找自己游戏的CALL

游戏中的功能一般都是通过函数实现的，找到函数的地址，模拟函数调用，就相当于在游戏中直接调用该功能。

- 查找血量基址
- 下硬件断点，触发相关功能就会断下
- 在注入器中模拟测试call的地址
- 在程序中实现

```
hp基址：00416664
硬件断点：hw 00416664
加血：call 0x00402460
减血：call 0x004024E0
```

代码展示

```
void remoteCall(int call_addr) {
    HWND hwnd = ::FindWindow(NULL, L"我的游戏");
    DWORD pid, tid;
    tid = ::GetWindowThreadProcessId(hwnd, &pid);

    HANDLE hwnd_process = ::OpenProcess(PROCESS_ALL_ACCESS, FALSE, pid);
    ::CreateRemoteThread(hwnd_process, NULL, 0,
(LPTHREAD_START_ROUTINE)call_addr, NULL, 0, &tid);
    /*CString str;
    str.Format(L"进程：%p  线程：%p\n", pid, tid);
    OutputDebugString(str);*/
}

void CFindCallDlg::OnBnClickedBtnAdd()
{
    remoteCall(0x00402460);
}


void CFindCallDlg::OnBnClickedBtnSub()
{
    remoteCall(0x004024E0);
}
```