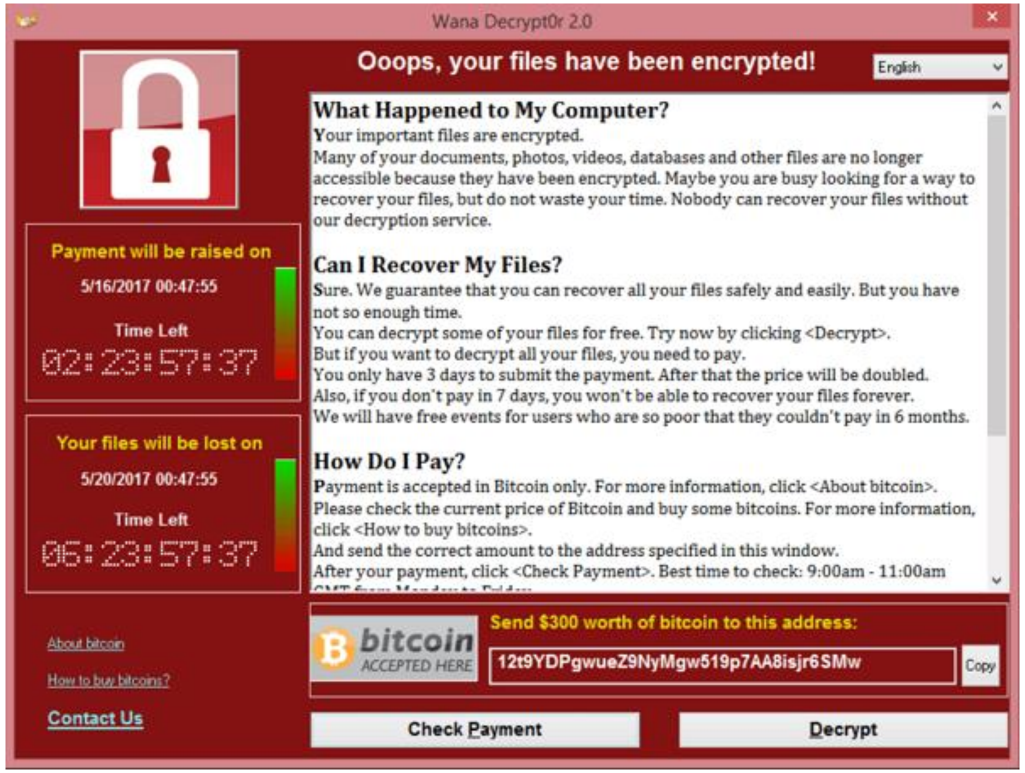
Software Reverse Engineering

Hashdump Security Club

Why reverse engineer software?

- Suppose you’re a security researcher who obtained a malware sample
- To address the malware in the wild, it’s important to analyze its behavior
- Part of the analysis can be done by running it in an isolated, sandboxed environment
  - Network requests and other behavior can be monitored
- But for more detailed analysis, it may be necessary to look at the actual code of the program



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

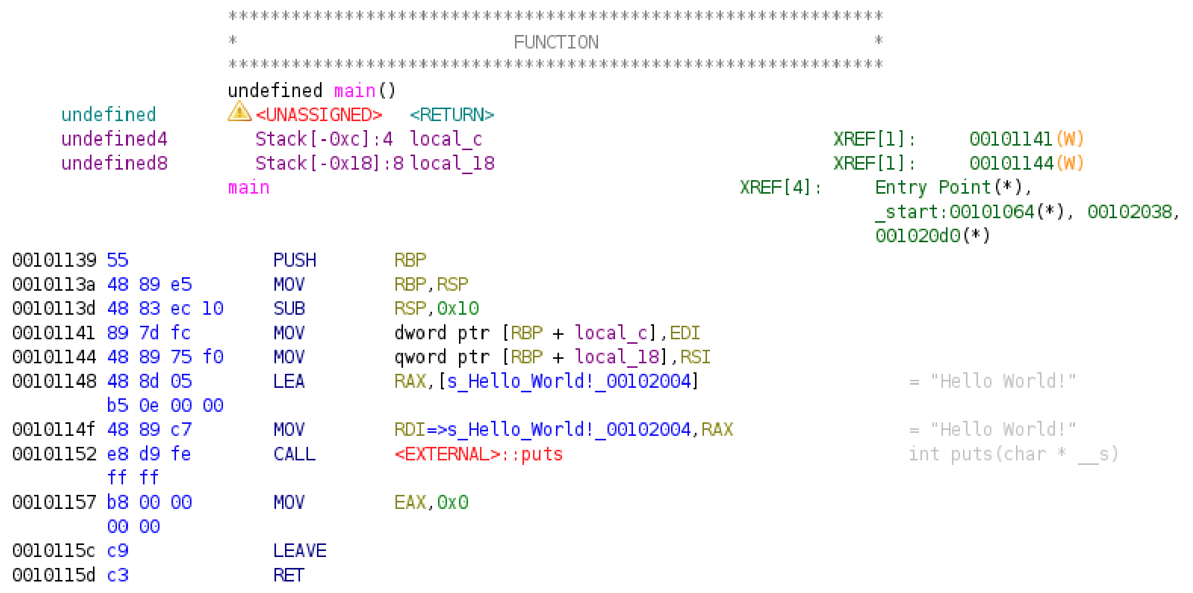
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

https://en.wikipedia.org/wiki/WannaCry_ransomware_attack

How does it work?

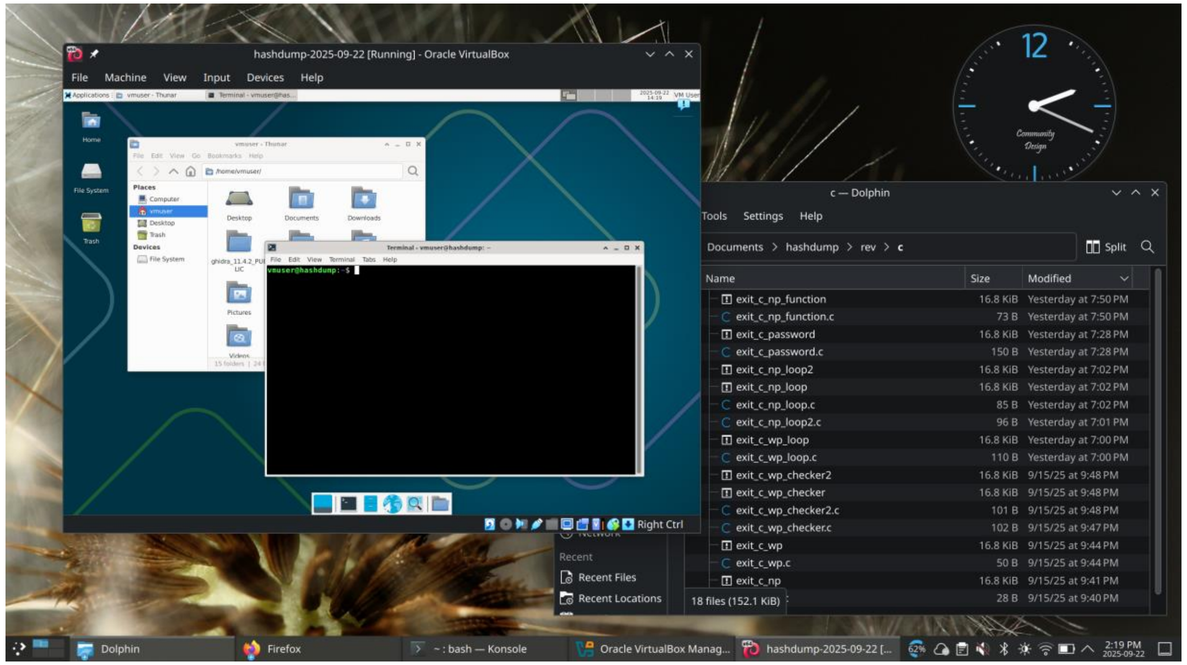
- SRE tools can disassemble and decompile programs from binaries
- Provides assembly code and a partial decompilation back to C or C++
- But this decompilation isn’t perfect: some information is lost, which the user may need to reconstruct
    - For example, variable names and types



```
                    **************************************************************
                    *                          FUNCTION                          *
                    **************************************************************
                    undefined main()
     undefined        <UNASSIGNED>   <RETURN>
     undefined4       Stack[-0xc]:4  local_c                         XREF[1]:     00101141(W)
     undefined8       Stack[-0x18]:8 local_18                        XREF[1]:     00101144(W)
                    main                                    XREF[4]:     Entry Point(*),
                                                                         _start:00101064(*), 00102038,
                                                                         001020d0(*)
00101139 55              PUSH       RBP
0010113a 48 89 e5        MOV        RBP,RSP
0010113d 48 83 ec 10     SUB        RSP,0x10
00101141 89 7d fc        MOV        dword ptr [RBP + local_c],EDI
00101144 48 89 75 f0     MOV        qword ptr [RBP + local_18],RSI
00101148 48 8d 05        LEA        RAX,[s_Hello_World!_00102004]                    = "Hello World!"
         b5 0e 00 00
0010114f 48 89 c7        MOV        RDI=>s_Hello_World!_00102004,RAX                 = "Hello World!"
00101152 e8 d9 fe        CALL       <EXTERNAL>::puts                                 int puts(char * __s)
         ff ff
00101157 b8 00 00        MOV        EAX,0x0
         00 00
0010115c c9              LEAVE
0010115d c3              RET
```

Virtualization

- Runs a guest operating system within a host OS
- Provide a semi-isolated environment from the host system
  - Allows features like networking to be turned on or off
- Example software: VirtualBox, QEMU, VMWare, HyperV
- VMs make untrusted software safer, but not completely safe [1]
  - For the strongest isolation, use air-gapped machines



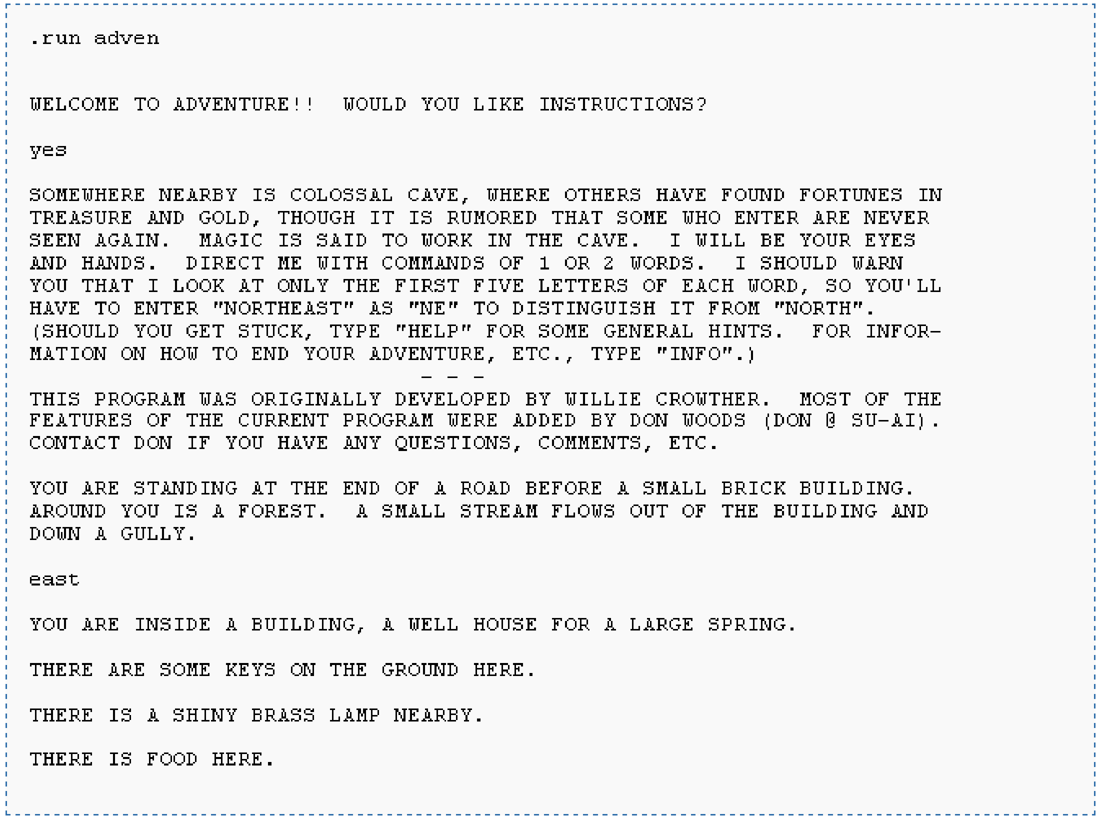
```
vmuser@hashdump:~$
```

Name	Size	Modified
exit_c_np_function	16.8 KiB	Yesterday at 7:50 PM
exit_c_np_function.c	73 B	Yesterday at 7:50 PM
exit_c_password	16.8 KiB	Yesterday at 7:28 PM
exit_c_password.c	150 B	Yesterday at 7:28 PM
exit_c_np_loop2	16.8 KiB	Yesterday at 7:02 PM
exit_c_np_loop	16.8 KiB	Yesterday at 7:02 PM
exit_c_np_loop.c	85 B	Yesterday at 7:02 PM
exit_c_np_loop2.c	96 B	Yesterday at 7:01 PM
exit_c_wp_loop	16.8 KiB	Yesterday at 7:00 PM
exit_c_wp_loop.c	110 B	Yesterday at 7:00 PM
exit_c_wp_checker2	16.8 KiB	9/15/25 at 9:48 PM
exit_c_wp_checker	16.8 KiB	9/15/25 at 9:48 PM
exit_c_wp_checker2.c	101 B	9/15/25 at 9:48 PM
exit_c_wp_checker.c	102 B	9/15/25 at 9:47 PM
exit_c_wp	16.8 KiB	9/15/25 at 9:44 PM
exit_c_wp.c	50 B	9/15/25 at 9:44 PM
exit_c_np	16.8 KiB	9/15/25 at 9:41 PM
[illegible]	28 B	9/15/25 at 9:40 PM

18 files (152.1 KiB)

Today's activity

- We have prepared some example programs to decompile
  - Multiple bite-size C programs demonstrating language features
  - A short text adventure that is otherwise impossible to beat: can you win the game?
- The software we'll be decompiling here is not malicious, but we will use a VM to model best practice regardless
- Note we will **not** be using CS lab machines here

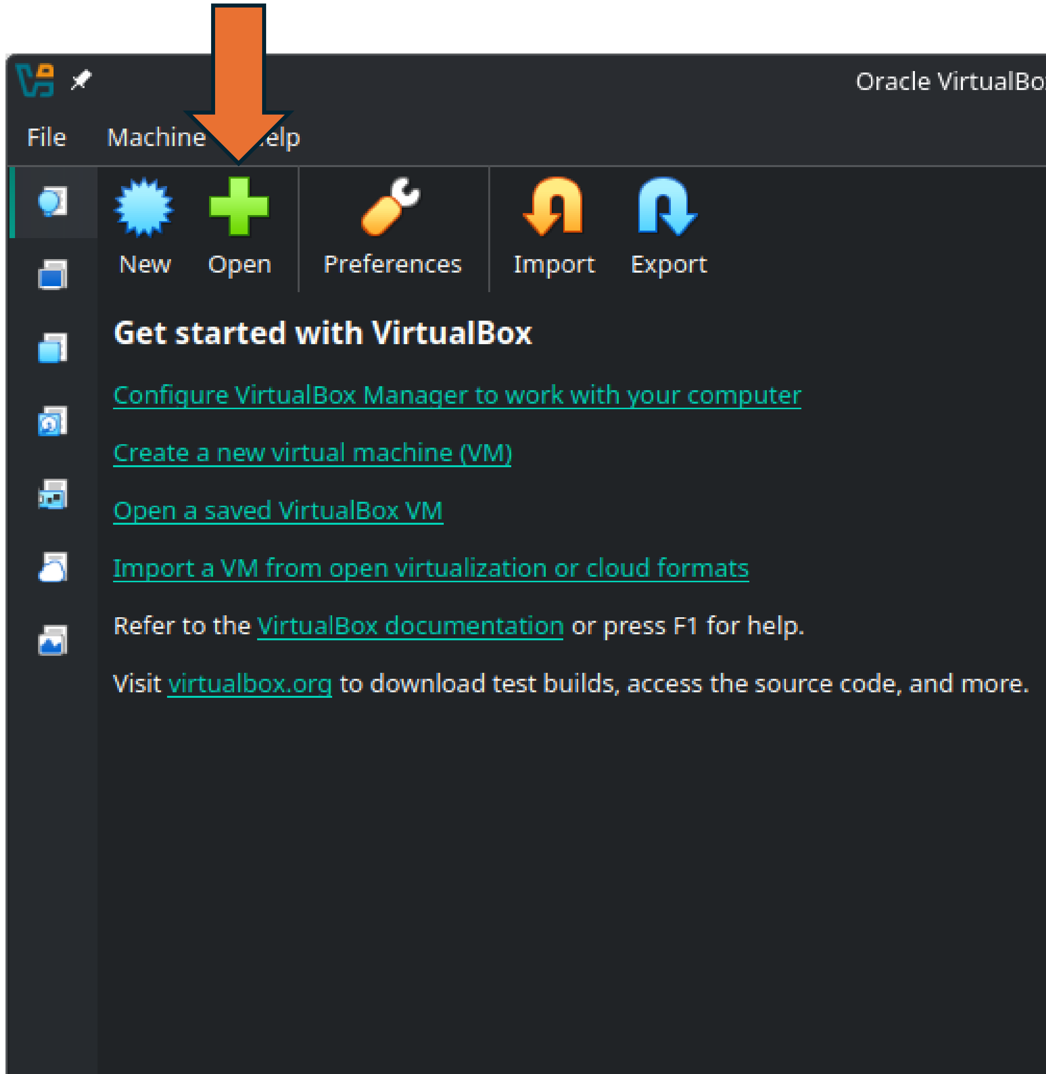


```
.run adven


WELCOME TO ADVENTURE!!  WOULD YOU LIKE INSTRUCTIONS?

yes

SOMEWHERE NEARBY IS COLOSSAL CAVE, WHERE OTHERS HAVE FOUND FORTUNES IN
TREASURE AND GOLD, THOUGH IT IS RUMORED THAT SOME WHO ENTER ARE NEVER
SEEN AGAIN.  MAGIC IS SAID TO WORK IN THE CAVE.  I WILL BE YOUR EYES
AND HANDS.  DIRECT ME WITH COMMANDS OF 1 OR 2 WORDS.  I SHOULD WARN
YOU THAT I LOOK AT ONLY THE FIRST FIVE LETTERS OF EACH WORD, SO YOU'LL
HAVE TO ENTER "NORTHEAST" AS "NE" TO DISTINGUISH IT FROM "NORTH".
(SHOULD YOU GET STUCK, TYPE "HELP" FOR SOME GENERAL HINTS.  FOR INFOR-
MATION ON HOW TO END YOUR ADVENTURE, ETC., TYPE "INFO".)
                              - - -
THIS PROGRAM WAS ORIGINALLY DEVELOPED BY WILLIE CROWTHER.  MOST OF THE
FEATURES OF THE CURRENT PROGRAM WERE ADDED BY DON WOODS (DON @ SU-AI).
CONTACT DON IF YOU HAVE ANY QUESTIONS, COMMENTS, ETC.

YOU ARE STANDING AT THE END OF A ROAD BEFORE A SMALL BRICK BUILDING.
AROUND YOU IS A FOREST.  A SMALL STREAM FLOWS OUT OF THE BUILDING AND
DOWN A GULLY.

east

YOU ARE INSIDE A BUILDING, A WELL HOUSE FOR A LARGE SPRING.

THERE ARE SOME KEYS ON THE GROUND HERE.

THERE IS A SHINY BRASS LAMP NEARBY.

THERE IS FOOD HERE.
```

https://en.wikipedia.org/wiki/Colossal_Cave_Adventure
An influence on the game you'll be playing today

Getting started

- Install VirtualBox: https://www.virtualbox.org/
    - For an ARM Mac, use UTM instead: this can emulate an x86 CPU for our VM. https://mac.getutm.app/
- Download the virtual machine image from the link sent in Discord/Teams
    - This image contains the Ghidra SRE toolkit and example programs for you to reverse engineer
- Open and run the virtual machine in VirtualBox or UTM
    - If you run into issues, let us know
    - Text too small?
      Reduce host screen resolution to 1920x1080
- Username: vmuser, password: hashdump



Get started with VirtualBox

Configure VirtualBox Manager to work with your computer

Create a new virtual machine (VM)

Open a saved VirtualBox VM

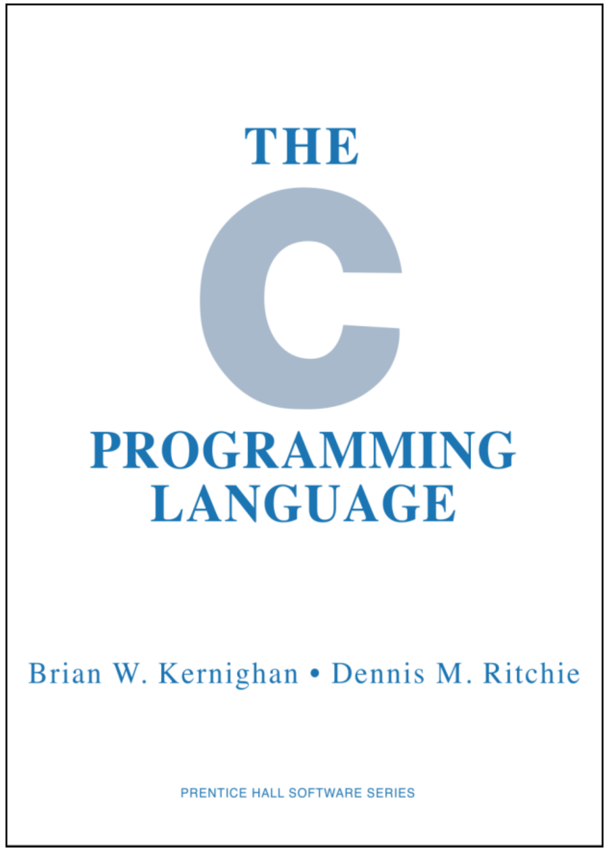
Import a VM from open virtualization or cloud formats

Refer to the VirtualBox documentation or press F1 for help.

Visit virtualbox.org to download test builds, access the source code, and more.

Useful C functions to know

- `puts(char *c)`: displays text
- `printf(char *c, args...)`: display formatted text
  - For example:
    `printf("Hello, %s, good to meet you.", "Alex")`
    `=> "Hello, Alex, good to meet you."`
- `strlen(char *c)`: get the length of a string
- `strncmp(char *lhs, char *rhs, int count)`: compare up to count characters of two strings [2]
  - returns negative number if `lhs` is alphabetically before `rhs`, positive number if `lhs` is alphabetically after `rhs`, zero if `lhs == rhs`


THE
C
PROGRAMMING LANGUAGE
Brian W. Kernighan • Dennis M. Ritchie
PRENTICE HALL SOFTWARE SERIES

References

1. Leek, Tom. Answer to "Is it safe to run untrusted application inside a Virtual Machine." StackExchange, 2014, https://security.stackexchange.com/a/56982.
2. "strncmp." cppreference.com, https://en.cppreference.com/w/c/string/byte/strncmp.