1. How many states could has a process in Linux?

Linux has basically 5 states:

'D' = UNINTERRUPTABLE\_SLEEP

'R' = RUNNING & RUNNABLE

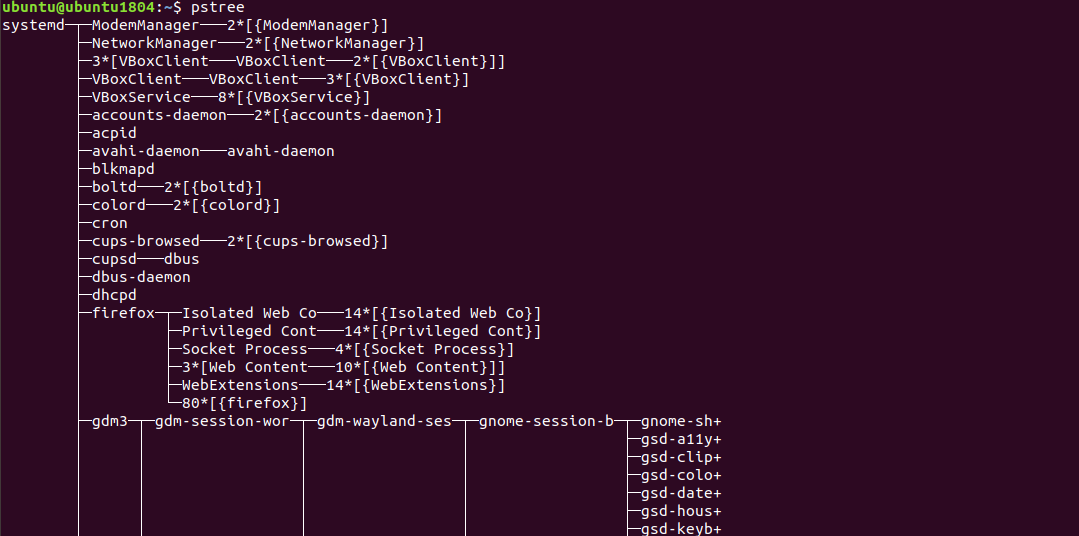
'S' = INTERRRUPTABLE\_SLEEP

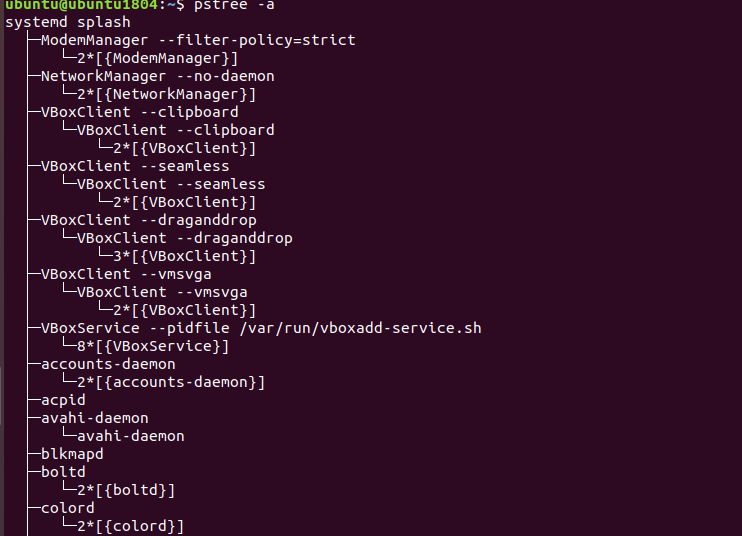
'T' = STOPPED

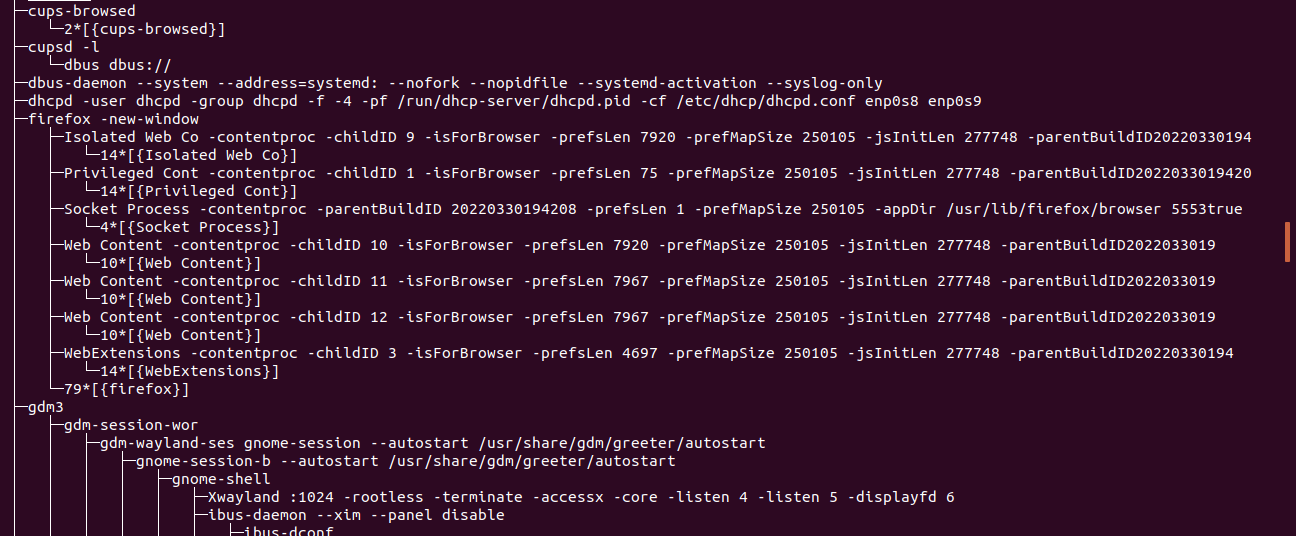
'Z' = ZOMBIE

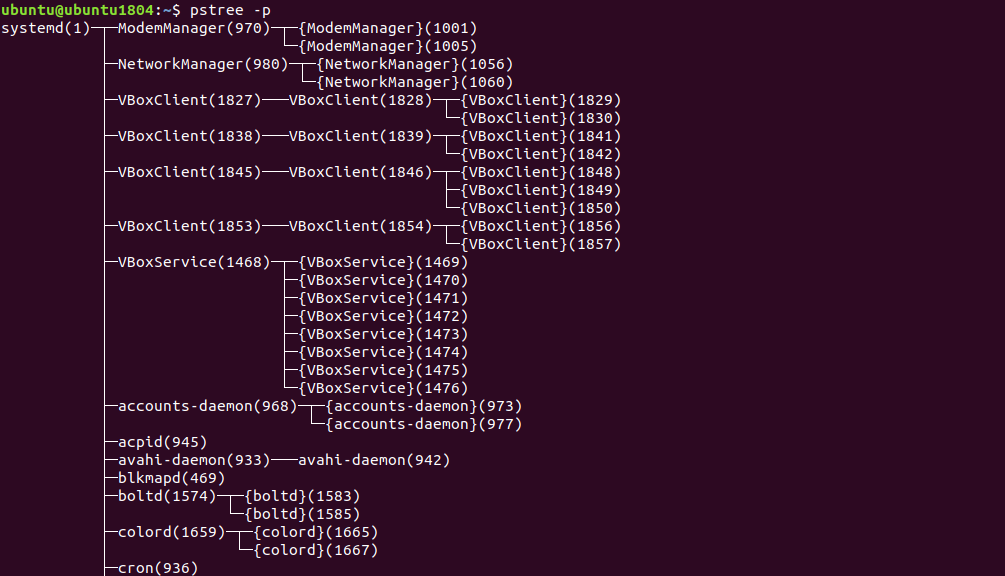
2. Examine the pstree command. Make output (highlight) the chain (ancestors) of the current process.

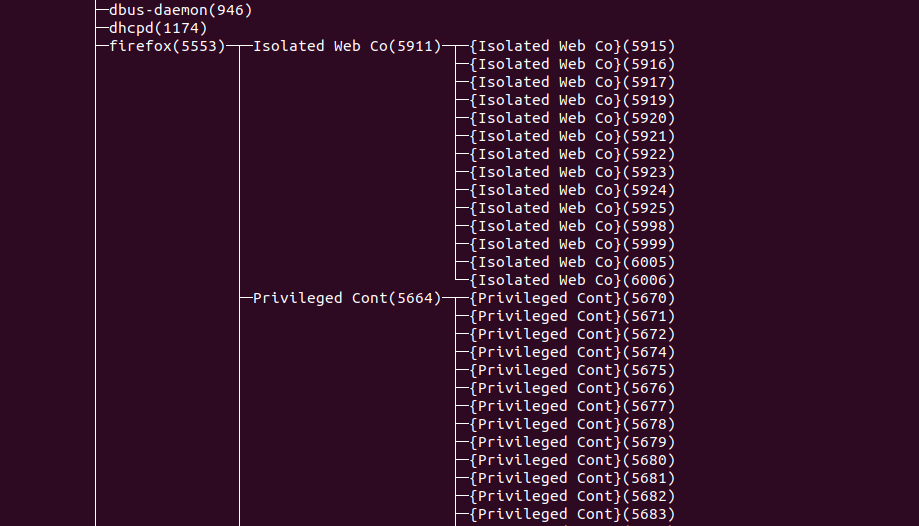
The pstree Linux command will display all trips on the tree, the tree view will be in the PID (if specified) or initializing this main route for the root (root), if a user ID is specified, then the tree will only belong to the user to display trips.

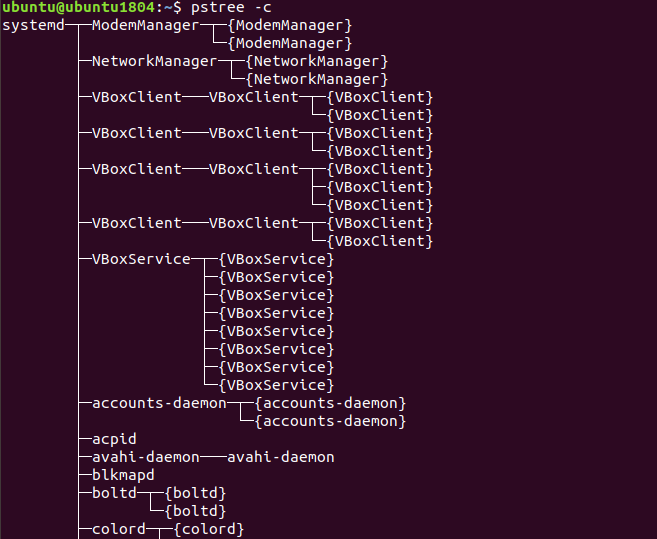


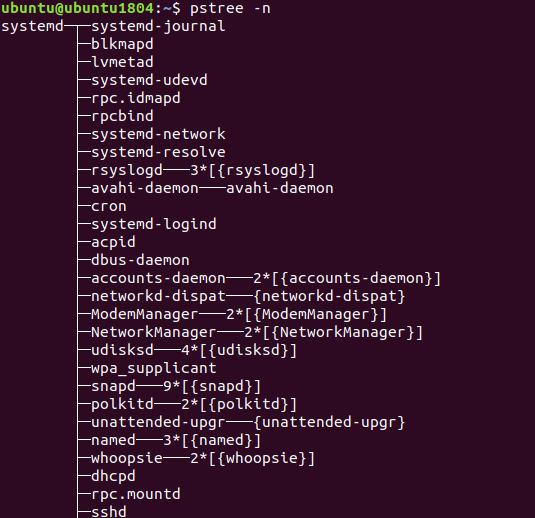






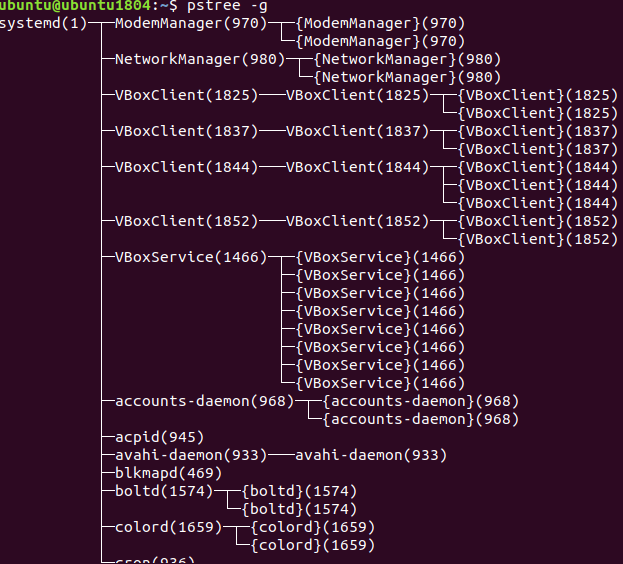


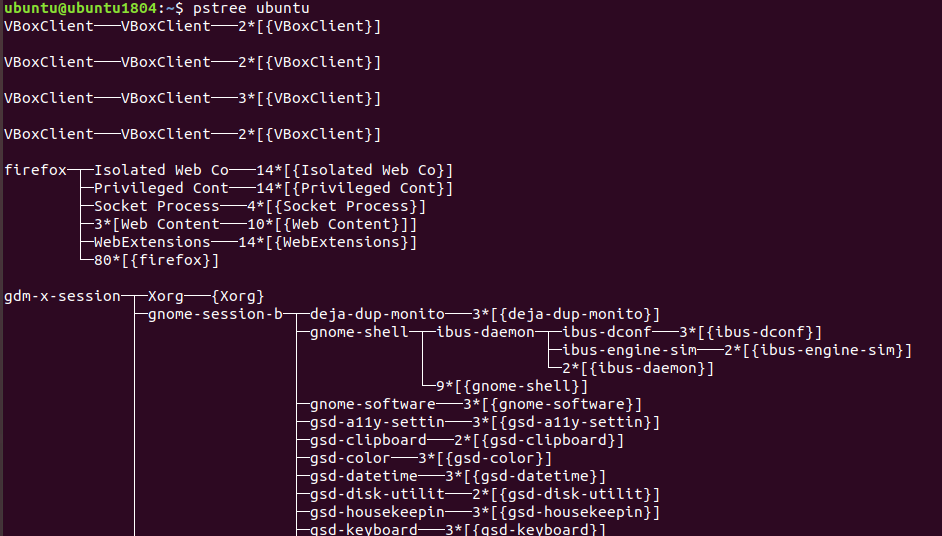


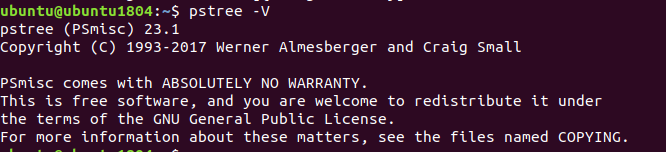










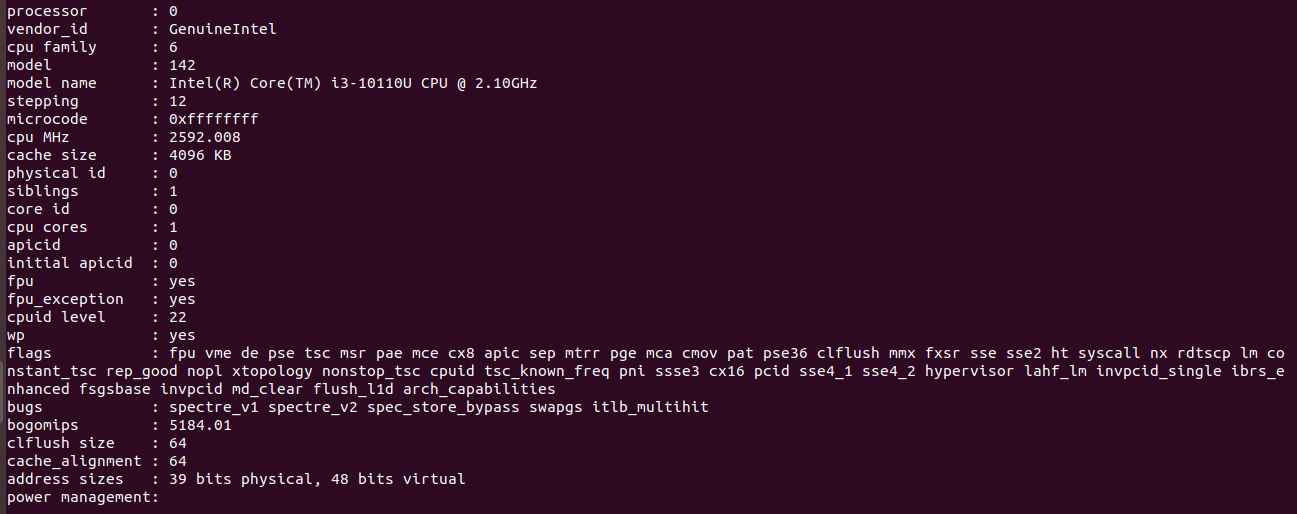


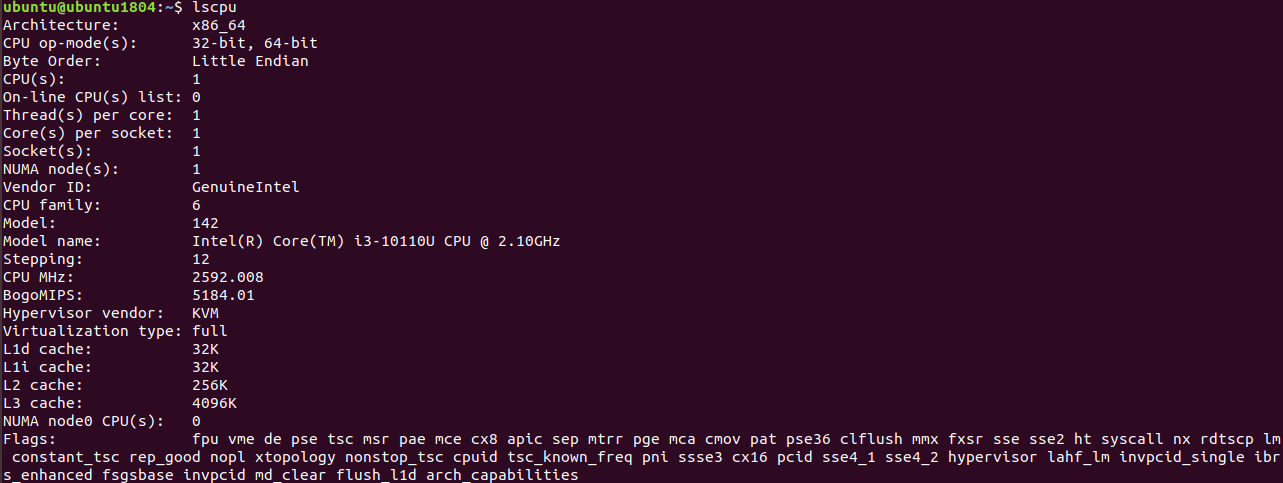
3. What is a proc file system?

The Proc file system (procfs) is a virtual file system that is created "on the fly" when the system boots and disintegrates when the system shuts down. It contains useful information about the processes currently running, it is treated as a control and information center for the kernel.

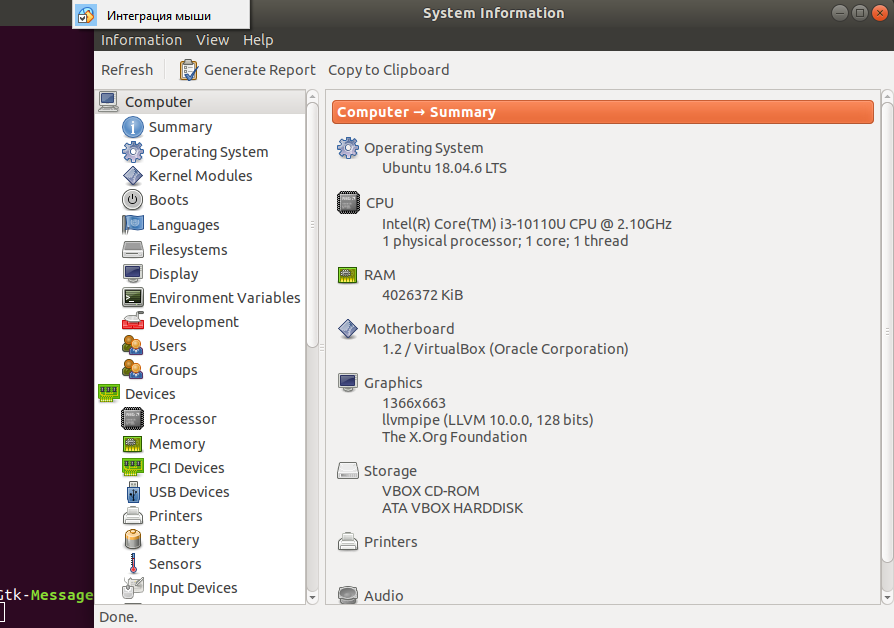
4. Print information about the processor (its type, supported technologies, etc.).

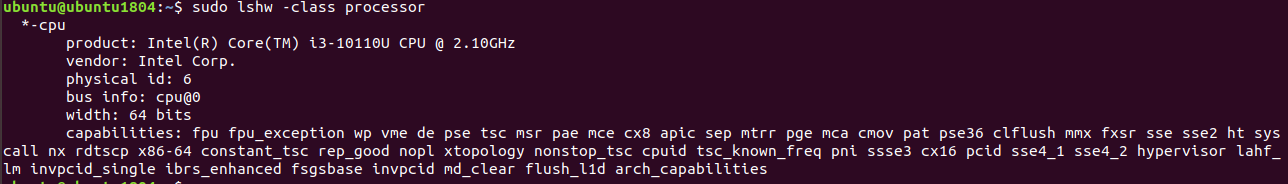




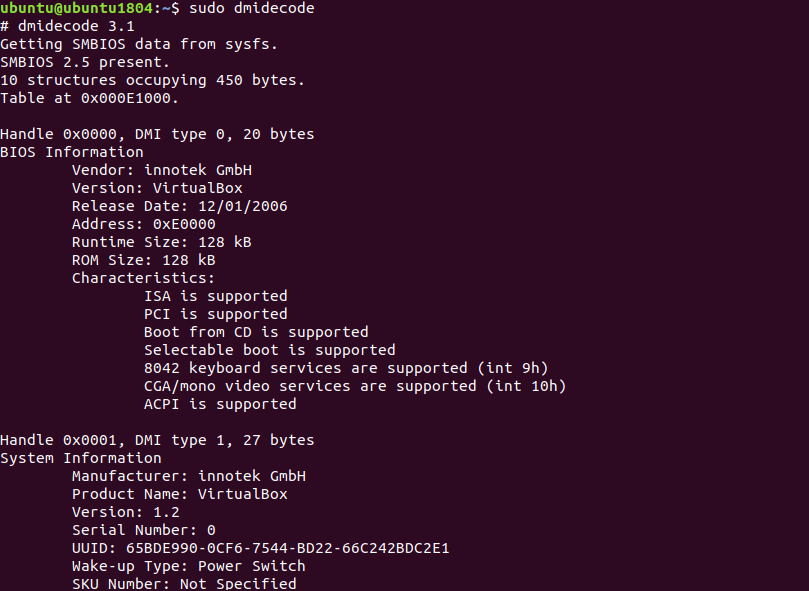






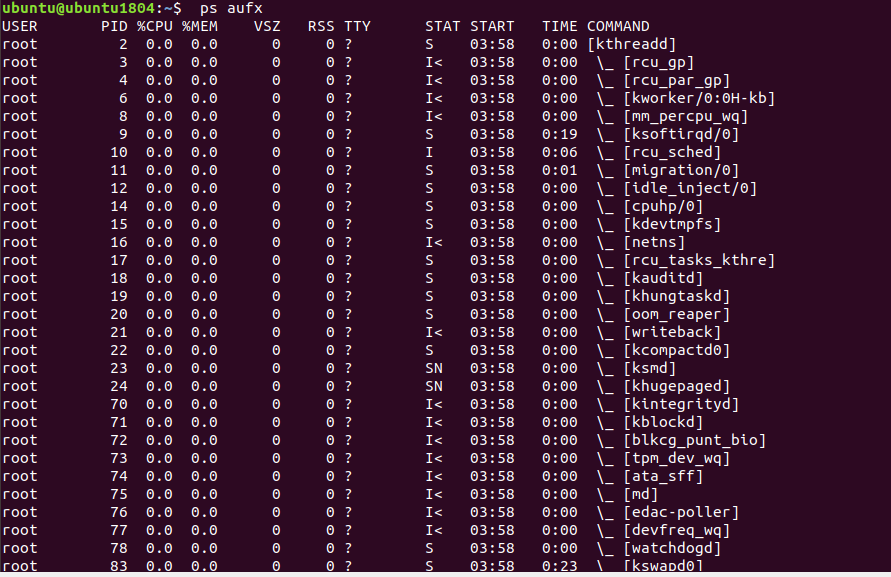


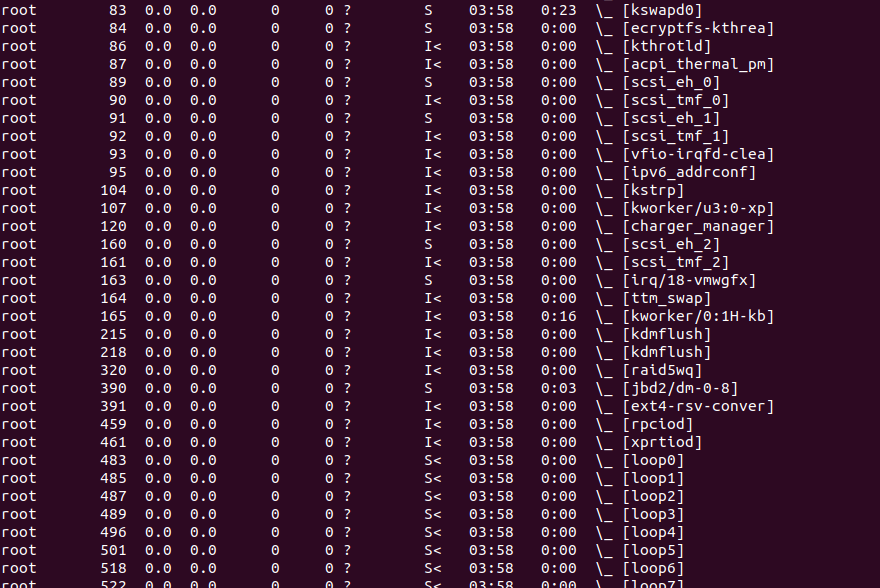






5. Use the ps command to get information about the process. The information should be as follows: the owner of the process, the arguments with which the process was launched for execution, the group owner of this process, etc.

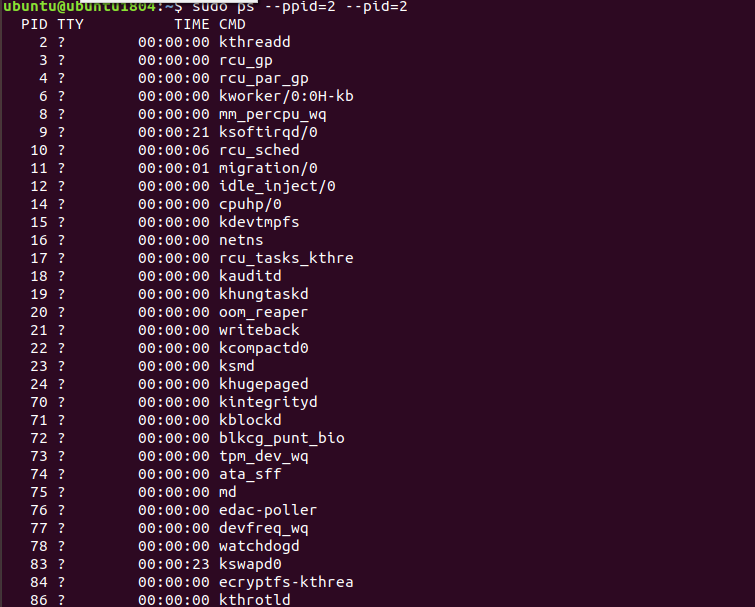




6. How to define kernel processes and user processes?

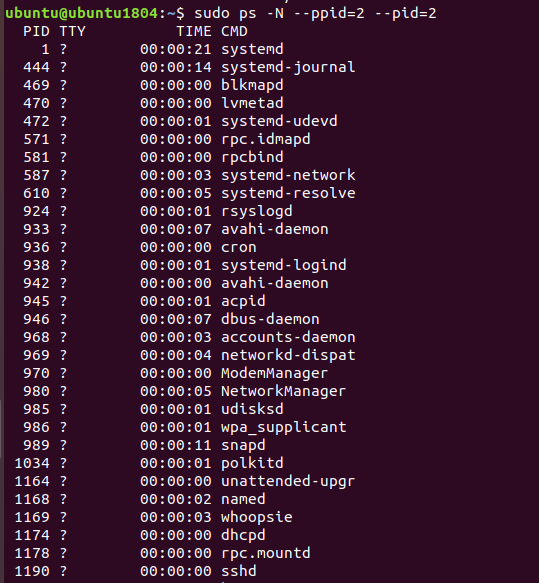
Command to define the kernel process:

sudo ps --ppid=2 --pid=2



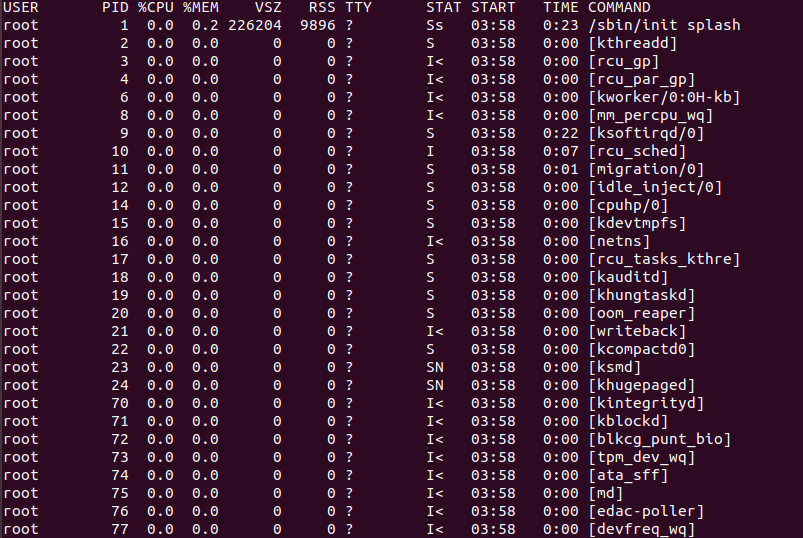
Command to define a user process:

sudo ps -N --ppid=2 --pid=2



7. Print the list of processes to the terminal. Briefly describe the statuses of the processes.What condition are they in, or can they be arriving in?

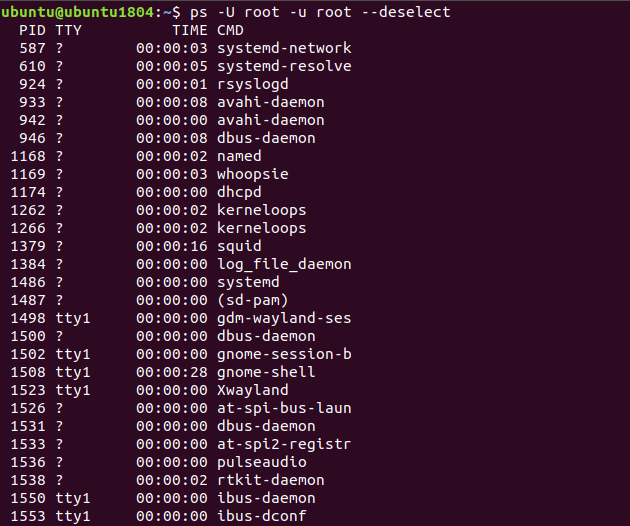




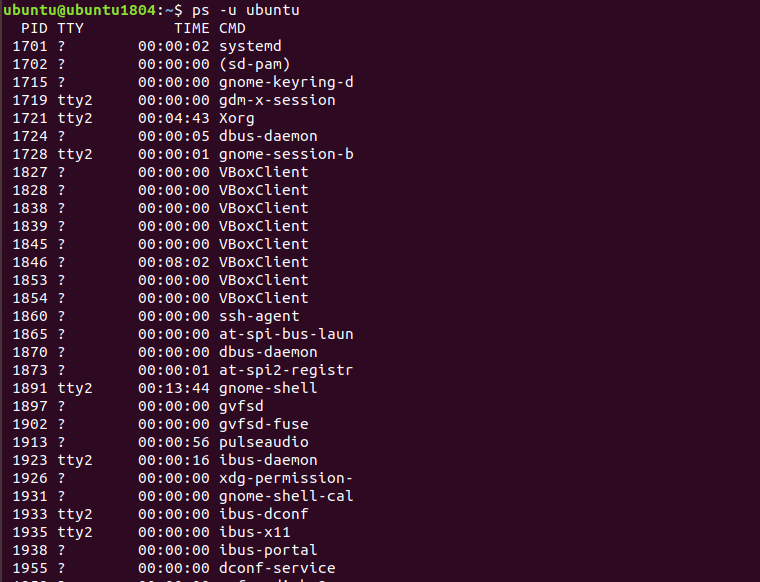
The option a specifies ps to display the processes of all users, except for those processes that are not associated with the terminal and leader group processes.

The u stands for user-oriented format, which provides detailed information about the processes.

The x option in ps lists processes without a controlling terminal. These are mainly processes which are started at boot time and run in the background.



8. Display only the processes of a specific user.

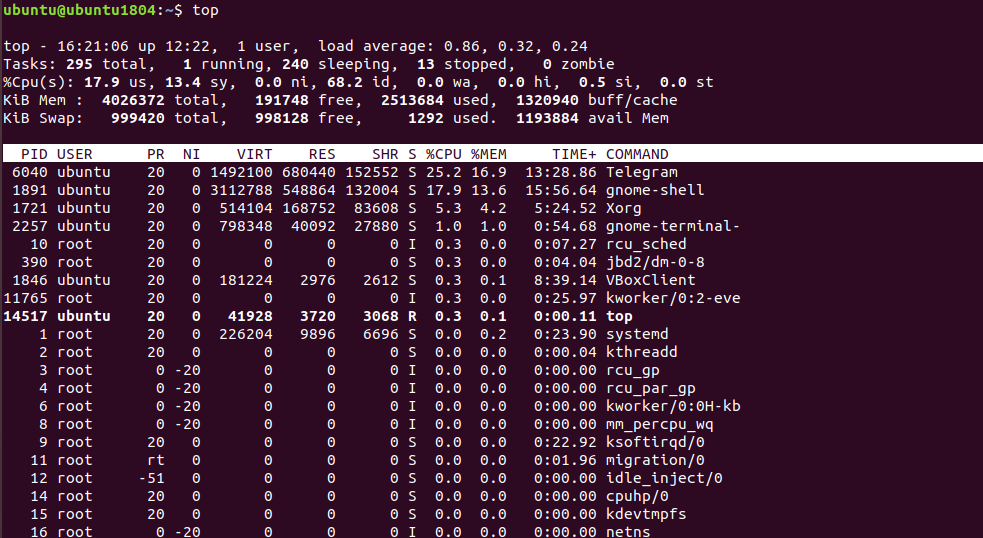


9. What utilities can be used to analyze existing running tasks (by analyzing the help for the ps command)?

free, fuser, htop, killall, pgrep, pidstat, pmap, pslog, pstree, pwdx, slabtop, systemd, systemd-cgls, systemd-firstboot, systemd-nspawn, tcpdump, tload, top, uptime, w, proc, credentials, pid\_namespaces, pthreads, sched, lsof, systemd-machined.service, tcpdump, vmstat

10. What information does top command display?

top command : Display and update sorted information about Linux processes.



The first two columns are the process number (PID) and the name of the user running it (USER).

The next 2 columns show the current process priority (PR) and the priority assigned to it by the NICE command (NI).

The information in the other columns directly describes the level of resource consumption. They are decoded in the following way:

\*\*VIRT - virtual memory used by the process

\*\*RES - physical memory used by the process

\*\*SHR - total amount of memory shared by the process with other processes

\*\*S - current status of the process: R - running; S - sleeping, Z - zombie

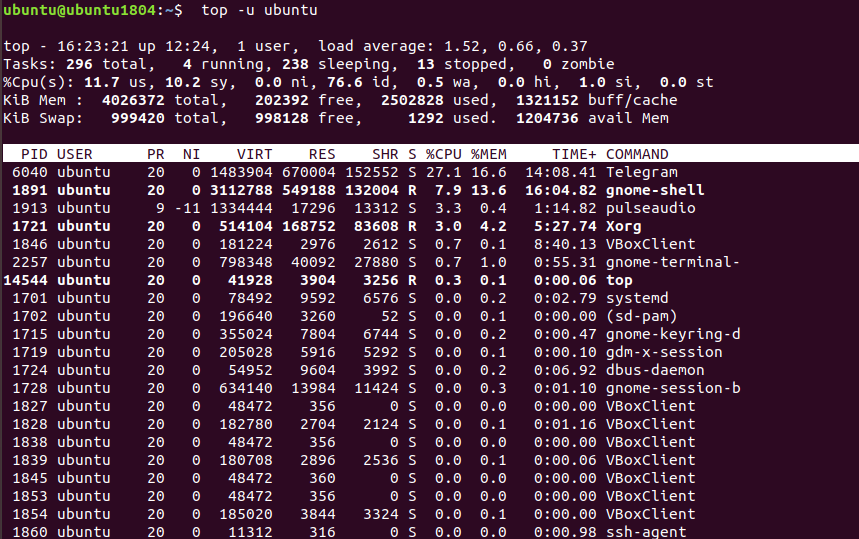
\*\*%CPU - percentage of CPU time used

\*\*%MEM - percentage of RAM used by the process

\*\*TIME+ - process duration since it started

\*\*COMMAND - name of the command (program) which initiated the process.

11. Display the processes of the specific user using the top command.



12. What interactive commands can be used to control the top command? Give a couple of examples.

h - outputs help for the utility;

q or Esc - exit top;

A - color scheme selection;

d or s - change the refresh interval of the information;

H - output process threads;

k - send signal to end process;

W - write current program settings to configuration file;

Y - view additional information about the process, open files, ports, logs, etc;

Z - change color scheme;

l - hide or display information about the average load on the system;

m - turn off or toggle the memory information display mode;

x - mark in bold the column by which the sorting is performed;

y - mark in bold the processes that are running at the moment;

z - switch between color and monochrome modes;

c - switches the mode of command output, full path and only command are available;

F - configuring of fields with information about the processes;

o - filtration of processes by arbitrary condition;

u - filtering of processes by user name;

V - displaying of the processes in the tree view;

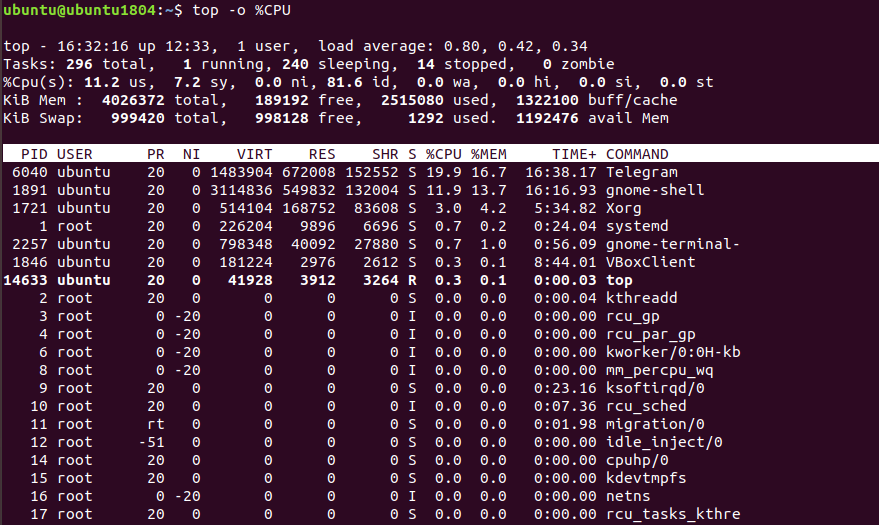
i - switching to displaying of the processes, which do not use the processor's resources at the moment;

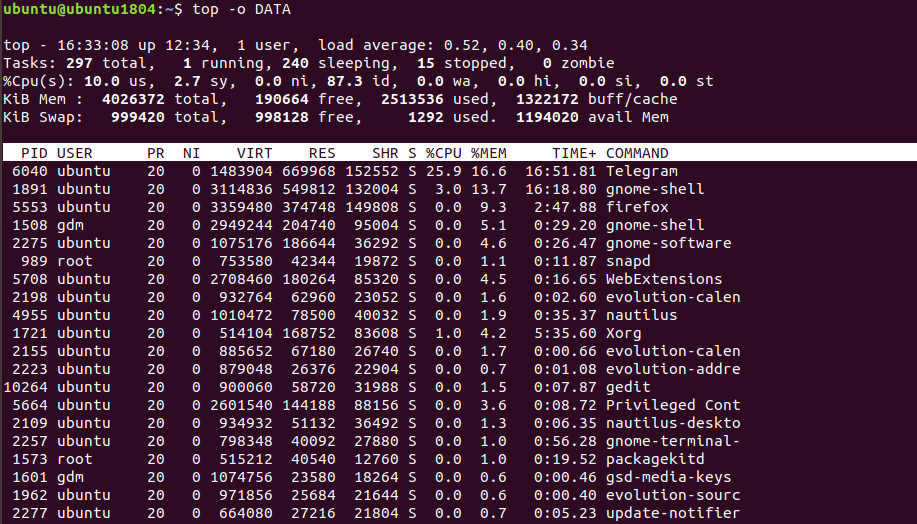
n - maximal number of processes to be shown in the program;

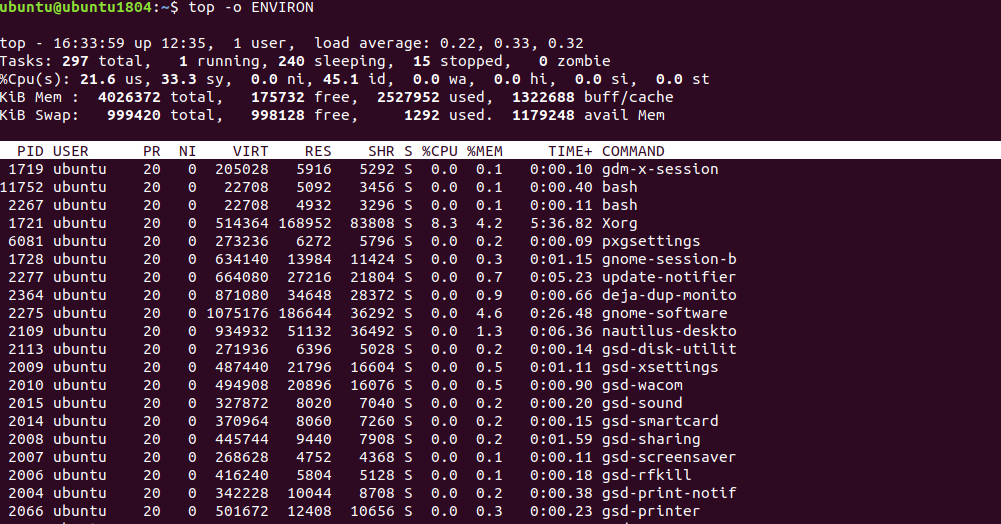
L - search by word;

<> - moves the sorting field to the right and to the left.

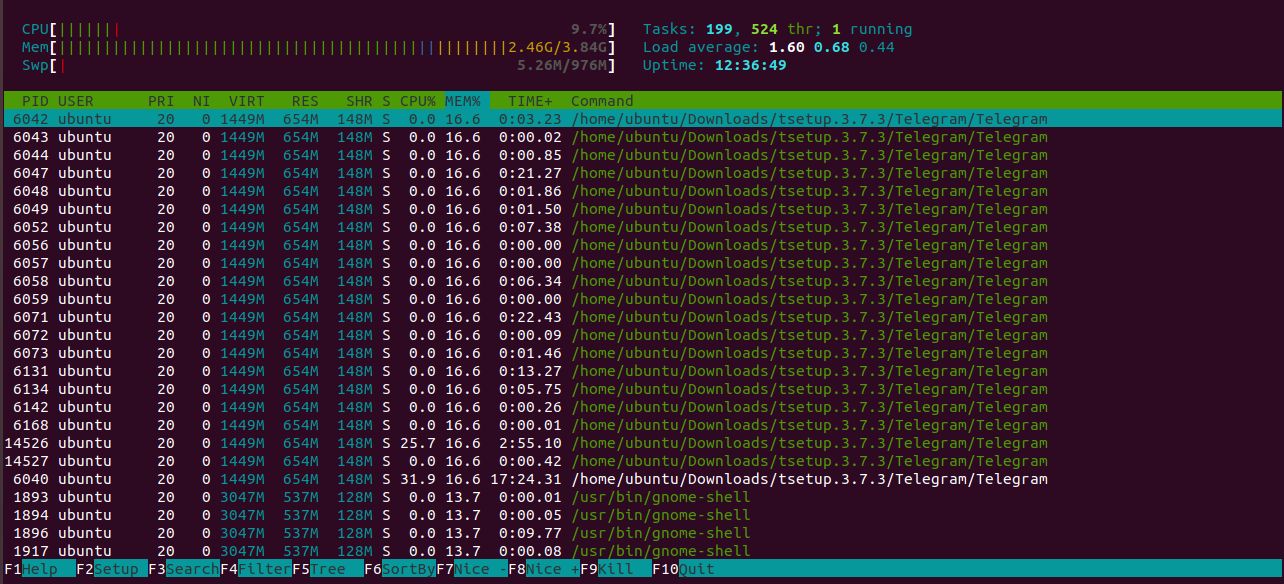
13. Sort the contents of the processes window using various parameters (for example, theamount of processor time taken up, etc.)











14. Concept of priority, what commands are used to set priority?

The priority of a linux process means how much more CPU time will be given to that process than to others.

The nice and renice commands are used to set the priority.

15. Can I change the priority of a process using the top command?If so, how?

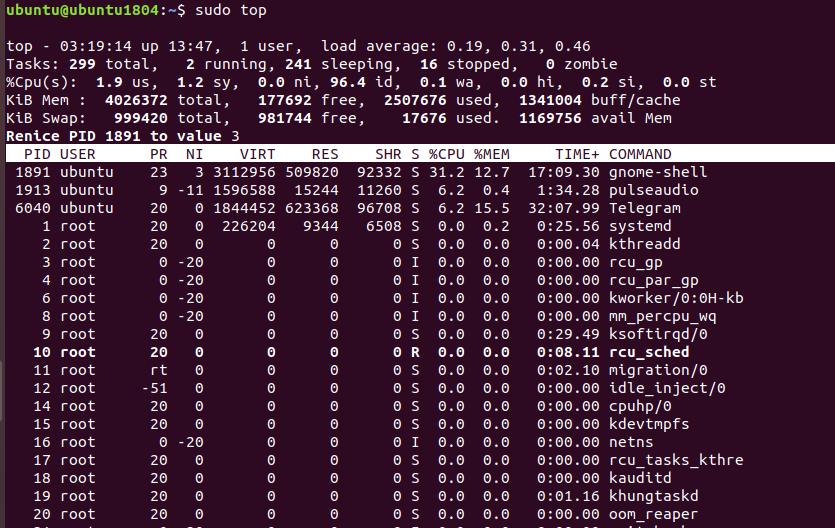
The top command allows you to change the priority of the process.

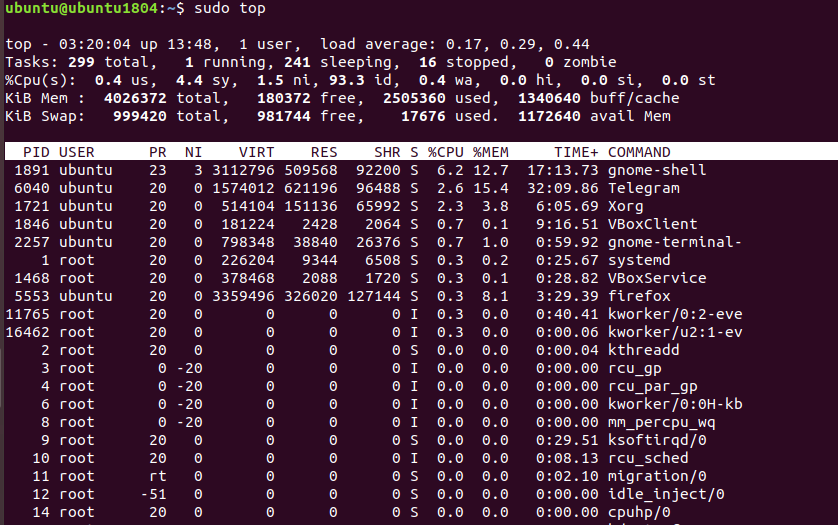
Procedure:

1. Start top and press the r key.

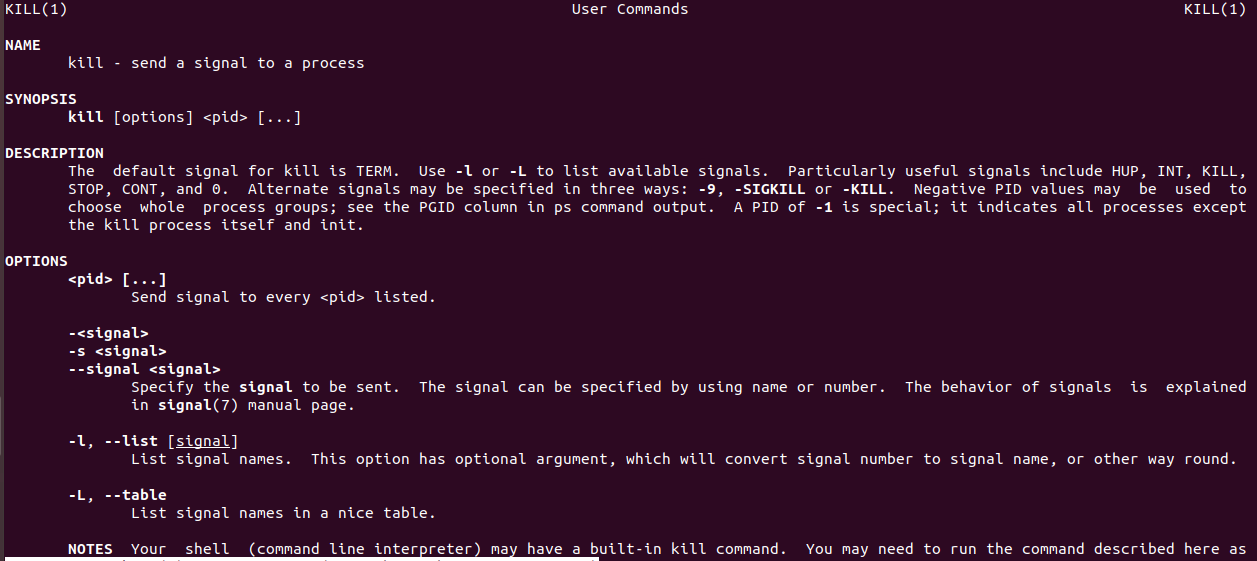
2. When prompted, enter the process ID and press Enter.

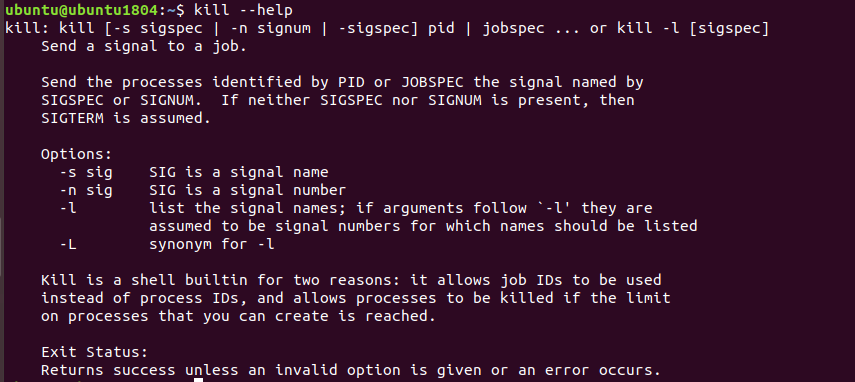
3. After entering the PID, the program prompts for a new nice value. Enter the new value and press Enter.

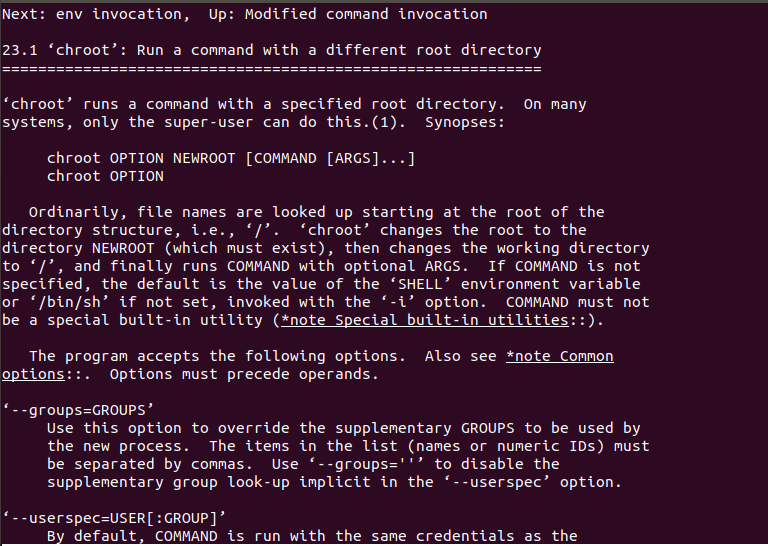


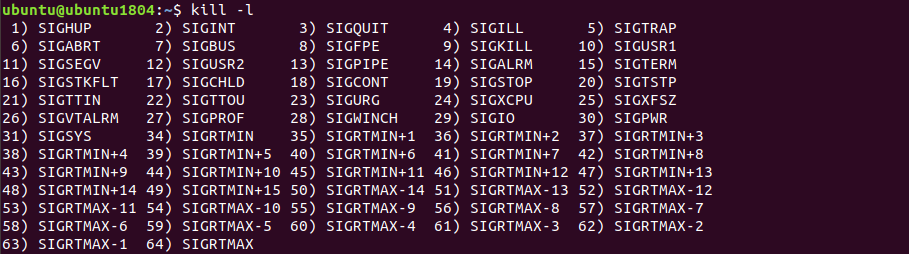


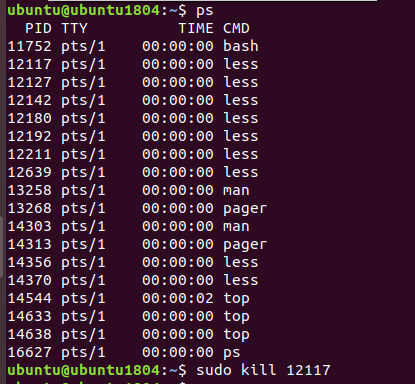
16. Examine the kill command. How to send with the kill commandprocess control signal? Give an example of commonly used signals.

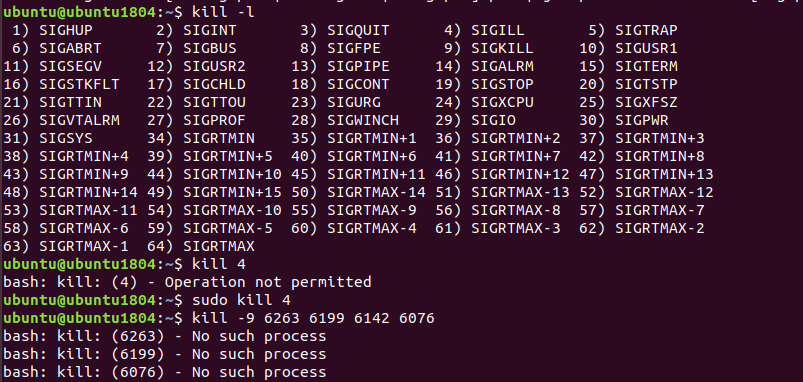




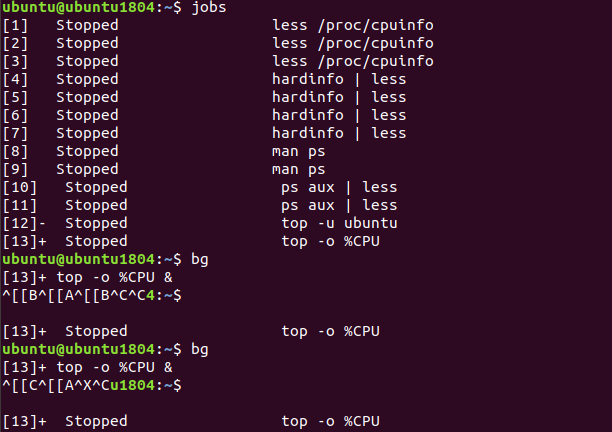






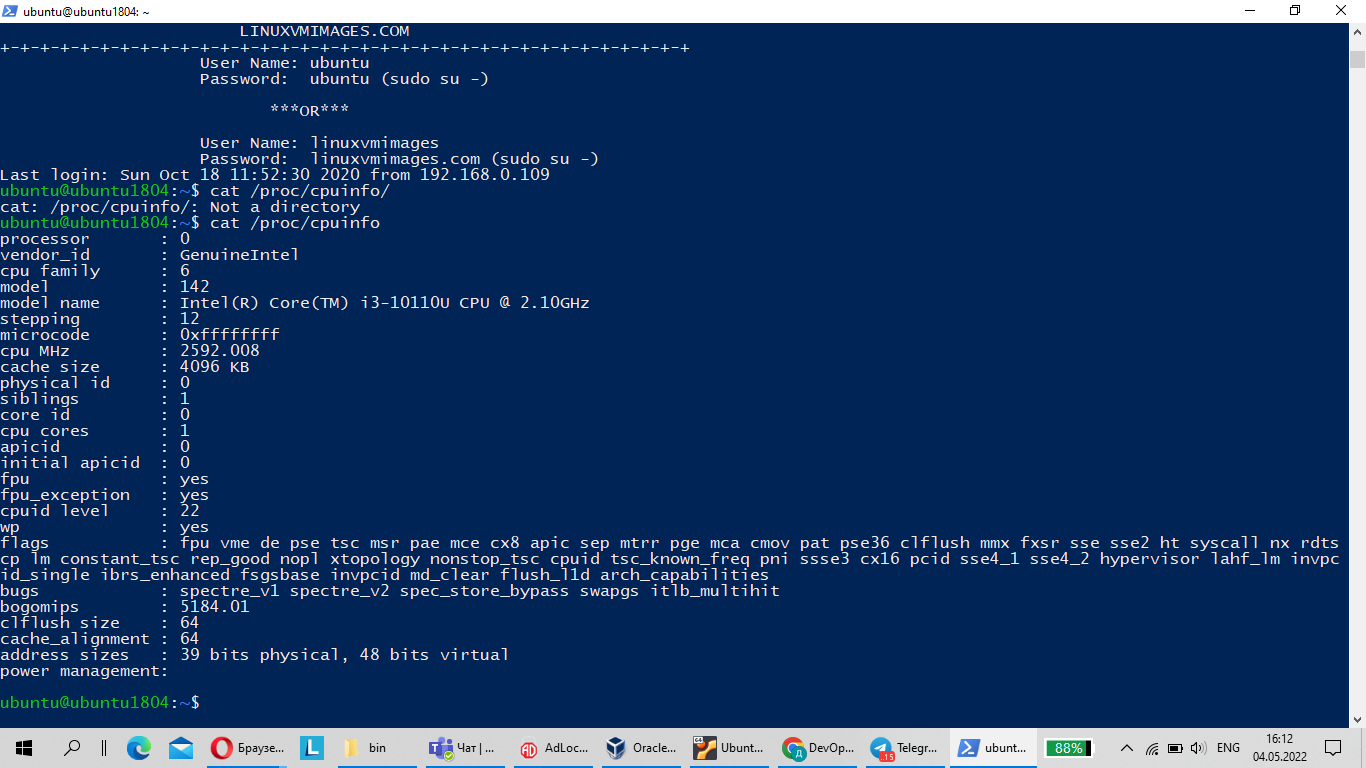


17. Commands jobs, fg, bg, nohup. What are they for? Use the sleep, yes command todemonstrate the process control mechanism with fg, bg.



Part2

1. Check the implementability of the most frequently used OPENSSH commands in the MSWindows operating system. (Description of the expected result of the commands +screenshots: command –result should be presented)

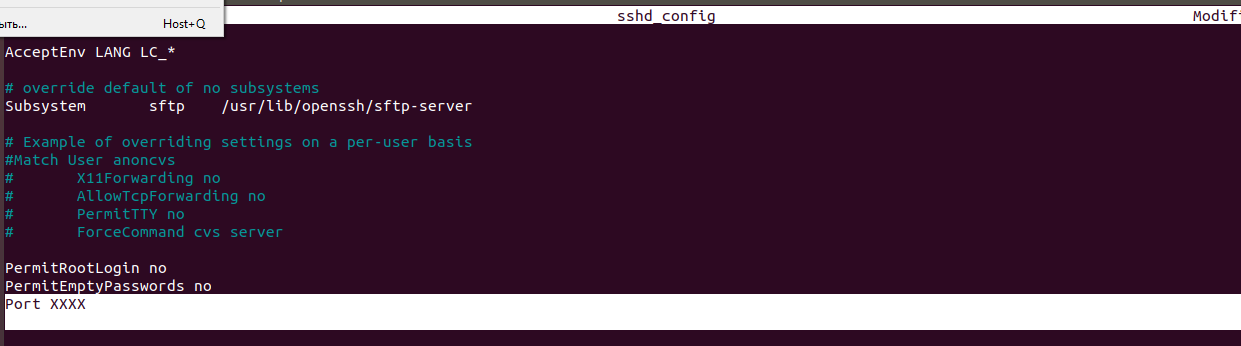


1. Implement basic SSH settings to increase the security of the client-server connection (at least)

Disabling blank passwords.

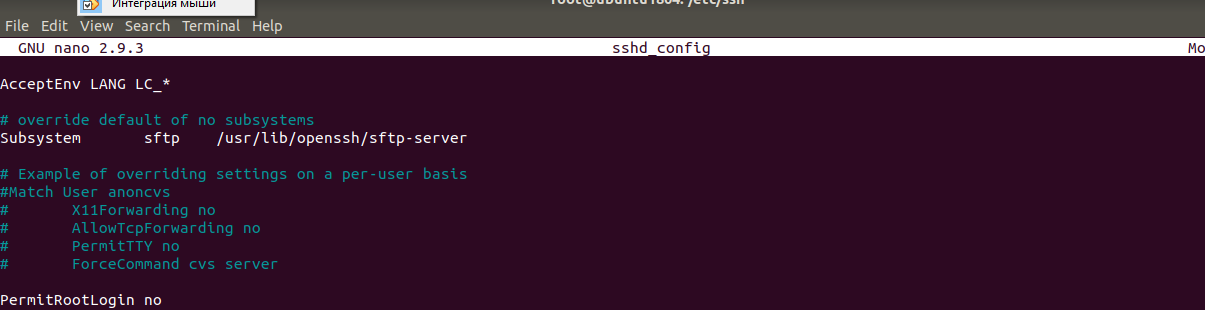


Change the port.

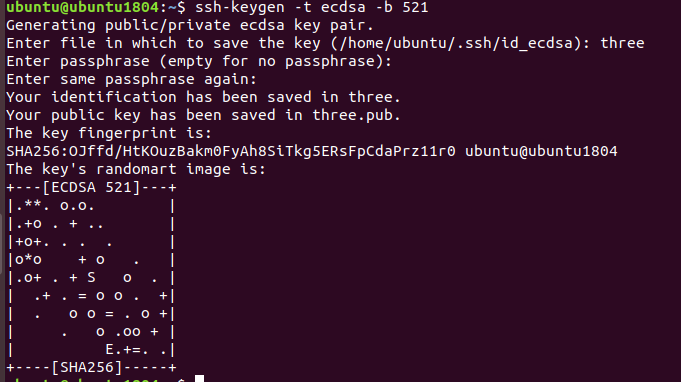


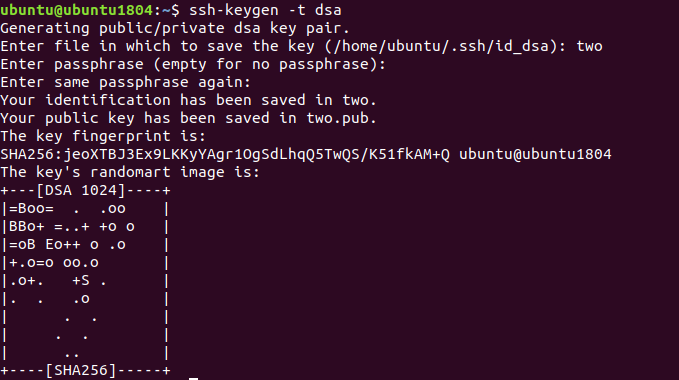
ХХХХ is the port value that will be ready for use.

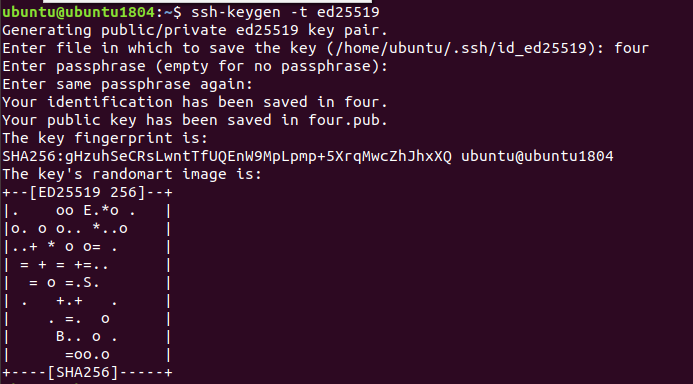
# Disable root login



3. List the options for choosing keys for encryption in SSH. Implement 3 of them.







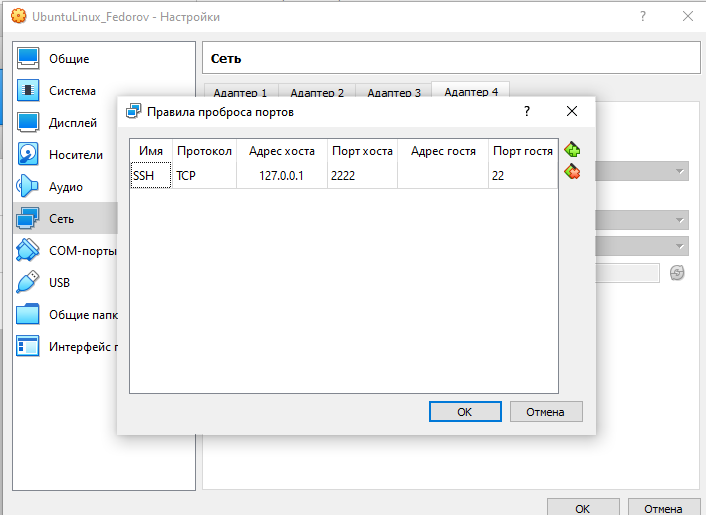
ssh-keygen -t rsa

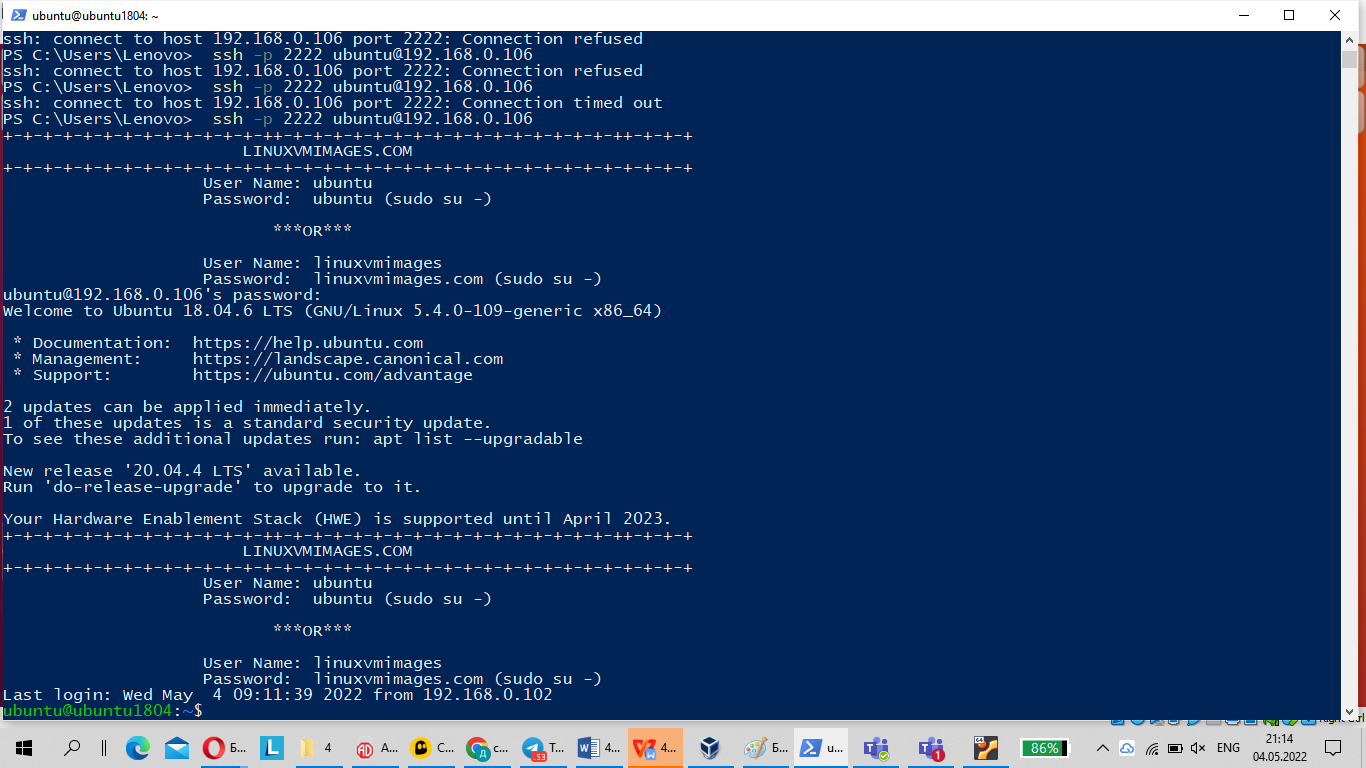
ssh-keygen -t dsa

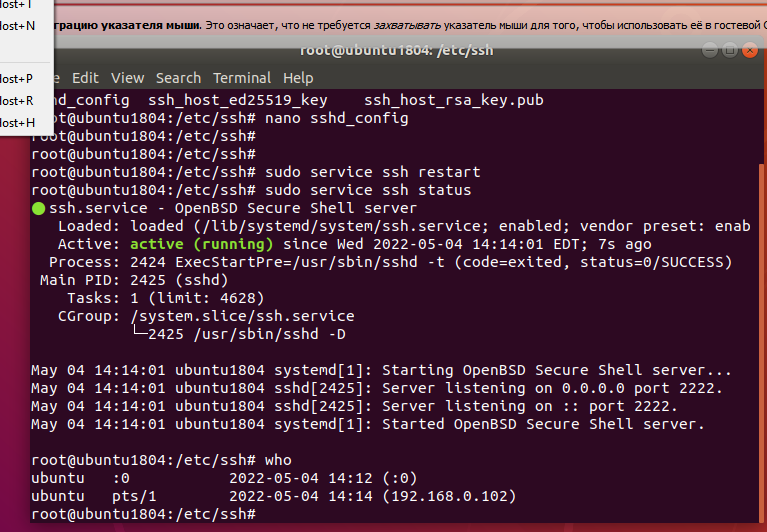
ssh-keygen -t ecdsa

ssh-keygen -t ed25519

4.Implement port forwarding for the SSH client from the host machine to the guest Linuxvirtual machine behind NAT.







5. Intercept (capture) traffic (tcpdump, wireshark) while authorizing the remote client on theserver using ssh, telnet, rlogin. Analyze the result.

tcpdump -vv -i any -nn port 22 -w tcp.pcap

tcpdump -vv -i any -nn port 23 -w tcp.pcap