When debugging a stack overflow, you want to focus on the repeating recursive part

devblogs.microsoft.com/oldnewthing/20090107-00

January 7, 2009

Raymond Chen

When your program breaks into the debugger with a stack overflow, you will get a ridiculously huge stack trace because your program has gone into some sort of recursive death. (This is not a statement of metaphysical certitude, but it is true with very high probability.) But the place where the program crashed is usually not interesting at all. Here's a sample stack trace. (Warning: Ridiculously long stack traces ahead because stack traces from stack overflows are always ridiculously long. Apologies to my blind readership.)

```
ntdll!RtlpAllocateHeap+0x394f2
ntdll!RtlAllocateHeap+0x151
ntdll!RtlFormatCurrentUserKeyPath+0xfa
ADVAPI32!BaseRegTranslateToUserClassKey+0xaf
ADVAPI32!BaseRegOpenClassKeyFromLocation+0xc0
ADVAPI32!BaseRegGetUserAndMachineClass+0x102
ADVAPI32!LocalBaseRegQueryValue+0xeb
ADVAPI32!RegQueryValueExW+0xef
SHLWAPI!_SHRegQueryValueW+0xfc
SHLWAPI!SHRegGetValueW+0xca
PROGRAM!GetPathFromRegistry+0x3d
PROGRAM!CPluginFinder::GetProviderDLL+0x79
PROGRAM!CPluginFinder::InitializeProvider+0x22
PROGRAM!CPluginFinder::Initialize+0xad
PROGRAM!LookupPluginInfo+0x49
PROGRAM!CPluginInfo::Create+0x1d4
PROGRAM!TList<CPluginInfo>::GetInfo+0x6d
PROGRAM!CPluginInfo::GetInfoTable+0x5d
PROGRAM!TList<CPluginInfo>::Enumerate+0x83
PROGRAM!CPluginRepository::GetGUID+0xc0
PROGRAM!CPrivateNodeInfo::GetPluginInfo+0xdf
PROGRAM!CPrivateNodeInfo::LoadPlugin+0x7a
PROGRAM!CPrivateNode::GetChild+0x2e3
PROGRAM!CPrivateNode::FindChild+0x2be
PROGRAM!CPrivateNode::FindItem+0x190
PROGRAM!CPrivateNode::FindChild+0x289
PROGRAM!CPrivateNode::FindItem+0x190
PROGRAM!CLocalNode::FindItem+0xca
PROGRAM!CCompoundTreeNode::FindItem+0x70
PROGRAM!CCompoundTreeNode::FindChild+0xaf
PROGRAM!CCompoundTreeNode::FindItem+0x55
PROGRAM!FindTreeItem+0x78
PROGRAM!CToolbarCommand::Initialize+0x6c
PROGRAM!CompoundMenu_InitMenu+0x1d2
PROGRAM!CItemMenu::InitMenu+0x4e0
PROGRAM!InvokeViaContextMenu+0xce
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102
PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
comctl32!CReBar::s_WndProc+0x4a
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
```

```
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102
PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
comctl32!CReBar::s_WndProc+0x4a
USER32!UserCallWinProcCheckWow+0x1ad
```

```
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102
PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
comctl32!CReBar::s_WndProc+0x4a
```

```
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102
PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
```

```
comctl32!CReBar::s_WndProc+0x4a
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102
PROGRAM!CToolbar::OnAction+0x97
```

If you go hunting through your defect tracking database trying to see whether this is a known issue or not, a search for the top functions on the stack is unlikely to find anything interesting. That's because stack overflows tend to happen at a random point in the recursion; each stack overflow looks superficially different from every other one even if they are the same stack overflow.

Suppose you're singing the song *Frère Jacques*, except that you sing each verse a few tones higher than the previous one. Eventually, you will reach the top of your singing range, and precisely where that happens depends on where your vocal limit lines up against the melody. In the melody, the first three notes are each a new "record high" (*i.e.*, the notes are higher than any other note sung so far), and new record highs appear in the three notes of the third measure, and a final record high in the second note of the fifth measure.

If the melody represented a program's stack usage, a stack overflow could possibly occur at any of those five locations in the program's execution. In other words, the same underlying runaway recursion (musically represented by an ever-higher rendition of the melody) can manifest itself in five different ways. The "recursion" in this analogy was rather quick, just eight bars before the loop repeated. In real life, the loop can be quite long, leading to dozens of potential points where the stack overflow can manifest itself.

If you are faced with a stack overflow, then, you want to ignore the top of the stack, since that's just focusing on the specific note that exceeded your vocal range. You really want to find the entire melody, since that's what's common to all the stack overflows with the same root cause.

To do this, look for the part of the stack trace that repeats itself. That's the pattern that is causing the problem, the *stack overflow melody*, you might say. (And if you do say it, everybody will look at you funny since it's just a dumb analogy I made up on the spot.) Let's take another look at that stack trace above.

```
ntdll!RtlpAllocateHeap+0x394f2
ntdll!RtlAllocateHeap+0x151
ntdll!RtlFormatCurrentUserKeyPath+0xfa
ADVAPI32!BaseRegTranslateToUserClassKey+0xaf
ADVAPI32!BaseRegOpenClassKeyFromLocation+0xc0
ADVAPI32!BaseRegGetUserAndMachineClass+0x102
ADVAPI32!LocalBaseRegQueryValue+0xeb
ADVAPI32!RegQueryValueExW+0xef
SHLWAPI!_SHRegQueryValueW+0xfc
SHLWAPI!SHRegGetValueW+0xca
PROGRAM!GetPathFromRegistry+0x3d
PROGRAM!CPluginFinder::GetProviderDLL+0x79
PROGRAM!CPluginFinder::InitializeProvider+0x22
PROGRAM!CPluginFinder::Initialize+0xad
PROGRAM!LookupPluginInfo+0x49
PROGRAM!CPluginInfo::Create+0x1d4
PROGRAM!TList<CPluginInfo>::GetInfo+0x6d
PROGRAM!CPluginInfo::GetInfoTable+0x5d
PROGRAM!TList<CPluginInfo>::Enumerate+0x83
PROGRAM!CPluginRepository::GetGUID+0xc0
PROGRAM!CPrivateNodeInfo::GetPluginInfo+0xdf
PROGRAM!CPrivateNodeInfo::LoadPlugin+0x7a
PROGRAM!CPrivateNode::GetChild+0x2e3
PROGRAM!CPrivateNode::FindChild+0x2be
PROGRAM!CPrivateNode::FindItem+0x190
PROGRAM!CPrivateNode::FindChild+0x289
PROGRAM!CPrivateNode::FindItem+0x190
PROGRAM!CLocalNode::FindItem+0xca
PROGRAM!CCompoundTreeNode::FindItem+0x70
PROGRAM!CCompoundTreeNode::FindChild+0xaf
PROGRAM!CCompoundTreeNode::FindItem+0x55
PROGRAM!FindTreeItem+0x78
PROGRAM!CToolbarCommand::Initialize+0x6c
PROGRAM!CompoundMenu_InitMenu+0x1d2
PROGRAM!CItemMenu::InitMenu+0x4e0
PROGRAM!InvokeViaContextMenu+0xce
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102

PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
comctl32!CReBar::s_WndProc+0x4a
USER32!UserCallWinProcCheckWow+0x1ad
```

```
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102

PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
```

```
comctl32!CReBar::s_WndProc+0x4a
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102

PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
```

```
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
comctl32!CReBar::s_WndProc+0x4a
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102

PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
```

```
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
comctl32!CReBar::s_WndProc+0x4a
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102

PROGRAM!CToolbar::OnAction+0x97
```

Once you get past the initial turmoil, the stack trace settles down into a nice repeating pattern consisting of the same 53 functions over and over again. Identifying the start of the repeating pattern isn't important, because the starting point will be different for each crash, in the same way that the precise note which exceeds your singing range varies from crash to crash. When I go looking for the repeating pattern, I ignore the first hundred or so functions in the stack trace. That usually takes me well past the momentary weirdness at the top of the stack and dumps me straight into the repeating part.

Once you've identified the repeating part, pick a function from it that is somewhat unusual and search for it in your defect database. In our example, `SendMessageW` would probably be a bad choice, since sending a message is a pretty common operation in most Windows programs. I would go with `CTreeItem::GetDescriptionFromServer`.

It so happens that a query for all defects that involve the function `CTreeItem::GetDescriptionFromServer` turned up the following stack trace:

```
ntdll!RtlpAllocateHeap+0x33
ntdll!RtlAllocateHeap+0x151
ntdll!RtlDebugAllocateHeap+0xcd
ntdll!RtlpAllocateHeap+0x39592
ntdll!RtlAllocateHeap+0x151
PROGRAM!CopyString+0x24
PROGRAM!CopyDirectoryName+0x11
PROGRAM!GetItemLongPath+0xe
PROGRAM!CPrivateNode::GetSourceLongPath+0x6d
PROGRAM!CPrivateNode::GetSourcePath+0x57
PROGRAM!CPrivateNode::GetSource+0x123
PROGRAM!GetDownloadSource+0x23
PROGRAM!GetCustomizedButtonSource+0xcc
PROGRAM!CCustomizableToolbar::IsWarningNeeded+0x69
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x1b6
PROGRAM!CCustomizableToolbar::OnCommand+0x102

PROGRAM!CToolbar::OnAction+0x97
PROGRAM!CToolbarSite::SendToToolbar+0x66
PROGRAM!CToolbarSite::OnAction+0x1ff
PROGRAM!CToolbarSite::HandleMessage+0xaa
PROGRAM!CSite::HandleMessage+0x61
PROGRAM!CMainWindow::WindowProc+0xc92
PROGRAM!CWindow::WindowProc+0x91
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CReBar::_WndProc+0x1b5
comctl32!CReBar::s_WndProc+0x4a
USER32!UserCallWinProcCheckWow+0x1ad
USER32!SendMessageWorker+0x64a
USER32!SendMessageW+0x5b
comctl32!CToolbar::TBOnLButtonUp+0x181
comctl32!CToolbar::ToolbarWndProc+0xed1
comctl32!CToolbar::s_ToolbarWndProc+0xd6
USER32!UserCallWinProcCheckWow+0x1ad
USER32!CallWindowProcAorW+0xdb
USER32!CallWindowProcW+0x18
comctl32!CallOriginalWndProc+0x1d
comctl32!CallNextSubclassProc+0x8d
comctl32!DefSubclassProc+0x7c
PROGRAM!DefSubclassProc+0x56
PROGRAM!CToolbar::WindowProc+0x142
PROGRAM!CCustomizableToolbar::WindowProc+0xb3
PROGRAM!CWindowSubclass::SubclassWndProc+0xeb
comctl32!CallNextSubclassProc+0x8d
comctl32!MasterSubclassProc+0xe1
USER32!UserCallWinProcCheckWow+0x1ad
USER32!DispatchMessageWorker+0x389
PROGRAM!MsgWaitForCompletion+0xe0
PROGRAM!AsyncFinishCall+0x22
PROGRAM!SynchronousCallService+0x48a
```

```
PROGRAM!GetItemDescriptionFromServer+0x49c
PROGRAM!CTreeItem::GetDescriptionFromServer+0x15f
PROGRAM!CTreeItem::TryGetDescriptionFromServer+0x127
PROGRAM!CTreeItem::GetDescriptionWorker+0x198
PROGRAM!CTreeItem::GetDescription+0x188
PROGRAM!CTreeItemWrapper::GetDescriptionWorker+0x90
PROGRAM!CTreeItemWrapper::GetDescription+0x20b
PROGRAM!CItemPropertiesMenu::RefreshProperties+0xf2
PROGRAM!CItemPropertiesMenu::Execute+0xe7
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!CCompoundMenu::ExecuteDirect+0x308
PROGRAM!CCompoundMenu::Execute+0xf4
PROGRAM!CompoundMenu_DispatchCommand+0x108
PROGRAM!CItemMenu::Execute+0x29c
PROGRAM!InvokeViaContextMenu+0x11c
PROGRAM!CCustomizableToolbar::TrySimpleCommand+0x23e
PROGRAM!CCustomizableToolbar::OnCommand+0x102

PROGRAM!CToolbar::OnAction+0x97
```

Yup, there's that recurring 53-function cycle again. The initial part of the stack trace is different, of course, but the important part is right there. This is another manifestation of the same underlying bug.

Moral of the story: When studying a stack overflow, the stragglers at the top of the stack are the least important functions. You really want the meaty bit in the middle.

Raymond Chen

Follow