APT Install: package mgr confirmed installed

```
analyst@99857b9c00ba:~$ apt
apt 2.2.4 (amd64)
Usage: apt [options] command

apt is a commandline package manager and provides commands for
searching and managing as well as querying information about packages.
It provides the same functionality as the specialized APT tools,
like apt-get and apt-cache, but enables options more suitable for
interactive use by default.

Most used commands:
  list - list packages based on package names
  search - search in package descriptions
  show - show package details
  install - install packages
  reinstall - reinstall packages
  remove - remove packages
  autoremove - Remove automatically all unused packages
  update - update list of available packages
  upgrade - upgrade the system by installing/upgrading packages
  full-upgrade - upgrade the system by removing/installing/upgrading packages
  edit-sources - edit the source information file
  satisfy - satisfy dependency strings
```

Now installing Suricata (network analyzing tool)

```
analyst@99857b9c00ba:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7
  libhiredis0.14 libhtp2 libhyperscan5 libjansson4 libluajit-5.1-2
  libluajit-5.1-common libmagic-mgc libmagic1 libmaxminddb0 libmnl0 libnet1
  libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8
  libyaml-0-2 python3-simplejson python3-yaml suricata-update
Suggested packages:
  file mmdb-bin libtcmalloc-minimal4
Recommended packages:
  snort-rules-default
The following NEW packages will be installed:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7
  libhiredis0.14 libhtp2 libhyperscan5 libjansson4 libluajit-5.1-2
  libluajit-5.1-common libmagic-mgc libmagic1 libmaxminddb0 libmnl0 libnet1
  libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8
  libyaml-0-2 python3-simplejson python3-yaml suricata suricata-update
0 upgraded, 27 newly installed, 0 to remove and 0 not upgraded.
Need to get 7961 kB of archives.
```

Successfully installed

```
analyst@99857b9c00ba:~$ suricata
Suricata 6.0.1
USAGE: suricata [OPTIONS] [BPF FILTER]

        -c <path>                               : path to configuration file
        -T                                      : test configuration file (use with -c)
        -i <dev or ip>                          : run in pcap live mode
        -F <bpf filter file>                    : bpf filter file
        -r <path>                               : run in pcap file/offline mode
        -q <qid[:qid]>                          : run in inline nfqueue mode (use colon
to specify a range of queues)
        -s <path>                               : path to signature file loaded in addit
```

Now to remove it. Successfully removed:

```
analyst@99857b9c00ba:~$ sudo apt remove suricata
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7
  libhiredis0.14 libhtp2 libhyperscan5 libjansson4 libluajit-5.1-2
  libluajit-5.1-common libmagic-mgc libmagic1 libmaxminddb0 libmnl0 libnet1
  libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8
  libyaml-0-2 python3-simplejson python3-yaml suricata-update
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  suricata
0 upgraded, 0 newly installed, 1 to remove and 0 not upgraded.
After this operation, 6634 kB disk space will be freed.
Do you want to continue? [Y/n] y
(Reading database ... 23406 files and directories currently installed.)
Removing suricata (1:6.0.1-3+deb11u1) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for man-db (2.9.4-2) ...
analyst@99857b9c00ba:~$ suricata
-bash: /usr/bin/suricata: No such file or directory
analyst@99857b9c00ba:~$
```

Now installing tcpdump:

```
analyst@99857b9c00ba:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libbpf0 libelf1 libevent-2.1-7 libevent-core-2.1-7 libevent-pthreads-2.1-7
  libhiredis0.14 libhtp2 libhyperscan5 libjansson4 libluajit-5.1-2
  libluajit-5.1-common libmagic-mgc libmagic1 libmaxminddb0 libmnl0 libnet1
  libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libyaml-0-2
  python3-simplejson python3-yaml suricata-update
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  apparmor
The following NEW packages will be installed:
  tcpdump
```

Successfully installed:

```
analyst@99857b9c00ba:~$ apt list --installed
Listing... Done
adduser/oldstable,now 3.118+deb11u1 all [installed,automatic]
apt/oldstable,now 2.2.4 amd64 [installed,automatic]
```

```
tar/oldstable,now 1.34+dfsg-1+deb11u1 amd64 [installed,automatic]
tcpdump/oldstable,now 4.99.0-2+deb11u1 amd64 [installed]
tree/oldstable,now 1.8.0-1+b1 amd64 [installed]
```

Now to remove tcpdump:

```
analyst@99857b9c00ba:~$ sudo apt remove tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  tcpdump
```

Successfully removed:

```
analyst@99857b9c00ba:~$ tcpdump
-bash: /usr/bin/tcpdump: No such file or directory
```