CS6963 Midterm

RELEASE DATE: **MARCH 20 2017**
DUE: **MARCH 26 2017 @ 11:55PM EDT**

INSTRUCTIONS:

- You have the **CHOICE** of completing either **Question A** or **B**.
- The work must be done individually and without assistance.
- Review the NYU Policy on Academic Honesty
- Be sure to provide proper attribution where necessary
- If you decide to complete both we will grade only the last one submitted
- There will be **no extensions**
- In keeping with the course objectives, only open-source or free tools may be used.
- Email me if you have questions.

A

M57 Patents: Illegal Materials

http://digitalcorpora.org/corp/nps/scenarios/2009-m57-patents/docs/M57-Patents-Illegal.pdf

You are tasked with determining the following:

1. Is Jo responsible for the files found on the purchased machine? What evidence is there to support this? (35 Points)
2. How did this machine get onto the secondary market? (15 Points)
3. Who (if anyone) from the company is responsible for the sale of the machine? (20 Points)
4. Are there any other suspicious activities occurring within M57? (30 Points)

What to Submit: A single PDF report answering the questions with your methodology. Include screenshots of relevant information.

URLs:

- Hard Drive Images: http://digitalcorpora.org/corp/nps/scenarios/2009-m57-patents/drives-redacted/
- Flash Drive Images: http://digitalcorpora.org/corp/nps/scenarios/2009-m57-patents/usb/
- RAM Images: http://digitalcorpora.org/corp/nps/scenarios/2009-m57-patents/ram/
- Network Traffic: http://digitalcorpora.org/corp/nps/scenarios/2009-m57-patents/net/

B

IP Geolocation

Create a script that performs domain name analysis and IP geolocation of the provided list of URLs. Your script should be able to perform the following at a minimum:

- Retrieve whois information for the URL (15 Points)
- Lookup the associated IP Address for the DNS record (15 Points)
- Basic fingerprinting of the server based on a response header (15 Points)
- Retrieve geolocation information for the URL (20 Points)

As output, the script should have the options to create the following:

- Text-based report file (10 Points)
- SQLite Database containing the information (10 Points)
- KML file to visualize geolocation on Google Earth (15 Points)

What to Submit: A single PDF describing the environment in which you created your script (i.e. Ubuntu ver, MacOS, Windows, etc) + Libraries, and a screenshot of it successfully running (a video would be nice, but not necessary). A copy of your script (not a pdf).

Reminder: Any code that is not your own needs to have a reference to the original source. The majority (75%+) of your script must be your own code.

References:

- List of URLs: http://isis.poly.edu/~marcbudofsky/cs6963-spring2017/URLs