eForensics Magazine

E-BOOK

REAL LIFE COMPUTER FORENSICS

MUCH MORE THAN JUST KNOWING HOW TO USE TOOLS

Contents


KPMG
cutting through complexity
Are you prepared?
kpmg.ca/forensic
SECURITY
ROL • COMPLEXITY • RISK
CTRONIC
ITY • THREAT • CONTROL
FORENSICS
CONTROL • RISK • DATABASE
HNOLOGY
MPLEXITY • THREAT • ATTACK
VESTIGATIONS
OMPLEXITY • ELECTRONIC • CYBER SECURITY • RISK • THREAT
ORPORATE • INTELLIGENCE
YBER SECURITY • ATTACK • THREAT • CYBER SECURITY
TECHNOLOGY • eDISCOVERY
OMPLEXITY • ELECTRONIC • INFORMATION • THREAT • CONTROL
DATA ANALYTICS • INFORMATION
SK • INFORMATION • TECHNOLOGY • ATTACK • RISK
NTELLIGENCE • DATA RECOVERY
OMPLEXITY • ELECTRONIC • INFORMATION • THREAT • CONTROL
PROTECTION • INFORMATION
TELLIGENCE • ELECTRONIC • CONTROL • RISK • COMPLEXITY
ISK • COMPLEXITY • INTRUSION
© 2013 KPMG LLP, a Canadian limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.
IFORMATION • RISK • TECHNOLOGY • ATTACK • RISK

Editor: Artur Inderike *artur.inderike@eforensicsmag.com*

Betatesters/Proofreaders: M1ndl3ss, Andrew J. Levandoski, Scott Taylor, Kishore P.V., Massa Danilo, Gabriele Biondo

Senior Consultant/Publisher: Paweł Marciniak

CEO: Ewa Dudzic *ewa.dudzic@software.com.pl*

Art Director: Ireneusz Pogroszewski *ireneusz.pogroszewski@software.com.pl*

DTP: Ireneusz Pogroszewski

Production Director: Andrzej Kuca *andrzej.kuca@software.com.pl*

Marketing Director: Joanna Kretowicz *jaonna.kretowicz@eforensicsmag.com*

Publisher: Software Media Sp. z o.o. SK

02-682 Warszawa, ul. Bokserska 1

Phone:1 917 338 3631

www.eforensicsmag.com

Recommended

Keep your PC at peak performance!

It incorporates Wise Registry Cleaner, Wise Disk Cleaner and many other useful features like System Slimming, Startup Manager, Disk Eraser, etc.

The software has amazing scan & clean speed, which makes it outstanding from similar products. You'll love the clean and user-friendly interface and the pragmatic efficiency!

WiseCleaner

Wise Care 365 2

- Over 15,000,000 downloads worldwide.
- Clean & Tune up Windows system.
- Protect digital privacy effectively.

★★★★★

5-Star Reviewed by
Top Download Websites

Official Website for More Information:
www.wisecleaner.com/wisecare365.html

Compatible with Windows 7

Windows 8 Compatible

Support system:
Windows XP, Vista, Win7/8
(both 32-bit and 64-bit)

ABSTRACT

Just think about this… You are a Homeland Security Investigator who goes into a court room to defend a forensic investigation. Your results and testimony about your findings are flawless. Then steps in a forensic specialist hired by the accused who explains to the judge the right process of a forensic investigation according to the National Institute of Standards and Technology (NIST) and he explains that you failed to provide your documented process of acquiring the physical evidence, chain of custody and missed vital points on your report. The District Attorney can't recover from that blow and your evidence is declared inadmissible, the case gets dismissed and your hard work goes out of the window. Well, this is not an imaginary story; I was there and I wasn't the Homeland Security Agent.

What you will learn:

- The basics of handling and analyzing of digital evidence
- What to think when requesting a search warrant
- What can be considered evidence?
- How to seize a computer or digital device
- What comprises a good report?

What you should know:

- Basic knowledge of FTK
- Good writing skills

INTRODUCTION

There are many tutorials and articles out there that teach you how to use different forensic tools but the majority mention the seizure, reporting and testimony briefly if at all. In my opinion all of that is equally important in real life. If any of those components are weakly developed you risk all the process. In this e-book my main purpose is to demonstrate the full process that is comprised of:

1. Executing a warrant and seizing evidence following a methodology.

2. Getting the chain of custody correctly

3. Doing a sound forensic analysis assuring evidence integrity

4. Obtaining evidence while keeping its integrity

5. Validating and documenting the whole process along with the continuation of the chain of custody

6. Writing a report conclusion that correlates the evidence with the possible charges

7. Creating a final report that can sustain as evidence in court

This is all done by showing you the theory behind these processes and then showing you how those things are executed in a practical way by following examples that I've given my students so they can have practical scenarios to hone their skills. Your first experience with this type of procedures should not be on a real investigation. I hope that you enjoy this e-book and get a basic idea of how forensic analysis it's not just using tools, it a lot more and it's an incredibly rewarding job!

ACKNOWLEDGEMENTS

First of all thanks to Mr. Artur Inderike for allowing me the opportunity to write for eForensics Magazine. Also big thanks to all my students at EDP University. I am really honored to be a part of your educational process in the field of information security and digital forensics. Last but not least to my family, my son Nicky for being just him and keeping me sane and balanced and to my beautiful partner Melissa for being so understanding of all my crazy schedules and always supporting me, no matter what.

PART I: THE THEORY

HANDLING AND ANALYSIS OF DIGITAL EVIDENCE

It is critical to carry out a computer crime investigation once the organization has discovered a potential criminal violation produced through the use of its resources and information systems. It must conduct a preliminary investigation by taking into account the following steps:

- Determine if a crime has been committed. This step is critical. The organization must be careful to distinguish between failures of equipment, non-intentional misuse (user error) and deliberate criminal intent. The internal auditors of the company, the IT department and senior management should be involved in making such decisions.

- Determine the status of the incident. When the incident occurred? Where did the intrusion occur? Was it internal or external? This incident is still happening? If not, when it stopped?

- Revise organizational policies, security and audit procedures to determine the best method to continue the investigation.

- Determine the need for police assistance. The organization will have to decide if the violation is serious enough to call the police or other law enforcement agencies. Most computer crimes are not reported to the police due to several factors, but the most important is the desire of the organization to maintain its flaws and weaknesses from public scrutiny, its customers and shareholders. This is a difficult decision for the company. However, as also mentioned above, if companies do not report computer crimes, the law cannot do anything to help and criminals have a free hand to continue their activities.

HANDLING OF EVIDENCE

One of the main differences between the investigation of computer crime and conventional criminal activities (theft, murder etc.) is the volatility of the evidence that resides on computers. In fact, the evidence of a hack can be removed or changed as part of the investigation. Therefore it is very important that the organization and law and order agencies apply a quick and effective solution to acquire, and properly manage and document the evidence obtained.

CRIMINAL ACTIVITY

The admissibility of evidence obtained from computers in a court case is really no different than the admissibility of any other evidence. Evidence must be:

- Relevant

- With solid foundation for introduction in court

- Obtained legally

- Preserved with integrity

In the management of computer data in criminal investigations, the examiner or investigator must be aware of some of the vulnerabilities of computer evidence:

- The researcher must ensure that disconnecting some equipment will not cause the destruction or alteration of evidence required for investigation.

- Keep in mind that the magnetic storage media are susceptible to the magnetic fields. Evidence can be deleted without the investigator being aware of it if you make the mistake of bringing the equipment near strong magnetic sources.

- Note that other devices connected to the computer may be required to complete the investigation of the data residing on the computer.

- The investigator should write-protect all disks that are being analyzed in the investigation so they cannot be inadvertently altered.

THE INTEGRITY OF THE EVIDENCE

There are aspects that should be considered in the treatment of data. These must be addressed regardless of whether the incident will be prosecuted as a criminal offense, or civil litigation. If the organization decides not to take any action, it is important to understand that if a digital forensics examination was conducted wrong, the company could become liable and trouble may arise for both the organization and the examiner. If the examiner is able to discover evidence of any type of crime in a computer system, then he should be able to prove to the state unequivocally that the evidence has not been modified in any way by his actions. This requires strict forensic methodologies designed to meet the necessary tests and ensure the integrity of proof “beyond reasonable doubt”. This is important when submitting a report to the company or in court. Therefore, forensic examiners must be aware of the next element about computer evidence seizure:

> *Search and Seizure / expectation of privacy: The first question to ask on a computer fraud investigation relates to the expectation of privacy of any employee or person outside the company that may be involved in the incident. For example: we investigate an incident in which an employee was caught using a company computer for personal use. The company had not established policies for computer use. The employee has never been formally notified that the use of the computer for personal matters was prohibited and that the company had the right to inspect the contents of the computer at any time. Therefore, the employee may protest the act as an invasion of privacy. This shows that appropriate policies are crucial. This may have created a situation in which the company will need a court order to examine the contents of their own computers!!!*

PREPARATION (PRE – SEARCH)

You should get as much information as possible about the location of potential evidence before drafting affidavits, search warrants etc. Some questions might include:

- Have you determined the type of computer system that is involved in?
- What operating system is used?
- Are the computers connected to the internet?
- How many people are needed to carry out the search?
- Do they require experts with specific experience?
- Have you determined the resources required to carry out the research?
- Did you consider the time required to perform searches in the investigation?
- Did you consider other peripheral devices (USB drives, printers, etc.) might be needed for the investigation?

PREPARATION FOR SEARCH WARRANTS

Application for Search Warrants has been affected a lot by new technologies and the changing nature of criminal law. Nowadays you should consider several issues that had not been encountered before. The forensic examiner must know how to write an application to get an order to seize property that contains evidence (both intangible and tangible). The order must consider contingencies such as the ability to separate data files relevant to the case that resides on the same storage device with irrelevant files. The order must be broad enough to defend the search and seizure of all the evidence necessary for the investigation, but narrow enough to exclude all material that is not relevant. This can be a very difficult standard to meet, and will depend on the judge to whom the affidavit is directed to. To satisfy the “particularity” of the Fourth Amendment of the U.S. Constitution, the forensic examiner must be able to justify each and every one of their applications so the judge understands that each item to be seized may contain evidence.

THINGS THAT CAN BE CONSIDERED EVIDENCE

- Computers
- PC Components
- Peripherals
- Word processing equipment
- Modems
- Monitors
- Printers
- Plotters
- Scanner
- Data storage devices.
- Cables
- Documents
- Manuals
- File lists

PROCESSING EVIDENCE TO ELIMINATE IRRELEVANT INFORMATION

The search and seizure of technical equipment require specific procedures to be followed by forensic examiners to ensure the integrity of the evidence, and to protect the organization from civil litigation. These guidelines are written to meet the requirements of criminal evidence, and every step in the process is there for a reason.

- If possible, before executing a Search Warrant, where teams are assembled to seize computers, make sure someone familiar with this type of equipment will be present to assist in the identification of the different components.
- It is very important that anyone not involved in the process stays away from any computer equipment, and is not allowed to touch the equipment.
- Take pictures to the computer screens when systems are on.
- If there is a computer or peripheral that is not covered by the Search Warrant leave it under supervision until a further order may be obtained.
- Never use the keyboard or mouse to search for information in the system using any associated media that can alter the state of the data at the time of the seizure.
- Do not move the computer more than necessary. A sudden movement could cause destruction of data or damage to the equipment itself.
- Photograph the computer system from multiple angles. Move the computer as little as possible before taking this photographs to indicate how the equipment was originally placed. Consider filming the confiscation procedure to complete documentation of all actions taken. However, caution is advised, because video captures everything that is said and done.
- Document equipment status when first observed (was on, off, had data on the screen)

Depending on the experience of the person, it may be recommended to disconnect power before taking any action. Although this action will cause the loss of all information in RAM, it could prevent damaging other data. NOTE: This applies to workstations that are not connected to a network.

- Disconnect the other components and / or parts of peripheral equipment (printers, monitors, etc.) Note that many peripherals use RAM that may contain evidence that are lost when disconnected (printers).
- If possible, photograph all cable connections (usually in the back of the system) before disconnecting.
- Disconnect all components are connected to an external power source (for example from an electrical outlet, etc.).
- Never connect or disconnect cables from the system (keyboard, mouse, USB etc.) when the equipment is operating.
- Label all cable connections, including telephone cables are connected to the system so that the system can be reconstructed at a later time for analysis.
- Label each item that will be confiscated. This includes CPU, monitor, printer, etc.
- Each element that has a removable outer casing must be sealed with adhesive tamper proof stickers. This helps prevent allegations that the components have been removed or altered.

Document the specific location of all items seized (in what room, reference to the photographs to be taken, the person who took the photo, serial numbers, identifying marks, etc..)

- Inspect all optical drives to determine if they contain CD / DVD. If so, you must remove the disk from the drive and place it in a protected packing. Label the optical drive and its packaging.
- If there is any uncertainty as to any equipment, do not speculate. Label the equipment and leave the issue for further analysis.
- If they are covered in the Search Warrant, confiscate all manuals and other documentation.
- After all equipment and magnetic media are labeled and inventoried, store them in a cardboard box seal it properly and make sure it's identified. You should place a list of the inventory inside the box, one outside the box and another should be used for the final delivery to be signed and copied
- Check the inventory of everything that is removed from the location. This will be necessary for the return of any equipment (if applicable), but also serves to provide a measure of protection from liability of the person seized.

STORAGE OF EVIDENCE

After a seizure, most criminal justice agencies have a data storage center where the equipment is transported and stored until needed for processing or used in court. The storage environment must be:

- Relatively free from dust
- With temperature and humidity controlled
- Free electronic and magnetic fields

METHODOLOGY

For this booklet we will be using all protocols established by NIST (National Institute of Standards and Technology). This applies to all law enforcement agencies within the US and its territories whether they are local, state, federal or military. These standards of forensic incident management are written by various authors including representatives from Homeland Security, so it's a solid methodology that will allow you to develop a case management system according to the industry standards accepted in the US. Also it will help other law enforcement agencies to work with you in case you find evidence that requires a formal criminal investigation. For example, if by any chance you find child's pornography within a disk you are analyzing you are required by law to immediately stop your analysis, call the

FBI and hand all the evidence to them. If you follow the same standard they use the transition will be effortless and the evidence will stand in court as long as all chain of custody documentation is in order. To read more about this visit *http://csrc.nist.gov/publications/* and do a search for the forensic standards documentation

If you are from another country you need to verify what laws and methodologies are applicable for your particular case.

ANALYSIS OF EVIDENCE

The primary concern in the analysis of electronic evidence is to maintain the integrity of the evidence. This means that procedures must be developed to ensure there are no complaints with the court that the methodology used for the analysis damaged or altered the hardware, media, or data that constitute proof.

EXTRACTION PROCESS TESTS

Before you Start doing any type of extraction process you need to have the right tools. If you are doing a live capture you can use Helix or Live Response. Both are products manufactured by e-fense that are worth checking out and are considered as standards in the industry and are approved by NIST. Helix allows you to do a multitude of tasks from dumping RAM and/or creating an image, doing a full inventory of the machine etc. What is nice is that the memory dump and imaging process can be done via a network so if you need to send the image to a machine on the network you can. This is beyond the scope of this writing but now that you know it you can experiment with this feature.

Live response is a USB designed to do a multitude of tasks including searching the system for known hash values. Live Response can also capture of the following things:

- physical memory from all Windows systems
- clipboard content
- device list
- state of encrypted drives
- list of installed applications
- open network ports
- running processes
- general system information
- user list and login information

If you are interested in these products visit *https://www.e-fense.com* for more information. There's a free Helix live CD available for you to download all other products including Live Response are paid products. There are other commercial tools approved by NIST like EnCASE and FTK that are worth checking out. As far as open source tools the Autopsy Forensic Suite created by Brian Carries is also approved by NIST. If you use a tool not approved by this organization and also a tool that is not an Industry Standard you are allowing the possibility that a good lawyer might bring that up and render your process as invalid. The good news is that is very easy to verify if the tool you want to use is on the NIST catalog. To do this just go to *http://www.cftt.nist.gov/* This site includes a link to a Computer Forensic Tool Catalog that let you search for all NIST approved tools. By doing this you will be sure that your analysis is done following the standards established and you can even print the information of your tool from the site and add it to your report to help you validate that you are using the right tools.

Also you need to use a write blocker. These are devices that allow the acquisition of information on a storage device without creating the possibility of accidentally damaging the device contents. They allow you to use read commands but block write commands, this way you only can look at what's on the device but not change it. This is our bridge between the real device, our tools and the drive we will use to store the bit by bit image. The website we just mentioned also provides valuable information regarding write blockers so make sure you read it too. Remember, adhering to a standard is the best thing you can do in order to develop a solid procedure that will be validated by the

industry, law enforcement agencies and most importantly, the court. So make sure you read all the documentation mentioned before and if possible add this to your company's incident handling policies. Once we are clear on the tools that we need and we have done the proper research according to NIST we can continue.

Many times the equipment seized as evidence is inventoried according to information available on their enclosures, i.e. the brand, model and serial number of the particular unit. The hard drive is the only component inside the CPU case that is examined, so he/she should consider the following:

- Mirror Copies: The forensic examiner must make a mirror copy of any medium to be analyzed. This will ensure that no changes occur to, or damage the original evidence. When there is no choice but to examine the original evidence, you must use a write blocker to ensure that the information cannot be altered while examining the original device. This will protect the integrity of the original evidence and avoid accidental alteration of the original data.

- Virus detection: All data storage media should be screened for viruses. This will protect the fraud examiner of possible allegations that evidence destroyed due to the presence of a virus.

- Search for keywords: Due to the huge storage capacity of current computer resources, it might be easier for the forensic examiner to perform a "keyword search" to find names, dates, account numbers, etc. which are important to the case. This will reduce the amount of time used to complete the analysis, and also protect the forensic examiner from claims that his search was too broad.

- Hidden and deleted files: Most operating systems allow files to be hidden, preventing visibility to normal search procedures. There are programs to show "hidden" files. It should be inspected if these files exist then try to determine whether they were hidden intentionally, and see if they contain relevant evidence. In addition, many users do not realize that deleting a file does not necessarily mean that the content of the files has been destroyed. There is also software to recover deleted files.

- File Slack Area: There is a difference in most operating systems between the "logic" size of a file and the "physical" size of a file. Logical size refers to the size in number of bytes the file occupies. In a directory listing, this is the number that is displayed in the option file size. The physical size of a file depends on how the operating system stores files. On most operating systems, the disk is organized into blocks called clusters. Files occupy a number of groups, although the logical size of the file is smaller than the cluster size. In these cases, the difference in space between the space of physical file and logical file space is called File Slack Area. This area can contain data from previously deleted files that might have evidence.

- File Signatures: When reviewing a directory listing in Windows Explorer, the File Signature File is one of the options that may appear. This information may indicate that the file is an "application" which is a "Word Document" or some other type. However, this designation is usually based on the "extension" of the file, and may not be an accurate indication of the content. For example, if a file was created in Microsoft Word and saved with the name "file.doc" directory listing correctly indicate that this file is a "Word Document". However, if the file is renamed to "program.exe," the directory listing for error indicates that the file is an "application", even though the contents of the file itself have not changed. The inspection of each file on the media seized would be extremely tedious, however, there are programs that can automate this process and report any discrepancies. If you need to find a good tool for this remember to search the previous sites mentioned. Also if you are analyzing just a few files and want to get your hands dirty you can do a hex analysis of the file and look for clues that might let you know that something is not what it seems.

As an example if you find a file on FTK that shows itself as a JPEG/Exif file this means that something is hidden inside that picture. If you go inside the hex view of FTK you can use the search function and look for different signature patterns like Rar! If you find the Rar! string inside the hex view of the file this means that the JPEG might be hiding something inside.

The next thing to do might be to change the extension of the file from jpeg to rar, extract the file and you may be in for a surprise. This is a good way to polish your hex skills, so learn more about the specific hex signatures of as many file extensions as you can.

- Encrypted files: If the forensic examiner finds files that have been encrypted he will need some software to decrypt documents. There are also several companies that specialize in this type of job. There is a precedent to force the suspect to disclose the decryption code or password via a court order. Consider that the computer is a container

and that the encryption is a blocking tool. If a valid search warrant authorizing examination of the data is provided, this would be no different than a court that orders a suspect to open a file cabinet to allow inspection of its contents.

RECONSTRUCTION OF FACTS

After reviewing all the evidence collected you should try to reconstruct the incident in question. This process is a useful tool for the investigation of cybercrime. You need to make digital forensics evidence “talk” about what happened. The analysis may be used in one of the following categories:

- Forensics: recovering evidence to support or refute a hypothesis court to identify suspects and / or crimes.

- Data collection: find data to support or refute hypotheses about the incident. This process usually begins with a search of the commonplaces of use based on the type of incident. For example, if we investigate the web browsing habits, we examine the browser cache, the history, and bookmarks. When investigating intrusions we seek signs of a rootkit or new user accounts. With the findings, the hypothesis is developed and you can begin searching for evidence to refute or support it. It is important to look for evidence for both. The search process is quite simple. Define the characteristics of the object (s) sought and use specialized tools to get them. For example, do a search to extract and identify all items with a file type of “JPG”, search for files based on their content signatures, etc. This allows you to find all files of a certain type, even if someone has changed their name. By analyzing data coming from the network, you can search all packages in a specific source address or all packets going to a specific port.

- Reconstruction of events: the evidence found is used to recreate the events that occurred on the system. During the search for evidence, you may find files that violate corporate policy, but we cannot answer questions about events. The download of a malicious file may have been the effect of an event, but you should also try to determine the application that allowed the file to be downloaded. Ask yourself questions such as: Is there evidence that was intentionally downloaded from the web, or it could be a malware that causes the downloads? You have to be able to correlate the digital events with physical events. The event reconstruction requires knowledge of the operating system and applications that are installed on your system in order to create a scenario that makes sense.

After all this you should feel comfortable to attempt you first seizure process. Let’s move on to a practical demonstration of the procedure.

PART II: THE PRACTICAL PART

SECTION A: SEIZURE OF EQUIPMENT

In this section I will be using part of a report made by one of my group of students as required for their master's degree computer forensics class. You will be able to understand the mechanics of executing a warrant in order to seize a computer that is part of a forensic investigation. A big thanks to Jorge, Karla, Kenia, Krystal and Luis for being a great team, both Luis and Krystal have formal education in law enforcement and it was a pleasure working with them. We had a great learning environment in that class

NOTE TO READERS: This section relates only with the process of executing a search warrant. Even when the PC on the example is powered on we will not be focusing on doing a live memory dump. The main idea here is to focus on the proper procedure of getting a warrant, going to the intended facility and seize the equipment mentioned in the warrant following the right procedures so your chain of custody and process cannot be questioned by any lawyer or court. For this example the warrant only states that we will pick up a PC. Remember that the order must be broad enough to defend the search and seizure of all the evidence necessary for the investigation, but narrow enough to exclude all material that is not relevant. As a forensics specialist you CAN perform a memory dump right on the scene if the machine is working when you arrive and that doesn't have to be specified on your warrant. This raise the question: do you always do a memory dump when the system is powered on? The answer is: It's your choice as a forensic investigator. If you are able to see a note with a name and a phone number and an excel chart you will be covering the proper procedure by just taking pictures of the screen and writing down the specifics of your findings. Then you can unplug the system and proceed with the seizure.

Now let's move on to the next section to see an example of a seizure:

COMPLETION REPORT: SEARCH WARRANT

Order No. 3142013 Case: 05182013 – May 18, 2013

On May 18, 2013 at 8:00 am MIF6830-G2 staff arrived at the facilities of EDP University, Hato Rey campus by request, of Mr. Jose Ruiz forensic investigator in charge of the case to enforce a search warrant issued by the court regarding digital evidence located in one of their computers. EDP University is located at Ponce de Leon Avenue Building # 560, San Juan, Puerto Rico, 00918.

At 8:15 am the order was presented to the security guard, Officer Maria Gerena from Omega Services Company, Corp, who escorted the technical group to the fourth floor to room 401. We arrived at room 401 at 8:20 am it was observed that the room was made up of three rows of computers all black. There were twenty-five (25) computer stations, two (2) front rows of eight (8) stations each and the third row of nine (9).

Pictures of the room (Figure 1 and 2):

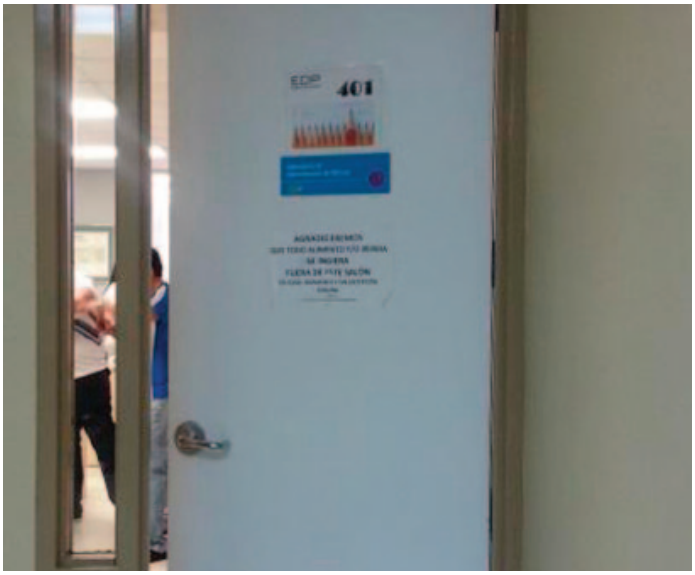


Figure 1: Room 401 where the computer was located

Figure 2: View of the room from the entrance door

The room measures 30 feet long by 25 feet wide. From the front door, (south) to the wall of windows at the end (north) it measures 25 feet. From the side solid wall, (east) to the wall with windows (west) it measures 30 feet. Once inside the technical staff proceeded to put on latex gloves and start checking the serial numbers of the CPU of the twenty-five (25) stations. The computer included in the warrant was the one with serial #20A-02-01GZ1 (Figure 3).

The system was the first station on the third row near to the back of the room (Figure 4 – 7). The system was on and it could be seen that a worksheet from Excel 2010 was open (Figure 8). The open file had the name “Regions-test cases”. It was also found a sticky notes application with the following information, 787-345-1722 (Figure 9).

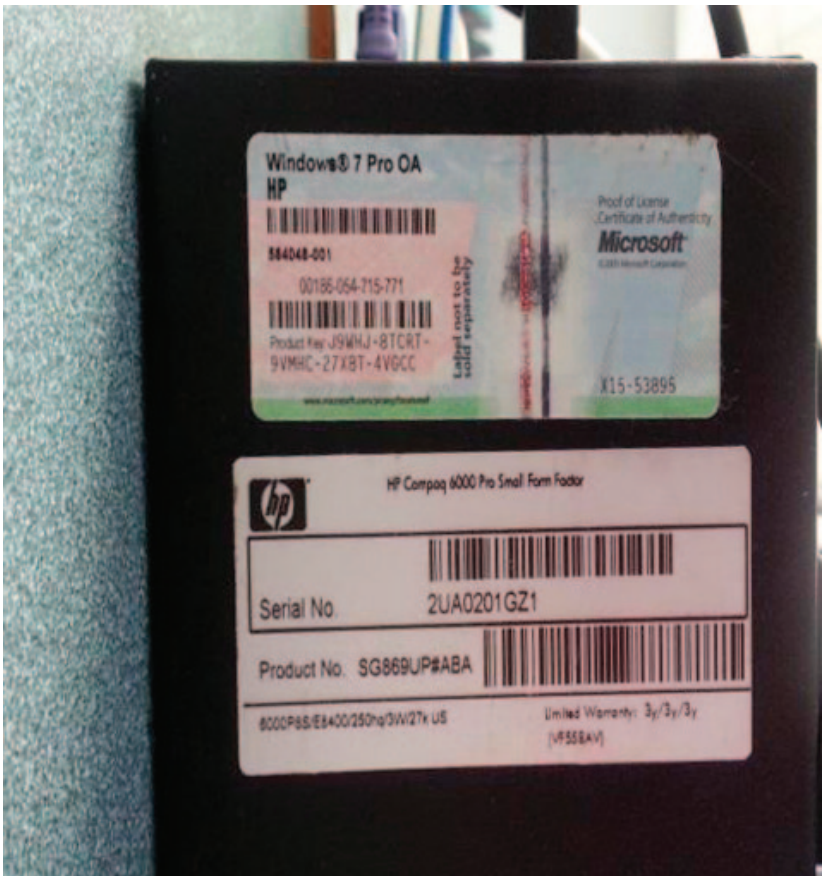


Figure 3: Picture that details the serial number and aditional information of the unit to seize

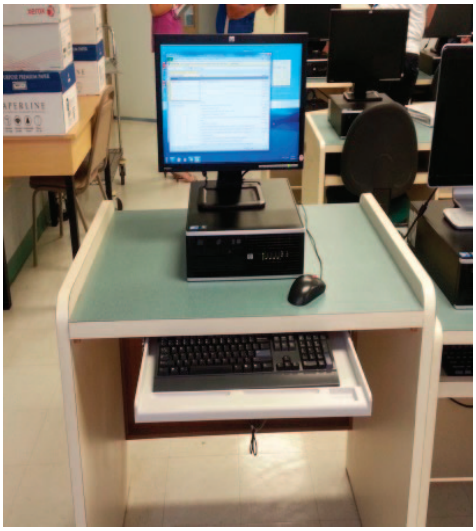


Figure 4: Computer to seize, wide view, system on

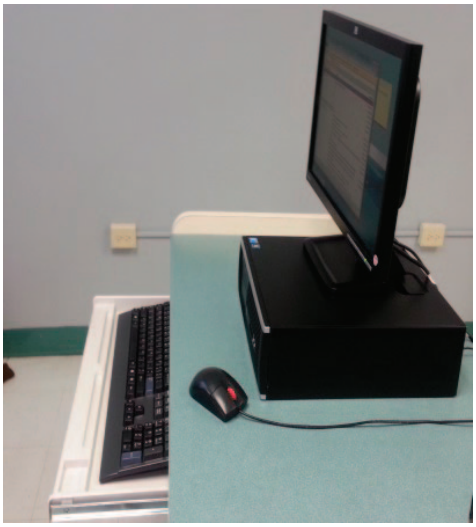


Figure 5: Computer to seize, side view.

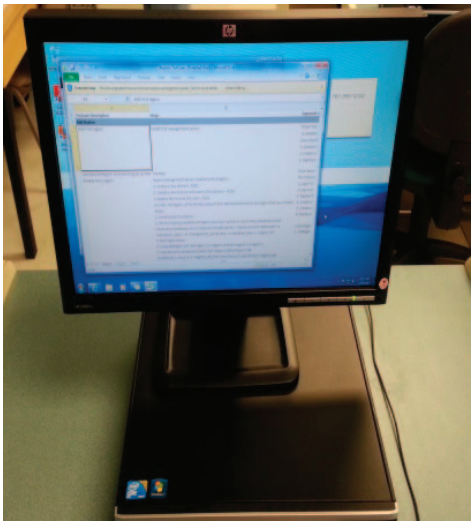


Figure 6: Computer to seize, monitor closer view (1)

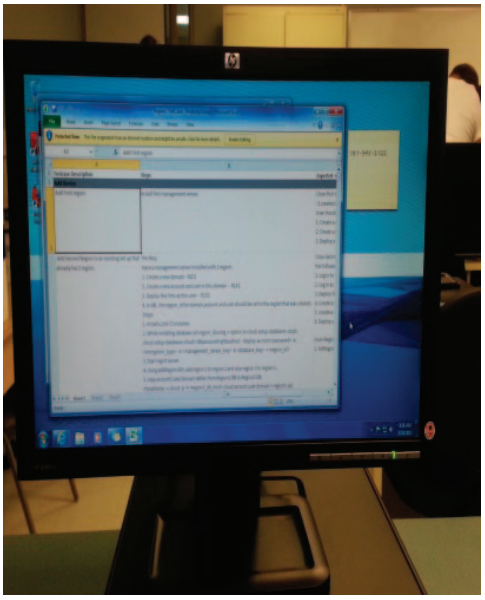


Figure 7: Computer to seize, monitor closer view (2)

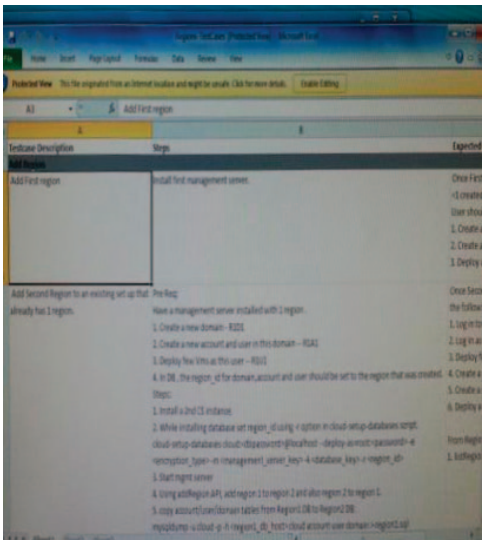


Figure 8: Excel table “Regions-test cases” chart

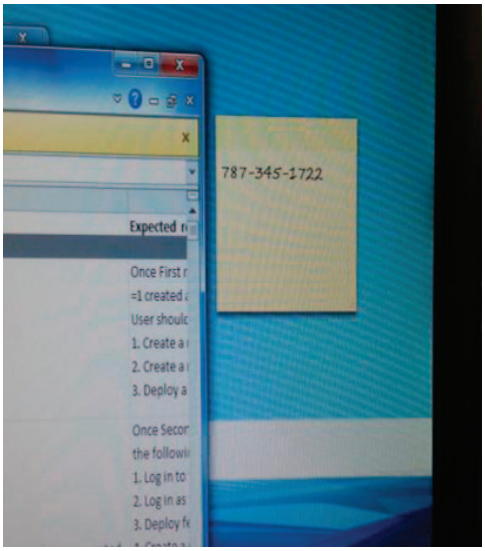


Figure 9: sticky notes – 787-345-1722 telephone written

Once all the photos taken at 8:35 am we began the process of disconnection of components.

- 8:35:02 a.m. disconnect the CPU HP S / N 20A-02-01GZ1 from the outlet.
- 8:35:27 a.m. disconnect Monitor HP model HPLE 1551W S / N CNC007PC72 from the outlet.
- 8:36:10 a.m. disconnect the blue LAN cable from the CPU.
- 8:36:18 a.m. disconnect monitor cable from CPU.
- 8:36:40 a.m. disconnect the USB mouse black with red button on the CPU.
- 8:36:51 a.m. disconnect the black keyboard from CPU.

Once done we began the tagging process (Figure 10):

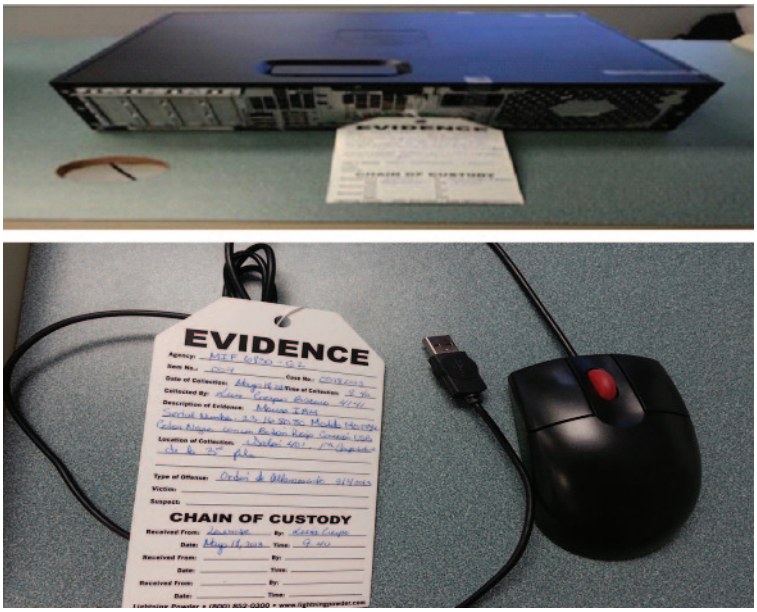


Figure 10: The tagging process for CPU and mouse

At 9:42:07 am all evidence was properly tagged and inventoried. Once all components were properly tagged we put them in a box. The box was sealed and signed by all members of the team to prevent tampering. The box also contained a copy of the full inventory of items seized. That inventory was copied 3 more times to attach one copy at the top of the box and to have 2 signed at the point of delivery to prove successful delivery of items and validate the chain of custody (Figure 11).

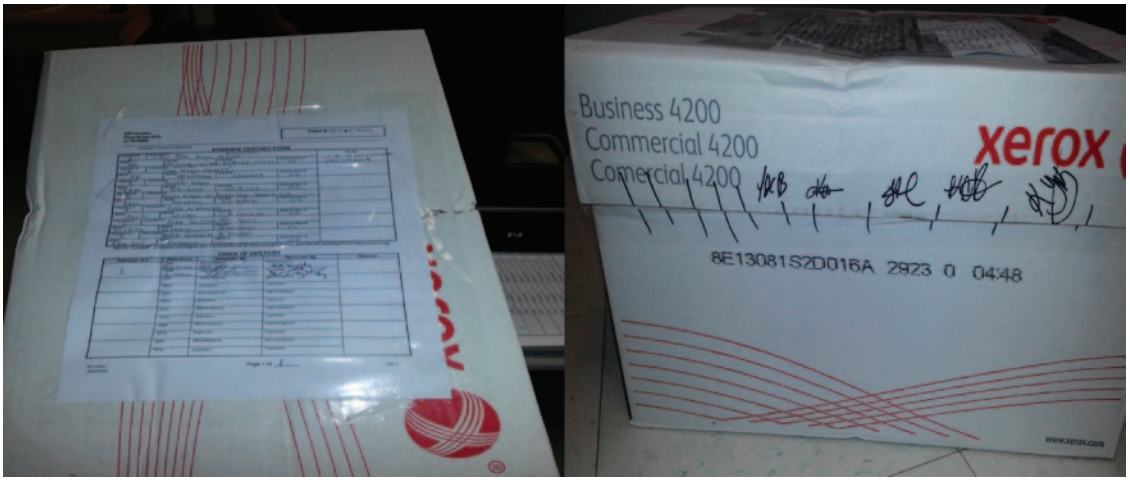


Figure 11: All the evidence is placed inside a box that is fully sealed and signed by all members of the team.

At 10:20 am we delivered the box to Mr. Jose Ruiz who signs 2 copies and we end our chain of custody (Figure 12)

EDP Forensics
Ponce de Leon #123
SJ, PR 00918

Case #: 05187 2013

Computer Forensics Laboratory

EVIDENCE CUSTODY FORM

Package #:	Description:	Model:	Serial #:	Agency Item #:	Notes
1	CPU Color Negro 10 USB				orden de allanamiento 03/14/2013
Make: HP	Model: HP Compaq dc5700 Pro	Serial #: 2UA-02-01621	Agency Item #: 01		
Package #: 1	Description: Monitor Color Negro Aprox 14"				
Make: HP	Model: HPLE1951W	Serial #: CNC207	Agency Item #: 02		
Package #: 1	Description: Teclado Negro				
Make: IBM	Model: KB-0225	Serial #: 4378307	Agency Item #: 03		
Package #: 1	Description: Mouse Negro con Boton Rojo Conexion USB				
Make: IBM	Model: MO2840L	Serial #: 23-K68080	Agency Item #: 04		
Package #: 1	Description: Cable de Monitor				
Make: AWM	Model: 20276	Serial #: E246588	Agency Item #: 05		
Package #: 1	Description: Cable Corriente PC 300V				
Make: SVTFTZ	Model: SVTFTZ	Serial #: E553333	Agency Item #: 06		
Package #: 1	Description: Cable Corriente de Monitor				
Make: FAN JET	Model: 544001	Serial #:	Agency Item #: 07		

NOTE: Contents of sealed packages are not inventoried at time of submission, but will be cataloged during processing

CHAIN OF CUSTODY

Package #'s	Date/Time	Released By	Received By	Reason
1	Date: Mayo 18, 2013 Time: 10:20am	Name/Agency: MFF 6830-G2 Signature	Name/Agency: URM Jce/Jose Ruiz Signature	Received Evidence Box JARM
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	
	Date	Name/Agency	Name/Agency	
	Time	Signature	Signature	

EC-4108.2
2006/03/23

Page 1 of 1

Rev. 1

Figure 12: A closer look of the chain of custody document attached to the box

Sample of a tag for a better look (Figure 13):

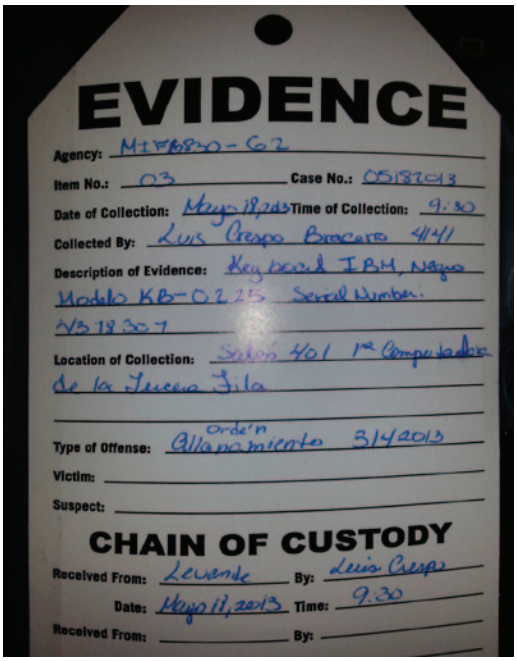


Figure 13: A closer look at an evidence seizure tag.

Once you deliver the evidence box to your final destination you are finished with your duty of seizing the system. Make sure that you have a document that states that you successfully delivered the evidence and add it to your chain of custody so you can clearly prove the correctness of your process. At this point this part of the process ends and the forensic analysis starts. If you are also in charge of this analysis it should be stated in the chain of custody.

SECTION B: DATA ANALYSIS AND REPORT

For this example I will be using a simulation I did back in 2011 for one of my forensics courses. I "analyzed" evidence related to the Albert Gonzales case to produce a report that will be held in court as admissible. You can use this as a template for your reports:

EXECUTIVE SUMMARY

Heartland Payment is a company dedicated to handling financial transaction processes for a great variety of clients. They have over 250,000 customers worldwide including TJX Industries – holding company that manages the Marshall's Stores chain. TJX together with his team of lawyers and federal prosecutor Stephen P. Heymann has requested our services to discover and retrieve electronic information apparently located on a USB device owned by Albert Gonzalez, currently charged with penetrating TJX's computer systems and steal sensitive information.

According to Mr. Heymann, the device is part of the body of evidence collected by FBI agents who conducted raids at the residence of the accused. Mr. Heymann understood that this device may contain incriminating evidence vital to the prosecution and conviction of Albert Gonzalez and his accomplices.

OBJECTIVE

The U.S. federal government hires JRM Security services in order to analyze, discover and retrieve electronic information stored on a hard drive allegedly empty, with the purpose of obtaining evidentiary material to help federal prosecutors to prosecute and obtain a conviction of the accused Albert Gonzalez.

SCOPE OF WORK

On December 7, 2011 the U.S. Attorney Stephen P. Heymann gives Jose A Ruiz Marquez (JRM Security Forensic Investigator) a seemingly empty USB device viewed by prosecutors as evidence. We will analyze the device to see if it's possible to find relevant data that serve as incriminating evidence in the case U.S. v Albert Gonzalez. JRM Security task is to discover, collect and preserve any relevant evidence found on the USB device in order to be analyzed and later be presented as evidence by District Attorney Heymann. Following industry standards forensic analysis process we will be using the following technology:

- Access Data FTK Forensic Toolkit
- FTK Imager
- FTK Pro Discover Basic
- Access Data FTK Registry Viewer

The tools mentioned above are considered standards of excellence in forensic research industry and are highly accepted in research processes conducted by the FBI, Interpol and multiple agencies of law and order. This ensures that the investigative process conducted by JRM Security meets or exceeds the requirements set by the Federal Government for processing, preparation and submission of evidence to be used in legal proceedings.
With this established JRM Security begins with the process of acquisition and analysis of evidence. JRM Security will create a report of findings and notify the prosecutor in writing of all findings.

CASE DESCRIPTION

- Case number: C-1-2011-12-07 (C = case 1 = number, year, month, and day of the delivery of "evidence" by the customer)
- Forensic Examiner: Jose A Ruiz Marquez

- Customer: U.S. Federal Government
- Customer Representative: Stephen P. Heymann

DESCRIPTION OF DEVICES USED

The devices used during the research process:

- Laptop Toshiba Satellite L-505 model where reside all the tools and applications that will be used in this process. The machine is used solely for this purposed and it's not connected to a network or the internet.
- Ultra Block USB: Write Blocker-USB device that allows the acquisition of information from a disc without creating the possibility of accidentally damaging the contents of the original unit which extracts the data. This is accomplished by blocking any write command to the device analyzed and making it a read-only device.
- Sans 2 GB USB Serial No. B60QLCYH. Given to JRM Security by District Attorney Heymann.

SUMMARY OF FINDINGS

The process of digital forensics involves the acquisition, preservation, analysis, and presentation of digital evidence. This type of evidence is fragile and the researcher may unwittingly alter, or destroy the information in any device that is being analyzed. The consequence is that this evidence is inadmissible in court. To minimize the possibility of this happening reference JRM Security uses the Electronic Data Recovery Model (EDRM) in order to obtain evidence properly preserved, integrated and reliable, thereby making it legally defensible electronic evidence. A model is shown below (Figure 14):

Figure 14: The forensic process

CHAIN OF CUSTODY

As we begin our process we must make sure to establish a chain of custody of all evidence integrated into our investigation. The chain of custody helps notarize the process of acquisition, analysis and control of all evidence. The following details the chain of custody followed by JRM Security (this is not an official document, it's a sample of how you can detail your events – Make sure each event is signed by all people involved):

Detail of chain of custody

First event:

Event Description: Evidence collected in the FBI evidence room. Evidence handed by Attorney Stephen B. Heymann and collected by Mr. Jose A Ruiz Marquez, JRM Security researcher. The evidence consists of: Sans 2 GB USB Serial No. B60QLCYH

- Event verified by: Jose A. Ruiz Marquez and Stephen Heymann.
- Number of evidence: E-1-2011-12-07
- Start Date: December 7, 2011 – 1:51 PM
- Completion date: December 7, 2011 – 3:22 PM

- Place of Origin: FBI office evidence room
- Destination: Forensic Laboratory – JRM Security

Second event:

Event Description: Creating case number and allocation of the same evidence.

- Event verified by: Jose A. Ruiz Marquez and Victor Betancourt.
- Number of evidence: Evidence # E-1-2011-12-07 Assigned to Case # C-1-2011-12-07
- Start Date: December 7, 2011 – 3:43 PM
- Completion date: December 7, 2011 – 4:02 PM
- Place of Origin: Forensic Laboratory – JRM Security
- Destination: Forensic Laboratory – JRM Security.

Third event:

Event Description: The process of acquisition and analysis of evidence. Refer to the procedures section in this report for specific details of the process.

- Event verified by: Jose A. Ruiz Marquez and Victor Betancourt.
- Number of evidence: Evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07
- Start Date: December 8, 2011 – 9:07 a.m.
- Completion date: December 9, 2011 – 2:02 PM
- Place of Origin: Forensic Laboratory – JRM Security
- Destination: Forensic Laboratory – JRM Security

Fourth event:

Event Description: Delivery of forensic analysis report to the prosecutor Stephen P. Heymann for evaluation. The report was delivered directly to the prosecutor Heymann by the investigator in charge of the evidence, José A. Ruiz Marquez

- Event verified by: Jose A. Ruiz Marquez and Stephen P. Heymann
- Number of evidence: Report concerning evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07
- Start Date: December 13, 2011 – 9:27 a.m.
- End Date: December 13, 2011 – 11:08 a.m.
- Place of Origin: Forensic Laboratory – JRM Security
- Destination: Office of the U.S. Attorney Stephen P. Heymann

Fifth event:

Event Description: Returning to the original evidence submitted by Attorney Joseph A. Heymann Ruiz Marquez. The evidence was delivered directly to the prosecutor Heymann by researcher in charge of the evidence, José A. Ruiz Marquez

- Event verified by: Jose A. Ruiz Marquez and Stephen P. Heymann
- Number of evidence: Evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07

- Start Date: December 13, 2011 – 11:21 a.m.
- Completion date: December 9, 2011 – 11:48 a.m.
- Place of Origin: Forensic Laboratory – JRM Security
- Destination: FBI office evidence room

EVIDENCE ACQUISITION WITH FTK

After the evidence analysis on item: Sans 2 GB USB Serial No. B60QLCYH was processed through FTK Forensic Toolkit tool we found multiple files in the following formats:

- Jpg
- Gif
- Txt
- Xls
- Sql

The scanned files are categorized in two ways:

- Existing: detected by FTK as being present without the need for specialized tools to retrieve them.
- Deleted: detected by FTK as being present with assistance of specialized tools to retrieve them.

The following are the files found that the nature of the information contained incriminating evidence are classified as related to the defendants in this case:

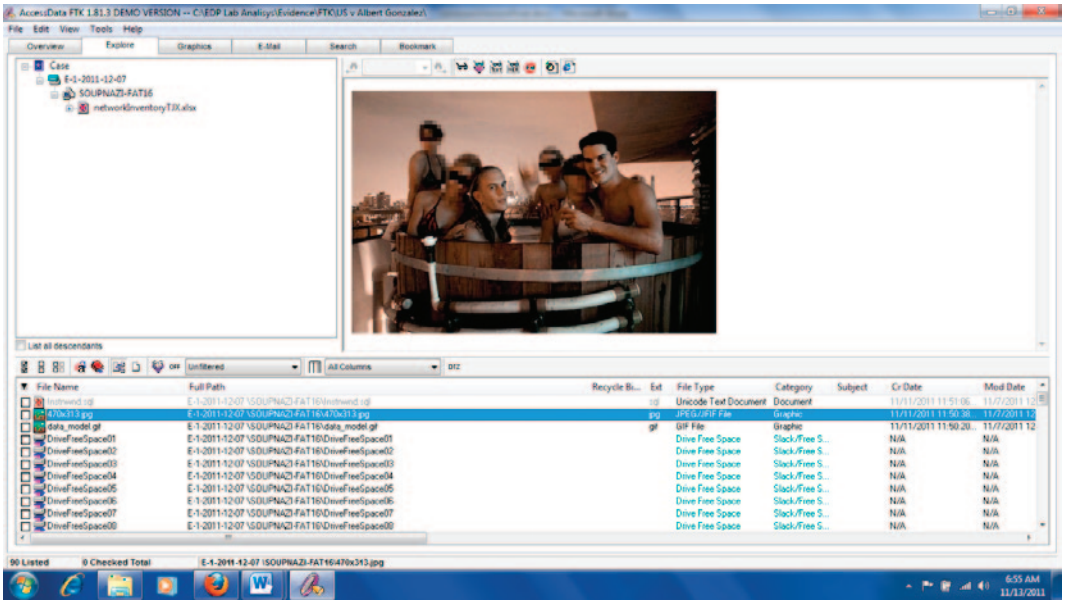


Figure 15: File 1 – existing – photo (. Jpg): Stephen Watts (left) and Albert Gonzalez (right) Gonzalez's apartment in Miami.

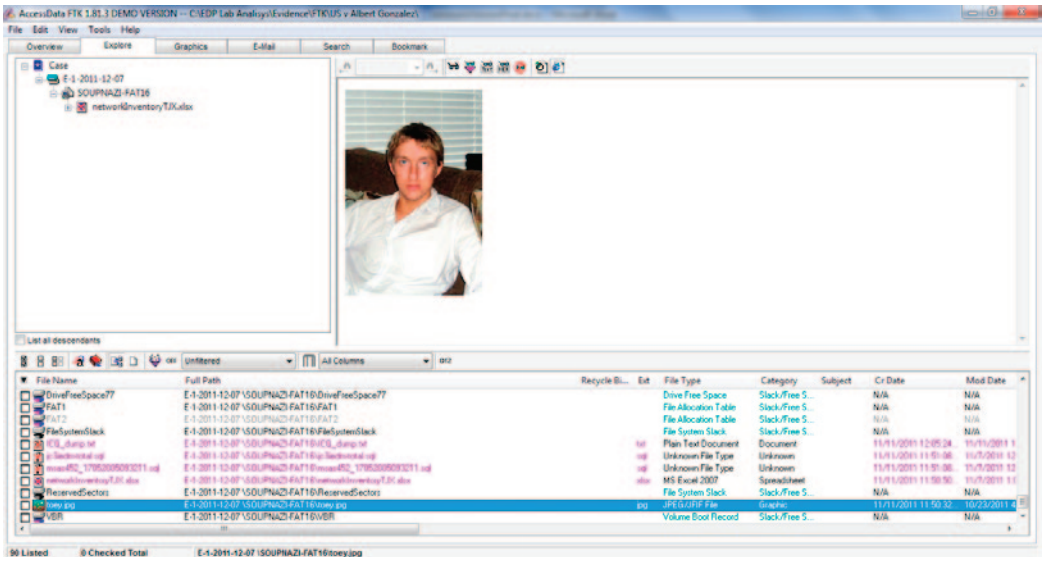


Figure 16: File 2-existent – photo (. Jpg): Photo of Patrick Toey.

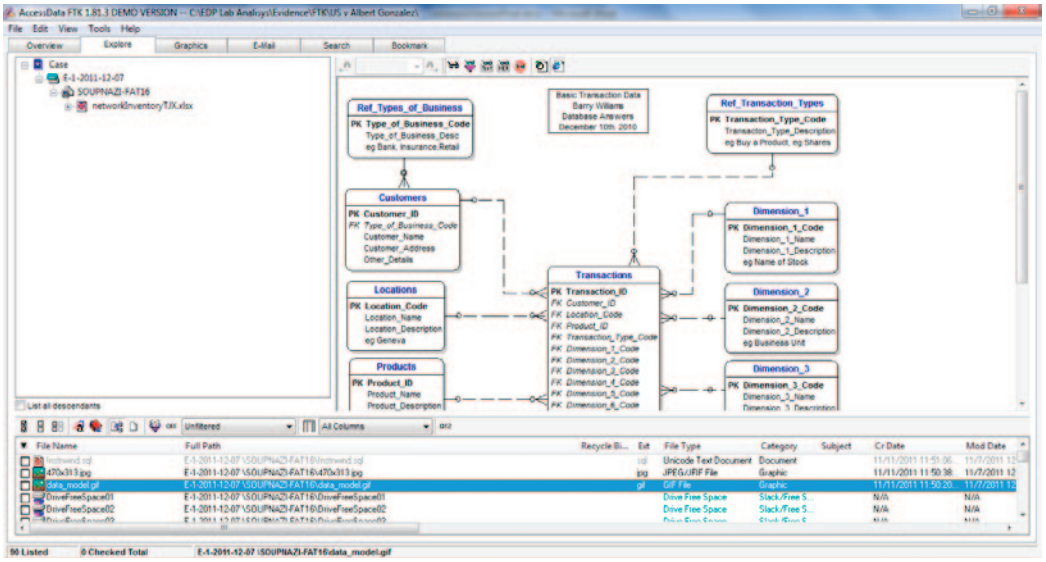


Figure 17: File 3 – deleted – file (. Jpg): Data Flow Diagram system POS (Point of Sales) used by Marshall's to process transactions in their cash registers.

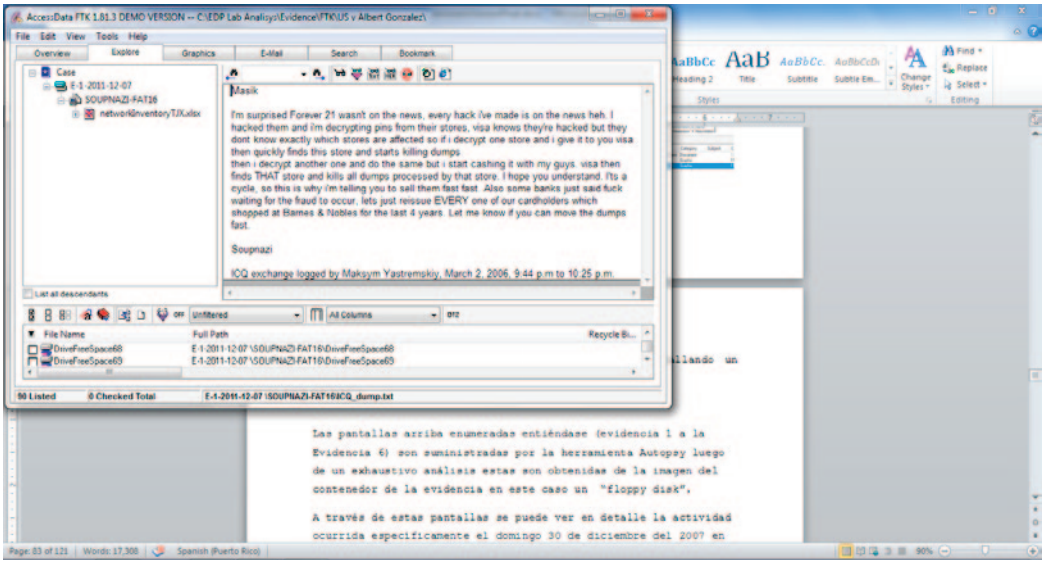


Figure 18: FILE 4 – deleted – text (. Txt) – Record of ICQ message detailing communications between Albert Gonzalez (soupnazi) and Maksym Yastremskiy (Masik).

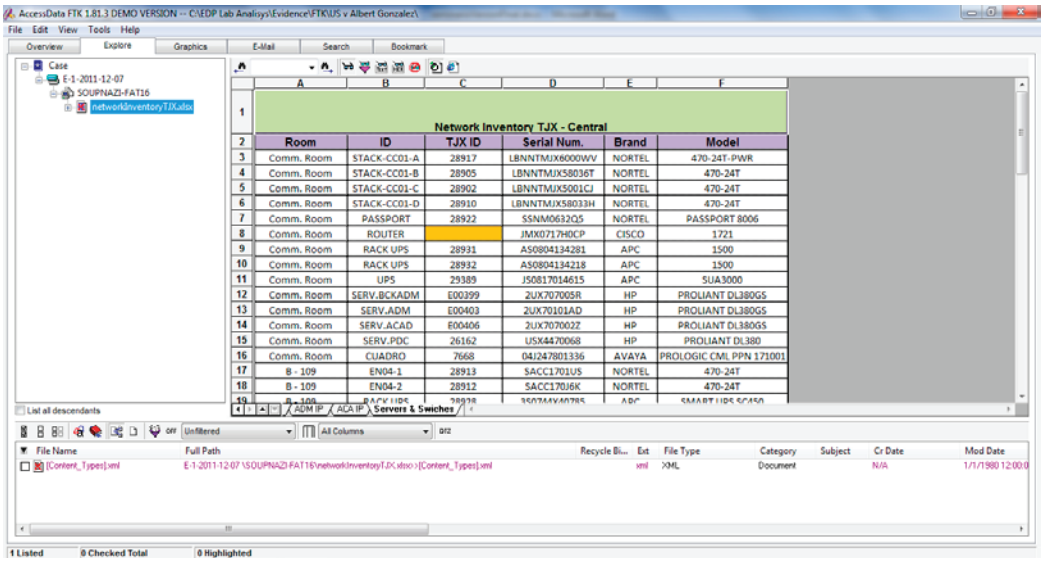


Figure 19: File 5 a – deleted – excel table (. Xls): Document showing the existing equipment inventory in the core network of TJX.

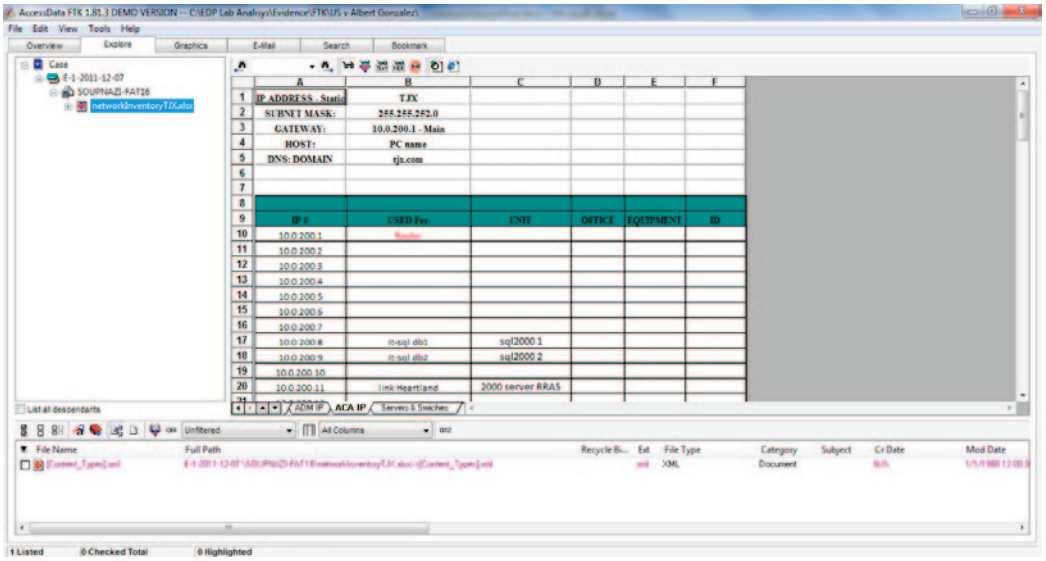


Figure 20: 5b file – deleted – excel table (. Xls): A document that shows the distribution of existing SQL servers in the core network of TJX.

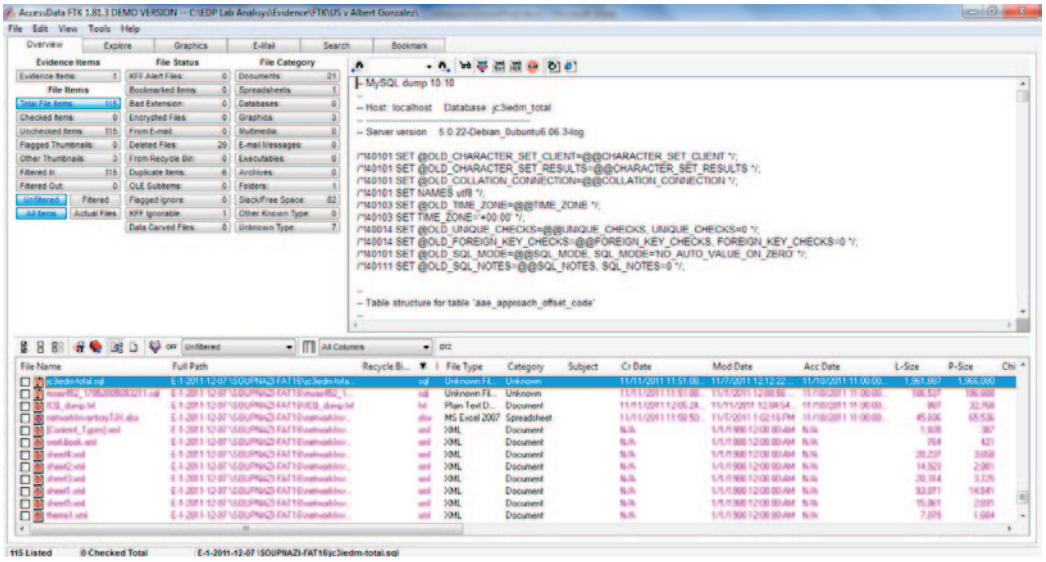


Figure 21: File 6 – deleted – sql dump (. Sql): Dump a SQL database recovered from Forever 21.

Through the screens listed above you can see in detail evidence that proves that the defendants Gonzalez, Toey and Watts were directly related and in fact there were communications between Gonzalez and Yastrzemski. In addition to these events, the device contained confidential files from TJX, Marshall's, and Forever 21, showing that there was an intrusion to the systems of those companies to obtain highly sensitive and confidential documents.
NOTE: For more details on the extraction process and device content recovered files via FTK, refer to the procedures section of this report

NOTE TO READERS: When you are analyzing files from an evidence image you need to verify the metadata and the creation, modification and access timestamps. It's important to notice that if the modified timestamp is for example indicating Monday but the creation timestamp is indicating Tuesday you know that the file you are analyzing was moved from some other place to the device you imaged. This is an excellent way of requesting an additional warrant to pick up other things that can provide evidence. By the same token if the file you found was allegedly stolen this proves that it was moved from another place so you need to check the alleged victim's devices and look for that file. If you find it, proceed to analyze its metadata and look for information such as author, software used to create it, and path to the original file. In this situation you can check the MD5 but if the file was modified this value will change and it won't help you at all. By doing this you can diffuse any questions from a lawyer because you can prove that the file was moved from the victim's system based on the fact that you have metadata matches in information and the mismatch on dates from the modified and creation metadata dates on the file you found in the evidence. If by any chance you need to investigate if the alleged hacker has an accomplice it will be good to see if the system admin has a logging system deployed that allows him to monitor any external device that was plugged into the network. You can go as far as getting the serial number of such device and if you are lucky enough the device you are analyzing matches that serial number! Finally, when you are about to analyze evidence you need to convert it to a format that is compatible to the biggest amount of tools possible. DD format is well read by Autopsy, FTK and EnCASE so by doing this conversion you are opening the door to creating an image that can easily be analyzed by multiple tools so you can validate your analysis in more than one tool or provide an image to be analyzed by other technician that has a tool different than yours (you use FTK, he uses EnCASE). Legally speaking, this conversion is not debatable as it is considered a standard procedure.

PROCEDURES

The following section describes the procedures used during the process of discovery, acquisition, analysis and preservation of evidence.

Procedure 1: Create Case

- Tool: FTK Pro – Discover
- Tool: Ultra Block USBWrite Blocker
- Evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07
- Start Date: December 7, 2011 – 3:47 PM
- Completion date: December 7, 2011 – 4:02 PM
- Description:

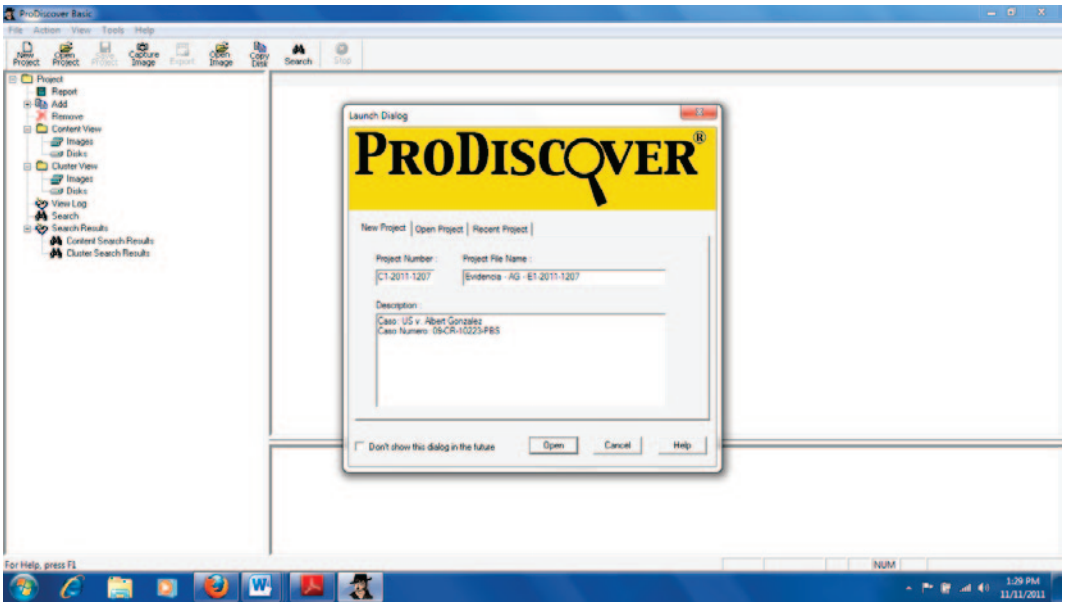


Figure 22: Creating a case with FTK Basic Pro Discover. Here we are adding the information for identifying the case including project number and name and a description of our scope of work

Procedure 2: Image preparation

a. Capture the image to be used

b. Tool: FTK Pro Discover

c. Evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07

d. Start Date: December 8, 2011 – 9:07 a.m.

e. Completion date: December 8, 2011 – 9:29 a.m.

f.Description:

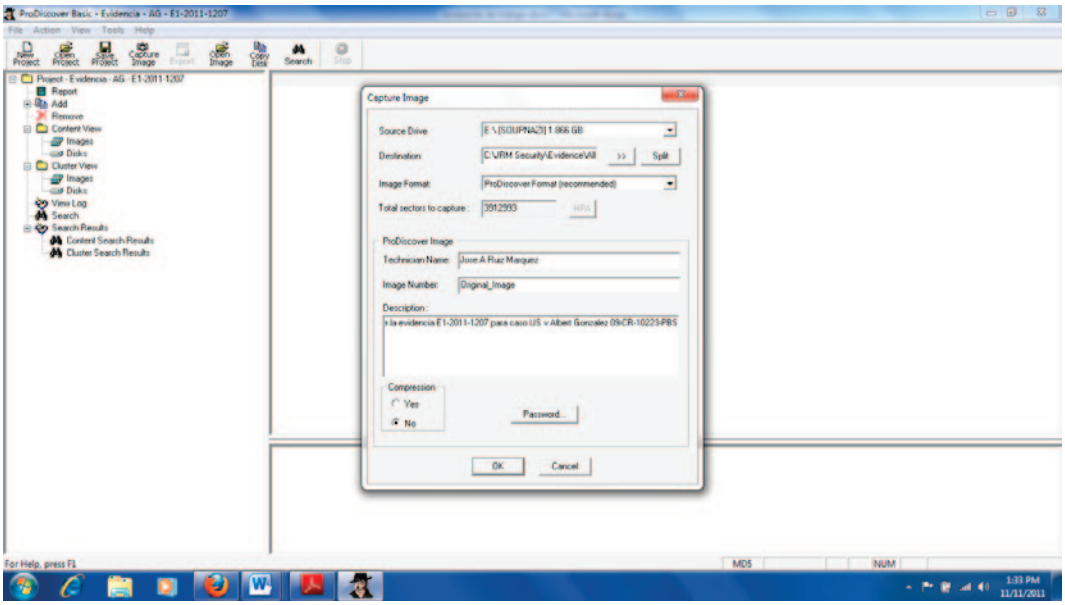


Figure 23: Image capture process. On this slide we are showing part of the bit by bit image creation process. This is where you create 3 copies of the original file, one to save with the original disk, one to use as a master in case the third image gets damaged and the image we will use to work with.

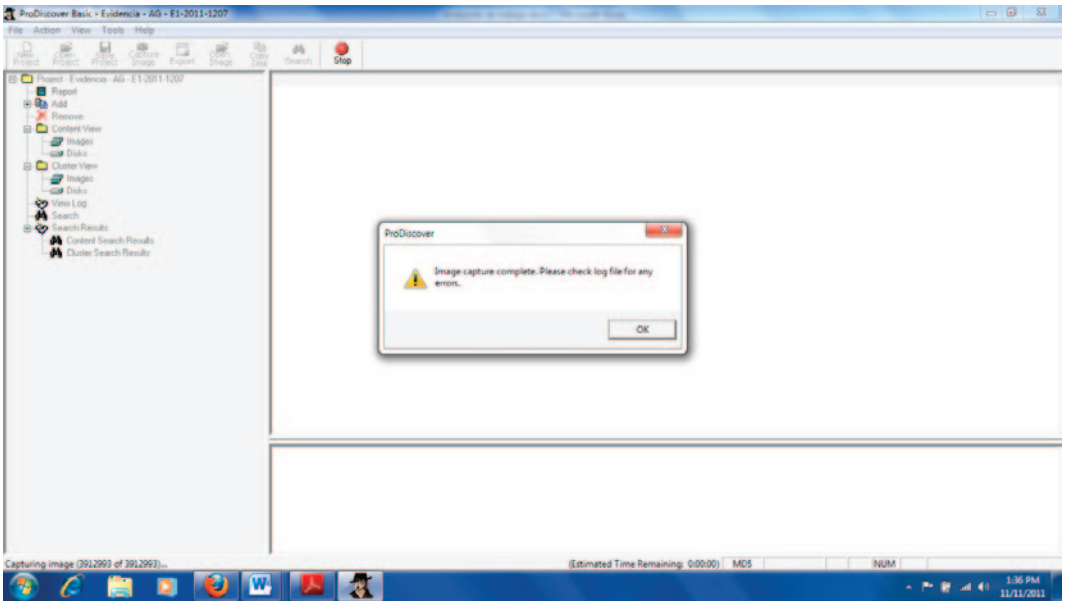


Figure 24: Successful completions of the image capture process. When you finish your logs MUST show zero errors otherwise you will have problems with the evidence and your process could be invalidated in court.

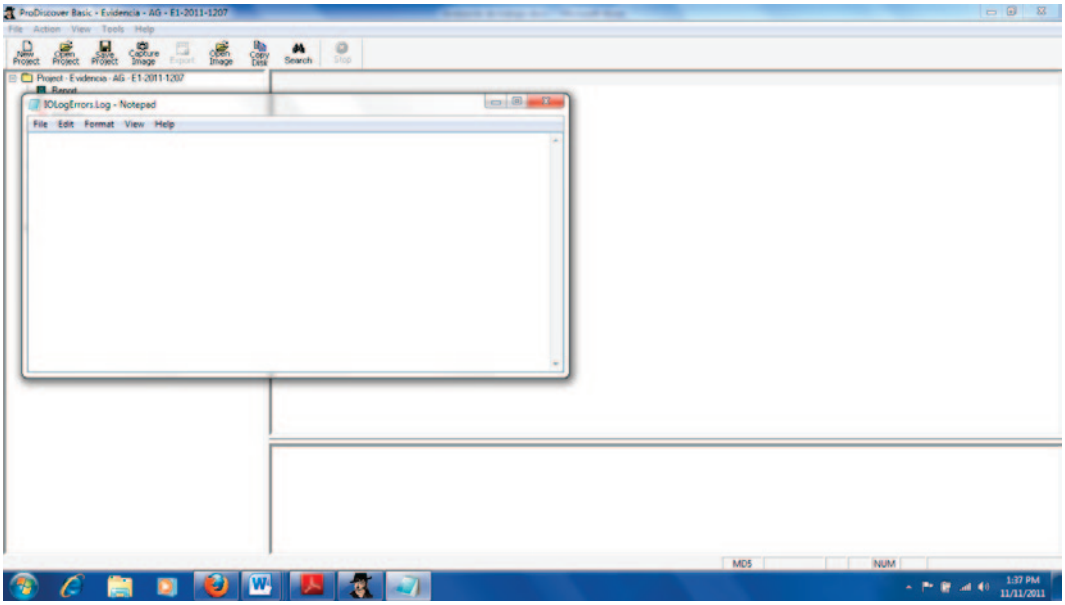


Figure 25: Evidence that the capture was successful and without errors

Procedure 3: Image conversion

- Conversion of the captured image format. Dd to allow analysis of the evidence in other forensic applications.
- Tool: FTK Pro Discover
- Evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07
- Start Date: December 8, 2011 – 9:40 a.m.
- Completion date: December 8, 2011 – 9:52 a.m.
- Description:

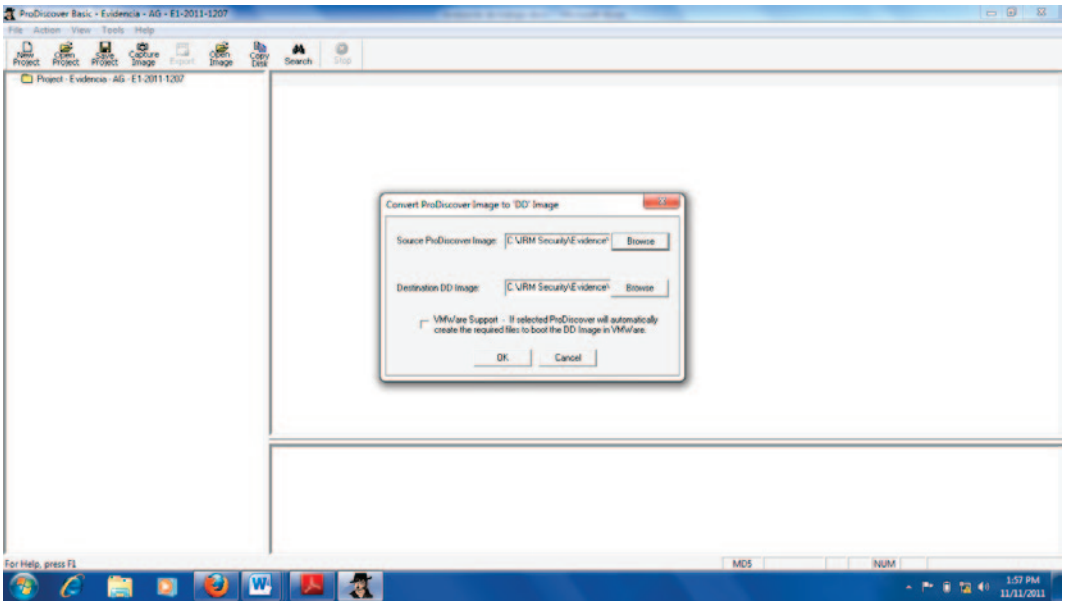


Figure 26: Preparing the conversion environment. Here we will convert our image to a standard format for analysis. One of the most popular formats used is DD, is well accepted in the community and the most important tools Autopsy and EnCASE) support it

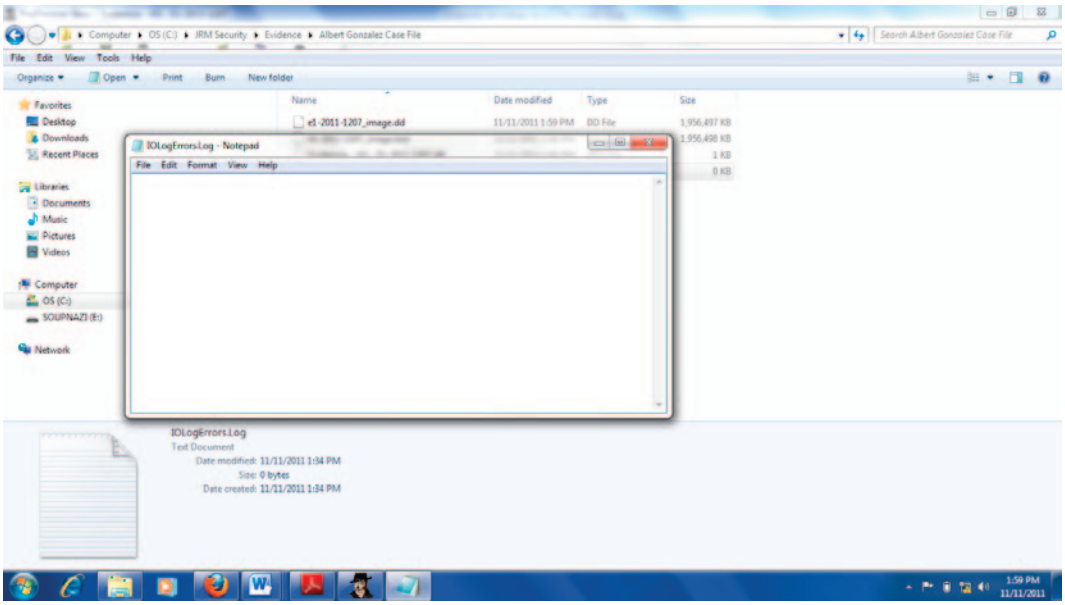


Figure 27: Finished image conversion. Notice the log showing an error-free process to validate the integrity of the conversion.

Procedure 4: the image hash

- At this point the image is processed to obtain a hash to validate the integrity of that image. The hash proves that there were no changes to it by third parties.
- Tool: FTK Imager
- Evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07
- Start Date: December 8, 2011 – 10:04 a.m.
- Completion date: December 8, 2011 – 10:12 a.m.
- Description:

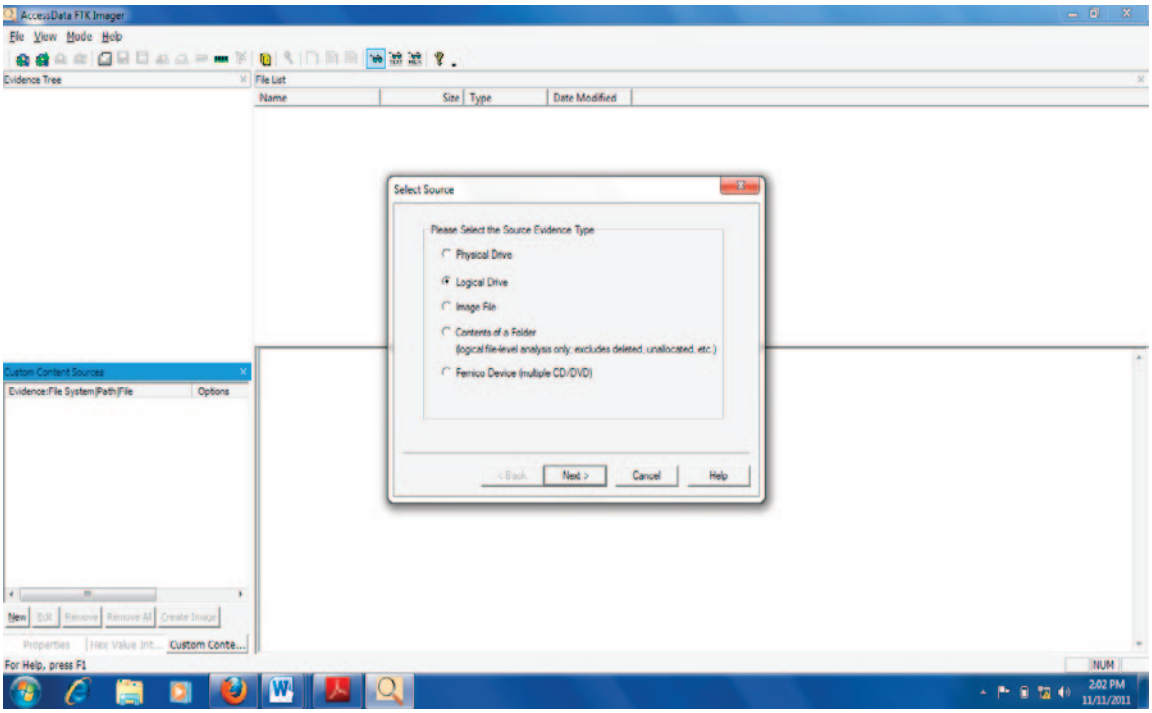


Figure 28: Select the image to be hashed. Now we create the hashes to validate the integrity of the images we will analyze. Failure to do this will get your evidence thrown out of a case

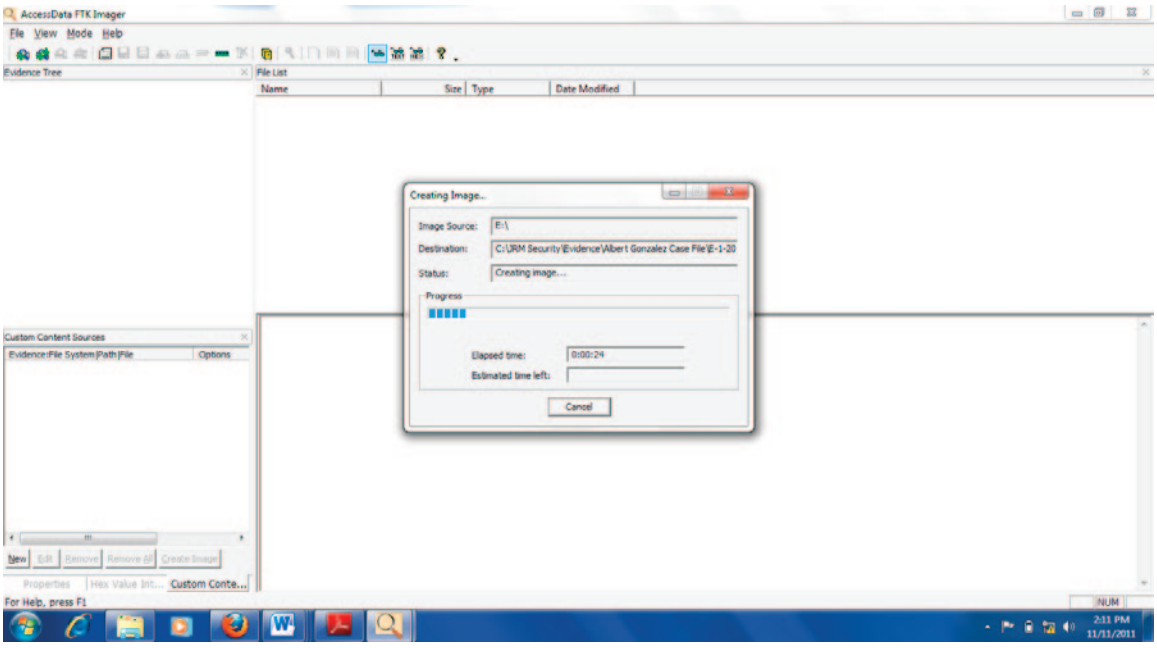


Figure 29: Creation of hash for integrity.

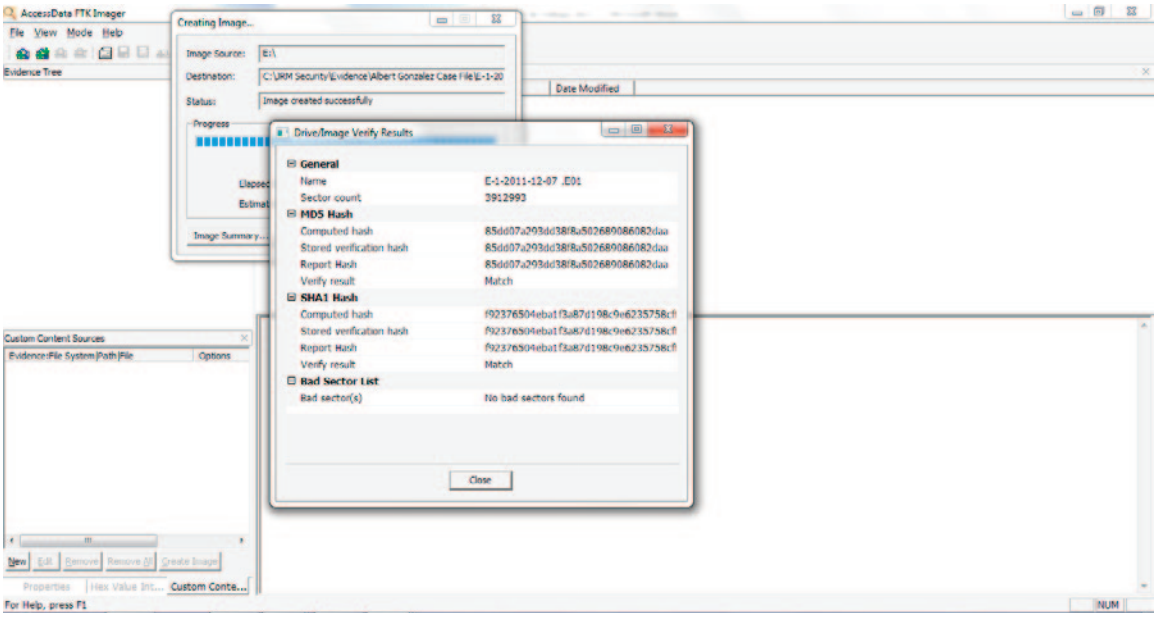


Figure 30: Image hashes to check image integrity. This numbers will need to remain unaltered during all your analysis. It's a good thing to calculate your hashes every time you work on your case. This way you can show that if you worked on your case 3 times every time you got the exact same hashes so your evidence preserved its integrity throughout the whole investigation process.

Procedure 5: image analysis

- At this point the image is processed for possible incriminating evidence and test the hypothesis of federal prosecution. Existing documents were searched and deleted (recovery of these).
- Tool: FTK Imager
- Evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07
- Start Date: December 8, 2011 – 10:34 a.m.
- Completion date: December 8, 2011 – 11:22 a.m.
- Description:

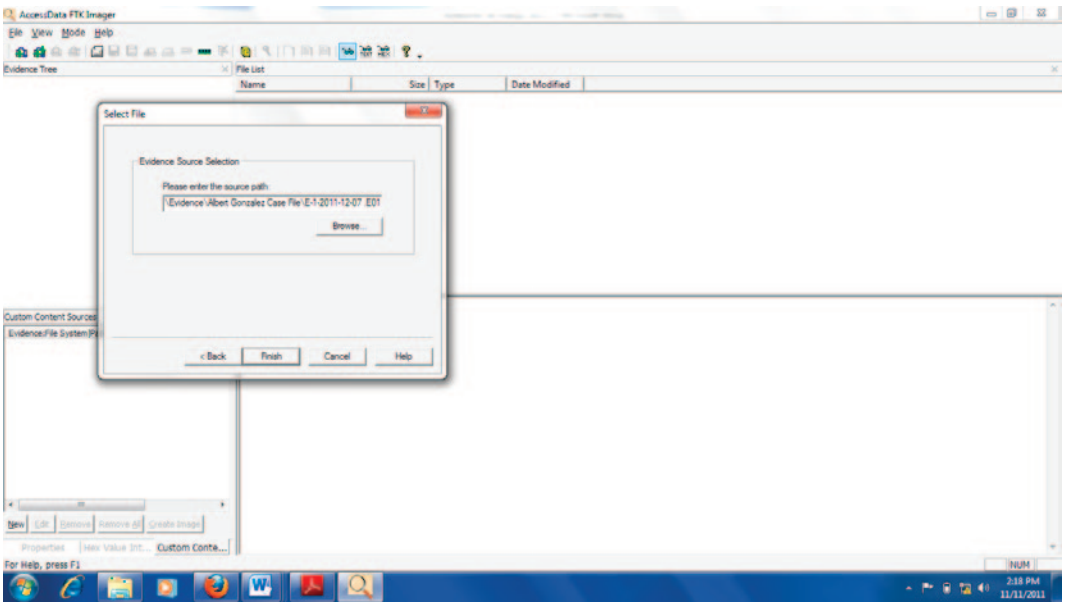


Figure 31 – Image analysis to generate existing files or deleted from the device.

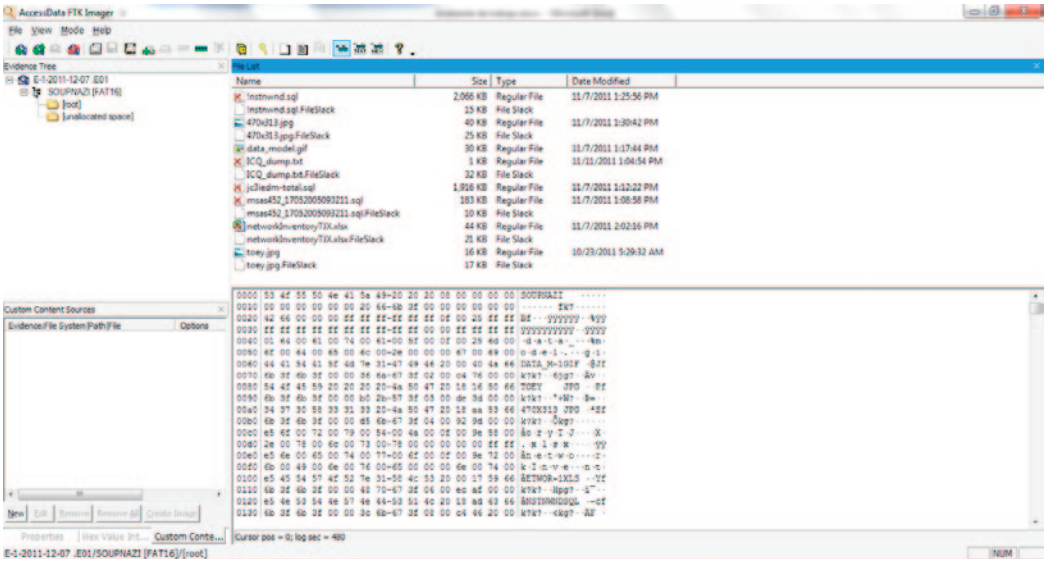


Figure 32: Existing and deleted files from the device.

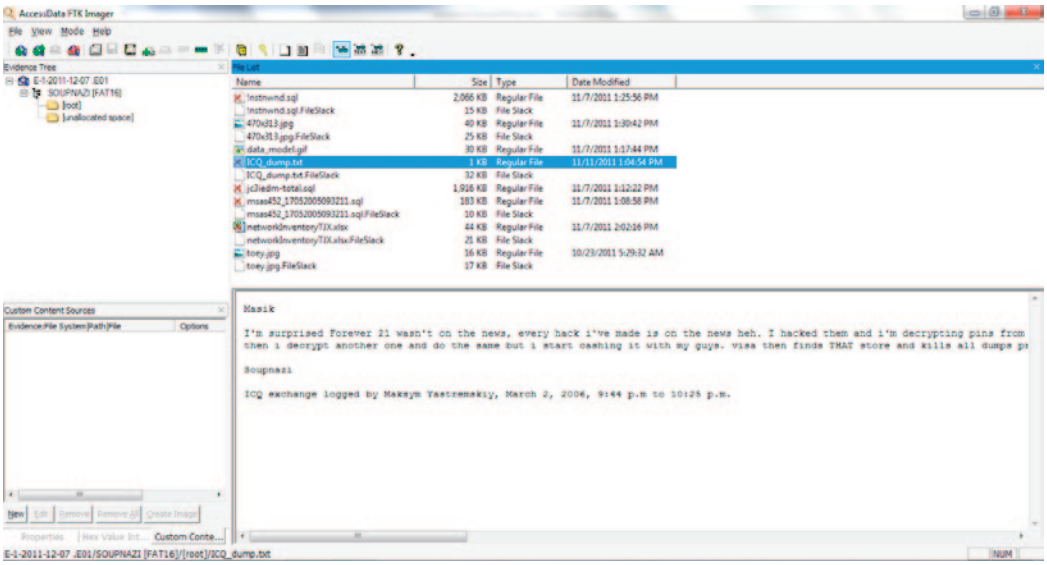


Figure 33: Analysis of deleted document evidencing a note sent via ICQ to Maksym Yastremskiy by Albert Gonzalez under the pseudonym "soupnazi".

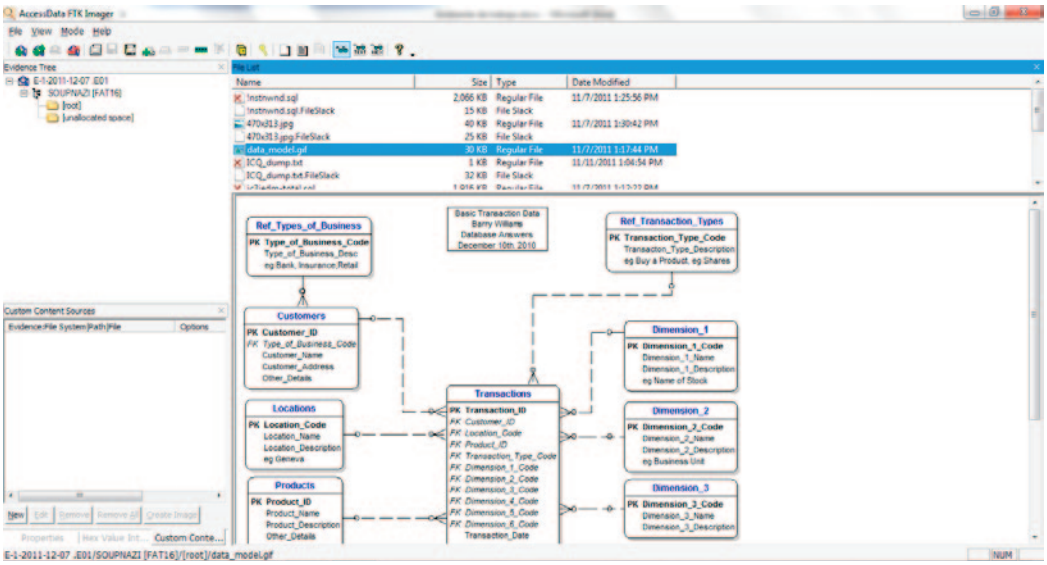


Figure 34: Existing document of a flow chart showing the management system of Marshall's POS.

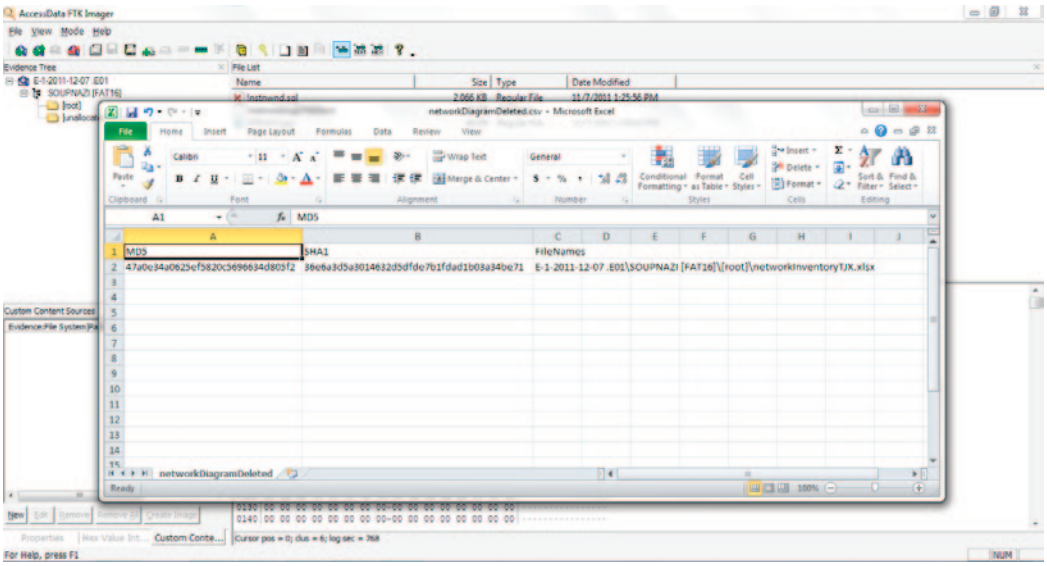


Figure 35: Integrity check hash of a deleted document that was recovered.

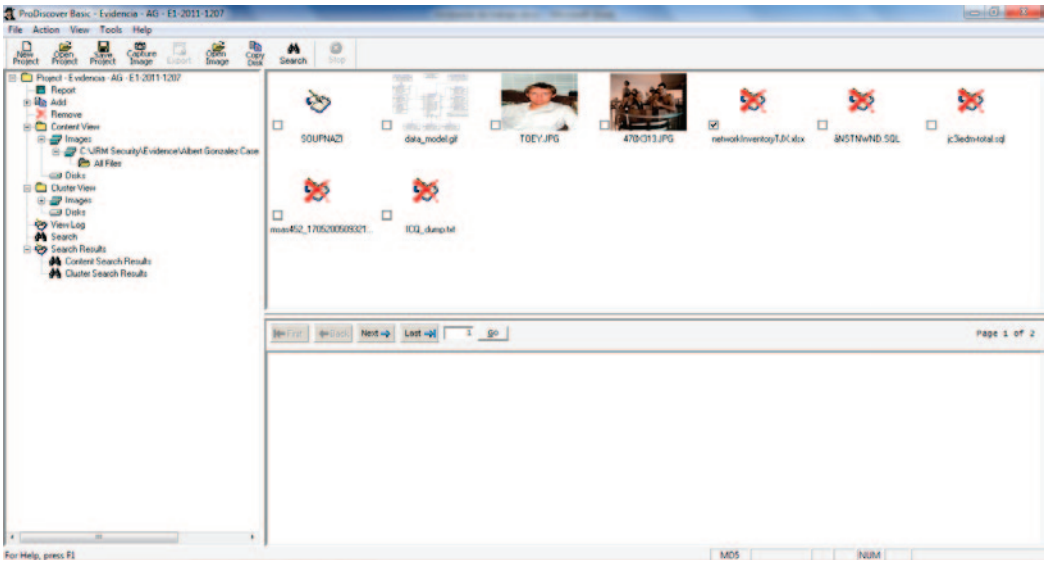


Figure 36: Viewing the image in gallery view we were able to find photos of Gonzalez, Watts and Toey.

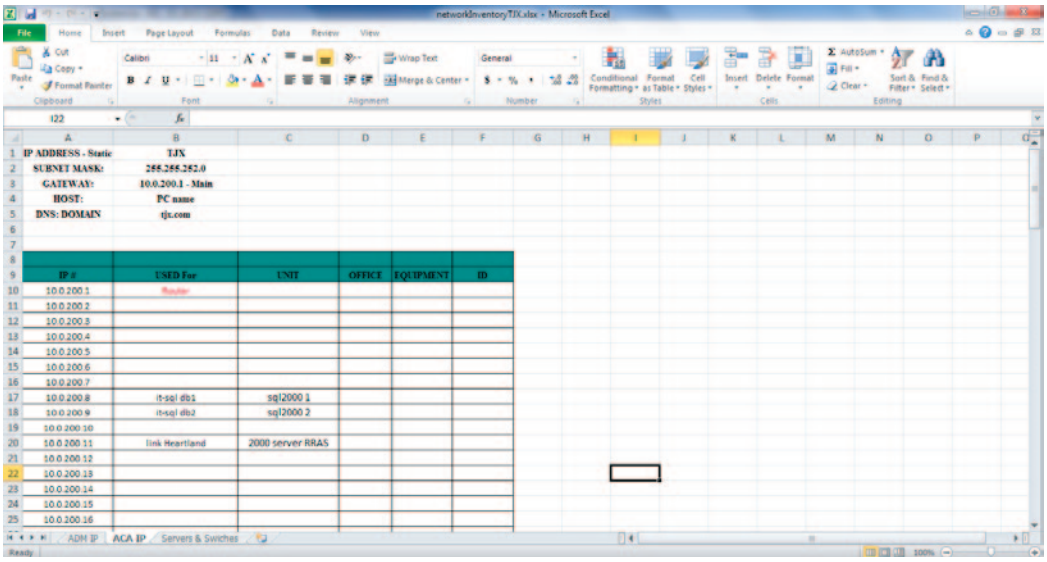


Figure 37: While using Gallery View we were able to find an Excel file with detailed information on the distribution of IP's of TJX and allocation of SQL servers.

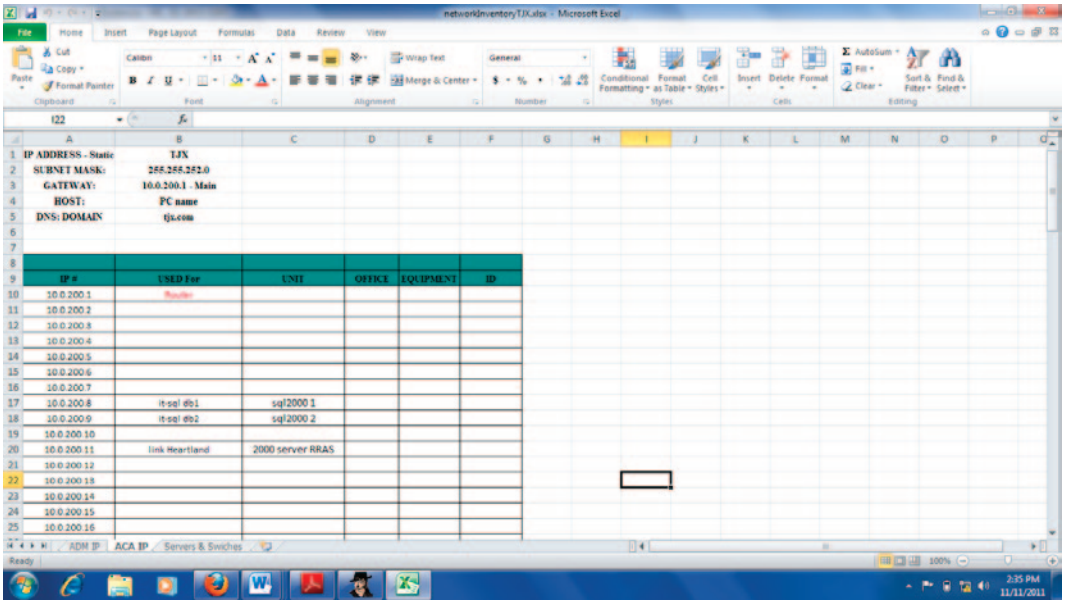


Figure 38: TJX equipment inventory.

Procedure 6: re-validation and reporting

- At this point we will process the evidence with FTK Forensic Toolkit 1.81 to validate the previous results and create an automated report and an Access database with all the evidence properly cataloged and hashed.
- Tool: FTK Forensic Toolkit 1.81
- Evidence # E1-2011-1207 – Assigned to Case # C-1-2011-12-07
- Start Date: December 9, 2011 – 10:00 AM
- Completion date: December 9, 2011 – 2:22 PM
- Description:

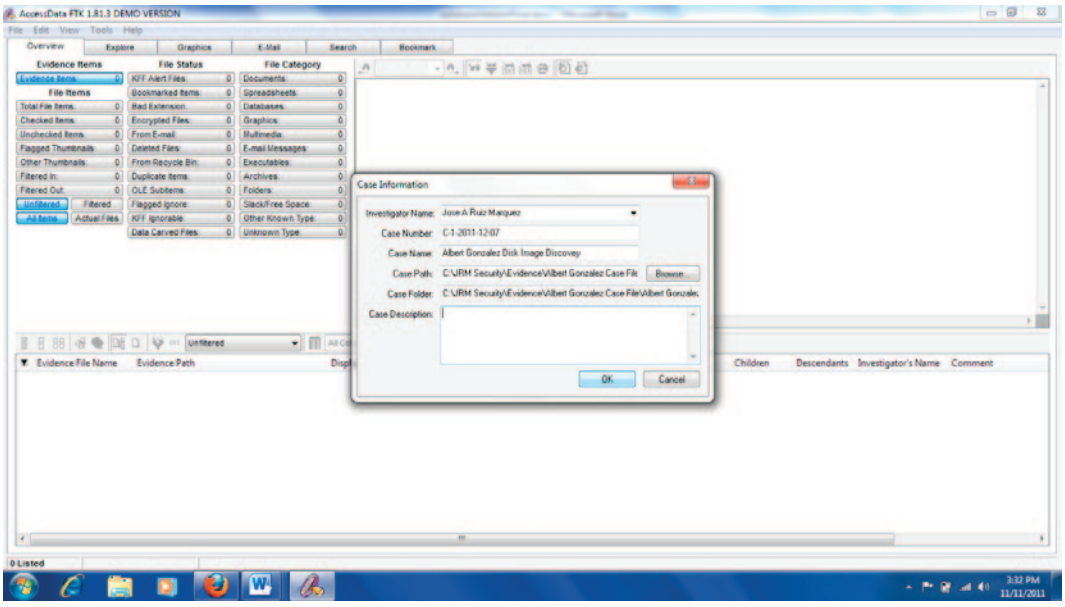


Figure 39: Preparing the case to be re-examined. This is used to re-validate results. Now we are re-doing the process using another tool. If we can get the same results we validate our findings as solid evidence.

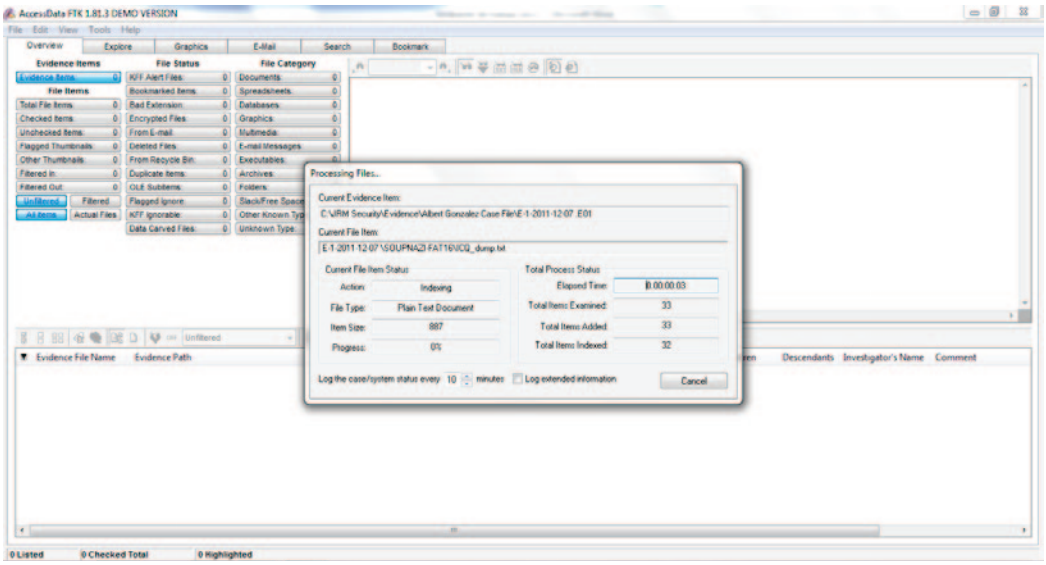


Figure 40: Analyzing the image with the new tool

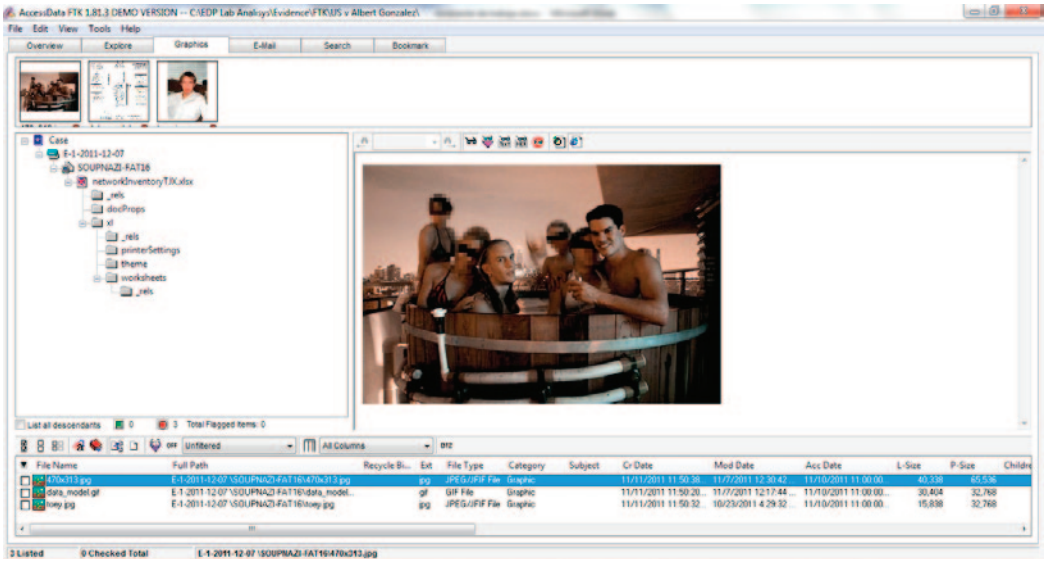


Figure 41: Re-validating the existence of the photos linked to Gonzalez and Toey Watts. (Existing document)

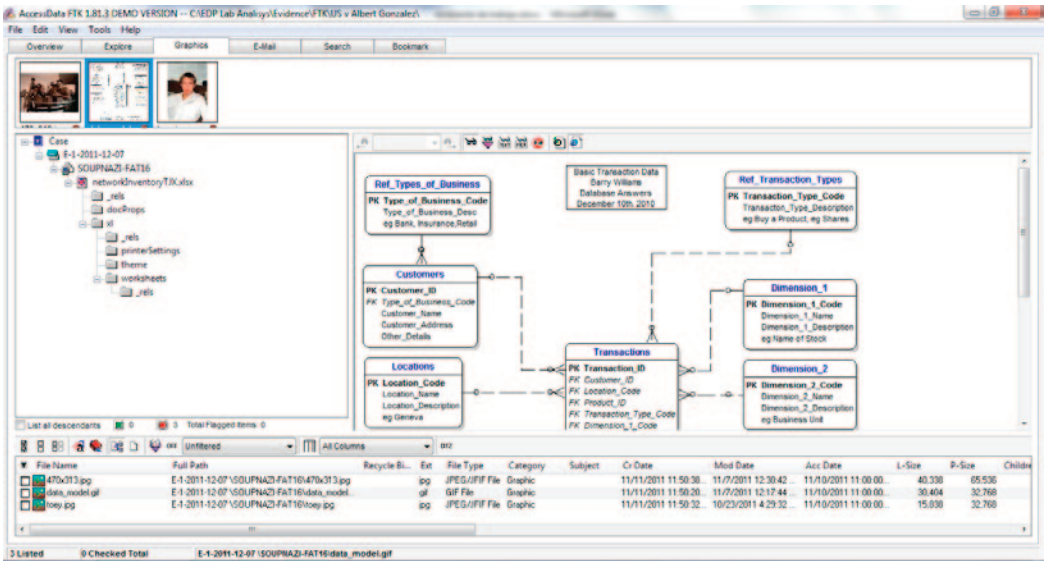


Figure 42: Re-validating the existence of Marshall's transactional management processes flow chart. (Existing document)

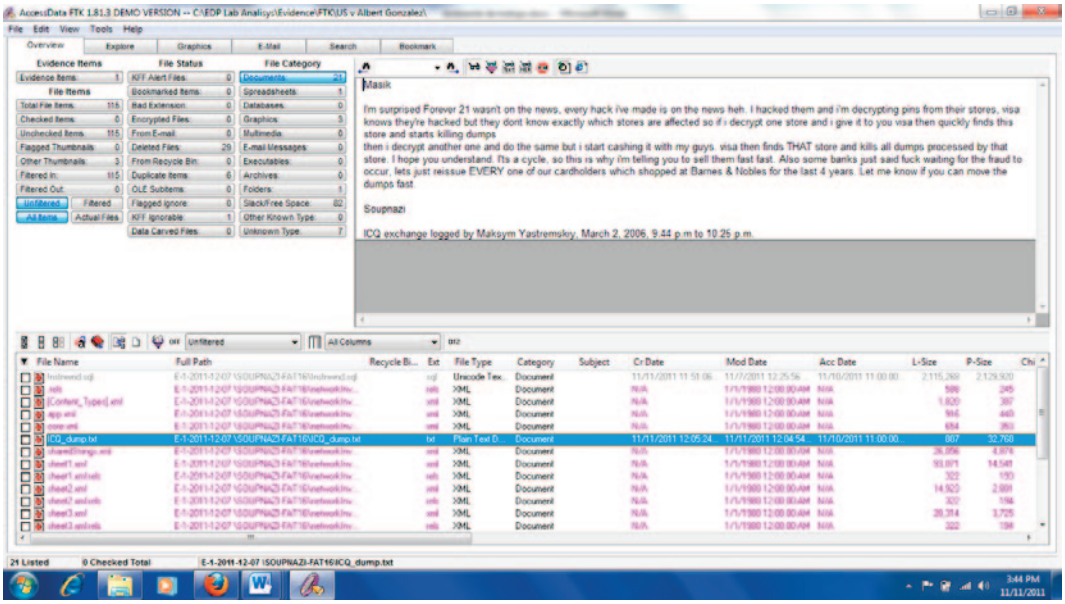


Figure 43: Re-validating the existence of written communication between Maksym Yastremskiy and Albert Gonzalez. (Document deleted and recovered)

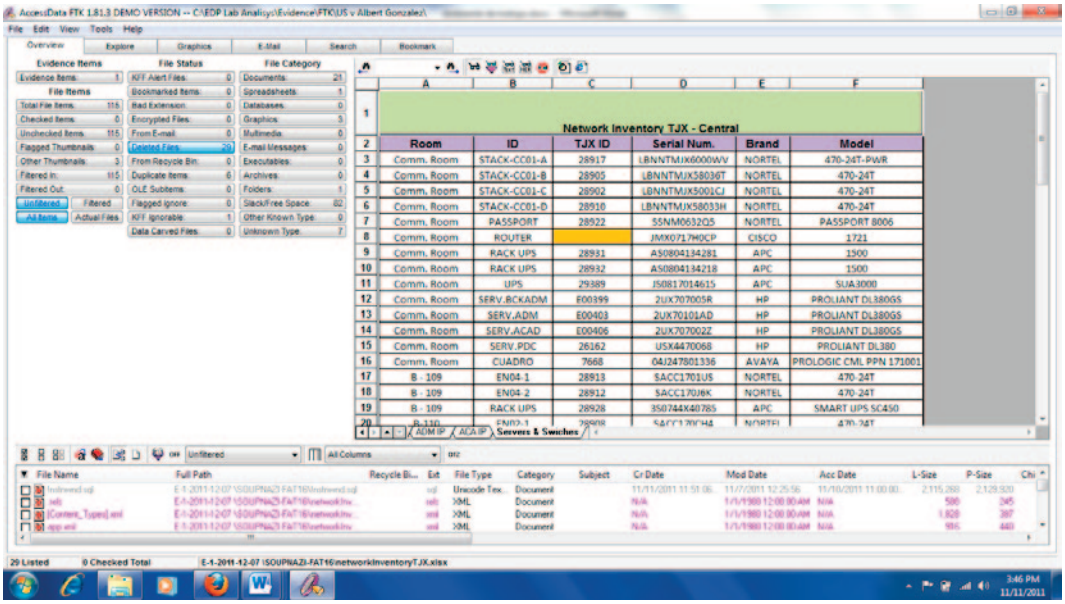


Figure 44: Re-validating the existence of documents with confidential information describing multiple TJX telecommunications equipment. (Document deleted and recovered).

While doing this, don't forget to get your hashes so you can compare with the previous ones to maintain evidence integrity.

REPORT

In addition to the written report a digital report should be generated and included with all the documentation that will be submitted to either internal investigators or the court.

NOTE TO READERS: FTK provides the option of attaching any type of file to your digital report. So make sure that you get all your documents regarding chain of custody, warrant, pictures taken, notes etc., prepare a good report, scan it and convert it to PDF and then attach it to the FTK report. This way you will be able to show EVERYTHING and your work will be more solid in all aspects of the process

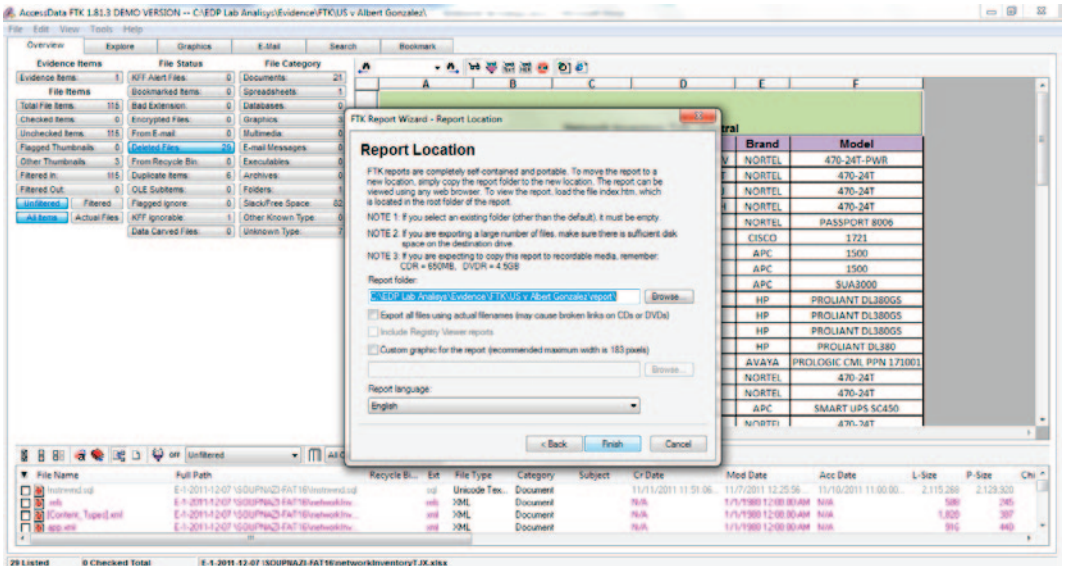


Figure 45: Report Wizard.

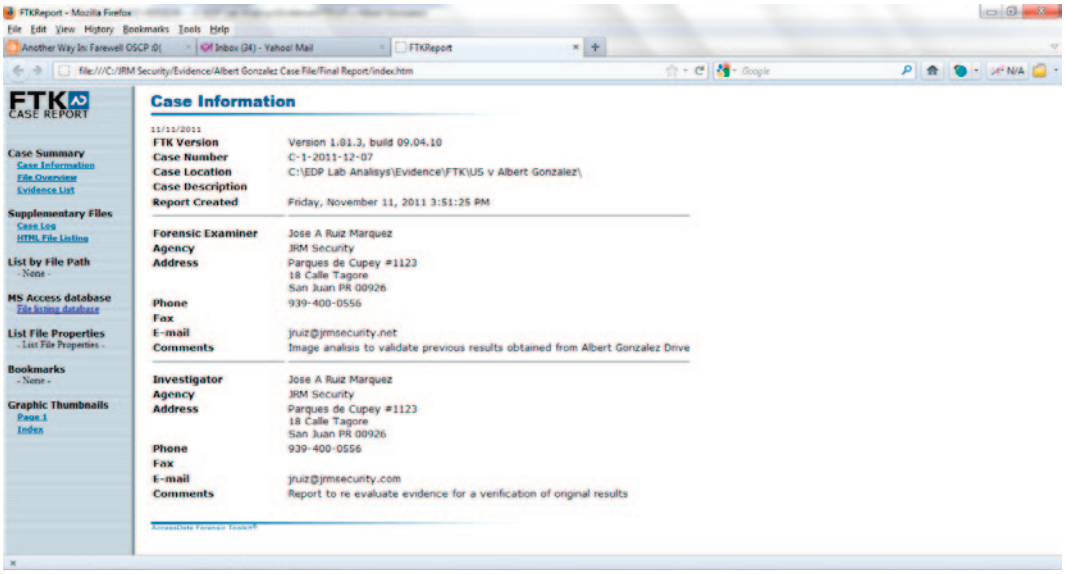


Figure 46: Overview of report in HTML format

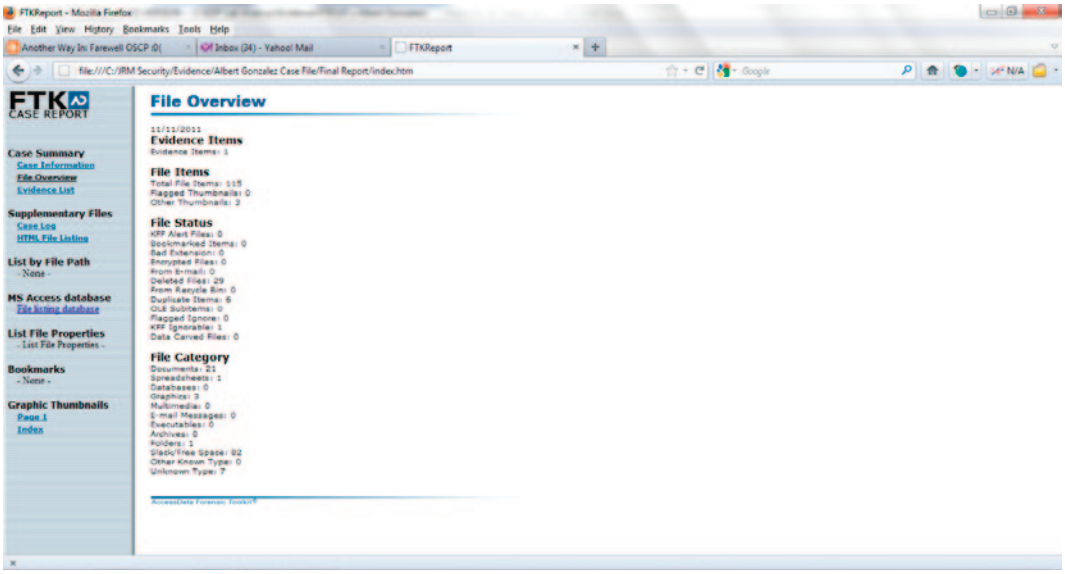


Figure 47: Summary of findings

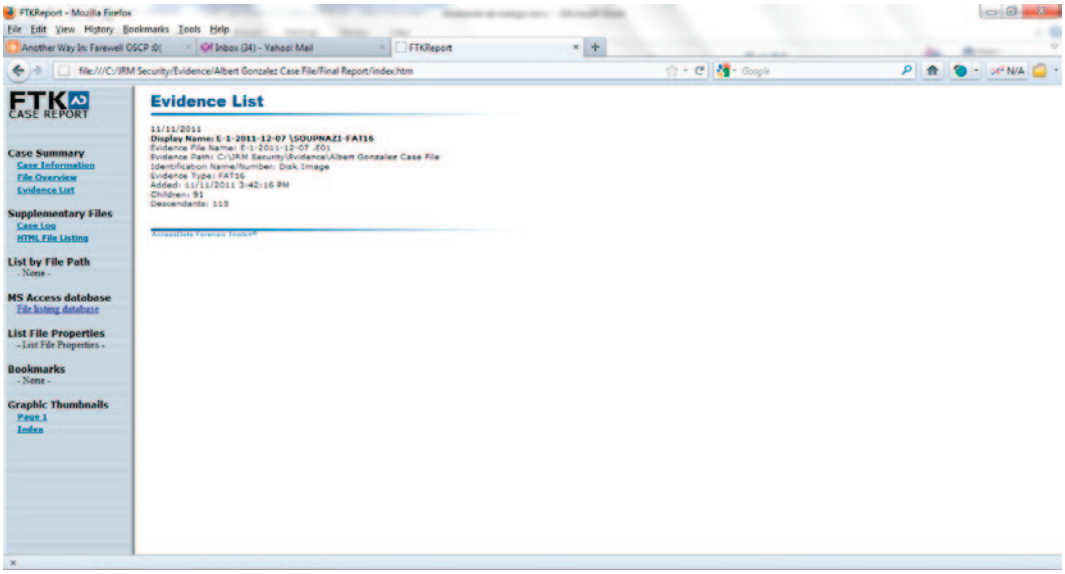


Figure 48: Overview of the evidence.

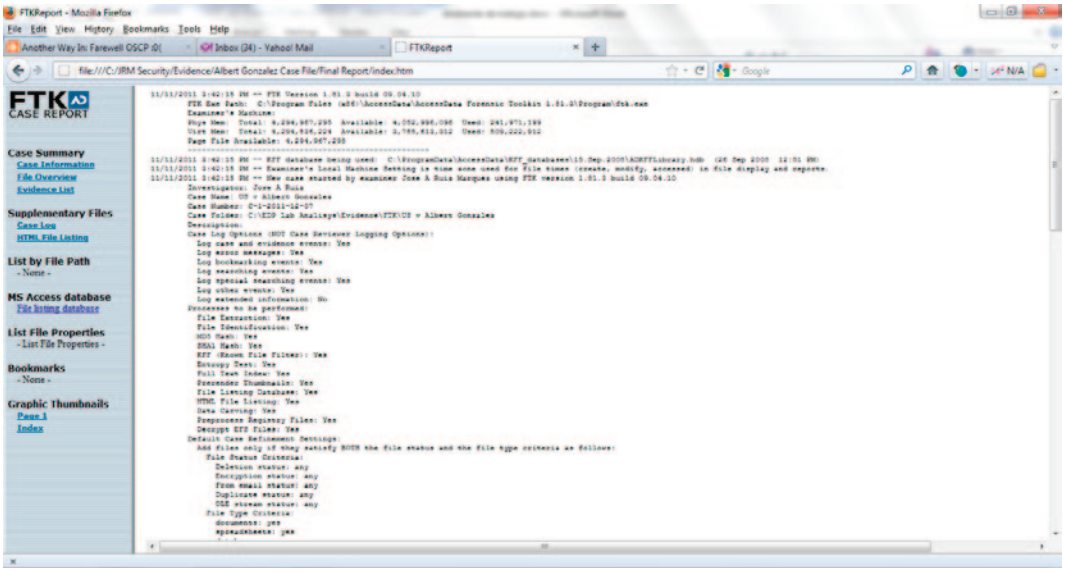


Figure 49: Log of the research process.

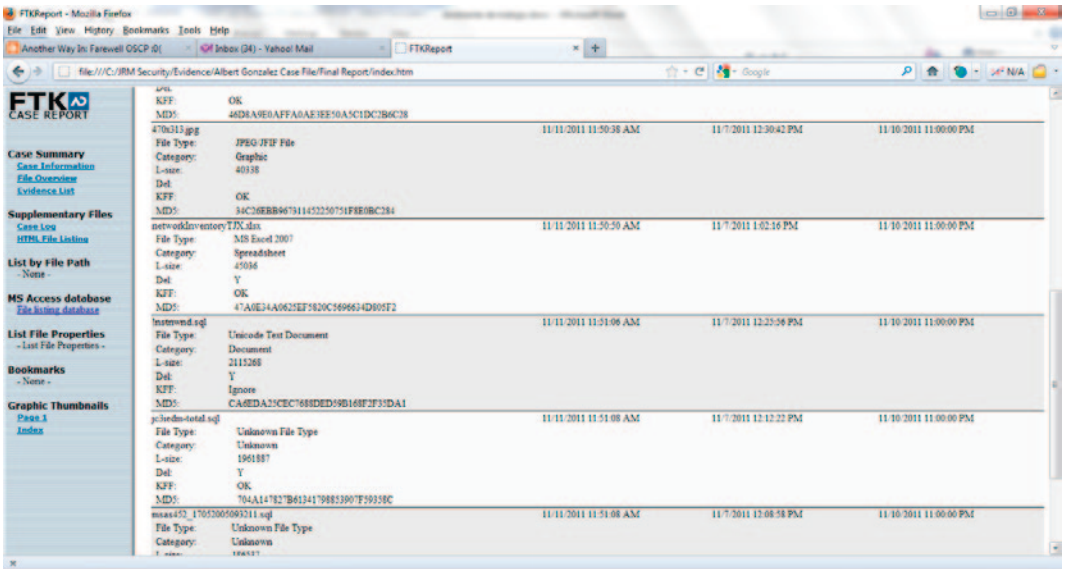


Figure 50: Description of objects found in the device.

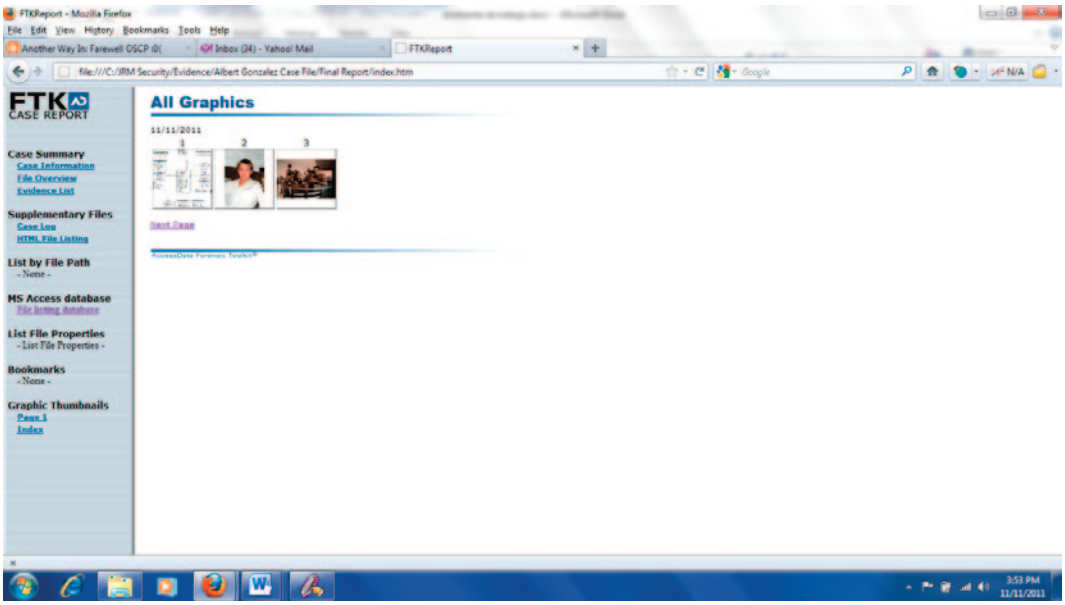


Figure 51: List of Figures and / or pictures

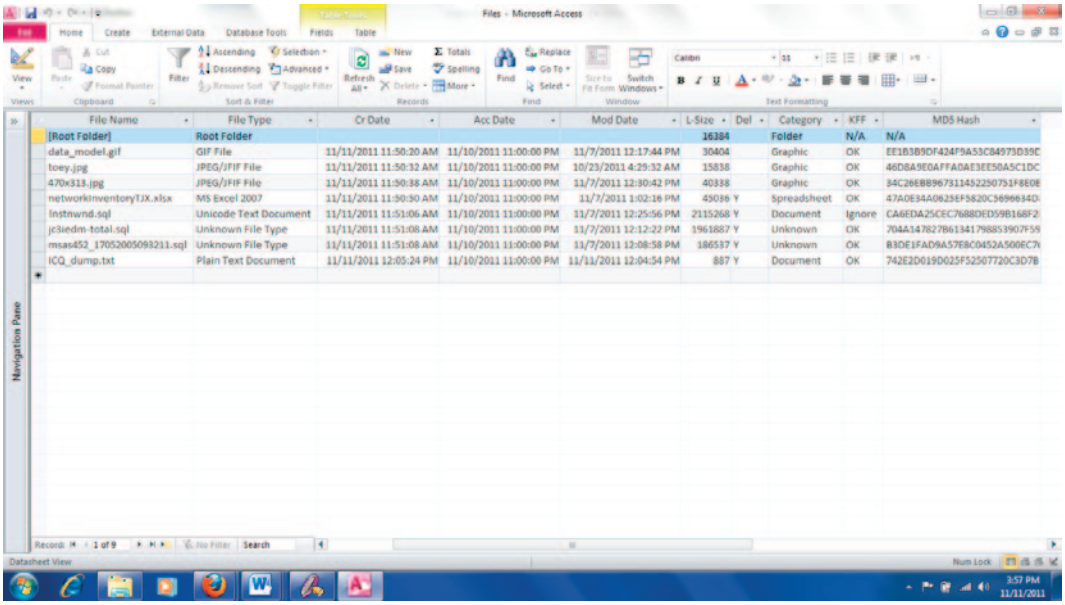


Figure 52: Access Database detailing the evidence, relevant information and the hash of each object found in the device. With this you can validate the original hash obtained on the previous procedure to prove that the evidence was unaltered

REPORT CONCLUSION

After evaluating the evidence found in the device we can conclude that part of the contents thereof clearly indicates that the defendant Albert Gonzalez knew the co-defendants Watts and Toey and also had direct communication through written means with co-defendant Yastrzemski. It was also found that Gonzalez was in possession of confidential information of the companies who were victims. This was concluded because of the existence of equipment lists, distribution lists and inventory lists of servers and their respective functions. These documents clearly identify the company TJX as its source.

It is established that the device was not altered by anyone at the time of delivery. The chain of custody created by JRM Security clearly states that the device to be analyzed was picked up at the FBI evidence room under the supervision of the prosecutor DA Heymann and that this evidence was placed there by the agents who seized it. There is a copy of the chain of custody of such agents that states that the evidence was seized from Gonzalez in compliance with a search warrant issued by Judge Marianne B. Bowler and transported without delay to the FBI evidence room without third party intervention in the process. There is also a copy of the full seize process detailing every step taken to serve the warrant issued by judge Bowler that establishes that the warrant was served following the standard protocols established by law.

That's why we conclude that all the evidence here presented meets all standards of integrity and reliability for use in any legal proceedings. Also we certify that all of the processes used to obtain such evidence meets or exceeds the parameters set by the federal government and industry standard practices digital forensics.

DISCUSSION OF CASE

According to all information obtained in the legal documents of the case: 09-CR-10223-PBS – United States of America vs. Albert Gonzalez, the defendant Albert Gonzalez is accused of multiple counts of credit card fraud victimizing companies such as TJ Maxx, Heartland, and others. Specifically, he is charged with the following offenses:

- Gain illegal access to computer networks for processing debit card transactions for companies such as BJ Club, DSW, OfficeMax, Sports Authority, Forever 21, TJX Companies, Heartland Payment Systems and others.
- Get confidential documents from these companies in order to be able to intercept internal information communication networks and steal transactional data.
- Stealing millions of credit card numbers and personal information of customers.
- Contact hackers in the Soviet Republic to decrypt data stolen from the victims.
- Sold stolen card information for fraudulent use in the United States and Eastern Europe.

Using as a reference for comparison and corroboration of the allegations above the evidence found in the Sans 2 GB USB, Serial No B60QLCYH, confiscated in 6400 SW 32 Street, Miami, Florida on May 7, 2008 we can conclude the following:

- It is confirmed that if the device described was used to store data that links directly to Albert Gonzalez with the crimes committed.
- It is confirmed that Gonzalez was involved in the hack at Forever 21:

  Refer to the following document found on the device – ICQ_dump.txt where Gonzalez makes explicit admission of his role in this hack.
- It is confirmed that Gonzalez was selling stolen cards and information companies concerned individuals in Europe.

  Refer to the following document found on the device – ICQ_dump.txt where Gonzalez makes explicit admission of his role in the process of selling the information to co-defendant Maksym Yastrzemski.
- It is confirmed that Gonzalez had access to confidential information of TJX, and Marshall's.
  - Refer to the following document found on the device – data_model.gif that shows a diagram describing the process of information flow for the Transactional Point of Sales of Marshall's at Heartland Payment. This is privileged information for the exclusive use of TJX as it clearly explains the flow of data from all Marshall's stores to their main TJX database. This is not a public document as it explains internal corporate procedures so it has no reason whatsoever for being inside a device belonging to someone who is not a direct employee of TJX in charge of financial data transport through a network.
  - Refer to the following document found on the device – networkInventory.xlsx that shows a list of telecommunications equipment owned by TJX Central and Miami. In these documents there is information that identifies the IP's and names of the servers that store TJX databases and servers that establishes the connection between these databases and Heartland Payment.
- It is confirmed that Gonzalez was holding SQL dumps containing confidential information database of private companies.
  - Refer to the following document found on the device – jc3iedm-total.sql where it shows a SQL database derived from company Forever 21. This database contains information about credit card numbers and personal information of the owners of such cards. It also displays information on usernames and passwords of the administrators of the database.

PART III: CONCLUSION

As you've seen throughout this article forensics is more than just using FTK or Autopsy. It's about knowing all legal procedures regarding seizure of evidence, the proper analysis process including minute documentation of everything done in every step of the investigation. You also must know about the various aspects of both cyber and evidence law. When you are dealing with internal auditors, lawyers, judges etc. you must always assume that they do not know how this forensic processes are executed but they are well versed on policies and standards, evidence management, admissibility procedures etc.

They might not be able to question your results, but they sure will try with everything they have available to get a hole in your process that will allow them to get your evidence rendered inadmissible. If that happens then you have nothing to support your findings and that might end the case prematurely. It doesn't matter if you are working as an expert for the state or the accused, both the DA and the accused attorney will do everything in their power to decimate your report so they can get it out of the way.

So make sure you develop your report writing skills as well as your knowledge of the law in your country. Take some courses about legal history, penal codes, evidence procedures, report writing (with emphasis on legal reports), etc. Remember, even if you are a Homeland Security Agent you can get whipped if someone steps in and find a few holes in your process.

PART IV: BIBLIOGRAPHY

- Association of Fraud Examiners (2012) – Fraud Examiners Manual – (2012 Edition) ACFE/Wiley – *http://www.acfe.com*
- Nelson, B., Phillips, A., & Steuart, C – (2009) – Guide to computer forensics and investigations. (4ed.) – Course Technology – ISBN: 1435498836
- Blitz, Andrew – (2010) – Lab manual to Guide to computer forensics and investigations. (4ed.) – Course Technology – ISBN: 1435498852
- Altheide, Cory – (2011) – Digital Forensics with Open Source Tools (1ed.) – Syngress – ISBN: 1597495867
- Newman, Robert C. – (2007) – Computer Forensics: Evidence Collection and Management (1ed) – Auerbach Publications – ISBN: 0849305616

PART V: WEB RESOURCES

- *http://www.nist.gov*
- *http://csrc.nist.gov/*
- *http://csrc.nist.gov/publications/PubsTC.html#Forensics*
- *http://www.cftt.nist.gov/*
- *http://www.forensicfocus.com/*
- *http://www.dfinews.com/*
- *http://www.fbi.gov/about-us/lab*

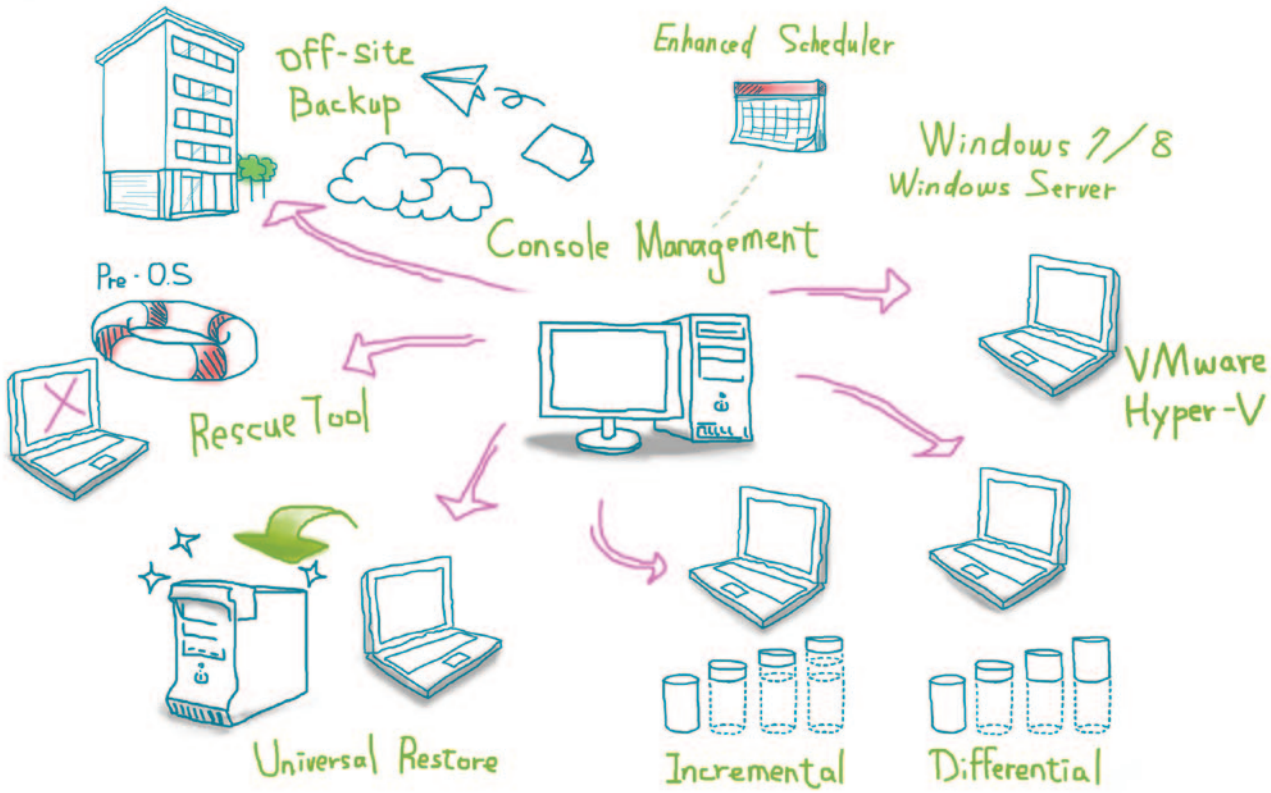
About the Author

Jose Ruiz has over 12 years of experience in the computer field. His formal education includes a Master's Degree in Information Security and Computer Fraud Investigation, and multiple certifications, including: MCT (Microsoft Certified Trainer), MCSA 2000/2003/2008, A +, Network +, Security + and Offensive Security Wireless Professional (OSWP). He is also a member of ACFE (Association of Certified Fraud Examiners). Jose works as an independent consultant specializing in the areas of physical and logical network security with tasks ranging from policy audit, vulnerability assessment, mitigation plan implementation, business continuity digital forensics and others. He also works investigating cases ranging from corporate misuse of resources, phishing, pornography, false document production and wireless intrusion and has served as an expert witness in both administrative and criminal cases dealing with forensic analysis and document forgery. Jose is also an IT instructor and Microsoft Certified Trainer teaching courses for both Microsoft and CompTIA certifications and a college professor at undergraduate and graduate level teaching forensics, networking, wireless and ethical hacking courses at both EDP University and Interamerican University in Puerto Rico. He is also an active contributor to the ISECOM Hacker's High School project and Hakin9 magazine.

FARSTONE®

Total Backup Recovery®

We make it easy for you.



FarStone 2013 Distributor / Reseller Partner Recruitment

www.farstone.com

inquiry@farstone.com

Recommended

A useful freeware to remove obsolete, temporary, invalid, and redundant registry items for Windows System.

Wise Registry Cleaner adopts an advanced algorithm and takes only a few seconds to scan & clean the entire Windows Registry. Automatic and manual backup supported.

WiseCleaner

Wise Register Cleaner 7

- ✔ Clean registry
- ✔ Defrag registry
- ✔ Tune up system
- ✔ Fast, safe & effective

★★★★★

Recommended as "Outstanding" on CNET

Official Website for More Information:
www.wisecleaner.com/wiseregistrycleanerfree.html

Compatible with Windows 7

Windows 8 Compatible

Support system:
Windows XP, Vista, Win7/8
(both 32-bit and 64-bit)