



# Debugging.TV

Frame 0x16

Presenter: Dmitry Vostokov

MEMORY DUMP ANALYSIS SERVICES

[DumpAnalysis.com](http://DumpAnalysis.com)

Including Crash and Hang Analysis Audit, Training and Seminars

Sponsors

**OPENTASK**

Iterative and Incremental Publishing

# Topics

- Window 8 Memory Dumps
- New WinDbg
- New Patterns
- New Commands

# WinDbg and W8 Dumps

	6.12.0002.633	6.2.9200.16384
Process user memory dumps	+	+
Complete memory dumps	-	+

[WinDbg.org](http://WinDbg.org)

# Complete Memory Dumps

## Stack Trace Collection

```
!process 0 1f
```

```
!process 0 16 (with 4 arguments per frame)
```

# New Patterns

## Frozen Process

```
0: kd> !process 0 0
```

```
[...]
```

```
PROCESS fffffa8002cb2940
```

```
  SessionId: 2  Cid: 0c80  Peb: 7f6c41dd000  ParentCid: 0288
```

**DeepFreeze**

```
  DirBase: 2ef45000  ObjectTable: fffff8a002f215c0  HandleCount: <Data Not Accessible>
```

```
  Image: iexplore.exe
```

```
PROCESS fffffa8003816940
```

```
  SessionId: 2  Cid: 0d04  Peb: 7f6c3aca000  ParentCid: 0c80
```

**DeepFreeze**

```
  DirBase: 34024000  ObjectTable: fffff8a001749a00  HandleCount: <Data Not Accessible>
```

```
  Image: iexplore.exe
```

```
PROCESS fffffa8001e0f740
```

```
  SessionId: 2  Cid: 0d7c  Peb: 7f65412f000  ParentCid: 0c78
```

```
  DirBase: 0e165000  ObjectTable: fffff8a00055ff00  HandleCount: <Data Not Accessible>
```

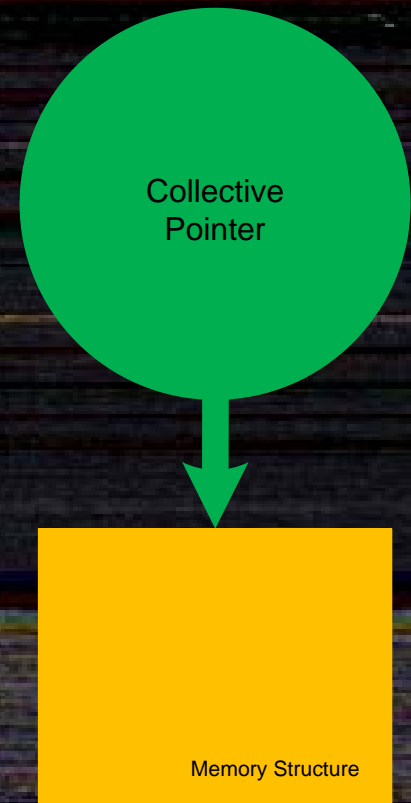
```
  Image: notepad.exe
```

```
[...]
```

# New Commands



Collective Pointer  
structural pattern



```
!for_each_register -c dps @#RegisterValue l1
```



# !Ad Hardcore Software Support Training

Nov 30 – Dec 3, 2012	<u>Accelerated Windows Software Trace Analysis</u>
November 16-26, 2012	<u>Accelerated Windows Memory Dump Analysis</u>
December 7-10, 2012	<u>Accelerated Windows Malware Analysis</u>
December 17, 2012	<u>Philosophy of Software Diagnostics</u> (FREE)
December 17, 2012	<u>Pattern-Based Software Diagnostics</u> (FREE)
Early 2013	The New Old Debugging

# Debugging<sup>3</sup>

Coming soon

# Debugging.TV

Now on YouTube!

<http://www.youtube.com/DebuggingTV>