Cell Phone Investigations™

Almost every criminal investigation involves a cell phone. The evidence needed to arrest and convict is contained on the device itself, the records of calls kept by the cell phone company, and in the cell towers covering the crime scene. The course covers the search and seizure basics specific to mobile devices, determining what information is available from the cell phone companies and how to obtain it, how to recover digital evidence and intelligence from the handset using free software tools, and how to avoid legal landmines.

Aaron Edens
Police Technical

Table of Contents

Welcome!

Good morning and thank you for attending this **POLICE TECHNICAL** course.

My name is Thomas M. Manson, founder of **POLICE TECHNICAL**, the company which is presenting this technical training course. Today you will be an attendee in a course which **POLICE TECHNICAL** and your instructor have been preparing for many months, and, truthfully, have been preparing for many years.

POLICE TECHNICAL has worked for several months to make your class today a reality. Each year we receive training requests from agencies across the country, and every successful class is the culmination of 4-6 months of coordination, marketing, and logistics. A May or June class likely began with a training request from the previous year.

Your instructor has also worked for many years preparing to teach this class. In addition to several years of law enforcement experience, many dedicated to the subject of your class; he or she has completed a lengthy process with **POLICE TECHNICAL** to become one of our instructors. This process involves a documented hiring process, a thorough background investigation, a detailed instructor and materials development process, and a continuing program of mentorship.

POLICE TECHNICAL and our instructors work hard to provide superior quality training for law enforcement in computer applications, online investigations, and forensics. I can tell you without hesitation, "*Your course today will be one of the best you have ever had in this subject, and your instructor is one of the best in the field of law enforcement*".

I know you'll find this class valuable, but if ever want to talk with me about your experience, or if you would like to talk about bringing a **POLICE TECHNICAL** training course to your agency or department I would happily speak with you.

Enjoy your class, and thank you again for attending this **POLICE TECHNICAL** course.

Respectfully,

Thomas M. Manson
POLICE TECHNICAL
812-232-4200 | www.policetechnical.com **|** info@policetechnical.com

Our History

In 2004 POLICE TECHNICAL LLC was establish to further professionalize the law enforcement training process created by Thomas M. Manson.

In 2007 POLICE TECHNICAL was recognized as a Sole Source Provider by federal law enforcement agencies, offering a level of training unavailable from any other source. POLICE TECHNICAL incorporated in 2009 to provide a suitable structure to expand business operations.

In 2010, POLICE TECHNICAL scheduled more than 50 national training courses.

In 2012, six new classes were developed and being taught by six additional instructors.

Goals of the Course

Day One

- The legal foundation for proper search and seizure of phones and phone company records
- Writing effective search warrants, court orders, and subpoenas
- How to investigate a phone number from beginning to end, using free and open source tools
- Who to contact when cellular companies fail to produce the records in a timely
- How to obtain “blocked” caller identification phone numbers
- Dealing with suspects who use calling cards and what to do when your suspect “drops” their phone number
- International call records-what to do when your suspect calls overseas
- Disposable or “burner” phones-why they aren’t as bad as most people think and how to investigate them

Day Two

- How criminals use free and low cost tools to conceal evidence and remotely delete the contents of their phones and how to prevent it from happening during your investigation
- Cell phone handsets: Obtaining physical evidence from the device, what types of digital evidence are available, where to find and how to recover deleted information
- Dealing with locked phones. Security code bypass techniques and how to still recover evidence when they don’t work
- Where to find and how to use free and low cost tools when the expensive forensic devices don’t work,
- How to enhance low quality cell phone videos
- How to properly utilize ‘hidden’ EXIF data found in almost every cell phone photograph, and determining location if the GPS was turned off.
- How to properly request and use cell tower data in your investigations to locate suspects, fugitives, and missing persons.

Legal Authority to Search Cell Phones

Search warrant

4th Amendment waiver as a condition of release (probation/parole)

Consent

Parental consent

Plain view

Border searches

Schools

Prisons/correctional institutions

Abandoned property

Search incident to arrest

Legal Citations

U.S. v. *Robinson*, the U.S. Supreme Court recognized the authority to search a person incident to arrest, including seizing evidence unrelated to the arrest to prevent its destruction or concealment.

"[a] full search of the person, his effects, and the area within his immediate reach at the time of a lawful custodial arrest may be conducted without regard to any exigency or the seriousness of the offense, and regardless of any probability that the search will yield a weapon or evidence of the crime for which the person is arrested."

U.S. v. Robinson, 414 U.S. 218 (1973).

United States v. Diaz-Lizaraza, 981 F.2d 1216, 1223 (11th Cir. 1993).

Agents reasonably activated defendant's pager to confirm its number.

United States v. Chan, 830 F. Supp. 531, 535-536 (N.D. Cal. 1993).

Warrantless search of pager memory comparable to a search of container contents; search was not so remote in time to invalidate it as a search incident to arrest.

United States v. Reyes, 922 F. Supp. 818, 834 (S.D.N.Y. 1996).

Warrantless searches of the stored memory of two pagers justified (i) as incident to arrest and (ii) by general consent.

U.S. v. Ortiz, 84 F.3d 977 (7th Cir. 1996).

In *U.S.* v. *Ortiz*, a pager was searched incident to arrest, and the telephone numbers were admissible because of its "finite memory," meaning incoming pages could potentially destroy existing telephone numbers with evidentiary value.

United States v. Thomas, 114 F.3d 403, 404 n.2 (3d Cir. 1997).

Noting that the retrieval of a phone number from a pager found on defendant was a valid search incident to arrest.

United States v. Parada, 289 F. Supp. 2d 1291, 1304 (D. Kan. 2003).

Phone seized incident to valid arrest; exigent circumstances justified accessing cell phone's call records because continuing incoming calls would overwrite memory and destroy evidence.

Overruled search of phone book

United States v. Morales-Ortiz, 376 F. Supp. 2d 1131 (D.N.M. 2004).

Otherwise unlawful search of cell phone's memory for names and numbers was justified under the inevitable discovery doctrine.

United States v. Finley, 477 F.3d 250, 259-260 (5th Cir. 2007).

The search of the stored text messages was permissible as incident to a valid arrest.

United States v. Deans, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008).

Agreeing with the Fifth Circuit that, "if a cell phone is lawfully seized, officers may also search any data electronically stored in the device."

*United States v. Dennis, 2007 WL 3400500, at *7 (E.D. Ky. Nov. 13, 2007).*

Search of a cell phone incident to valid arrest no different from the search of any other type of evidence seized incident to arrest.

United States v. Lottie, 2008 WL 150046, (N.D. Ind. Jan. 14, 2008).

Warrantless search of a cell phone justified by exigent circumstances.

*United States v. Valdez, 2008 WL 360548, at *3 (E.D. Wis. Feb. 8, 2008).*

Search of defendant's phone was contemporaneous with his arrest and the officer was reasonably concerned that if he delayed, the information on the phone would be lost.

*United States v. Wall, 2008 WL 5381412, at *3-4 (S.D. Fla. Dec. 22, 2008).*

Declining to follow Finley; exigent circumstances might justify a warrantless search of a cell phone; but declining to allow a search of arrestee's cell phone incident to arrest; likening information stored in cell phone to a sealed letter.

*United States v. Park, 2007 WL 1521573, at *9 (N.D. Cal. May 23, 2007).*

Based on "the quantity and quality of information that can be stored" a cell phone "should not be characterized as an element of an individual's clothing or person [subject to search incident to arrest], but rather as a 'possession within an arrestee's immediate control that has fourth amendment protection at the station house.'"

United States v. Quintana, 594 F. Supp. 2d 1291, 1299 (M.D. Fla. Jan 20, 2009).

Officers may be justified in searching the contents of a cell phone for evidence related to the crime of arrest, but "[w]hether a cell phone may be searched incident to an arrest to prevent the destruction or concealment of evidence of another crime is a different issue."

United States V. Murphy 552 F.3d 405 (4th Cir. January 15, 2009):

Murphy argues that a cell phone may be searched without a warrant can be determined only upon the officers ascertaining the cell phone's storage capacity. A device with a small storage capacity may be searched without a warrant due to the volatile nature of the information stored, but that a search of a cell phone with a larger storage capacity would require a warrant to be issued.

Exigent Circumstances

Largely unused as an authority to search

Allows for search of phone and obtaining records

There is an urgency to collect and retain data stored on a cellular phone because remote deleting is a reality or the records sought are imperative

Several 'prongs' that need to be addressed:

Degree of urgency (amount of time necessary to obtain a warrant)

Ready destructibility of evidence (information the possessors of the evidence know police are investigating them and/or know that efforts to dispose of evidence are characteristic behavior)

Knowledge of volatility of evidence

Gravity of offense

Strength or weakness of the facts establishing PC

Proof by testimony (prior knowledge based on training and experience)

Sample Report Language

I searched **suspect's** phone incident to arrest in order to preserve evidence that may be located within. I know from my training and experience that cell phone call logs, text messages, phone contacts, photographs, and other information stored on such devices can be lost, altered, or destroyed through several means. I am aware of a process called "flooding" in which a friend or accomplice of the arrestee may call and/or text the phone numerous times after he or she is arrested in order to purge the old call logs and text messages, thereby destroying possible incriminating evidence or evidence of conspiracy. I also know there are cell phone companies, third party software programs, and cell phone models on the market which offer the service of and have the ability to remotely delete information stored on the phone. In these cases the suspect and/or an accomplice can access the phone remotely and permanently delete cell phone call logs, text messages, phone contacts, photographs, and other information stored on the phone. This can include information stored on external storage media inserted into the phone.

I know from my training and experience that there are thousands of cell phone models currently in use in the world, with an average of four new models released each month. It would be impossible for me to know by simply looking at the cell phone whether or not this model had remote delete capability. There is no way to tell from looking at the exterior of the phone and be able to determine what sort of security or remote delete software is installed on the phone. I would not be able to tell by looking at a phone and be able to determine whether the cellular service provider offers a remote deleting service and whether the suspect subscribed to such a service.

Also, I lacked the appropriate equipment and expertise necessary to preserve to phone for subsequent forensic examination. I am aware there are methods of preventing a cellular phone from communicating with the cellular service provider which would inhibit the ability of co-conspirators or prohibit the activation of remote deletion features. These methods include field expedient means such as wrapping the phone in metal foil or securing in a metal container. I know from prior training and experience such methods are inherently unreliable and their effectiveness can depend on several factors including the amount of charge retained in the battery, the type of cellular device, and the proximity of the device to a cell tower. I know there are commercial products available for laboratory forensic use which are either too cumbersome or too expensive to be used in the field. Additionally, the effectiveness of the listed shielding materials have not been evaluated in the laboratory setting and there is no documentation to establish their reliability. I am aware of cellular signal disruption devices, also known as cell phone 'jammers' which are available commercially. I am aware the use of those devices is prohibited by the Federal Communications Commission and that there is no exception to their regulations for state or local law enforcement officers.

For the reasons stated above, I searched **suspect's** cell phone incident to arrest in order to preserve any possible evidence from being intentionally deleted or otherwise deleted or destroyed.

Title 18 USC § 2703(b)-(d)

Generally the authority for obtaining cell phone records under federal law is Title 18 USC **§** 2703(b)-(d)

Codifies the principals outlines by the US Supreme Court in Smith v. Maryland

Created as a component of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

> (d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

Relevant- bearing upon or connected with the matter in hand; pertinent.

Material- a group of ideas, facts, data, etc., that may provide the basis for or be incorporated into some integrated work.

Searching for Phone Numbers

Instead of just checking a phone number in Google, try these other resources.

Pipl

Pipl is a free internet search engine that not only automatically checks Google, but also searches what is known as the 'deep web'. Pipl initially was limited to a search for name and phone number but has expanded to include email addresses, user names, and business names. I have found the results to be surprisingly good.

Metasearch Engines

Another method is to use a metasearch engine. A metasearch engine is simply a web service which queries multiple search engines at the same time and consolidates the results on one page. Using these free services it is possible to search Google, Yahoo, Bing, Ask.com, and About.com all at the same time. Dogpile.com, mama.com, and metacrawler.com are all good metasearch engines.

Commercial Database Services and Companies

Most law enforcement agencies have access to a commercial database service such as Accurint or CP CLEAR. These companies aggregate data from a wide variety of commercial and government sources to form as complete a picture as possible of an individual or business. Where exactly do these companies obtain their information? They won't tell you. Some company representatives, usually salespeople, will allude to having exclusive access to various super secret squirrel data sets. In reality, most of the information comes from three primary sources:

> Public/open source government records and databases such as court filings relating to bankruptcies and judgments, real estate assessor records, and, in some states, driver license and criminal records
>
> Publicly available information such as data from social networking sites, blogs, and forums
>
> Non-public information from commercial sources such as financial institutions and utilities. This information can also include so-called credit header information consisting of dates of birth, social security numbers, and addresses. Credit header information is data obtained from credit reporting agencies but which does not include the corresponding financial information.

While these databases are good, no single database aggregator is going to be able to acquire data from every source. These databases also have another inherent issue which can be a double edged sword. As a commercial database aggregator compiles data from their sources, the compile them and can automatically create a relationship between entities, addresses, and people. For example, a cellular phone subscriber cancels his service with a particular provider in order to change to another service. The subscriber's phone number is eventually recycled and issued to another customer, in this case a female. During that time the first customer's financial institutions continued to report the phone number to the credit reporting agencies, as he had yet to change his phone number with them. Some commercial databases would now associate both subscribers with the same phone number and could even infer there was a relationship between the two when, in fact, they have never met. This is particularly true with several of the prepaid cellular service providers who can recycle their phone numbers in as little as four to six weeks.

Commercial databases can be a tremendous advantage during criminal investigations, but they are not without their drawbacks. They should not be viewed a definitive, nor should they ever be the sole source of information.

LP Police

Most law enforcement executives are familiar with the bigger names in the commercial database industry. However, there are other smaller companies which do just as good a job as the larger companies or who have specialized data sets which the larger companies lack. An often overlooked database aggregator is LP Police. Their cellular telephone number database is very good for certain providers and it is relatively inexpensive compared to some of the other companies. However, I have found some of their other data sources to be very dated when compared to identical results from other databases such as Choicepoint or Lexis Nexis.

iTACT

Another excellent database is iTACT provided by TargusInfo. This company has a very comprehensive dataset from a variety of sources, including at least some financial services companies, including some major banks. Targus allows for batch importing of target numbers and batch downloading of the results which is very helpful when dealing with a large number of inquiries. Furthermore, the service automatically provides information regarding the provider and whether the phone number has been ported to another provider (more on both of these topics later). Unfortunately, the service is more expensive than many of the other providers and reportedly they will only allow Federal law enforcement subscribers. The good news is the service is subscribed to by most High Intensity Drug Trafficking Areas (HIDTAs) who can perform the checks at your request for free.

A Free Alternative

Among the many commercial database services arrives a newcomer; TLO XP. What makes TLO XP different? The service provides the same results, or very similar results, as the other major database services. What sets the company apart is that it provides their services free to law enforcement…forever. What's the catch? I haven't found one yet. The search results are comparable to any of the other paid services and they have developed some advanced features which are not found with the other companies' products. I was able to run approximately 200 side-by-side searches with TLO XP and another major commercial database. The results were almost identical. In 12 cases TLO XP had better, more current information than the other service. In two instances the other database had better results than TLO XP. The cost savings for most law enforcement agencies can be significant and it is possible to equip every officer in a department with access instead of just a few key individuals. TLO XP can be reached at 888-493-2209 or CustomerSupport@TLO.com

Determining the Provider

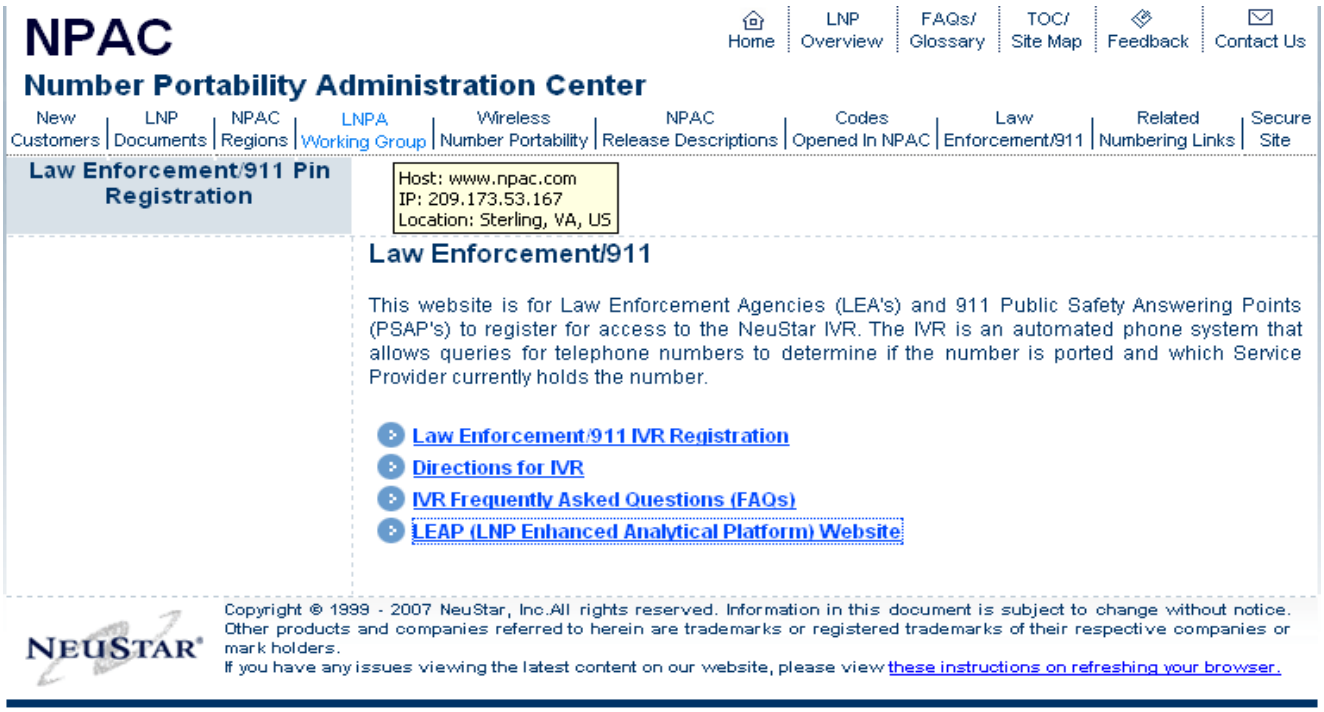
Many officers use open source or commercial databases to determine the provider (fonefinder.net, ChoicePoint, Accurint) Fonefinder.net is often wrong.

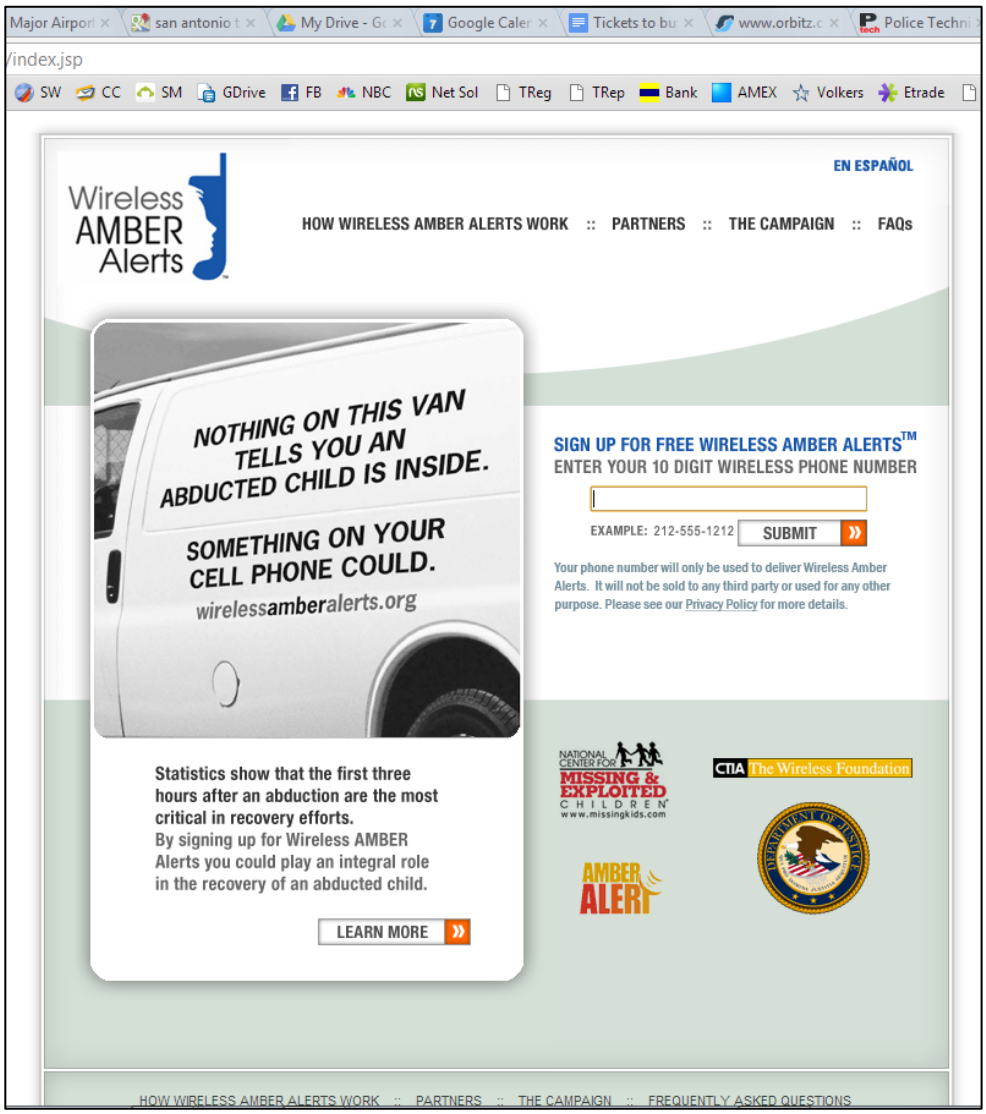
These services typically will only tell you the provider at the time you query the record.

They will not necessarily tell you if the number was ported to another provider or who the provider was six months ago.

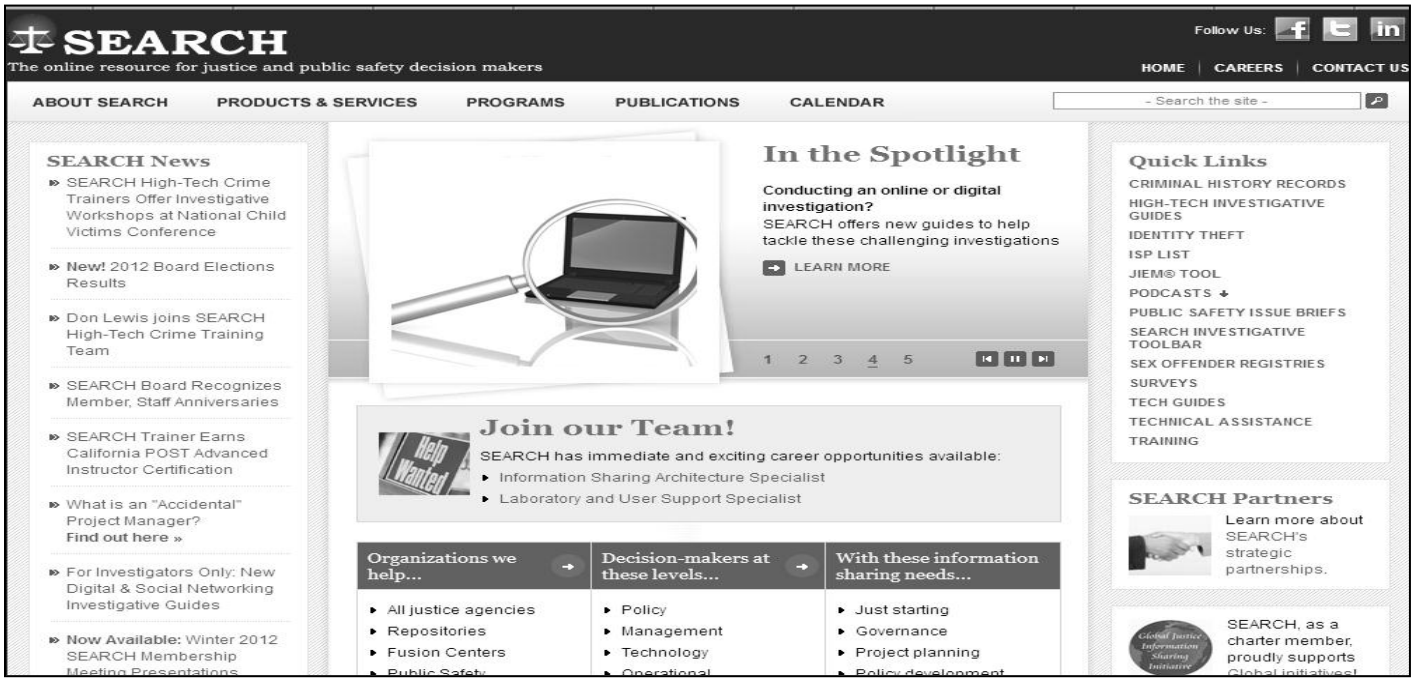
Failing to properly identify the provider will mean unnecessary delays of up to several weeks and repeat visits to the judge to get your orders signed.

NPAC-Number Portability Administration Center




Major Airport
san antonio t
My Drive - Gc
Google Caler
Tickets to bu
www.orbitz.c
Police Techni
/index.jsp
SW
CC
SM
GDrive
FB
NBC
Net Sol
TReg
TRep
Bank
AMEX
Volkers
Etrade
EN ESPAÑOL
Wireless AMBER Alerts
HOW WIRELESS AMBER ALERTS WORK :: PARTNERS :: THE CAMPAIGN :: FAQs
NOTHING ON THIS VAN TELLS YOU AN ABDUCTED CHILD IS INSIDE.
SOMETHING ON YOUR CELL PHONE COULD.
wirelessamberalerts.org
SIGN UP FOR FREE WIRELESS AMBER ALERTS™
ENTER YOUR 10 DIGIT WIRELESS PHONE NUMBER
EXAMPLE: 212-555-1212
SUBMIT
Your phone number will only be used to deliver Wireless Amber Alerts. It will not be sold to any third party or used for any other purpose. Please see our Privacy Policy for more details.
Statistics show that the first three hours after an abduction are the most critical in recovery efforts.
By signing up for Wireless AMBER Alerts you could play an integral role in the recovery of an abducted child.
LEARN MORE
NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN www.missingkids.com
CTIA The Wireless Foundation
AMBER ALERT
HOW WIRELESS AMBER ALERTS WORK :: PARTNERS :: THE CAMPAIGN :: FREQUENTLY ASKED QUESTIONS

www.search.org (ISP list)



Hash Function/Verification of Files

A cryptographic hash function is an algorithm which, when applied to a block of data such as a file, will return a fixed-length string consisting of numbers and/or letters. This fixed length string of numbers and/or letters will reflect a change in the underlying data if there is any change to the file or the information contained in the file.

There are a number of different hash algorithms and several are commonly used by popular forensic tools and applications. For example, Cellebrite's Universal Forensic Extraction Device (UFED) generates two hash algorithms for data extracted from using the device.

Examination Report Page 29 of 33

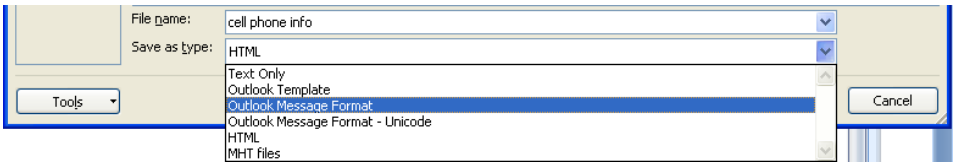
13	File Source: Phone File Size: 104251 Bytes File Date/Time: 08/25/11 11:40:12 MD5: 477242DFA0E34D35B4922C7B01249828 SHA256: D652C4B6 7D92ABBA046F8D 15CABB6 1BC7F95D3C9A3E 0C232F9 E98530E2BE2B45	Pixel Resolution: 573x768	
14	File Name: Photo0243.jpg File Path: /Photos File Source: Phone File Size: 445670 Bytes File Date/Time: 08/25/11 11:35:54 MD5: EA47979535845ACFA5DB6E504053ACDB SHA256: C52E2482 2288137F890C4F 0FBBC68 16C0CE2680EC6F FFF3271 E30E9017170AB5	Resolution: 72x72 (unit: inch) Pixel Resolution: 1280x960 Camera Make: SAMSUNG Camera Model: SGH-T259 Date/Time: 2011:08:25 11:35:53	

MD5 and SHA256 are commonly used cryptographic hash functions to insure evidence integrity. There are multiple online and downloadable programs to verify the hash of evidence obtained using forensic tools, as well as, data received from electronic means such as court order/search warrant responses.

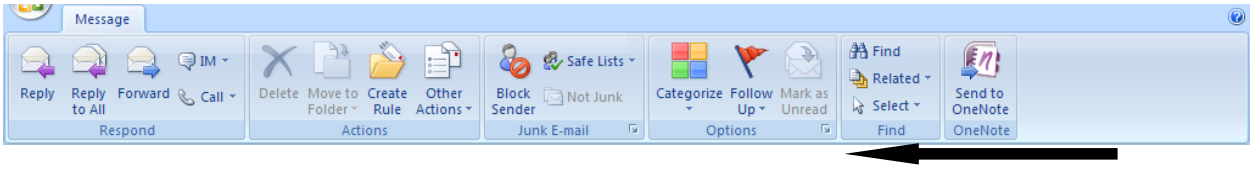
Securing Search Warrant/Court Order Returns Sent Via E-Mail

Upon receipt of a court order or search warrant return from a cellular service provider an investigator should immediately take steps to preserve the integrity of the evidence. The following example is shown using Microsoft Outlook 2007.

Before opening the email message or any of the attachments, highlight the email message and click the **File** located in the upper left corner of the screen. Select **Save As** and choose the option **Outlook Message Format**.



Selecting this option saves the message, the files, as well as the header information which documents the internet protocol address(es) of the sender and the route the message took to get to your department's server. The IP information can be found by selecting the small drop down arrow in the **Options** box.

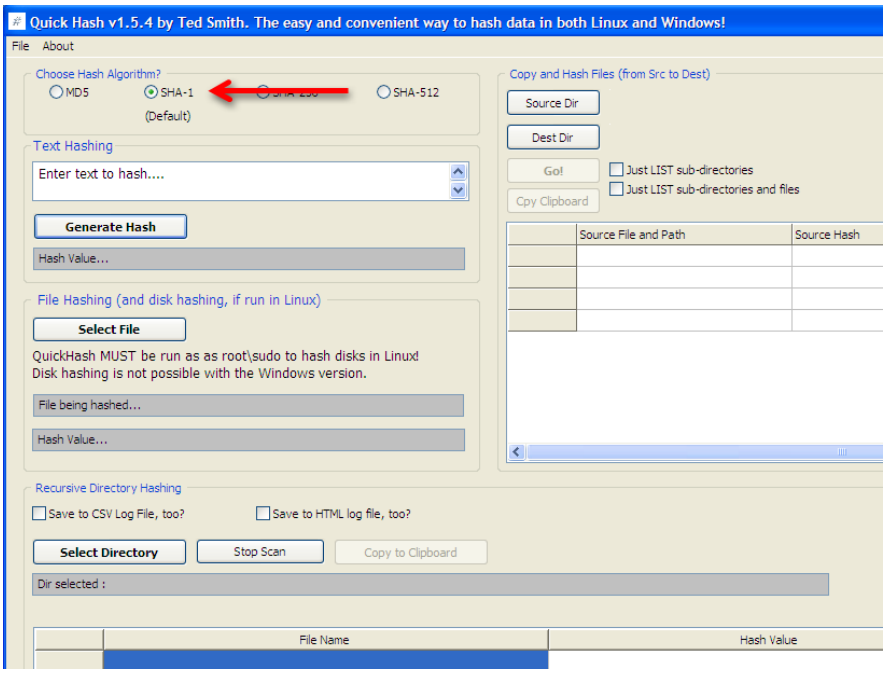


From there select **Message Options** and you will be able to view the IP and routing information which can help verify the integrity of the message.

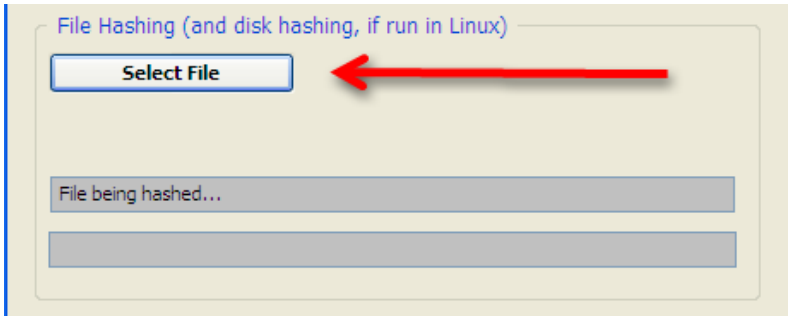
Choose a location to save the file to, preferably in a folder with the case number or other identifiers.

The next step is to verify the hash of the email message. There are a number of free online services which will calculate the hash value of documents but many law enforcement officers and their agencies are leery of allowing an anonymous third party web application access to their data. You may choose to use one of these services or to download and install an application to calculate the hash value. [NOTE: Some of these programs are designed to be run from the command line prompt. If you are not familiar with command line, make sure the program you select has a graphic user interface (GUI) and is designed to run on your department's operating systems (Windows).]

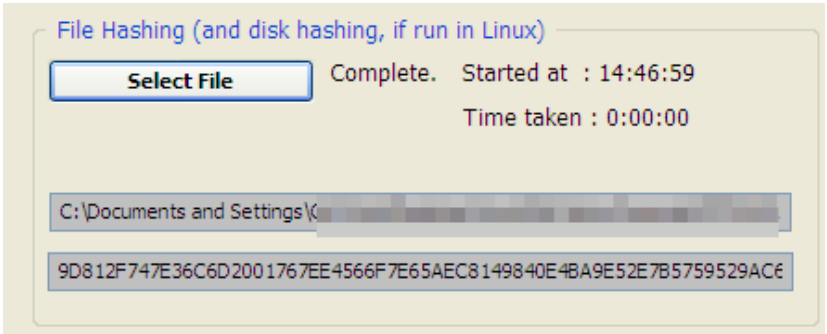
This example illustrates the use of a program called Quick Hash available for free from Source Forge. Open the program and note the default hash algorithm is set at SHA-1 (Secure Hash Algorithm-1). You can choose from several different options in this program but for illustration I selected a more comprehensive algorithm, SHA-256



Navigate to your save Outlook file using the **Select File** function.

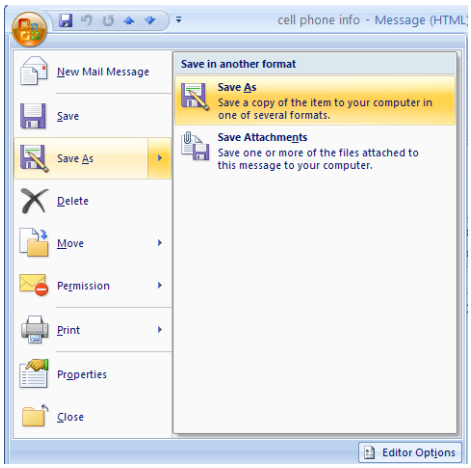


The software will automatically calculate the hash value using the algorithm selected. From here you can **Copy** and **Paste** the hash value into a report or other document for preservation.



Quick Hash also has a function which allows you to calculate the hash value of files whenever you move them or transfer them to another storage medium. While doing so the program automatically calculates the hash value of all of the files contained in the folder and then creates a .csv (Comma Separated Value) file which is readable using Excel.

If you already opened the email, it's not too late. Just don't open the files. Within Outlook press the Windows button in the upper left corner of the message box. Select **Save As**



Call Detail Records

There are two types of information that can be obtained from electronic communications services: records and content. "Content" is the actual communication, typically the words spoken by the parties to a telephone conversation or the message contained in an e-mail. "Records," on the other hand, consist of raw data pertaining to a communication.

"Content" 18 USC § 2510(8) ; *Jessup-Morgan v. AOL (1998) 20 F. Supp.2d 1105, 1108*

*"*Records" Smith v. Maryland (1979) 442 US 735, 741

Depending on the provider, subscriber information can contain:

Name

Address

Identifying information such as SSN, CDL

Billing Address

Other Contact Numbers (known in the industry as 'can be reached' numbers)

Other phone numbers on the same account

Email Addresses

Make, model, and serial numbers of the phone

Customer service rep comments and notes

Method and source of payment information

Preservation Letters

It is critically important that if you believe text message content may be important to your case that you submit a preservation letter to the provider as soon as possible.

In fact, if you are a criminal investigator (homicide, rape, etc.) you should be submitting preservation letters on everyone as soon as you ID a phone number.

18 USC 2703(f)

- (f) **Requirement To Preserve Evidence.—** (1) **In general.—** A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.
- (2) **Period of retention.—** Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

Preservation Letter Example

AT&T Wireless

VIA FAX to (888) 938-4715

Re: 18 USC 2703(f) Preservation Request – AT&T Wireless Number 510-207-9999, 510-207-9999 and 510-276-9999.

Dear Madam/Sir:

I am writing to make a formal request for the preservation of records and other evidence pursuant to 18 U.S.C. § 2703(f) pending further legal process regarding AT&T Wireless Number 510-207-9999 and 510-276-9999.

You are hereby requested to preserve, for a period of 90 days, the records described below currently in your possession, including records stored on backup media, in a form that includes the complete record. You also are requested not to disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request may result in a permanent or temporary termination of service to the accounts described below, or otherwise alert the subscriber or user of these accounts as to your actions to preserve the referenced files and records, please contact me before taking such actions.

This preservation request applies to the following records and evidence:

All Call Detail Records of user activity for user account AT&T Wireless 510-207-9999, 510-207-9999 and 510-276-9999 including but not limited to all numbers associated with the account, all customer service notes, number changes prior to and any after this number was activated.

Subscriber information including:

1. Mailing addresses, residential addresses, business addresses, e-mail addresses and any other address information.

2. Telephone numbers or other subscriber number or identifier number.

3. Account comments, notes, and any number changes associated with past and present.

4. Credit information obtained or used by the company to grant account status.

5. Billing records.

Outbound and inbound call detail from Date of creation to present, including duration of communication

Call origination / termination location from creation of the account associated with AT&T Wireless 510-207-9999, 510-207-9999 and 510-276-9999 to present.

All of the above records whether possessed by cellular service provider AT&T or any other cellular service provider providing cellular service for 510-207-9999, 510-207 9999 and 510-276-9999.

All stored communications or files, including voice mail, text messages (including numbers text to and received from and any related content), email, digital images, buddy lists, video calling, data connections (to include ISPs, Bookmarks, Websites accessed) and any other files including all cell-site and sector information associated with each record and associated with user accounts identified as: mobile numbers 510-207-9999, 510- 207-9999 and 510-276-9999, or e-mail account thugsuspect@yahoo.com.

All connection logs and records of user activity for each such account including:

1. Connection dates and times.

2. Disconnect dates and times.

3. Method of connection (e.g., telnet, ftp, http)

4. Data transfer volume.

5. User name associated with the connections.

6. Telephone caller identification records.

7. Any other connection information, such as the Internet Protocol address of the source of the connection.

8. Connection information for the other computer to which the user of the above referenced accounts connected, by any means, during the connection period, including the destination IP address, connection time and date, disconnect time and date, method of connection to the destination computer, and all other information related to the connection from cellular service provider.

9. Any other records or accounts, additional numbers on the account or associated with the BAN (Billing Account Number), including archived records related or associated to the above referenced names, user names, social security number(s), federal I.D. number(s) or accounts and any data field name definitions that describe these records.

Paying for Call Detail Records

18 USC 2706(a) says the provider shall be paid a fee for reimbursement "for such costs as are reasonably necessary…"

If a provider requests $50 per phone number for subscriber information and call detail records, ask them for an accounting of the time. As the results are typically sent via e-mail there are no reproduction costs. The bulk of their expense is personnel expenditure. Many subpoena compliance personnel are paid between $10-20 per hour. Did it really take two to five hours to fulfill your search warrant or court order?

18 USC 2706(b) states the amount of the fee will be mutually agreed upon.

Many boiler plate search warrants include language stipulating the provider will be paid or reimbursed for expenses. Take that language out of there and stop agreeing in advance to pay.

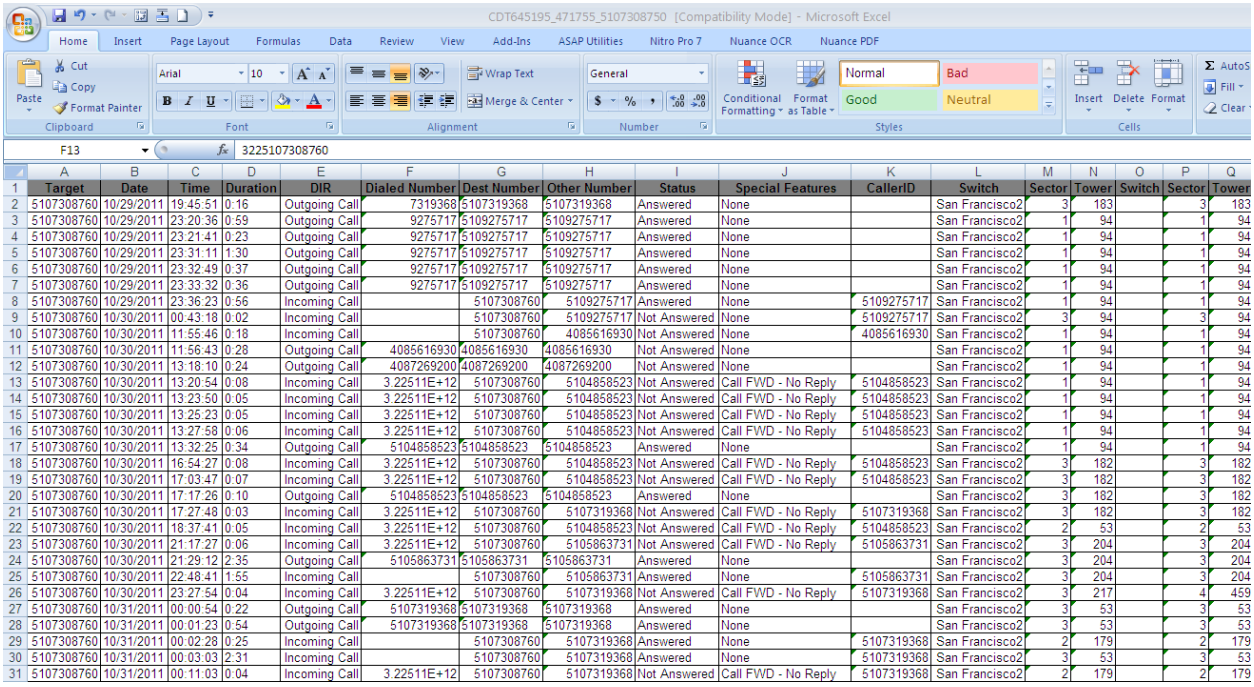
18 USC 2706(c) states (b) shall not apply to information about toll records and telephone listings.

Many providers will try and tell you the records they are providing are not toll records and telephone listings. Ask them what they are providing then because the information is the same.

Pivot Tables for Call Detail Record Analysis

Pivot tables are a powerful function built into Microsoft Excel which can be used to translate call detail records (CDRs) into something useable.

Remember: NEVER WORK WITH YOUR ORIGINAL DATA! You should only use a copy of the files and not the originals you received from the cellular service provider.

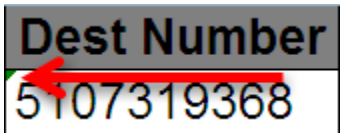


	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Target	Date	Time	Duration	DIR	Dialed Number	Dest Number	Other Number	Status	Special Features	CallerID	Switch	Sector	Tower	Switch	Sector	Tower
2	5107308760	10/29/2011	19:45:51	0:16	Outgoing Call	7319368	5107319368	5107319368	Answered	None		San Francisco2	3	183		3	183
3	5107308760	10/29/2011	23:20:36	0:59	Outgoing Call	9275717	5109275717	5109275717	Answered	None		San Francisco2	1	94		1	94
4	5107308760	10/29/2011	23:21:41	0:23	Outgoing Call	9275717	5109275717	5109275717	Answered	None		San Francisco2	1	94		1	94
5	5107308760	10/29/2011	23:31:11	1:30	Outgoing Call	9275717	5109275717	5109275717	Answered	None		San Francisco2	1	94		1	94
6	5107308760	10/29/2011	23:32:49	0:37	Outgoing Call	9275717	5109275717	5109275717	Answered	None		San Francisco2	1	94		1	94
7	5107308760	10/29/2011	23:33:32	0:36	Outgoing Call	9275717	5109275717	5109275717	Answered	None		San Francisco2	1	94		1	94
8	5107308760	10/29/2011	23:36:23	0:56	Incoming Call		5107308760	5109275717	Answered	None	5109275717	San Francisco2	1	94		1	94
9	5107308760	10/30/2011	00:43:18	0:02	Incoming Call		5107308760	5109275717	Not Answered	None	5109275717	San Francisco2	3	94		3	94
10	5107308760	10/30/2011	11:55:46	0:18	Incoming Call		5107308760	4085616930	Not Answered	None	4085616930	San Francisco2	1	94		1	94
11	5107308760	10/30/2011	11:56:43	0:28	Outgoing Call	4085616930	4085616930	4085616930	Not Answered	None		San Francisco2	1	94		1	94
12	5107308760	10/30/2011	13:18:10	0:24	Outgoing Call	4087269200	4087269200	4087269200	Not Answered	None		San Francisco2	1	94		1	94
13	5107308760	10/30/2011	13:20:54	0:08	Incoming Call	3.22511E+12	5107308760	5104858523	Not Answered	Call FWD - No Reply	5104858523	San Francisco2	1	94		1	94
14	5107308760	10/30/2011	13:23:50	0:05	Incoming Call	3.22511E+12	5107308760	5104858523	Not Answered	Call FWD - No Reply	5104858523	San Francisco2	1	94		1	94
15	5107308760	10/30/2011	13:25:23	0:05	Incoming Call	3.22511E+12	5107308760	5104858523	Not Answered	Call FWD - No Reply	5104858523	San Francisco2	1	94		1	94
16	5107308760	10/30/2011	13:27:58	0:06	Incoming Call	3.22511E+12	5107308760	5104858523	Not Answered	Call FWD - No Reply	5104858523	San Francisco2	1	94		1	94
17	5107308760	10/30/2011	13:32:25	0:34	Outgoing Call	5104858523	5104858523	5104858523	Answered	None		San Francisco2	1	94		1	94
18	5107308760	10/30/2011	16:54:27	0:08	Incoming Call	3.22511E+12	5107308760	5104858523	Not Answered	Call FWD - No Reply	5104858523	San Francisco2	3	182		3	182
19	5107308760	10/30/2011	17:03:47	0:07	Incoming Call	3.22511E+12	5107308760	5104858523	Not Answered	Call FWD - No Reply	5104858523	San Francisco2	3	182		3	182
20	5107308760	10/30/2011	17:17:26	0:10	Outgoing Call	5104858523	5104858523	5104858523	Answered	None		San Francisco2	3	182		3	182
21	5107308760	10/30/2011	17:27:48	0:03	Incoming Call	3.22511E+12	5107308760	5107319368	Not Answered	Call FWD - No Reply	5107319368	San Francisco2	3	182		3	182
22	5107308760	10/30/2011	18:37:41	0:05	Incoming Call	3.22511E+12	5107308760	5104858523	Not Answered	Call FWD - No Reply	5104858523	San Francisco2	2	53		2	53
23	5107308760	10/30/2011	21:17:27	0:06	Incoming Call	3.22511E+12	5107308760	5105863731	Not Answered	Call FWD - No Reply	5105863731	San Francisco2	3	204		3	204
24	5107308760	10/30/2011	21:29:12	2:35	Outgoing Call	5105863731	5105863731	5105863731	Answered	None		San Francisco2	3	204		3	204
25	5107308760	10/30/2011	22:48:41	1:55	Incoming Call		5107308760	5105863731	Answered	None	5105863731	San Francisco2	3	204		3	204
26	5107308760	10/30/2011	23:27:54	0:04	Incoming Call	3.22511E+12	5107308760	5107319368	Not Answered	Call FWD - No Reply	5107319368	San Francisco2	3	217		4	459
27	5107308760	10/31/2011	00:00:54	0:22	Outgoing Call	5107319368	5107319368	5107319368	Answered	None		San Francisco2	3	53		3	53
28	5107308760	10/31/2011	00:01:23	0:54	Outgoing Call	5107319368	5107319368	5107319368	Answered	None		San Francisco2	3	53		3	53
29	5107308760	10/31/2011	00:02:28	0:25	Incoming Call		5107308760	5107319368	Answered	None	5107319368	San Francisco2	2	179		2	179
30	5107308760	10/31/2011	00:03:03	2:31	Incoming Call		5107308760	5107319368	Answered	None	5107319368	San Francisco2	3	53		3	53
31	5107308760	10/31/2011	00:11:03	0:04	Incoming Call	3.22511E+12	5107308760	5107319368	Not Answered	Call FWD - No Reply	5107319368	San Francisco2	2	179		2	179

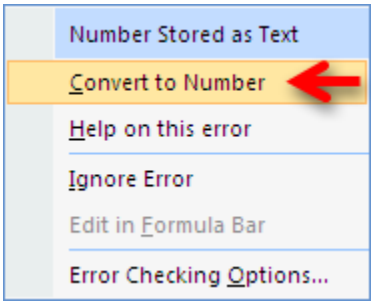
Step 1-Clean Your Data

In order for a pivot table to work effectively the call detail record data must be standardized. Some cellular service providers include routing codes, extra digits, and additional information in the same text box as the phone number. These extra digits will need to be cleaned from the data. You may also see additional data in the Dialed Number column which does not reflect an actual phone call such as the case when someone only enters a partial or incomplete phone number before pressing the send button. As those are not actual calls, but merely records of incomplete calls I delete those records. Depending on the provider you may also see extra routing numbers or extra digits, such as *67 when someone blocks their phone number from appearing on caller ID. There are a number of methods for removing those leading digits including the Find and Select function from the Home tab of Excel. However, after much trial and error I have become a faithful user of a free suite of tools called **ASAP Utilities**. These tools make it very easy to format all of your data quickly.

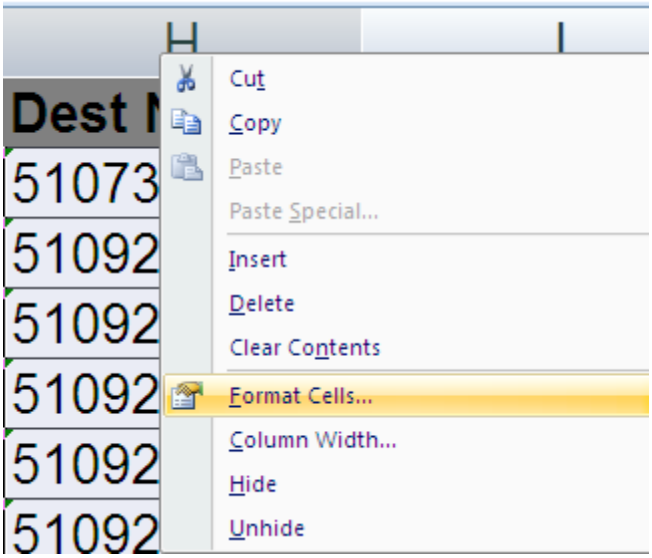
You may also note that Excel interprets some or all of your data contained in call detail records as text and not as numbers. When Excel detects numbers stored as text is places a small green triangle in the upper left of the cell.



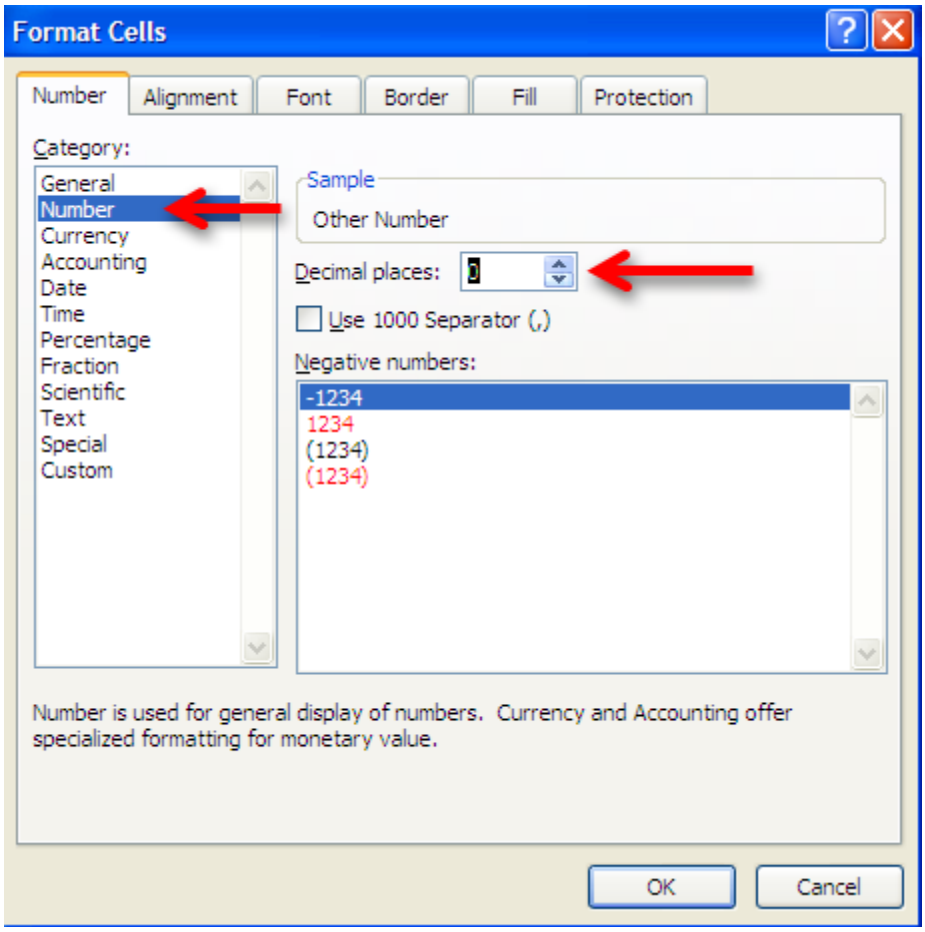
You could click on the green triangle and manually change each cell of text into a number but that would take forever.



To quickly convert all text to numbers highlight the entire column by clicking the cell with a letter in it at the top of the column. **Right click** and select **Format Cells**.

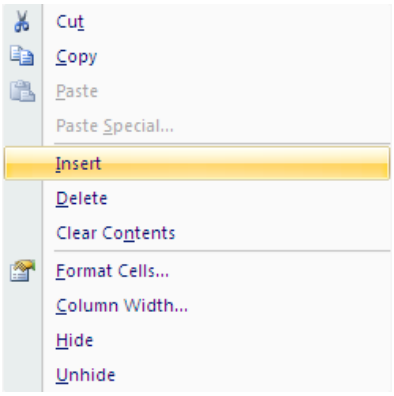


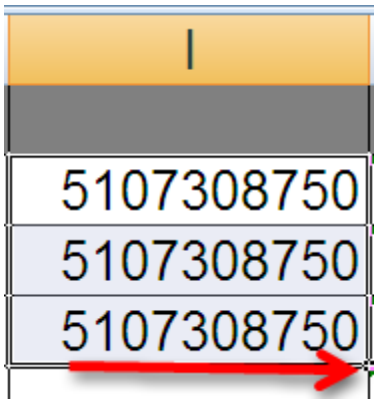
Select **Number**. By default you will see the number 2 in the box marked **Decimal Places**. Change that to **0**.



Step 2-Insert New Columns

If you call detail records do not have a separate column for the target phone number you will need to create one. The easiest way is to right click you mouse button on the column header **A** and select **Insert**. This will automatically insert a column and shift the data over. In the A1 cell type something to help you remember what this data is such as **Target Number**. This will be important later as there will be multiple columns to choose from and you want to make sure you select the proper one.





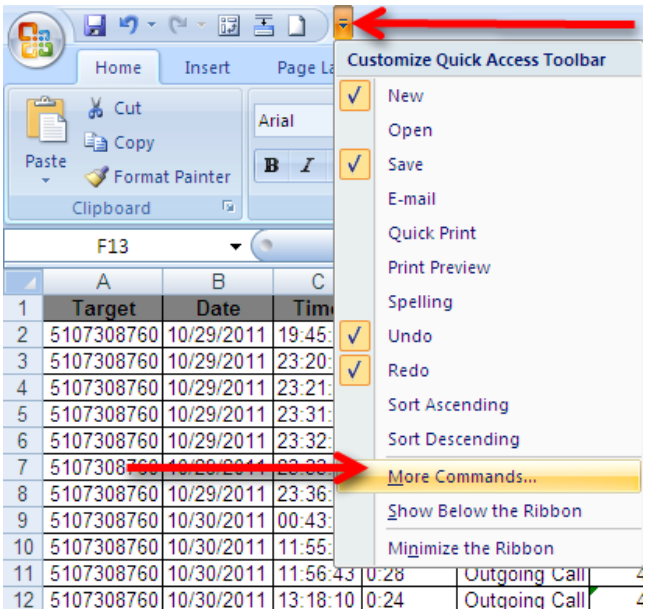
Insert the target number and then fill the entire column with your target telephone number. The easiest way to do this is to copy the phone number three times into the first three cells. Then highlight all three cells by left clicking you mouse button and dragging it downwards until all three cell are highlighted. If you hover your mouse cursor over the lower right corner of the last cell what looks like a small plus sign **+** will appear. Left click the plus sign **+** and Excel will automatically populate all of the cells below it with the target number.

You are also going to need to insert another column for your **Other Numbers**. This data already exists in the call detail records but some providers display this information in multiple different columns. Right click you mouse button and select Insert again to place a new blank column in your data and label it with something you will remember such as **Other Number**. The other phone numbers need to be consolidated in one column. Depending on the provider, you may have to sort your data by the **Direction** of the call or the **Caller ID** column to obtain this information. Copy the data from those rows into your new column so that all of the other phone numbers are in one place.

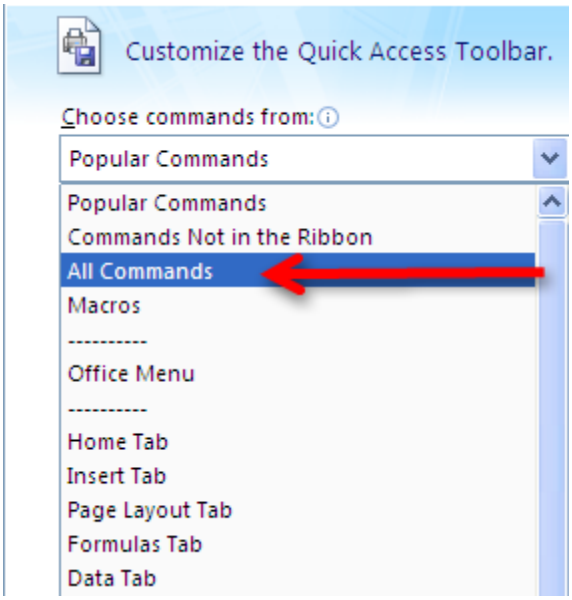
Step 3-Finding the Pivot Table

The Pivot Table function is located in two places in Excel. The first in the **Insert** tab located at the top of the Excel workbook.

You may also wish to add the Pivot Table to the Quick Access Toolbar located at the upper left corner of the Excel workbook. In order to add the Pivot Table to the toolbar, select the drop down error to the right of the toolbar. You will need to select **More Commands** to locate the Pivot Table function.



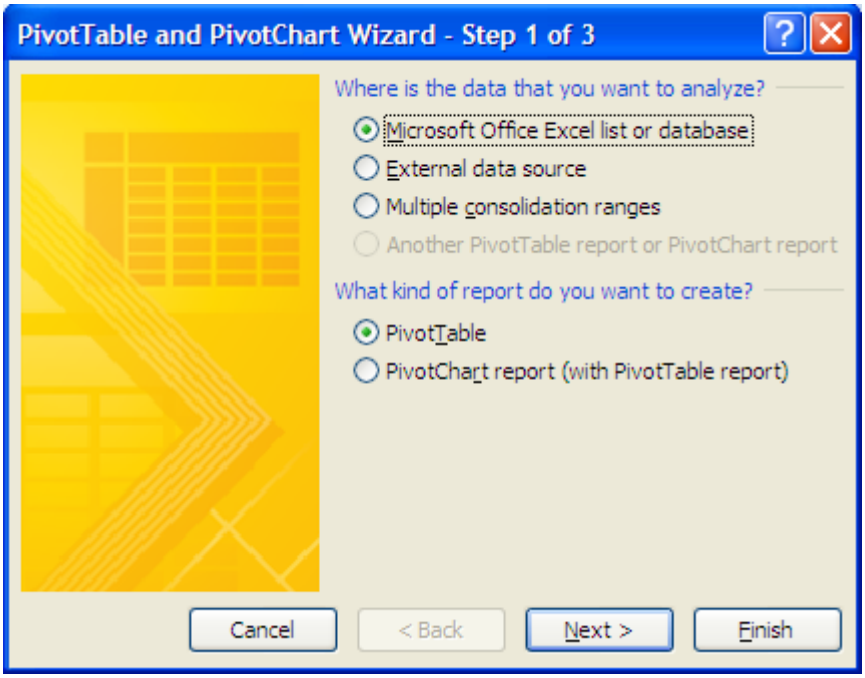
Next select **All Commands** and scroll down until you see the **Pivot Table Wizard**. Select the **Add** button to include the Pivot Table Wizard in the toolbar.



When you are done you should see this icon in your Quick Launch Toolbar.

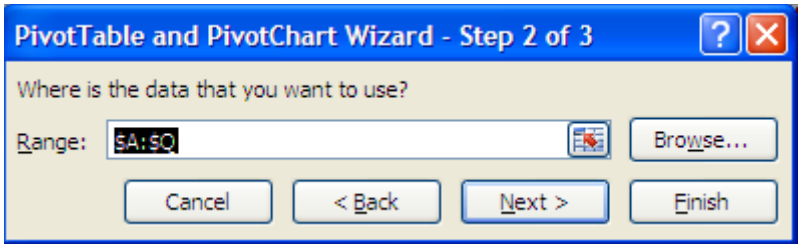
Step 4-Using the Pivot Table Wizard

Select **Pivot Table** from either the Insert Tab or the newly created icon the Quick Launch Toolbar. This will start the program and automatically bring up this screen:

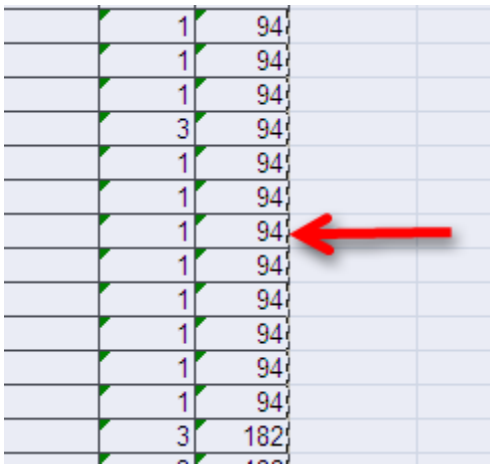


We are not going to do anything fancy from this screen so select **Next**. You could select Finish from this screen but there are some different options in the following steps.

The Step 2 screen tells the Pivot Table Wizard where the data is going to come from.

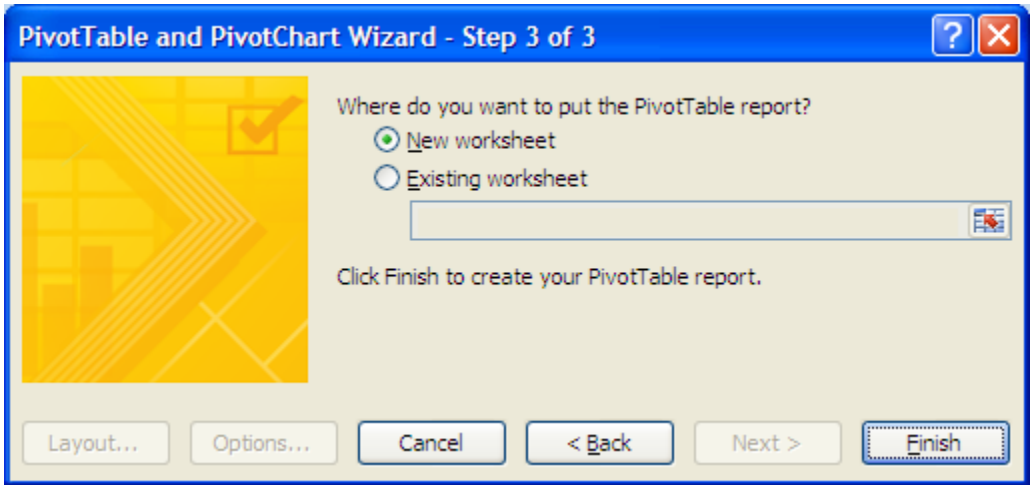


Before selecting next make sure all of the data in your sheet is selected. The data in the sheet should be surrounded by a moving row of dashes sometimes referred to as 'marching ants'.



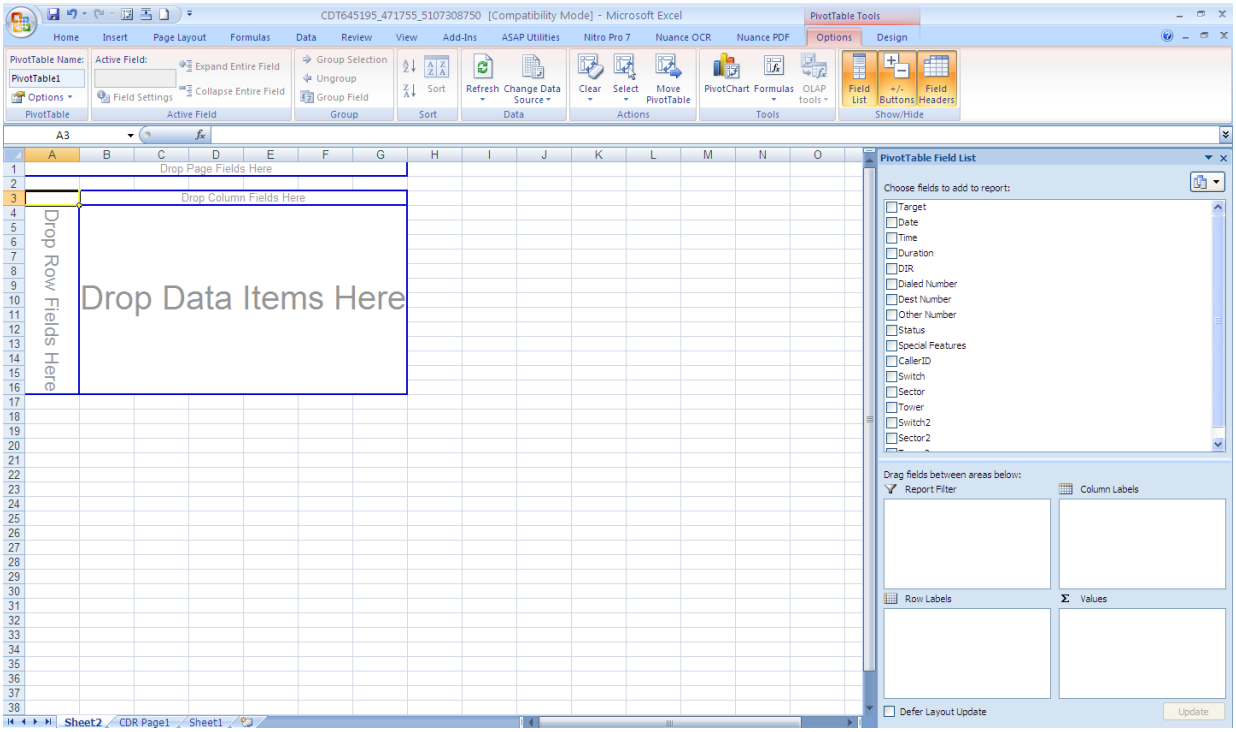
All of the data inside the highlighted area and surrounded by the marching ants is going to be imported into the Pivot Table. If for some reason all of the data is not selected, or if the entire work sheet is highlighted including columns and rows with no data in it, select cancel and click on any cell containing data on the sheet and re-run the Pivot Table Wizard.

To complete the setup of the Pivot Table select the finish button from the Step 3 screen. By default this will create the Pivot Table in a new worksheet which will be added in front of your existing worksheets.



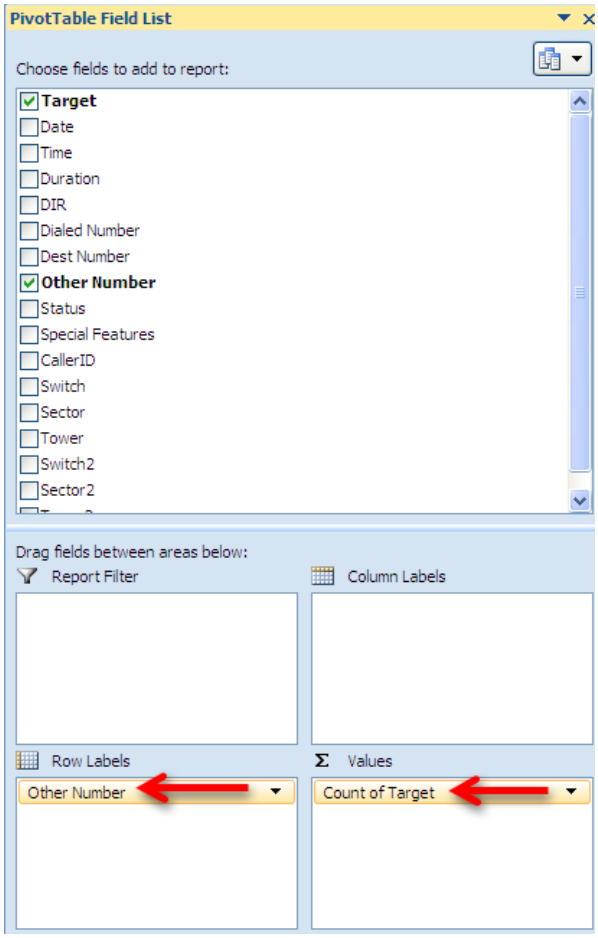
Step 5-Using the Pivot Table

Once the Pivot Table process has been completed you should be presented with the following in a new sheet added to your Excel workbook:

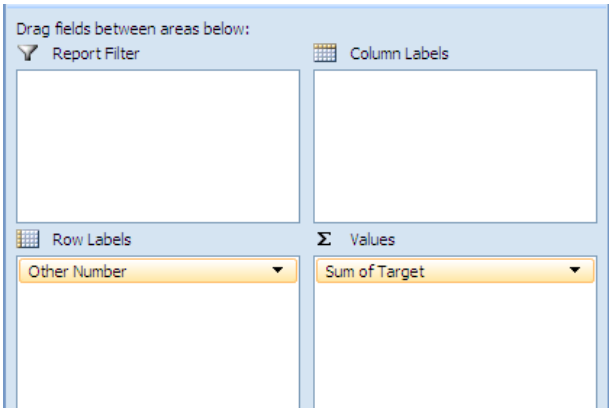


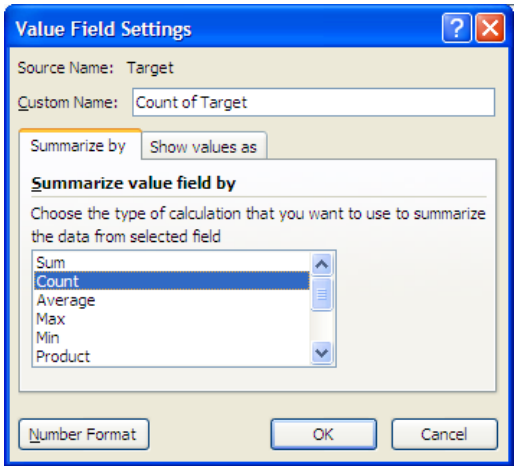
All of the column headers, including the **Target Number** and **Other Number** should appear in the Pivot Table Field List located in the upper right of the screen. From this screen you can perform basic call frequency analysis using the data from the call detail records.

Select **Target Number** and **Other Number** by placing a check mark in the boxes. You data may appear in the boxes labeled **Row Labels** and **Values**. If the data is not automatically in those boxes, click and drag the data so it appears as below:



Sometimes the data in the **Values** box will be different and will say **Sum of Target** and not **Count of Target**. If this happens you will see strange numbers in the Pivot Table because the software has decided to add up the total of all of the phone numbers instead of count how often they occur. If that happens select the drop down menu in **Sum of Target**.

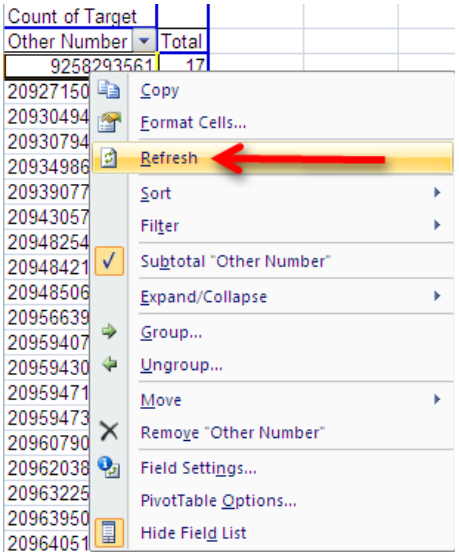




Once the Value Field Setting has been properly configured you should see each unique phone number listed with a total representing the number of times the target phone number was in contact with the other phone number.

	A	B
1	Drop Page Fields Here	
2		
3	Count of Target	
4	Other Number	Total
5	9258293561	17
6	2092715069	119
7	2093049461	1
8	2093079461	2
9	2093498686	1
10	2093907769	3
11	2094305701	1
12	2094825418	50
13	2094842134	6
14	2094850628	43

However, in the example listed above you can see that the first phone number is not listed sequentially. In this case, the number was not properly formatted and is still viewed by Excel as text and not a number. If this happens to you go back and reformat the other numbers so they are all represented as a number.



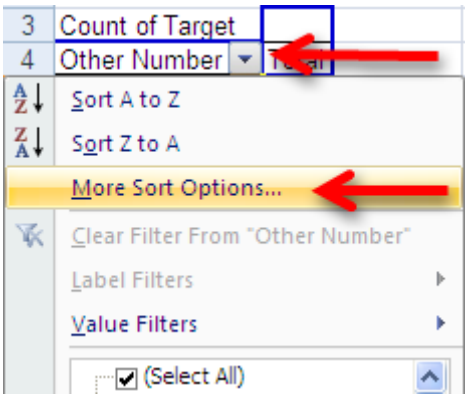
It is not necessary to re-run the Pivot Table. Select the sheet containing the data and make the necessary corrections. Then select the drop down box located above the phone numbers and select **Refresh**.

If everything looks good, move on to the next step.

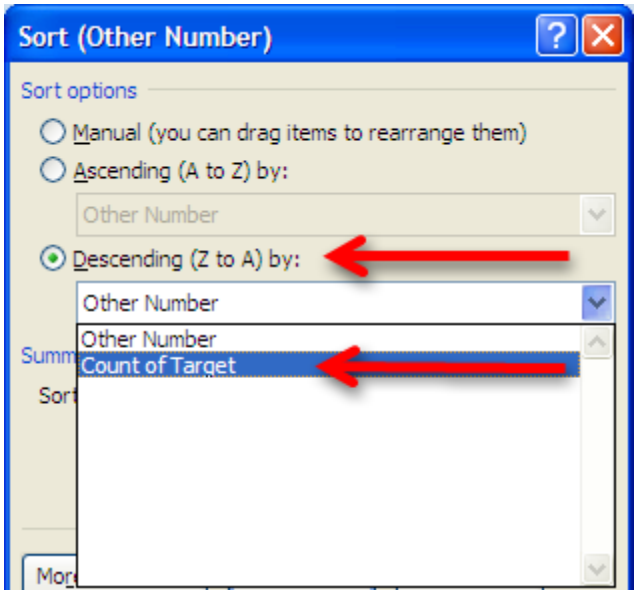
Step 6-Sorting the Numbers

The Pivot Table has given us some good information. You should have a list of unique phone numbers and a sum of the number of occurances the target was in contact with that number. However, by default, the Pivot Table is sorted by the phone number and not the total number of contacts. In order to find the phone number the target was in contact with the most often, we must change the **Sort** order of the Pivot Table.

Click the drop down box located at the top of the column and select **More Sort Options**.



In order to see the target number's most frequent contacts in order, select the **Descending** option from the **Sort** menu and then select **Count of Target**.



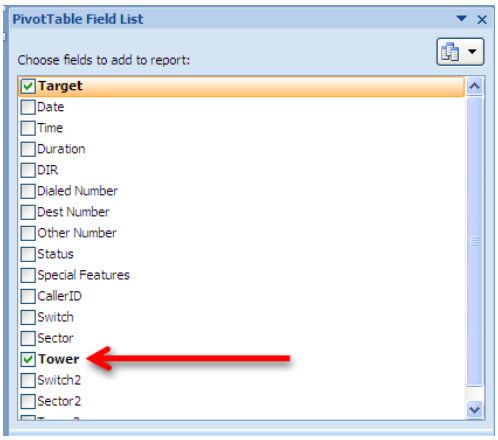
This will re-sort the data by the highest number of contacts to the lowest and allow you to easily visualize the most frequent contacts. Note that the target number will almost always be the largest number of contacts. Depending on the service provider these calls are actually incoming calls that were routed to voicemail or they were the user checking their voicemail messages. The next steps are basic police work-identify the subscribers and users of the high frequency contacts.

	A	B
1	Drop Page Fields Here	
2		
3	Count of Target	
4	Other Number	Total
5	5107319368	1632
6	5105863731	402
7	6502901549	264
8	5107308750	235
9	5105769450	202
10	5103149041	196
11	9259612247	191
12	5103631974	183
13	5107122982	146
14	2096322581	142
15	9259612222	121
16	2092715069	119
17	9162844639	118
18	5106904099	111
19	5106774697	105
20	5102274598	100

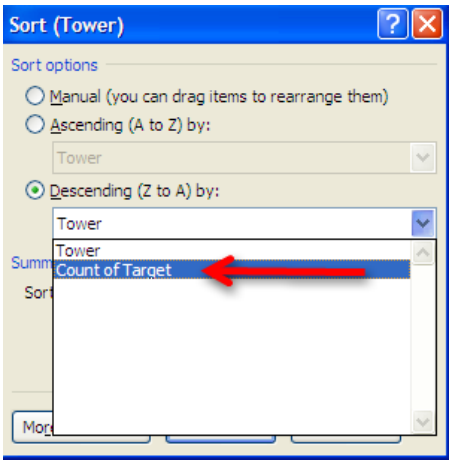
Other Uses for Pivot Tables

Another use for the Pivot Table is basic cell tower analysis. A Pivot Table can quickly and easily add up the most frequent cell towers which were in communication with the cellular phone. This can provide clues to a suspect's location or other areas they are known to frequent. Visualizing cell tower data in a Pivot Table will require a key from the cellular service provider or from the FBI's CALEA (Communications Assistance to Law Enforcement Act) Unit. However, the basic Pivot Table functions are essentially identical to those used in determining high frequency contacts.

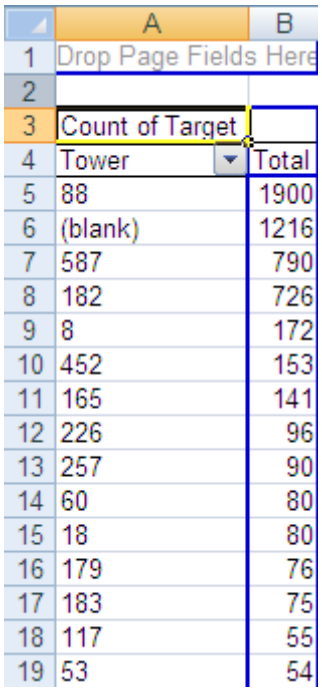
Follow the steps listed above until the Pivot Table is generated. However, instead of listing the Target Number and the Other Number you will highlight the **Target Number** and the **Tower**. Note that the provider in this example provides both beginning and ending cell tower data so you may need to run the Pivot Table on both sets of data in order to get an accurate idea of the location of the handset.



By changing the Sort order in a similar fashion to the one illustrated above, you can easily sort the cell towers by their frequency of use.



In this example you can see there are only a few towers with a significant number of hits. You might also note the second most common data point is listed as Blank. This is because the provider from this example does not record cell tower information when the call is forwarded to voicemail. Most of the major cellular service providers do not record cell tower information for calls forwarded to voicemail. Nor do most of the major companies provide cell tower data for text message or data events. However, AT&T is an exception to that rule as they capture cell tower data during phone calls, text messages, and data events such as internet browsing.



	A	B
1	Drop Page Fields Here	
2		
3	Count of Target	
4	Tower	Total
5	88	1900
6	(blank)	1216
7	587	790
8	182	726
9	8	172
10	452	153
11	165	141
12	226	96
13	257	90
14	60	80
15	18	80
16	179	76
17	183	75
18	117	55
19	53	54

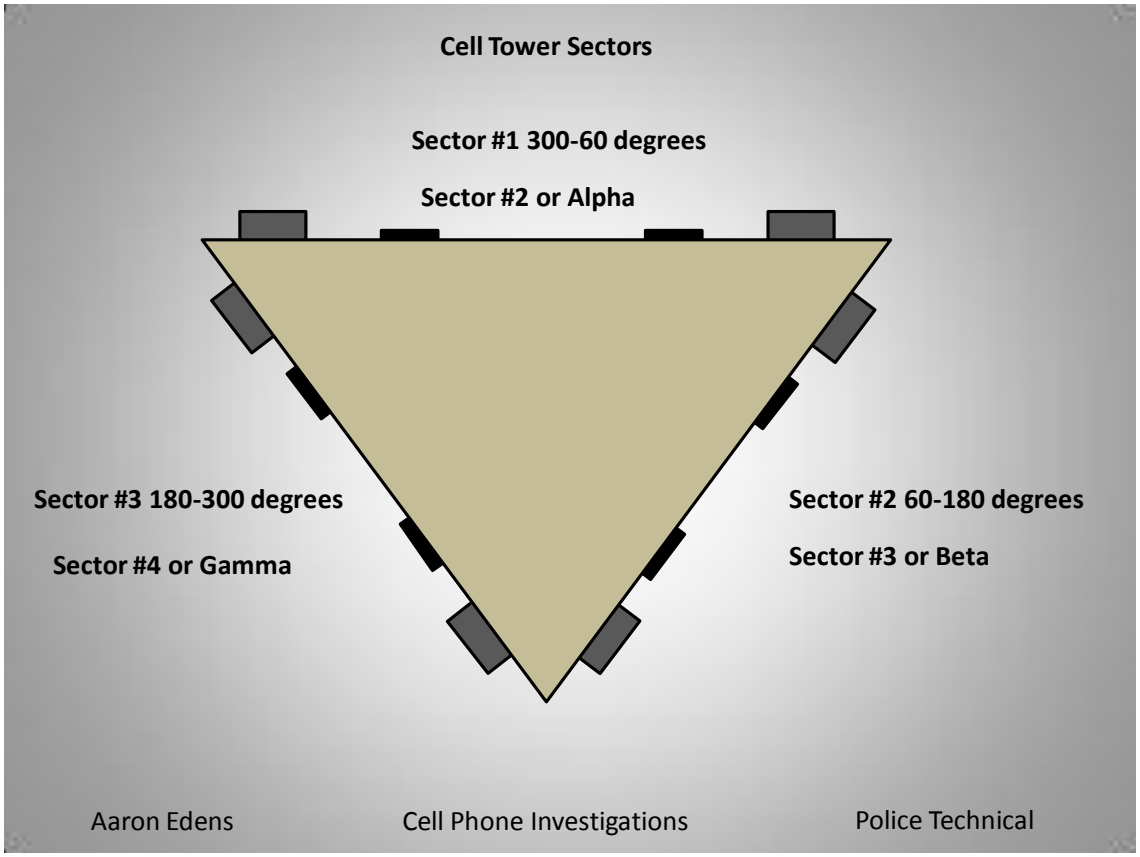
Most cell towers have three sectors and they cover 120 degrees.

Sector 1 covers 300-60 degrees.

Sector 2 covers 60-180 degrees.

Sector 3 covers 180-300 degrees.

- There may be as much as a 20 degree overlap between sectors



Cell Towers Five Fatal Flaws

1. Failing to request or preserve cell tower data early in the investigation

2. Presuming the communicating tower is the closest and not the tower with the best signal

3. Using the cell phone location and the suspect location interchangeably

4. Trusting the theoretical layout of cell tower antennas

5. Failing to note the azimuth of the tower

Per Call Measurement Data (PCMD)

PCMD was originally referred to as Measurement Data in Call Records (MDCR). Both MDCR and PCMD are engineering terms referring to techniques used to measure the effectiveness of cellular service in a particular area. PCMD collects select measurement data on every completed call including information regarding the nature of terminated, dropped, and normal calls. Another data set collected by PCMD is the time it takes a signal to leave a cellular handset and the return back to the tower. It is this information which can provide previously unavailable information regarding the location of a particular handset.

PCMD was originally designed to be used for quality assurance purposes by gauging the number of dropped calls in a particular area. Based on this information a cell site engineer could recommend re-orienting a cell tower or other changes to improve the coverage in a particular area. However, someone within Alcatel-Lucent, one of the major manufacturers of cell tower equipment, discovered PCMD is accurate enough to be used for location based marketing without any upgrades to the existing cellular infrastructure or the customer's equipment. Because the speed of a cellular signal is a known constant it is possible to calculate the distance the handset is from the tower by measuring the time it takes for the signal to make a roundtrip. When combined with the cell sector information, there is now an opportunity to gauge how far away the handset is from the cell tower. This might not seem like an immediately revolutionary data set. Knowing that someone is three quarters of a mile away from a cell tower in the middle of downtown Atlanta is not likely to produce any great leads for missing persons or fugitive tracking. However, the data can be much more accurate than it initially appears.

Unlike the cell site and sector information obtained from call detail records, PCMD is captured not only for every phone call, but also for every text message and data event. Traditionally, most call detail records do not capture the cell site or sector used during text messages or data events such as voicemail and email notifications. These are not phone calls so the cellular service providers have no motivation to capture the information. PCMD is captured anytime there is a connection or data event between the cell site and the mobile device.

PCMD data has both quality assurance and location based marketing information applications and is already built into the existing cellular infrastructure. Subsequently, PCMD is able to provide relatively accurate location based information. Is it accurate as GPS? No way. But it does add a dimension when combined with other information such as the cell site and sector. PCMD is not going to magically locate someone's handset but it is going to provide investigators clues which they might not otherwise have.

Now for the bad news. PCMD is only found in Alcatel-Lucent cell site products on code division multiple access (CDMA) networks. CDMA coverage in the United States is approximately 50% of the market but not all CDMA providers use Alcatel-Lucent equipment. Currently, PCMD is made available to law enforcement pursuant to proper legal request or exigent circumstances on the Sprint-Nextel and Verizon Networks only. In theory, it should be available from any cellular service provider using Alcatel-Lucent equipment on a CDMA network. Unfortunately, only those two providers acknowledge the information is available and are able to extract it for law enforcement use.

Here's some more bad news. PCMD is extremely perishable information. It appears the data may only be available for 7-14 days. This is not something that is going to be routinely preserved with the receipt of a preservation letter pursuant to 18 USC 2703(f). If your suspect or victim is using one of the two providers who acknowledge their ability to

collect and retrieve PCMD, you must request the information as quickly as possible. I have seen PCMD data which was much older than 14 days but it was extremely sporadic and would not be useful in most criminal investigations.

Another limitation of PCMD which falls into the bad news category is that it is not real time information. The data is collected at the switch level and then updated to a call file hourly. Again, this is not done in real time so there will be a delay between when the information is captured and recorded and when it available for review.

PCMD records a tremendous amount of information. It does not come to you nicely formatted and with a cheat sheet for easy interpretation. Because there is no documentation it can be very easy to become confused by PCMD data. You may need to get the assistance of a cell site engineer or an electronic surveillance specialist in order to make sense of it. Fortunately, Verizon translates this information for you during exigent circumstances requests and will be able to tell you the distance, measured in meters, between the handset and the cell tower.

Verizon

PCMD is routinely provided to law enforcement officials pursuant to exigent circumstances requests, such as in missing persons cases, by Verizon. They refer to it as Real Time Data (RTD). However, they do not provide RTD/PCMD during routine requests, such as court orders and search warrants. This may be due to the fact that exigent circumstances requests are handled through the electronic surveillance division of Verizon, the people who provision wiretaps and pen registers, and not through the subpoena compliance department. You must specifically ask for RTD/PCMD in your court orders, subpoenas, and search warrants or you will not receive it.

Sprint

Sprint offers its L-Site service to law enforcement officers. This allows an investigator to activate the GPS positioning feature of a targeted device on demand. Consequently, many investigators forget about the availability of PCMD data from Sprint. As with Verizon, if you do not specifically request PCMD from Sprint, you will not receive the information.

Caller ID Spoofing

Caller ID spoofing is the use of technology to cause a telephone network to display a number on a receiving phone's caller identification (caller ID) system which is not in fact the true originating phone number.

There are a variety of technological methods for spoofing caller ID but the advent of voice over internet protocol (VOIP) systems have made spoofing easy and inexpensive. The most common method for spoofing caller ID is to use a subscription based service or a web based interface. Anyone can purchase a number of prepaid spoof minutes from a variety of internet based providers. These minutes are similar to a calling card and the purchaser is assigned a PIN number and an access number. The user then contacts the access number from any landline or mobile phone, enters their PIN number, enters the phone number to be called, followed by the phone number they want displayed. Some services offer additional features such as voice alteration and recordings of the calls emailed to the user at the conclusion of the call.

Caller ID spoofing has been used by criminals in a variety of harassing and stalking type crimes. Several high profile instances involving caller ID spoofing involved making 911 calls to report false crimes in order to elicit a high profile response from law enforcement. The action has been coined 'SWATing'. According to published report numerous instances of SWATing have resulted in tactical units responding to reports of violent crimes only to find unsuspecting subjects who have been victimized by this 'prank'.

In order to understand how caller ID spoofing works, you must understand what is transmitted when you make an outgoing phone call. When you make an outgoing phone call a packet of data is transmitted which contains the following data fields:

ANI (Automatic Number Identification)-ANI is the phone number you called from

ANI II (Automatic Number Identifier II)-ANI II is a two digit code containing information about the type of phone number you called from such as landline, coin operated payphone, correctional institution, mobile phone, etc.

CPN (Calling Party Number, also sometimes referred to as CID-Caller ID, CLID-Calling Line Identification, and/or CNID-Calling Number ID)-This is also the phone number you are calling from. However, the data in this field is able to be manipulated unlike the ANI.

CPN data is designed to be manipulated for a number of legitimate reasons. For example, CPN data contains a marker which designates if the calling number is private or can be displayed. If the number is flagged as private, the system displays 'PRIVATE' in lieu of the number. CPN data is also changed on outgoing phone numbers originating from a private branch exchange (PBX) used by a private office or organization. Many law enforcement organizations use a PBX which displays a general outgoing phone number and not the desk number of the originating officer or investigator.

Caller ID spoofing takes advantage of the ability of CPN information to be manipulated and changed. Using voice over internet protocol (VOIP) technology, caller ID spoofing providers can change the CPN data to display the data entered by their customer.

Costs for these services vary depending on the total number of minutes, also called credits, purchased. One popular internet vendor offers plans consisting of anywhere from 25 credits for $4.95 to 2,500 credits for $299.95. A credit is

equal to one minute of talk time and five credits for a spoofed text message. Payment is as easy as entering your credit card number or using PayPal.

Some law enforcement agencies have explored using caller ID spoofing in their investigations with mixed results. There are a number of drawbacks for using caller ID spoofing during law enforcement investigations. Some agencies have reported running out of minutes or credits in the middle of a call which caused them some obvious difficulties. The other challenge involves returned calls. If the spoofed call is unanswered, attempts to return the call to the spoofed number may reveal that the phone call did not actually originate from that number.

The Truth in Caller ID Act of 2009

In December 2010 the President signed the Truth in Caller ID Act. The Act makes it a federal crime "…to cause any caller identification service to knowingly transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value…" This law is a watered down version of other legislation which would have essentially stopped caller ID spoofing. Violators of this law face the possibility of fines for every instance they misuse caller ID. There is an exception in the law for law enforcement officers conducting "any authorized activity." Unfortunately, many of the caller ID spoofing countries are based overseas and are not covered by this law.

Caller ID Spoofing Weaknesses

Caller ID spoofing suffers from a couple of weaknesses which can be exploited during law enforcement investigations. Since commercial caller ID spoofing services first started, the number of companies have dwindled and consolidated into a few large providers. These companies faced the possibility of prohibitive regulation in the Truth in Caller ID Act of 2009 and seek to avoid any further legal restrictions which may force them out of business. This may cause some of the larger companies to cooperate with law enforcement legal process requests. In fact, in some of the 'SWATing' stories discussed earlier, it appears those companies did cooperate with law enforcement investigations. However, somewhat complicating the issue is the fact that some of these companies are based in Canada. This would likely involve seeking assistance from the FBI Legal Attache for assistance in service of process.

Users of the VOIP service Skype have the ability to change the displayed number on caller ID systems. Cases involving Skype are notoriously difficult to investigate due to a variety of reasons including the fact they are based in the tiny country of Luxembourg. Skype does respond to law enforcement requests but they do not always capture information which may be relevant to an investigation. Skype does generate user logs on the host computer which can show calling activity using the service. If a suspect in a caller ID spoofing case is known or believed to be using Skype, a forensic examination of their computer may reveal evidence contained in the activity log which can assist in prosecution.

Another vulnerability of caller ID spoofing is that it is not feasible, at this time, to alter the ANI. As discussed earlier caller ID spoofing changes the CPN but the underlying ANI remains unchanged. This is one reason why calls to 911 public safety answering points (PSAPs) still reveal the incoming call, even when the caller ID blocking in enabled.

The ANI is also accessed when calls are made to toll free phone numbers such as 800 numbers. As the owner of the toll free line is paying for the phone call, they are entitled to see the underlying phone number.

The ability of toll free numbers to reveal the ANI is the basis for the service known as Trap Call. Trap call is a service offered by one of the major caller ID spoofing companies. Trap Call offers users a subscription service which allows the user to reject unknown or caller ID blocked incoming calls. Those rejected calls are then routed to Trap Call's service which is, in essence, an enhanced toll free number. The call is then routed back to the subscriber's phone which can be answered or sent to voicemail. Trap Call then sends the subscriber a text message which contains the ANI of the incoming call. Trap Call also offers a premium service which offers the subscriber the added feature of running the incoming phone number through public records databases for subscriber information, digitally recording and transcribing incoming conversations, and creating black lists of prohibited incoming callers.

Trap Call does not work with all cellular service providers. According to their website, Trap Call only works with AT&T, T-Mobile, Verizon, and Sprint. Many of the prepaid providers such as Metro PCS and Boost are not supported. Trap Call also has applications which can be installed on phones using Blackberry, Apple, and Android operating systems.

I learned about Trap Call first hand during a wiretap investigation. The case agent in the investigation had the main suspect under surveillance. In order to confirm the suspect was still using the phone number which was the target of the pending wiretap, the case agent made a phone call to the suspect using his department issued phone. The suspect was observed answering the phone and the surveillance was terminated. Several minutes later the case agent received an incoming call from the suspect asking why he had called him. The case agent was able to convince the suspect he had dialed the phone number in error but was unable to figure out how the suspect had obtained his caller ID blocked law enforcement mobile phone number. It was not until the wiretap was operational that we were able to see the incoming text messages from Trap Call regarding the unblocked incoming calls.

Most government agencies obtain their cell phone contracts under a broad umbrella contract by city, county, or federal entity. Fortunately the suspect in the above case did not have the public records check feature which would have likely indicated the subscriber of the phone was the State of California. Even if the records check did not reveal the name of the investigative agency, it would have seriously hampered the investigation if the suspect became concerned and dropped his phone.

Trap Call has some obvious advantages for law enforcement investigators. However, I see no reason why we should patronize a company which also offers caller ID blocking services and thrives by allowing criminals to mask their identities. The Law Enforcement Telecommunications System from Orion Systems offers the same services, among many others. They are also heavily involved with a number of local, state, and federal law enforcement agencies in a wide variety of investigations. Consider Orion Systems before shelling out personal or department money to a caller ID spoofing company.

iPhone/iPad/iPod touch Backup Files

An iPhone synchronizes (synchs) with an authorized computer which has iTunes on it every time it is plugged in, unless the user interrupts the process. Connecting to an internet enabled computer is also required in order to download larger applications and files although this connection may be wireless or through a data cable. The synching process creates a backup file on the computer which is designed to allow a user to reinstall their contacts, text messages, calendar entries, photos, videos, and application data in the event their phone is damaged, malfunctions, or is lost or stolen. By default, iTunes stores the backup file created during the synch process in set locations based on the underlying operating system. For this book, we are presuming the majority of readers are using a version of Windows operating system. The location of the iPhone backup file generated by iTunes is as follows:

For computers using Windows XP:

\Documents and Settings\USERNAME\Application Data\Apple Computer\MobileSync\Backup\

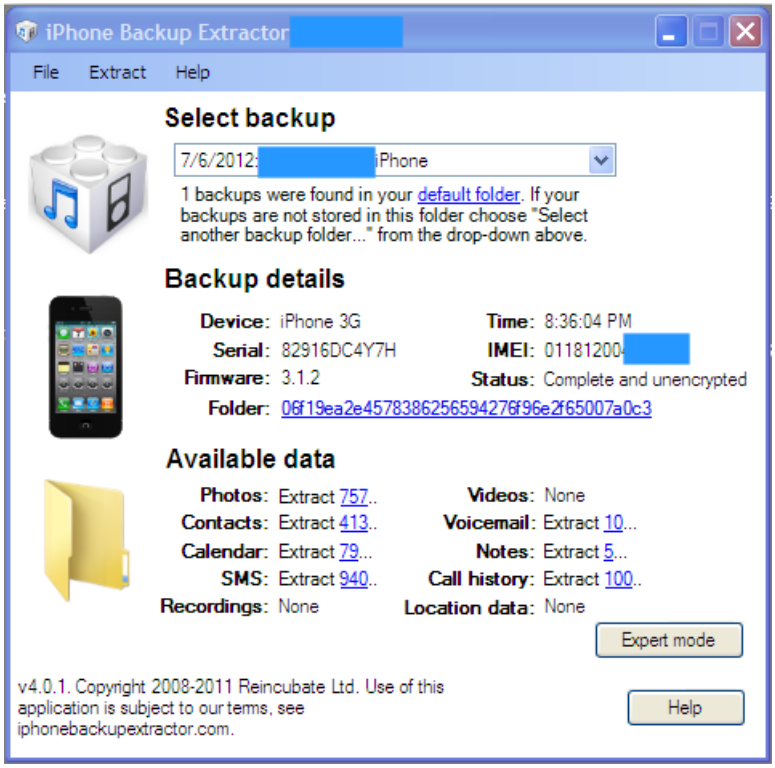
For computer using Windows Vista or Windows 7:

\Users\USERNAME\AppData\Roaming\Apple Computer\MobileSync\Backup\

Replace USERNAME with your personal account/computer name.

Running the Program

After purchasing, install and run the program. It will automatically detect the version of Windows installed on your computer. It will also detect multiple backups from different devices on the same computer so it is possible to run the software on a computer where multiple people synch their Apple devices to.



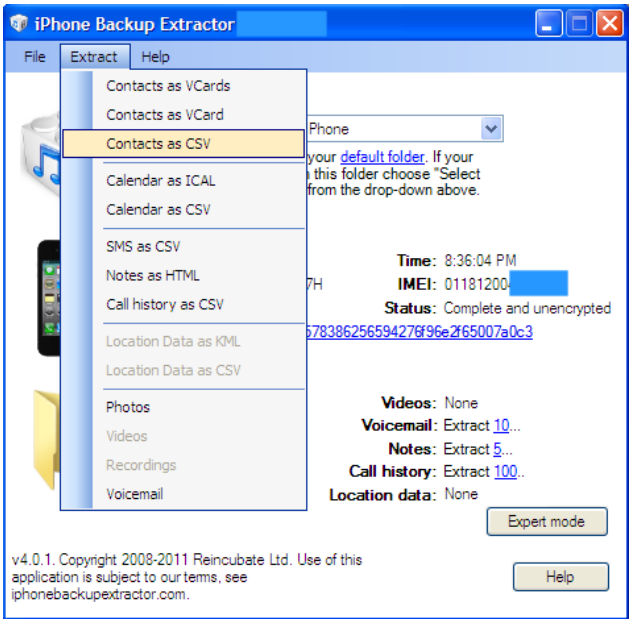
Simple Mode

Simple mode is the easiest method for viewing the contents of an iPhone backup file. From the simple user interface you can check the photos, videos, and image files, the contacts/electronic phone book, voicemail messages stored which were stored on the phone, calendar entries, notes, text messages, call history, and possibly location data. In order to view the data in any of these files, simply click on the blue underlined number after the entry. If there is no blue underlined entry then there is no data for that field. Clicking on an underlined number will open a dialog box which states **Browse for Folder**. This is asking you where you want to save the information from the backup file. For ease of use, it is probably best to place the files somewhere easy to find such as the desktop. You can create a special file to store everything by clicking **Create New Folder** and naming it whatever you want. Alternately, you can right click on your mouse button, select **New**, and then **Folder**. This will create a new unnamed folder for you to store the files in.

Before you start clicking madly away at the blue underlined numbers, there is some important information about the software's preferences which you must understand. By default the iPhone Backup Extractor will transfer information in certain predefined formats. For example, if you select Contacts by clicking the blue underlined number the program will automatically export every contract as a vCard. A vCard is an electronic business card format which can be attached to e-mail messages or exchanged via text messages. vCards commonly contain information such as name, address, phone numbers, e-mail addresses, web site addresses, and sometimes, photographs or graphics files. While this is a convenient way to store and share information from the Contacts backup file, it doesn't show us all the information we want to see.

Extract Contacts

A better way to extract and view the contents of the Contacts file using the iPhone Backup Extractor is use the option found in the **Extract** menu to place the contacts into **CSV format**. CSV stands for Comma Separated Value and is one of many formats used to view information in Excel. A vCard can only be opened using Microsoft's Outlook e-mail. An advantage to using the export to CSV function instead of using the default export to vCard function is the loss of some precious information. When the vCards are exported they are automatically sorted alphabetically. When the contacts are exported using the export to CSV function the contacts are sorted in a hybrid format which can show which contacts were added recently. For example, when looking at the results of the contacts exported in the CSV formats you may see that not all of the contacts are sorted alphabetically. This may show which contacts were stored chronologically and show which ones were added recently. You will not be able to see that in the vCard format because of the way they are extracted. Groups of contacts with no phone number, but only an email address, are those contacts which were automatically added to the file when the user responded to an email. Again, these are chronologically and not alphabetically. So the most recent contact with only an email address stored was one of the most recent contacts the user responded to an email from. This does not mean it was the last email they sent, only that when they responded to the email it was not already stored in the phone. Because they responded to the email, the iPhone automatically added them as a contact.



Calendar

Calendar entries should be viewed using the same technique as the Contacts file. Instead of clicking on the blue underlined numbers next to Calendar, you should use the **Extract** button in the menu bar to view them as a **CSV file**. Otherwise, the calendar entries will be extracted as an iCal file. iCal is a calendar function for Apple manufactured devices. For ease of use, it is best to export the calendar function as a CSV file.

The exported field will include the summary of the event entered by the user, the location, any additional description, the start and end date and time, the time zone, and whether the event was scheduled to be all day long.

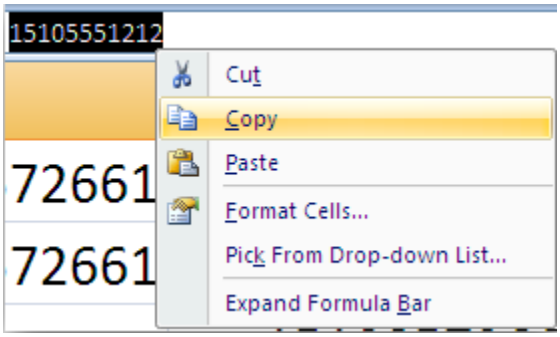
Summary	Location	Descriptic	Start date	End date	Time Zone	All Day	Frequency
New Event			5/24/2012 13:00	5/24/2012 14:00	US/Pacific	FALSE	OneTime
Bridal shower			6/2/2012 19:00	6/2/2012 20:00	US/Pacific	FALSE	OneTime
Jack and Robyns			6/16/2012 19:00	6/16/2012 20:00	US/Pacific	FALSE	OneTime
MD appointment			6/4/2012 13:00	6/4/2012 14:00	US/Pacific	FALSE	OneTime
Dentitst Appointment			6/25/2012 12:00	6/25/2012 13:00	America/Los_Angeles	FALSE	OneTime

SMS/Text Messages

SMS is an acronym which stands for Short Messaging System which you probably know by the name text messages. The iPhone Backup Extractor will automatically download all text messages which were on the device when it was last synched with the computer. Unlike the Contacts and Calendar fields you do not need to use the Extract tab to get the messages into CSV format. Simply clicking the blue underlined number will download a spreadsheet with all of the text message content, the sender, and the date/time the message was received.

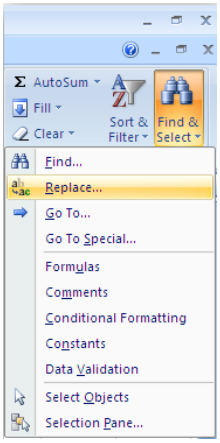
Unfortunately, the spreadsheet will only list the phone number the messages was sent from and it does not automatically fill in the name from the Contacts file. The spreadsheet also lists each text message separately and it does not show the conversation in a single step like you might be used to seeing on your phone. In order to match the name with the phone number you may have to switch between the Contacts spreadsheet and the SMS spreadsheet in order to make sense of who said what to who. Any easy way to do this is to use the **Replace** function found in the **Find and Select** feature in the Home screen of Excel.

1) Find the phone number you want to replace with the contact name. Click in the cell or box and highlight the phone number. In order to copy the phone number you can either click the right mouse button and select **Copy** or press the **Control (CTRL) button** and the **C key**.

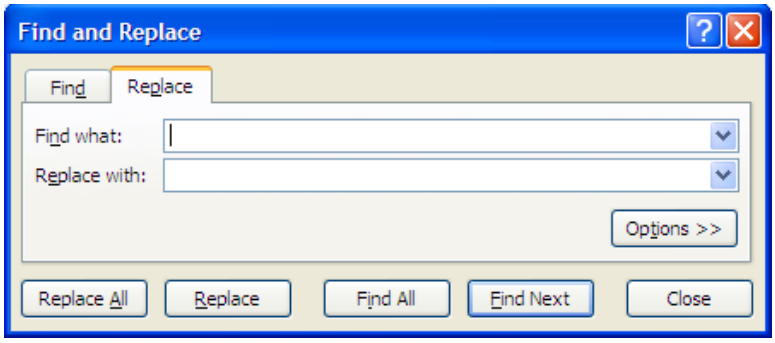


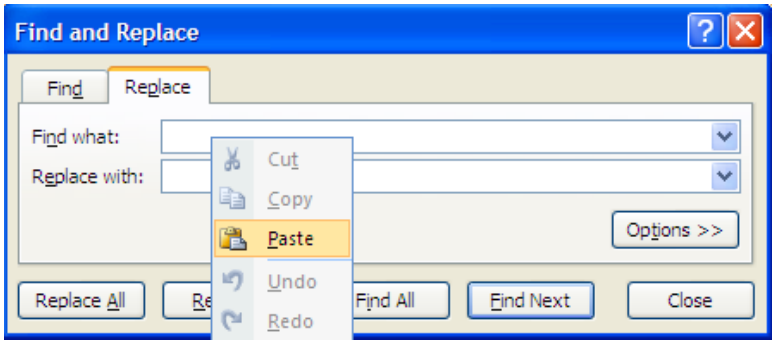
2) Highlight the columns which contain the phone numbers you want to replace with the name of sender or receiver. This will be the first two columns in Excel labeled From and To. In order to select both columns at the same time hold the **Control (CTRL) button** while using the **left mouse button** the click on the From and To columns.

3) Select the **Find and Select** button and drop down to the **Replace** function.



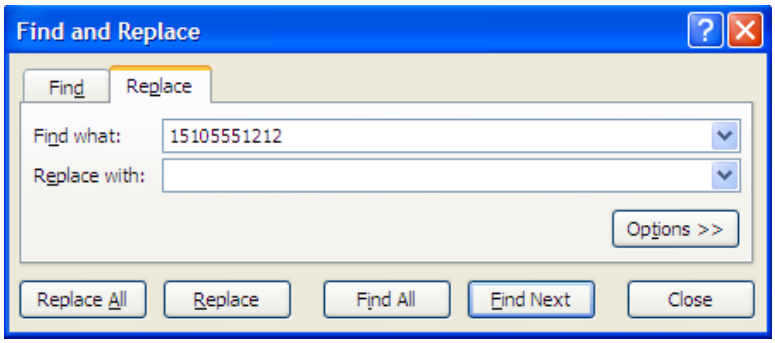
4) Click inside the box that says **Find What:** and either **right click** and select **Paste** or press the **Control (CTRL) button** and the **V key** to paste the phone number.

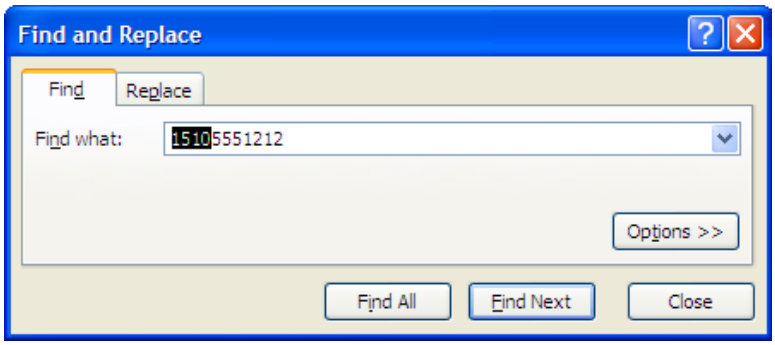


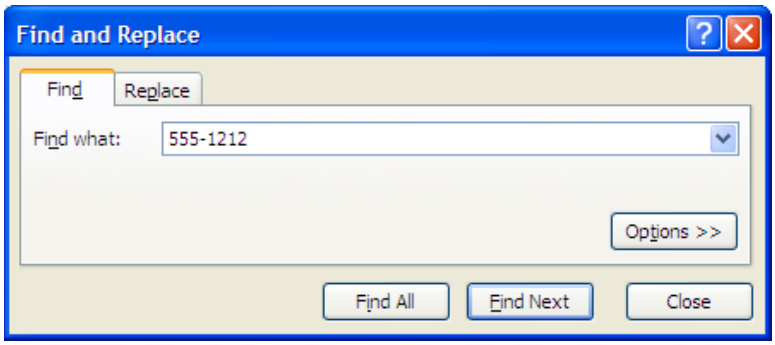


5) Open up the Contacts spreadsheet and find the name associated with the phone number. You should know that the phone number stored in the Contacts file is not always the same as the phone number in the SMS file. The SMS file contains the full eleven digit phone number, including the number 1 before the area code, and it is in a different format than the phone numbers stored in the contacts file. The phone numbers in the SMS file appear as 15105551212 while the phone numbers in the Contacts are formatted as (510) 555-1212. In order to find the phone number and the contact name you will open the **Find and Select** function again. Instead of Replace, you will select the **Find** tab. The phone number you entered should still be there but because it may be stored in a different format you should search for the last seven digits of the phone number, such as 5551212. Highlight the first four digits, the number 1 and the area

code, and delete them. You will also need to put a dash in between the prefix, the first three numbers, and the last four numbers of the phone number. Now you can search for the name associated with the phone number.

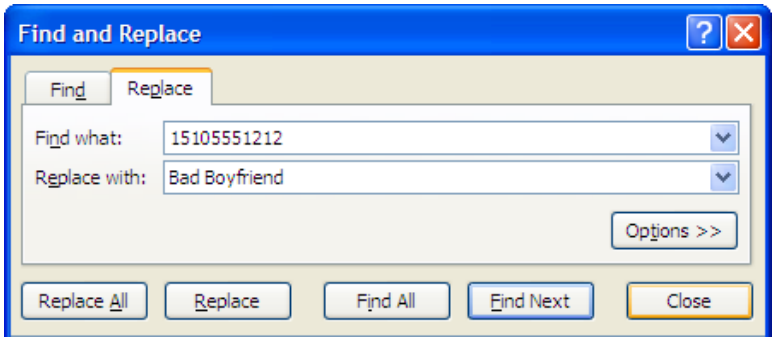






6) Select **Find All** in the **Find and Replace** box. Excel will automatically highlight the phone number with a black box around the number.

7) Go back to the SMS worksheet and replace the phone number with the Contact name using the **Find and Replace** function. The phone number should still be there but it will be in the seven digit format you changed it to in order to find the contact. Put the full eleven digit phone number in the Find What box without using the dash (for example 15105551212). Place the Contact's name in the **Replace With** field.



8) Press the **Replace All** button and all of the phone numbers in the From and To columns will be replaced with the Contact's name.

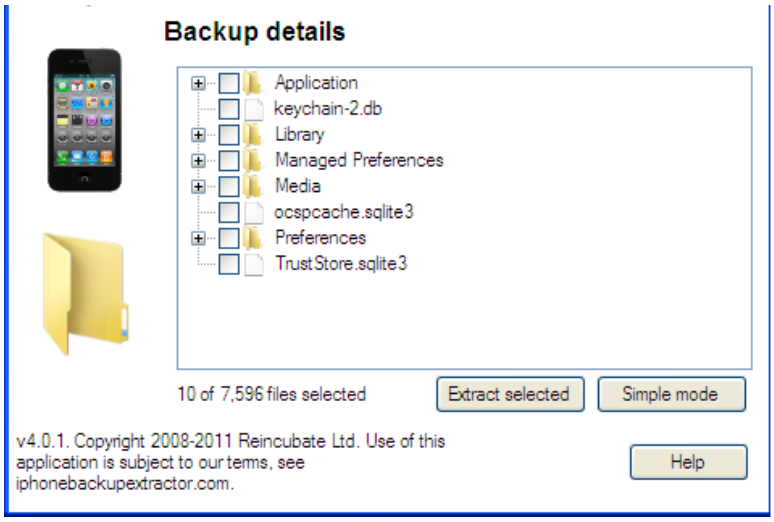
Deleted Text Messages

The iPhone Backup Extractor cannot retrieve text messages if they were deleted prior to a backup of the phone being made by iTunes.

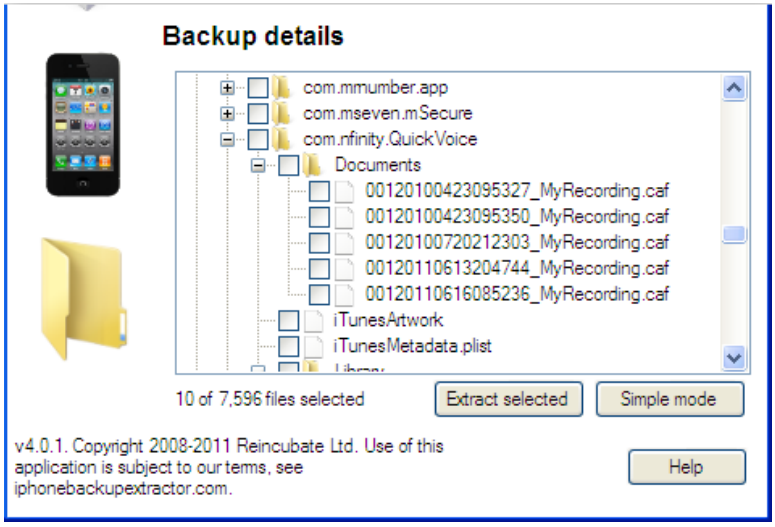
Recordings

Recordings are sound files created using the Apple application. For a variety of reasons, this application is not frequently used and is commonly replaced by other sophisticated applications from the iTunes store. If there are no recordings listed in the Simple Mode of the iPhone Backup Extractor, you may have check the Expert Mode to see if there are any other applications which may be used to record voice memos or conversations.

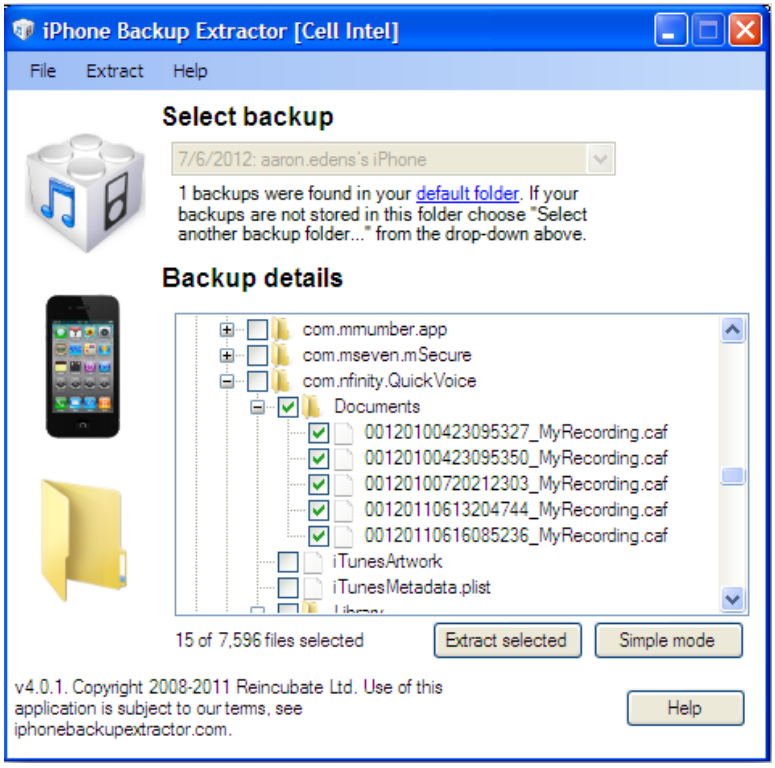
Click on the **Advanced Mode** button on the iPhone Backup Extractor.



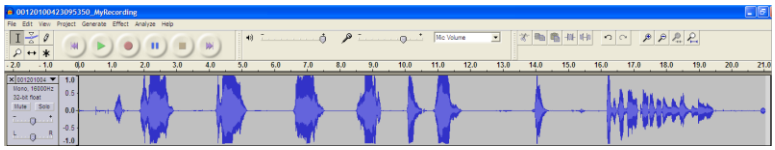
Next to the word Application should be a small **+ symbol**. Clicking that expands the tree and allows you to view all of the applications installed on the phone. This can be an eye opener by itself. In order to see if there are any other applications which may have been used to make voice recordings you will have to examine each application individually. Some of them are pretty self explanatory such as Angry Birds. But others may require you to search Google or iTunes to see exactly what the application is or does.



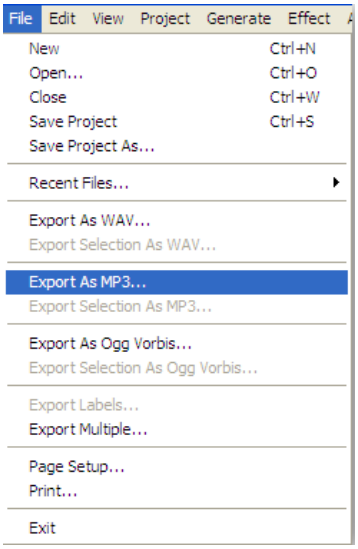
In this example you can see we have discovered an application called Quick Voice. By clicking on the **+ symbol** next to the application name we open up a tree which includes a file entitled Documents. Inside the Documents file are several files labeled myrecording.caf. .caf files stands for Core Audio Format which is a file type developed by Apple to overcome some limitations in older audio file types.



To recover these files, place a **check mark** in each box. Clicking in the box above the files will automatically select all of the files below it. Next press the **Extract Selected** button and navigate to where you want to extract the files to.

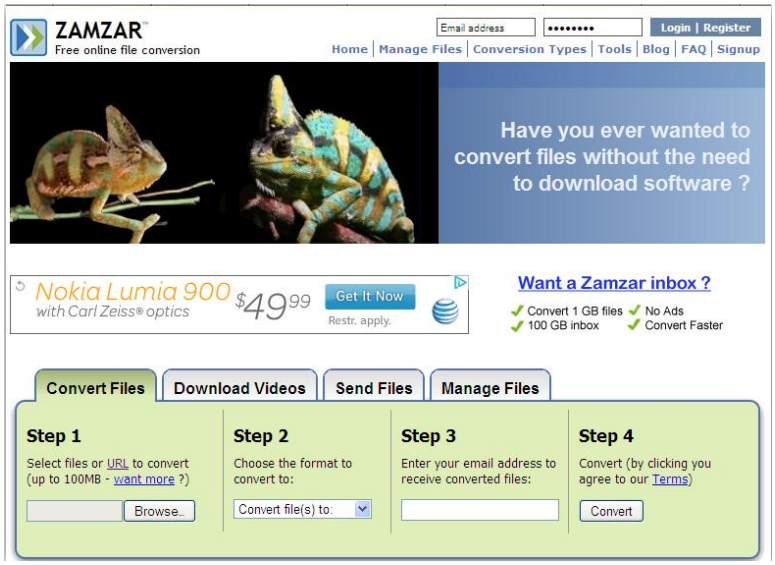


In most cases you will need to either download software to play the software or using an online service to convert the software to a format which can be played from your computer. Apple's QuickTime Player allows you to play many types of audio and video files associated with their products but in order to save them into a more universal file type you are required to purchase the upgraded version of the software. You can download the software from http://audacity.sourceforge.net/. Follow the prompts to install the software. When you are finished open the software and select **Open** from the **File** tab. Press the green triangle button to play the recording. If you decide you need to save the recording as a file type that can be shared with and listened to by others, such as law enforcement, you can easily convert the CAF file into something more user friendly. Simply select Save As from the File tab and you can save the file as an MP3 or WAV file, two of the most common media formats.


File
Edit
View
Project
Generate
Effect
New Ctrl+N
Open... Ctrl+O
Close Ctrl+W
Save Project Ctrl+S
Save Project As...
Recent Files...
Export As WAV...
Export Selection As WAV...
Export As MP3...
Export Selection As MP3...
Export As Ogg Vorbis...
Export Selection As Ogg Vorbis...
Export Labels...
Export Multiple...
Page Setup...
Print...
Exit

Videos

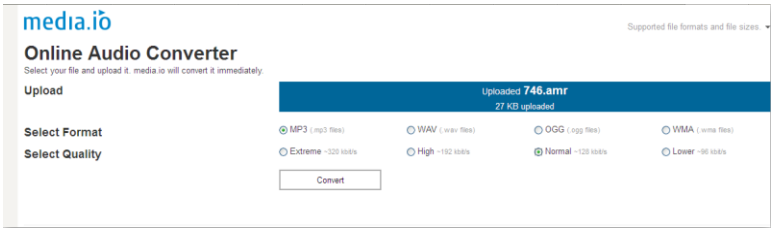
Video files taken with an Apple device are typically saved as 3GP and 3G2 formats. These are usually playable by most video players including QuickTime but, as with audio files, you may need to convert them into something more user friendly. There are a couple of ways to do this including installing software such as Format Factory or VLC Media Player which will allow you to play and convert video files between any number of common formats. In order to expose you to a wide array of tools, I'd like to introduce you to Zamzar.



Zamzar is a free online media conversion service which works on a large number of document, audio, and video file formats After agreeing to the terms by clicking the Convert button a link will be emailed to you. This can sometimes take a few minutes so don't worry. From the email you will be able to download and save the converted file. If giving out your email address or uploading a video file containing possible evidence on it still causes you concern try using one of the free software programs such as Format Factor or VLC Media Player. Format Factory is a straight conversion utility which changes the file type from one video file to another. VLC allows you to play the video and then Save As a different file type.

Voicemail

Not many people know the iPhone is one of the only phones on the market which stores incoming voicemails on the device itself. Most voicemail messages are stored on the computers of the cellular phone company and requires the user to call in to the network in order to retrieve their messages. This means that all voicemail messages which are stored on the phone at the time it is synched with an authorized computer can be retrieved and listened to. In order to give you the widest variety of tools in your investigative toolbox, I'm going to recommend you try using an online conversion service found at http://media.io/.



The service is quick and free although it does seem to want me to go to Amazon and look around. In order to use the service simply navigate to the file you want to convert, upload it, and decide on the format you want to download it as.

Call History

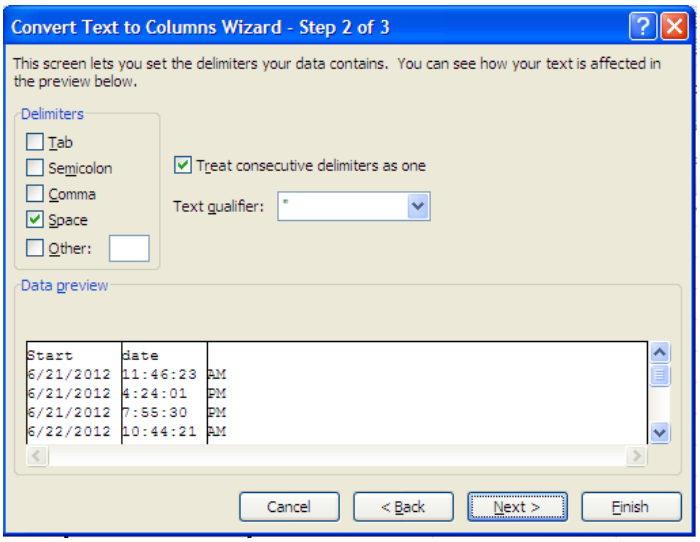
The iPhone Backup Extractor is only able to retrieve 100 of the most recent dialed or received callsand this appears to be one of the only drawbacks to using the iPhone Backup Extractor.

	A	B	C	D	E
1	From	To	Start date	Duration	
2	9.25E+09	Me	########	0h 00m 34s	
3	9.25E+09	Me	########	0h 02m 158s	
4	9.25E+09	Me	########	0h 02m 148s	
5	5.1E+09	Me	########	0h 01m 67s	
6	9.26E+09	Me	########	0h 00m 00s	
7	9.25E+09	Me	########	0h 00m 00s	
8	Me	9.26E+09	########	0h 10m 633s	
9	8.01E+09	Me	########	0h 00m 00s	
10	Me	5.11E+09	########	0h 01m 66s	
11	9.25E+09	Me	########	0h 03m 236s	
12	4.15E+09	Me	########	0h 00m 00s	
13	Me	9.25E+09	########	0h 00m 35s	
14	Me	4.15E+09	########	0h 10m 607s	
15	9.25E+09	Me	########	0h 01m 95s	

The files are automatically downloaded into CSV format when you click the blue underlined number. However, you may see some data which does not make sense or which does not even appear. Never fear, there's an easy fix for that. When the files are downloaded into the Excel spreadsheet and exceed the length of the cell or box, the program automatically reduces the number in size. The simple fix is click on the far right side on the column which contains the data. You should see a solid black line with an arrow on either side of it. By **double clicking** you will automatically increase the size of all of the cells to accommodate the length of the information contained in the field.

	A	B	C	D	E
9	8E+09	Me	6/22/2012 13:53	0h 00m 00s	
10	Me	5.1E+09	6/22/2012 17:11	0h 01m 66s	
11	9.3E+09	Me	6/22/2012 17:43	0h 03m 236s	
12	4.2E+09	Me	6/22/2012 21:34	0h 00m 00s	
13	Me	9.3E+09	6/23/2012 11:44	0h 00m 35s	
14	Me	4.2E+09	6/23/2012 14:34	0h 10m 607s	
15	9.3E+09	Me	6/23/2012 14:50	0h 01m 95s	
16	Me	1.5E+10	6/24/2012 14:09	0h 07m 467s	

In order to correlate the phone number and a with a name from the contact list you first need to right click on the Duration column so the entire column is highlighted in blue. **Right click** and scroll down to **Insert** which will place a blank column in between the Start Date and Duration column. Do this again so you have two blank columns. Select the **Start Date** column so that the entire column is highlighted in blue and then select the **Data** tab at the top of the screen. **Select Text to Columns** and then **Delimited**. Make sure the box next to **Space** is checked-this may require you to uncheck Tab or another field. Select finish and you will find the dates and times are now separated.



Select the button on the left side of the worksheet that contains a **triangle** or press **Control (CTRL)** and the **A key** to highlight the entire page. Go back to the **Data** tab and select **Sort**. **Sort** by AM/PM and then time and you will be able to see what time the last 100 phone calls were made or received.

Another important consideration is the Duration of the phone calls. It can be pretty important to see who your target communicated with the longest. Make sure to examine any lengthy phone calls by sorting by the Duration column as well.

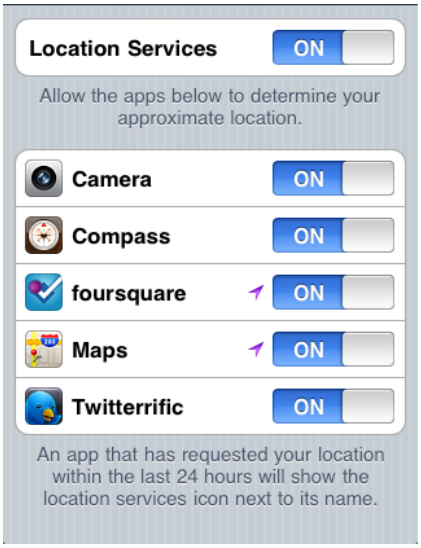
Me	4.2E+09	6/23/2012 0:00	2:34:33	PM	0h 10m 607s
Me	9.3E+09	6/22/2012 0:00	12:08:27	PM	0h 10m 633s
Me	4.2E+09	7/1/2012 0:00	4:06:52	PM	0h 11m 688s
Me	9.3E+09	6/27/2012 0:00	11:19:48	AM	0h 12m 723s
Me	5.1E+09	6/25/2012 0:00	10:29:40	AM	0h 15m 927s
Me	2.1E+09	7/2/2012 0:00	5:21:12	PM	0h 16m 974s
Me	1.9E+10	7/2/2012 0:00	6:47:38	PM	0h 17m 1077s

When you examine the Duration column you might find information which does not make sense. In this example you can see the highest duration call is listed as 17 minutes and 1077 seconds. You are seeing the same data reflected in two different formats. The most accurate way to view the call is to look at the seconds and then divide by 60.

Location Data

You may remember when the story broke in 2011 about the secret cache of location data Apple's products were storing. The media attention was furious and probably overblown but it caused Apple to make changes in the data it stored. When Apple introduced it's operating system upgrade version 4.3.3 they limited the quantity of data stored to about a week and stropped storing location information altogether in future backups. If you never had a chance to look at the data, it wasn't as scary or intrusive as initially portrayed. The location information was frequently inaccurate and was

used purely for application and services installed on the device. You should view the location data obtained by the iPhone Backup Extractor cautiously as it can be very, very inaccurate.

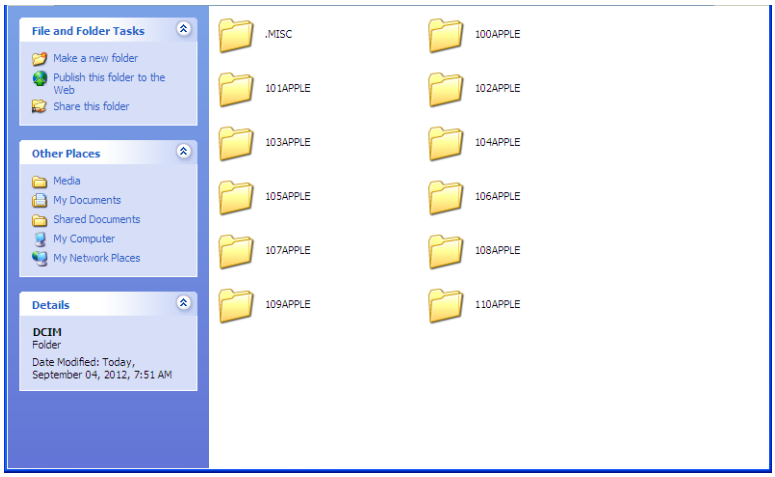


If you are concerned about location data being stored on your, or your family's phone, you can turn the services off by going into Settings and then Location Services. The Location Services are turned on by default but you can turn it off if you don't want to use this feature. You can also individually control which application have access to Location Services information. However, if you turn Location Services off, you'll need to turn it on again the next time an application attempts to use the feature such as when looking up a location in the maps application.

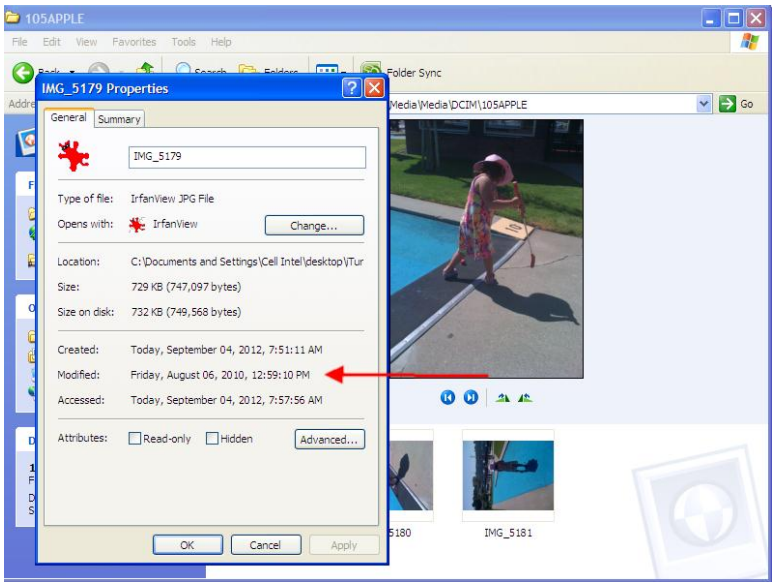
Photos

Photos can be some of the most telling and important things an investigator looks at in our target phone backup and the iPhone Backup Extractor offers an easy way to recover the digital images stored on the phone. Simply click on the blue underlined number and direct the software to the file you want to recover the images to.

This is one of the few processes which can take a long time with the iPhone Backup Extractor so be patient. You will see small green squares covering the icons on the phone in the main screen to show you have far and how fast it is progressing. Using a test database it took about two minutes to download 757 images. Your results should look like this:

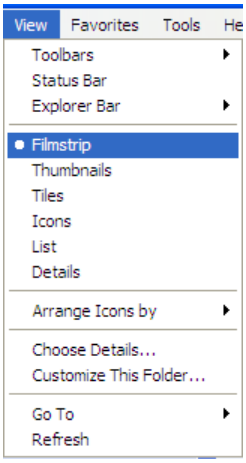


While the images themselves can be important, there is additional information contained in the image which can be important for investigators. By right clicking on any image and scrolling down to Properties you can see the date and time the image was created, modified, and last accessed. In this example you can see the dates and times the file was created is listed as the date the iPhone Backup Extractor was run and the image files recovered. The modified data and time is closer to the actual date and time but does not necessarily show the actual date and time the image was made. If your target used any applications to modify the image, such as adding effects or cropping the image, the modified date and time will be different than the actual date and time the image was taken.

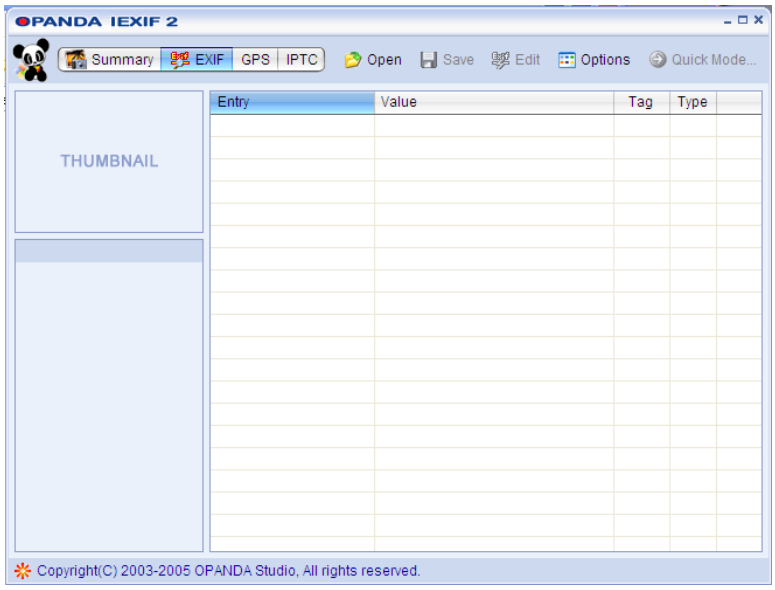


In order to get the true data and time an image was taken, as well as additional information such as the GPS (Global Positioning System) coordinates where the image was shot, we have to delve deeper into the file. Specifically we are going to be looking for EXIF data. EXIF data is sometimes referred to as data about data. More precisely it is data about the container information is stored in. Image files contain a ton of EXIF data which is not normally viewable by the user and can include the make and model of the camera or phone used to take the picture, the date and time the picture was taken, and, in some cases, the GPS coordinates where the picture was taken.

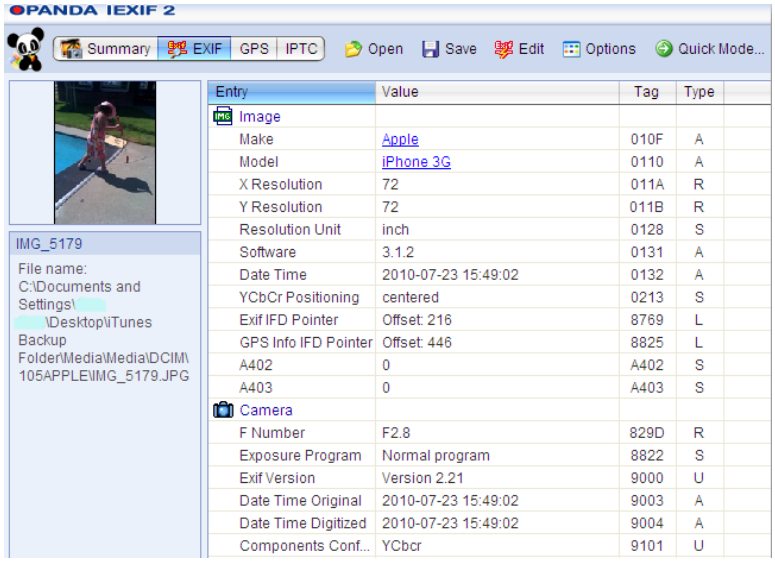
Before we begin you are going to need to know which image or images you want to examine. You may need to write down the file name and or the image name so you can come back to it later. The file the iPhone Backup Extractor saved the images to should will be named **Media**. Inside the Media file will be another Media file containing yet another folder named DCIM. DCIM stands for Digital Camera IMage and, depending on how many pictures your target took, will likely contain a number of other files labeled 100Apple, 101Apple, 102Apple, etc. These files are arranged chronologically so the file folder with the highest number will contain the most recent images. An easy way to scan all of the images in a folder is to select **View** at the top of the screen and then **Film Strip**. This will allow you to easily view all of the images in a folder and quickly identify any which need further investigating.



In order to view the EXIF data we are going to need to install yet another free software program. There are a number of EXIF reader programs available for free on the internet but the one I like using most is Opanda iExif which can be downloaded from http://www.opanda.com/en/iexif/. After installing the program double click the new icon on your desktop to open it. You should see this screen:



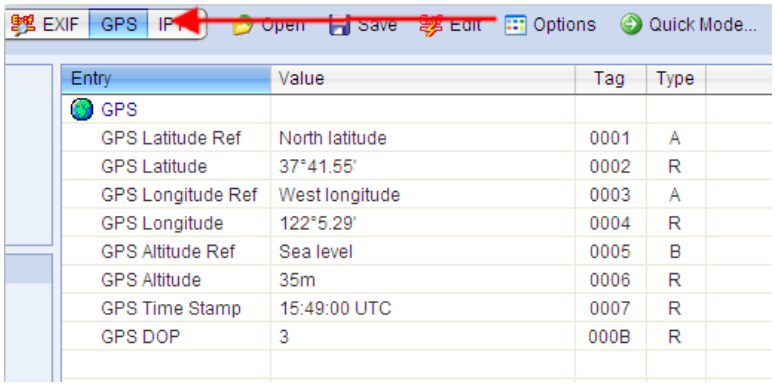
Select Open from the top of the Opanda program and navigate to the folder where you extracted the pictures to. When you have found the picture you are interested in click on it and Open it in Opanda. You should see a screen similar to this:



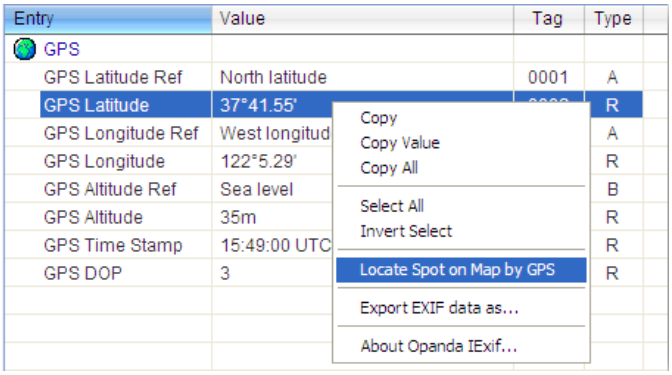
The data displayed on the right side of the screen includes some of the information we are looking for. In this example you can see the type of phone the image was taken on and the date and time it was taken. There is also additional data about the image but most of it is not really important at this point.

However, there is additional information contained in this image, specifically GPS coordinates where the picture was taken. Before we proceed you need to be aware of a couple of things. In order for GPS to be accurate, the Apple device must have the GPS feature enabled on it. Sometimes suspects turn this off. You should also know that in order for GPS to work accurately, the iPhone, iPad, or iPod Touch must be able to communicate with at least three satellites in orbit above the Earth. Sometimes, there are environmental factors which prevent the device from communicating with the GPS satellites which can lead to a lack of information or inaccurate positioning information. Remember, the GPS data can sometimes be off by a considerable degree.

In this example we can see the GPS data by clicking on the **GPS button** at the top of the Opanda software. If there is GPS data embedded within the image file it should appear something similar to this:



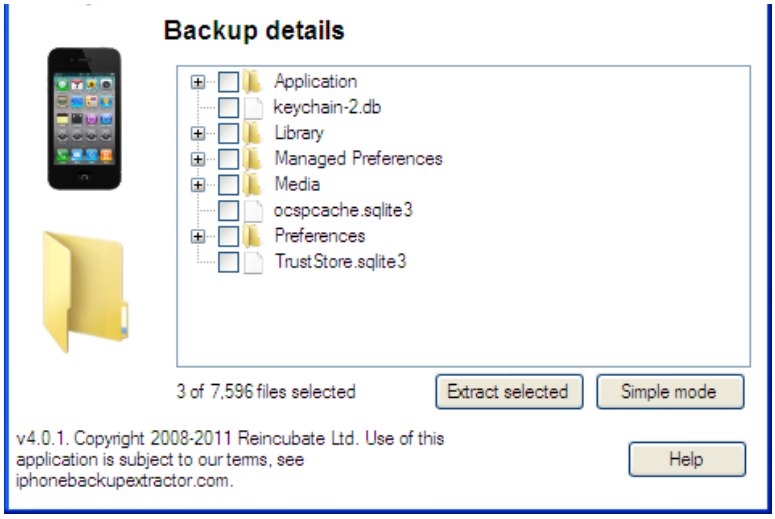
Opanda has made it very easy for us to view the location using Google Maps. Simply click the **right mouse** button over the latitude or longitude and scroll down to **Locate Spot on Map by GPS**.



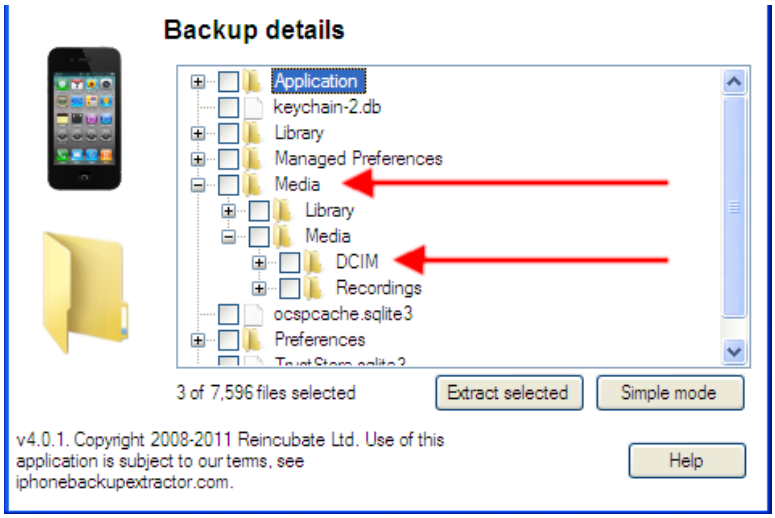
If you are connected to the internet this will automatically take you to the location on Google Maps, like so:

In this example the GPS coordinates are literally within feet of where the picture was actually taken from. Just remember not every GPS reading is going to be as accurate. I have seen GPS information taken from cellular phone pictures be off by as much as 1/2 mile.

One of the most common excuses suspects use for having pictures on their phone that they are not supposed to have is that the message was sent to them from a friend via text message (known as MMS or Multi-Media Message Service) or e-mail. Photos sent to an Apple device are stored in a different location than the DCIM folder. To find images which were sent via text message we need to look in a different place. In the Media folder where we found the Media subfolder and the DCIM files is another folder labeled **Library**.



By clicking on the **Library** folder we will drill down through folders named SMS (this means you are in the right place- SMS stands for Short Message Service, another name for text messages) and then a folder named Parts. Inside the **Parts** folder may be a number of subfolders. Each subfolder contains one or more media files, including pictures, which were sent or received as an attachment to a text message. Photos received via text message are downloaded to a different file. Depending on the operating system used by the Apple device received photos can either be found by entering the Expert Mode and clicking **Media**, then **PhotoData**, and then **100Apple** or by drilling down through Expert Mode to **Media** to **PhotoData**, to **MetaData** to **DCIM** to **100Apple**. Older operating systems lump photos received or sent from incoming and outgoing messages into the **Parts** file listed above.

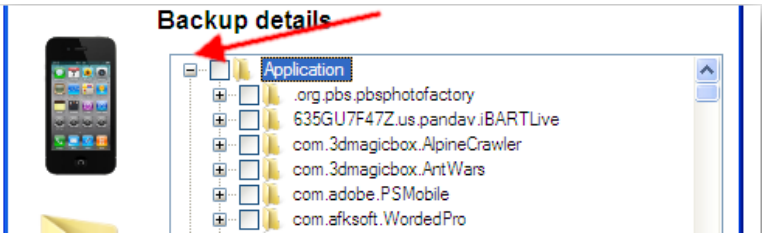


Here's the bad news. The EXIF data is partially removed from the picture when it is sent from one phone to another. For some reason Opanda and other software are not able to read the EXIF data from these images. You will have to right click on the image and select Properties in order to see that data the image was modified. Unfortunately, this may or may not be the date the picture was taken.

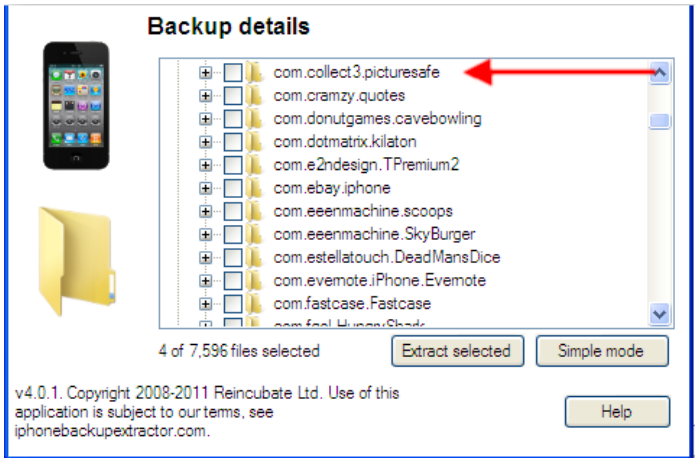
Expert Mode

Expert mode scares a lot of investigators from looking at the data. But there can be some important clues hiding in those files and we are going to find them. The files obtained using the iPhone Backup Extractor are not the full applications themselves, that would take up a lot of room and could possibly take hours to download. Instead, the recovered files contain the information stored inside the application or program. For example the data stored by the Angry Birds application contains the levels completed, scores, and achievements-not the actual files needed to play the game. Examining the information contained within the applications can be a real eye opener but you need to know what applications to spend time researching and investigating.

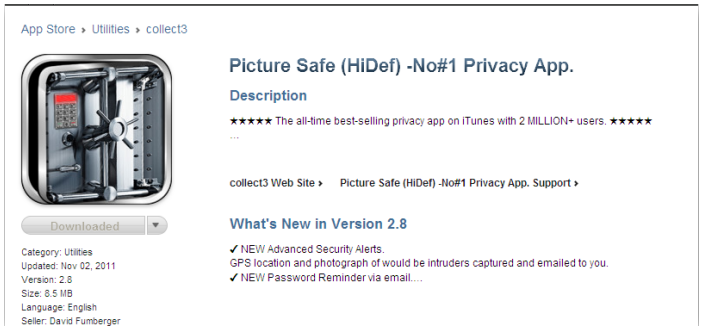
The first step is the enter **Expert Mode** and then select the **+ symbol** located next to Applications. This will populate a tree of every installed application.



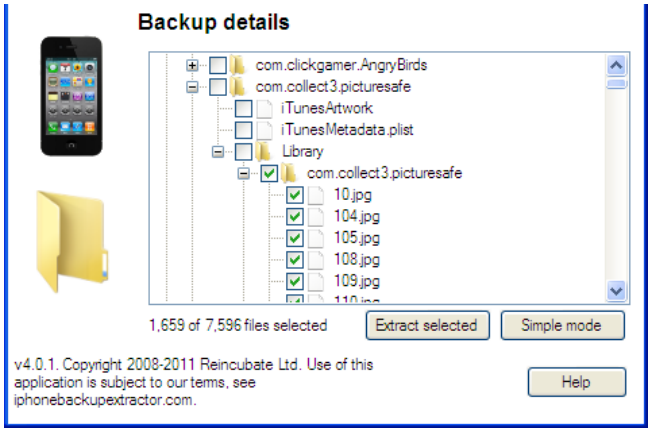
Each application is listed by their domain first (such as .com or .org) and then the developer's name followed by the name of the application. Pay attention to the application names and either check them in Google or from the iTunes store to see exactly what it does.



In this example we can see that PictureSafe is a password protected application for storing images.



If you find a suspicious application you can click on the **+ symbol** next to it to expand the sub tree and see what information is contained in the file. In this example you can see there are a number of .JPG files which are usually pictures or graphics files.



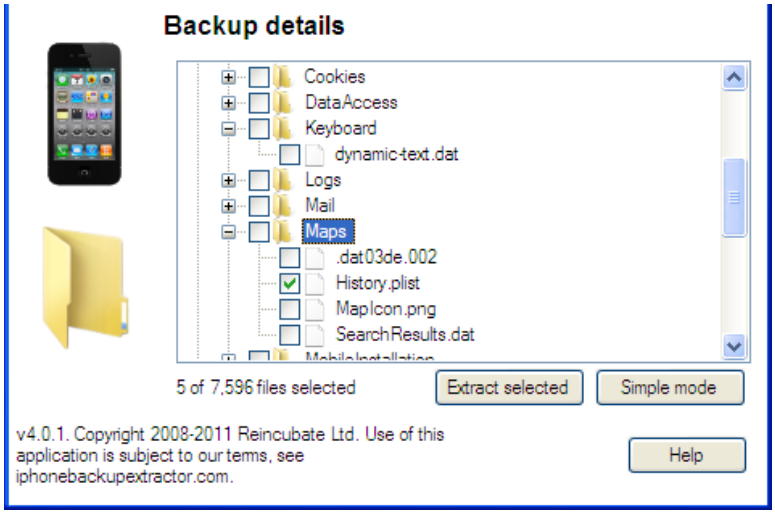
One of the nice things about using the Expert Mode is that you are able to access the underlying information used by the application without activating the application itself. In this case, if you were to look at the actual phone you might not find the suspicious application because it has a feature which allows the user to conceal the application as something innocuous and non-threatening. Even if you did locate the application, it is protected by a password which our little darling might not be willing to give up. Placing a **check box** in the file above the .JPG picture files will select all files contained in the sub tree. Unfortunately, some sophisticated security applications will actually encrypt the data and it may be impossible to recover but in this case it is possible to obtain the images. They can be copied to your desktop file folder by pressing the **Extract Selected** button. Similar to retrieving photos, this process can take a while. The iPhone Backup Extractor will display green boxes over the icon on the screen of the phone in the main window to show you the progress it is making.

There is some EXIF data contained in the images which can be accessed using the techniques discussed in the Photos section.

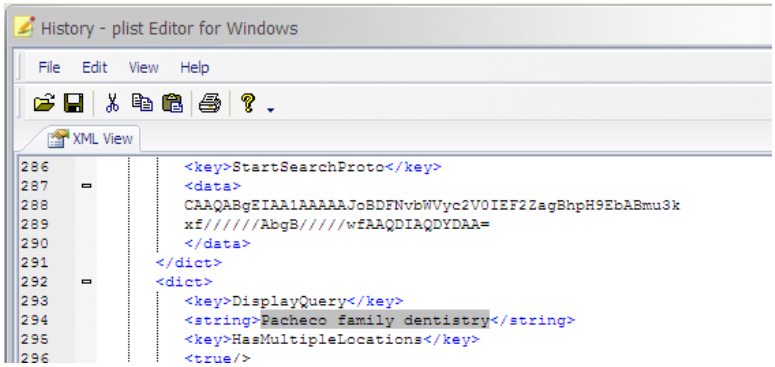
PLISTs, DATs, and DBs

The Expert Mode in the iPhone Backup Extractor allows you to search for an recover an amazing amount of information which has been stored in your target's phone. These files are stored in three main types of database files which requires specialized tools to read. In addition to the free tools you are going to need a lot of patience, a little bit of comfort dealing with computers, and an inquisitive mind. The three main file types you will encounter while snooping in Expert Mode are:

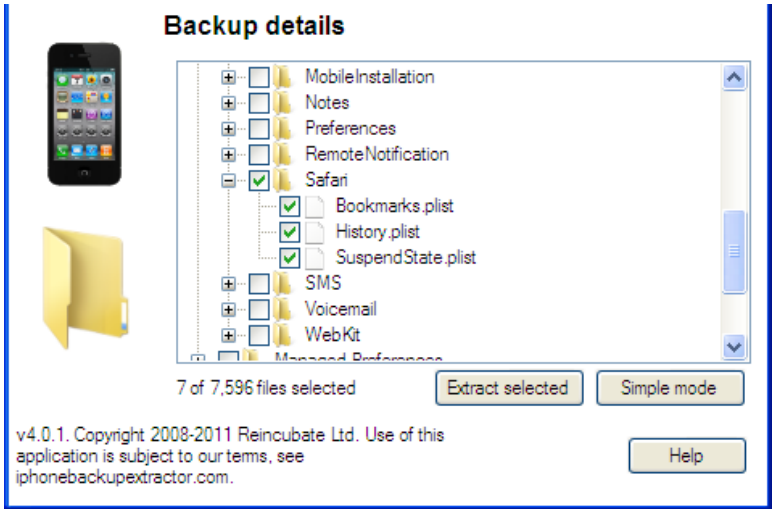
PLIST-Stands for property list files which are used to store serialized data including a user settings. To read these files you will need to first download a plist editor from http://www.icopybot.com/plist-editor.htm.

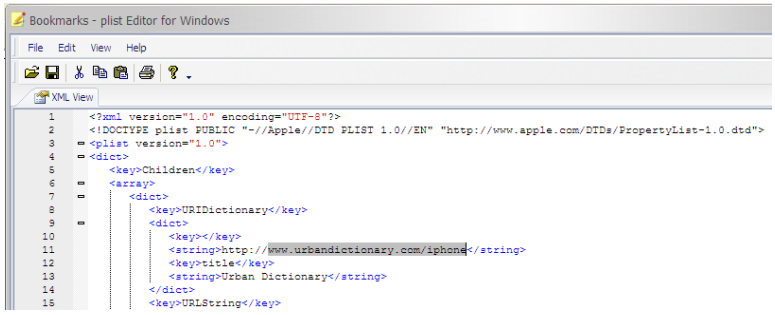


An example of information you can view from a plist database is the information contained in **Library** and then **Maps**. Using the plist editor you will be able to view recent queries into Apple's mapping application. The results will show you the destination location the user queried. Export the Map file from within **Expert Mode** by selecting the **History.plist** file. There should be a green check mark next to the box. Export the file to your Desktop folder. Open the plist editor and select **Open** from the File menu. Navigate to where you exported the History.plist file, select it, and press **Open**. The destination addresses will be listed in plain text.



You can also use the plist editor to view files such as Internet browsing history, Internet bookmarks, and Internet Cache files. From the **Expert Mode** select **Library** and then **Safari** (Apple's Internet browser.) This will automatically select the plist files below. View them in the plist editor and you will be able to see your targets Internet browsing history and bookmarks.

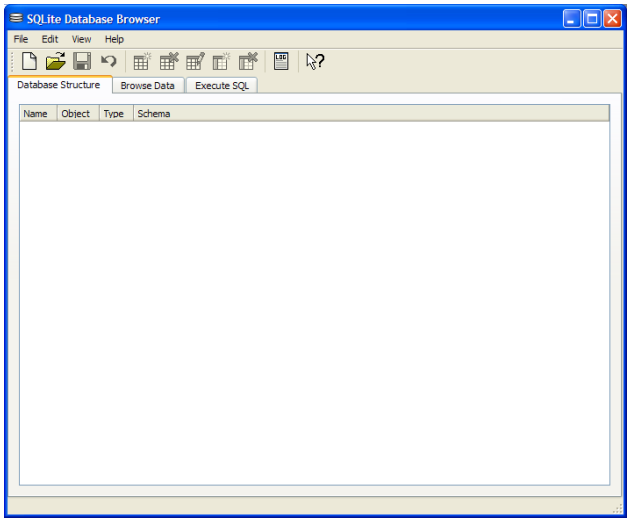




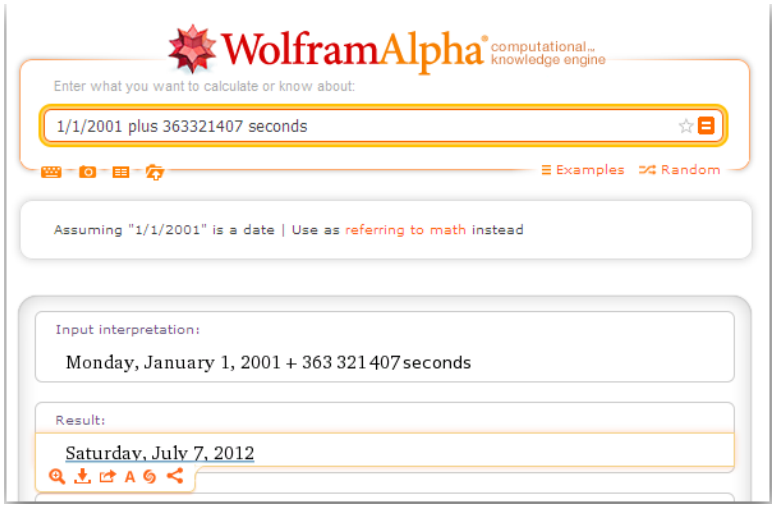
DAT-A DOS operating system database file. DAT databases can be difficult to view. The simplest method is to open the file using Windows Notepad (you can usually find it by pressing the **Start** button and then **Accessories** and then **Notepad**) and then copying the information from the Notepad into Windows Excel or a similar spreadsheet program.

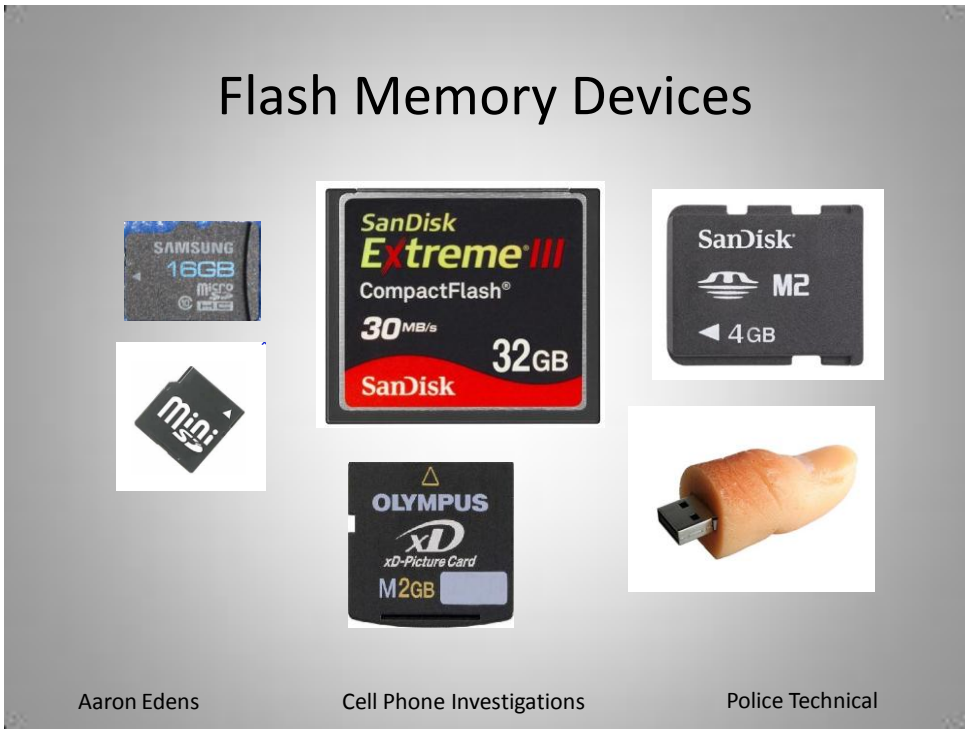
I don't know why but if you try and open the file using Excel directly it does not seem to work as well. An example of information viewable using this technique can be found by navigating to the Library in Expert Mode, selecting Keyboard, and then selecting the file which reads dynamic-text.dat. This file contains information from the custom dictionary of your target's phone and has snippets of conversations they may have had via text message or email. A word of caution: there is no context for this information and there are no dates and times associated with the information. However, some pieces of conversation can be especially useful even without context or dates and times.

DB-A SQLite database file. In order to view these database files you will need yet another software program available at http://sourceforge.net/projects/sqlitebrowser/files/latest/download. Most of the files viewable using the sqlite browser are recovered by the iPhone Backup Extractor but it's nice to have a backup in case you find an interesting file using the Expert Mode.



A note about Apple and times. You may note there are not very many dates and times listed in some of the database files. Instead you will probably see what appear to be random, nonsensical numbers such as 363321407.4. This is a representation of an epoch which is an instant in time chosen as the origin of a particular era. The "epoch" serves as a reference point from which time is measured. In computing, most systems use an epoch date of 1/1/1970, commonly called UNIX time and the number 363321407.4 is a representation of the number of seconds since epoch of UNIX time. Unfortunately, Apple had to be different and they programmed their systems using an epoch of 1/1/2001 to commemorate the release of Mac OS X 10.0. This makes most of the online time calculators ineffective because they are based off the UNIX epoch of 1/1/1970 and not 1/1/2001. The simplest way to calculate the date based off Apple's epoch is to go to the website Wolframalpha.com. Wolfram Alpha is sort of like Google but on steroids, lots and lots of steroids. It is designed to handle scientific calculations and complex problems using simple commands. Fortunately, you can enter the date 1/1/2001 plus 363321407 seconds and it will return the appropriate date of 7/7/2012.


WolframAlpha computational knowledge engine
Enter what you want to calculate or know about:
1/1/2001 plus 363321407 seconds
Examples
Random
Assuming "1/1/2001" is a date | Use as referring to math instead
Input interpretation:
Monday, January 1, 2001 + 363 321 407 seconds
Result:
Saturday, July 7, 2012



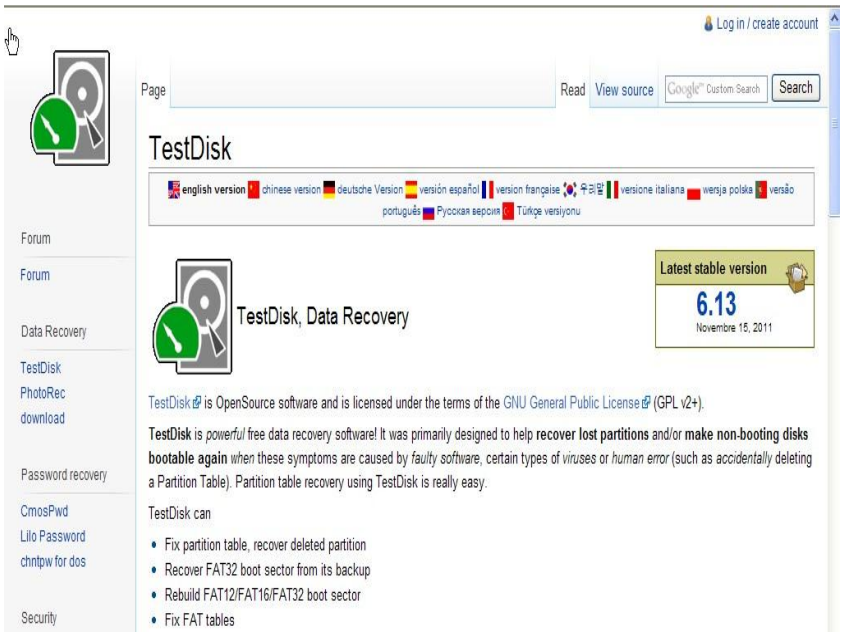
Flash memory is commonly used as storage media for cameras and cellular phones. It does not need to be connected to a power source in order to maintain stored data. Flash memory is extremely durable and can survive prolonged immersion in water, exposure to heat/fire, and survive explosions.

Evidence recovery from flash media which may be part of an investigation involving a cellular phone should be done by a forensic examiner. If an examiner is not available, an investigator should use forensically sound techniques including using a **write-blocked** card reader and software which has been tested and found to work.

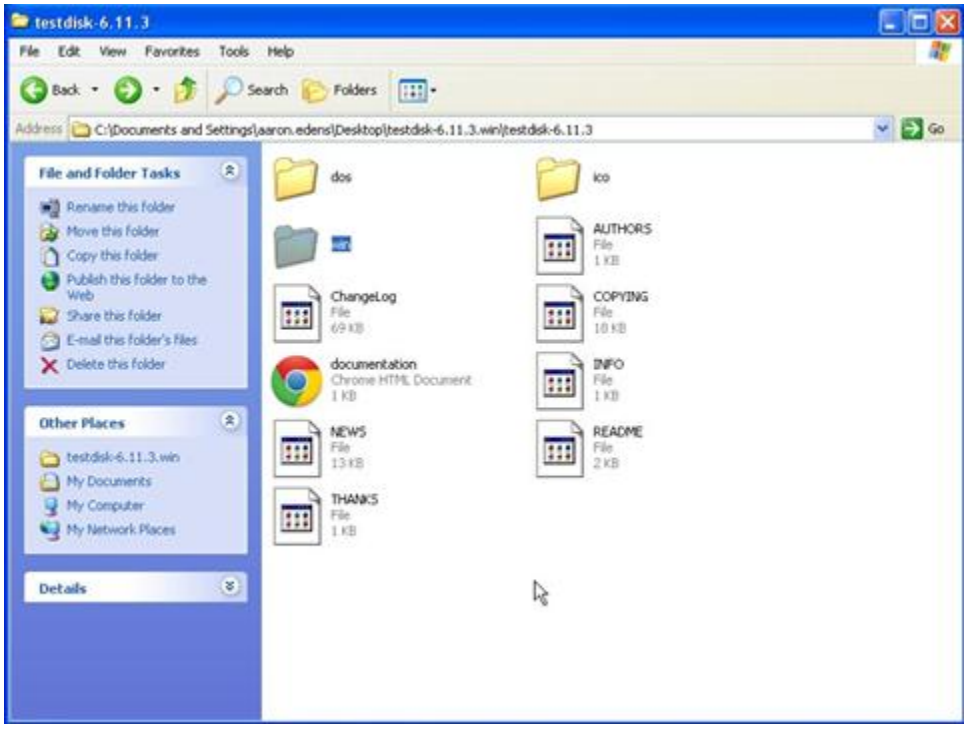
Write block card readers include the product distributed by Digital Intelligence and free software can be found in the Test Disk/PhotoRec group of tools.

Using TestDisk to Recovery Deleted Content from Flash Memory

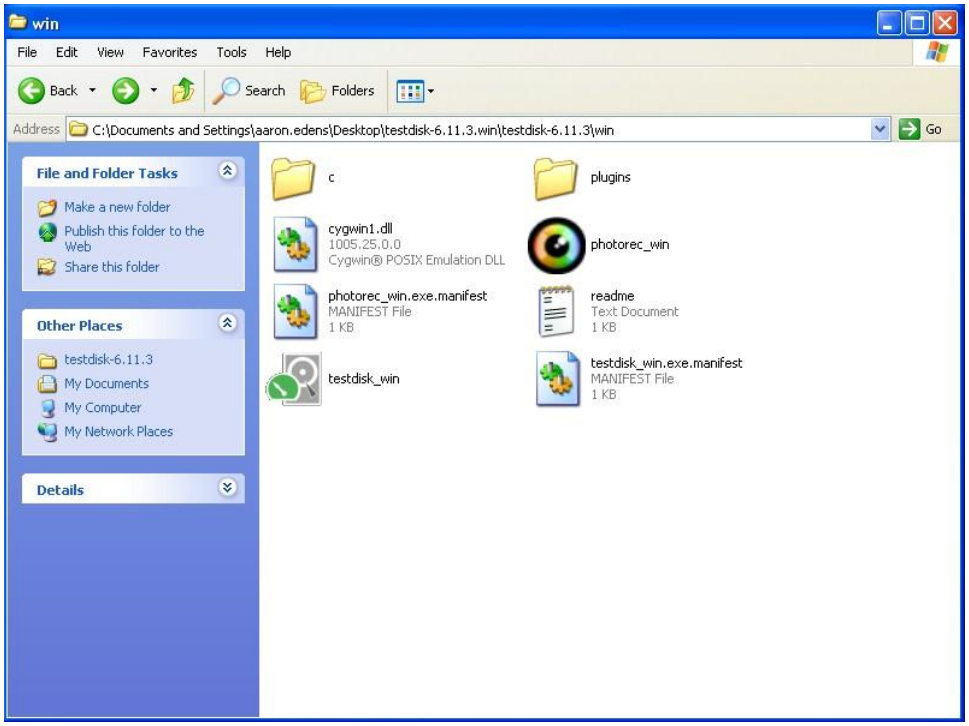
Download and install PhotoRec from www.cgsecurity.org



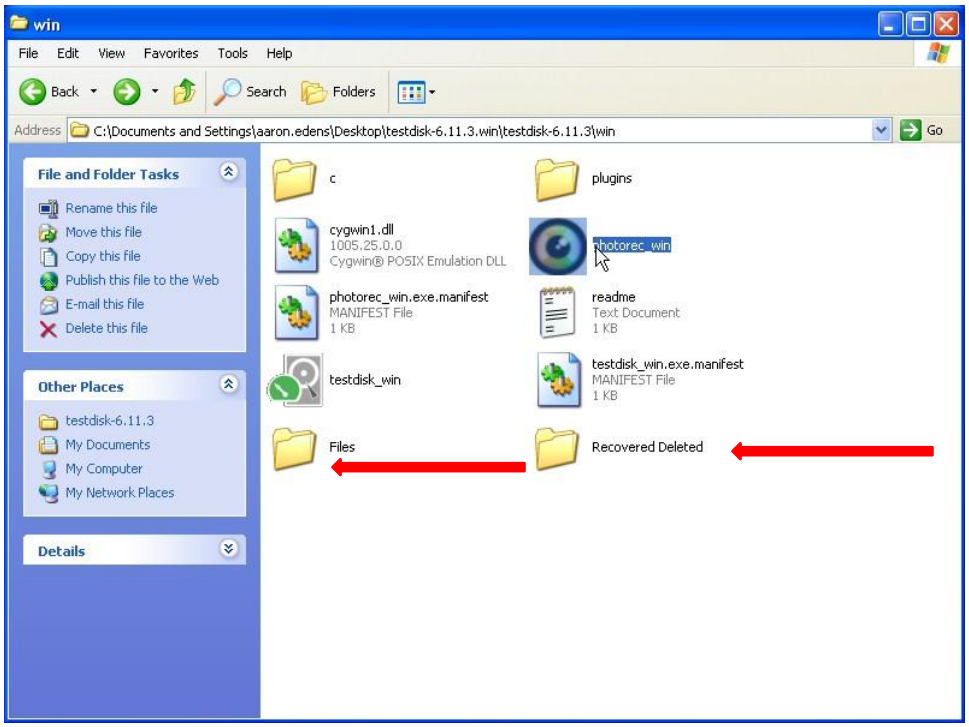
Once installed select the **win** (Windows) folder



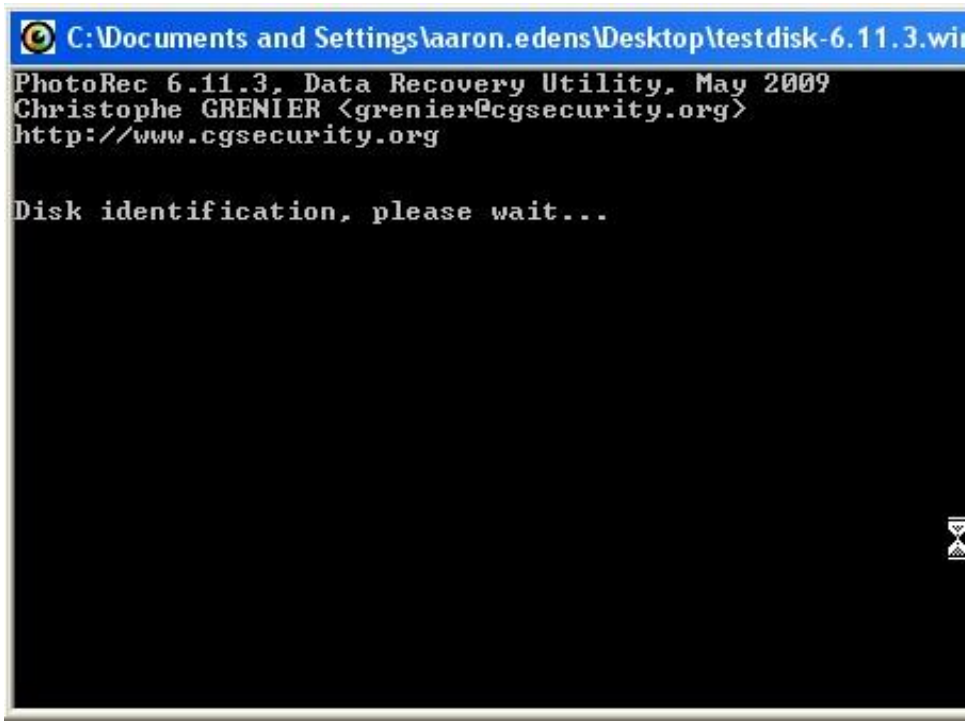
Once the win folder is opened you should see files similar to the following. Double clicking **photorec_win** will launch the program but there you must create folders to receive the data **before** running the program.



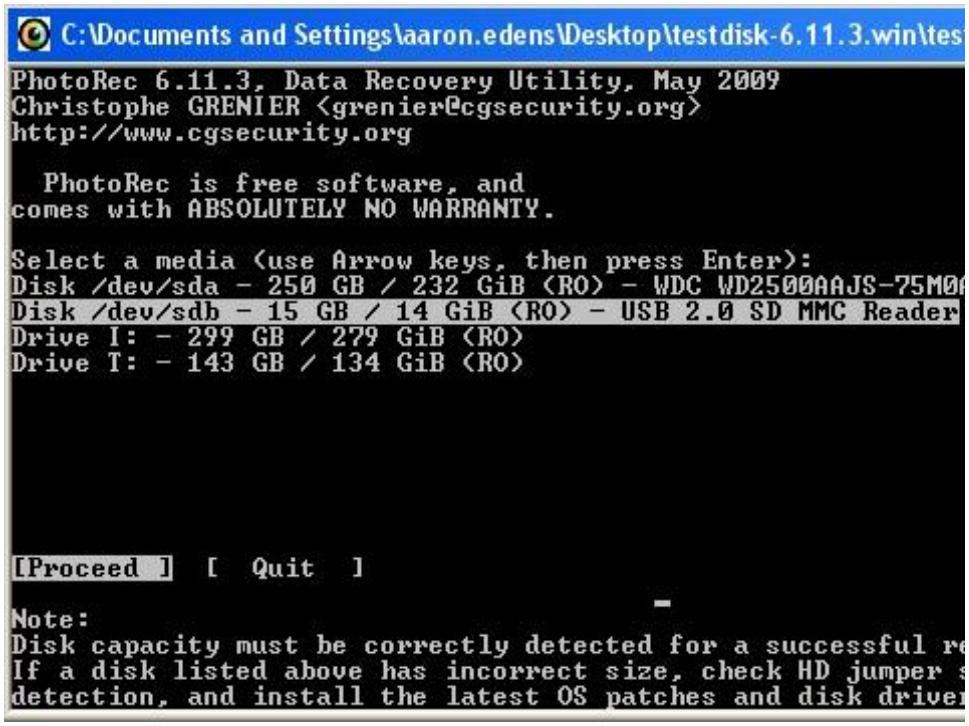
Within the PhotoRec folder, **right click** your mouse button and create two new folders; one for **Files** (those which are visible) and one for **Recovered Deleted** files.



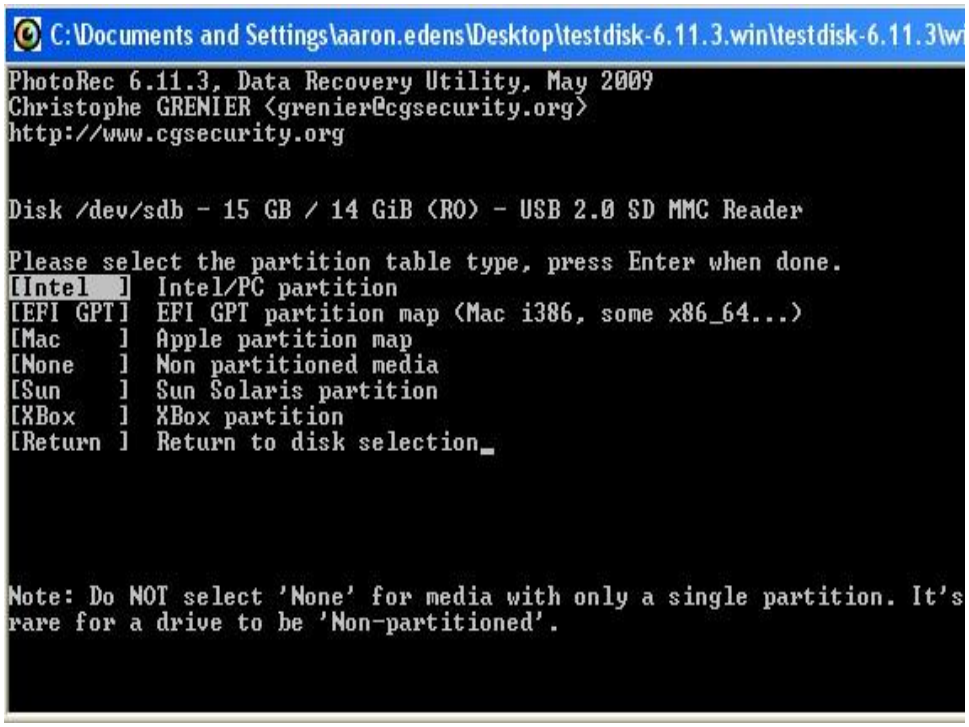
Once the files have been created and labeled, **double click** the photorec_win icon to launch the software. It should not take very long for the software to detect the card reader.



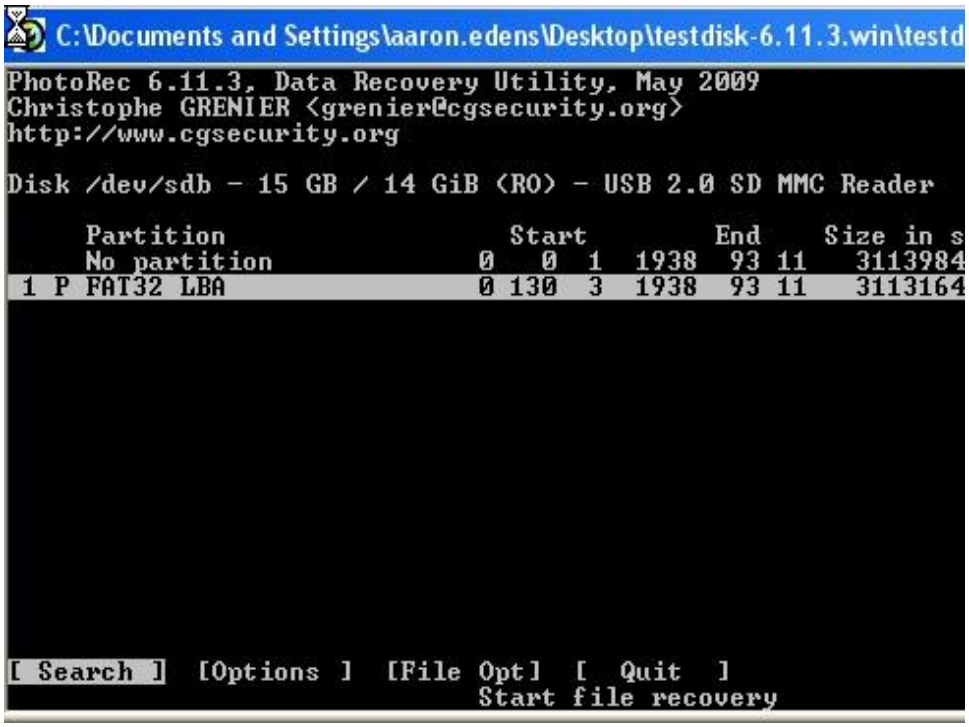
In most cases when using Photorec you can accept the default choices. However, in this screen it is important to navigate to the card reader using the **arrow keys**. Select the card reader and press **Enter** to **Proceed**.

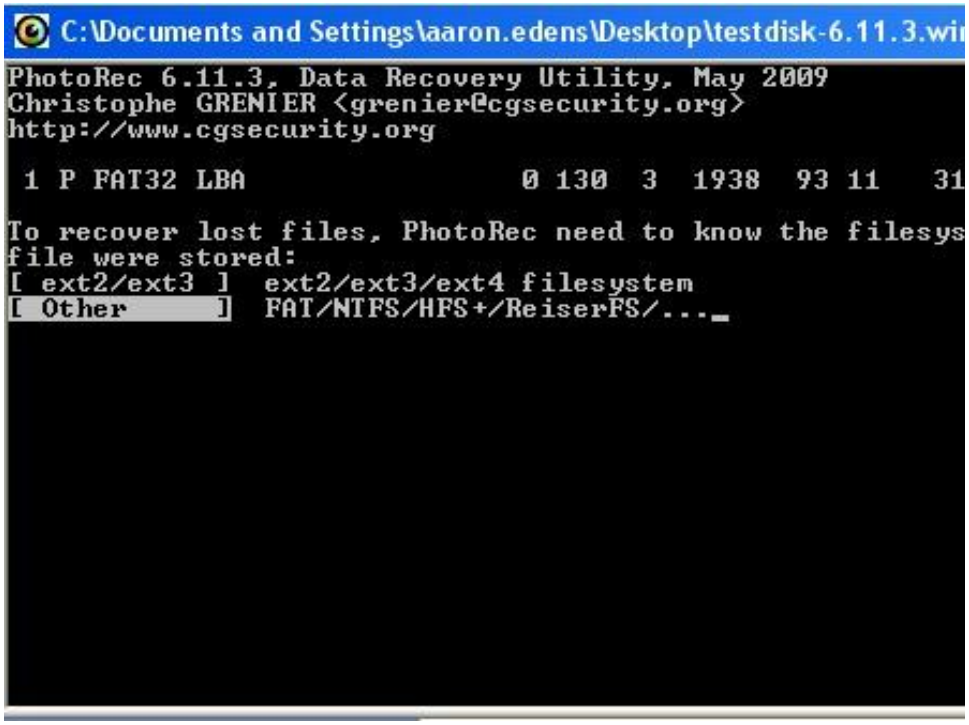


Select the default options by pressing **Enter**.



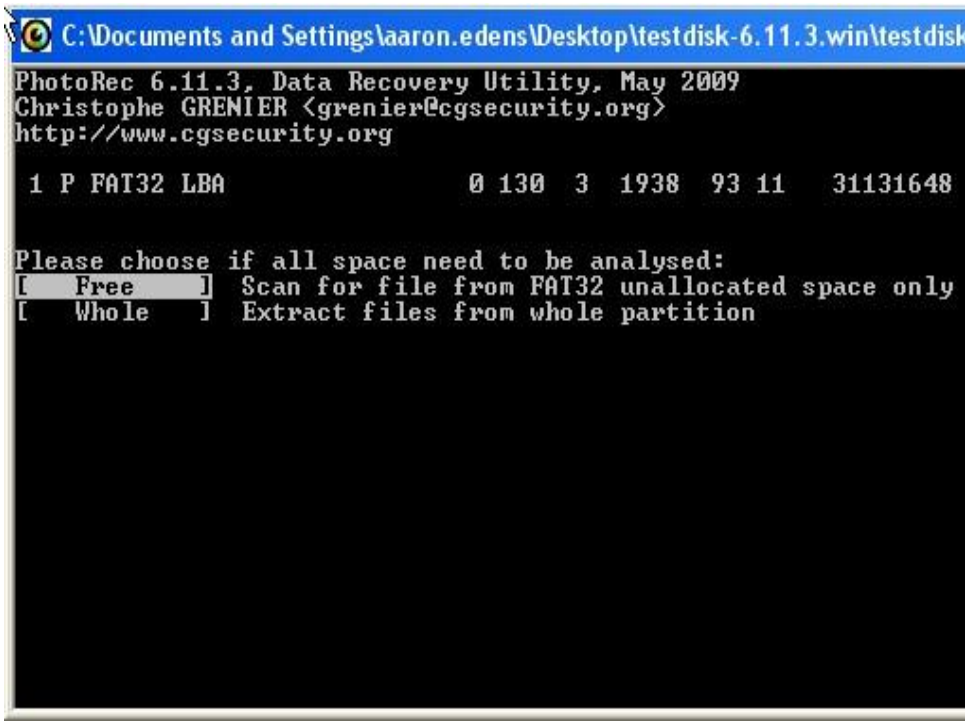
Continue to accept the default selections by pressing **Enter**.



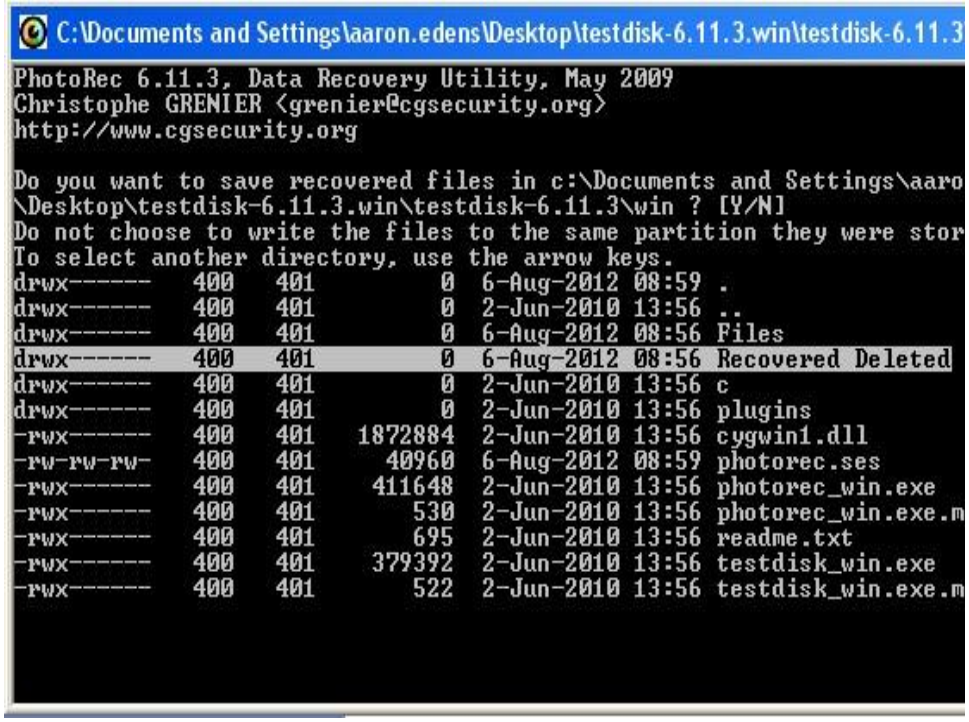


This is the screen where you need to make a decision. You can opt to recover the files from **Free** which is where deleted content lives or you can select **Whole**. Many investigators opt to run the program twice, once for the **Whole** partition

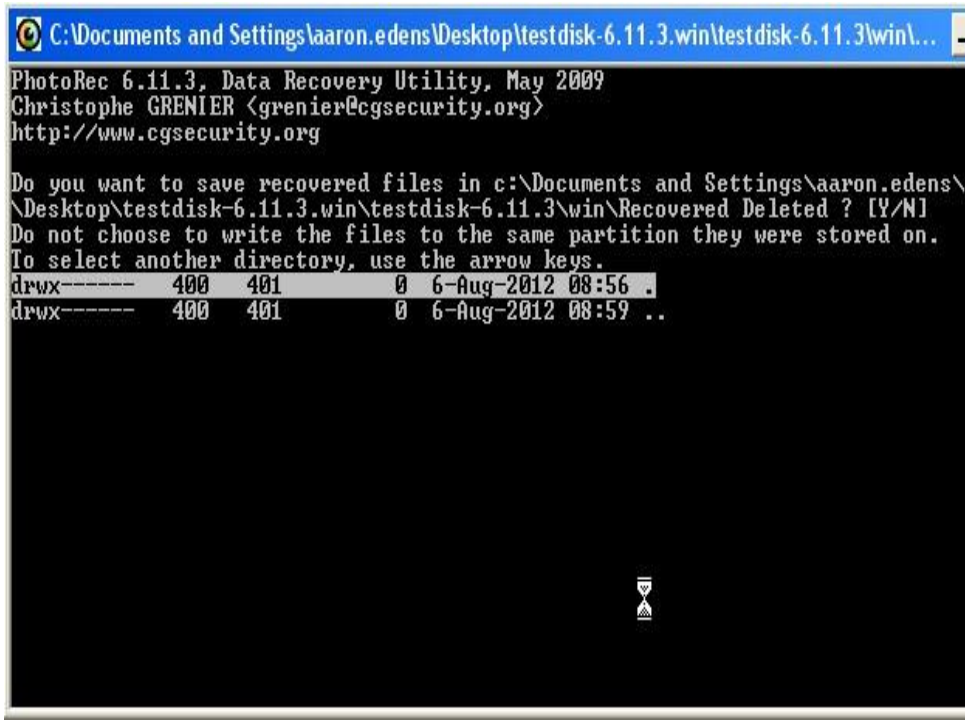
and once for **Free**. This allows the investigator to differentiate between deleted content and that which is undeleted. Use the **up/down arrow** keys and press **Enter**.



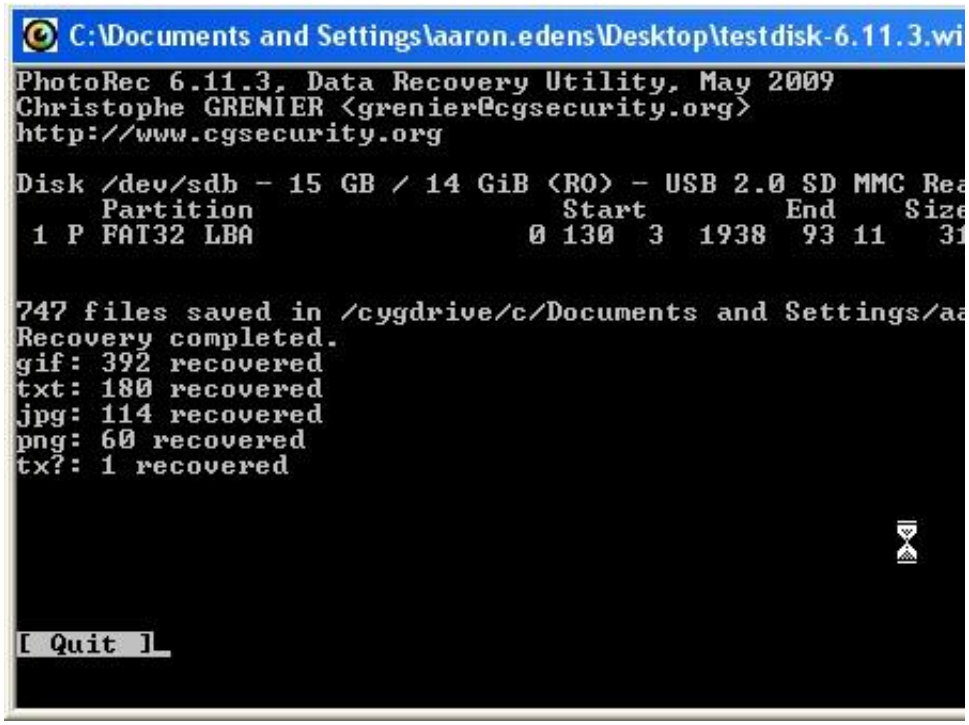
Depending on which files you are after, you must choose where to direct the software to place the recovered files. Using the **up/down arrow** keys select the destination based on the files you wish to recover. If you want to recover deleted content navigate to the **Recovered Deleted** folder you created earlier.



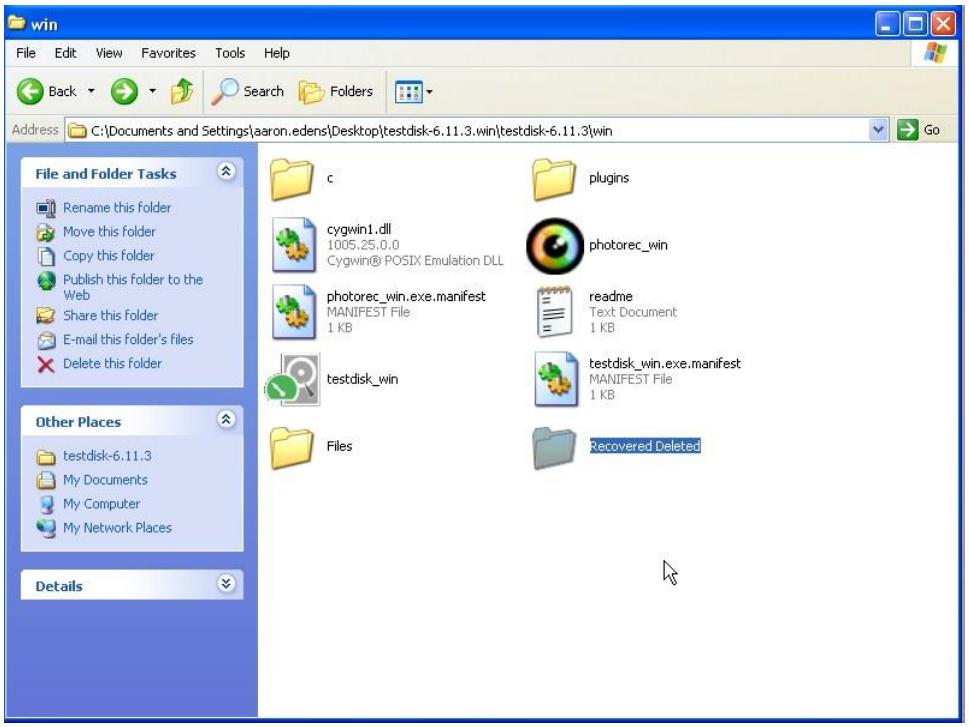
Select **Y** (for Yes) and the recovery process will begin.



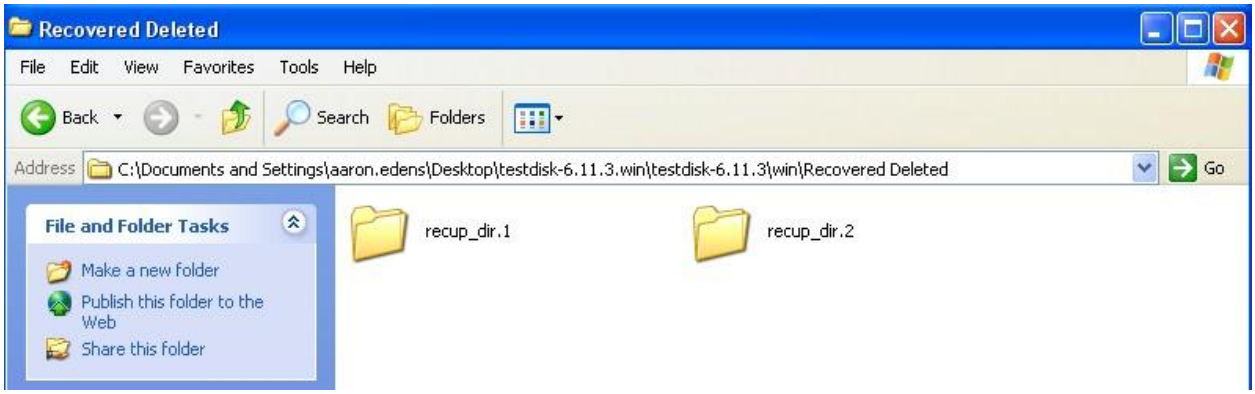
Depending on the size of the flash memory device you are examining the resulting process can take a bit of time. The software will display the number and types of files recovered, as well as, how long the program has been running and an estimated time to completely examine the media. Be patient.



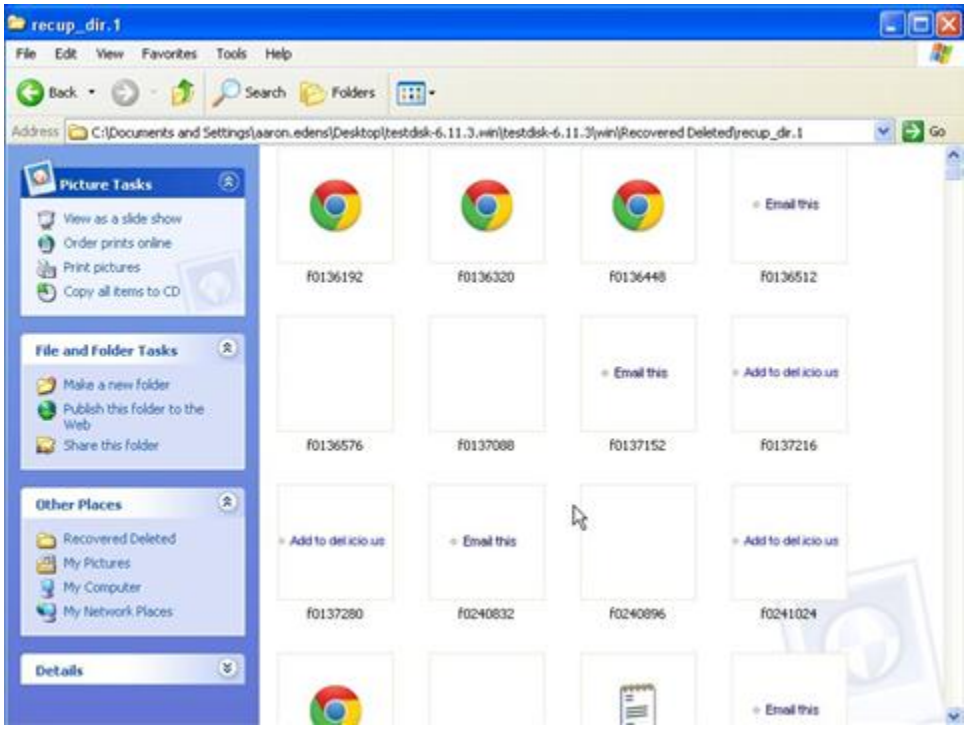
Once the software is finished, the recovered files will be in the folder you selected.



The software automatically breaks up the data in sub-directory folders. You will need to examine each folder separately to view the recovered files.



Keep in mind there are many different types of files stored on flash memory, particularly those used in cellular phones. In addition to pictures and videos, you will also be able to see information, such as graphics, of visited web pages and other data artifacts.



Police Technical National Courses

Cell Phone Investigations

Data from cell phones. Simply the most comprehensive course on cell phone examination and investigations. From the handset to the tower to the phone company to the courtroom.

Craigslist Investigations

Methods and tools for successful Craigslist investigations. Case examples include property related crimes, drug investigations, prostitution, and enticement of juveniles.

Digital Forensics and Evidence Handling

Data from devices. How the process works, how to handle digital evidence, what not to do, how to win in court, future directions, and building on your own in-house lab.

Excel® for Public Safety

Harnessing the power of Microsoft Excel® to better manage data and improve investigations. Telephone tolls, financials, arrest stats, fugitive lists and calls for service analyzed with a few clicks.

PowerPoint® for Public Safety

Designed to assist all personnel become more efficient and proficient with PowerPoint® Faster development, internet videos, E911 audio, Splash Screens® and custom animation.

Social Media Methods

Designed to help departments and their personnel utilize social media effectively to manage their online presence; a prerequisite for any online investigation.

Bring a POLICE TECHNICAL class to your agency

POLICE TECHNICAL has provided technical training to law enforcement since 1998

In-Service Training

An In-Service is the fastest, most cost effective way to provide technical training to your personnel.

We typically provide 2 days of training for up to 40 people at your facility.
An optional 3rd day of training for most classes offers students more hands-on time with the instructor.

Simplified pricing includes all expenses: Instructor fees, meals, travel, lodging, and training materials.

Contact our office for rates and scheduling:

812.232.4200 or at info@policetechnical.com