09 Jan 2017

Subj: SY486 COURSE POLICY – AY2017 Spring

Ref: (a) ACDEANINST 1531.58, Administration of Academic Programs

(b) ACDEANINST 1531.64, Academic Accountability

(c) CYBSCIINST 3120.32, Cyber Science Department Standard Organization and

Regulations Manual

(d) ACDEANNOTE 1531, Academic Scheduling and Start of Semester Items

Encl: (1) SY486 Collaboration Policy

1. Purpose.

Per references (a) through (d), the following comprises the course policies for SY486 – Cyber Crime Investigations, AY2017 Spring term.

*WARNING: As a student in this class, you will learn concepts and gain experience with tools that could be used unethically. DO NOT use knowledge or experience gained for unethical purposes. You MAY NOT use tools and techniques learned in this class to violate USNA policy, or any other government restrictions on information system use. You should never employ offensive cyber operations on any information system without the express written consent of the information system owner or legal authority.*

1. General Information.
   1. Course: SY486 – Cyber Crime Investigations
   2. Credits: 1-1-1
   3. Term: AY2017 Spring
   4. Prerequisites: None
2. Course Description

The course covers the digital forensic processes and technologies used to preserve, extract, analyze and present digital evidence for prosecution purposes. Evidence handling, chain of custody, imaging and hashing, file systems, Windows registry, mobile forensics, virtual machine forensics, email investigations, laws regarding digital evidence, advanced topics in digital forensics and reporting are covered. Hands-on exercises, team discussion forums, and team project reinforce the subject matter.

1. Course Learning Outcomes
   1. Through this course and your collective efforts you will be able to:
   2. Discuss the rules, laws, policies, and procedures that affect digital forensics.
   3. Demonstrate proper use of forensic tools to create and analyze a forensic image and produce the associated report.
   4. Perform the steps included in digital investigations from the initial recognition of an incident through the steps of evidence gathering, preservation and analysis, through the completion of legal proceedings.
   5. Write professional quality reports that include both a summary report and a notes section, which describes the technical procedures used in the investigation.
   6. Identify major components of the NTFS and EX2 file systems and associated forensic artifacts.
   7. Identify important file metadata and apply their use in a forensic investigation.
   8. Identify procedures used in network forensics and correlate network evidences to rationalize the implications of the incident
   9. Conduct a forensic investigation on a mobile device.
   10. Perform email investigations
   11. Discuss latest trends in digital forensics; IoT, cloud forensics, SSD, virtual machine
2. Tentative Content organization

|  |  |
| --- | --- |
|  | **Topic** |
| 1 | Introduction to the course and digital forensics concepts |
| 2 | Investigative methodology and report writing |
| 3 | Laws, rules, affecting digital evidence/Processing evidence |
| 4 | Data acquisition and verification (seizing, imaging, hashing) |
| 5 | Digital forensics tools and tool validation |
| 6 | Hierarchy of access |
| 7 | File Systems and Partitions |
| 8 | Logical analysis |
| 9 | Hard drive and physical analysis |
| 10 | Windows Application Analysis |
| 11 | Windows registry analysis |
| 12 | Network forensics |
| 13 | Email and Internet Forensics |
| 14 | Mobile Forensics |
| 15 | Advanced forensic topics(Virtual machines, IoT, Cloud Forensics) |

1. Required Texts

Guide to Computer Forensics and Investigations. 5th EditionISBN: 978-1285060033

1. Recommended text (especially on File Systems)

Carrier, Brian, *File System Forensic Analysis*, Addison-Wesley, 2005, pgs 569. (ISBN 0-32-126817-2)

Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.) London, England: Academic Press.

1. Computer

You are required to bring your government issued laptop sufficiently charged or additionally bring your laptop battery charger to every class meeting. You will make heavy use of your laptop in most class meetings. You will be marked as late if you have to return to your room to get your laptop or your laptop battery charger.

1. Materials

Class materials, including grades, will be posted to Blackboard. It is your responsibility to come to every class with all of the required materials, in an uncompressed format. The materials can be saved on a laptop and must be easily accessible for in-class labs.

1. Assessment

* **10% : Discussion (graded each week)**

You have been placed in teams of four. Each week you are expected to visit the following Websites:

:<https://cybercrimeinvestigators.com/gallery>, Here you will find a collection of videos relating to computer forensics, cybercrime and malware. Here is what you are expected to do:

At the start of each week, decide. As a team on a video to watch. This excludes the spring break week, and two last weeks of classes.

Individually watch/read the video/article and post a thoughtful comment (initial post) to your team discussion board in Blackboard by Thursday midnight. Post a response to another student post by Sunday midnight. A post should between 50 and 100 words.

Some of my favorite websites include: http://www.forensicfocus.com/; . http://www.digital-detective.net/news-and-events/digital-forensic-news/

* **15% Labs and Assignments**

Most classes will involve labs. MIDNs are expected to complete and submit in Blackboard.

* **35%: (20% each): Six week and 12 week exam**

The Six week and the 12 week exam will each account for 20% of the MIDN’s grade in the course. Each of the exams will be composed of multiple choices, true/false, and short questions. The six-week exam will contain questions that are cumulative from the first half of the semester. The 12 week exam will contain questions from the 7th week to the 12th week. The exams will be closed book, however, each MIDN will be allowed to bring in standard size index card (3 by 5 inches) of hand-written notes to use as reference. You may write on both sides of the page.

* **20%: Final Exam**

Final Exam will be composed of multiple choice, true/false, and short questions. The six-week exam will contain questions that are cumulative from the entire course. The exam accounts for 20% of the final grade. The exams will be closed book, however, each MIDN will be allowed to bring in standard size index card (3 by 5 inches) of hand-written notes to use as reference. You may write on both sides of the page.

* **20% :Team Project-** More details on the project are on a separate handout.
* **Late Policy:** Late work will not be accepted for credit (a 0 will be recorded in the grade book), but will be reviewed and returned with feedback provided.
* **Absences:** As a leader you are expected to look ahead, identify issues, and propose solutions. It is your responsibility to discuss your plans to make up course material with your Instructor at least one week prior to a planned absence (MO, medical/dental appointment, etc.). If an unplanned absence occurs at the last minute you shall contact your Instructor (likely via email) to arrange plans to make up course material as soon as possible. A plan approved by your Instructor overrides the Late Policy. Failing to discuss plans to make up material prior to a planned absence or by the day you return from an unplanned absence will result in the missed assignments being treated as late. Effort will be made to make the requisite course material available to you before a planned absence to allow you to complete assignments prior to your departure to support you not falling behind academically.
* **Honor Policy:** Unless stated otherwise on a specific assignment, the following collaboration policies shall apply to the assignments of that type. You are charged with understanding and executing the honor policy, and seeking clarification at any time if there is a potential misconception; if in doubt, seek clarification from your Instructor.
* **Other:** No use of cell phones in class. Beverages are permitted in classrooms and laboratories provided they are in closed containers. No food or smokeless tobacco products are permitted in classrooms or laboratories. You shall attend to personal matters before the start of class.
* Section Leader. The Section Leader will:
  + Call the class to attention at the beginning and end of each class session, and report muster results
  + In the event the Instructor is not present five minutes after the start of a class session, report to the Mathematics and Science Division front office (MI380) and report that your Dr. Shumba is not present;
  + Assist the Instructor as directed by the Instructor.
  + Act as Section liaison to the Instructor.
* Assistant Section Leader. The Assistant Section Leader will:
  + Assist the Section Leader as directed by the Section Leader;
  + Act as Section Leader in the absence of the Section Leader.

A. S. PARRISH

Chair, Cyber Science Department