

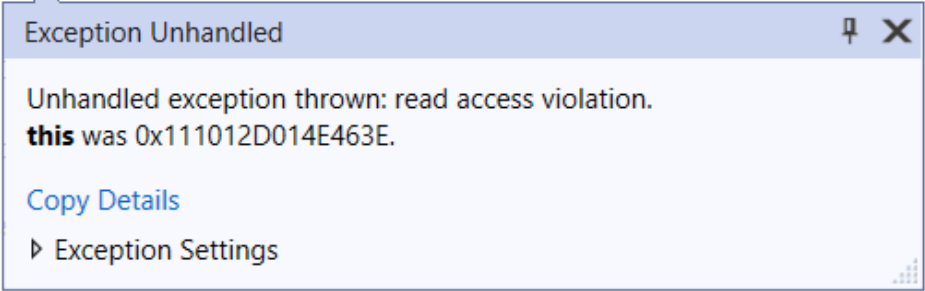
C:\Users\user\apps\dn-wine\Dn-FamiTracker_v0500_x64_Release but analyze on Windows.

The screenshot displays the Visual Studio IDE with a C++ source file open. The code defines a template class `_Invoker1` and a function `invoke`. An unhandled exception dialog box is overlaid on the code, reporting a 'read access violation' on the variable `this` at memory address `0x111012D014E463E`. The call stack on the right shows the following sequence of calls:

- Dn-FamiTracker.exe!CPatternData::GetFramePattern(unsigned int Frame, unsigned int * pFrameData) C++
- Dn-FamiTracker.exe!CFamiTrackerDoc::GetNoteData(unsigned int Track, unsigned int * pNoteData) C++
- Dn-FamiTracker.exe!CFamiTrackerDoc::RetrieveSoundState(unsigned int Track, unsigned int * pSoundState) C++
- Dn-FamiTracker.exe!CSoundGen::ApplyGlobalState() Line 1380 C++
- Dn-FamiTracker.exe!CSoundGen::BeginPlayer(play_mode_t Mode, int Track) Line 1380 C++
- [Inline Frame] Dn-FamiTracker.exe!CSoundGen::OnStartPlayer(unsigned __int64 * pSoundState) Line 1380 C++
- Dn-FamiTracker.exe!CSoundGen::DispatchGuiMessage(GuiMessage msg) Line 94 C++
- Dn-FamiTracker.exe!CSoundGen::ThreadEntry() Line 774 C++
- [Inline Frame] Dn-FamiTracker.exe!CSoundGen::BeginThread::_J2:<lambda_65...> C++
- [Inline Frame] Dn-FamiTracker.exe!std::invoke(CSoundGen::BeginThread::_J2:<lambda_65...>, std::tuple<...>) C++
- Dn-FamiTracker.exe!std::thread::_Invoke<std::tuple<...>, <lambda_65ec325f4822cc3...>> C++
- Dn-FamiTracker.exe!thread_start<unsigned int (&cdecl*)(void *),1>(void * cons... C++
- [Frames may be missing, no binary loaded for kernel32.dll]
- kernel32.dll!000000007b627da9() Un...

the sinking feeling when you look at a crash dump and see the code you wrote

```
756 void CSoundGen::ThreadEntry()  
757 {  
758     m_audioThreadID = std::this_thread::get_id();  
759  
760     if (!InitInstance()) {  
761         ExitInstance();  
762         return;  
763     }  
764     while (true) {  
765         while (auto pMessage = m_MessageQueue.front()) {  
766             GuiMessage message = *pMessage;  
767             m_MessageQueue.pop();  
768             if (message.message == WM_QUIT) {  
769                 goto end_while;  
770             }  
771             if (!DispatchGuiMessage(message)) {  
772                 goto end_while;  
773             }  
774         }  
775     }  
776     // On  
777 }  
778 end_wh  
779 ExitIn  
780  
781  
782 }  
783
```



ghidra v1

Error Loading PDB

Error processing PDB file: C:\Users\user\apps\dn-wine\Dn-FamiTracker_v0500_x64_Release\Dn-FamiTracker.pdb
 Index 24 out of bounds for length 9

```

java.lang.reflect.InvocationTargetException
    at ghidra.app.plugin.core.analysis.AutoAnalysisManager$AnalysisWorkerCommand.applyTo(AutoAnalysisManager.java:1706)
    at ghidra.app.plugin.core.analysis.AutoAnalysisManager$AnalysisTaskWrapper.run(AutoAnalysisManager.java:688)
    at ghidra.app.plugin.core.analysis.AutoAnalysisManager.startAnalysis(AutoAnalysisManager.java:788)
    at ghidra.app.plugin.core.analysis.AutoAnalysisManager.startAnalysis(AutoAnalysisManager.java:667)
    at ghidra.app.plugin.core.analysis.AutoAnalysisManager.startAnalysis(AutoAnalysisManager.java:632)
    at ghidra.app.plugin.core.analysis.AnalysisBackgroundCommand.applyTo(AnalysisBackgroundCommand.java:58)
    at ghidra.framework.plugintool.mgr.BackgroundCommandTask.run(BackgroundCommandTask.java:102)
    at ghidra.framework.plugintool.mgr.ToolTaskManager.run(ToolTaskManager.java:336)
    at java.base/java.lang.Thread.run(Thread.java:833)
Caused by: java.lang.IndexOutOfBoundsException: Index 24 out of bounds for length 9
    at java.base/jdk.internal.util.Preconditions.outOfBounds(Preconditions.java:64)
    at java.base/jdk.internal.util.Preconditions.outOfBoundsCheckIndex(Preconditions.java:70)
    at java.base/jdk.internal.util.Preconditions.checkIndex(Preconditions.java:266)
    at java.base/java.util.Objects.checkIndex(Objects.java:359)
    at ghidra.util.LittleEndianDataConverter.getValue(LittleEndianDataConverter.java:72)
    at ghidra.util.DataConverter.getValue(DataConverter.java:128)
    at ghidra.program.model.data.PointerDataType.getStoredOffset(PointerDataType.java:557)
    at ghidra.program.model.data.PointerDataType.getAddressValue(PointerDataType.java:405)
    at ghidra.program.model.data.PointerDataType.getAddressValue(PointerDataType.java:368)
    at ghidra.program.database.data.PointerDB.getValue(PointerDB.java:243)
    at ghidra.program.database.code.DataDB.getValue(DataDB.java:693)
    at ghidra.program.database.code.CodeManager.addDataReferences(CodeManager.java:2058)
    at ghidra.program.database.code.CodeManager.addDataReferences(CodeManager.java:2073)
    at ghidra.program.database.code.CodeManager.addDataReferences(CodeManager.java:2073)
    at ghidra.program.database.code.CodeManager.createCodeUnit(CodeManager.java:2010)
    at ghidra.program.database.ListingDB.createData(ListingDB.java:283)
    at ghidra.app.util.pdb.pdbapplicator.DataSymbolApplier.createData(DataSymbolApplier.java:180)
    at ghidra.app.util.pdb.pdbapplicator.DataSymbolApplier.createData(DataSymbolApplier.java:124)
    at ghidra.app.util.pdb.pdbapplicator.DataSymbolApplier.createData(DataSymbolApplier.java:94)
    at ghidra.app.util.pdb.pdbapplicator.DataSymbolApplier.apply(DataSymbolApplier.java:77)
    at ghidra.app.util.pdb.pdbapplicator.DefaultPdbApplicator.procSym(DefaultPdbApplicator.java:1465)
    at ghidra.app.util.pdb.pdbapplicator.DefaultPdbApplicator.processGlobalSymbolsNoTypedefs(DefaultPdbApplicator.java:1190)
    at ghidra.app.util.pdb.pdbapplicator.DefaultPdbApplicator.processSymbols(DefaultPdbApplicator.java:305)
    at ghidra.app.util.pdb.pdbapplicator.DefaultPdbApplicator.applyTo(DefaultPdbApplicator.java:208)
    at pdb.LoadPdbTask.parseWithNewParser(LoadPdbTask.java:150)
    at pdb.LoadPdbTask$2.analysisWorkerCallback(LoadPdbTask.java:84)
    at ghidra.app.plugin.core.analysis.AutoAnalysisManager$AnalysisWorkerCommand.applyTo(AutoAnalysisManager.java:1700)
    ... 8 more
  
```

Build Date: 2022-Nov-15 1249 EST
 Ghidra Version: 10.2.2
 Java Home: C:\Program Files\Eclipse Adoptium\jdk-17.0.6.10-hotspot
 JVM Version: Eclipse Adoptium 17.0.6
 OS: Windows 10 10.0 amd64
 Workstation: WINDOWS-PC


#	Message	Time
1	Error processing PDB file: C:\Users\user\apps\dn-wine\Dn-...	Jan 23, 2023 02:55 PM

Filter:

OK

Load PDB File

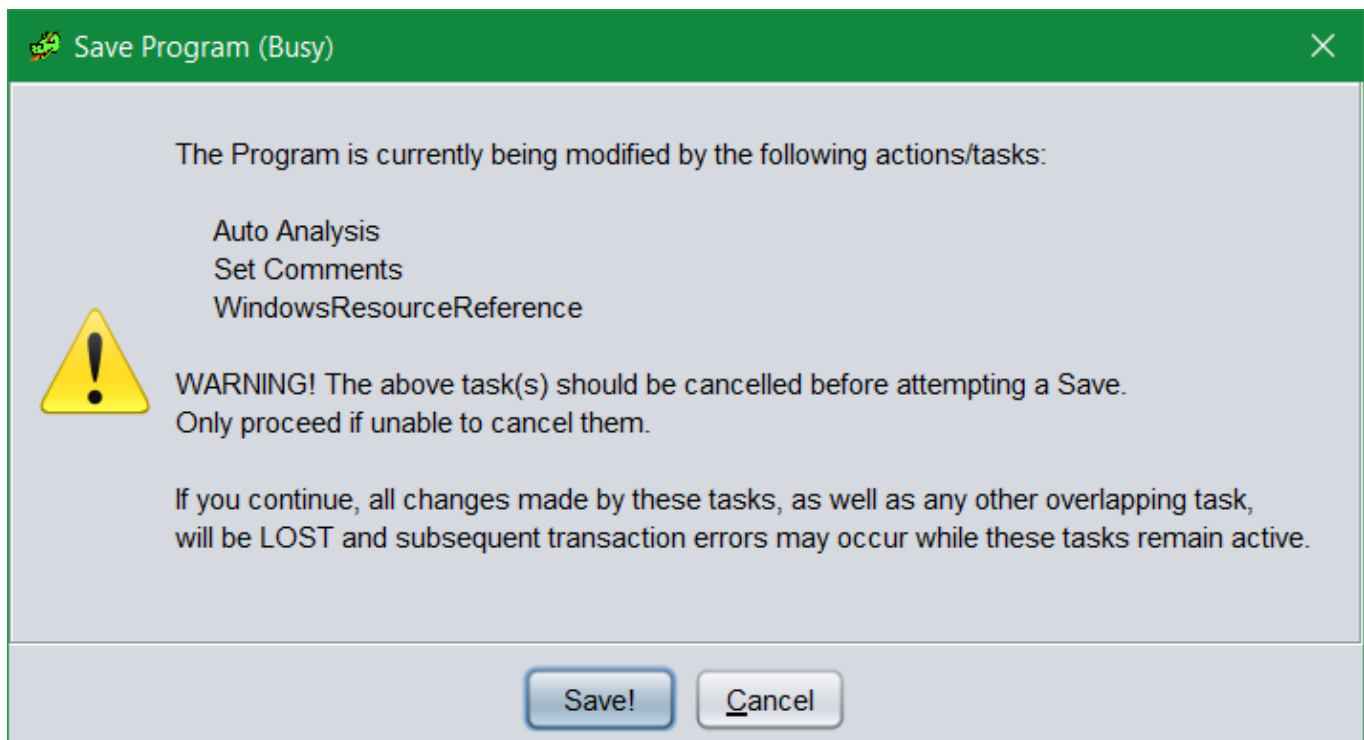
There were warnings/errors loading PDB file: C:\Users\user\apps\dn-wine\Dn-FamiTracker_v0500_x64_Release\Dn-FamiTracker.pdb

 PDB IO Error: Problem parsing or applying PDB information: Symbol list must contain at least one symbol name!

OK

universal "Public Symbols Only" seems to bypass the issue.

ghidra hangs on analysis. why?



turn off WindowsResourceReference i guess

...now importing the whole hog pdb works?! it fucks up decomp but adds type info, so reanalyze.

...still fucked up names!

reimport time.

v2 reimport

- in analysis, uncheck WindowsResourceReference, apply and cancel.
- import pdb, universal, symbols only
 - it starts decomp
 - TODO
- import pdb, universal, types only.
 - now there are two separate `CFamiTrackerDoc`, an empty one from the demangler followed by a populated one from the pdb parser?!

v3 types first

- in analysis, uncheck WindowsResourceReference, apply and cancel.
- import pdb, universal, types only
 - creates `CFamiTrackerDoc`.
- import pdb, universal, symbols only
 - decompiles `CFamiTrackerDoc::GetNoteData` using real `CFamiTrackerDoc` !!!

```
void __thiscall
CFamiTrackerDoc::GetNoteData
(CFamiTrackerDoc *this, uint Track, uint Frame, uint Channel, uint Row, stChanNote
```

```

*pData)

{
    int Pattern;
    stChanNote *p_Data;
    CPatternData *pTrack;

    pTrack = this->m_pTracks[Track];
    /// ^ ~pTrack is invalid!~~ or not? idk.

    Pattern = CPatternData::GetFramePattern(pTrack,Frame,Channel);
        uint __thiscall CPatternData::GetFramePattern(CPatternData *this,uint
Frame,uint Channel)

        {
            /* crash */
            return (uint)this->m_iFrameList[Frame][Channel];
        }
    p_Data = CPatternData::GetPatternData(pTrack,Channel,Pattern,Row);
    memmove(pData,p_Data,0xc);
    return;
}

```

we lose Track.

but the parent frame RetrieveSoundState has Track=0.

so why would track 0 have a corrupted m_pTracks?

or is it valid?! CFamiTrackerDoc::RetrieveSoundState has a similar this, and
CPatternData::GetFramePattern was passed frame 4 billion!

What Channel? `RAX=0000001C003D44E4 = Frame * 0x1c + RCX, RCX=00000000003D4500`, solve for Frame:

- $(0x0000001C003D44E4 - 0x00000000003D4500) / 0x1c$
- = 4294967295

Frame = (uint)-1 !!!

i'm a dumbass. What is Channel?

Channel=R8=4.

i have determined that famitracker has crashed trying to restore channel state as of frame `(unsigned)-1 = 0xffffffff`, on channel 4 (presumably it would crash on all channels and 4 is the first one restored)

```

void CSoundGen::BeginPlayer(play_mode_t Mode, int Track)
{

```

```

...
switch (Mode) { // optimized away!
case:
    m_iPlayFrame = m_pTrackerView->GetSelectedFrame();
    [unsigned int CFamiTrackerView::GetSelectedFrame() const]
    {
        return m_pPatternEditor->GetFrame();
        // **god save me, more data races... and the .dmp
        // didn't catch the other threads!**
        // can you convert coredumpctl into a pdb?
        [int CPatternEditor::GetFrame() const]
        {
            return m_cpCursorPos.m_iFrame; // // //
        }
    }
case MODE_PLAY_MARKER: // // // 050B
    m_iPlayFrame = m_pTrackerView->GetMarkerFrame();
    [int CFamiTrackerView::GetMarkerFrame() const] {
return CFamiTrackerView::m_iMarkerFrame; } // // // 050B
    }
    ...
    m_bPlaying = true;
    ...
    ApplyGlobalState();
    [void CSoundGen::ApplyGlobalState()] // // //
    {
        IsPlaying()
        [bool IsPlaying() const] { return m_bPlaying; };
        /// true, just set above.
        int Frame = ^ (=true) ? GetPlayerFrame() : ~m_pTrackerView-
>GetSelectedFrame()~~;
        [int CSoundGen::GetPlayerFrame() const]
        {
            return CSoundGen::m_iPlayFrame;
            /// = -1
        }
        Frame = -1
        /// BUG: Frame = -1!!!
    }
}

```

Who writes to CPatternEditor::m_cpCursorPos as CCursorPos? `::m_iFrame?

search m_cpCursorPos.m_iFrame . many readers.

not many pointers.

m_cpCursorPos\.m_iFrame *=[^=] ?

idk.

```
m_iMarkerFrame(-1), // // // suspicious
```

one possibility is playing from a "row marker (bookmark)" when there was none

ok i have a theory

i set and unset a row marker (ctrl+b) but it didn't disable static_cast<CFamiTrackerView*>(GetActiveView())->IsMarkerValid(), changed song options, then hit a shortcut by mistake to play from marker

or i played from marker, then changed song options, and it reset the marker and tried playing from the same spot

idk really

...but that is unlikely, i would never hit ctrl+f7 by mistake, and song properties doesn't erase row markers

...so the other theory i have involves multiple threads and unprotected sex data access

in other words, "give up trying"