

Digital Information & Technology Center of Excellence

Computer Systems Networking Department (Cybersecurity, Linux, Microsoft, Cisco, BCIS)

# ITSY 2443: Computer System Forensics | OnCampus | #23370

Fall 2020 | 16 Weeks (08.24.2020-12.13.2020)

3 Credit Hours | 96 hours per semester

## Instructor Contact Information

Instructor: Ryan Hill Office Phone: TBD

Office: TBD Office Hours: By Appt

HCC Email: ryan.hill@hccs.edu Office Location:

As your instructor, I am here to support you. Please feel free to schedule an appointment with me and discuss any problems that you are experiencing in this course or any other courses. Your performance in my class is very important to me.

### Instructor’s Preferred Method of Contact

I will respond as soon as possible during the week and in most cases during weekends. My preferred method is via email.

## What’s Exciting About This Course

In-depth study of system forensics including methodologies used for analysis of computer security breaches. Gather and evaluate evidence to perform postmortem analysis of a security breach.

## My Personal Welcome

The best way to really discuss issues is in person and I’m available during the week to tackle the questions. My goal is for you to learn Computer and Network Forensics skills that you can enhance further by tying in more networking, security, and programming. So please visit me or contact me by email whenever you have a question.

## Prerequisites and/or Co-Requisites

ITSC 1307 requires college-level reading and writing skills. Research indicates that you are most likely to succeed if you have already taken and passed ENGL 1301. The minimum requirements for enrollment in ITSC 1307 include placement in college-level reading (or take INRW 0420 or ESOL 0360 as a co-requisite). If you have enrolled in this course having satisfied these prerequisites, you have a higher chance of success than students who have not done so. Please carefully read and consider the repeater policy in the [HCCS Student Handbook.](http://www.hccs.edu/resources-for/current-students/student-handbook/)

### *Fall 2020 Modalities*

*This semester, there are three modalities for this course: Online Anytime, Online on a Schedule, and Flex Campus.* ***Note: all classes will meet online for the first six-weeks of the semester.****Online Anytime (WW) classes are traditional online courses; coursework is online, and there are no meetings at specific times. Online on a Schedule (WS) classes are online courses with traditional meeting components; coursework is online, and there are specific times to log in for scheduled class meetings. Flex Campus (FC) are in-person classes; coursework is online, and students have the choice to come to campus or to participate online during scheduled class meetings.*

*This section of ITSY 2443 is Online Anytime WW.*

## Canvas Learning Management System

This section of ITSY 2443 will use [Canvas](file:///C%3A%5CUsers%5CMatt%20Webster%5CAppData%5CLocal%5CTemp%5CCanvas) (<https://eagleonline.hccs.edu>) to supplement in-class assignments, exams, and activities. Please follow all the modules on Canvas and be sure to start with the first module titled “Getting started.” You will use Canvas to access all the course material including: class notes, exam reviews, videos, labs, and so on. You do not need to purchase anything for this course. You will also use Canvas to take your Midterm and Final exams (will be held in person).

HCCS Open Lab locations may be used to access the Internet and Canvas. **USE** [**FIREFOX**](https://www.mozilla.org/en-US/firefox/new/) **OR** [**CHROME**](https://www.google.com/chrome/browser/desktop/index.html) **AS THE INTERNET BROWSER**.

### HCC Online Information and Policies

Here is the link to information about HCC Online classes including the required Online Orientation for all fully online classes: <http://www.hccs.edu/online/>

### Scoring Rubrics, Sample Assignments, etc.

The scoring rubric is:

Midterm Exam: 35%

Final Exam: 30%

Assignments/Labs: 25%

Participation: 15%

# Instructional Materials

Guide to Computer Forensics and Investigations, 5th Edition;

AUTHORS: Nelson/Phillips/Steuart; ISBN13: 978-1-285-06003-3

Although you are required to purchase the book, I do send my notes which I derived & filtered from the book and added my own stuff. I send a review before each exam which is all you will need to do Well in the course. Of course, you are encouraged to read the book and even look at other books or resources for information – the more the better! Hearing from different perspectives will help shape your learning.

We have 16 chapters to cover and it’s a lot of material (much of it is repetitive) and I’ll focus on the main points. I also want this class to be as hands-on as possible. Expect to try many forensics tools and feel free to explore outside of the class and bring your own forensics tools & ideas.

The course content is accessible via Canvas on eagleonline.hccs.edu –you will find the class notes, PowerPoint slides, syllabus, articles/links, lab info, and more!

You will also have access to the VMware Academy as you will need it to retrieve the VMware Workstation (Windows) or VMware Fusion (Mac) in order to power Virtual Machines running a Windows Forensics Machine and a Linux VM.

## Other Instructional Resources

You will also have access to the VMware Academy as you will need it to retrieve the VMware Workstation (Windows) or VMware Fusion (Mac) in order to power Virtual Machines running Linux. We will be using Centos 7 as the Linux operating system and Centos 6.X is also welcome as well as Windows 10.

### Tutoring

HCC provides free, confidential, and convenient academic support, including writing critiques, to HCC students in an online environment and on campus. Tutoring is provided by HCC personnel in order to ensure that it is contextual and appropriate. Visit the [HCC Tutoring Services](http://www.hccs.edu/resources-for/current-students/tutoring/) website for services provided.

### Libraries

The HCC Library System consists of 9 libraries and 6 Electronic Resource Centers (ERCs) that are inviting places to study and collaborate on projects. Librarians are available both at the libraries and online to show you how to locate and use the resources you need. The libraries maintain a large selection of electronic resources as well as collections of books, magazines, newspapers, and audiovisual materials. The portal to all libraries’ resources and services is the HCCS library web page at [http://library.hccs.edu](http://library.hccs.edu/).

### Supplementary Instruction

Supplemental Instruction is an academic enrichment and support program that uses peer-assisted study sessions to improve student retention and success in historically difficult courses. Peer Support is provided by students who have already succeeded in completion of the specified course, and who earned a grade of A or B. Find details at <http://www.hccs.edu/resources-for/current-students/supplemental-instruction/>.

# Course Overview

In-depth study of system forensics including methodologies used for analysis of computer security breaches. Gather and evaluate evidence to perform postmortem analysis of a security breach.

## Core Curriculum Objectives (CCOs)

ITSY 2443 satisfies the computer science requirement in the HCCS core curriculum. The HCCS Computer Systems Networking Discipline Committee has specified that the course address the following core objectives:

* ***Critical Thinking***: Students will demonstrate the ability to engage in inquiry and analysis, evaluation and synthesis of information, and creative thinking by completing a written assignment such as a book report, research paper, or essay.
* ***Communication Skills***: Students will demonstrate effective development, interpretation and expression of ideas through written, oral, and visual communication by completing a written assignment such as a book report, research paper, or essay.
* ***Quantitative and Empirical Literacy***: Students will demonstrate the ability to draw conclusions based on the systematic analysis of topics using observation, experiment, and/or numerical skills by completing textbook reading assignments, completing assignments, and answering questions on quizzes and exams that pertain to Course Student Learning Outcome #2 below.
* ***Social Responsibility***: Students will demonstrate cultural self-awareness, intercultural competency, civil knowledge, and the ability to engage effectively in regional, national, and global communities by completing textbook reading assignments, completing assignments, and answering questions on quizzes and exams that pertain to Course Student Learning Outcome #4 below.
* ***Personal Responsibility (PR)***: To include the ability to connect choices, actions and consequences to ethical decision-making.

## Program Student Learning Outcomes (PSLOs)

Can be found at:

<https://www.hccs.edu/programs/areas-of-study/science-technology-engineering--math/computer-systems-networking--telecommunications/>

## Course Student Learning Outcomes (CSLOs)

Upon completion of ITSY 2443, the student will be able to:

• Chapter 1: Describe the field of digital forensics; Explain how to prepare for computer investigations and summarize the difference between public-sector and private-sector investigations; Explain the importance of maintaining professional conduct Describe how to prepare a digital forensics investigation by taking a systematic approach; Describe procedures for private-sector digital investigations; Explain requirements for data recovery workstations and software; Summarize how to conduct an investigation, including critiquing a case.

• Chapter 2: Describe certification requirements for digital forensics labs; List physical requirements for a digital forensics lab; Explain the criteria for selecting a Computer Science Technology Department basic forensic workstation; Describe components used to build a business case for developing a forensics lab.

• Chapter 3: List digital evidence storage formats; Explain ways to determine the best acquisition method; Describe contingency planning for data acquisitions; Explain how to use acquisition tools; Describe how to validate data acquisitions; Describe RAID acquisition methods; Explain how to use remote network acquisition tools; List other forensics tools available for data acquisitions.

• Chapter 4: Explain the rules for controlling digital evidence Describe how to collect evidence at private-sector incident scenes Explain guidelines for processing law enforcement crime scenes List the steps in preparing for an evidence search Describe how to secure a computer incident or crime scene Explain guidelines for seizing digital evidence at the scene List procedures for storing digital evidence Explain how to obtain a digital hash Review a case to identify requirements and plan your investigation.

• Chapter 5: Explain the purpose and structure of file systems Describe Microsoft file structures Explain the structure of NTFS disks List some options for decrypting drives encrypted with whole disk encryption Explain how the Windows Registry work; Describe Microsoft startup tasks Explain the purpose of a virtual machine.

• Chapter 6: Explain how to evaluate needs for digital forensics tools; Describe available digital forensics software tools; List some considerations for digital forensics hardware tools; Describe methods for validating and testing forensics tools.

• Chapter 7: Describe Linux file structures; Describe Macintosh file structures; Use Linux forensics tools.

• Chapter 8: Describe types of graphics file formats; Explain types of data compression; Explain how to locate and recover graphics files; Describe how to identify unknown file formats; Explain copyright issues with graphics.

• Chapter 9: Determine what data to analyze in a digital forensics investigation; Explain tools used to validate data; Explain common data-hiding techniques.

• Chapter 10: Explain standard procedures for conducting forensic analysis of virtual machines; Describe the process of a live acquisition; Explain network intrusions and unauthorized access; Describe standard procedures in network forensics and network-monitoring tools.

• Chapter 11: Explain the role of e-mail in investigations; Describe client and server roles in e-mail; Describe tasks in investigating e-mail crimes and violations; Explain the use of e-mail server logs; Explain how to approach investigating social media communications; Describe some available e-mail forensics tools.

• Chapter 12: Explain the basic concepts of mobile device forensics; Describe procedures for acquiring data from mobile devices.

• Chapter 13: Describe the main concepts of cloud computing; Summarize the legal challenges in conducting cloud forensics; Give an overview of the technical challenges with cloud forensics; Describe how to acquire cloud data; Explain how to conduct a cloud investigation; Explain what remote access tools can be used for Computer Science Technology Department cloud investigations.

• Chapter 14: Explain the importance of reports; Describe guidelines for writing reports; Explain how to use forensics tools to generate reports.

• Chapter 15: Explain guidelines for giving testimony as a fact witness or an expert witness; Describe guidelines for testifying in court; Explain guidelines for testifying in depositions and hearings; Describe procedures for preparing forensics evidence for testimony.

• Chapter 16: Explain guidelines for giving testimony as a fact witness or an expert witness; Describe guidelines for testifying in court; Explain guidelines for testifying in depositions and hearings; Describe procedures for preparing forensics evidence for testimony.

## Learning Objectives

Learning Objectives for each CSLO are mapped to each module on Canvas.

# Student Success

There are 16 chapters, videos, discussions, a midterm, and a final. It will be up to you to be on top of your work every week. Please do not procrastinate! Forensics will be very useful to you if you plan on getting into the IT field, so why not pay close attention now and enjoy learning? I would expect that you spend a few hours every week. This course is meant to be a baseline to explore further. Successful completion of this course requires a combination of the following:

* Reading the notes
* Watching the videos
* Completing assignments
* Participating in the discussions
* Being punctual

There is no short cut for success in this course; it requires reading (and probably re-reading) and studying the material using the course objectives as a guide. It will also require you to try all the commands and sequences introduced to you many times as repetition is your best ally to learn and memorize Forensic programs.

## Instructor and Student Responsibilities

As your Instructor, it is my responsibility to**:**

* Provide the grading scale and detailed grading formula explaining how student grades are to be derived
* Facilitate an effective learning environment through learner-centered instructional techniques
* Provide a description of any special projects or assignments
* Inform students of policies such as attendance, withdrawal, tardiness, and making up assignments
* Provide the course outline and class calendar that will include a description of any special projects or assignments
* Arrange to meet with individual students before and after class as required

As a student, it is your responsibility to**:**

* Attend class in person and/or online
* Participate actively by reviewing course material, interacting with classmates, and responding promptly in your communication with me
* Read and comprehend the textbook
* Complete the required assignments and exams
* Ask for help when there is a question or problem
* Keep copies of all paperwork, including this syllabus, handouts, and all assignments
* Attain a raw score of at least 50% on the departmental final exam
* Be aware of and comply with academic honesty policies in the [HCCS Student Handbook](http://www.hccs.edu/resources-for/current-students/student-handbook/)

# Assignments, Exams, and Activities

## Written Assignment

The assignment will be checked for plagiarism so please do not try. If you do copy material, then be sure to reference the website. The assignments and discussions are worth about 25-30% of your grade.

## Exams

You will have two exams: a midterm and a final. They are both 50 questions. The Midterm exam has many short-answer questions, multiple-choice, and true-false. The Final exam is all multiple-choice. You will receive reviews and jeopardy games as study material. Both exams will be taken in person. You will take them on Canvas.

## Grading Formula

I utilize a percentage-based points grading system. I group the Midterm and Final exam into a 60% exam group grade. I also add a third exam that I name “the best between the Midterm and Final” where I double the best grade between the Midterm & Final and I make an average of the three scores.

Midterm Exam 30%

Final Exam 30%

Labs 25%

Attendance/Participation 15%

| **Grade** | **Total Points** |
| --- | --- |
| A | 90+ |
| B | 80+ |
| C | 70+ |
| D | 60+ |
| F | <60 |

### Incomplete Policy:

In order to receive a grade of Incomplete (“I”), a student must have completed at least 85% of the work in the course. In all cases, the instructor reserves the right to decline a student’s request to receive a grade of Incomplete.

### HCC Grading Scale can be found on this site under Academic Information:

[**http://www.hccs.edu/resources-for/current-students/student-handbook/**](http://www.hccs.edu/resources-for/current-students/student-handbook/)

# Course Calendar

|  |  |  |  |
| --- | --- | --- | --- |
| **Week** | **Date** | **Topics** | **Assignment** |
| Week 1 |   | Chapter 1 | Assignment 1 |
| Week 2 |   | Chapter 2 | Assignment 2 |
| Week 3 |   | Chapter 3 | Assignment 3 |
| Week 4 |   | Chapter 4 | Assignment 4 |
| Week 5 |   | Chapter 5 | Assignment 5 |
| Week 6 |   | Chapter 6 | Assignment 6 |
| Week 7 |   | Chapter 7 | Assignment 7 |
| Week 8 |   | MIDTERM | MIDTERM |
| Week 9 |   | Chapter 8 | Assignment 8 |
| Week 10 |   | Chapter 9 | Assignment 9 |
| Week 11 |   | Chapter 10 | Assignment 10 |
| Week 12 |   | Chapter 11 | Assignment 11 |
| Week 13 |   | Chapter 12 | Assignment 12 |
| Week 14 |   | Chapter 13 | Assignment 13 |
| Week 15 |   | Chapter 14, 15, 16 | Assignment 14, 15, 16 |
| Week 16 |   | FINAL EXAM | FINAL EXAM |

## Syllabus Modifications

The instructor reserves the right to modify the syllabus at any time during the semester and will promptly notify students in writing, typically by e-mail, of any such changes.

# Instructor’s Practices and Procedures

## Missed Assignments

I do my best to accommodate your schedule and personal issues. Missed assignments can be submitted but with a 10-point penalty. I do not accept late discussion submissions. I may accept an exam make-up with ample notification and untestable claim for missing the exam. A make-up exam is not a retake. That is, make-up exams are allowed only for missed exams. Again, if you turn in any missed assignment then there will be a 10-point penalty assigned to it.

## Academic Integrity

Academic integrity is important to me and note that I will report any student that cheats during an exam. I give students a change to redo their projects should it have too much content that is plagiarized. Scholastic Dishonesty will result in a referral to the Dean of Student Services. See the link below for details.

Here’s the link to the HCC information about academic integrity (Scholastic Dishonesty and Violation of Academic Scholastic Dishonesty and Grievance):

<http://www.hccs.edu/about-hcc/procedures/student-rights-policies--procedures/student-procedures/>

## Attendance Procedures

I will use Canvas course participation analytics and my own judgement to give a participation grade of 15%. I expect that you login to Eagle Online (Canvas) at least once a week and that you regularly follow the due dates of your assignments. This course is fully online and you do not need to come in person unless you wish to meet me and for your midterm & final exams.

## Student Conduct

I expect you to read and study the course material in a timely fashion. You are expected to check your email regularly. You are expected to practice the commands and not just retain theory. You are expected to have fun. You are required to respect and help your peers. Cheating will not be allowed and tolerated.

# HCC Policies

Here’s the link to the HCC Student Handbook <http://www.hccs.edu/resources-for/current-students/student-handbook/> In it you will find information about the following:

* Academic Information
* Academic Support
* Attendance, Repeating Courses, and Withdrawal
* Career Planning and Job Search
* Childcare
* disAbility Support Services
* Electronic Devices
* Equal Educational Opportunity
* Financial Aid TV (FATV)
* General Student Complaints
* Grade of FX
* Incomplete Grades
* International Student Services
* Health Awareness
* Libraries/Bookstore
* Police Services & Campus Safety
* Student Life at HCC
* Student Rights and Responsibilities
* Student Services
* Testing
* Transfer Planning
* Veteran Services

## EGLS3

The EGLS3 ([Evaluation for Greater Learning Student Survey System](http://www.hccs.edu/resources-for/current-students/egls3-evaluate-your-professors/)) will be available for most courses near the end of the term until finals start. This brief survey will give invaluable information to your faculty about their teaching. Results are anonymous and will be available to faculty and division chairs after the end of the term. EGLS3 surveys are only available for the Fall and Spring semesters. EGLS3 surveys are not offered during the Summer semester due to logistical constraints.

<http://www.hccs.edu/resources-for/current-students/egls3-evaluate-your-professors/>

## Campus Carry Link

Here’s the link to the HCC information about Campus Carry: <http://www.hccs.edu/departments/police/campus-carry/>

## HCC Email Policy

When communicating via email, HCC requires students to communicate only through the HCC email system to protect your privacy. If you have not activated your HCC student email account, you can go [to HCC Eagle ID](http://www.hccs.edu/resources-for/current-students/student-e-maileagle-id/) and activate it now. You may also use Canvas Inbox to communicate.

## Housing and Food Assistance for Students

Any student who faces challenges securing their foods or housing and believes this may affect their performance in the course is urged to contact the Dean of Students at their college for support. Furthermore, please notify the professor if you are comfortable in doing so.

This will enable HCC to provide any resources that HCC may possess.

# Office of Institutional Equity

Use the link below to access the HCC Office of Institutional Equity, Inclusion, and Engagement (<http://www.hccs.edu/departments/institutional-equity/>)

## disAbility Services

HCC strives to make all learning experiences as accessible as possible. If you anticipate or experience academic barriers based on your disability (including long and short term conditions, mental health, chronic or temporary medical conditions), please meet with a campus Abilities Counselor as soon as possible in order to establish reasonable accommodations. Reasonable accommodations are established through an interactive process between you, your instructor(s) and Ability Services. It is the policy and practice of HCC to create inclusive and accessible learning environments consistent with federal and state law. For more information, please go to <http://www.hccs.edu/support-services/disability-services/>

## Title IX

Houston Community College is committed to cultivating an environment free from inappropriate conduct of a sexual or gender-based nature including sex discrimination, sexual assault, sexual harassment, and sexual violence. Sex discrimination includes all forms of sexual and gender-based misconduct and violates an individual’s fundamental rights and personal dignity. Title IX prohibits discrimination on the basis of sex-including pregnancy and parental status in educational programs and activities. If you require an accommodation due to pregnancy please contact an Abilities Services Counselor. The Director of EEO/Compliance is designated as the Title IX Coordinator and Section 504 Coordinator. All inquiries concerning HCC policies, compliance with applicable laws, statutes, and regulations (such as Title VI, Title IX, and Section 504), and complaints may be directed to:

David Cross
Director EEO/Compliance
Office of Institutional Equity & Diversity
3100 Main
(713) 718-8271
Houston, TX 77266-7517 or Institutional.Equity@hccs.edu

<http://www.hccs.edu/departments/institutional-equity/title-ix-know-your-rights/>

## Office of the Dean of Students

Contact the office of the Dean of Students to seek assistance in determining the correct complaint procedure to follow or to identify the appropriate academic dean or supervisor for informal resolution of complaints.

<https://www.hccs.edu/about-hcc/procedures/student-rights-policies--procedures/student-complaints/speak-with-the-dean-of-students/>

## Department Chair Contact Information

Fidelis Ngang. Fidelis.Ngang@hccs.edu

Naseem Nikooei, Naseem.nikooei@hccs.edu. 713-718-7631.