Digital Forensics

MET CS-693

Course Description

MET CS693 – E1

Digital Forensics

This course presents students with a comprehensive understanding of digital forensic principles and the collection, preservation, and analysis of digital evidence. Students will learn about the importance of forensic principles and procedures, legal considerations, digital evidence controls, and the documentation of forensic analysis. Course topics will include computer and network technologies, operating system architectures, disk structures, and file system analysis. Students will develop an understanding of the different applications and methods for conducting network and digital forensic acquisition and analysis. This course will incorporate laboratory exercises and demonstrations to reinforce practical applications of digital forensic theory.

Course Objectives / Learning Outcomes

At the successful completion of the course, you will have developed a comprehensive understanding of digital forensic principles. You will be able to:

- Describe the attributes of file systems and storage media.
- Identify potential sources of electronic evidence.
- Understand the importance of maintaining the integrity of digital evidence.
- Demonstrate the ability to perform basic forensic data acquisition and analysis using computer and network-based applications and utilities.
- Demonstrate the ability to accurately document forensic procedures and results.
- Identify career opportunities for digital forensic professionals.
- Demonstrate the ability to conduct research to develop an in depth understanding of a topic relating to digital forensics.

Course Outline

- **Calendar Tool** - You can see many due dates in the calendar tool. You may add your own events there as well. However, please be aware that you may not find all of the important dates for the course listed there. You will stay current by checking announcements, discussions, and emails throughout the course.
- **Readings** - Each module has both textbook readings and online readings. Your professor may suggest additional readings during the course.
- **Discussions** - There are both class and group threaded discussions for each module. These discussions are moderated by your facilitator. Postings for each discussion should be completed by the assigned due dates. There are also general discussions boards, which are not graded, for you to use to discuss any issues with your classmates. Please see the Class Discussion and Users and Groups menus on the home page for more details.
- **Assignments and labs** - There are assignments and labs that are due throughout the course. Please access from the Assignments menu.
- **Midterm and Final Exams** - Assessments are also listed in the course calendar and accessed from the Assessments menu.

Module 1: Digital Forensics and Incident Response

Overview of Digital Forensics and Incident Response and Incident Response and Investigations: Legal Aspects of Digital Forensics.

Module 2: Computing and Network Devices

Introduction to Computing and Network Devices and Operating System Architecture and Disk Structures.

Module 3: Digital Forensic Acquisition and Authentication

Principles of Digital Forensic Acquisition and Authentication and Digital Evidence Handling and Processing Digital Forensic Media Acquisition, Midterm Examination

Module 4: Digital Forensic Analysis

Principles of Digital Forensic Analysis and Applications and Digital Forensic Media Analysis (UNIX/Linux).

Module 5: Network Forensic Analysis

Principles of Network Forensic Analysis (Laboratory Session) and Digital Forensic Media Analysis (Microsoft Windows)

Module 5: Forensic Reports and Testimony

Forensic Reports and Testimony Special Topics in Digital Forensics

Course Materials and Resources

Required Book Bundle

BU MET CS693 requires a bundle comprised of a textbook { e-copy or hardcopy, and a lab manual which gives you a six-month window to the Cengage portal for material / downloads, etc. }

We have recently joined with the BU BN Bookstore and Cengage to offer this at a reduced cost through the “First Day” program.

WELCOME TO FIRST DAY™ DELIVERY FOR YOUR COURSE

{DEPT – COURSE - SECTION}

To enhance your learning experience and simplify access to the right materials for your class, your course materials have been integrated directly into your course.

BENEFITS OF THIS PROGRAM

- Exclusive preferred pricing
- Guaranteed the right materials
- Single Sign-On
- Ready to go on day one
- Course materials charge will be placed on your student account
- Option to Opt-Out on the first day of class.

ACCESSING YOUR MATERIALS

To access your required materials for your course, Log into Blackboard and follow instructions provided by your instructor.

Boston University will bill you at the discounted

- We will be using the 7th edition of the course text.
- The 5th or 6th edition content will NOT be an acceptable resource.
- *Note:* You MUST purchase the Lab Manual. The lab assignments depend on the content provided.

Register and Access Cengage Link

Please Register to access Cengage online (via the access code you will receive for MindTap access).

This is accomplished through the First Day Link.

Course Downloads and References

Forensic Examination of Digital Evidence: A Guide for Law Enforcement

NCJ 199408, April 2004, Special Report, National Institute of Justice

Electronic Crime Scene Investigation: A Guide for First Responders

NCJ 187736, July 2001, NIJ Guide, National Institute of Justice

Digital Evidence in the Courtroom: A Guide for Law Enforcement & Prosecutors

Investigations Involving the Internet and Computer Networks

NCJ 210798, January 2007, Special Report, National Institute of Justice

Cloud Computing Forensic Science Challenges

GRIZZLY STEPPE - Russian Malicious Cyber Activity: Joint Analysis Report

GRIZZLY STEPPE - Russian Malicious Cyber Activity: Indicators

Additional References

- Incident Response

  Purdue University Incident Response Policy (VII.B.3)
- Conditions on Use and Policy on Computing Ethics

  Boston University
- Designing and Developing an Application for Incident Response Teams

  FIST 2006 Conference
- United States Code
- *Investigations Involving the Internet and Computer Networks*

  NCJ 210798, January 2007, Special Report, National Institute of Justice

Instructor

Scot Arena

Master Lecturer

Computer Science Department

Metropolitan College

Boston University

1010 Commonwealth Ave, 3rd floor – Rm. 319

Boston, MA 02215 **sdarena@bu.edu**

The best way to reach me outside of our class sessions is to email me at my BU email address.

Boston University Library Information

Boston University has created a set of videos to help orient you to the online resources at your disposal. A link will be available within the course for these videos.

All of the videos in the series are available on the Online Library Resources page, which is also accessible from the Campus Bookmarks section of your Online Campus Dashboard. Please feel free to make use of them.

As Boston University students, you have full access to the BU Library. From any computer, you can gain access to anything at the library that is electronically formatted. To connect to the library, use the link http://www.bu.edu/library. You may use the library's content whether you are connected through your online course or not, by confirming your status as a BU community member using your Kerberos password.

Once in the library system, you can use the links under "Resources" and "Collections" to find databases, eJournals, and eBooks, as well as search the library by subject. Some other useful links follow:

> Go to Collections to access eBooks and eJournals directly.
>
> If you have questions about library resources, go to Ask a Librarian to email the library or use the live-chat feature.
>
> To locate course eReserves, go to Reserves.

Please note that you are not to post attachments of the required or other readings in the water cooler or other areas of the course, as it is an infringement on copyright laws and department policy. All students have access to the library system and will need to develop research skills that include how to find articles through library systems and databases.

Microsoft Imagine for Academic Institutions

Metropolitan College is a member of Microsoft Imagine for Academic Institutions (formerly DreamSpark), a Microsoft program that supports technical education by providing access to Microsoft software for learning, teaching, and research purposes. Our membership allows faculty and students currently enrolled in MET courses to obtain certain Microsoft products free of charge. All MET students are granted access to download the software for the duration of their study at MET College.

FAQ and basic information are at Microsoft Imagine Software Center.

VMware Academic Program

Metropolitan College is a member of The VMware Academic Program. VMAP enables current MET students and faculty to gain easy access to cutting-edge virtualization technology and resources.
All current MET students are granted access to download.

For information on how to login and get support, please visit VMware Academic Program.

Study Guide

The following material is collected here for your convenience but the required readings, discussion details, and assignment particulars can be found within the modules, in the "Discussion" section of the course, and in the "Assignment" sections respectively.

In preparation for this course you should read:

Forensic Examination of Digital Evidence: A Guide for Law Enforcement

NCJ 199408, April 2004, Special Report, National Institute of Justice

Digital Evidence in the Courtroom: A Guide for Law Enforcement & Prosecutors

Module 1 Study Guide and Deliverables

Readings: Online lecture material and *Guide to Computer Forensics and Investigations,* Chapters 1; Optional: *File System Forensic Analysis*, Chapter 2

Discussions: Post your introductions.

Discussion 1 and Discussion 2.

Assignments: Homework Assignment 1 ***Refer to Calendar for Due Dates***

Labs: Please attempt labs 1.1 - 1.4 that are listed in the module 2 labs. These labs install software you will need going forward. Take screenshots so you can use them for your Module 2 lab submission.

Assessments: Quiz 1 ***Refer to Calendar for Due Dates***

Module 2 Study Guide and Deliverables

Readings: Online lecture material and *Guide to Computer Forensics and Investigations,* Chapters 2 and 5; Optional: *File System Forensic Analysis*, Chapter 2

Discussions: Discussion 3

Discussion 4

Assignments: Homework Assignment 2 ***Refer to Calendar for Due Dates***

Labs: Lab 2

Module 3 Study Guide and Deliverables

Readings: Online lecture material and *Guide to Computer Forensics and Investigations,* Chapters 3 and 13; Optional: *File System Forensic Analysis*, Chapter 3

Discussions: Discussion 5

Discussion 6.

Assignments: Homework Assignment 3 ***Refer to Calendar for Due Dates***

Labs: Lab 3

Assessments: Mid-Term Exam.

Module 4 Study Guide and Deliverables

Readings: Online lecture material and *Guide to Computer Forensics and Investigations,* Chapters 4, 6, 8;

Discussions: No more Discussions past 6.

Assignments: Homework Assignment 4 ***Refer to Calendar for Due Dates***

Labs: Lab 4

Module 5 Study Guide and Deliverables

Readings: Online lecture material and *Guide to Computer Forensics and Investigations,* Chapters 9, 10, 11;

Discussions: No more Discussions past 6.

Assignments: Homework Assignment 5 ***Refer to Calendar for Due Dates***

Labs: Lab 5

Module 6 Study Guide and Deliverables

Readings: Online lecture material and *Guide to Computer Forensics and Investigations,* Chapters 12, 14;

Discussions: No more Discussions past 6.

Assignments: ***Refer to Calendar for Due Dates***

Labs: Lab 6

Final Exam Details

The Computer Science department requires that all final exams in the program be proctored. Consequently, the Final Exam in this course will be held on the last scheduled class : **Date TBD**.

During the final exam, students are required to work independently without using any additional notes or material. The Final is an Open-Book exam however accessing online material, lecture notes, emails, discussion boards, chat features or any other online material during the exam is **not** permitted, and some features of the online course may be disabled.

Please note that student activity during the final exam may be monitored and recorded in log files. Accessing any online or other material during the final exam is a major violation of the course policy and can result in serious academic disciplinary actions.

Course Grading Structure

Each module in this course will cover one or more core digital forensic principles, along with details on the collection, preservation, and analysis of digital evidence. Most modules will also have at least one lab component. Students will be able to demonstrate their understanding of the fundamental of digital forensics through these assignments.

Grading Policy

All students **will** be expected to demonstrate digital forensics knowledge and techniques. To obtain an exceptional grade you have to exceed expectations in your projects, quizzes and assignments.

Grading Structure and Distribution

The grade for the course is determined by the following:

Grading Scheme	
Homework Assignments	10%
Labs 5% & 10%	15%
Discussions/Participation	5%
Midterm Examination	10%
Group Lab	20%
Final Examination	30%
SE Project	10%

Grade Scale for class below :

Letter Grade	Honor Points	Decimal Range
A	4.0	95 +
A-	3.7	91 - 94
B+	3.3	88 - 90
B	3.0	84 - 87
B-	2.7	81 - 83
C+	2.3	78 - 80
C	2.0	74 - 77
C-	1.7	71 - 73
D	1.0	68 - 70
F	0.0	Below 67

The decimal range shows whole numbers, actual is always From X.00 to Y.99 (i.e. 91.00 – 94.99)

Course Requirements

Participation / Discussions

- Graded Discussions - all discussions will be graded on a 100-point scale.

Assignments and Labs

Assignments will be assigned during the semester to reinforce topics presented during classroom lectures. All homework must be the original effort of the student submitting the assignment.

Expectations

Many learning activities require sharing your assignments and opinions with your classmates. For example, you may be given a set of criteria on the basis of which to evaluate other classmates' assignments, and asked to submit the results to your facilitator by a specified date. It is, therefore, very important that you, as well as your classmates, submit your assignments on a timely basis. Timely submission by all will result in each of you being able to evaluate each other's assignments. Due dates will be indicated for each assignment in the Assignments section of the course.

Lateness

We recognize that emergencies and unexpected but significant extensions in work hours occur in professional and personal lives. If one occurs that prevents your completion of a course item by a deadline, please make this plain to your instructor. This must be done well **in advance** of the deadline (unless it is an emergency that makes this impossible, of course), and should be accompanied by particulars that back it up. Additional documentation may be requested. If this is permitted at the discretion of the instructor, a minimum of Twenty points will otherwise be deducted for late submissions on a per day basis: we want to be fair to everyone in this process, including the vast majority of you who sacrifice so much to submit your homework on time in this demanding schedule.

Academic Conduct Policy

Please visit Metropolitan College's website for the full text of the department's *Academic Conduct Code*.

A Definition of Plagiarism

> "The academic counterpart of the bank embezzler and of the manufacturer who mislabels products is the plagiarist: the student or scholar who leads readers to believe that what they are reading is the original work of the writer when it is not. If it could be assumed that the distinction between plagiarism and honest use of sources is perfectly clear in everyone's mind, there would be no need for the explanation that follows; merely the warning with which this definition concludes would be enough. But it is apparent that sometimes people of goodwill draw the suspicion of guilt upon themselves (and, indeed, are guilty) simply because they are not aware of the illegitimacy of certain kinds of "borrowing" and of the procedures for correct identification of materials other than those gained through independent research and reflection."
>
> "The spectrum is a wide one. At one end there is a word-for-word copying of another's writing without enclosing the copied passage in quotation marks and identifying it in a footnote, both of which are necessary. (This includes, of course, the copying of all or any part of another student's paper.) It hardly seems possible that anyone of college age or more could do that without clear intent to deceive. At the other end there is the almost casual slipping in of a particularly apt term which one has come across in reading and which so aptly expresses one's opinion that one is tempted to make it personal property."
>
> "Between these poles there are degrees and degrees, but they may be roughly placed in two groups. Close to outright and blatant deceit-but more the result, perhaps, of laziness than of bad intent-is the patching together of random jottings made in the course of reading, generally without careful identification of their source, and then woven into the text, so that the result is a mosaic of other people's ideas and words, the writer's sole contribution being the cement to hold the pieces together. Indicative of more effort and, for that reason, somewhat closer to honest, though still dishonest, is the paraphrase, and abbreviated (and often skillfully prepared) restatement of someone else's analysis or

conclusion, without acknowledgment that another person's text has been the basis for the recapitulation."

The paragraphs above are from **H.** Martin and R. Ohmann, *The Logic and Rhetoric of Exposition, Revised Edition.* Copyright 1963, Holt, Rinehart and Winston.

Academic Conduct Code

I. **Philosophy of Discipline**

The objective of Boston University in enforcing academic rules is to promote a community atmosphere in which learning can best take place. Such an atmosphere can be maintained only so long as every student believes that his or her academic competence is being judged fairly and that he or she will not be put at a disadvantage because of someone else's dishonesty. Penalties should be carefully determined so as to be no more and no less than required to maintain the desired atmosphere. In defining violations of this code, the intent is to protect the integrity of the educational process.

II. **Academic Misconduct**

Academic misconduct is conduct by which a student misrepresents his or her academic accomplishments, or impedes other students' opportunities of being judged fairly for their academic work. Knowingly allowing others to represent your work as their own is as serious an offense as submitting another's work as your own.

III. **Violations of this Code**

Violations of this code comprise attempts to be dishonest or deceptive in the performance of academic work in or out of the classroom, alterations of academic records, alterations of official data on paper or electronic resumes, or unauthorized collaboration with another student or students. Violations include, but are not limited to:

A. **Cheating on examination.** Any attempt by a student to alter his or her performance on an examination in violation of that examination's stated or commonly understood ground rules.

B. **Plagiarism.** Representing the work of another as one's own. Plagiarism includes but is not limited to the following: copying the answers of another student on an examination, copying or restating the work or ideas of another person or persons in any oral or written work (printed or electronic) without citing the appropriate source, and collaborating with someone else in an academic endeavor without acknowledging his or her contribution. Plagiarism can consist of acts of commission-appropriating the words or ideas of another-or omission failing to acknowledge/document/credit the source or creator of words or ideas (see below for a detailed definition of plagiarism). It also includes colluding with someone else in an academic endeavor without acknowledging his or her contribution, using audio or video footage that comes from another source (including work done by another student) without permission and acknowledgement of that source.

C. **Misrepresentation or falsification of data** presented for surveys, experiments, reports, etc., which includes but is not limited to: citing authors that do not exist; citing interviews that never took place, or

field work that was not completed.

D. **Theft of an examination.** Stealing or otherwise discovering and/or making known to others the contents of an examination that has not yet been administered.

E. **Unauthorized communication during examinations.** Any unauthorized communication may be considered prima facie evidence of cheating.

F. **Knowingly allowing another student to represent your work as his or her own.** This includes providing a copy of your paper or laboratory report to another student without the explicit permission of the instructor(s).

G. **Forgery, alteration, or knowing misuse of graded examinations, quizzes, grade lists, or official records of documents,** including but not limited to transcripts from any institution, letters of recommendation, degree certificates, examinations, quizzes, or other work after submission.

H. **Theft or destruction of examinations or papers** after submission.

I. **Submitting the same work in more than one course** without the consent of instructors.

J. **Altering or destroying another student's work or records,** altering records of any kind, removing materials from libraries or offices without consent, or in any way interfering with the work of others so as to impede their academic performance.

K. **Violation of the rules governing teamwork.** Unless the instructor of a course otherwise specifically provides instructions to the contrary, the following rules apply to teamwork: 1. No team member shall intentionally restrict or inhibit another team member's access to team meetings, team work-in-progress, or other team activities without the express authorization of the instructor. 2. All team members shall be held responsible for the content of all teamwork submitted for evaluation as if each team member had individually submitted the entire work product of their team as their own work.

L. **Failure to sit in a specifically assigned seat during examinations.**

M. **Conduct in a professional field assignment that violates the policies and regulations of the host school or agency.**

N. **Conduct in violation of public law occurring outside the University that directly affects the academic and professional status of the student, after civil authorities have imposed sanctions.**

0 . **Attempting improperly to influence the award of any credit, grade, or honor.**

P. **Intentionally making false statements to the Academic Conduct Committee or intentionally presenting false information to the Committee.**

Q. **Failure to comply with the sanctions imposed under the authority of this code.**

Disability Services

In accordance with University policy, every effort will be made to accommodate unique and special needs of students with respect to speech, hearing, vision, or other disabilities. Any student who feels he or she may need an accommodation for a documented disability should contact Disability & Access Services at (617) 353-3658 or at access@bu.edu for review and approval of accommodation requests.

Netiquette

The Office of Distance Education has produced a netiquette guide to help you understand the potential impact of your communication style.

Before posting to any discussion forum, sending email, or participating in any course or public area, please consider the following:

Ask Yourself ...

- How would I say this in a face-to-face classroom or if writing for a newspaper, public blog, or wiki?
- How would I feel if I were the reader?
- How might my comment impact others?
- Am I being respectful?
- Is this the appropriate area or forum to post what I have to say?

Writing

When you are writing, please follow these rules:

- **Stay polite and positive in your communications.** You can and should disagree and participate in discussions with vigor; however, when able, be constructive with your comments.
- **Proofread your comments before you post them.** Remember that your comments are permanent.
- **Pay attention to your tone.** Without the benefit of facial expressions and body language your intended tone or the meaning of the message can be misconstrued.
- **Be thoughtful and remember that classmates' experience levels may vary.** You may want to include background information that is not obvious to all readers.
- **Stay on message.** When adding to existing messages, try to maintain the theme of the comments previously posted. If you want to change the topic, simply start another thread rather than disrupt the current conversation.

- **When appropriate, cite sources.** When referencing the work or opinions of others, make sure to use correct citations.

Reading

When you are reading your peers' communication, consider the following:

- **Respect people's privacy.** Don't assume that information shared with you is public; your peers may not want personal information shared. Please check with them before sharing their information.
- **Be forgiving of other students' and instructors' mistakes.** There are many reasons for typos and misinterpretations. Be gracious and forgive other's mistakes or privately point them out politely.
- **If a comment upsets or offends you, reread it and/or take some time before responding.**

Important Note

Don't hesitate to let your instructor or your faculty and student support administrator know if you feel others are inappropriately commenting in any forum.

All Boston University students are required to follow academic and behavioral conduct codes. Failure to comply with these conduct codes may result in disciplinary action.

Technical Support

Boston University technical support is available via email (ithelR.@bu.edu), the support form, and phone (888-243-4596). Please note that the IT Help Center has multiple locations. All locations can be reached through the previously mentioned methods. For IT Help Center hours of operation please visit their contact page. For other times, you may still submit a support request via email, phone, or the support form, but your question won't receive a response until the following day. If you aren't calling, it is highly recommended that you submit your support request via the technical-support form as this provides the IS&T Help Center with the best information in order to resolve your issue as quickly as possible.

Examples of issues you might want to request support for include the following:

- Problems viewing or listening to sound or video files
- Problems accessing internal messages
- Problems viewing or posting comments
- Problems attaching or uploading files for assignments or discussions
- Problems accessing or submitting an assessment

To ensure the fastest possible response, please fill out the online form using the link below:

IT Help Center Support
888-243-4596 or 617-353-4357 or Web
Check your open tickets using BU's ticketing system.

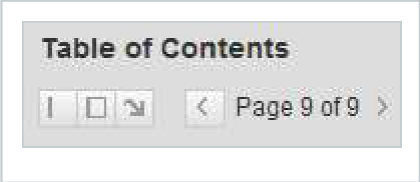
Navigating Courses

For best results when navigating courses, it is recommended that you use the Mozilla Firefox browser.

The Table of Contents may contain folders. These folders open and close(+ and - signs) and may conceal some pages. To avoid missing content pages, you are advised to use the next- and previous-page buttons (and icons) in the top-right corner of the learning content.

Please also familiarize yourself with the navigation tools, as shown below; these allow you to show and hide both the Course Menu and the Table of Contents on the left. This will be helpful for freeing up screen space when moving through the weekly lecture materials.

Navigation tools for the Table of Contents are shown in the image below:



Clicking on the space between the Course Menu and the Table of Contents allows you to show or hide the Course Menu on the left:

Web Resources/Browser Plug-Ins

To view certain media elements in this course, you will need to have several browser plug-in applications installed on your computer. See the Course Resources page in the syllabus of each individual course for other specific software requirements .

- Check your computer's compatibility by reviewing Blackboard's System Requirements
- Check your browser settings with Blackboard's Connection Test
- Download most recent version of Adobe Flash Player
- Download most recent version of Adobe Acrobat Reader

How to Clear Your Browser Cache

The IT Help Center recommends that you periodically clear your browser cache to ensure that you are viewing the most current content, particularly after course or system updates.

This page is also found within the "How to... " section of the online documentation, which contains a list of some of the most common tasks in Blackboard Learn.