

Network Forensic Analysis

MET CS 703

Instructor

Stuart Jacobs, MSc, CISSP

Lecturer, Computer Science Department Metropolitan College Boston University

Office hours: By Appointment

Office Address: 808 Commonwealth Ave., Room 250. Boston, MA 02215.

E-mail: sjjacobs@bu.edu

Course Description

This course provides an introduction to the methodology and procedures associated with digital forensic analysis in a network environment. Students will develop an understanding of the fundamentals associated with the topologies, protocols, and applications required to conduct forensic analysis in a network environment. Students will learn about the importance of network forensic principles, legal considerations, digital evidence controls, and documentation of forensic procedures. This course will incorporate demonstrations and laboratory exercises to reinforce practical applications of course instruction and will require an independent research paper related to the course topic.

Prerequisites

Knowledge of information technology fundamentals (computer hardware, operating systems, applications and networking) is required. Successful completion of CS 625, CS 535, or permission of the instructor is also required.

Required Course Books

- **Computer Forensics : Investigating Network Intrusions and Cyber Crime**, EC-Council, ISBN-13: 978-1-4354-8352-1, ISBN-10: 1-4354-8352-9
- **Computer Forensics : Investigating Wireless Networks and Devices**, EC-Council, ISBN-13: 978-1-4354-8353-8, ISBN-10: 1-4354-8353-7
- **Handbook of Digital Forensics and Investigations**, Eoghan Casey ed., Elsevier Academic Press, ISBN 13: 978-0-12-374267-4

These textbooks can be purchased from Barnes and Noble at Boston University.

Students should make sure to purchase new copies of the two EC-Council books so they will be able to access the on-line Student Resources area which will be required for the course.

Courseware

This course uses Online Campus (Blackboard 9). Once the course starts all students must use the Online Campus Dashboard internal messages service. Students are required to use Online campus:

- for reading assignments beyond text book assigned reading,
- Submitting homework assignments,

- Submitting lab exercises,
- Taking on-line quizzes,
- Participating in discussion threads,
- Taking the on-line final examination and practice final exam, and
- All course related email correspondence.

Class Policies

1) Attendance & Absences

- Students are required to attend the four scheduled on-campus lectures (9/9, 10/07, 11/04, 12/09 and the final exam on 12/16)
- Students must notify the instructor in advance if unable to attend any on-campus lecture

2) Assignment, Lab Exercise and Discussion Completion & Late Work

- Homework assignments are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course. For each day after the submission date a homework assignment is due will result in a penalty of 3 points. Homework assignments passed in that are over 5 days late will receive a grade of zero (0). If a student will be unable to submit an assignment by its due date, the student must contact the instructor **in advance** to avoid the late submission penalty.
- Lab exercises: are mandatory, must be completed and submitted in a timely manner, and are required to be submitted via Online Campus for this course. For each day after the submission date a lab exercise is due will result in a penalty of 3 points. Lab exercises passed in that are over 5 days late will receive a grade of zero (0). If a student will be unable to submit a Lab exercise by its due date, the student must contact the instructor **in advance** to avoid the late submission penalty.
- Student postings to discussion topic after the listed closing dates will not be counted when calculating a student's discussion grades.

3) Academic Conduct Code – Cheating and plagiarism will not be tolerated in any Metropolitan College course. Such activities/behavior will result in no credit for the assignment or examination and may lead to disciplinary actions. Please take the time to review the Student Academic Conduct Code:

http://www.bu.edu/met/metropolitan_college_people/student/resources/conduct/code.html.

Such activities/behavior includes copying (even with modifications) of another student's work or letting your work to be copied. Your participation in interactions with the instructor and your classmates is encouraged, but the work you submit must be your own. Collaboration is not permitted.

Class Meetings, Lectures, Assignments, Lab Exercises & Examinations

The course will include four (4) class sessions held at the Boston University campus. The class session will include lectures, laboratory exercises, and an interactive exchange of course related concepts and materials. These sessions also provide students with the opportunity to interact with other students and the course instructor. The proposed class session dates are listed below (subject to change based on course and instruction requirements):

On-campus class session	Will occur on
Session 1	September 7, 2013 between 1 PM and 4 PM EDT
Session 2	October 5, 2013 between 1 PM and 4 PM EDT
Session 3	November 2, 2013 between 1 PM and 4 PM EST
Session 4	December 7, 2013 between 1 PM and 4 PM EST

On-line Live sessions

- There will be a number of one hour on-line sessions, in addition to on-campus meetings identified above, which will be held on:
Thursday evening on 9/12, 9/19, 9/26, 10/3, 10/10, 10/17, 10/31, 11/7, 11/14, 11/21, and 12/5 at 8:00 PM ET
Saturday afternoon on 9/28, 10/5, 10/12, 11/9, 11/16, and 11/23 at 2:00 PM ET

During these on-line sessions I will be reviewing some material from the current course module and hold a question & answer period.. Attendance is not required at these sessions but highly recommended. All on-line sessions will be recorded and archived. The archived recordings will be accessible from the Online Campus Dashboard under the heading “Live Classroom (Question & Answer) Sessions”.

Assignments

- All homework assignments are identified within the Online campus Study Guide.
- File names for assignment documents should be:

CS703-HW<number>-<student last name>.doc

An example assignment document file name is:

CS703-HW5-Jacobs.doc

Student submissions which fail to follow this direction will have 5 points deducted!

- Student assignment submissions must be no more than 4 pages in length, be single spaced, use 12 point Times Roman type font and 1” margins on all sides. Student submissions which fail to follow this direction will have 5 points deducted!
- Include the file name in the header and a page number in the footer of you assignment submission document. Student submissions which fail to follow this direction will have 5 points deducted!
- Title cover pages are not required and should not be used;
- Assignment submission documents MUST be in Word 2003 or Word 2007 file formats

that are NOT encoded in XML;

- Quoted material and citations must follow the American Psychological Association (APA) format with a reference section at the end of a student's submitted work. Please refer to the <http://www.apastyle.org/> web site for guidance on following the APA style guide.
- Students are required to comply with the directions contained within the document **APA Criteria for Course.pdf** whenever the work of others is used as part of a student's assignment submission. Failure to do so will result in points being deducted for the assignment grade.
- Wikipedia is a useful starting point for finding information about a subject BUT NOT an acceptable direct reference source. One should only reference or quote from primary (source) documents.

Lab Exercises

- Lab exercises(Hands-on Projects) are identified within the Assignment description document for each course module.
- File names for lab exercise documents should be:

CS703-LAB<number>-<student last name>.doc

An example lab exercise document file name is:

CS703-LAB5-Jacobs.doc

Student submissions which fail to follow this direction will have 5 points deducted!

- Students should enter their lab exercise answers direct within each lab exercise document and then submit the completed document appropriately renamed as stated above;
- Lab exercise submission documents MUST be in Word 2003 or Word 2007 file formats that are NOT encoded in XML.

Discussion Threads

- Each course module includes a discussion topic that students are required to participate in. Student discussion postings will be graded as per the "Discussion Grading Rubric" under the Online Campus "Syllabus and Course Information" area.

Examinations

- Students are required to take six on-line quizzes (one per module) while the course is running. Students will be allowed 60 minutes to complete each quiz. A student may take each of these quizzes starting when a quiz becomes available via Online Campus. Each quiz will close at 6 AM ET on the date the next Module starts and not be reopened except for unusual circumstances as decided by the instructor. If a student cannot complete a quiz during the week each quiz is available, the student must make prior arrangements with the instructor.
- On-campus and EL students are required to take a proctored final exam that will be held in class on Friday 12/20/2013 and last 3 hours. This exam is open book and open notes

but no electronic resources allowed.

- If the final will be missed it will be the responsibility of the student to arrange with the professor a mutually agreeable schedule for completion of work.
- A practice final exam will be available on Online Campus which can be taken as many times as a student wishes.
- If any work is to be completed beyond the scheduled dates of this course the student must negotiate a Boston University "Contract for an Incomplete Grade" with the professor prior to the end of the class.

Grading Criteria

Students will have to do homework assignments to help you master the material. You will also have to read the textbooks and to be ready to discuss the issues related to the current class topics.

Grades will be based on:

- home work assignments (25%)
- quizzes (25%)
- lab exercises (10%)
- discussion thread participation (10%)
- proctored final exam (30%)

Grade ranges are as follows:

- 94 <= is an A
- 90 <= and < 94 is an A-
- 87 <= and < 90 is a B+
- 84 <= and < 87 is a B
- 80 <= and < 84 is a B-
- 77 <= and < 80 is a C+
- 74 <= and < 77 is a C
- 70 <= and < 74 is a C-
- 60 <= and < 70 is an F

Course Learning Objectives

Upon successful completion of this course you will understand:

- How to look for evidence in both wired and wireless networks
- Perform end to end forensic investigations
- Collect evidence from log files
- Understand the importance of time synchronization
- How to use typical forensic investigation tools
- Follow a scientific approach to investigate network security events and incidents

Course Outline

Module 1:

Introduction to Network Forensics and Investigating Logs
Network Traffic Investigations

Module 2:

Web Attack Investigations
Router Forensics

Module 3:

Denial of Service Investigations
Internet Crime Investigations
Email Crime Investigations

Module 4:

Wireless Attack Investigations
PDA Forensics

Module 5:

iPod and iPhone Forensics
Blackberry Forensics

Module 6:

Corporate Espionage Investigations
Trademark and Copyright Investigations
Investigating Sex Related Activities

Non-required textbooks and references good for further study**Suggested Course Books**

There will be no reading assignments from the following book. However you will find it a valuable resource to anyone involved in the Information Security area.

Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance, Stuart Jacobs, IEEE Press Series on Information and Communication Networks Security, Wiley-IEEE Press; 1 edition, ISBN-10: 0470565128, ISBN-13: 978-0470565124
The above book covers the subject area of information security from an engineering perspective

Recommended Books

There will be no reading assignments from these books. However you will find each to be valuable resources to anyone involved in the Information Security area.

Firewalls and Internet Security, Repelling the Wily Hacker, William R. Cheswick, and Steven M. Bellovin, Addison-Wesley, 1994
The above book is a classic for its very detailed treatment for stateful firewalls and DMZs and is still relevant today.

Practical UNIX & Internet Security, 2nd Edition, ,Simson Garfinkel and Gene Spafford: O'Reilly, 1996

The above book is a classic for its very detailed treatment of general networking security and hardening of unix type operating systems and is still relevant today.

Hacking Expose Network Security Secrets & Solutions, 2nd Edition, Joel Scambray, Stuart McClure, and George Kurtz, McGraw-Hill, 2001

The above book provides an interesting look into those involved in malware and some of the techniques used for breaching targeted systems.

Security Engineering; A Guide to Building Dependable Distributed Systems, Ross Anderson, Wiley, 2001

The above book is an interesting collection of discussions on security engineering and associated challenges.

Computer Related Risks, Peter G. Neumann, Addison-Wesley, 1995

The above book is one of the definitive texts on the basic concepts of what constitutes risks, especially information security risks.

Applied Cryptography, Bruce Schneier, 2nd Edition, Wiley & Sons, 1996

The above book is an excellent source for details on most any encryption algorithm you are likely to encounter. Most any version, starting with the 2nd edition, will be invaluable.

Student Conduct Responsibilities

Notice of Criminal, Civil, and Administrative Responsibility

The legal and authorized use of the materials, software, applications, processes, techniques or services described in this course, presented in written or verbal form, are the sole responsibility and liability of the individual student. The course instructor and Boston University assume no liability as for any damages resulting from unauthorized use of the knowledge gained by student(s) from material covered in this course.

The content and use of the course materials, software, applications, processes, techniques or services described in presentation materials or conveyed verbally by the course instructor may be limited or restricted by federal, state or local criminal and/or civil laws or the acceptable use in corporations, businesses or organizations.

It is the responsibility of the student to ensure that they do not perform any action, process or technique that could violate any criminal, civil or administrative laws, regulations and/or policies.

There shall be no liability on the part of the course instructor for any loss or damage, direct or consequential arising from the use of this information or any action by student(s) that is determined to be in violation of any federal, state and/or local civil or criminal law, or for violation of any administrative regulation, policy or acceptable use policy that results in prosecution, or any loss, to include termination of employment, forfeiture, restitution or fines.

Student enrollment in this course will constitute an agreement to the aforementioned terms and conditions of student responsibilities and liabilities.