MIS 5216 – Organizational Forensic
Fall 2019

Instructor

Paul Warner
Email:
tuk55116@temple.edu
paul.warner@temple.edu
Telephone: 718-450-7171 Use Text Only
e-profile: *http://community.mis.temple.edu/lbrandolph/*
Office hours: by appointment

Class Location and Time

Online
WebEx: When it's time, 6:45PM Tuesday Evenings
WebEx: Access code: 648 637 290
1-855-244-8681 Call-in toll-free number (US/Canada)
1-650-479-3207 Call-in toll number (US/Canada)
Time: Tuesday 6:45pm – 8:00pm Eastern Daylight Time
Class blog: http://community.mis.temple.edu/mis5170sec002sec702sp2018/

Course Description

The focus of the course is on gaining a broad understanding of the field of Computer forensic, now most commonly called "digital forensics." Digital forensics is based on the investigation of digital data to gather evidence relating to criminal or other legal incidents and events. We will examine how technology and law interact to form digital forensic. Through the lecture and hand-on exercises student will learn phase of incident response, processing a crime/incident scene and gathering evidence, performing forensics analysis and conducting forensics investigation. Digital forensics experts and investigators may also be called to testify in court about their findings.

In an organization it's more than just computer forensics specialists and searching hard drives for hidden files or recover deleted files. Internet activity, email, shared network storage, cloud services, social media, cellular devices, and cameras. This course helps students understand how to respond to computer incidents. Legal issues involved in responding to computer attack are explored, including employee monitoring, working with law enforcement and handling evidence.

Course Objectives

1. Gain an overview of the nature of digital forensics
2. Learn the concepts of how digital forensics is completed and the steps/stages
3. Demonstrate the ability to identify, size, catalog, store, search, secure and process digital evidence.
4. Develop an understanding to process a crime and incident scene
5. Identify, describe, implement and test various acquisitions methods
6. Develop an understanding of how forensics is effected by company policies, laws and ethics
7. Develop an understanding of Legal Holds, E-Discovery and Reasonable Search
8. Identify various key components of a forensics toolkit, which includes a digital forensics workstation, and a suite of forensics investigative software.

9. Demonstrate the ability to validate and test various tools used in digital forensics and information gathering
10. Gain experience working as part of team, developing and delivering a professional presentation on after a forensic case assignment

Required Text and Readings

Guide To computer Forensics and Investigations Sixth Edition: Bill Nelson Amelia Phillips and Chris Steuart. ISBN: 978-1-337-568974-4

Course Grade Components

Component	Weight	Notes
Quizzes	5%	End of Chapter Quizzes
Exam #1	10%	Non-cumulative - See Exams Section
Exam #2	20%	Non-cumulative - See Exams Section
Labs	30%	Hands-On answering Questions
Final Project	20%	Large lab, Team Presentation, Team 360 Feedback
Assignments	10%	Blogs, In the News and Case Studies
Participation/Discussion Board	5%	Class participation

Exams

There will be two exams for this course. All exams will be comprised of multiple choose questions and answers. Check the schedule for dates. A missed exam can only be made up in the case of documented and verifiable extreme emergency situations. Exams are non-cumulative.

Labs…

Hardware Requirement

1. Computer with Internet access, speaker and a microphone
2. Virtual Machine Software (VMware Player or VMware Workstation)
3. Windows Live or Windows 8 or 10 operating system running in a Virtual environment (Can we boot off USB or CD?)
    a. Minimum 300 Gigs of HD
    b. Minimum of 4-8 Gigs of Physical Memory
    c. Microsoft Office 201x or higher
4. External USB Drive
5. Linux Live or Linux Virtual Machine (Kali or Ubuntu)
    a. Minimum of 60 Gigs of HD
    b. Minimum of 4 Gigs of Memory

Final Project…

There will be a final team project. Team membership will be appointed by the instructor/professor. The project will be a large lab exercise testing all the other lab components you have already completed, with a team presentation prepared for the C-Suite.

Assignments

Much of your learning will occur as you prepare for and participate in discussions about the course material. The assignments, analysis, and readings have been carefully chosen to bring the real world into class discussion while also illustrating fundamental concepts.
To encourage participation, a percentage of the course grade is earned through preparation before class, and participation during and between classes. Evaluation is based on a consistent demonstrated engagement with the process of learning. Assessment is based on what you contribute, not simply what you know.

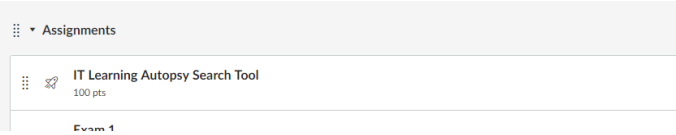
- Assignments between classes – To facilitate learning the course material, we will also discuss course material on the class blog in between classes. I ask students to post questions on the class blog based on the following week's topic, In the News and Case Studies. The questions should be related to the assigned readings, a topic to be discussed in class, or a relevant current event. Reading and commenting on these analyses will contribute to the quality of our in-class discussions. Every student is expected to contribute to the online class discussion minimum twice each week. Online contributions will be graded on both the quality of your submissions and the overall quantity. Four substantive posts a week will be considered a B.

Participation

Participation during class – We will typically start each discussion with "opening" questions about the assigned readings and analysis. I may ask for volunteers, or I may call on you. Students called on to answer should be able to summarize the key issues, opportunities, and challenges in the case study. All students should be prepared to answer these questions. The criteria for class participation includes attendance, punctuality, level of preparation, professionalism, answering questions, discussing readings, discussing case studies, contributing to group activities, and contributing to a positive learning environment.

Assignment Submissions

Your assignments will be submitted through Temple's Learning Management System - Canvas. Accessible via https://TUportal.temple.edu or direct https://canvas.temple.edu.
Sample view below…



Course Topic Outline

- Understanding Digital Forensic and Investigations
- Data acquisition, analysis, validation and reporting
- Processing Crime and Incident Scenes
- Current issues in Cyber law
- Computer ethics/Organizational Human Resources
- Building a partnership to respond: Working with counsel and law enforcement
- Operating system, Virtual Machines, Live Acquisition and Network Forensic
- Mobile device, social media, cloud, Graphic File recovery and forensics
- Using a diverse set of forensics tools
- Breach notification, media, PR and customer coverage

Weekly Cycle
As outlined above in the Participation section, much of your learning will occur as you prepare for and participate in discussions about the course content. To facilitate learning the course material, we will discuss course material on the class blog in between classes. Each week this discussion will follow this cycle:

- You: Read, view, etc. content for week (see course blog's Schedule menu)
- You: Post Questions/Comments (Thursday AM)
- You: Respond to questions and read & respond to other's answers (thru Monday 11:59 pm).
    - Note: 2 substantive posts a week will be considered a B
- Us: Class (Tuesday)

Late Assignment Policy
An assignment is considered late if it is turned in after the assignment deadlines stated in the schedule. No late assignments will be accepted. Plan ahead and backup your work. Equipment failure is not an acceptable reason for turning in an assignment late.
***** Remember, no late assignments will be accepted!**

Additional Grading Policies

Please note that it is against my policy to discuss grades on any test, graded assignment or any other direct component of your final grade via e-mail. If you would like to discuss how an assignment was graded, please see me during office hours. If you are not available during office hours, please make an appointment with me for another time.

Please note that two weeks after a grade has been posted, the grade will be considered "final." If you have an issue with a grade you are required to meet with me or make an appointment to meet with me during this two week period. After this two week period a grade will be considered "final" and is not up for discussion.

Disability Resources and Services

Any student who has a need for accommodation based on the impact of a documented disability, including special accommodations for access to technology resources and electronic instructional materials required for the course, should contact me privately to discuss the specific situation by the end of the second week of classes or as soon as practical. If you have not done so already, please contact Disability Resources and Services (DRS) at 215-204-1280 in 100 Ritter Annex to learn more about the resources available to you. I will work with DRS to coordinate reasonable accommodations for all students with documented disabilities.

Citation Guidelines

If you use text, figures, and data in reports that was created by others you must identify the source and clearly differentiate your work from the material that you are referencing. If you fail to do so you are plagiarizing. There are many different acceptable formats that you can use to cite the work of others. The format is not as important as the intent. You must clearly show the reader what is your work and what is a reference to someone else's work.

Academic Honesty

Source: Temple University Undergraduate Bulletin, 2012-2013. Available online at: http://www.temple.edu/bulletin/responsibilities_rights/responsibilities/responsibilities.shtm

> *Temple University believes strongly in academic honesty and integrity. Plagiarism and academic cheating are, therefore, prohibited. Essential to intellectual growth is the development of independent thought and a respect for the thoughts of others. The prohibition against plagiarism and cheating is intended to foster this independence and respect.*
>
> *Plagiarism is the unacknowledged use of another person's labor, another person's ideas, another person's words, another person's assistance. Normally, all work done for courses — papers, examinations, homework exercises, laboratory reports, oral presentations — is expected to be the individual effort of the student presenting the work. Any assistance must be reported to the instructor. If the work has entailed consulting other resources — journals, books, or other media — these resources must be cited in a manner appropriate to the course. It is the instructor's responsibility to indicate the appropriate manner of citation. Everything used from other sources — suggestions for organization of ideas, ideas themselves, or actual language — must be cited. Failure to cite borrowed material constitutes plagiarism. Undocumented use of materials from the World Wide Web is plagiarism.*
>
> *Academic cheating is, generally, the thwarting or breaking of the general rules of academic work or the specific rules of the individual courses. It includes falsifying data; submitting, without the instructor's approval, work in one course which was done for*

another; helping others to plagiarize or cheat from one's own or another's work; or actually doing the work of another person.

The penalty for academic dishonesty can vary from receiving a reprimand and a failing grade for a particular assignment, to a failing grade in the course, to suspension or expulsion from the university. The penalty varies with the nature of the offense, the individual instructor, the department, and the school or college.
Students who believe that they have been unfairly accused may appeal through the school or college's academic grievance procedure.

Academic dishonesty will not be tolerated in this class. In cases of cheating, both parties will be held equally responsible, i.e. both the student who shares the work and the student who copies the work. Penalties for such actions are given at my discretion, and can range from a failing grade for the individual assignment, to a failing grade for the entire course.

Classroom Etiquette

The environment you and your fellow students create in class directly impacts the value that is gained from the course. To that end, the following are my expectation of your conduct in this class:

- Arrive on time and stay until the end of class.
- Turn off cell phones, pagers and alarms while in class.
- Limit the use of electronic devices (e.g., laptop, tablet computer) to class-related usage such as taking notes. Restrict the use of an Internet connection (e.g., checking email, Internet browsing, sending instant messages) to before class, during class breaks, or after class.
- During class time speak to the entire class (or breakout group) and let each person "take their turn."
- Be fully present and remain present for the entirety of each class meeting.

Student and Faculty Academic Rights and Responsibilities

The University has adopted a policy on Student and Faculty Academic Rights and Responsibilities (Policy # 03.70.02) which can be accessed through the following link: http://policies.temple.edu/getdoc.asp?policy_no=03.70.02

Schedule

The schedule is subject to updates and modifications as the course progresses. Updates to the schedule will be announced in class and posted to the class blog**. It is your responsibility to ensure you are aware of the updated class schedule. In-class activities may occur in any class meeting.** Turn-in hard copy by end of class when activity occurs. They will be graded Pass/Fail based on completeness.

Week	Unit	Learning Outcomes, Topics & Required Reading	Labs
1	Chapter 1 & Chapter 2	• Class Introduction Understanding the Digital Forensics Profession and Investigation • The Investigator Office and Laboratory • Describe role of IT in Forensic • Examining Images for specific files, deleted files and keywords **Topics and Required Reading** • Computer Forensic US-CERT -http://www.merriam-webster.com/dictionary/forensic • The Role of Digital Forensics within a Corporate Organization - http://www.digitalforensics.ch/nikkel06a.pdf **Required Viewing** • Computer and Digital Forensic Career - https://www.youtube.com/watch?v=QPi6fQNwxbI • Computer Forensic Analyst - https://www.youtube.com/watch?v=K1YklHbHTZY • NIST - Putting the Science in Forensic Science- https://www.nist.gov/video/putting-science-forensic-science	Independent Lab • Setting Up Forensics Workstation a. Optional: Bootable Window Live or Linux Live Chapter 1 • Hand-on Project 1-1 • Hand-on Project 1-5 • Hand-on Project 1-6 Chapter 2: Case Project 2-3 pg. Research your state, province, or neighboring states and provinces to determine whether digital forensics examiners require licenses. Write a one-page summary of the licensing requirements in the region you selected. If your region doesn't have any requirements, research one of the following states: Michigan, Texas, or Georgia.
2	Chapter 3 & Chapter 4	• Understanding storage formats • Understanding acquisition planning, methods, tools and validation • Explain guidelines, rules and procedures for controlling, processing and storing digital evidence and crime scenes.	Take Screen shot to show completion Chapter 3 Hands-on Project 3-1 Hands-on Project 3-2

		Topics and Required Reading • Forensic Control - https://forensiccontrol.com/resources/beginners-guide-computer-forensics/ • Five Phases of Forensic Investigation - http://forensicandinvestigativeauditing.blogspot.com/2010/08/five-phases-of-investigation.html **Required Viewing** • Forensic Investigation Process - https://www.youtube.com/watch?v=NmuhGa4QekU • Understanding Forensic Science - https://www.lynda.com/Security-tutorials/Applying-science-digital-investigations/419360/455990-4.html • Digital Forensics | Davin Teo | TEDxHongKongSalon - https://www.youtube.com/watch?v=Pf-JnQfAEew	Chapter 4 Hand-on Project 4-3 Case Project 4-3 Your spouse works at a middle school and reports rumors of a teacher, Zane Wilkens, molesting some students and taking illicit pictures of them. Zane allegedly viewed these pictures in his office. Your spouse wants you to take a disk image of Zane's computer and find out whether the rumors are true. Write a summary outlining how you would tell your spouse and school administration to proceed. Also, explain why walking into Zane's office to acquire a disk image wouldn't preserve the integrity of the evidence
3	Chapter 6	• Evaluate, examine and test current digital forensics tools **Topics and Required Reading** • Emerging Challenges in Digital Forensic - http://www.forensicmag.com/article/2015/12/emerging-challenges-digital-forensics	Take a screen to show you completed this lab Chapter 6 Hand-on Project 6-2 Hand-on Project 6-3: Case Project 6-1 Do online research on two widely used GUI tools, Guidance Software EnCase and Access Data FTK, and compare their features with other products such as

		• Popular Computer Forensic Top Tools - https://resources.infosecinstitute.com/computer-forensics-tools/#gref **Required Viewing** • Mobile devices investigation is a challenging - https://cyberforensicator.com/2018/11/27/forensic-challenges-due-to-encryption-mechanisms/ • Cyber Forensics Investigations, Tools and Techniques - https://www.youtube.com/watch?v=OkFj1ePW2cU	NUIX(www.nuix.com) and Ontrack Easy Recover Professional. Write a one page report on features you would find most beneficial as it relates to Emerging Challenges in digital forensics
4	Chapter 9	• Digital Forensics Analysis and Validation Data hiding Techniques • Determine what data to analyze • Data Validation **Topics and Required Reading** • The importance of developmental validation In Forensic Science - https://blog.bizzmine.com/en/the-importance-of-developmental-validation-in-forensic-science **Required Viewing** • Chapter 9 Book Video - https://slideplayer.com/slide/7414434/	Take a screen to show you completed this lab Chapter 9 Hand-on Project 9-1 Hand-on Project 9-2: Case Project 9-2 Several graphics files were transmitted via e-mail from an unknown source to a suspect in an ongoing investigation. The lead investigator gives you these graphics file and tells you that at least four messages should be embedded in them. Use your problem solving skills and brainstorming skills to determine a procedure to follow. Write a short report outlining what to do.
5	Exam	**Exam #1 - Assess Weeks 1-4 learning objectives**	**Case Project:** Computer Forensic Reference Data Sets (CFReDS) Final Project Prep (Guidelines)

6	Chapter 10	• Live acquisitions • Using forensic tools for internal and external threats • Conducting forensics analysis on Virtual machines **Virtual Machine Forensics, Live Acquisitions and Network Forensics** **Topics and Required Reading** • Investigating Live Virtual Environments - https://www.sciencedirect.com/topics/computer-science/forensic-acquisition • Live vs Dead Computer Forensic Image Acquisition - https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080331.pdf **Required Viewing** • Chapter 10 - VM - Live Acquisitions - and Network Forensics - https://www.youtube.com/watch?v=JVTv3JaRfjY • Capturing RAM from a live system - https://www.youtube.com/watch?v=hRmHm5jQIQo	Chapter 10 Hands-on Project 10-1 Hands-on Project 10-3 Hands-on Project 10-4 Case Project You have acquire a forensic image of a suspect's laptop. After doing an examination, you discover at least one VM installed, and you think more data can be found, but you aren't sure. You decide to make a copy of the VM's file and mount the VM as an external drive. Write the best procedure for this situation
7	Chapter 11	• Email investigations, email acquisitions and analysis • Email Recovery • Social Media Forensics	Chapter 11 Hands-on Project 11-1 Hands-on Project 11-2 Hands-on Project 11-3

		Email and Social Media Forensics **Topics and Required Reading** • Litigation Holds: Ten Tips in Ten Minutes - https://www.ned.uscourts.gov/internetDocs/cle/2010-07/LitigationHoldTopTen.pdf • Facebook User Data Requests - https://www.cnet.com/news/facebook-law-enforcement-requests-for-user-data-up-9/ **Required Viewing** • Understanding Google Vault - https://www.youtube.com/watch?v=q2HFJb_JP2Q • Social Media Forensic - https://www.youtube.com/watch?v=JyU4l_6vFzQ	Case Project A mother call you and report that her 15-year old daughter has run away from home. She has access to her daughter's e-mail and says her daughter has e-mail in her inbox suggesting she has run away to be with a 35 year old woman. Her daughter has also made related post on Snapchat. Write a brief report explaining how you should proceed.
8	Chapter 12 and 13	• Acquisition procedures for Mobile Forensics • IOT Forensics • Cloud legal and technical challenges • Cloud investigation, acquisition and forensics tools **Mobile Device Forensics & IoT and Cloud Forensics** **Topics and Required Reading** • Suspect OKs Amazon to hand over Echo recordings in murder case -https://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case/index.html	Chapter 12 Hands-on Project 12-1 Hands-on Project 12-2 Hands-on Project 12-4 Chapter 13 Hands-on Project 13-1 Hands-on Project 13-2 Case Project 12-1 Download the most current version of NIST Mobile Device Forensics Guidelines. Write a brief summary of mobile device tools and how you may apply them.

		• Apple vs FBI - https://www.cnbc.com/2016/03/29/apple-vs-fbi-all-you-need-to-know.html • Cloud computing crime poses unique forensics challenges - https://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges • Popular Cloud Forensic Tools - http://resources.infosecinstitute.com/computer-forensics-tools/#gref **Required Viewing** • Cloud Forensic Discussion - https://www.youtube.com/watch?v=ZvAaTKbPzH8 • Challenges of Cloud Computing - https://arxiv.org/ftp/arxiv/papers/1410/1410.2123.pdf • Cloud computing crime poses unique forensics challenges - http://searchcloudcomputing.techtarget.com/feature/Cloud-computing-crime-poses-unique-forensics-challenges	
9	Exam	**Exam #2 – Assess week 6-9 learning objectives**	Cyber Challenge Practice Lab Final Project Prep (Step 1) Select Incident(s) and use as step 1 to draft an incident response plan. Do we use Temple's last 4 TTX? Need assumptions, but looking for process flow and lesson learned.

	Spring Break		
10	Chapter 15	**Expert Testimony in Digital Investigations** **Topics and Required Reading** • Computer Forensics Expert Witness Testimony - https://www.forensicon.com/services/computer-forensics/computer-forensics-expert-witness-testimony/ • What Role Does a Computer Forensics Expert Witness Play? - https://discovery.precise-law.com/computer-forensics-expert-witness/ **Required Viewing** • Digital Forensics Expert Testifies in Hernandez Trial - https://www.youtube.com/watch?v=aB2cbdinxhQ	Case Project 15-4 The general council for Superior Bicycles has asked you to create a Microsoft PowerPoint, LibreOffice Impress, or Web page presentation on the work you've done for him. Insert any evidence such as e-mails, documents, and photographs. He plans to have you make this presentation to the jury during the trial. Final Project Prep (Step 2)
11	Chapter 16	• Code of Ethics at it applies to individuals and organizations • Challenges in Testimony • Data Carving **Topics and Required Reading** • Ethics in Computer Forensics (Part 1) - https://www.forensicmag.com/article/2014/03/professional-ethics-digital-forensics-discipline-part-1 • Ethics in Computer Forensics (Part 2) - http://www.forensicmag.com/article/2014/06/professional-ethics-digital-forensics-discipline-part-2	Hands-On Project 16-1 Hands-On Project 16-2 Hands-On Project 16-3 Hands-On Project 16-4 Case Project 16-4→pg 679 Write an opinion paper of at least two pages describing your findings in the in-chapter activities and hands-on

		• There's no code of ethics to govern digital forensics – and we need one - http://theconversation.com/theres-no-code-of-ethics-to-govern-digital-forensics-and-we-need-one-45755 • What is a reasonable Search - https://bowtielaw.wordpress.com/2012/07/18/what-is-a-reasonable-search/ • Digital Search Warrants - http://www.iacpcybercenter.org/prosecutors/digital-search-warrants/ • Search and Seizure from a Digital Perspective - http://www.forensicfocus.com/search-and-seizure-digital-perspective **Required Viewing found here** • Ethical Insights: IT Forensics, Ethics and Risks - https://www.youtube.com/watch?v=UiqzV2NNPW8 • Ethics in Forensics - https://www.youtube.com/watch?v=2jao8xBFpTg • Can my employer monitor by computer? -https://www.g-s-law.com/blog/can-my-employer-monitor-my-computer • Privacy at Work. What are your Rights? - http://employment.findlaw.com/workplace-privacy/privacy-at-work-what-are-your-rights.html • Beyond Search & Seizure | Jeffrey Rosen | TEDxPhiladelphia - https://www.youtube.com/watch?v=iV4q4nRPyoY	projects for Jim Shu's second computer. Review the contents of the files you extracted, and make your own conclusion as to whether the data was corrupted intentionally or by an unknown virus. Include the facts that support your opinion and explain how you arrived at this conclusion

12	E-Discovery (Retention and Collection)	**Topics and Required Reading** 7.0. • E-Discovery 101:KISS - http://ediscoveryinsight.com/2011/10/e-discovery-101-5-tips-to-help-you-keep-it-short-and-simple-%E2%80%9Ckiss%E2%80%9D • E-Discovery Reference Model - http://www.edrm.net/frameworks-and-standards/edrm-model/ • Federal Rules Civil Procedures Discovery - http://www.lexology.com/library/detail.aspx?g=931cf0d9-00bd-402a-a575-b0920765b19d • The Need for Archiving - https://ediscovery101.com/2016/02/17/the-need-for-archiving-and-frcp-37e/ **Required Viewing found here** • EDiscovery LexisNexis - https://www.youtube.com/watch?v=gUdQAIgxJ5Y … …	Cyber Challenge Practice Lab Final Project Prep (Step 3)
13	Breach notification	**Topics and Required Reading** Developing a cyber incident notification process Sections - Security Breach Questionnaire - Next Steps: Developing the Plan https://iapp.org/resources/article/security-breach-response-plan-toolkit/	Cyber Challenge Practice Lab Final Project Prep (Mock Presentation)

		Experian Data Breach Response https://www.experian.com/assets/data-breach/brochures/response-guide.pdf Resource for Rules by State/Country https://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/Data_Breach_Charts.pdf **Required Viewing found here** Standardizing Data Breach Response https://vimeo.com/191596762 Why small companies should have an incident management plan https://vimeo.com/149619235 Public Relations in a Cyber Crisis https://vimeo.com/144897629	
14	Presentations	**Forensic Plan Presentations**	Final Project Presentation
15	Final Exams		

Other interesting articles and videos

- Social Engineering https://www.youtube.com/watch?v=lc7scxvKQOo
- Social Engineering - https://www.youtube.com/watch?v=PWVN3Rq4gzw
- Hacking - http://digg.com/video/white-hat-wireless-hacking
- US Power Grid Hack -https://www.youtube.com/watch?v=pL9q2lOZ1Fw