



Crash, Recovery, Logging Pertemuan 13



Crash

- Terjadi ketika program komputer seperti software atau sistem operasi berhenti berfungsi dan keluar (dirty exit)
- Jika program yang crash adalah program kritis sistem operasi dapat berakibat
 - Hang
 - Kernel Panic
 - Fatal System Error

System Failure: cpu=0; code=00000007 (Corrupt skip lists)w Help

Latest crash info for cpu 0:

Exception state (sv=0x3F099000)

PC=0x000A3D74; MSR=0x00001000; DAR=0x01328C90; DSISR=0x40000000; LR=0x0009D

Backtrace:

0x00000000 0x0009A39C 0x00099118 0x000627F0 0x000A875C 0x000ABC80

backtrace terminated - frame not mapped or invalid: 0xF0100CB0

Proceeding back via exception chain:

Exception state (sv=0x3F099000)

PC=0xFFFF9230; MSR=0x0200D030; DAR=0x053B2000; DSISR=0x40000000; LR=0xFFFF91

Kernel version:

Darwin Kernel Version 8.3.0: Mon Oct 3 20:04:04 PDT 2005; root:xnu-792.6.22.obj~2

Memory access exception (1,0,0)

ethernet MAC address: 00:11:24:71:0a:f2

ip address: 66.130.136.28

Waiting for remote debugger connection.

Message 1

From: Agean

Hi, lilithlucas [logout]

New Messages

MESSAGES

Inbox: 148

Drafts: 0

Sent: 106



Penyebab

- Nilai Address yang tidak benar di Program Counter
- Buffer overflow
- Menulis sebagian kode program karena bug
- Mengakses memori yang tidak valid
- Menggunakan opcode ilegal
- Dan program exception



Jenis Crash

- Aplikasi Crash
 - Crash ke Desktop
- Sistem Operasi Crash



Aplikasi Crash

- Disebabkan oleh aplikasi yang melakukan operasi yang tidak diizinkan sistem operasi
- Aplikasi Unix/Unix-like akan membuat dump core
- Aplikasi Windows dan Unix GUI akan mengeluarkan dialog error



Tipe Error Aplikasi

- Mengakses memory yang tidak dialokasikan (segmentation fault)
- Mengakses level lebih tinggi
- Mengakses perangkat I/O tanpa hak akses
- Mencoba untuk mengeksekusi perintah yang buruk



Crash ke Desktop

- Hal tipikal yang terjadi ketika aplikasi layar penuh (fullscreen) tiba-tiba kembali ke desktop tanpa ada error yang jelas
- Cara mudah untuk mendeteksi error adalah menggunakan mode Window
- Menggunakan logger dari Aplikasi itu sendiri



Sistem Operasi Crash

- Crash yang muncul karena Hardware Exception dan tidak bisa ditangani
 - Power Failure
 - Driver Hardware
 - Kesiram Kopi
- Bisa juga dikarenakan file-file dari sistem sudah tidak lagi konsisten / korup



Lanjutan

- Sistem Operasi modern (Linux dan MacOS) biasanya tidak akan mengalami kerusakan ketika ada aplikasi yang rusak
- Sistem operasi z/OS memiliki kemampuan untuk Realibility sehingga SO dapat memperbaiki dari Crash Komponen Penting

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

Your computer restarted because of a problem. Press a key or wait a few seconds to continue starting up.


Votre ordinateur a redémarré en raison d'un problème. Pour poursuivre le redémarrage, appuyez sur une touche ou patientez quelques secondes.

El ordenador se ha reiniciado debido a un problema. Para continuar el arranque, pulse cualquier tecla o espere unos segundos.

Ihr Computer wurde aufgrund eines Problems neu gestartet. Drücken Sie zum Fortfahren eine Taste oder warten Sie einige Sekunden.

問題が起きたためコンピュータを再起動しました。このまま起動する場合、いずれかのキーを押すか、数秒間そのままお待ちください。

电脑因出现问题而重新启动。请按一下按键，或等几秒钟以继续启动。



```
grsec: use of CAP_SYS_ADMIN in chroot denied for /sysroot/sbin/load_policy[load_
policy:2601 uid/euid:0/0 gid/egid:0/0, parent /init[init:1] uid/euid:0/0 gid/egi
d:0/0
grsec: use of CAP_SYS_ADMIN in chroot denied for /sysroot/sbin/load_policy[load_
policy:2601 uid/euid:0/0 gid/egid:0/0, parent /init[init:1] uid/euid:0/0 gid/egi
d:0/0
dracut: FATAL: Initial SELinux policy load failed. Machine in enforcing mode. To
  disable selinux, add selinux=0 to the kernel command line.
dracut: Refusing to continue
```

```
Kernel panic - not syncing: Attempted to kill init!
```



Apa itu Crash Recovery?

- Ketika kamu membuat file
- Kemudian power failure dan reboot
- Apakah file tersebut bisa diakses kembali?



Crash Recovery

- Sebuah kegiatan yang dilakukan Sistem Operasi secara otomatis maupun oleh Pengguna untuk mengembalikan sistem seperti semula
- Sistem Operasi akan mengecek apakah File System dalam keadaan bersih via Journal nya



Lanjutan

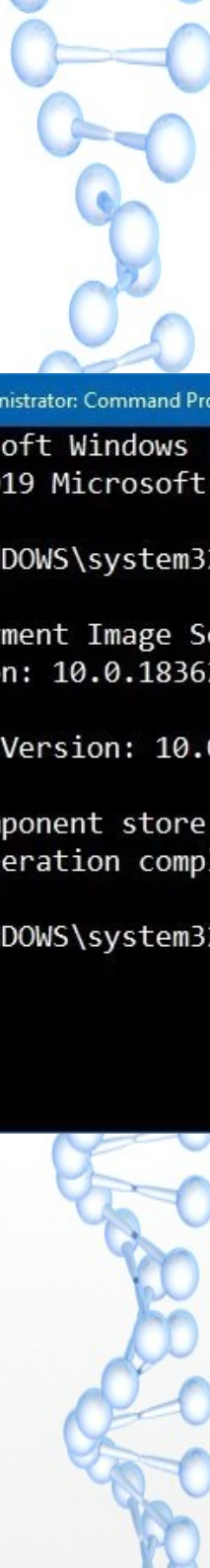
- Pengguna dapat melakukan recovery dengan memerintah Sistem Operasi melakukan pemulihan sistem file yang rusak
- System File Checker (Windows)
- Deployment Image Servicing and Management/DISM (Windows)



SFC

```
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Windows\system32>sfc /scannow  
  
Beginning system scan. This process will take some time.  
Beginning verification phase of system scan.  
Verification 2% complete.
```

DISM



```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.18362.113]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>DISM /Online /Cleanup-Image /CheckHealth

Deployment Image Servicing and Management tool
Version: 10.0.18362.1

Image Version: 10.0.18362.113

No component store corruption detected.
The operation completed successfully.

C:\WINDOWS\system32>
```




Backup and Restore

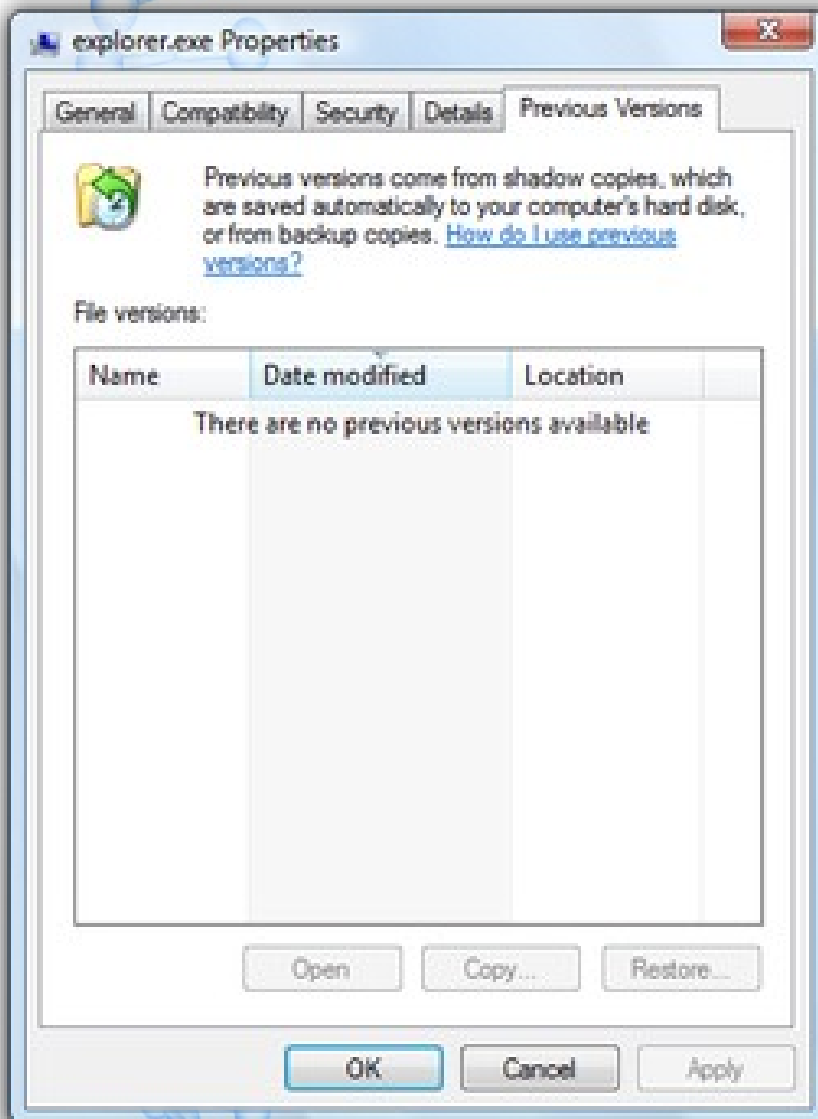
- Sebuah teknik untuk melakukan pengamanan data secara mudah
 - Shadow Copy/Snapshot
 - Bare Metal Restore/Clone



Shadow Copy / Snapshot

- Dikenal sebagai Volume Snapshot Service sebuah teknologi dari Ms Windows yang dapat melakukan backup secara otomatis maupun manual
- Mengandung informasi dari suatu sistem di suatu waktu
- Di MacOS dikenal dengan TimeMachine nya

Lanjutan





Plus Minus Shadow Copy

- + File terbackup secara kronologis
- + Bisa dikembalikan sesuai waktu tertentu
- + Bersifat Incremental
- - Bersifat internal
- - Jika Disk korup maka backup juga bisa korup



Bare-Metal Restore

- Sebuah teknik mengembalikan sistem operasi seperti semula secara menyeluruh
- Sehingga pengguna tidak perlu lagi melakukan instalasi driver dan aplikasi lagi
- Bisa dilakukan di Sistem Operasi apapun



Lanjutan

- Tool yang digunakan bisa berupa
 - Disk Dump (DD)
 - Disk Clone
- Tool akan membaca semua informasi dari ujung ke ujung dan menyimpannya sebagai satu file berukuran besar



Plus Minus Bare-Metal Restore

- + Kemudahan Setelah Restore
- + Satu File memuat semua informasi yang ada
- + Bisa disimpan di HDD luar
- - Bisa berukuran raksasa >50GB
- - Ketika dikembalikan ukuran file < hd
- - Satu backup untuk satu waktu



Logging

- Kenapa butuh logging?
- Kita ingin semua yang dilakukan sistem terekam di sebuah file
- Jadi ketika crash apa yang telah dilakukan sistem hingga selesai bisa dilakukan kembali
- Biasanya digunakan di DB



Lanjutan

- Journaling juga bisa disebut sebagai Logging
- Merekam segala aktivitas yang belum di commit ke file system
- Bisa merekam meta-data saja maupun dengan data yang tersimpan



Jenis Journaling

- Physical Journal
 - Adalah kopian dari setiap block yang nantinya dituliskan ke file system
- Logical Journal
 - Hanya menyimpan metadata ke dalam jurnal dengan mengorbankan fault tolerance



Teknik Journaling EXT4

- File system EXT3/4 memiliki 2 mode dalam journaling
 - Ordered (Ordered Mode)
 - Writeback (Writeback Mode)
- Yang membedakan keduanya adalah Fault Tolerance dan Performance