

Task 1. Ensure that APT is installed

```
analyst@6b6b1e9a0d5d:~$ apt
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.
```

Task 2. Install and uninstall the Suricata application

```
analyst@6b6b1e9a0d5d:~$ 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 libhttp2 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 liblua5.1-2 liblua5.1-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 libhttp2 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 liblua5.1-2 liblua5.1-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
```

```

analyst@6b6b1e9a0d5d:~$ 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:
  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 libhttp2 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 liblua5.1-2 liblua5.1-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
Use 'sudo apt autoremove' to remove them.
The following packages will be REMOVED:
  suricata suricata-oinkmaster
0 upgraded, 0 newly installed, 2 to remove and 34 not upgraded.
After this operation, 5298 kB disk space will be freed.
Do you want to continue? [Y/n]
(Reading database ... 24795 files and directories currently installed.)
Removing suricata-oinkmaster (1:4.1.2-2+deb10u1) ...
Removing suricata (1:4.1.2-2+deb10u1) ...
invoke-rc.d: could not determine current runlevel
invoke-rc.d: policy-rc.d denied execution of stop.
Processing triggers for man-db (2.8.5-2) ...

```

Task 3. Install the tcpdump application

```

analyst@6b6b1e9a0d5d:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  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 libhttp2 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 liblua5.1-2 liblua5.1-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
  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
Use 'sudo apt autoremove' to remove them.
Suggested packages:
  apparmor
The following NEW packages will be installed:
  tcpdump
0 upgraded, 1 newly installed, 0 to remove and 34 not upgraded.
Need to get 400 kB of archives.

```

Task 4. List the installed application

```
analyst@6b6ble9a0d5d:~$ 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]
binutils-common/oldoldstable,now 2.31.1-16 amd64 [installed,automatic]
binutils-x86-64-linux-gnu/oldoldstable,now 2.31.1-16 amd64 [installed,automatic]
binutils/oldoldstable,now 2.31.1-16 amd64 [installed,automatic]
bsdmainutils/oldoldstable,now 11.1.2+b1 amd64 [installed,automatic]
bsdutils/oldoldstable,now 1:2.33.1-0.1 amd64 [installed,automatic]
build-essential/oldoldstable,now 12.6 amd64 [installed,automatic]
bzip2/oldoldstable,now 1.0.6-9.2~deb10u2 amd64 [installed,automatic]
ca-certificates/oldoldstable,oldoldstable-updates,now 20200601~deb10u2 all [installed,automatic]
coreutils/oldoldstable,now 8.30-3 amd64 [installed,automatic]
cpp-8/oldoldstable,now 8.3.0-6 amd64 [installed,automatic]
cpp/oldoldstable,now 4:8.3.0-1 amd64 [installed,automatic]
dash/oldoldstable,now 0.5.10.2-5 amd64 [installed,automatic]
dbus/oldoldstable,now 1.12.24-0+deb10u1 amd64 [installed,automatic]
debconf/oldoldstable,now 1.5.71+deb10u1 all [installed,automatic]
debian-archive-keyring/oldoldstable,now 2019.1+deb10u1 all [installed,upgradable to: 2019.1+deb10u2]
debianutils/oldoldstable,now 4.8.6.1 amd64 [installed,automatic]
dh-python/oldoldstable,now 3.20190308 all [installed,automatic]
diffutils/oldoldstable,now 1:3.7-3 amd64 [installed,automatic]
dirmngr/oldoldstable,oldoldstable,now 2.2.12-1+deb10u2 amd64 [installed,automatic]
dmsetup/oldoldstable,now 2:1.02.155-3 amd64 [installed,automatic]
```