CFRS 772: Forensic Artifact Extraction
Homework 9

1. **Write a module as follows...**
   - i. Create a sqlite3 database with two tables (t_ipaddress and t_macaddress) with one field each (both varchar): ipaddress and macaddress
     1. You can use the sqlite3 command line tool or python to create the db
     2. Call the database file "endpoints.db"
   - ii. Call your python module hw9.py
   - iii. The module should have one function called "endpoints" and it should take a pcap filename (a string, not a filehandle) as its only argument
   - iv. The module should parse a pcap file and write unique IP addresses and MAC addresses to the database; notes:
     1. Assume the pcap file is well-formatted (and not pcapng)
     2. Only parse IP addresses and MAC addresses from the packet headers (not from payloads)
     3. Only parse IP addresses from IP packets (ignore IP addresses in non-IP packets, like ARP, but do report the MAC addresses from non-IP packets)
     4. Only parse and report IPv4 addresses (but do report the MAC addresses from IPv6 packets)
     5. You do not need to associate IP and MAC addresses
     6. You can use the HW6 pcap for initial testing (you should also create a small pcap on your own and test against it as well)
     7. Only store unique IP and MAC addresses in the database (i.e., no duplicates)
     8. You may want to store the IP addresses and MAC addresses as Python sets before writing (or test uniqueness and write to the db file as you go)
     9. Remember to commit() and close() the connection in your code
     10. BONUS (+1 point and optional): add counts in the database (how many packets contained each IP address and MAC address); note that you might want two tables for this, or two additional uniquely named fields, …
   - v. I'll test this with a new pcap file
   - vi. Use your main code for testing; I'll call the endpoint function directly from my test code

On BlackBoard, submit your Python code as a zipped version of hw9.py. In the comments section on BlackBoard, paste the output of the sqlite3 .schema command for your database, e.g.,

```
CREATE TABLE tbl1(one varchar(10), two smallint);
```