CYBER FORENSICS

Course Introduction

ITMS 538/438/IT-S 838 Course

This is a lecture and lab for 3 (3) course sections of Cyber Forensics:

Class	Section #	CRN
ITMS 538	01	14750
ITMS 538	01	14751
ITMS 438	02	14749

All sections are online.

© 2022 W.P. Lidinsky, D. Nelson

ITMS 538/438/IT-S 838 Course

- Blackboard
  - All sections have been combined into a single Blackboard course
    - Title: Fall 2022 – Cyber Forensics (ITMS-438/538)

- Current Enrollment: 17

© 2022 W.P. Lidinsky, D. Nelson

Your Instruction & Lab Team

Don Nelson
Instructor

- dnelson@iit.edu
- Office hours online: by appointment

Phil Matuszak
RADISH Lab Manager

- matuphi@iit.edu
- Contact me first with any RADISH issues

Bill Lidinsky
Professor Emeritus

Created course
Many thanks for his support

© 2022 W.P. Lidinsky, D. Nelson

COURSE DESCRIPTION

Course Description

- Broadly stated:

  This is a course in Cyber Forensics.

  Also known as "Digital Forensics" or "Computer Forensics"

  You'll learn what how to:

    Collect, process, analyze and present computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence or law enforcement investigations.

  In a real sense, you will learn to be an investigator who applies their forensic knowledge and skill to matters of law.

© 2022 W.P. Lidinsky, D. Nelson

Topics Covered

- Nature of Cyber Forensics
- Legal and Civil Issues
- The Investigation Process
- Forensic Methodologies & Evidence Control
- Forensic Laboratories
- Forensic Tools (throughout course)
- Mass Storage Forensics
  - Rotating magnetic
  - SSD
- Partitions (MBR & GPT)
- File Systems & Booting (DOS, Windows, Linux)
- Data Acquisition
- Cyber Forensic Analysis
- Network Forensic Analysis*
- Mobile Forensics
- Digital Image Forensics aka Forensic Image Analysis
- RAM Forensics*
- Email, web and social media investigations
- Cloud Forensics
- Forensic reporting and the role of the expert witness

** As time permits*

© 2022 W.P. Lidinsky, D. Nelson

Texts

Guide to Computer Forensics and Investigations

Authors: B. Nelson, A. Phillips, F. Enfinger, C. Steuart

6th edition

Publisher: Cengage Learning

ISBN-13: 978-1-337-56894-4

Publication date: 2019

Similar to 4th and 5th editions – but not the same

File System Forensic Analysis

Author: B. Carrier

Publisher: Addison Wesley

ISBN-13: 978-0-321-26817-4

ISBN-10: 0-32-126817-2

Publication date: 2005

Everything that you ever wanted to know about file systems from a forensics vantage point

Not a text

© 2022 W.P. Lidinsky, D. Nelson

Course Plan: Texts

- As an overall plan, we will follow the *Nelson* text
- But the *Nelson* text is weak on some topics such as file systems
  - Although the 6th edition of *Nelson et al* is better than previous editions
- We will use *Carrier's* book for:
  - Disk, volume and file system analysis
  - Certain software tool descriptions and usages (e.g., TSK)
- We will supplement the texts with added topics such as:
  - Advanced volume and file system topics
  - Deep dives into particular topics (e.g., Forensic Linguistics)
  - Tools

© 2022 W.P. Lidinsky, D. Nelson

Course Plan: Systems

- This course will use a combination of several systems
  - Lab (*RADISHng*)
    - A separate virtual machine will be assigned to each student:
      - Windows 10
    - You will be running other virtual environments on this desktop
      - E.g., Kali Linux
    - These virtual environments will provide you with the tools and environment needed to complete your labs and assignments
  - Class Information (*Blackboard*)
    - Lectures
    - Zoom meeting information
    - Communications (announcements, discussion boards)
    - Class postings
    - Exams

© 2022 W.P. Lidinsky, D. Nelson

Some Software Tools You Will Use

Windows 10 (RADISH)

- WinHex
- Autopsy
- TSK (Sleuthkit tools)
- FTK Imager
- ProDiscover Basic
- DB Browser for SQLite
- MATLAB
- VMWare Workstation Pro

Workstation Pro VMs

- Kali Linux
- Other Linux VMs

© 2022 W.P. Lidinsky, D. Nelson

This Course Will Include…

- Lectures
- Labs
  - During lectures
  - As assignments
  - As part of exams
- Assignments
  - Nelson (end of chapter)
    - Review Questions
    - Hands-on/Case Projects
  - Carrier
    - Nothing at end of chapters
  - Me
    - Special Problems
- Exams
  - Midterm
  - Final

© 2022 W.P. Lidinsky, D. Nelson

Blackboard

- All students should be able to access the following class materials
  - Lectures
  - Assignments
  - Discussions Forums
- We'll use the following Blackboard tools for class communication
  - Zoom (online office hours)
  - Discussion forums (class-wide communication, anyone to many)
  - Announcements (class-wide communication, me to all)

© 2022 W.P. Lidinsky, D. Nelson

Prerequisite Knowledge

- Familiarity with command line interface and/or scripting language
  - Command line: Linux, Windows, Bash, Windows Terminal, Powershell
  - Scripting: JavaScript, Python, etc.
- Computer Architecture Basics
  - CPU, RAM, Mass storage, Boot Process, Operating Systems, etc.
- Networking
  - Basic understanding for the lower 4 layers of Internet architecture
  - Cloud Storage

Lack of such knowledge will put you at an initial disadvantage

© 2022 W.P. Lidinsky, D. Nelson

RADISH

aka RADISHng

© 2022 W.P. Lidinsky, D. Nelson

RADISHng

- RADISHng refers to the next generation of RADISH
  - Remotely Accessible Dynamic Infrastructure for Students to Hack (next generation)
- You will be using RADISHng for almost all your labs and assignments
- On your desktop there will be several applications that you will need in this course
- Each of you will be assigned their own virtual desktops accessible remotely (Windows 10)

© 2022 W.P. Lidinsky, D. Nelson

RADISHng

- You will receive instructions telling you
  - How to access RADISHng
  - Your RADISHng credentials
  - How to open and log in to your virtual desktops
  - How to report any issues with RADISHng
- These instructions will be sent via email to each of you by early next week (either from Phil Matuszak or myself)
- The instructions for RADISHng access will also be posted on Blackboard

© 2022 W.P. Lidinsky, D. Nelson

RADISHng

- When you receive the email regarding your RADISH VM,
  - Install the necessary software on your computing device (e.g., VMWare Horizon Client)
  - Verify that you can access your RADISH virtual desktops from your personal computing device
  - Report any issues that you encounter
- Be sure this has been done before next class!

© 2022 W.P. Lidinsky, D. Nelson

ASSIGNMENTS

Types, Submissions, and Expectations

© 2022 W.P. Lidinsky, D. Nelson

Assignment Types

- Two primary types of assignments
  - Reading/Discussion Assignments
    - Naming Convention: Assignxx_rd
  - Submission Assignments
    - Naming Convention: Assignxx_s

© 2022 W.P. Lidinsky, D. Nelson

Course Requirements
Reading/Discussion Assignments

- Reading/Discussion Assignments
  - Generally involves:
    - Reading selected material from the text and/or
    - Reading material from additional references
  - Not directly graded
    - See next slide

© 2022 W.P. Lidinsky, D. Nelson

Course Requirements
Reading/Discussion Assignments

- Reading/Discussion Assignments
  - Before the next class
    - You are given a reading assignment from the text or supplementary material
      - Must read it before next class begins
    - A discussion forum has been created for the assignment
      - You must post a separate thread in that forum with your thoughts and questions
      - Participation is graded
  - In next class
    - Topics posted to forum will be discussed
  - After next class
    - Students must respond to at least one post of their choosing (not their own)
    - Create thread in new forum for next class's topics
  - You are graded by the timeliness and content of your posts

© 2022 W.P. Lidinsky, D. Nelson

Course Requirements
Submission Assignments

- **Submission** Assignments
  - Generally involves:
    - Answering questions from the text and/or
    - Completing a lab and/or
    - Completing an activity assigned by me
  - Always graded
  - Expectations
    - See next slides

© 2022 W.P. Lidinsky, D. Nelson

Course Requirements
Submission Assignments

- Submission Assignments
  - Problem Assignments
    - E.g., you will be asked to respond to questions or solve problems at end of chapter
  - Lab Assignments
    - These assignments require you to use the RADISHng desktop environment
    - Will have the opportunity to get hands-on experience
    - Will need to submit artifact, e.g.,
      - Procedure
      - Conclusion/Results
  - Due Date
    - See following slides

© 2022 W.P. Lidinsky, D. Nelson

Submission Assignment Process
Slide 1 of 7

- Submission assignments will usually be due (i.e., submitted to Blackboard) on or before 11:55pm on the second Sunday after the class when it was assigned (unless otherwise specified)
  - Exceptions to this policy will be clearly stated
  - Submission assignments will generally be posted no later than the day after the associated classroom lecture

© 2022 W.P. Lidinsky, D. Nelson

Submission Assignment Process

Slide 2 of 7

- The rationale behind the due date scheme
  - Gives students 9-11 days, including 2 weekends to do assignments
  - Affords students the opportunity to try the assignment before the next class session and get help if needed
  - Also accommodates students who are busy or away for an entire week. They should still be able to submit assignments on time
- Because of this, late homework will NOT be accepted
  - Blackboard will be configured to not accept homework submissions after the specified due date and time
- Suggested Strategy:
  - Do the assignment during the first 1st 5 days after it is assigned
  - Get help, if needed, during the next class session

© 2022 W.P. Lidinsky, D. Nelson

Submission Assignment Process
Slide 3 of 7

- Submission assignments will include
  - Problem assignment submissions done in the conventional manner
  - Lab assignment submissions that you will do using your computer and your access to RADISHng and/or the internet
    - Lab assignment submissions will typically consist of brief written reports containing screen shots of your results
- Each problem in your assignment must have the following 3 items:
  1. The problem number
  2. The statement of the problem as it was presented
  3. The execution or working of the problem

© 2022 W.P. Lidinsky, D. Nelson

Submission Assignment Process

Slide 4 of 7

- All submissions must be submitted in PDF format
  - Create it using whatever word processing tools you like (RADISH has LibreOffice)
  - Convert it to (save as) PDF format
- Screen shots must be copied from your screen and pasted into the document
  - Paste windows from your desktop, not the entire desktop screen
- Make sure that your screen shots and other pasted-in figures fit within the boundaries of your homework document
  - In the past, students have pasted in screen shots or other figures that extend why outside the viewing area
  - Points will be taken off your grade if this requirement is not met

© 2022 W.P. Lidinsky, D. Nelson

Submission Assignment Process
Slide 5 of 7

- Before you submit your assignment
  - View it in .pdf format
  - This will make sure that your submission is properly formatted after converting it to PDF
- You will lose points if submissions are not formatted correctly

© 2022 W.P. Lidinsky, D. Nelson

Submission Assignment Process
Slide 6 of 7

- Explanatory words must accompany each figure, table or screen shot in your homework submission
  - Adequate words must be put into the homework document explaining each screen shot or other figure
    - E.g., for a screen shot of a log file, sentences such as “This is a log file” are definitely NOT adequate
  - A submission containing screen shots or figures without adequate accompanying explanatory works will have its grade reduced

© 2022 W.P. Lidinsky, D. Nelson

Submission Assignment Process

Slide 7 of 7

1. Problem Number
2. Statement of Problem
3. Working of the problem

Problem 12a-3: *Determine the TCP and UDP ports that are open and provide an overall explanation of the columns and what is going on.*

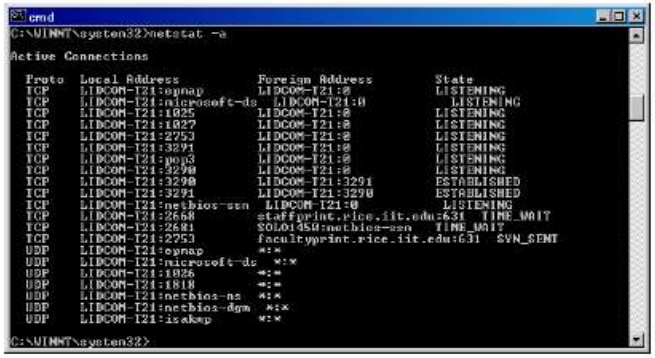

Figure 15: Screen Shot of `netstat -a` for Nelson's Notebook Computer

The above screen shot shows that a number of high numbered (>1024) TCP ports are open and in a listening state. This state means that... Note that both the local and foreign addresses are the same. The reason for this is...

Screen Shot figure

Explanation of figure

© 2021 W.P. Lidinsky, D. Nelson

Deliverables & Grading

- Grading
  - Midterm Exam: 30%
  - Final Exam: 30%
  - Assignments & Labs: 40%
- Nature of exams
  - Each exam has two parts
    - Online exam (taken on Blackboard)
    - Forensic Investigation (typically ~5 days to complete)
      - Submit zip file containing:
        - Investigation Report
        - Results of your investigation (including artifacts)

© 2022 W.P. Lidinsky, D. Nelson

Academic Honesty

You are expected to follow IIT's Code of Academic Honesty for ALL the work you do for this class:

- Never submit work that isn't your own
- No unauthorized assistance in all assessments
- Do not provide unauthorized assistance to others
- more (see policy)

Confirmed violations will result in academic disciplinary measures consistent with the Academic Honesty Policy

Please look over this policy:

https://www.iit.edu/student-affairs/student-handbook/fine-print/code-academic-honesty

© 2022 W.P. Lidinsky, D. Nelson

Assignments For This Week

- Assign01a_rd:
  - Read Chapter 1 in your Nelson text
  - Post a new thread in the Week 1 Discussion board on Blackboard
  - Due next Tuesday, 30 August
- Assign01b_s:
  - Log into your RADISHng desktop (Windows 10)
  - Take and submit screenshots of your desktops as evidence that you successfully logged in
  - Submit any maintenance request associated with issues you have accessing RADISHng
  - Due next Tuesday, 30 August

© 2022 W.P. Lidinsky, D. Nelson