1)Installation steps for Ghidra:

Move the ghidra zip file to the /opt/ directory

```
sudo mv ghidra_11.4_PUBLIC_20250620.zip /opt/
```

Here you can unzip the file and then remove the zip version

```
cd /opt/
sudo unzip ghidra_11.4_PUBLIC_20250620.zip
sudo rm -r ghidra_11.4_PUBLIC_20250620.zip
```

Then rename the the unzipped directory to ghidra

```
sudo mv ghidra_11.4_PUBLIC/ ghidra
```

Now cd into the ghidra directory

```
 cd ghidra/
```

Try running ghidra

```
 sudo ./ghidraRun
```

2)Executing Python script:

```
./analyze_firmware.py Flash_1.03/loader.bin
```

What This Script Detects

Check	What It Means	Output
Debug Symbols	If names like `main`, `printf` are present	`stripped` or `not stripped`
High Entropy	Encrypted/compressed data	Lists suspicious memory addresses
Control Flow	Obfuscated dispatchers or switch cases	Reports complex blocks

Feature	Description
🔎 Suspicious Function Detection	Lists functions with generic names like `FUN_1234` or `sub_4567`
🔐 XOR Operation Scan	Finds functions that contain XOR instructions
📌 Ghidra Bookmarks	Adds bookmarks to high-entropy areas, unnamed functions, and XOR-heavy functions
📝 Output File	Saves report to the same folder as the script file

Feature	Description
🔍 AES Constant Detection	Scans for AES S-box
🔄 XOR Loop Scan	Flags functions using `xor` (often obfuscators/decryptors)
📁 JSON Report	Machine-readable structured output
📊 CSV Report	Easy to open in Excel/sheets
📌 Ghidra Bookmarks	Add visual markers inside the disassembly

To run the Python (Jython) script in Ghidra, follow these simple steps:

✅ Prerequisites
Make sure you've already opened a project and imported a firmware binary in Ghidra.

Ghidra uses Jython, so the script is written in Python 2-style syntax and runs in Ghidra's Script Manager.

🧰 Steps to Run the Script
1. Open Ghidra and load your firmware project
Start Ghidra.

Open your project.

Import the firmware binary and analyze it (you can accept default options for most cases).

2. Open Script Manager
Go to Window → Script Manager
(or press Shift + F3)

3. Create a New Python Script
In the Script Manager, click File → New...

Choose Python as the language.

Name it something like firmware_analysis.py.

Click OK — this will open the script in Ghidra’s built-in editor.

4. Paste the Script Code
Delete any default code.

Paste the full script I gave you (or your version with enhancements).

Save the file (Ctrl+S or click the disk icon).

5. Run the Script
In the Script Manager, find your script in the list.

Click it and press the green play/run button (triangle).

The script will:

Analyze symbols

Search for XOR and crypto patterns

Identify high-entropy regions

Save a JSON and CSV report

Add bookmarks to Ghidra views

6. View the Output
Console output: Bottom panel in Ghidra will show logs.

Bookmarks: Use Window → Bookmarks to jump to flagged areas.

Output files: JSON and CSV reports are saved in the same folder as your script (check the path in the console log).

Optional: Verify Python Support is Installed

If you **don't see "Python" at all** in the language list:

1. Go to `Help → About Ghidra → Installed Extensions`
2. Ensure **"Python" or "Jython Scripting"** is installed
3. If not installed:
   - Go to `File → Install Extensions`
   - Check **"Python" or "Jython support"**
   - Click **Next** → **Finish**
   - Restart Ghidra