

# 5. WINDOWS SYSTEM ARTIFACTS BAGIAN 1

# TOPIK

- Mendelete data
- File Hibernation
- Registry

**MENDELETE DATA**

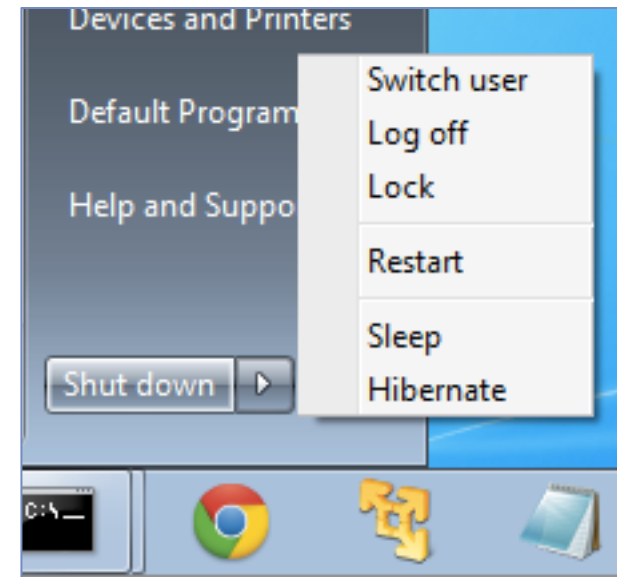
# RECOVER DATA YANG DIDELETE

- 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](#)

C:\ Administrator: Command Prompt

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>powercfg -h on

C:\Windows\system32>
```

C:\ Command Prompt

```
C:\>dir /a h*
Volume in drive C has no label.
Volume Serial Number is B0A6-54CD

Directory of C:\

02/16/2013  05:13 PM          1,610,211,328 hiberfil.sys
               1 File(s)      1,610,211,328 bytes
               0 Dir(s)      20,274,450,432 bytes free
```

C:\>

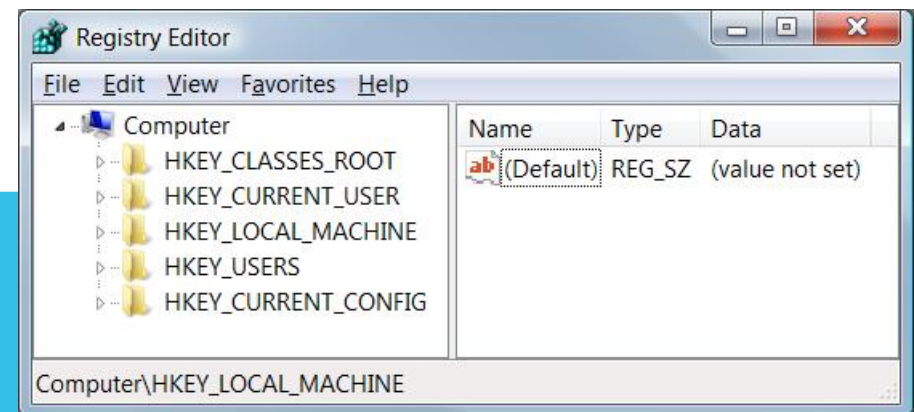


**REGISTRY**



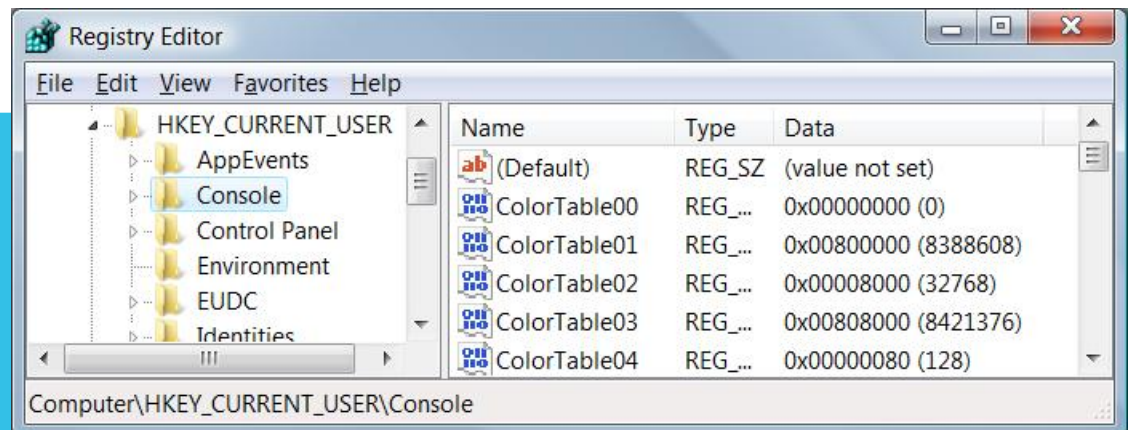
# MEMAHAMI STRUKTUR REGISTRY

- 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



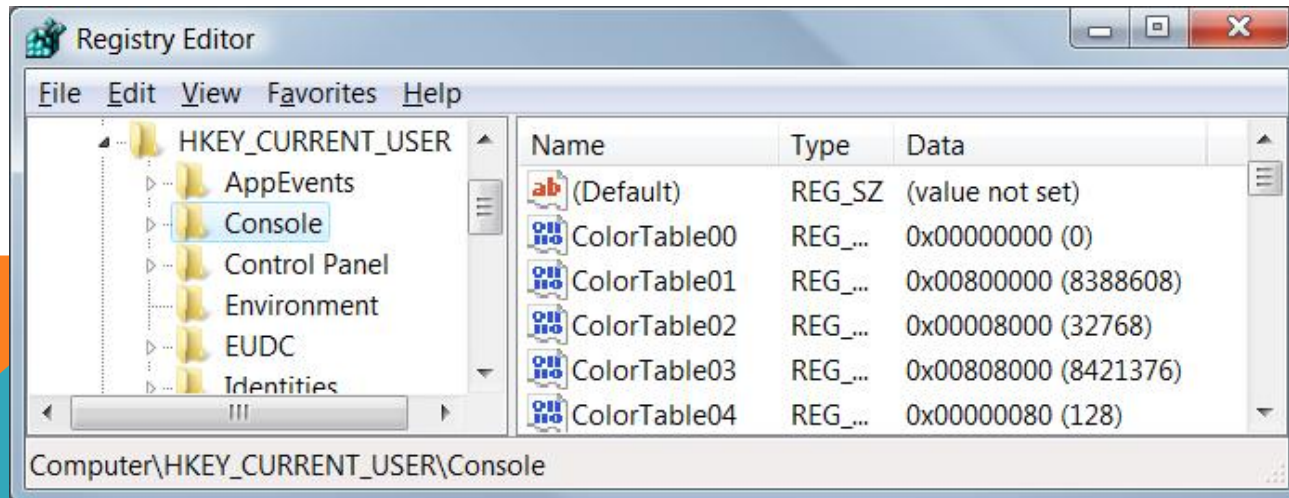
# SUBKEYS

- **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 memiliki name, data type, dan data**

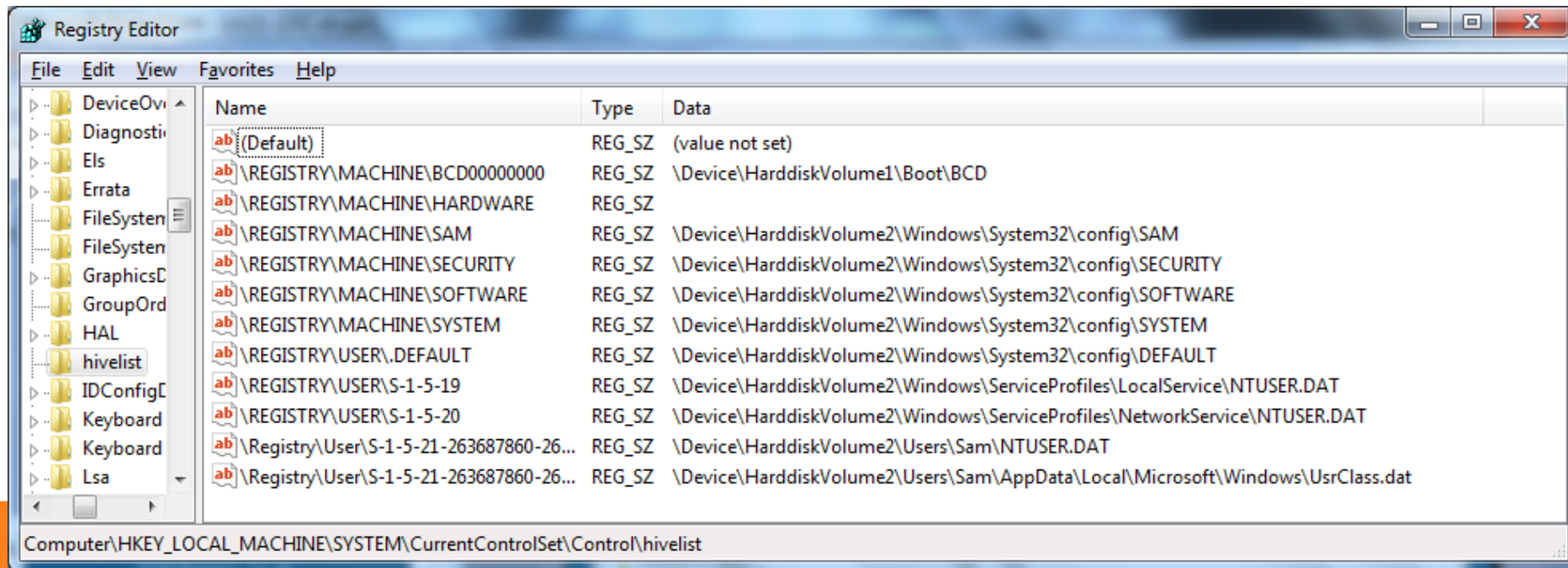


# HIVES

- **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

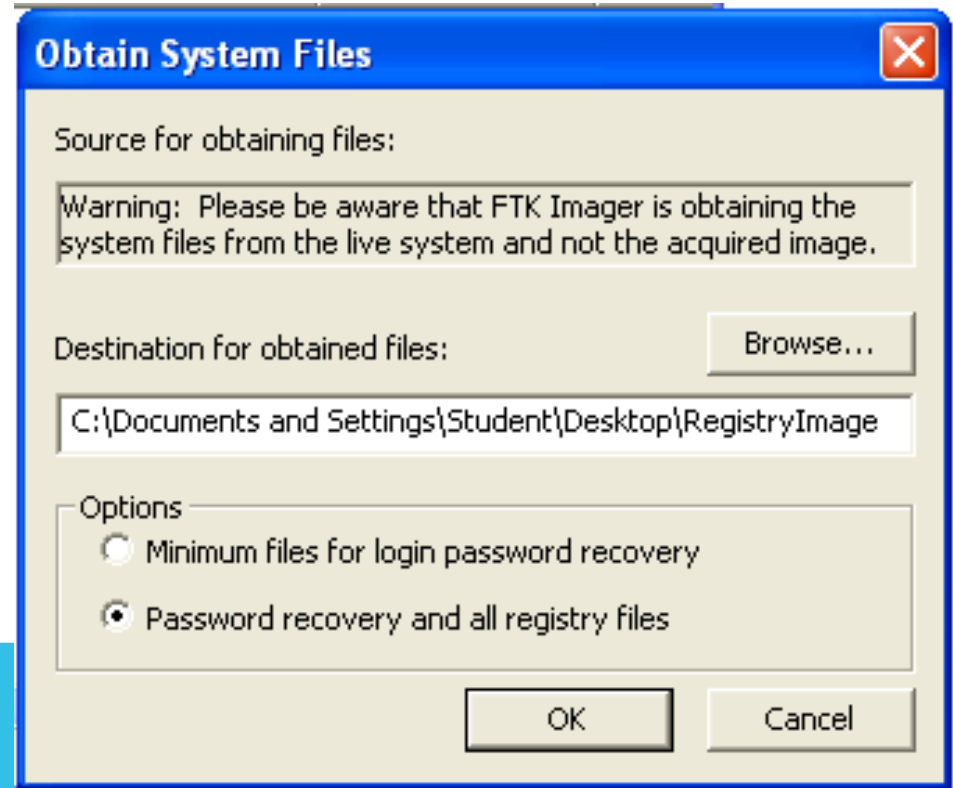
# TUJUAN REGISTRY

- 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

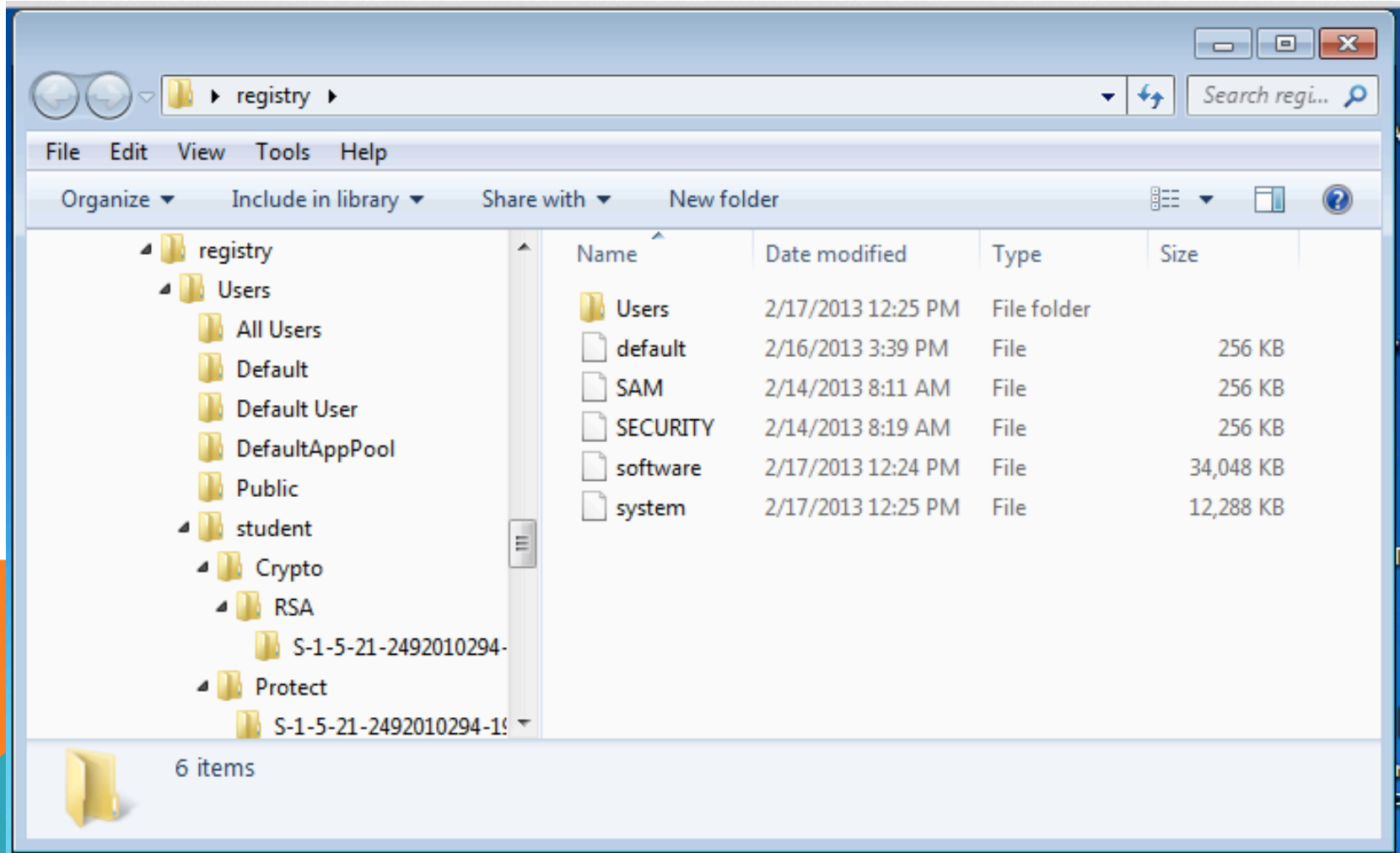


# MENDAPATKAN REGISTRY

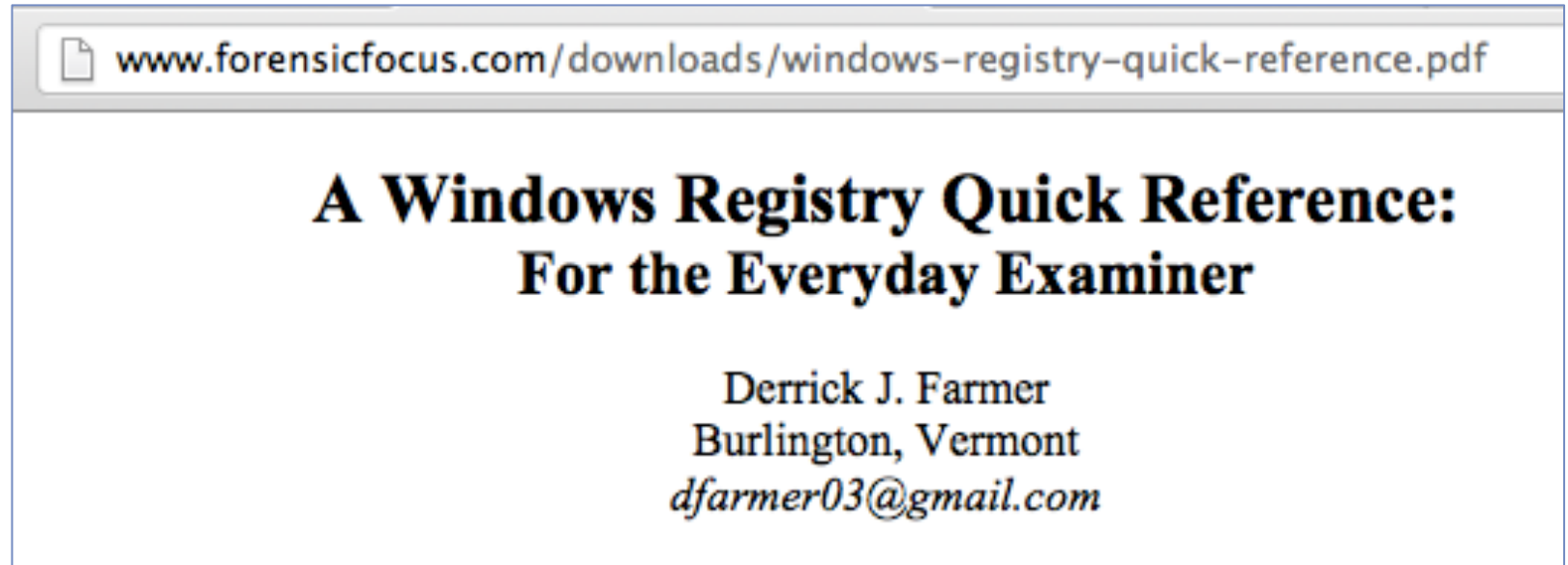
FTK Imager



# FILE YANG DIPERLUKAN




# REFERENSI



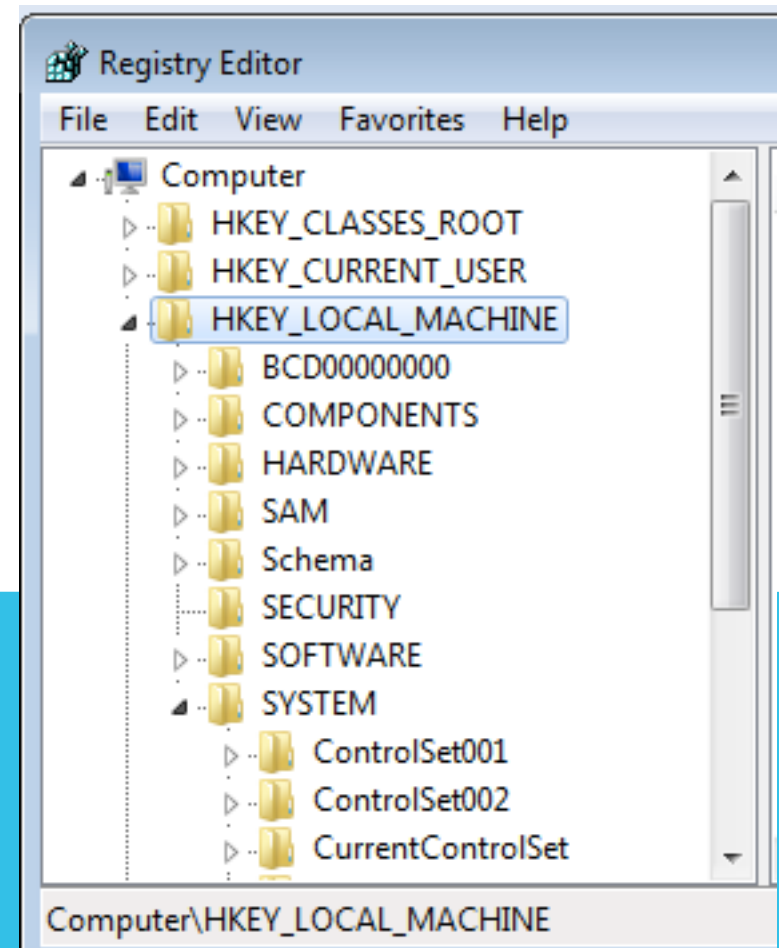
Link [Ch 5c: A Windows Registry Quick Reference](#)

# REGISTRY DATA YANG PENTING

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

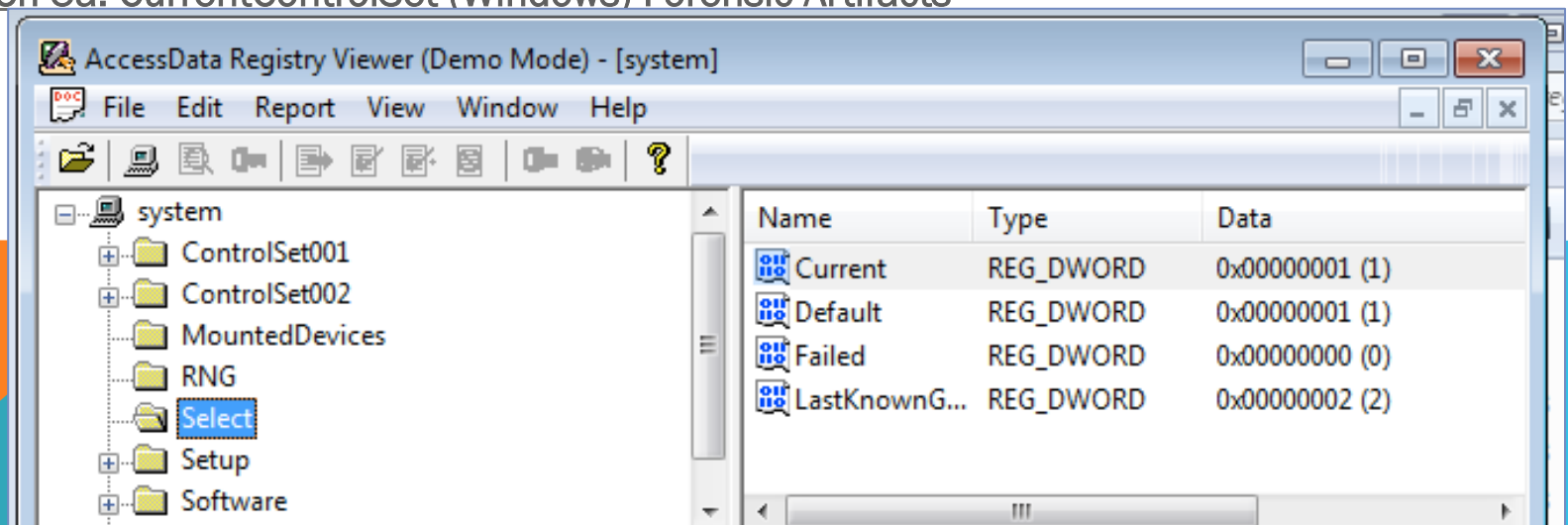
# CONTROL SET

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



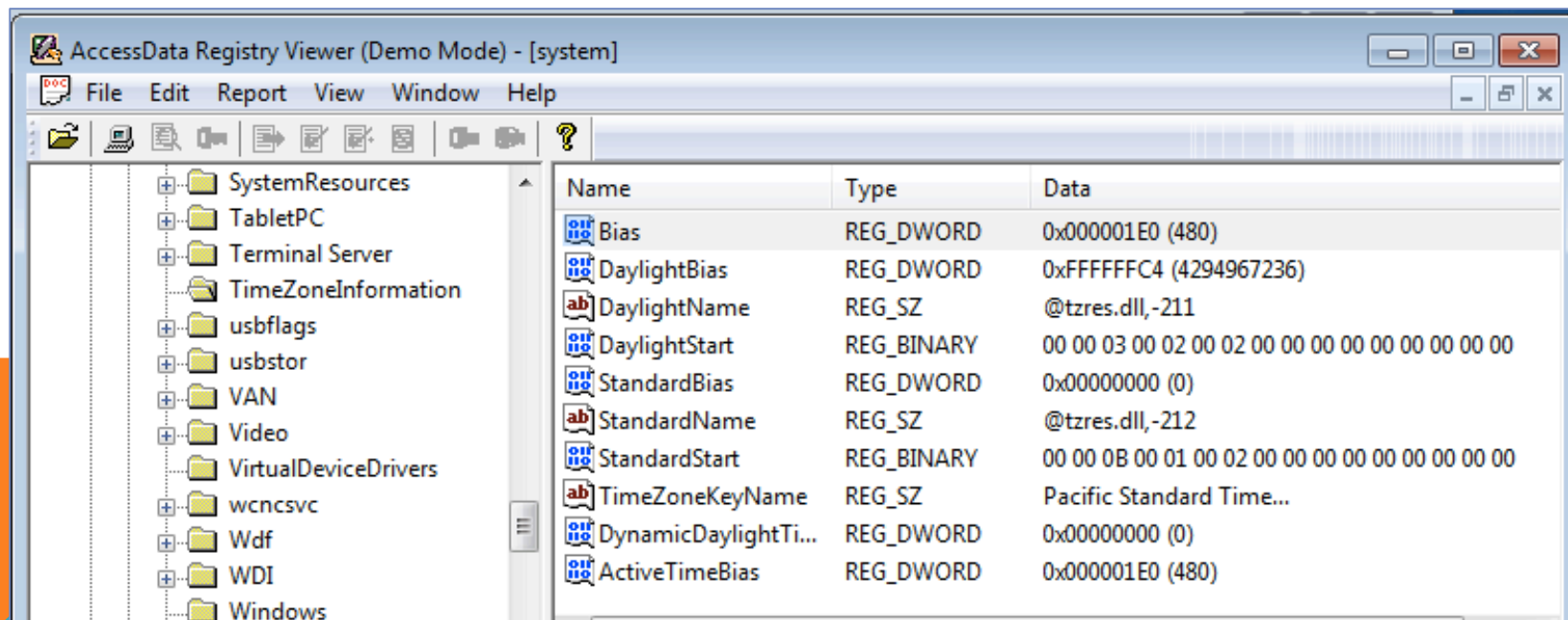
# CONTROL SET

- 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](#)



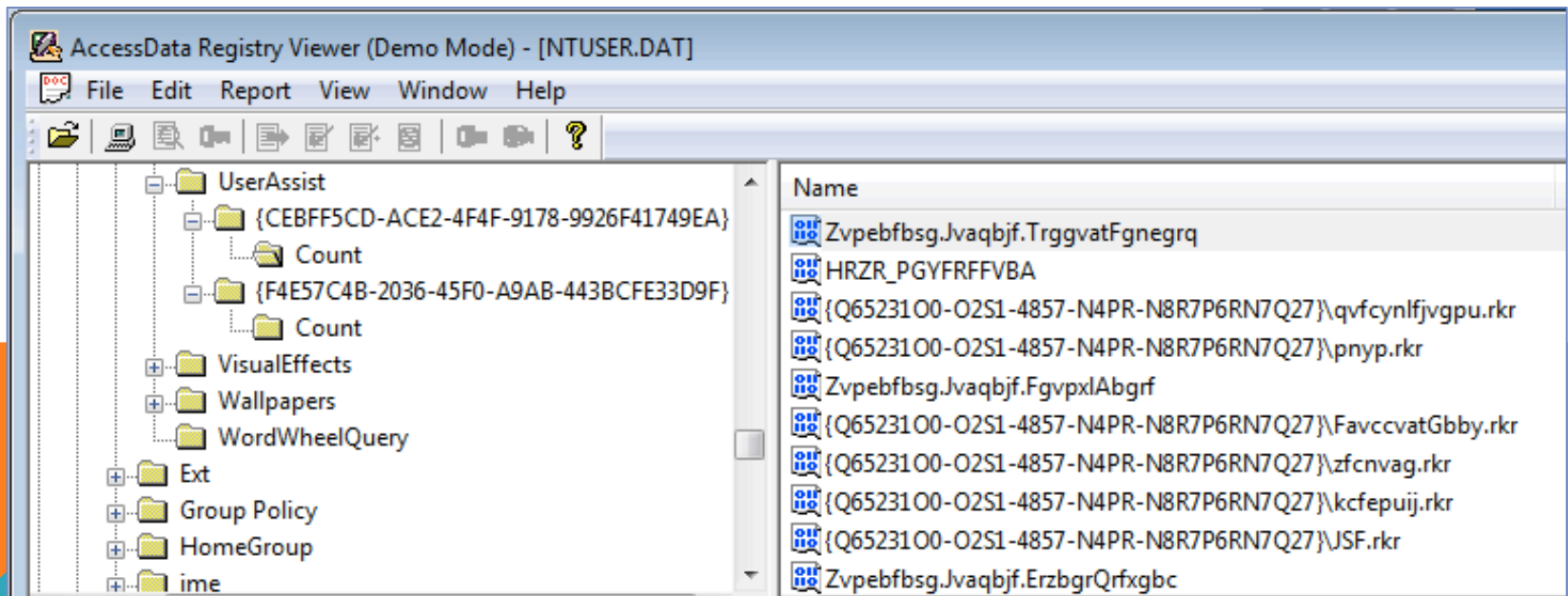
# TIME ZONE

- 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

The screenshot shows the AccessData Registry Viewer (Demo Mode) interface. The left pane displays the registry tree with 'UserAssist' expanded. The right pane shows a list of registry values under the path '{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\pnyp.rkr'. The bottom-left pane shows the 'Key Properties' and 'Value Properties' for the selected value. The bottom-right pane shows the decoded data in hexadecimal and ASCII format.

**Registry Tree (Left Pane):**

- StuckRects2
- Taskband
- TypedPaths
- User Shell Folders
- UserAssist
  - {CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
    - Count
  - {F4E57C4B-2036-45F0-A9AB-443BCFE33D9F}
  - VisualEffects
  - Wallpapers
  - WordWheelQuery
- Ext
- Group Policy

**Registry Values (Right Pane):**

Name
Zvpebfbsg.Jvaqbjf.TrggvatFgnegrq
HRZR_PGYFRFFVBA
{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\qvfcynlfjvgpu.rkr
<b>{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\pnyp.rkr</b>
Zvpebfbsg.Jvaqbjf.FgvpxlAbgrf
{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\FavccvatGbby.rkr
{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\zfcnvag.rkr
{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\kcfepuij.rkr
{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\JSF.rkr
Zvpebfbsg.Jvaqbjf.ErzbgRrfgbc
{Q6523100-02S1-4857-N4PR-N8R7P6RN7Q27}\zntavsl.rkr
HRZR_PGYPHNPbhag:pgbe
Zvpebfbsq.Jvaqbjf.PbaqebYcNary

**Key Properties (Bottom-Left):**

- Last Write: 2/17/2013 20:24:55 UTC

**Value Properties (Bottom-Left):**

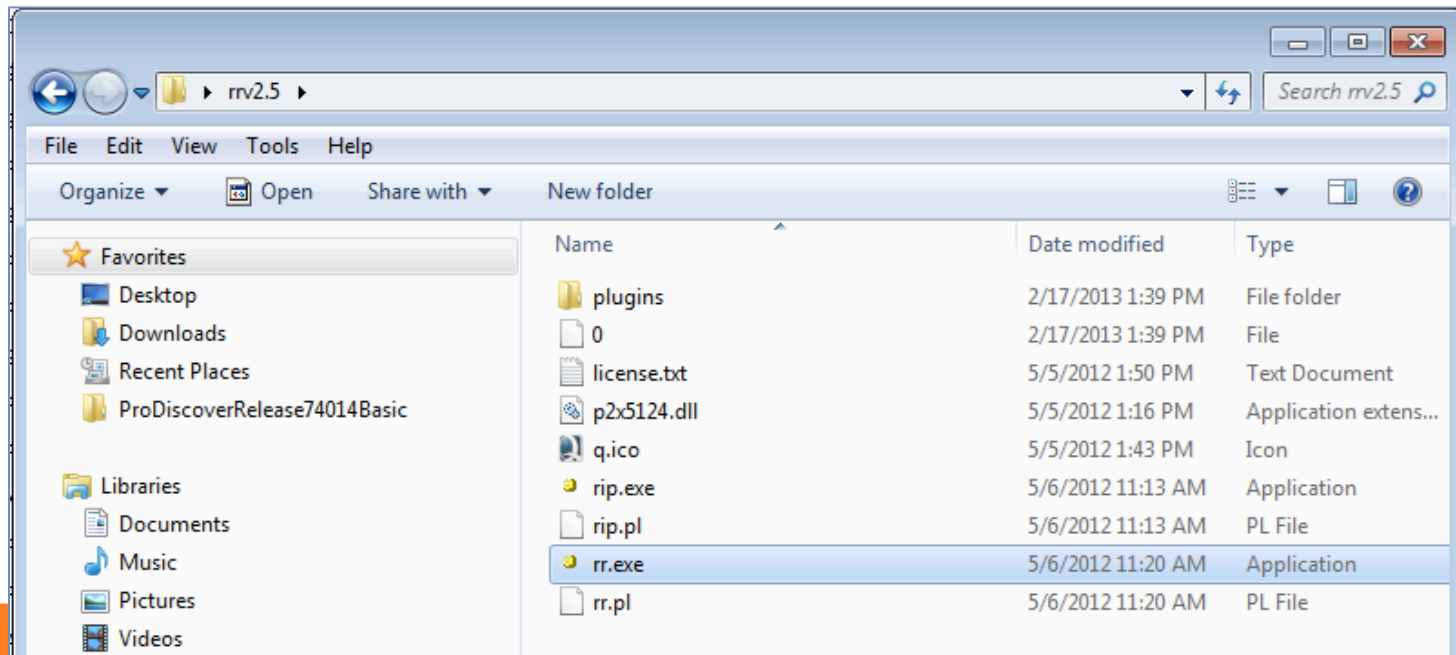
- Value Name: {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\calc.exe
- Time: 2/16/2013 21:08:33 UTC
- Times Exec: 14

**Decoded Data (Bottom-Right):**

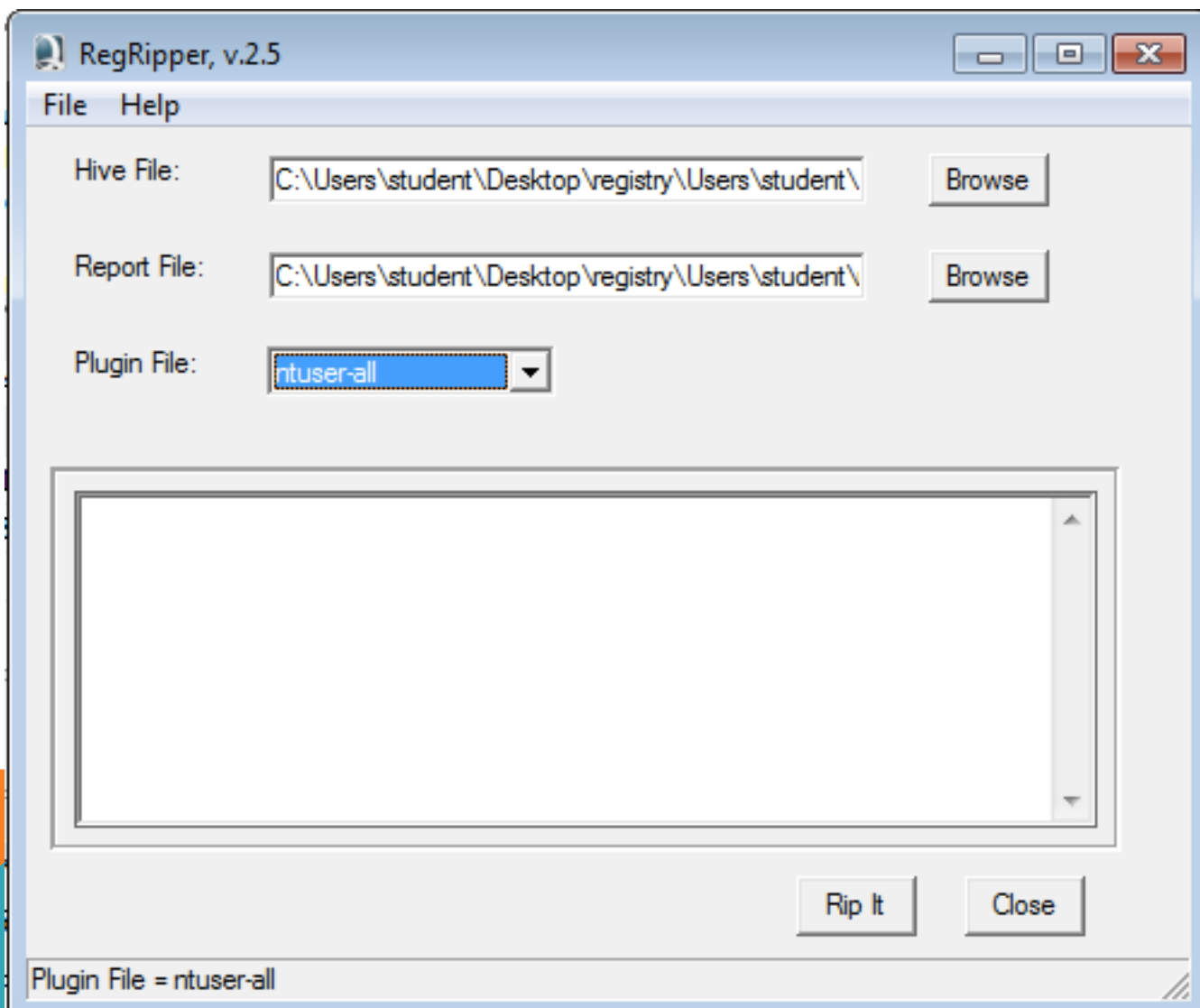
00	00	00	00	00	0E	00	00	00	19	00	00	00	D6	C8	06	00	.....
10	00	00	80	BF	00	00	80	BF	00	00	80	BF	00	00	80	BF	...z..
20	00	00	80	BF	00	00	80	BF	00	00	80	BF	00	00	80	BF	...z..
30	00	00	80	BF	00	00	80	BF	FF	FF	FF	FF	B0	B2	33	C7	...z..
40	89	0C	CE	01	00	00	00	00	-	-	-	-	-	-	-	-	..i..

AccessData Registry Viewer | Offset: 0

# REGRIPPER



Link [Ch 5k: regripper](#)



# RIPPED REGISTRY

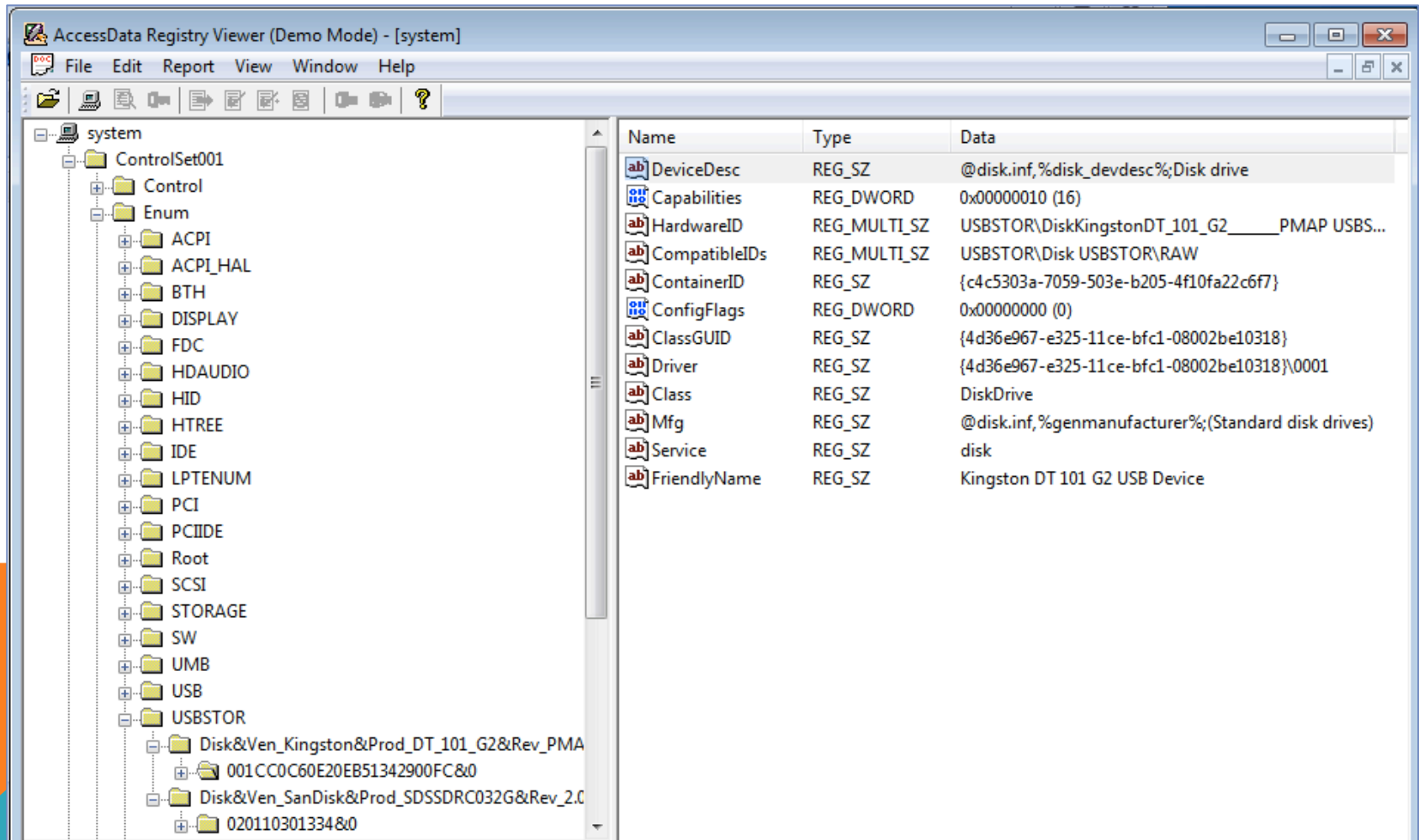
```
ripped.txt - Notepad
File Edit Format View Help
-----
User Assist
Software\Microsoft\windows\CurrentVersion\Explorer\UserAssist
LastWrite Time Fri Nov 16 01:10:33 2012 (UTC)

{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}
Sun Feb 17 20:24:55 2013 Z
  C:\Users\student\Downloads\Imager_Lite_3.1.1\FTK Imager.exe (4)
Sun Feb 17 20:18:51 2013 Z
  {F38BF404-1D43-42F2-9305-67DE0B28FC23}\regedit.exe (4)
Sun Feb 17 01:13:46 2013 Z
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\cmd.exe (58)
Sun Feb 17 01:12:02 2013 Z
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\rundll32.exe (4)
Sat Feb 16 23:42:15 2013 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\HxD\HxD.exe (35)
Sat Feb 16 23:41:19 2013 Z
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\notepad.exe (62)
Sat Feb 16 23:39:34 2013 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\Internet Explorer\iexplore.exe (5)
Sat Feb 16 21:41:26 2013 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\HashCalc\HashCalc.exe (10)
Sat Feb 16 21:08:33 2013 Z
  {D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\calc.exe (14)
Sat Feb 16 17:32:27 2013 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\AccessData\Registry Viewer\RegistryViewer.exe (3)
Fri Feb 15 21:50:51 2013 Z
  {7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\AccessData\AccessData Forensic Toolkit 1.81.6\Program\ftk.exe (7)
Fri Feb 15 00:19:44 2013 Z
```

# USBSTOR

System\ControlSet001\Enum\USBSTOR

- Pada contoh Current Control Set adalah 1



The screenshot shows the AccessData Registry Viewer (Demo Mode) window. The left pane displays the registry tree structure, with the path System\ControlSet001\Enum\USBSTOR expanded. The right pane shows a list of registry values for this path.

Name	Type	Data
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	REG_DWORD	0x00000010 (16)
HardwareID	REG_MULTI_SZ	USBSTOR\DiskKingstonDT_101_G2____PMAP USBS...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\Disk USBSTOR\RAW
ContainerID	REG_SZ	{c4c5303a-7059-503e-b205-4f10fa22c6f7}
ConfigFlags	REG_DWORD	0x00000000 (0)
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}
Driver	REG_SZ	{4d36e967-e325-11ce-bfc1-08002be10318}\0001
Class	REG_SZ	DiskDrive
Mfg	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
Service	REG_SZ	disk
FriendlyName	REG_SZ	Kingston DT 101 G2 USB Device