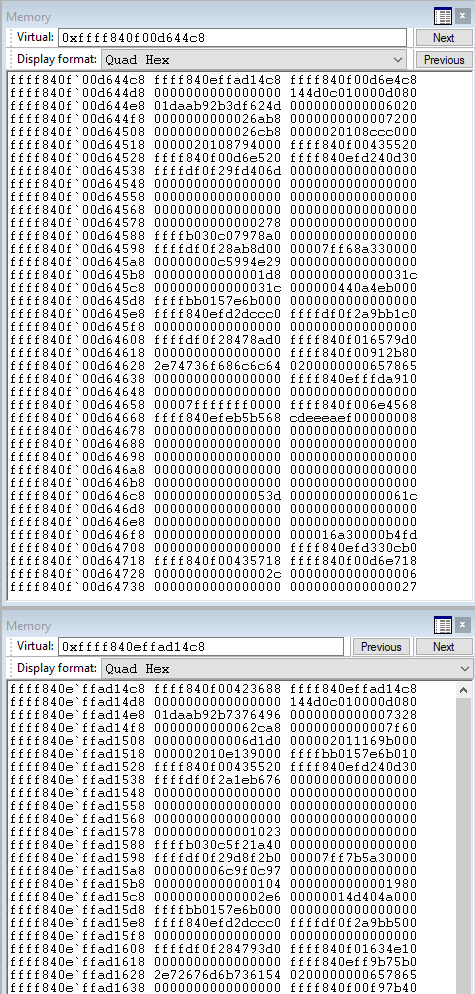
**Detection Avoidance Lab - Brian Guerrero**  


After breaking in with the kernel debugger, I see that the address of the notepad.exe process’ list entry is: 0xffff840f004354c8

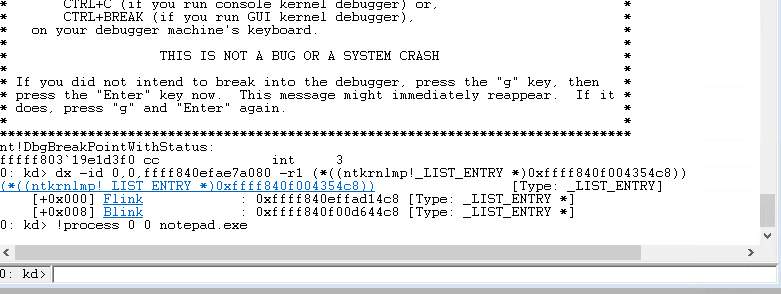


This memory dump shows the memory of the Blink on the top, and Flink on the bottom.

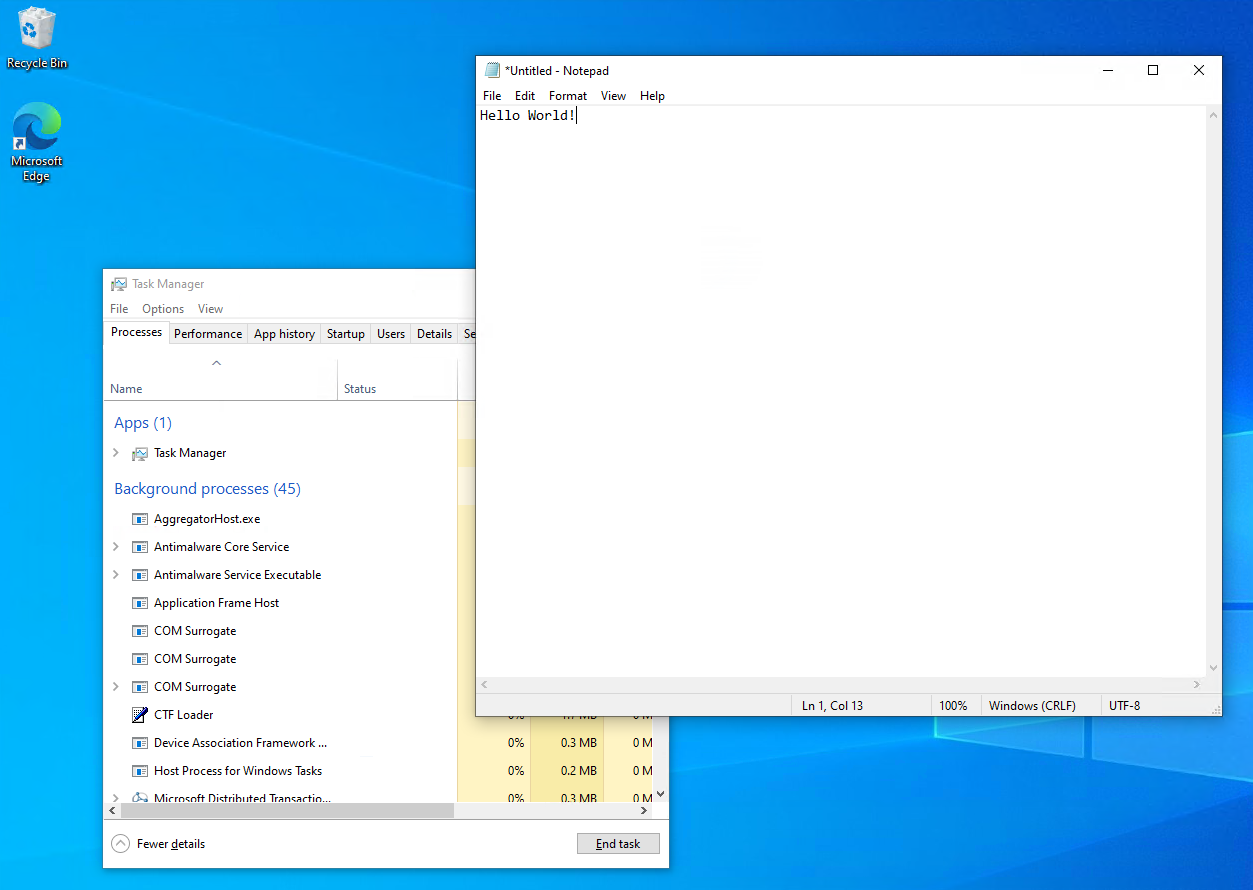
I have edited the Blink->Flink to point to Notepad’s Flink.

I also edited the Flink->Blink to point to Notepad’s Blink.

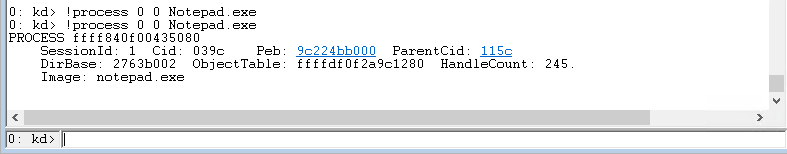
With this configuration, there is no reference to Notepad.exe from either its preceding or following list entries.



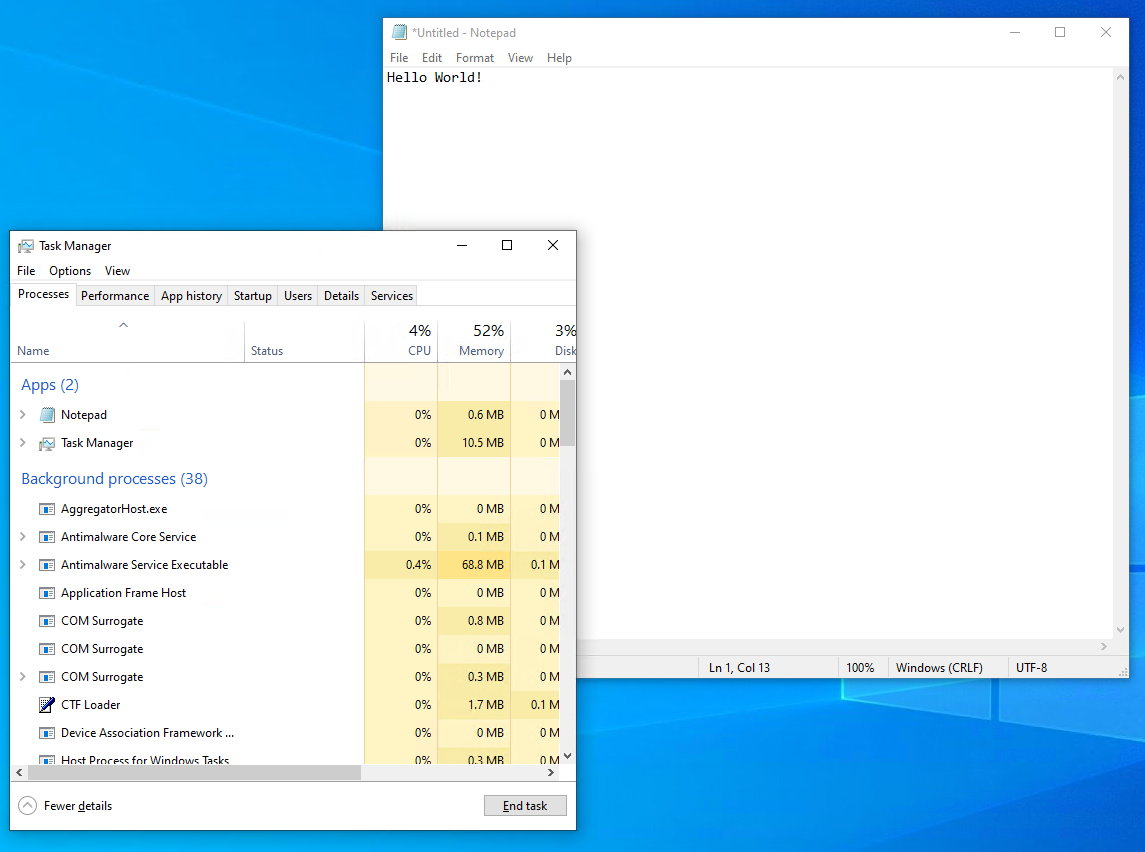
The above WinDbg output shows that a search for the notepad.exe process shows nothing.



Restoring execution of the VM being debugged, we see that Notepad.exe is working as expected (I could type into it) but it doesn’t appear in Task manager.



After restoring the Blink->Flink and Flink->Blink to their original values of 0xffff840f004354c8 (Notepad.exe’s list entry), we see that a search for the process returns a value once again.



Returning to the VM, Notepad is still running and is appearing once again in Task Manager.