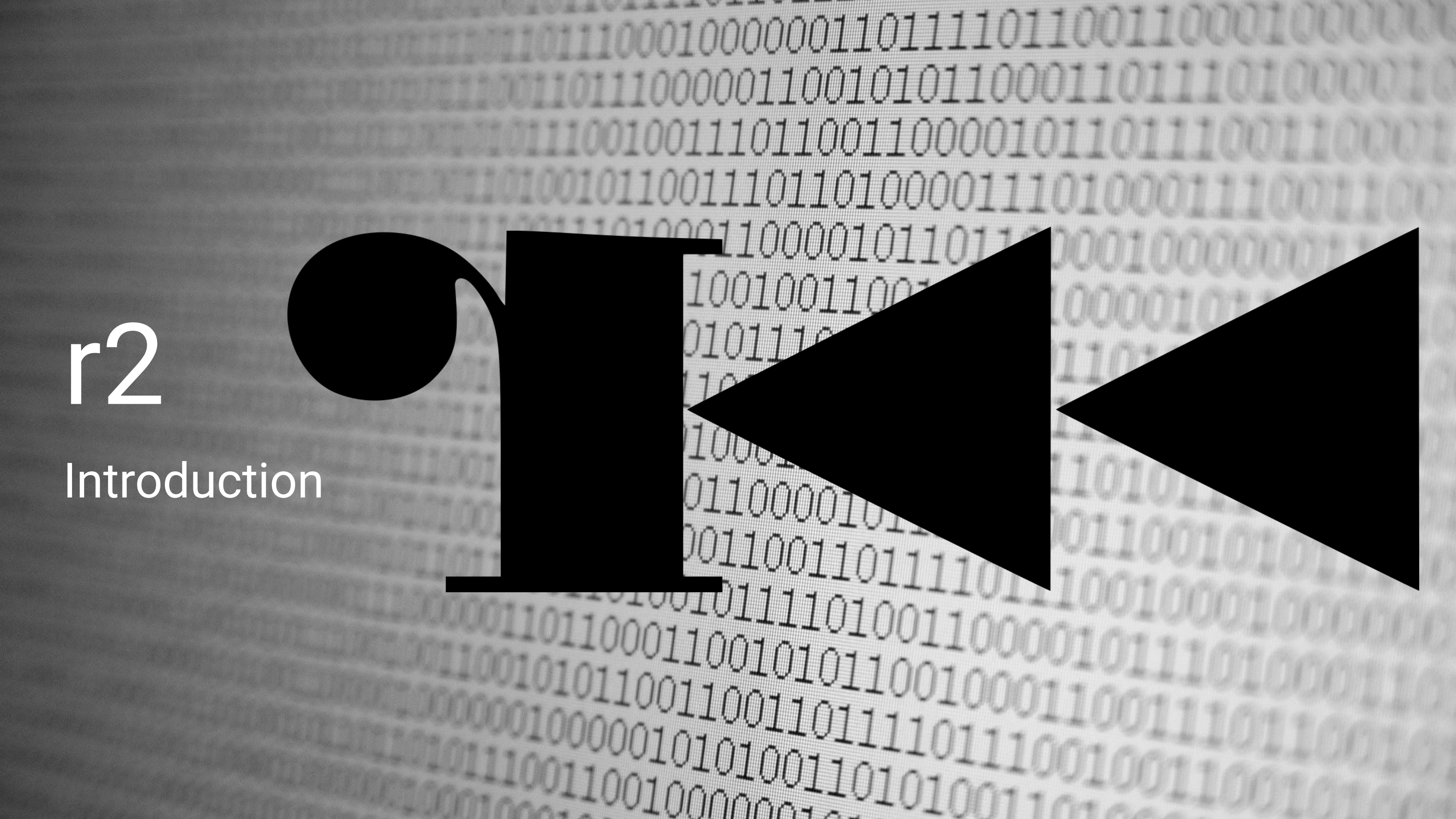


r2

Introduction

# TODO

- → What *exactly* is Radare2?
- → Brief tools overview
- → Brief commands overview
- → Package manager
- → Decompiler
- → Installing, updating & uninstalling

What *exactly* is radare2?

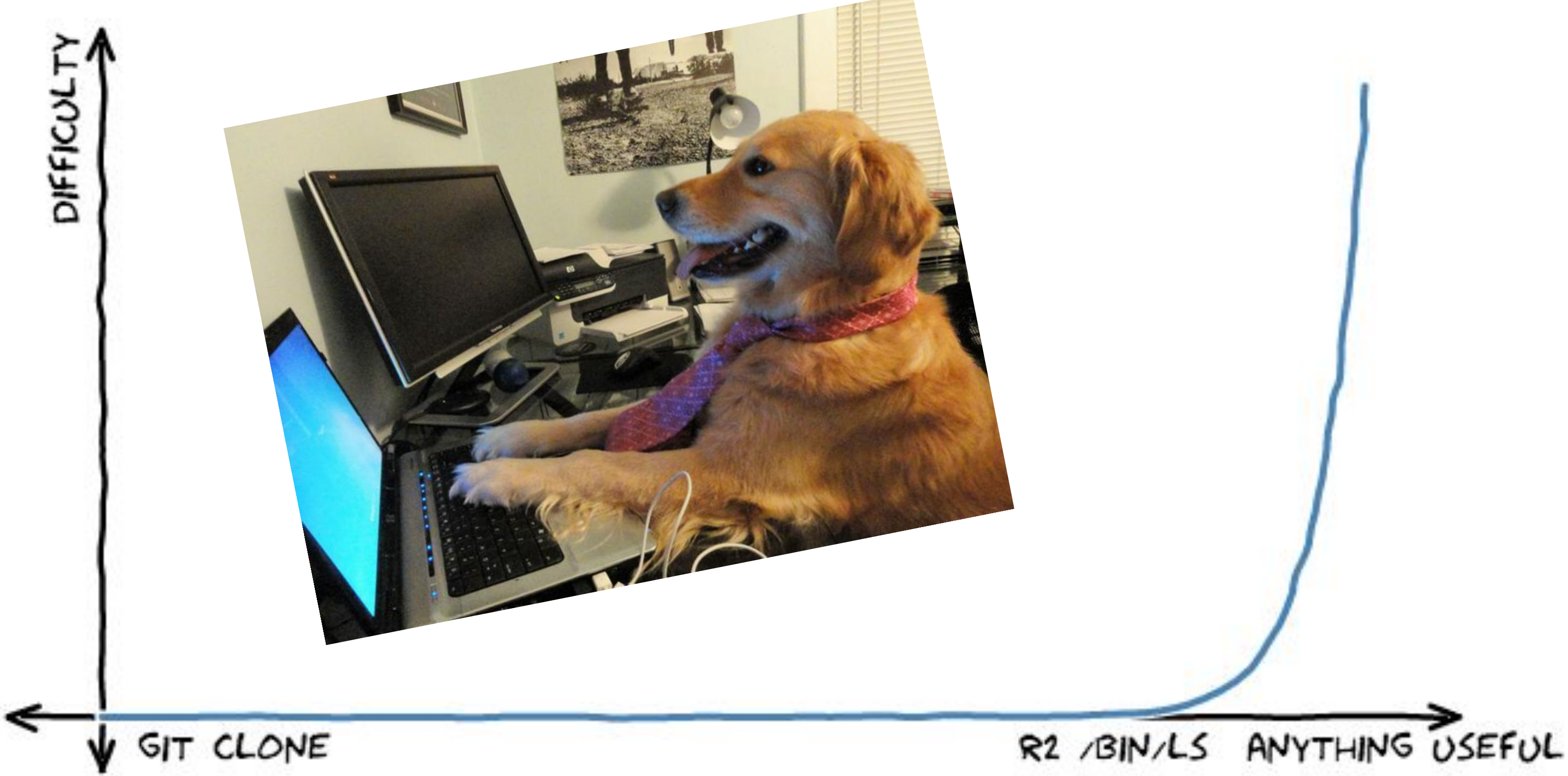
Definition & features listed on site

- By definition on the site
  - A free/libre toolchain for easing several low level tasks like forensics, software reverse engineering, exploiting, debugging, etc.
  - It is composed by a bunch of libraries (which are extended with plugins) and programs that can be automated with almost any programming language
- Features
  - Batch, command line, visual and panels interactive modes
  - Embedded web server with JS scripting and webui
  - Assemble and disassemble a large list of CPUs
  - Runs on Windows and any other UNIX flavor out there
  - Analyze and emulate code with ESIL
  - Native debugger and GDB, WINDBG, QNX, and FRIDA
  - Navigate ascii-art control flow graphs
  - Ability to patch binaries, modify code or data
  - Search for patterns, magic headers, function signatures
  - Command line, C API, script with r2pipe in any language
  - Easy to extend and modify

My about it

- A *free & open source software* security researching ***framework***
  - Set of command-line tools that can be used together or independently
- RA-DA-RE stands for RAw DAta REtrieval
  - Originally built as a forensics tool
- Disassemble / assemble for many different architectures
- Compatible with Linux, *BSD, Windows, OSX, Android, iOS, Solaris, etc.
- Debug with native and remote debuggers (gdb, webui, r2pipe, windbg, etc.)
- Emulate a binary fast with ESIL (Evaluable Strings Intermediate Language)
- Can be scripted w/ Python, Node, and more. [r2pipe]
- r2 will be the vi of reverse engineering in years to come!
- *Notorious for a high learning curve*

R2 LEARNING CURVE



Brief tools overview

Brief

Tools

Overview

- r2agent
  - Remoting manager
- r2pm
  - Package manager
- rabin2
  - Extracts information from binaries
- radare2
  - Core tool that encapsulates the rest.
- radiff2
  - Unified binary diffing utility
- rafind2
  - Advanced command line hexadecimal editor
- ragg2
  - Compiles programs into tiny binaries (x86 / arm)
- rahash2
  - Block based hashing utility
- rarun2
  - Utility to run programs in exotic environments
- rasm2
  - Command line assembler / disassembler
- rax2
  - Minimalistic base converter

Brief commands overview

Brief

Commands

Overview

- ➔ Documented in C
  - ◆ ?
    - alone prints all possible commands, appended to a command prints detailed help about that command
- ➔ Commands that do *mostly* everything
  - ◆ pd
    - print disassembly
  - ◆ aa
    - analyze all functions & symbols
  - ◆ afl
    - list all functions
  - ◆ s
    - seek
  - ◆ w
    - write
  - 🏆 ◆ V
    - visual mode
  - ◆ q
    - quits

Brief

Commands

Overview

continued...

➔ ***Inside*** **visual mode**

- ?
  - prints visual mode help
- p
  - toggles print modes (hex, disasm, debug, words, buf)
- V
  - graph mode
- !
  - window mode
- c
  - cursor mode

Brief

Commands

Overview

continued...
continued...

- ➔ Each character in the command is a sub command of the previous one
  - ◆ p?
    - prints usage of ‘p’
  - ◆ px
    - print hexdump
  - ◆ pxw
    - print hexdump of words
  - ◆ pxw 12
    - Print 12 bytes of a hexdump of words

Brief

Commands

Overview

continued...
continued...
continued...

- Helpful commands I always find myself using
  - axt
    - references *to* current address
  - axff
    - references from current function
  - fs
    - manage flag spaces (f prints flags)
  - ~
    - Radare’s internal grep tool
  - /
    - built-in search tool
  - pdj~{}
    - print disassembly prettified json
  - ? 42 * 12
    - evaluate math expression

Package manager

radare2pm - r2pm

Just like other package managers r2pm enables us to install, update, uninstall and discover plugins and tools that can be used with radare2.

To start using for the first time

```
> r2pm init
> r2pm update
```

Usage

```
> r2pm -i [package name]
```

A few plugins pancake finds interesting

Decompiler

Decompiler - r2ghidra-dec

Before Ghidra was released, r2dec was used - it was pretty terrible. Now we used Ghidra's decompiler with the r2 package r2ghidra-dec. There are still other options but this is hands down the best.

Install

```
> r2pm -i r2ghidra-dec
```

Usage

```
> pdg      # Decompile current function
> pdgd     # XML debug dump
> pdgx     # XML of decompiled current function
> pdgj     # JSON of decompiled current function
> pdgo     # Decompiled side-by-side with offsets
> pdgs     # Display loaded Sleigh languages
```

* *Decompiled code is returned to r2 as comment*

Installing, updating & uninstalling

Installing, updating & uninstalling

Installing directly from GitHub is the recommended method of install. System package managers like *apt* have a radare2 repo as well but it’s generally well behind the live version on GitHub.

Install

```
> git clone git@github.com:radare/radare2.git
> cd radare2 && sys/install.sh
```

Update

```
> cd radare2 && sys/install.sh
```

Uninstall

```
> make uninstall          # Uninstall current version
> make purge              # Remove all previous versions
> make system-purge       # Removes all libraries & other stuff
```