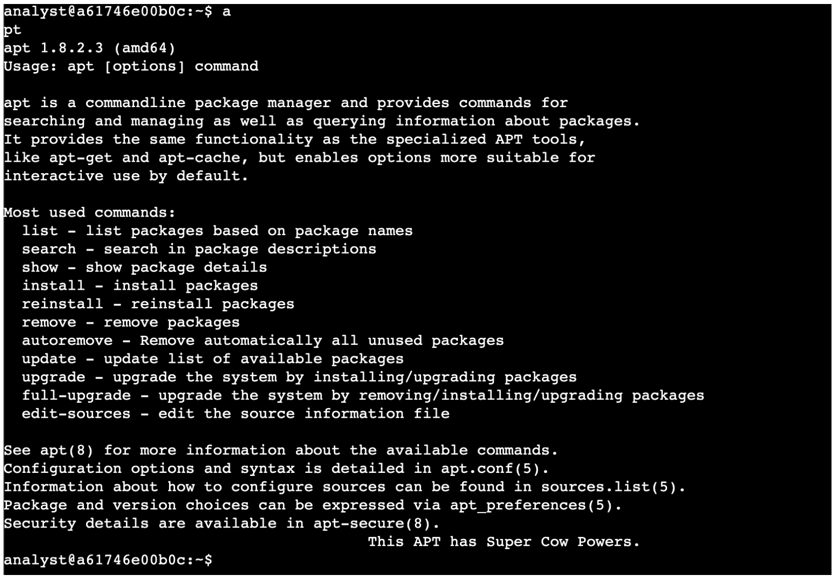
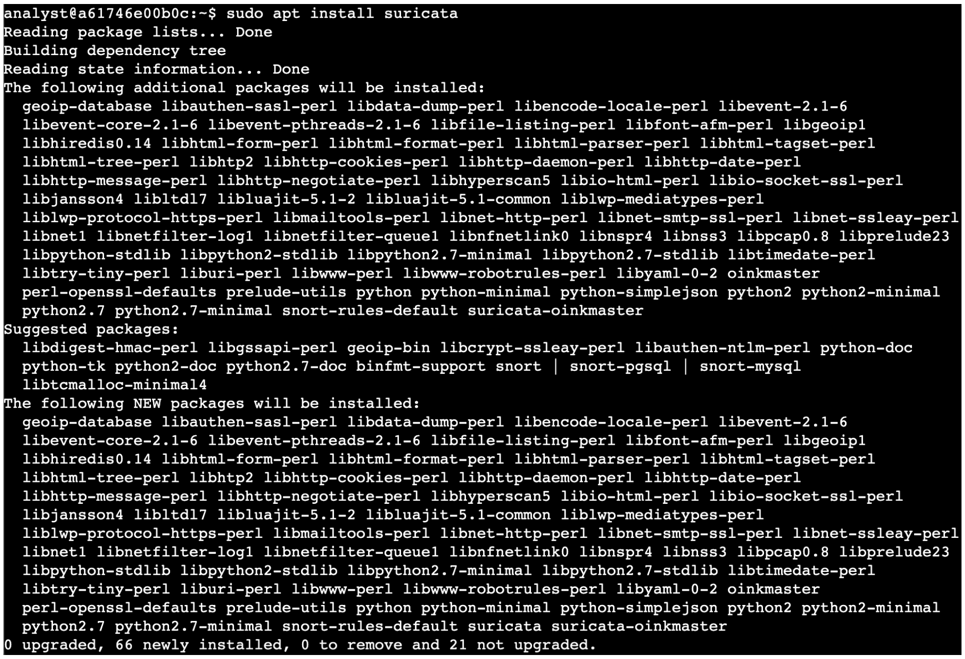
Installing Software in a Linux Distribution - Juan Cardenas

1. Confirmed APT packet manager is installed in Linux environment



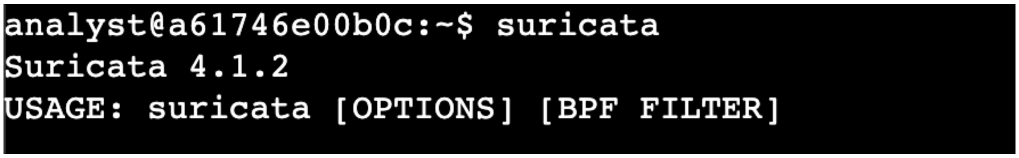
```
analyst@a61746e00b0c:~$ a
pt
apt 1.8.2.3 (amd64)
Usage: apt [options] command

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

See apt(8) for more information about the available commands.
Configuration options and syntax is detailed in apt.conf(5).
Information about how to configure sources can be found in sources.list(5).
Package and version choices can be expressed via apt_preferences(5).
Security details are available in apt-secure(8).
                                        This APT has Super Cow Powers.
analyst@a61746e00b0c:~$
```

2. Installed suricata application



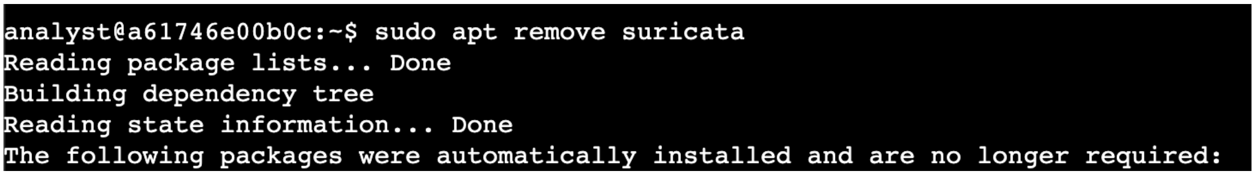
```
analyst@a61746e00b0c:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  geoip-database libauthen-sasl-perl libdata-dump-perl libencode-locale-perl libevent-2.1-6
  libevent-core-2.1-6 libevent-pthreads-2.1-6 libfile-listing-perl libfont-afm-perl libgeoip1
  libhiredis0.14 libhtml-form-perl libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl
  libhtml-tree-perl libhtp2 libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libhttp-negotiate-perl libhyperscan5 libio-html-perl libio-socket-ssl-perl
  libjansson4 libltdl7 libluajit-5.1-2 libluajit-5.1-common liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl libnet-ssleay-perl
  libnet1 libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8 libprelude23
  libpython-stdlib libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib libtimedate-perl
  libtry-tiny-perl liburi-perl libwww-perl libwww-robotrules-perl libyaml-0-2 oinkmaster
  perl-openssl-defaults prelude-utils python python-minimal python-simplejson python2 python2-minimal
  python2.7 python2.7-minimal snort-rules-default suricata-oinkmaster
Suggested packages:
  libdigest-hmac-perl libgssapi-perl geoip-bin libcrypt-ssleay-perl libauthen-ntlm-perl python-doc
  python-tk python2-doc python2.7-doc binfmt-support snort | snort-pgsql | snort-mysql
  libtcmalloc-minimal4
The following NEW packages will be installed:
  geoip-database libauthen-sasl-perl libdata-dump-perl libencode-locale-perl libevent-2.1-6
  libevent-core-2.1-6 libevent-pthreads-2.1-6 libfile-listing-perl libfont-afm-perl libgeoip1
  libhiredis0.14 libhtml-form-perl libhtml-format-perl libhtml-parser-perl libhtml-tagset-perl
  libhtml-tree-perl libhtp2 libhttp-cookies-perl libhttp-daemon-perl libhttp-date-perl
  libhttp-message-perl libhttp-negotiate-perl libhyperscan5 libio-html-perl libio-socket-ssl-perl
  libjansson4 libltdl7 libluajit-5.1-2 libluajit-5.1-common liblwp-mediatypes-perl
  liblwp-protocol-https-perl libmailtools-perl libnet-http-perl libnet-smtp-ssl-perl libnet-ssleay-perl
  libnet1 libnetfilter-log1 libnetfilter-queue1 libnfnetlink0 libnspr4 libnss3 libpcap0.8 libprelude23
  libpython-stdlib libpython2-stdlib libpython2.7-minimal libpython2.7-stdlib libtimedate-perl
  libtry-tiny-perl liburi-perl libwww-perl libwww-robotrules-perl libyaml-0-2 oinkmaster
  perl-openssl-defaults prelude-utils python python-minimal python-simplejson python2 python2-minimal
  python2.7 python2.7-minimal snort-rules-default suricata suricata-oinkmaster
0 upgraded, 66 newly installed, 0 to remove and 21 not upgraded.
```

3. Verified Suricata is installed



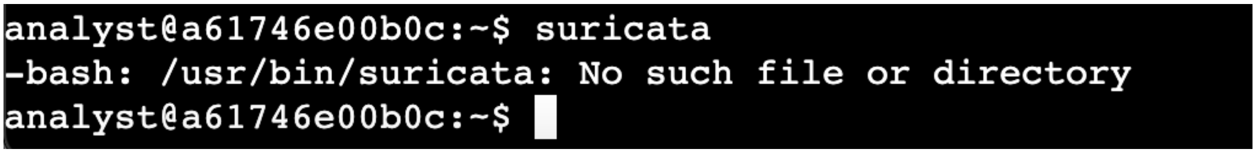
```
analyst@a61746e00b0c:~$ suricata
Suricata 4.1.2
USAGE: suricata [OPTIONS] [BPF FILTER]
```

4. Used apt packet manager to uninstall suricata



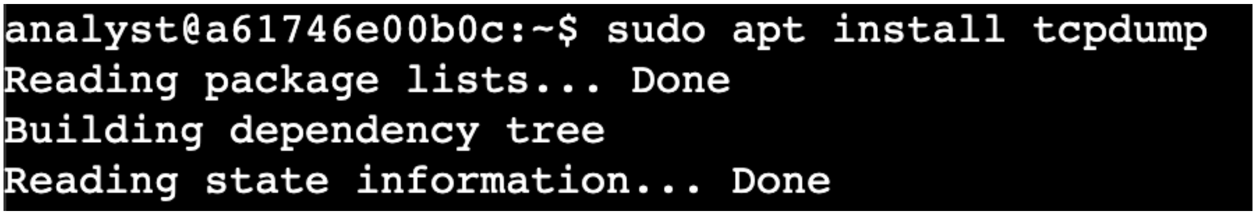
```
analyst@a61746e00b0c:~$ sudo apt remove suricata
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
```

5. Verified Suricata has been uninstalled



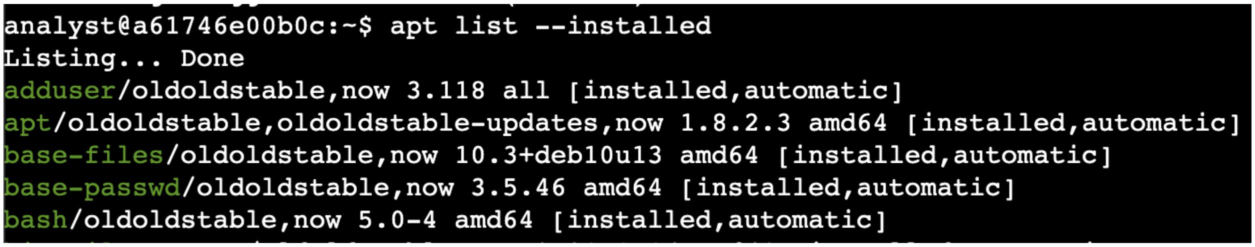
```
analyst@a61746e00b0c:~$ suricata
-bash: /usr/bin/suricata: No such file or directory
analyst@a61746e00b0c:~$
```

6. Installed Tcpdump



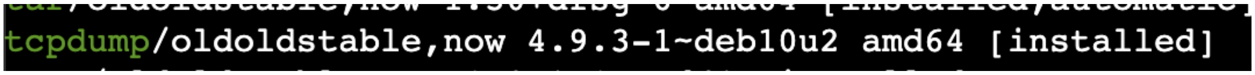
```
analyst@a61746e00b0c:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
```

7. Used APT packet manager to list all applications



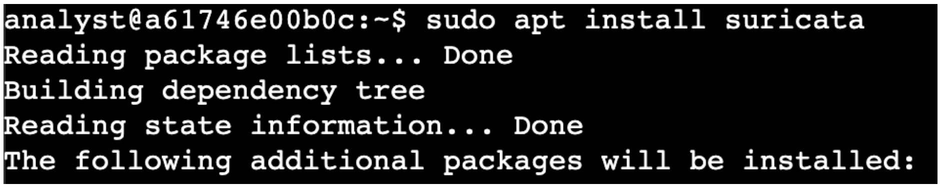
```
analyst@a61746e00b0c:~$ apt list --installed
Listing... Done
adduser/oldoldstable,now 3.118 all [installed,automatic]
apt/oldoldstable,oldoldstable-updates,now 1.8.2.3 amd64 [installed,automatic]
base-files/oldoldstable,now 10.3+deb10u13 amd64 [installed,automatic]
base-passwd/oldoldstable,now 3.5.46 amd64 [installed,automatic]
bash/oldoldstable,now 5.0-4 amd64 [installed,automatic]
```

8. Verified tcpdump is in the list



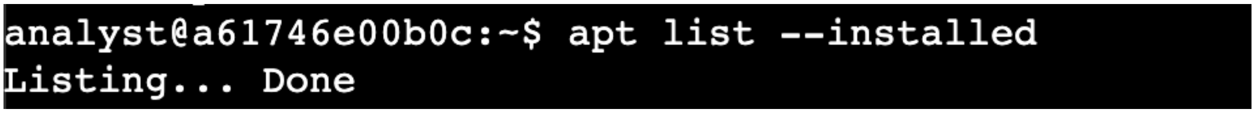
```
tcpdump/oldoldstable,now 4.9.3-1~deb10u2 amd64 [installed]
```

9. Reinstalled Suricata

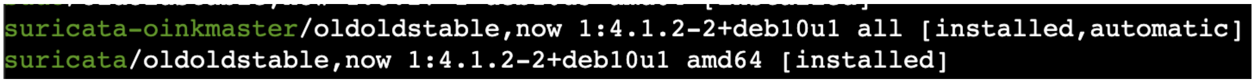


```
analyst@a61746e00b0c:~$ sudo apt install suricata
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
```

10. Verified Suricata is installed



```
analyst@a61746e00b0c:~$ apt list --installed
Listing... Done
```



```
suricata-oinkmaster/oldoldstable,now 1:4.1.2-2+deb10u1 all [installed,automatic]
suricata/oldoldstable,now 1:4.1.2-2+deb10u1 amd64 [installed]
```