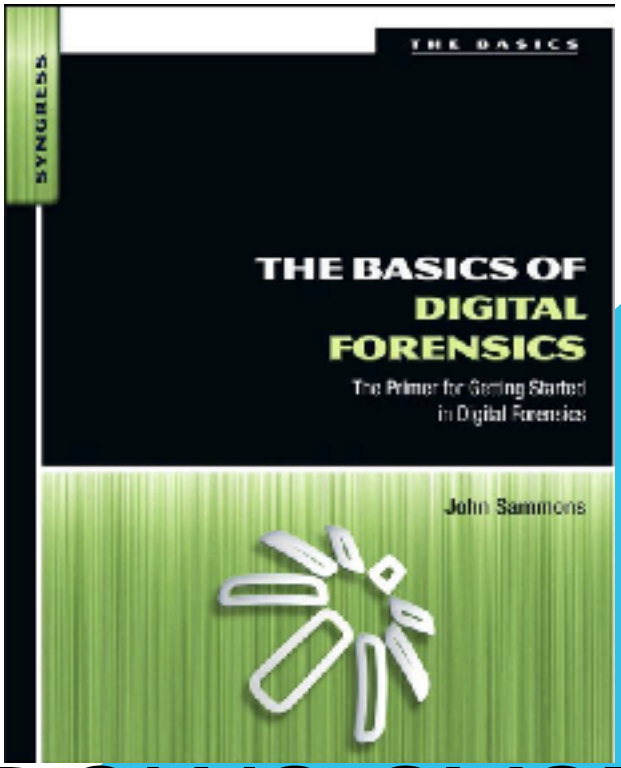


5. WINDOWS SYSTEM ARTIFACTS BAGIAN 1

TOPIK

- Mendelete data
- File Hibernation
- Registry

MENDELETE DATA

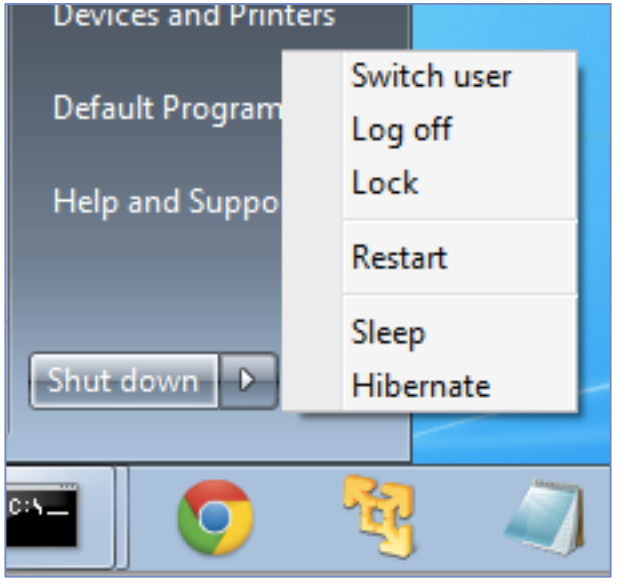
RECOVER DATA YANG DIDELETE

- File Carving
- Allocated space berisikan active data
- File yang didelete berada di unallocated space
- Tools yang bisa digunakan:
  - ProDiscover
  - FTK or EnCase
  - Foremost
  - Recuva
  - Photorec

FILE HIBERNATION

PILIHAN SHUTDOWN

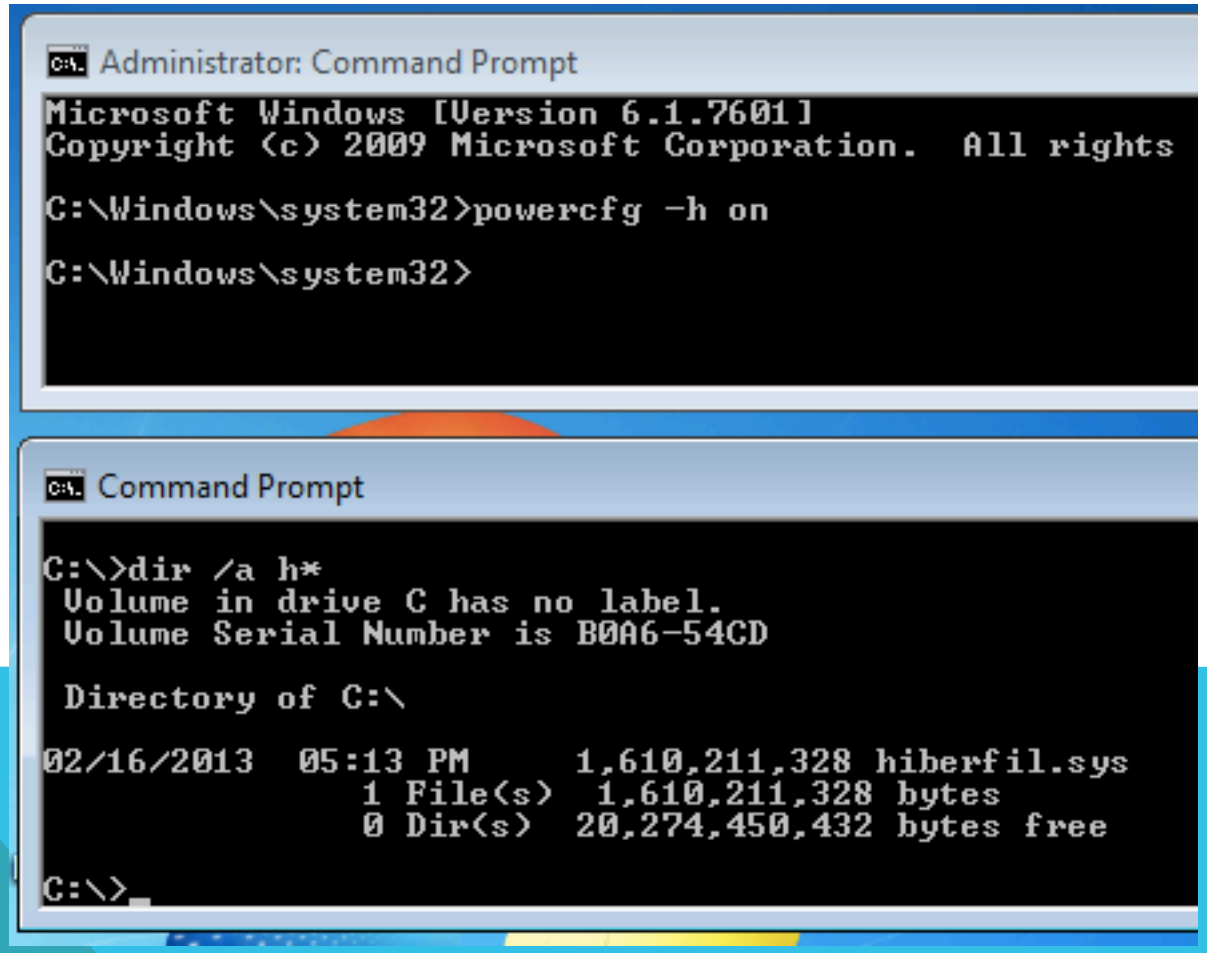
- Sleep – data tersimpan di RAM
  - Power masih menyala
  - Dokumen hilang jika power mati
- Hibernate – RAM dikopik e Hiberfil.sys
  - Power off
  - Dokumen tidak hilang
- Hybrid Sleep
  - Default untuk desktop Windows 7
  - Meletakkan dokumen yang terbuka dan programs di disk
  - Menyimpannya di RAM agar segera bisa dijalankan
  - Dokumen tidak hilang meskipun power mati



ENABLING HIBERNATION

Link

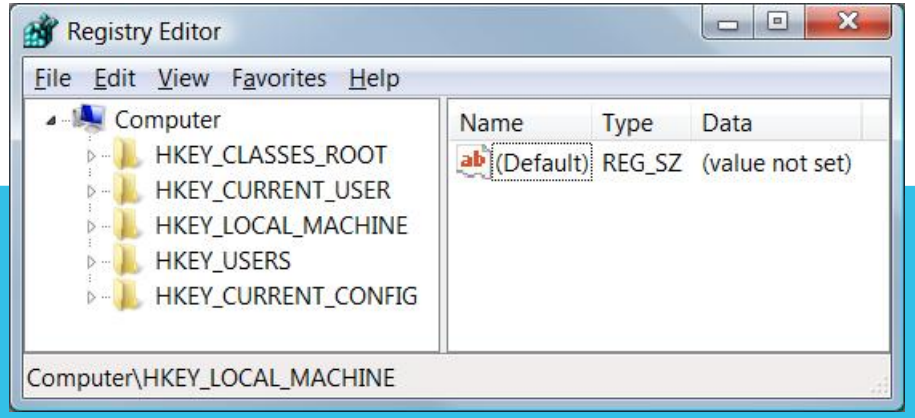
Ch 5i: Hibernate - Enable or Disable - Windows 7 Support Forums



REGISTRY

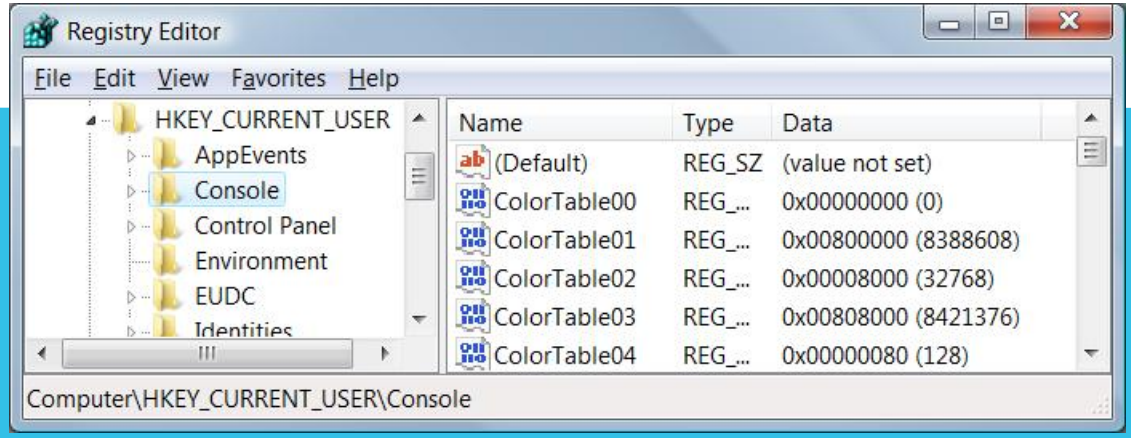
MEMAHAMI STRUKTUR REGISTRY

- **Registry terdiri dari lima root keys**
  - **HKey_Classes_Root**
  - **HKey_Current_User**
  - **HKey_Local_Machine**
  - **HKey_Users**
  - **HKey_Current_Config**
- **atau HKCR, HKCU, HKLM, HKU, dan HKCC**



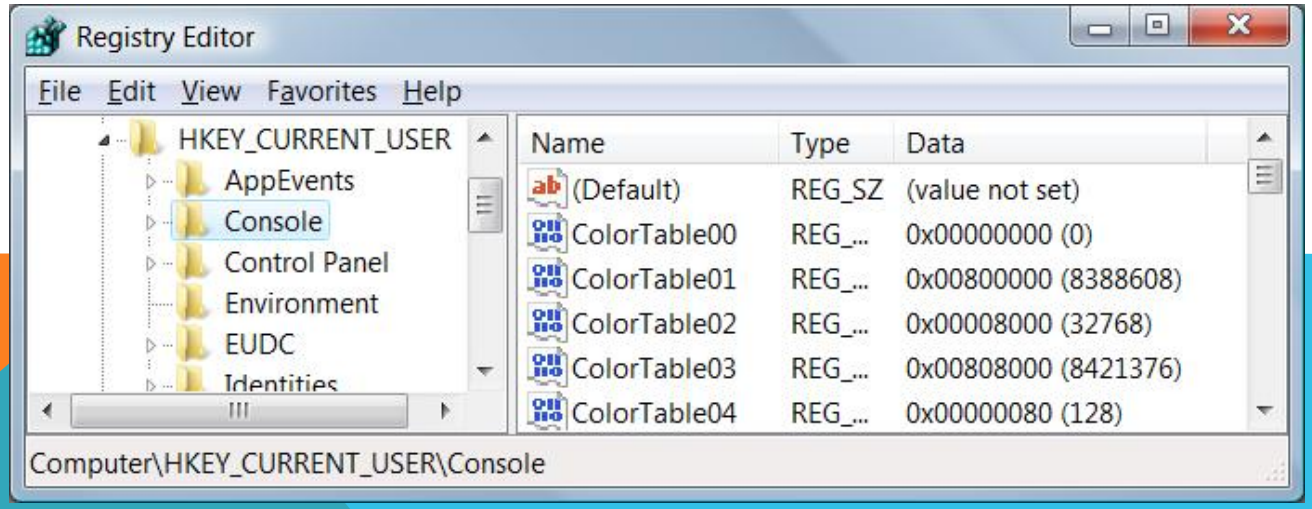
SUBKEYS

- **Root keys (kadang-kadang disebut *predefined keys*), berisikan subkeys**
  - **Subkeys terlihat seperti folders di Regedit**
- **HKCU memiliki beberapa top-level subkeys: AppEvents, Console, Control Panel, …**
  - **root key dan subkeys berbentuk path**
  - **HKCU\Console**



VALUE

- **Setiap Subkey berisi minimal satu value**
  - **Tapi bisa jadi tidak ada (value not set)**
- **default value (biasanya undefined)**
- **Values memilik name, data type, dan data**

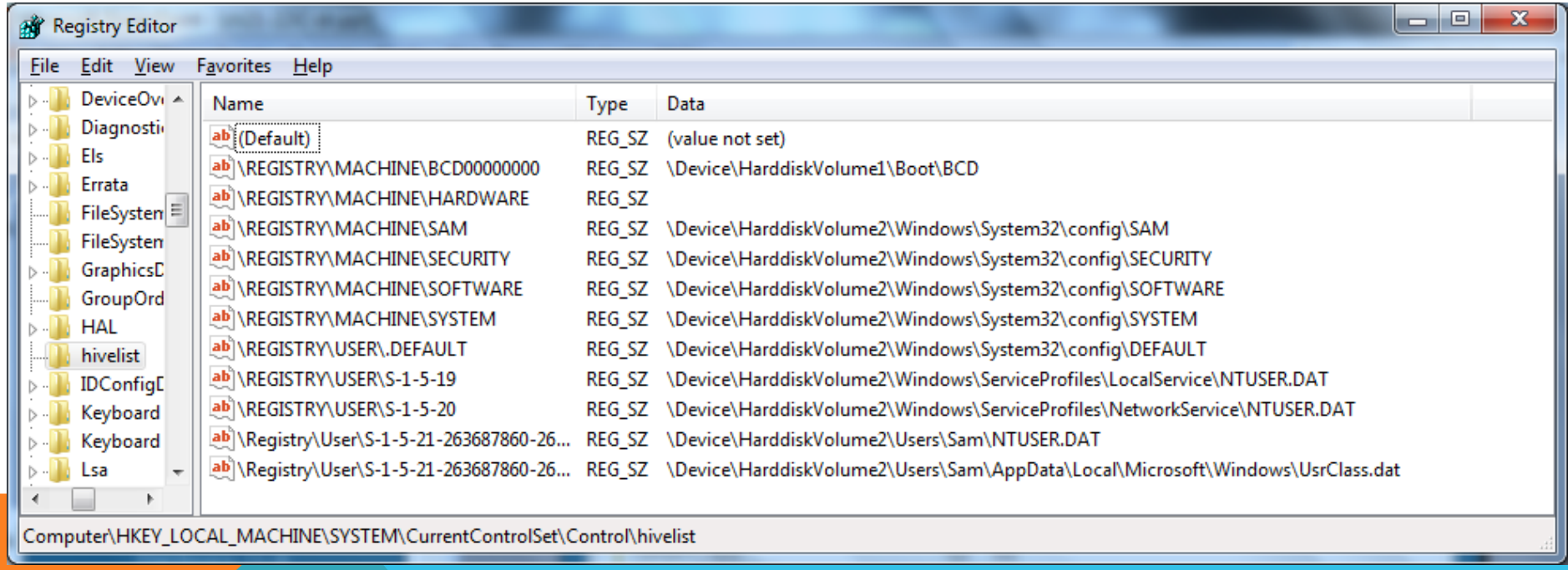


HIVES

- **Key dengan subkeys dan values disebut *hive***
- **Registry disimpan di disk dalam bentuk beberapa *hive files* terpisah**
- **Hive files dibaca dalam memory ketika sistem operasi berjalan (atau saat pengguna baru logs on)**

HIVELIST

- **HKLM\System\CurrentControlSet\Control\HiveList**



HARDWARE HIVE

- **\Registry\Machine\Hardware tidak berkaitan dengan file disk**
- **Windows 7 membuat file ini saat tiap kali komputer dinyalakan**

HKCR DAN HKCU

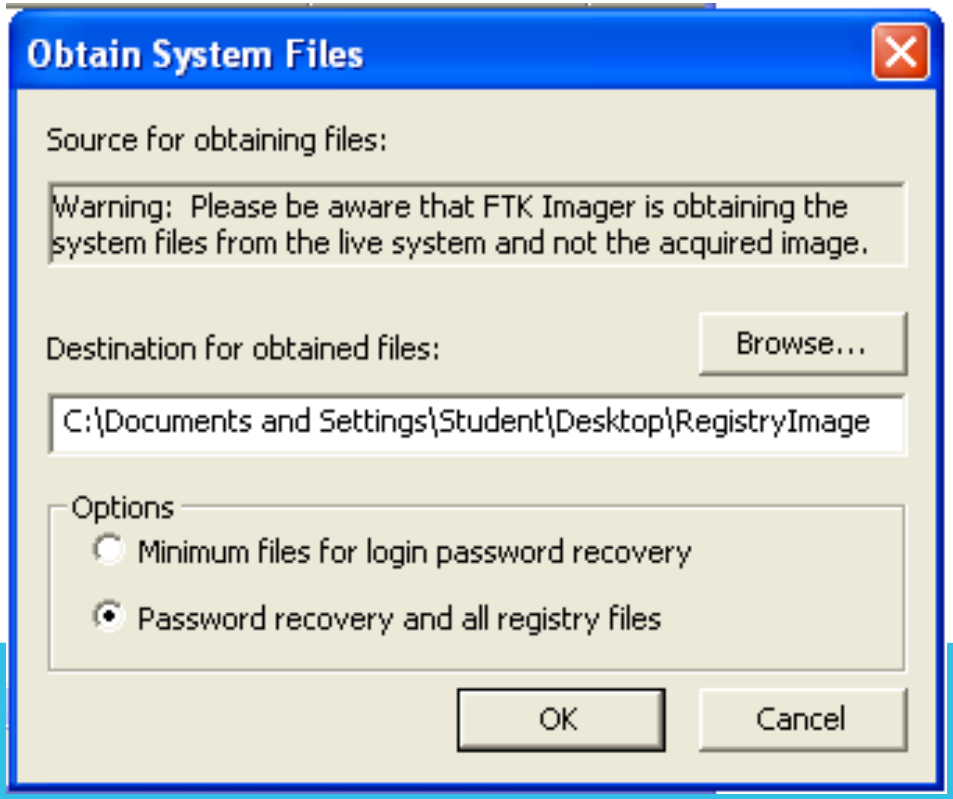
- **Keys tersebut dihubungkan ke items yang berada pada root keys yang lain**
  - HKey_Classes_Root (HKCR)
    - Digabungkan dari keys dalam HKLM\Software \Classes dan HKU*sid*_Classes
      - *sid* merupakan security identifier dari user yang sedang log on
  - HKey_Current_User (HKCU)
    - HKU*sid*

TUJUAN REGISTRY

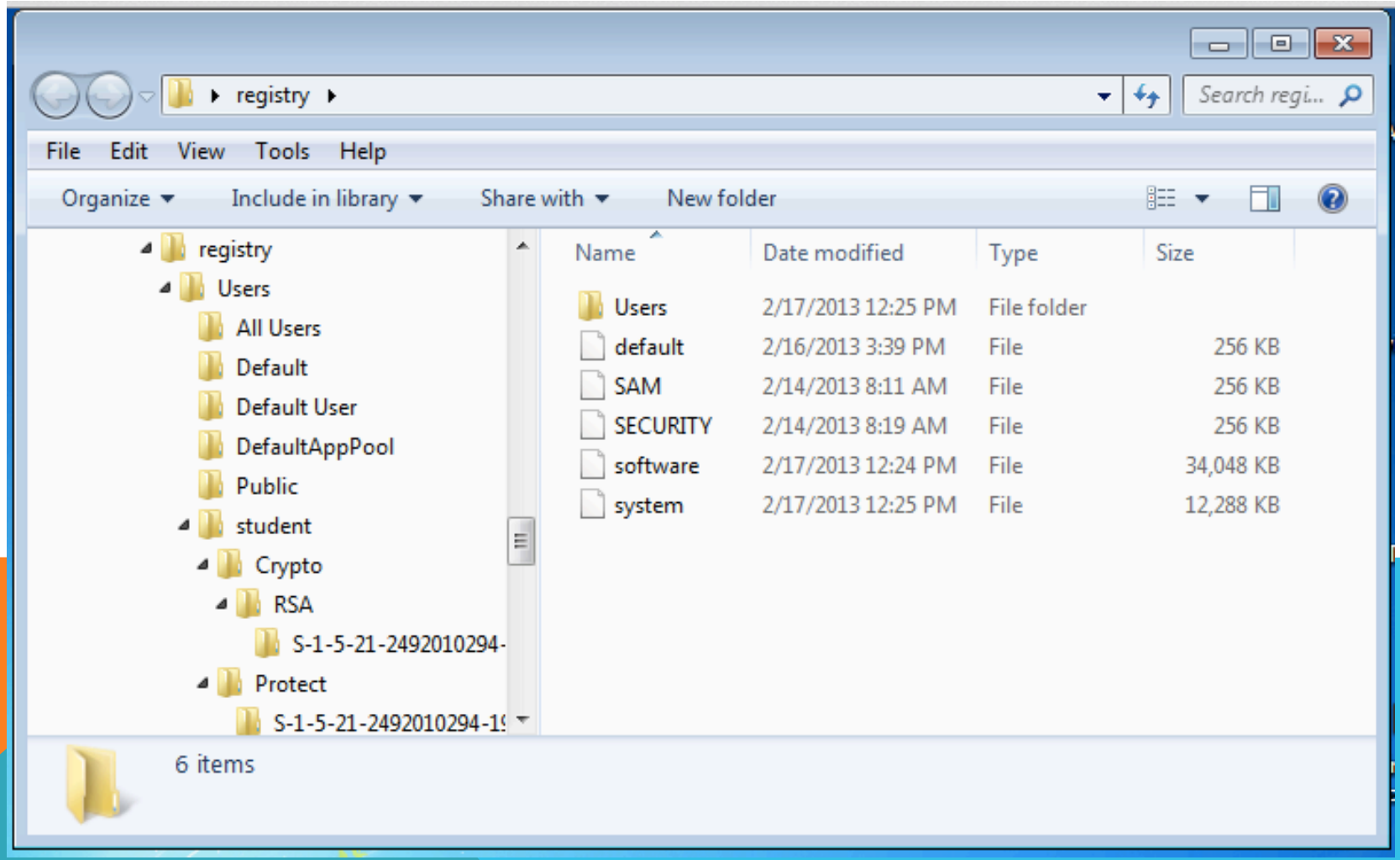
- Database untuk file konfigurasi
- Registry artifacts sangat bernilai untuk forensik
  - Kata kunci pencarian
  - Programs dijalankan atau diinstal
  - Web addresses
  - Files yang baru dibuka
  - USB devices yang terkoneksi

MENDAPATKAN REGISTRY

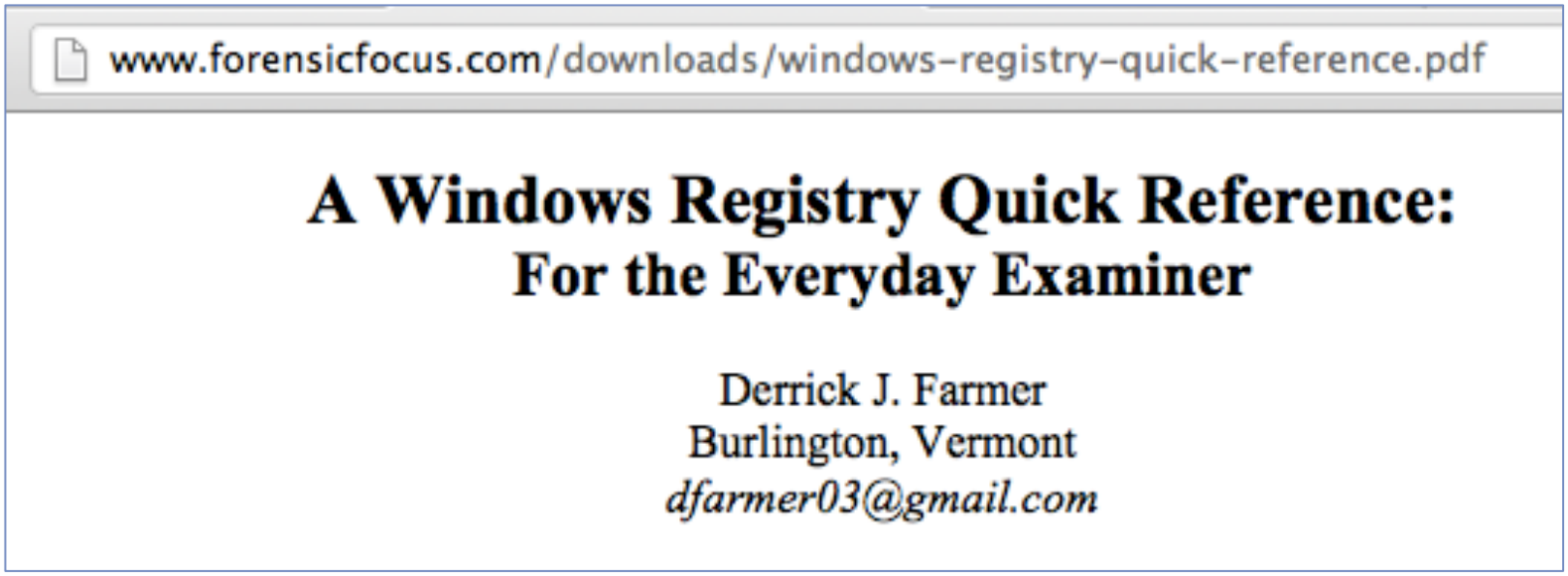
FTK Imager



FILE YANG DIPERLUKAN



REFERENSI



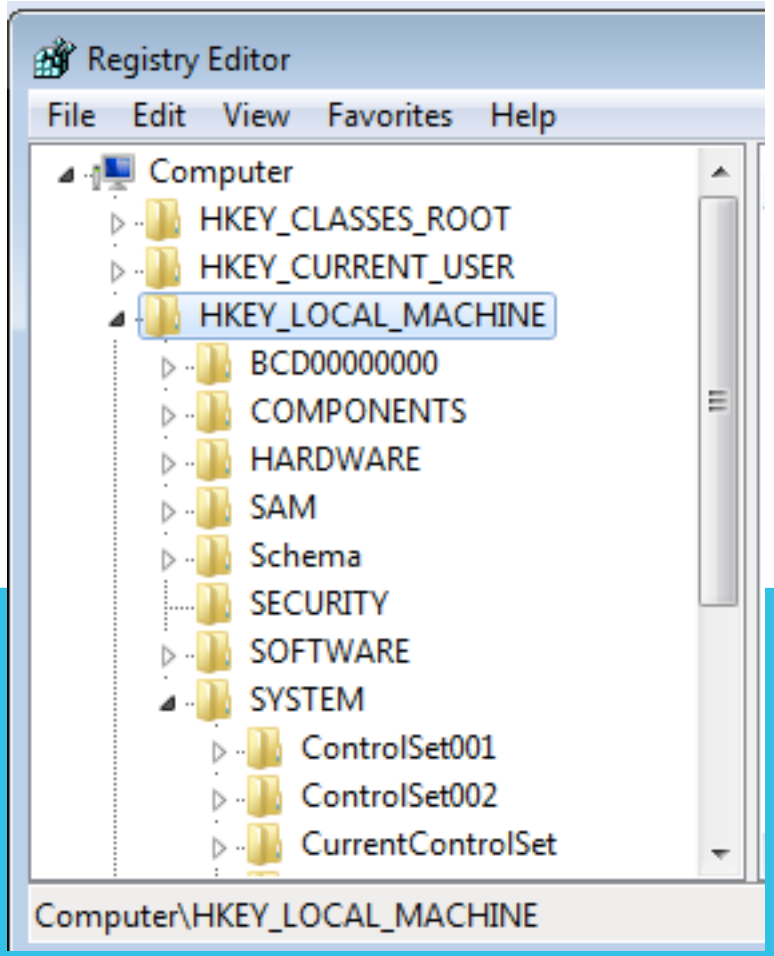
Link Ch 5c: A Windows Registry Quick Reference

REGISTRY DATA YANG PENTING

- Control Set
- Time Zone
- User Assist
- USB Store

CONTROL SET

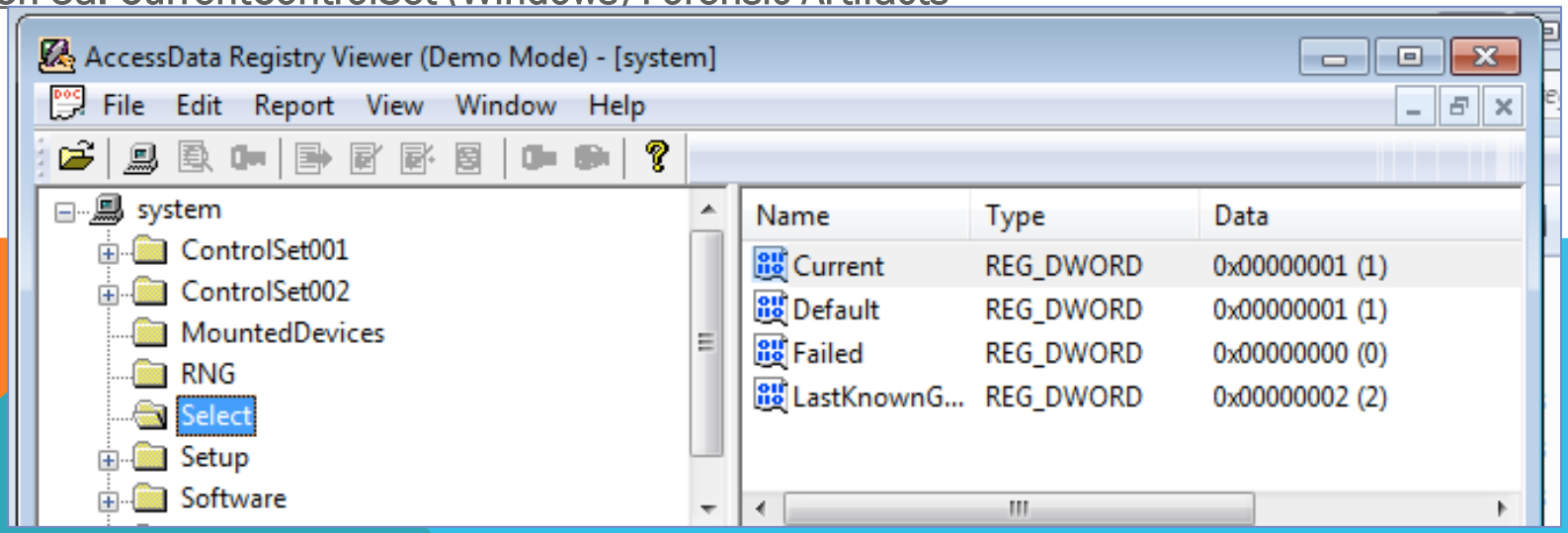
- Live Registry memiliki kunci penting yang bernama HKLM \System\CurrentControlSet
- Berisikan Time Zone, USBSTOR, dan informasi lainnya



CONTROL SET

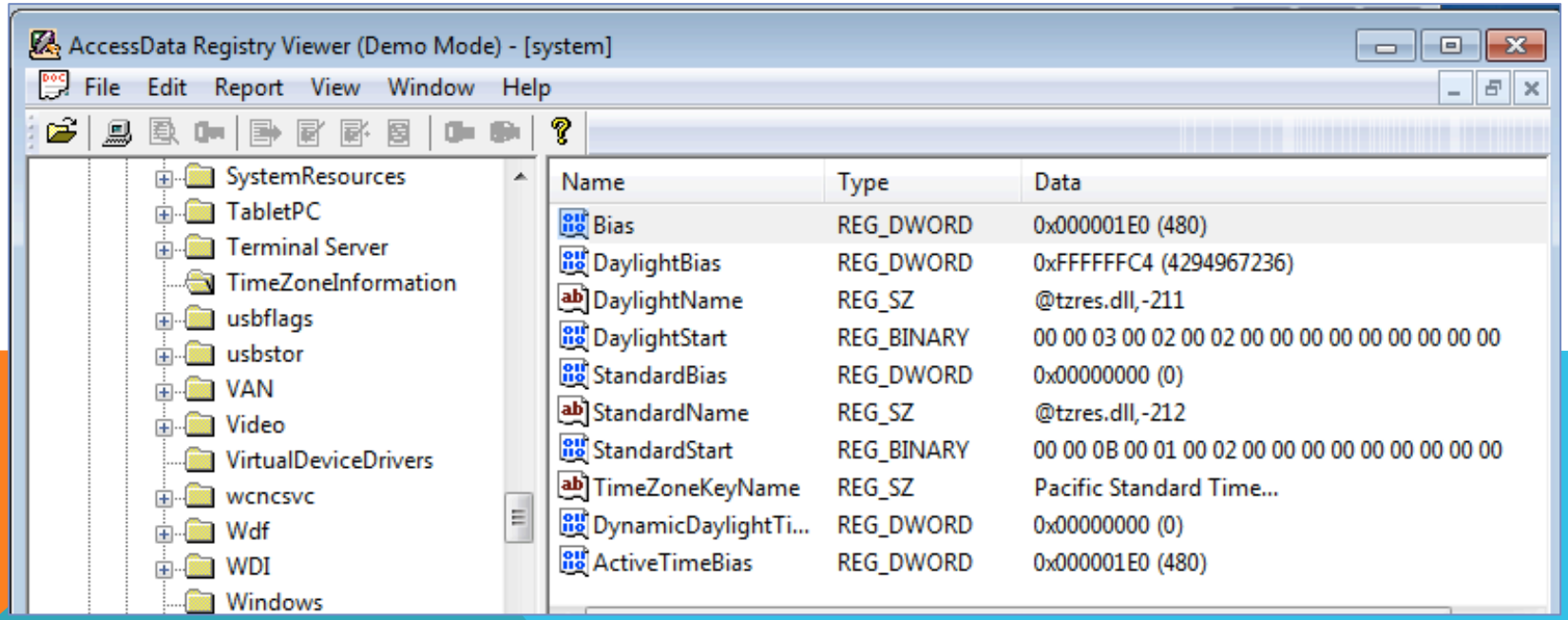
- Image registry yang dikopi tidak berisi CurrentControlSet
- Data yang bersifat sementara tidak disimpan dalam file hive
- Untuk menentukan ControlSet yang digunakan sekarang, lihat di System\Select
- Pada contoh, ControlSet001 yang sekarang digunakan

- Link Ch 5a: CurrentControlSet (Windows) Forensic Artifacts



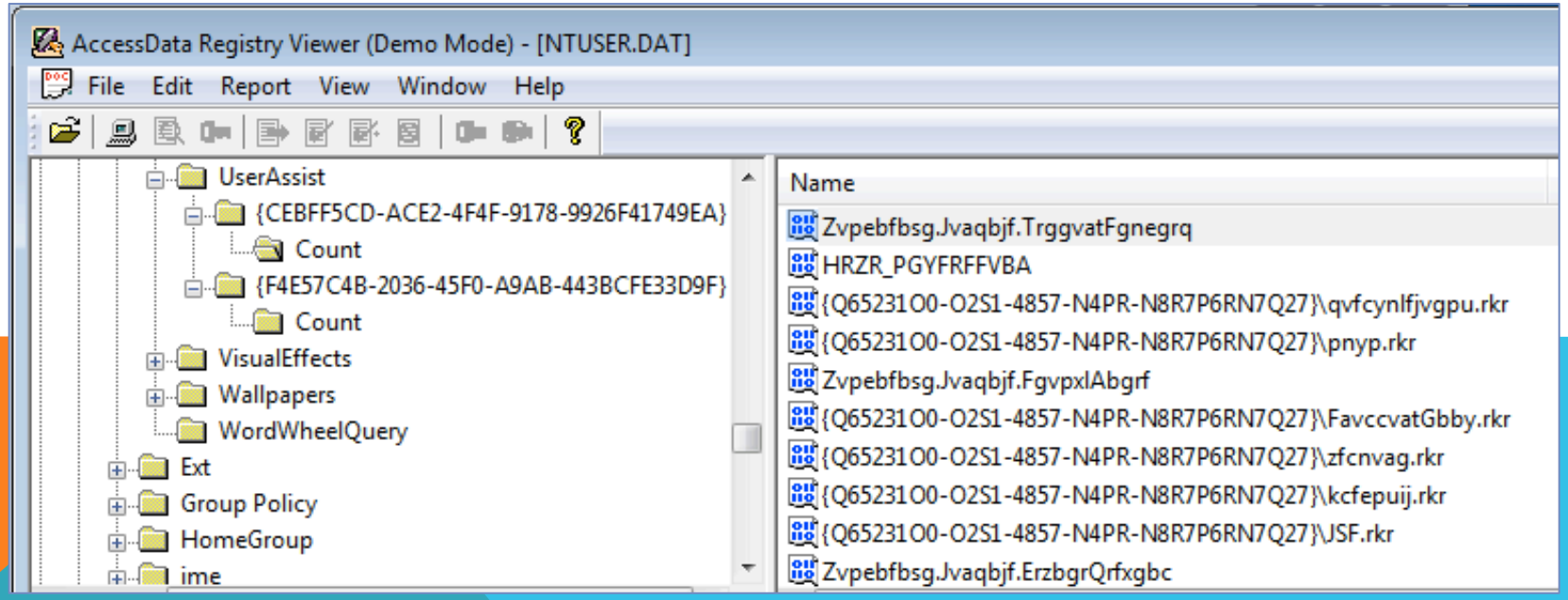
TIME ZONE

- System\ControlSet001\Control\TimeZoneInformation
  - Terlihat di contoh ControlSet001

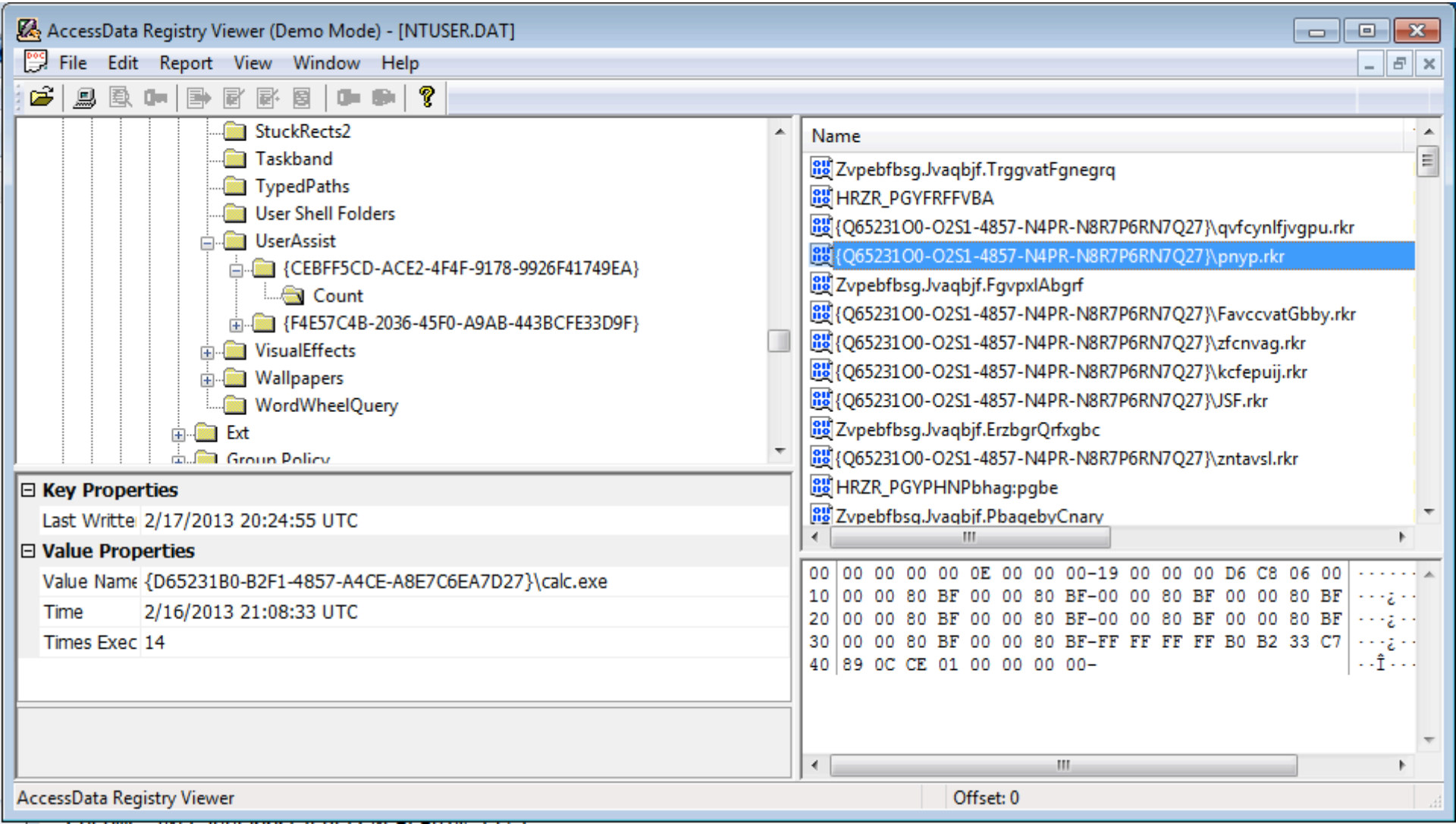


USERASSIST

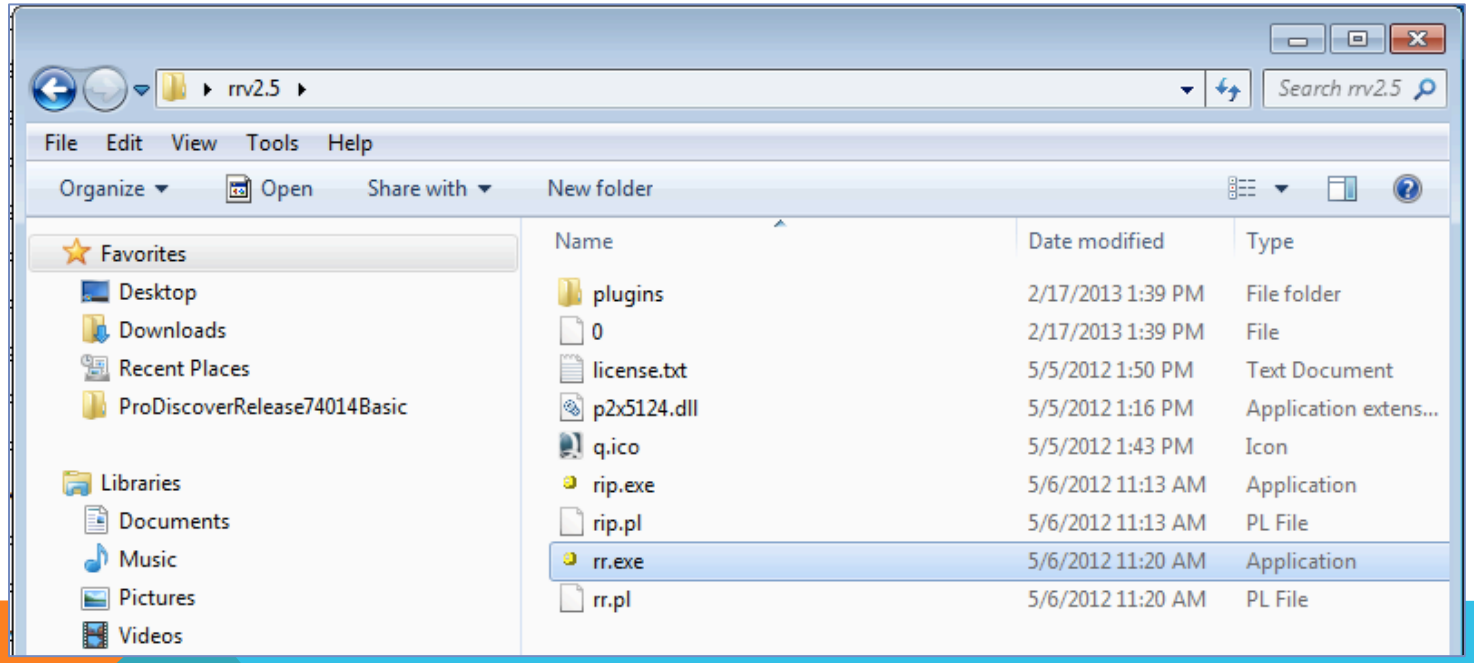
- Memperlihatkan objects yang sudah diakses user
- Untuk melihatnya, buka Users*Username*\NTUSER.DAT
- Arahkan ke Software\Microsoft\Windows\CurrentVersion \Explorer\UserAssist



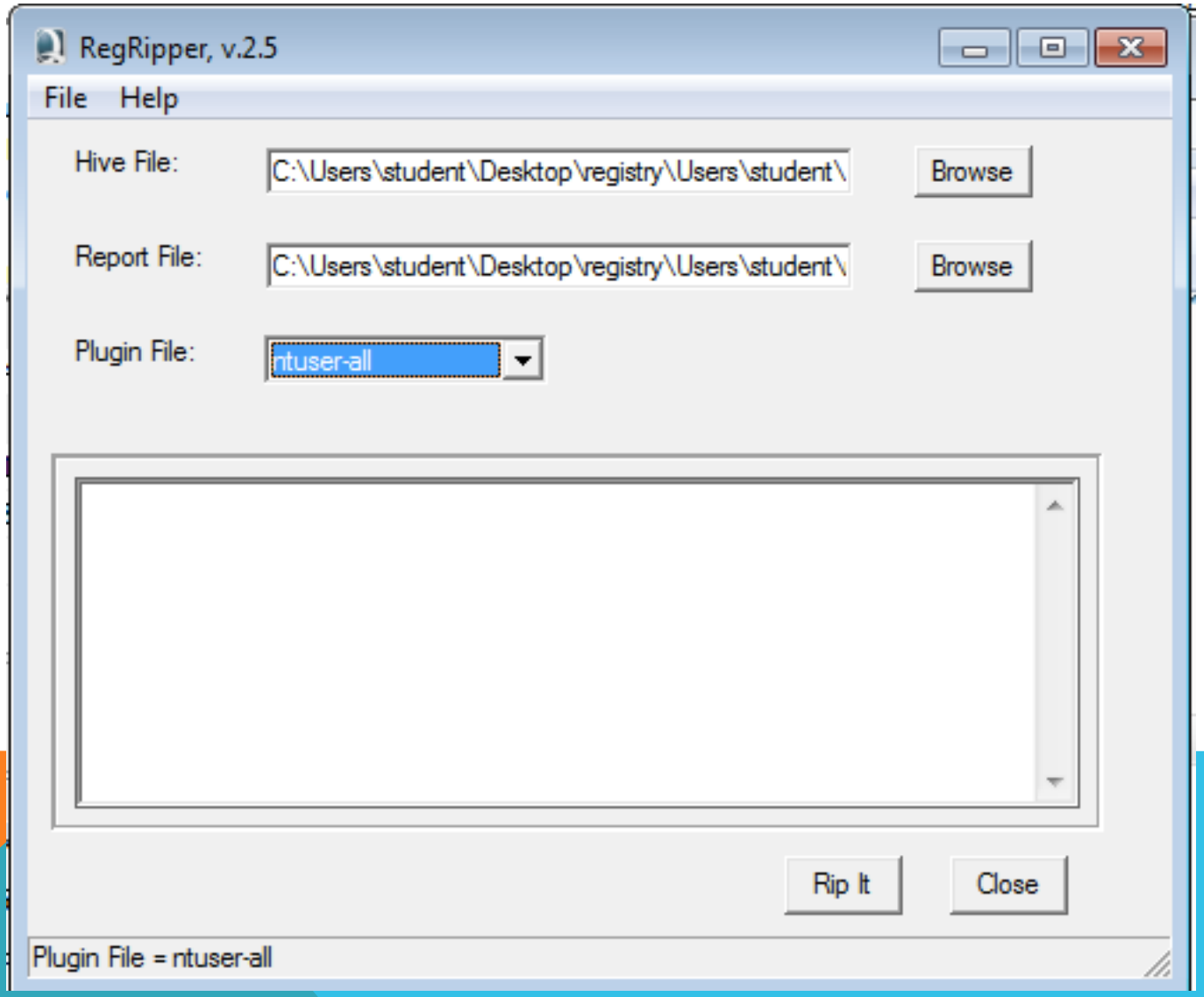
USERASSIST DECODED PADA PANEL KIRI BAWAH



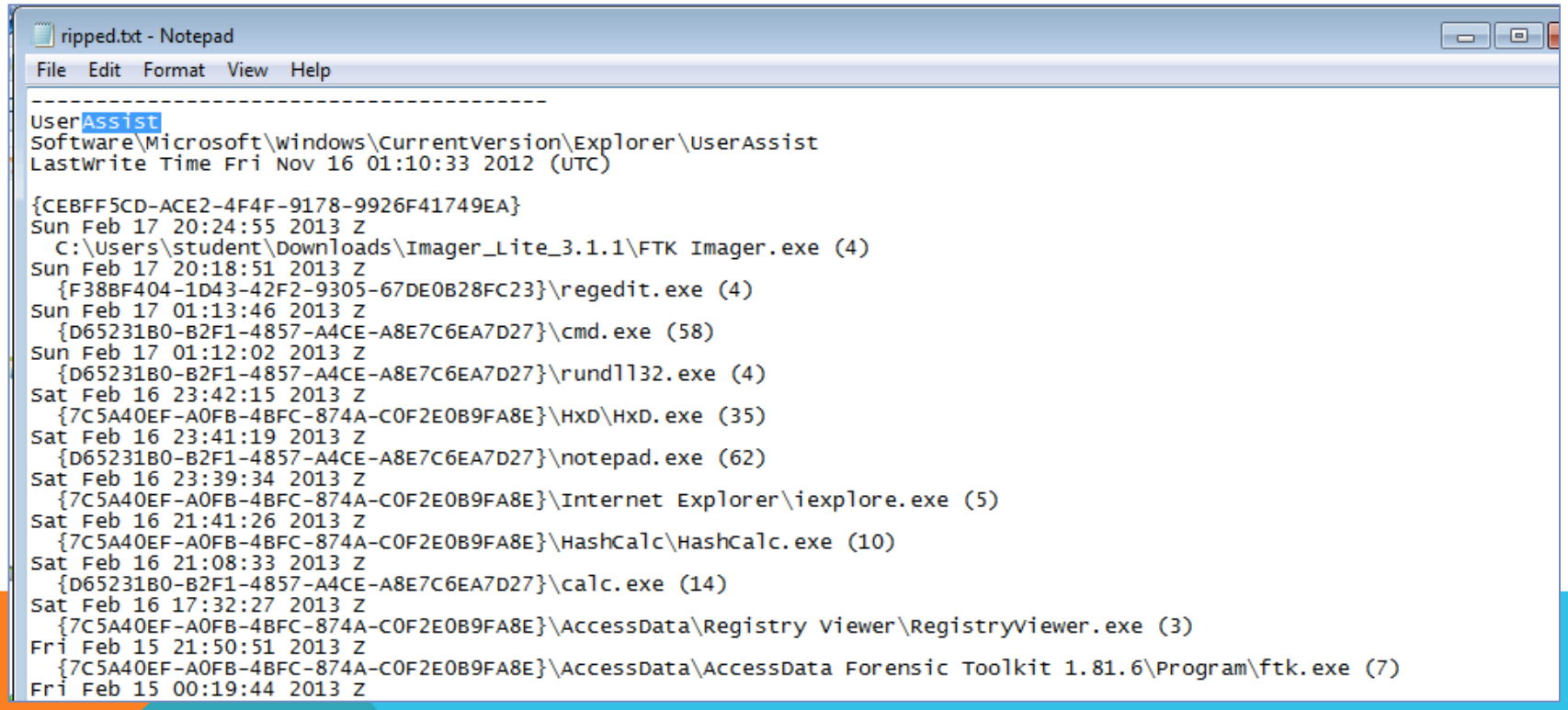
REGRIPPER



Link Ch 5k: regripper


RegRipper, v.2.5
File
Help
Hive File:
C:\Users\student\Desktop\registry\Users\student\
Browse
Report File:
C:\Users\student\Desktop\registry\Users\student\
Browse
Plugin File:
ntuser-all
Rip It
Close
Plugin File = ntuser-all

RIPPED REGISTRY



USBSTOR

System\ControlSet001\Enum\USBSTOR

- Pada contoh Current Control Set adalah 1