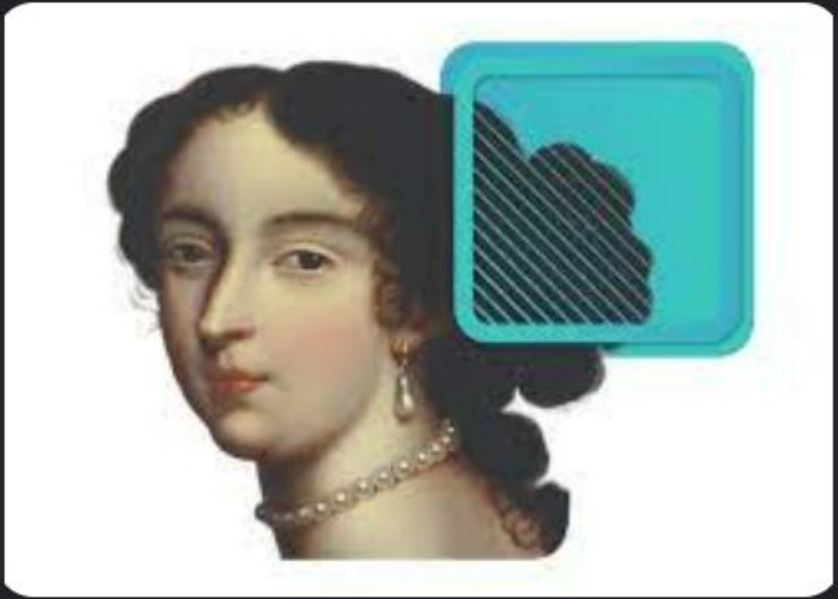
IDA and GHIDRA

Joshua Reynolds
NMSU Reverse Engineering
SP 2024

Ghidra

IDA



Interactive DisAssembler (IDA) by Hex Rays

Owned by European private equity firm: Smartfin

First version written by Ильфак Гильфанов (Ilfak Guilfanov) from Russia in 1991

License costs $1K+ per year, usually paid by companies

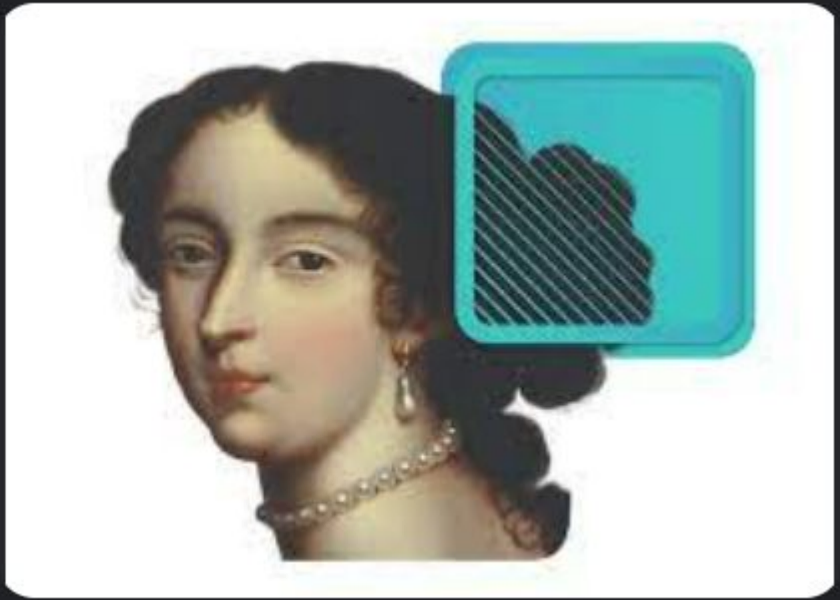
Has a freeware version without the decompiler, and a cheaper version with their cloud decompiler

Cloud decompiler == they get your binary samples

Closed-source

IDA Logo

Uses portrait of Françoise d'Aubigné 1635-1719, who was married to King Louis XIV of France.



Ghidra by the NSA

Was an internal NSA tool, now open-source

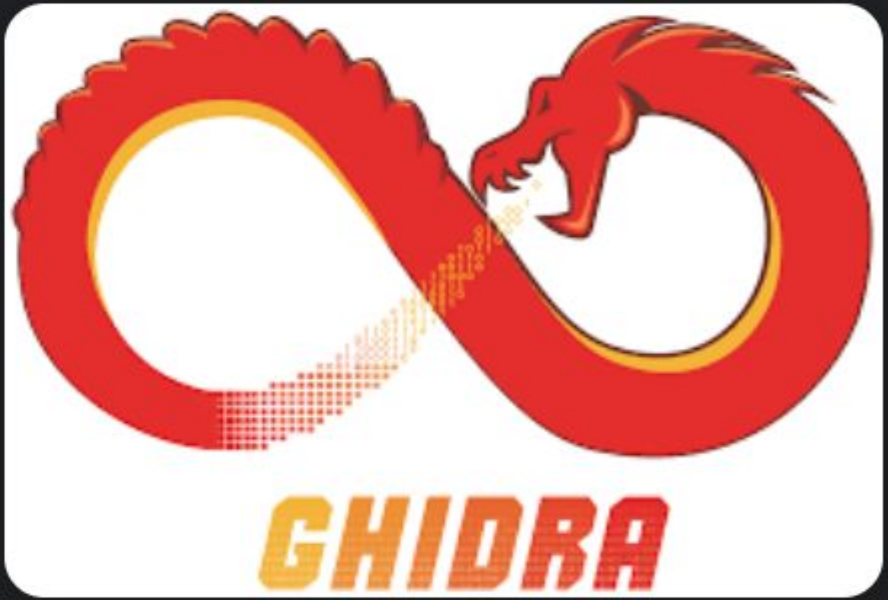
Existence first leaked on WikiLeaks in 2017

Released open-source in 2019

Active development, and lots of 3rd party support

Ghidra Logo

Named for an antagonist dragon monster character in the Japanese Godzilla series.



Other similar tools - may work better for specific samples

Binary Ninja

Radare

JEB Decompiler

Java Decompiler

.NET Reflector

RE Training: “Crackmes”

Programs that accept some kind of password or key.

You don’t get the key, or even the source code.

Your goal is to create a “keygen”, a program which outputs valid keys.

Sometimes the keys are checked with math, string operations, checksums, etc.

One in this week’s assignment.

More in the next 3 assignments, with increasing difficulty