Debugging.TV

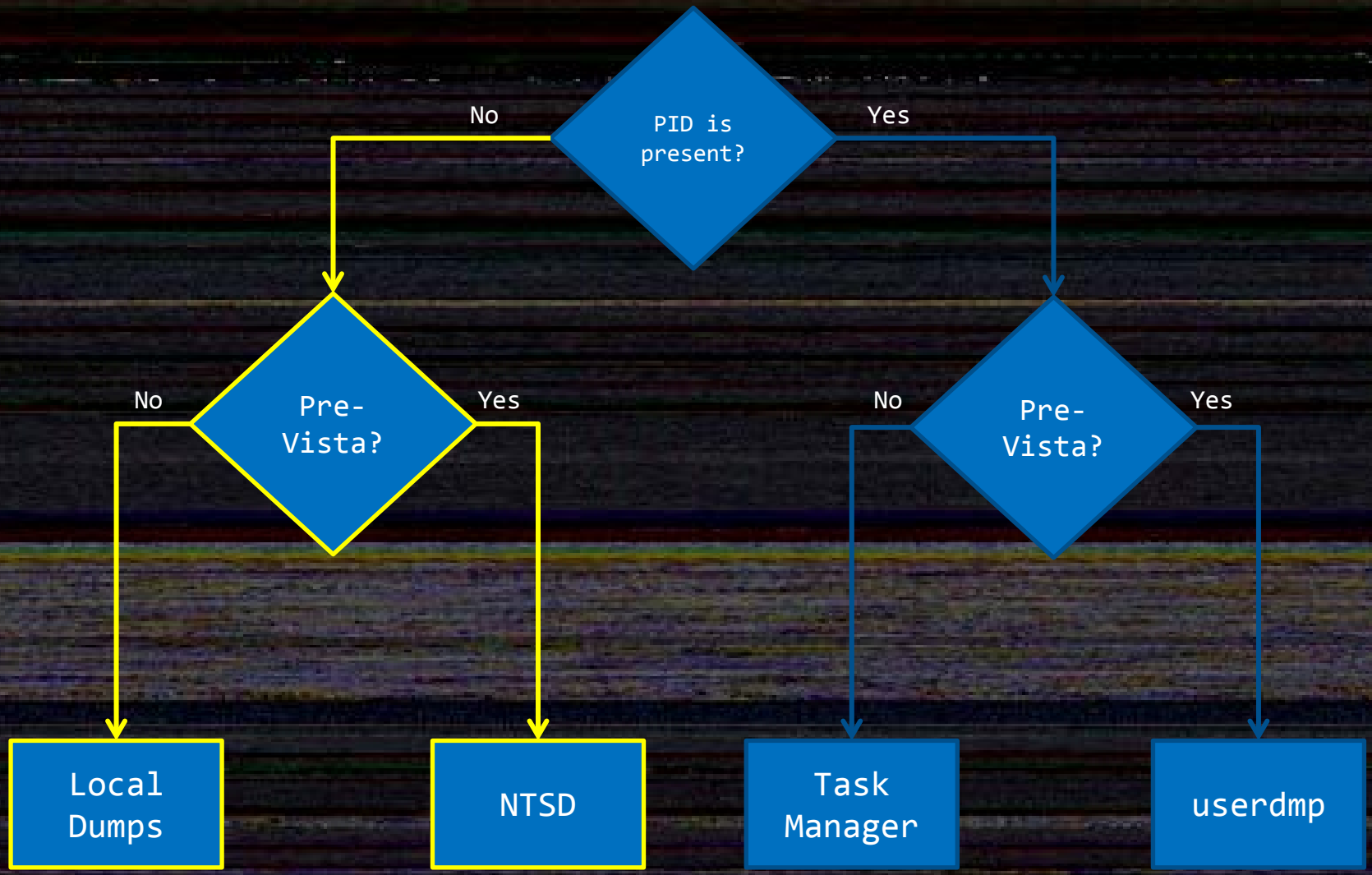
Frame 0x21

Presenter: Dmitry Vostokov

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	Accelerated Windows Memory Dump Analysis
March, 25, 2013	Malware Narratives (FREE)
April, 26-29, 2013	Accelerated Windows Debugging^3
May, 13, 2013	Philosophy of Software Diagnostics (FREE)
Summer, 2013	Accelerated Windows Network Trace Analysis
2013	The New Old Debugging

Debugging^3

Now Available for Booking

Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV