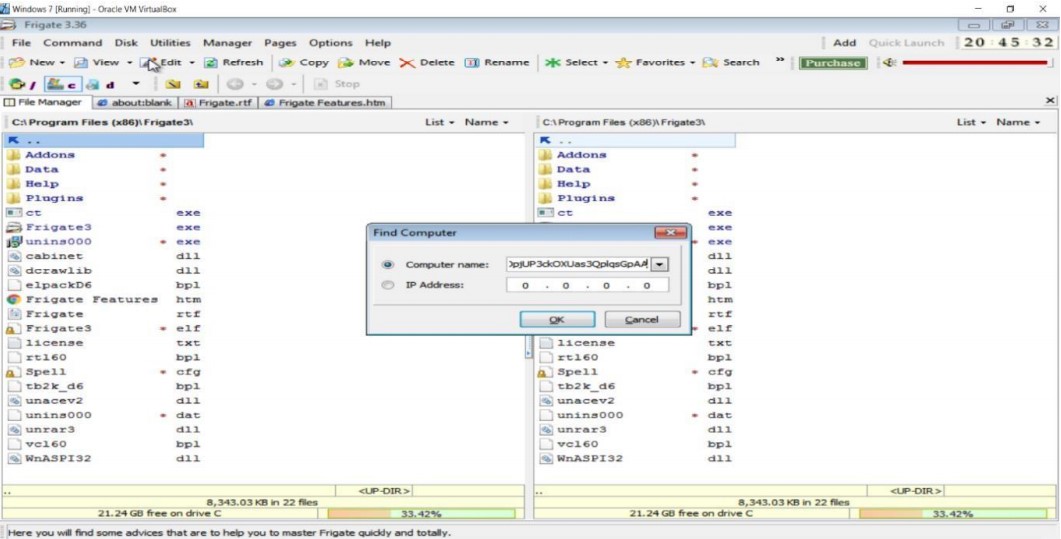
**SECURE CODING (Lab\_10)**

Venkata Lokesh

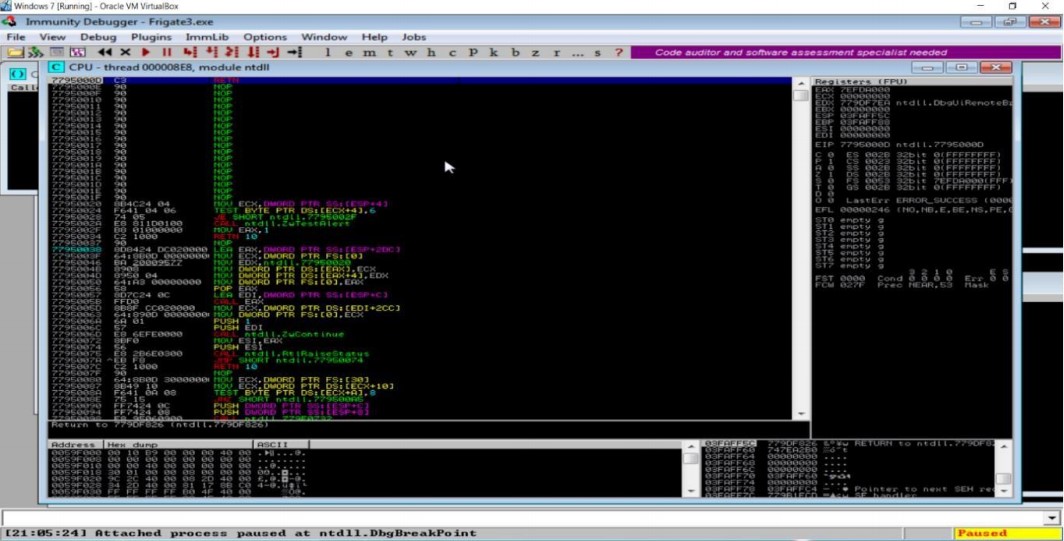
19BCE7776

L23+L24

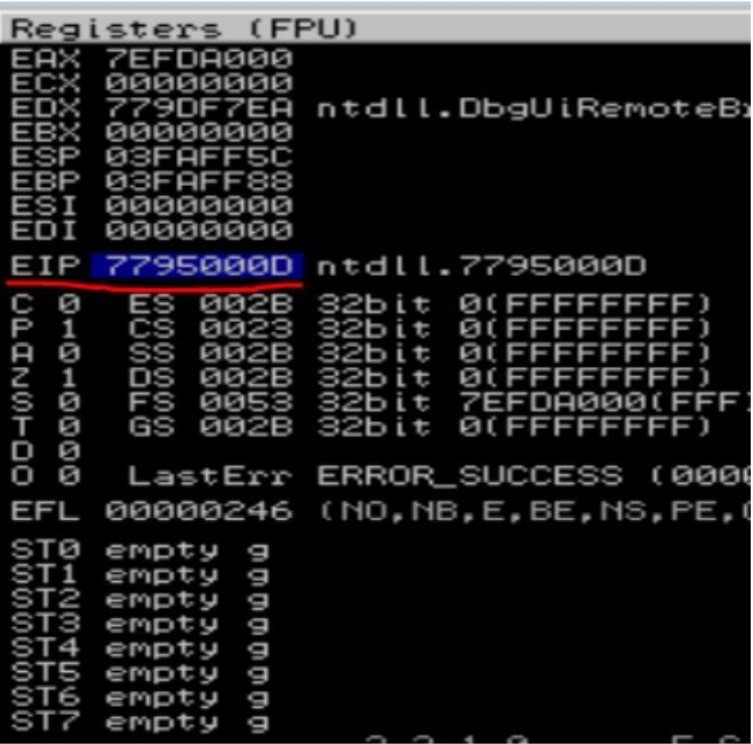
Crashing the Frigate3\_Pro\_v36 application and opening calc.exe (Calculator) by triggering it using the above generated payload:



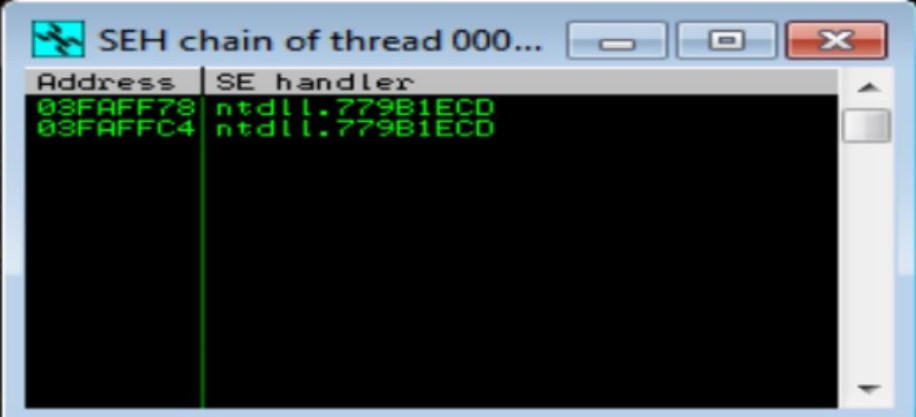
Before Execution (Exploitation): Attaching the debugger (Immunity debugger) to the application Frigate3\_Pro\_v36 and analysing the address of various registers:

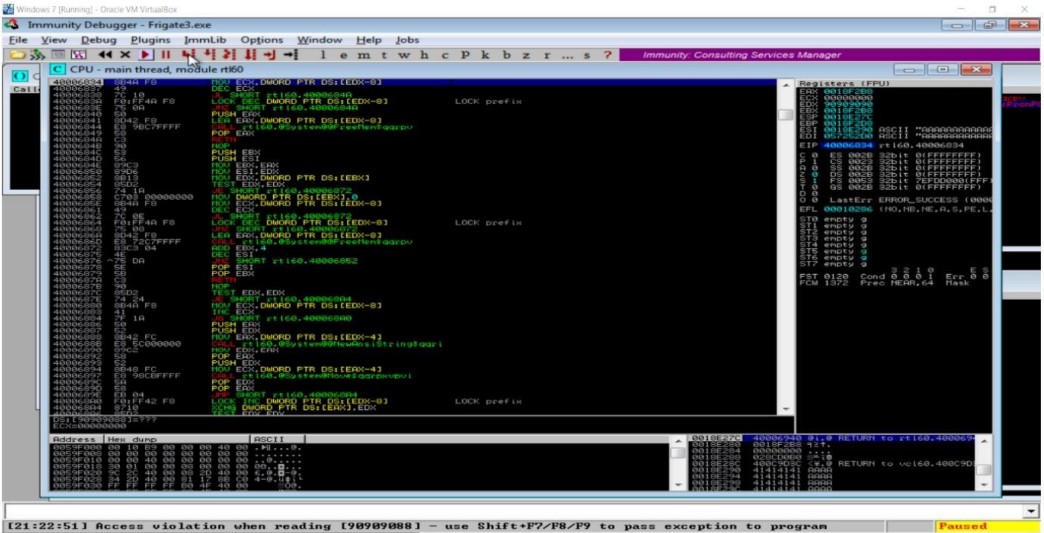


Checking for EIP address:

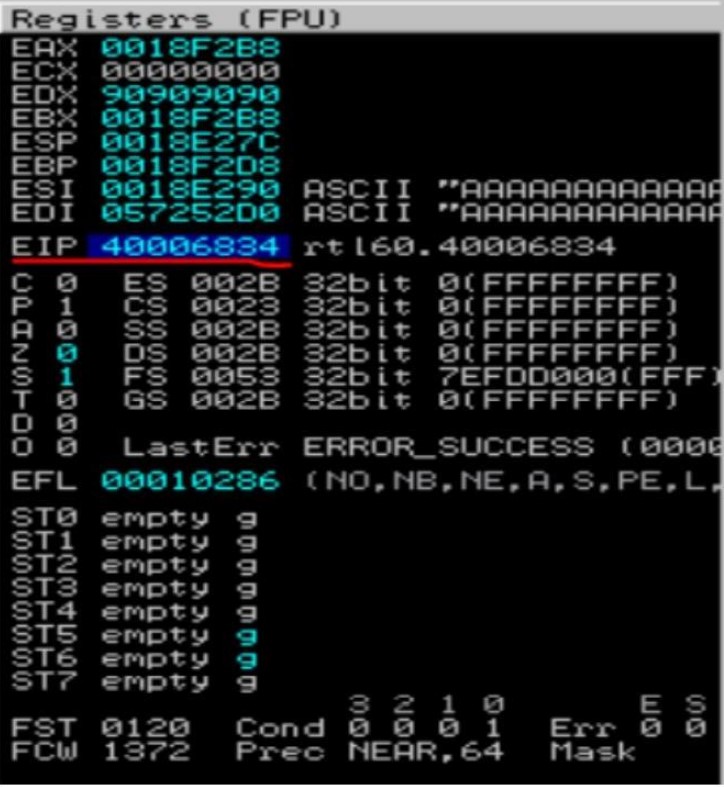


Verifying the SHE chain:





Checkingfor EIP address:



Verifying the SHE chain and reporting the dll loaded along with the addresses:



Hence from the above analysis we found that the dll ‘rtl60.40010C4B’iscorruptedandislocatedatthe address ‘0018F2A0’.