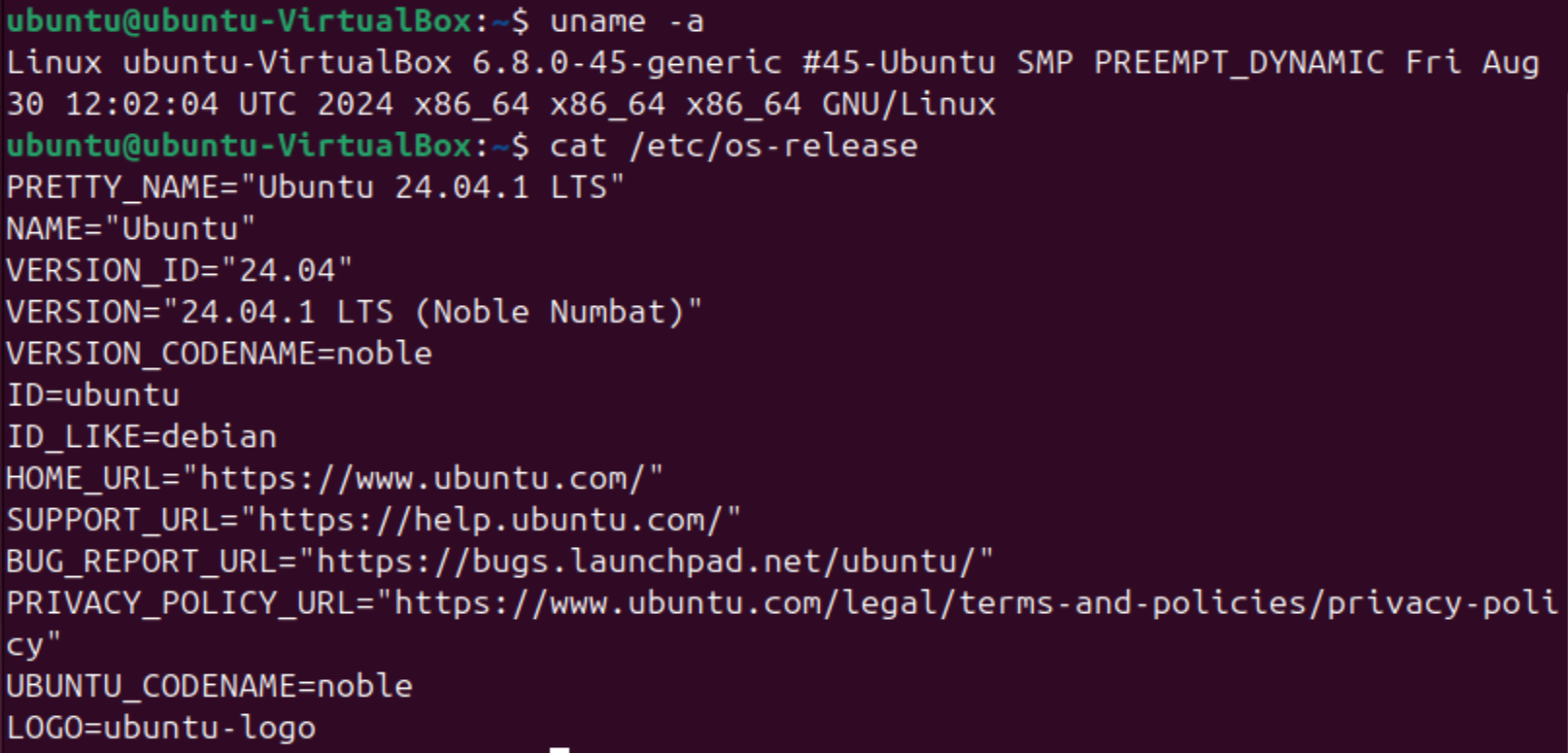
目录

[环境 1](#_Toc180054419)

[LLVM编译linux-5.4内核并获取CFG 1](#_Toc180054420)

[以sysfs\_get\_uname函数为例 3](#_Toc180054421)

# 环境



# LLVM编译linux-5.4内核并获取CFG

**# 安装llvm clang graphviz**

apt install llvm lld clang graphviz build-essential python-is-python3 python3-pip python3.12-venv flex bison libelf-dev libssl-dev

**# 下载**[**Linux-5.4 tarball**](https://cdn.kernel.org/pub/linux/kernel/v5.x/linux-5.4.284.tar.xz)

wget https://cdn.kernel.org/pub/linux/kernel/v5.x/linux-5.4.284.tar.xz

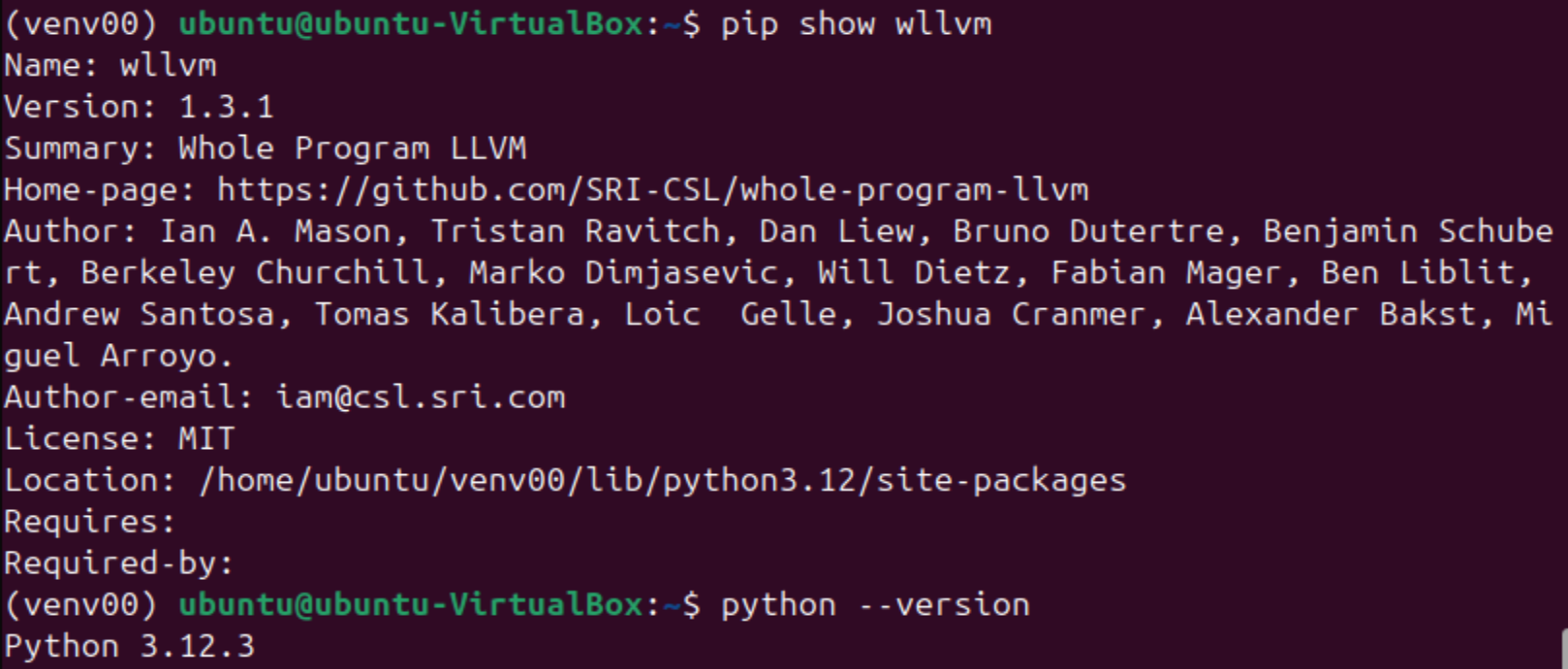
tar -xvf linux-5.4.284.tar.xz

**# 安装**[**wllvm**](https://github.com/travitch/whole-program-llvm)

python -m venv ~/venv00

source ~/venv00/bin/activate

pip install wllvm



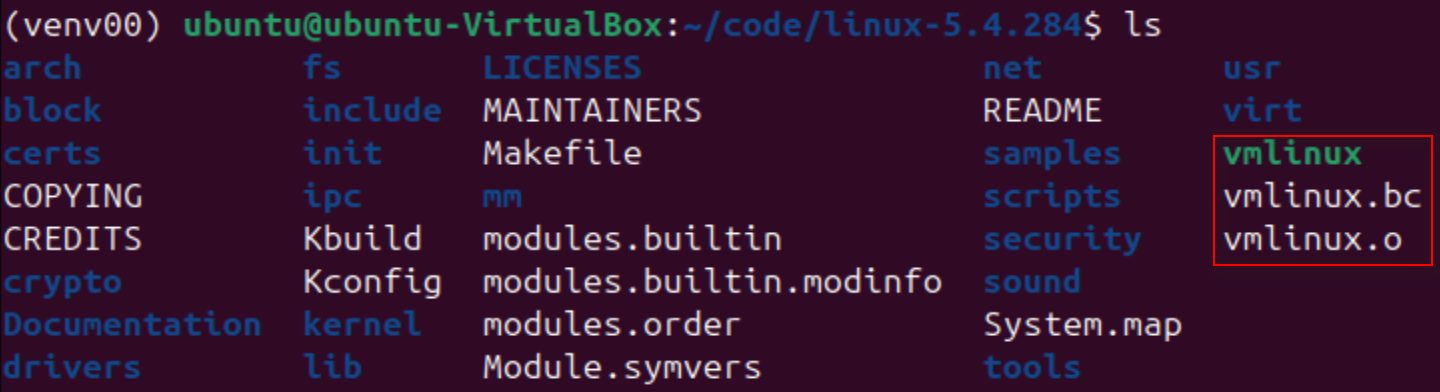
**# 编译linux-5.4**

cd linux-5.4.284

export LLVM\_COMPILER=clang

make CC=wllvm defconfig

make CC=wllvm LLVM=1



**# 从object提取bitcode**

extract-bc vmlinux

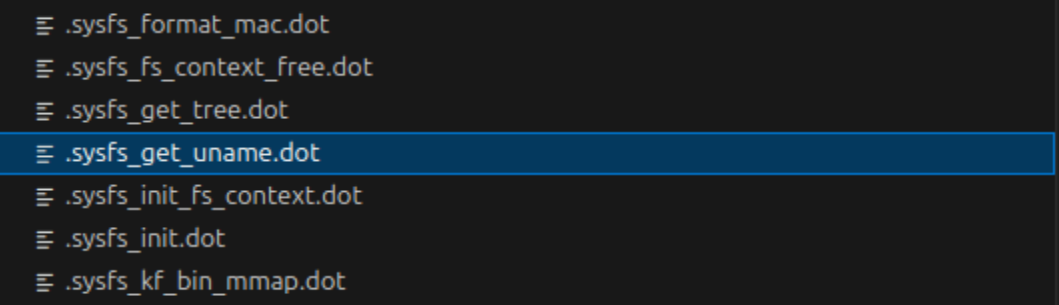
extract-bc -m vmlinux

**# 从bc转换为ll**

llvm-dis vmlinux.bc

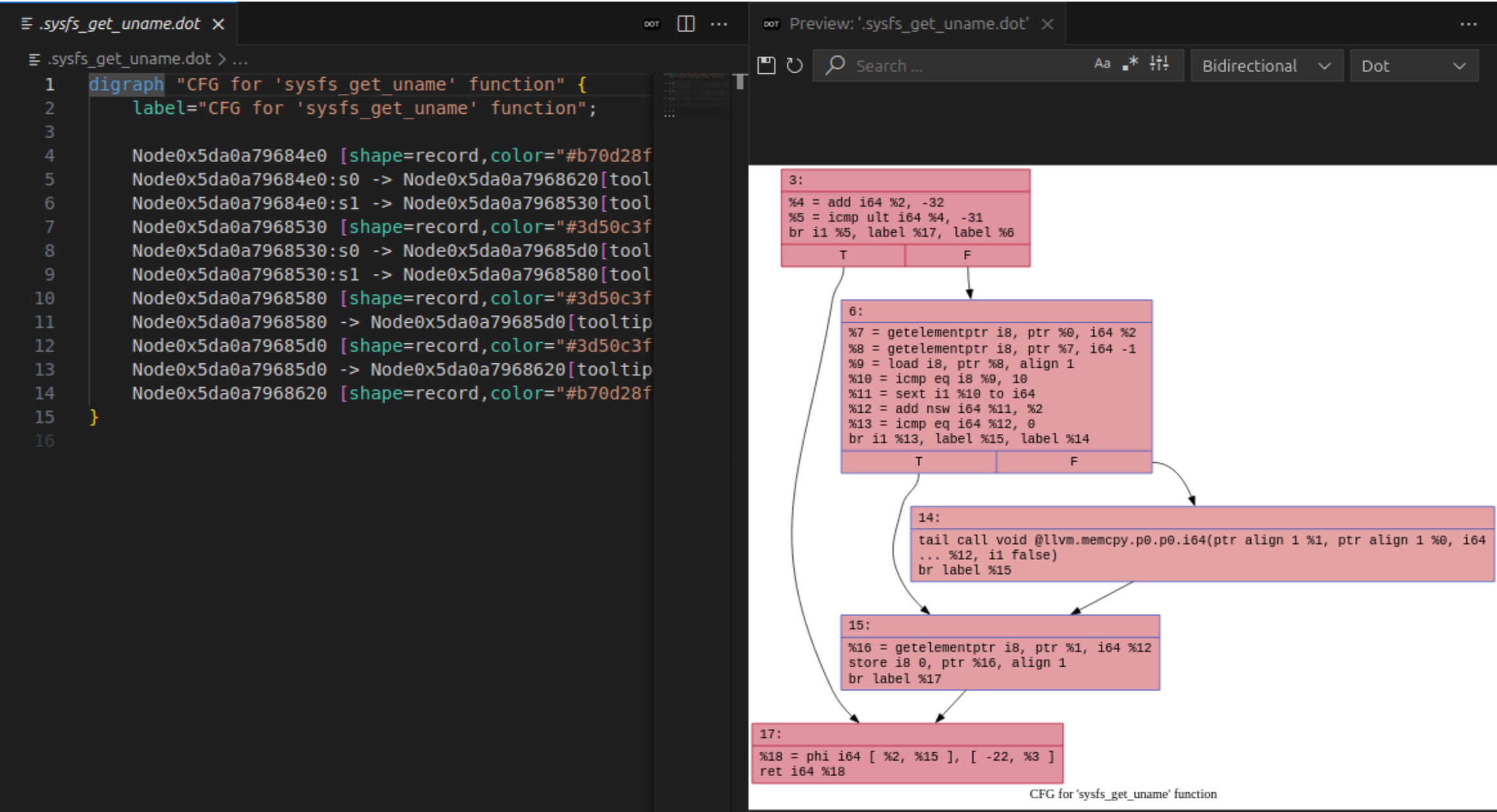
**# 从bitcode提取dot(dot文件很多)**

opt -passes=dot-cfg vmlinux.bc



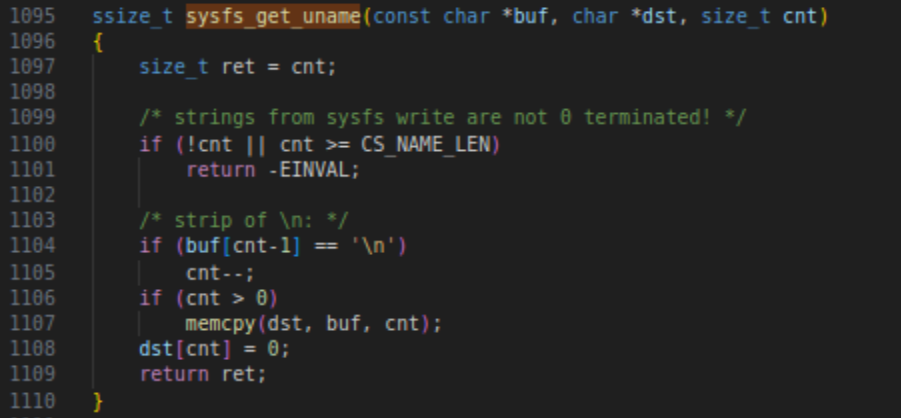
**# dot文件转换为CFG图**

# 借助vscode中的Graphviz Interactive Preview插件



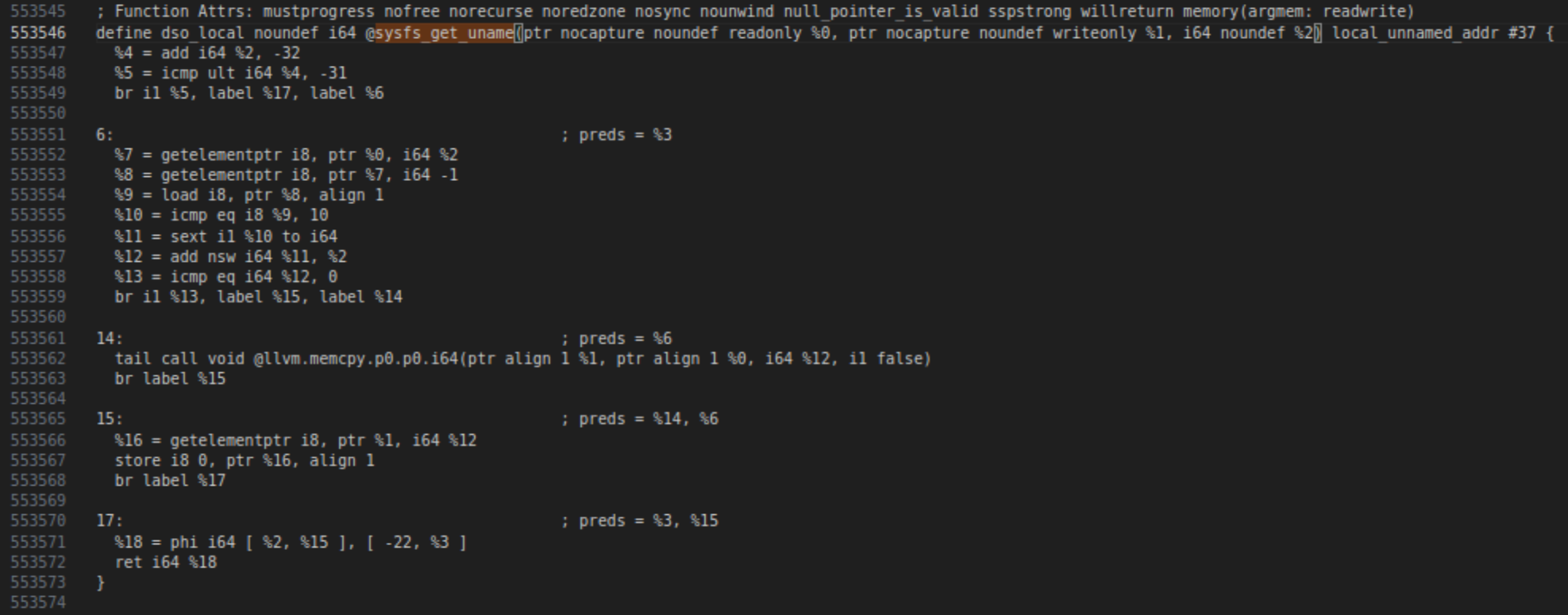
# 以sysfs\_get\_uname函数为例

* sysfs\_get\_uname函数位于kernel/time/clocksource.c文件中



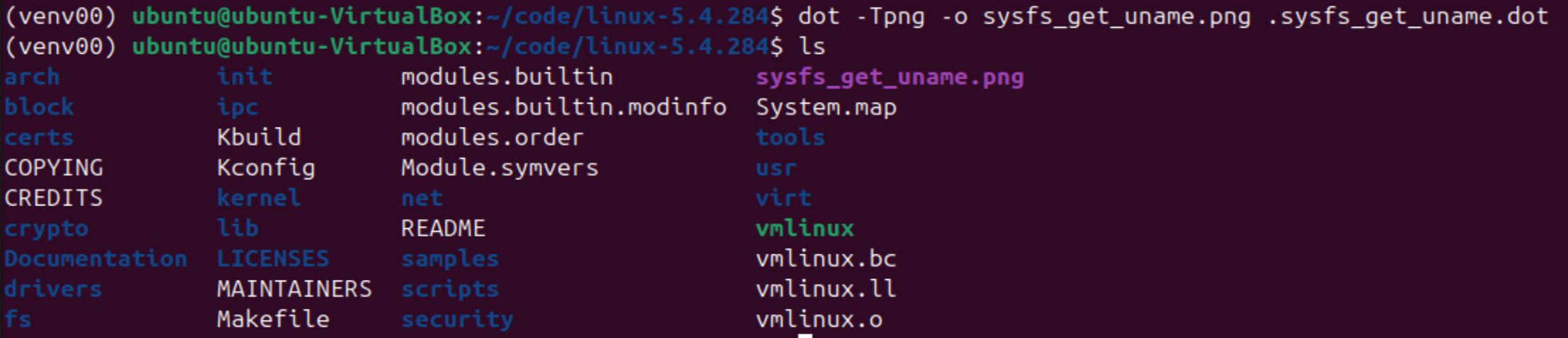
* 将vmlinux.bc转换为可阅读的vmlinux.ll，全局搜索sysfs\_get\_uname找到对应的代码

llvm-dis vmlinux.bc



* 通过dot命令获取CFG的png图片

dot -Tpng -o sysfs\_get\_uname.png .sysfs\_get\_uname.dot



* 查看CFG图片

