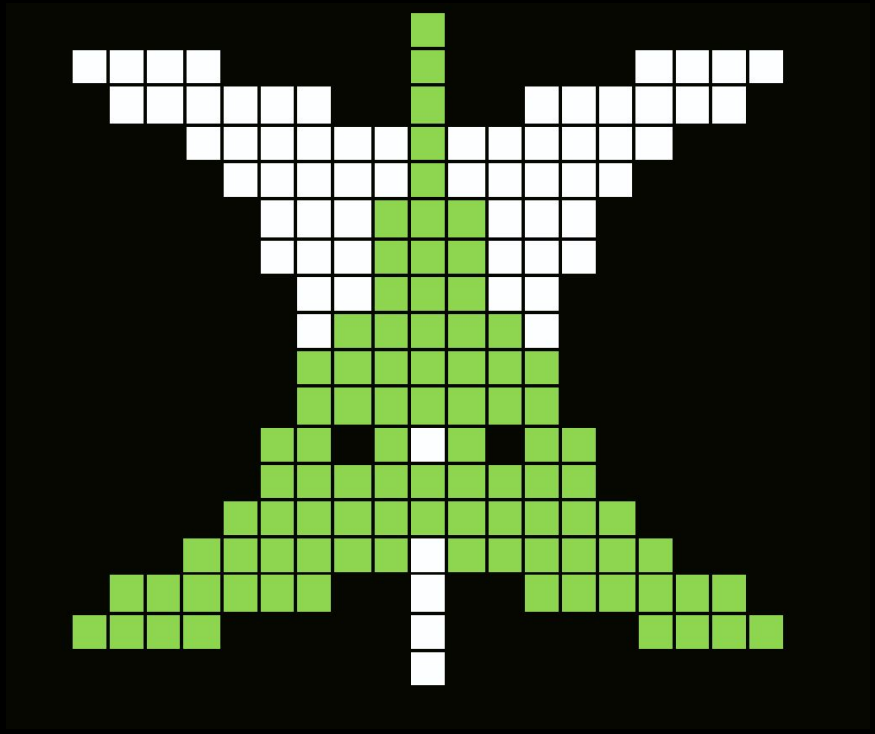


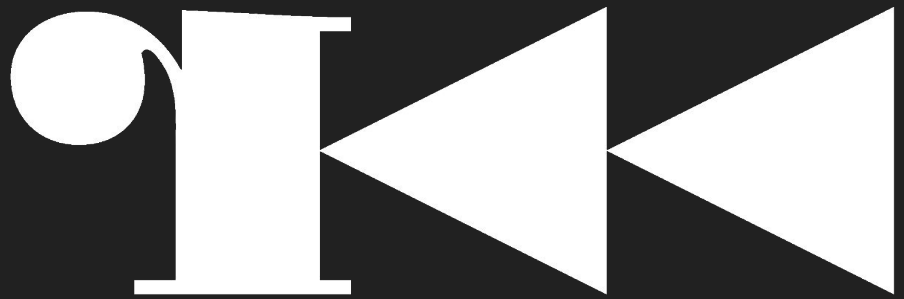
趣味と実益のために radare2を始めてみよう！

AvTokyo2017 / by pancake

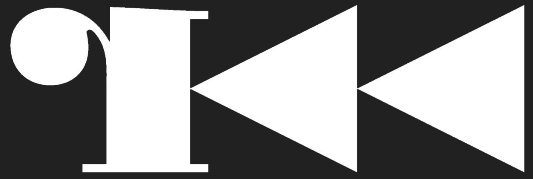
Re-translated by：Prof. Sonoda, Michio (main) & Mr. Terashima, Takayuki & unixfreaxjp (assist)

Dedicated to: AvTokyo avtokyo.org & r2jp (radare2 Japan community) github.com/radareorg/r2jp

Radare2とは?



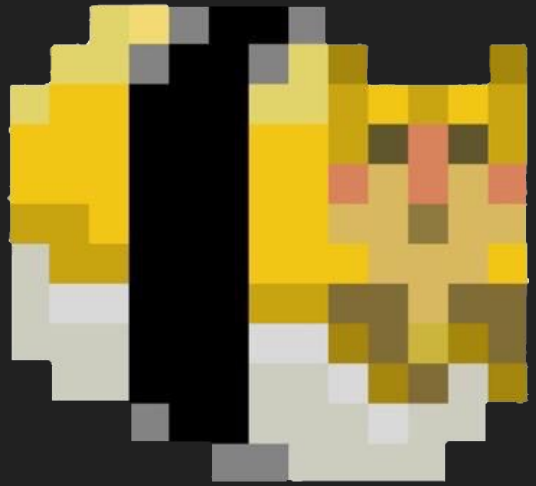
Radareとは?



- 12年間開発されているオープンソースプロジェクト（無料）
- リバースエンジニアリングのフレームワークとツールセットで構成
- オリジナル(初期）は私（pancake）が開発
- コミュニティとコントリビューターのコーダーが参加
- 個人による開発スタイルから、プロジェクトリーダー、メンテナーのスタイルに移行

- 現状は6週間ごとにマイナーバーションアップをリリース
- +1.0となるメージャーバージョンアップは毎年r2conの後にリリース
- r2conはバルセロナで開催（2017年はおよそ230人の参加者）
- r2conの全セッションはYouTubeにて公開

Who Am I?



- フリーソフトの愛好家でありオタク
  - バルセロナ、カタルーニャ地方の生まれ
  - いくつかフリーソフトウェアの開発とメンテをしている
  - DEF CON CTF に3年連続の出場
  - 絵を描くことが趣味
  - 父親として頑張ります
- リンク
  - github、bitbucket でradare、ユーザ名 trufaeで探してみてください
  - ツイッターにプロフィールがあります： https://twitter.com/trufae
- NowSecure社所属 (モバイルセキュリティアナリスト,研究開発)
  - mips、arm、x86用のアセンブリでのコーデックの最適化
  - 高速道路におけるリアルタイム交通解析のための組み込み機器向けファームウェアの開発
  - 主にWindowsプラットフォームでのフォレンジック
  - プログラミングとハッキングに関するコースのインストラクター

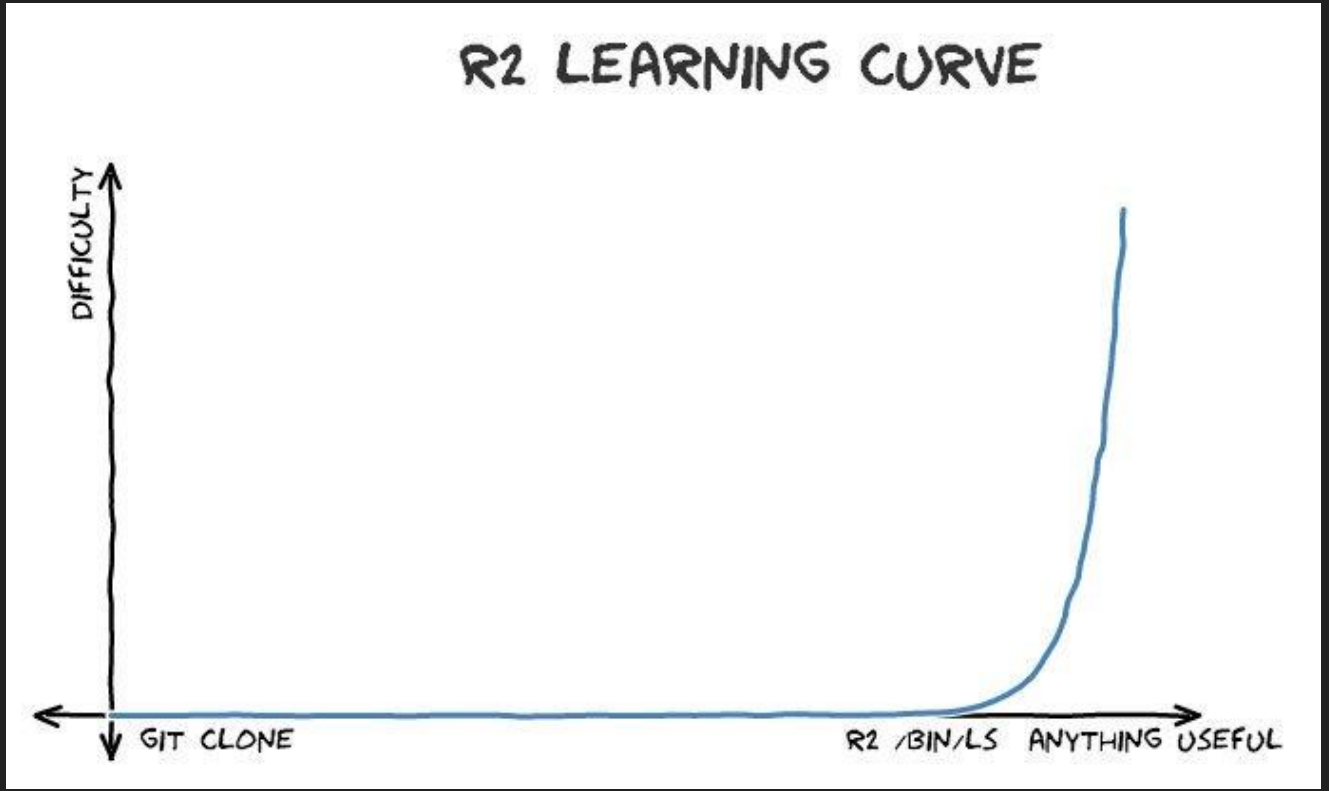
radare2の機能

- プログラムを解析して動作を理解する
- 様々なエンコード文字列の認識 (中国語, 韓国語, キリルなど)
- いくつかの異なるテクニックを用いて文字列を検索
- メモリダンプやファームウェアなどのフォレンジック調査
- ファイルシステムのマウントとパーティションテーブルの解析
- その他のデバッガーとの連携機能(gdb, r2, frida, windbg,など）
- プログラムの一部をエミュレートしてブロックを復号
- 外部デコンパイラまたはグラフ作成ツールを使用
- 2つのバイナリの違いを確認できるdiff機能
- 2048やr2warsのようなゲームもプレイできる！

どんな環境でも使えます！

- 対応OS:
  - Windows, Linux, Mac, QNX, Solaris, NetBSD, FreeBSD, BeOS, Android, iOS, ….
- 対応アーキテクチャー:
  - x86, arm, mips, sparc, ppc, z80, 6502, 8051, avr, wasm, snes, java, dalvik, hppa, ...
- ほとんどのos/アーキの組み合わせでのネイティブデバッガをサポート
- web-assembly と asm.jsにも対応
- ローカルまたはリモートでも使用可能

(demo rasm2 -L rabin2 -L r2 -L)


R2 LEARNING CURVE
DIFFICULTY
GIT CLONE
R2 /BIN/LS
ANYTHING USEFUL

学習曲線

- 最初の段階はステップバイステップで学ぶ必要があるが、長期的には楽しい
- 10個の実行コマンドが分かれば使えるようになる
- コマンドは組み合わせたり拡張することができる
- 初心者でも2週間程度で使えるようになる

- 実際に使って学ぶ
- 関心と献身が必要
- いくつかの類似ツールとは違う手法を採用
- オープンソースなので、自由に（rwx）！

文書化® されたもの

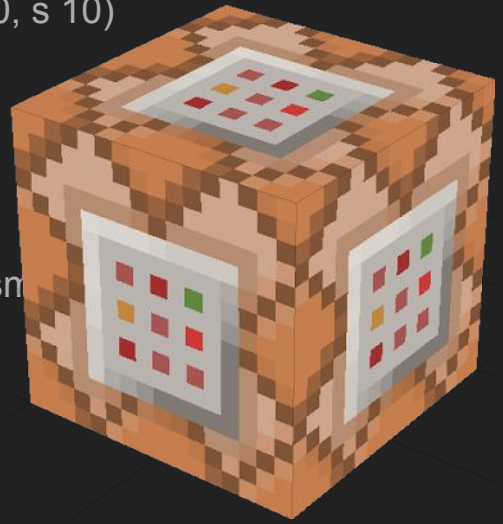
- ソースコードはCで書かれている
- オンラインマニュアル有り（ただしバージョンは古い）
- ブログ記事(Twitterをフォローしてね： @radareorg)
- YouTube とVimeoビデオで
  - r2con の2016, 2017のビデオはすべて公開
- コマンドラインのヘルプマニュアル（"?"コマンド）
- UNIX系のmanページ
- IRC と Telegram チャンネルのQ & Aコニュニティ(800人)

https://twitter.com/radareorg

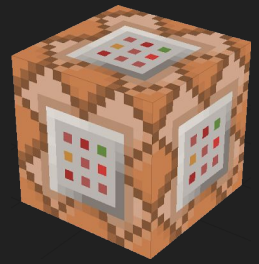
https://t.me/radare

基本機能とコマンド

- 検索
  - Relative / Absoluteのアドレスと部分的なアドレス (s+0x10, s..10, s 10)
  - 履歴/History (!, s!)
  - ブロックサイズ / blocksize (b, @!)
- ダンプ/プリント
  - Hexdump (px, pxr, pxa, prc, pxA, …)
  - アセンブリの種類に夜、ディスアセンブリ (pd, pD) @a:mips, e asm
  - デコード構造 (pf)
  - Checksums, entropy, statistics (p=, ph)
- バイナリの書き込み
  - アセンブリの書き込み (wa)
  - ストリヌスや文字列 (w)
  - Hexpairs (wx)
  - 全体的なファイルの中身 (wf)



コマンド修飾子



プレフィックス

- [1-9]
  - Repeat command n times
- . (backtick)
  - Interpret the output of the command as r2
- “
  - Ignore special characters
- `
  - Insert the output of a command
- !
  - Shell escape
- $
  - Alias command
- \
  - Alias for =!

サフィックス

- @
  - temporal seek
- |
  - system pipe
- ~
  - internal grep
- >
  - file redirect
- #
  - Comment
- ?
  - Show help
- j
  - Output in JSON

デモ

ファイルシステムのマウントと検索機能

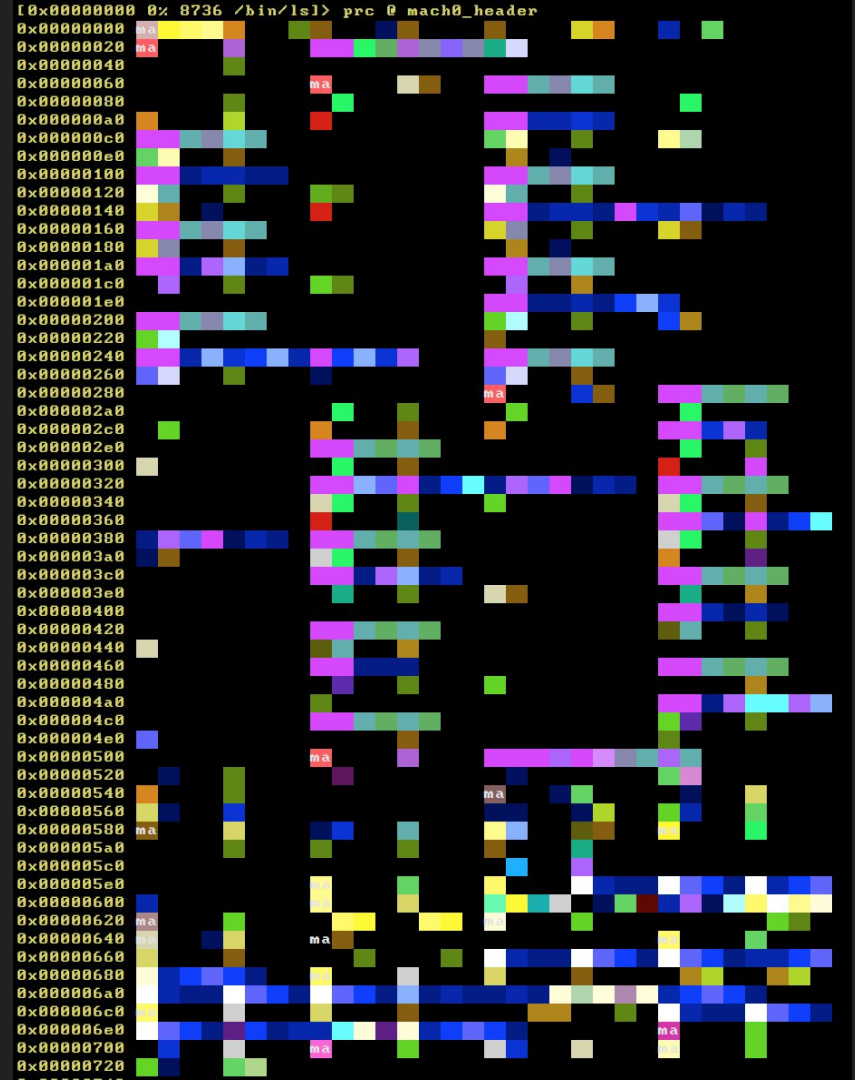
- radare2はもともとフォレンジックツール
- ファイルの中身のoffset 検索,その逆もOK
- パターンや既知のヘッダの検索、ダンプ機能
- HFS, FAT, NTFS, EXT2に対応
- Squash, jffs2はまだ未対応で開発中

- コマンド ‘m’でパーティションテーブル読み込みとファイルシステムマウント
  - GRUBコードでのプラグイン. (GPL warning)
  - io や r2 ファイルシステムも (開発中)

デモ

バイナリヘッダの解析

- 多種類のバイナリヘッダに対応可
- rabin2 -I
- 破損したバイナリの認識・調査機能
- ディスクやメモリからの読み込み
- IO レイヤーはデータへのアクセスを抽象化
- 仮想アドレス空間をエミュレーション
- r2 -nn
- rabin2 -H
- メモリヘッダの解析 (oba, .!rabin2 -r)
- リソース、エンタイトルメントの抽出



デモ

解析とディスアセンブリ

初心者向けの一般的な調査機能

- -A, aa, aaa, aaaa, aaaaa, aaaaaaaah!

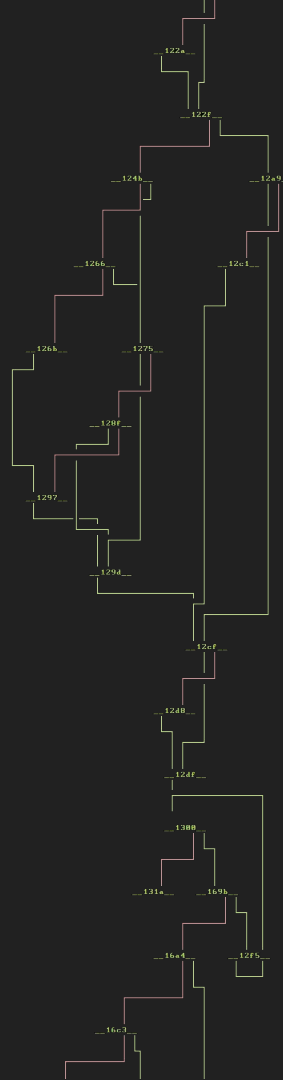
実はもっと面白いコマンドが沢山あります:

- e??anal.

さらに詳細な調査を狙う為のコマンド:

- aac, aar, aae, aav, aab, ...

いくつかのコマンドでESILによるエミュレーターを使用できる



解析とディスアセンブリ

リスト機能

- afl

基本ブロックのリスト

- afb

グラフ化

- agf

名前の変更

- afn

単一オペコードの解析

- ao

単一関数の解析

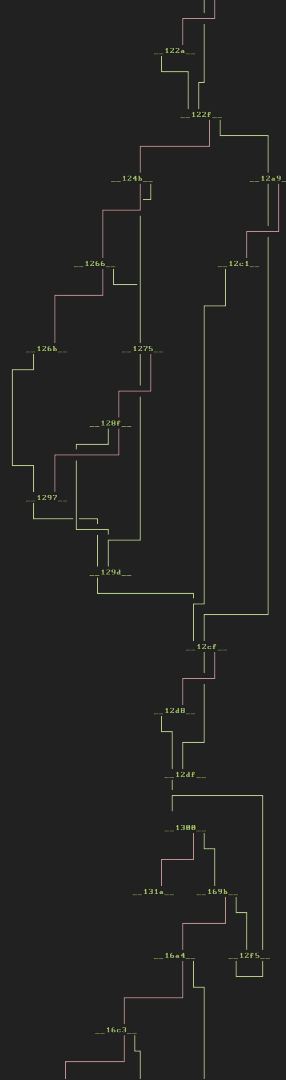
- af (e anal.hasnext)

代替解析ループ

- a2f

オートネーム機能

- afna



解析オプション

もっと調べるコードがある場合：

- anal.hasnext

文字列検索：

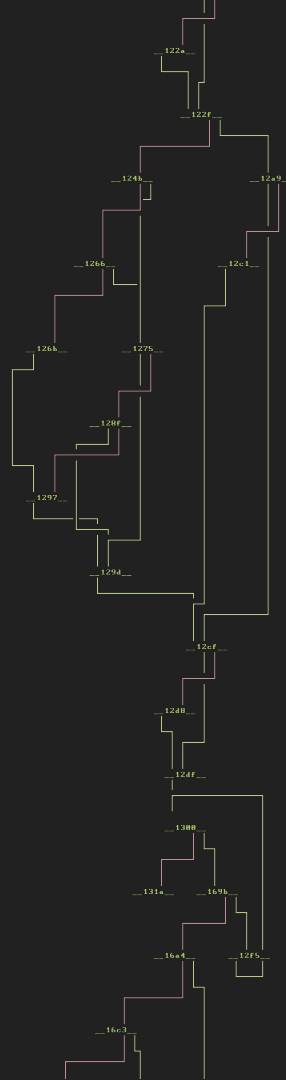
- anal.strings

実行コマンドが存在しない領域では下記のコマンドが便利

- anal.noncode

xrefやJump-Tables調査

- anal.jmptbl



デモ

複数フォーマットでデータを表示する機能

デフォルトは‘b’（ブロックサイズ）表示

ズームビュー機能, エントロピー調査, データブロックのカラーリング, 実行命令コード　など

- "p" コマンドとは？

指定されたアドレスのメモリをパースして文字列のように整形する

- pf xxi foo bar cow @ addr

デモ

デバッギングとエミュレーター機能

スタティック解析モードではR2は全てのデバッガアクションを エミュレーターエンジン (ESIL VM)にブリッジする。-d のオプションでターゲットファイルをダイナミック解析モード（デバッガ）で動かす事が出来る

- r2 -d

指定アドレスへのジャンプ命令

- dcu addr

ステップイン/ステップオーバー

- ds や dso

デバッギングとエミュレーター機能

ネイティブとリモートデバッギングエンジンに接続可能

- dbg:// winedbg:// gdb:// windbg:// qnx:// ..

その他多数のローレベルデバッギング機能:

- バックステップ (Thanks Ren Kimura!)
- メモリスナップショット
- ソフトウェア/ハードウェア ブレークポイント
- デバッグのアシスト (emulation + debug)
- トレース
- Filedescriptor 操作

Rarun2 プロファイル

実行環境は下記のような設定が可能:

- r2 -r または dbg.profileでテキストファイル指定
- dor または -R コマンドラインフラグによるカンマ区切りリスト指定

radare2環境の上でgid, uid, chroot, chdir, environment, arguments, filedescriptors の変更する事ができる

- 任意のディレクティブ値は、文字列、明示的なファイル、またはプログラムの出力とすることができます

$ man rarun2

デバッガーのデータ表示

スタックの内容を表示

- dbt - backtrace
- pxr@r:SP

ローカル変数とその値を表示

- afvd

カラーバーを見失ったら

- p=

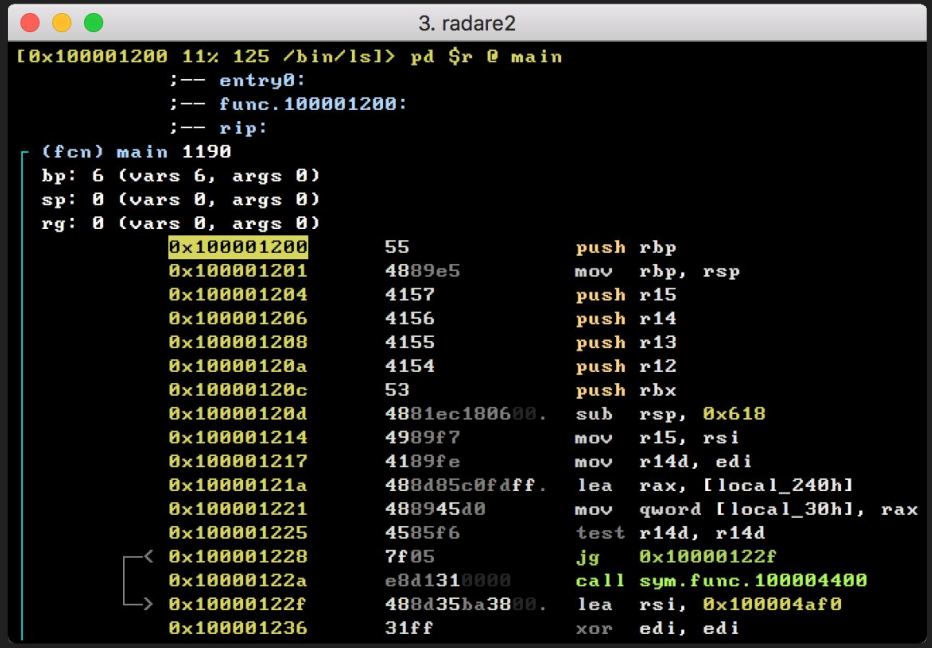
デモ

インターフェース

- メインはコマンドプロンプトCLI
- 最近はビジュアルモードが人気
- ウェブサーバのGUI (r2 -c=H)

ビジュアルモードの時には、コマンドでなくはキーにアクションをバインド

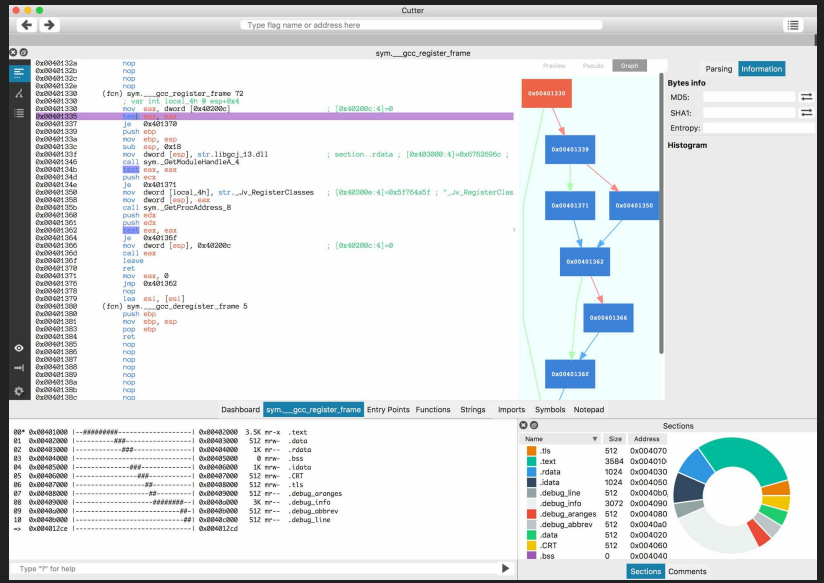
- pP"|=... でビューの変更
- ‘s’を押すと, bpを循環的に切り替える
- コマンド履歴/history
- ビジュアルアセンブラー
- インタラクティブ・グラフ



グラフUI / GUIについて

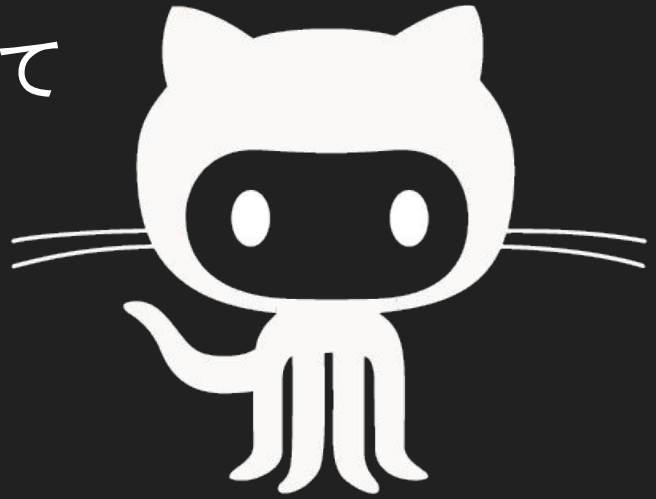
必要な時に r2pmでインストール可能（時系列）

- Gradare2 (simple gtk2/3 + vte ui)
- Ragui (unreleased)
- Bokken (unmaintained)
- Blessr2 (nodejs-blessed based UI)
- WebUIs (material, enyo, tiled, …)
- Radare2gui (.net for windows)
- Cutter (previously known as laito)
- …



デモ

カスタマイズ(read:"r2 hack")について



- ライブラリー
  - symlinksによる規定のインストール方法
  - cd libr/* ; vim ; make; run
- プラグイン
  - ./configure-plugins
  - r2pm
- バインディング
  - C APIのバインディング (Python, Perl, Ruby, Scheme, Haskell)
  - Thanks to Valabind
- スクリプト
  - スクリプトは RLangでPython, C, やValaでコーディングが可能
  - バンドの自動ローディング設定も可能

r2pipe

r2を自動化する簡単な方法

- シングル api 機能: 1個コマンドを実行、結果出力
- 多くのプログラミング言語をサポート

複数のpipeコミュニケーションチャンネル

- Pipe
- Socket
- HTTP
- Native
- Spawn

デモ

Third Party アドオンについて

色んなアドオン機能の開発プロジェクトがあります、例えば:

- scripts, plugins, patchesでr2は拡張可能…
- r2pmまたはパッケージマネージャー経由でインストール
  - デフォルトでホームにインストール（ -g を使用しない場合）
- デコンパイラ, SMT ソルバ, 多くの逆アセンブラ, ツール, …
- r2pm -sのコマンドで一覧を見ることができる

(デモ)

r2frida

- Fridaはradare2のフックエンジンであり, javascript をインジェックションし、ローカルやリモートのプロセスにフックした後さまざまなやりとりを行います
  - REPL, トレーサー, プロセスリスト, など..
- Radare2 を使えばFridaのフロントエンドとして使う事ができます
  - IO プラグインの機能を使うことができる
  - io->system 経由でのアクセス機能
  - \ や =! を使用するコマンド
- rarun2にあるr2preload を使うとself:// で自分自身のプロセスインジェクションも可能

WineDBG

- Wine は Windows エミュレータではない
- winedbgに付属し, とても素朴なコマンドライン低レベルデバッガ
- io.winedbg プラグインとのインターフェイスが可能
- bochs:// と似ている
- LinuxおよびMacプラットフォームでr2を使用してWindowsのプログラムをデバッグできます。
- 開発の初期段階
    - 多くの可能性

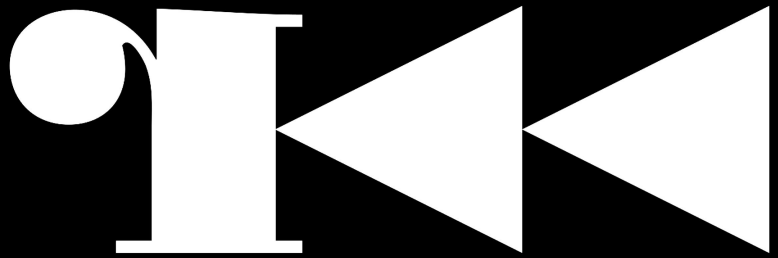
その他 3rd Partyデバッガーバックエンド

- GDB / LLDB
  - qemu、vmware、vbox、..に埋め込まれたgdbserverを介してカーネルをデバッグする ..
  - Appleのデバッグサーバ、GNUのgdbserver
  - AVRエミュレータとJTAG
- WINDBG
  - windbgサーバーに接続する
- WINEDBG
  - wine (Linux, Mac, ..)でWindowsプログラムをデバッグ
- QNX
  - 自動車で使用されるデバッグサーバ
- Bochs
  - X86 CPUデバッガーdebugger

デモ

ご質問は？

(Questions?)



Thanks For Watching!