Debugging.TV

Frame 0x15

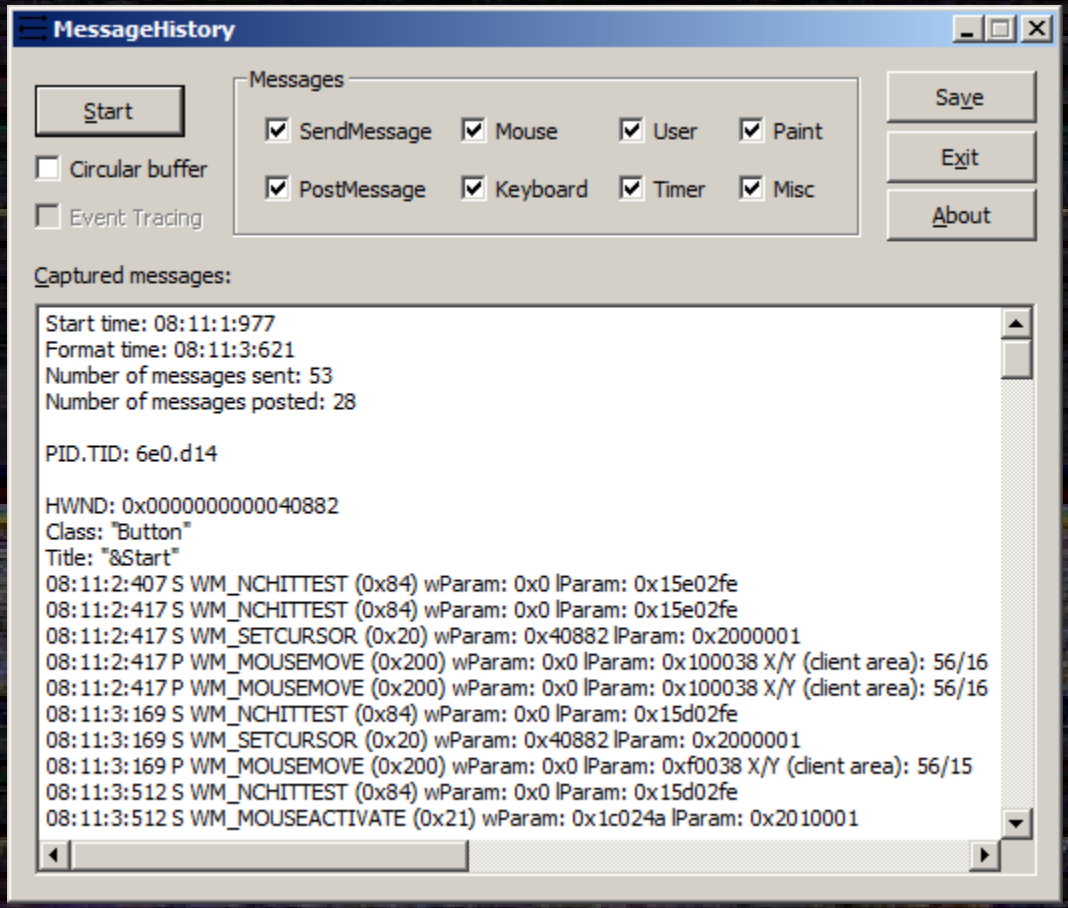
Presenter: Dmitry Vostokov

Topics

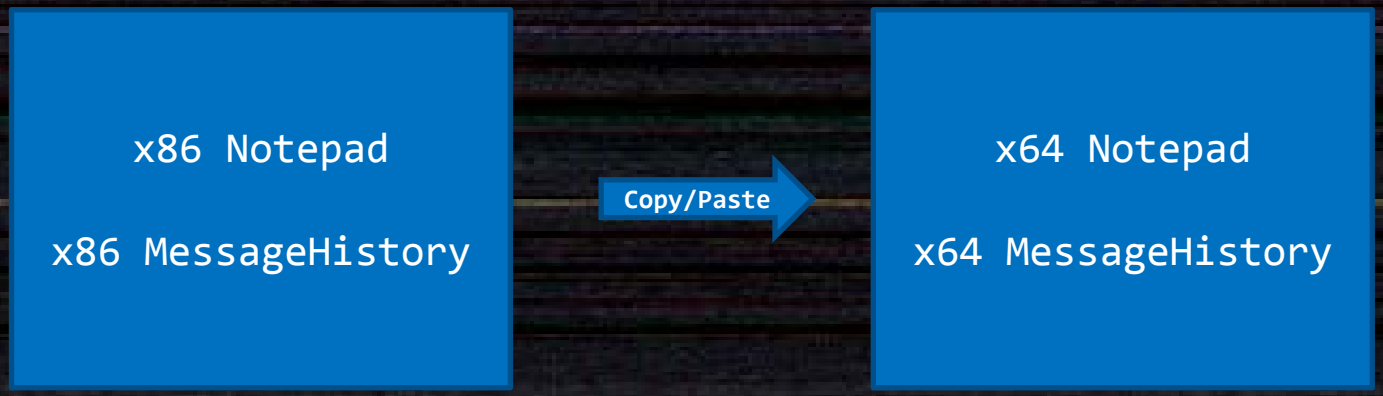
- Window Message Tracing
- Citrix MessageHistory
- Inter-Correlation Trace Analysis
- Using Excel for Trace Analysis

MessageHistory

http://support.citrix.com/article/CTX111068



Inter-Correlation




```
148920 08:37:09:420 P PID: d20  TID: 2ac  HWND: 0x002B06C2         Class: Edit Msg: WM_COPY  (0x301)
133333 08:37:13:660 P PID: 128c TID: 11a8 HWND: 0x00000000002D06F4 Class: Edit Msg: WM_PASTE (0x302)
```

Analysis Challenges

- Different data field formats
- Different column ordering

Solution: A Proposal for CSTF

Common Software Trace Format

References

Trace correlation analysis patterns:

- Intra-Correlation
- Inter-Correlation

Tools for tracing windows and window messages:

- WindowHistory x64
- MessageHistory

!Ad Hardcore Software Support Training

November 2-5, 2012	Accelerated Windows Software Trace Analysis
November 16-26, 2012	Accelerated Windows Memory Dump Analysis
December 7-10, 2012	Accelerated Windows Malware Analysis
December 17, 2012	Philosophy of Software Diagnostics (FREE)
December, 2012	Pattern-Based Software Diagnostics
Early 2013	The New Old Debugging

Debugging^3 Coming soon

Debugging.TV

Now on YouTube!

http://www.youtube.com/DebuggingTV