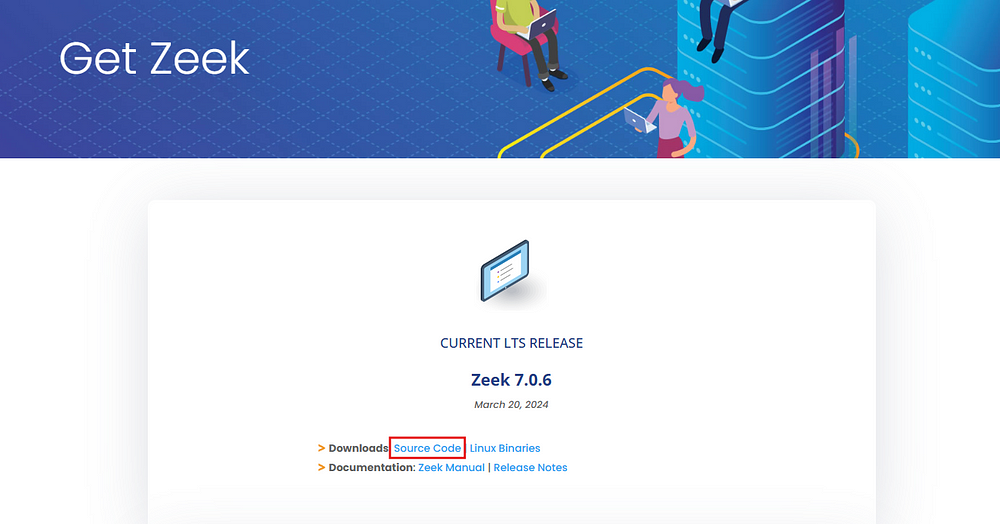
### **Zeek-7.0.4 Installation — Ubuntu**

To begin, navigate to Zeek.org/get-zeek/ to acquire the latest stable release of Zeek.



Subsequently, it is necessary to update and upgrade the Ubuntu repositories. Execute the following command:

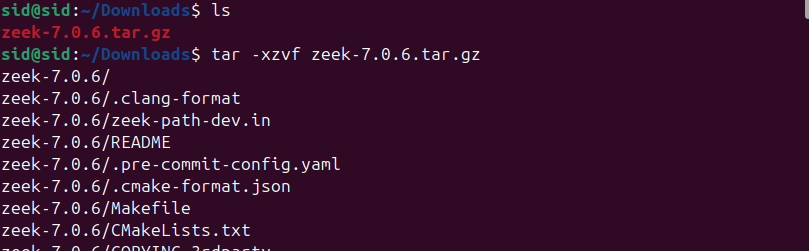
sudo apt-get update && sudo apt-get upgrade -y

Following this, install the prerequisite tools for compiling Zeek packages with the command:

sudo apt-get install cmake make gcc g++ bison libcap-dev libssl-dev python3-dev swig zlib1g-dev flex

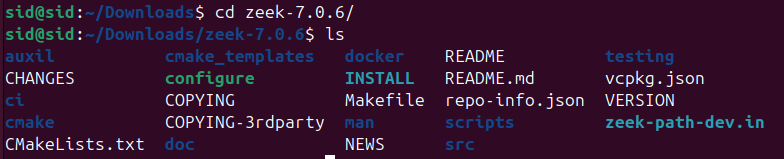
Next, extract the Zeek archive:

tar -xzvf <zeek-filename>



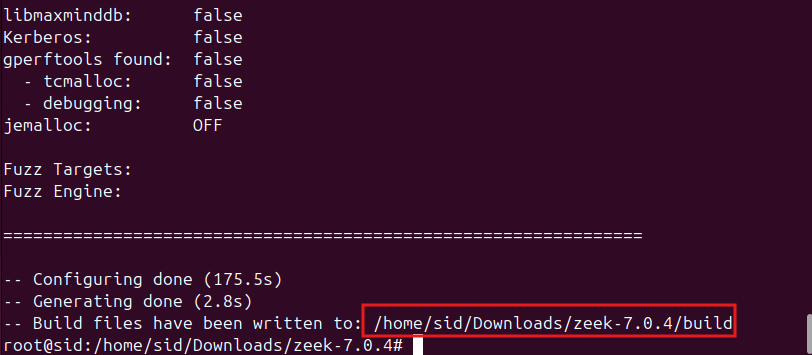
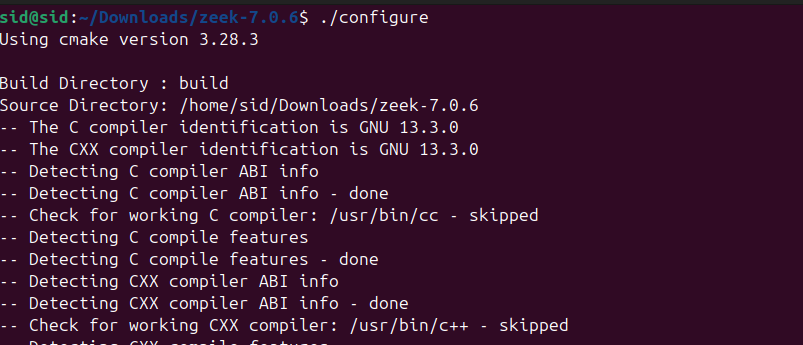
Change the directory to the extracted folder:

cd Zeek-<version>



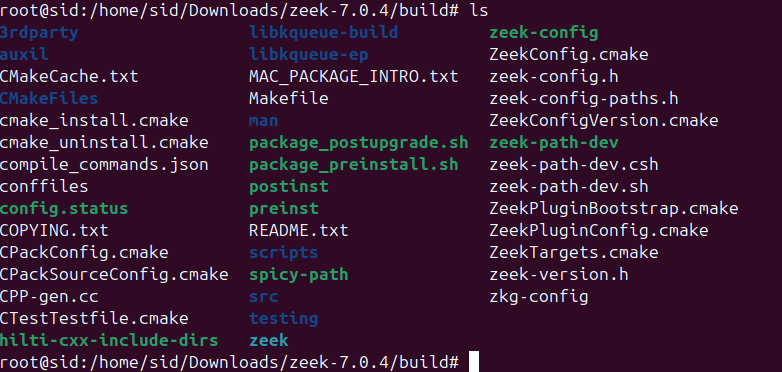
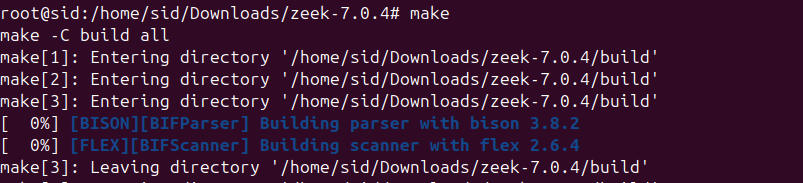
Proceed to compile the source code:

./configure



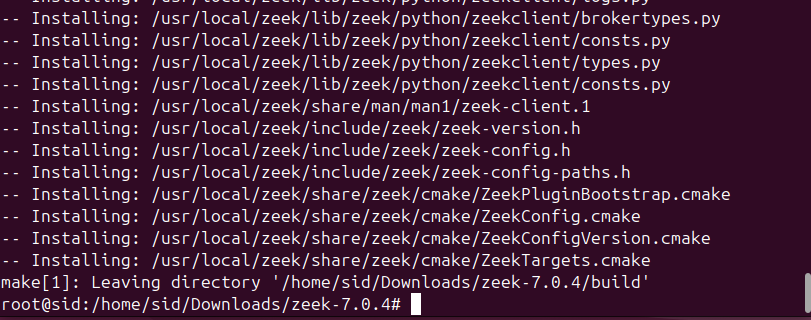
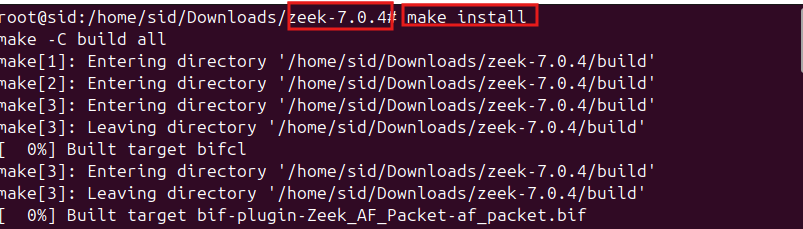
Upon completion of the configuration, initiate the build process:

make



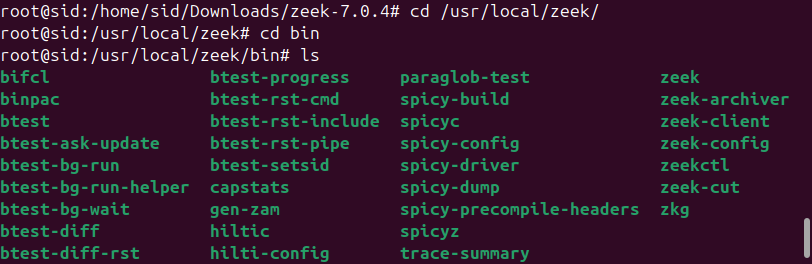
After the build is finalized, return to the Zeek directory and execute the installation command:

make install



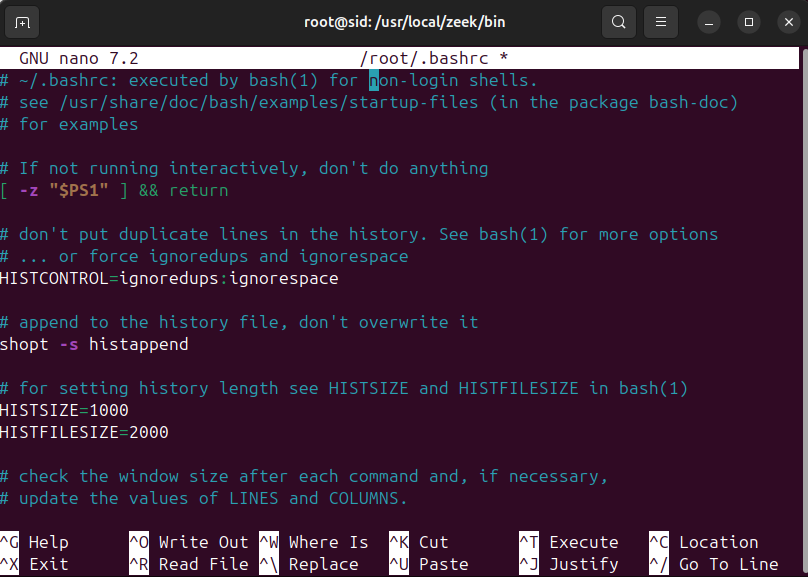
Once, this is complete navigate to the local folder where zeek is installed to check if it is installed successfully.

cd /usr/local/zeek/bin



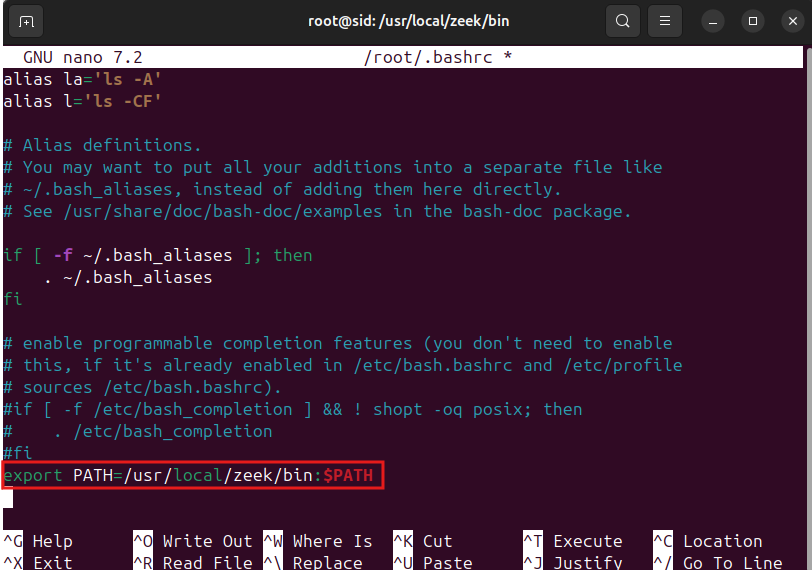
To incorporate the Zeek binary path into the system environment, edit the ~/.bashrc file:

nano ~/.bashrc

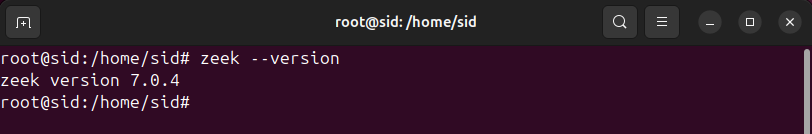


Append the following line to the end of the file:

export PATH=/usr/local/zeek/bin:$PATH

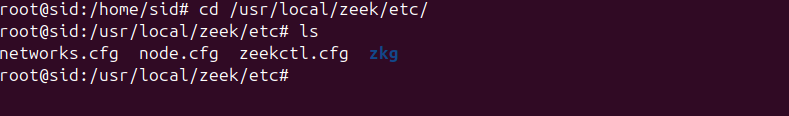


Now, save and exit this file.



Navigate to the Zeek configuration directory:

cd /usr/local/zeek/etc

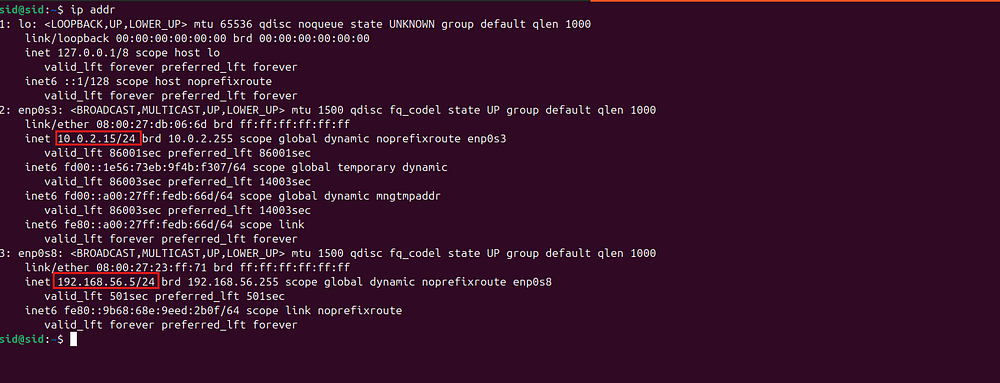


Locate the configuration files and begin by editing the networks.cfg file:

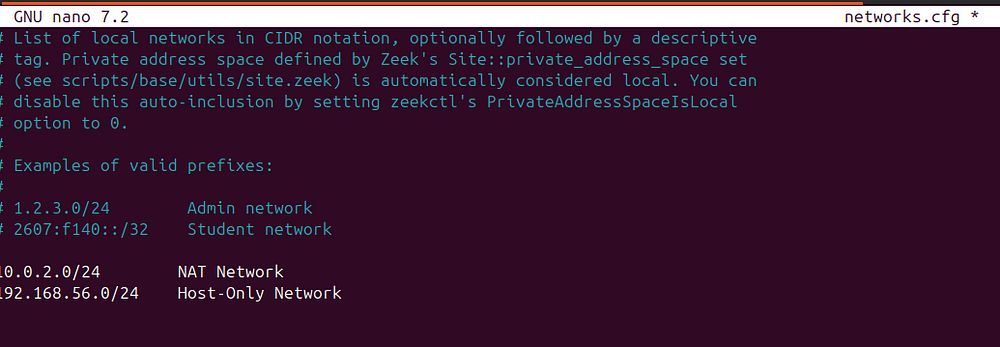
nano networks.cfg

Prior to this, determine the machine's IP address in another terminal:

ip addrr



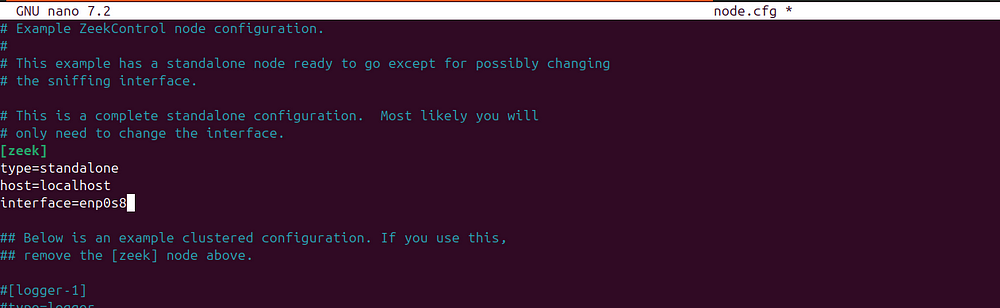
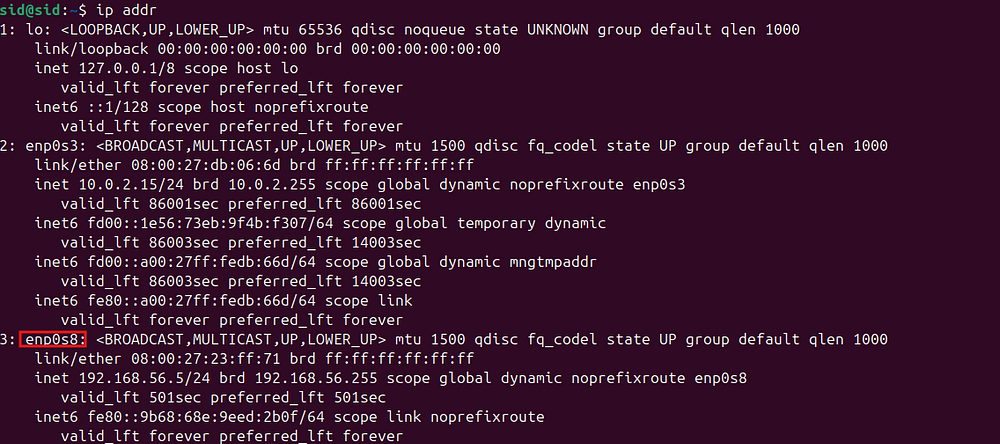
Depending on the network adapters, multiple IP addresses may be listed. Add the relevant IP subnet to the Zeek configuration, then save and close the file.



Depending on the network adapters, multiple IP addresses may be listed. Add the relevant IP subnet to the Zeek configuration, then save and close the file.

Proceed to edit the node.cfg file:

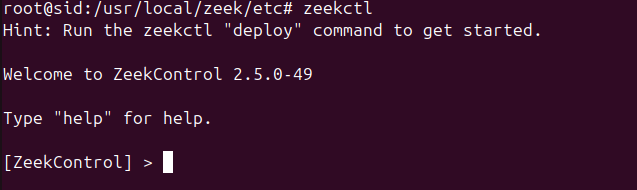
nano node.cfg



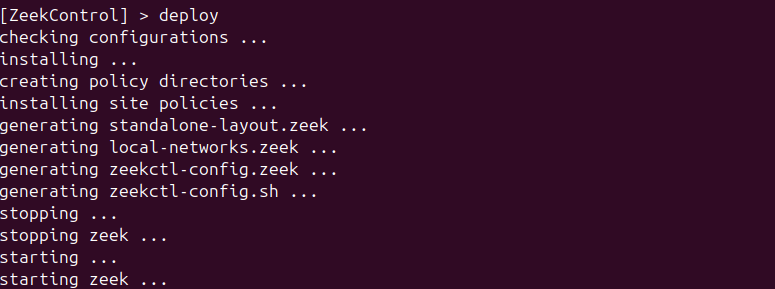
Within this file, set the interface variable to the network interface intended for monitoring. Save and exit the file.

Launch Zeek by invoking ZeekControl:

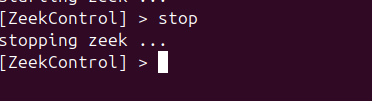
zeekctl



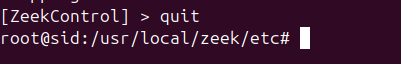
Deploy the configuration and start Zeek by entering deploy at the ZeekControl prompt.



To stop Zeek, on the ZeekControl prompt type stop. This will stop Zeek.



Exit ZeekControl by entering quit.



The installation and configuration of Zeek are now successfully concluded.