In this lab, we will investigate some web-based tools which can provide insight into different facets of the Internet. Perform the following tasks, taking notes and/or screen captures as instructed (you may wish to review the questions to be answered at the end of these lab instructions before starting these tasks):

1. **Mapping IXPs**

As we have learned, Internet Exchange Points (IXPs) form the backbone of the global Internet. We can actually see the physical IXP site locations displayed on a global map.

* Open a web browser and go to [https://www.internetexchangemap.com/](about:blank)
* Zoom and reposition the interactive map until the 3 IXPs located nearest to San Antonio are visible. Use the [Windows Snipping Tool](about:blank) or other method to save a screenshot of the website with this view.
* Select each IXP on the map in turn, and record (screenshot or snip, copy/paste, or manual) the building information (name, if given, and address) for each [Question 1a]
* Zoom out to the world view again. Look for areas with a dense concentration of IXP pins on the map and zoom in slightly to read country names. Identify at least one country (not the United States) which appears to have a high concentration of IXPs relative to its geographic boundaries. Zoom and reposition to an appropriate position and get a screenshot/snippet. [Question 1b]

1. **Domain Name Search**

Part of establishing a presence on the Internet is registering a domain name. Although the Internet Corporation for Assigned Names and Numbers ([ICANN](about:blank)) ultimately coordinates the assignment of domain names, there are a number of organizations that will help search for, and register, a unique domain name. In this part of the Lab, we will investigate one of these services.

* Using a web browser, go to the site [https://who.is/](about:blank)
* In the form field that reads, Domain names or IP addresses…, type “amazon.com” and press Enter
* The page that results tells you that amazon.com is already registered (duh!). It also provides a good deal of information about the existing amazon.com domain account. Note the information in the **Registrar Info**, **Important Dates** and **Name Servers** blocks. You may want to screenshot/snip, save the page, or print the page to answer specifics in [Question 2a]
* Try entering some potential domain names that would be meaningful to you and see if one is available (possibly with a .net, .org or .news extension). For example, I tried “AceInstructorHuddleston.com” and it was available. Screenshot or note the response of your attempt--it’s okay if your selected domain name is not available [Question 2b]

1. **Basic Tools - NSLookup**

There is a simple tool built into the operating system which allows us to look up IP addresses corresponding to Internet domain names. This tool makes use of the Domain Name System (DNS) we studied previously.

* Open a console window (In the Windows search bar, type “command prompt” and open it)
* At the user prompt, type “nslookup www.espn.com”
* Save a screenshot of the results [Question 3a]
* In the same console window (or new one, if you like), use the nslookup command to find IP addresses for www.utsa.edu
* Capture a screenshot of these results [Question 3b]

1. **Online Virus Scanners**

There are many online virus scanners available to scan URLs, IP addresses, files, hashes, etc. and run them against dozens of antivirus engines. Many different antivirus engines are used to scan information entered into VirusTotal, which means several different perspectives are used to determine whether a file is malicious or not. One such tool is VirusTotal.

* Open VirusTotal at <https://www.virustotal.com/gui/home/upload>
* Search the URL: www.utsa.edu and capture a screenshot of the results [Question 4a]
* Search the URL: 1866809.securefastserver.com and capture a screenshot of the results [Question 4b]
* Search the IP Address: 184.164.143.90 and capture a screenshot of the results [Question 4c]
* Search the file hash: 0b376074c5a6f6fbf80bc867b87d10aa and capture a screenshot of the results [Question 4d]

**Turn-in Requirements**: To complete the assignment, upload a Word (.docx) or Adobe (.pdf) file with answers to the questions below as your submission to the M10 Lab B assignment in Blackboard.

1a. (3 pts) Provide a screenshot of the Internet Exchange Map showing the 3 IXPs located nearest to San Antonio. What is the building information (name, if given, and address) for each of these IXPs?

Map

Description automatically generated

Map

Description automatically generated with medium confidenceGraphical user interface, application, map

Description automatically generated

Graphical user interface, map

Description automatically generated

Graphical user interface, application, map

Description automatically generated

1b. (3 pts) What country (other than the United States) do you think has a high concentration of IXPs relative to its geographic boundaries? Include a screenshot/snippet.

The Kingdom of the Netherlands has a high concentration of IXP

Map

Description automatically generated

The northern tip of Italy has a high concentration of IXP

Map

Description automatically generated

2a. (3 pts) What is the Name listed in the Registrar Info for amazon.com? When was this domain registered and when is the registration scheduled to expire? What is the IP address of the first Name Server listed?

Logo

Description automatically generated with medium confidenceGraphical user interface, text, application, chat or text message

Description automatically generatedGraphical user interface, text, application, chat or text message

Description automatically generated

2b. (3 pts) What domain name did you test for registration availability? Was it available as a .com? If not, to whom was it registered (Name in Registrar Info)?

Graphical user interface

Description automatically generated

I tested cybernet.com for registration availability. It was not available in .com but .co . It was registered under Network Solutions, LLC

3a. (3 pts) What IP addresses were provided for www.espn.com (provide a screenshot)?

Graphical user interface, text

Description automatically generated

3b. (3 pts) What IP addresses were provided for www.utsa.edu (provide a screenshot)?

Text

Description automatically generated with medium confidence

Graphical user interface

Description automatically generated with medium confidence4a. (3 pts) How many anti-virus engines detected this URL as a threat (provide a screenshot)?

Table

Description automatically generated

Zero anti-virus engines detected this URL as a threat however 17 Security vendors were not able to rate this URL

4b. (3 pts) How many anti-virus engines detected this URL as a threat (provide a screenshot)?

Graphical user interface, text, application, email

Description automatically generated

Table

Description automatically generated

6 anti-virus engines detected this URL as a threat. 17 Security vendors were not able to rate this URL and on top of that Sophos rated this URL as Spam.

4c. (3 pts) How many anti-virus engines detected this IP Address as a threat (provide a screenshot)?

Graphical user interface, text, application, email

Description automatically generated

A picture containing text, document

Description automatically generated

Zero anti-virus engines detected this URL as a threat; however, 17 Security vendors were not able to rate this URL. Another thing I see is that one vendor, Forcepoint ThreatSeeker, has rated this ip as Spam.

4d. (3 pts) How many anti-virus engines detected this file hash as a threat (provide a screenshot)?

Graphical user interface, text, application

Description automatically generated

Graphical user interface

Description automatically generated with medium confidence

Graphical user interface, text, application, email

Description automatically generated

32 anti-virus engines detected this URL as a threat and the same 17 Security vendors were not able to rate this URL.