CpE-435 Computer Incident Response

[August 17, 2014]…rsn

DRAFT

Semester : Fall 2014

Table of Contents

"We assumed the digital footprints we left behind
– our clickstream exhaust, so to speak --
were as ephemeral as a phone call, fleeting, passing, unrecorded.
…Our tracks through the digital sand are [in fact] eternal."

T. Zeller, Jr., "Link by Link; Lest We Regret Our Digital Breadcrums." The New York Times, 12 June 2006. www.nytimes.com/2006/06/12/technology/12link.html

CpE-435 Computer Forensics

Semester : Fall-2014

Course Format
and Credit Hours : 3 hr Lecture, 3 hr Credit

Pre-requisites : CpE-310/311 AND CS-350, OR Consent
i.e. Student should be knowledgeable in a high level language as well as assembly language, have computer architecture or computer organization background. Preferred to have CS-453, TCP/IP, as well but not required.

Co-requisites : none

Instructor : Dr. Roy S Nutter, Office: 933 ESB
Tel: 293-9131
e-mail: rnutter@wvu.edu

Schedule : MWF 10-10:50

Location : 355 ESB
Labs will be in the West Virginia Cyber Crime Cooperative (WV3C) facility, Suite 3102 (Prete Bld), 3040 University Ave, Morgantown, WV

Office Hours : MWF 1100-1200 or by appointment (best to call or e-mail me to be sure I will be there.

(*PLEASE use Subject Line beginning with "CpE-435" in all e-mail to me.)*

Course Objectives: This course is to serve as an overview course of digital forensics and incident response. Objectives include proper and legal investigation procedures, the legal basis thereof, and the technical basis. The student should be capable of good decision making with due regard for the legal process and procedures during and following investigation of computer incidents. When completed, the student shall be prepared to embark upon more detailed computer forensics endeavors.

Expected Learning
Outcomes : Upon successful completion of this course:
Law and ethics: The Student shall be able to

1. Describe the basics of the justice system and how it relates to digital forensics and digital evidence.
2. Understand the basics of the legal system and the differences between the civil and criminal processes

    a. discuss ethical (as well as legal issues) such as software piracy, reverse engineering, import/export rules, music sharing, etc and its impacts on a company's financial bottom line,
    b. discuss Intellectual property, patents, copyright, piracy, reverse engineering, import/export rules

3. discuss a basic knowledge of the Bill of Rights and constitutional law
    a. discuss the 4th Amendment to the US Constitution and how it applies to computer and network search and seizure,
4. discuss and recommend industrial computer policies,
5. Learn the rules and issues relating to the admissibility of evidence, both constitutional and statutory, to include search and seizure, chain of custody, and suppression; highlight the differences between civil and criminal situations and employer/employee issues
    a. apply the rules of evidence as they relate to an electronic crime scene and to obtaining computer evidence. (i.e. recognize what can and can NOT be seized at an electronic crime scene.)
6. Understand statutes such as the ECPA and the legal requirements for obtaining electronic information
7. Understand the fundamentals of preparing for and providing depositions and court testimony
8. discuss the implications of the US Patriot Act,

Security, management, and forensics: The student shall be able to

1. Identify the file systems usually associated with the most common digital media storage devices.
2. Understand and demonstrate application-level digital evidence for the most common types of applications:
    a. Internet
    b. Email
    c. Documents
    d. Graphics

3. describe the vulnerabilities that a computer system and/or network to which the organization may be exposed,
4. describe policies and associated controls to assist in safeguarding the organization,
5. describe and apply modern principles of physical, computer, network security controls,
6. and describe Intellectual Property, such as patents, copyrights, critical or confidential information from which an computer incident might arise.

Data Storage Fundamentals (If time permits): The student shall be able to

1. describe the basics of NTFS vs FAT32 vs. UNIX file systems and data storage

2. describe wide varieties of data storage devices and how they operate
3. describe how these devices contain evidence
4. capture critical system information from Windows 9X disks
5. capture critical system information from Windows 7 disks
6. capture critical system information from Linux disks
7. capture critical information from a network incident.

Recommended but not Required Text:

"Principles of Incident Response and Disaster Recovery"
by Michael E. Whitman and Herpert J. Mattrord
ISBN = 1-4188-3663-X

Reference Reading:

"Incident Response". By Kevin Mandia & Chris Prosise,
Publisher Osbourne/McGraw-Hill, ISBN 0-07-213182-9
FIRST Edition ONLY

Grading : Semester grades will be computed as follows:

Assignments:	
Homework (includes lab assignments)	30%
Reading and Research papers	15%
Portfolio	5%
Mid-Term Test	25%
Final Project	25%
	100 %

Grade Assignment : A= 90-100
B= 80-89
C= 70-79
D= 60-69
F= 59 and below

"e-Campus":

I will be using the e-campus system this semester.
You may find this at https://ecampus.wvu.edu
Be sure to run the "browser check" before you login and check your system for up to date software.

Grading Policy :

1. All Assignments are due ONLY on the "e-Campus" on or before the date and time due.

2. Some labs will discuss vulnerabilities in widely deployed computer systems. This is NOT an invitation to exploit those vulnerabilities. Responsible behavior and avoidance of all unethical behavior is expected. WVU's policy (and our own) on this is clear: you may not break into machines that are not your own. In addition to an F in the course and WVU proceedings under the Student Code of Conduct, legal proceedings and legal

penalties may be brought against you for such actions.

3. Homework joint work: Students are encouraged to discuss homework assignments but **must** submit their own individually prepared assignments. Jointly prepared and/or copied assignments **WILL** be severely penalized.

4. Reading and Research joint work is prohibited. No discussion with anyone until after work is turned in. Jointly prepared and/or copied assignments **WILL** be severely penalized

5. Other notes on academic dishonesty in addition to the above 3 and 4:
    - I consider it academic dishonesty if you share final assignments, work, solutions, etc with other students.
    - Changing variable names and/or output messages does not make it original work!
    - If ANYTHING, including code, is "reused," you must site the source (code source can be cited in the comments for that code or routine. This includes your own previous work!)
    - Allowing others to view your work by leaving permissions set incorrectly or leaving files on hard drives or other disks accessible by others will be considered academic dishonesty and will result in an F in the course.
    - If a student does discuss and share work with another, thinking that the person who is receiving that information will not copy it, both people will be held responsible for academic dishonesty if identical work is submitted and both claim that it is original.
6. Makeup Exams: No make-up exams (except by prior arrangement with the instructor.)

Assignments:

1. Assignments will be made via e-campus.
2. It may consist of reports, class presentations, assignments, and laboratory investigations.
3. We will be using the WV3C lab at 3102 Prete Bld several times during the semester. You will be REQUIRED to do your work there.
4. ALL ASSIGNMENTS will be submitted on e-campus. No paper copies or e-mail submissions will be accepted.
5. Each assignment will be worth approximately the same amount of credit unless otherwise noted.
6. Assignments are due at the time and date assigned.
7. No late HW or other assignments will be accepted.
8. Assignments and final project at the end of the semester may also require the use of computers and equipment that are located in 3102 Prete (USC.)
9. You must plan on using time ONLY WHEN WE ARE SCHEDULED in the lab to complete these assignments (investigations.)

Class Communications:

All class communications will be via ecampus.wvu.edu
Lecture notes and assignments will be posted here as well.

Class reading and research assignments:

1. The results of these assignments will be submitted on e-campus before time and date due.
2. These will require you to read on line and to find outside references.
3. The results will typically require a summary of the reading material in approximately 600 words or about a page or less.
4. Diagrams may be used as part of the page to illustrate your summary.
5. You may also choose to use instead, 10 to 15 PowerPoint slides instead.
6. Your final submission for each of these assignments should look professional and have good English form.

Attendance Policy: This class will be difficult to pass without attending class.

WVU Inclusivity Statement:

"The West Virginia University community is committed to creating and fostering a positive learning and working environment based on open communication, mutual respect, and inclusion. If you are a person with a disability and anticipate needing any type of accommodation in order to participate in this class, please advise me and make appropriate arrangements with Accessibility Services (293-6700). For more information on West Virginia University's Diversity, Equity, and Inclusion initiatives, please see http://diversity.wvu.edu."

Class Cancellations: If a class is cancelled, notice will be posted on e-campus and mailed to your MIX ACCOUNT. Generally, assignments will be posted as well to replace the missed lecture time. Students are responsible for getting cancellation information and assignments. In all emergency situations, however, we rely on individuals to make the best decision for themselves about their safety.

Class distractions: Cell phones, pagers, etc must be turned OFF during class. These are distracting for all.

Laptops and pads in Class: You may use your laptop in class provided that you are using it to take notes or to view e-campus pages for class notes.

E-mail, IM, general surfing and game playing are forbidden during class !!

Course Schedule **[DRAFT]**

TOPICS	Approx. # of lectures
1) Overview of the Law and Ethics	[4 weeks]
a) Preparation for Computer Investigation	
b) The Legal Process, justice system and how it relates to digital forensics and digital evidence.	

i) basics of the legal system and the differences between the civil and criminal processes
ii) discuss ethical (as well as legal issues) such as software piracy, reverse engineering, import/export rules, music sharing, etc and its impacts on a company's financial bottom line,
iii) discuss Intellectual property, patents, copyright, piracy, reverse engineering, import/export rules

c) CF Definitions

d) basic knowledge of the Bill of Rights and constitutional law
i) how it applies to computer and network search and seizure,
ii) discuss the 4th Amendment to the US Constitution and
e) statutes such as the ECPA and the legal requirements for obtaining electronic information
i) Computer Fraud and Abuse Act (1986) and amendment
ii) West Virginia state guidelines
iii) US federal guidelines, and International guidelines
iv) Industrial computer and network policies
f) USA Patriot Act of 2001
g) the rules and issues relating to the admissibility of evidence, both constitutional and statutory, to include search and seizure, chain of custody, and suppression; highlight the differences between civil and criminal situations and employer/employee issues
i) apply the rules of evidence as they relate to an electronic crime scene and to obtaining computer evidence. (i.e. recognize what can and can NOT be seized at an electronic crime scene.)
ii) and discuss the methods of ensuring the chain of custody of evidence.

2) Recognizing the signs of an incident [1 week]
a) Non-liturgical forensics exam
b) Investigating Windows 2000
c) Investigating Windows XP
d) Password Access

3) System Vulnerabilities :
a) Understanding TCP/IP [1 week]
i) Protocols
ii) OSI std
iii) TCP/IP addressing
iv) The IP header
v) IP fragmentation
vi) Routers, switches, hubs, intrusion detection systems
vii) E-mail, instant messaging
viii) etc
b) WINDOWS 2000/XP system and network vulnerabilities [1week]
c) Policies and Controls for safeguarding the organization [1week]
i) Policies
ii) Login banners

iii) Logging
d) Investigating a live system with multiple users! [2 weeks]

2) Data Forensics Definitions and Procedures [4 weeks]
a) file systems and data storage NTFS vs. FAT32
how these devices contain evidence
b) varieties of data storage devices and how they operate
c) how these devices contain evidence
d) capture of critical system information from Windows 9X
e) Sources of information for stand-alone machine investigation.
(a) Temp files, history files, trash bins,
(b) Slack and Swap Areas
f) contextual knowledge of the crime

4) Linux Systems [1 week]
a) File Formats
b) Multi-user system

5) Possible Guest lectures by NW3C
a) Cell phones and Towers
b) Basic Files systems i.e. FAT
c) E-mail and file formats
d) IExplorer and Firefox artifacts

Other Policies:

1. From time to time, we may discuss with student participation, interesting papers, cases, tools, and vulnerabilities in widely deployed computer systems. This is not intended as an invitation to exploit those vulnerabilities. It is important that we be able to discuss real-world experience candidly; students are expected to behave responsibly. The tools and systems used in this class are exclusively meant for student experimentation and project work connected with the class. They are not to be used outside of that environment, and certainly not to impede or disturb the work of others. Responsible behavior and avoidance of all unethical behavior is expected. WVU's policy (and our policy) on this is clear: you may not break into machines that are not your own; you may not attempt to attack or subvert any system security. Breaking into other people's systems is inappropriate as well as illegal! The existence of a security hole is no excuse. A Grade of F and dismissal from the class at a minimum is automatic for such behavior. WVU penalties will then be assessed as well. In addition, there may be criminal proceedings that can be brought against you for such actions. Unauthorized access, use, modification, destruction, or disclosure of any computer system or computer network or any computer software, program, documentation, or data contained in such computer system or computer network is computer crime and will be prosecuted as such.

It should not be necessary to say that you ARE expected to abide by all WVU Policies at a minimum.

2. If you expect to work in this field in the future, for many branches of government as well as many companies, you will be expected to be capable of passing a background check. Many government and private companies may require a security clearance as well.

3. Drug Policy: See next page-

Student Name ______________________

Last, First MI

This Computer Forensics class requires that all students in the class acknowledge that they have been informed about the Program's drug policy. This policy supports a drug-free lifestyle and recognizes that internship sites and prospective law enforcement agencies and companies wishing to employ our graduates may require drug testing and polygraph assessment as a condition of internship or employment. Each student must recognize this possibility as they enter the forensics field. We, therefore, require each student to read and sign the following statement acknowledging that this information has been presented to him or her.

Computer Forensics PROGRAM DRUG POLICY

The Computer Forensics program encourages all students to maintain a **totally** drug-free lifestyle to insure they will not be denied access to internship sites or employment especially with various security and law enforcement agencies as the result of any past or present use of illegal drugs.

A number of security and law enforcement agencies will require prospective employees from our program to sign a statement affirming that they have never used these substances and will require them to take a polygraph related to their statements.

Some agencies providing internships will also require our Computer Forensic students to take a polygraph related to their drug history. Students must recognize they can be denied access to some internship sites and employment at security and law enforcement agencies if they fail any of the checks or the polygraph questions related to the use of illegal drugs.

I agree that I have been informed of the above.

____

Signature of Student Date

____

Signature representative of the
WVU Computer Forensics Program

CpE-435: Computer Forensics

Portfolio Guidelines

last update 8/19/2012 by rsn

Portfolios are used as an assessment tool. The learning objectives for the course are specific and are enumerated in the course syllabus. The portfolio then serves to document your progress toward the learning objectives of this course. You will turn in your portfolio at the final exam. It is best if you collect your material as the semester progresses.

THE PORTFOLIO

It is important to include all of the following:

1. **Title page**: Should include name and class.

2. **Cover Letter** “About the author” and “What my portfolio shows about my progress in this class (written at the end of the semester, but put at the beginning of the portfolio). The cover letter summarizes the evidence of a student’s learning and progress.

3. **Self-Evaluation:** Your overall class self-evaluation, written at the end of the semester. You should include in this, a well-supported argument for the course grade you think you deserve.

4. **Table of Contents with**
   - Numbered pages.
   - Index tabs.

5. **Entries –**

   Required
   - Using the learning objectives in the syllabus as an organizational guide, you should provide a complete and well organized record of the class.
   - This material should be organized as a summary of the class so that you can use it in the future as a reference since you may now be the expert at your new company.
   - Appendix:
     1. A list of the software in your ‘Incident Response Kit.”
     2. CDs or DVD’s that include your “incident Response Kit.”

   Optional Appendixes:

   These items allow the folder to represent the uniqueness of each student.
   - You may choose to include “best work” or your “favorite pieces of work.”
   - You may include also a piece of work which gave trouble or one that was less successful, and give reasons why.
   - **Reflections** can appear at different stages in the learning
     1. For each item - a brief rationale for choosing the item should be included. This can relate to students’ performance, to their feelings regarding their progress and/or themselves as learners. Students can choose to reflect upon some or all of the following:
     2. What did you learn from it?
     3. What did you do well?
     4. Why did you choose this item?
     5. What do you want to improve in the item?
     6. What were the problem areas?
     7. How did I perform on this?

REMEMBER: Do NOT put extra items into the portfolio just for volume. It is **quality** that counts, not quantity, and the main point of portfolio assessment is the thoughtful selection **of evidence of learning.**