FLORIDA INTERNATIONAL UNIVERSITY

EEE 4752

Introduction to Network Forensics and Incident Response

Section: RVC

Internet/Fully Online

Spring Term 2026

Course Time Zone | Eastern Time (ET). Course due dates are according to this time zone.

Professor Information

Yu Du

Roles: Primary Instructor

Email: ydu@fiu.edu

Phone: 305-348-2886

Office Hours: by appointment

Office Location: EC3832

Website: yudu.fiu.edu

Department or Academic Unit: Electrical and Computer Engineering

Course Prerequisites

Course prerequisites, if any, are listed below.

Prerequisite: Senior Standing

Course Description

The course covers the theoretical and practical aspects of the foundations of computer network security, incident response tools and techniques.
(3 credits)

Textbook and Course Materials

EBK NETWORK FORENSICS

Required/Recommended: Required

Authors: MESSIER

Publisher: VST

Publication Date: July 14, 2017

Copyright Date: July 14, 2017

ISBN 10: 1119329183

ISBN 13: 9781119329183

Chapters/Pages: Chapter 2~12

Hands-On Network Forensics

Required/Recommended: Recommended

Authors: Nipun Jaswal

Publisher: Packt

Publication Date: 03-2019

Copyright Date: 03-2019

ISBN 10: 1789344522

ISBN 13: 9781789344523

Chapters/Pages: NA

Panther Book Pack

Get all required course materials for $20.50 per undergrad credit hour through Panther Book Pack. You'll be charged automatically unless you opt out within 3 days after the add/drop deadline.

For more details, to compare costs, and to learn how to access your course materials, visit the Panther Book Pack information page on FIU OneStop.

Readings, Materials, and Open Educational Resources (OER)

Hardware and Software Requirements

To successfully participate in this course, students are required to have access to the following hardware and software:

Hardware:

A computer running **Windows 10 or Windows 11 (required).**
Please note: ***Mac computers and Chromebooks are not compatible*** *with the software used in this course and cannot be used as substitutes.*

Reliable internet connection for accessing course materials, participating in virtual sessions, and submitting assignments.

A webcam and microphone for virtual meetings, presentations, and office hours.

Software:

Your Windows computer must be capable of installing **Oracle VirtualBox**, and running both **Kali Linux** and **Ubuntu Linux** virtual machines.

Your Windows computer must be capable of installing **Wireshark**.

Zoom (or equivalent video conferencing tool) for virtual meetings.

Canvas (course management system) access.

Note:
Installation guides and tutorials for VirtualBox, Kali Linux, Ubuntu Linux, Wireshark and other required software will be provided during the first week of class. Please ensure all necessary hardware and software are set up by the end of the first week to avoid falling behind in coursework.

Student Learning Outcomes/Objectives

- **Level I – Remembering (Knowledge): o Recall the basics of network forensics. o List fundamental networking concepts and protocols. o Identify various types of network attacks. o Recognize key host-side artifacts and their relevance in forensics.**

- **Level II – Understanding: o Explain fundamental networking concepts and their protocols. o Describe the process of packet capture and its role in feature extraction. o Summarize the importance of location awareness in acquired information. o Explain the role of encryption in network forensics.**

- **Level III – Applying: o Apply techniques for analyzing host-side artifacts. o Implement packet capture and processing methods for feature extraction. o Utilize appropriate event logging methods to prepare for potential attacks. o**

Apply intrusion detection systems to identify network anomalies. o Use networking scanning techniques to gather relevant information.

- **Level IV – Analyzing: o Analyze the effectiveness of various network attack types. o Contrast packet capture methods and their use in feature extraction. o Evaluate intrusion detection systems and their data. o Analyze firewall and application logs for identifying networking artifacts. o Assess the implications of cloud computing on network forensics.**

- **Level V – Evaluating: o Critique the effectiveness of different networking scanning techniques. o Evaluate the correlation of information gathered through network scanning. o Assess how encryption affects network forensics. o Judge the significance of event logging in preparing for and responding to network attacks.**

- **Level VI – Creating: o Design strategies for detecting and analyzing network intrusions. o Propose improvements for network scanning and intrusion detection techniques. o Develop methods for analyzing cloud-based artifacts in network forensics. o Create a comprehensive approach for handling encrypted network data in forensic analysis.**

Expectations of this Course

This is an online course, which means most (if not all) of the course work will be conducted online. Expectations for performance in an online course are the same as a traditional course. In fact, online courses require a degree of self-motivation, self-discipline, and technology skills which can make these courses more demanding for some students.

Students are expected to:

- Review the how to get started information located in the course content
- Introduce yourself to the class during the first week by posting a self introduction in the appropriate discussion forum
- Take the practice quiz to ensure that your computer is compatible with the LMS
- Interact online with instructor/s and peers
- Review and follow the course calendar
- Log in to the course four times per week
- Respond to discussion boards, blogs and journal postings within two days
- Respond to emails within two days
- Submit assignments by the corresponding deadline

The instructor will:

- Log in to the course at least four times per week
- Respond to discussion boards, blogs and journal postings within seven days
- Respond to emails within two days
- Grade assignments within seven days of the assignment deadline

Course Communication

Communication in this course will take place via the Canvas Inbox. Check out the Canvas Conversations Tutorial or Canvas Guide to learn how to communicate with your instructor and peers using Announcements, Discussions, and the Inbox. I will respond to all correspondences within 72 hours.

Policies & Resources

Before starting this course, please review the Policies & Resources Page in Canvas which includes comprehensive information on various University and Course Level Policies such as:

- University Policies
- Accessibility and Accommodations
- Online Etiquette
- Technical Requirements and Skills
- Computer & Digital Literacy Skills
- Course Technology Accessibility Statements and Privacy Policies
- Academic Integrity
- Copyright Statement
- Core Principles of This Course
- Nondiscrimination Statement
- Panthers Care & Counseling and Psychological Services (CAPS)
- Fair Use Policy

Assignments & Assessments

Discussion Forums

Keep in mind that your discussion forum postings will likely be seen by other

members of the course. Care should be taken when determining what to post.

Introduce Yourself:

- Students will post their course self introduction in this forum using the guidelines posted within the first week of class
- Available dates (unlimited)

Open Forum:

- Students may post general concerns related to the class
- Students cannot post any assignment results/answers or related files
- Available dates (unlimited)
- Forums are not graded, it is another mean to help students via peer discussion

Topic Discussion Forum:

- Students will be given an open-ended prompt pertaining to module content.
- Students are expected to post/respond to a forum. This includes a student post and a student response post. It is very important that the student response post provides new knowledge.
- The approximate length of a posting should be no less than 200 words, and a student response no less than 100 words.
- You need 1 primary + 2 peer reviews to qualify a full credit. Please check the discussion rubric carefully.
- Forums will be available Monday at 8:00 AM - Sunday at 11:59 PM
- Refer to the Discussion Participation Rubric posted in the course when compiling your post.
- The expected turn-around time for feedback is seven days.

Assessment Expectations

In order to mitigate any issues with your computer and online assessments, it is very important that you take the "Practice Quiz" from each computer you will be using to take your graded quizzes and exams. It is your responsibility to make sure your computer meets the minimum hardware requirements.

All assessments will auto-submit when (1) the timer runs out OR (2) the closing date/time is reached, **whichever happens first**. For example, if a quiz has a closing time of 5:00 pm but the student begins the exam at 4:55 pm, the student will only have 5 minutes to complete the quiz.

Quiz Expectations:

- This course consists of 12 quizzes, consisting of multiple modules.
- These quizzes serve primarily as a source of self-assessment.
- Quizzes will be available from Monday 12:00 am – Sunday 11:59 pm.
- Students will be given one attempt for each quiz.
- Students will be given 10-30 minutes to complete each quiz, based on number of questions.
- Students will be able to see their score upon submission.

Exam Expectations:

- The exams are composed of three parts, multiple-choice, problem solving and practical exercises. The multiple-choice question are directly related to reading assignments from the course textbook and self-assessments. The problem solving portion consist of course materials demonstrated during the course modules and the practical part is related to performing the lab assignments.

- Exams will be available.
    - Midterm Exam: 3**/1/26 Sunday from 12:00 AM to 11:59 PM**
    - Final Exam: 4**/18/26 Saturday from 12:00 AM to 11:59 PM**
- Students will be given one attempt for each exam.
- Students will be given 60 - 120 minutes to complete each exam, based on number of questions.
- Students will be able to see their score approximately seven days after submission.

Assessments in this course are not compatible with mobile devices and should not be taken through a mobile phone or a tablet. If you need further assistance please contact FIU Canvas Help Team.

Lab Assignment Expectations

- Explicit instructions and grading criteria will be provided for all assignments.
- Please see the Lab Assignment Rubric posted in the course for grading criteria.
- Unless specified otherwise, all assignments are to be completed by the individual student.
- Each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at least a failing grade for the course.
- All work is to be submitted via Canvas. **DO NOT send assignments by emails. You can use the comments area under the task to submit your makeup contents and files.**
- All work submitted should display Panther ID number and should be signed, as the students' own work, and that no unauthorized help was obtained.
- Assignments are due on the date specified. Assignments submitted late (within 1 week) will receive half credit.
- Students are encouraged to ask questions and to discuss course topics with the instructor and with each other.
- To get assistance try to see me by an appointment.
- The expected turn-around time for feedback or grades within seven days.
- Please provide a screenshot for the questions using Kali, Wireshark, software tools or commands, etc. ***Please make sure you should have a question answer with a screenshot as a proof***. Without the screenshot as a

proof, I can't give you a full score if you don't have a proof. ***You can eliminate some sensitive or private information from the screenshot, if you like.***

LinkedIn Learning Quiz Expectations

- This class requires that students work on an individual basis to complete a LinkedIn Learning course taught by an industry expert.
- The course is assigned in the Getting Started module and is titled “Network Forensics."
- Students earn full credit by submitting the certificate provided upon completion of the course quizzes.
- Late submissions are not permitted.
- No cost is associated with LinkedIn Learning as all students at Florida International University automatically have access.

Proctored Exams

Please note that the information contained in this section applies only if your course requires a proctored exam.

Through a careful examination of this syllabus, it is the student’s responsibility to determine whether this online course requires proctored exams. Please visit our Student Proctored Exam Instructions webpage for important information concerning proctored exams, proctoring centers, and important forms.

Zoom Video Conference

Zoom is a video conference tool that you can use to interact with your professor and fellow students by sharing screens, chatting, broadcasting live video/audio, and taking part in other interactive online activities.

Zoom meetings can be accessed via the Zoom link in the course navigation menu. Once you click on the Zoom link, it will route you to join the meeting for the respective class session. You will also be able to view upcoming meetings, previous meetings that you have already joined, and meeting recordings. Before joining an actual class session:

Reference the Zoom Student Tutorials to learn about the tool, how to access your meeting room, and share your screen.

Access the Zoom Test Meeting Room to test out the software before joining an actual session.

If you encounter any technical difficulties, please contact the FIU Canvas Help Team. Please ensure you contact support immediately upon the issue occurring.

Grading

COURSE REQUIREMENTS	NUMBER OF ITEMS	POINTS FOR EACH
LinkedIn Learning Quizzes	5	1
Quizzes	12	15
Exams	2	100
Discussions	12	16
Case Study	1	100
Assignments	11	100
Total	38	N/A

Grade Schema

GRADE	RANGE	
A	94% - 100%	
A-	90% - 93%	
B+	87% - 89%	
B	83% - 86%	
B-	80% - 82%	

Schedule of Topics

Module 1 - Network Forensics and Incident Response Basics | 1/5 - 1/11

Module 2 - Networking Fundamentals | 1/12 - 1/18

Module 3 - Networking Fundamentals II | 1/19 - 1/25

Module 4 - Search for Host-side Artifacts | 1/26 - 2/1

Module 5 - Packet Capture and Analysis | 2/2 - 2/8

Module 6 - Attack Types | 2/9 - 2/15

Module 7 - Location Awareness | 2/16 - 2/22

Module 8 - How to Prepare for an Attack | 2/23 - 3/1

Module 9 - Intrusion Detection Systems | 3/2 - 3/8

Module 10 - Using Firewall and Application Logs | 3/9 - 3/15

Module 11 - Correlating Attacks | 3/16 - 3/22

Module 12 - Network Scanning | 3/23- 4/5 (Two weeks in this module)

Module 13 - Encryption and Cloud Computing | 4/6 - 4/18 (Two weeks in this module. Everything will be due on Saturday)

Nondiscrimination Statement

The **Office of Civil Rights Compliance and Accessibility** (CRCA) is responsible for ensuring that FIU maintains a workplace and learning environment free from discrimination, where current and prospective faculty, staff, and students are treated equitably. If any student, employee, or applicant has a sincere and reasonable belief that they have been discriminated against or harassed based on age, color, disability, marital status, ethnic or national origin, race, religion, retaliation, sex, or any other protected category, they can report their concerns to the CRCA team through report.fiu.edu.