EN.650.431 Ethical Hacking Home Work #2

Recent examples such as [1] remind us that knowledge of core computer science courses is not a requirement to become an expert hacker. The only real requirements are a tenacious spirit and an analytical mind. Given these facts, please use your available resources to perform the below tasks.

1. Focusing on the wireless connection between the Bebop and its controller (smartphone running the FreeFlight Application), use Wireshark to analyze this interaction and technically document its **NEW and IMPROVED ARDiscovery Process**:
    a. What is the IP address of the Bebop?
    b. What ports are open on the Bebop?
    c. What operating system does the Bebop use?
    d. Explain the new Bebop 2 ARDiscovery process
    e. In the Bebop 2, what were the JSON records replaced with?
2. How can you wage a denial of service (DoS) attack against the Bebop ARDiscovery Process?
    a. Find a weakness in the ARDiscovery Process that you documented in question #1, write code to exploit this weakness, then demonstrate that it works.
        i. Note, DoS-ing the ARDiscovery Process will break the link between the controller and the Bebop. One side effect would be the streaming video sent from the Bebop to the smartphone stops.
3. Study the Bebop 2 and proved that the legacy Bebop 1 ARDiscovery Process exists within the Bebop2. Now, perform a DoS attack against the Bebop 2 using this legacy process.

In a 5-minute (or less) video, explain and illustrate the results from your work above. You can work in groups of no more than five. Please email to Lanier.Watkins@jhuapl.edu and put **EN.650.431 and** all student names and in subject

References:

[1] A. Greenberg. "iPhone Super-Hacker Comex, Let Go From Apple, Goes To Work For Google". Forbes Online Magazine, April 24, 2013. Available at: http://www.forbes.com/sites/andygreenberg/2013/04/24/iphone-super-hacker-comex-let-go-from-apple-goes-to-work-for-google/#fe1536a60528