FORENSIC CRASH DUMP ANALYSIS

Yes BSOD do provide some value

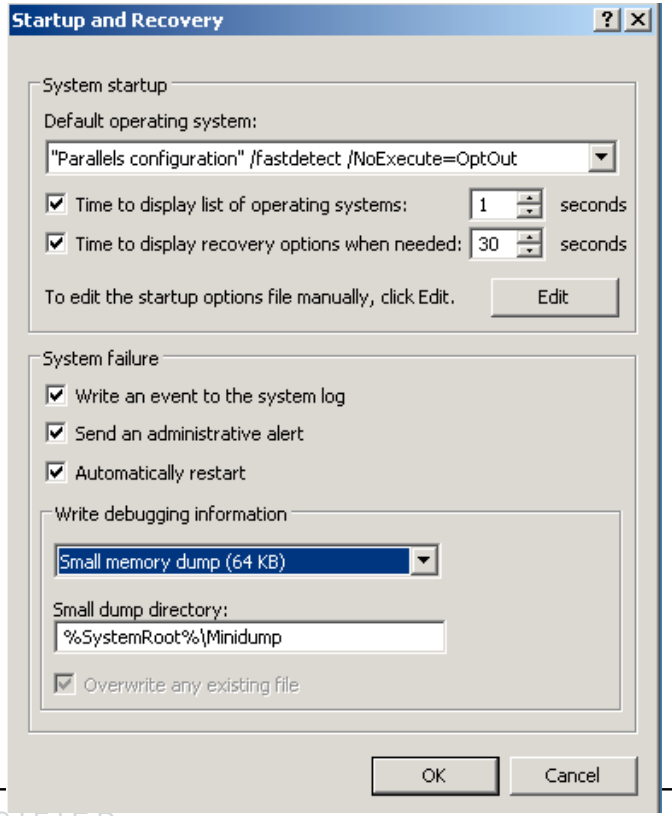
System Crash Dump = BSOD

System Crash Dump Analysis Basics

- System Crash Dumps happen when something in the Kernel goes wrong
  - Unhandled exception
  - OS or driver detects inconsistency
  - Referencing paged out memory at interrupt level
  - Reschedule is attempted at dispatch level IRQL or higher
  - Hardware error
- Microsoft wants to keep the integrity of your data so they crash your system.

System Crash Dump Settings

- My Computer-> Properties-> Advanced-> Startup and Recovery



How Big is Your Dump

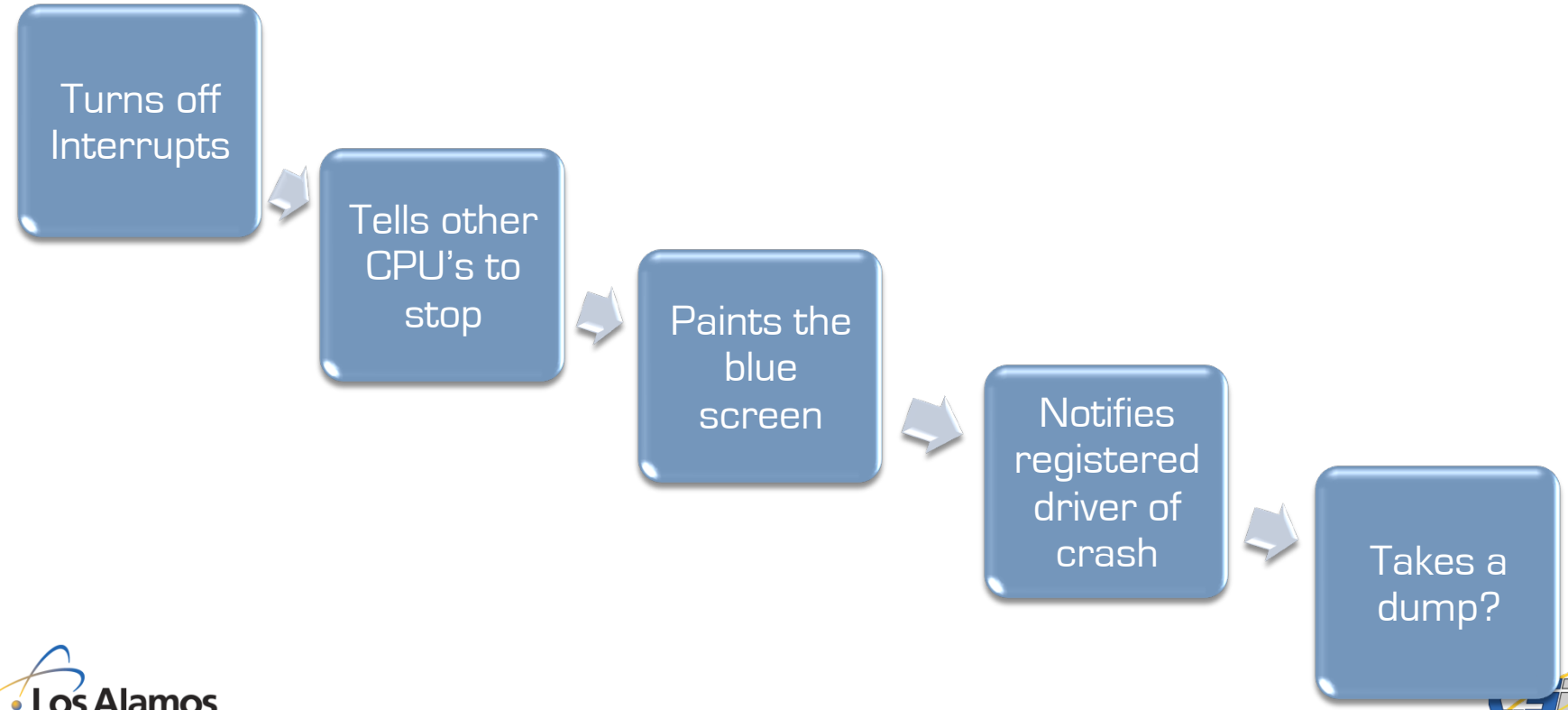
- Sizes of crash dumps
  - Small Memory Dump – 64K
    - XP default
    - Kept across time
  - Kernel Memory Dump
    - Size dependent on kernel memory space
    - Vista default
    - Small Memory dump created as well
  - Complete Memory – size of memory
    - Pagefile.sys must be large enough to hold entire memory dump

System Crash Dump Locations

- Small default location:
  - %SYSTEMROOT%\minidump\
- Kernel and Complete
  - %SYSTEMROOT%\Memory.DMP
- Check the system settings to if not located in this directory

System Crash - KeBugCheckEX

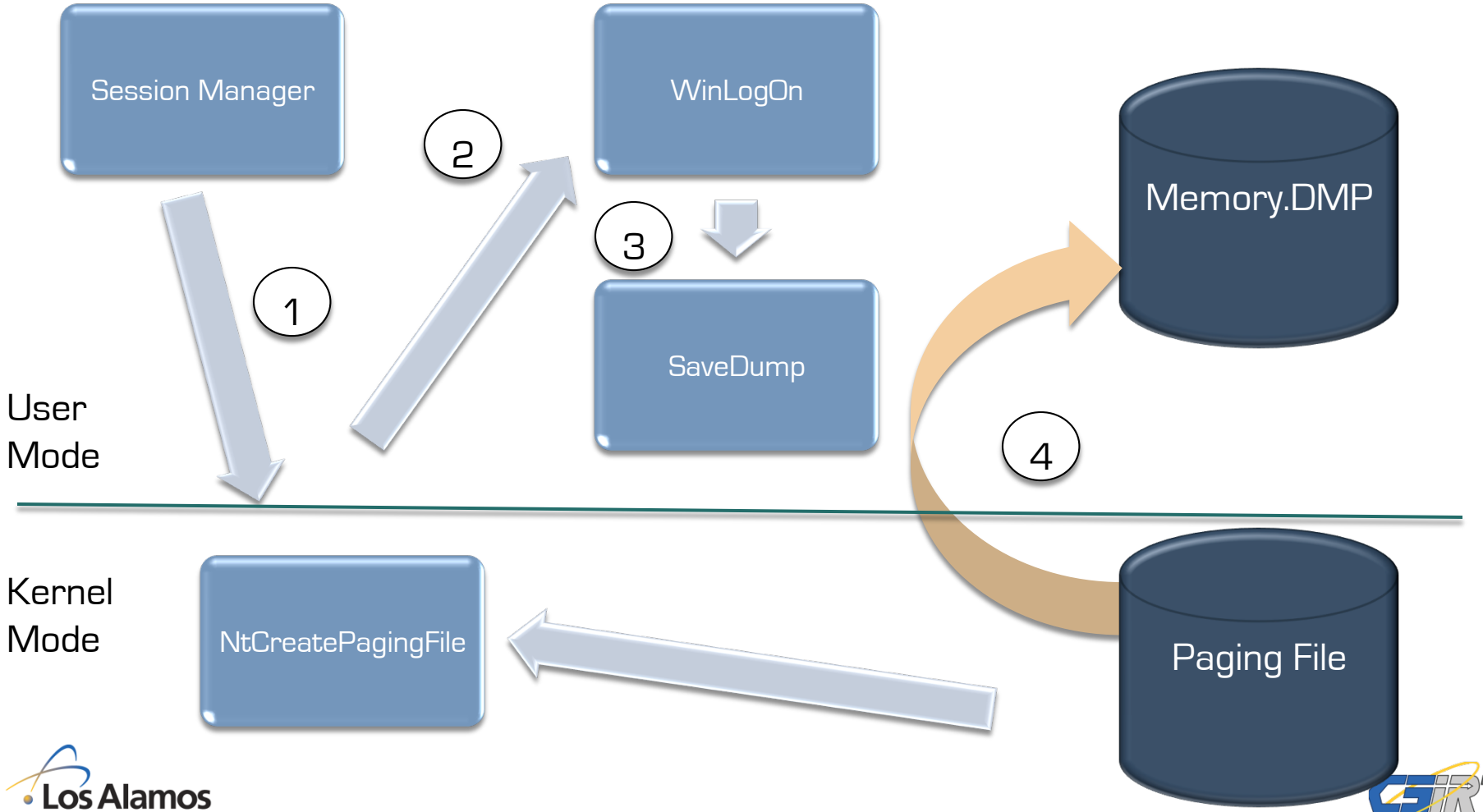
- KeBugCheckEX Process



System Crash - KeBugCheckEX

- Takes 5 Parameters
  - Stop Code (Bug Check)
  - 4 Stop Code defined parameters
- Most common Stop Codes
  - IRQL_NOT_LESS_OR_EQUAL
    - Access of invalid memory access
  - INVALID_KERNEL_MODE_TRAP and KMODE_EXCEPTION_NOT_HANDLED
    - Executing garbage instructions
    - Stack is trashed

System Crash Dump Process on Reboot



System Crash Dump Analysis

- What you need
  - WinDBG
- Open WinDBG
  - Set Symbol Files (File->File Symbol Path)
    - "srv*c:\symbols*http://msdl.microsoft.com/downloads/symbols"
  - Set Image File Path as well if mini dump
  - Open dump file
    - File->Open Crash Dump

System Crash Dump Analysis - WinDBG

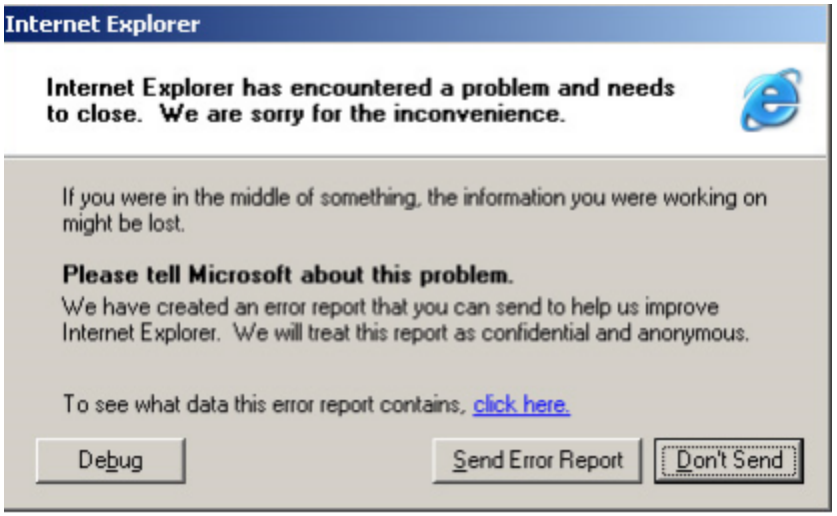
- !analyze –v
  - Data about the crash
- !process 0 0
  - Running processes during the crash
- lmkv
  - List of driver s on system
- List of Bug Codes (Stop Codes)
  - http://www.thewindowsclub.com/windows-bug-check-or-stop-error-codes

System Crash Dump Analysis - KMSAnalyzer

- Kernel Memory Space Analyzer
  - http://www.microsoft.com/downloads/details.aspx?familyid=e84d3b35-63c3-445b-810d-9fed3fdeb13f&displaylang=en
- Install by downloading then xcopy extracted files to "Windows Debugging folder"
- Includes a wizard and command line tool

Application Crash Dump Process

- Crash dialog appears
- Users can see what the report contains
- Send or don't send the crash dump data



Application Crash Dumps - Files

- myapp.exe.mdmp
  - Collects stacks and loaded modules
- myapp.exe.hdmp
  - Includes heap data in addition to the minidump
- appcompat.txt
  - Stands for application compatibility
  - Dll's associated with the crashing application
- manifest.txt
  - What crashed
  - What files were collected

Application Crash Dumps

- Location:
  - C:\Documents and Settings\<user>\Local Settings\Temp\WER???.dir00\
  - ?-represents alpha or numeric character
- Dumps are deleted once the hanging or crashing process finishes

Application Crash Dump Analysis

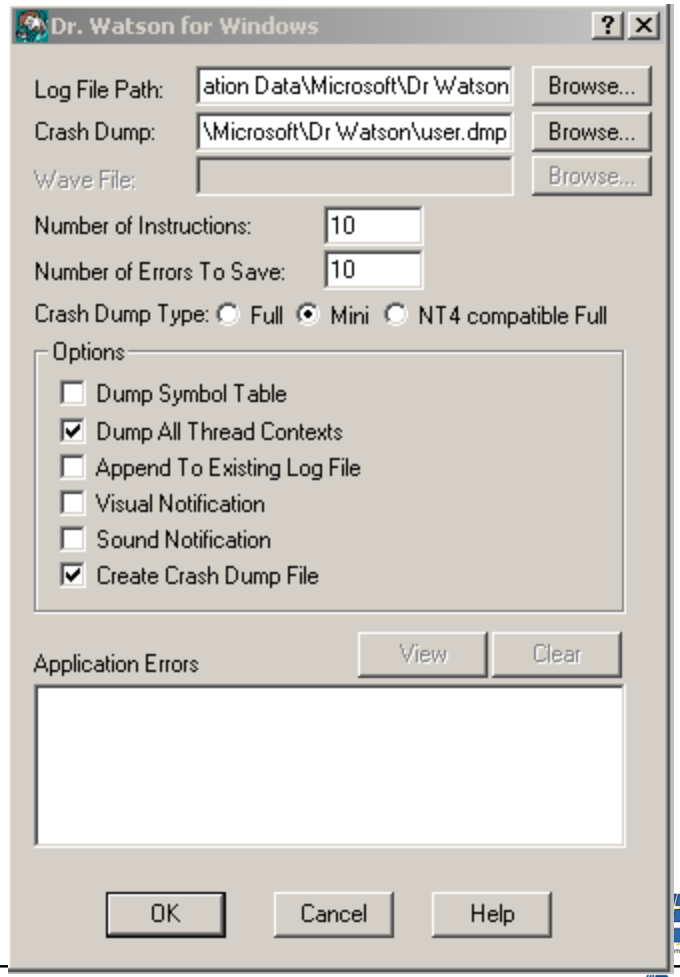
- !analyze -v
- lmcf
  - List modules with checksum and full path
- peb
  - System environmental variables, computer name
- lmv m<modulename>
  - Detailed information of loaded module

What to Look For

- Rouge Drivers
- Checksums == 0
- Known evil image sizes
- Date and time stamps of drivers

Dr. Watson Dumps

- Dr. Watson (drwtsn32)
- Start->Run->drwtsn32



Dr. Watson Logs

- Logs Application Crashes
  - Logs data about the system and the application that crashed
  - Tracks
    - Processes running
    - Logged on user
    - Path to crashing application
    - Dll's loaded by application

Dr. Watson Logs

```
Microsoft (R) DrWtsn32
Copyright (C) 1985-2001 Microsoft Corp. All rights reserved.


Application exception occurred:
        App: C:\Program Files\Mozilla Firefox\firefox.exe (pid=168)
        When: 2/8/2010 @ 16:28:57.311
        Exception number: 80000003 (hardcoded breakpoint)

*----> System Information <----*
        Computer Name: XPWINRAR
        User Name: student
        Terminal Session Id: 0
        Number of Processors: 1
        Processor Type: x86 Family 6 Model 23 Stepping 10
        Windows Version: 5.1
        Current Build: 2600
        Service Pack: 3
        Current Type: Uniprocessor Free
        Registered Organization: Company
        Registered Owner: XPVM

*----> Task List <----*
   0 System Process
   4 System
 540 smss.exe
 604 csrss.exe
 628 winlogon.exe
 672 services.exe
 684 lsass.exe
 840 vmacthlp.exe
 856 svchost.exe
```

Dr. Watson Logs

- Location of log and dump
  - C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\drwatson.log
  - C:\Documents and Settings\All Users\Application Data\Microsoft\Dr Watson\user.dmp
- Dump file overwritten by default

Dr. Watson Logs – What to Look For

- Suspicious Process
  - Yes the bad guys processes are buggy
- Injected DLL's
  - BHO's etc
- Users logged on to system
  - Should the user be on there?

Corporate Error Reporting

- Error Reporting set up to "improve the Windows ecosystem"
- CER can collect application crashes, application hangs and system crashes
- Remember: Crash dumps can contain sensitive information

CER - Setup

- Need a SMB Share to send crash dumps too
- Set the Registry to reflect CER
  - HKLM\Software\Policies\Microsoft\PCHealth\ErrorReporting\DW
  - HKLM\Software\Microsoft\PCHealth\ErrorReporting\DW

CER Registry Values

Registry Value Name	Type	Notes
DWFileTreeRoot	**SZ**	UNC or link to System Center Operations Manager for more information about Corporate Error Reporting.
DWBypassQueue	**DWORD**	Maximum number of reports in each queue.
DWNeverUpload	**DWORD**	Hide **Send Report** button, and cancel report.
DWNoExternalURL	**DWORD**	Suppress response URL or Trident.
DWNoFileCollection	**DWORD**	Cancel upload when a file or user document is requested.
DWNoSecondLevelCollection	**DWORD**	Cancel upload for any second-level request.
DWNoSignOffQueueReporting	**DWORD**	Turned on and turned off by a check box on the **Signoff Queued** dialog box.

CER Registry Values

Registry Value Name	Type	Notes
DWQueuePesterInterval	**DWORD**	Allow this number of minutes to elapse before prompting user again.
DWReporteeName	**SZ**	Replace "Microsoft" with another company name in reporting dialog boxes.
DWTracking	**DWORD**	Log user name, computer name, and time/date to the CER log.
DWURLLaunch	**SZ**	Ignore response, and always display this URL in the final dialog box.
DWVerboseLog	**DWORD**	Display a diagnostic log for integrators.
DWExplainerURL		Replace the data use feedback link with the corporate page.
DWCloseTransferDialogWhenDone	**DWORD**	Turned on and turned off by a check box on the **Report Transfer Progress** dialog box.
DWBypassQueue	**DWORD**	Report immediately if the user is online. Cancel report if offline.
DWAlwaysReport	**DWORD**	Hide **Don't Send** button, and encourage the user to send a report.

Corporate Error Reporting

- What LANL is researching
  - Analyzing crash dumps on mass
    - Do what we just did just on several crashes a day across the enterprise
  - Helps to find zero days
  - Discover compromises through the data collected and analyzed from the crash dumps

References

- Carvey, Harlan. “Windows Forensic Analysis”. 219-220. (2007)
- *Ganapathi, Archana.* “Windows XP Kernel Crash Analysis”. (Dec. 2006)
- Orgovan, Vince “Harvesting Error Reports from Windows Systems”. (2008)
- Russinovich, Mark. “Windows Hand and Crash Dump Analysis”. (2006)
- Russinovich, Mark. Solomon, David. “Microsoft Windows Internals 4th Edition”. 845-870. (2005)
- Microsfot. “How to: Configure Microsoft Error Reporting”. http://msdn.microsoft.com/en-us/library/bb219076.aspx#MicrosoftErrorReporting_RegistrySettings. (2006)
- Schuster, Andreas . “Microsoft Kernel Memory Space Analyzer”. http://computer.forensikblog.de/en/2006/09/microsoft_kernel_memory_space_analyzer.html(Sep. 2009)