

Nama: Moh irvan afandi
Nim: 1310651094
Kelas: B

Cari software atau tools pendukung keamanan informasi kemudian cobalah fungsional software tersebut untuk menangani kasus tertentu. Buatlah step by step yang terdiri dari screenshot, keterangan gambar, dan analisis. Misalnya penggunaan Wireshark dalam melakukan analisis paket data jaringan (pcap file), penggunaan FTK Forensic untuk mengetahui file steganografi, dan lain sebagainya. Review software boleh sama, akan tetapi kasusnya harus berbeda dengan teman-temannya.

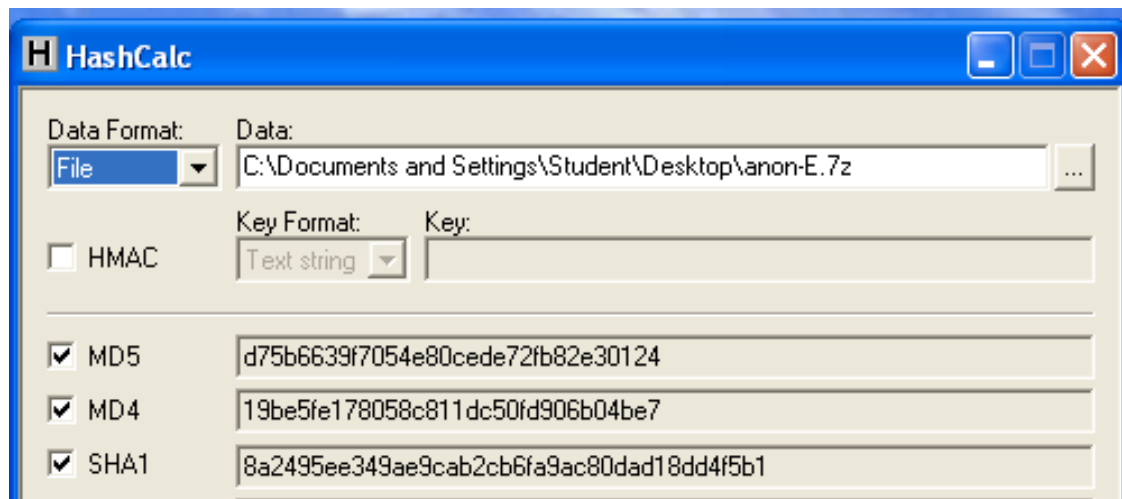
Project: Menggunakan FTK

Kebutuhan Project

- Komputer Windows, real atau virtual. Bisa menggunakan Windows XP /7 virtual machine.

Mendownload Evidence File

1. Download file evidence
2. Gunakan Hashcalc (bisa di download di sini : <http://www.slavasoft.com/hashcalc/>) untuk menghitung nilai hash dari file yang didownload. Hasilnya harusnya sama dengan berikut:



Lakukan Unzip dengan software 7-Zip (yang bisa didownload di : <http://www.7-zip.org/download.html>).

Menginstall FTK

3. Download file yang tersedia di elearning "**FTK-Forensic_Toolkit-1.81.6.exe**" install software dengan default options.

Menjalankan FTK

4. Setelah proses instalasi, jalankan FTK. **Cat: Jika menggunakan Windows 7 klik kanan icon dan pilih "Run as Administrator".**
 - a. Ketika ada pesan Error "No security device was found...", click **No**.
 - b. Jika ada pesan Error box "The KFF Hash library file was not found...", click **OK**.
 - c. Ketika ada kotak pops up menjelaskan keterbatasan versi demo, click **OK**.

Memulai Kasus Baru

5. Pada korak "AccessData FTK Startup", pilih "**Start a new case**" dan click **OK**.
 - a. Pada layar berjudul titled "Wizard for Creating a New Case", isi seperti berikut seperti terlihat di gambar, rubah "YOUR_NAME" menjadi nama kalian. click **Next**.

New Case

Find, Organize, & Analyze Computer Evidence

Forensic Toolkit®
Find Computer Evidence Quickly and Easily

**AccessData's
Forensic Toolkit®-FTK®**
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name: Your name

Case Information

Case Number: 18-YOURNAME

Case Name: 18-YOURNAME

Case Path: c:\ Browse...

Case Folder: c:\18-YOURNAME

Case Description:

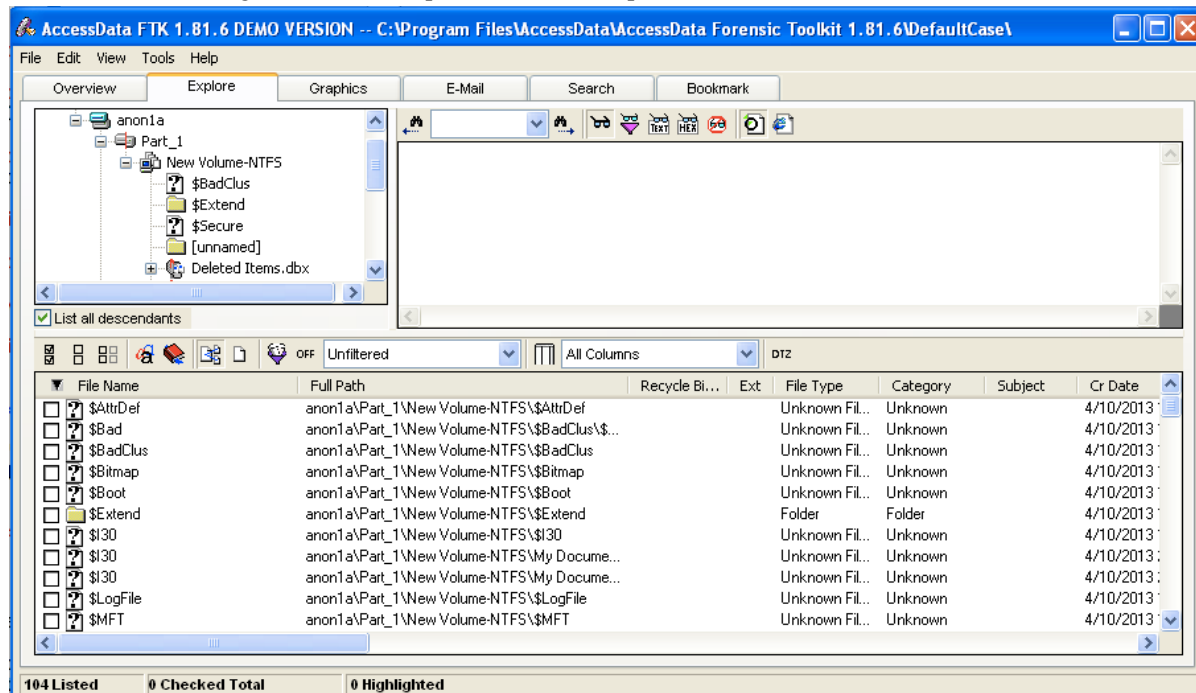
Next > Cancel

- b. Pada layar berjudul "Forensic Examiner Information", biarkan fields nya kosong dan click **Next**.
- c. Pada layar yang bagian "Case Log Options", biarkan pihan default, yang akan mencatat semua log. click **Next**.
- d. Pada bagian "Processes to Perform", buang pilihan "**KFF Lookup**" dan "**Decrypt EFS Files**". click (Next Karena untuk versi demo fitur ini tidak tersedia).
- e. Pada bagian "Refine Case-Default", pilih default "Include All Items". click **Next**.
- f. Pada bagian "Refine Index - Default", click **Next**.

Menambahkan Evidence

6. Pada kotak "Add Evidence", click tombol "**Add Evidence...**"..
 - a. Pada bagian kotak "Add Evidence to Case", pilih "Acquired Image of Drive", dan click Continue.
 - b. Pada kotak "Browse for Folder", arahkan ke Desktop, buka folder "E", dan double-click file **anon1a.E01**.
 - c. Pada kotak "Evidence Information", click **OK**.
 - d. Pada kotak "Add Evidence", click **Next**.
 - e. Pada kotak "New Case Setup is Now Complete", click **Finish**.
 - f. Kotak pesan "Processing Files..." akan muncul. Tunggu beberapa detik sampai proses selesai.
 - g. Click tab **Explore**.

- h. Pada kiri tengah, entang kotak **"List all Descendants"**. Akan terlihat deretan files, dengan **"104 Listed"** pada Status Bar, seperti terlihat di bawah ini.



Background Kasus

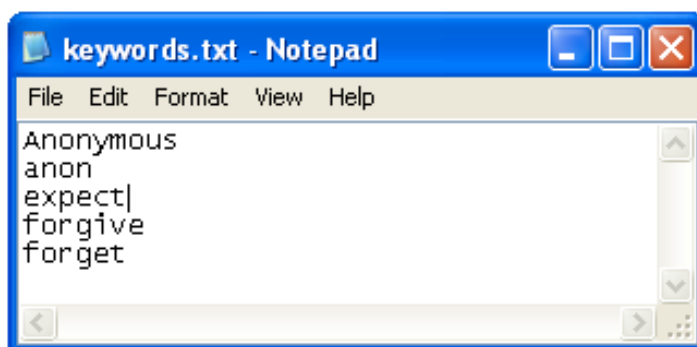
7. Barang bukti diambil dari komputer yang ditemukan di ruangan yang digunakan oleh tersangka hacker komputer dari Anonymous gang.

Prosedur Pencarian 1: File-demi-file

8. Pada panel bagian bawah FTK, click item yang pertama. Cari pada panel kanan atas apa yang ada pada file. Tekan panah ke bawah pada keyboard untuk pindah ke file berikutnya. 20 file yang pertama berisi sangat sedikit informasi yang berguna –bisa kita lihat, cara seperti ini tidak efisien untuk mencari barang bukti yang relevan.

Prosedur Pencarian 2: Pencarian Keyword

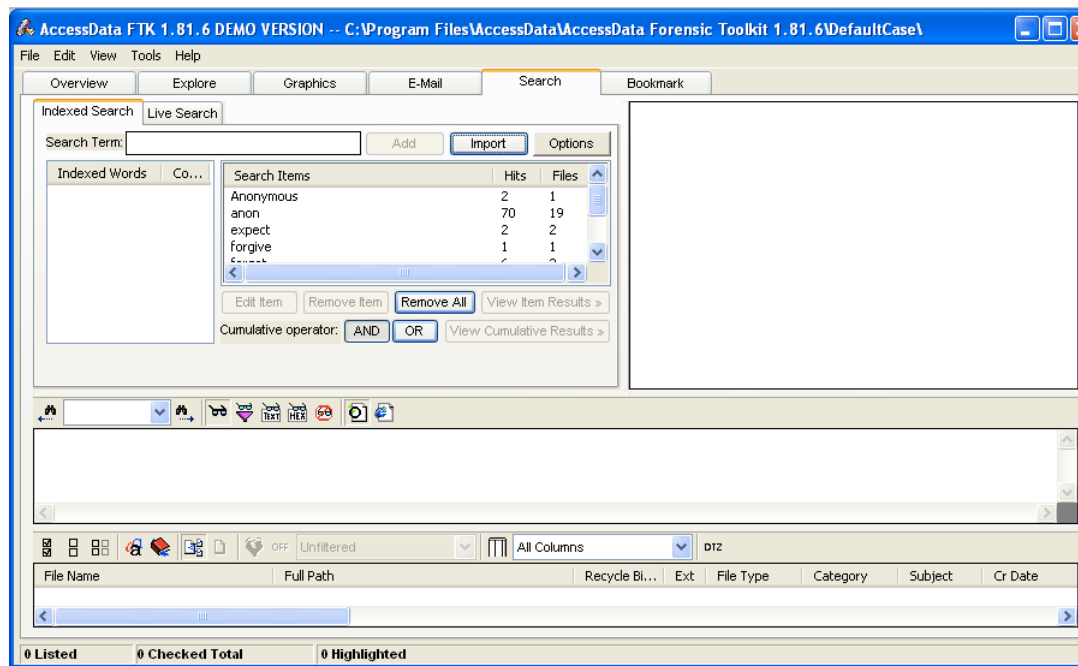
9. Prosedur yang lebih baik dengan menggunakan pencarian keyword. FTK didesain untuk bekerja dengan cara ini – dengan cara membuat index dari daftar pada file evidence. Buka Notepad dan ketikkan keywords yang terlihat pada gambar di bawah ini. Misalnya seperti kita ketahui pada kasu melibatkan gang Anonymous, keywords juga berasal dari slogan gang Anonymous "Expect Us" dan "We never forgive, we never forget".



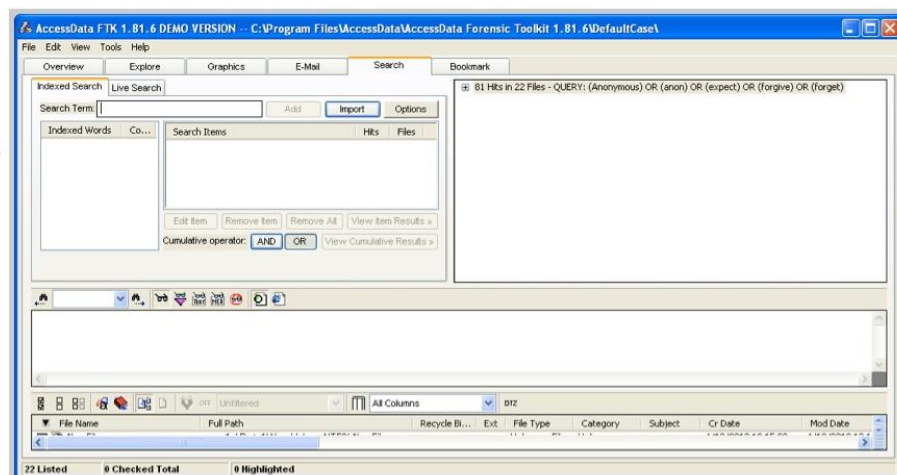
- Simpan file di desktop sebagai "keywords.txt".
- Pada FTK, click tab **Search**.
- Click tombol **Import**.
- Pada kotak "Import Search Terms", arahkan ke desktop dan double-click file **keywords.txt**.
- Kotak pop up "Import Search Terms" muncul, yang mengatakan 'Do you wish to show items that have 0 hits?'. Click **No**.

Hasil Pencarian

10. Lima keywords ditemukan, seperti berikut pada panel atas FTK:



- Pada baris "Cumulative Operator", click tombol **OR**.
- Pada baris "Cumulative Operator", click tombol **View Cumulative Results**.
- Pada kotak "Filter Search Hits", terima pilihan default "All files" dan click tombol **OK**.
- Pada panel kanan atas terlihat "81 Hits in 22 Files", seperti berikut.



Simpan Screen Image

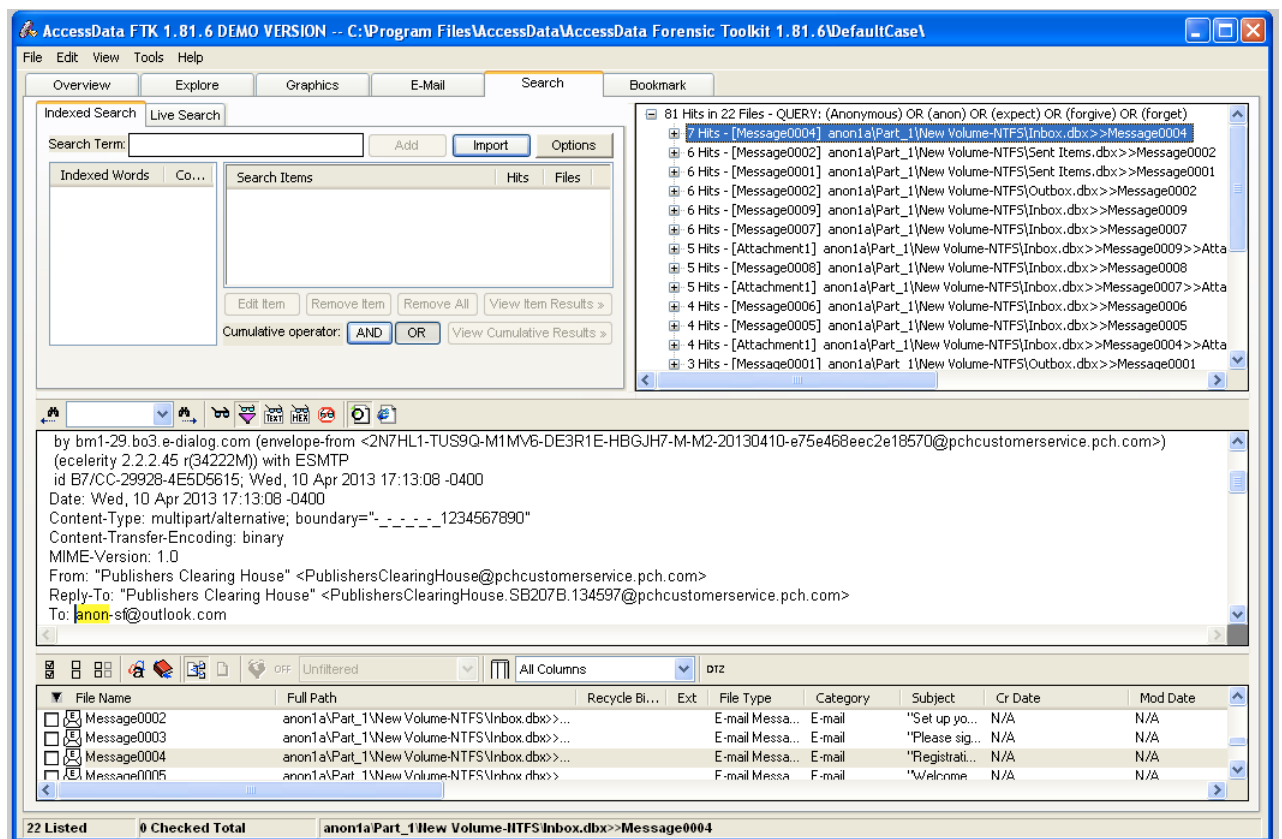
11. Pastikan di layar terlihat "81 Hits in 22 Files". Tekan PrintScrn key untuk mengkopir seluruh desktop.

UNTUK MENDAPAT POIN MAKSIMAL KUMPULKAN DESKTOP IMAGE KESELURUHAN.

Simpan dengan nama file "NamaKamu_Project15a".

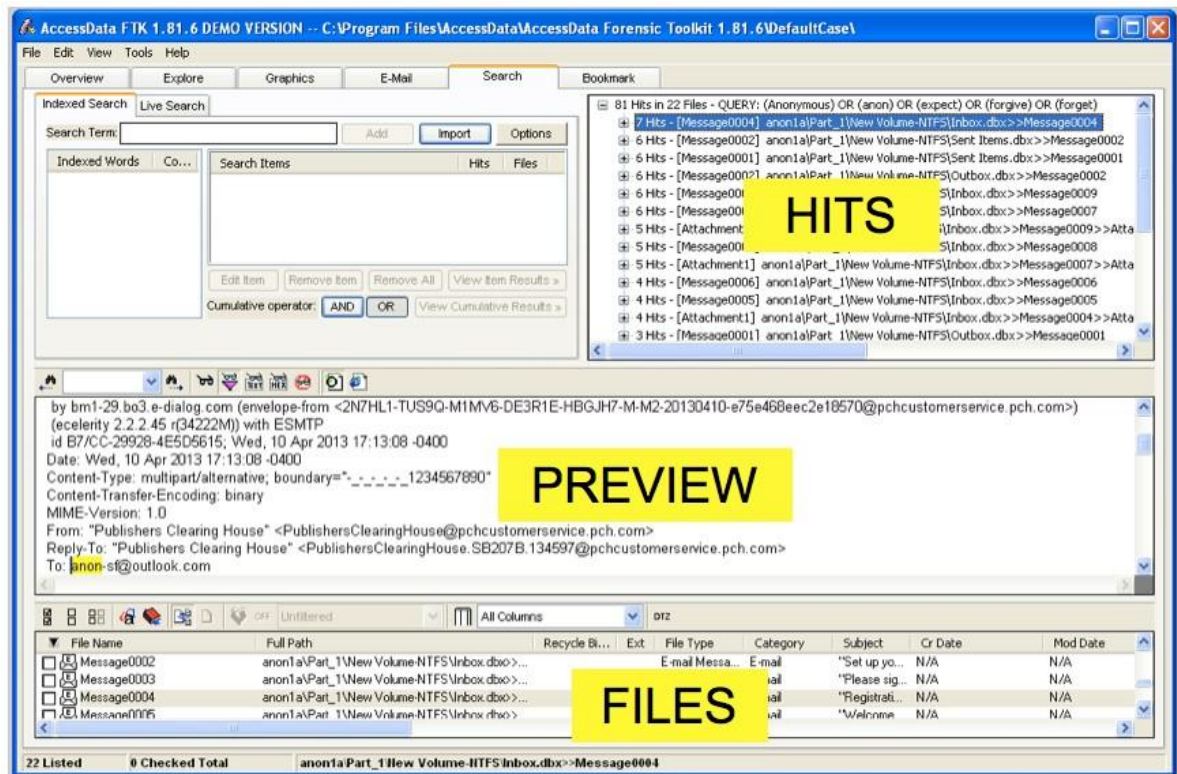
Memeriksa Hits

12. Click item pertama pada panel kanan atas. Item ini berisi, label "81 Hits in 22 Files". Expand dengan menekan panah kanan key di keyboard. Kemudian tekan panah ke bawah untuk ke item berikutnya, yang berlabel "[7 Hits -- Message004]".
13. Di layar akan terlihat seperti pada gambar berikut. File ini merupakan email message, dan bisa di baca pada panel bawah-tengah. File ini jelas berupa unimportant spam.



Prosedur

14. Berikut ini cara memeriksa hits dengan cepat. Ikuti petunjuk berikut.
 - a. Pada bagian HITS di kanan atas, tekan panah ke bawah untuk memilih item berikutnya.
 - b. Perhatikan PREVIEW pada layar tengah.
 - c. Jika filenya penting, check kotak pada baris yang berbayang pada bagian FILES di bawah layar.



- d. Proses sampai semua 22 files dengan cara ini.
- e. Cari email yang berisi kejahatan kriminal, dan beberapa file yang dicurigai.

Simpan Screen Image

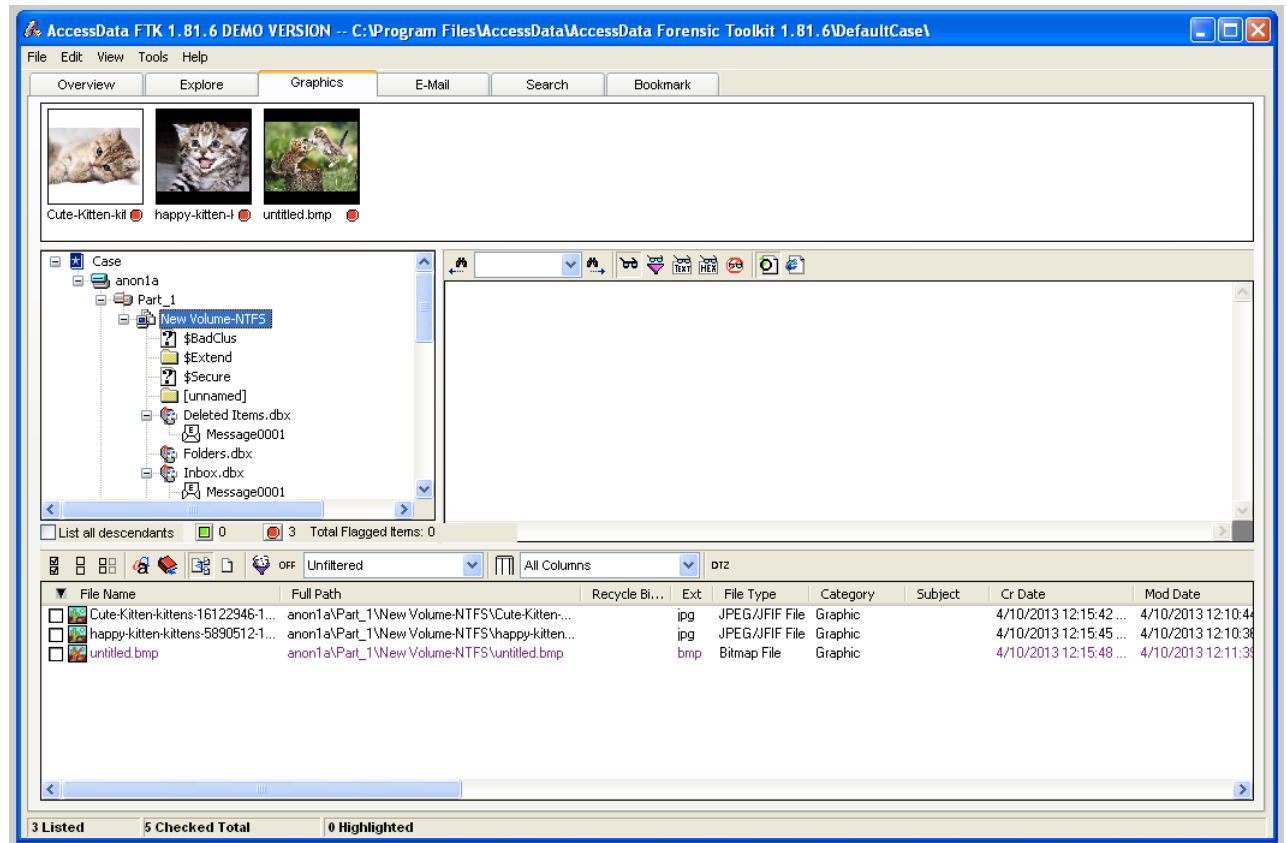
15. Pastikan di layar menampilkan email berisi kejahatan criminal yang ditemukan. Tekan tombol PrintScrn key.

HARUS MENGUMPULKAN COMPLETE DESKTOP IMAGE UNTUK MENDAPATKAN POIN MAKSIMAL.

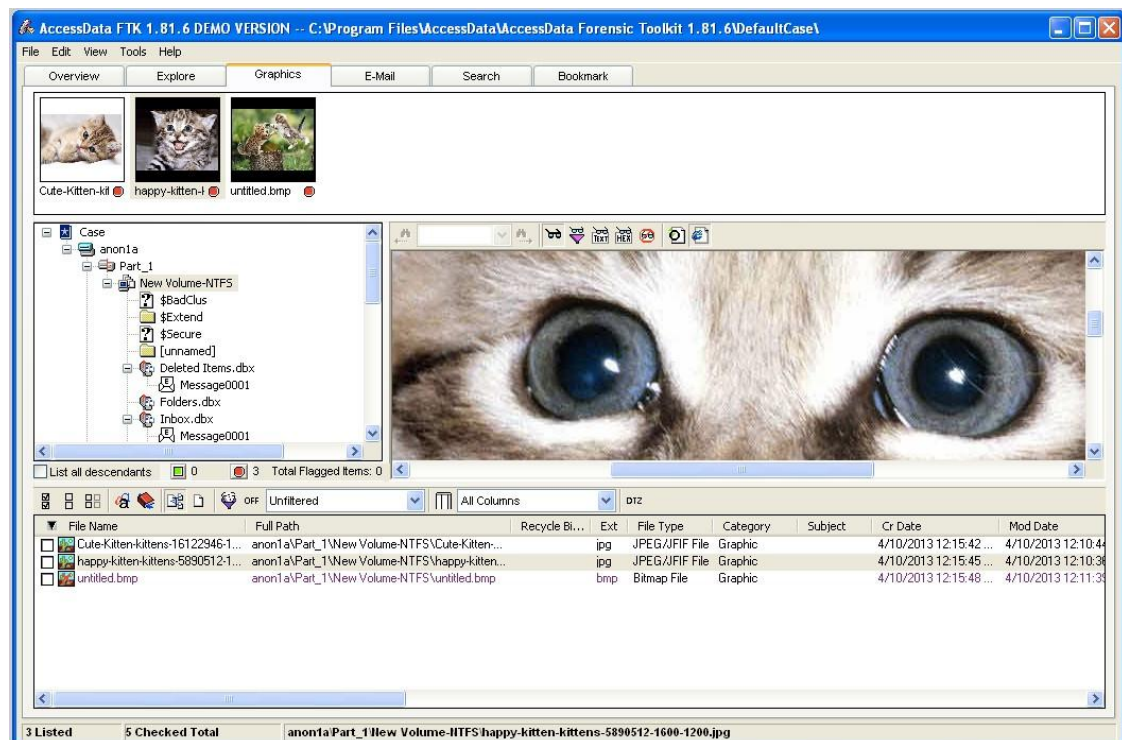
Simpan gambar dengan nama file "NamaKamu_Proj15b".

Melihat Gambar

16. Salah satu kelemahan pencarian menggunakan pencarian keyword adalah tidak akan menemukan kata dalam gambar. Untuk melihat gambar, click tab **Graphics** pada bagian atas jendela FTK.
 - a. Pada kiri tengah, terdapat tiga struktur yang memperlihatkan file dan folder. Click item teratas, **Case**, dan gunakan panah ke bawah untuk pindah ke item berikutnya.
 - b. Ketika ingin membuka folder, gunakan panah kanan untuk membukanya.
 - c. Ketika memilih folder yang berisi gambar di dalamnya, akan terlihat thumbnails pada panel atas seperti berikut:



- d. Kucing tersebut memang bukan bentuk kejahatan, tapi coba lihat lebih dekat untuk meyakinkan.
- e. Pada panel atas, click salah satu dari thumbnails. Maka gambar akan terlihat dalam ukuran penuh pada panel kanan atas, seperti berikut:



- f. Lanjutkan dengan memeriksa semua folder sampai ditemukan gambar yang mencurigakan. Tandai semua gambar yang mencurigakan dengan mencentang kotak pada panel bawah, seperti yang dilakukan pada email messages.
- g. Salah satu gambar memperlihatkan halaman Web yang diserang. Pastikan mendapatkannya untuk membuktikan penyerangan.

Simpan Screen Image

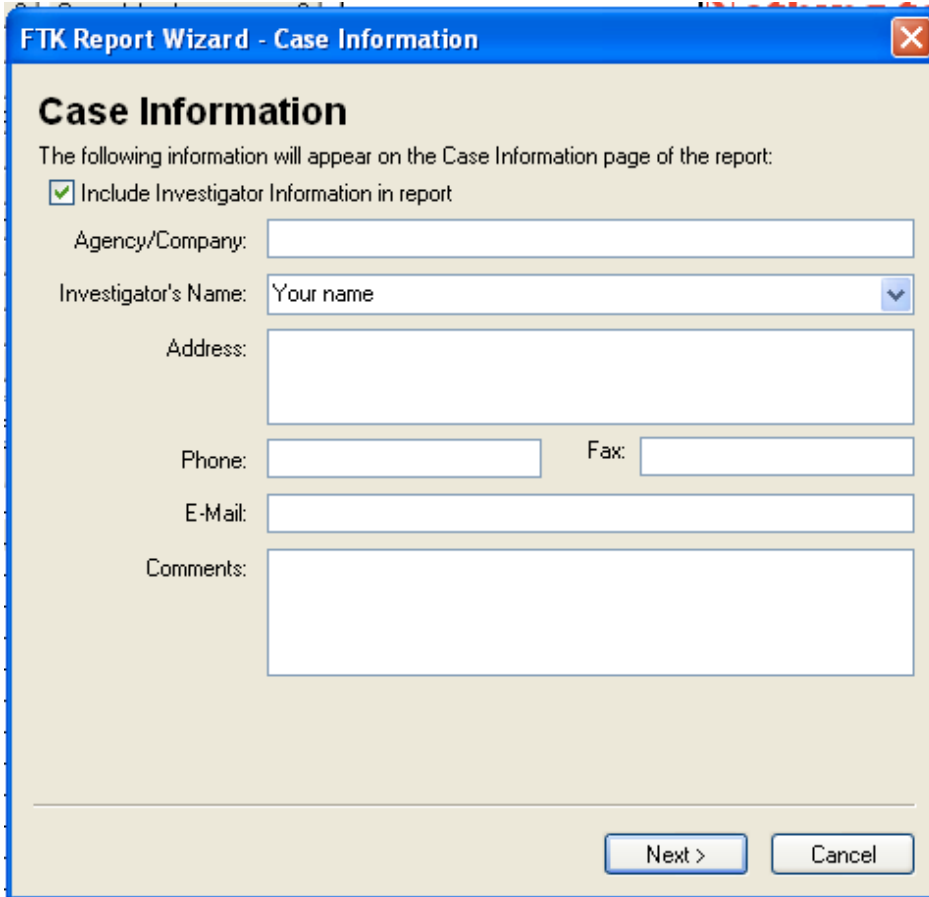
17. Pastikan di layar menampilkan gambar yang berisi kejahatan criminal yang ditemukan. Tekan tombol PrintScrn key.

HARUS MENGUMPULKAN COMPLETE DESKTOP IMAGE UNTUK MENDAPATKAN POIN MAKSIMAL.

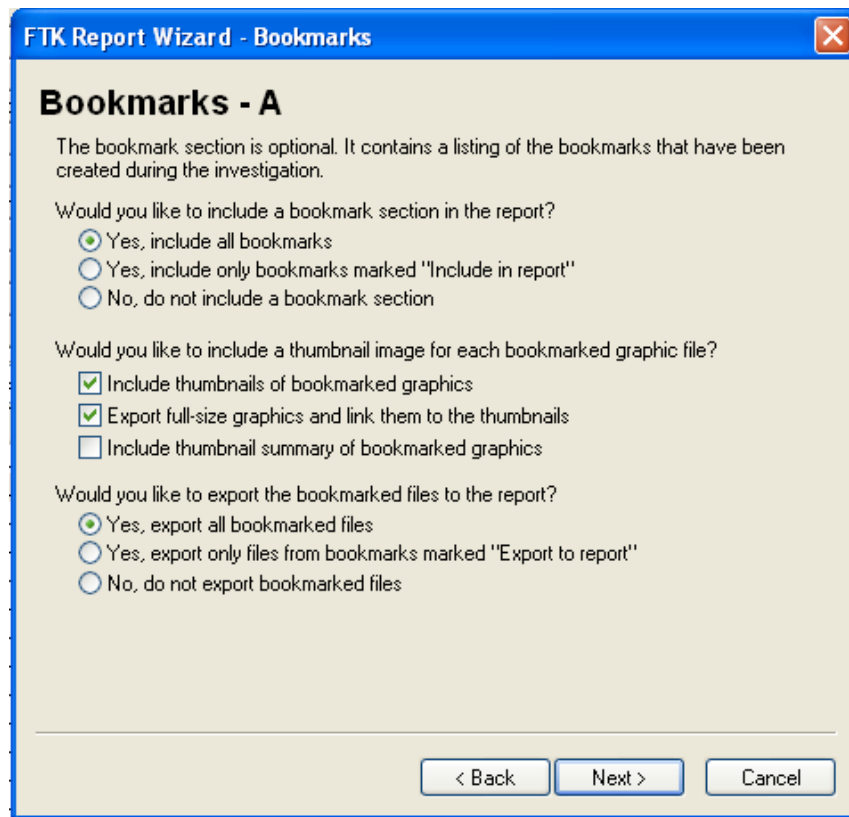
Simpan gambar dengan nama file "**NamaKamu_Proj15c**".

Membuat Report/Laporan

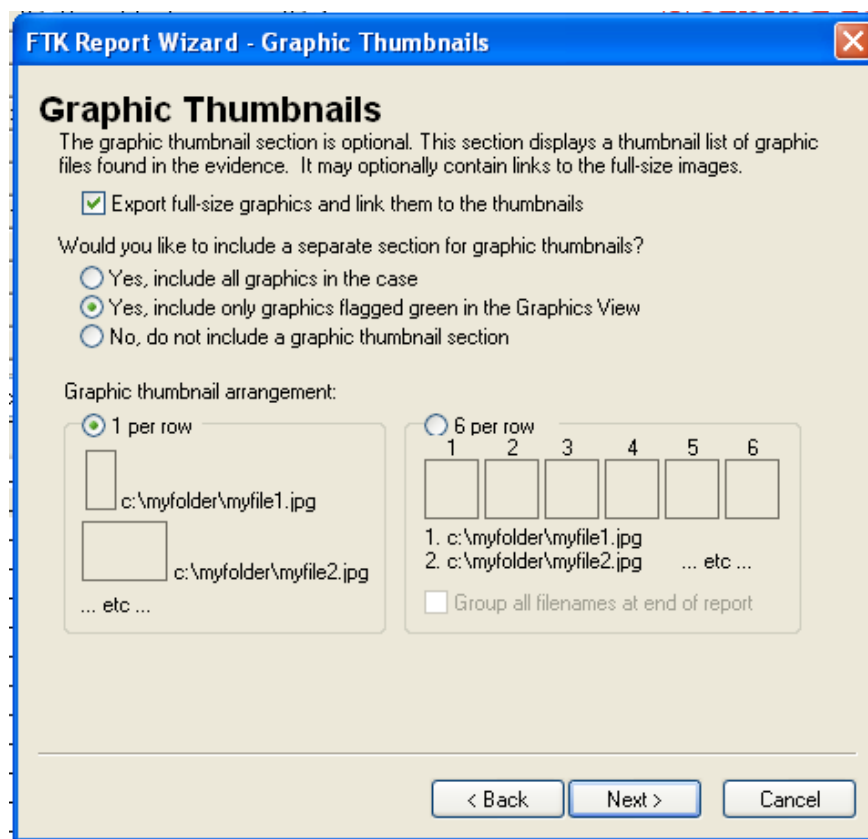
18. Pada FTK, dari baris menu bagian atas, click **File**, "**Report Wizard**".
- a. Pada bagian "Case Information", click **Next**, seperti terlihat di bawah ini.



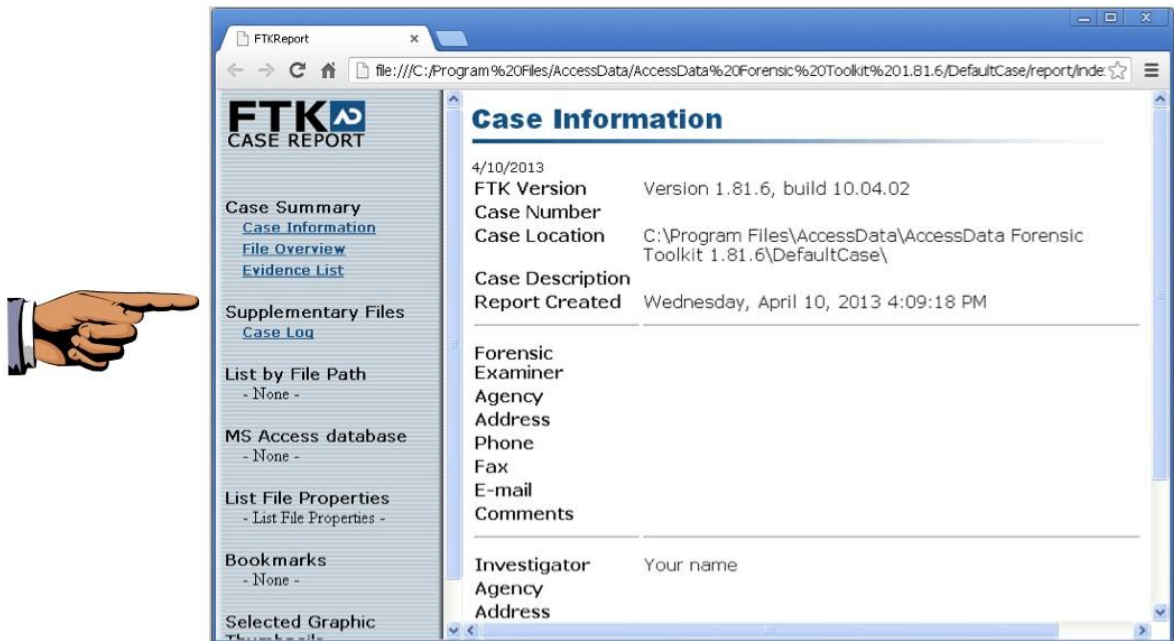
- b. Pada halaman "Bookmarks - A", click tombol "**Yes, export all bookmarked files**", seperti terlihat di bawah ini. Kemudian click **Next**.



- c. Pada halaman "Bookmarks - B", click **Next**.
- d. Pada halaman "Graphic Thumbnails", click "**Export full-size graphics and link them to the thumbnails**", seperti berikut. Kemudian click **Next**.



- e. Pada halaman "List by File Path", click **Next**.
- f. Pada halaman "List File Properties - A", click **Next**.
- g. Pada halaman "Supplementary Files", click **Next**.
- h. Pada halaman "Report Location", click **Finish**.
- i. Kotak pop up "Report Wizard" akan muncul, menanyakan "Do you wish to view the report?".
- j. Click **Yes**.
- k. Report muncul, seperti berikut.



Simpan Screen Image

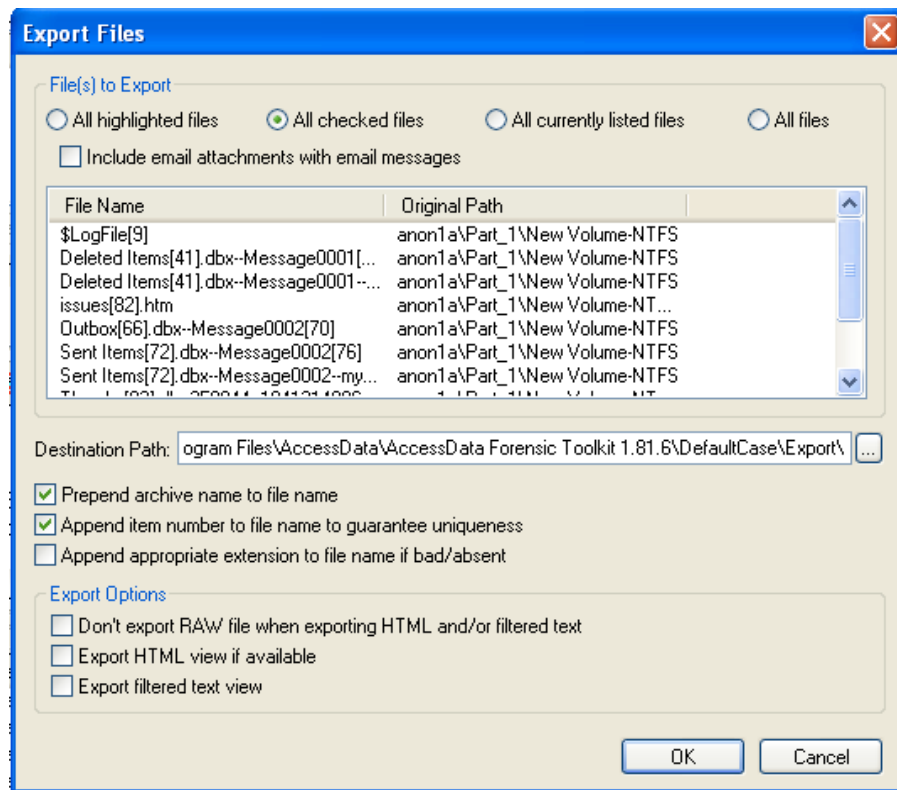
19. Pastikan di layar menampilkan report dengan nama kalian Investigator seperti terlihat di atas. Tekan tombol PrintScrn key.

HARUS MENGUMPULKAN COMPLETE DESKTOP IMAGE UNTUK MENDAPATKAN POIN MAKSIMAL.

Simpan gambar dengan nama file "NamaKamu_Proj15d".

Mengekspor File yang dipilih

20. Pada Report tidak menyertakan file yang dipilih –kita perlu melakukannya secara terpisah.
 - a. Pada FTK, dari baris menu atas, click **File**, "**Export Files**".
 - b. Pada kotak "Export Files", click "**All checked files**", seperti berikut. Kemudian click **OK**.



- c. Untuk melihat file yang diekspor, click **Start, Computer**, dan arahkan ke folder C:\Program Files\AccessData\AccessData Forensic Toolkit 1.81.6\DefaultCase\Export".
- d. File-file tersebut akan terlihat seperti berikut.

