

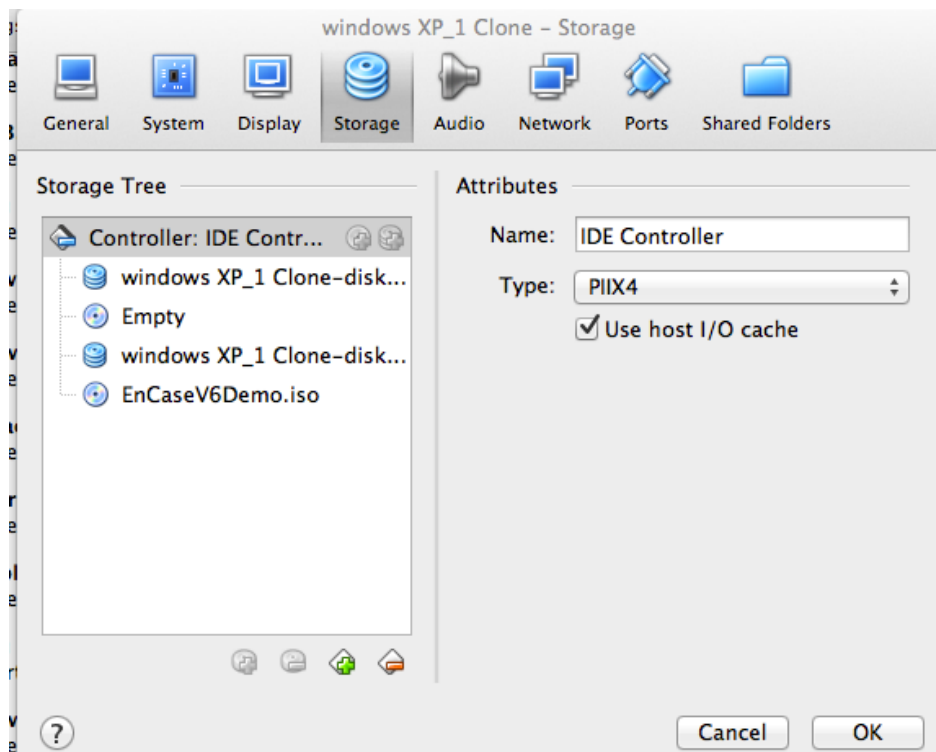
Project 18: Menggunakan Encase (15 pts.)

Kebutuhan Project

- Komputer Windows, real atau virtual. Bisa menggunakan Windows XP /7 virtual machine
- Encase Demo file (tersedia di lab)
- Instruksi berikut menggunakan Windows 7.

Download & Ekstrak File EnCaseV6Demo.zip

1. Copy the encaseV6demo.iso.zip file kemudian ekstrak sehingga menjadi encasedemo.iso.
2. Jika menggunakan Windows virtual, gandeng file ISO sebelum menjalankan Windows virtual. Dengan mengklik kanan icon Windows kemudian klik storage, tambahkan “add CD/DVD” arahkan ke file ISO yang sudah dibuat.



Menjalankan EnCaseDemo

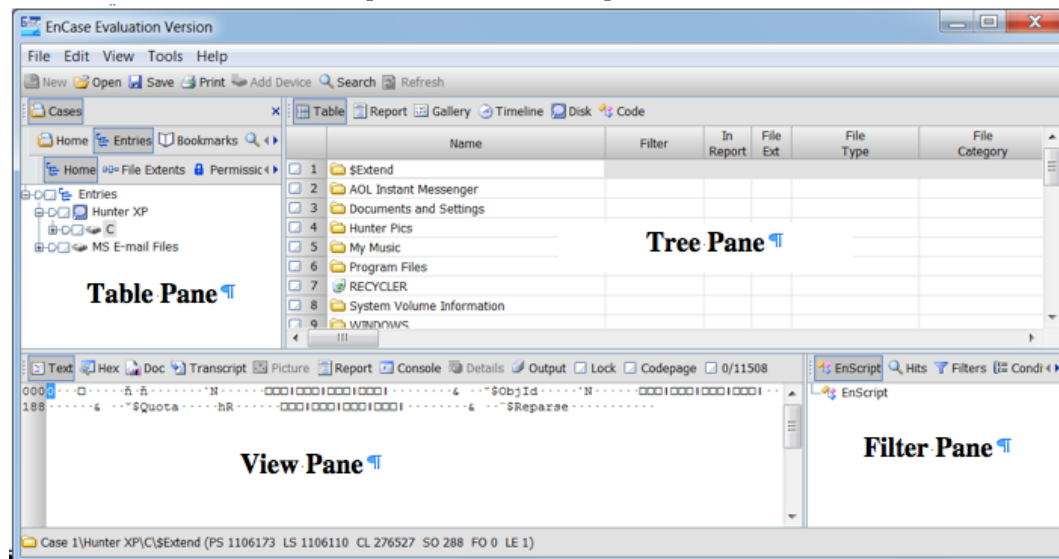
3. Jalankan Windows, kemudian buka Windows Explorer. Arahkan untuk membuka DVD EnCaseV6Demo yang sudah digandeng tadi.
4. Buka file encasedemo. Double-click **EnCaseDemo.exe**
5. Maka akan jalan Encase Evaluation version.

6. Pada folder encasedemo, cari file "**Hunter XP.E01**". Tarik file tersebut dan letakkan di jendela "EnCase Evaluation Version" window.
7. Pada kotak "Case Options", masukan PROJECT19, dan masukkan nama kalian sebagai "Examiner Name" dan click "**Finish**".
8. Jika satu atau lebih kotak pops up menanyakan untuk membuat folders, allow saja.
9. Pada folder encasedemo, cari file "**MS E-mail Files.E01**". Tarik dan letakkan ke jendela Encase.

EnCase Layout

Terdapat empat panel di jendela Utama EnCase:

- **Table Pane** – tempat untuk memilih device atau folder yang akan diperiksa
- **Tree Pane** – memperlihatkan files dan folders pada direktori aktif
- **View Pane** – memperlihatkan file atau folder dalam format Text, Hex, atau tampilan yang lain
- **Filter Pane** – memperlihatkan hasil pencarian atau filter



Memeriksa Tree Pane

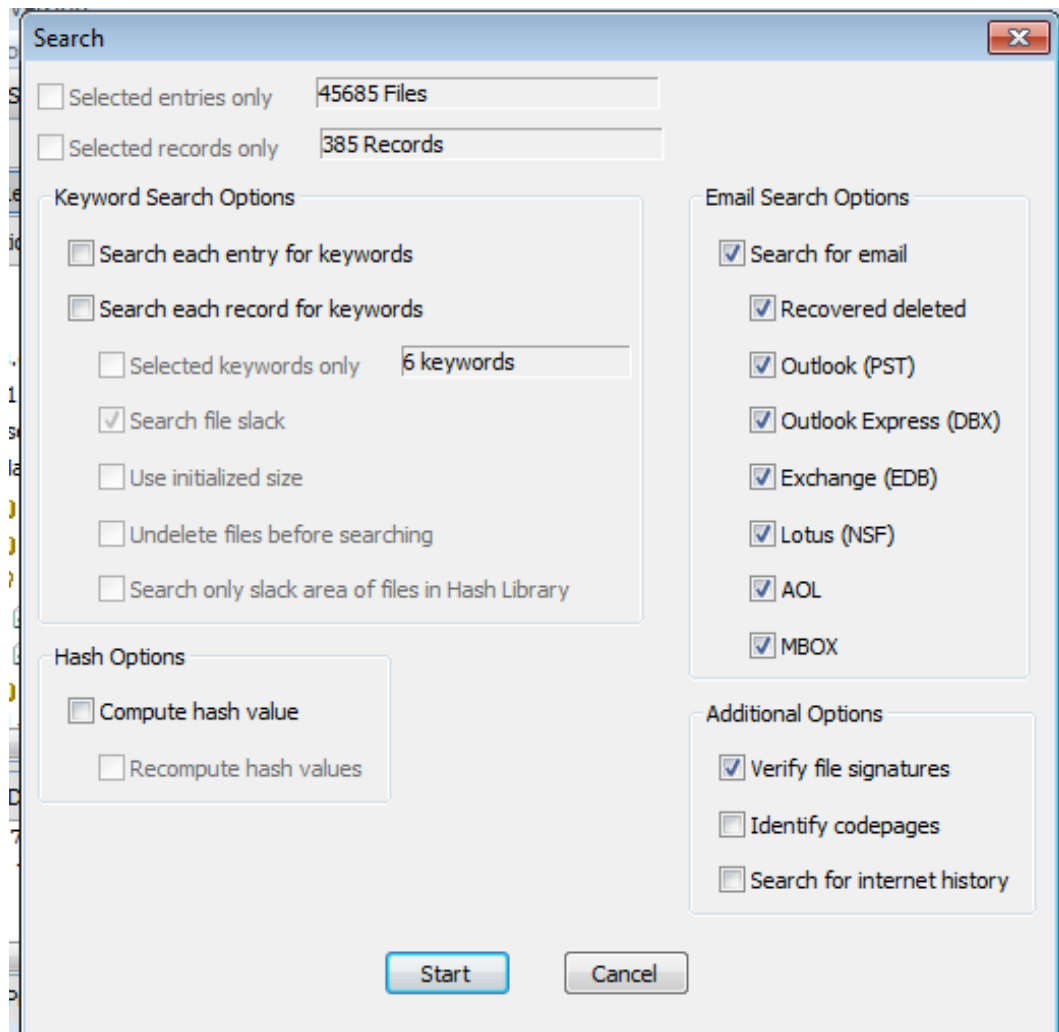
10. In the Table Pane, expand "**Hunter XP**" and click **C** to select the C: drive.
11. Pada Tree Pane memperlihatkan files pada direktori root C:. Gulung ke bawah dan click **boot.ini**.
12. Coba semua views pada Tree pane: Table, Report, Gallery, Timeline, Disk, and Code.

Pencarian Email

13. Pada bagian tengah atas jendela "EnCase Evaluation Version", click tombol **Search**.

14. Pada kotak Search box, di sebelah kanan, click kotak "**Search for email**", dan check semua jenis email. Di sisi kiri, bersihkan semua centang, seperti terlihat di bawah ini.

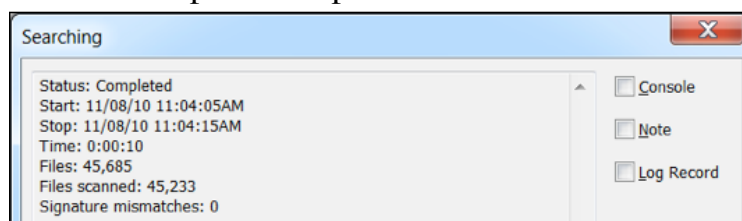
Hasil pencariannya sekitar 2 menit.



Click tombol **Start** .

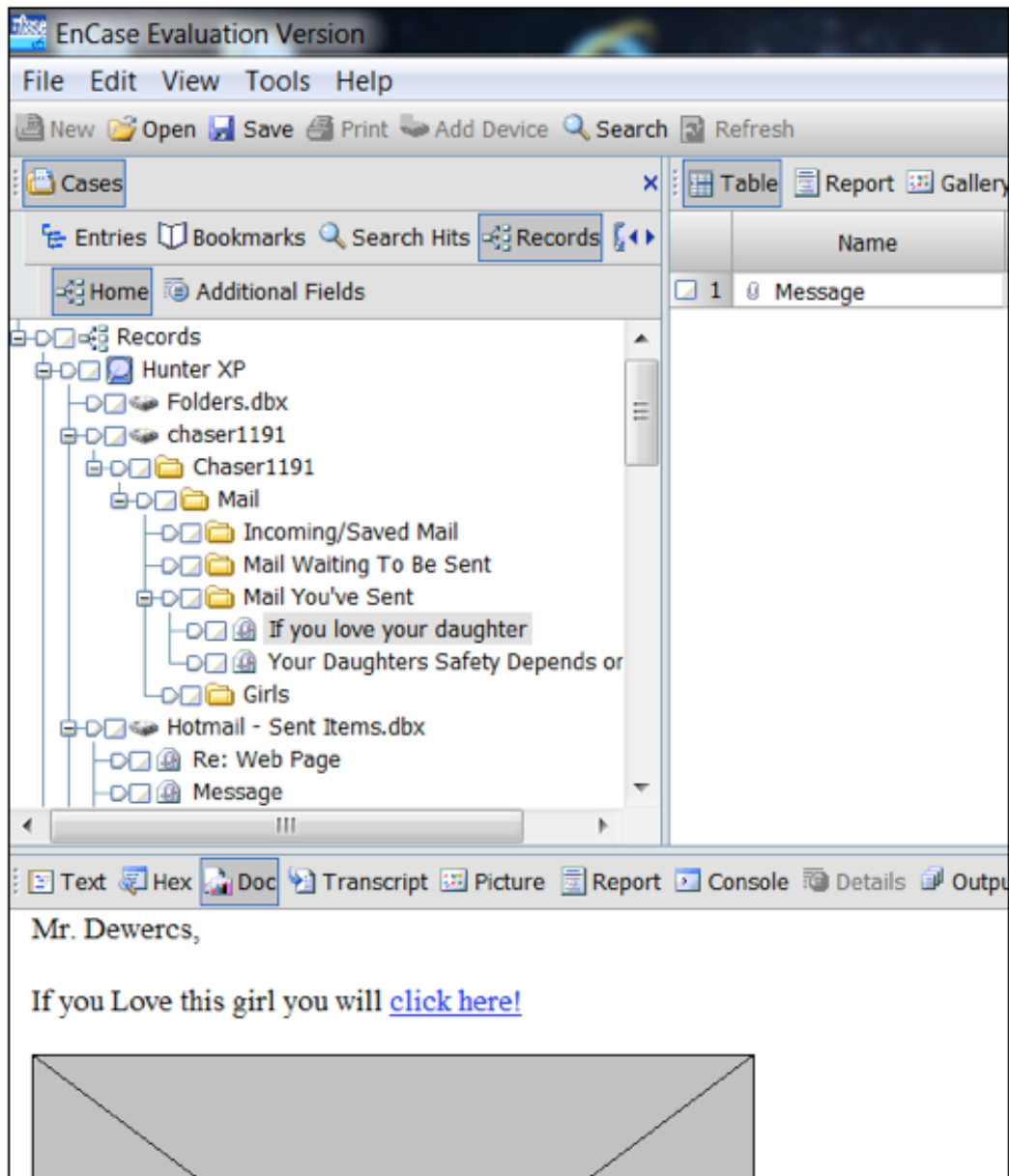
Proses pencarian berjalan dengan dua little progress bars terlihat pada bawah kanan jendela "EnCase Evaluation Version".

15. Ketika hasil pencarian selesai, suatu kotak pops up akan muncul "Completed" seperti terlihat di bawah ini. Click **OK**.



Melihat Hasil Pencarian

16. Dari menu "EnCase Evaluation Version", click **View**, "**Cases Sub-Tabs**", **Records**.
17. Akan terlihat tree entries pada Table Pane. Gunakan panah ke bawah untuk melihat tiap baris dan membaca emails pada View Pane pada kiri bawah. Seperti yang terlihat, kasus ini berisi rencana penculikan anak.

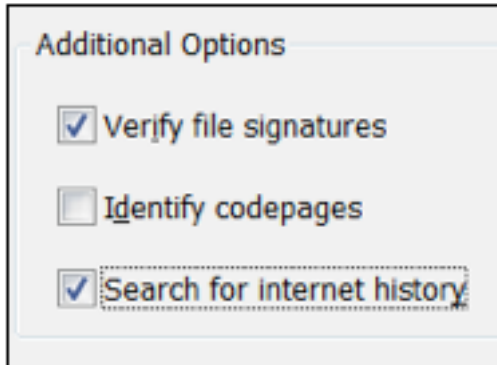


Mencari License Plate Number

18. Cari emails dan temukan photo orang (yang bisa jadi korban) meletakkan gas di mobil. Cari plat nomor mobil dan tulisdalam file teks.
19. Jika perlu click thumbnail untuk melihatnya dalam ukuran full size.

Pencarian Internet History/Cache

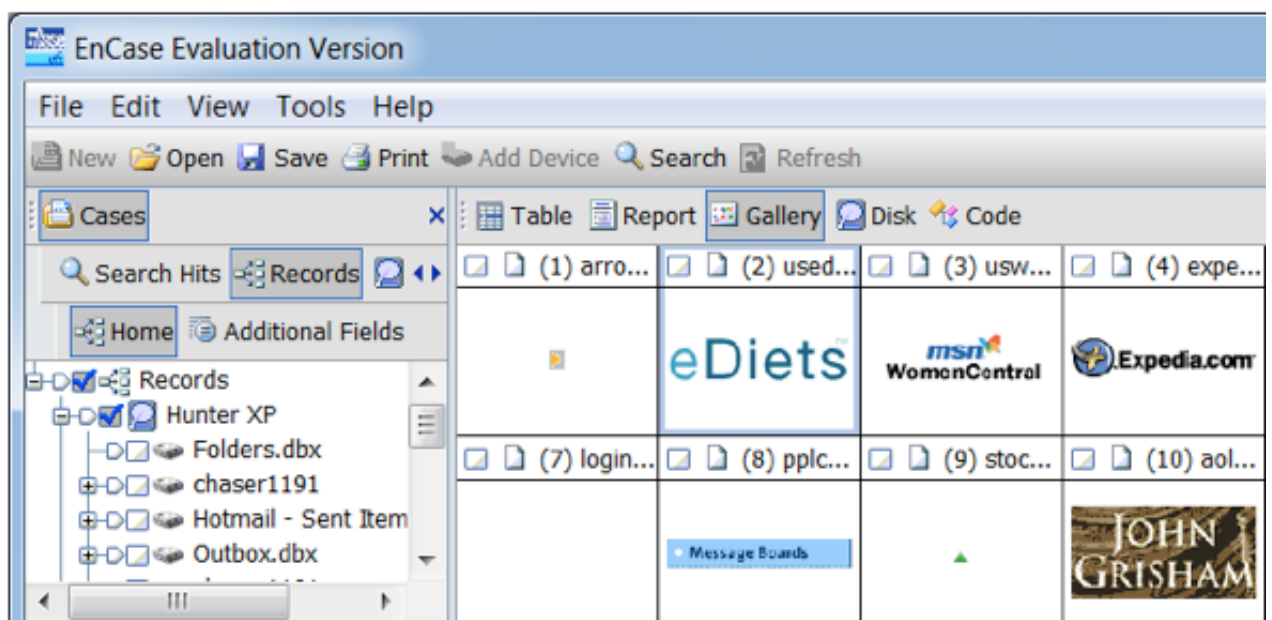
20. Pada bagian atas jendela "EnCase Evaluation Version" window, click tombol **Search**.
21. Pada kotak Search, pada sisi kanan, cari kotak "**Search for email**", seperti berikut.



22. Pada bagian bawah, check kotak "**Search for internet history**". Click tombol **Start**.
23. Ketika kotak Searching pops up, mengatakan "Completed", click **OK**.

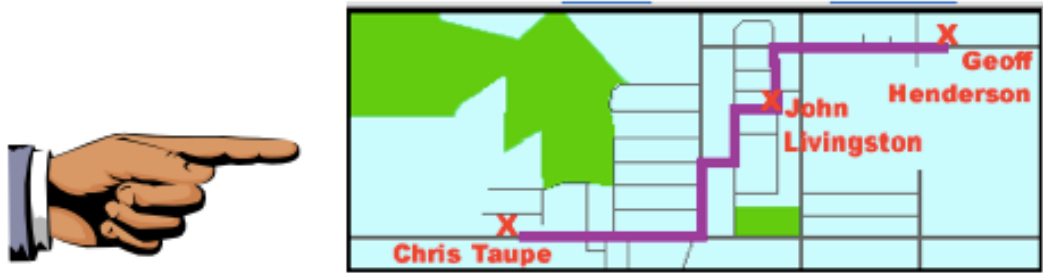
Melihat Hasil Pencarian

24. Dari menu "EnCase Evaluation Version", click **View**, "**Cases Sub-Tabs**", **Records**.
25. Pada Table Pane, buka "**Hunter XP**" dan buka **C**.
26. Buka "**Internet Explorer (Windows)**". Click **Cache** untuk memilihnya.
27. Pada Tree Pane, click **Gallery**. Kotak grid memperlihatkan gambar dari cache muncul, seperti berikut ini.



Mencari Peta

28. Cari seluruh gambar untuk menemukan peta seperti di bawah ini. Ketika ketemu, pilih pada Tree Pane dan pilih **Picture** pada View Pane, maka bisa terlihat versi kecil dari peta pada Tree Pane dan peta ukuran penuh pada View Pane.



Simpan Screen Image

29. Pastikan terlihat gambar peta pada gambar di atas. Simpan dengan nama file "**NamaKamu_Proj18**".

Mengumpulkan Project

30. Kirim melalui elearning.

Last Modified: 28-5-13