



Debugging.TV

Frame 0x21

Presenter: Dmitry Vostokov

SOFTWARE DIAGNOSTICS SERVICES

www.DumpAnalysis.com

Including Memory Dump and Software Trace Analysis Audit, Seminars,
Certification and Training

Sponsors

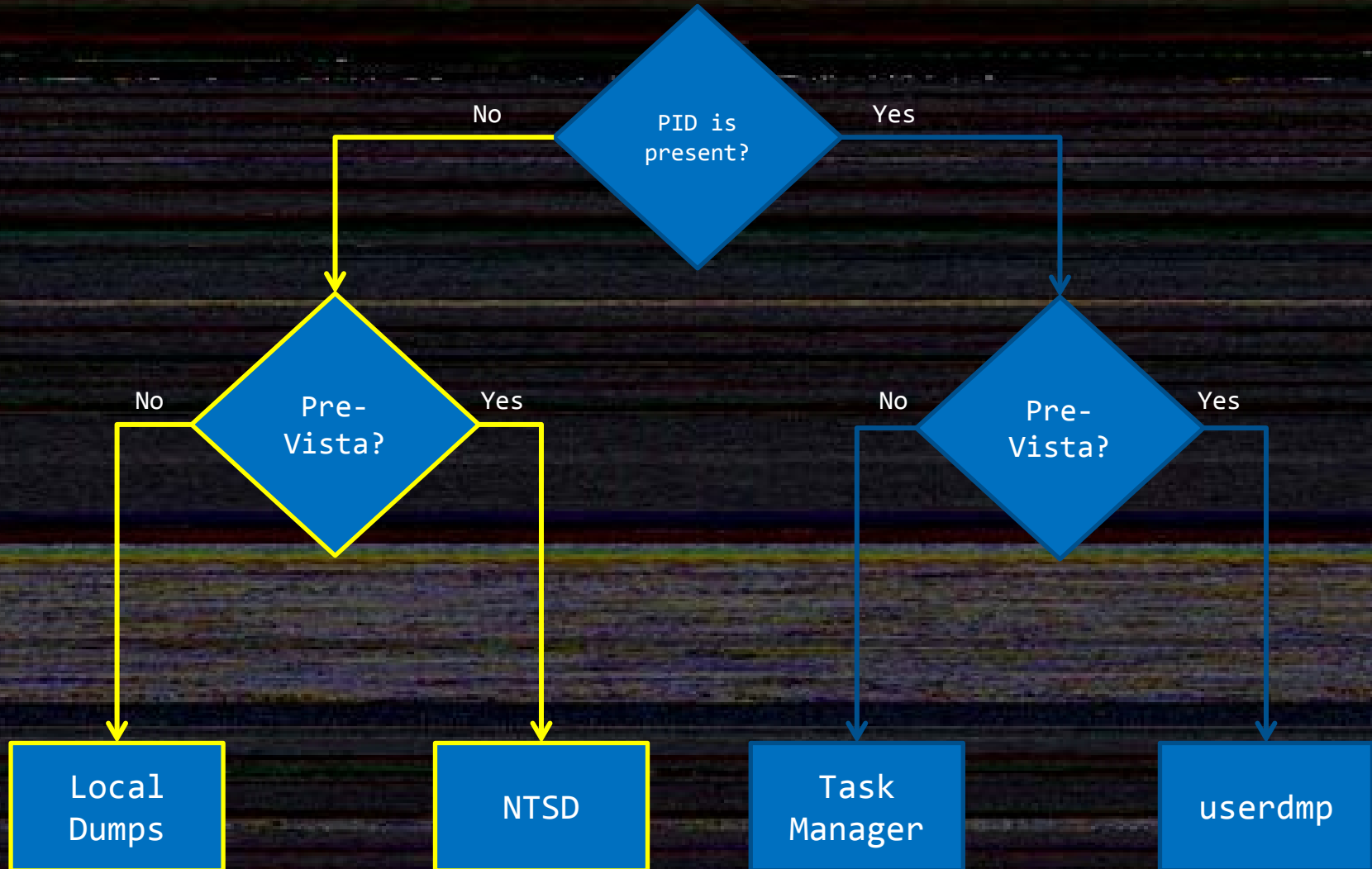
OPENTASK

Iterative and Incremental Publishing

Topics

- Process dumps: main algorithm
- NTSD and LocalDumps example
- Troubleshooting process dumps

Main Algorithm



NTSD

- x64

```
HKLM\S\M\WNT\CV\AeDebug\Debugger =  
    ntsd -p %ld -e %ld -c ".dump /f /u c:\NTSDumps\x64\new.dmp; q"
```

- x86 on x64

```
HKLM\S\Wow6432Node\M\WNT\CV\AeDebug\Debugger =  
    ntsd -p %ld -e %ld -c ".dump /f /u c:\NTSDumps\x86\new.dmp; q"
```

- native x86

```
HKLM\S\M\WNT\CV\AeDebug\Debugger =  
    ntsd -p %ld -e %ld -c ".dump /f /u c:\NTSDumps\new.dmp; q"
```

- /ma switch instead of /f for new NTSD

LocalDumps

HKLM\S\M\W\Windows Error Reporting\LocalDumps

Name: DumpFolder

Type: REG_SZ

Value: C:\MemoryDumps

Name: DumpType

Type: REG_DWORD

Value: 0x2

Useful Links

- [NTSD as a default debugger](#)
- [TestWER](#)
- [Process Monitor](#)
- [WinDbg.org](#)

!Ad Hardcore Software Diagnostics Training

February 20-25, 2013	<u>Accelerated Windows Memory Dump Analysis</u>
March, 25, 2013	<u>Malware Narratives</u> (FREE)
April, 26-29, 2013	<u>Accelerated Windows Debugging³</u>
May, 13, 2013	<u>Philosophy of Software Diagnostics</u> (FREE)
Summer, 2013	Accelerated Windows Network Trace Analysis
2013	The New Old Debugging

Debugging³

Now Available for Booking

Debugging.TV

Now on YouTube!

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