- Name and partner's name
    - Sean Folan (No partner)
- Project Description: Generally describe your project and why you think it is relevant to this class
    - Scavenger Hunt using disk, network and memory forensics. It will be a disk image of an investigator who was investigating something that required them to look at disk, network and memory forensics. So on the investigator's disk image, there are disk images, pcap files and memory snapshots that students will use for the scavenger hunt.
    - The computer will be that of an alleged counterfeiter
    - This is relevant because it allows students to get experience with 3 different kinds of forensics through a fun scavenger hunt
- Milestone Goals: What pieces of coding and evaluation will you complete for your milestone goals. You should choose these milestone goals as intermediate steps leading you to the final project goals. It may even be helpful to develop the final project goals first and then work backwards towards the Milestone Goals. These goals should be very specific: "Develop a library merging Rust and Spark to form Thermite." I suggest a bulleted list.
    - Come up with a list of evidence
        - Complete the following list
        - 10-15 pieces of evidence
            - Disk
                - Pdfs of counterfeit bills
                - Letters of correspondence with other counterfeiters
                - etc.
            - Network
                - HTTP get requests to monopoly money websites
                - etc.
            - Memory
                - Make a dummy process called "counterfieting.exe"
                - etc.
    - Develop all files that will be on the investigator's computer
        - Make the disk images
            - Made by running a VM on Virtual Box
                - Disk Image can be extracted from Virtual Box
            - These can be analyzed by the student using Sleuth Kit
        - Make the pcap
            - Made with Wireshark
            - These can be analyzed by the student using Wireshark
        - Make the memory snapshots
            - Made by running a VM on Virtual Box
                - Memory snapshots can be captured by Virtual Box
            - These can be analyzed using Volatility
    - Develop the investigator's computer

        - Put all of the above files on a Virtual Machine
        - Extract from Virtual Box
- Final Project Goals: What specific pieces of coding and evaluation will you complete for your final project report. These should be very specific: e.g. “A chart assessing the performance of the algorithm runtime versus the number of intermediate variables chosen.” I suggest a bulleted list.
    - Make Scavenger Hunt
    - First they get the investigator’s computer. They have to ignore the files on the investigator’s computer except for the ones labeled as evidence for the investigation
        - They can collect these files with Sleuth Kit
        - They will be asked to list all of the evidence files
    - Once they have the files, they must analyze them with tools and answer
        - Some specific questions
            - 1-2 questions about the specifics of each form of memory to ensure they look into each file. These should be easy to find but specific such as “what time was IMG_002.jpeg created” or “Is the transport layer protocol of packet 53 in ‘evidence.pcap’ TCP or UDP” etc.
        - Investigative Questions
            - These will ask the student to present 3-5 pieces of evidence to support their hypothesis
            - The computer will be that of an alleged counterfeiter and there may be evidence such as files “fake_money.pdf”, search history “How to make counterfeit bills” or programs running like “counterfeit.exe”