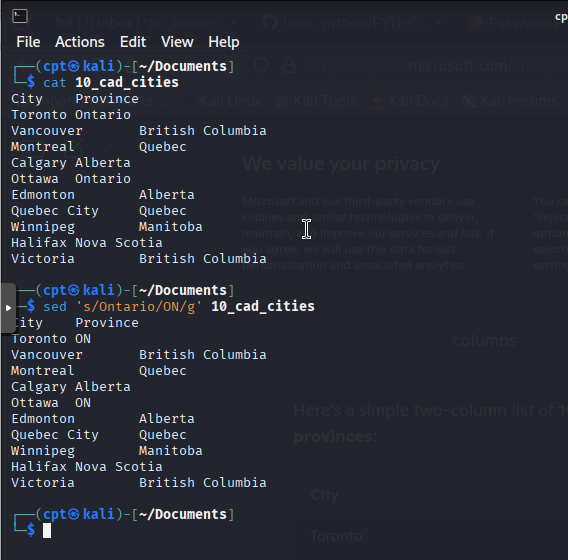
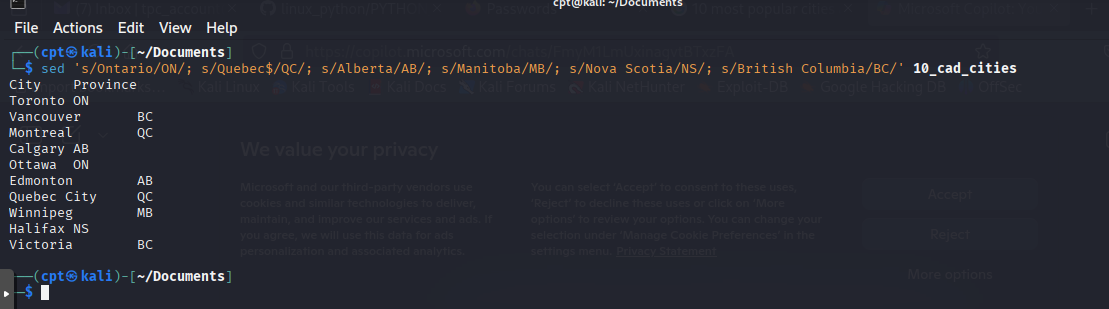
Very often in cyber security, analyst has to perform so called “non-interactive” stream-oriented editing. Usually this comes from necessity to process a large ASCII files that regular editor would be able to perform at all and resulted in GUI handing of the program. Even so efficient command line Linux based editor as “vim” would failed to do this job. Sometime simple well-known tools as “cut”, “grep”, “tr” as sufficient but in other case non-interative editors as “sed” and “awk” must be utilized.

Out of the two, sed is more minimalistic and it is not a bad approach of using appropriate tool for the appropriate job and avoid overkill. We’ll concentrate on it in this part1. And part2 will be dedicated to more advanced editor called awk that particularly appropriate for parsing “zeek” output files.

The simplest example of using sed is what one word/pattern must be found and replaced on another. In the example below we replace “Ontario” to “ON”.



If there is a need to perform a few replacement on the same document, it’s also not an issue.



(Note: try to understand why for Quebec province replacement I had to use character $).