GRACE HOPPER CELEBRATION

ANITA B.ORG

Ghidra - NSA's Software Reverse Engineering Tool

#GHC19

Ghidra

Many Heads Make Light Work

Gwen Lilly

#GHC19

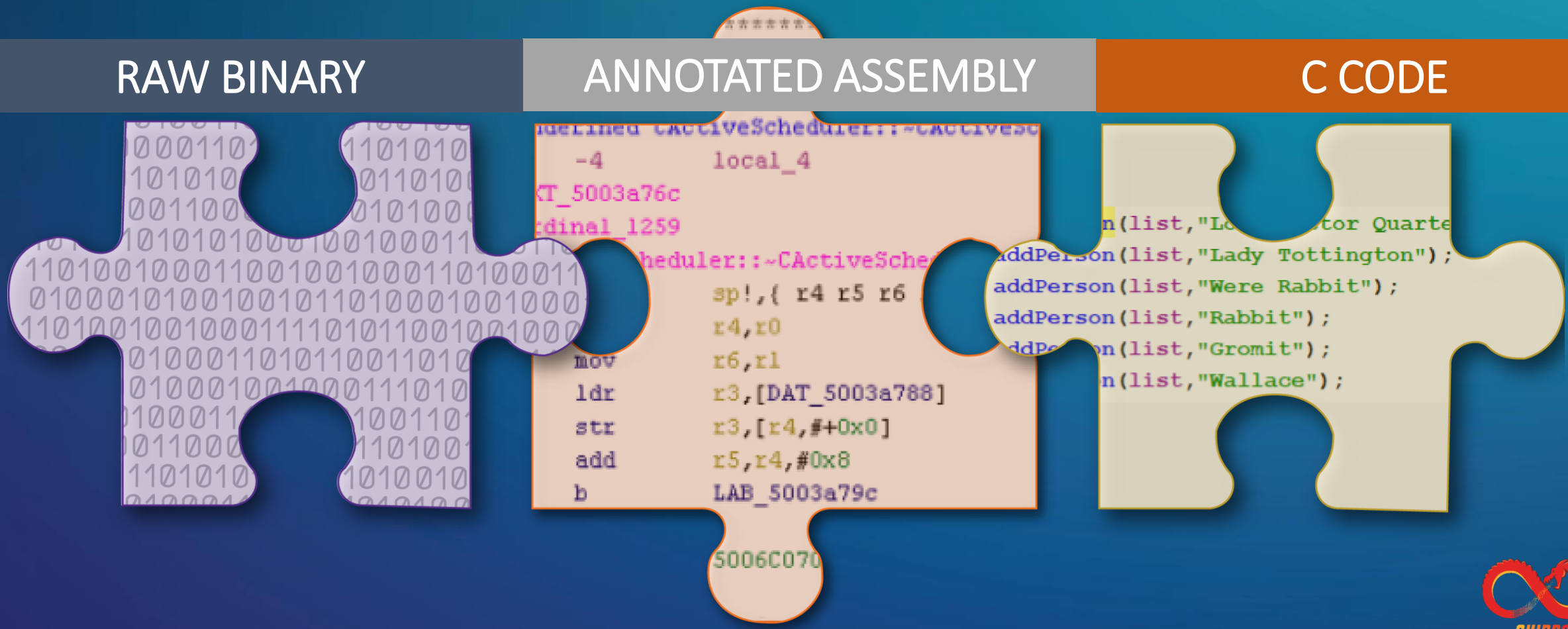
What's in your binary?

Assembling the puzzle

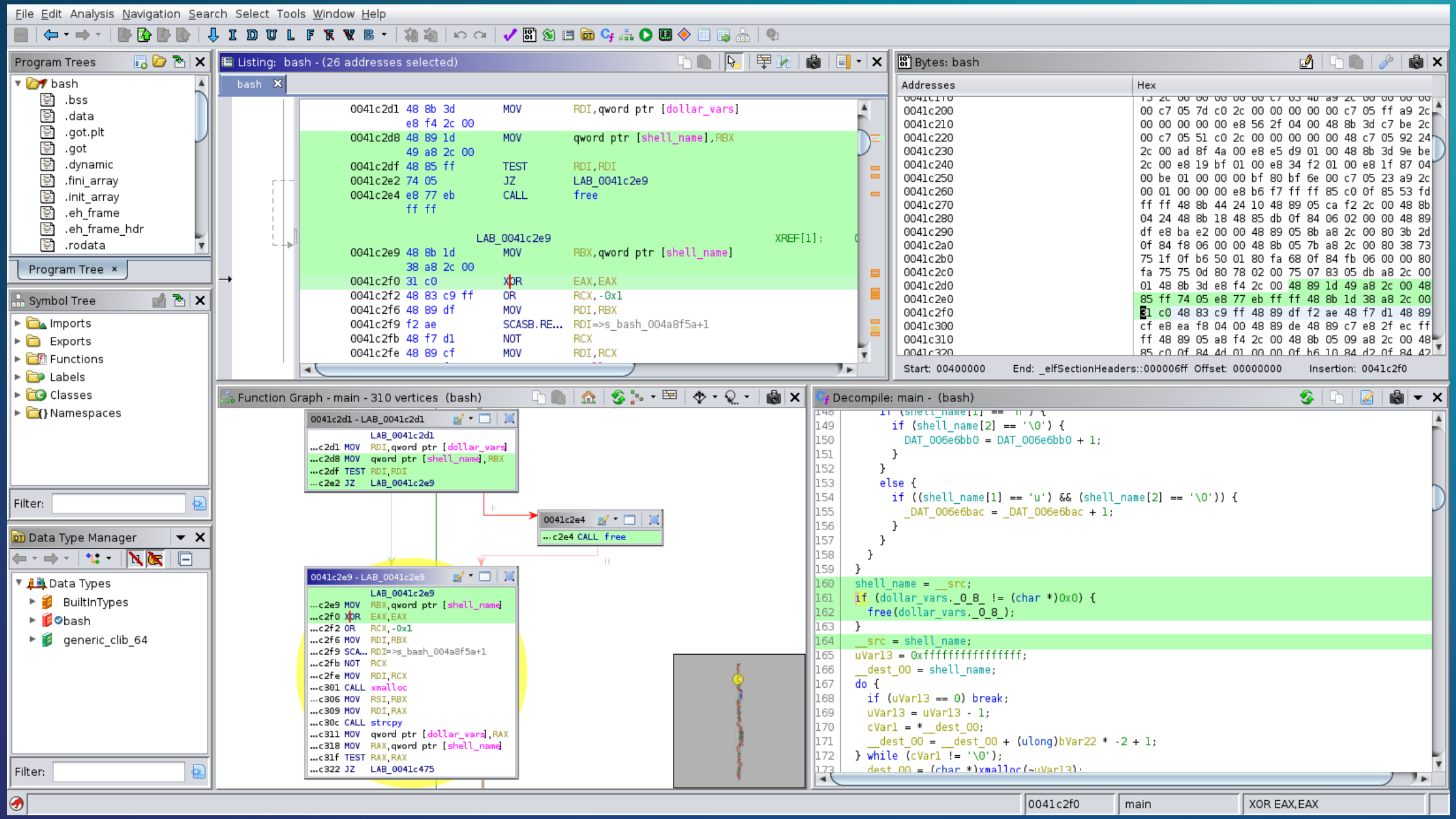
RAW BINARY

ANNOTATED ASSEMBLY

C CODE



GHIDRA


File Edit Analysis Navigation Search Select Tools Window Help
Program Trees
bash
.bss
.data
.got.plt
.got
.dynamic
.fini_array
.init_array
.eh_frame
.eh_frame_hdr
.rodata
Program Tree
Symbol Tree
Imports
Exports
Functions
Labels
Classes
Namespaces
Filter:
Data Type Manager
Data Types
BuiltInTypes
bash
generic_clib_64
Filter:
Listing: bash - (26 addresses selected)
bash
0041c2d1 48 8b 3d e8 f4 2c 00 MOV RDI,qword ptr [dollar_vars]
0041c2d8 48 89 1d 49 a8 2c 00 MOV qword ptr [shell_name],RBX
0041c2df 48 85 ff TEST RDI,RDI
0041c2e2 74 05 JZ LAB_0041c2e9
0041c2e4 e8 77 eb ff ff CALL free
LAB_0041c2e9 XREF[1]:
0041c2e9 48 8b 1d 38 a8 2c 00 MOV RBX,qword ptr [shell_name]
0041c2f0 31 c0 XOR EAX,EAX
0041c2f2 48 83 c9 ff OR RCX,-0x1
0041c2f6 48 89 df MOV RDI,RBX
0041c2f9 f2 ae SCASB.RE... RDI=>s_bash_004a8f5a+1
0041c2fb 48 f7 d1 NOT RCX
0041c2fe 48 89 cf MOV RDI,RCX
Bytes: bash
Addresses
Hex
0041c200 00 c7 05 7d c0 2c 00 00 00 00 00 c7 05 ff a9 2c
0041c210 00 00 00 00 00 e8 56 2f 04 00 48 8b 3d c7 be 2c
0041c220 00 c7 05 51 c0 2c 00 00 00 00 00 48 c7 05 92 24
0041c230 2c 00 ad 8f 4a 00 e8 e5 d9 01 00 48 8b 3d 9e be
0041c240 2c 00 e8 19 bf 01 00 e8 34 f2 01 00 e8 1f 87 04
0041c250 00 be 01 00 00 00 bf 80 bf 6e 00 c7 05 23 a9 2c
0041c260 00 01 00 00 00 e8 b6 f7 ff ff 85 c0 0f 85 53 fd
0041c270 ff ff 48 8b 44 24 10 48 89 05 ca f2 2c 00 48 8b
0041c280 04 24 48 8b 18 48 85 db 0f 84 06 02 00 00 48 89
0041c290 df e8 ba e2 00 00 48 89 05 8b a8 2c 00 80 3b 2d
0041c2a0 0f 84 f8 06 00 00 48 8b 05 7b a8 2c 00 80 38 73
0041c2b0 75 1f 0f b6 50 01 80 fa 68 0f 84 fb 06 00 00 80
0041c2c0 fa 75 75 0d 80 78 02 00 75 07 83 05 db a8 2c 00
0041c2d0 01 48 8b 3d e8 f4 2c 00 48 89 1d 49 a8 2c 00 48
0041c2e0 85 ff 74 05 e8 77 eb ff ff 48 8b 1d 38 a8 2c 00
0041c2f0 31 c0 48 83 c9 ff 48 89 df f2 ae 48 f7 d1 48 89
0041c300 cf e8 ea f8 04 00 48 89 de 48 89 c7 e8 2f ec ff
0041c310 ff 48 89 05 a8 f4 2c 00 48 8b 05 09 a8 2c 00 48
Start: 00400000 End: _elfSectionHeaders::000006ff Offset: 00000000 Insertion: 0041c2f0
Function Graph - main - 310 vertices (bash)
0041c2d1 - LAB_0041c2d1
LAB_0041c2d1
...c2d1 MOV RDI,qword ptr [dollar_vars]
...c2d8 MOV qword ptr [shell_name],RBX
...c2df TEST RDI,RDI
...c2e2 JZ LAB_0041c2e9
0041c2e4
...c2e4 CALL free
0041c2e9 - LAB_0041c2e9
LAB_0041c2e9
...c2e9 MOV RBX,qword ptr [shell_name]
...c2f0 XOR EAX,EAX
...c2f2 OR RCX,-0x1
...c2f6 MOV RDI,RBX
...c2f9 SCA... RDI=>s_bash_004a8f5a+1
...c2fb NOT RCX
...c2fe MOV RDI,RCX
...c301 CALL xmalloc
...c306 MOV RSI,RBX
...c309 MOV RDI,RAX
...c30c CALL strcpy
...c311 MOV qword ptr [dollar_vars],RAX
...c318 MOV RAX,qword ptr [shell_name]
...c31f TEST RAX,RAX
...c322 JZ LAB_0041c475
Decompile: main - (bash)
149 if (shell_name[2] == '\0') {
150 DAT_006e6bb0 = DAT_006e6bb0 + 1;
151 }
152 }
153 else {
154 if ((shell_name[1] == 'u') && (shell_name[2] == '\0')) {
155 _DAT_006e6bac = _DAT_006e6bac + 1;
156 }
157 }
158 }
159 }
160 shell_name = __src;
161 if (dollar_vars._0_8_ != (char *)0x0) {
162 free(dollar_vars._0_8_);
163 }
164 __src = shell_name;
165 uVar13 = 0xffffffffffffffff;
166 __dest_00 = shell_name;
167 do {
168 if (uVar13 == 0) break;
169 uVar13 = uVar13 - 1;
170 cVar1 = *__dest_00;
171 __dest_00 = __dest_00 + (ulong)bVar22 * -2 + 1;
172 } while (cVar1 != '\0');
0041c2f0
main
XOR EAX,EAX

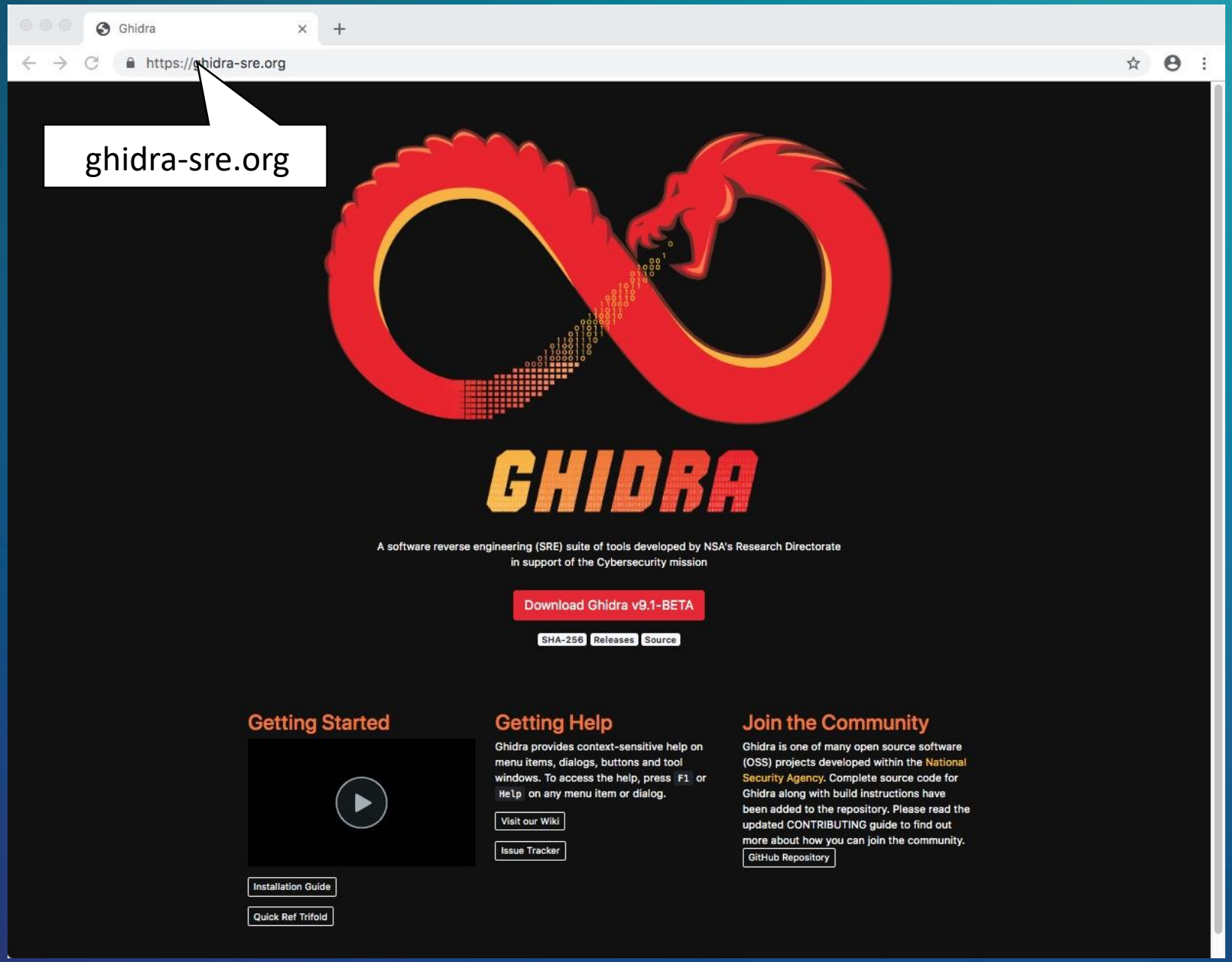
#GHC19

Why Release?

- Tax $$ at work
- Improve Cybersecurity Tools
- Enhance Education Programs
- Build a Community of Users

ghidra-sre.org Stats (Sept 23)

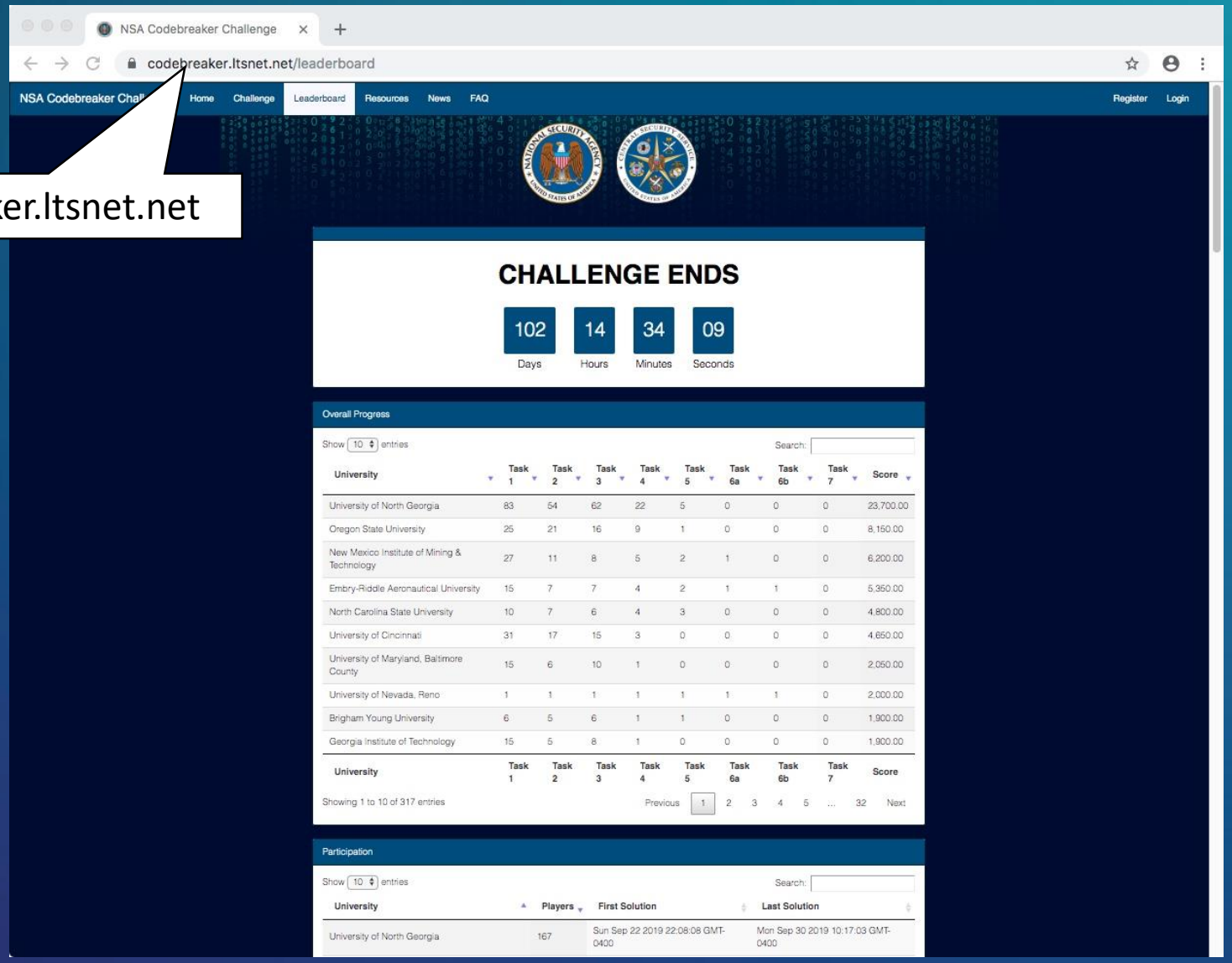
- 9.0.0: 302k downloads
- 9.0.1: 36k downloads
- 9.0.2: 107k downloads
- 9.0.4:155k downloads
- Site views: 13.9M
- Video hits: 818k



#GHC19

Level the playing field ➡ Feed the pipeline

Codebreaker.ltsnet.net

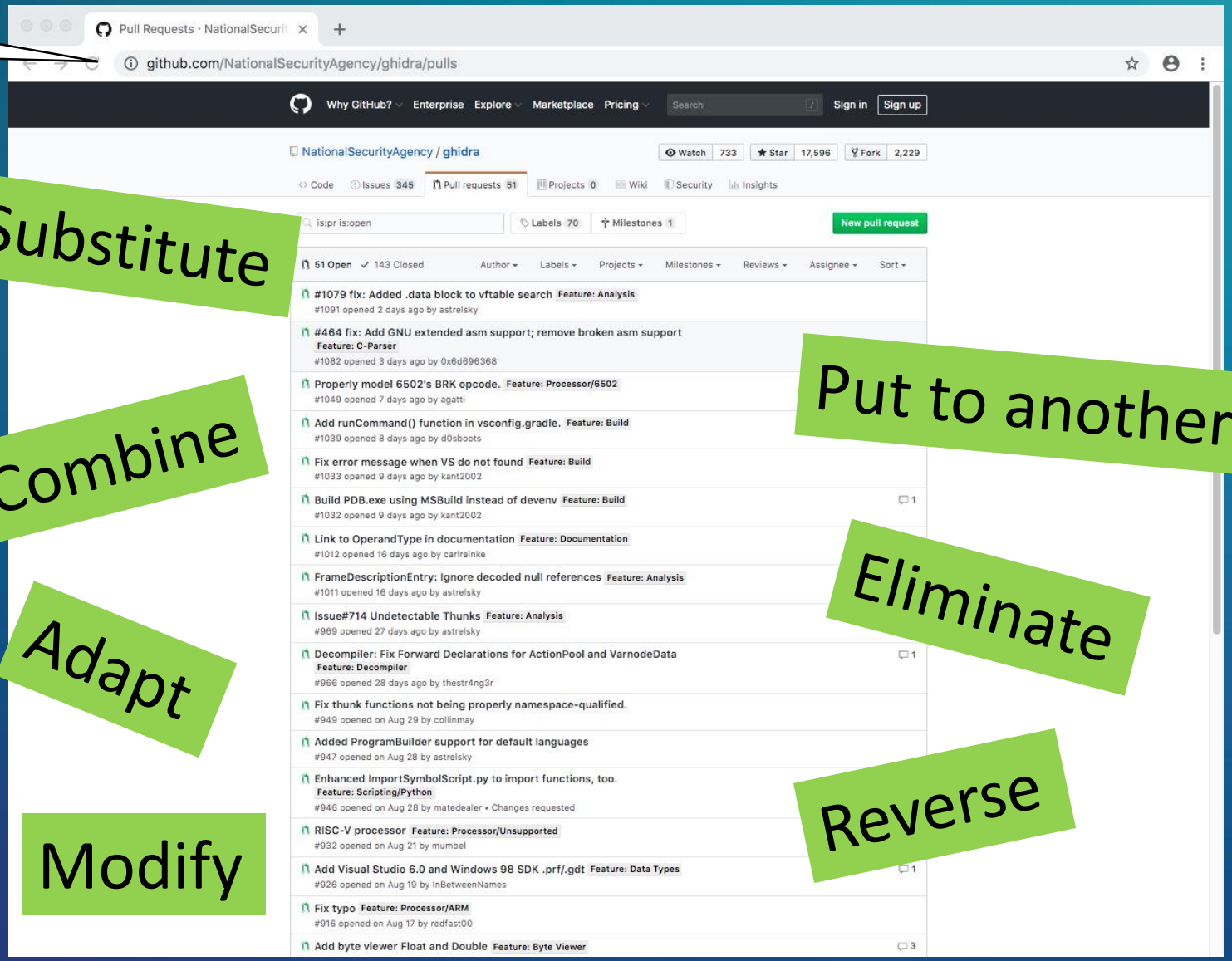


GHIDRA

#GHC19

Full access to code components ➡ SCAMPER

Github.com/National SecurityAgency/ghidra



Substitute

Combine

Adapt

Modify

Put to another use

Eliminate

Reverse

GitHub Project Stats (Sept 30)

- 17598 stars
- 2229 forks
- 733 watching
- 1099 issues submitted
  - 346 open issues
- 194 pull requests
  - 51 open

GHIDRA

#GHC19

Open participation ➡ Diversity

"On the Internet, nobody knows you're a dog."

Peter Steiner's cartoon, as published in *The New Yorker*

GHIDRA

#GHC19

Please remember to complete the session survey in the mobile app.

Please join our community:

www.ghidra.-sre.org

https://github.com/NationalSecurityAgency/ghidra

Please visit us at Booth T1856

@NSAUSGov

@_national_security_agency_

@NSAGov

GRACE HOPPER CELEBRATION

ANITA B.ORG

#GHC19

Framework Components

Database for artifacts and analytic results

Standard schema

Architecture agnostic tool platform

Network collaboration

Includes the basics

Scalable

Extensible