# Assignment – 2

Name: Ishan Aakash Patel

Student ID: 146151238

Course: Threat Intelligence (CYT-245)

**Exploratory Data Analysis of IP addresses**

**Task – 1**

**Questions and Answers**

1. **Why would you need to convert dotted-decimal presentation of IP address to integer form?**
   - ⇨ Converting an IP address from its dotted-decimal format (e.g., 192.168.0.1) to an integer form (e.g., 3232235521) simplifies the processing and comparison of IP addresses. Integer representation makes it easier to perform mathematical operations, such as calculating ranges or subnetting, and is more efficient for storage and computational purposes.
2. **Why would you need to do segmenting, or grouping, of IP addresses?**
   - ⇨ Segmenting or grouping IP addresses helps in organizing and managing large sets of IP data. This process is crucial for network analysis, security monitoring, and incident response. By grouping IPs, you can identify patterns, detect anomalies, and apply specific rules or policies to certain segments, enhancing the effectiveness of network security measures.
3. **Explain CIDR prefix format.**
   - ⇨ CIDR (Classless Inter-Domain Routing) prefix format is a method for allocating IP addresses and routing IP packets. It represents an IP address and its associated network mask in the form of `a.b.c.d/n`, where `a.b.c.d` is the IP address and `/n` indicates the number of bits in the subnet mask. For example, `192.168.1.0/24` means the first 24 bits of the IP address are used for the network identifier, leaving the remaining bits for host addresses within the network.
4. **Explain what is AS and ASN. How it can be useful for segmenting or grouping task?**
   - ⇨ An Autonomous System (AS) is a collection of IP networks and routers under the control of a single organization that presents a common routing policy to the internet. Each AS is assigned a unique Autonomous System Number (ASN). ASNs are useful for segmenting or grouping IP addresses because they indicate which organization or entity owns and manages the network. This information helps in network management, security analysis, and identifying the origin of network traffic.
5. **Play with https://www.maxmind.com/en/home. Describe the value of the services and data provided (you are not supposed to buy anything there, just go through description)**
   - ⇨ MaxMind offers services for IP geolocation and online fraud prevention. Their databases and APIs provide accurate information about the geographical location of IP addresses, including

country, region, city, and ISP. This data is valuable for enhancing security measures, detecting fraudulent activities, personalizing user experiences, and conducting market analysis.

6. **Why would you need to augment IP address data?**

   ⇨ Augmenting IP address data involves enriching it with additional information, such as geolocation, ASN, and associated domain names. This enhanced data provides better context and insights, improving the accuracy of security analysis, threat detection, and incident response. It helps security professionals understand the source and nature of network traffic, facilitating more informed decision-making.

7. **Play with www.iana.org. Describe what kind of information you can obtain from this service.**

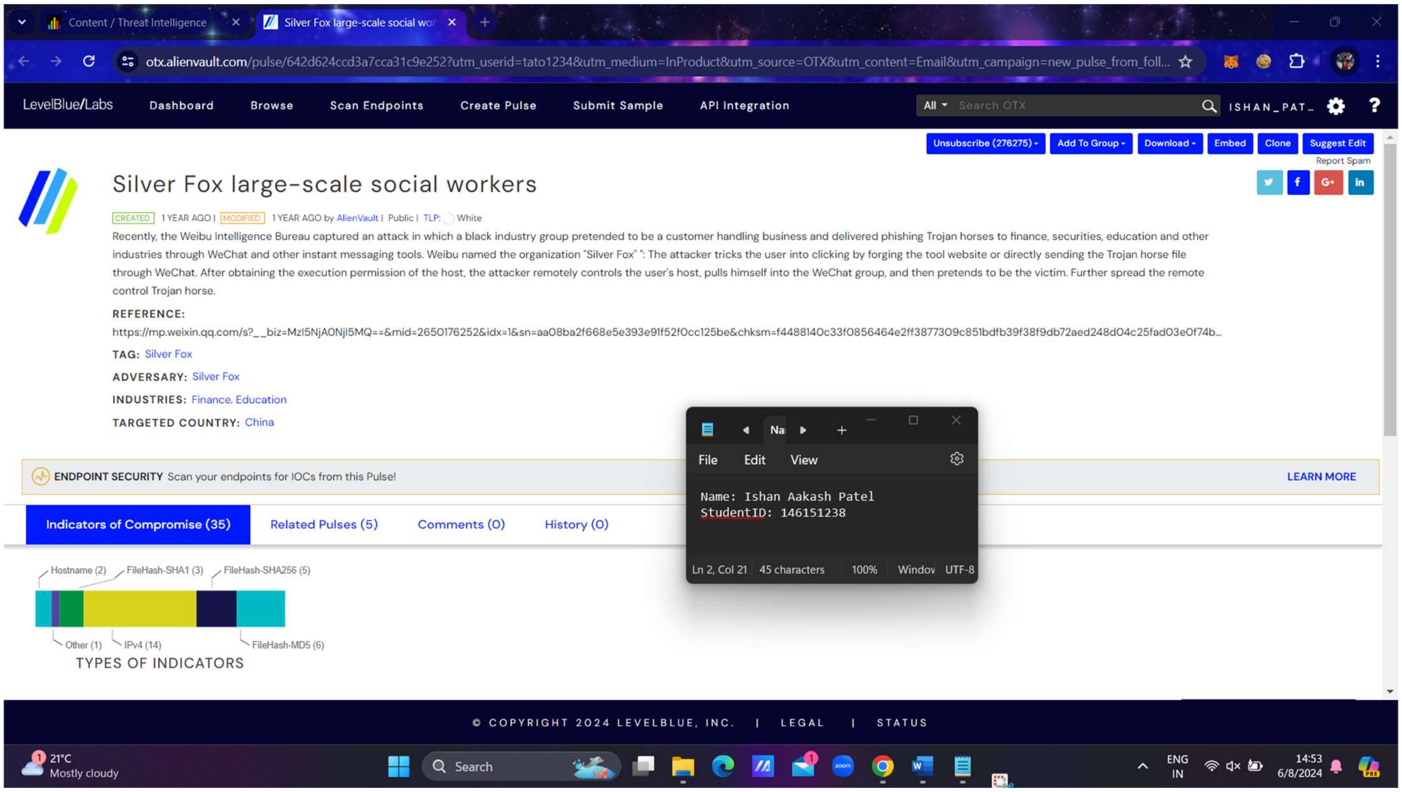
   ⇨ IANA is responsible for coordinating the global pool of IP addresses and ASNs. From IANA, you can obtain information about the allocation of IP address ranges, management of ASNs, and the assignment of other internet protocol resources. This information is crucial for network management, ensuring the proper allocation and use of internet resources, and maintaining the stability and interoperability of the internet.

## Task – 2

### Implement the following Use Case

Context: You are security analyst of the AAA company, and you are given the task to do analysis of IP addresses associated with the threat alert.

1. Connect to AlienVault site and retrieve certain network indicators (individual and CIDR)



Silver Fox large-scale social workers

CREATED 1 YEAR AGO | MODIFIED 1 YEAR AGO by AlienVault | Public | TLP: White

Recently, the Weibu Intelligence Bureau captured an attack in which a black industry group pretended to be a customer handling business and delivered phishing Trojan horses to finance, securities, education and other industries through WeChat and other instant messaging tools. Weibu named the organization "Silver Fox" ": The attacker tricks the user into clicking by forging the tool website or directly sending the Trojan horse file through WeChat. After obtaining the execution permission of the host, the attacker remotely controls the user's host, pulls himself into the WeChat group, and then pretends to be the victim. Further spread the remote control Trojan horse.

REFERENCE:
https://mp.weixin.qq.com/s?__biz=MzI5NjA0NjI5MQ==&mid=2650176252&idx=1&sn=aa08ba2f668e5e393e91f52f0cc125be&chksm=f4488140c33f0856464e2ff3877309c851bdfb39f38f9db72aed248d04c25fad03e0f74b...

TAG: Silver Fox

ADVERSARY: Silver Fox

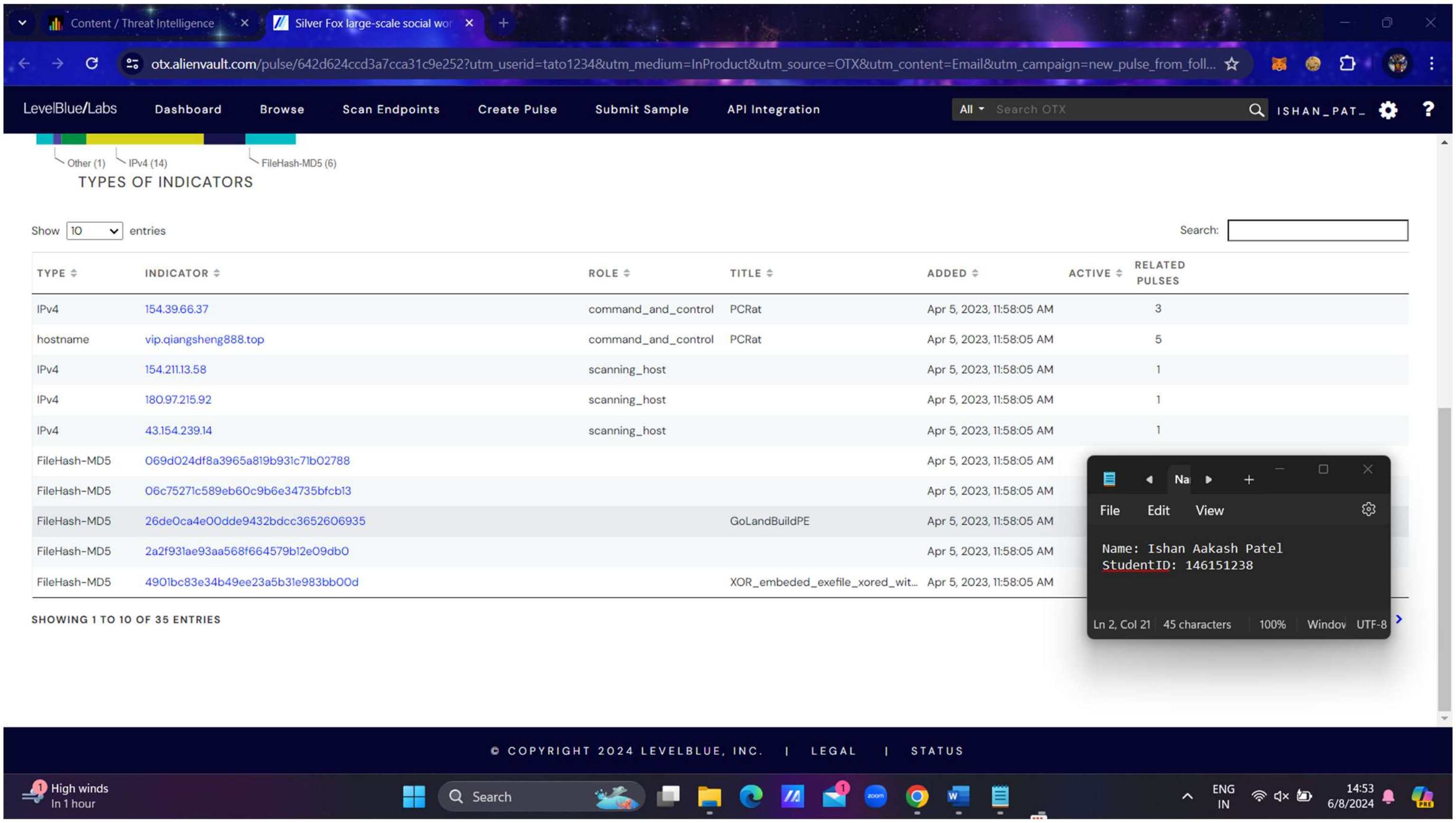
INDUSTRIES: Finance, Education

TARGETED COUNTRY: China

ENDPOINT SECURITY Scan your endpoints for IOCs from this Pulse!

Indicators of Compromise (35) | Related Pulses (5) | Comments (0) | History (0)

```
Name: Ishan Aakash Patel
StudentID: 146151238
```


Content / Threat Intelligence
Silver Fox large-scale social wor
otx.alienvault.com/pulse/642d624ccd3a7cca31c9e252?utm_userid=tato1234&utm_medium=InProduct&utm_source=OTX&utm_content=Email&utm_campaign=new_pulse_from_foll...
LevelBlue/Labs
Dashboard
Browse
Scan Endpoints
Create Pulse
Submit Sample
API Integration
All
Search OTX
ISHAN_PAT_
Other (1)
IPv4 (14)
FileHash-MD5 (6)
TYPES OF INDICATORS
File
Edit
View
Ln 2, Col 21
45 characters
100%
Windov
UTF-8
© COPYRIGHT 2024 LEVELBLUE, INC. | LEGAL | STATUS
High winds
In 1 hour
Search
ENG
IN
14:53
6/8/2024

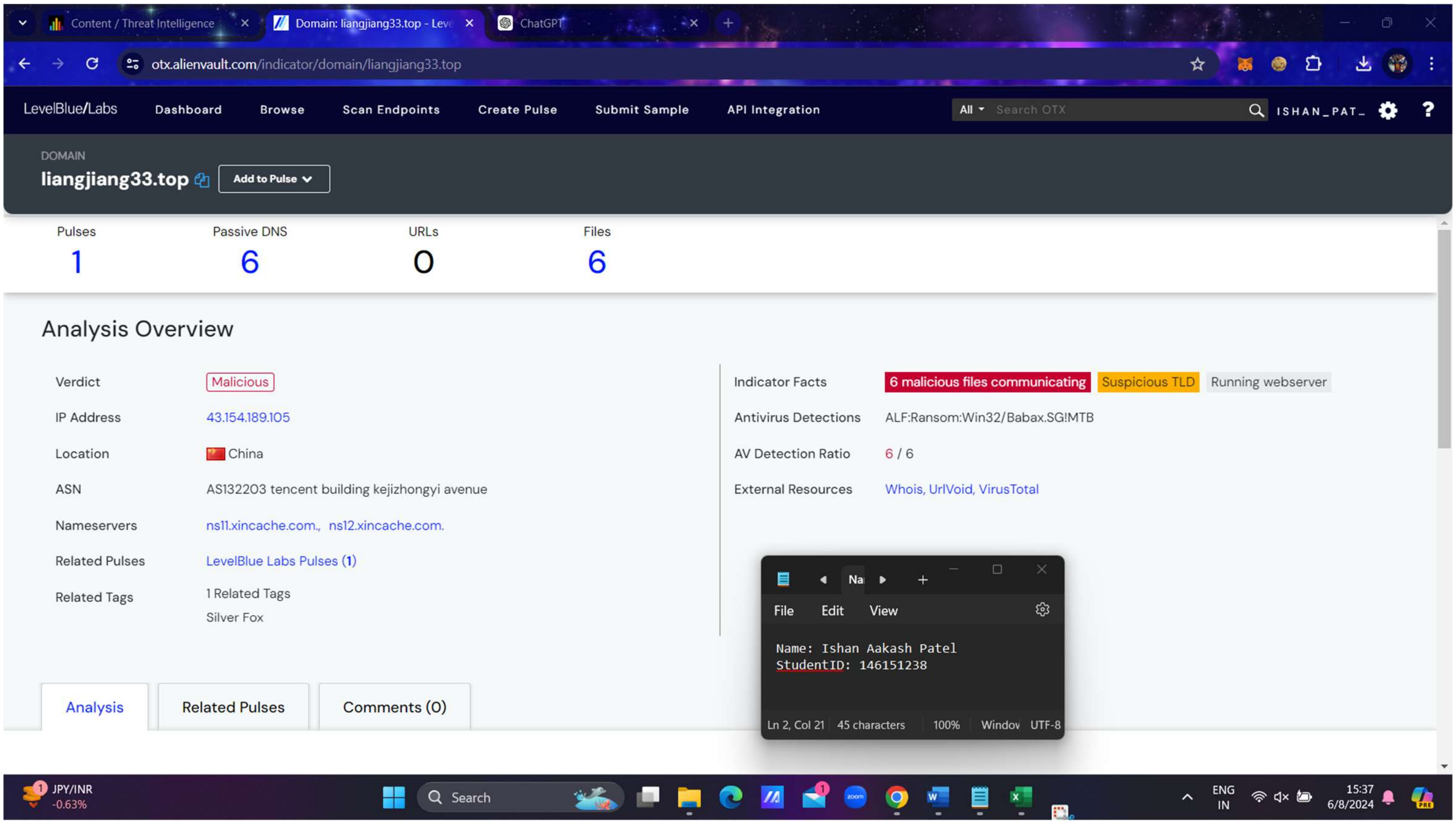
Show 10 entries Search:

| TYPE | INDICATOR | ROLE | TITLE | ADDED | ACTIVE | RELATED PULSES |
|---|---|---|---|---|---|---|
| IPv4 | 154.39.66.37 | command_and_control | PCRat | Apr 5, 2023, 11:58:05 AM | | 3 |
| hostname | vip.qiangsheng888.top | command_and_control | PCRat | Apr 5, 2023, 11:58:05 AM | | 5 |
| IPv4 | 154.211.13.58 | scanning_host | | Apr 5, 2023, 11:58:05 AM | | 1 |
| IPv4 | 180.97.215.92 | scanning_host | | Apr 5, 2023, 11:58:05 AM | | 1 |
| IPv4 | 43.154.239.14 | scanning_host | | Apr 5, 2023, 11:58:05 AM | | 1 |
| FileHash-MD5 | 069d024df8a3965a819b931c71b02788 | | | Apr 5, 2023, 11:58:05 AM | | |
| FileHash-MD5 | 06c75271c589eb60c9b6e34735bfcb13 | | | Apr 5, 2023, 11:58:05 AM | | |
| FileHash-MD5 | 26de0ca4e00dde9432bdcc3652606935 | | GoLandBuildPE | Apr 5, 2023, 11:58:05 AM | | |
| FileHash-MD5 | 2a2f931ae93aa568f664579b12e09db0 | | | Apr 5, 2023, 11:58:05 AM | | |
| FileHash-MD5 | 4901bc83e34b49ee23a5b31e983bb00d | | XOR_embeded_exefile_xored_wit... | Apr 5, 2023, 11:58:05 AM | | |

SHOWING 1 TO 10 OF 35 ENTRIES

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

In the above two screenshots, I simple connected to AlienVault website and started looking into the Indicators. Below I will provide few IOCs details.



DOMAIN

liangjiang33.top

| Pulses | Passive DNS | URLs | Files |
|---|---|---|---|
| 1 | 6 | 0 | 6 |

Analysis Overview

| | |
|---|---|
| Verdict | Malicious |
| IP Address | 43.154.189.105 |
| Location | China |
| ASN | AS132203 tencent building kejizhongyi avenue |
| Nameservers | ns11.xincache.com., ns12.xincache.com. |
| Related Pulses | LevelBlue Labs Pulses (1) |
| Related Tags | 1 Related Tags<br>Silver Fox |

| | |
|---|---|
| Indicator Facts | 6 malicious files communicating<br>Suspicious TLD<br>Running webserver |
| Antivirus Detections | ALF:Ransom:Win32/Babax.SG!MTB |
| AV Detection Ratio | 6 / 6 |
| External Resources | Whois, UrlVoid, VirusTotal |

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Type of Indicator: Domain

Indicator: liangjiang33.top

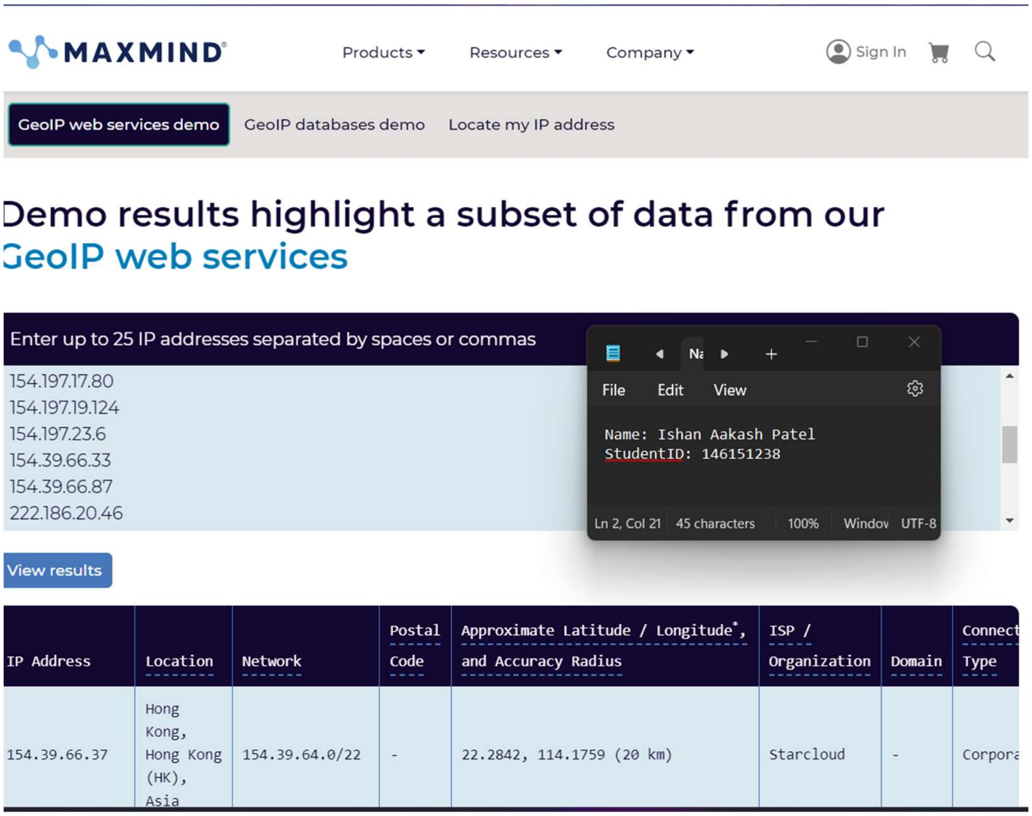
IP address: 43.154.189.105

Location: China

As you can check all the details in the above screenshot of the particular domain. In the same way you can check this for all the domains, IPv4s, hostnames, URLs.

I will attack the updated CSV file with this pdf file which includes all the additional details and it also includes the comparison between MaxWind and AlienVault – Geolocation.

2. Obtain geolocation of  via Maxmind services and compare the versions of geolocation (from AlienVault and MaxMind).



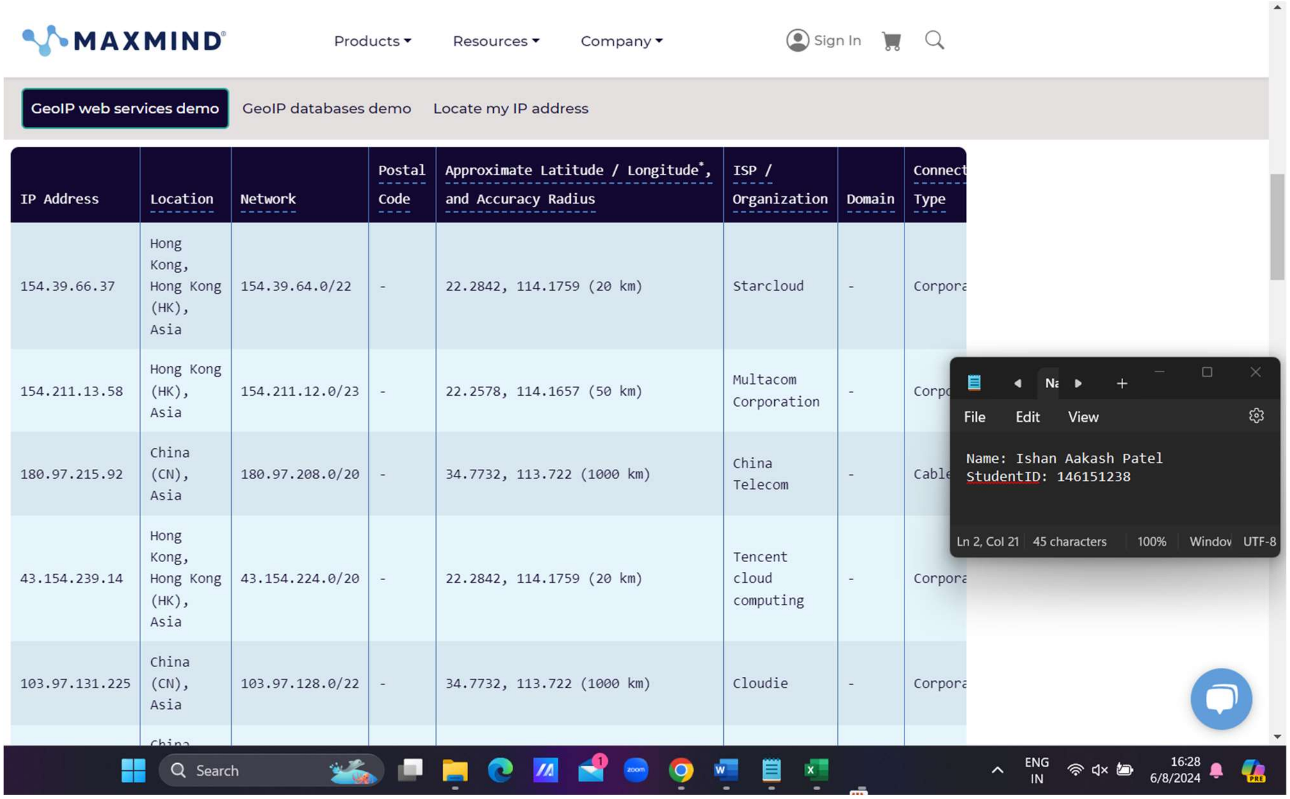
Demo results highlight a subset of data from our GeoIP web services

Enter up to 25 IP addresses separated by spaces or commas

```
154.197.17.80
154.197.19.124
154.197.23.6
154.39.66.33
154.39.66.87
222.186.20.46
```

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

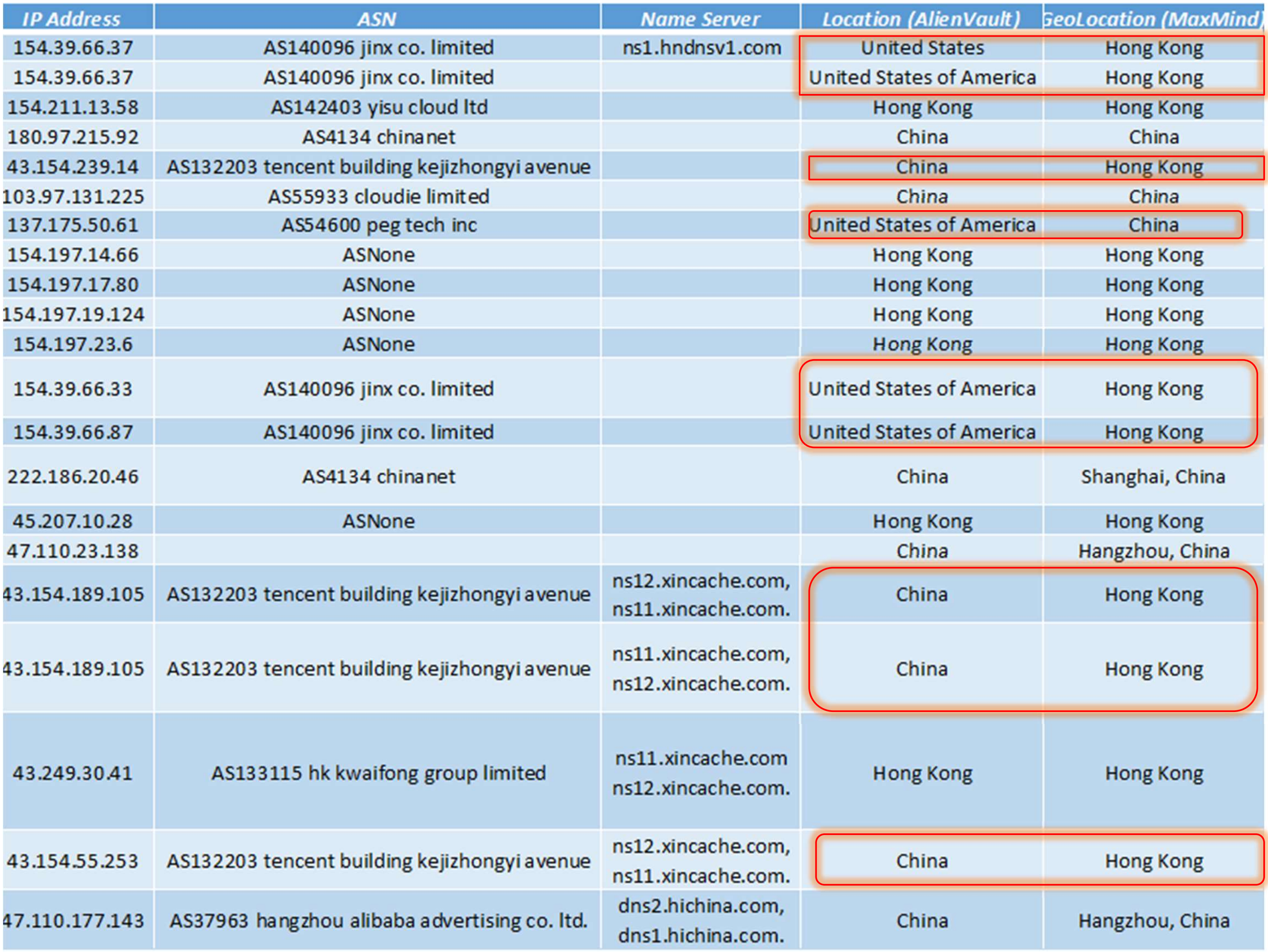
| IP Address | Location | Network | Postal Code | Approximate Latitude / Longitude*, and Accuracy Radius | ISP / Organization | Domain | Connect Type |
|---|---|---|---|---|---|---|---|
| 154.39.66.37 | Hong Kong, Hong Kong (HK), Asia | 154.39.64.0/22 | - | 22.2842, 114.1759 (20 km) | Starcloud | - | Corpora |



| IP Address | Location | Network | Postal Code | Approximate Latitude / Longitude*, and Accuracy Radius | ISP / Organization | Domain | Connect Type |
|---|---|---|---|---|---|---|---|
| 154.39.66.37 | Hong Kong, Hong Kong (HK), Asia | 154.39.64.0/22 | - | 22.2842, 114.1759 (20 km) | Starcloud | - | Corpora |
| 154.211.13.58 | Hong Kong (HK), Asia | 154.211.12.0/23 | - | 22.2578, 114.1657 (50 km) | Multacom Corporation | - | Corp |
| 180.97.215.92 | China (CN), Asia | 180.97.208.0/20 | - | 34.7732, 113.722 (1000 km) | China Telecom | - | Cable |
| 43.154.239.14 | Hong Kong, Hong Kong (HK), Asia | 43.154.224.0/20 | - | 22.2842, 114.1759 (20 km) | Tencent cloud computing | - | Corpora |
| 103.97.131.225 | China (CN), Asia | 103.97.128.0/22 | - | 34.7732, 113.722 (1000 km) | Cloudie | - | Corpora |
|  | China |  |  |  |  |  |  |

```
Name: Ishan Aakash Patel
StudentID: 146151238
```

Comparison – Overall, most the geolocation was the same but there were few differences in few locations and also MaxWind gives you a much more accurate location with Network, Co-oridinates and radius , also Organization it belongs to.



| IP Address | ASN | Name Server | Location (AlienVault) | GeoLocation (MaxMind) |
|---|---|---|---|---|
| 154.39.66.37 | AS140096 jinx co. limited | ns1.hndnsv1.com | United States | Hong Kong |
| 154.39.66.37 | AS140096 jinx co. limited | | United States of America | Hong Kong |
| 154.211.13.58 | AS142403 yisu cloud ltd | | Hong Kong | Hong Kong |
| 180.97.215.92 | AS4134 chinanet | | China | China |
| 43.154.239.14 | AS132203 tencent building kejizhongyi avenue | | China | Hong Kong |
| 103.97.131.225 | AS55933 cloudie limited | | China | China |
| 137.175.50.61 | AS54600 peg tech inc | | United States of America | China |
| 154.197.14.66 | ASNone | | Hong Kong | Hong Kong |
| 154.197.17.80 | ASNone | | Hong Kong | Hong Kong |
| 154.197.19.124 | ASNone | | Hong Kong | Hong Kong |
| 154.197.23.6 | ASNone | | Hong Kong | Hong Kong |
| 154.39.66.33 | AS140096 jinx co. limited | | United States of America | Hong Kong |
| 154.39.66.87 | AS140096 jinx co. limited | | United States of America | Hong Kong |
| 222.186.20.46 | AS4134 chinanet | | China | Shanghai, China |
| 45.207.10.28 | ASNone | | Hong Kong | Hong Kong |
| 47.110.23.138 | | | China | Hangzhou, China |
| 43.154.189.105 | AS132203 tencent building kejizhongyi avenue | ns12.xincache.com,<br>ns11.xincache.com. | China | Hong Kong |
| 43.154.189.105 | AS132203 tencent building kejizhongyi avenue | ns11.xincache.com,<br>ns12.xincache.com. | China | Hong Kong |
| 43.249.30.41 | AS133115 hk kwaifong group limited | ns11.xincache.com<br>ns12.xincache.com. | Hong Kong | Hong Kong |
| 43.154.55.253 | AS132203 tencent building kejizhongyi avenue | ns12.xincache.com,<br>ns11.xincache.com. | China | Hong Kong |
| 47.110.177.143 | AS37963 hangzhou alibaba advertising co. ltd. | dns2.hichina.com,<br>dns1.hichina.com. | China | Hangzhou, China |

I have highlighted the differences above. Once again I will provide the whole csv file with it.