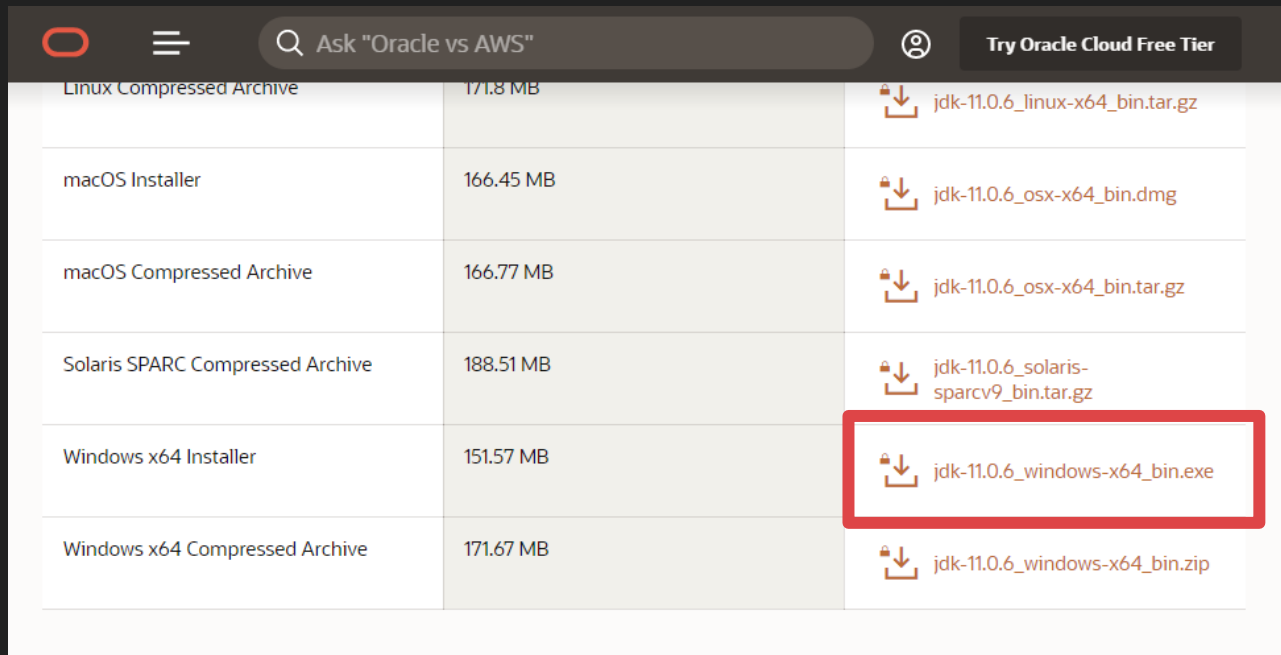








Ghidra Tutorial

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>



Linux Compressed Archive	171.8 MB	 jdk-11.0.6_linux-x64_bin.tar.gz
macOS Installer	166.45 MB	 jdk-11.0.6_osx-x64_bin.dmg
macOS Compressed Archive	166.77 MB	 jdk-11.0.6_osx-x64_bin.tar.gz
Solaris SPARC Compressed Archive	188.51 MB	 jdk-11.0.6_solaris-sparcv9_bin.tar.gz
Windows x64 Installer	151.57 MB	 jdk-11.0.6_windows-x64_bin.exe
Windows x64 Compressed Archive	171.67 MB	 jdk-11.0.6_windows-x64_bin.zip

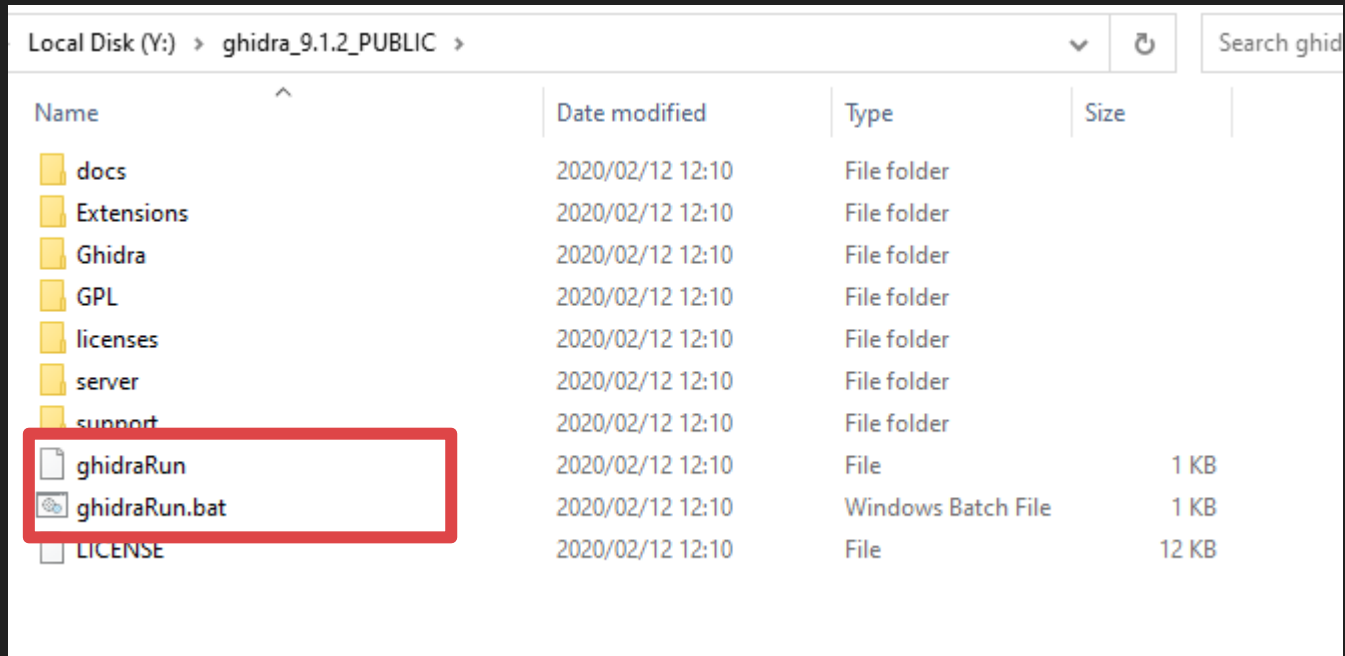
Download and extract Ghidra

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



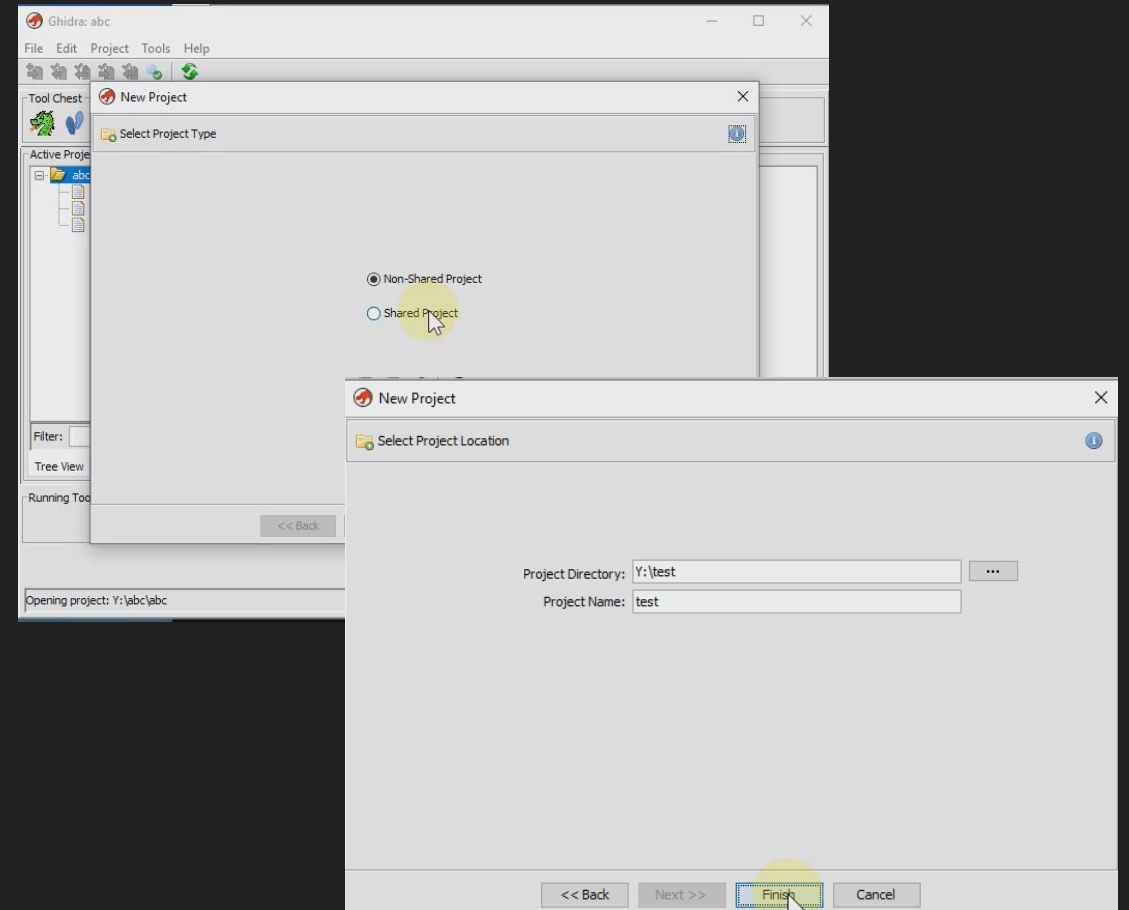
Download and extract Ghidra

- Unzip it and run ghidraRun.bat



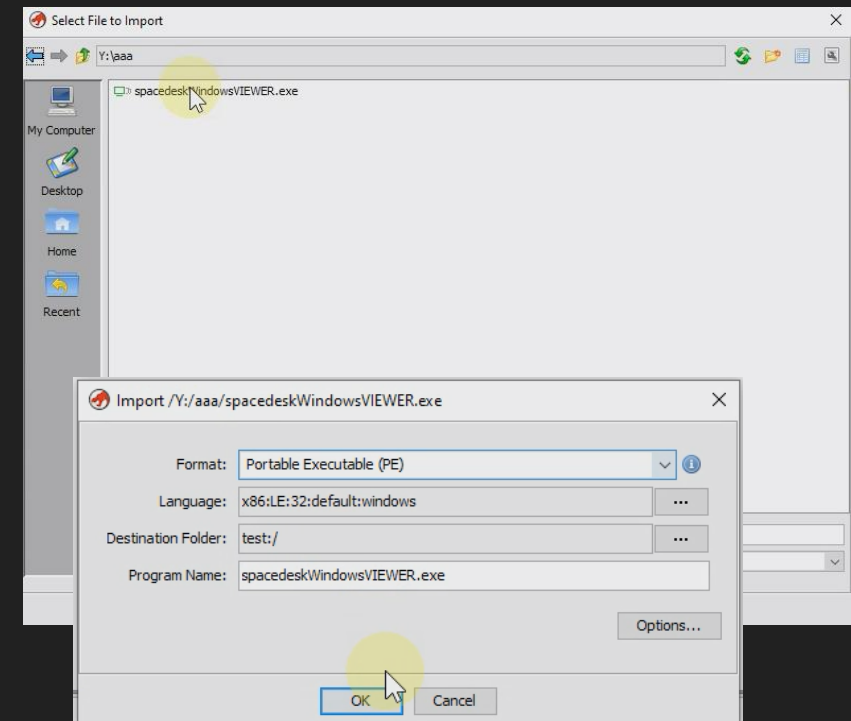
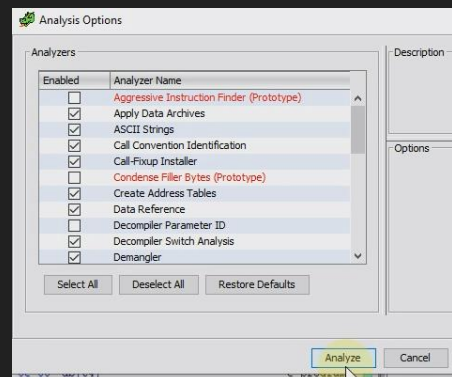
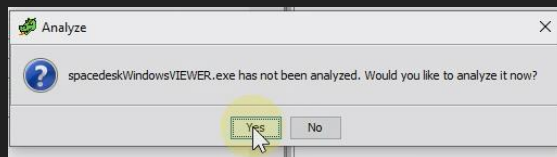
Create New Project

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



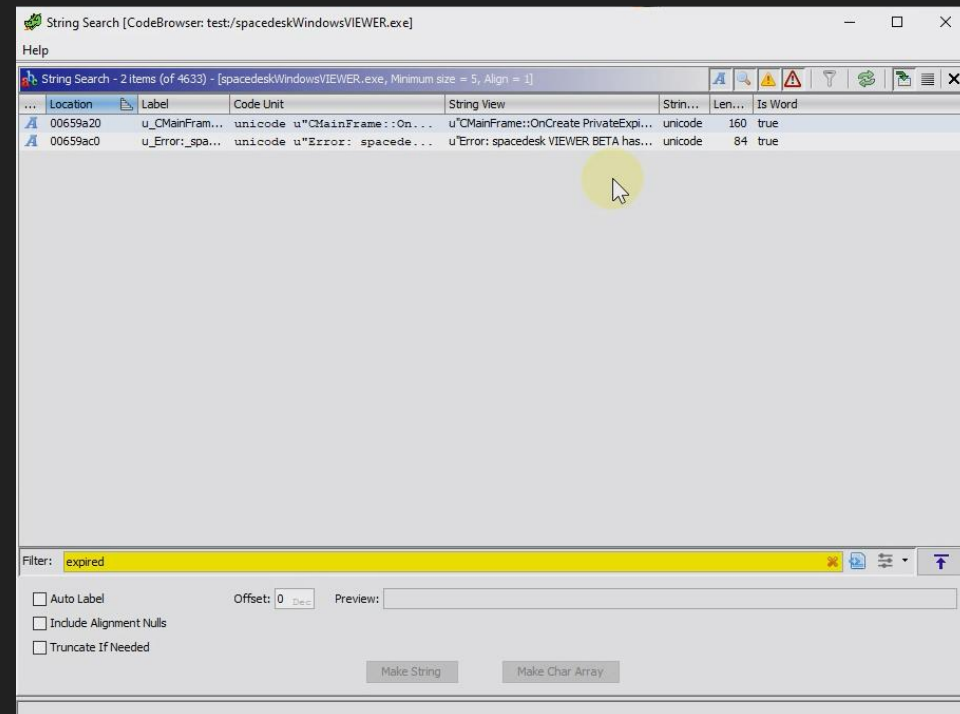
Import executable file

- [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.



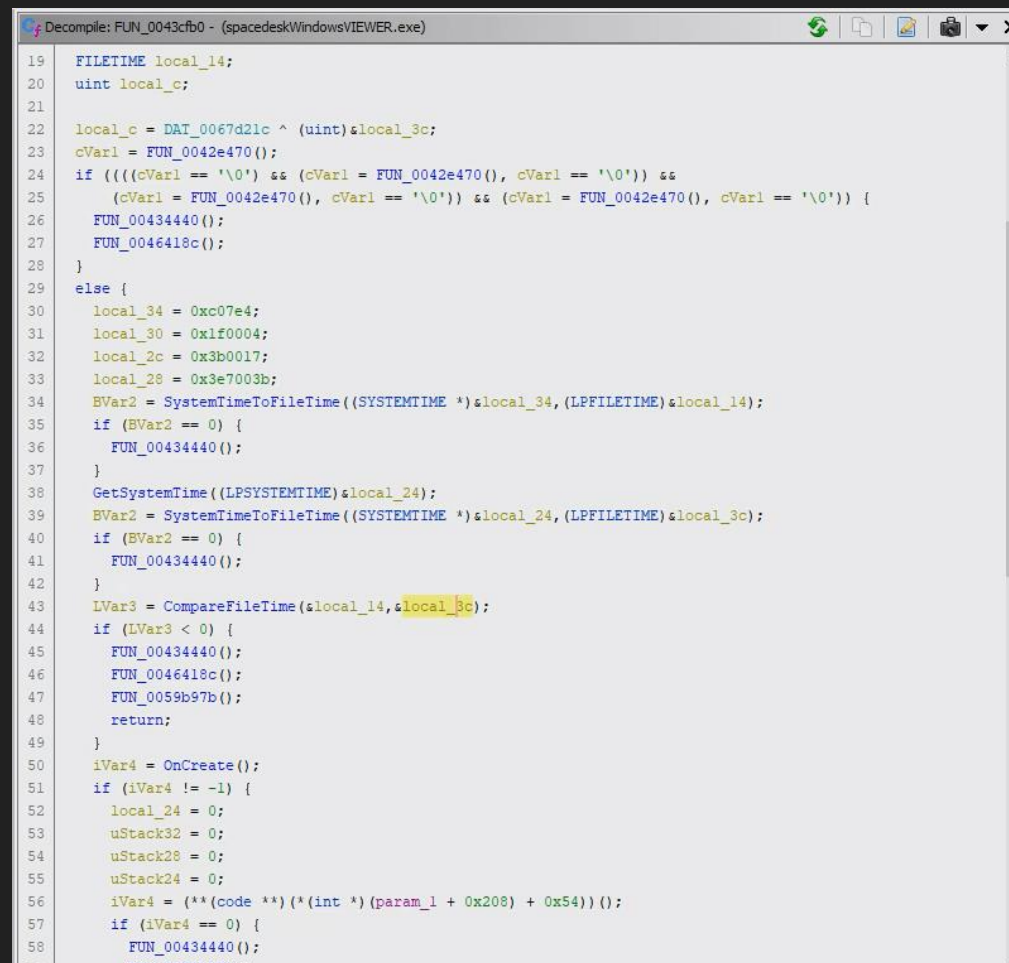
Find string reference

- 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: FUN_00434440 - (spacedeskWindowsVIEWER.exe)
19 FILETIME local_14;
20 uint local_c;
21
22 local_c = DAT_0067d21c ^ (uint)&local_3c;
23 cVar1 = FUN_0042e470();
24 if (((cVar1 == '\0') && (cVar1 = FUN_0042e470(), cVar1 == '\0')) &&
25     (cVar1 = FUN_0042e470(), cVar1 == '\0')) && (cVar1 = FUN_0042e470(), cVar1 == '\0')) {
26     FUN_00434440();
27     FUN_0046418c();
28 }
29 else {
30     local_34 = 0xc07e4;
31     local_30 = 0x1f0004;
32     local_2c = 0x3b0017;
33     local_28 = 0x3e7003b;
34     BVar2 = SystemTimeToFileTime((SYSTEMTIME *)&local_34, (LPFILETIME)&local_14);
35     if (BVar2 == 0) {
36         FUN_00434440();
37     }
38     GetSystemTime((LPSYSTEMTIME)&local_24);
39     BVar2 = SystemTimeToFileTime((SYSTEMTIME *)&local_24, (LPFILETIME)&local_3c);
40     if (BVar2 == 0) {
41         FUN_00434440();
42     }
43     LVar3 = CompareFileTime(&local_14, &local_3c);
44     if (LVar3 < 0) {
45         FUN_00434440();
46         FUN_0046418c();
47         FUN_0059b97b();
48         return;
49     }
50     iVar4 = OnCreate();
51     if (iVar4 != -1) {
52         local_24 = 0;
53         uStack32 = 0;
54         uStack28 = 0;
55         uStack24 = 0;
56         iVar4 = (*(code *) *)(int *)(param_1 + 0x208) + 0x54;
57         if (iVar4 == 0) {
58             FUN_00434440();
59             FUN_0046418c();
60         }
61     }
62 }
```


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.

```
Decompile: FUN_0043cfb0 - (spacedeskWindowsVIEWER.exe)
19 FILETIME local_14;
20 uint local_c;
21
22 local_c = DAT_0067d21c ^ (uint)&local_3c;
23 cVar1 = FUN_0042e470();
24 if (((cVar1 == '\0') && (cVar1 = FUN_0042e470(), cVar1 == '\0')) &&
25     (cVar1 = FUN_0042e470(), cVar1 == '\0')) && (cVar1 = FUN_0042e470(), cVar1 == '\0')) {
26     FUN_00434440();
27     FUN_0046418c();
28 }
29 else {
30     local_34 = 0xc07e4;
31     local_30 = 0x1f0004;
32     local_2c = 0x3b0017;
33     local_28 = 0x3e7003b;
34     BVar2 = SystemTimeToFileTime((SYSTEMTIME *)&local_34, (LPFILETIME)&local_14);
35     if (BVar2 == 0) {
36         FUN_00434440();
37     }
38     GetSystemTime((LPSYSTEMTIME)&local_24);
39     BVar2 = SystemTimeToFileTime((SYSTEMTIME *)&local_24, (LPFILETIME)&local_3c);
40     if (BVar2 == 0) {
41         FUN_00434440();
42     }
43     LVar3 = CompareFileTime(&local_14, &local_3c);
44     if (LVar3 < 0) {
45         FUN_00434440();
46         FUN_0046418c();
47         FUN_0059b97b();
48         return;
49     }
50     iVar4 = OnCreate();
51     if (iVar4 != -1) {
52         local_24 = 0;
53         uStack32 = 0;
54         uStack28 = 0;
55         uStack24 = 0;
56         iVar4 = (**(code **))(*(int *) (param_1 + 0x208) + 0x54)();
57         if (iVar4 == 0) {
58             FUN_00434440();
59             FUN_0059b97b();
60         }
61     }
62 }
```