COURSE SYLLABUS

LAST REVIEW	Fall 2022	
COURSE TITLE	Digital Forensics	
COURSE NUMBER	CIST 0155	
DIVISION	Career and Technical Education	
DEPARTMENT	CIST	
CIP CODE	24.0101	
CREDIT HOURS	3	
CONTACT HOURS/WEEK	Class: 2	Lab: 2
PREREQUISITES	None	
COREQUISITES	CIST 0101	

COURSE DESCRIPTION

This course provides students with the fundamentals of digital forensics and the methods used in the investigation of computer crimes. Students will understand and implement principles and procedures of data forensics. Students will gain the proper knowledge about investigating and illustrating evidence of Cybercrimes including the process of collection, examination, analysis, and presentation of the evidence. Topics included in this course (but not limited to) are applications of hardware and software to digital forensics, volume and file system analysis, proper equipment seizure methodology, confiscated materials analysis, follow up processes relating to an incident and computer forensics investigations.

PROGRAM ALIGNMENT

This course is part of a program aligned through the Kansas Board of Regents and Technical Education Authority. For more information, please visit: https://kansasregents.org/workforce_development/program-alignment

PROGRAM LEARNING OUTCOMES

1. Demonstrates the necessary skills to score at least a 70% in the Network 1 course.
2. Obtain the skills necessary to pass the Certification COMPTIA SEC+ certification.
3. Applies judicious and ethical offensive security techniques using knowledge gained through cyber security coursework.
4. Obtain the skills necessary to pass the NET+ certification.

TEXTBOOKS

http://kckccbookstore.com/

METHOD OF INSTRUCTION

A variety of instructional methods may be used depending on content area. These include but are not limited to lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE

I. Computer Forensics Fundamentals
   A. Incident response
   B. Hard disk structure
   C. Forensic tools
   D. Computer Investigations
   E. Computer forensics solutions
II. Computer Forensics and Investigations
   A. Computer forensics and investigations basics
   B. Computer investigations preparation
   C. Professional conduct
III. Computer Investigations
   A. Preparation of computer investigation
   B. Systematic approach of computer investigation
   C. Data-recovery
   D. Investigation execution
IV. Windows and DOS Systems
   A. Introduction of file systems
   B. Microsoft file structures
   C. NTFS file system and disks examination
   D. Windows boot & DOS startup tasks
V. Macintosh and Linux
   A. Macintosh file structure
   B. Macintosh boot tasks
   C. UNIX and Linux disk structures
   D. UNIX and Linux boot processes
   E. Compact disc data structures
VI. Forensic Laboratory
   A. Forensic lab certification requirements
   B. Lab physical layout
   C. Basic forensic workstation
   D. Forensic boot disks
VII. Computer Forensics Tools
   A. Software evaluation
   B. Command line forensics tools
   C. GUI forensics tools

    D. Other forensics tools

VIII. Digital Evidence Controls
    A. Digital evidence security & evaluation
    B. Digital evidence cataloging & storage
    C. Digital signature

IX. Crime and Incident Scenes Processing
    A. Private sector incident scenes
    B. Law enforcement crime scenes
    C. Search preparation
    D. Computer incident or crime scene security
    E. Digital evidence seizure & collection

X. Data Acquisition
    A. Data acquisition method & Data recovery
    B. DOS & Windows acquisition tools
    C. Linux acquisition
    D. Forensic acquisition tools

XI. Computer Forensic Analysis
    A. Computer forensic analysis basics
    B. Digital Intelligence forensics tools
    C. Computer forensic analysis performance
    D. Data hiding techniques

XII. E-Mail Investigation
    A. Internet fundamentals
    B. E-mail roles, servers & forensic tools

XIII. Image Files Recovery
    A. Image files recovery
    B. Image file headers analysis
    C. Copyright issues
    D. Image file recognition
    E. Data compression

XIV. Investigation Reports
    A. Importance of reports
    B. Opinion expression
    C. Report writing fundamentals

XV. Expert Witness
    A. Technical testimony
    B. Testimony preparation
    C. Deposition preparation

COURSE LEARNING OUTCOMES AND COMPETENCIES

Upon completion of the course, the student will:

A. Explain the concepts of Computer Forensics.

1. Understand the incident response.

2. Understand Forensic tools.
3. Explain computer forensics solutions.
4. Explain hard disk structure.

B. Explain computer investigations process.

5. Explain computer forensics and investigations basics.
6. Explain preparation of computer investigation.
7. Explain Systematic approach of computer investigation.
8. Understand data-recovery.
9. Understand investigation execution.

C. Explain Windows, DOS, MAC, and Linux operating systems basics.

10. Explain variety of file systems.
11. Explain variety of file structures.
12. Explain the boot processes of variety of operating systems.
13. Explain the NTFS file system and disks examination.
14. Understand the compact disc data structures.

D. Define forensic laboratory principles.

15. Understand forensic lab certification requirements.
16. Handle lab physical layout.
17. Explain basic forensic workstation.

E. Show knowledge of computer forensics tools.

18. Explain software evaluation.
19. Utilize command line and GUI forensics tools.

F. Explain digital evidence controls principals.

20. Explain digital evidence security & evaluation.
21. Explain digital evidence cataloging & storage.
22. Understand digital signature.

G. Explain incident scenes.

23. Understand private sector incident scenes.
24. Understand law enforcement crime scenes.
25. Explain search preparation principles.
26. Explain computer incident or crime scene security.
27. Understand digital evidence seizure & collection.

H. Explain data acquisition principles.

28. Understand data acquisition method & Data recovery.
29. Explain DOS & Windows acquisition tools.
30. Explain Linux acquisition.
31. Utilize forensic acquisition tools.

I. Analyze computer forensic.
  32. Analyze computer forensics.
  33. Utilize digital Intelligence forensics tools.
  34. Understand data hiding techniques.

J. Explain E-mail investigation.
  35. Explain Internet fundamentals.
  36. Understand E-mail roles, servers & forensic tools.

K. Perform image files recovery.
  37. Explain image files recovery.
  38. Analyze image file headers.
  39. Understand copyright issues.
  40. Explain image file recognition.
  41. Understand data compression.

L. Create investigation reports.
  42. Explain the importance of investigation reports.
  43. Explain opinion expression.
  44. Understand report writing fundamentals.

ASSESSMENT OF COURSE LEARNING OUTCOMES AND COMPETENCIES

Student progress is evaluated through both formative and summative assessment methods. Specific details may be found in the instructor's course information document.

COLLEGE POLICIES AND PROCEDURES

Student Handbook
https://www.kckcc.edu/files/docs/student-resources/student-handbook-and-code-of-conduct.pdf

College Catalog
https://www.kckcc.edu/academics/catalog/index.html

College Policies and Statements
https://www.kckcc.edu/about/policies-statements/index.html

Accessibility and Accommodations
https://www.kckcc.edu/academics/resources/student-accessibility-support-services/index.html.