KERIO

Connect. Communicate. Collaborate. Securely.

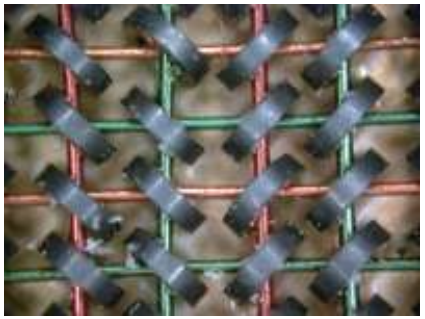
Analýza crashdumpů a post-mortem debuggování

Pavel Dobrý, pdobry@kerio.com

Agenda

- Co je to crashdump (core dump) ?
- Jak jej získat ?
- Obsah crashdump souboru
- Nástroje pro analýzu
- Ukázka analýzy
- Tipy a triky
- Debuggovací a chybové informace z klientů
- Automatická analýza

Co je crashdump



- též core dump, core file, minidump

- přesný obraz běžícího procesu v daném časovém okamžiku
- uložen v binárním souboru
- obsahuje obraz procesu a obsah paměti (adresního prostoru procesu)

- potenciálně velký soubor (až stovky MB)
  - výhoda: maximum dostupných informací
  - nevýhoda: horší manipulace, někdy až moc informací

Použití crashdumpu

- post-mortem analýza při pádu programu
  - získání crashdumpu od zákazníka
  - analýza vývojářem, hledání příčiny pádu
  - oprava chyby

- offline analýza chování programu (userdump)
  - záměrné vytvoření dumpu
  - analýza stavu procesu, vláken a paměti
  - např. 100% CPU, deadlock

Vznik crashdumpu

- reakce na neočekávaný stav programu
  - nezachycené výjimky
  - programátorské chyby
  - neošetřené signály (Linux, Mac)
  - HW chyby

- zpravidla dump vytváří operační systém
- lze jej vytvořit aplikací
- liší se podle OS

A problem has been detected and Windows has been shut down to prevent damage
to your computer.

The problem seems to be caused by the following file: SPCMDCON.SYS

PAGE_FAULT_IN_NONPAGED_AREA

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

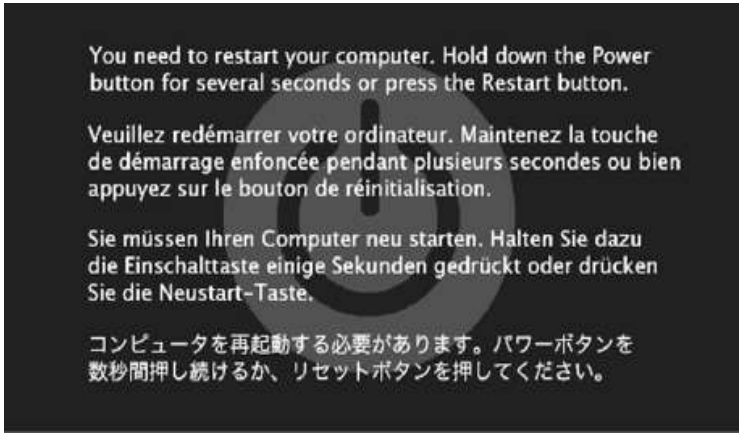
Technical information:

*** STOP: 0x00000050 (0xFD3094C2,0x00000001,0xFBFE7617,0x00000000)

*** SPCMDCON.SYS - Address FBFE7617 base at FBFE5000, DateStamp 3d6dd67c

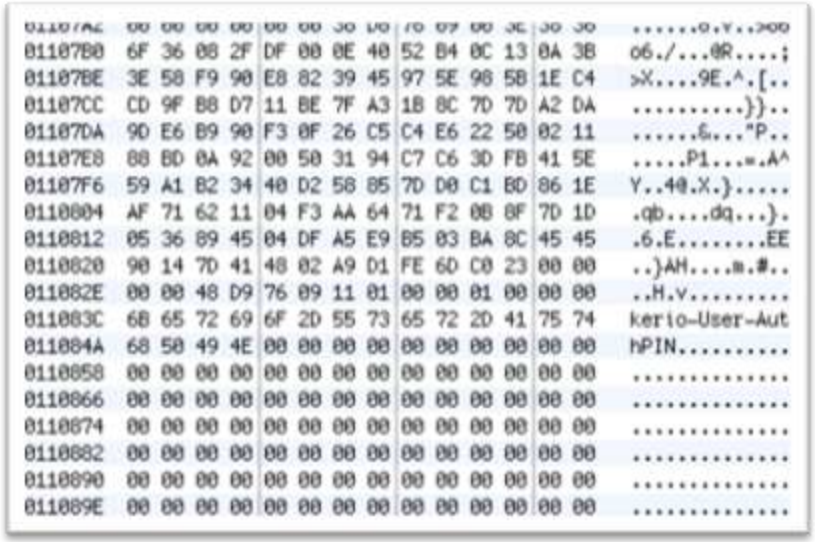
Typy dumpů

- kernelové
  - chyby v driverech
  - chyby v kernelu
  - HW problémy
  - BSOD, GSOD, kernel panic



- userspace
  - uživatelské aplikace
  - systémové služby
  - HW problémy

Obsah crashdumpu



- obraz procesu v paměti
  - spustitelný soubor
  - info o sdílených knihovnách
- obsah registrů procesoru
- adresní prostor procesu
  - stack pro jednotlivá vlákna
  - segmenty heapu
  - statické proměnné, řetězce
- parametry prostředí, informace o OS
- Často obsahuje citlivá uživatelská data vzniklá za běhu programu (např. hesla) !

Předpoklady pro zpracování

- tabulka symbolů
  - vzniká při překladu
  - obsahuje názvy funkcí, proměnných a jejich scope
  - usnadňuje analýzu a orientaci v dumpu
  - není třeba ji distribuovat s programem k zákazníkovi

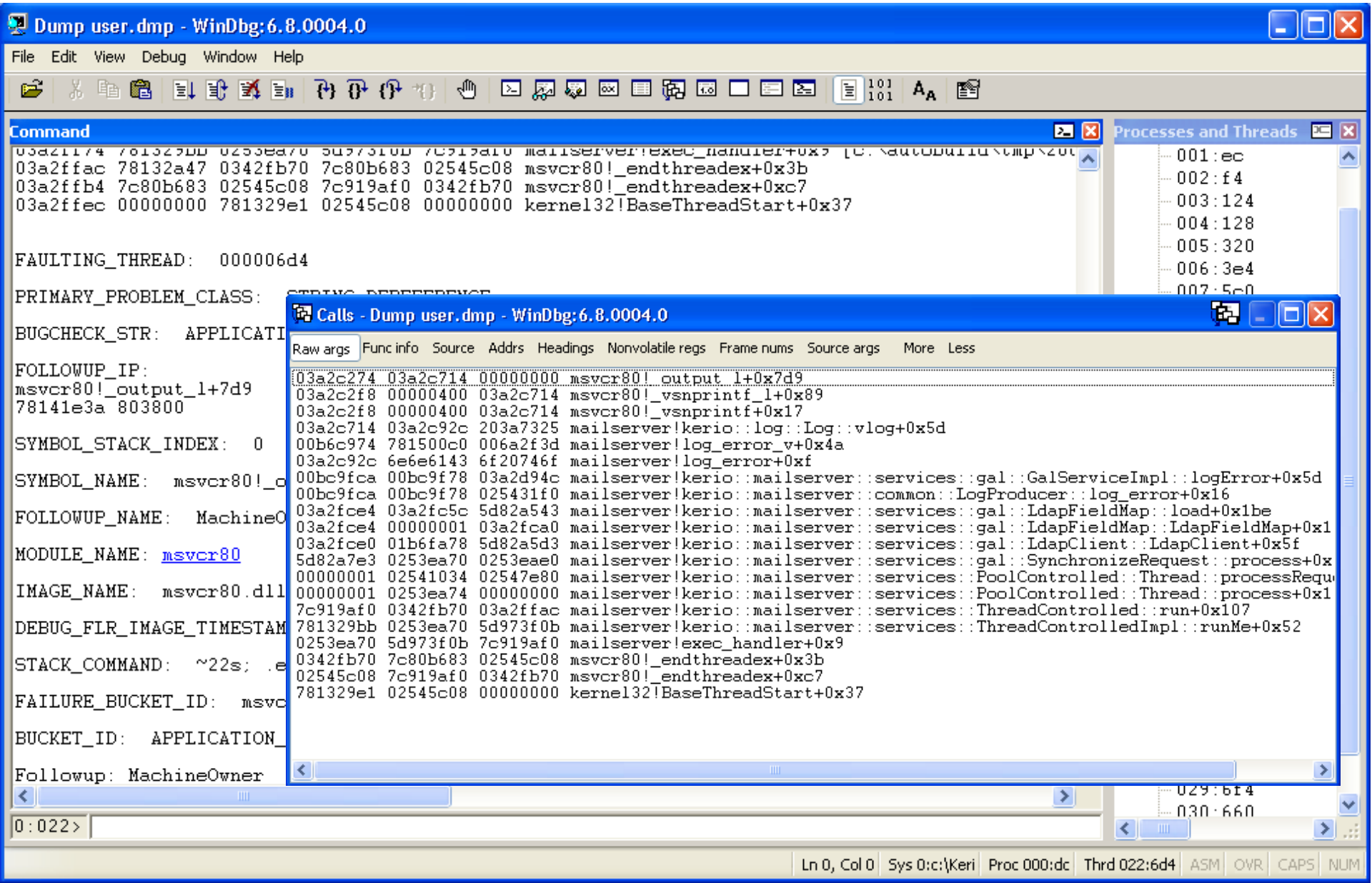
- alespoň základní znalost ASM a architektury (Intel, PPC)
- mít vhodné nástroje a umět s nimi
- trpělivost

Windows

- symbol table je v souboru .pdb
  - volby kompilátoru /Zi /DEBUG /OPT:REF
- nástroje
  - WinDBG, Visual Studio C++
- lze použít symbol server pro centrální správu
  - privátní se symboly k aplikaci (.exe, .dll, .pdb)
  - veřejný s public symboly Microsoft knihoven
- automatické rozpoznání verze aplikace a načtení symbolů
- dump lze zapsat samotnou aplikací: MiniDumpWriteDump()

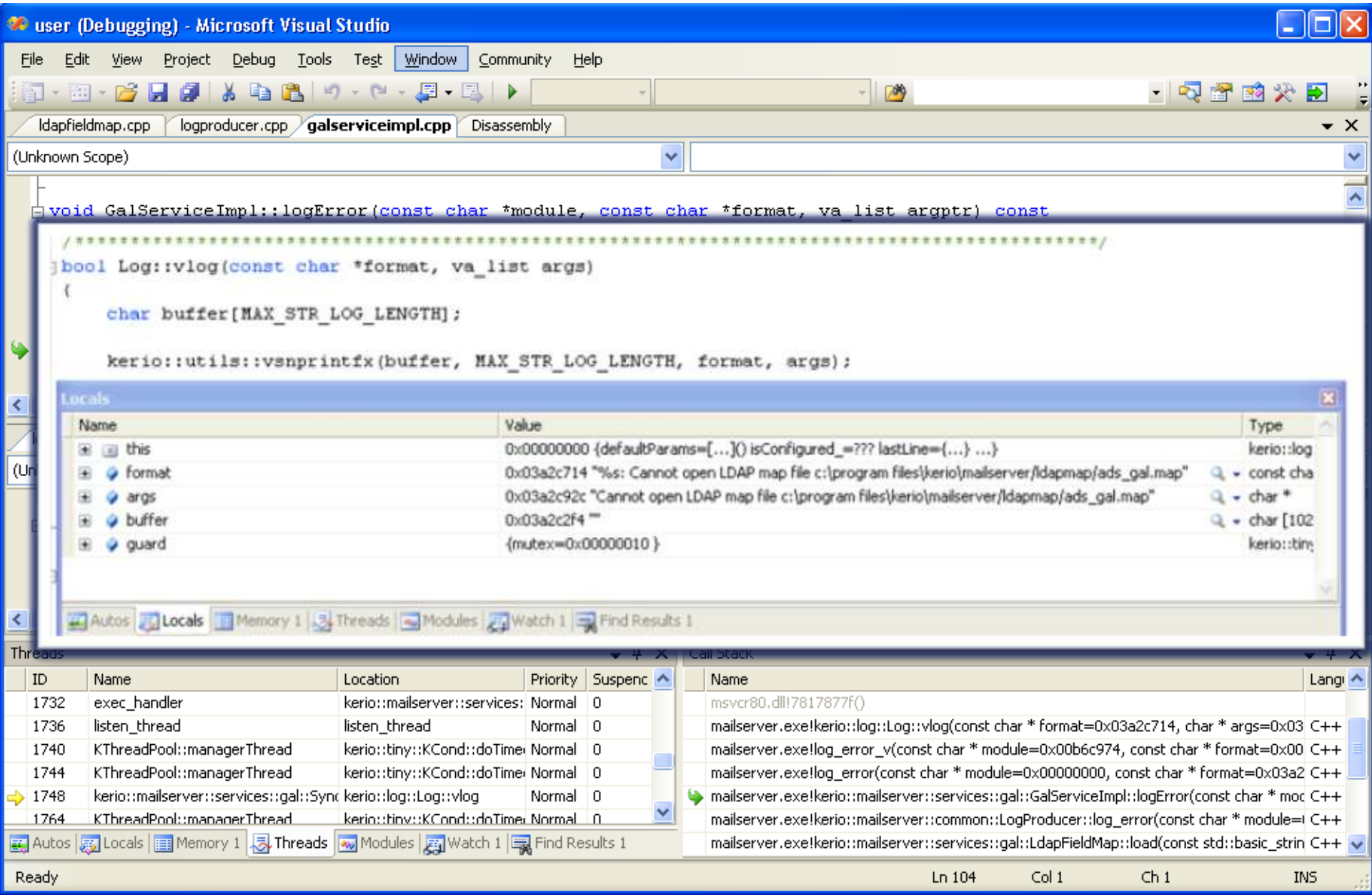
WinDBG

- zdarma ke stažení
- velmi dobrý debugger
- umí pracovat s user i kernel dumpy
- možnost napsat si vlastní plugin (skript)
- integrace se symbol serverem
- analýza a zobrazení heapu, detekce leaku
- “gdb s nešikovnýma okýnkama”

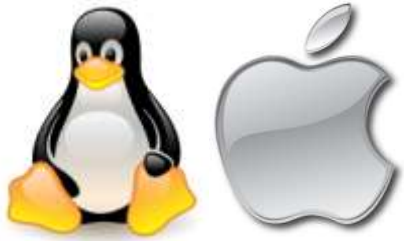

Dump user.dmp - WinDbg:6.8.0004.0
File Edit View Debug Window Help
Command
03a2ffac 78132a47 0342fb70 7c80b683 02545c08 msvcr80!_endthreadex+0x3b
03a2ffb4 7c80b683 02545c08 7c919af0 0342fb70 msvcr80!_endthreadex+0xc7
03a2ffec 00000000 781329e1 02545c08 00000000 kernel32!BaseThreadStart+0x37
FAULTING_THREAD: 000006d4
PRIMARY_PROBLEM_CLASS:
BUGCHECK_STR: APPLICATI
FOLLOWUP_IP:
msvcr80!_output_l+7d9
78141e3a 803800
SYMBOL_STACK_INDEX: 0
SYMBOL_NAME: msvcr80!_o
FOLLOWUP_NAME: MachineO
MODULE_NAME: msvcr80
IMAGE_NAME: msvcr80.dll
DEBUG_FLR_IMAGE_TIMESTAM
STACK_COMMAND: ~22s; .e
FAILURE_BUCKET_ID: msvc
BUCKET_ID: APPLICATION_
Followup: MachineOwner
0:022>
Processes and Threads
001:ec
002:f4
003:124
004:128
005:320
006:3e4
029:6f4
030:660
Calls - Dump user.dmp - WinDbg:6.8.0004.0
Raw args Func info Source Addrs Headings Nonvolatile regs Frame nums Source args More Less
03a2c274 03a2c714 00000000 msvcr80!_output_l+0x7d9
03a2c2f8 00000400 03a2c714 msvcr80!_vsnprintf_l+0x89
03a2c2f8 00000400 03a2c714 msvcr80!_vsnprintf+0x17
03a2c714 03a2c92c 203a7325 mailserver!kerio::log::Log::vlog+0x5d
00b6c974 781500c0 006a2f3d mailserver!log_error_v+0x4a
03a2c92c 6e6e6143 6f20746f mailserver!log_error+0xf
00bc9fca 00bc9f78 03a2d94c mailserver!kerio::mailserver::services::gal::GalServiceImpl::logError+0x5d
00bc9fca 00bc9f78 025431f0 mailserver!kerio::mailserver::common::LogProducer::log_error+0x16
03a2fce4 03a2fc5c 5d82a543 mailserver!kerio::mailserver::services::gal::LdapFieldMap::load+0x1be
03a2fce4 00000001 03a2fca0 mailserver!kerio::mailserver::services::gal::LdapFieldMap::LdapFieldMap+0x1
03a2fce0 01b6fa78 5d82a5d3 mailserver!kerio::mailserver::services::gal::LdapClient::LdapClient+0x5f
5d82a7e3 0253ea70 0253eae0 mailserver!kerio::mailserver::services::gal::SynchronizeRequest::process+0x
00000001 02541034 02547e80 mailserver!kerio::mailserver::services::PoolControlled::Thread::processRequ
00000001 0253ea74 00000000 mailserver!kerio::mailserver::services::PoolControlled::Thread::process+0x1
7c919af0 0342fb70 03a2ffac mailserver!kerio::mailserver::services::ThreadControlled::run+0x107
781329bb 0253ea70 5d973f0b mailserver!kerio::mailserver::services::ThreadControlledImpl::runMe+0x52
0253ea70 5d973f0b 7c919af0 mailserver!exec_handler+0x9
0342fb70 7c80b683 02545c08 msvcr80!_endthreadex+0x3b
02545c08 7c919af0 0342fb70 msvcr80!_endthreadex+0xc7
781329e1 02545c08 00000000 kernel32!BaseThreadStart+0x37
Ln 0, Col 0 Sys 0:c:\Keri Proc 000:dc Thrd 022:6d4 ASM OVR CAPS NUM

Visual Studio

- snadné a jednoduché ovládání
- post-mortem analýza je prakticky shodná s debuggováním během vývoje aplikace
- lze zprovoznit se symbol serverem
- přehledné zobrazení zdrojového kódu (syntax highlighting)
- přehledné zobrazení lokálních proměnných, STL kontejnerů
- chybí některé speciální funkce (např. procházení heapu)


user (Debugging) - Microsoft Visual Studio
File Edit View Project Debug Tools Test Window Community Help
ldapfieldmap.cpp logproducer.cpp galserviceimpl.cpp Disassembly
(Unknown Scope)
void GalServiceImpl::logError(const char *module, const char *format, va_list argptr) const
/***/
bool Log::vlog(const char *format, va_list args)
{
char buffer[MAX_STR_LOG_LENGTH];
kerio::utils::vsnprintfx(buffer, MAX_STR_LOG_LENGTH, format, args);
Locals
Name Value Type
this 0x00000000 {defaultParams=[...]() isConfigured_=??? lastLine={...} ...} kerio::log
format 0x03a2c714 "%s: Cannot open LDAP map file c:\program files\kerio\mailserver/ldapmap/ads_gal.map" const cha
args 0x03a2c92c "Cannot open LDAP map file c:\program files\kerio\mailserver/ldapmap/ads_gal.map" char *
buffer 0x03a2c2f4 "" char [102
guard {mutex=0x00000010 } kerio::tin
Autos Locals Memory 1 Threads Modules Watch 1 Find Results 1
Threads
ID Name Location Priority Suspenc
1732 exec_handler kerio::mailserver::services: Normal 0
1736 listen_thread listen_thread Normal 0
1740 KThreadPool::managerThread kerio::tiny::KCond::doTime Normal 0
1744 KThreadPool::managerThread kerio::tiny::KCond::doTime Normal 0
1748 kerio::mailserver::services::gal::Sync kerio::log::Log::vlog Normal 0
Call Stack
Name Lang
msvcr80.dll!7817877f()
mailserver.exe!kerio::log::Log::vlog(const char * format=0x03a2c714, char * args=0x03 C++
mailserver.exe!log_error_v(const char * module=0x00b6c974, const char * format=0x00 C++
mailserver.exe!log_error(const char * module=0x00000000, const char * format=0x03a2 C++
mailserver.exe!kerio::mailserver::services::gal::GalServiceImpl::logError(const char * moc C++
mailserver.exe!kerio::mailserver::common::LogProducer::log_error(const char * module= C++
mailserver.exe!kerio::mailserver::services::gal::LdapFieldMap::load(const std::basic_strin C++
Autos Locals Memory 1 Threads Modules Watch 1 Find Results 1
Ready
Ln 104 Col 1 Ch 1 INS

Linux, Mac OS X



- symbol table je součástí spustitelného souboru
  - parametr gcc –g
  - z distribuovaného souboru se odstraní (strip)
- nástroje
  - gdb, strings, strace
- je třeba přesně znát verzi produktu a OS
- core dump generuje přímo systém (kernel)
  - ‘ulimit –c unlimited’
  - ukládá se do pracovního adresáře nebo /cores
- Mac: CrashReporter, Intel, PowerPC

GDB

- velmi mocný debugger
- CLI interface
- skriptovatelný
- podporuje různé architektury (-oah pro PPC)
- je nutné mít přesnou verzi binárky produktu
- stejné verze sdílených knihoven jako u zákazníka
- obdobné možnosti jako u WinDBG

```
[root@kms-rhel4 ~]# gdb mailserver core.32205
GNU gdb Red Hat Linux (6.3.0.0-1.153.el4_6.2rh)
This GDB was configured as "i386-redhat-linux-gnu"...add symbol table from file
"/root/.gdb/StlStdContainers.o" at

Reading symbols from /lib/libpthread.so.0...done.
Loaded symbols for /lib/libpthread.so.0
Reading symbols from /usr/lib/libz.so.1...done.
Loaded symbols for /usr/lib/libz.so.1

Core was generated by `/opt/kerio/mailserver/mailserver /opt/kerio/mailserver'.
Program terminated with signal 11, Segmentation fault.
#0  0x081e83ef in imap_handler (con=0x4) at /Autobuild/Builds/KMS-6426-
XfQAOzR/autobuild/mailserver/wrmail/mail_imaps.cpp:7389
        in /Autobuild/Builds/KMS-6426-XfQAOzR/autobuild/mailserver/wrmail/mail_imaps.cpp

(gdb) where
Thread 1 (process 8512):
#0  0x081e83ef in imap_handler (con=0x4) at /Autobuild/Builds/KMS-6426-
XfQAOzR/autobuild/mailserver/wrmail/mail_imaps.cpp:7389
#1  0x080ae84b in KServerTask::handler (this=0xacdc0c20) at /Autobuild/Builds/KMS-6426-
XfQAOzR/autobuild/mailserver/wrmail/services.cpp:172
#2  0x0809935e in KThreadPool::workerThread (workerThreadParamPtr=0xabf74fb8) at
/Autobuild/Builds/KMS-6426-
XfQAOzR/autobuild/BUILD/libs/common/external/include/boost/shared_ptr.hpp:252
#3  0x08b781fc in thread (ptr=0x975bd320) at /Autobuild/Builds/KMS-6426-
XfQAOzR/autobuild/BUILD/libs/common/internal/src/libs/libtiny/Thread.cpp:138
#4  0x00c2d45b in start_thread () from /lib/libpthread.so.0
#5  0x00b84c4e in iopl () from /lib/libc.so.6
#6  0x78362b90 in ?? ()
```

Kroky analýzy

- nalezení příčiny pádu
  - zkoumání callstacku a proměnných (i v jiných vláknech)
  - registry, obsah paměti, assembler
- někdy poměrně obtížné (corrupted heap) a nejednoznačné - čím víc dumpů, tím lépe
- hledání společných znaků
  - přesná verze OS, počet procesorů
  - další instalovaný SW, možné konflikty
- simulace, reprodukování problému
- spuštění procesu s debuggováním
  - gflags, malloc debugging, PageHeap

Problémy z praxe

- Nemám tabulku symbolů.
- Jak zjistit z jakého OS dump pochází?
- O jakou verzi produktu se jedná?
- Při pádu se nevytvoří žádný dump.
- Crashující thread nemusí být ten pravý.
- Optimalizace kompileru, inline funkce, šablony, makra.
- Poslední funkce na stacku zpravidla není ten problém.
- Jak to, že to padá jen na Linuxu/Windows/etc.?

Zajímavé tipy a triky 1.

Kontrola integrity souboru.

```
 !chkimg mailserver -d
00675582-00675583 2 bytes - mailserver!kerio::crypto::KLicenseManager::load_license+be2
[ 0f 84:90 e9 ]
006759f7-006759fb 5 bytes - mailserver!kerio::crypto::KLicenseManager::load_license+1057 (+0x475)
[ e8 b4 dd ff ff:b8 00 00 00 00 ]
00675a99-00675a9c 4 bytes - mailserver!kerio::crypto::KLicenseManager::load_license+10f9 (+0xa2)
[ 66 ff ff ff:00 00 00 00 ]
11 errors : mailserver (00675582-00675a9c)
```

Zjištění verze OS

```
 vertarget
Windows XP Version 2600 (Service Pack 2) UP Free x86 compatible
Product: WinNt, suite: SingleUserTS
kernel32.dll version: 5.1.2600.2180 (xpsp_sp2_rtm.040803-2158)
Debug session time: Tue Sep 9 08:31:21.000 2008 (GMT+2)
System Uptime: 0 days 2:35:43.656
Process Uptime: 0 days 0:01:19.000
Kernel time: 0 days 0:00:05.000
User time: 0 days 0:00:01.000
```

Zajímavé tipy a triky 2.

Process Environment Block

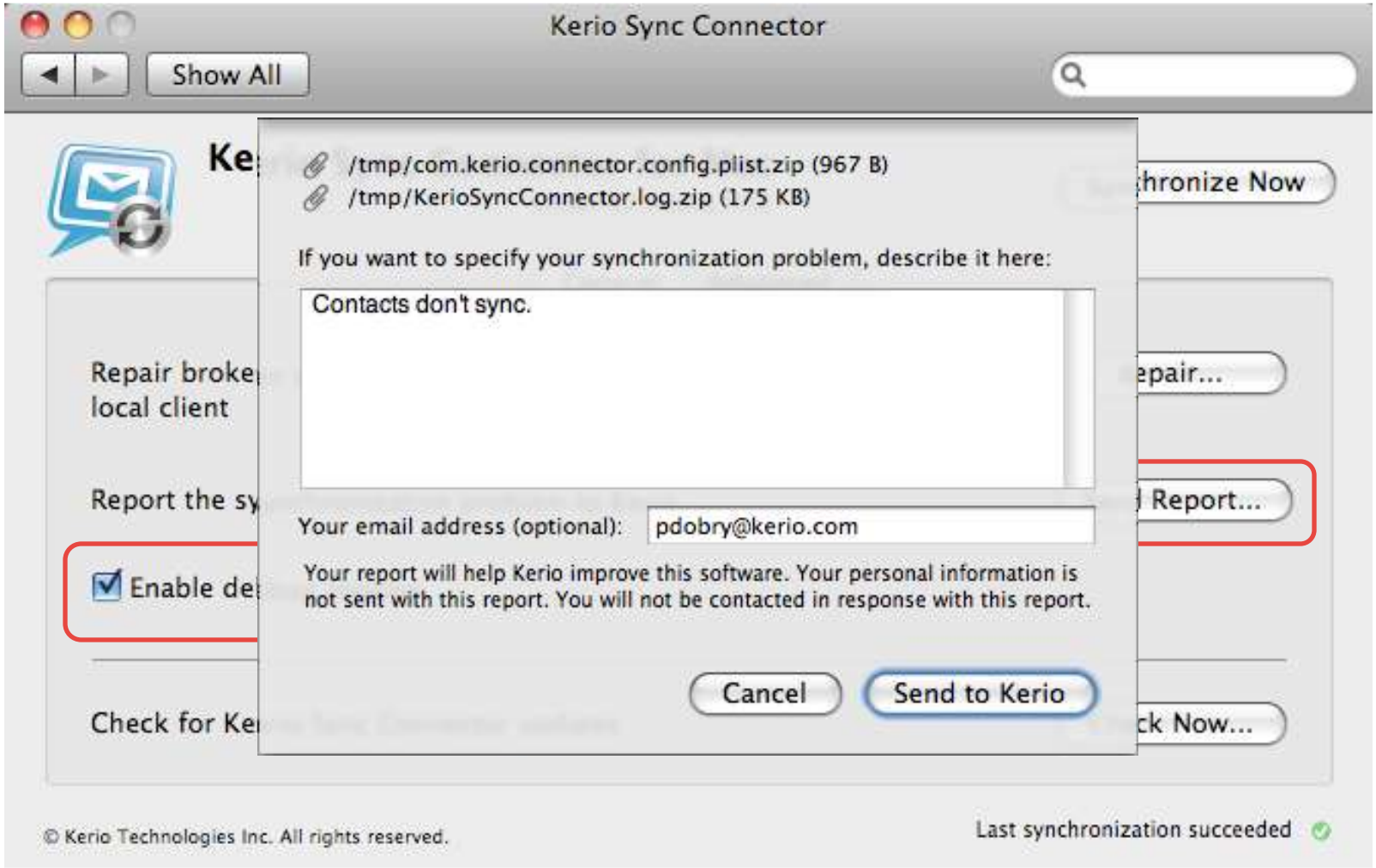
```
 !peb
PEB at 7ffde000
InheritedAddressSpace: No
ReadImageFileExecOptions: No
ImageBaseAddress: 00400000
Ldr 00241e90
Ldr.Initialized: Yes
Base TimeStamp Module
400000 44f41555 Aug 29 12:22:13 2006 C:\Program Files\Kerio\MailServer\mailserver.exe
7c900000 411096b4 Aug 04 09:56:36 2004 C:\WINDOWS\system32\ntdll.dll
76bf0000 411096ca Aug 04 09:56:58 2004 C:\WINDOWS\system32\psapi.dll
ProcessHeap: 00140000
ProcessParameters: 00020000
CommandLine: '"C:\Program Files\Kerio\MailServer\mailserver.exe"'
COMPUTERNAME=WINGATE
ComSpec=C:\WINDOWS\system32\cmd.exe
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 15 Model 2 Stepping 9, GenuineIntel
PROCESSOR_LEVEL=15
PROCESSOR_REVISION=0209
SystemRoot=C:\WINDOWS                                          (zkráceno)
```

Klientské aplikace

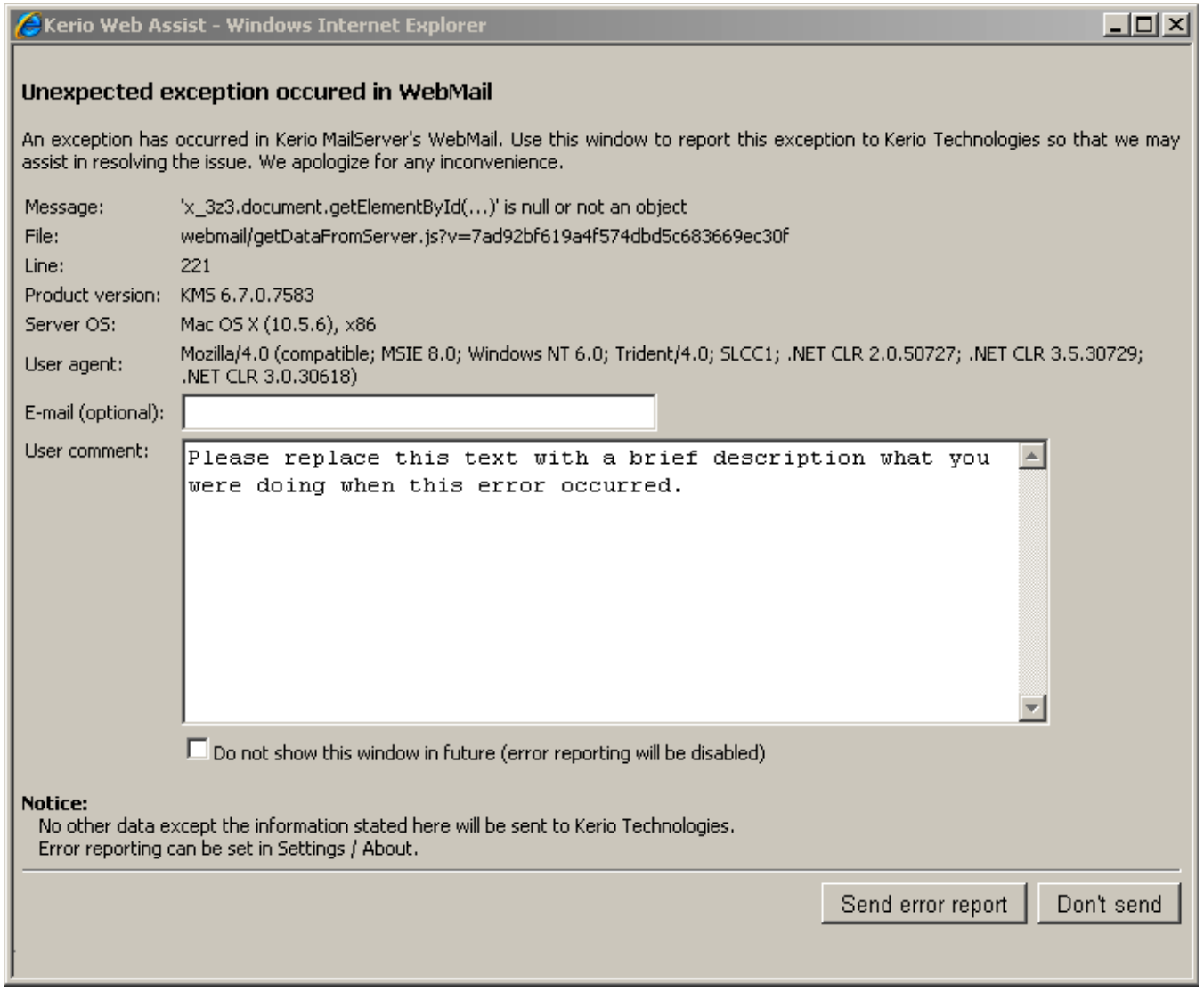
- Chceme se dozvědět o všech problémech, které mají koncoví uživatelé
- Chyby vetšinou nehrožují hlavní aplikaci, ale jsou pro uživatelé “otravné”.

- Může se lišit podle typu aplikace
  - Samostatně spustitelné aplikace
    - crashe, divné chování
  - Webové aplikace
    - javascript chyby, nečekané stavy

Spustitelné aplikace



Webové aplikace

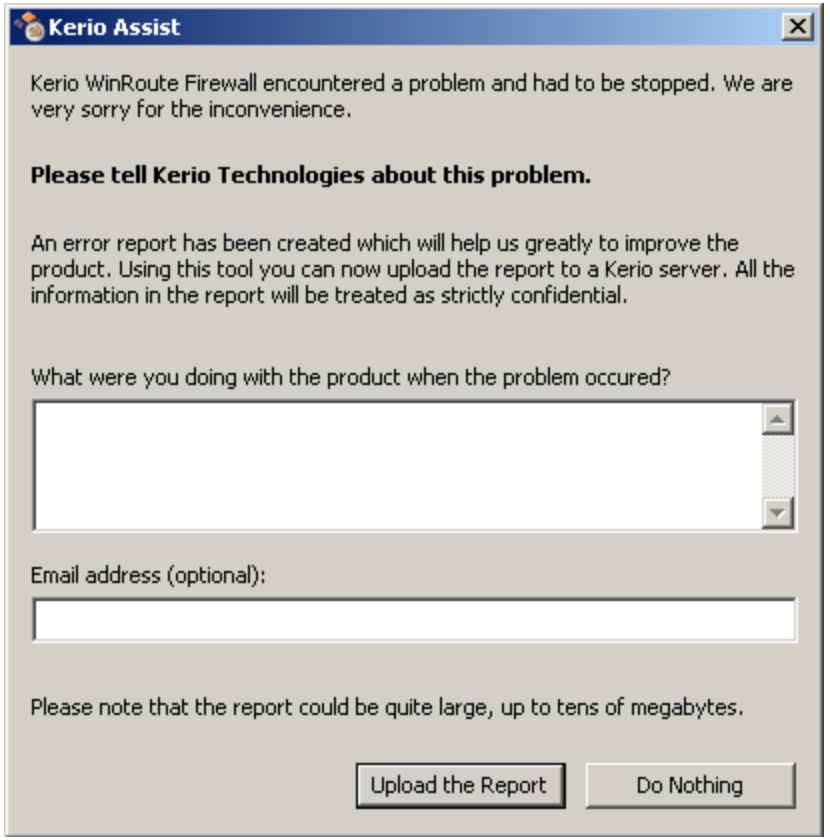


Motivace pro automatizaci

- chceme dump co nejdříve
  - čím dříve bude chyba odstraněna, tím menší bude mít dopad
- chceme co nejvíce dumpů
  - z více dumpů se snáze odhalí chyba
  - telefonická podpora vs. anonymní upload
- chceme mít co nejméně práce
- pozitivní vliv na zákazníka
  - „Dobrý den, včera Vám spadl mailserver, víme čím to je.“

Vznik a odeslání crashdumpu

- součástí balíku aplikace utilita assist
  - detekuje a zachytí pád aplikace
  - restartuje aplikaci
  - odešle informace na FTP server
  - provádí analýzu OS
  - po naběhnutí OS analyzuje kernel memory dump



Příjem crashdumpu

- FTP server
- 1x denně zpracování příchozích souborů
- rozdělení podle produktů

Zpracování crashdumpu

- 1x denně staženy dumpy analyzátorem
- Perlové skripty
- rozdělení podle komponent
- analýza pomocí kd (řádkový debugger, součást WinDBG) + extension pro Kerio produkty
- zpracování výstupního logu
- odeslání výsledků na prezentační server
- odeslání přehledového emailu

```
!kwfkd.delim
!analyze -v
!kwfkd.delim
!chkimg mailserver -d
!kwfkd.delim
...
!kwfkd.delim
q
```

Uchovávání a prezentace výsledků

- WWW server + databáze
- přijímá výsledky od analyzátoru, ukládá je do databáze
- prezentační rozhraní
  - poznámky
  - vyhledávání

KERIO

CD Upload | Show uploaded | Search

Show CD# 70114 Show

September 2008						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30				

<< today >>

Only product: KWF
Show: All
Type: All
Release: All

Engine	70114	KWF-6.5.0
Engine	70113	KWF-6.5.0
AV-Serv	70112	KWF-6.4.2
AV-Serv	70111	KWF-6.4.2
Service	70109	KWF-6.1.4
Service	70108	KWF-6.1.3

KWF-6.5.0

ID	70114
Release	Beta
Type	Engine
UUIN	54134927-07D9-0AA6-3B81-5B5B09FE
File info	KWF-6.5.0-BUILD-4794-WIN-ENGINE
Uploaded	2008-09-19 04:03:00
Last change	2008-09-19 04:03:00
Result URL	http://fin.kerio.local/kcd/view.php?id=70114
Archive	Get from FTP

Crash info

Customer comment:
Winroute crashed after several days.
Customer e-mail:
kburns@meddowsecurity.com
Customer upload time:
18/09/2008 17:25:57
Dump archive size:
32791394 B

Analyze

Click to collapse

- **!analyze -v**
- **!chkimg -d WinRoute**
- **!kwfkd.testBug10250**
- **!kwfkd.ctracktab**
- **!kwfkd.license**
- **!kwfkd.uptime**
- **vertarget**
- **.ecxr**
- **kb**

```
*** Stack trace for last set context - .thread/.cxr resets it
ChildEBP RetAddr Args to Child
1704ff18 00422795 000ce0ef 008bbf04 77e6bb9d winroute!DnsResolver::resendQueries+0x2d4
1704ff3c 004228c2 1704c991 00000000 12d79978 winroute!wrTimerUnlocked+0x375
1704ff60 00636e78 00000000 00000000 00000000 winroute!wrTimerThread+0xf2
1704ff78 781329bb 12d79978 0f4596e3 00000000 winroute!kerio::tiny::thread+0x48
1704ffb0 78132a47 00000000 77e6608b 12d79b30 msvcr80!_endthreadex+0x3b
1704ffb8 77e6608b 12d79b30 00000000 00000000 msvcr80!_endthreadex+0xc7
WARNING: Stack unwind information not available. Following frames may be wrong.
1704ffec 00000000 781329e1 12d79b30 00000000 kernel32!GetModuleFileNameA+0xeb
```

- **!kwfkd.sc /disasm**
- **!peb**
- **!kwfkd.debug10038**

Flags

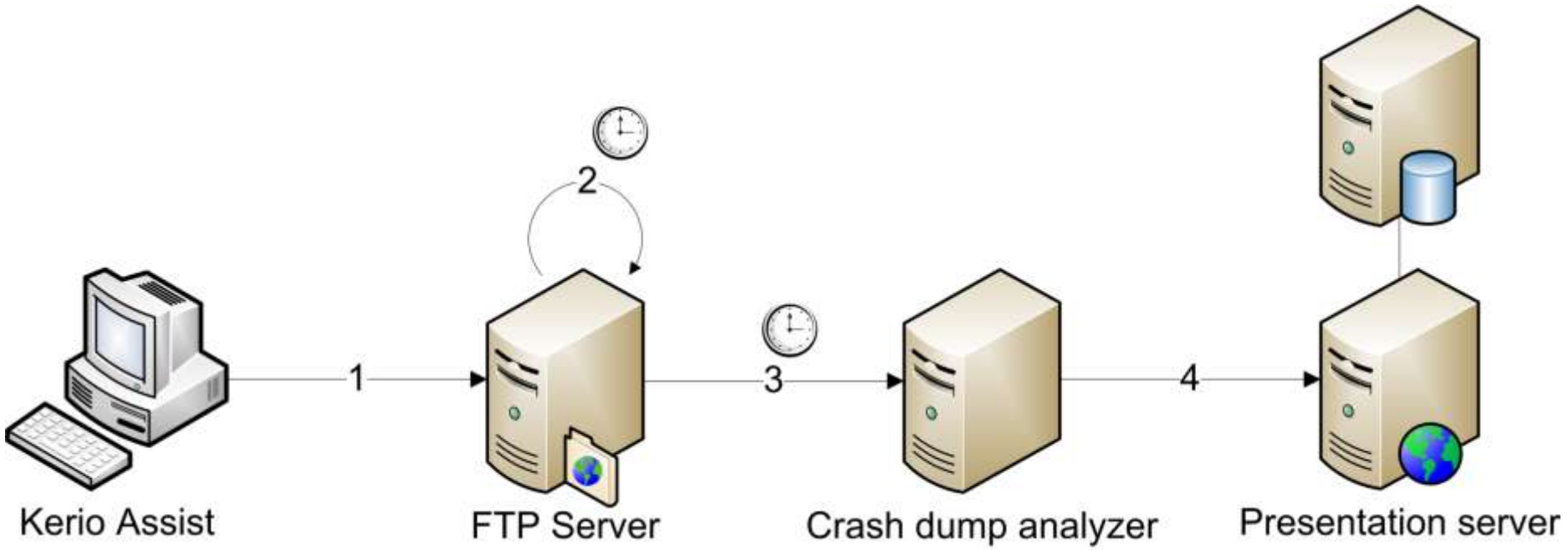
Solved Cracked

Bugzilla bug #:

Internal comments

Official comments

Komponenty systému - shrnutí

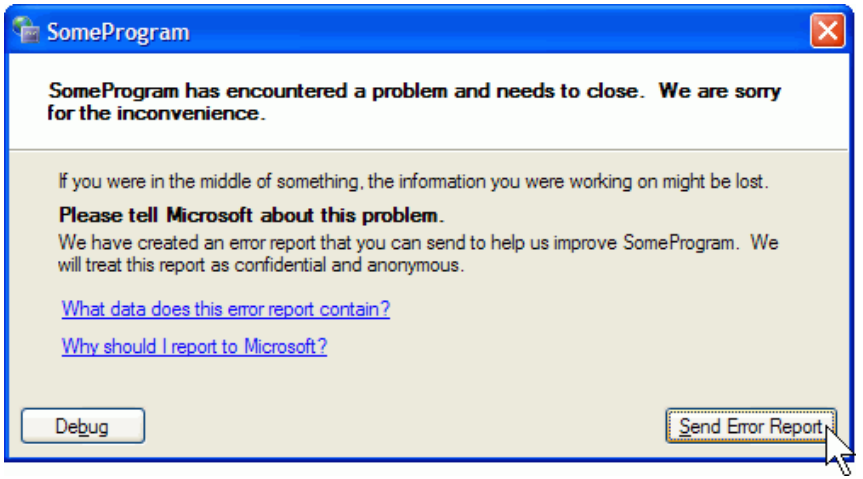


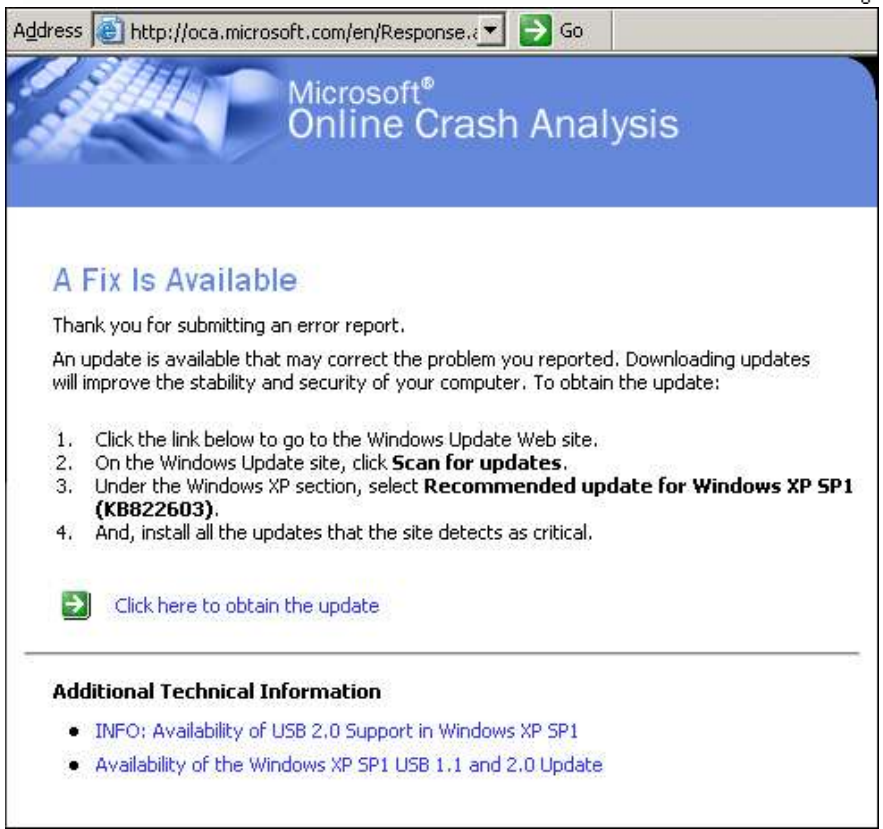
Budoucnost systému

- fetch -> push
- konsolidace výsledků podle callstacku
- assist z desktopu do administrační konzole
- automatická zpětná vazba k zákazníkovi

Alternativy

- Windows Logo Program, Windows Error Reporting
- odešle popis + minidump
- server sdružuje dumpy podle callstacku
- udržuje statistiky
- popis řešení zpět až k uživateli
- registrace zdarma





Závěr

- crashe byly, jsou a vždy budou
- počítejte s nimi, buďte připraveni
- připravte si potřebná data už za běhu programu
  - zohledněte při návrhu a implementaci
  - ‘***Coredump 6.2.2.4262***’

- Když se o problému nedozvíte, nemůžete jej vyřešit.
- Proaktivní přístup se vyplácí.
- Velký prostor pro automatizaci. Nechte hrubou práci strojům.

Odkazy

Debugging and Error Reporting (Windows)
http://msdn.microsoft.com/en-us/library/ms679300(VS.85).aspx
Crash Dump Analysis and Debugging Portal
http://www.dumpanalysis.org/
Debugging Tools for Windows – WinDbg
http://www.microsoft.com/whdc/devtools/debugging/default.mspx
Debugging with GDB
http://sourceware.org/gdb/current/onlinedocs/gdb_toc.html
Microsoft Winqual
https://winqual.microsoft.com

Otázky ?

Děkuji za pozornost !