Debugging.TV

Frame 0x08

Presenter: Dmitry Vostokov

Topics

- Logging WinDbg extension
- Adding your API for logging
- Different logging formats
- Viewing verbose logging extension logs

Tracing Win32 API while debugging a process

Activation Context pattern

Custom Logging

C:\Program Files\Debugging Tools for Windows (x64)\winext\manifest\contexts.h

```
// ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
//
//                          Activation Context API
//
// ++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
category ActivationContext:
module KERNEL32.DLL:
FailOnFalse ActivateActCtx(HANDLE hActCtx, [out] PULONG_PTR lpCookie);
FailOnFalse DeactivateActCtx(DWORD dwFlags, ULONG_PTR upCookie);
```

C:\Program Files\Debugging Tools for Windows (x64)\winext\manifest\main.h

```
[...]
#include "contexts.h"
```

Enabling Logging

```
0:001> !logexts.loge

Windows API Logging Extensions  v3.01
Parsing the manifest files...
Location: C:\Program Files\Debugging Tools for Windows (x64)\winext\manifest\main.h
   Parsing file "main.h" ...
   Parsing file "winerror.h" ...
   Parsing file "kernel32.h" ...
[...]
Parsing completed.
Logexts injected. Output: "C:\Users\Training\Desktop\LogExts\"
Logging enabled.

0:001> !logc d *
All categories disabled.

0:001> !logc
Categories:

  1 ActivationContext               Disabled
  2 AdvApi32                        Disabled
[...]

0:001> !logc e 1
 1 ActivationContext               Enabled
```

Logging Output

```
0:001> !logo
Logging currently enabled.

Output directory: C:\Users\Dump Analysis\Desktop\LogExts\

Output settings:
  Debugger           Disabled
  Text file          Disabled
  Verbose log        Enabled

0:001> !logo e t
  Debugger           Disabled
  Text file          Enabled
  Verbose log        Enabled

0:001> !logo e d
  Debugger           Enabled
  Text file          Enabled
  Verbose log        Enabled
```

Tracing Example

```
0:001> g
ModLoad: 00000000`56bd0000 00000000`56c35000   C:\Program Files\Debugging Tools for Windows (x64)\winext\logexts.dll
[...]
Thrd 1498 000000013F5F1163 ActivateActCtx( 0x000000000044DD58) -> TRUE ( 0x000000000031F8F8)
Thrd 1498 000000013F5F11CD ActivateActCtx( 0x0000000000460188) -> TRUE ( 0x000000000031F908)
Thrd 1498 000000013F5F1201 ActivateActCtx( 0x000000000044E038) -> TRUE ( 0x000000000031F8F0)
(13f0.1498): Unknown exception - code 00000001 (first chance)
(13f0.1498): Unknown exception - code c015000f (first chance)
(13f0.1498): Unknown exception - code c015000f (!!! second chance !!!)
ntdll! ?? ::FNODOBFM::`string'+0x13ab0:
00000000`77c4fd5c 488b36          mov     rsi,qword ptr [rsi] ds:00000000`030b04d0=00000000030b0470

0:000> kL
Child-SP          RetAddr           Call Site
00000000`0031f5b0 00000000`77ac42d3 ntdll! ?? ::FNODOBFM::`string'+0x13ab0
00000000`0031f690 00000000`56c0d163 kernel32!DeactivateActCtx+0x23
00000000`0031f6c0 00000000`56bed394 logexts!LogHookCallFunction+0x73
00000000`0031f730 00000000`56c0d0e5 logexts!LogProcessHook+0x514
00000000`0031f870 00000001`3f5f1254 logexts!LogHook+0x45
00000000`0031f8c0 00000001`3f5f13db TestActCtx!wmain+0x224
00000000`0031f930 00000000`77ad652d TestActCtx!__tmainCRTStartup+0x13b
00000000`0031f970 00000000`77c0c521 kernel32!BaseThreadInitThunk+0xd
00000000`0031f9a0 00000000`00000000 ntdll!RtlUserThreadStart+0x1d

0:000> g
Thrd 1498 000000013F5F1254 DeactivateActCtx( 0x00000000 0x13AB3BF900000002) -> TRUE
Thrd 1498 000000013F5F1263 DeactivateActCtx( 0x00000000 0x13AB3BF900000001) -> TRUE
ntdll!NtTerminateProcess+0xa:
00000000`77c315da c3              ret
```

!Ad Hardcore Technical Support Training

April 11-16, 2012: Accelerated Windows Memory Dump Analysis

April 20-23, 2012: Advanced Windows Memory Dump Analysis

April 27-30, 2012: Accelerated Software Trace Analysis

Forthcoming: Accelerated Mac OS X Core Dump Analysis

Linux Core Dump Analysis

Training Schedule

Debugging.TV