Fall 2015

University of Rhode Island

Computer Forensics 1

CSF 410
Fall 2015 Syllabus

Course Instructor: Daniel Dickerman (dickermand@cs.uri.edu)

Teaching Assistant: Brian Lattuada (brian_lattuada@my.uri.edu)

Online: September 9 – December 11, 2015

Final Exam: December 15th - 21st

Course Goals

Learn about the field of Computer Forensics. Learn the techniques and tools used in basic computer evidence recovery. Study the legal issues relating to digital evidence. Gain hands–on experience using Computer Forensic tools.

Course Materials

No textbook is required for this course. You were provided information this summer directing you to the Sakai site "CSF 102" which provides all the necessary background material/knowledge required to succeed in this course. If you find that you are struggling with any course material this semester, you are advised to revisit the CSF 102 site for a refresher on this background information.

Software:

- WinHex Specialist (Note: if you did not already purchase this during a prerequisite course, you must purchase at this time. To purchase WinHex Specialist please go to the following webpage: http://www.x-ways.net/order.html) URI is typically able to arrange an academic discount with the vendor, X-Ways - contact your TA for instructions.
- Other forensic and special purpose software provided in exercises or other methods announced by teaching staff.

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 (AVI or WMV 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:

- Weekly Quizzes - There will be a quiz most weeks. 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 Saturdays) 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 available download or on a course DVD that is US-mailed to students.
- Mandatory Discussions - These discussion topics require each student to make at least one posting (either an original posting or a response to a thread concerning another student's original posting) on the topic within a week of the topic's creation. The quality of your posts affect the class participation portion of your grade (see Grading below), so you should be prompt, thoughtful, and thorough in what you write.
- 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.

Quality of Work:

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.

Late Penalty for Exercises:

Most exercise reports are due as an upload to the course web site within one week of being assigned. Exercise reports submitted after the due date will receive a 5% late penalty per day. 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.

Feedback:

Feedback on the exercises is available on the course web site after grading has been completed. Students 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 are not considered.

Confidentiality:

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. You will notice that when you post on the discussion board is by a generically created user ID to ensure your comfort and confidentiality when posting material to the Mandatory Discussion Board and Help Forum.

Course Grades

Grades will be determined according to these weights:

- Quizzes: 20%
- Exercises: 40%
- Final Exam: 25%
- Class Participation: 15%

Additional Course Information

Announcements:

All course announcements, from your instructor or TA, including reminders about due dates, changes to assignments, or general course announcements are posted on the Course Announcements page. These announcements are also sent in an email you your officially listed URI email address. There is no way to change where these emails are sent, so please make sure that you regularly check this email address for all course correspondence.

Typical Weekly Schedule:

Our typical assignment week runs from Friday to Friday.

Friday

- New readings, lectures, assignments, and mandatory discussion questions (when given) are posted for the week.

Following Friday

- Quiz on the readings and lectures that were assigned the previous Friday. The quiz is actually available that Thursday through Saturday.
- Assignments due by midnight (US Eastern time).
- Any posts to mandatory discussions that were assigned, must be made my midnight (US Eastern time) to be counted.

Receiving Help

Help Forum:

The Help Forum is a discussion board that is separate from the Mandatory Discussion Board, where all questions about the course or assignments should be posted.

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 Fridays that assignments are due. Nor will any help about an assignment be given by the TA after the assignment is due. However, we encourage you to continue to use the discussion board for help from each other.

Once again, 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. You will notice that when you post on the discussion board is by a generically created user ID to ensure your comfort and confidentiality when posting material to the Mandatory Discussion Board and Help Forum.

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.

Email:

You should contact the TA via email with questions related to grading issues or homework questions that cannot be posted to the discussion board.

You should **not** contact the TA via email with general question related to troubleshooting or not understanding homework assignments.

If you are having personal, technical, or any other unforeseen issues that will prevent you from taking a quiz or completing an assignment on time, you must contact the TA by no later than noon on Wednesday to ask for an extension. Any requests made after noon on Wednesday, barring an emergency situation, will not be considered.

Meetings:

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.

For those of you that are not on campus, please do not discount the use of our 'online help' sessions. These are conducted using software that allows phone or VOIP discussion, while providing both the student and the teaching staff a means to share their desktops with each other.

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.

The TA's schedule is typically more flexible than Professor Dickerman's and all initial inquiries for help or meetings should be directed towards the TA.

Tentative Schedule of Topics by Week

1. Intro to Forensic Procedures and Methodology
2. Controlled Boot Process
3. Write Blocking
4. Hashing Concepts
5. Data Acquisition
6. Image Authentication
7. Image Restoration
8. Live Acquisition
9. Basic Searching & File Signatures
10. Data Carving

11. Passwords and Encryption
12. Intro to FTK

Hardware Requirements

Primary student computer should meet these requirements:

- A Windows 7 or Windows 8.1 computer
- At least 20 GB of free hard drive space
- At least 2GB of RAM
- A DVD-R drive (read-only is sufficient)
- Sound card and speakers or headphones for listening to video lectures
- A digital camera that allows students to take pictures and save them in an electronic format (such as jpgs) for submission
- 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.

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.

Therefore, students should also consider obtaining a second computer (forensic workstation) that can be dismantled and 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.

If you do not have access to a secondary computer, you should make sure to frequently back up all important data (documents, pictures, music, etc) so that if you do experience problems you have a backup of your files.

Using a Mac:

Using a Mac, or any platform where you are attempting to complete the assignments in a virtual environment, in this class is not recommended. The assignments in this class have been designed to run on a physical Windows 7 system, although they will run on XP or Vista systems as well. However, VMWare running Windows on top of another host OS (in this case your Mac) can be very problematic when it comes to certain aspects of forensics, especially when you get to the write blocking topic this semester.

When you plug a storage device (i.e. USB thumbdrive) into your Mac, the Mac "touches" the drive first and then if you are running Windows in VMWare Fusion, your Mac "hands off" control of that storage device to VMWare where the guest OS (i.e. Windows XP) then takes control of the device. Unless write blocking is in effect on the OSs that "touch" the drive, the OS will in most cases modify the drive. So if you have SAFE Block write blocker installed in Windows (within VMWare Fusion), that Safe Block write blocking does not protect your USB thumbdrive until WIndows sees and controls the storage device. This means that the Mac has touched the drive and quite possibly modified the drive before Safe Block even gets a chance to write block it and protect it from writes.

Using VMWare as a "sandbox" or test environment is very useful to a forensic examiner. VMware is also commonly used as an environment to run certain forensic analysis tools or run software from restored copies of seized computers. Our main caution when it comes to using VMware as your main forensic platform is to not access original evidence or live evidence without properly understanding and implementing write blocking and how using host versus guest virtualization affects media access.

Those in the forensic profession that use Macs typically either use the Mac platform completely where they run Mac forensic tools instead of Windows tools like you will be using in this class....or they install Boot Camp and boot the Mac computer into a physical install of Windows running on their Mac hardware instead of running within a VMWare world.

If you MUST use a mac within VMWare and this is your only real option for this course, then at a minimum you MUST turn off Disk Arbitration on the Mac OS so that the Mac does not touch and modify drives you attach. Instructions to do so are here: http://www.appleexaminer.com/MacsAndOS/OperSys/DiskArbitration/DiskArbitration.html