**Capture the flag exercise: Manual code reversing**

For this exercise, search for and download tools to your VM to perform this activity. Hints are provided throughout the module and in the questions below. For help, refer to the Capture the Flag exercise demo video in Module 2.

From re\_exercises.zip, you will analyze:

furiousfast.exe

**Answer the following questions and capture the flag:**

Using Hashcalc, I could extract all hashes that I needed for this exercise.

A screenshot of a computer

Description automatically generated

* What is the MD5 hash of the file?

**5ce1013a5bc6a894ecf5051dd07f92cd**

* What is the SHA256 hash of the file?

**9c2306783dc9d8f44e36c7725babfeceec03be7bac8d12be93be02925a270d07**

Before continuing with the next questions, I checked on VirusTotal to see any malicious behavior of this executable was reported.

A screenshot of a computer

Description automatically generated

* Where does this program externally connect?

[**www.netfixed.com**](http://www.netfixed.com)

* What is the flag? (Hint: you will have to debug this with a debugger like x64dbg or ida to get the flag)

**F7\_AND\_F8\_AR3\_GREAT\_MOVIES\_X-Force**