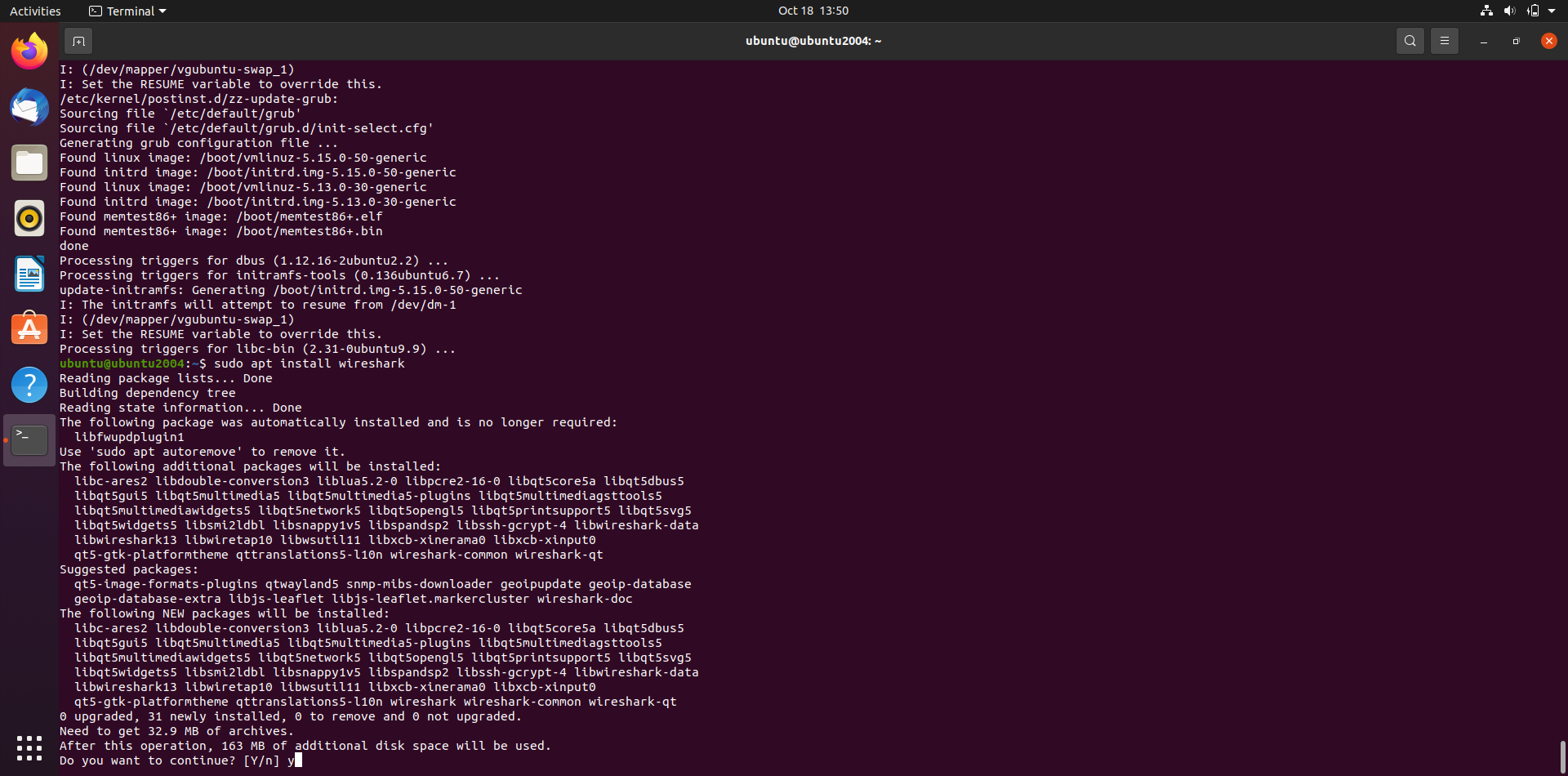
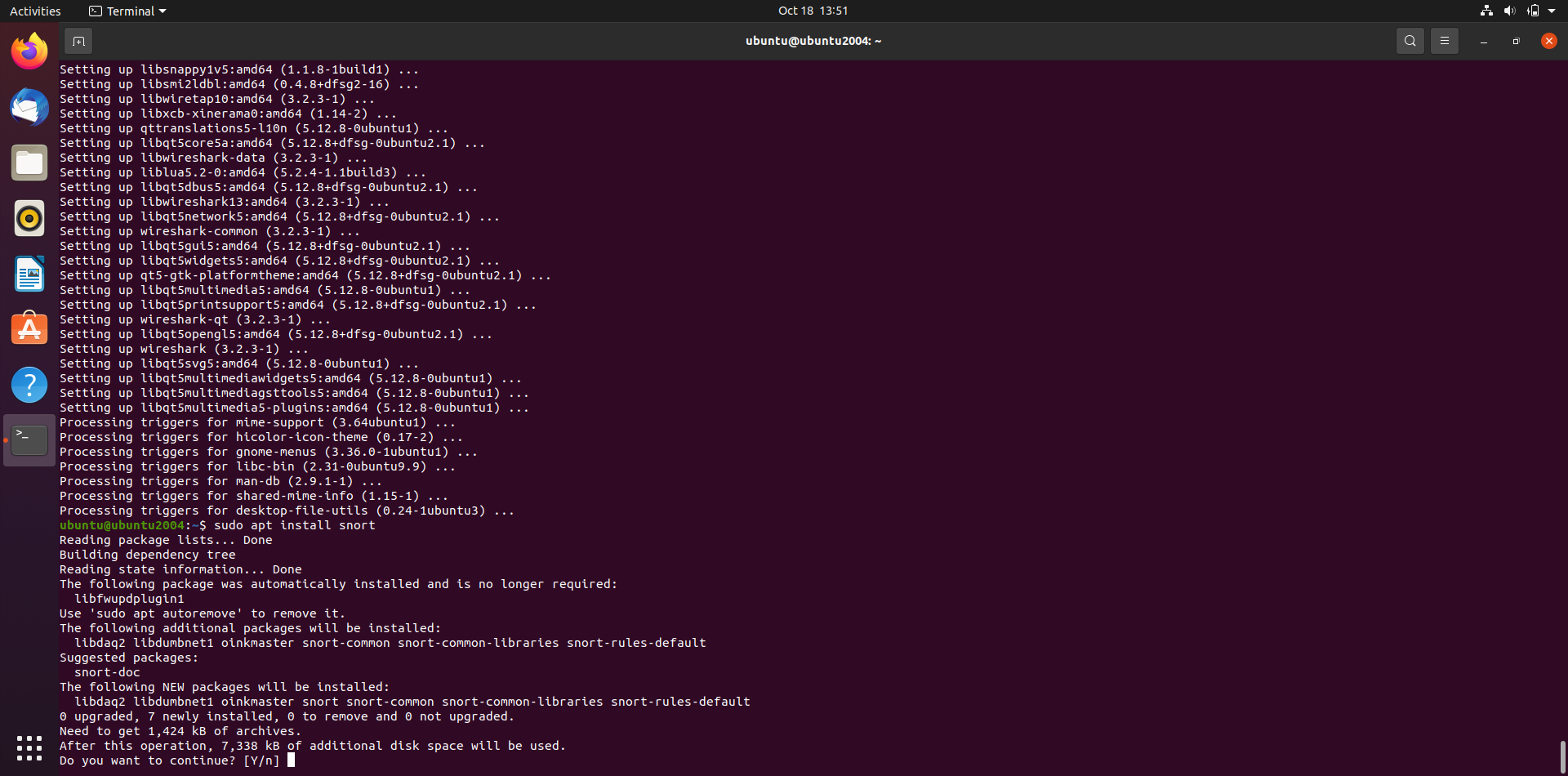
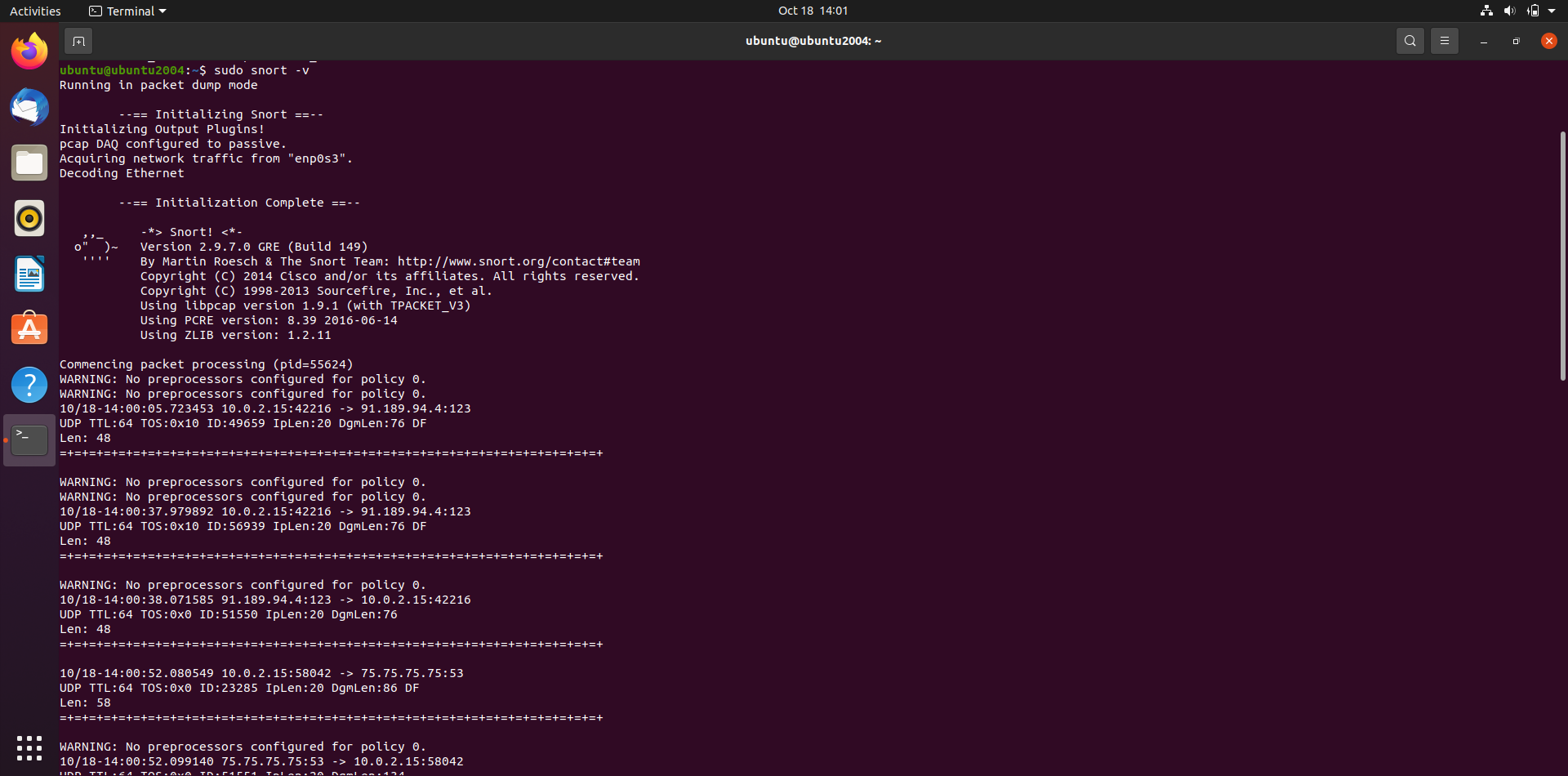
**Assignment 04 – Wireshark and Snort IDS**

* **Installing snort and wire shark:**

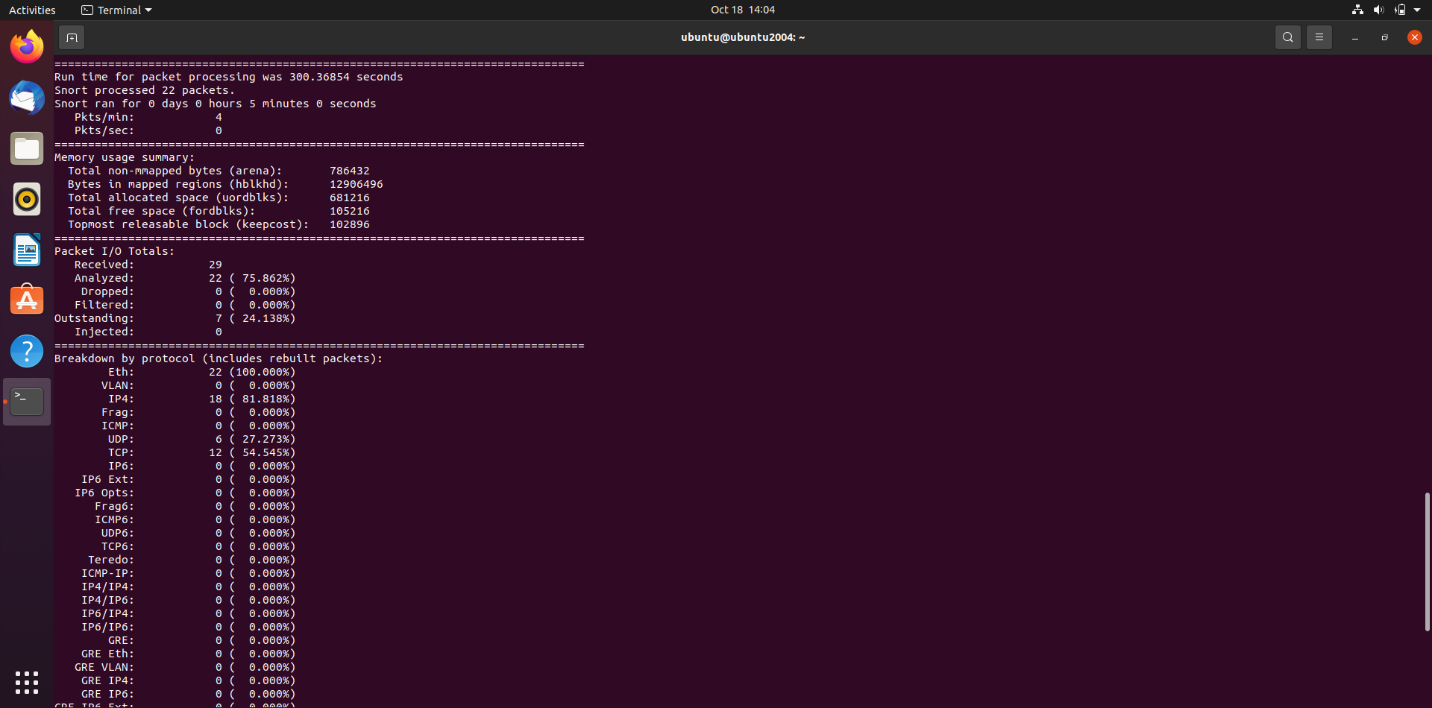
****

****

* **Using snort in verbose mode**

****

* **Information shown when snort is stopped**

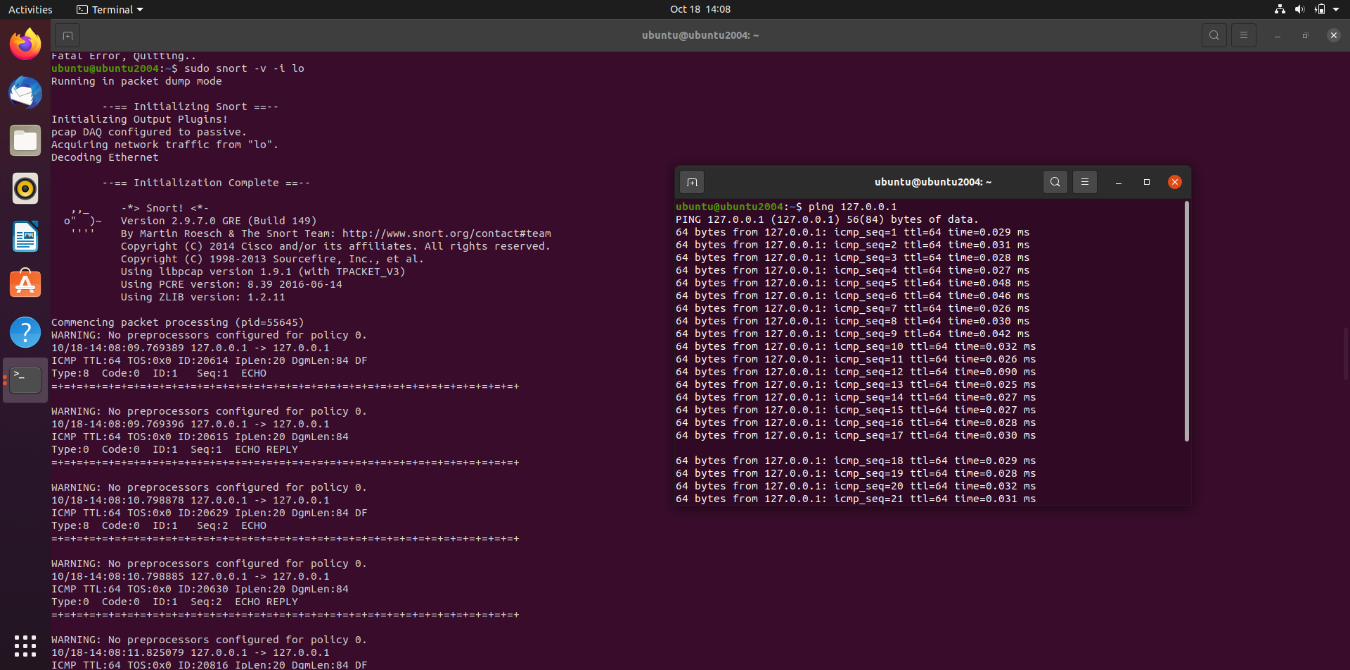
****

* **Pinging Ubuntu VM from local machine**

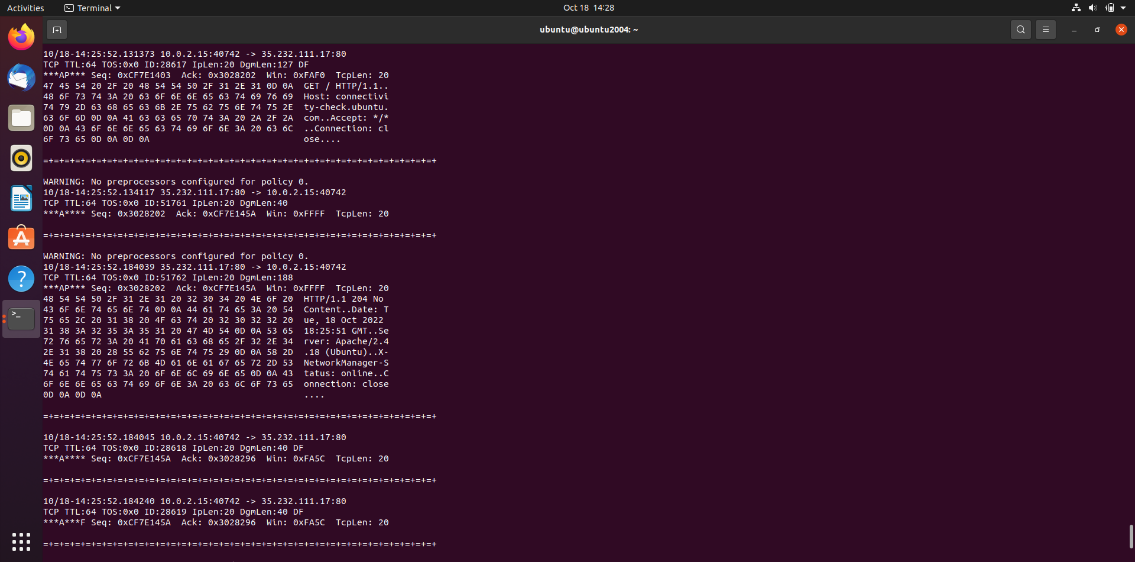
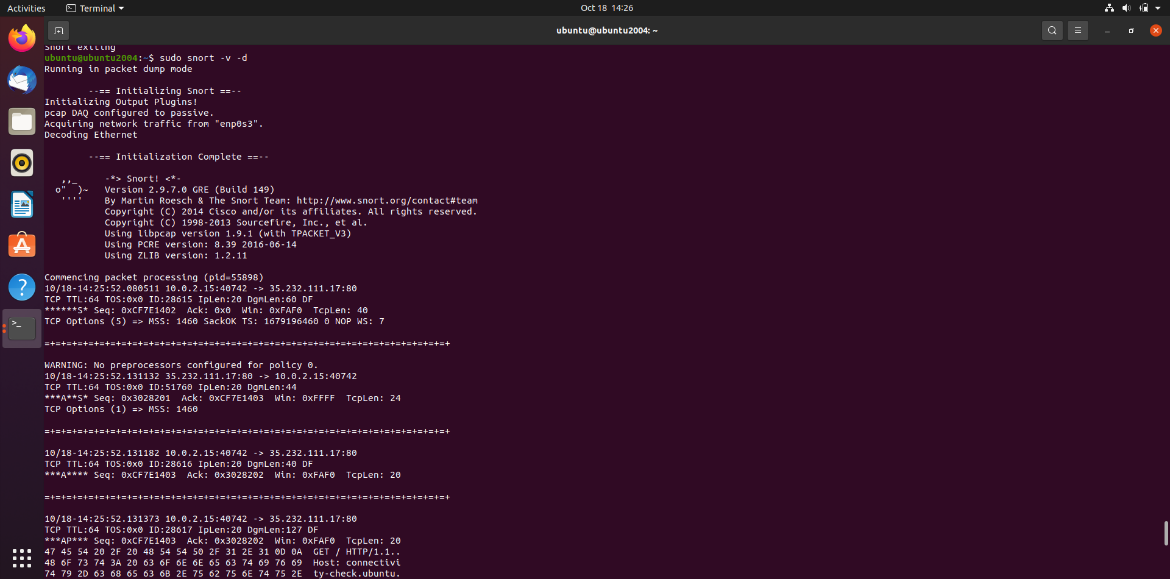
A screenshot of a computer

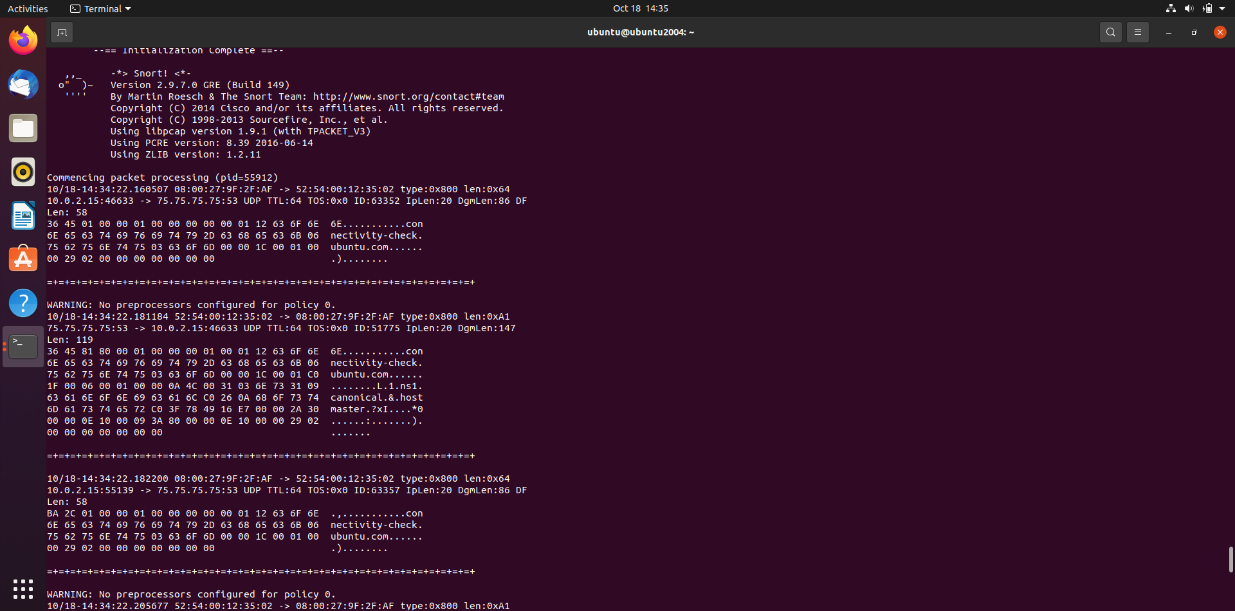
Description automatically generated

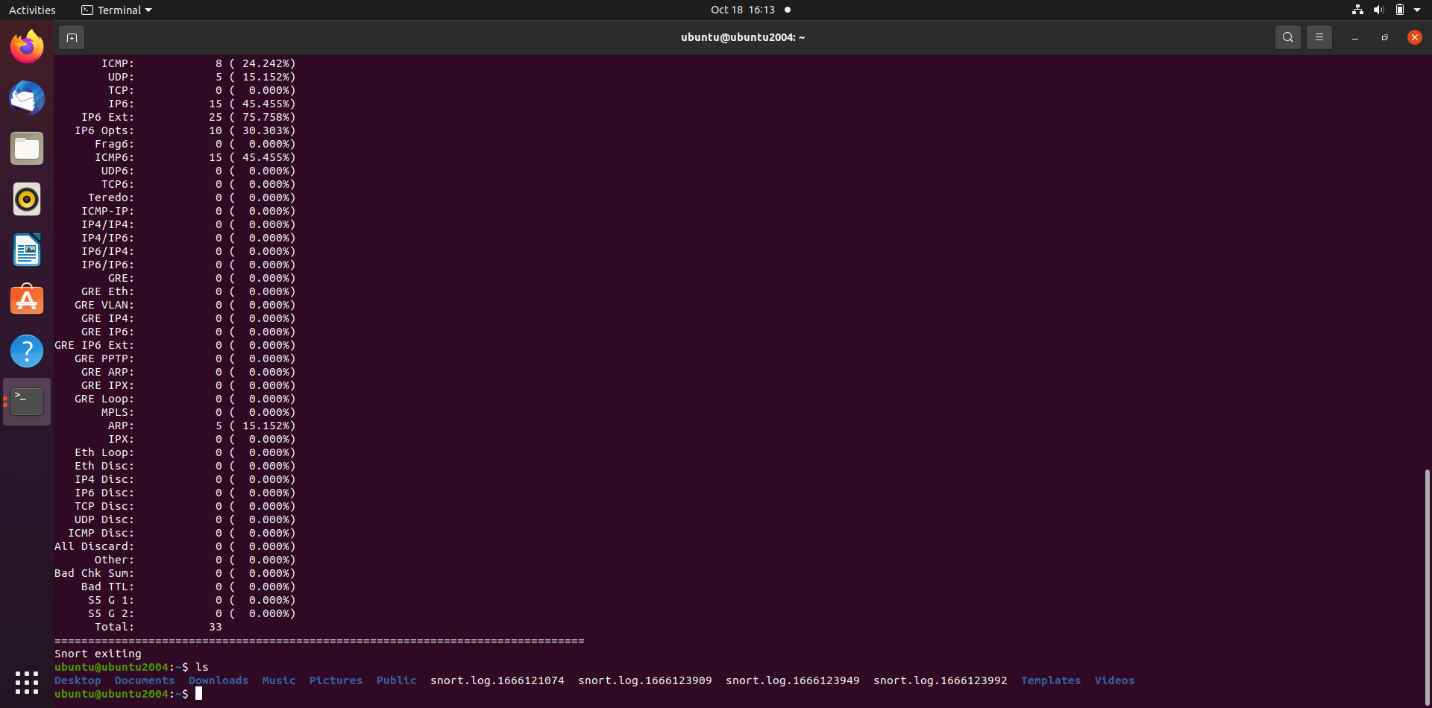
* **Pinging 127.0.0.1 while running snort**

****

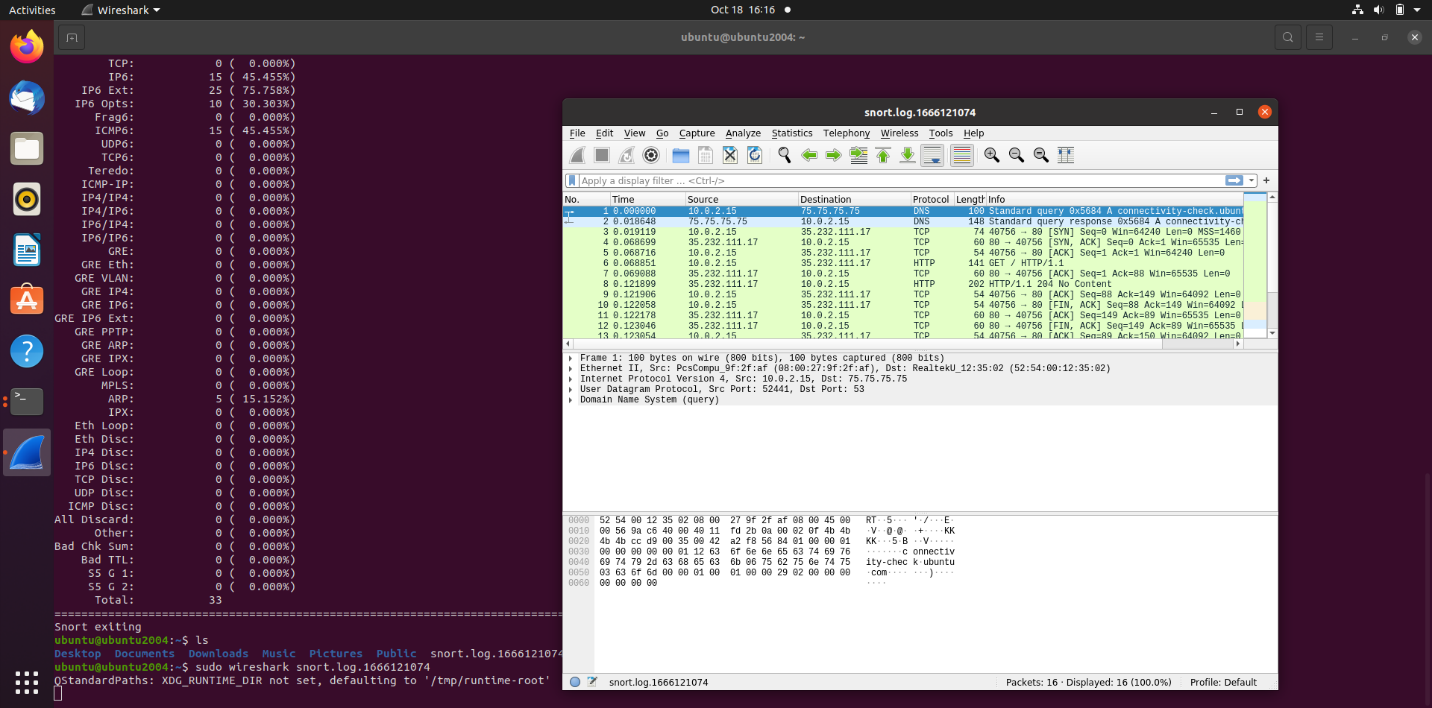
* **Running snort to display information about layer 3 and layer 4**



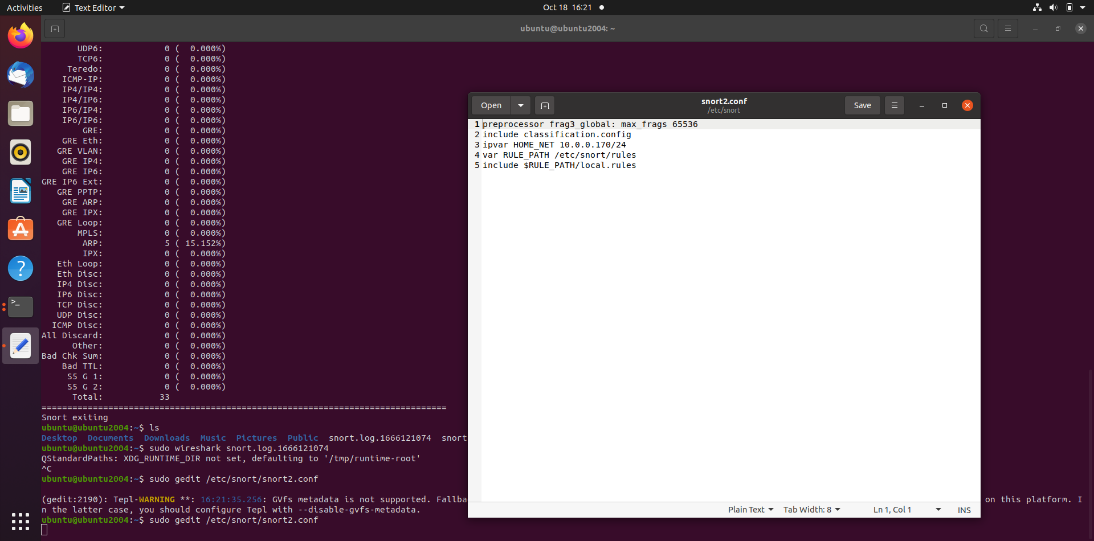
* **Running snort with -vde **
* **Files generated when pinging Ubuntu VM from local windows machine**

****

* **Inspecting log file with wireshark**



* **Adding rules to snort**

Graphical user interface, text

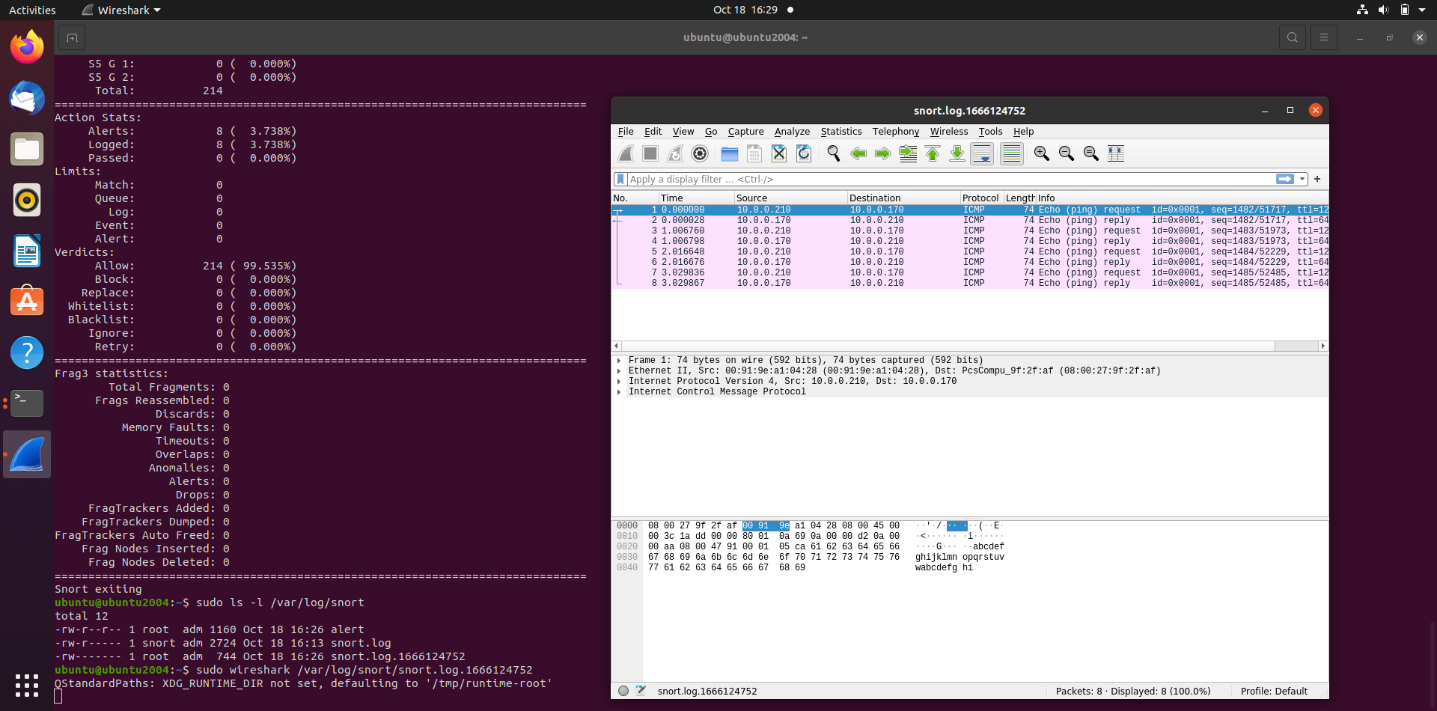
Description automatically generated

* **Pinging from windows local machine to Ubuntu VM after rules are set**

Graphical user interface, text

Description automatically generated

* **Inspecting log file with wireshark**

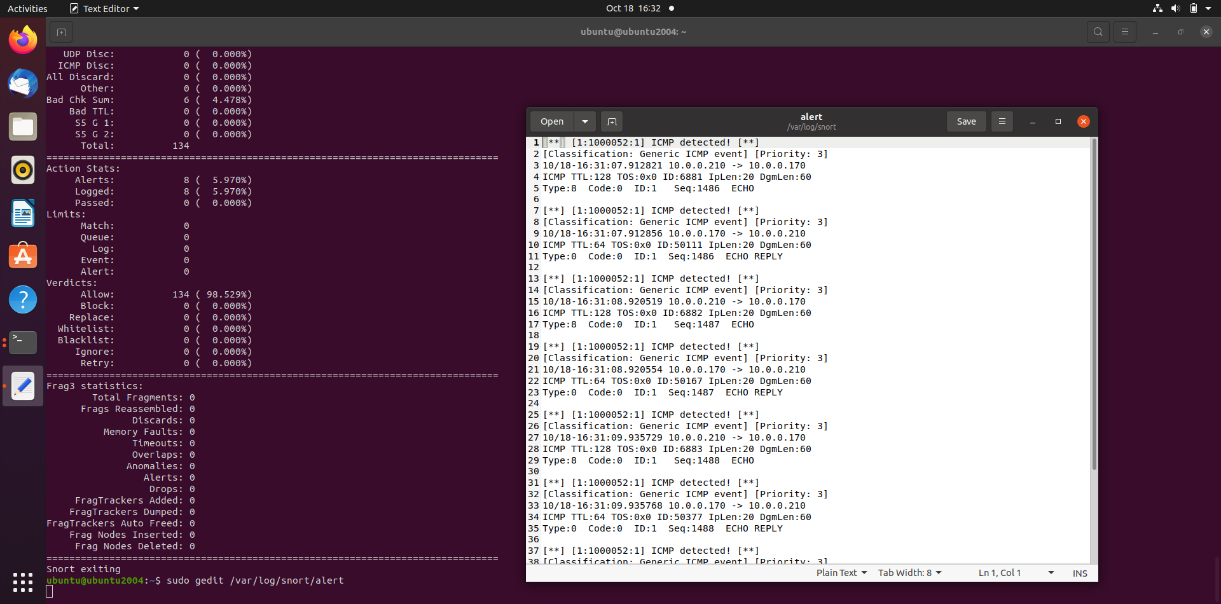
****

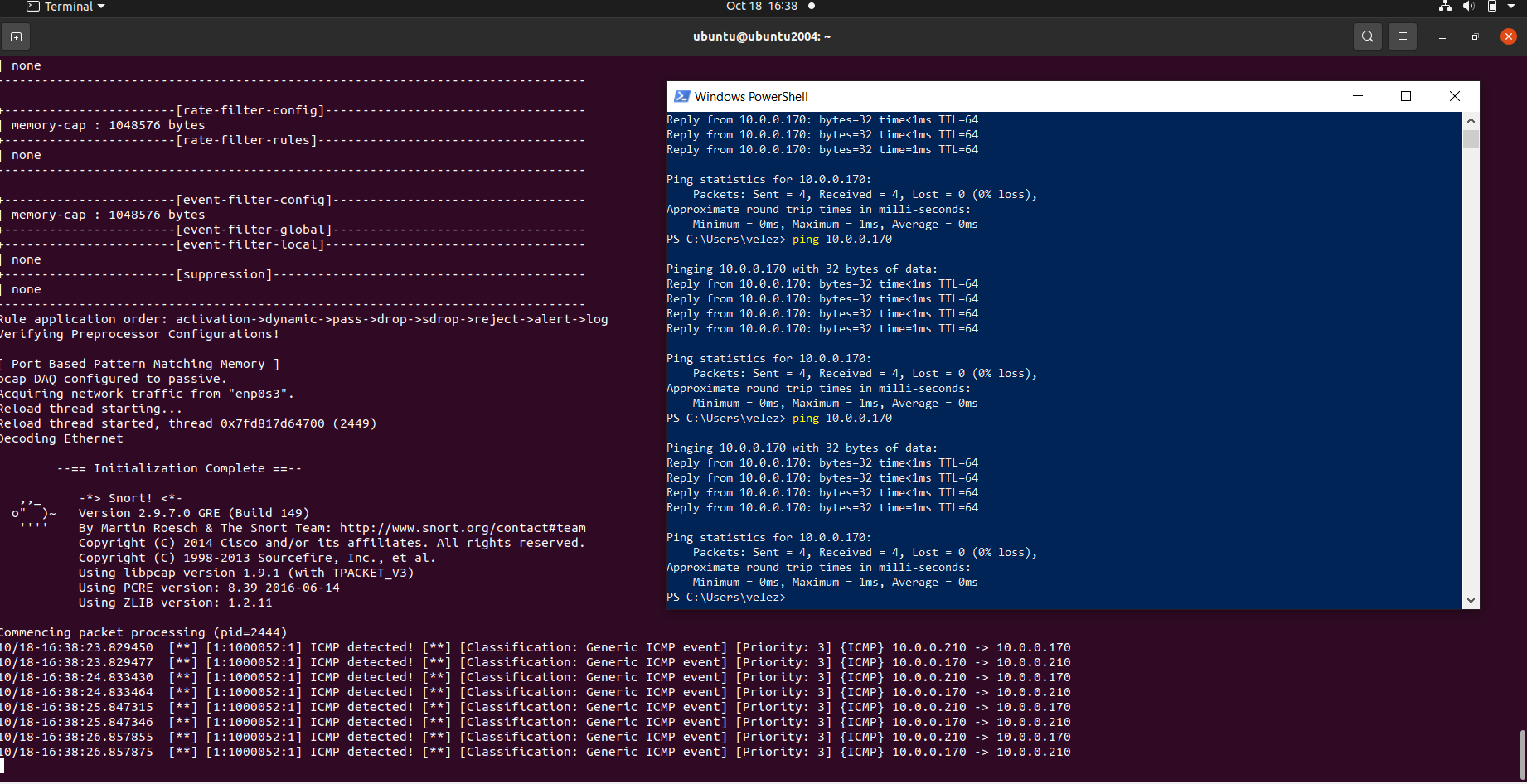
* **Pinging after changing the -A value from fast to full:**

A screenshot of a computer

Description automatically generated

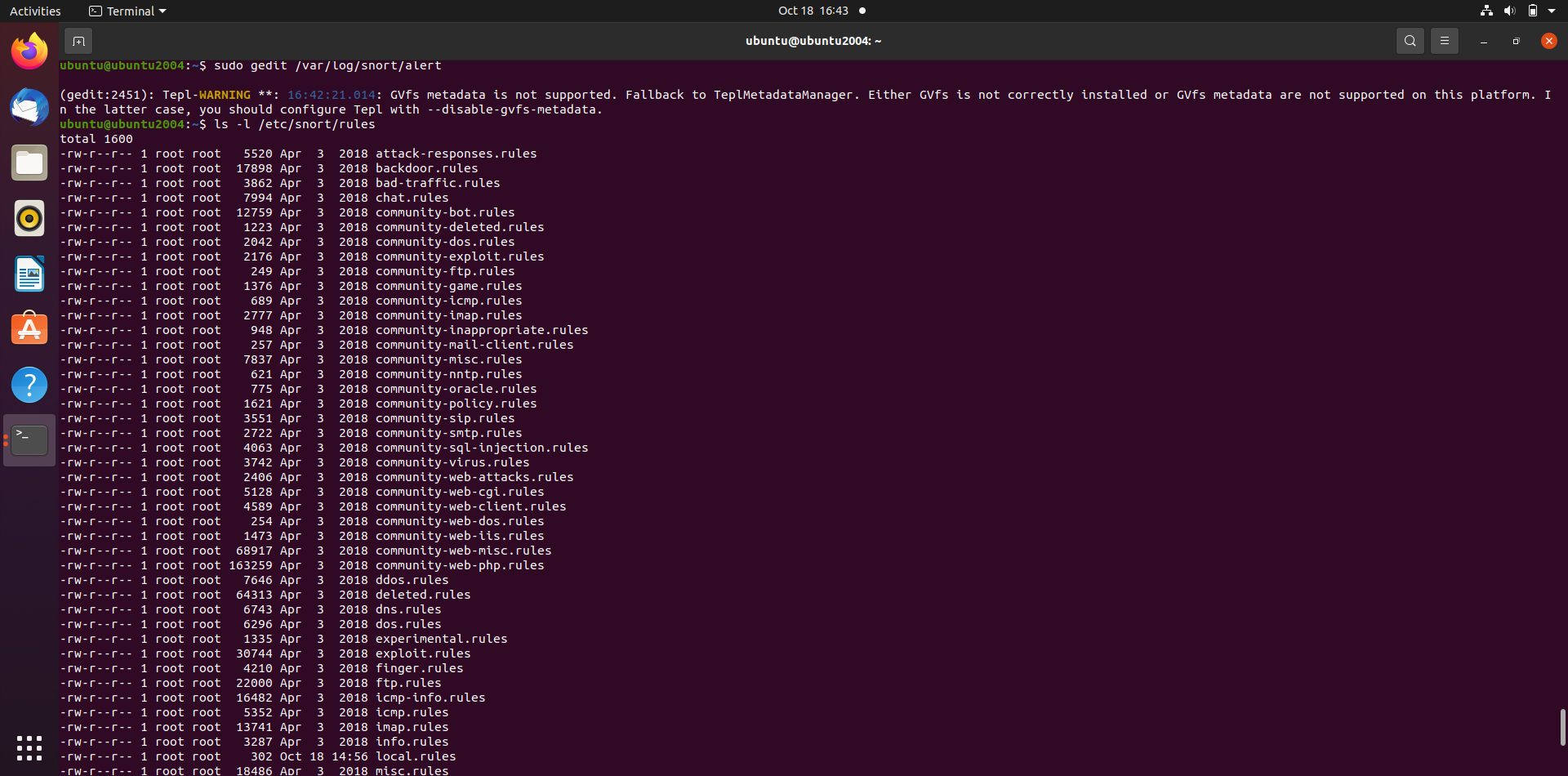
* **Inspecting alert file**



* **Pinging with both full and fast and two -A** 
* **Inspecting log file**

****

* **snort rules**

****