Disclaimer: Scenarios for all of my assignments are *completely fictional*, but may include actual names, locations, and landmarks to add realism.
SCENARIO:

Nice job taking over Greg's work last week. There's another hot case brewing...

HELP!

The University of Texas Health Science Center (UTHSC) has fallen victim to a Ransomware attack by known hacking group **GFK** - the *GetFreshKrew*.

In addition to numerous labs systems being compromised, a notable researcher has had her critical documents encrypted, to include the only image she has of her blackboard solution to a breakthrough with cancer research. The GFK is demanding a 5-million dollar ransom and left a password-protected tool to assist with decryption. The GFK's ransom note says they will provide a password to reveal the XOR decryption key once the ransom is paid.

It's all up to you! Can you reverse engineer the tool's password to unlock the XOR key and decrypt this life-saving research?

Assignment -- Your mission should you choose to accept it:

--Download the UTHSC zip file from Professor Ervin's OneDrive account.
--Also, Install Cutter to assist with your reverse-engineering efforts.

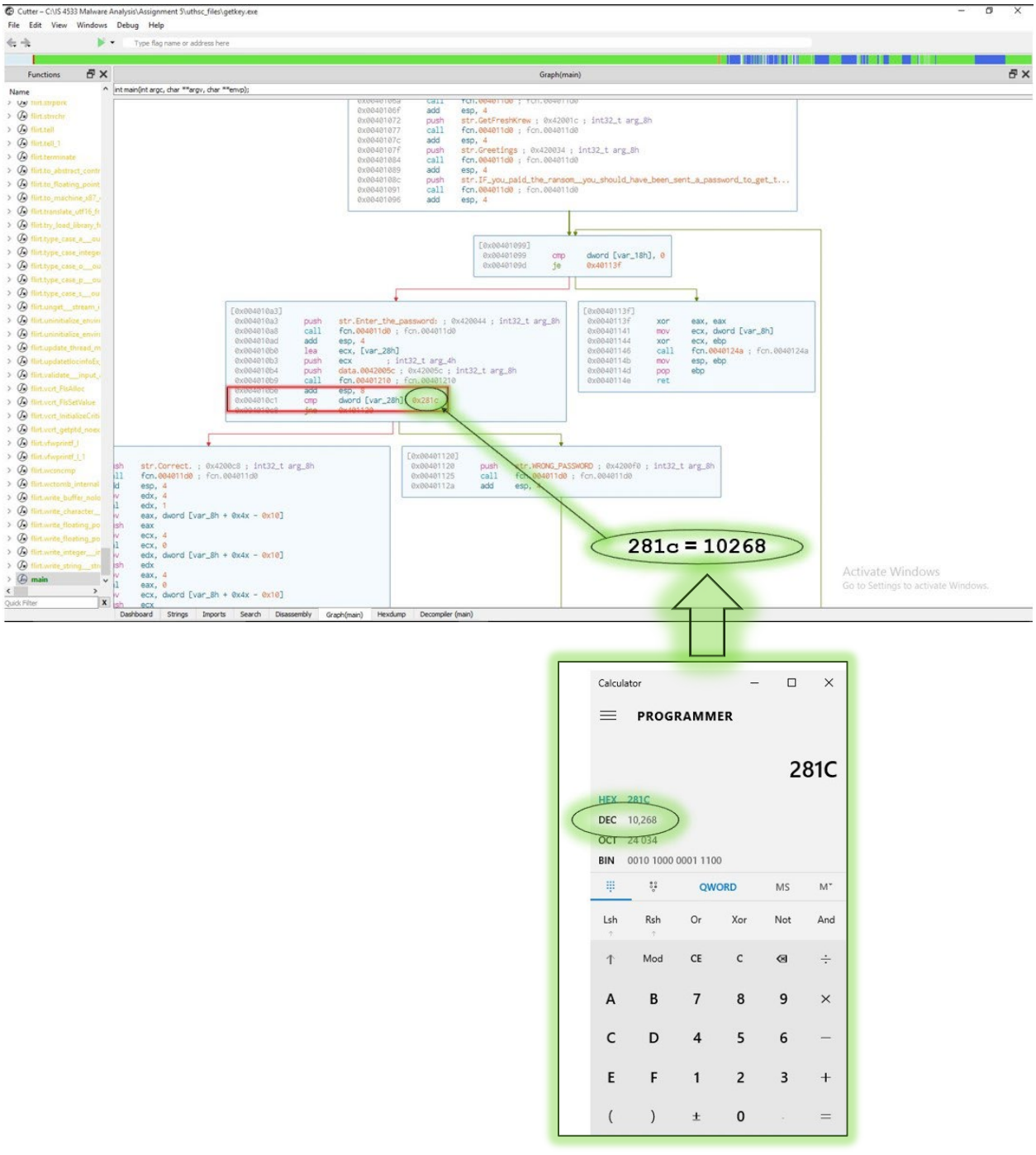
--To assist you, please reference Prof Ervin's lecture that demonstrates how to use Cutter to disassemble executables and identify values of arguments to functions. Additionally, how to use the XOR utility to decrypt data.

GRADING RUBRIC -- To receive full credit for this assignment, you must answer the following:

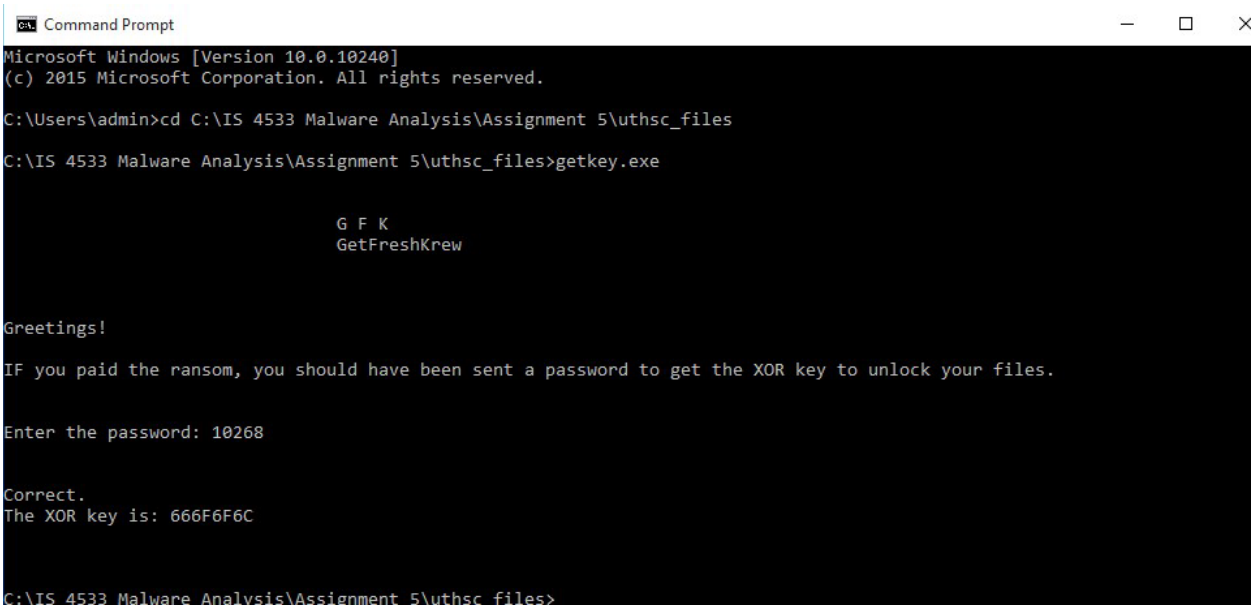
1. Use Cutter to disassemble the getkey.exe tool and determine the password from your analysis. Submit a screenshot of the disassembly routine that enabled you to make the determination.
2. Use the password you discover in Step-1 to execute getkey.exe and reveal the XOR decryption key. Submit a screenshot supporting your findings.
3. Use the XOR to decrypt blackboard.jpg and reveal the life-saving research. Submit a screenshot supporting your findings.

Good Luck!!

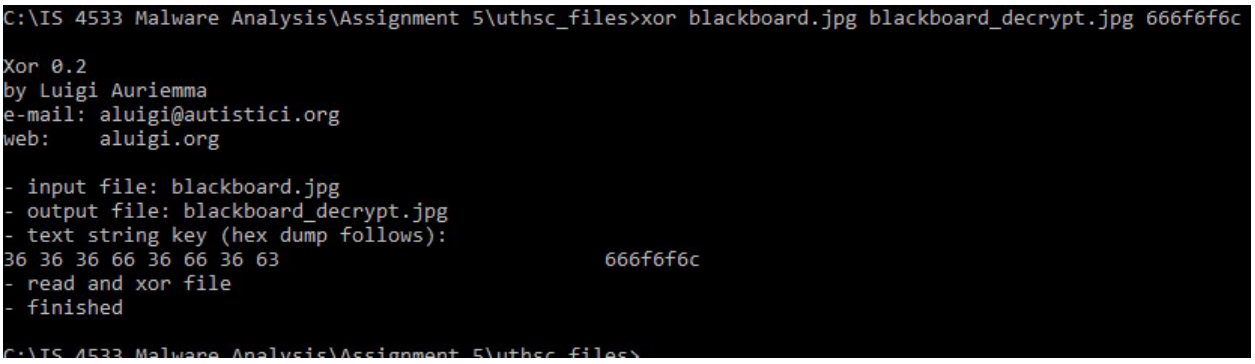
1. Used Cutter to disassemble the `getkey.exe` tool and determine the password was `10268` from my analysis.



2. Used the password I discovered in Step-1 to execute getkey.exe in the command terminal and revealed the XOR decryption key, `666F6F6C`.



3. Used the XOR to decrypt `blackboard.jpg`.



Revealed blackboard.jpg decrypted: