Introduction, Course Overview and Prerequisite material

**Module Description:** The intent of this Knowledge Unit is to provide students with an introduction to this course and to review prerequisite information.

**Prerequisite Knowledge:**  Students are expected to have a solid understanding of binary data representations, including endianness; students are expected to have a familiarity with different types of networks and network devices; students are expected to have a knowledge of cyber security consistent with a one semester introductory level course discussing cyber security principles, threats, vulnerabilities and mitigations.

**Length of Completion**: 1 lecture/meeting/active learning hours

**Level of Instruction:** This module intended for advanced undergraduate students majoring in computer science or computer engineering.

**Learning Setting:** This module is suitable for many forms of delivery: online/in-class/hybrid.

**Lab Environment:** Students will have programming assignment outside of class. No specific environment required. Grading script is written in python.

Instructor may require submitted executables for a specific environment.

**Activity/Lab Tasks:** There will be in-class discussion, out-of-class written assignment, and out-of-class programming assignment.

**Lab Files that are Needed:**

http.cap sample input file

http\_decode.json sample output file

# learning outcomes

MODULE learning oUTCOMES

Upon completion of this lesson, students will be able to

* state the course requirements.
* explain terminology and concepts of the course prerequisite material
  + Data Representations
  + Cyber Security Fundamentals
  + IT Fundamentals

# module Details

**Instructional Files and Online Resources that are Needed:**

* + Lecture1.pptx
  + http.cap – sample pcap capture file
  + access to a terminal with ‘hd’ or other binary editor
    - Can use “Linux Subsystem for Windows”, Cygwin, Linux
    - Can use other standalone hex editors/viewers
  + pcap file format documentation
    - <https://wiki.wireshark.org/Development/LibpcapFileFormat>

**Assessment:**

* Written homework questions about C.I.A.
  + Module\_0\_Written\_HW.docx
  + Students with 80% or greater score pass
* Programming Lab – pcap decoder.
  + Module\_0\_Programming\_LAB.docx
  + Review submitted source code for standard programming style, comments, etc. Students should submit readable/maintainable buffer-overflow proof code.
  + Review submitted program with different input files samples and outputs. Using test script, expect 100% match.

# lesson

**Warm Up:** Instructor self-introduction

**Lesson Part 1:**

* Discuss the course materials, format and expectations
* Discuss needs for self-learning, for active learning.
* Discuss needs for “experimenting” – playing with code, modules, systems, and tools as a good way to learn.
* Present McCumber Cube Model

**Active Learning Activity:**

**Discussion:** Ask students where Network security fits into the McCumber Cube Model.

Make sure discussion includes: *Data in Transit, Confidentiality, Integrity (maybe Availability – or is that just network reliability?); Discuss technology (mechanisms) vs policy & procedure; Discuss Training & Education.*

**Lesson Part 2:**

* Present overview of network layers
* Demo ‘hd’ (or other binary editor) review of http.cap file. Want to highlight mapping of layer headers to pcap file format

Please attribute Dr. Jim Alves-Foss and Dr. Jia Song, University of Idaho  
  
  
  
Except where otherwise noted, this work is licensed under <https://creativecommons.org/licenses/by-nc-sa/4.0/>  
  
Notwithstanding the non-commercial license terms, non-profit educational institutions are granted a non-exclusive, royalty-free license to adapt and use this material, with attribution.  
  
Creative Commons and the double C in a circle are registered trademarks of Creative commons in the United States and other countries. Third party marks and brands are the property of their respective holders.