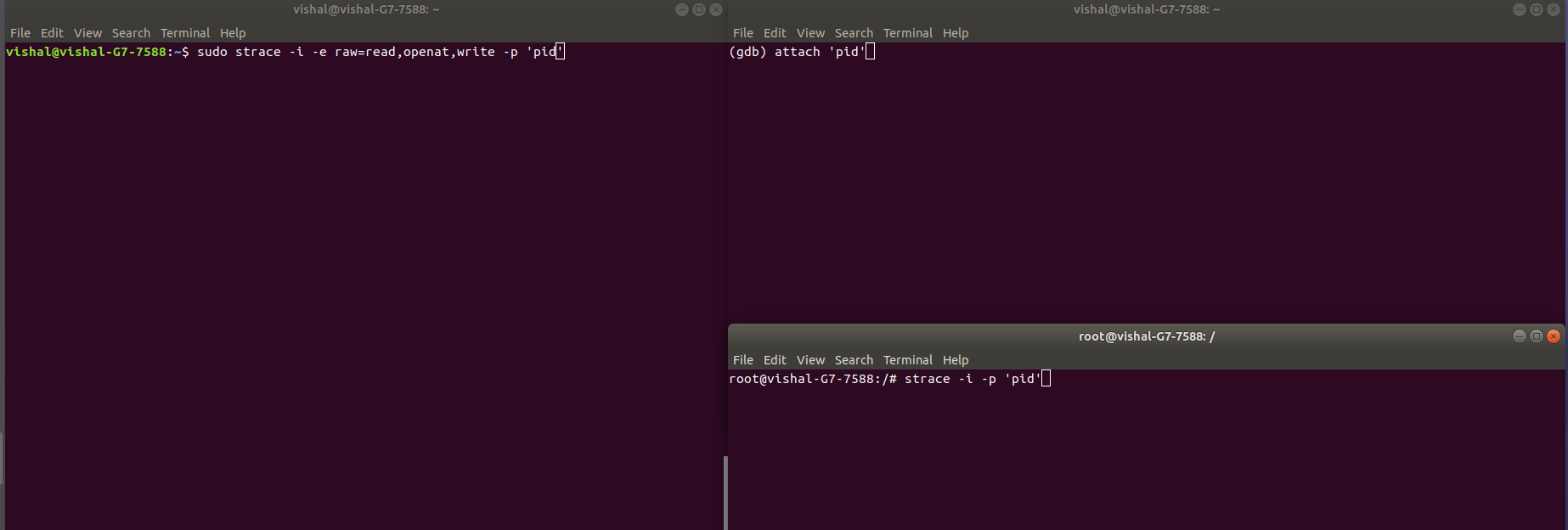
**Lastpass Linux Report**

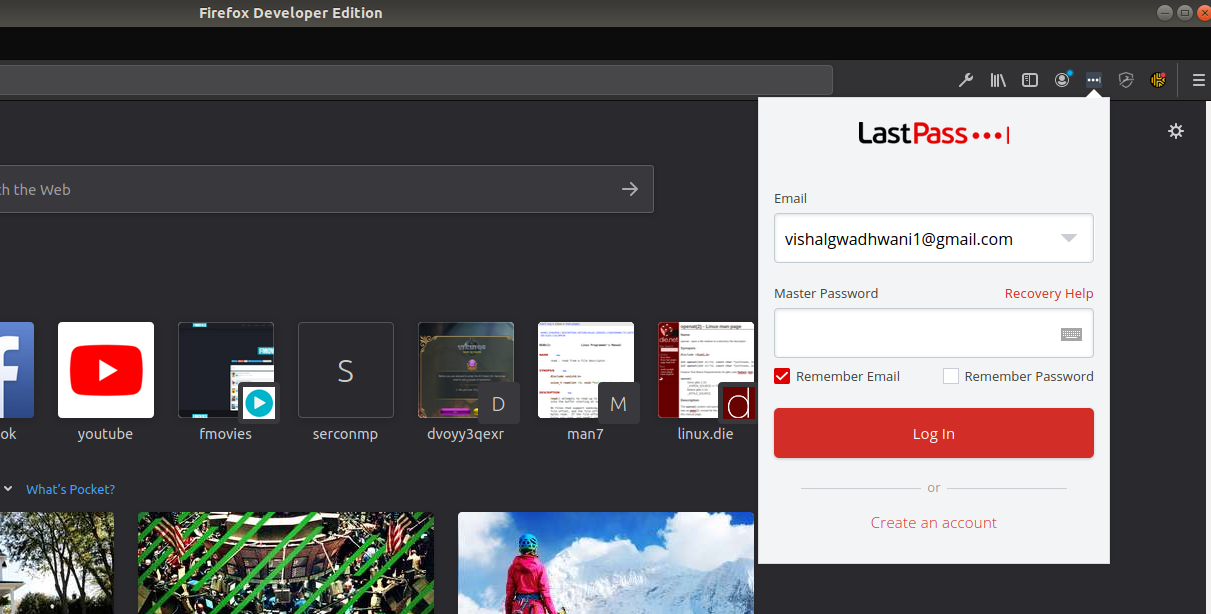
**(Note : The main information that we found out was that Lastpass’s linux process sets up multiple buffers in memory for different purposes. Everytime it has to achieve the same purpose, it rewrites the data in the buffer instead of clearing it out and then writing into it.)**

1. **Debugging setup :**
2. Trace for system call with raw memory details
3. Gdb attached to the process for checking memory
4. Trace for system call with runtime memory details

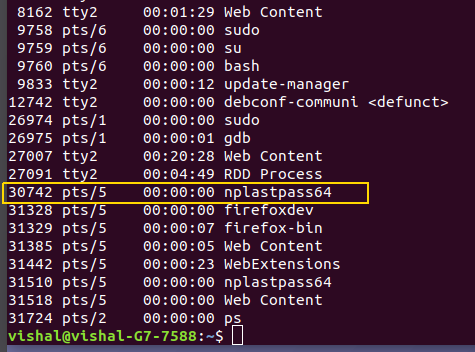
****

**2. Start by checking the initial commands provided to the process by fd=0. (This can be done by starting the browser and a new lastpass out of extension process spawns. Don’t login at this moment.)**

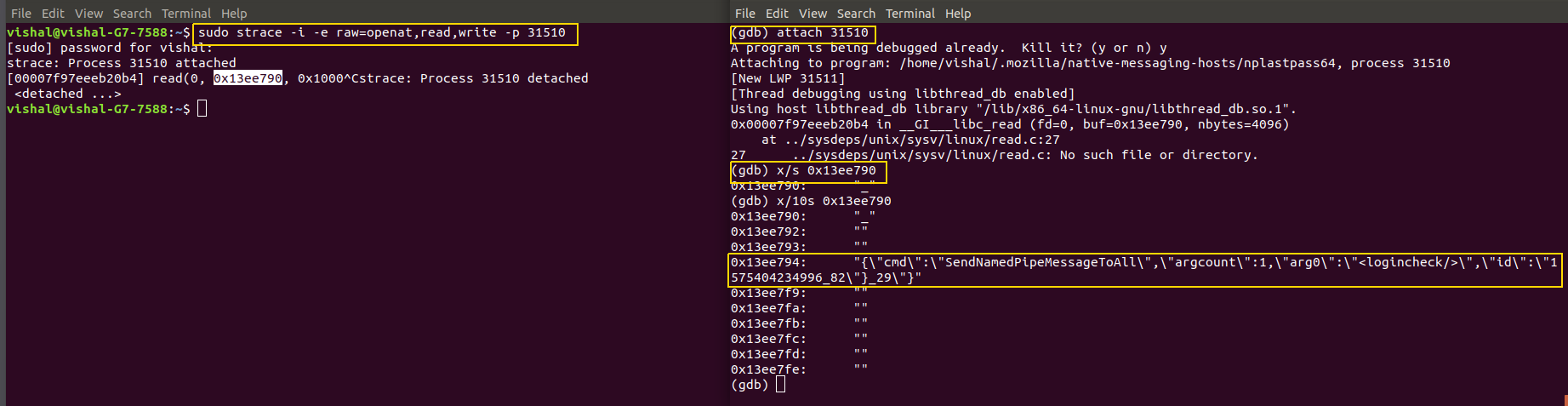
1. Browser opened and lastpass isn’t logged in.

****

1. New out of extension process is spawned.



1. Initiating the debugging setup with the latest pid i.e. in our case 31510.



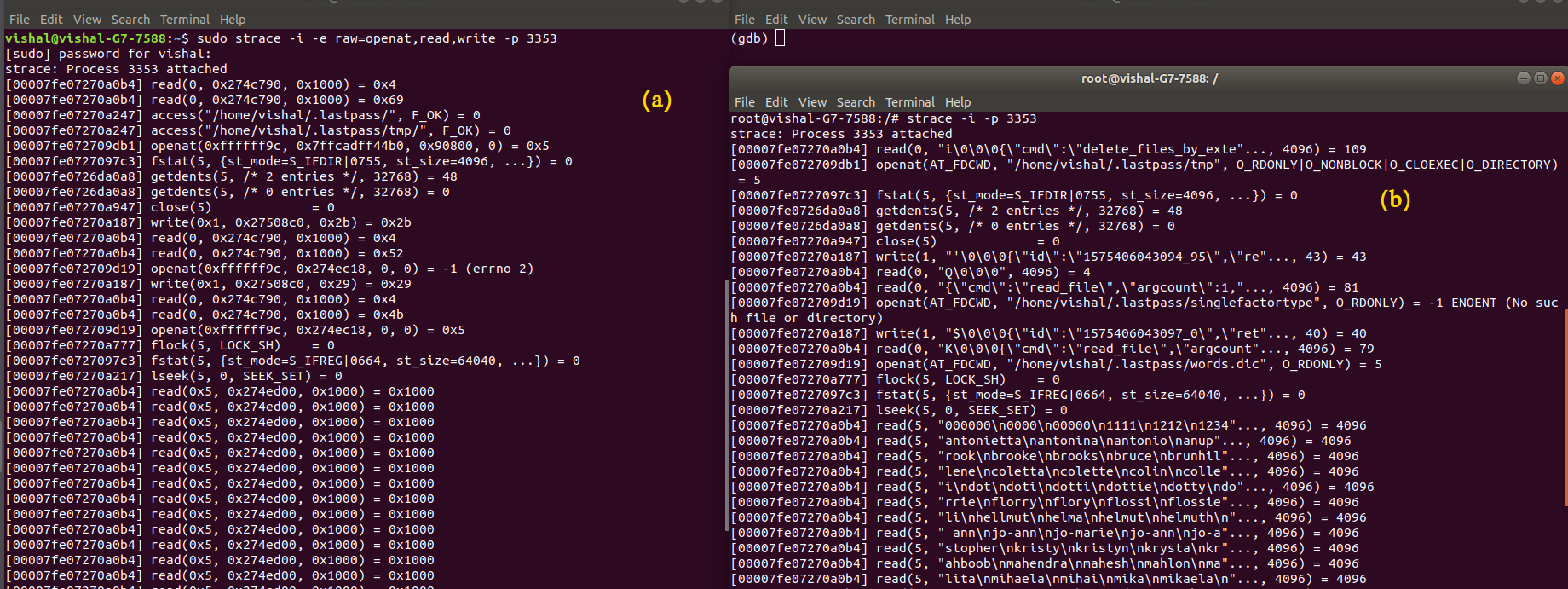
*Observations : The Basic process communication happens with the following command structure.*

*“{\"cmd\":\"SendNamedPipeMessageToAll\",\"argcount\":1,\"arg0\":\"<logincheck/>\",\"id\":\"1575404234996\_82\"}\_29\"}”*

*(Highlighted command gives us the idea that the process is performing a login check. Now since we have not entered the password, this is the first message that we could extract from the memory buffer whose offset was obtained from the processes system call trace.)*

**2. Now, we log in with the legitimate password and logout and analyse the system calls trace and buffer memory after that.**

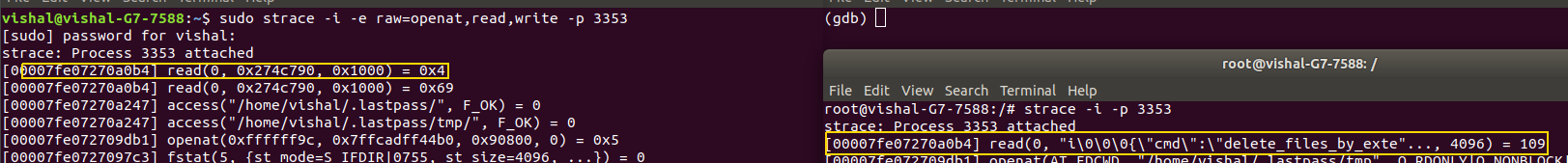
1. **Raw Trace**
2. **Trace with data in the buffer at runtime.**

****

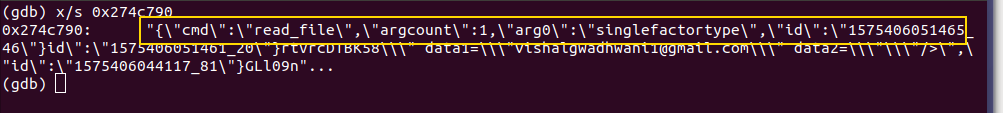
**Figures (a) and (b) are similar traces. The only difference is the raw trace contains the physical addresses of the buffers whereas the normal trace contains the data in buffer at runtime.**

1. **As per the note described, Laspass overwrites buffers. Proof of that is shown below.**

* **Buffer values during runtime**

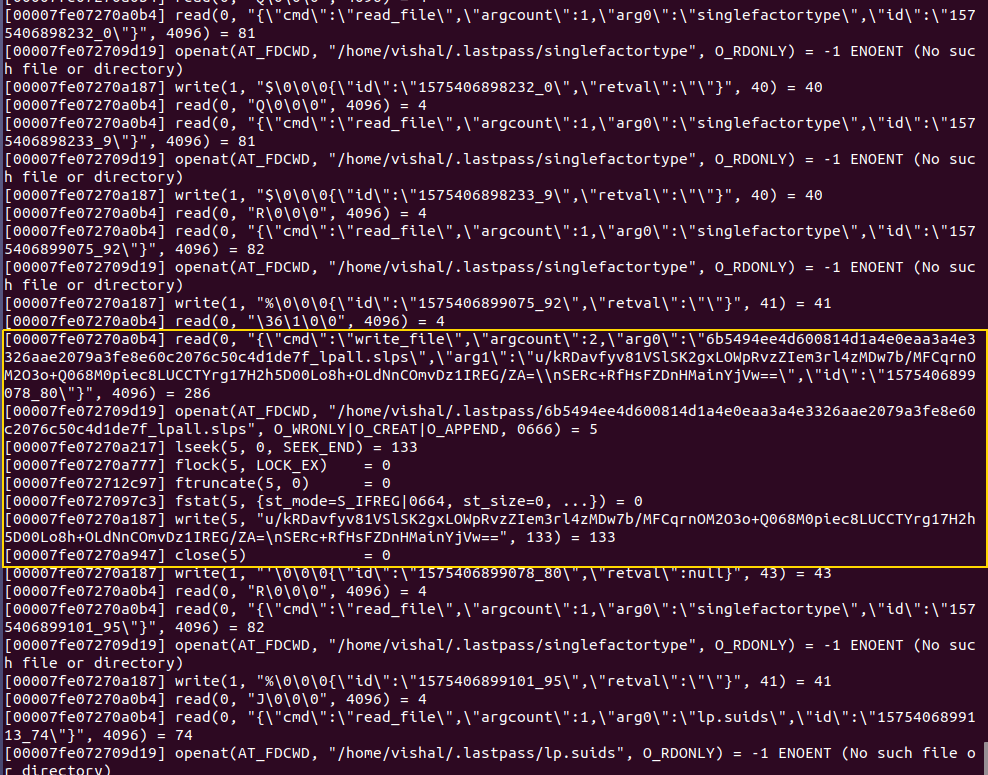
****

* **Buffer values currently in memory**

**

*Observations : Username is passed in plain text.*

1. **Scanning through the trace.**

****

*Observations : The contents of this file are altered at every login.*

*Explanation : (Explain the highlighted part)*

*Proof : Provide the previous and new contents of the file.*