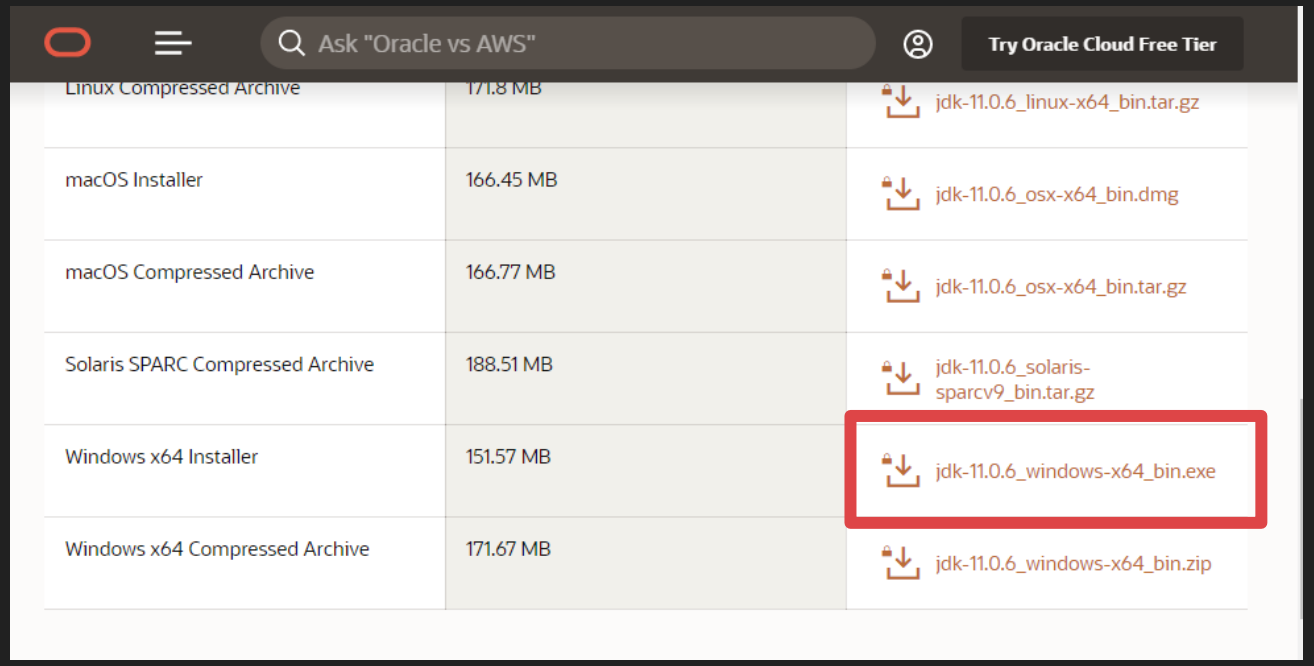
Ghidra Tutorial

0856069 Weichun, Lin

Installation: Java

- Download Java environment from following link (An Oracle account required) : https://www.oracle.com/java/technologies/javase-jdk11-downloads.html

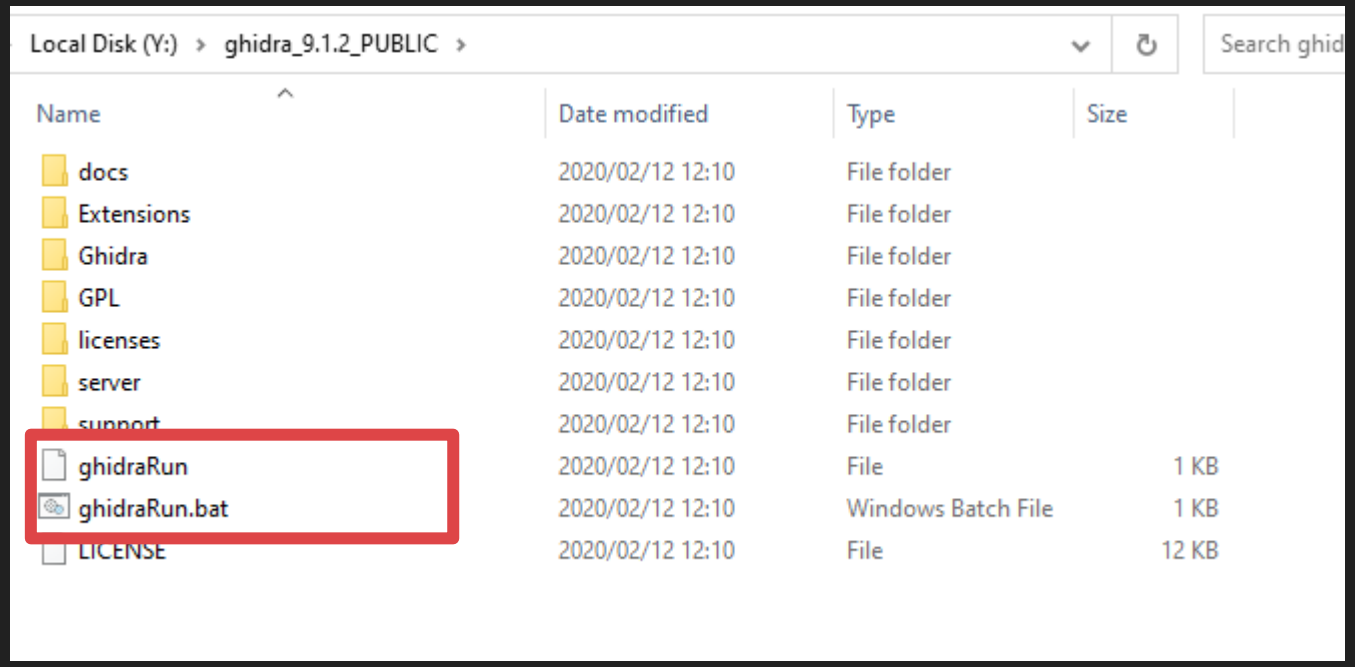


Download and extract Ghidra

- Download Ghidra from following link: https://ghidra-sre.org/

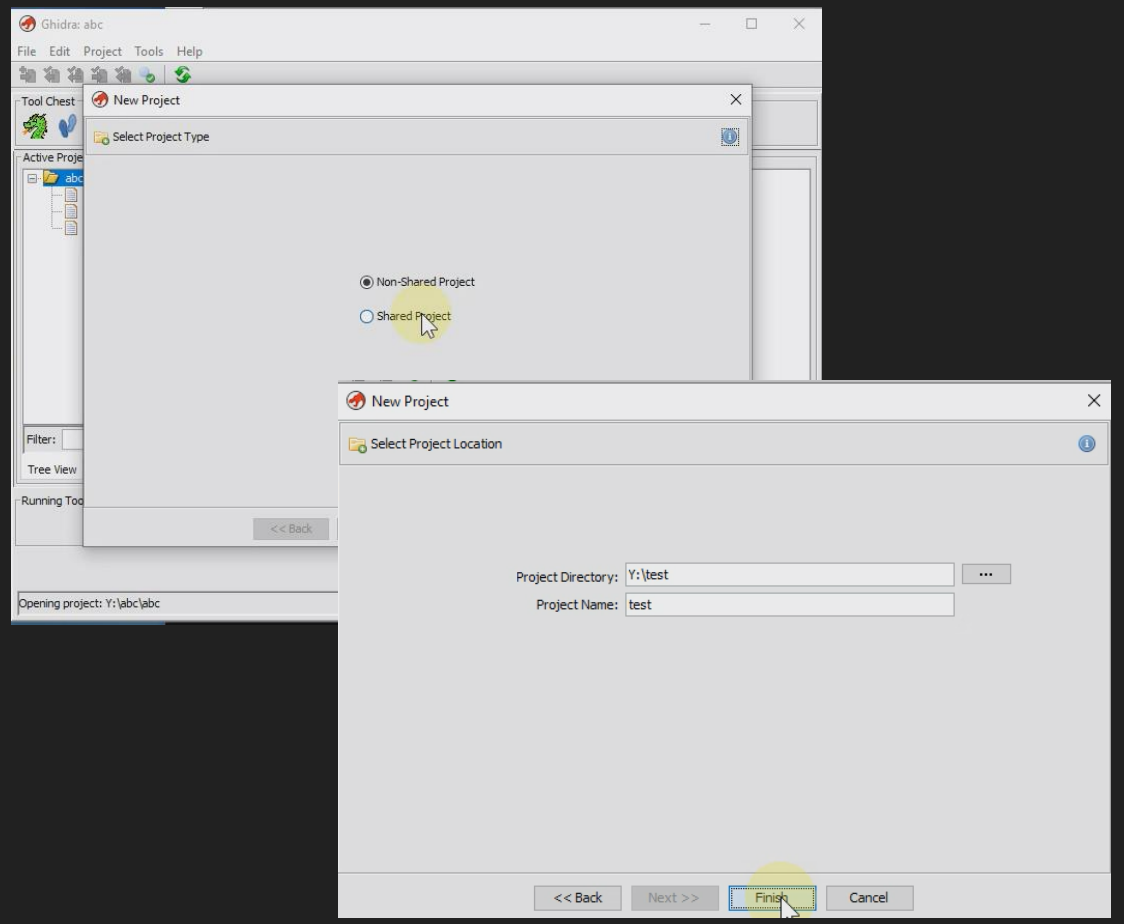
Download and extract Ghidra

- Unzip it and run ghidraRun.bat



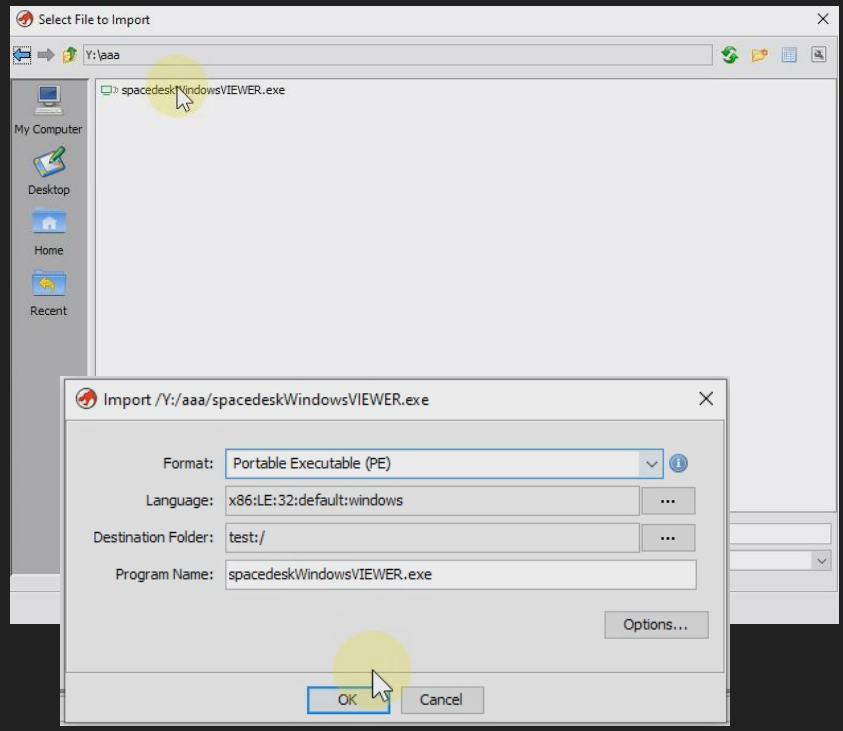
Create New Project

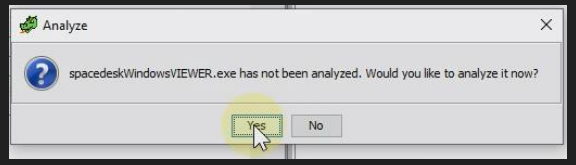
- [File]/[New Project]
- Select [Non–shared project]
- Enter Project directory and name (ensure directory for project exists)
- [Finish]

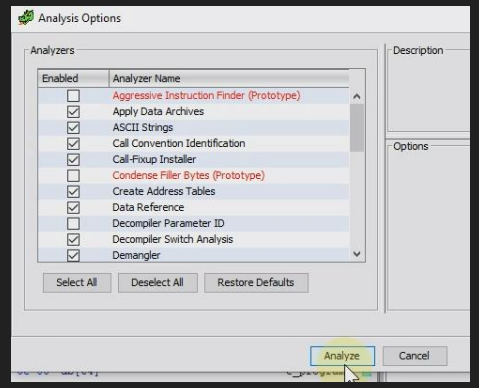


Import executable file

- [File]/[Import File]
- Select file that you want to analysis.
- Click [OK]
- On [Analyze] dialog, click [Yes] and [Analyze]
- Wait a moment until analysis done, progress can check by right–bottom of window.

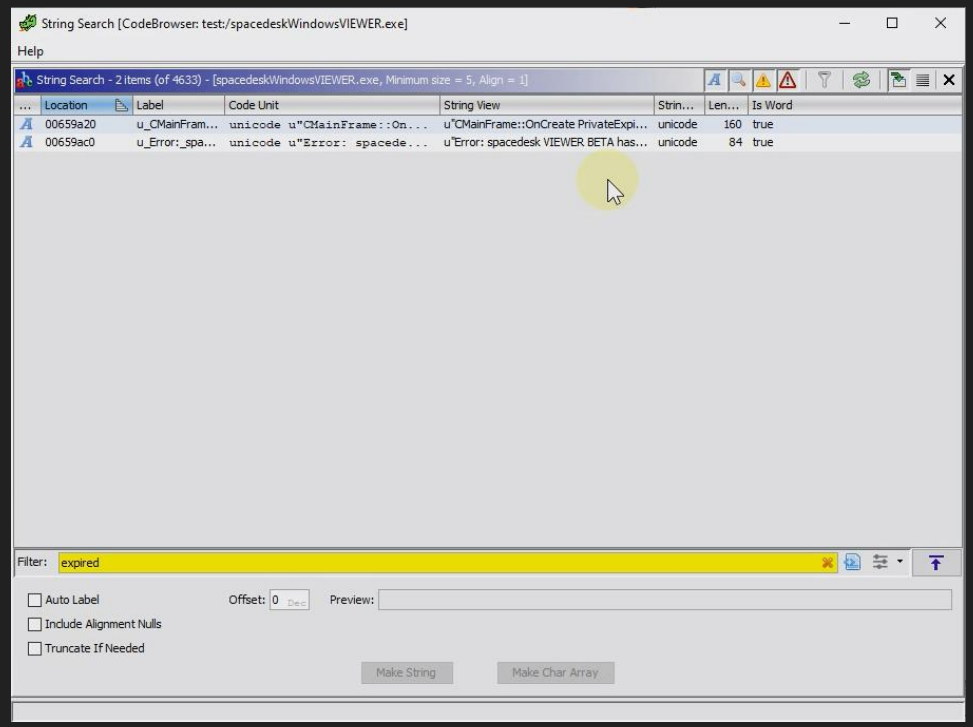






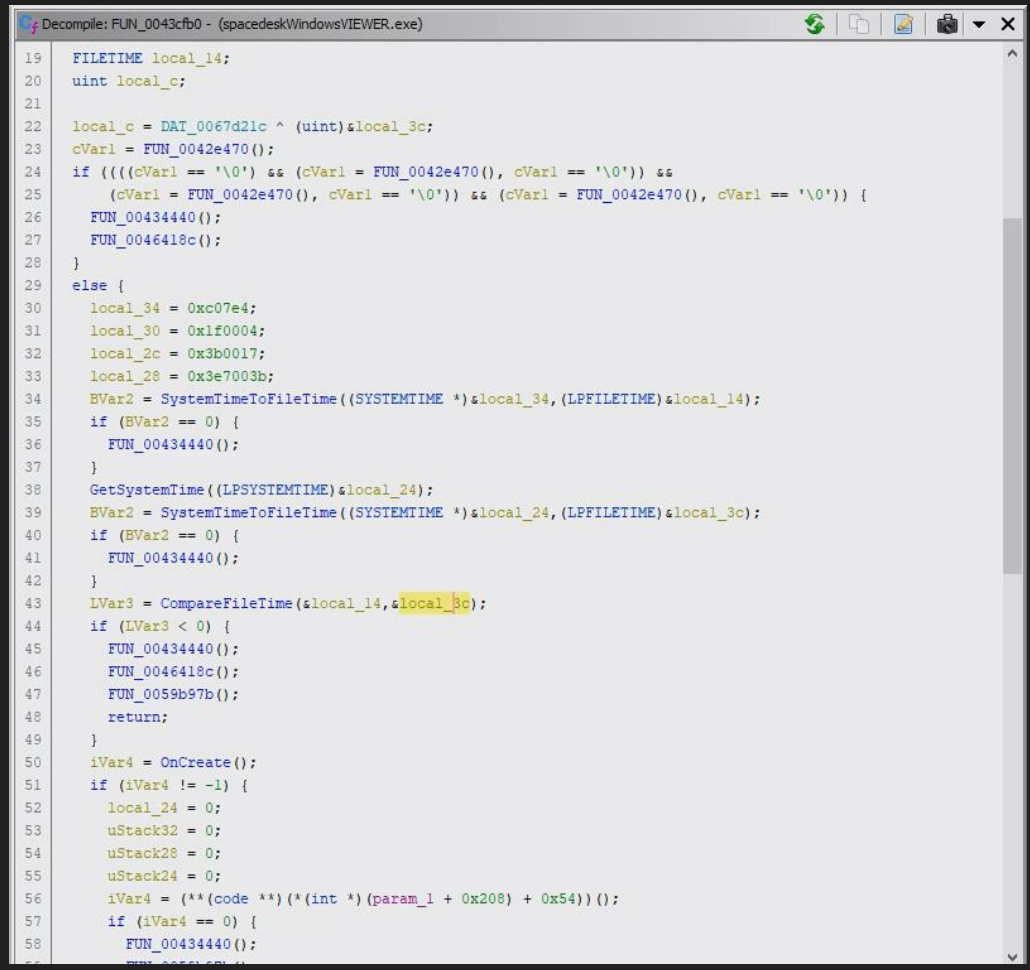
Find string reference

- We can find string reference by [Search]/[For Strings]
- Double click on row can go to string location.



Decompile

- After we go to referenced function, Decompile window will show this function in C.
- As we see in right panel, local_34 is a specified date, local_14 is FILETIME converted from local_34, and local_24 is current time, local_3c is FILETIME converted from local_24.



Decompile

- LVar3 is result of compare local_14 and local_3c.
- If local_14 is less than local_3c, that is after specified date, this program will show expired dialog and no longer to use.