

CSC341: FUNDAMENTALS OF INFORMATION SECURITY

Individual Project, Fall 2022

Wireshark PCAP Dissection

Kutztown University, [Computer Science and Information Technology Department](#)

ASSIGNMENT INFORMATION

- Purpose:** The purpose of this assignment is to provide students the opportunity to learn the inner workings of Wireshark, dissect a unique sample PCAP file, and write up and present the findings. This individual project will help to prepare for the team project.
- Grade/Points:** There are two parts to this project: the write-up (20%) and the presentation (10%).
- Due Date:** **Sunday, October 9th, 11: 30 p.m. (both paper and slides). A 5-minute presentation the week of Oct. 9th, alphabetical order by last name.**

INSTRUCTIONS

The following instructions were not meant to be comprehensive. Additional steps will be discussed in class. Students may need to perform additional steps depending on their selection of the PCAP. You are to select ONE PCAP from this website (<https://gitlab.com/wireshark/wireshark/-/wikis/SampleCaptures#sample-captures>) by **Sunday, September 25th**. Select your PCAP ONLY from the "General/Unsorted" section. You are welcome to play with the other PCAP on your own. Next, reserve your PCAP by writing your full name in the NAME and your PCAP file name in the PCAP SELECTED of the *PCAP Selection* file that was emailed to you. The PCAP selection is based on a first-come-first-serve basis. No two students can select the same PCAP.

1. *Individual write-up:* Learn about Wireshark and apply it to your PCAP selection. Your write-up must be original (from your own words – do NOT plagiarize), and it will be graded based on the quality of your findings, not quantity/fillers. Your write-up needs to explain the following questions:
 - Page 1: One page
 - Question #1: What is Wireshark and why it is important to IT security?
 - Question #2: What are the advantages AND disadvantages of Wireshark?
 - Page 2: Can be one or more pages
 - Question #3: Explain in detail based on the Wireshark dissection of your PCAP, and what is the purpose(s) of its use in IT security. Include a snapshot of a partial Wireshark of your PCAP.
 - Question #4: Explain the key protocol used, its purpose(s), strength(s), and weakness(es) where applicable.
2. *Individual presentation:* Provide a five-minute presentation of your findings to the class (PPT format) – mainly your Page 2.

CSC341: FUNDAMENTALS OF INFORMATION SECURITY

Individual Project, Fall 2022

Wireshark PCAP Dissection

Kutztown University, [Computer Science and Information Technology Department](#)

GRADE: WORTH 30% OF YOUR COURSE GRADE

Part I: Individual write-up: Upload your write-up onto D2L under Assessments -> Assignments -> Individual Midterm Project (Write-up) before the deadline.

- Page 1: 5%
- Page 2: 10%
- Overall: 5% (spelling, grammar, neatness, and quality do count)

Part II: Individual presentation: 5 minutes. Upload your slides onto D2L under Assessments -> Assignments -> Individual Midterm (Short Presentation) before the deadline.

- Slides and quality of the presentation: 10%