Instructions:

You have 1 week to complete this challenge. Due date is Monday, March 7th
You can use any programming / scripting language of your choice to complete the test.
Please provide detailed instructions for us to run and test the code.
Please comment your code

Challenge:

Attached is a sample dataset from a public honeypot that records various security events. Your task would be to consume the data, parse it based on the type (Attacker IP, Victim IP, Port, Connection Type, Source, Timestamp, etc). The goal of this exercise is to accept Indicators Of Compromise (IOC) (IP address, port, source, domain, URL) as arguments to the program and to look up all information related to the IOC(s) and provide the information in an user-friendly fashion.

Eg., python threatintel.py 192.161.23.45, 192.161.34.52 -----> Executing the code assuming threatintel.py is the code that does the above mentioned task. The output should provide this type of information:

Information for Victim IP 192.161.23.45
Attacker IP: 21.6.7.83
Connection Type : Initial
Source: Honeypot
Time stamp: 2015-05-21

Information for Victim IP 192.161.34.52
Attacker IP: 21.6.7.84
Connection Type : Initial
Source: Honeypot
Time stamp: 2015-05-23

The above is the basic challenge. The honeypot is just one source of data. Also IP address is just one type of IOC, the argument could be a single or multiple hashes, domains, URLs, files. The scope of the assignment is to correlate data against multiple sources like these:

https://isc.sans.edu/api/
https://www.virustotal.com/en/documentation/public-api/
https://malwr.com/about/terms/
http://www.phishtank.com/phish_archive.php

https://developers.google.com/safe-browsing/?csw=1

Each of these have public API's (a registration might be required but it is free) which you could query, so what is expected is that when an IOC is provided like python threatintel.py 192.161.23.45, the IOC 192.161.23.45 is queried against the honeypot data provided as well as the above public API's and the output received as shown above is displayed to the user.

Bonus points are awarded for creative end-user display and scalable correlation algorithm.