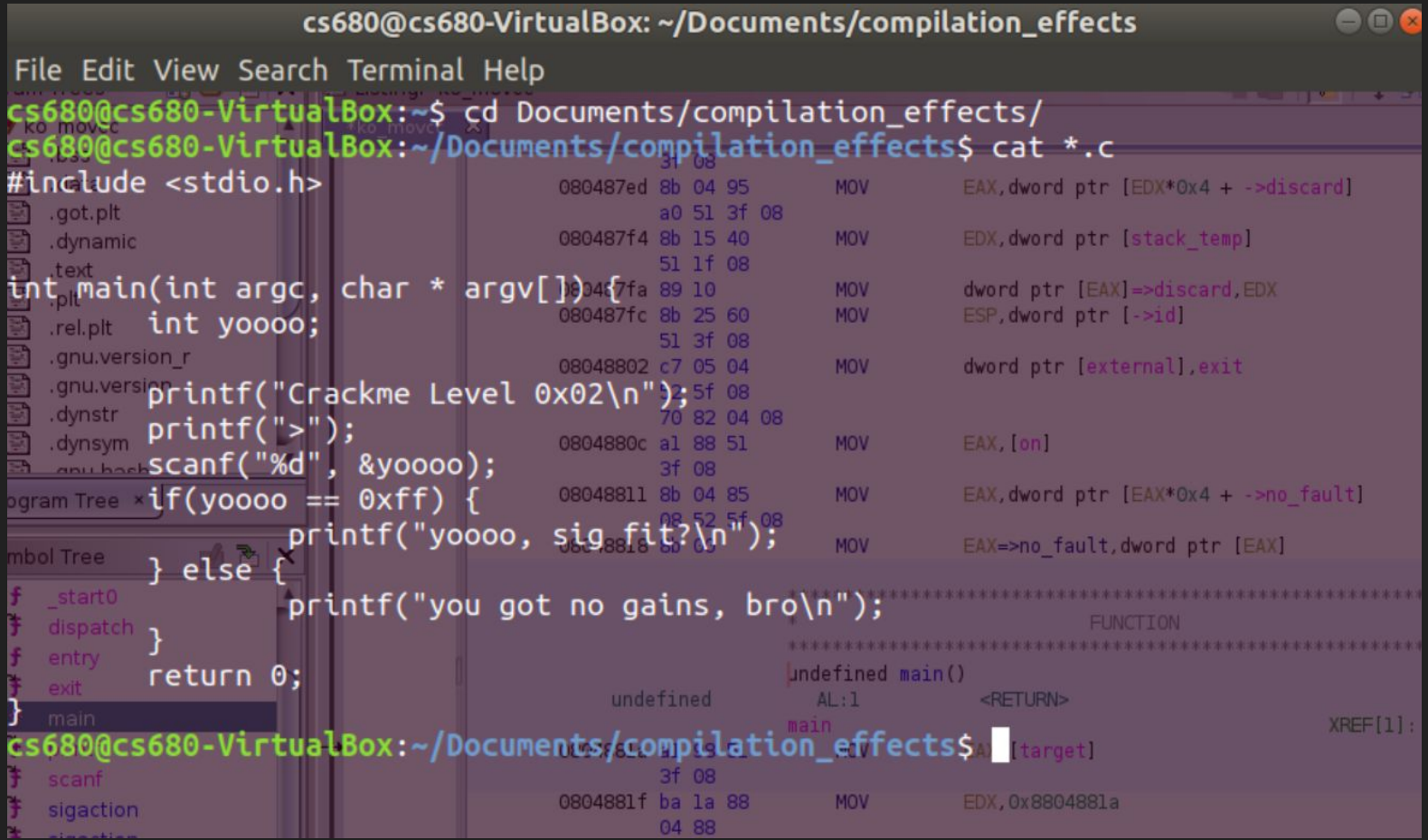
Sig • Mal

Meeting 8

crackme0x02



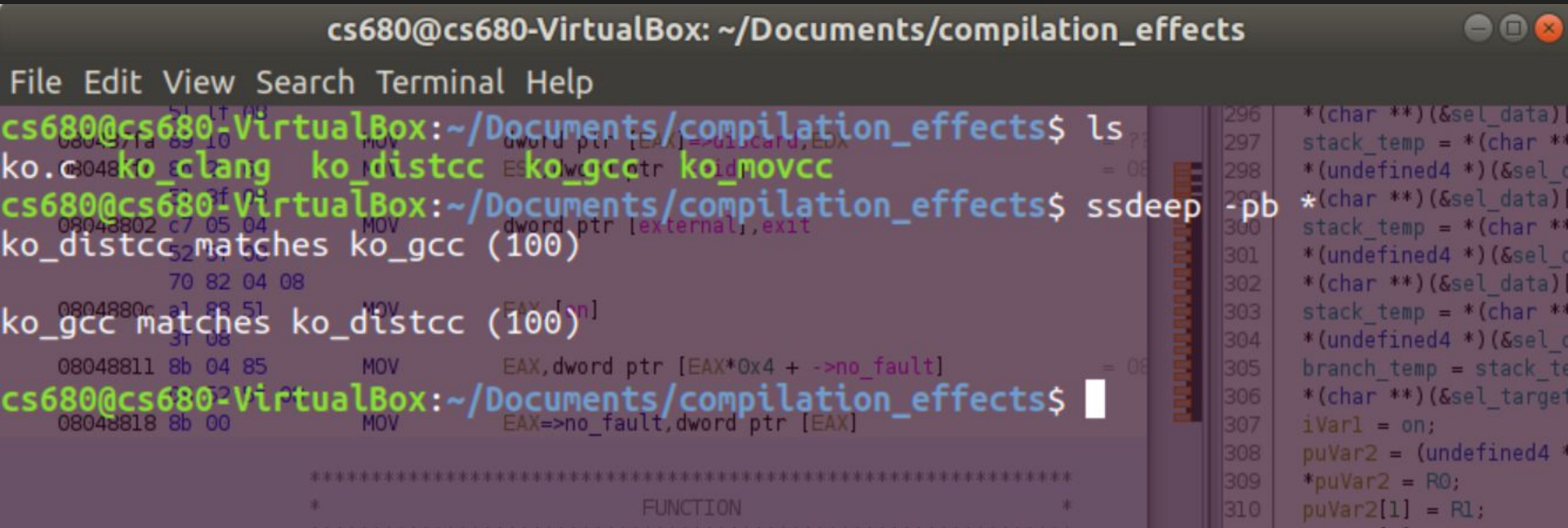
Different Decompilation Methods

- GCC / G++ → GNU C Compiler
- Clang → is a compiler front end for the C, C++, Objective-C and Objective-C++ programming languages, as well as the OpenMP, OpenCL, RenderScript, CUDA and HIP frameworks. It uses the LLVM compiler infrastructure as its back end and has been part of the LLVM release cycle since LLVM 2.6
- MOVCC → movfuscator for reversing
- Distcc → tool for speeding up compilation of source code by using distributed computing over a computer network. With the right configuration, distcc can dramatically reduce a project's compilation time

Application for Fuzzy Hashing

- Let’s use our boy, ssdeep

>> ssdeep -pb *



Compilation Methods (CLICK ME)

GCC

CLANG

MOVCC

DISTCC

Hypotheticals Hacks

- ServiceMain
+ In software, normally you write functions names that provide useful information

So your ‘program’ doesn’t run so then Hypothetically...

Hypotheticals Hacks

- ServiceMain
+ In software, normally you write functions names that provide useful information

→ Check Microsoft Documentation → Learn that in order to run a program as a service, define a ‘ServiceMain’ function
→ The presence of an exported function function called ‘ServiceMain’ tells you that your software runs as part of a service

LIVE DEMO TIME