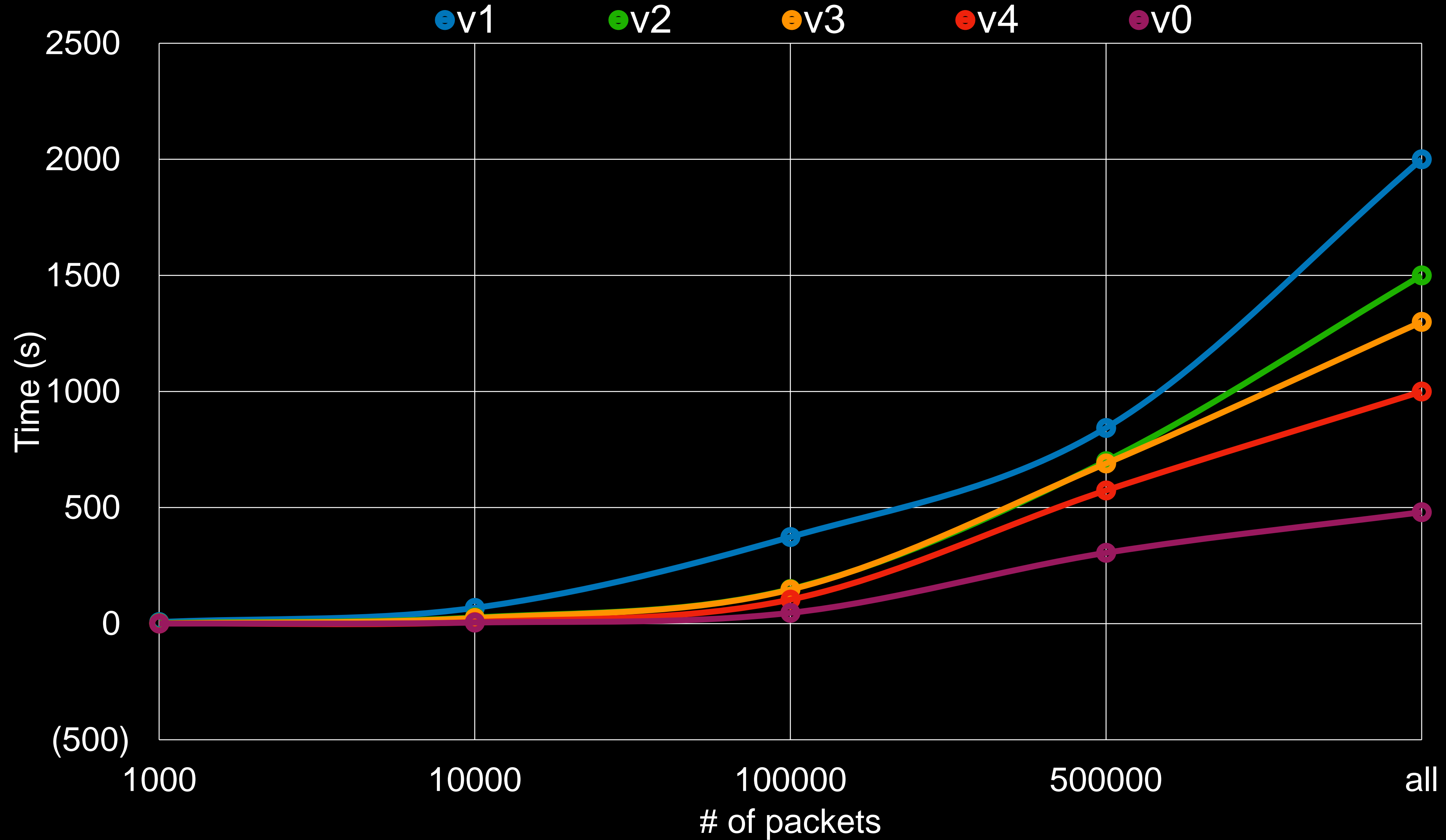


PCAP file analysis

Niccolò Didoni and Francesco Ferrari

Looking for efficiency



- Integration with Python dictionaries
- Direct DataFrame export to .csv format
- Matplotlib support
- Complete documentation

Pandas

DataFrames.

DataFrame

Columns

	Country	Capital	Population
1	Belgium	Brussels	11190846
2	India	New Delhi	1303171035
3	Brazil	Brasilia	207847528

Index

A two-dimensional labeled data structure with columns of potentially different types

```
>>> data = {'Country': ['Belgium', 'India', 'Brazil'],
            'Capital': ['Brussels', 'New Delhi', 'Brasilia'],
            'Population': [11190846, 1303171035, 207847528]}

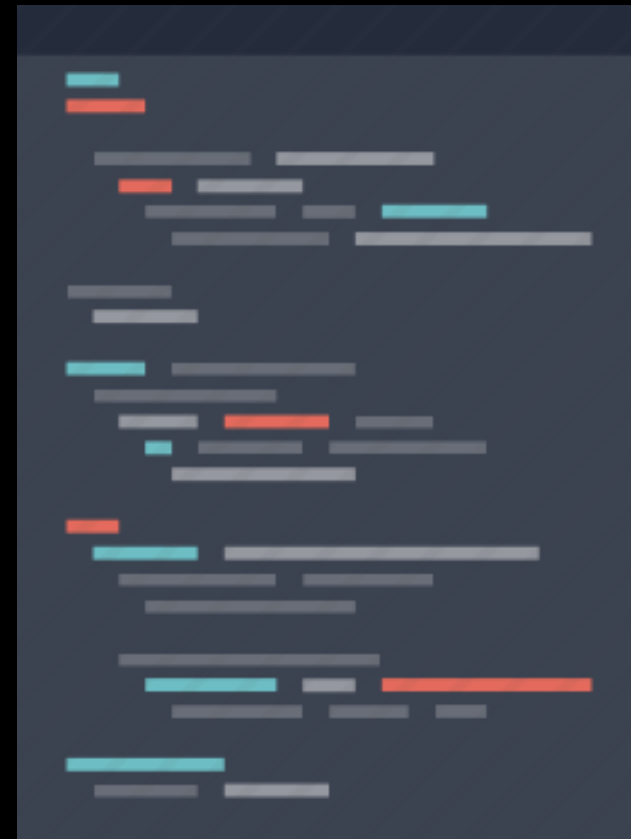
>>> df = pd.DataFrame(data,
                       columns=['Country', 'Capital', 'Population'])
```

Dictionaries

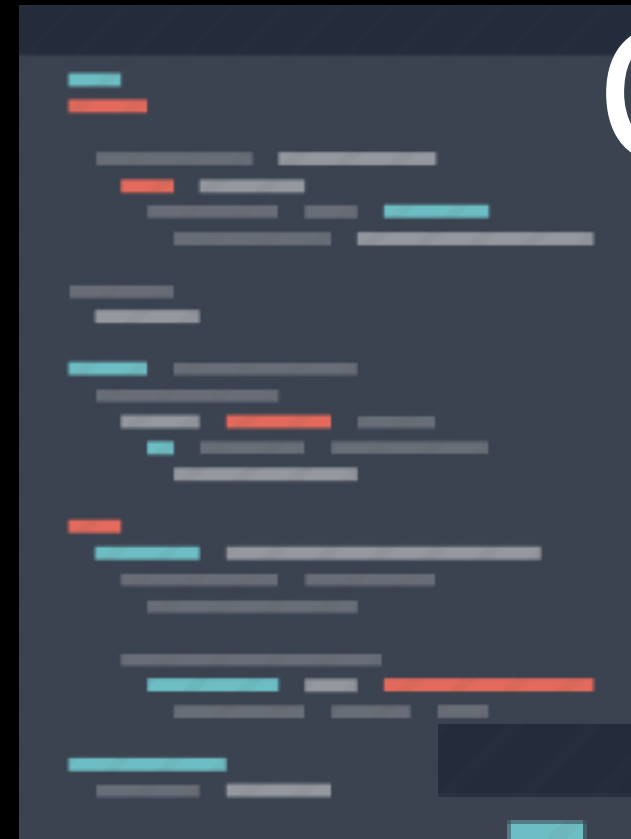
```
class Packet:
    lenght : int
    occurrences : int
    protocol_array : Packet[int, int, int]
    srcPort_array : [[int, int, int]]
    destPort_array : [[int, int, int]]
```

'IP address' {:-}

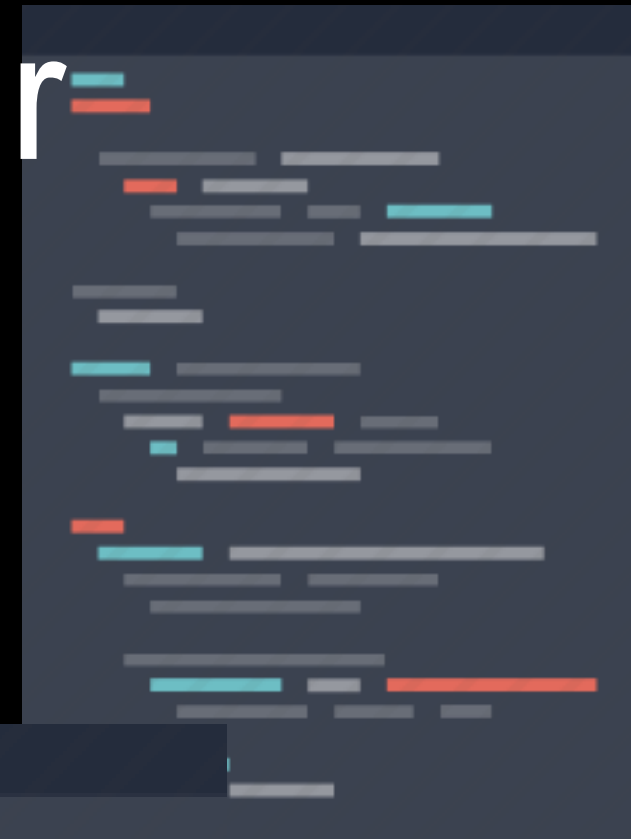
task 1



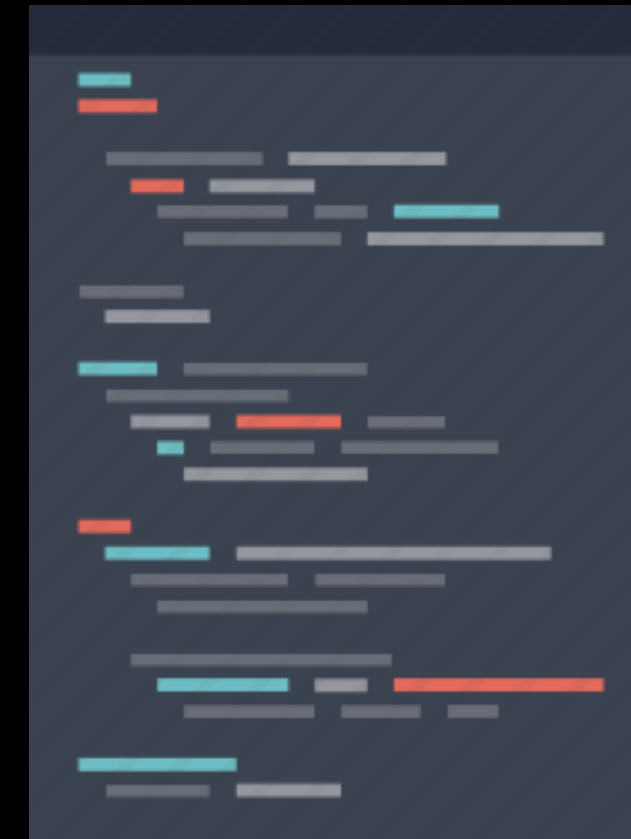
task 2



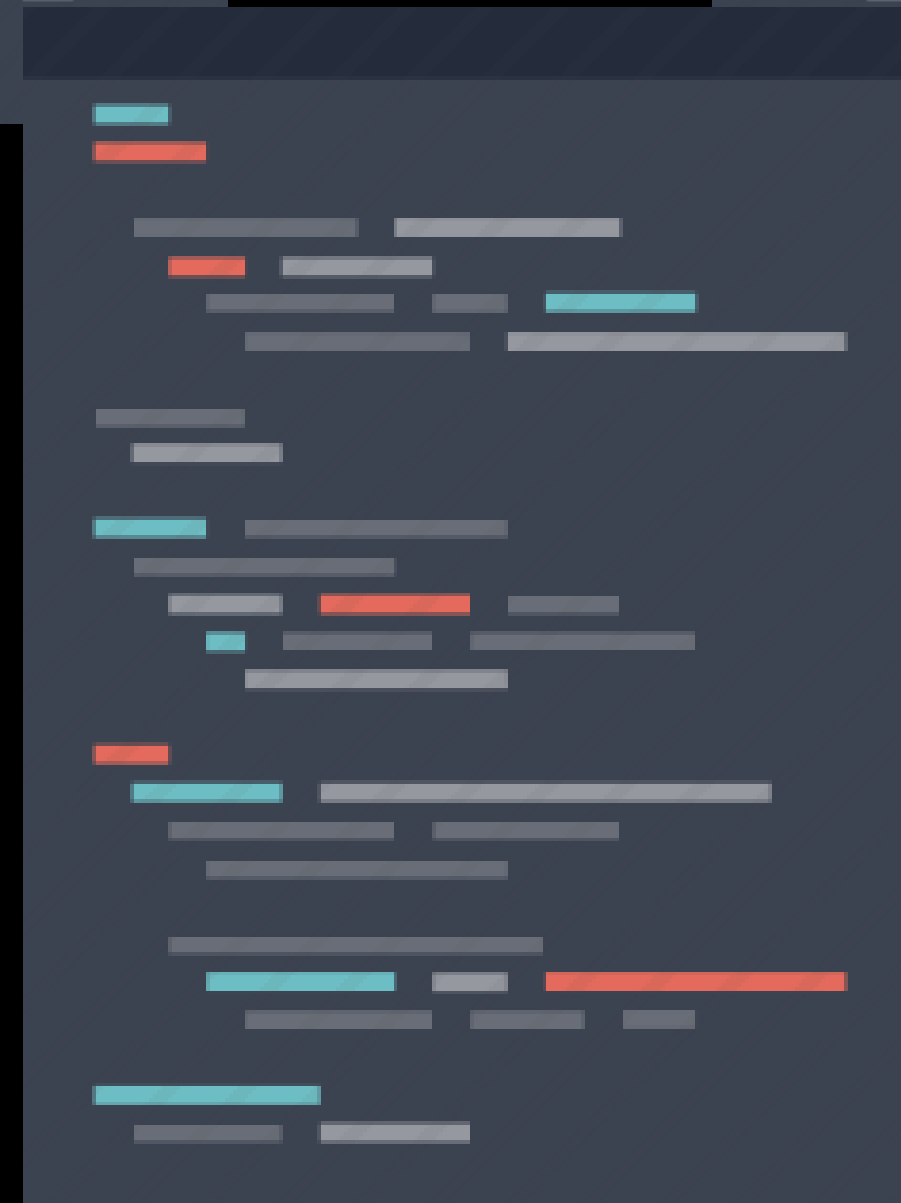
task 3



task 4



Cocker



Cocker

PCAP file analyzer

- **Intuitive terminal interface**
- **Sessions manager**
- **Data export and plotting**
- **Expandability**

```
CCCCCCCCCCCC 00000000 CCCCCCCCCCKKKKKKKK KKKKKKKEEEEEEEEEEEEEEEEEERRRRRRRRRRRRRR
CCC:CCCCCCCC C 00:00:00 CCC:CCCCCCCCCK:K K:KE:ER:R
CC:CCCCCCCC C 00:00:00 CC:CCCCCCCCCK:K K:KE:ER:RRRRR:R
C:CCCCCCCC C 00:00:00 C:CCCCCCCCCK:K K:KEE:EEEEEEEE:ERR:R R:R
C:CCCCCCCC C 00:00:00 C:CCCCCCCCCK:K K:KKK E:E EEEEE R:R R:R
C:CCCCCCCC C 00:00:00 C:CCCCCCCCCK:K K:K K:K E:E R:R R:R
C:CCCCCCCC C 00:00:00 C:CCCCCCCCCK:K K:K:K E:EEEEEEEE R:RRRRR:R
C:CCCCCCCC C 00:00:00 C:CCCCCCCCCK:K K:K E:EEEEEEEE R:RRRRR:R
C:CCCCCCCC C 00:00:00 C:CCCCCCCCCK:K K:K:K E:EEEEEEEE R:R R:R
C:CCCCCCCC C 00:00:00 C:CCCCCCCCCK:K K:K K:K E:E R:R R:R
C:CCCCCCCC C 00:00:00 C:CCCCCCCCCK:K K:K:K E:EEEEEEEE:ERR:R R:R
CC:CCCCCCCC C 00:00:00 CC:CCCCCCCCCK:K K:KE:ER:R R:R
CCC:CCCCCCCC C 00:00:00 CCC:CCCCCCCCCK:K K:KE:ER:R R:R
CCCCCCCCCCCC 00000000 CCCCCCCCCCKKKKKKKK KKKKKKKEEEEEEEEEEEEEEEEEERRRRRRRR RRRRRR

WEELCOME TO COCKER
here's a list of useful commands
getport
getip
gettll
help to see these and other commands

$$$ getip -v
```