revng

1. 构建revng工作环境

https://github.com/revng/revng

`revng` is a static binary translator. Given a input ELF binary for one of the supported architectures (currently i386, x86-64, MIPS, ARM, AArch64 and s390x) it will analyze it and emit an equivalent LLVM IR. To do so, `revng` employs the **QEMU intermediate representation** (a series of TCG instructions) and then translates them to LLVM IR.

由于官网表示构建过程ubuntu only，开一个ubuntu的docker容器。

1. 首先构建docker

```
docker pull ubuntu:20:04
docker run -it --privileged \
-v /work/stu/wtxiao/WorkSpace/revng/dockerimages:/work/stu/wtxiao/WorkSpace/revng/dockerimages \
--name revng-x86_64-ubuntu_20.04 ubuntu:20.04 /bin/bash
#项目映射路径为/work/stu/wtxiao/WorkSpace/revng/dockerimages，你可以更改为你自己的
```

2. 由于官网说明需要先有orchestra工作环境，所以先build orchestra，进入/work/stu/wtxiao/WorkSpace/revng/dockerimages目录并build：

```
apt update
apt upgrade

cd /work/stu/wtxiao/WorkSpace/revng/dockerimages
git clone https://github.com/revng/orchestra
cd orchestra

./.orchestra/ci/install-dependencies.sh
#这一步可能要很久,估计是因为pip源在国外，你可以试着先下载一个pip,然后换个源站

pip install -U pip    #它那个脚本中下载的pip版本太低了,升级一下,否则下面的某些命令用不了

pip3 cache remove orchestra
pip3 install --user --force-reinstall https://github.com/revng/revng-orchestra/archive/master.zip
#这一步也需要一些时间，等一会

export PATH="$HOME/.local/bin:$PATH" #设置环境变量

orc components    #初始化orc
```

3. 测试能否正常工作

```
# Install revng
orc install revng
orc configure revng

# Install the ARM toolchain
orc install toolchain/arm/gcc

# Enter in the build directory
orc shell -c revng

# Build
ninja

# Create hello world program
cat > hello.c <<EOF
#include <stdio.h>

int main(int argc, char *argv[]) {
  printf("Hello, world!\n");
}
EOF

# Compile
armv7a-hardfloat-linux-uclibceabi-gcc \
  -Wl,-Ttext-segment=0x20000 \
  -static hello.c \
  -o hello.arm

# Translate
./bin/revng translate hello.arm

# Run translated version
./hello.arm.translated
# Hello, world!
```

2. revng无法正常工作说明

本人在官网所提问题记录：https://github.com/revng/revng/issues/314

相似的问题：https://github.com/revng/revng/blob/develop/docs/GeneratedIRReference.rst

情况描述：

1. 书写的程序转化出的ll和bc字节码程序无法正常运行，会报类似这样的错误：

```
jit session error: symbols not found:,
```