From Unexpected Restart to Understand the System

By : Meylira Kagaya Eisenberg

Malam ini, tiba2 laptop mey nge-restart sendiri tanpa hang/pesan error yg biasa terjadi pada umumnya...lha setelah ditelusuri, berikut ini adalah jalan cerita log nya.... lognya mey potong yah.. langsung ke pokok masalah :D

========== log(1):log critical kernel-power.xml ==========

- <System>

<Provider Name="Microsoft-Windows-Kernel-Power" Guid="{331C3B3A-2005-44C2-AC5E-77220C37D6B4}" />

<EventID>41</EventID>

<Version>2</Version>

<Level>1</Level>

<Task>63</Task>

<Opcode>0</Opcode>

<Keywords>0x8000000000000002</Keywords>

<TimeCreated SystemTime="2011-07-14T16:31:17.696407300Z" />

<EventRecordID>6822</EventRecordID>

<Correlation />

<Execution ProcessID="4" ThreadID="8" />

<Channel>System</Channel>

<Computer>Elixiroflife</Computer>

<Security UserID="S-1-5-18" />

</System>

- <EventData>

<Data Name="BugcheckCode">0</Data>

<Data Name="BugcheckParameter1">0x0</Data>

<Data Name="BugcheckParameter2">0x0</Data>

<Data Name="BugcheckParameter3">0x0</Data>

<Data Name="BugcheckParameter4">0x0</Data>

<Data Name="SleepInProgress">false</Data>

<Data Name="PowerButtonTimestamp">0</Data>

</EventData>

</Event>

========== log(1)End ==========

Hmmmm.....sedikit analysis....

EventID 41 Task 63 [SystemTime] 2011-07-14T16:31:17.696407300Z

Dilihat lihat ada task jalan dari proses ber-id 4 ==> pada umumnya yang id kecil biasanya system.

Yup akhirnya ketemu juga keywordnya 0x8000000000000002 ==> kalau udah keyword tersebut error biasanya akan terjadi crash, restart atau bisa jadi BSOD ....hohohohoho... Tapi belum tentu juja karena “power kernel”.

==========

Selanjutnya cari tahu lebih detail lagi.... :D

Bisa langsung lihat log(2) ==> http://myfreefilehosting.com/f/407c105e5d_0.74MB

Ternyata win 7 yang mey pakai ini bermaksud memudahkan user untuk mengerti arti system restore... Yup, bahasanya diperhalus menjadi "backup". Padahal pada sistem operasi sebelumnya tidak didefinisikan sebagai backup.

Dalam pemrograman DOS kita mengenal istilah "shadow copy", jadi setiap kali kita buat/simpan file itu selalu ada shadow copynya tanpa kita sadari. Hal ini berhubungan dengan bahasan text log berikutnya yang menyangkut shadow copy.

Pada log(2) "<Channel>Application</Channel>" yang terkait untuk mengeksekusi system restore, yang dilanjutkan dengan :

<EventData><Data>Shadow Copy Optimization Writer</Data>

<Data>{4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}</Data><Data> < serial HD mey

lalu di baris berikutnya ternyata sudah 4x log me-record pengulangan untuk me-write shadow copy.

Terus disambung dengan adanya event lagi dari system :

<Provider Name="System Restore"/><EventID Qualifiers="0">8195</EventID><Level>4</Level>

Tapi eksekusi tersebut gagal... So, apa buktinya gagal???

Dalam event diatas terdapat string binary yang diekseskusi yaitu :

<Binary>000000008900000083000000000000004386252307000000000000000000000000000</Binary>

Ternyata yg keluar event selanjutnya adalah...

<System><Provider Name="Windows Error Reporting"/><EventID Qualifiers="0">1001</EventID><Level>4</Level><Task>0</Task>

Disinilah kekacauan dimulai.. fufufu...

Tapi, apakah benar error tersebut yang menyebabkan restart misterius pada laptop mey.. ?

Kembali pada log (2), pada string selanjutnya didapatkan :

<Data>0</Data><Data>PnPGenericDriverFound</Data><Data>Not available</Data><Data>0</Data><Data>x86</Data><Data>USB\VID_174F&PID_5216&REV_0326&MI_00</Data>

Mungkin ini adalah fungsi plugNplay yang lagi patroli, maklum wedhus a.k.a windows suka lupa klo udah pernah ketemu, maka ditanyain lah driver tersebut.

System tidak menemukan driver tersebut: <Data>Not available</Data> .. Lho emang kemana yah ??

Lalu disambung dengan report seperti ini

<Data>C:\ProgramData\Microsoft\Windows\WER\ReportQueue\NonCritical_x86_eb66e5f355ba4b67d37bdaadd59165e1cebbe026_cab_07c5f72a</Data>

Jadi inilah yang terjadi, waktu si system volume information itu bikin shadow kopi, dia minjem data asli. dalam waktu yang hampir bersamaan, ada yang nanyain tentang file tersebut, system bilangnya tidak ada (padahal lagi dipinjemin ke si shadow copy). Hal ini dimungkinkan karena task berjalan lambat karena adanya task yang menunggu dari aplikasi lain, coba perhatikan urutan lognya :D

Hemat! >,<

Jadi system restore bekerja dengan cara membuat backup yang simpan di folder beratribut system+hidden di setiap partisi HD, jika fungsi system restore diaktifkan maka proses read - write berjalan 2 kali lipat lebih berat dimana saat user menghapus/memodifikasi file maka system restore akan menulis log point, jika user membuat/menambah file maka system restore akan menambahkan file backup pada direktorinya, ditambah lagi kadang system restore bekerja di background untuk check read - write.

Walaupun memang user dapat menentukan point dan melakukan "backup"/setting point. Tapi proses penggandaan akan terus berlangsung dengan maksud backup oleh system yang dapat dijadikan user point berikutnya. Ditambah lagi karena aksesnya yang terbatas, menjadikan ada beberapa jenis virus/trojan/malware memanfaatkan celah ini (bagi pengguna format harddist FAT bisa melihatnya), celakanya bagi pengguna format harddisk NTFS folder ini sama sekali tidak bisa diakses!

Fufufu, backup cara lama lebih baik ternyata, lebih baik kita menyimpan data backup pada CD atau media lain dibandingkan memanfaatkan fitur system restore yang nyatanya menguras resource :'(

Setelah mey ingat-ingat, sepertinya ada system yg mirip cara kerja system restore. Yup, Recycle Bin! sebenarnya recycle bin terdapat pada semua partisi dan file yang dihapus dan dilarikan ke recycle bin dapat di restore karena datanya masih terdapat pada shadow volume.

Jika menilik pada sejarah perkembangan sistem operasi keluarga windows ternyata windows makin

mentutupi teknologi underdosnya, dengan menggunakan kata-kata ganti yang lebih user friendly, berbeda dengan keluarga nix* yang cenderung apa adanya. Seperti stilah "shadow copy", tentunya user interface tidak akan memuat kata-kata seperti itu, mungkin maksudnya supaya user mudah mengerti, karena keluarga windows diciptakan memang untuk unggul pada user interface, sesuai dengan pepatah 'akar yang kuat akan membuat batang yang kuat", karena console nix* tercipta dengan command console yang lebih rich dibanding wedhus underdos yang langsung melesat pada pengembangan interface, sampai2 wedhus pernah ingat pada hal tersebut dan membuat windows powershell :P coba lihat perkembangan *nix sekarang, kadang desktopnya anak2 yang pake ubuntu lebih “cling” dibanding wedhus user, malah bisa dibuat agar-agar kenyal.. lho ???

Maaf mey ngelantur kemana-mana, soalnya mey ngantuk waktu nulis ini.. Padahal cuma gara-gara laptop mey restart sendiri (_ _")

Greatz: bang leo retro yang mau nemenin mey diskusi mpe mata elek, keluarga laknat_na mey di facebook, penghuni priv8 server, and all my friends in this worlds :D

Now, waktunya ikan bobo zzzzZZZZ....

Meylira Kagaya .E =,='