Identification, Collection, and Preservation of Digital Forensic Evidence
PARK UNIVERSITY
Continuing Education **Digital Forensic Computer Investigation Certificate**

Course	**Course 001 - Identification, Collection, and Preservation of Digital Forensic Evidence**
Meeting Time	Fall-2, 2018
Instructor	Faculty; Dr. Fred Cohen and Dr. Tom Johnson
Catalog Description	This course addresses identification, collection, and preservation of digital evidence. It introduces many techniques and includes practical examples and activities.
Prerequisites	
Course Level Learning Outcomes	**Expected Student Outcomes:** This course is designed to provide the student with an opportunity to: 1. Identify digital evidence, sources, processes, and devices 2. Collect digital evidence in a forensically sound manner and demonstrate proper collection and preservation.
Materials	**Required Text:** Fred Cohen. Challenges to Digital Forensic Evidence. ASP Press, 2008. The following documents/mechanisms will be made available online: • https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/forensic_science_progress_2-14-14.pdf and all referenced documents therein. • 2012-09-21 The Future of Digital Forensics - 1st Chinese Conf. on Digital Forensics – Talk

Teaching Methods:

This course involves reading, class discussions, homework, online activities, and projects to promote learning. A significant portion of the learning will take place outside the class setting. Students are expected to be active participants, asking questions, challenging the instructor, and taking responsibility for their own learning. The class will be delivered live online remote over the Internet.

Assignments:

The students will be assigned a variety of activities to support their learning experience. These will engage the use of tools provided through the Cyber Lab, the use of the Internet for research, and performing experiments in the real world.

Assignment 1:

Students will use the Internet to try to create a list of at least 50 digital devices that might contain evidence in a legal matter, including sample pictures of those devices, size specifications, the amount and type of digital evidence they might contain, whether the content is transitive, static, requires power to maintain, and the format in which they store the digital information. They will produce this result in a CSV files with URLs to point to sources and pictures.

Assignment 2:

Using the results from Assignment 1, the student will identify 10 of the devices for further processing. For each of those 10 devices, the student will identify commercially available methods or other methods if no commercial method is readily available, for making forensically sound image of the digital content, including the creation of a "data collection sheet" detailing the relevant contextual information collected in a forensically sound process.

Assignment 3:

Using example images provided from the Cyber Lab, students will produce forensically sound copies on their own systems, verifying that the images are correct, and transmit those images from student to student, each student creating an appropriate chain of evidence associated with each of the images, and each independently providing verification of proper transmission and receipt of both the material being transmitted and the associated chain of evidence. After the information is passed from student to student and reaches all of the students in the class, each student will verify that the final version of the content and the entire chain of evidence is consistent with proper chain of custody and unaltered in the process.

Presentation will count as 40%
Participation will count as 40%
Final Exam will count as 20%

Identification, Collection, and Preservation of Digital Forensic Evidence
PARK UNIVERSITY
Continuing Education **Digital Forensic Computer Investigation Certificate**

WEEK	*REQUIREMENTS*
1	Where can digital evidence come from: • Traces in storage, transit, and use • Forms and formats of records • Sources of evidence and digital devices • Other properties of those devices and storage **Assignment 1 starts.**
2	**Assignment 1 due.** Identifying and finding digital devices • Physical observation of devices • Other devices • Concealment methods for devices • **Assignment 2 starts.**
3	**Assignment 2 due.** Results to be discussed as part of class participation. Collection of evidence from storage devices • Disks and similar magnetic storage devices • USB sticks and similar electronic storage devices • Cell phones, "smart" devices, and IoT devices **Assignment 3 starts.**
4	Chain of custody • How it came to be • How it came to me • What did I do with it • Documenting chain of custody Technical verification for change detection
5	**Presentation of Assignment 3 results.** Results to be discussed and demonstrated as part of class participation. Final Exam

Instructor Availability (Pool of Available Instructors)

Park University Faculty;
Dr. Fred Cohen; Dr. Tom Johnson