

RAT Protocol

The client opens a connection with the server and *informs* the server whether it wants to *Reboot* the system or *Capture the system* or *List* the running processes using a *header*.

Reboot

If the client wants to reboot the system, then the header will be as the following:

- **reboot[one space][line_feed]**

Upon receiving this header, the server will be rebooted for 5 seconds.

The sample output produced by this program is:

Shutting down the PC after 5 seconds.

List

If the client wishes to receive the list of running processes in the server ,the header will be as following:

- **List[one space][line_feed]**

After sending the header, the client shall send the bytes of the file

The remote machine receives the List header and it will send the list of running process back to the client to read it.

Capture

If the client wants to receive the screenshots of the remote system, the header will be as following:

- **Capture [one space][line_feed]**

If the file is not found, then the server shall reply with a header as the following:

- **Capture [one space]ERROR[Line Feed]**

If the screenshot is done, so it will be generated in the server, the server will reply with a header as following

- **NOT[one space]FOUND[Line Feed]**
- If the file is found, then the server shall reply with a header as the following:
 - **OK[one space][file size][Line Feed]**
 - o Followed by the bytes of the file