

Homework #8: Forensics II

Assignment Details

This homework is due by Saturday, April 10th at **11:59 PM** ET. Remember there are no late submissions for the homework so please complete it by then.

For this assignment, be sure to document your process, don't just give the answers! Write as if you were explaining to yourself before you figured it out.

Please add the following header to your assignment:

Name: {Firstname Lastname}

UID: {Your UID}

Honor Pledge: *I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.*

Assignment Goal: Apply techniques learned during the Forensics II lecture to solve various problems surrounding wireshark and network forensics.

Assignment Questions

- **Question 1**

- We intercepted some sensitive communication during an infamous meme exchange. Could you extract the important files from this pcap?

- **Question 2:**

- There is a lot of the same looking traffic, though I heard there's some gold in this stream. Can you find the secret in this?
 - *Hint:* Use the search :)

- **Question 3:**

- I see a lot of noise in this pcap... some of the hosts don't seem super relevant, can you find the one with the secret?
 - *Hint:* Keep an eye on your POSTs :)
 - Corporate wanted to keep an eye on network statistics, could you attach a screenshot of the packet statistics for the pcap?
-

Scoring

This homework will be out of 100 points total.

Partial credit will be awarded where possible, as long as a good-faith attempt was made.

Point breakdown:

- Question 1 - 25 points
- Question 2 - 25 points
- Question 3 - 25 points
- Formatting - 25 points
 - Make sure to talk through the process, not just show the answers!