

# Searching and sort in Splunk

Reference: [https://asecuritysite.com/cyberdata/ch13\\_1](https://asecuritysite.com/cyberdata/ch13_1)

1. Let's open up the **broadband.csv** data set. This data setup contains a measurement of the percentages of the Internet connections that achieve a given data rate for different countries

```
| inputlookup broadband.csv
```

Using the broadband.csv dataset, answer the following:

Question	Answer
1. Which country has the largest percentage of 10Mbps broadband?	
2. Which country has the lowest percentage of 10Mbps broadband?	
3. Which country has the largest average speed for broadband?	
4. Which country has the lowest average speed for broadband?	
5. Which country has the largest average peak speed for broadband?	
6. Which country has the highest GDP per head of the population?	
7. Which country has the lowest GDP per head of the population?	
8. Which is country name is the first in the alphabet?	
9. Which is country name is the last in the alphabet?	
10. What is the GDP per capita for Thailand?	
11. In what position is the United Kingdom for average speed?	
12. For the UK and the USA, who has the highest average speed?	

2. Let's open up the internet\_traffic.csv data set. This data set contains the total number of bits sent over an Internet connection. First open up the data, and then select the Visualisation tab, and produce a graph of the data:

```
| inputlookup internet_traffic.csv
```

Using the broadband.csv dataset, answer the following:

Question	Answer
1. What can be said about the profile of the traffic over time?	
2. What is the time interval for the samples?	
3. What was the time for highest bits transferred?	
4. What was the time for lowest bits transferred?	

4. Now where can use the "where" modifier to filter our request. In this case we will filter for Internet connections where the average speed is greater than 6Mbps:

```
| inputlookup broadband.csv where ("Average speed">6)
| reverse
```

Q. Using the broadband.csv dataset, answer the following:

Question	Answer
1. How many countries have an average speed of greater than 6Mbps?	
2. Which country has an average speed of 11.4Mbps?	
3. How many countries have an average speed of less than 2Mbps? Which countries are they?	
4. How many countries have a GDP per capita of less than 5,000? Which countries are they?	
5. For countries with a GDP per capita of less than 5,000, which country has the highest Average speed?	

5. With filtering we can use logical operators. In this case we will find the records with an average speed of greater than 6Mbps and where the GDP per capita is less than 10,000:

```
| inputlookup broadband.csv where ("Average speed">6 AND "GDP per capita"<10000)
| sort "Average speed"
| reverse
```

Now answer the following questions:

Q. Using the broadband.csv dataset, answer the following:

Question	Answer
1. How many countries have an average speed of greater than 6Mbps and an average peak of less than 50Mbps?	
2. How many countries have an average speed of greater than 6Mbps or an average peak of less than 50Mbps?	
3. Which countries have an average speed less than 5Mbps and a GDP per capita of greater than 10,000?	
4. Which countries have an average peak of greater than 20Mbps and a GDP per capita of greater than 50,000?	

5. Which country has over 30% or more for above 15Mbps speeds and where the average speed is greater than 20Mbps?	
---	--