Syllabus

This syllabus is specific to section B01

Logistics

Day: Monday/Wednesday
Time: 7:20 – 10:00 PM
Location: Fairfax Campus (Nguyen Engineering Building 1505)

Course-specific Hardware/Software

You will need access to a computer with VMWare (Windows 7) installed to complete the labs. These programs are available to you free through GMU. Additional information will be provided on Blackboard. It is suggested, but not mandatory, that you bring this with you to class to work on labs.

Some assignments will require additional software installation. Software downloads will be available for free download online.

University Policies

The University Catalog is the central resource for university policies affecting student, faculty, and staff conduct in university affairs. Unless explicitly noted, any conflict between the policies in the University Catalog and the content of this document is unintentional. Please notify the author to resolve any such conflicts.

Course Description

IT 357 - Computer Crime, Forensics, and Auditing
CRIM 304 - Computer Crime, Forensics, and Auditing

Credits: 3
Covers computer crime, relevant laws, agencies, and standards. Presents auditing, logging, forensics, and related software. Explores legal principles such as chain of evidence, electronic document discovery, eavesdropping, and entrapment. Students get hands-on experience with forensics tools.

Equivalent to CRIM 304 (2011-12 Catalog)

**Prerequisite(s):** IT 103 and IT 223; or permission of department.

Prerequisite enforced by registration system.

**Notes:** Students cannot receive credit for both IT 222 and 357.

**Hours of Lecture or Seminar per week:** 3


### Prerequisites

The prerequisites for this course are [IT 103](http://catalog.gmu.edu/preview_course.php?catoid=17&coid=111263) and [IT 223](http://catalog.gmu.edu/preview_course.php?catoid=17&coid=108606); or permission from the Department of Applied Information Technology. Unless a waiver is granted, a grade of "C" or better must be achieved in each prerequisite course before a student is qualified to take this course. The prerequisite courses must be completed prior to, not concurrently with, this course.

Note: Departmental permission to waive the prerequisite requirement is rarely given, and only where a student can demonstrate mastery of the course material – this typically requires significant industry experience, a recognized certification, and passing a waiver exam.

This requirement will be strictly enforced. Any student who does not meet the prerequisite requirement will be dropped from the course by the Instructor at the start of the semester and the student will be responsible for any consequences of being dropped.

### Rationale

This course is intended to help prepare students for careers in homeland defense, law enforcement, or commercial IT security, and for graduate work in security, information systems, or law.

Students will learn the principles of computer investigations and digital evidence. They will learn about jurisdiction, chain of evidence, and legal authority. Social, legal, and ethical implications will be carefully considered. Hands-on exercises will give students experience imaging disks, recovering system files, and analyzing logs on both Windows and Linux platforms.

This course is an option in the Information Security (INFS) concentration of the IT major, an elective in the IT minor, and an elective in the Criminology, Law and Society major and minor.
**Objectives**

On successful completion of this course, students will:

- Understand the legal and technical aspects of computer forensics.

- Understand applicable laws, and the roles of legal authorities.

- Understand how to obtain and handle digital evidence, and will have been exposed to a range of freeware forensic tools.

**References**

**Textbooks**

There are two required textbooks for this course:

|------------|---------|-----------|---------|---------|---------------------|
There is one recommended (but not required) textbook for this course:

**Cyber Crime Fighters: Tales from the Trenches**  
Felicia Donovan and Kristyn Bernier  
ISBN-10: 0-7897-3922-4  
© 2009; Que Publishing

Publisher’s pricing (as of 1/14/2013):  
Paperback: $17.59  
Electronic: $14.39

---

**Faculty and Staff**

Instructor:  
Rebecca J. Tenally  
Email:  rredman@gmu.edu  
Office hours:  [http://mason.gmu.edu/~rredman](http://mason.gmu.edu/~rredman)

Administrative support:  
Cindy Woodfork  
Prince William campus  
Bull Run Hall, Suite 102  
Email:  cwoodfo1@gmu.edu  
Phone:  703-993-8461
Grading

Grades will be awarded in accordance with the Mason Grading System for undergraduate students. See the University Catalog, Academic Policies, Grading System for more information.

The grading scale for this course is:

<table>
<thead>
<tr>
<th>Percentage</th>
<th>Grade</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>97 – 100%</td>
<td>A+</td>
<td>Passing</td>
</tr>
<tr>
<td>93 – 96%</td>
<td>A</td>
<td>Passing</td>
</tr>
<tr>
<td>90 – 92%</td>
<td>A-</td>
<td>Passing</td>
</tr>
<tr>
<td>87 – 89%</td>
<td>B+</td>
<td>Passing</td>
</tr>
<tr>
<td>83 – 86%</td>
<td>B</td>
<td>Passing</td>
</tr>
<tr>
<td>80 – 82%</td>
<td>B-</td>
<td>Passing</td>
</tr>
<tr>
<td>77 – 79%</td>
<td>C+</td>
<td>Passing</td>
</tr>
<tr>
<td>73 – 76%</td>
<td>C</td>
<td>Passing</td>
</tr>
<tr>
<td>70 – 72%</td>
<td>C-</td>
<td>Passing*</td>
</tr>
<tr>
<td>60 – 69%</td>
<td>D</td>
<td>Passing*</td>
</tr>
<tr>
<td>0 – 59%</td>
<td>F</td>
<td>Failing</td>
</tr>
</tbody>
</table>

* Grades of "C-" and "D" are considered passing grades for undergraduate courses. However, some majors may require a higher grade when one course is a prerequisite for another. See the University Catalog for prerequisite requirements.

Raw scores may be adjusted by the Instructor to calculate final grades.

Final grades will be determined based on the following components:

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Work</td>
<td>15%</td>
</tr>
<tr>
<td>Current Event Reports</td>
<td>10%</td>
</tr>
<tr>
<td>Quizzes</td>
<td>10%</td>
</tr>
<tr>
<td>Project</td>
<td>25%</td>
</tr>
<tr>
<td>Mid-term exam</td>
<td>20%</td>
</tr>
<tr>
<td>Final exam</td>
<td>20%</td>
</tr>
</tbody>
</table>

These components are outlined in the following sections.

Class Work (Labs and In Class Assignments)

Labs and other exercises will be assigned in class. Class sessions will include time in a computer lab classroom. Students are expected to attend every class session and work on labs during class time; some labs may require additional time outside of the class session. Any student who misses an in class assignment due to an unexcused absence will receive zero (0) for that assignment.
Current Event Reports
Each student is required to research three current events related to course content, as directed by the Instructor. For each event, the student will write a summary and an opinion, and submit the report as directed.

Quizzes/Blogs
Quizzes will be given in selected classes throughout the semester, and will not be announced in advance. Any student who misses a quiz due to an unexcused absence will receive zero (0) for that quiz. Blog topics may be posted on Blackboard in response to lectures or current events. Each student is required to respond to the topic on the discussion board within one week of its posting or specified due date.

Project
The Instructor will assign a project that will involve both group and individual activities. Each student individually will prepare and submit a project in accordance with requirements to be discussed in class.

Mid-term exam
The mid-term exam will be conducted during the fifth scheduled class session and will be based on topics addressed in Lectures 1-4. The mid-term exam will be “closed book” – no reference materials other than those provided with the exam paper will be permitted. Mid-term exams will be returned to students once all mid-term exams for all sections have been graded. Exams are timed. If you are late, you will not get extra time on the exam. No one will be admitted to the exam after someone has left the room.

Final exam
The final exam will be held during the scheduled final exam session (see http://summer.gmu.edu/finalexams/) and will be based on topics addressed throughout the entire course. The final exam will be “closed book” – no reference materials other than those provided with the exam paper will be permitted. Final exams will be retained by the Department of Applied Information Technology and will not be returned to students. Exams are timed. If you are late, you will not get extra time on the exam. No one will be admitted to the exam after someone has left the room.

Students are expected to submit work as scheduled by the Instructor. Late work may not be accepted – if accepted, a penalty may be applied. Acceptance of late work and/or application of penalties will be at the sole discretion of the Instructor. In general it is better to submit an incomplete assignment on time for partial credit than to submit a complete assignment late and risk receiving no credit.
EXAM/QUIZ POLICY

The exams will begin promptly at the scheduled time and is timed. If you arrive late, you will not get additional time on the exam. Students arriving late will not be permitted to take the exam or quiz if they arrive after any student has left the room. No exceptions. You must present your GMU ID at the exam. No card = zero for the exam.

In order to take exams at an alternate time, a formal request must be made and approved by the instructor, course coordinator, and the Dean prior to the final exam date. See the forms below.  
http://volgenau.gmu.edu/forms/RescheduleFinalExamInstructions.pdf  
http://volgenau.gmu.edu/forms/final_examination_reschedule.pdf

Mid-term and final grades will be posted to PatriotWeb, which is the only vehicle for students to obtain those grades. A student with a "hold" on his/her PatriotWeb account will be unable to access grades until the hold has been removed by the Registrar.
### Schedule *(Subject to Change)*

<table>
<thead>
<tr>
<th>Lecture</th>
<th>Content</th>
<th>Reading*</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>IP&amp;R</td>
</tr>
<tr>
<td>1</td>
<td>Introduction to course/syllabus/policies</td>
<td>Ch. 1,</td>
</tr>
<tr>
<td></td>
<td>Introduction to Computer Forensics</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>Crime &amp; Law – pt 1</td>
<td>§3-1 to 3-9</td>
</tr>
<tr>
<td>3</td>
<td>Crime &amp; Law – pt 2</td>
<td>Ch. 3,</td>
</tr>
<tr>
<td></td>
<td>Search &amp; seizure; Crime scene procedures</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>Hardware forensics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Review for mid-term exam</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>Mid-term exam</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Class work</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Report Writing</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Crime Scene Activity</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Field Trip Activity</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Software/Windows Forensics – pt 1</td>
<td>Ch. 6</td>
</tr>
<tr>
<td>10</td>
<td>Holiday <em>(no class session)</em></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Software/Windows Forensics – pt 2</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Individual project lab time</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Linux, Unix, Mac file systems and forensics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cell phone forensics; Password cracking</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Network forensics, Logging and auditing</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Review for final exam</td>
<td></td>
</tr>
<tr>
<td>-</td>
<td><strong>Final exam</strong></td>
<td></td>
</tr>
</tbody>
</table>
The reading assignment shown for each lecture is to be completed prior to that lecture.

* IP&R: Computer Forensics: Investigation Procedures and Response
  IHD: Computer Forensics: Hard Disk and Operating Systems

Important Dates

Please see http://summer.gmu.edu/ for important dates, including the last days to add and drop courses.

Religious Holidays

A list of religious holidays is published by University Life. Any student whose religious observance conflicts with a scheduled course activity must contact the Instructor at least 2 weeks in advance of the conflict date in order to make alternative arrangements.

Attendance Policy

Students are expected to attend every class, to complete any required preparatory work (including assigned reading – see Schedule above) and to participate actively in lectures, discussions and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with Instructor if they know in advance that they will miss any class and to consult with the Instructor as soon as possible if they miss any class without prior notice. Any student who expects to miss more than one class session is strongly advised to drop the course and take it in a later semester when he/she can attend every class.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam will result in a score of zero (0) for that exam, in accordance with Mason policy on final exams. Students should not make travel plans or other discretionary arrangements that conflict with scheduled classes and/or exams. If the University is closed due to weather or other unforeseen conditions, final exams may be rescheduled – students are strongly advised not to make plans that would prevent them from attending exams that may be rescheduled during the entire exam period, including the scheduled make-up dates.
Classroom conduct

Students are expected to conduct themselves in a manner that is conducive to learning, as directed by the Instructor. Any student who negatively impacts the opportunity for other students to learn may be asked to leave the classroom.

Electronic devices are potential distractions in the classroom environment. Cell phones, pagers and other handheld devices must be turned off or set to "silent" mode and not used while class is in session. Laptop computers and similar devices may be used only if such use is directly related to the classroom activity in progress – for some activities the Instructor may require that such devices not be used in order to maximize student engagement.

Communications

Registered students will be given access to a Blackboard section for this course. Blackboard will be used as the primary mechanism (outside of lectures) to disseminate course information, including announcements, lecture slides, homework and other assignments, and scores for homework and exams.

Communication with the Instructor on issues relating to the individual student should be conducted using Mason email, via telephone, or in person - not in the public "Discussions" forums on Blackboard. Federal privacy law and Mason policy require that any communication with a student related in any way to a student’s status be conducted using secure Mason systems – if you use email to communicate with the Instructor you MUST send messages from your Mason email account. Students must activate and monitor their Mason email accounts to receive important information from the University, including messages related to this class.

Lecture slides are complements to the lecture process, not substitutes for it - access to lecture slides will be provided in Blackboard as a courtesy to students provided acceptable attendance is maintained.

All course materials (lecture slides, assignment specifications, etc) are published on Blackboard in Adobe® Portable Document Format (PDF). This allows users of most computing platforms to view and print these files. Microsoft® Word (or a compatible word processing application) is required for preparing assignments – it is available on computers in the Mason open labs.

Privacy

Instructors respect and protect the privacy of information related to individual students.

As described above, issues relating to an individual student will be discussed via email, telephone or in person. Instructors will not discuss issues relating to an individual student with other students (or anyone without a need to know) without prior permission of the student.
Homework, quizzes, mid-term exams and other assessable work will be returned to individual students directly by the Instructor (or by a faculty or staff member or a Teaching Assistant designated by the Instructor, or via another secure method). Under no circumstances will a student's graded work be returned to another student.

Instructors, staff, and Teaching Assistants will take care to protect the privacy of each student's scores and grades.

**Disability Accommodations**

The Office of Disability Services (ODS) works with disabled students to arrange for appropriate accommodations to ensure equal access to university services. Any student with a disability of any kind is strongly encouraged to register with ODS as soon as possible and take advantage of the services offered.

Accommodations for disabled students **must** be made in advance – ODS cannot assist students retroactively, and at least one week's notice is required for special accommodations related to exams. Any student who needs accommodation should contact the Instructor during the first week of the semester so the sufficient time is allowed to make arrangements.

**Campus Notifications**

Students are encouraged to subscribe to the Mason Alert system to receive notifications of campus emergencies, closings, and other situations that could affect class activities.

Each classroom has a poster explaining actions to be taken in different types of crisis. Further information on emergency procedures is available at [http://www.gmu.edu/service/cert](http://www.gmu.edu/service/cert). In the event of an emergency, students are encouraged to dial 911.

**Other Resources**

Mason provides many useful resources for students. The following resources may be particularly useful:

- The Writing Center
- The Academic Advising Center
- The University Libraries
- Counseling and Psychological Services
- University Career Services

See [http://www2.gmu.edu/resources/students/](http://www2.gmu.edu/resources/students/) for a complete listing of Mason resources for students.
Academic Integrity

All members of the Mason community are expected to uphold the principles of scholarly ethics.

The IT program is designed to achieve several specific outcomes. One of those outcomes is: “An understanding of professional, ethical, legal, security, and social issues and responsibilities.”

Graduating students are bound by the ethical requirements of the professional communities they join. The ethics requirements for some of the communities relevant to IT graduates are available via the following links:

- ACM Code of Ethics and Professional Conduct
- IEEE Code of Ethics
- EC-Council Code of Ethics

On admission to Mason, students agree to comply with the requirements of the Mason Honor Code. The Honor Code will be strictly enforced in this course. Honor Code cases are heard by a panel of students – students who meet the requirements are encouraged to nominate themselves to serve on the Honor Committee.

Any use of the words or ideas of another person(s), without explicit attribution that clearly identifies the material used and its source in an appropriate manner, is plagiarism and will not be tolerated. Dean Griffiths has mandated a "zero tolerance" policy for plagiarism within the Volgenau School of Engineering. The Instructor reserves the right to use manual and/or automated means (including such services as SafeAssign) to detect plagiarism in any work submitted by students for this course, and to direct Teaching Assistants and/or other faculty and/or staff members to do likewise in support of this course.

For this course, the following requirements are specified:

- All assessable work is to be prepared by the individual student, unless the Instructor explicitly directs otherwise.

- All work must be newly created by the individual student for this course for this semester. Any usage of work developed for another course, or for this course in a prior semester, is strictly prohibited without prior approval from the Instructor.
Students may seek assistance with assigned work (and are encouraged to do so if they feel the need), provided:

- The directions for the assigned work do not prohibit such assistance.
- Such assistance is explicitly acknowledged in the submitted work, clearly identifying the person(s) giving assistance and the nature of the assistance given.
- Any work to be submitted is prepared entirely and exclusively by the student submitting it. Students are expressly prohibited from sharing any assessable work for this course in any manner with other students (except students assigned as Teaching Assistants or Undergraduate Peer Mentors to this course and the student's section), unless all students involved have had their work graded and returned by the Instructor, or the Instructor has explicitly approved such sharing.

Another aspect of academic integrity is the free exchange of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions.

Students are encouraged to ask for clarification of any issues related to academic integrity and to seek guidance from the Instructor, other faculty members or advisors, or the Office for Academic Integrity.