

NAMA : EDO NOERMAN YULIANSYAH
NIM : 1310651011
KELAS : E

Jawaban UAS

Physical (Environmental) Security

1.

Bollards

A traffic bollard is a strong post designed to stop a car. The term derives from the short/strong posts (called mooring bollards) used to tie ships to piers when docked.

Lights

Lights can act as both a detective and deterrent control. Light should be bright enough to illuminate the desired field of vision (the area being protected). Types of lights include Fresnel; these are the same type of lights originally used in light-houses, which used Fresnel lenses to aim light in a specific direction.

Light measurement terms include lumen, the amount of light one candle creates. Light was historically measured in foot-candles; one foot-candle is one lumen per square foot. Lux, based on the metric system, is more commonly used now: one lux is one lumen per square meter.

CCTV

Closed-Circuit Television (CCTV) is a detective device used to aid guards in detecting the presence of intruders in restricted areas. CCTVs using the normal light spectrum require sufficient visibility to illuminate the field of view that is visible to the camera. Infrared devices can “see in the dark” by displaying heat. Older “tube cameras” are analog devices. Modern cameras use CCD (Charged-Coupled Discharge), which is digital.

CCTV cameras may also have other typical camera features such as pan and tilt (moving horizontally and vertically).

Magnetic tape such as VHS is used to back up images from tube cameras. CCD cameras use DVR (Digital Video Recorder) or NVR (Network Video Recorder) for backups.

Locks

Locks are a preventive physical security control, used on doors and windows to prevent unauthorized physical access. Locks may be mechanical, such as key locks or combination locks, or electronic, which are often used with smart cards or magnetic

Key locks

Key locks require a physical key to unlock. Keys may be shared or sometimes copied, which lowers the accountability of key locks. A common type is the pin tumbler lock, which has two sets of pins: driver pins and key pins. The correct key makes the pins line up with the shear line, allowing the lock tumbler (plug) to turn.

Ward or warded locks must turn a key through channels (called wards); a “skeleton key” is designed to open varieties of warded locks.

Combination locks

Combination locks have dials that must be turned to specific numbers, in a specific order (alternating clockwise and counterclockwise turns) to unlock. Button or keypad locks also use numeric combinations. Limited accountability due to shared combinations is the primary security issue concerning these types of locks.

Smart cards and magnetic stripe cards

A smart card is a physical access control device that is often used for electronic locks, credit card purchases, or dual-factor authentication systems. "Smart" means the card contains a computer circuit.

Smart cards may be "contact" or "contactless." Contact cards must be inserted into a smart card reader, while contactless cards are read wirelessly. One type of contactless card technology is Radio-Frequency Identification (RFID). These cards contain RFID tags (also called transponders) that are read by RFID transceivers.

A magnetic stripe card contains a magnetic stripe that stores information. Unlike smart cards, magnetic stripe cards are passive devices that contain no circuits. These cards are sometimes called swipe cards: they are used by swiping through a card reader.

Tailgating/piggybacking

Tailgating (also known as piggybacking) occurs when an unauthorized person follows an authorized person into a building after the authorized person unlocks and opens the door. Policy should forbid employees from allowing tailgating and security awareness efforts should describe this risk.

Mantraps and turnstiles

A mantrap is a preventive physical control with two doors. The first door must close and lock before the second door may be opened. Each door typically requires a separate form of authentication to open. The intruder is trapped between the doors after entering the mantrap.

Turnstiles are designed to prevent tailgating by enforcing a "one person per authentication" rule, just as they do in subway systems.

Contraband checks

Contraband checks seek to identify objects that are prohibited to enter a secure. These checks are often used to detect metals, weapons, or explosives. Contraband checks are casually thought to be a detective control, but their presence being known makes them also a deterrent to actual threats.

Motion detectors and other perimeter alarms

Ultrasonic and microwave motion detectors work like "Doppler radar" used to predict the weather. A wave of energy is sent out, and the "echo" is returned when it bounces off an object. The echo will be returned more quickly when a new object (such as a person walking in range of the sensor) reflects the wave.

A photoelectric motion sensor sends a beam of light across a monitored space to a photoelectric sensor. The sensor alerts when the light beam is broken.

Ultrasonic, microwave, and infrared motion sensors are active sensors, which means they actively send energy. A passive sensor can be thought of as a "read-only" device. An example is a passive infrared (PIR) sensor, which detects infrared energy created by body heat.

Doors and windows

Always consider the relative strengths and weaknesses of doors, windows, walls, floors, ceilings, etc. All should be equally strong from a defensive standpoint: attackers will target the "weakest link in the chain" and should not find a weak spot to expose.

Egress must be unimpeded in case of emergency, so a simple push button or motion detectors are frequently used to allow egress. Externally facing emergency doors should be marked for emergency use only and equipped with panic bars. The use of a panic bar should trigger an alarm.

Glass windows are structurally weak and can be dangerous when shattered. Bulletproof or explosive-resistant glass can be used for secured areas. Wire mesh or security film can lower the danger of shattered glass and provide additional strength. Alternatives to glass windows include polycarbonate such as Lexan and acrylic such

as Plexiglass.

Walls, floors, and ceilings

Walls around any internal secure perimeter such as a data center should be “slab to slab,” meaning they should start at the floor slab and run to the ceiling slab. Raised floors and drop ceilings can obscure where the walls truly start and stop. An attacker should not be able to crawl under a wall that stops at the top of the raised floor or climb over a wall that stops at the drop ceiling.

Guards

Guards are a dynamic control that may be used in a variety of situations. Guards may aid in inspection of access credentials, monitor CCTVs, monitor environmental controls, respond to incidents, act as a deterrent (all things being equal, criminals are more likely to target an unguarded building over a guarded building), and much more.

Professional guards have attended advanced training and/or schooling; amateur guards (sometimes derogatively called “Mall Cops”) have not. The term pseudo guard means an unarmed security guard.

Dogs

Dogs provide perimeter defense duties, guarding a rigid “turf.” They are often used in controlled areas, such as between the exterior building wall and a perimeter fence. The primary drawback to using dogs as a perimeter control is legal liability.

SITE SELECTION, DESIGN, AND CONFIGURATION

Selection, design, and configuration describe the process of building a secure facility such as a data center, from the site selection process through the final design.

Site selection issues

Site selection is the process of choosing a site to construct a building or data center.

Utility reliability

The reliability of local utilities is a critical concern for site selection purposes. Electrical outages are among the most common of all failures and disasters we experience. Uninterruptible Power Supplies (UPSs) will provide protection against electrical failure for a short period (usually hours or less). Generators provide longer protection but will require refueling in order to operate for extended periods.

Crime

Local crime rates also factor into site selection. The primary issue is employee safety: all employees have the right to a safe working environment. Additional issues include theft of company assets.

Site design and configuration issues

Once the site has been selected, a number of design decisions must be made. Will the site be externally marked as a data center? Is there shared tenancy in the building? Where is the telecom demarc (the telecom demarcation point)?

Site marking

Many data centers are not externally marked to avoid drawing attention to the facility (and the expensive contents within). Similar controls include attention-avoiding details such as muted building design.

Shared tenancy and adjacent buildings

Other tenants in a building case pose security issues: they are already behind the physical security perimeter. Their physical security controls will impact yours: a tenant’s poor visitor security practices can endanger your security, for example.

Adjacent buildings pose a similar risk. Attackers can enter a less secure adjacent building and use that as a base to attack an adjacent building, often breaking in

through a shared wall.

A crucial issue to consider in a building with shared tenancy is a shared demarc (the demarcation point, where the ISP's (Internet Service Provider) responsibility ends and the customer's begins). Access to the demarc allows attacks on the confidentiality, integrity, and availability of all circuits and the data flowing over them.

2.

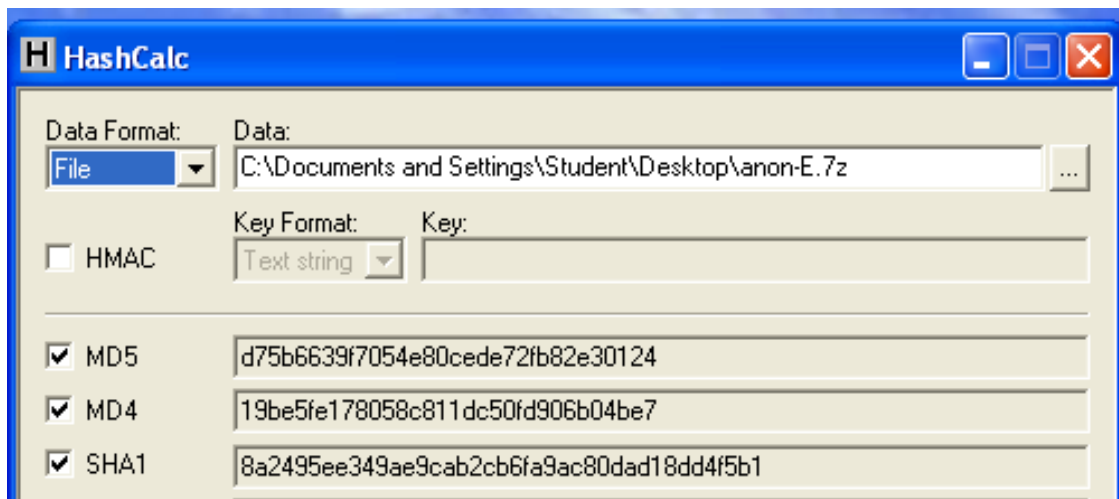
Penggunaan FTK

Kebutuhan Project

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

Mendownload Evidence File

1. Download file evidence yang ada di elearning: [anon-E.7z](#)
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**.

Menggunakan FTK

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

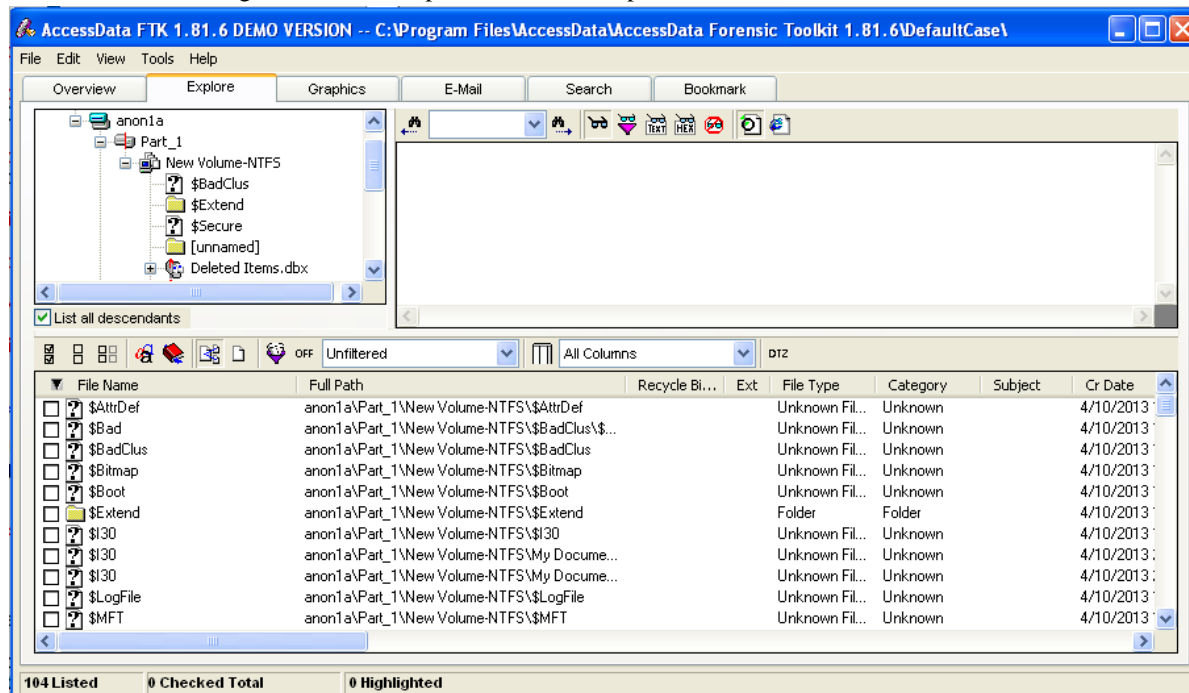
- b. Pada layar berjudul "Forensic Examiner Information", biarkan fields nya kosong dan click **Next**.
- c. Pada layar yang bagian "Case Log Options", biarkan pihan default, yang akan mencatat semua log. click **Next**.
- d. Pada bagian "Processes to Perform", buang pilihan "**KFF Lookup**" dan "**Decrypt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

Menggunakan FTK

- 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

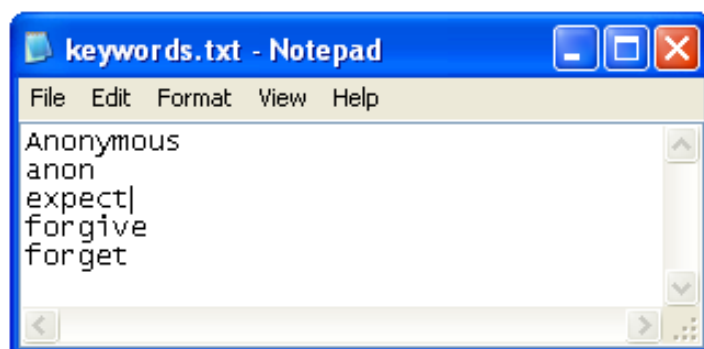
7. Barang bukti diambil dari komputer yang ditemukan di ruangan yang digunakan oleh tersangka hacker komuter dari Anonymous gang.

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".

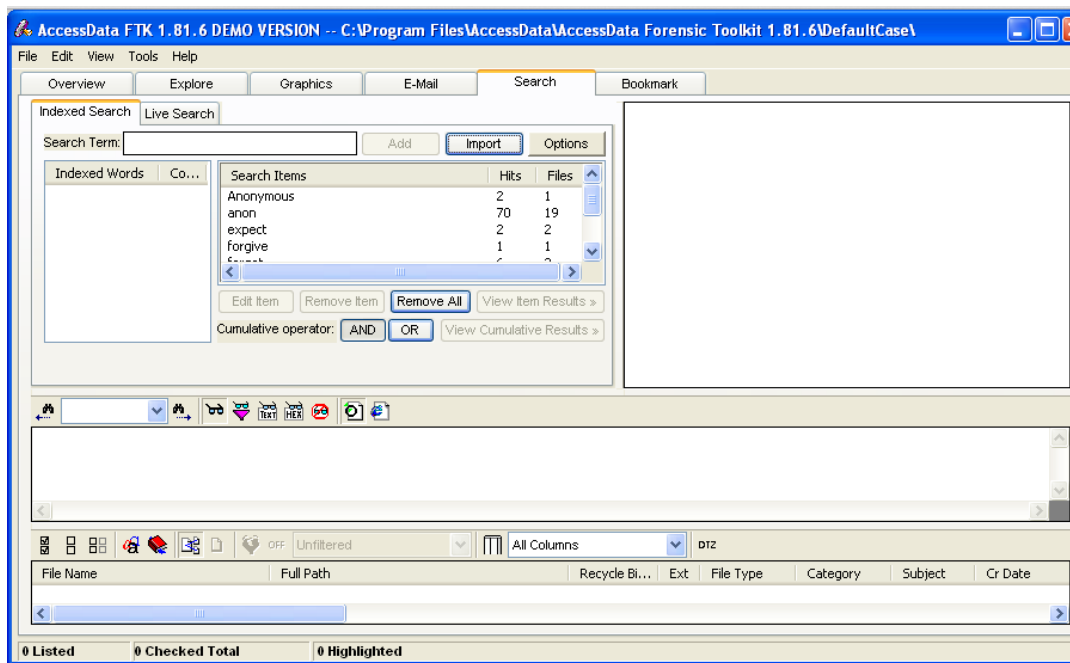


Menggunakan FTK

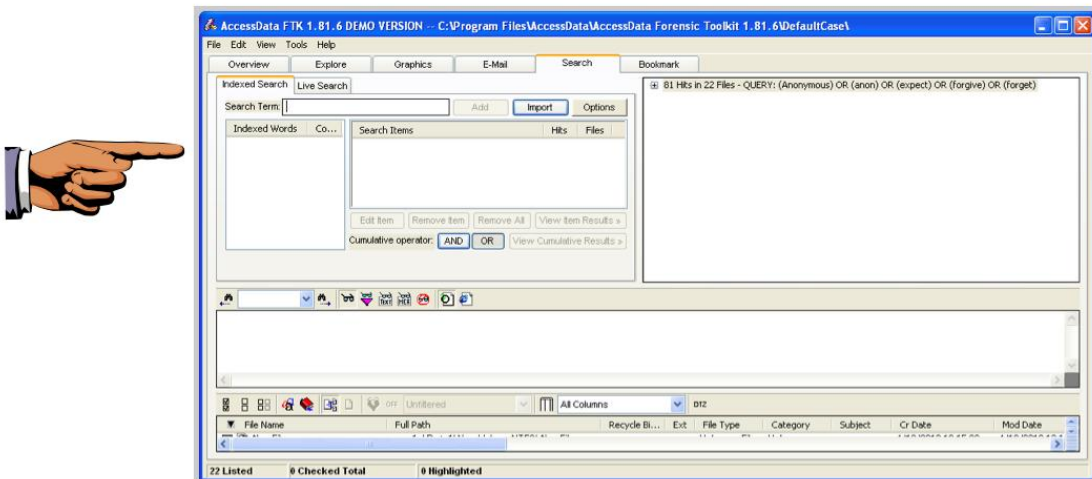
- Simpan file di desktop sebagai "keywords.txt".
- Pada FTK, click tab **Search**.
- Click tombol **Import**.
- Pada kotak "Import Search Terms", arahkan ke desktop dan double-click file **keywords.txt**.
- Kotak pop up "Import Search Terms" muncul, yang mengatakan 'Do you wish to show items that have 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

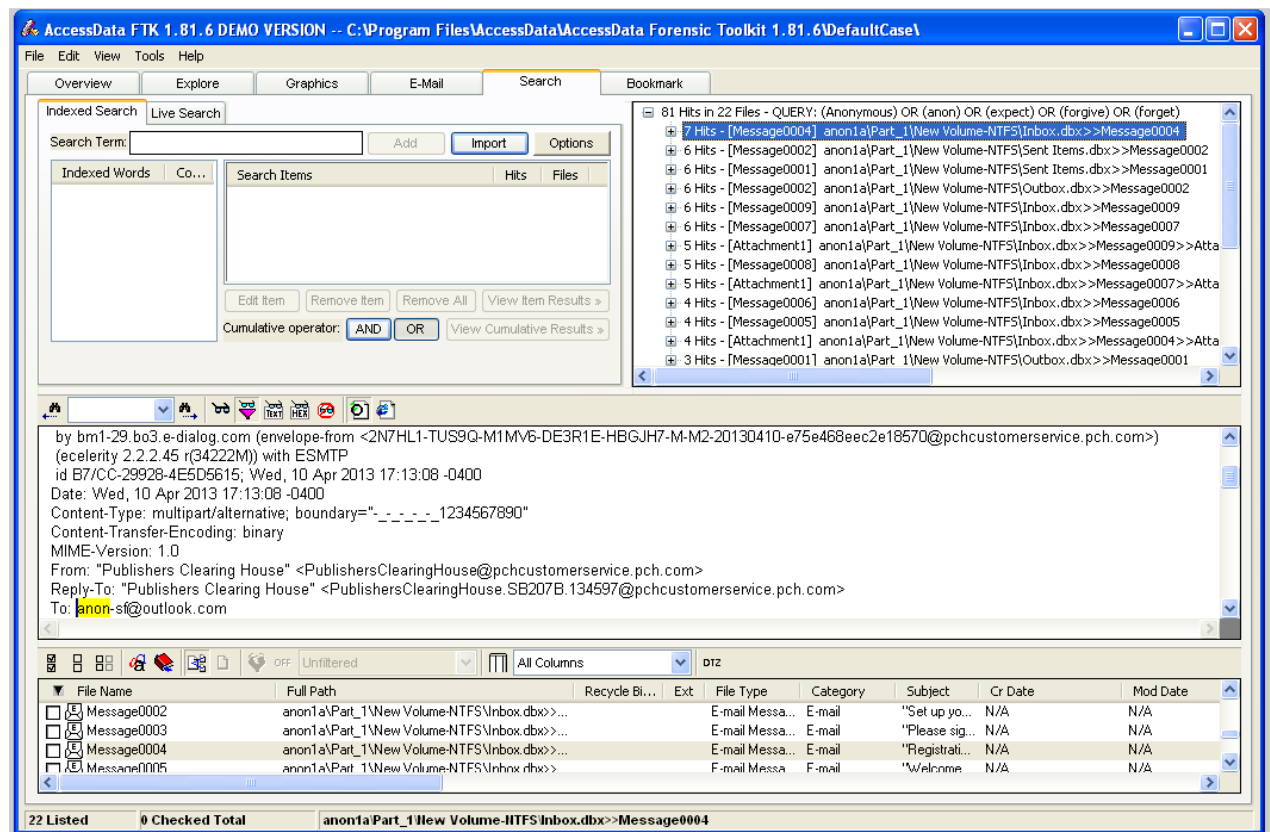
11. Pastikan di layar terlihat "81 Hits in 22 Files". Tekan PrintScrn key untuk mengkopir seluruh desktop.

UNTUK MENDAPAT POIN MAKSIMAL KUMPULKAN DESKTOP IMAGE KESELURUHAN.

Simpan dengan nama file "NamaKamu_Project15a".

Memeriksa Hits

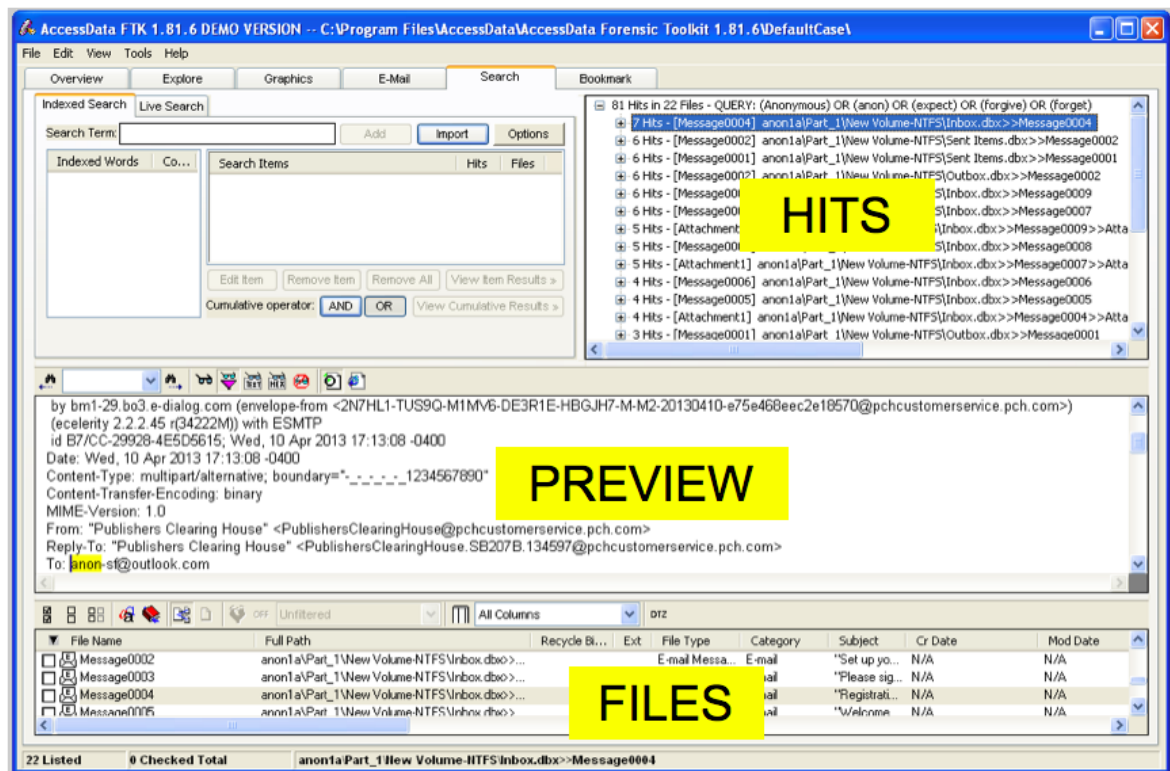
12. Click item pertama pada panel kanan atas. Item ini berisi label "81 Hits in 22 Files". Expand dengan menekan panah kanan key di keyboard. Kemudian tekan panah ke bawah untuk ke item berikutnya, yang berlabel "[7 Hits -- Message004]".
13. Di layar akan terlihat seperti pada gambar berikut. File ini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

Menggunakan FTK



- 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.

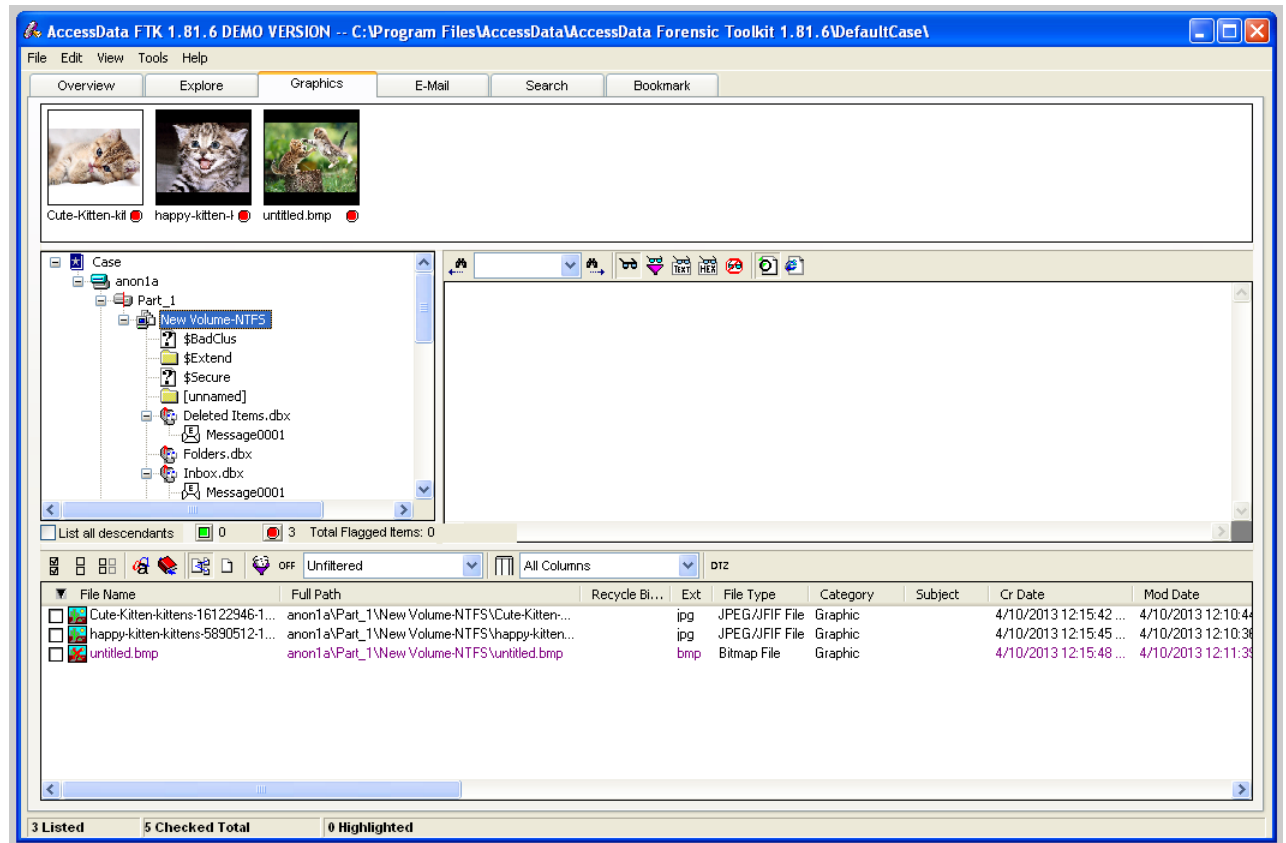
HARUS MENGUMPULKAN COMPLETE DESKTOP IMAGE UNTUK MENDAPATKAN POIN MAKSIMAL.

Simpan gambar dengan nama file "**NamaKamu_Proj15b**".

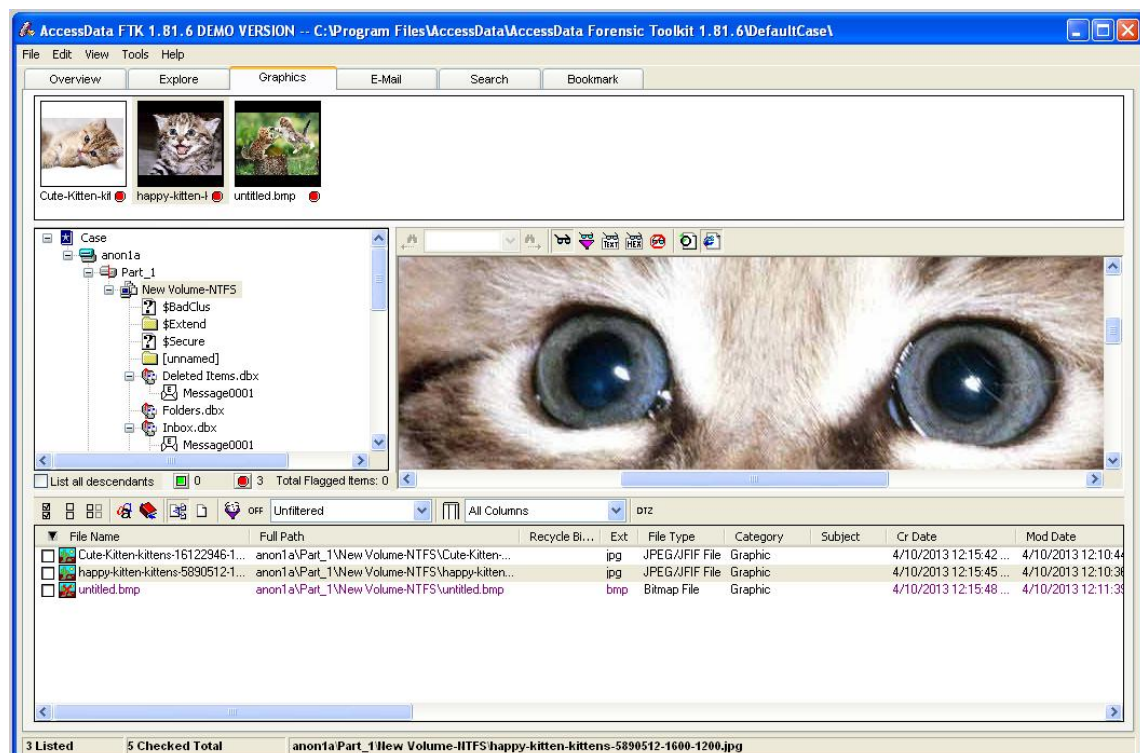
Melihat Gambar

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.
- 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.
 - Ketika ingin membuka folder, gunakan panah kanan untuk membukanya.
 - Ketika memilih folder yang berisi gambar di dalamnya, akan terlihat thumbnails pada panel atas seperti berikut:

Menggunakan FTK



- 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:



Menggunakan FTK

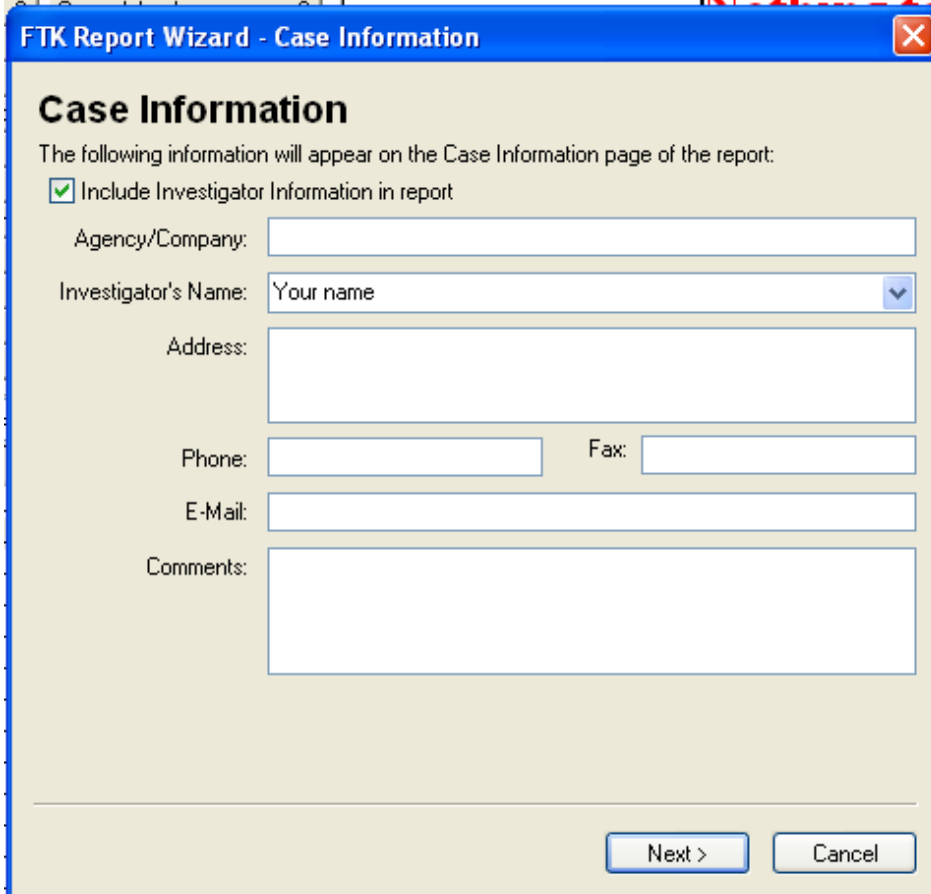
- f. Lanjutkan dengan memeriksa semua folder sampai ditemukan gambar yang mencurigakan. Tandai semua gambar yang mencurigakan dengan mencentang kotak pada panel bawah, seperti yang dilakukan pada email messages.
- g. Salah satu gambar memperlihatkan halaman Web yang diserang. Pastikan mendapatkannya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

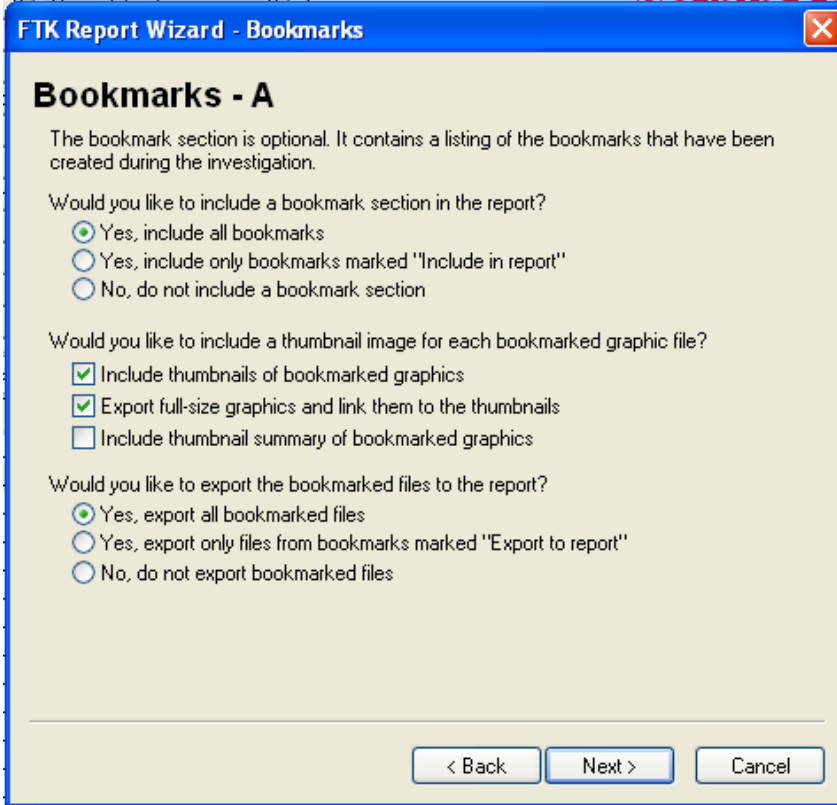
18. Pada FTK, dari baris menu bagian atas, click **File**, "**Report Wizard**".
 - a. Pada bagian "Case Information", click **Next**, seperti terlihat di bawah ini.



The screenshot shows the "FTK Report Wizard - Case Information" dialog box. It has a title bar with a close button. The main area is titled "Case Information" and contains the text: "The following information will appear on the Case Information page of the report:". Below this is a checked checkbox labeled "Include Investigator Information in report". There are several input fields: "Agency/Company:" (text box), "Investigator's Name:" (dropdown menu showing "Your name"), "Address:" (text box), "Phone:" (text box), "Fax:" (text box), "E-Mail:" (text box), and "Comments:" (large text area). At the bottom right 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**.

Menggunakan FTK



FTK Report Wizard - Bookmarks

Bookmarks - A

The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.

Would you like to include a bookmark section in the report?

- ☒ Yes, include all bookmarks
- ☐ Yes, include only bookmarks marked "Include in report"
- ☐ No, do not include a bookmark section

Would you like to include a thumbnail image for each bookmarked graphic file?

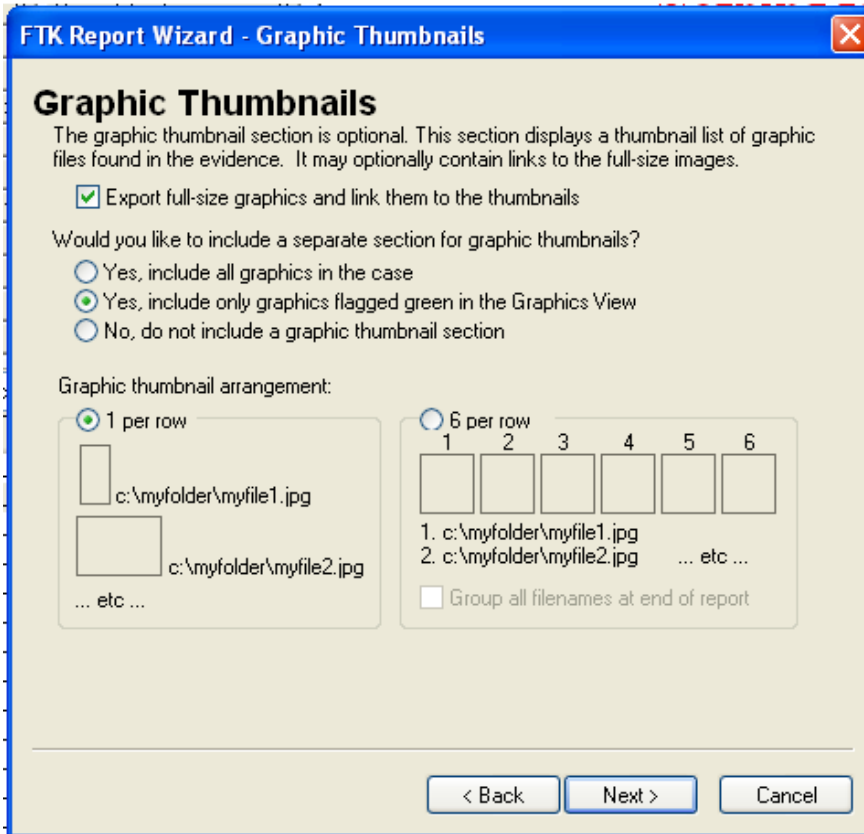
- ☒ Include thumbnails of bookmarked graphics
- ☒ Export full-size graphics and link them to the thumbnails
- ☐ Include thumbnail summary of bookmarked graphics

Would you like to export the bookmarked files to the report?

- ☒ Yes, export all bookmarked files
- ☐ Yes, export only files from bookmarks marked "Export to report"
- ☐ No, do not export bookmarked files

< Back Next > Cancel

- 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**.



FTK Report Wizard - Graphic Thumbnails

Graphic Thumbnails

The graphic thumbnail section is optional. This section displays a thumbnail list of graphic files found in the evidence. It may optionally contain links to the full-size images.


- ☒ Export full-size graphics and link them to the thumbnails


Would you like to include a separate section for graphic thumbnails?

- ☐ Yes, include all graphics in the case
- ☒ Yes, include only graphics flagged green in the Graphics View
- ☐ No, do not include a graphic thumbnail section

Graphic thumbnail arrangement:

☒ 1 per row







 c:\myfolder\myfile1.jpg

 c:\myfolder\myfile2.jpg

... etc ...

☐ 6 per row

1 2 3 4 5 6

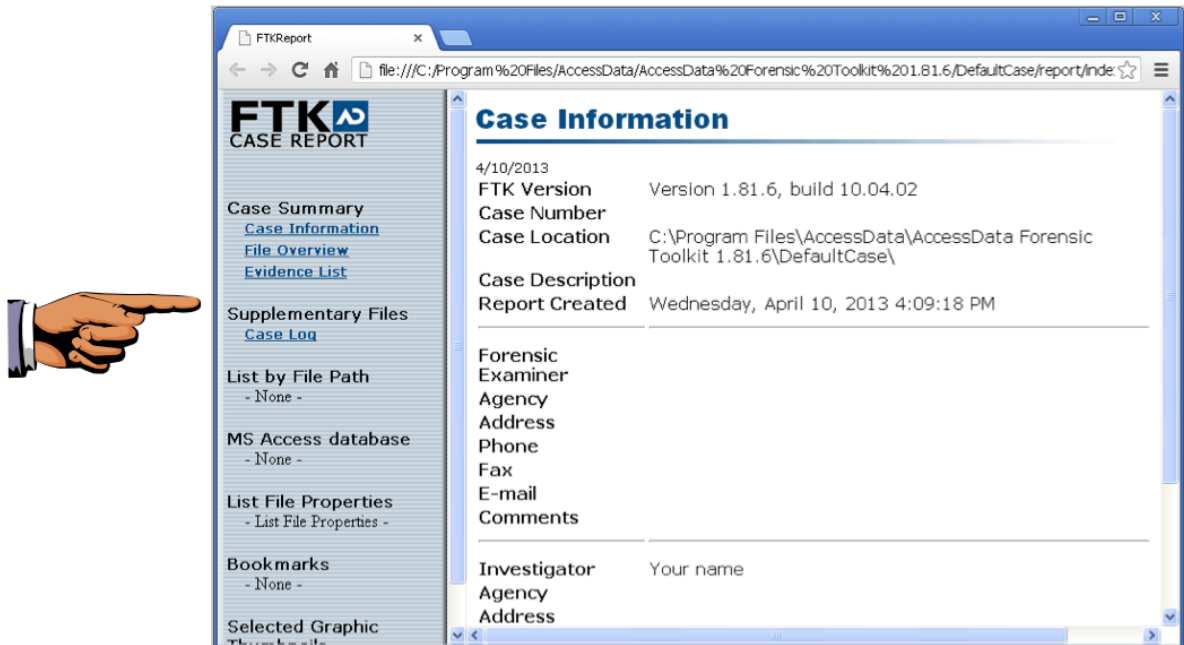
1. c:\myfolder\myfile1.jpg
2. c:\myfolder\myfile2.jpg ... etc ...

☐ Group all filenames at end of report

< Back Next > Cancel

Menggunakan FTK

- 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.



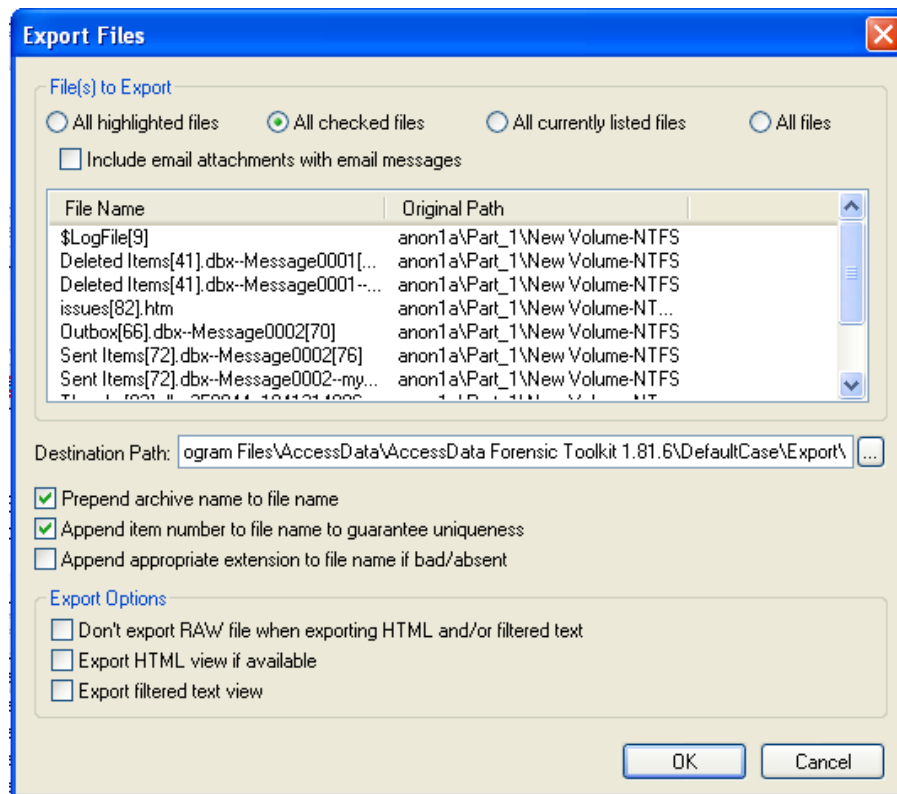
Simpan Screen Image

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**.

Menggunakan FTK



- 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.

