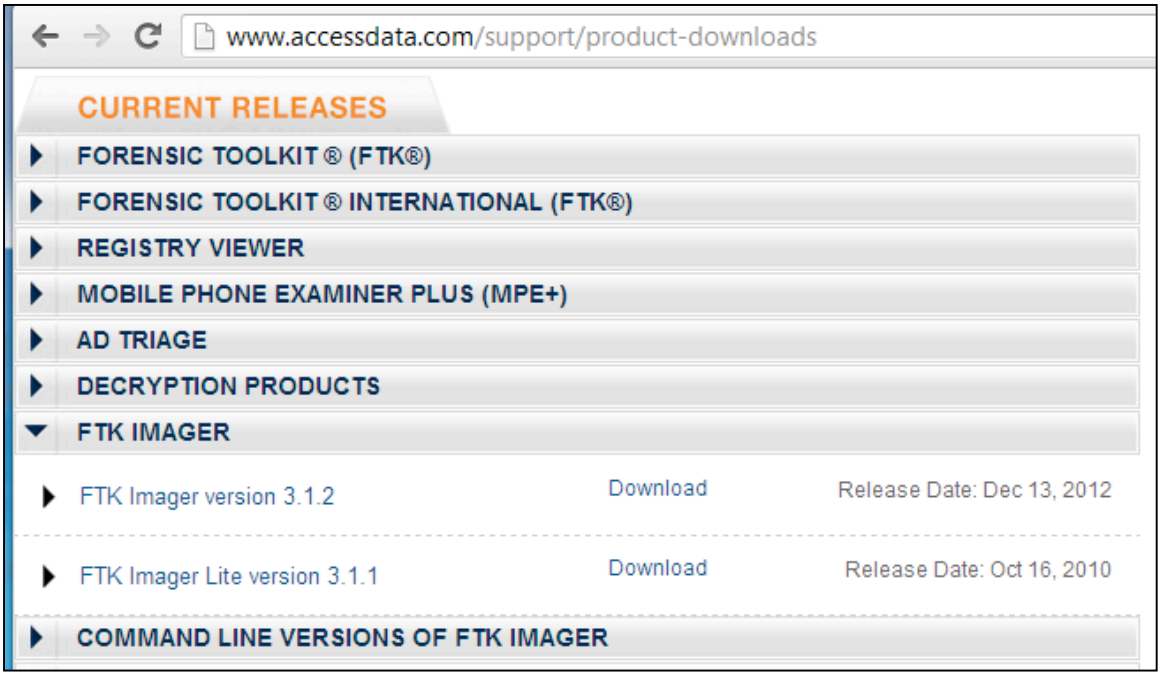
Project 4: Capture Registry menggunakan FTK Imager

Kebutuhan Project

- Komputer Windows, real atau virtual. Instruksi berikut menggunakan Windows 7.

Mendownload FTK Imager Lite

1. Buka browser dan arahkan ke **accessdata.com**
2. Di bagian pojok kanan atas, arahkan ke **SUPPORT**. Click "**Product Downloads**".
3. Pada bagian "Current Releases", buka bagian "**FTK Imager**", seperti terlihat di bawah. Di bagian baris "FTK Imager Lite version 3.1.1", click **Download** (atau bisa juga di download di elearning).
4. Masukan email address ketika diminta.
5. Simpan file pada folder Downloads.



Mendownload FTK Registry Viewer

6. Buka Web browser dan arahkan ke **accessdata.com**
7. Di sisi kanan atas, arahkan ke **SUPPORT**. Click "**Product Downloads**".

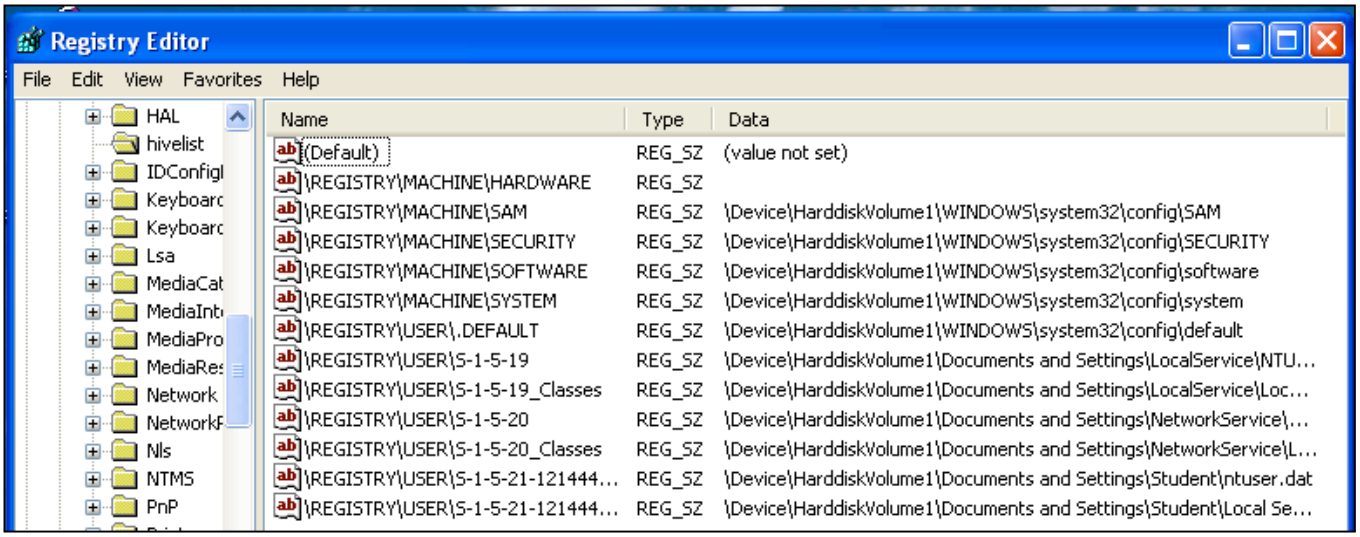
8. Pada bagian "Current Releases", buka bagian "**Registry Viewer**", seperti terlihat di bawah. Pada baris "Registry Viewer 1.6.3", click **Download**.
9. Simpan file pada folder Downloads.

Menginstall FTK Registry Viewer

10. Double-click file **AccessData Registry Viewer.exe** dan install software dengan options default.
11. Right-click file **Imager Lite 3.1.1.zip** dan click "**Extract All…**", **Extract**. Jendela "Downloads ▸ Imager_Lite_3.1.1" jendela terbuka memperlihatkan file-file yang diekstrak. Biarkan jendelanya terbuka.

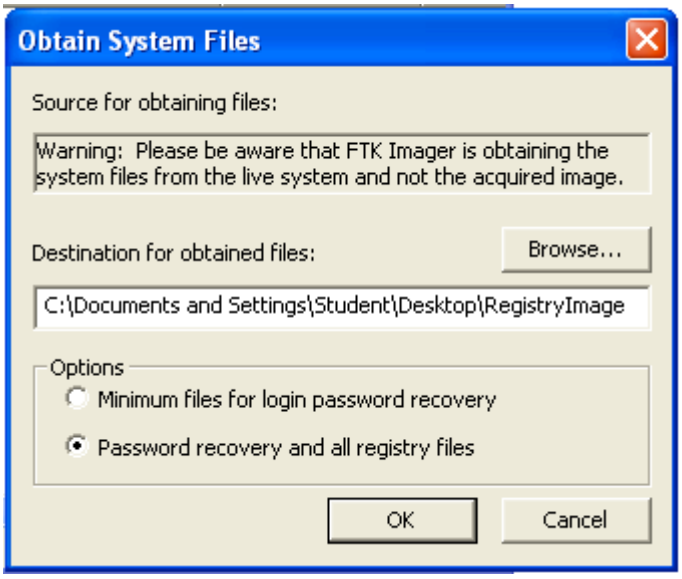
View Hive Files

12. Click **Start**. Ketikkan **REGEDIT** dan tekan Enter.
13. Pada Registry Editor, arahkan ke **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\HiveList**
14. Maka akan terlihat baris berisikan filr-file yang tersimpan di Registry, sperti terlihat di bawah ini. Pada project ini, kita akan meng-capture file-file tersebut, dan bukan file lain yang ada di disk. FTK Imager membuatnya menjadi lebih mudah!

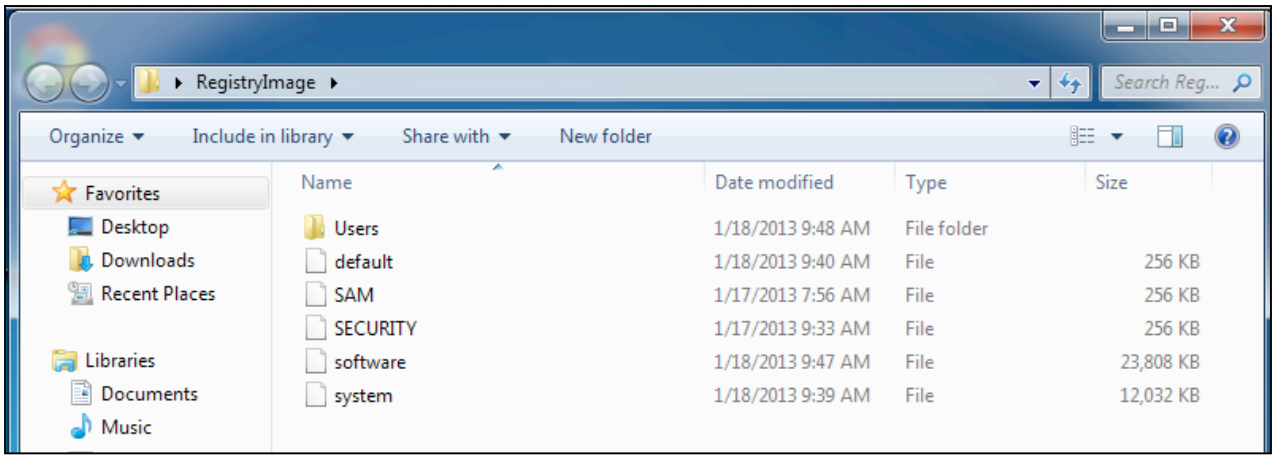


Membuat Registry Image dengan FTK Imager Lite

15. Pada jendela "Downloads ▸ Imager_Lite_3.1.1", double-click file **FTK Imager.exe**.
16. Pada jendela "AccessData FTK Imager 3.1.1", click **File**, "**Obtain Protected Files**".
17. Kotak "Obtain System Files" terbuka. ***Notice the Warning at the top of this box.*** Yang akan kita ambil adalah data dari komputer kita sendiri, bukan dari data evidence image.
18. Pada kotak "Obtain System Files", click tombol **Browse** dan arahkan ke desktop. Click tombol "**Make New Folder**", dan beri nama folder baru **RegistryImage**. Pilih folder **RegistryImage** dan click **OK**. Click tombol "**Password recovery and all registry files**", seperti terlihat di gambar. Click **OK**.



19. Tunggu hingga proses selesai. Hanya membutuhkan beberapa menit. Close FTK Imager.
20. Di jendela desktop, buka folder **RegistryImage**. Seharusnya berisi lima file dan satu folder seperti terlihat di bawah. Perhatikan nama-nama file tersebut –inilah yang dinamakan Hive Files, dan banyak kegiatan forensic yang membutuhkan file ini.

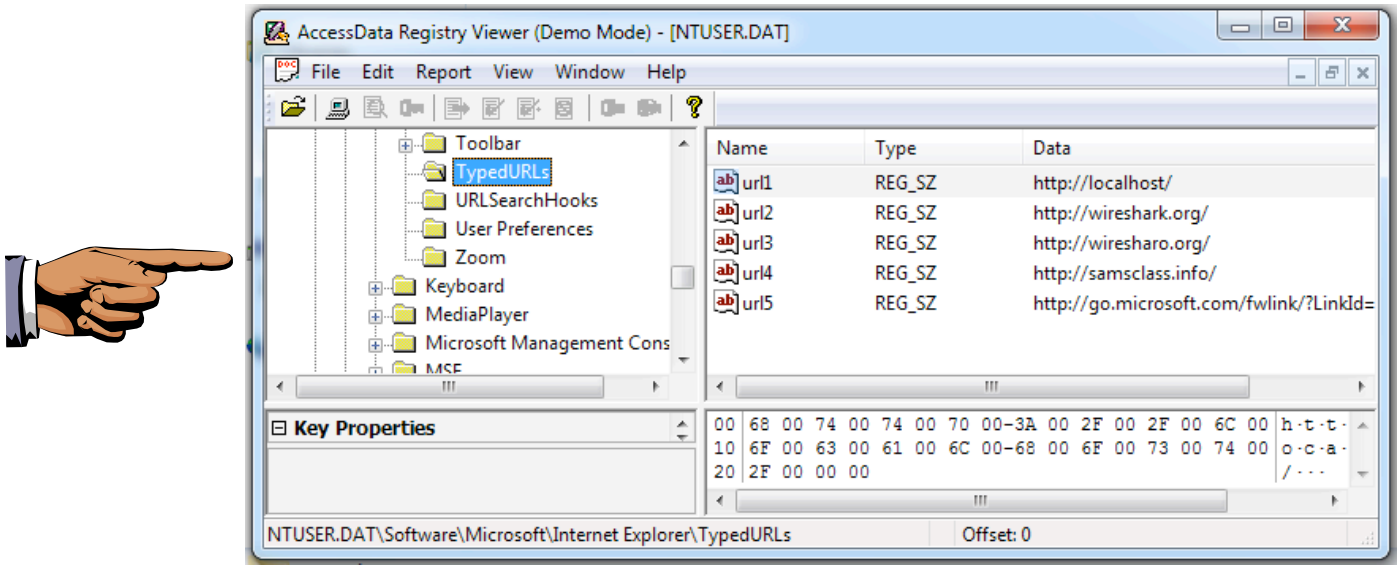


Melihat System Files

21. Pada jendela "RegistryImage", click **Organize**, "**Folder and Search Options**". Pada tab View, click tombol "**Show hidden files, folders, and drives**" dan buang tanda centang pada kotak "**Hide protected operating system files (Recommended)**". Click **OK**.

Menjalankan Registry Viewer

22. Pada desktop, click **Start**, **Registry Viewer**.
23. Pada kotak "No security device was found." Pada pesan ini menunjukkan kita menggunakan product in Demo mode, bukan full version. Click **No**.
24. Jotak pesan berisi "No dongle found." Click **OK**.
25. Pada Registry Viewer, click **File**, **Open**. Arahkan ke Desktop, dan buka file **RegistryImage\Users\Student\NTUSER.DAT**.
26. Registry Viewer sama dengan REGEDIT. Pada panel sebelah kiri, arahkan ke **Software\Microsoft\Internet Explorer\TypedURLs**. Panel sebelah kanan sekarang memperlihatkan URLS yang baru saja dikunjungi, seperti terlihat di sebelah kiri:



Simpan Screen Image

27. Pastikan di layar terlihat **TypedURLs** di sisi kiri.
28. Tekan tombol Printscreen. Simpan dengan nama **NamaKamu_Proj4** dengan format **PNG** atau **JPEG**.

Mengumpulkan Project

29. Kirim melalui elearning.

Last Modified: 3-20-13