American Public University System

The Ultimate Advantage is an Educated Mind

School: Science and Technology
Course Number: ISSC 459
Course Name: Digital Forensics: Hard Disk and Operating System
Credit Hours: 3
Length of Course: 8 Weeks
Prerequisite: None

Table of Contents

Instructor Information	Evaluation Procedures
Course Description	Grading Scale
Course Scope	Course Outline
Course Objectives	Policies
Course Delivery Method	Academic Services
Course Resources	Selected Bibliography

Instructor Information

Course Description (Catalog)

This course is designed to expose the student to the process of detecting attacks and collecting evidence in a forensically sound manner with the intent to report crime and prevent future attacks. Learners are introduced to advanced techniques in computer investigation and analysis with interest in generating potential legal evidence. The course provides a basic understanding of file systems, hard disks and digital media devices. Boot processes, Windows and Linux Forensics and application of password crackers.

Course Scope

This course provides a basic understanding of file systems, hard disks and digital media devices. Boot processes, basic and advanced features in the Windows forensic process. The application of password crackers is another area of emphasis in this course.

Course Objectives

The successful student will fulfill the following learning objectives:

1. Analyze file systems and hard disks
2. Examine various types of digital media
3. Utilize Application password crackers
4. Explain Windows, Linux, and Macintosh boot processes
5. Develop basic Windows forensics examination procedures
6. Prepare advanced Windows forensics examination procedures

Course Delivery Method

This is an eight-week course delivered in the APUS Educator; Distance learning will enable students to complete academic work in a flexible manner, completely online. Resources and access to an online learning management system will be made available to each student. **Online assignments are due by the last day of each week** and include Forum questions (accomplished in groups through a threaded Forum), online labs, and individual assignments (submitted for review by the Faculty Member). Assigned faculty will support the students throughout this eight-week course.

Course Resources

Required Course Textbooks

Computer Forensics: Investigating Hard Disks, File and Operating Systems. (2010). Published by: Cengage Learning. ISBN: 1-4354-8350-2 or 978-1-4354-8350-7

Additional Resources

Anson, S., & Bunting, S. (2007). *Mastering Windows network forensics and investigation* [electronic resource]. Retrieved from
http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=18160

Carvey, H. (2011). *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry* [electronic resource]. Retrieved from
http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=41894

Frietas, L. (2011). How to recover data of a Hard Drive for Forensic Investigation. Retrieved from http://blog.luisfreitas.pt/2011/06/22/how-to-recover-data-of-a-hard-drive-for-forensic-investigation/

Reuters. (2012). Aramco Says Cyber attack was Aimed at Production. Retrieved from
http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. Retrieved from
http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

Sammons, J. (2012). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics* [electronic resource]. Retrieved from
http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=44731

Wiles, J., Cardwell, K., & Reyes, A. (2007). *The best damn cybercrime and digital forensics book period* [electronic resource]. Retrieved from
http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=25452

Evaluation Procedures

The grading will be based on eight weekly assignments, eight weekly Forum postings, six weekly labs, an individual project paper with topic, outline, presentation, and a case study.

1. There will be **eight assignments (3% each) counting a total of 24% of the final grade**. The assignments will follow each of the major milestones of the course. These assignments will be problems or questions from the text. They are a combination of Lesson Reviews and Lesson Activities and/or Labs. They are selected to provide the student with information to understand the concepts discussed. Assignments should be prepared in Microsoft Word using the following file naming convention: ISSC459_Week#Assignment_First_Last.doc(x) (where the # is the week number, and first and last are your first and last names resp.) and submit the file in this assignments' area and uploaded into the student folder by the due

STUDENT WARNING: This course syllabus is from a previous semester archive and serves only as a preparatory reference. Please use this syllabus as a reference only until the professor opens the classroom and you have access to the updated course syllabus. Please do NOT purchase any books or start any work based on this syllabus; this syllabus may NOT be the one that your individual instructor uses for a course that has not yet started. If you need to verify course textbooks, please refer to the online course description through your student portal. This syllabus is proprietary material of APUS.

date. Any necessary Visio diagrams should be incorporated within the Word document as part of the document.

2. There will be **eight weekly Forum postings you will need to respond to**. Answers should be 3-4 paragraphs with a **topic sentence** that **restates the question** and **supporting sentences** using the terms, concepts, and theories from the required readings. Each answer should be a **minimum of 400 words** (about 8 good sentences). You may **attack**, **support** or **supplement** other students' answers using the terms, concepts and theories from the required readings. All responses should be a **courteous paragraph** that contains a **topic sentence** with good **supporting sentences**. You may respond multiple times with a continuous discussion with points and counter points. The key requirement is to express your idea and then **support your position** using the terms, concepts and theories from the required readings to demonstrate to me that you understand the material. The Forum postings will count as 20% (2.5% for each discussion posting) of the final grade.

3. There will be **a project paper (10%)** with **topic selection (2%)**, **outline (4%)**, and **presentation (6%)**, and a **case study (10%)** throughout the session, counting as 32% total of the final grade. Please practice using the same file naming convention established in this class for each of these files.

4. There will be **labs (4% each) a total 24% of the final grade**. The labs will be online hands-on labs using the necessary tools required in digital forensics.

All assignments, Forum question responses, and the labs are due by 11:55 Eastern Time Sunday of the week assigned.

Grade Instruments	Points Possible	% of Final Grade
Assignment (Weeks 1 to 8) (3 points each)	24	24%
Forum Posts (Weeks 1 to 8) (2.5 points each)	20	20%
Labs (Weeks 2 to 7) (4 points each)	24	24%
Project Paper Topic (Week 2)	2	2%
Project Paper Outline (Week 4)	4	4%
Project Paper Presentation (Week 6)	6	6%
Project Paper Final Product (Week 7)	10	10%
Case Study (Week 8)	10	10%
TOTAL	**100 Points**	**100%**

Project Paper (Topic, Outline, PowerPoint Presentation, and Paper) Topics:
Week 2: Topic selection due
Week 4: Outline due
Week 6: PowerPoint Presentation due
Week 7: Paper due

Topics: Acceptable topics unless I have already approved one:

- Corporate Forensics
- The Boot Process
- Software Piracy
- Password Crackers
- Digital Media Devices
- File systems
- Windows Architecture Vs. Mac Architecture
- Intellectual Property

Details of Project Paper (10%): You must include at least ten references.
Prepare a 10-15 page paper in Microsoft Word (counts as 10% of the final grade) in APA format (see writing expectations in the Policies section) (350 words per page). The paper should be between 3500 to 5300 words excluding the title page content and the references page content. At a minimum include the following:

- o Detailed description of the area researched
- o Technology involved in the area
- o Future trends in the area
- o Example companies involved in the area
- o Regulatory issues surrounding the area
- o Global implications for the area
- o References (minimum of 10)

You may use resources from the APUS Online Library, any library, government library, or any peer-reviewed reference (Wikipedia and any other publicly-reviewed source is not accepted). The paper must be at least 10 pages double-spaced, 1" margin all around, black 12 point font (Times New Roman or Arial) with correct citations of all utilized references/sources, (pictures, graphics, etc... are extra - allowed but extra for the minimum page count). The title page and references are also required but don't count in the minimum page count. A minimum of 10 references are required.

The paper will be subjected to checking against plagiarism. The paper must follow acceptable originality criteria (no more than 15% max total, and 2% per individual source match are allowed).

Save the file using the following file naming convention: ISSC459_Project_First_Last.doc(x) (where first and last are your first and last names resp.) and submit the file in this assignment area

Here are the originality report requirements:

1. The originality report must be less than 15% match

2. No single source shall be above 2%
3. You must submit the originality report with your paper to your AMU classroom

If you don't follow these three requirement instructions you will get a 0 for your project paper assignment. I will give you the chance to rework your papers until an acceptable level of match is achieved.

At the end of the class, if you have not submitted your paper to turnitin.com, I will submit it anyways even after you'd get a 0, to see the level of plagiarism found, if any. If turnitin.com matches more than 40% you will be subject to academic reporting.

Case Study (10%): You are hired by JLA Enterprise to conduct a Digital Media Investigation after it was discovered the Chief Financial Officer was embezzling money from the company's accounts. Your job is to review all digital media involved in the case to determine if a crime has been committed. Here are some things to consider when explaining what happened during the investigation:

- Who was involved in the embezzlement?
- How much money was taken?
- How can you prove the individual took the money?
- What programs were used to embezzle the money?
- When did they start embezzling the money?
- Were they working with anyone else?

Your submission should be about 3 to 5 pages (not including the title page and the references page) long in APA format with proper citations and references if you are using them. It will be subjected to checking against plagiarism. The final product must follow acceptable originality criteria (no more than 15% max total, and 2% per individual source match are allowed).

Save the file using the following file naming convention: ISSC459_CaseStudy_First_Last.doc(x) (where first and last are your first and last names resp.) and submit the file in this assignment area

8 – Week Course Outline

Please see the Student Handbook to reference the University's grading scale.

Week	Topic	Learning Objectives	Readings	Assignment
1	Understanding File Systems and Hard Disks	**CO-1**: Analyze file systems and hard disks	Lesson 1 Ch1 Presentation	Week 1 Forum* Week 1 Assignment*
2	Understanding Digital Media Devices	**CO-2**: Examine various types of digital media	Lesson 2 Ch2 Presentation	Week 2 Forum* Week 2 Assignment* Week 2 Lab1* Week 2 Project Paper Topic*
3	Application Password Crackers	**CO-3**: Utilize Application password crackers	Lesson 3 Ch7 Presentation	Week 3 Forum* Week 3 Assignment* Week 3 Lab2*
4	Windows Boot Process	**CO-4**: Explain Windows, Linux, and Macintosh boot processes	Lesson 4 Ch3 Presentation	Week 4 Forum* Week 4 Assignment* Week 4 Lab3* Week 4 Project Paper Outline*
5	Linux Boot Process	**CO-4**: Explain Windows, Linux, and Macintosh boot processes	Lesson 5 Ch3 Presentation	Week 5 Forum* Week 5 Assignment* Week 5 Lab4*
6	Macintosh Boot Process	**CO-4**: Explain Windows, Linux, and Macintosh boot processes	Lesson 6 Ch3 Presentation	Week 6 Forum* Week 6 Assignment* Week 6 Lab5* Project PowerPoint Presentation*
7	Windows Forensics I	**CO-5**: Develop basic Windows forensics examination procedures	Lesson 7 Ch4 Presentation	Week 7 Forum* Week 7 Assignment* Week 7 Lab6* Project Paper with Acceptable Originality Report*
8	Windows Forensics II	**CO-6**: Prepare advanced Windows forensics examination procedures	Lesson 8 Ch5 Presentation	Week 8 Forum* Week 8 Assignment* Case Study* (plus Originality Report)

Policies

Please see the Student Handbook to reference all University policies. Quick links to frequently asked question about policies are listed below.

> Drop/Withdrawal Policy
> Plagiarism Policy
> Extension Process and Policy
> Disability Accommodations

Writing Expectations

All written submissions should be submitted in a font and page set-up that is readable and neat. It is recommended that students try to adhere to a consistent format, which is described below.

- Typewritten in double-spaced format with a readable style and font and submitted inside the electronic classroom (unless classroom access is not possible and other arrangements have been approved by the professor).
- Arial 11 or 12-point font or Times New Roman styles.
- Page margins Top, Bottom, Left Side and Right Side = 1 inch, with reasonable accommodation being made for special situations and online submission variances.

Citation and Reference Style

Assignments completed in a narrative essay or composition format must follow APA guidelines. This course will require students to use the citation and reference style established by the American Psychological Association (APA), in which case students should follow the guidelines set forth in *Publication Manual of the American Psychological Association* (6th ed.). (2010). Washington, D.C.: American Psychological Association.

Late Assignments

Students are expected to submit classroom assignments by the posted due date and to complete the course according to the published class schedule. As adults, students, and working professionals I understand you must manage competing demands on your time. Should you need additional time to complete an assignment please contact me before the due date so we can discuss the situation and determine an acceptable resolution. Routine submission of late assignments is unacceptable and may result in points deducted from your final course grade. Assignments submitted late without a prearranged extension will be subject to a 10% late penalty. **No late assignments will be accepted after the last day of the course.**

Netiquette

Online universities promote the advancement of knowledge through positive and constructive debate – both inside and outside the classroom. Forums on the Internet, however, can occasionally degenerate into needless insults and "flaming." Such activity and the loss of good manners are not acceptable in a university setting – basic academic rules of good behavior and proper "Netiquette" must persist. Remember that you are in a place for the rewards and excitement of learning which does not include descent to personal attacks or student attempts to stifle the Forum of others.

- **Technology Limitations:** While you should feel free to explore the full-range of creative composition in your formal papers, keep e-mail layouts simple. The Sakai classroom may not fully support MIME or HTML encoded messages, which means that bold face, italics, underlining, and a variety of color-coding or other visual effects will not translate in your e-mail messages.
- **Humor Note:** Despite the best of intentions, jokes and especially satire can easily get lost or taken seriously. If you feel the need for humor, you may wish to add "emoticons" to help alert your readers: ;-), :), ☺

Disclaimer Statement
Course content may vary from the outline to meet the needs of this particular group.

Online Library

The Online Library is available to enrolled students and faculty from inside the electronic campus. This is your starting point for access to online books, subscription periodicals, and Web resources that are designed to support your classes and generally not available through search engines on the open Web. In addition, the Online Library provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to **librarian@apus.edu**.

- *Charles Town Library and Inter Library Loan:* The University maintains a special library with a limited number of supporting volumes, collection of our professors' publication, and services to search and borrow research books and articles from other libraries.
- *Electronic Books:* You can use the online library to uncover and download over 50,000 titles, which have been scanned and made available in electronic format.
- *Electronic Journals:* The University provides access to over 12,000 journals, which are available in electronic form and only through limited subscription services.

- *Tutor.*com: AMU and APU Civilian & Coast Guard students are eligible for 10 free hours of tutoring provided by APUS. Tutor.com connects you with a professional tutor online 24/7 to provide help with assignments, studying, test prep, resume writing, and more. Tutor.com is tutoring the way it was meant to be. You get expert tutoring whenever you need help, and you work one-to-one with your tutor in your online classroom on your specific problem until it is done.

Request a Library Guide for your course (http://apus.libguides.com/index.php)
The AMU/APU Library Guides provide access to collections of trusted sites on the Open Web and licensed resources on the Deep Web. The following are specially tailored for academic research at APUS:

- Program Portals contain topical and methodological resources to help launch general research in the degree program. To locate, search by department name, or navigate by school.
- Course Lib-Guides narrow the focus to relevant resources for the corresponding course. To locate, search by class code (e.g., SOCI111), or class name.

If a guide you need is not available yet, please email the APUS Library: librarian@apus.edu.

Turnitin.com

Faculty may require assignments be submitted to Turnitin.com. Turnitin.com will analyze a paper and report instances of potential plagiarism for the student to edit before submitting it for a grade. In some cases professors may require students to use Turnitin.com. Typically the course professor will establish a Turnitin.com access code for his/her classes. If the code has not been established, those who wish to use Turnitin.com may ask their professor to establish the code.

Special Note to Faculty: Please be <u>certain</u> to provide accurate directions and to set up the functionality appropriately.

Selected Bibliography

Computer Forensics: Investigating Hard Disks, File and Operating Systems. (2010). Published by: Cengage Learning. ISBN: 1-4354-8350-2 or 978-1-4354-8350-7

Anson, S., & Bunting, S. (2007). *Mastering Windows network forensics and investigation* [electronic resource]. Retrieved from http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=18160

Carvey, H. (2011). *Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry* [electronic resource]. Retrieved from http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=41894

Frietas, L. (2011). How to recover data of a Hard Drive for Forensic Investigation. Retrieved from http://blog.luisfreitas.pt/2011/06/22/how-to-recover-data-of-a-hard-drive-for-forensic-investigation/

Reuters. (2012). Aramco Says Cyber attack was Aimed at Production. Retrieved from http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html?_r=0

Rowlingson, R. (2004). A Ten Step Process for Forensic Readiness. Retrieved from http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf

Sammons, J. (2012). *The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics* [electronic resource]. Retrieved from http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=44731

Wiles, J., Cardwell, K., & Reyes, A. (2007). *The best damn cybercrime and digital forensics book period* [electronic resource]. Retrieved from http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=25452