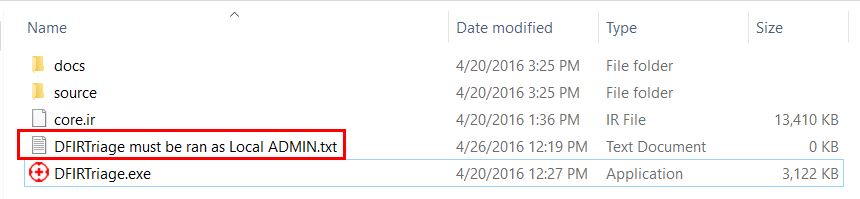
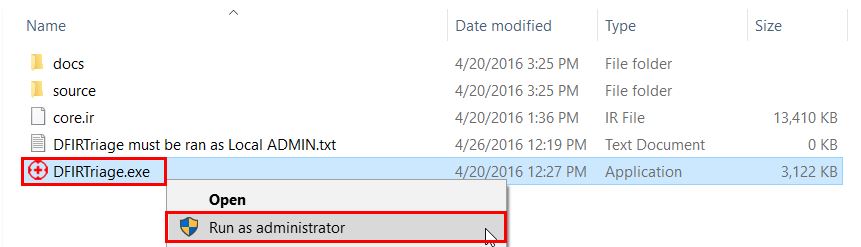
[DFIRTriage] -- quick Start Guide

# **Execution**

DFIRTriage.exe and core.ir must be in the same directory when executing and DFIRTriage.exe must be ran with administrative privileges. If not, it will close out and drop a text file reminder in the tool root directory.

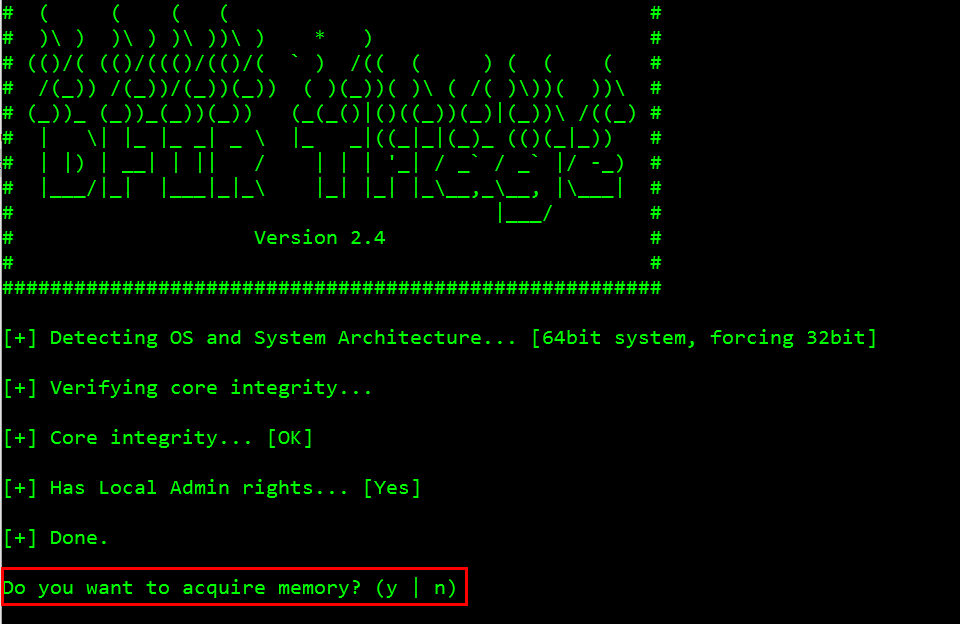


To execute, right click DFIRTriage.exe and choose "Run as administrator".



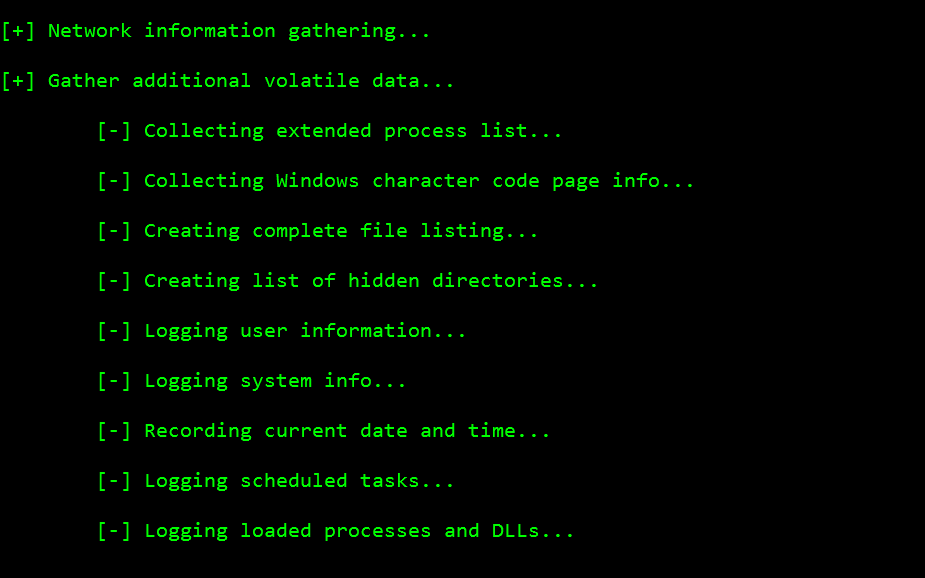
# **Memory Acquisition**

Immediately upon execution, you will be prompted to either acquire a memory image from the target or to skip memory acquisition all together. Choose either "y" or "n" to continue running the script.

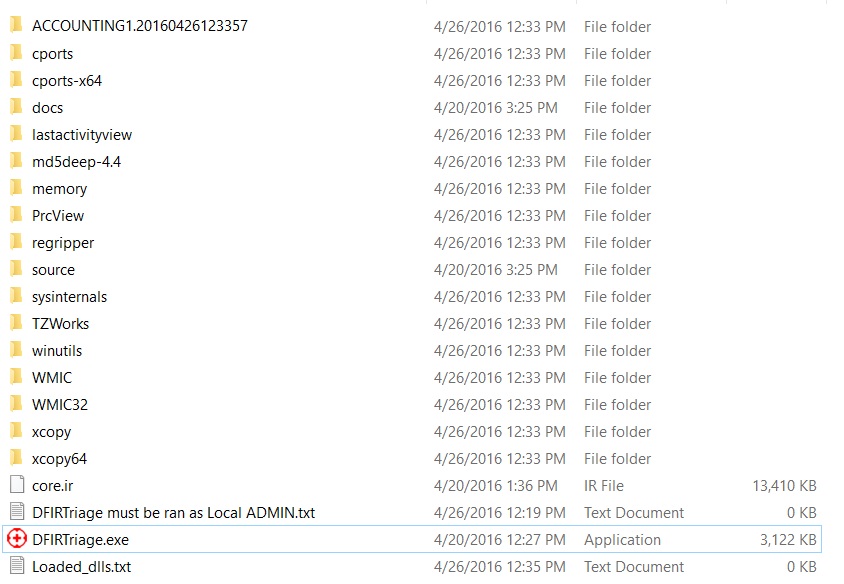


# **Runtime**

During runtime you will see information scrolling through the console as the script progresses.

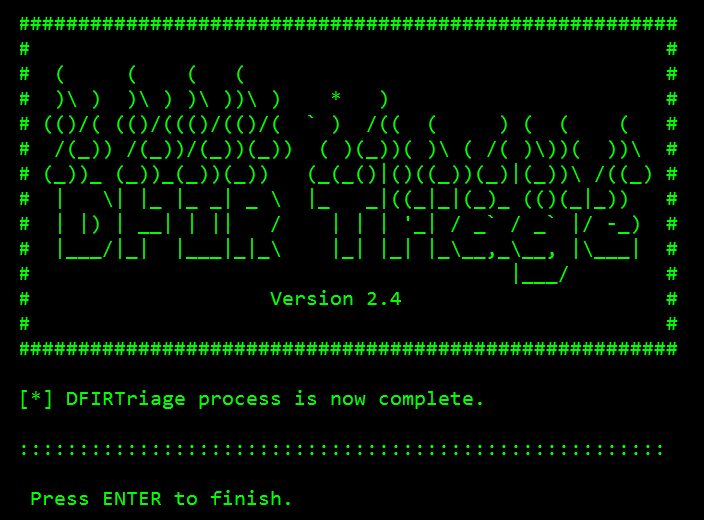


The tool root directory will be populated with several folders and files as core.ir toolset is expanded.



# **Completion**

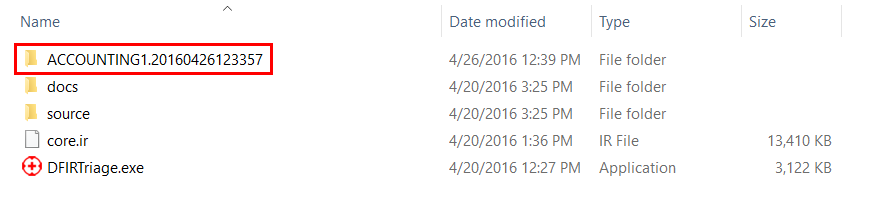
You will see the following message upon successful completion of the script.



# **Output**

The clutter in the tool root will be cleaned up leaving you with one additional directory containing the triage output data.

The output directory naming convention is "target-hostname.YYMMDDHHMMSS".



All of the output data is organized into the following folder structure.

