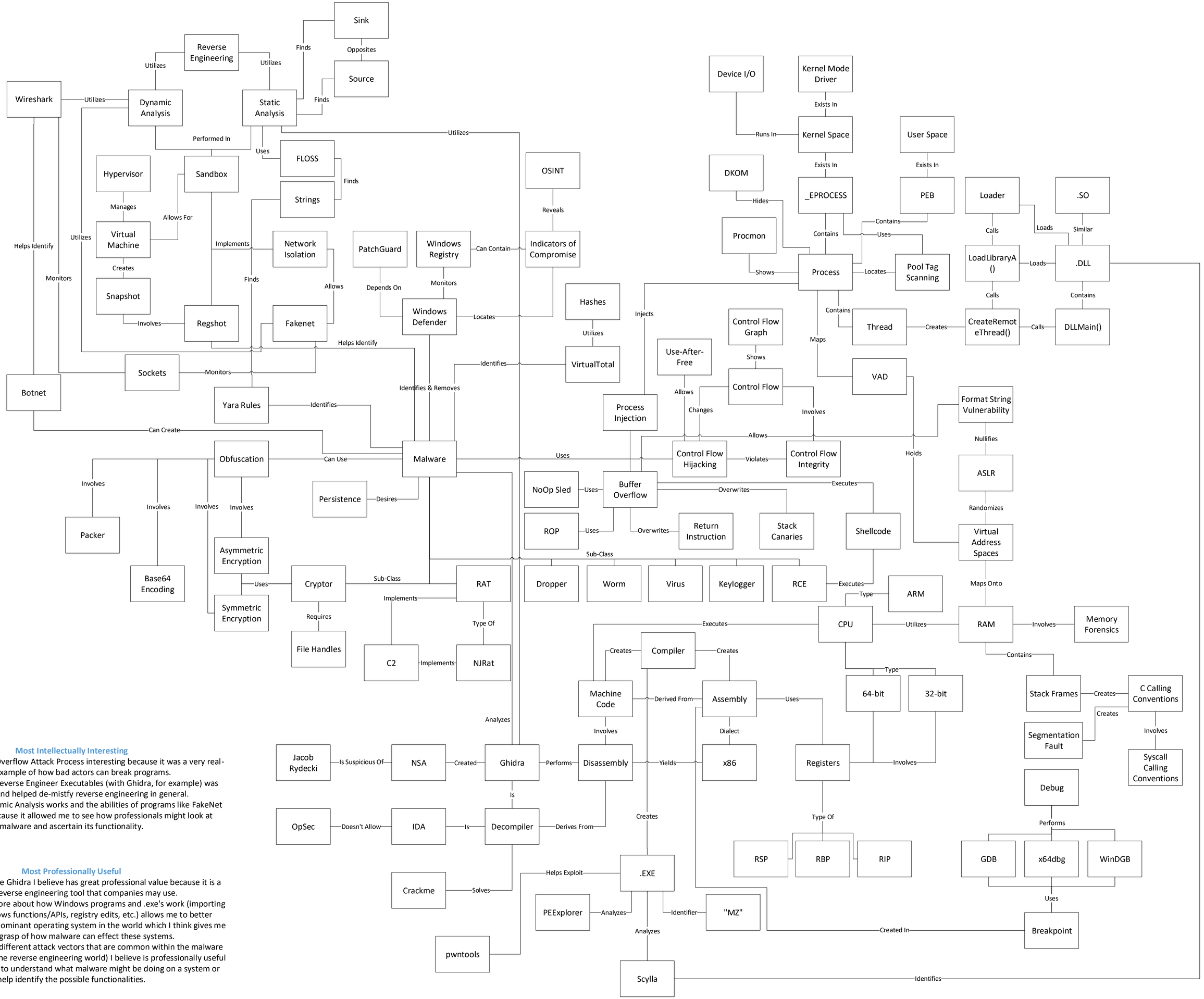

Most Intellectually Interesting

1. I found the Buffer Overflow Attack Process interesting because it was a very real-world example of how bad actors can break programs.
2. Learning how to Reverse Engineer Executables (with Ghidra, for example) was interesting and helped de-mistfy reverse engineering in general.
3. Learning how Dynamic Analysis works and the abilities of programs like FakeNet was interesting because it allowed me to see how professionals might look at malware and ascertain its functionality.

Most Professionally Useful

1. Learning how to use Ghidra I believe has great professional value because it is a popular reverse engineering tool that companies may use.
2. I believe learning more about how Windows programs and .exe's work (importing DLLs, calling Windows functions/APIs, registry edits, etc.) allows me to better understand the most dominant operating system in the world which I think gives me a better grasp of how malware can effect these systems.
3. Understanding the different attack vectors that are common within the malware world (and therefore the reverse engineering world) I believe is professionally useful because it allows me to understand what malware might be doing on a system or help identify the possible functionalities.