. These appointments should be made with a minimum of 24 hrs notice. The teaching staff will not offer help on an assignment at any time, through any means (discussion board, email, in person) after noon on the Friday that the assignment is due. In addition, no assistance will be provided for past-due assignments.

Grading:

Grades will be determined according to these weights:

- Quizzes: 20%
- Exercises: 40%
- Final Exam: 30%
- Class Participation: 10%

Feedback on quizzes, exams, and exercises will either be available on the course web site, emailed to you or placed in your submit folder. You have one week from the posting of a grade to submit any concern about that grade, in email to the TA. Concerns expressed after one week from posting will not be considered.

Tentative Schedule of Topics by Week:

0. Intro to Windows Forensics
1. The Windows Registry
2. Windows USB Device Tracking
3. Windows UserAssist
4. Windows Prefetch
5. Windows Shortcuts
6. Windows Jump Lists
7. Windows Thumbnail Cache
8. Windows Recycle Bin
9. Windows Shadow Copy
10. Windows ESE Databases

**Hardware Requirements:**

Primary student computer should meet these requirements:

- A Windows 7 (or later) computer
- At least 40 GB of free hard drive space
- At least 4 GB of RAM
- A DVD-R drive (read-only is sufficient)
- Sound card and speakers or headphones for listening to video lectures

Students should also consider obtaining a second computer (forensic workstation) that can be dismantled and/or used for forensic exercises in place of your primary everyday computer. Some exercises in this course include the possibility of causing damage to the data on your hard drive if not done properly and as such would be catastrophic if you rely on the computer daily. **Warning:** Past experience has proven that new forensic students can sometimes confuse storage devices and accidentally overwritten their own primary hard drive or other media not intended to be overwritten during forensic imaging and restoration exercises.

The ability to take pictures and get them into electronic format (e.g. digital camera, or scanned jpegs from non-digital)

High speed Internet connection for downloading and/or streaming. Downloading on a remote computer (e.g. a public library) and bringing files home on a USB drive or CD is sufficient, although not ideal.