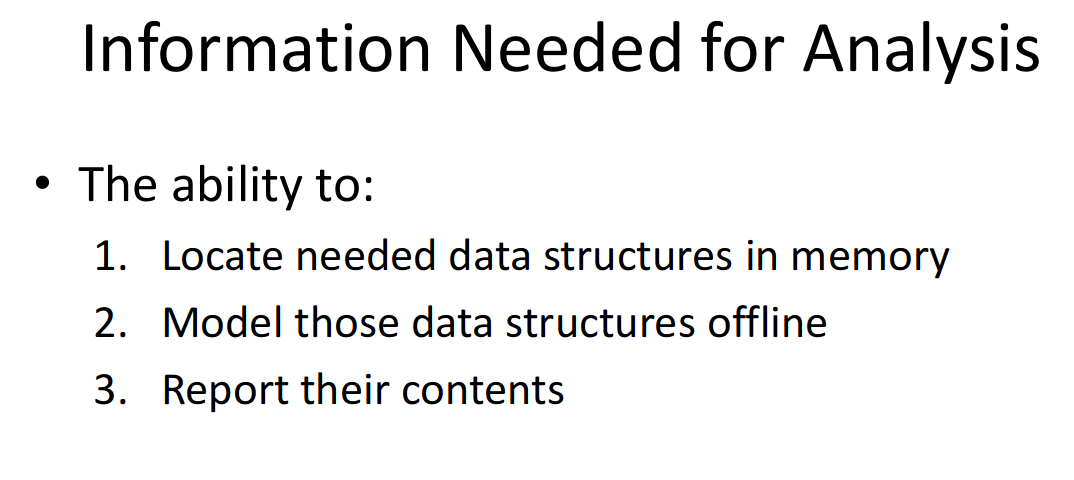
**Performing Memory Analysis (Ubuntu)**

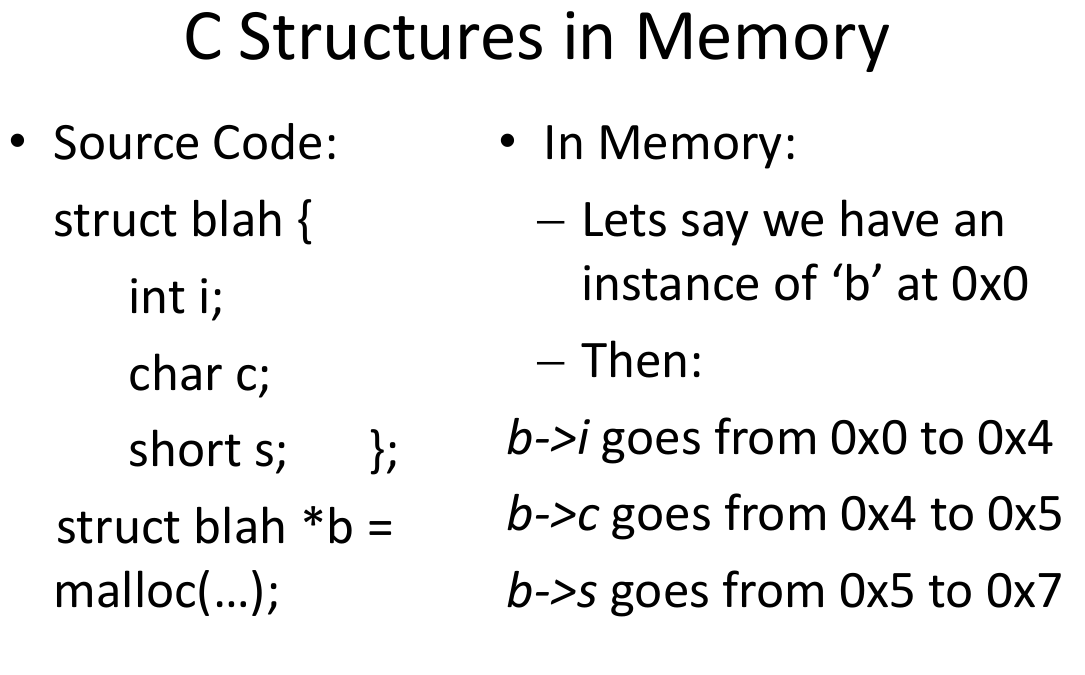
References : https://media.blackhat.com/bh-us-11/Case/BH\_US\_11\_Case\_Linux\_Slides.pdf

****

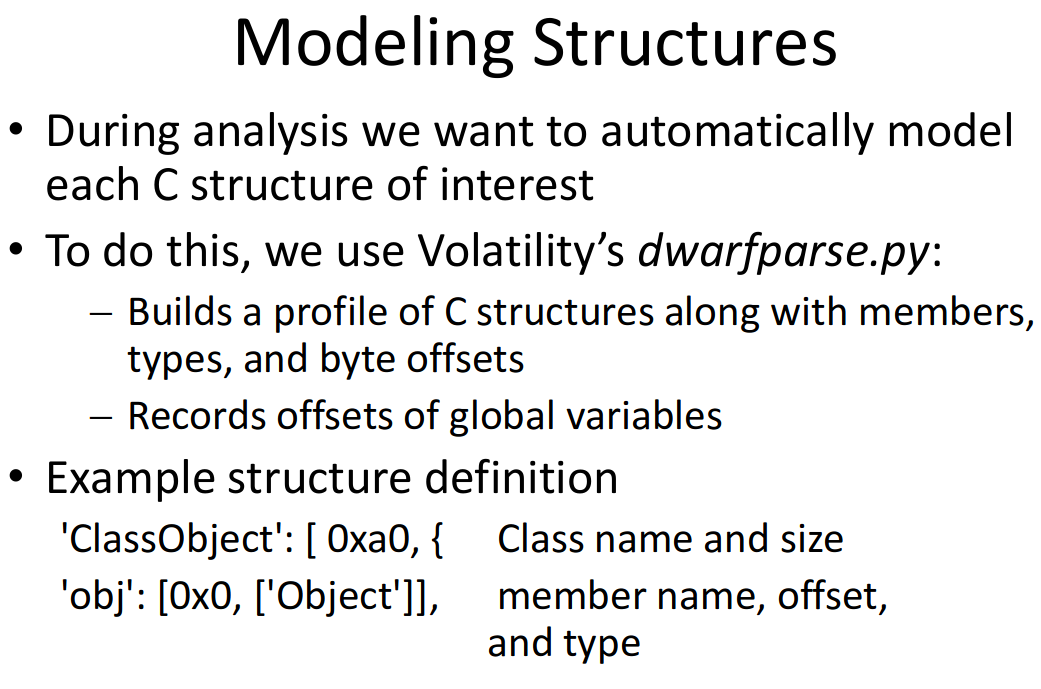
**To locate static data structures :**

System.map file :

Contains the name and address of every static data structure used in the kernel.

****

dwarfparse.py (In Volatility)

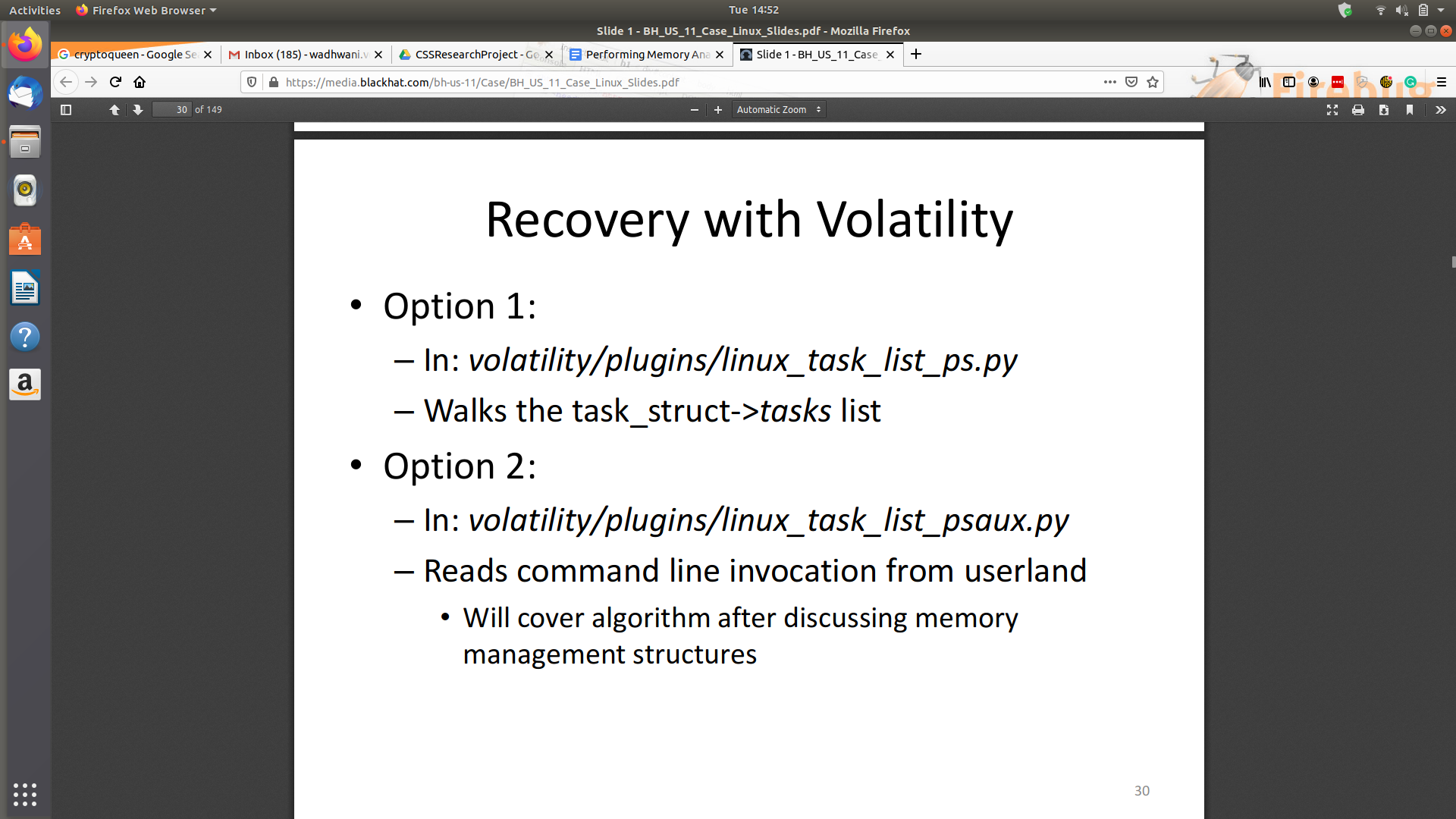
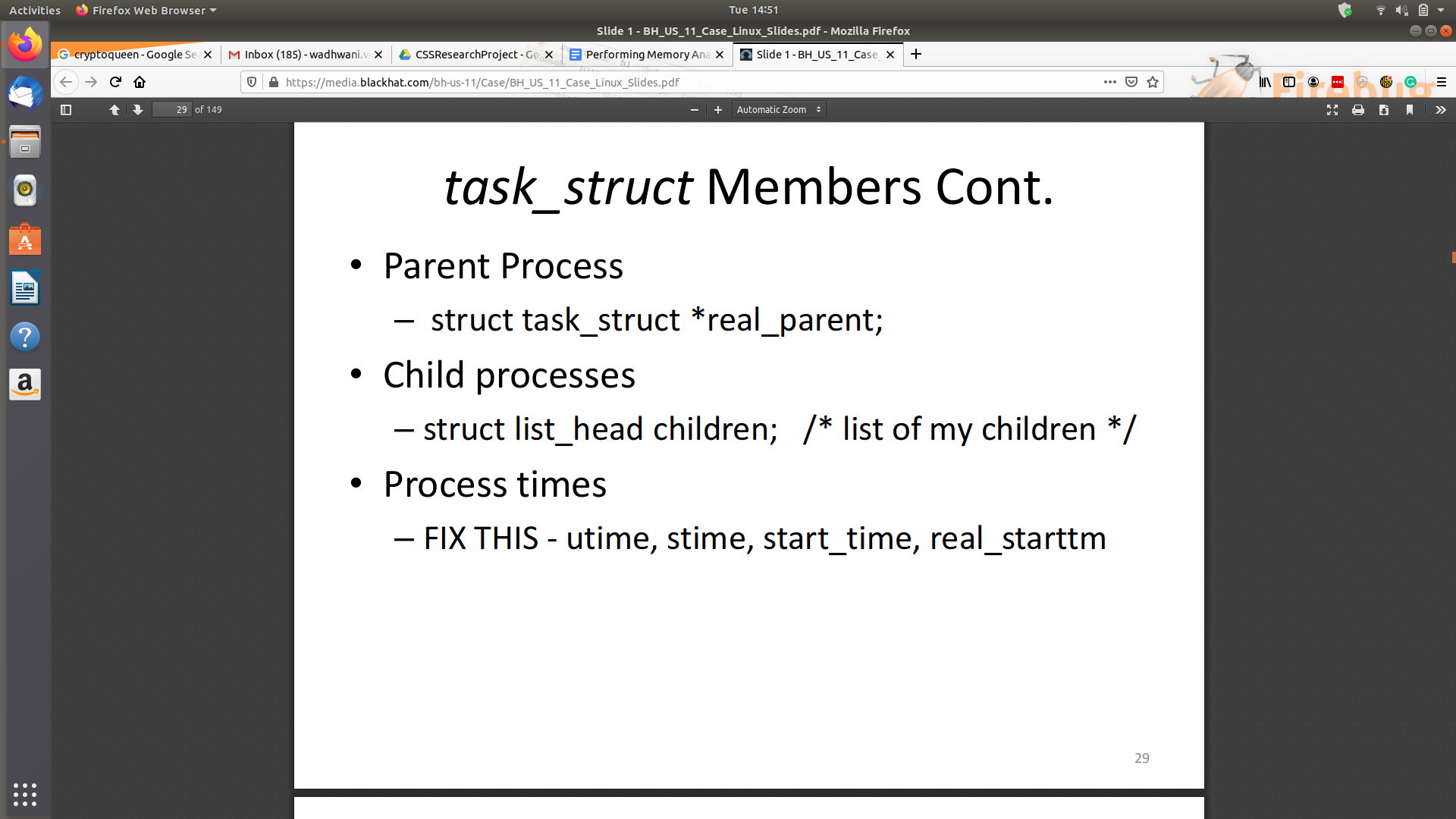
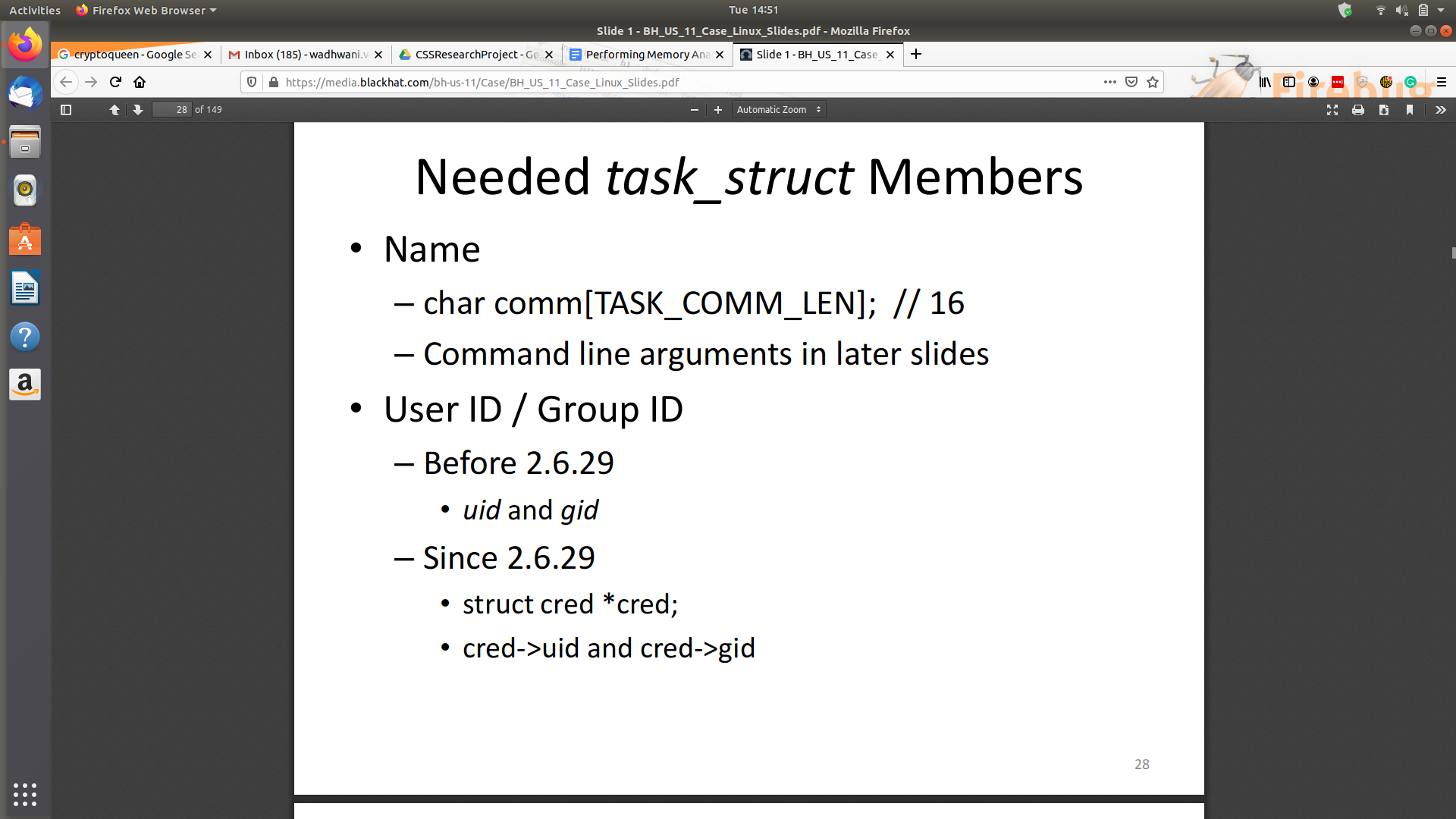
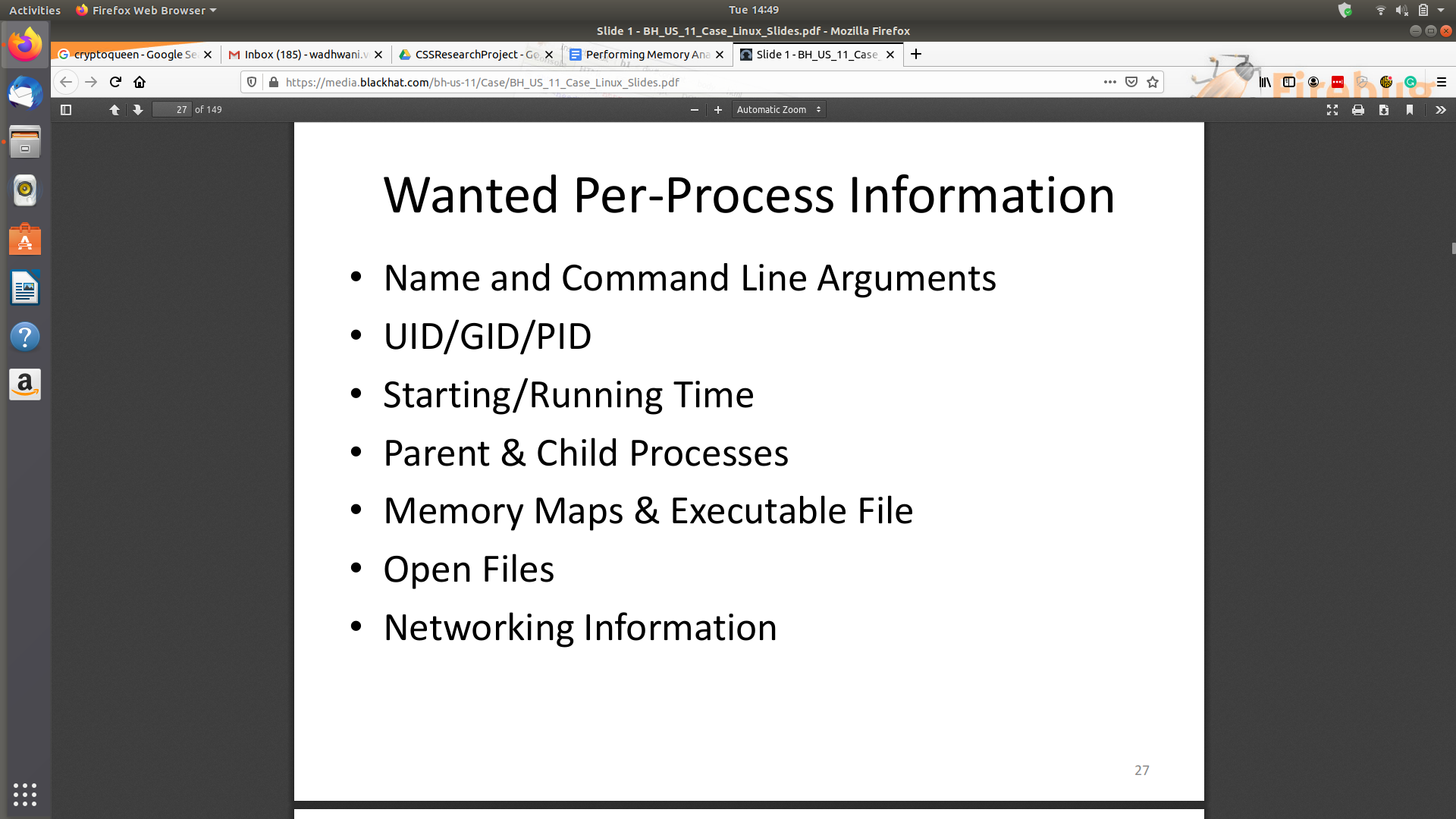
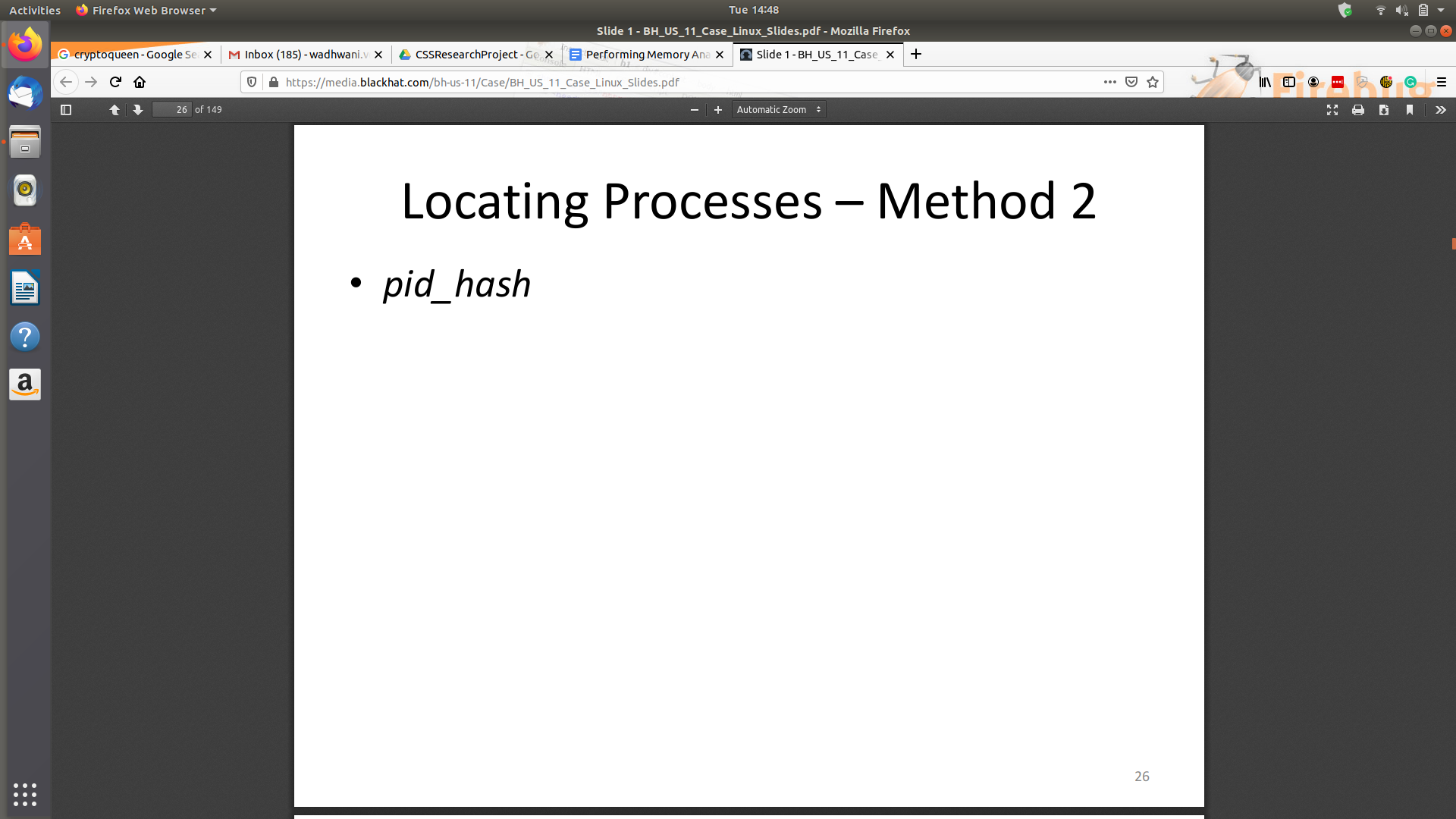
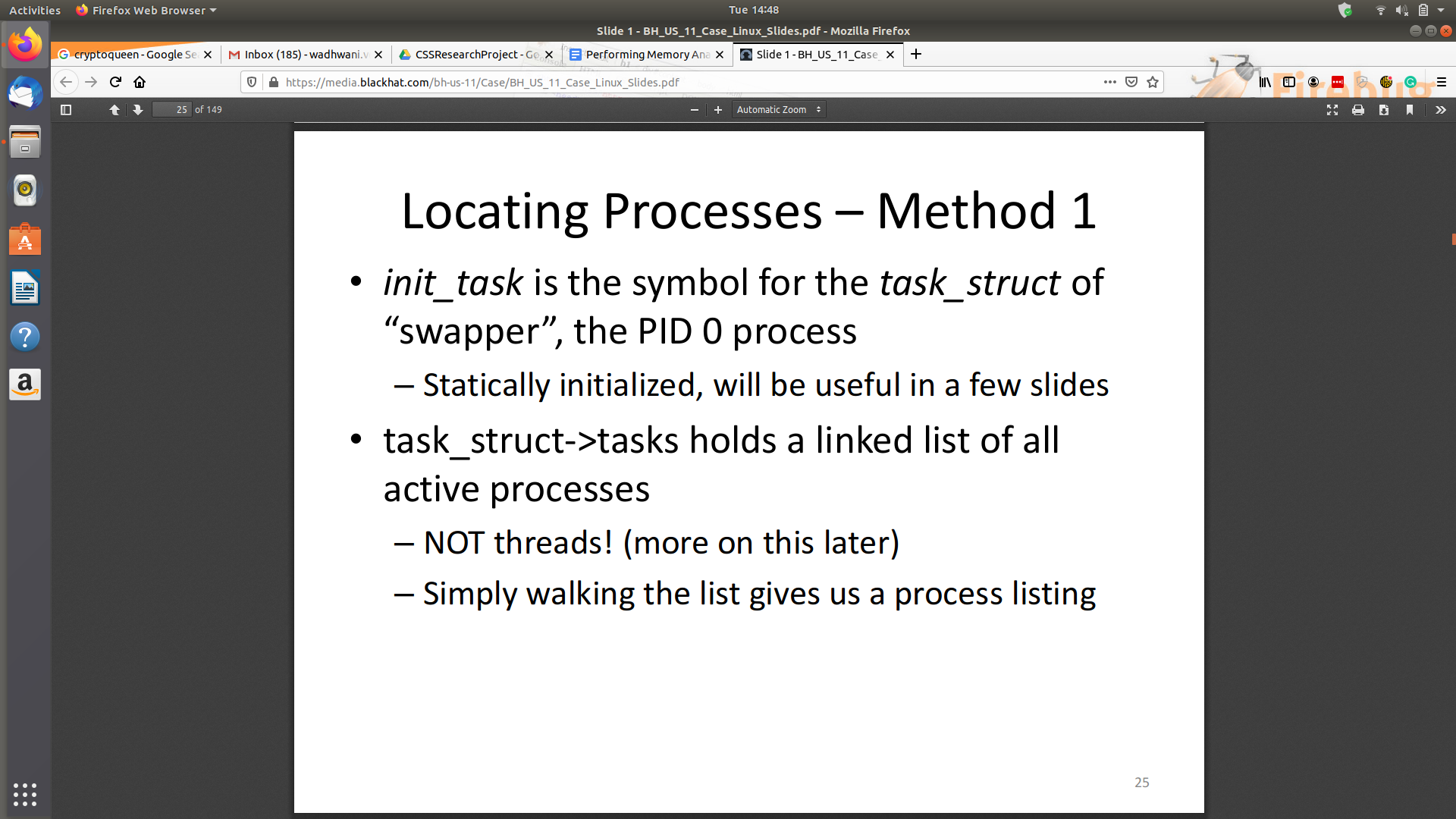
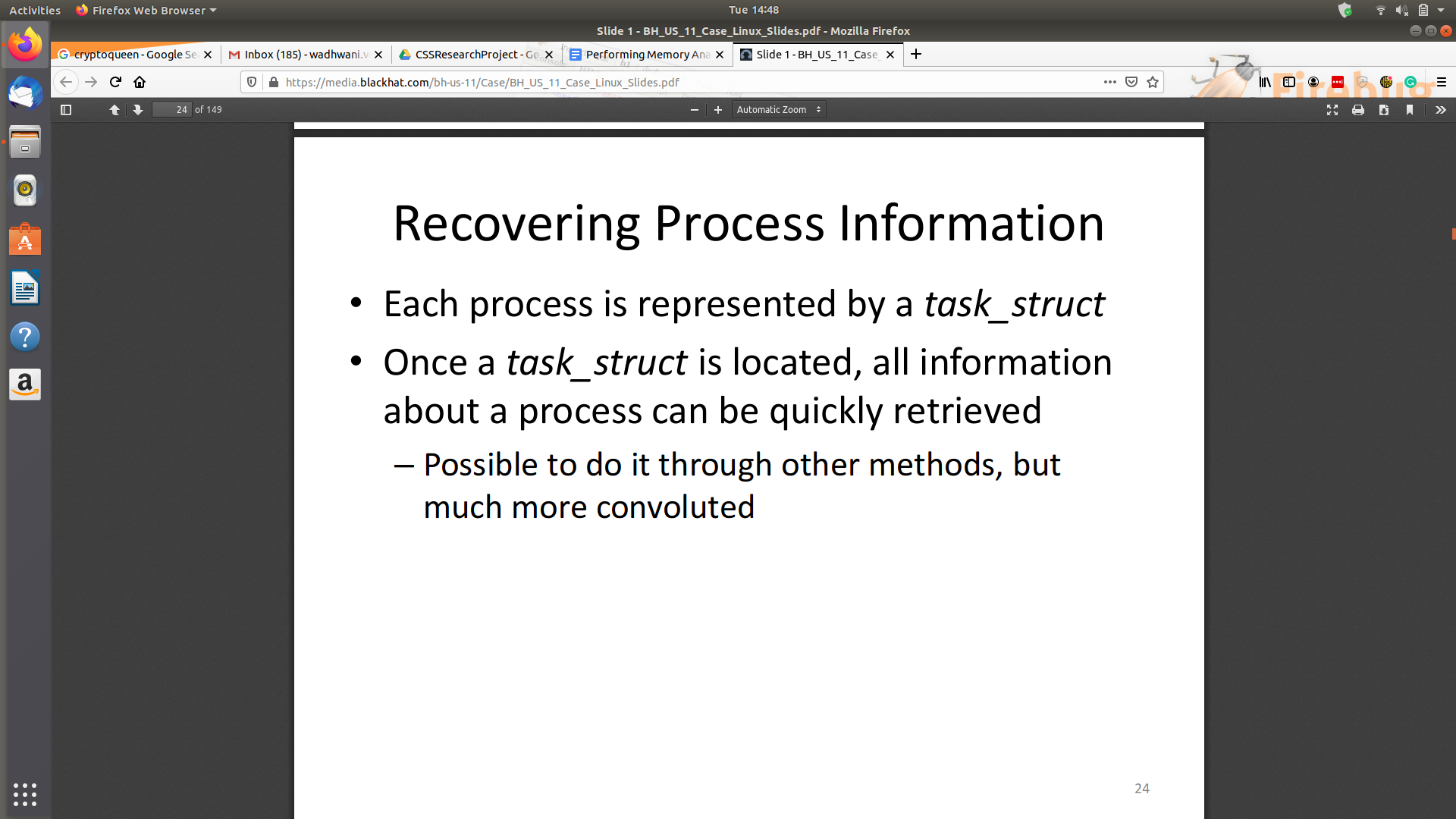
****

**Volatility**

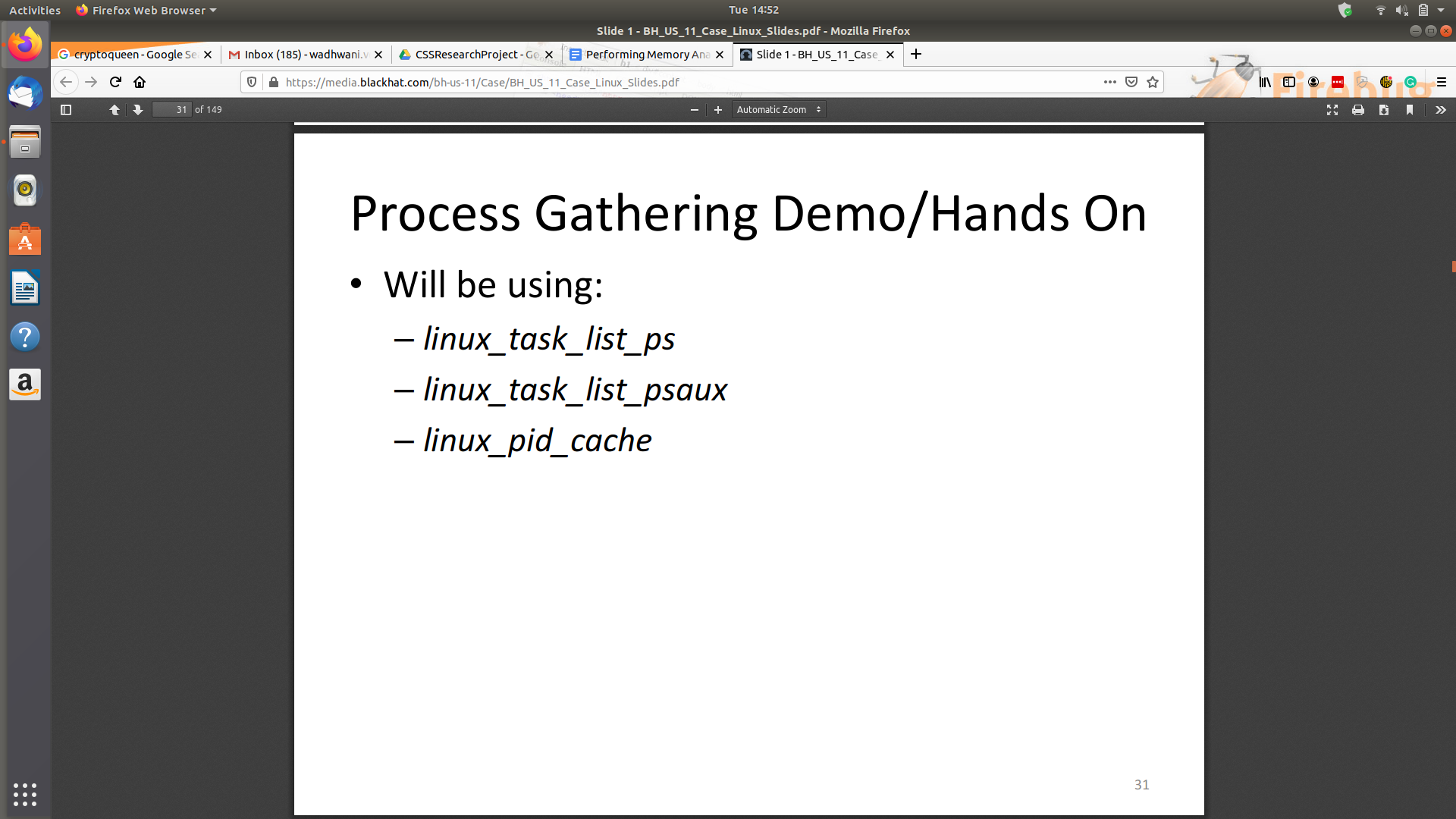
Popular Memory Analysis Framework

Allows for analysis plugins to be easily written

**RECOVERING PROCESS INFO**



**DEMO**



**Slide 31 (To be continued ….)**