

Page 1:

What is Reverse Engineering?

Reverse engineering is the process of analyzing software to understand its structure, functionality, and behavior. Often used on malware.

Page 2:

Tools of the Trade

- Ghidra
- x64dbg
- IDA Free
- Procmon, Wireshark

Also use virtual machines for safety.

Page 3:

Analyzing Malware

Steps:

1. Static Analysis (strings, file type)
2. Dynamic Analysis (sandbox)
3. Network Behavior

Never test on real systems.