Project 3 Pemeriksaan Forensic Registry Key dengan Regedit

Kebutuhan Project

- Komputer Windows, real atau virtual
- Komputer setidaknya pernah dikoneksikan dengan USB flashdisk sebelumnya
- Instruksi berikut menggunakan Windows 7

Pengenalan Registry

Registry memilki ribuan values yang digunakan untuk mengontrol setiap detail OS Windows, nilai value ini merekam berbagai informasi yang telah terjadi di komputer.

Regedit merupakan tool primer yang digunakan untuk memeriksa dan memodifikasi Registry pada komputer Windows. Pada projek berikutnya kita akan mengcapture registry dari komputer evidence, dan memeriksa file registry yang ditangkap. Tapi pada project ini kita belajar memeriksa live Registry komputer secara langsung, hanya untuk mempelajari keys-key paling penting yang perlu diperiksa.

Mengkoneksikan USB flashdisk di Komputer Windows 7 (Virtual)

1. Jalankan Komputer Windows Virtual.
2. Colokkan USB di komputer, agar flashdisk bisa terbaca di komputer Virtual. Di bagian bawah menu VirtualBox klik kanan gambar USB, kemudian centang Flashdisk yang terkoneksi (perhatikan pilih sesuai dengan merk dan jenis Flash disk).
3. Flashdisk bisa diakses menggunakan Windows Explorer.
4. Setelah selesai mengakses flashdisk, lakukan unmount flashdisk sperti biasa dilakukan di komputer Windows. Jangan lupa untuk membuang tanda centang untuk flashdisk yang selesai digunakan di baris bawah menu VirtualBox (seperti instruksi no. 2)

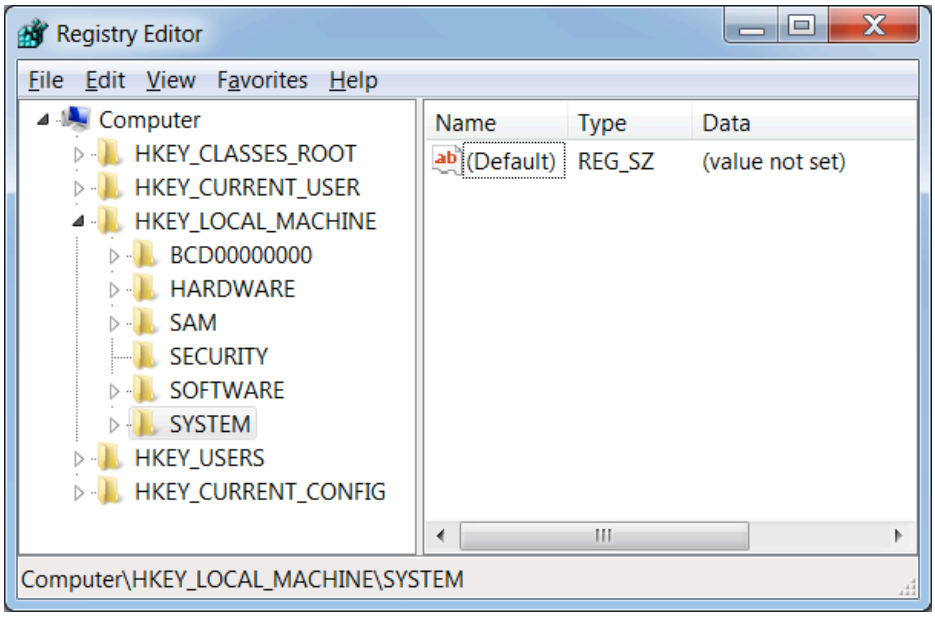
Membuat Restore Point di Komputer Windows 7

5. Regedit merupakan tools yang berbahaya untuk digunakan. Jika anda membuat kesalahan pada saat menjalankannya, maka saudara bisa merusak Windows OS di komputer. Sehingga perlu hati-hati, yang perlu dilakukan pertama kali adalah membuat restore point, yang akan membacks up file Registry dan semua file sistem.
6. Di komputer Windows 7, Click **Start**, dan ketikkan **RESTORE** pada kotak Search.
7. Click "**Create a Restore Point**".
8. Pada kotak "System Properties" box, click "**Create**".

9. PADA KOTAK "Create a restore point", masukkan nama "***NameKamu* - SebelumEdit registry**" dan click tombol **Create**. Tunggu sampai restore point berhasil dibuat.
10. Kotak pesan akan muncul yang berisi "The restore point was created successfully". Click **Close**.
11. Close "System Properties".

Menjalankan Regedit

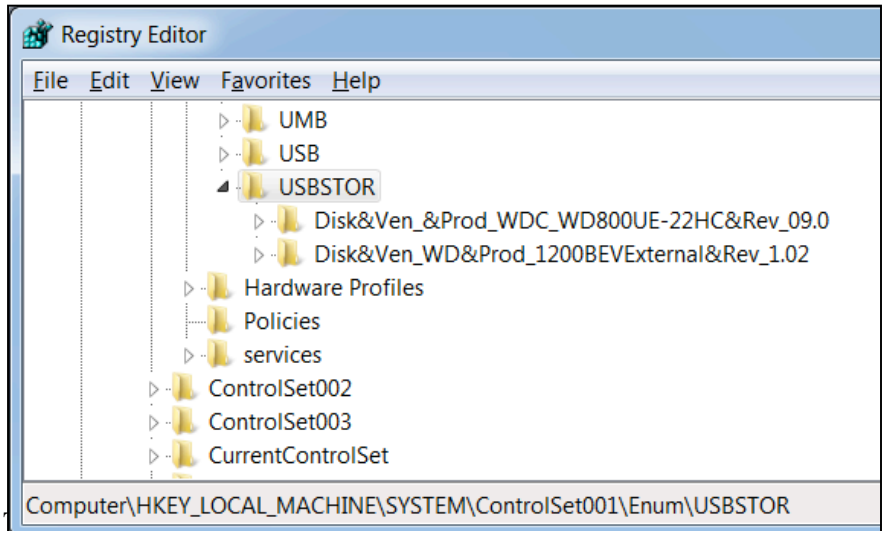
12. Click **Start**. Pada kotak pencarian, ketik REGEDIT dan tekan tombol Enter.
13. Regedit terbuka, seperti pada gambar di sebelah kanan.
14. Registry memiliki 5 **root keys** yang bernama:
    - HKEY_CLASSES_ROOT
    - HKEY_CURRENT_USER
    - HKEY_LOCAL_MACHINE
    - HKEY_USERS
    - HKEY_CURRENT_CONFIG



15. root keys tersebut sering disingkat menjadi HKCR, HKCU, HKLM, HKU, dan HKCC
16. "Folders" yang lain di sebelah kiri disebut **subkeys**, misalnya **HARDWARE**, **SAM**, and **SECURITY**. Dan item yang terlihat di sebelah kanan disebut **values**, misalnya **Default**.
17. Untuk menavigasi Registry hamper sama dengan menavigasi struktur folder dengan Windows Explorer.

USB Devices

18. Dalam forensic langkah ini merupakan langkah awal yang sebaiknya dilakukan (tapi tidak dilakukan langsung di komputer evidence… akan dijelaskan di project 3), karena bisa saja kita menemukan devices lain yang nantinya diperlukan

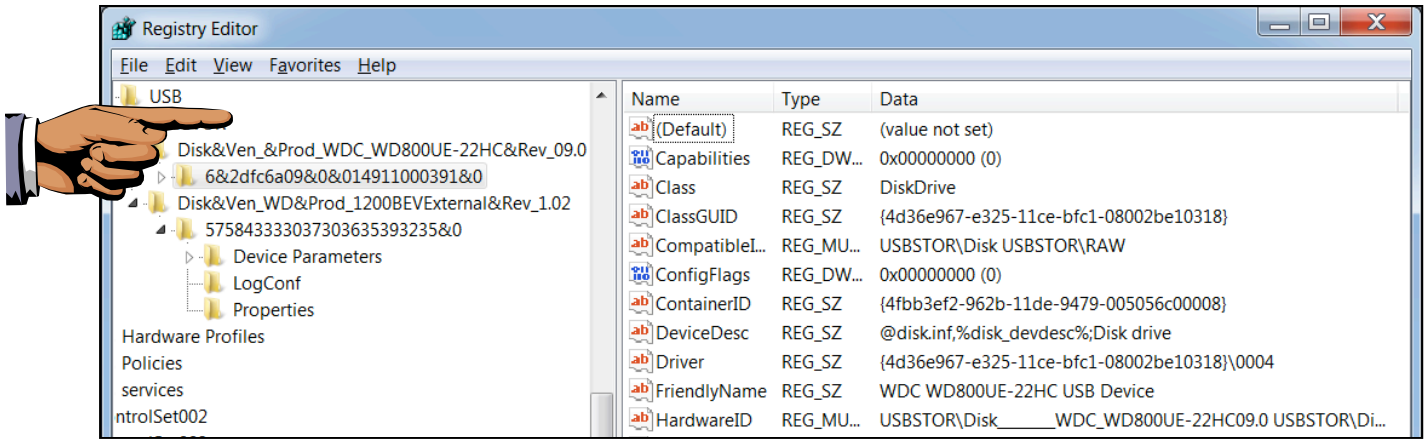


client(pihak kejaksaan penyidik) untuk diminta diselidiki, karena bisa saja devices tersebut merupakan barang bukti penting.

19. Navigasi ke **HKLM\SYSTEM\ControlSet001\Enum\USBSTOR**. Di sisi kiri panel Regedit, click segitiga untuk mengeksplorasi USBSTOR. *Jika tidak ada USBSTOR key, berarti komputer tidak pernah terkoneksi ke USB --colokkan USB drive dan click **View**, **Refresh**.*
20. Maka akan Nampak beberapa daftar USB devices yang terkoneksi ke komputer ini. Pada contoh di gambar, hanya ada dua devices.
21. Untuk melihat lebih detail, expand keys, dan click subkey yang pertama. Pada contoh yang diberikan, yang di-expanded (diperiksa) adalah USB device's key yang pertama, dan click subkey dengan nama panjang yang dimulai dengan "**6&2df**.."—ini merupakan device's serial number. Panel sebelah kanan memperlihatkan beberapa values yang bisa membantu mengidentifikasi devices tersebut, termasuk "FriendlyName" yang berisi informasi USB device's manufacturer dan model number.

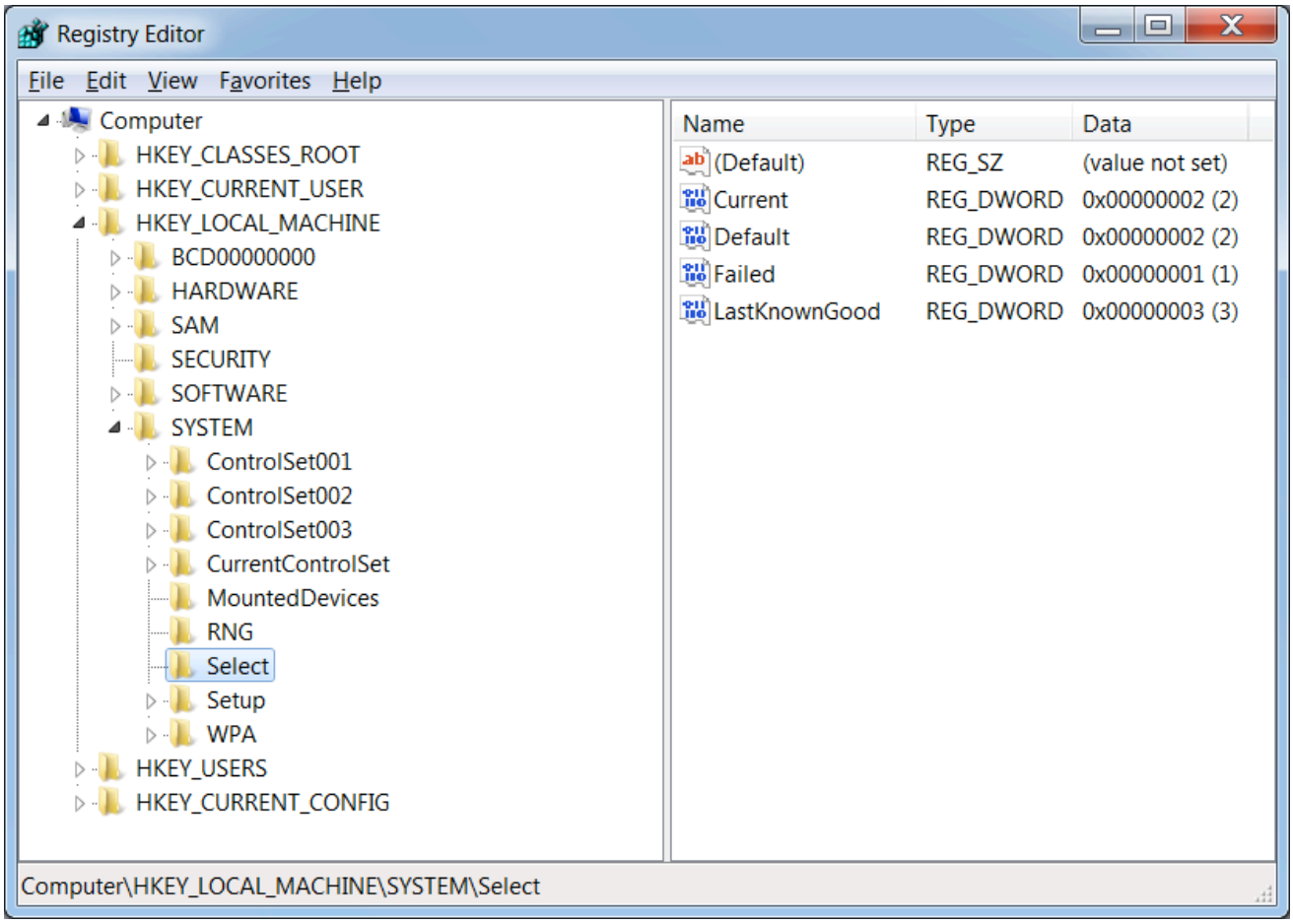
Simpan Screen Image

22. Pastikan di layar terlihat USB device's **FriendlyName**.
23. Tekan tombol **PrintScrn**. Simpan dengan nama **NamaKamu_ Proj2a**.



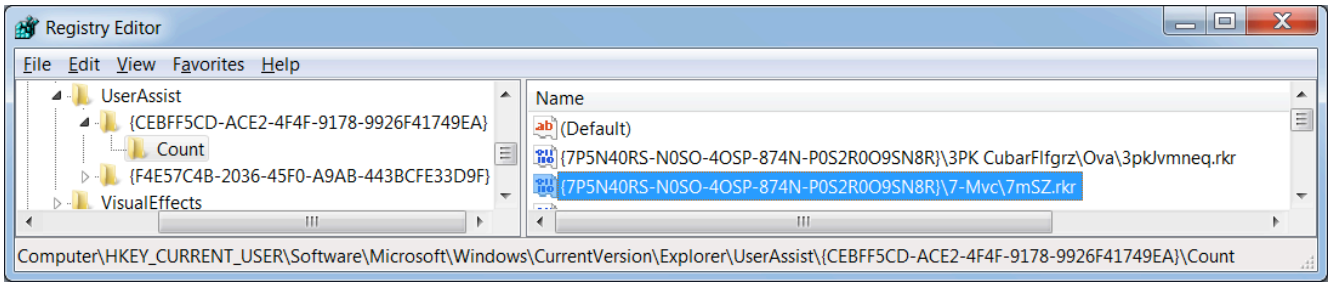
Memahami Control Sets

24. Perhatikan terdapat beberapa Control Set keys, ControlSet001, ControlSet002, dll. Untuk memahaminya, arahkan ke **HKLM\SYSTEM\Select**, seperti terlihat di bawah ini. Values di sini berisikan berisikan berbagai control sets –Lihat pada value Name dan Data di panel sebelah kanan. Maka akan terlihat control set aktual yang sedang digunakan (Current) adalah ControlSet002, dan ControlSet001 diset sebagai Failed set pada system yang dicoba di sini.



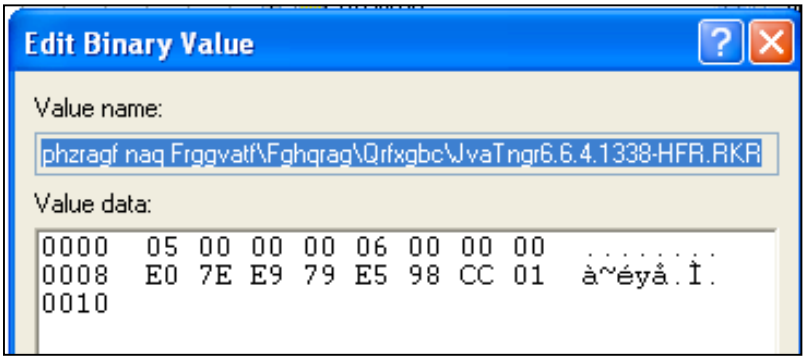
UserAssist

25. Arahkan ke **HCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist**. Pada panel sebelah kiri, periksa **UserAssist** key. Key ini memiliki dua atau lebih subkeys dengan nama yang panjang, seperti terlihat pada gambar di bawah. Peirksa satu dari subkey



tersebut, dan pilih **Count** subkey.

26. Pada sisi kanan, terdapat beberapa values dengan nama yang panjang. Double-click salah satunya, untuk membuka kotak "Edit Binary Value", seperti pada gambar sebelah kanan. Value Name berisikan nama dari aplikasi executable yang baru saja dijalankan user, periksa dengan metoda ROT-13. Coba untuk mencari value dengan ada tanda backslash di dalamnya, berarti value tersebut berisikan path direktori yang lengkap dan filename.



27. Untuk memecahkan data, sorot seluruh Value Name pada kotak "Edit Binary Value", klik kanan, dan click **Copy**.
28. Buka firefox atau browser yang lain dan buka situs **decode.org** (jika sudah down, cari di Google kata "ROT13 Decoder dan gunakan yang lain).
29. Paste teks tersebut pada kotak dan click tombol **Encrypt/Decrypt**.
30. Halaman ROT13 encoder/decoded dan click tombol "**Encode / Decode button**".

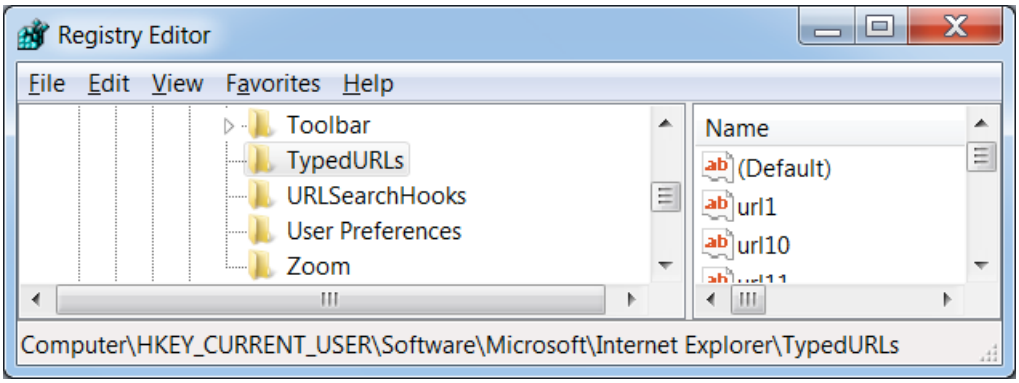
31. Maka akan terlihat path direktori, yang bisa berisi nama folder yang bisa dibaca seperti terlihat di gambar sebelaj sisi, atau nomor yang panjang (merupakan GUID). Pada contoh executable file yang dijalankan, adalah WinGate.

Simpan Screen Image

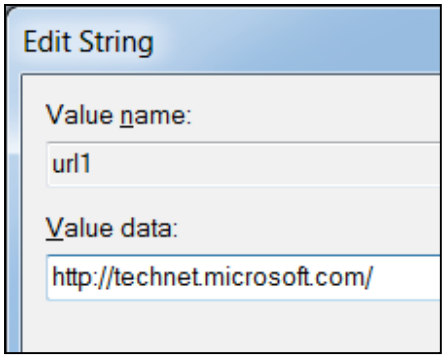
32. Pastikan di layar terlihat path folder executable's yang baru di baca pada ROT13 Encryptor & Decryptor.
33. Tekan **PrintScrn** key. Simpan dengan nama file **NamaKamu_Proj2b**.

URL Internet Explorer yang pernah dimasukkan

34. Navigasi ke **HKCU\Software\Microsoft\ Internet Explorer\TypedURLs**. Nilai di sini berisi **url1**, **url10**, dll. Yang berisi halam Web addresses yang pernah dimasukkan melalui Internet Explorer.



35. Di sisi kana, double-click satu dari **url** values.
36. Kotak "Edit String" muncul, seperti pada gambar sebelah kanan. Value data berisikan URL dalam bentuk plain text.



Simpan Screen Image

37. Perhatikan, pastikan layar memperlihatkan Web address pada kotak "Value data".
38. Tekan **PrintScrn** key. Beri nama **NamaKamu_ Proj 3c**.

Mengumpulkan Project

39. Kirim melalui elearning.

Sumber:

"A Forensic Analysis Of The Windows Registry", http://www.forensicfocus.com/a-forensic-analysis-of-the-windows-registry

Last Modified: 3-19-13