



# ILLINOIS VALLEY COMMUNITY COLLEGE

## COURSE OUTLINE

**DIVISION: Workforce Development**

**COURSE: CSC 2200 Digital Forensics**

Date: August 28, 2018

Credit Hours: 3

Prerequisite(s): CSO 2200, CSO 2202, CSN 1225

Delivery Method:  **Lecture**                      **2 Contact Hours (1 contact = 1 credit hour)**  
 **Seminar**                              **0 Contact Hours (1 contact = 1 credit hour)**  
 **Lab**                                      **2 Contact Hours (2-3 contact = 1 credit hour)**  
 **Clinical**                                **0 Contact Hours (3 contact = 1 credit hour)**  
 **Online**  
 **Blended**

Offered:  **Fall**     **Spring**     **Summer**

IAI Equivalent –**Only for Transfer Courses**–go to <http://www.itransfer.org>.

### CATALOG DESCRIPTION:

This course instructs the student in how to discover, identify, extract and document computer crimes and corporate policy violations. The student performs this work by analyzing computer data through digital forensic tools.

## GENERAL EDUCATION GOALS ADDRESSED

*[See last page for Course Competency/Assessment Methods Matrix.]*

### Upon completion of the course, the student will be able:

*[Choose up to three goals that will be formally assessed in this course.]*

- To apply analytical and problem solving skills to personal, social, and professional issues and situations.
- To communicate successfully, both orally and in writing, to a variety of audiences.
- To construct a critical awareness of and appreciate diversity.
- To understand and use technology effectively and to understand its impact on the individual and society.
- To develop interpersonal capacity.
- To recognize what it means to act ethically and responsibly as an individual and as a member of society.
- To recognize what it means to develop and maintain a healthy lifestyle in terms of mind, body, and spirit.
- To connect learning to life.

### EXPECTED LEARNING OUTCOMES AND RELATED COMPETENCIES:

*[Outcomes related to course specific goals. See last page for more information.]*

#### Upon completion of the course, the student will be able to:

1. Identify the scope of computer forensics.
2. Know the fundamental technology behind operating systems and file systems
3. Understand the use of computer hardware storage media in computer forensic investigations.
4. Determine how to set up a secure forensics lab.
5. Understand how to thoroughly document the forensic investigation.
6. Identify and document network breaches.
7. Identify and document mobile forensics.
8. Understand photograph forensics.

**Outcome 1** – Upon completion of the course, the student will be able to identify the scope of computer forensics.

Competency 1.1 – The student will be able to identify the types of forensics evidence recovered including email, images, video, internet searches, website visits, cell phone

Competency 1.2 – The student will be able to understand the importance of computer forensics across industries

**Outcome 2** – Upon completion of the course, the student will know the fundamental technology behind operating systems and file systems

Competency 2.1 - The student will be able to define an operating system

Competency 2.2 – The student will be able to convert between binary, decimal, and hexadecimal notation

Competency 2.3 – The student will be able to identify the physical structure of a hard drive and how files are stored and retrieved

Competency 2.4 – The student will be able to understand the booting process

**Outcome 3** – Upon completion of the course, the student will understand the use of computer hardware storage media in computer forensic investigations.

Competency 3.1 – The student will be able to understand the types of devices used to forensically extract data from different storage devices.

Competency 3.2 – The student will be able to understand how evidence should be handled and analyzed

Competency 3.3 – The student will be able to understand the use of storage media in actual investigations.

**Outcome 4** – Upon completion of the course, the student will be able to determine how to set up a secure forensics lab

Competency 4.1 – The student will be able to identify good practices for managing and processing evidence in a computer forensics lab

Competency 4.2 – The student will be able to know how to properly acquire, handle, and analyze digital evidence

Competency 4.3 – The student will be able to use UNIX commands to scour files for particular information of interest.

**Outcome 5** - Upon completion of the course, the student will be able to understand how to thoroughly document the forensic investigation

Competency 5.1 – The student will be able to obtain/seize evidence and handle it properly

Competency 5.2 – The student will be able to document the investigation through forensic tools and reports

Competency 5.3 – The student will be able to understand what digital evidence and reporting is required for legal systems

**Outcome 6** - Upon completion of the course, the student will be able to identify and document network breaches

Competency 6.1 – The student will be able to understand the importance of network forensics and the underlying structure of networks

Competency 6.2 – The student will be able to investigate a network intrusion

**Outcome 7** - Upon completion of the course, the student will be able to identify and document mobile forensics

Competency 7.1 – The student will be able to understand the types of evidence available from cellphone carriers

Competency 7.2 – The student will be able to retrieve evidence from a smart phone

Competency 7.3 – The student will be able to analyze cell phone operating systems.

**Outcome 8** - Upon completion of the course, the student will be able to understand photograph forensics

Competency 8.1 – The student will be able to understand different types of digital photograph files and the metadata associated with these files.

Competency 8.2 – The student will be able to analyze photographic images by social media users

## MAPPING LEARNING OUTCOMES TO GENERAL EDUCATION GOALS

*[For each of the goals selected above, indicate which outcomes align with the goal.]*

Goals	Outcomes
First Goal	
To apply analytical and problem solving skills to personal, social, and professional issues and situations	<ol style="list-style-type: none"> <li>3. Understand the use of computer hardware storage media in computer forensic investigations.</li> <li>4. Determine how to set up a secure forensics lab.</li> <li>5. Understand how to thoroughly document the forensic investigation.</li> <li>6. Identify and document network breaches.</li> <li>7. Identify and document mobile forensics.</li> <li>8. Understand photograph forensics.</li> </ol>
Second Goal	
To understand and use technology effectively and to understand its impact on the individual and society.	<ol style="list-style-type: none"> <li>1. Identify the scope of computer forensics.</li> <li>2. Know the fundamental technology behind operating systems and file systems.</li> <li>3. Understand the use of computer hardware storage media in computer forensic investigations.</li> <li>4. Determine how to set up a secure forensics lab .</li> <li>5. Understand how to thoroughly document the forensic investigation.</li> <li>6. Identify and document network breaches.</li> <li>7. Identify and document mobile forensics.</li> <li>8. Understand photograph forensics.</li> </ol>

### COURSE TOPICS AND CONTENT REQUIREMENTS:

- Computer forensics scope and definition
- Data acquisition and handling
- Online investigations
- Documenting the investigation
- Network forensics
- Mobile forensics
- Recovering graphic files
- Report writing
- MAC versus PC file systems and forensic tools

### INSTRUCTIONAL METHODS:

- Lecture, online discussion threads, case studies, group work/discussions

### INSTRUCTIONAL MATERIALS:

A Practical Guide to Computer Forensics Investigations by Dr. Darren R. Hayes

Publisher: Pearson Education, Inc.

Print ISBN: 978-0-7897-4115-8

**STUDENT REQUIREMENTS AND METHODS OF EVALUATION:**

A= 90-100

B= 80-89

C= 70-79

D= 60-69

F= 0-59

**OTHER REFERENCES**

Guide to Computer Forensics and Investigations by Bill Nelson, Amelia Phillips,  
Christopher Steuart

Publisher: Cengage Learning

Print ISBN: 978-1-337-56894-4

Edition: 6th

# Course Competency/Assessment Methods Matrix

(Dept/# Course Name)	Assessment Options																																
For each competency/outcome place an "X" below the method of assessment to be used.	Assessment of Student Learning	Article Review	Case Studies	Group Projects	Lab Work	Oral Presentations	Pre-Post Tests	Quizzes	Written Exams	Artifact Self Reflection of Growth	Capstone Projects	Comprehensive Written Exit Exam	Course Embedded Questions	Multi-Media Projects	Observation	Writing Samples	Portfolio Evaluation	Real World Projects	Reflective Journals	Applied Application (skills) Test	Oral Exit Interviews	Accreditation Reviews/Reports	Advisory Council Feedback	Employer Surveys	Graduate Surveys	Internship/Practicum /Site Supervisor Evaluation	Licensing Exam	In Class Feedback	Simulation	Interview	Written Report	Assignment	
Assessment Measures – Are direct or indirect as indicated. List competencies/outcomes below.	Direct/	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	D	I	I	I	I	D	D							
Competency 1.1 – The student will be able to identify the types of forensics evidence recovered including email, images, video, internet searches, website visits, cell phone.								X	X																								X
Competency 1.2 – The student will be able to understand the importance of computer forensics across industries.								X	X																								X
Competency 2.1 - The student will be able to define an operating system.								X	X																								X

Competency 2.2 – The student will be able to convert between binary, decimal, and hexadecimal notation.					X			X	X																													X
Competency 2.3 – The student will be able to identify the physical structure of a hard drive and how files are stored and retrieved.					X			X	X																													X
Competency 2.4 – The student will be able to understand the booting process.								X	X																												X	
Competency 3.1 – The student will be able to understand the types of devices used to forensically extract data from different storage devices.					X			X	X																											X		X
Competency 3.2 – The student will be able to understand how evidence should be handled and analyzed.					X			X	X						X																					X		
Competency 3.3 – The student will be able to understand the use of storage media in actual investigations..					X			X	X						X																					X		X
Competency 4.1 – The student will be able to identify good practices for managing and processing evidence in a computer forensics lab.					X			X	X						X																					X		X

Competency 4.2 – The student will be able to know how to properly acquire, handle, and analyze digital evidence								X	X																			X					
Competency 4.3 – The student will be able to use UNIX commands to scour files for particular information of interest					X			X	X									X										X				X	
Competency 5.1 – The student will be able to obtain/seize evidence and handle it properly					X			X	X																			X				X	
Competency 5.2 – The student will be able to document the investigation though forensic tools and reports					X			X	X																						X	X	
Competency 5.3 – The student will be able to understand what digital evidence and reporting is required for legal systems					X			X	X																						X	X	
Competency 6.1 – The student will be able to understand the importance of network forensics and the underlying structure of networks								X	X																					X			
Competency 6.2 – The student will be able to investigate a network intrusion					X			X	X																							X	



Competency 7.1 – The student will be able to understand the types of evidence available from cellphone carriers				X			X	X																						X		X
Competency 7.2 – The student will be able to retrieve evidence from a smart phone				X			X	X																						X		X
Competency 7.3 – The student will be able to analyze cell phone operating systems.				X			X	X																						X		X
Competency 8.1 – The student will be able to understand different types of digital photograph files and the metadata associated with these files				X			X	X																								
Competency 8.2 – The student will be able to analyze photographic images by social media users				X			X	X																								X