MIS 5170 – Organizational Forensic
Fall 2018

Instructor

Larry Brandolph
705 Conwell Hall
Email: larry.brandolph@temple.edu
Telephone: (215) 204-7088
e-profile: *http://community.mis.temple.edu/lbrandolph/*
Office hours: by appointment

Class Location and Time

Alter Hall 607
and
WebEx: When it's time, join the meeting.
WebEx: Access code: 641 521 199
1-855-244-8681 Call-in toll-free number (US/Canada)
1-650-479-3207 Call-in toll number (US/Canada)
Global call-in numbers | Toll-free calling restrictions
Can't join the meeting?
Time: Tuesday 5:30pm – 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 study and how technology and law interact to form forensic science. Computer forensics, or cyber forensics, is based on the investigation of digital data to gather evidence relating to criminal or other legal incidents and events. Computer 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 search hard drives for hidden files or recover deleted files. Internet activity, email, shared network storage, cloud services, social media, cellular devices, cameras. This course helps students understand how to find vulnerabilities, discovering intrusions and responding to computer incidents. Students will learn how attackers undermine and exploit systems so they can prepare, detect and respond to them. Legal issues involved in responding to computer attack are explored, including employee monitoring, working with law enforcement and handling evidence. Students will learn how to prepare to handle incidents, and participate in the process of incident identification, containment, eradication, recovery and lessons learned.

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. Develop an understanding of how forensics is effected by company policies, laws and ethics
4. Develop an understanding of Legal Holds, E-Discovery and Reasonable Search

5. Gain experience working as part of team, developing and delivering a professional presentation on an incident response plan
6. Gain insight into internal and external threats

Required Text and Readings

There is no required text for this course. There are assigned readings for each class. They are available via the Temple University library or for free online resources.

Course Grade Components

Component	Weight	Notes
Learn IT!	10%	Learn IT! assignments: 1. Hard Drive Search 2. Wireshark – What do I see on the Network?
Participation	10%	In class participation and class blog
Exam #1	20%	Non-cumulative - See Exams Section
Exam #2	20%	Non-cumulative - See Exams Section
Exam #3	20%	Non-cumulative - See Exams Section (Finals Week)
Forensic Plan	20%	Outline 5%; Plan 15%

Exams

There will be three exams for this course. All exams will be comprised of short-answer and/or longer open-ended questions. 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.

Learn IT! Assignment Grading Criteria

Grade	Criteria
Pass-High (100%)	The assignment consistently exceeds expectations. It demonstrates originality of thought and creativity throughout. Beyond completing all of the required elements, new concepts and ideas are detailed that transcend general discussions along similar topic areas. There are few mechanical, grammatical or organizational issues that detract from the presented ideas.
Pass (80%)	The assignment consistently meets expectations. It contains all the information prescribed for the assignment and demonstrates a command of the subject matter. There is sufficient detail to cover the subject completely but not too much as to be distracting. There may be some procedural issues, such as grammar or organizational challenges, but these do not significantly detract from the intended assignment goals.

Grade	Criteria
Fail (60%)	The assignment fails to consistently meet expectations. That is, the assignment is complete but contains problems that detract from the intended goals. These issues may be relating to content detail, be grammatical, or be a general lack of clarity. Other problems might include not fully following assignment directions.
Missing (0%)	Missing or late assignment.

Participation

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.

- Participation 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. 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 at least four times 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 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. Another important aspect of in-class participation is completion of in-class assignments and contribution to break-out group activities. 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

Email your document/assignment to: - MIS5170.nnhfmbl5tm7ugspb@u.box.com

You will receive this as a confirmation…
Your email attachment, AssignmentFile.pdf, was successfully uploaded into the CourseXYZ Spring 2018 Assignments folder

Course Topic Outline

- Current Issues in Cyber law
- Computer Ethics/Organizational Human Resources
- Cyber Incidents; building a partnership to respond
- Working with Inside and outside counsel
- Working with Law Enforcement
- Litigation Holds
- Reasonable search of available records
- Cloud Service and Social Media
- E-Discovery (Retention and Collection)
- Stolen Data by former employee
- Breach Notification, Media, PR and customer coverage
- Forensic Mobile Devices/BYOD

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	Due
1 – 1/16/2018	Introduction	Class Introduction Define Organizational Forensic Describe role of IT in Forensic **Topics and Required Reading** Introduction to Organizational Forensic http://www.merriam-webster.com/dictionary/forensic https://www.us-cert.gov/sites/default/files/publications/forensics.pdf http://www.digitalforensics.ch/nikkel06a.pdf **Required Viewing found here** 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	
2 – 1/23/2018	What is forensics?	Use of Forensic Stages of examination • Seizure, Acquisition, Analysis and Reporting • NIST – Collection, Examination, Analysis, Reporting **Topics and Required Reading** https://forensiccontrol.com/resources/beginners-guide-computer-forensics/ http://forensicandinvestigativeauditing.blogspot.com/2010/08/five-phases-of-investigation.html http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (Section 3)	

		Required Viewing found here Forensic Investigation Process https://www.youtube.com/watch?v=NmuhGa4QekU Applying science to digital investigations Understanding Forensic Science https://www.lynda.com/Security-tutorials/Applying-science-digital-investigations/419360/455990-4.html - Applying Science to digital investigations - Identifying digital evidence - Destroying digital evidence - Using forensic best practices - Examining forensic frameworks - Ensuring Scientific relevance Digital Forensics | Davin Teo | TEDxHongKongSalon https://www.youtube.com/watch?v=Pf-JnQfAEew	
3 – 1/30/2018	Cyber Laws	Current issues in Organization Forensic **Topics and Required Reading** United States Crime Laws and Procedures United Nations Office of Drugs and Crime – Search on United States https://www.unodc.org/cld/v3/cybrepo/legdb/search.html?lng=en 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 **Required Viewing found here** Computer Privacy in the Workplace, Featuring Attorney Wendi Lazar of Outten and Golden https://www.youtube.com/watch?v=lSnSl1HZDQA	Assignment – Hard Drive Search
4 – 2/6/2018	Ethics for Digital Forensics	**Topics and Required Reading** Ethics in Computer Forensics	

		https://www.forensicmag.com/article/2014/03/professional-ethics-digital-forensics-discipline-part-1 http://www.forensicmag.com/article/2014/06/professional-ethics-digital-forensics-discipline-part-2 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 **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	
5 – 2/13/2018	Exam	**Exam #1 - Assess week 1-4 learning objectives**	
6 – 2/20/2018	Current issues in the world of forensic	**Topics and Required Reading** 5.0. Emerging Challenges in Digital Forensic http://www.forensicmag.com/article/2015/12/emerging-challenges-digital-forensics 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 **Required Viewing found here** … … …	
7 - 2/27/2018	Cyber incidents, litigation holds, reasonable search	**Topics and Required Reading** 6.0. 4th Amendment https://www.law.cornell.edu/wex/fourth_amendment 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** Beyond Search & Seizure | Jeffrey Rosen | TEDxPhiladelphia https://www.youtube.com/watch?v=iV4q4nRPyoY …	
3/6/2018	Spring Break		
8 – 3/13/2018	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 … …	
9 – 3/20/2018	Breach notification	**Topics and Required Reading** 8.0. Developing an cyber incident notification process Sections - Security Breach Questionnaire - Next Steps: Developing the Plan https://iapp.org/resources/article/security-breach-response-plan-toolkit/ Experian Data Breach Response https://www.experian.com/assets/data-breach/brochures/response-guide.pdf	Assignment – Wireshark

		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	
10 – 3/27/2018	Exam	**Exam #2 – Assess week 6-9 learning objectives**	
11 – 4/3/2018	Internal Threats	**Topics and Required Reading** 9.0. 3 Types of Insider Threats http://www.csoonline.com/article/2128501/access-control/the-3-types-of-insider-threat.html 3 Types of Insider Threats and solutions https://www.healthitoutcomes.com/doc/the-types-of-insider-threats-and-how-to-stop-them-0001 4 Different Types of Attacks https://cloudtweaks.com/2015/01/4-different-types-attacks-understanding-insider-threat/ Recognizing Insider Threats https://securelist.com/threats/recognizing-different-types-of-insiders/ **Required Viewing found here** Insider Threat https://www.youtube.com/watch?v=p2ymPty1hsA Snowden Visualized https://www.youtube.com/watch?v=dPT6bYggalc … …	

12 – 4/10/2018	External Threats	**Topics and Required Reading** 10.0. … … … **Required Viewing found here** 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	Due - Final Project Outline
13 – 4/17/2018	Cloud and social media	**Topics and Required Reading** 11.0. Facebook User Data Requests https://www.cnet.com/news/facebook-law-enforcement-requests-for-user-data-up-9/ … **Required Viewing found here** … … …	
14 – 4/24/2018	Presentations	**Forensic Plan Presentations**	
5/8/2018 Time: TDB	Exam #3	**Exam #3 – Assess week 11-13 learning objectives**	