***NetSweep Specifications document***

*Contributors: Dillon Donovan, Andrew Landry*

Lang - Python (version 3.12)

IDE setup - Visual Studio (version 1.86)

Visual studio plugins:

1. Microsoft - Pylance v2023.12.1
2. Microsoft - Python v2024.0.1
3. Microsoft - Python Debugger v2024.0.0

GIT repo - <https://github.com/Dillon-Donovan/NetSweep>

**Required libraries**

* **igraph** – Could be used to visually represent data, library includes functionality to manipulate and analyze graphs
  + DOCS - <https://python.igraph.org/en/stable/>
* **Matplotlib** – Can be used as to graph and represent data gathered through network and packet analysis
* ***Network analysis library***
  + **Scapy** - allows users to send, sniff, dissect and forge network packets. This capability allows construction of tools that can probe, scan or attack networks.
    - Per Scapy documentation you can import individual components for use as you see fit
    - Compared to other libraries Scapy allows the user much deeper knowledge of what is going on behind any request being sent. This allows for greater customization and troubleshooting, as well as potential extensibility.
    - Advanced toolset with applications in both beginner and advanced settings
    - Potential dependencies based on use case
      * Python 3.7+
      * Windows will require NPcap ( <https://npcap.com/guide/> ) which could pose an issue while Linux and MacOS have native support
      * Plotting. plot() needs [Matplotlib](https://matplotlib.org/).
      * Graphs. conversations() needs [Graphviz](http://www.graphviz.org/) and [ImageMagick](http://www.imagemagick.org/).
      * 2D graphics. psdump() and pdfdump() need [PyX](http://pyx.sourceforge.net/) which in turn needs a LaTeX distribution: [texlive (Unix)](http://www.tug.org/texlive/) or [MikTex (Windows)](https://miktex.org/).
      * 3D graphics. trace3D() needs [VPython-Jupyter](https://github.com/vpython/vpython-jupyter/).
    - DOCS - <https://scapy.readthedocs.io/en/latest/introduction.html>
    - *Note: None of these dependencies above are necessary if running on Linux or MacOS*
* ***IP Geolocation*** methods (needs review by end of week)
  + **Geolocation DB** – Database used to geolocate IP addresses
  + **ip2geotools** is an alternate IP geolocation method is using python library, my only issue with this library is the large list of dependencies it would introduce. Needs more review by end of week.
    - DOCS - <https://pypi.org/project/ip2geotools/>
* ***GUI library***
  + PyQt5 – Used to create GUI’s for applications using python
    - Functional on all major OS’s
    - Professional and sleek
    - Supports more media than competitors
    - DOCS - <https://riverbankcomputing.com/software/pyqt/intro>
  + If issues arise with PyQt5 then **Tkinter** is a great fall back, Tkinter just lacks the high quality design and offers less support for displaying all types of media.

**Scope of project**

* To begin as a base network scanner that provides network information such as:
  + IP Addresses (selectable from a specific range)
  + Subnets
  + DNS Servers
  + Default Gateway
  + Ping Tests, Advanced Traceroutes, and Hop Counts
* And to expand upon the possibility of implementing:
  + Graphical Layout of Network
  + Visual Traceroutes
  + SYN/ACK information
  + Routing Protocol information
  + Packet Sniffing
  + Deep packet inspection
  + Custom packet design tool