

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.

American Public University System

The Ultimate Advantage is an Educated Mind

School of Science and Technology
Department of Information Technology
ISSC457: Digital Forensics: Investigating Network Intrusions and Cybercrime Security
3 Credit Hours
8 Week Course
Prerequisite(s): None

Table of Contents

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

Instructor Information

Instructor:
Email:
Office Hours:

Course Description (Catalog)

[TOC](#)

The increase in the use of the Internet and ensuing growth in cybercrime have given rise to the field of digital forensics. Students will be introduced to advanced techniques in computer investigation and analysis with interest in generating potential legal evidence. This course examines computer related crime and abuse cases in order to gather all necessary information and evidence to support prosecution in a court of law. Collection of evidence, investigating information hiding, and intrusion response techniques will be explored. This course will examine network intrusions, network traffic, web attacks, DoS attacks and corporate espionage. Current literature will be examined on such topics.

Course Scope

[TOC](#)

This course covers network forensics and investigating log files, understanding and recognizing the different types of Web attacks. Learning different router attacks as well as listing the steps used in the investigation of router attacks. Gaining a better understanding of investigating an Internet crime and tracking e-mails and investigating e-mail crime. Understanding the investigation process related to corporate espionage. Investigating sexual harassment incidents and child pornography.

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.

Course Objectives

[TOC](#)

The successful student will fulfill the following learning objectives:

1. Gain an understanding of network forensics and investigation logs
2. Become familiar with web attacks such as cross-site scripting and SQL injection attacks
3. Discuss router forensics and the types of router attacks
4. Examine e-mail tracking techniques and e-mail crime
5. Explain and evaluate the process to prepare and conduct a computer investigation
6. Discuss the importance of search warrants and chain of custody in a forensic investigation
7. Discuss corporate espionage and prevention techniques
8. Gain an understanding of the types of computer related crimes such as sexual harassment and child pornography and the laws

Course Delivery Method

[TOC](#)

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.

Resources

[TOC](#)

Required Book

Computer Forensics: Investigating Network Intrusions and Cybercrime. (2010). Published by: Cengage Learning. ISBN: 1-4354-8352-9 or 978-1-4354-8352-1

Cyber Safety. (2010). Published by: Cengage Learning. ISBN: 1-4354-8371-5 or 978-1-4354-8371-2

Web-based Readings – if these links are no longer available, conduct a web search on the topics

FBI. (2012). Computer Intrusions. Retrieved from <http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions>

Gragido, W., & Pirc, J. (2011). *Cyber Crime and Espionage: An Analysis of Subversive Multi-Vector Threats* [electronic resource]. Retrieved from <http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=41844>

Kerr, O. (2005). Search Warrants in an ERA of Digital Evidence. Retrieved from <http://www.olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf>

Mehan, J. (2008). *Cyberwar, cyberterror, cybercrime* [electronic resource]. Retrieved from <http://site.ebrary.com/lib/apus/Doc?id=10438090>

Newsbytes.ph (2012). 80% of cyber attacks in 2012 came from legit sites. Retrieved from <http://manilastandardtoday.com/2012/12/08/80-of-cyber-attacks-in-2012-came-from-legit-sites/>

Software Requirements

1. Microsoft Office (MS Word, MS Excel, MS PowerPoint)
2. Adobe Acrobat Reader ([Click here for free download](#))

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.

Evaluation Procedures

[TOC](#)

The grading will be based on eight weekly assignments, eight weekly Forum postings, six weekly labs, an individual project paper with topic, outline, and 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: ISSC457_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 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

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.

Week 7: Paper due

Topics: Acceptable topics unless I have already approved one:

- Corporate Espionage
- Computer Crimes
- Impacts of Computer Technology on Law Enforcement
- Computer Forensics
- Cyberbullying
- Software Piracy
- Digital Crime and Digital Terrorism
- Computer Hacking
- Cyber Terrorism
- How to Investigate Cybercrime
- Network Security

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:

- Detailed description of the area researched
- Technology involved in the area
- Future trends in the area
- Example companies involved in the area
- Regulatory issues surrounding the area
- Global implications for the area
- 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: ISSC457_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.

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.

Case Study (10%): You are hired by JLA Enterprise to conduct a Forensic Examination after a network intrusion occurs at their corporate office. Your job is to determine the source of the network intrusion and provide as much information regarding the attack as possible. Here are some things to consider when explaining what happened during the network intrusion:

- What time did the attack happen?
- How did the hacker get into the network?
- What computers were compromised?
- What computers were accessed?
- What data was extracted from the network?
- What type of attack was conducted?
- How long did the attacker have access to the network?
- Is there any persistence on the network for future attacks?

You are asked to conduct a forensics examination of the network and provide a forensic report explaining what happened during the attack and what corporate data was compromised. The report should cover the above information, as well as create a timeline that shows the attack from the initial stages of the attack to when the data was extracted from the network.

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: ISSC457_CaseStudy_First_Last.doc(x) (where first and last are your first and last names resp.) and submit the file in this assignment area

Grading Scale	TOC
----------------------	---------------------

Please see the [student handbook](#) to reference the University's [grading scale](#).

Course Outline	TOC
-----------------------	---------------------

Week	Topic	Learning Objectives	Reading(s)	Assignment(s) (*Graded)
1	Network Forensics and Investigating Logs	CO1	Lesson 1 Ch1 Presentation	Week 1 Forum* Week 1 Assignment*
2	Investigating Web Attacks	CO2	Lesson 2 Ch3 Presentation	Week 2 Forum* Week 2 Assignment* Week 2 Lab1* Week 2 Project Paper Topic*
3	Router Forensics	CO3	Lesson 3 Ch4 Presentation	Week 3 Forum* Week 3 Assignment* Week 3 Lab2*
4	Tracking E-Mails and Investigating E-Mail Crime	CO4	Lesson 4 Ch7 Presentation	Week 4 Forum* Week 4 Assignment* Week 4 Lab3* Week 4 Project Paper Outline*

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.

5	Investigating Internet Crime	CO5	Lesson 5 Ch6 Presentation	Week 5 Forum* Week 5 Assignment* Week 5 Lab4*
6	Search Warrants and Chain of Custody	CO6	Lesson 6 Wk6 Presentation	Week 6 Forum* Week 6 Assignment* Week 6 Lab5* Project PowerPoint Presentation *
7	Investigating Corporate Espionage	CO7	Lesson 7 Ch8 Presentation	Week 7 Forum* Week 7 Assignment* Week 7 Lab6* Project Paper with Acceptable Originality Report*
8	Investigating Sexual Harassment Incidents/Child Pornography	CO8	Lesson 8 Ch10/11 Presentation	Week 8 Forum* Week 8 Assignment* Case Study* (plus Originality Report)

Policies

[TOC](#)

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](#)

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.

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.

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.**

Academic Services

[TOC](#)

ONLINE LIBRARY RESEARCH CENTER & LEARNING RESOURCES

The Online Library Resource Center 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 Center provides access to special learning resources, which the University has contracted to assist with your studies. Questions can be directed to orc@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.
- **Turnitin.com:** Turnitin.com is a tool to improve student research skills that also detect plagiarism. Turnitin.com provides resources on developing topics and assignments that encourage and guide students in producing papers that are intellectually honest, original in thought, and clear in expression. This tool helps ensure a culture of adherence to the University's standards for intellectual honesty. Turnitin.com also reviews students' papers for matches with Internet materials and with thousands of student papers in its database, and returns an Originality Report to instructors and/or students.

Selected Bibliography

[TOC](#)

Computer Forensics: Investigating Network Intrusions and Cybercrime. (2010). Published by: Cengage Learning. ISBN: 1-4354-8352-9 or 978-1-4354-8352-1

Cyber Safety. (2010). Published by: Cengage Learning. ISBN: 1-4354-8371-5 or 978-1-4354-8371-2

FBI. (2012). Computer Intrusions. Retrieved from <http://www.fbi.gov/about-us/investigate/cyber/computer-intrusions>

Gragido, W., & Pirc, J. (2011). *Cyber Crime and Espionage: An Analysis of Subversive Multi-Vector Threats* [electronic resource]. Retrieved from <http://library.books24x7.com.ezproxy1.apus.edu/toc.asp?bookid=41844>

Kerr, O. (2005). Search Warrants in an ERA of Digital Evidence. Retrieved from <http://www.olemiss.edu/depts/ncjrl/pdf/02-KERR.pdf>

Mehan, J. (2008). *Cyberwar, cyberterror, cybercrime* [electronic resource]. Retrieved from <http://site.ebrary.com/lib/apus/Doc?id=10438090>

Newsbytes.ph (2012). 80% of cyber attacks in 2012 came from legit sites. Retrieved from <http://manilastandardtoday.com/2012/12/08/80-of-cyber-attacks-in-2012-came-from-legit-sites/>

Appendix A – Grading Rubric

All written assignments will be assessed according to this rubric. Note that a score of 0 may be assigned in any category where your work does not meet the criteria for the beginning level.

APUS Assignment Rubric Undergraduate Level 300-400	EXEMPLARY LEVEL 4	ACCOMPLISHED LEVEL 3	DEVELOPING LEVEL 2	BEGINNING LEVEL 1	TOTAL POINTS
FOCUS/THESIS	Student exhibits a defined and clear understanding of the assignment. Thesis is clearly defined and well-constructed to help guide the reader throughout the assignment. Student builds upon the thesis of the assignment with well-documented and exceptional supporting facts, figures, and/or statements.	Establishes a good comprehension of topic and in the building of the thesis. Student demonstrates an effective presentation of thesis, with most support statements helping to support the key focus of assignment.	Student exhibits a basic understanding of the intended assignment, but the thesis is not fully supported throughout the assignment. While thesis helps to guide the development of the assignment, the reader may have some difficulty in seeing linkages between thoughts. While student has included a few supporting facts and statements, this has limited the quality of the assignment.	Exhibits a limited understanding of the assignment. Reader is unable to follow the logic used for the thesis and development of key themes. Introduction of thesis is not clearly evident, and reader must look deeper to discover the focus of the writer. Student's writing is weak in the inclusion of supporting facts or statements.	10
CONTENT/SUBJECT KNOWLEDGE	Student demonstrates proficient command of the subject matter in the assignment. Assignment shows an impressive level of depth of student's ability to relate course content to practical examples and applications. Student provides comprehensive analysis of details, facts, and concepts in a logical sequence.	Student exhibits above average usage of subject matter in assignment. Student provides above average ability in relating course content in examples given. Details and facts presented provide an adequate presentation of student's current level of subject matter knowledge.	The assignment reveals that the student has a general, fundamental understanding of the Resource. Whereas, there are areas of some concern in the linkages provided between facts and supporting statements. Student generally explains concepts, but only meets the minimum requirements in this area.	Student tries to explain some concepts, but overlooks critical details. Assignment appears vague or incomplete in various segments. Student presents concepts in isolation, and does not perceive to have a logical sequencing of ideas.	20

CRITICAL THINKING SKILLS	Student demonstrates a higher-level of critical thinking necessary for 300-400 level work. Learner provides a strategic approach in presenting examples of problem solving or critical thinking, while drawing logical conclusions which are not immediately obvious. Student provides well-supported ideas and reflection with a variety of current and/or world views in the assignment. Student presents a genuine intellectual development of ideas throughout assignment.	Student exhibits a good command of critical thinking skills in the presentation of material and supporting statements. Assignment demonstrates the student's above average use of relating concepts by using a variety of factors. Overall, student provides adequate conclusions, with 2 or fewer errors.	Student takes a common, conventional approach in guiding the reader through various linkages and connections presented in assignment. However, student presents a limited perspective on key concepts throughout assignment. Student appears to have problems applying information in a problem-solving manner.	Student demonstrates beginning understanding of key concepts, but overlooks critical details. Learner is unable to apply information in a problem-solving fashion. Student presents confusing statements and facts in assignment. No evidence or little semblance of critical thinking skills.	20
ORGANIZATION OF IDEAS/FORMAT	Student thoroughly understands and excels in explaining all major points. An original, unique, and/or imaginative approach to overall ideas, concepts, and findings is presented. Overall format of assignment includes an appropriate introduction (or abstract), well- developed paragraphs, and conclusion. Finished assignment demonstrates student's ability to plan and organize research in a logical sequence. Student uses at least of 5-7 references in assignment.	Student explains the majority of points and concepts in the assignment. Learner demonstrates a good skill level in formatting and organizing material in assignment. Student presents an above average level of preparedness, with a few formatting errors. Assignment contains less than 5 resources.	Learner applies some points and concepts incorrectly. Student uses a variety of formatting styles, with some inconsistencies throughout the paper. Assignment does not have a continuous pattern of logical sequencing. Student uses less than 3 sources or references.	Assignment reveals formatting errors and a lack of organization. Student presents an incomplete attempt to provide linkages or explanation of key terms. The lack of appropriate references or source materials demonstrates the student's need for additional help or training in this area. Student needs to review and revise the assignment.	20
WRITING CONVENTIONS (GRAMMAR & MECHANICS)	Student demonstrates an excellent command of grammar, as well as presents research in a clear and concise writing style. Presents a thorough, extensive	Student provides an effective display of good writing and grammar. Assignment reflects student's ability to select appropriate word usage	Assignment reflects basic writing and grammar, but more than 5 errors. Key terms and concepts are somewhat vague and not completely explained by	Topics, concepts, and ideas are not coherently discussed or expressed in assignments. Student's writing style is weak and needs	20

	understanding of word usage. Student excels in the selection and development of a well-planned research assignment. Assignment is error-free and reflects student's ability to prepare a high-quality academic assignment.	and present an above average presentation of a given topic or issue. Assignment appears to be well written with no more than 3-5 errors. Student provides a final written product that covers the above-minimal requirements.	student. Student uses a basic vocabulary in assignment. Student's writing ability is average, but demonstrates a basic understanding of the subject matter.	improvement, along with numerous proofreading errors. Assignment lacks clarity, consistency, and correctness. Student needs to review and revise assignment.	
USE OF COMPUTER TECHNOLOGY/ APPLICATIONS	Student provides a high-caliber, formatted assignment. Learner exhibits excellent use of computer technology in the development of assignment. Quality and appropriateness of stated references demonstrate the student's ability to use technology to conduct applicable research. Given assignment includes appropriate word processing, spreadsheet and/or other computer applications as part of the final product.	Assignment presents an above-average use of formatting skills, with less than 3 errors. Students has a good command of computer applications to format information and/or figures in an appropriate format. Student uses at least two types of computer applications to produce a quality assignment.	Student demonstrates a basic knowledge of computer applications. Appearance of final assignment demonstrates the student's limited ability to format and present data. Resources used in assignment are limited. Student may need to obtain further help in the use of computer applications and Internet research.	Student needs to develop better formatting skills. The student may need to take additional training or obtain help from the Educator Help Desk while preparing an assignment. Research and resources presented in the assignment are limited. Student needs to expand research scope. The number of formatting errors is not acceptable.	10
TOTAL POINTS					100