Debugging.TV

Frame 0x06

Presenter: Dmitry Vostokov

Topics

- Value passing and register reuse
- Breakpoint execution commands
- WinDbg pseudo-registers and scripting
- Passing data between breakpoints
- Platform independent commands
- Logging window messages
- Module load events

GetMessage

```
BOOL WINAPI GetMessage
(
__out LPMSG lpMsg,                  // RCX
__in_opt HWND hWnd,                 // RDX
__in UINT wMsgFilterMin,            // R8d
__in UINT wMsgFilterMax             // R9d
);
```

MSG

```
typedef struct tagMSG {
  HWND   hwnd;              // 64
  UINT   message;           // 64
  WPARAM wParam;            // 64
  LPARAM lParam;            // 64
  DWORD  time;              // 32
  POINT  pt;                // 32, 32
} MSG, *PMSG, *LPMSG;
```

Event State Management

```
0:000> ub 00000000`ff2d1064
notepad!WinMain+0xf5:
[...]
00000000`ff2d1051 488d4c2440      lea     rcx,[rsp+40h]           * bp 0
00000000`ff2d1056 4533c9          xor     r9d,r9d
00000000`ff2d1059 4533c0          xor     r8d,r8d
00000000`ff2d105c 33d2            xor     edx,edx
00000000`ff2d105e ff1524b40000    call    qword ptr [notepad!_imp_GetMessageW
(00000000`ff2dc488)]

0:000> u 00000000`ff2d1064
notepad!WinMain+0x182:
00000000`ff2d1064 413bc4          cmp     eax,r12d                * bp 1
00000000`ff2d1067 0f84b2060000    je      notepad!WinMain+0x18b (00000000`ff2d171f)
[...]

0:000> bl
 0 e 00000000`ff2d105e     0001 (0001)  0:**** notepad!WinMain+0x17c "r $t0 = rcx; g"
 1 e 00000000`ff2d1064     0001 (0001)  0:**** notepad!WinMain+0x182 ".printf \"hwnd: %p message:
%p wParam: %p lParam: %p\", poi(@$t0), poi(@$t0+@$ptrsize), poi(@$t0+2*@$ptrsize),
poi(@$t0+3*@$ptrsize); .echo; g"
```

Commands and pseudo-registers

```
.logopen
kv
u
ub
bp
bl
g
r
dp
```

```
.printf
.echo
poi
$t0
$ptrsize
bc
dd
.logclose
```

!Ad Hardcore Technical Support Training

January 13, 2012: Advanced Windows Memory Dump Analysis

January 18-23, 2012: Accelerated Windows Memory Dump Analysis

January 26-27, 2012: Accelerated .NET Memory Dump Analysis

Training Schedule

Debugging.TV