

LAPORAN
KEAMANAN INFORMASI
TUGAS UAS



Oleh :

Riska Novia Nur Dianti

1310651194

TI-A

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH JEMBER
2014/2015

Tugas 1

Domain 10:

Fisik (Lingkungan) Keamanan

TUJUAN UJIAN DALAM BAB INI

- Pertahanan Perimeter
- Pemilihan, Desain, dan Konfigurasi
- Pertahanan Sistem
- Kontrol Lingkungan

PENGANTAR

Fisik (lingkungan) keamanan melindungi kerahasiaan dan integritas fisik aset: orang, bangunan, sistem, dan data. Ujian CISSP® menganggap manusia keselamatan sebagai perhatian yang paling penting dari domain ini, yang mengalahkan semua kekhawatiran lainnya.

PERIMETER DEFENSES

Pertahanan perimeter membantu mencegah, mendeteksi, dan akses fisik tidak sah yang benar. Bangunan, seperti jaringan, harus menggunakan pertahanan berlapis. sehingga aset penting yang harus dilindungi oleh beberapa kontrol keamanan fisik, seperti pagar, pintu, dinding, kunci, dll yang dapat mencegah, dan jika memungkinkan, menawarkan otentikasi dan akuntabilitas.

Fenses

Pagar harus dirancang untuk mengarahkan masuknya dan jalan keluar untuk poin dikendalikan, seperti pintu eksterior dan gerbang.

Gates

Gates/gerbang dirancang untuk mencegah akses.

FAST FACT

Berikut adalah empat kelas gerbang:

- Kelas I: Residential (digunakan di rumah)
- Kelas II: Komersial / Umum Akses (garasi parkir)

- Kelas III: Industri / Terbatas Access (dok pemuatan untuk truk 18 roda)
- Kelas IV: akses terbatas (bandara atau penjara)

Bollards

Sebuah tonggak lalu lintas untuk menghentikan kendaraan

Lights

Lampu dapat bertindak sebagai detektif dan kontrol jera. Cahaya harus terang cukup untuk menerangi bidang yang diinginkan visi (daerah yang dilindungi).

CCTV

Closed-Circuit Television (CCTV) adalah perangkat detektif yang digunakan untuk penjaga bantuan dalam mendeteksi kehadiran penyusup di daerah terlarang.

Locks

Kunci adalah kontrol keamanan fisik preventif, digunakan pada pintu dan jendela untuk mencegah akses fisik tidak sah.

Key locks

Key locks memerlukan kunci fisik untuk membuka. Kunci dapat dibagi atau kadang-kadang disalin, yang menurunkan akuntabilitas kunci kunci

Combination locks

Kunci kombinasi adalah masalah keamanan utama mengenai jenis kunci.

Smart cards and magnetic stripe cards

Kartu pintar adalah perangkat kontrol akses fisik yang sering digunakan untuk elektronik kunci, pembelian kartu kredit, atau sistem otentikasi dual-faktor.

Sebuah kartu magnetic stripe berisi strip magnetik yang menyimpan informasi. mereka digunakan dengan menggesekkan melalui kartu reader.

Tailgating/piggybacking

Tailgating terjadi ketika orang yang tidak berwenang dalam gedung. Kebijakan melarang karyawan dari memungkinkan Tailgating demi keamanan upaya menjelaskan risiko ini.

Mantraps and turnstiles

Sebuah jebakan kontrol fisik preventif dengan dua pintu. Setiap pintu biasanya membutuhkan bentuk terpisah dari otentikasi untuk membuka. Penyusup terjebak antara pintu setelah memasuki jerat tersebut.

Contraband checks

Contraband checks untuk mengidentifikasi benda-benda yang dilarang untuk memasuki aman. Seperti mendeteksi logam, senjata, atau bahan peledak

Motion detectors and other perimeter alarms

Ultrasonik dan gerak microwave detektor bekerja seperti "radar Doppler" yang digunakan untuk memprediksi cuaca. Gelombang energi dikirim keluar (Seperti orang yang berjalan di berbagai sensor

Sebuah sensor pasif dapat dianggap sebagai "read-only" perangkat. Contohnya adalah inframerah (PIR) sensor pasif, yang mendeteksi energi infra merah diciptakan oleh panas tubuh.

Doors and windows

Selalu mempertimbangkan kekuatan dan kelemahan relatif dari pintu, jendela, dinding, lantai, langit-langit, dll Semua harus sama-sama kuat dari sudut pandang defensif:

Walls, floors, and ceilings

Dinding di sekitar perimeter aman setiap internal seperti pusat data harus "slab untuk slab, "yang berarti mereka harus mulai dari lantai slab dan lari ke slab langit-langit.

Guards

Penjaga kontrol dinamis yang dapat digunakan dalam berbagai situasi. Yang telah mengikuti pelatihan lanjutan atau sekolah amatir penjaga.

Dogs

Anjing menyediakan perimeter tugas pertahanan. Kelemahan utama untuk menggunakan anjing sebagai kontrol perimeter adalah tanggung jawab hukum.

SITE SELECTION, DESIGN, AND CONFIGURATION

Seleksi, desain, dan konfigurasi menggambarkan proses membangun fasilitas yang aman seperti pusat data, dari proses pemilihan lokasi melalui desain akhir.

Site selection issues

Pemilihan lokasi adalah proses memilih situs untuk membangun gedung atau pusat data.

Utility reliability

Keandalan utilitas lokal untuk pemilihan lokasi.

Crime

Tingkat kejahatan lokal juga faktor dalam pemilihan lokasi. Masalah utama adalah keselamatan karyawan.

Site design and configuration issues

Setelah situs telah dipilih, sejumlah keputusan desain harus dibuat.

Site marking

Banyak pusat data tidak eksternal ditandai untuk menghindari menarik perhatian fasilitas termasuk menghindari rincian seperti desain bangunan diredam.

Shared tenancy and adjacent buildings

Penyewa lain dalam kasus bangunan menimbulkan masalah keamanan.

SYSTEM DEFENSES

Pertahanan sistem adalah salah satu garis pertahanan terakhir dalam strategi pertahanan-mendalam. Pertahanan ini mengasumsikan penyerang memiliki akses fisik ke perangkat atau media yang mengandung informasi sensitif.

Asset tracking

Rinci database pelacakan aset meningkatkan keamanan fisik. Anda tidak dapat melindungi data anda kecuali Anda tahu di mana (dan apa) itu.

Port controls

Komputer modern mungkin berisi beberapa "port" yang memungkinkan menyalin data ke atau dari sistem. Kontrol pelabuhan sangat penting karena sejumlah besar informasi dapat ditempatkan pada perangkat yang cukup kecil untuk menghindari perimeter cek selundupan.

Drive and tape encryption

Drive dan enkripsi pita melindungi data pada saat istirahat dan merupakan salah satu dari sedikit kontrol yang akan melindungi data setelah keamanan fisik telah dilanggar.

Media storage and transportation

Semua data backup sensitif harus disimpan off-site atau dipindahkan sebagai media backup

Media cleaning and destruction

Semua bentuk media harus aman dibersihkan atau dihancurkan sebelum dibuang untuk mencegah reuse objek, seperti file komputer. Benda dapat bersifat fisik (seperti file-file kertas di manila folder) atau elektronik (data pada hard drive).

Paper shredders

pemotong kertas untuk mencegah penggunaan kembali objek

Overwriting

Timpa menulis lebih setiap karakter dari file atau seluruh disk drive dan jauh lebih mengamankan dari menghapus atau memformat disk drive

Degaussing and destruction

digunakan untuk mencegah serangan menggunakan kembali objek terhadap media magnetik seperti

ENVIRONMENTAL CONTROLS

Kontrol lingkungan dirancang untuk memberikan lingkungan yang aman bagi personil dan peralatan. Listrik, HVAC, dan keselamatan kebakaran dianggap kontrol lingkungan.

Electricity

Listrik yang dapat diandalkan sangat penting untuk data center dan merupakan salah satu prioritas utama saat memilih, membangun, dan merancang sebuah situs. Kesalahan listrik melibatkan pendek dan jangka panjang gangguan listrik, serta berbagai kasus tegangan rendah dan tinggi.

Surge protectors, UPSs, and generators

Pelindung gelombang melindungi peralatan dari kerusakan akibat lonjakan listrik. Mereka berisi sirkuit atau sekering yang tersandung selama lonjakan listrik atau lonjakan, korslet listrik.

Uninterruptible Power Supplies (UPS) menyediakan tenaga cadangan sementara jika terjadi pemadaman listrik.

HVAC

HVAC (pemanas, ventilasi, dan pendingin udara) kontrol menjaga udara, suhu dan kelembaban. Hal ini membantu mengurangi debu dan kontaminan udara lainnya.

Static and corrosion

Statis diatasi dengan menjaga kelembaban yang tepat. Tingkat kelembaban yang tinggi dapat memungkinkan air di udara mengembun ke peralatan, yang dapat menyebabkan korosi.

Heat, flame, and smoke detectors

Detektor peringatan ketika suhu melebihi sebuah dasar yang aman didirikan. Detektor asap bekerja melalui dua metode utama: ionisasi dan fotolistrik. Sensor fotolistrik bekerja dengan cara yang sama, menghasilkan biaya kecil saat menerima cahaya. Detektor api mendeteksi inframerah atau ultraviolet cahaya yang dipancarkan dalam api

Personnel safety, training, and awareness

Keselamatan personil adalah nomor satu tujuan keamanan fisik. Pelatihan keselamatan memberikan keterampilan mengatur seperti belajar untuk mengoperasikan sistem tenaga darurat. pelatihan keselamatan dan kesadaran sangat penting untuk memastikan keberhasilan fisik program keamanan

Evacuation routes

Rute evakuasi harus jelas diposting, karena mereka berada di kamar hotel. Semua personil harus diberitahukan mengenai rute evakuasi tercepat dari daerah mereka. Semua situs harus menggunakan titik pertemuan, di mana semua personil akan bertemu dalam acara darurat

Evacuation roles and procedures

Kedua peran evakuasi utama adalah sipir keamanan dan pemimpin titik pertemuan. Itu Sisir keselamatan memastikan bahwa semua personel aman mengevakuasi bangunan dalam hal keadaan darurat.

ABCD fires and suppression

Isu keamanan utama dalam kasus kebakaran adalah evakuasi yang aman. Sistem ini biasanya dirancang dengan keselamatan personel sebagai primary perhatian.

Kelas agen kebakaran dan penindasan

Bahan kimia digunakan untuk memadamkan kebakaran kelas sesuai penyebab kebakarannya.

Types of fire suppression agents

Semua agen pencegah kebakaran bekerja melalui empat metode. mengurangi suhu api, mengurangi pasokan oksigen, mengurangi pasokan bahan bakar, dan campur dengan reaksi kimia dalam api.

Water

Air menekan api dengan menurunkan suhu di bawah titik ranting Air adalah yang paling aman dari semua agen penekan dan dianjurkan untuk pemadam kebakaran terbakar umum seperti kertas terbakar atau kayu.

Soda acid

Pemadam menggunakan asam soda dicampur dengan air. menciptakan busa yang dapat mengapung di permukaan beberapa kebakaran cair, kelaparan suplai oksigen.

Dry powder

Pemadam api dengan bubuk kering (seperti natrium klorida) bekerja dengan menurunkan suhu dan mencekik api, kelaparan itu oksigen. Bubuk kering terutama digunakan untuk memadamkan kebakaran logam.

Wet chemical

Bahan kimia basah untuk memadamkan kebakaran dapur ini mencakup minyak atau minyak api dalam film sabun yang menurunkan suhu.

CO₂

Kebakaran membutuhkan oksigen sebagai bahan bakar, sehingga kebakaran dapat menahan dengan menghapus oksigen. yang hanya direkomendasikan di daerah unstaffed seperti gardu listrik.

Halon and Halon substitutes

Halon memadamkan api melalui reaksi kimia yang mengkonsumsi energi dan menurunkan suhu api.

Montreal Accord

Halon memiliki ozon properti. Karena efek ini, 1989 Protokol Montreal (Secara resmi disebut "Protokol Montreal mengenai Bahan yang Merusak Ozon Layer ") dilarang produksi dan konsumsi Halon baru di negara-negara maju 1 Januari 1994. Ada sistem Halon dapat digunakan.

Sprinkler systems

Sistem Preaction adalah kombinasi dari basah, kering, atau sistem banjir dan memerlukan dua pemicu terpisah untuk melepaskan air. Sistem single-interlock melepaskan air ke pipa ketika alarm kebakaran memicu. Rilis air sekali kepala terbuka.

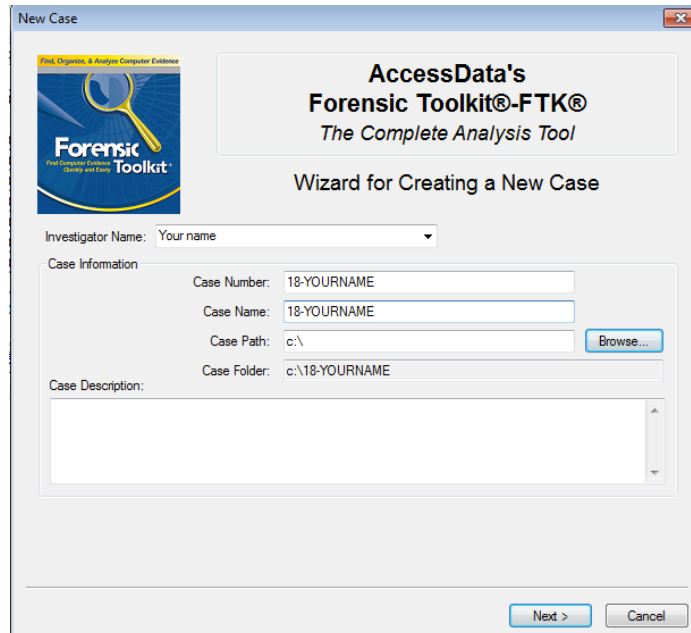
Portable fire extinguishers

Semua alat pemadam kebakaran portable harus ditandai dengan jenis api untuk memadamkan. Alat pemadam portabel harus cukup kecil untuk dioperasikan oleh personel setiap yang mungkin perlu menggunakan satu.

Tugas 2

Memulai Kasus Baru

1. 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**.

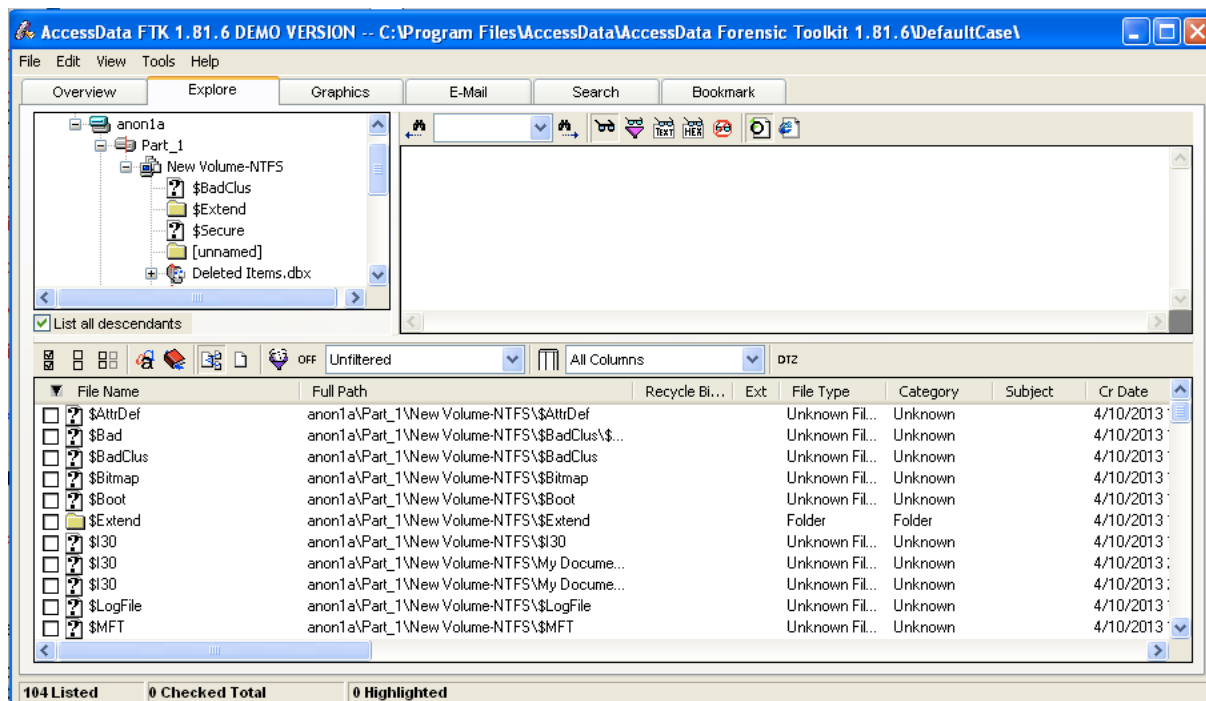


- b. Pada layar berjudul "Forensic Examiner Information", biarkan fields nya kosong dan click **Next**.
 - c. Pada layar yang bagian "Case Log Options", biarkan pihan default, yang akan mencatat semua log. click **Next**.
 - d. Pada bagian "Processes to Perform", buang pilihan "**KFF Lookup**" dan "**Decrypt 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

2. 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 doubleclick 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

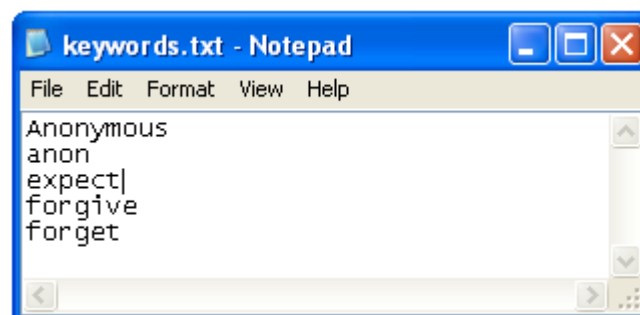
3. Barang bukti diambil dari komputer yang ditemukan di ruangan yang digunakan oleh tersangka hacker komuter dari Anonymous gang.

Prosedur Pencarian 1: File-demi-file

4. 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

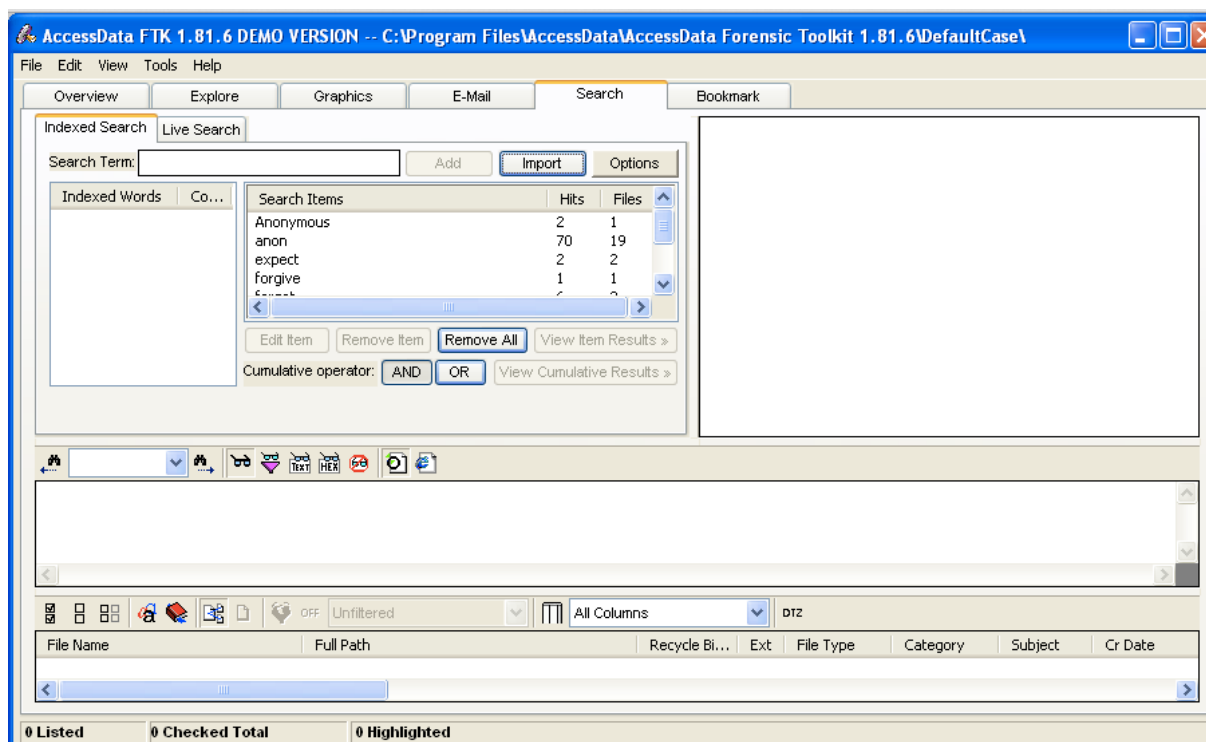
5. Prosedur yang lebih baik dengan menggunakan pencarian keyword. FTK didesain untuk bekerja dengan cara ini – dengan cara membuat index dari daftar pada file evidence. Buka Notepad dan ketikkan keywords yang terlihat pada gambar di bawah ini. Misalnya seperti Kita ketahui pada kasu melibatkan gang Anonymous,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



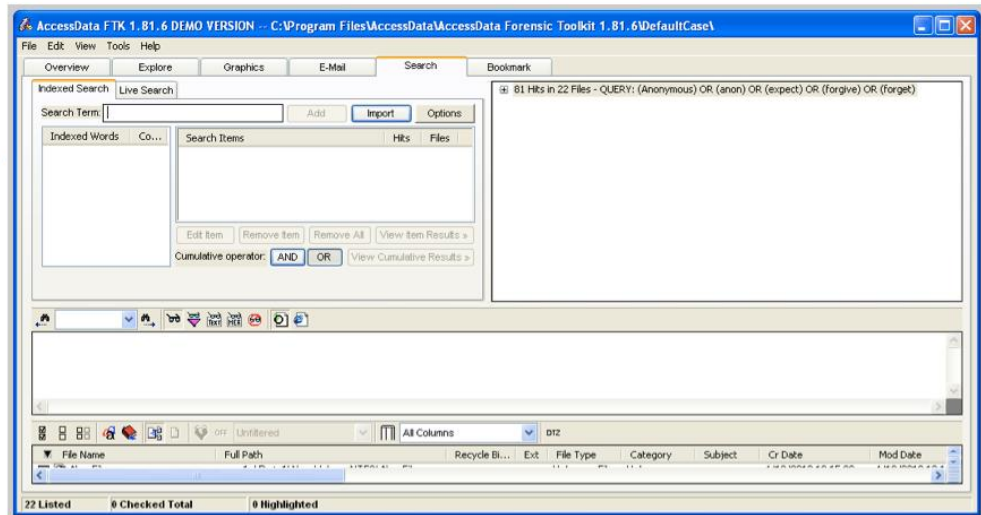
- Simpan file di desktop sebagai "keywords.txt".
- Pada FTK, click tab **Search**.
- Click tombol **Import**.
- Pada kotak "Import Search Terms", arahkan ke desktop dan double-click file **keywords.txt**.
- Kotak pop up "Import Search Terms" muncul, yang mengatakan 'Do you wish to show items that have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

Hasil Pencarian

- Lima keywords ditemukan, seperti berikut pada panel atas FTK:

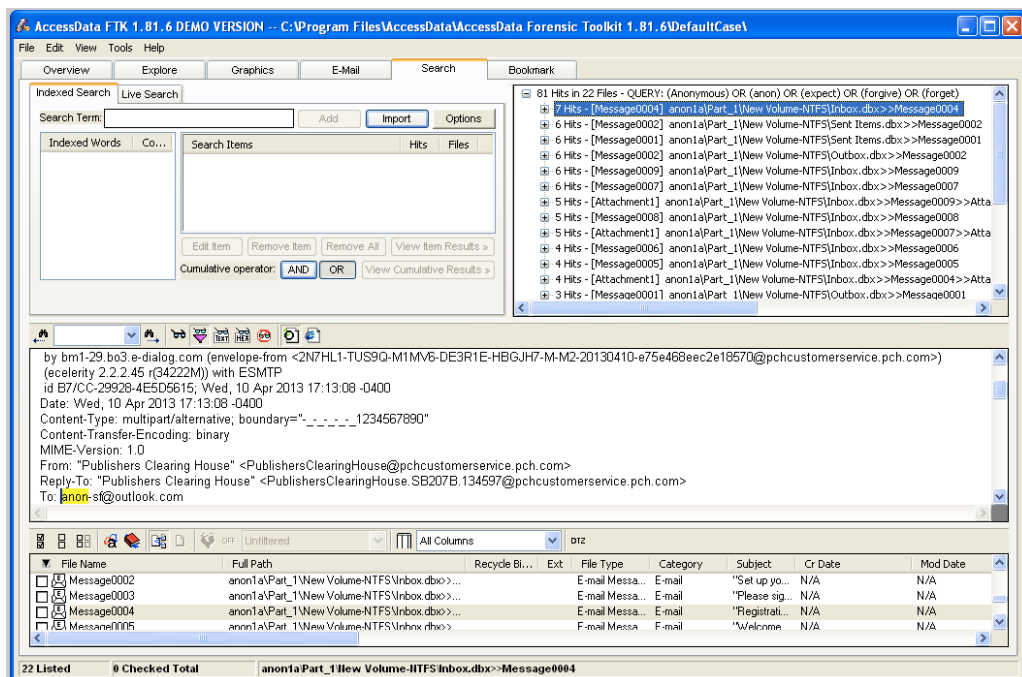


- Pada baris "Cumulative Operator", click tombol **OR**.
- Pada baris "Cumulative Operator", click tombol **"View Cumulative Results"**.
- Pada kotak "Filter Search Hits", terima pilihan default "All files" dan click tombol **OK**.
- Pada panel kanan atas terlihat "81 Hits in 22 Files", seperti berikut.



Memeriksa Hits

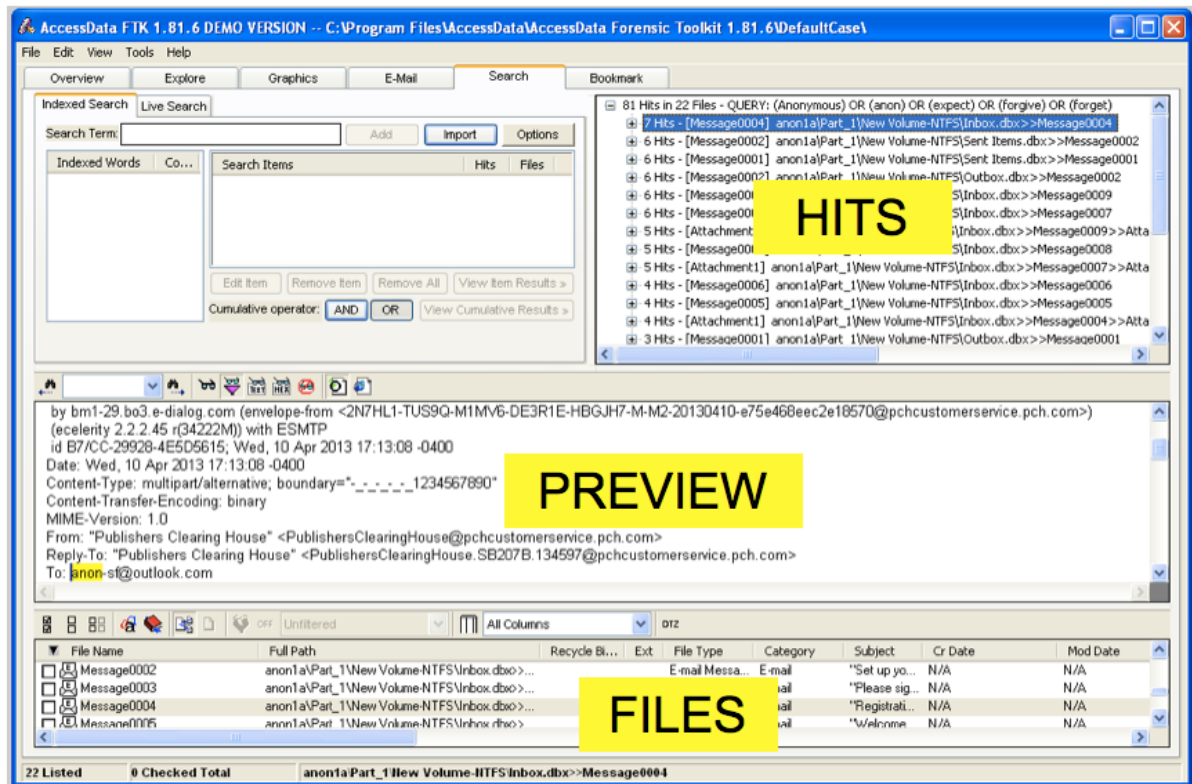
- Click item pertama pada panel kanan atas. Item ini berisi, label "81 Hits in 22 Files". Expand dengan menekan panah kanan key di keyboard. Kemudian tekan panah ke bawah untuk ke item berikutnya, yang berlabel "[7 Hits -- Message004]".
- Di layar akan terlihat seperti pada gambar berikut. File ini merupakan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



Prosedur

- Berikut ini cara memeriksa hits dengan cepat. Ikuti petunjuk berikut.
 - Pada bagian HITS di kanan atas, tekan panah ke bawah untuk memilih item berikutnya.
 - Perhatikan PREVIEW pada layar tengah.
 - 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.

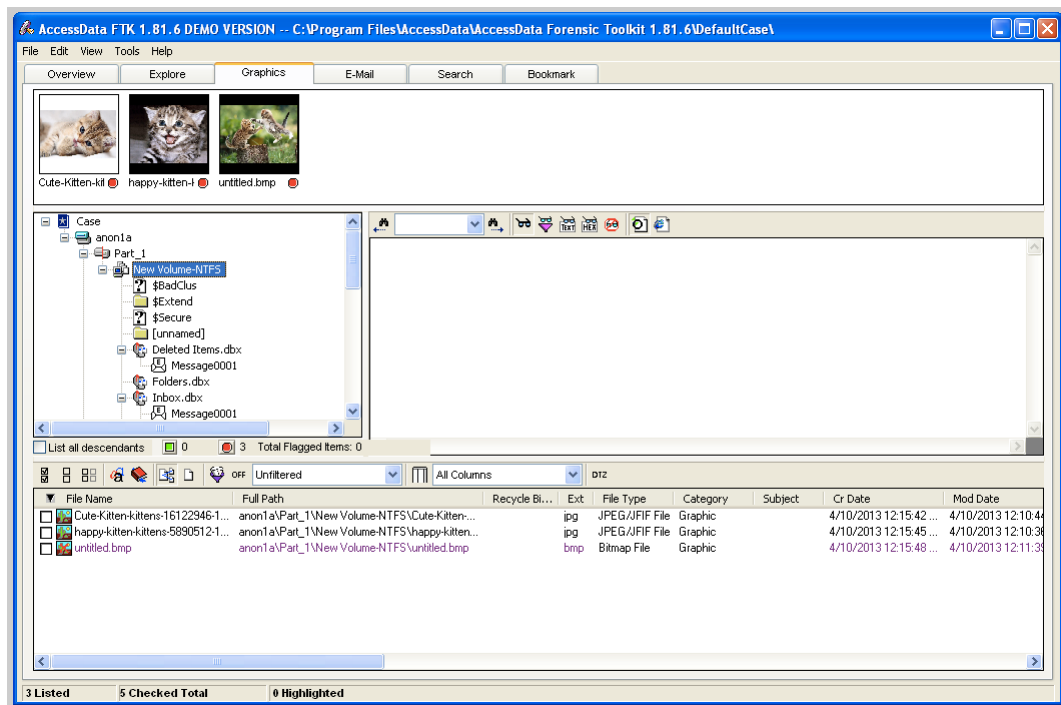
Melihat Gambar

10. 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.

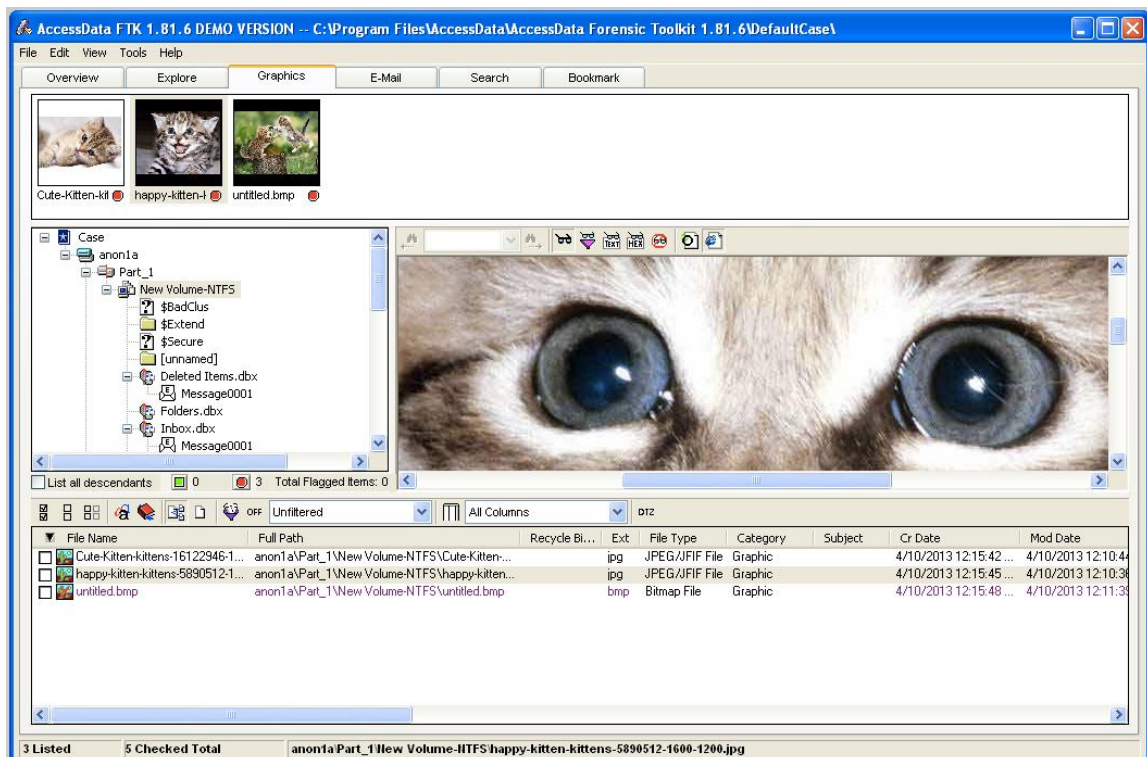
a. Pada kiri tengah, terdapat tiga struktur yang memperlihatkan file dan folder. Click item teratas, **Case**, dan gunakan panah ke bawah untuk pindah ke item berikutnya.

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:

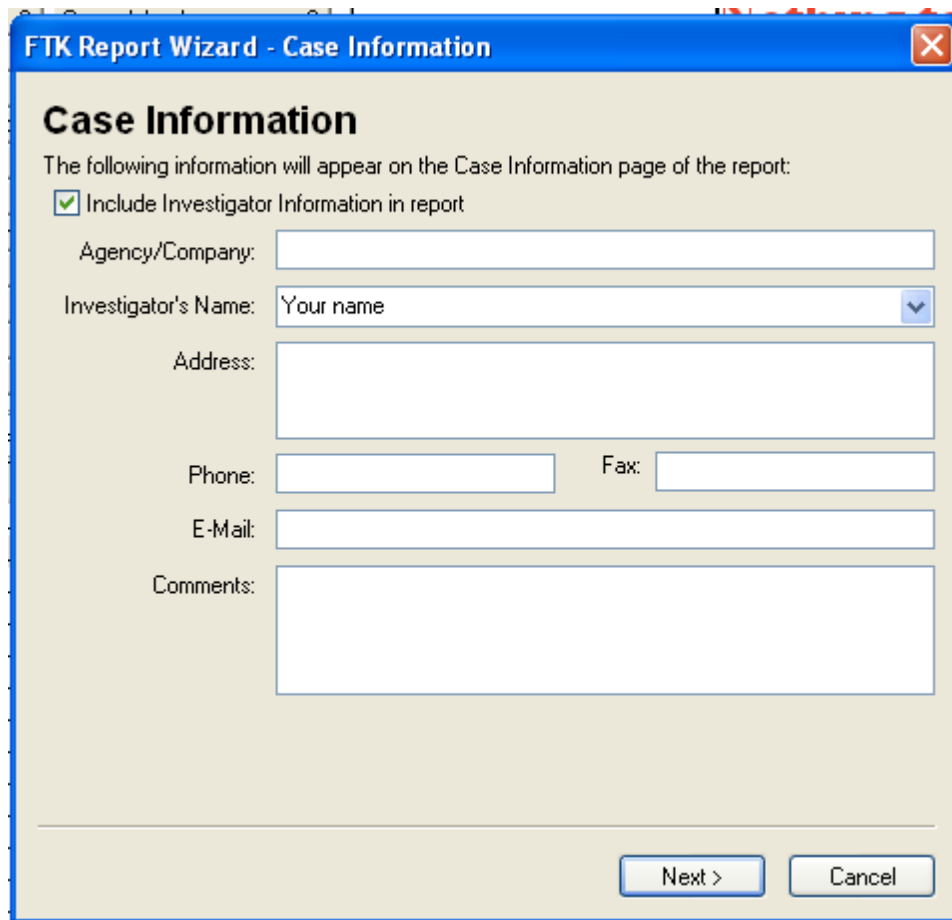


- f. Lanjutkan dengan memeriksa semua folder sampai ditemukan gambar yang mencurigakan. Tandai semua gambar yang mencurigakan dengan mencentang kotak pada panel bawah, seperti yang dilakukan pada email messages.

- g. Salah satu gambar memperlihatkan halaman Web yang diserang. Pastikan mendapatkannya untuk membuktikan penyerangan.

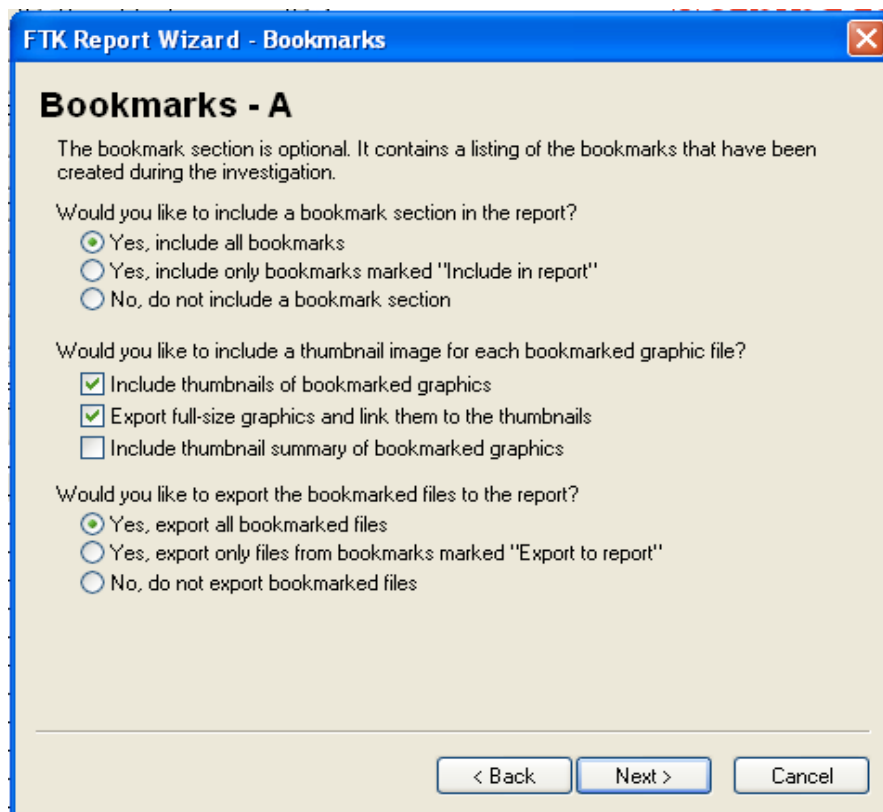
Membuat Report/Laporan

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

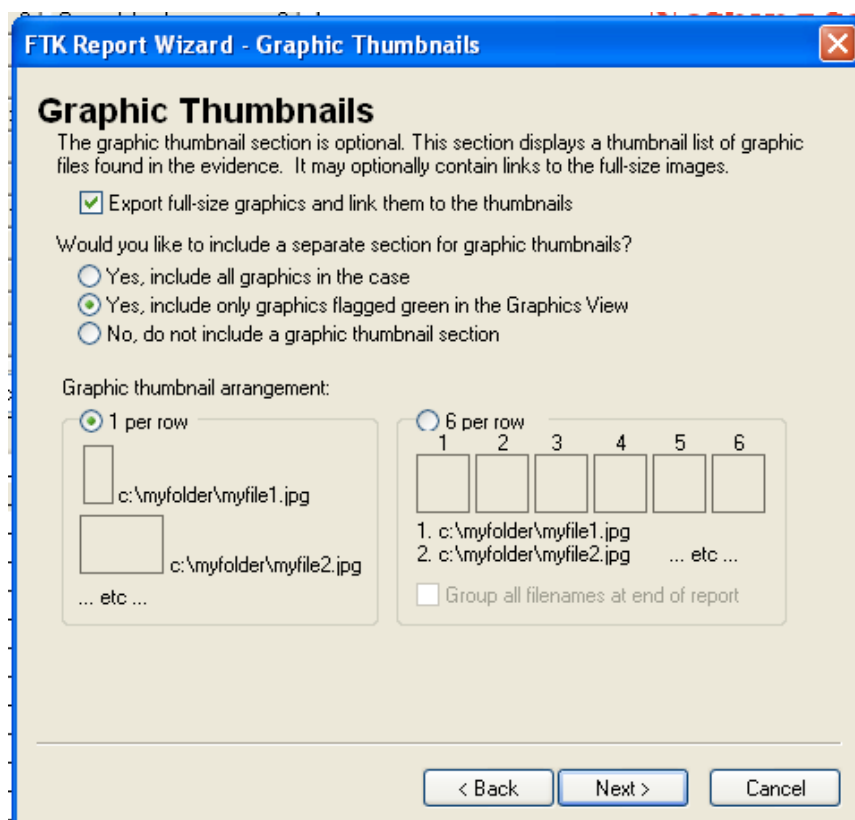


The screenshot shows the "FTK Report Wizard - Case Information" dialog box. The title bar is blue with a close button (X) in the top right corner. The main area has a light beige background. At the top, the text "Case Information" is displayed in bold. Below it, a message states: "The following information will appear on the Case Information page of the report:". A checkbox labeled "Include Investigator Information in report" is checked. Below this, there are several input fields: "Agency/Company:" with a text box, "Investigator's Name:" with a dropdown menu showing "Your name", "Address:" with a large text box, "Phone:" and "Fax:" with separate text boxes, "E-Mail:" with a text box, and "Comments:" with a large text box. At the bottom right, there are two buttons: "Next >" and "Cancel".

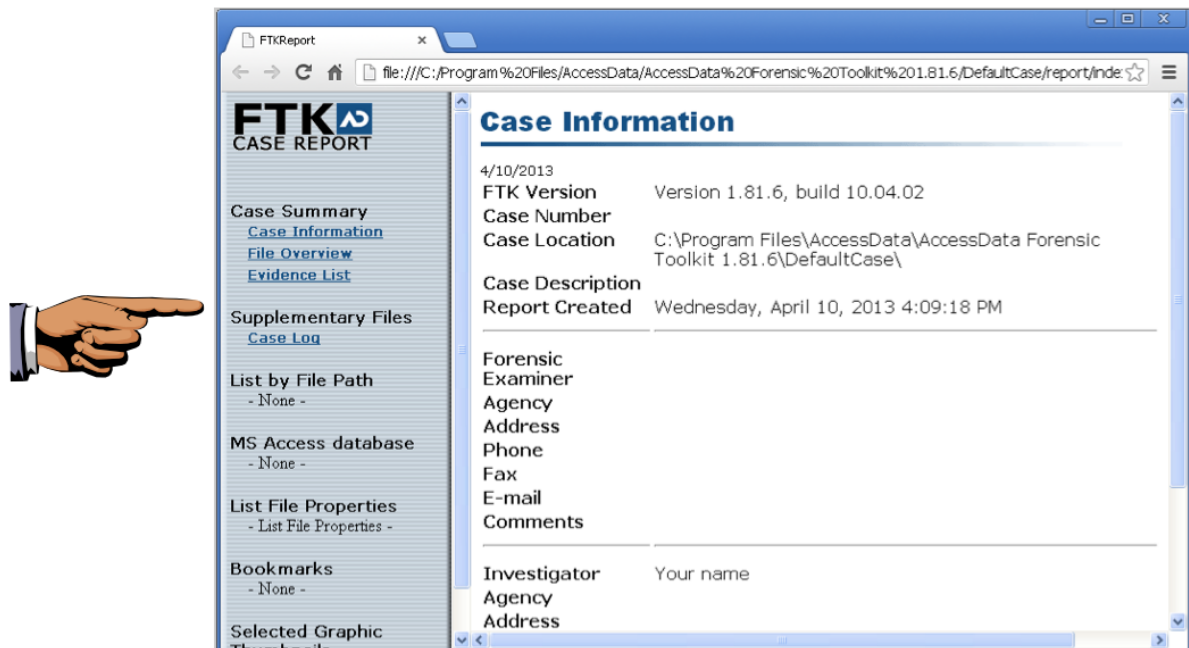
- b. Pada halaman "Bookmarks - A", click tombol "**Yes, export all bookmarked files**", seperti terlihat di bawah ini. Kemudian click **Next**.



- 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**.

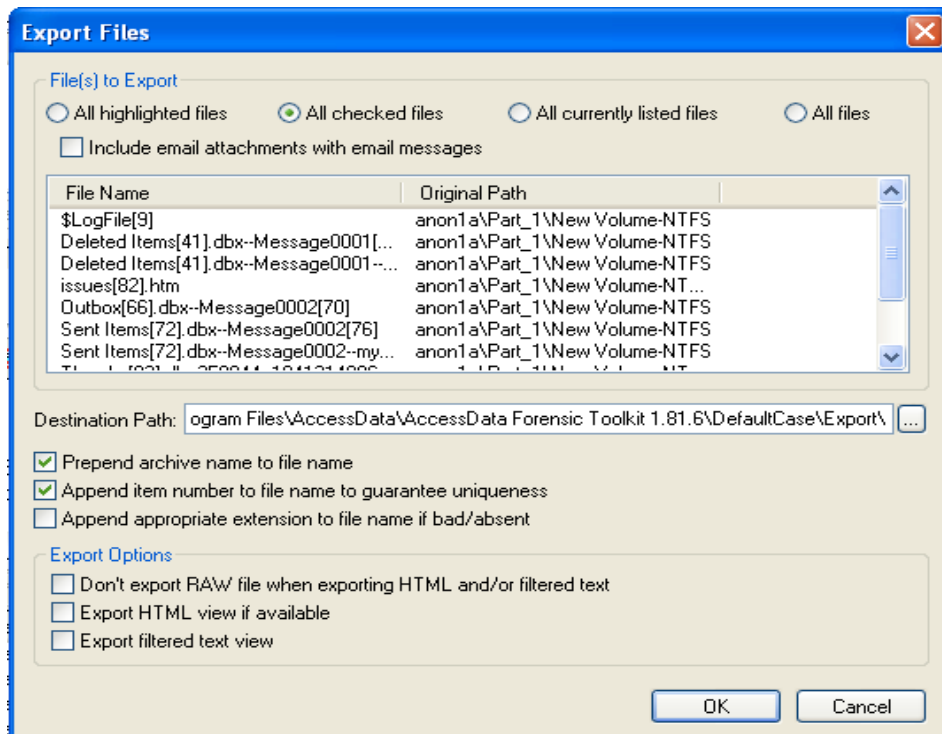


- e. Pada halaman "List by File Path", click **Next**.
- f. Pada halaman "List File Properties - A", click **Next**.
- g. Pada halaman "Supplementary Files", click **Next**.
- h. Pada halaman "Report Location", click **Finish**.
- i. Kotak pop up "Report Wizard" akan muncul, menanyakan "Do you wish to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



Mengekspor File yang dipilih

12. 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 Toolkit1.81.6\DefaultCase\Export".
- d. File-file tersebut akan terlihat seperti berikut.

