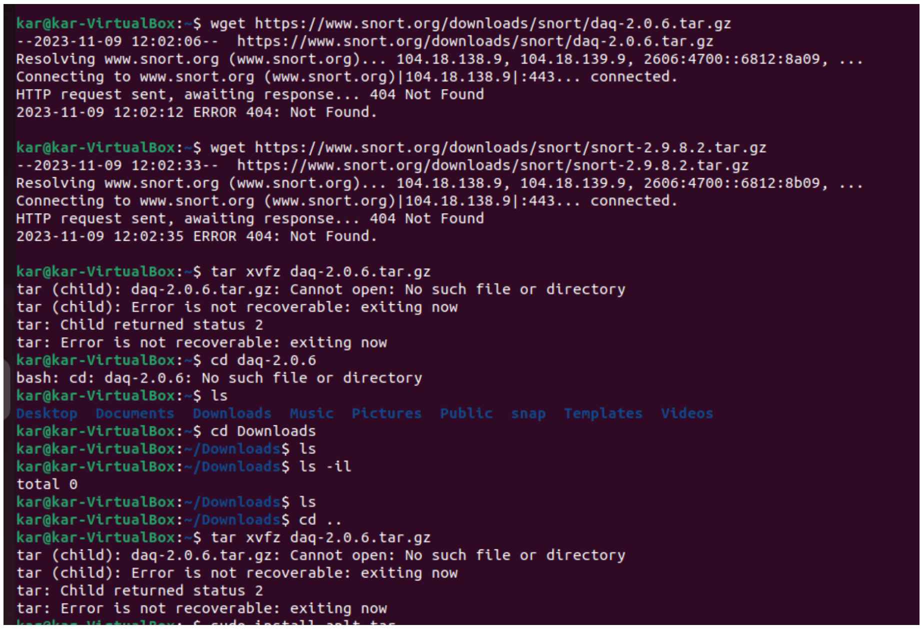
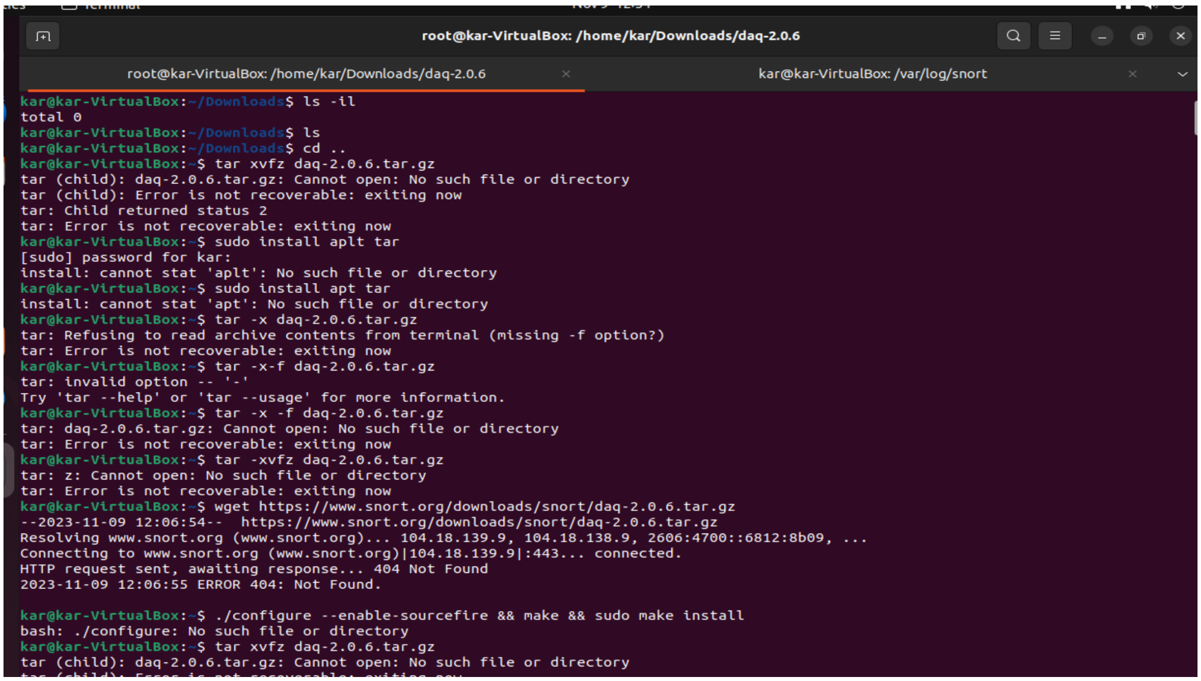
Snort tool

Installing Snort into the Operating System

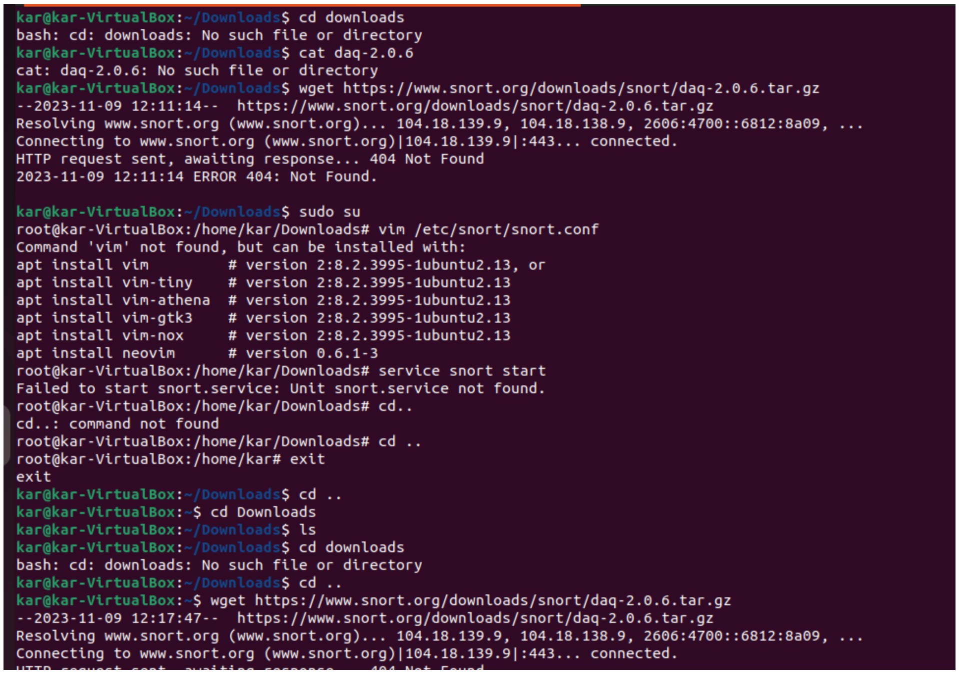


```
kar@kar-VirtualBox:~$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:02:06--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:02:12 ERROR 404: Not Found.

kar@kar-VirtualBox:~$ wget https://www.snort.org/downloads/snort/snort-2.9.8.2.tar.gz
--2023-11-09 12:02:33--  https://www.snort.org/downloads/snort/snort-2.9.8.2.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8b09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:02:35 ERROR 404: Not Found.

kar@kar-VirtualBox:~$ tar xvfz daq-2.0.6.tar.gz
tar (child): daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ cd daq-2.0.6
bash: cd: daq-2.0.6: No such file or directory
kar@kar-VirtualBox:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
kar@kar-VirtualBox:~$ cd Downloads
kar@kar-VirtualBox:~/Downloads$ ls
kar@kar-VirtualBox:~/Downloads$ ls -il
total 0
kar@kar-VirtualBox:~/Downloads$ ls
kar@kar-VirtualBox:~/Downloads$ cd ..
kar@kar-VirtualBox:~$ tar xvfz daq-2.0.6.tar.gz
tar (child): daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ sudo install aplt tar
```



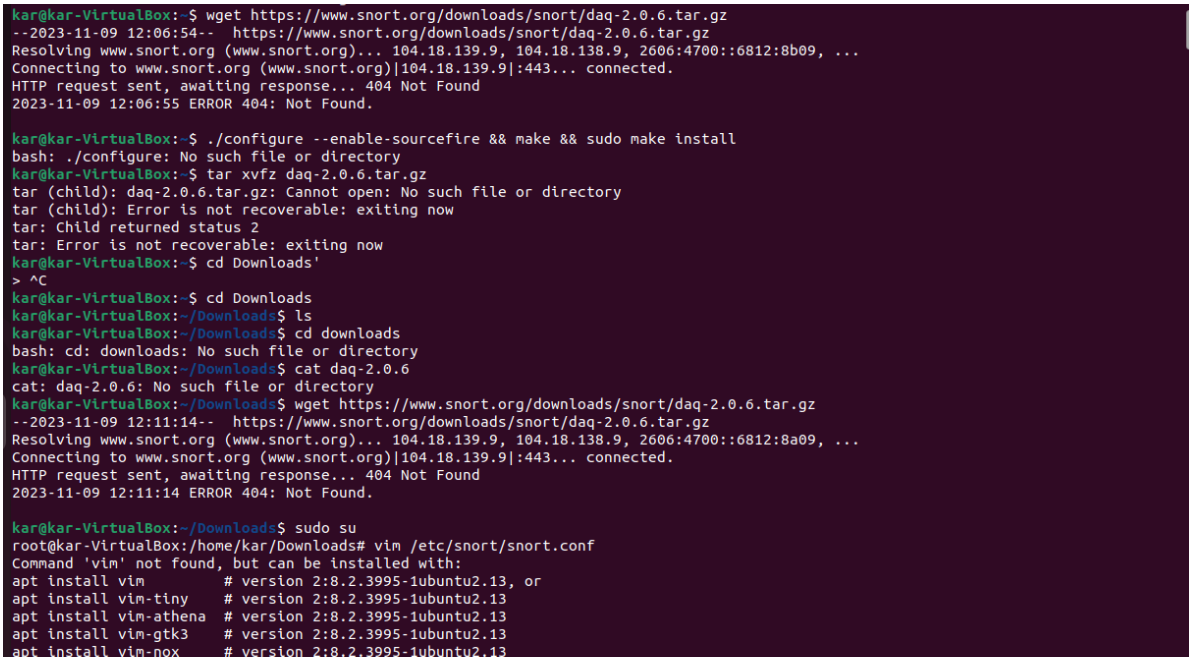
Terminal
Nov 9 12:54
root@kar-VirtualBox: /home/kar/Downloads/daq-2.0.6
root@kar-VirtualBox: /home/kar/Downloads/daq-2.0.6
kar@kar-VirtualBox: /var/log/snort

```
kar@kar-VirtualBox:~/Downloads$ ls -il
total 0
kar@kar-VirtualBox:~/Downloads$ ls
kar@kar-VirtualBox:~/Downloads$ cd ..
kar@kar-VirtualBox:~$ tar xvfz daq-2.0.6.tar.gz
tar (child): daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ sudo install aplt tar
[sudo] password for kar:
install: cannot stat 'aplt': No such file or directory
kar@kar-VirtualBox:~$ sudo install apt tar
install: cannot stat 'apt': No such file or directory
kar@kar-VirtualBox:~$ tar -x daq-2.0.6.tar.gz
tar: Refusing to read archive contents from terminal (missing -f option?)
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ tar -x-f daq-2.0.6.tar.gz
tar: invalid option -- '-'
Try 'tar --help' or 'tar --usage' for more information.
kar@kar-VirtualBox:~$ tar -x -f daq-2.0.6.tar.gz
tar: daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ tar -xvfz daq-2.0.6.tar.gz
tar: z: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:06:54--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8b09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:06:55 ERROR 404: Not Found.

kar@kar-VirtualBox:~$ ./configure --enable-sourcefire && make && sudo make install
bash: ./configure: No such file or directory
kar@kar-VirtualBox:~$ tar xvfz daq-2.0.6.tar.gz
tar (child): daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
```

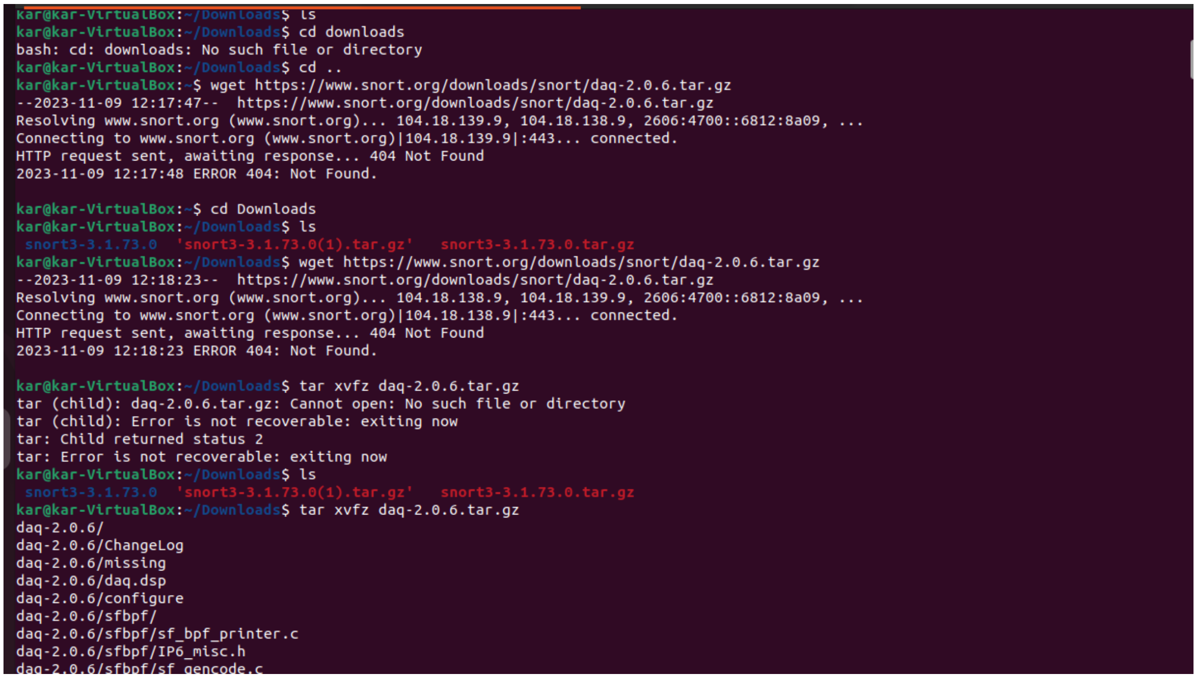


```
kar@kar-VirtualBox:~/Downloads$ cd downloads
bash: cd: downloads: No such file or directory
kar@kar-VirtualBox:~/Downloads$ cat daq-2.0.6
cat: daq-2.0.6: No such file or directory
kar@kar-VirtualBox:~/Downloads$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:11:14--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:11:14 ERROR 404: Not Found.

kar@kar-VirtualBox:~/Downloads$ sudo su
root@kar-VirtualBox:/home/kar/Downloads# vim /etc/snort/snort.conf
Command 'vim' not found, but can be installed with:
apt install vim         # version 2:8.2.3995-1ubuntu2.13, or
apt install vim-tiny    # version 2:8.2.3995-1ubuntu2.13
apt install vim-athena  # version 2:8.2.3995-1ubuntu2.13
apt install vim-gtk3    # version 2:8.2.3995-1ubuntu2.13
apt install vim-nox     # version 2:8.2.3995-1ubuntu2.13
apt install neovim      # version 0.6.1-3
root@kar-VirtualBox:/home/kar/Downloads# service snort start
Failed to start snort.service: Unit snort.service not found.
root@kar-VirtualBox:/home/kar/Downloads# cd..
cd..: command not found
root@kar-VirtualBox:/home/kar/Downloads# cd ..
root@kar-VirtualBox:/home/kar# exit
exit
kar@kar-VirtualBox:~/Downloads$ cd ..
kar@kar-VirtualBox:~$ cd Downloads
kar@kar-VirtualBox:~/Downloads$ ls
kar@kar-VirtualBox:~/Downloads$ cd downloads
bash: cd: downloads: No such file or directory
kar@kar-VirtualBox:~/Downloads$ cd ..
kar@kar-VirtualBox:~$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:17:47--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
```

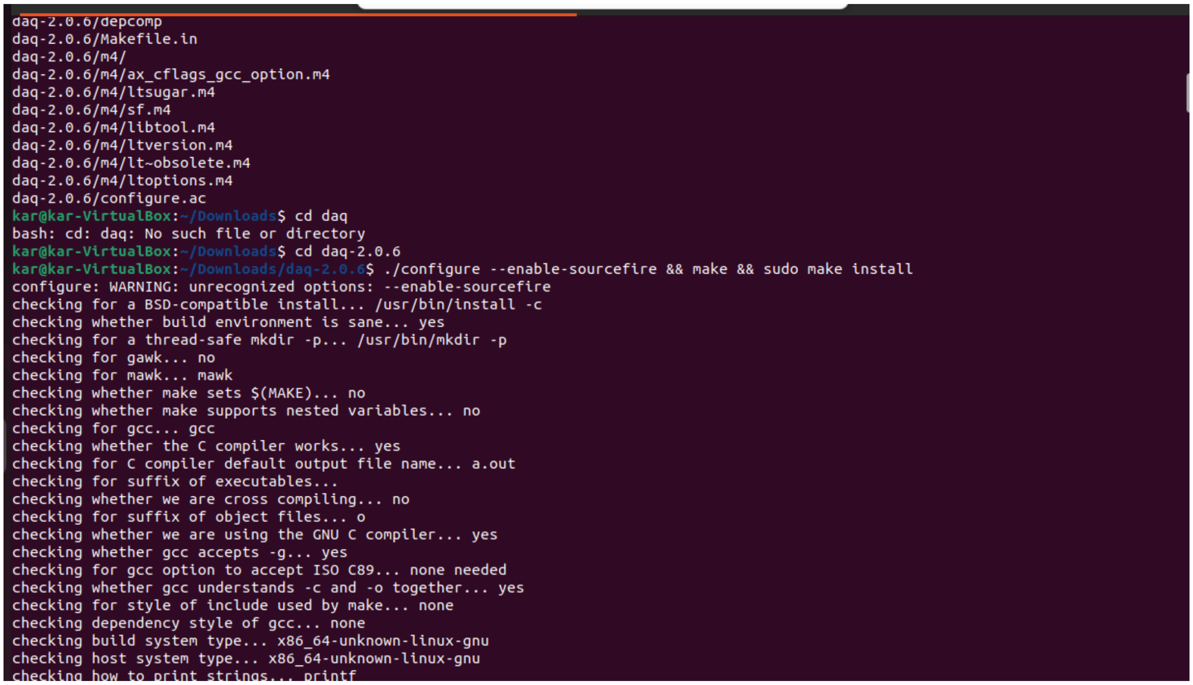
Configuring and Starting the Snort IDS



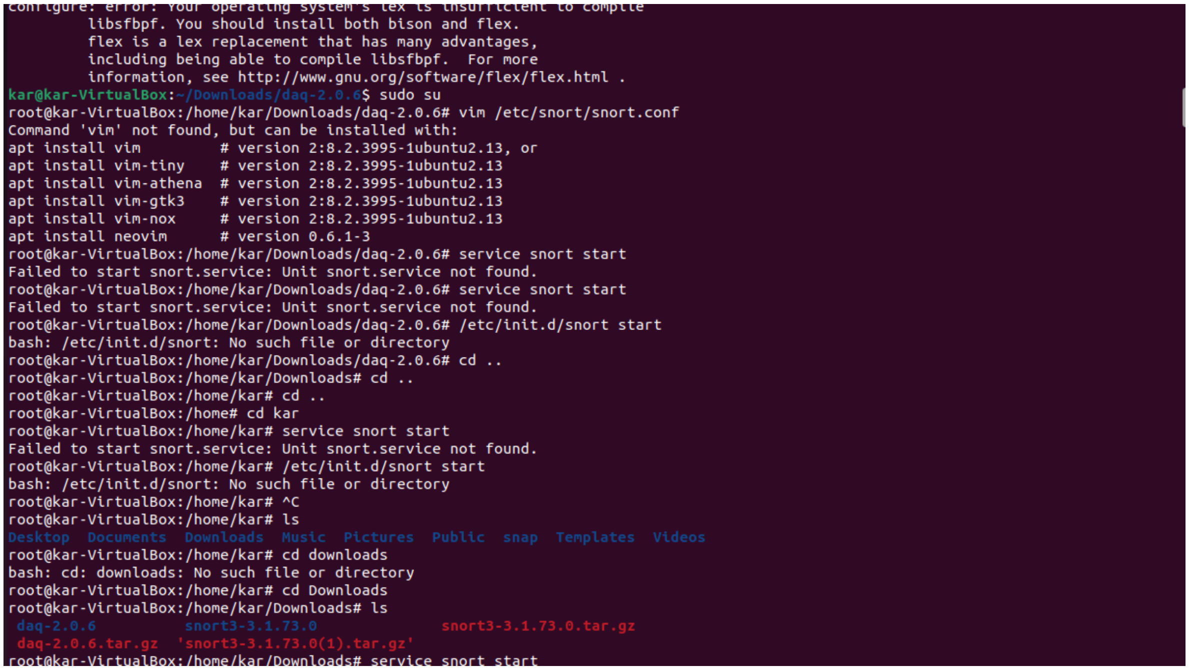
```
kar@kar-VirtualBox:~$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:06:54--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8b09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:06:55 ERROR 404: Not Found.

kar@kar-VirtualBox:~$ ./configure --enable-sourcefire && make && sudo make install
bash: ./configure: No such file or directory
kar@kar-VirtualBox:~$ tar xvfz daq-2.0.6.tar.gz
tar (child): daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ cd Downloads'
> ^C
kar@kar-VirtualBox:~$ cd Downloads
kar@kar-VirtualBox:~/Downloads$ ls
kar@kar-VirtualBox:~/Downloads$ cd downloads
bash: cd: downloads: No such file or directory
kar@kar-VirtualBox:~/Downloads$ cat daq-2.0.6
cat: daq-2.0.6: No such file or directory
kar@kar-VirtualBox:~/Downloads$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:11:14--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:11:14 ERROR 404: Not Found.

kar@kar-VirtualBox:~/Downloads$ sudo su
root@kar-VirtualBox:/home/kar/Downloads# vim /etc/snort/snort.conf
Command 'vim' not found, but can be installed with:
apt install vim         # version 2:8.2.3995-1ubuntu2.13, or
apt install vim-tiny    # version 2:8.2.3995-1ubuntu2.13
apt install vim-athena  # version 2:8.2.3995-1ubuntu2.13
apt install vim-gtk3    # version 2:8.2.3995-1ubuntu2.13
apt install vim-nox     # version 2:8.2.3995-1ubuntu2.13
```



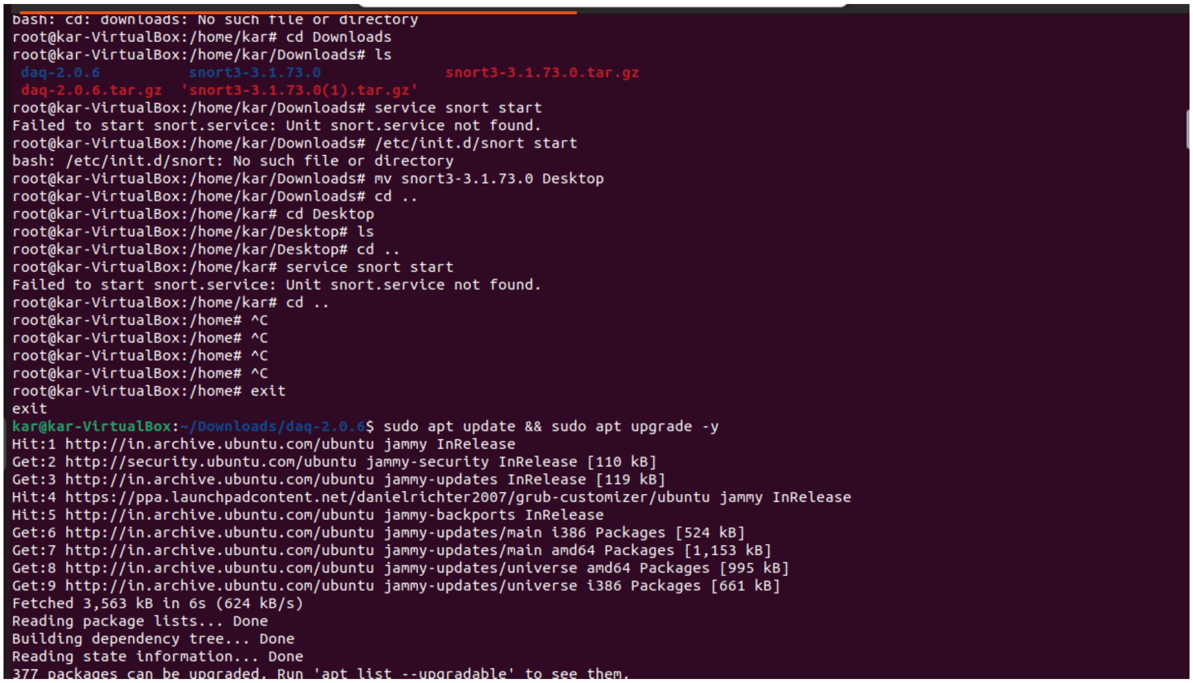
```
kar@kar-VirtualBox:~/Downloads$ ls
kar@kar-VirtualBox:~/Downloads$ cd downloads
bash: cd: downloads: No such file or directory
kar@kar-VirtualBox:~/Downloads$ cd ..
kar@kar-VirtualBox:~$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:17:47--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.139.9, 104.18.138.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.139.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:17:48 ERROR 404: Not Found.

kar@kar-VirtualBox:~$ cd Downloads
kar@kar-VirtualBox:~/Downloads$ ls
 snort3-3.1.73.0  'snort3-3.1.73.0(1).tar.gz'   snort3-3.1.73.0.tar.gz
kar@kar-VirtualBox:~/Downloads$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:18:23--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:18:23 ERROR 404: Not Found.

kar@kar-VirtualBox:~/Downloads$ tar xvfz daq-2.0.6.tar.gz
tar (child): daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~/Downloads$ ls
 snort3-3.1.73.0  'snort3-3.1.73.0(1).tar.gz'   snort3-3.1.73.0.tar.gz
kar@kar-VirtualBox:~/Downloads$ tar xvfz daq-2.0.6.tar.gz
daq-2.0.6/
daq-2.0.6/ChangeLog
daq-2.0.6/missing
daq-2.0.6/daq.dsp
daq-2.0.6/configure
daq-2.0.6/sfbpf/
daq-2.0.6/sfbpf/sf_bpf_printer.c
daq-2.0.6/sfbpf/IP6_misc.h
daq-2.0.6/sfbpf/sf_gencode.c
```



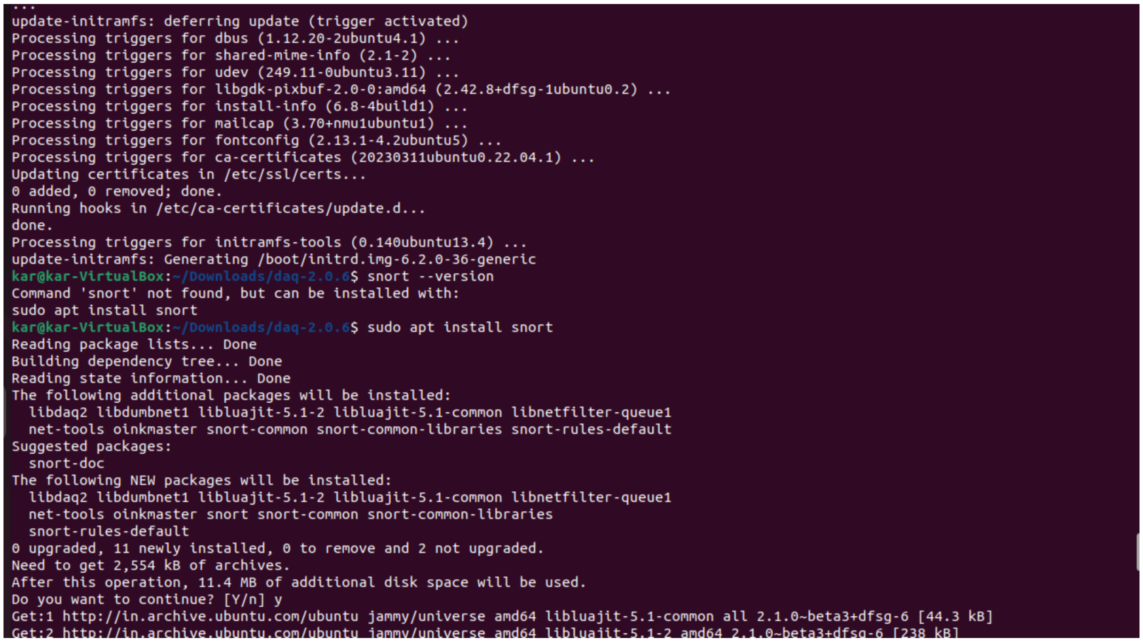
```
daq-2.0.6/depcomp
daq-2.0.6/Makefile.in
daq-2.0.6/m4/
daq-2.0.6/m4/ax_cflags_gcc_option.m4
daq-2.0.6/m4/ltsugar.m4
daq-2.0.6/m4/sf.m4
daq-2.0.6/m4/libtool.m4
daq-2.0.6/m4/ltversion.m4
daq-2.0.6/m4/lt~obsolete.m4
daq-2.0.6/m4/ltoptions.m4
daq-2.0.6/configure.ac
kar@kar-VirtualBox:~/Downloads$ cd daq
bash: cd: daq: No such file or directory
kar@kar-VirtualBox:~/Downloads$ cd daq-2.0.6
kar@kar-VirtualBox:~/Downloads/daq-2.0.6$ ./configure --enable-sourcefire && make && sudo make install
configure: WARNING: unrecognized options: --enable-sourcefire
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /usr/bin/mkdir -p
checking for gawk... no
checking for mawk... mawk
checking whether make sets $(MAKE)... no
checking whether make supports nested variables... no
checking for gcc... gcc
checking whether the C compiler works... yes
checking for C compiler default output file name... a.out
checking for suffix of executables...
checking whether we are cross compiling... no
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking whether gcc understands -c and -o together... yes
checking for style of include used by make... none
checking dependency style of gcc... none
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking how to print strings... printf
```



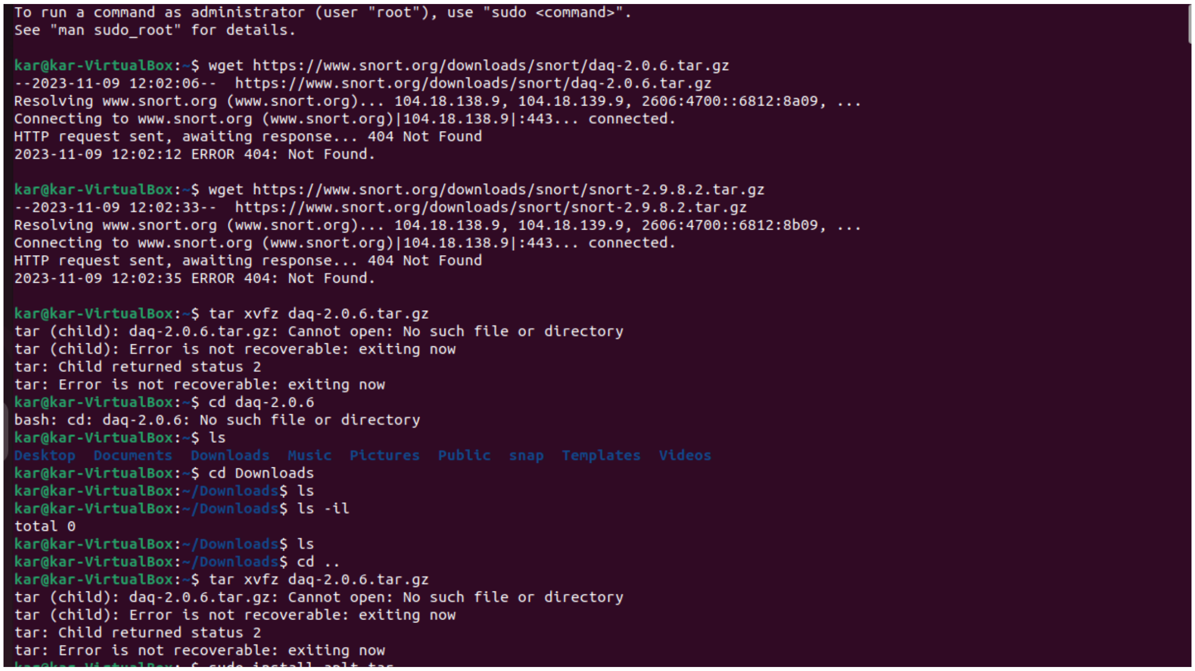
```
configure: error: Your operating system's lex is insufficient to compile
          libsfbpf. You should install both bison and flex.
          flex is a lex replacement that has many advantages,
          including being able to compile libsfbpf.  For more
          information, see http://www.gnu.org/software/flex/flex.html .
kar@kar-VirtualBox:~/Downloads/daq-2.0.6$ sudo su
root@kar-VirtualBox:/home/kar/Downloads/daq-2.0.6# vim /etc/snort/snort.conf
Command 'vim' not found, but can be installed with:
apt install vim         # version 2:8.2.3995-1ubuntu2.13, or
apt install vim-tiny    # version 2:8.2.3995-1ubuntu2.13
apt install vim-athena  # version 2:8.2.3995-1ubuntu2.13
apt install vim-gtk3    # version 2:8.2.3995-1ubuntu2.13
apt install vim-nox     # version 2:8.2.3995-1ubuntu2.13
apt install neovim      # version 0.6.1-3
root@kar-VirtualBox:/home/kar/Downloads/daq-2.0.6# service snort start
Failed to start snort.service: Unit snort.service not found.
root@kar-VirtualBox:/home/kar/Downloads/daq-2.0.6# service snort start
Failed to start snort.service: Unit snort.service not found.
root@kar-VirtualBox:/home/kar/Downloads/daq-2.0.6# /etc/init.d/snort start
bash: /etc/init.d/snort: No such file or directory
root@kar-VirtualBox:/home/kar/Downloads/daq-2.0.6# cd ..
root@kar-VirtualBox:/home/kar/Downloads# cd ..
root@kar-VirtualBox:/home/kar# cd ..
root@kar-VirtualBox:/home# cd kar
root@kar-VirtualBox:/home/kar# service snort start
Failed to start snort.service: Unit snort.service not found.
root@kar-VirtualBox:/home/kar# /etc/init.d/snort start
bash: /etc/init.d/snort: No such file or directory
root@kar-VirtualBox:/home/kar# ^C
root@kar-VirtualBox:/home/kar# ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
root@kar-VirtualBox:/home/kar# cd downloads
bash: cd: downloads: No such file or directory
root@kar-VirtualBox:/home/kar# cd Downloads
root@kar-VirtualBox:/home/kar/Downloads# ls
 daq-2.0.6          snort3-3.1.73.0              snort3-3.1.73.0.tar.gz
 daq-2.0.6.tar.gz  'snort3-3.1.73.0(1).tar.gz'
root@kar-VirtualBox:/home/kar/Downloads# service snort start
```



```
bash: cd: downloads: No such file or directory
root@kar-VirtualBox:/home/kar# cd Downloads
root@kar-VirtualBox:/home/kar/Downloads# ls
 daq-2.0.6          snort3-3.1.73.0              snort3-3.1.73.0.tar.gz
 daq-2.0.6.tar.gz  'snort3-3.1.73.0(1).tar.gz'
root@kar-VirtualBox:/home/kar/Downloads# service snort start
Failed to start snort.service: Unit snort.service not found.
root@kar-VirtualBox:/home/kar/Downloads# /etc/init.d/snort start
bash: /etc/init.d/snort: No such file or directory
root@kar-VirtualBox:/home/kar/Downloads# mv snort3-3.1.73.0 Desktop
root@kar-VirtualBox:/home/kar/Downloads# cd ..
root@kar-VirtualBox:/home/kar# cd Desktop
root@kar-VirtualBox:/home/kar/Desktop# ls
root@kar-VirtualBox:/home/kar/Desktop# cd ..
root@kar-VirtualBox:/home/kar# service snort start
Failed to start snort.service: Unit snort.service not found.
root@kar-VirtualBox:/home/kar# cd ..
root@kar-VirtualBox:/home# ^C
root@kar-VirtualBox:/home# ^C
root@kar-VirtualBox:/home# ^C
root@kar-VirtualBox:/home# ^C
root@kar-VirtualBox:/home# exit
exit
kar@kar-VirtualBox:~/Downloads/daq-2.0.6$ sudo apt update && sudo apt upgrade -y
Hit:1 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Hit:4 https://ppa.launchpadcontent.net/danielrichter2007/grub-customizer/ubuntu jammy InRelease
Hit:5 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Get:6 http://in.archive.ubuntu.com/ubuntu jammy-updates/main i386 Packages [524 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [1,153 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [995 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu jammy-updates/universe i386 Packages [661 kB]
Fetched 3,563 kB in 6s (624 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
377 packages can be upgraded. Run 'apt list --upgradable' to see them.
```



```
...
update-initramfs: deferring update (trigger activated)
Processing triggers for dbus (1.12.20-2ubuntu4.1) ...
Processing triggers for shared-mime-info (2.1-2) ...
Processing triggers for udev (249.11-0ubuntu3.11) ...
Processing triggers for libgdk-pixbuf-2.0-0:amd64 (2.42.8+dfsg-1ubuntu0.2) ...
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for mailcap (3.70+nmu1ubuntu1) ...
Processing triggers for fontconfig (2.13.1-4.2ubuntu5) ...
Processing triggers for ca-certificates (20230311ubuntu0.22.04.1) ...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for initramfs-tools (0.140ubuntu13.4) ...
update-initramfs: Generating /boot/initrd.img-6.2.0-36-generic
kar@kar-VirtualBox:~/Downloads/daq-2.0.6$ snort --version
Command 'snort' not found, but can be installed with:
sudo apt install snort
kar@kar-VirtualBox:~/Downloads/daq-2.0.6$ sudo apt install snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1
  net-tools oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1
  net-tools oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 2 not upgraded.
Need to get 2,554 kB of archives.
After this operation, 11.4 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-common all 2.1.0~beta3+dfsg-6 [44.3 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 libluajit-5.1-2 amd64 2.1.0~beta3+dfsg-6 [238 kB]
```



```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

kar@kar-VirtualBox:~$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
--2023-11-09 12:02:06--  https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8a09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:02:12 ERROR 404: Not Found.

kar@kar-VirtualBox:~$ wget https://www.snort.org/downloads/snort/snort-2.9.8.2.tar.gz
--2023-11-09 12:02:33--  https://www.snort.org/downloads/snort/snort-2.9.8.2.tar.gz
Resolving www.snort.org (www.snort.org)... 104.18.138.9, 104.18.139.9, 2606:4700::6812:8b09, ...
Connecting to www.snort.org (www.snort.org)|104.18.138.9|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2023-11-09 12:02:35 ERROR 404: Not Found.

kar@kar-VirtualBox:~$ tar xvfz daq-2.0.6.tar.gz
tar (child): daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ cd daq-2.0.6
bash: cd: daq-2.0.6: No such file or directory
kar@kar-VirtualBox:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
kar@kar-VirtualBox:~$ cd Downloads
kar@kar-VirtualBox:~/Downloads$ ls
kar@kar-VirtualBox:~/Downloads$ ls -il
total 0
kar@kar-VirtualBox:~/Downloads$ ls
kar@kar-VirtualBox:~/Downloads$ cd ..
kar@kar-VirtualBox:~$ tar xvfz daq-2.0.6.tar.gz
tar (child): daq-2.0.6.tar.gz: Cannot open: No such file or directory
tar (child): Error is not recoverable: exiting now
tar: Child returned status 2
tar: Error is not recoverable: exiting now
kar@kar-VirtualBox:~$ sudo install aplt tar
```