A Beginner’s Guide to Ghidra on Ubuntu 20

Derek J. Steel

SecureSet Academy

Author Note

In partial fulfillment of the requirements for SYS 400

Instructors: Bryan Frier, Eric Keith, and Kurt Schumaker

August 25, 2020

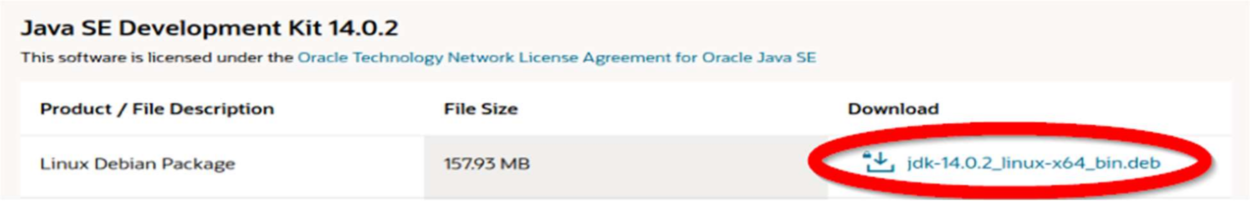
Setup

Installing Oracle's Java Development Kit (JDK)

Ghidra requires the use of a JDK. Two options are Oracle's JDK and OpenJDK. For this walkthrough, we will be using Oracle's JDK due to the ease of use and the simpler setup process for Ghidra.

One thing to be aware of is that Oracle's JDK is free to use for personal and development use, but certain commercial uses require a license. These licenses can range from $15 - $1,200 depending on the type of license needed. (Oracle, 2020) Below are the steps necessary to install the JDK on an Ubuntu 20 system.

1. Navigate to https://www.oracle.com/java/technologies/javase-downloads.html and click on **JDK Download**. This ensures that you are downloading the most current version of JDK.
2. Scroll down until you see **Java SE Development Kit** and choose the Linux Debian Package to download.



Java SE Development Kit 14.0.2

This software is licensed under the Oracle Technology Network License Agreement for Oracle Java SE

Product / File Description	File Size	Download
Linux Debian Package	157.93 MB	jdk-14.0.2_linux-x64_bin.deb

3. To install using the GUI, navigate to your downloads folder, right click on the downloaded file, and click **Install**. To install through the command line, **`sudo dpkg -i ~/Downloads/jdk-14.0.2_linux-x64_bin.deb`**
    a. Note that the JDK version number may vary depending on which version you downloaded.

Installing Ghidra

First, make sure you have a JDK installed on your Ubuntu 20 machine. Ubuntu 20 does not come with a native JDK installed. If you have not manually installed one, see the instructions on page 2 for how to install Oracle's JDK. These instructions are modified from Tristan Messner's video *Ghidra Tutorial 1: Installing Ghidra on linux*. (Messner, Ghidra Tutorial 1: Installing Ghidra on linux, 2019)

1. In your preferred web browser, navigate to https://ghidra-sre.org and click the download button. (National Security Agency, 2020)
2. In your terminal `cd ~/Downloads`
3. Unzip Ghidra by typing `unzip ghidra` into your console then hit the **Tab** to autocomplete the command. This will ensure that there are no errors in the command.
4. Change directories into the newly created directory. `cd ghidra` then hit **Tab**
5. Locate and run `./ghidraRun` from the new directory.

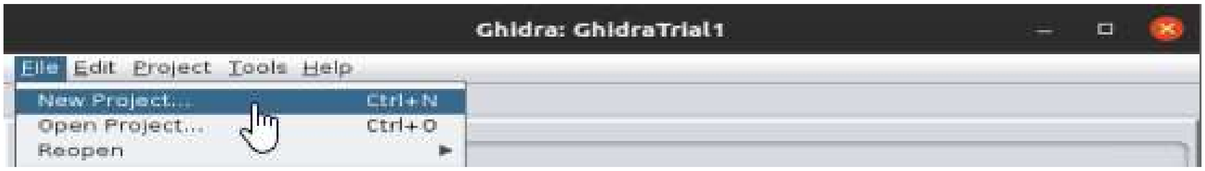
Running and Using Ghidra

Initial Startup

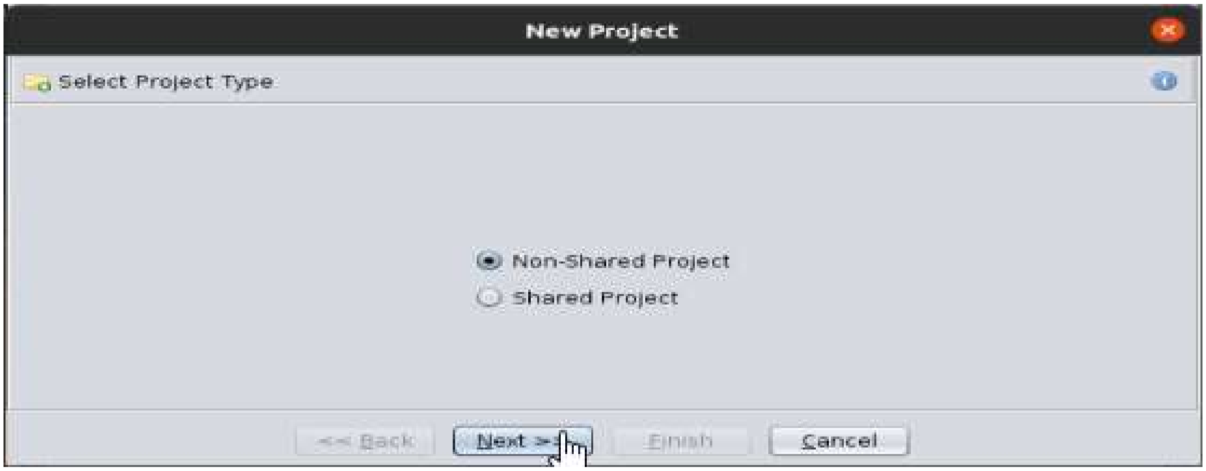
1. Either change directories into the Ghidra installation folder, then run `./ghidraRun` or run it from any other location using the following command.

   ```
   ~/Downloads/ghidra_9.1.2_PUBLIC/ghidraRun
   ```

2. If this is a fresh installation, Ghidra will not have any projects in it. To add a new project, click on **File > New Project**.

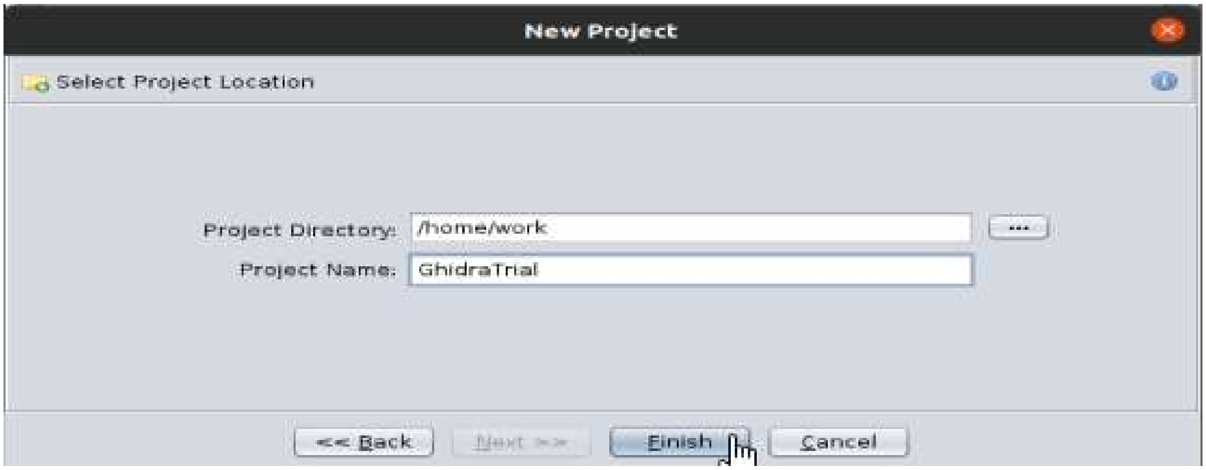


3. If you do not want to share this project, simply click **Next**.



● Non-Shared Project
○ Shared Project

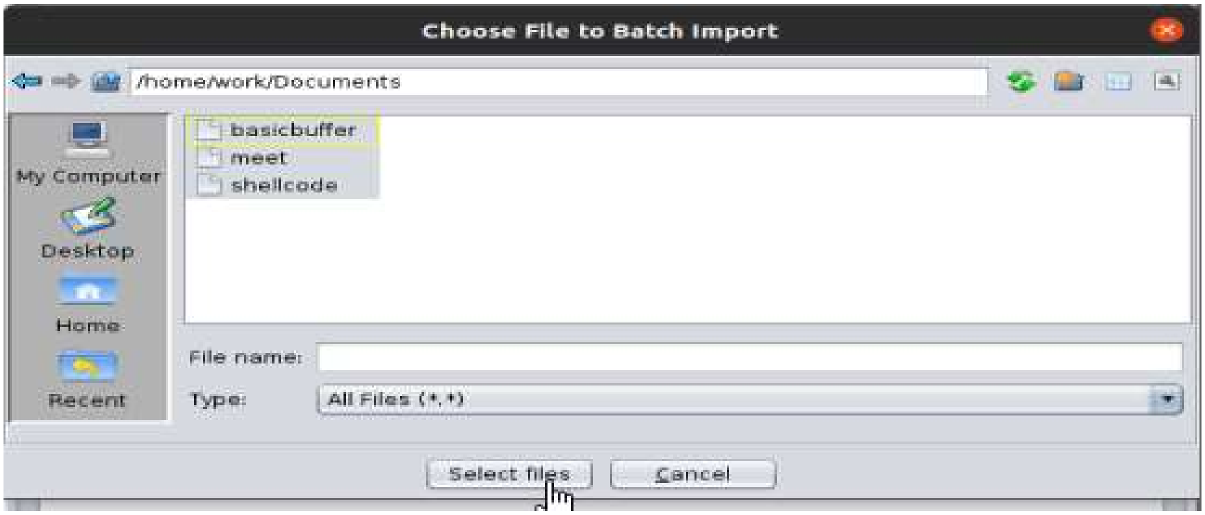
4. Select the directory where you want to save your project, name your project, then click **Finish** to create it.



Project Directory: /home/work
Project Name: GhidraTrial

Importing Files

1. To import files into your project, click on **File** then choose either **Import File** or **Batch Import**. While **Import File** will only let you import one file at a time, **Batch Import** will allow you to import multiple files at once.
2. Once you have chosen your import method, navigate to the files you want to import, select them, and choose **Select File**, then select **Okay** on the following window. (Messner, Ghidra Tutorial 2: Solving a very simple crackme, 2019)



/home/work/Documents

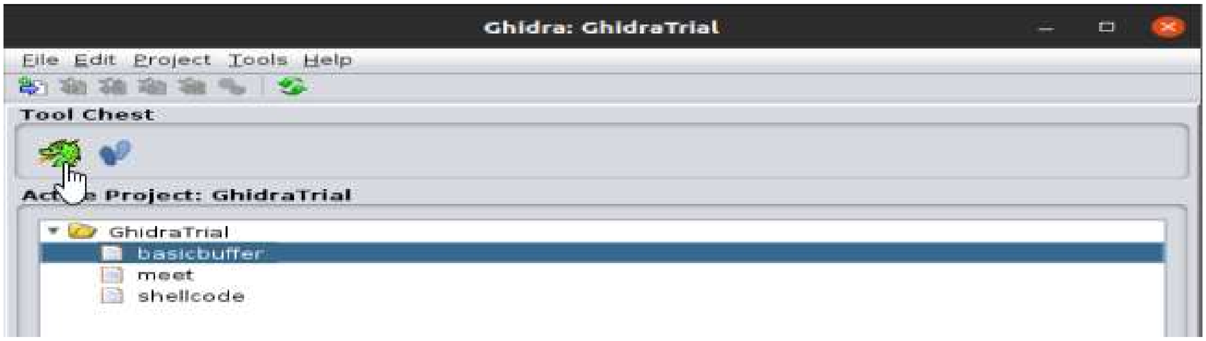
- basicbuffer
- meet
- shellcode

File name:

Type: All Files (*.*)

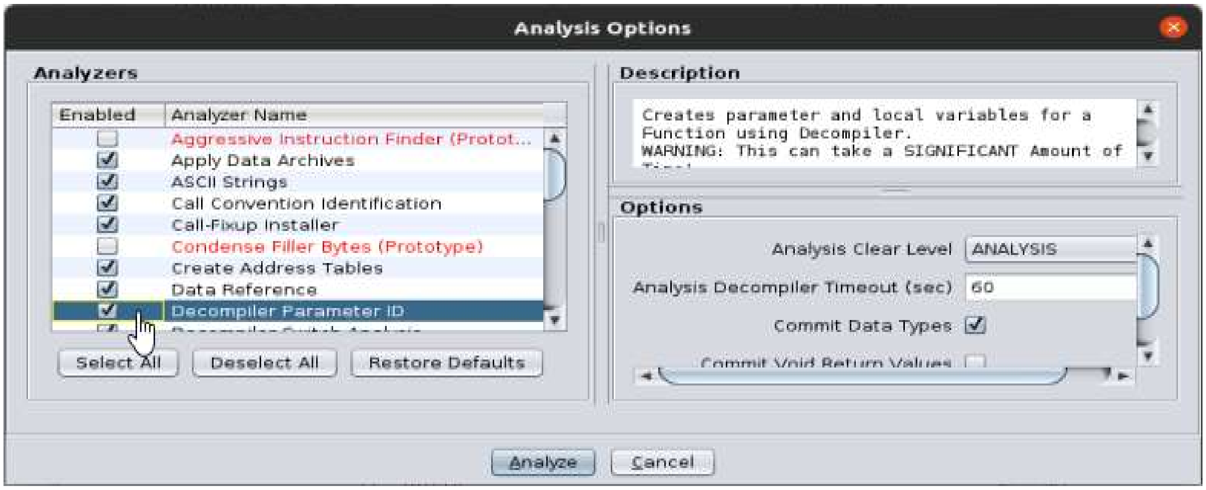
Working With Imported Files

Ghidra has a wide variety of tools available to users, including a decompiler, data type managers, program trees, and symbol trees. In order to use these functions, either double click on your file, or select a file and click on the Green Dragon’s Head.



- GhidraTrial
  - basicbuffer
  - meet
  - shellcode

A new window will open, and a pop-up will ask if you would like to analyze the selected file. Choose yes, then ensure that **Decompiler Parameter ID** is selected in the following window.



Enabled	Analyzer Name
□	Aggressive Instruction Finder (Protot...
☑	Apply Data Archives
☑	ASCII Strings
☑	Call Convention Identification
☑	Call-Fixup Installer
□	Condense Filler Bytes (Prototype)
☑	Create Address Tables
☑	Data Reference
☑	Decompiler Parameter ID

Description

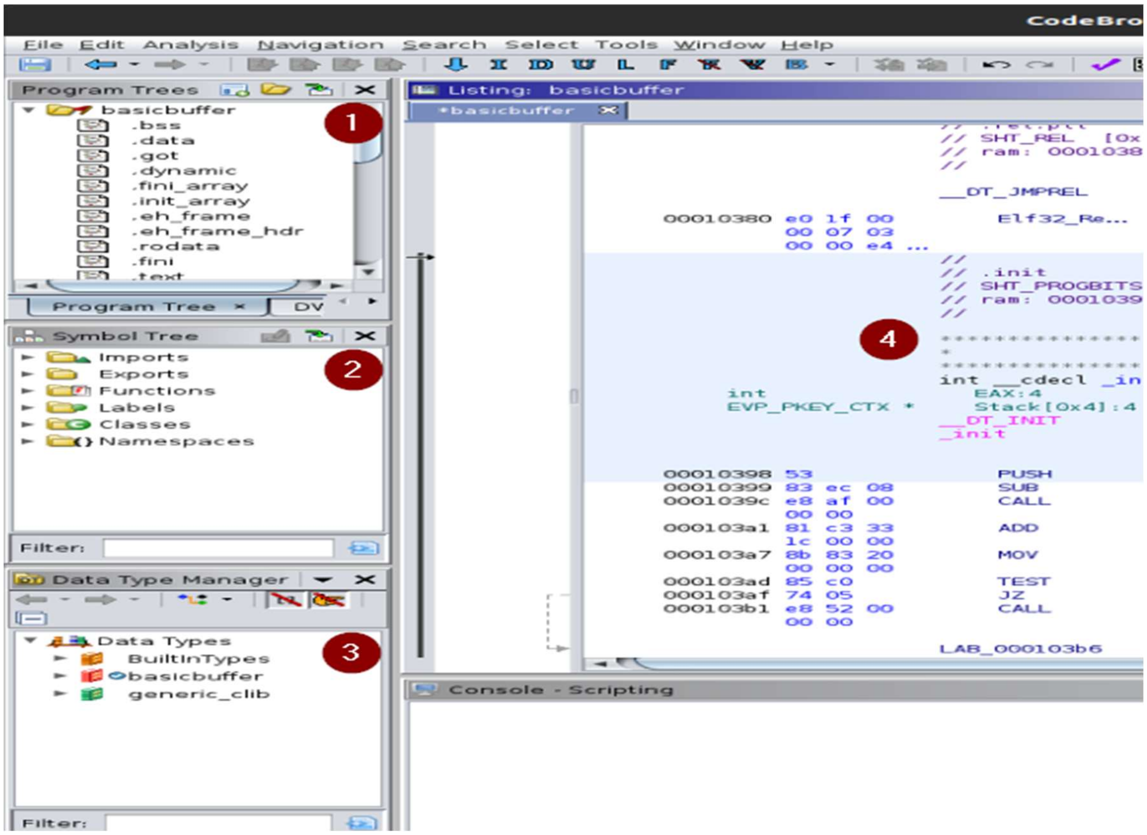
```
Creates parameter and local variables for a
Function using Decompiler.
WARNING: This can take a SIGNIFICANT Amount of
```

Options

Analysis Clear Level	ANALYSIS
Analysis Decompiler Timeout (sec)	60
Commit Data Types	☑
Commit Void Return Values	□

Ghidra will analyze the file and present you with a new interface to interact with it.

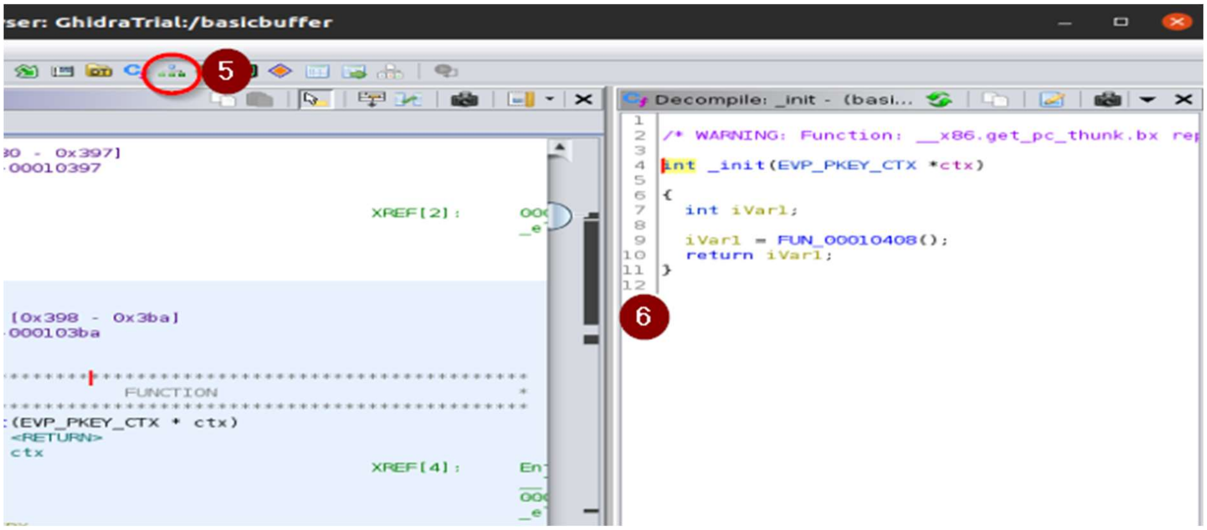
1. Program Trees
2. Symbol Tree
3. Data Type Manager
4. Display for analyzed code
5. Function Graphs
6. Decompiler



```
                                            //  SHT_REL    [0x
                                            //  ram:  0001038
                                            //
                                            __DT_JMPREL
      00010380 e0 1f 00                         Elf32_Re...
               00 07 03
               00 00 e4 ...
                                            //
                                            //  .init
                                            //  SHT_PROGBITS
                                            //  ram:  0001039
                                            //
                                            ****************
                                            *
                                            ****************
                                            int __cdecl _in
               int                             EAX:4
               EVP_PKEY_CTX *                  Stack[0x4]:4
                                            __DT_INIT
                                            _init

      00010398 53                               PUSH
      00010399 83 ec 08                         SUB
      0001039c e8 af 00                         CALL
               00 00
      000103a1 81 c3 33                         ADD
               1c 00 00
      000103a7 8b 83 20                         MOV
               00 00 00
      000103ad 85 c0                            TEST
      000103af 74 05                            JZ
      000103b1 e8 52 00                         CALL
               00 00

                                            LAB_000103b6
```



```
30 - 0x397]
00010397

[0x398 - 0x3ba]
000103ba

:(EVP_PKEY_CTX * ctx)
<RETURN>
ctx
```

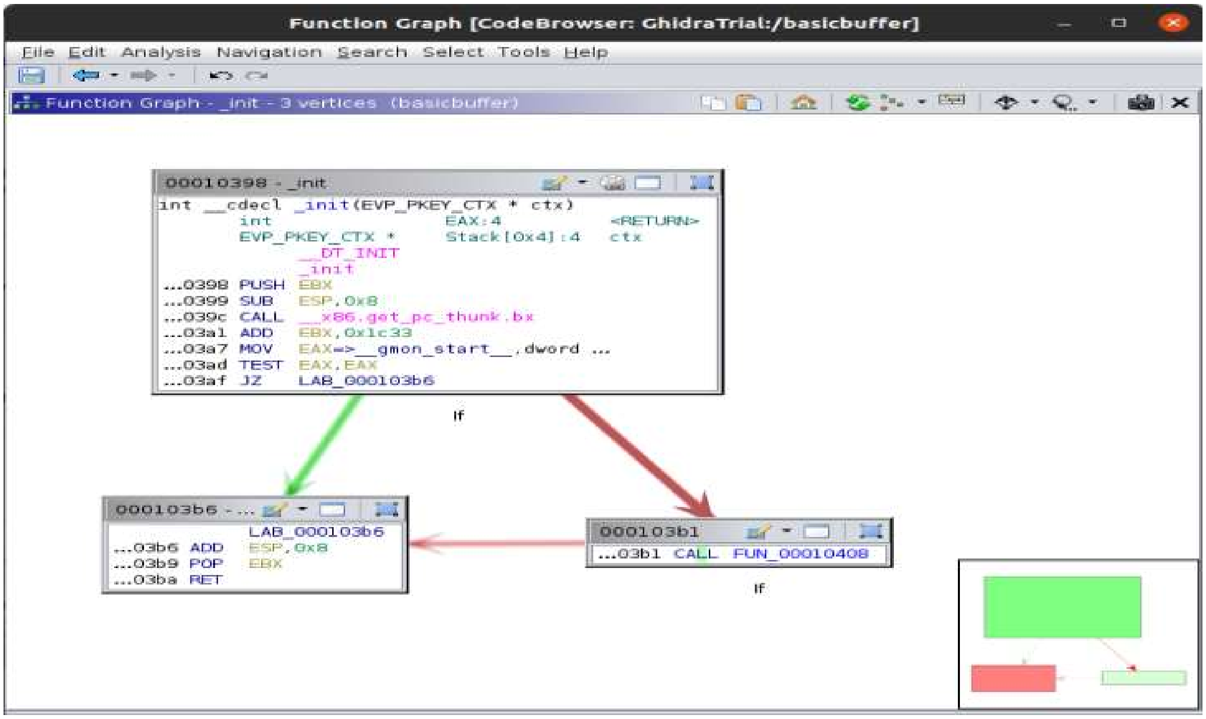
```
/* WARNING: Function: __x86.get_pc_thunk.bx rep

int _init(EVP_PKEY_CTX *ctx)

{
  int iVar1;

  iVar1 = FUN_00010408();
  return iVar1;
}
```

In order to use the function graph (5), scroll down in the display (4) until you see the word **FUNCTION**, and click on it. This will bring up the decompiled code in the decompiler (6), at which point you can click on the function graph button (5). The resulting window, shown below, shows how functions are related to each other, and how they interact.


Function Graph [CodeBrowser: GhidraTrial:/basicbuffer]
File Edit Analysis Navigation Search Select Tools Help
Function Graph - _init - 3 vertices (basicbuffer)
00010398 - _init
000103b6 - ...
000103b1
If
If

```
int __cdecl _init(EVP_PKEY_CTX * ctx)
        int              EAX:4          <RETURN>
        EVP_PKEY_CTX *   Stack[0x4]:4   ctx
              __DT_INIT
              _init
...0398 PUSH  EBX
...0399 SUB   ESP,0x8
...039c CALL  __x86.get_pc_thunk.bx
...03a1 ADD   EBX,0x1c33
...03a7 MOV   EAX=>__gmon_start__,dword ...
...03ad TEST  EAX,EAX
...03af JZ    LAB_000103b6
```

```
              LAB_000103b6
...03b6 ADD   ESP,0x8
...03b9 POP   EBX
...03ba RET
```

```
...03b1 CALL  FUN_00010408
```

References

Messner, T. (2019, May 11). *Ghidra Tutorial 1: Installing Ghidra on linux*. Retrieved August 25, 2020, from YouTube: https://youtu.be/OJlKtRgC68U

Messner, T. (2019, May 13). *Ghidra Tutorial 2: Solving a very simple crackme*. Retrieved August 25, 2020, from YouTube: https://youtu.be/yQTMvtutsjY

National Security Agency. (2020, April 04). *Ghidra Installation Guide*. Retrieved August 25, 2020, from Ghidra SRE: https://ghidra-sre.org/InstallationGuide.html

Oracle. (2020, July 14). *Java SE Downloads*. Retrieved August 25, 2020, from Oracle: https://www.oracle.com/java/technologies/javase-downloads.html