Lessons Learned
About
The Wolf in Childs Clothing,
Internet Sting Operations

Robert H. Featherston
Law Offices of Taylor & Correa, P.C.
4718 Camino Dorado
San Antonio, Texas 78233
robert@taylor-correa.com
http://www.taylor-correa.com
(210) 656-3711

41st Annual Criminal Law Institute
In Honor of the Honorable A.A. Semaan
April 16-17, 2004

INTRODUCTION

Law Enforcement Officers operating in an undercover capacity are now common on the Internet. Their level of training ranges from no formal training to true computer experts. Their principal tools are the computer and the telephone.

All types of crimes are being actively pursued. One category of which is the "Traveler Case," Criminal Solicitation of a Minor (TPC. §15.031). Law Enforcement officers or their agents, posing as children, drop the "bait" on the Internet in the hopes of landing a child sex predator by getting him/her to travel to the agent's location.

THERE IS NO CHILD INVOLVED IN THIS CASE!

SCOPE OF PAPER

This paper will focus on the Texas state crime of "Criminal Solicitation of a Minor" (TPC. §15.031), in an *attempt* to commit: "Aggravated Sexual Assault of a child" (TPC. §22.021), "Indecency with a Child by exposure" (TPC. §21.11(A)(2)), and/or "Indecency with a Child by contact" (TPC. §21.11(A)(1)).

Sections on the following basic issues will be included:

- Typical client,
- Attorney fees,
- Computer basics,
- Forensic collection of computer evidence;
- Yahoo! Messenger overview
- Criminal statute,
- Defensive strategies,
- Pretrial motions
- Voir dire,
- Opening/closing statements,
- In-courtroom equipment.
- Sample Yahoo! Chat session
- Sample case evidence diagram

Federal involvement will not be discussed.

The medium for the contact with the undercover agent will be the World Wide Web via the Internet and the telephone.

The computers of both the defendant and the agent use the Windows 98 (second edition) operating system with Microsoft's Internet Explorer as the Internet browser program.

Access to the Internet will be through computer modem and an Internet Service Provider (ISP). Computer based communication between the defendant and the agent will be established through the Yahoo!© web site (http://www.yahoo.com), using the Yahoo! Messenger service, Yahoo! Mail and Yahoo! greeting cards.

The telephone contacts will be by cell phone and POTS land line.
If you don't understand some of the terminology used above, don't worry! Read on!

TYPICAL CLIENT
Usually male, late teens on up. Enough education to use a computer, surf the web and know how to use Yahoo! Messenger and Email. A word of caution here, initially, the client probably knows more about computers and how to communicate on the internet than you do, be very careful about discussing technical issues on your first interview! Most have never been in trouble with law enforcement. Almost invariably all will suffer from some form of social ineptness. This ineptness may or may not rise to the level of a DSM-IV diagnosis; however it may not be a bad idea to have the client evaluated by a psychiatrist and have an Abel Assessment of Sexual Interest completed.

ATTORNEY'S FEES
Set a trial fee and demand payment up front! These cases are time consuming for the attorney; besides the identification of all legal issues associated with the case the attorney is going to have to spend time learning about those technical issues specific to their case. It's not unusual to spend over 300 hours preparing for trial.

Experts are hard to find and expensive. Most are asking from $150.00 per hour up to $300.00 per hour. The client needs to know up front what the ball park figure is for expert witnesses and these monies should be collected up front with the attorney's fee. Do not be surprised if expert witness fees exceed $15,000.00.

Now that being said we will discuss below some ways to save some of that money. Additionally, possession of **child pornography** goes hand in hand with these types of cases, be sure to discuss this with your prospective client before setting your fee!

COMPUTER BASICS
Knowing the basics of how computers operate is essential to your case. Here, though important, especially in determining the creditability of the State's expert, all of the components of a computer will not be discussed, instead this paper shall concentrate on an overview of data storage with an eye on forensic collection of data.

FILE PROPERTIES. Whenever you save a "file" to a computer, besides the content of the file, the file will have properties assigned to it by the computer. Some of the more important properties are:

- File Name and Path (path is a complete description of where to find that file on a particular computer),
- File Creation date and time,
- Last Written to by date and time,
- Last Modified by date and time,
- Last Accessed by date (FAT files),
- File Size, and
- File Type or Extension.

File Name and Path. These are extremely important.

Different files with the same name can exist all over the computer. What gives you notice as to which file the State is talking about is the path.

For example if the file name is 11.jpg, (.jpg is a file extension for a picture file), the computer could have a file located at C:\WINDOWS\Temporary Internet Files\11.jpg and the computer might also have the same file name located at C:\My Documents\My Pictures\11.jpg.

So, the first issue here is, has the State given you sufficient notice as to what file they are proceeding on? If only the file name is given then the answer is probably no.

Additionally, if the file is indeed located in the Temporary Internet Files folder, then their may be an argument about knowing and intentional possession, this is because that particular folder is used as a dumping ground by the Internet Explorer browser program for among other things, picture files, the user really does not have control of that folder, the software does. On the other hand if the file is located in a folder that requires the user to put it their manually, such as the My Pictures folder then it probably is intentional and knowing possession, unless of course some hacker stashed it there!

Location of the offending file can make a world of difference in your case!

File Creation Date and Time. "Creation time" is usually (but not always) the time the file was created. More specifically, it is the time when the file was first created **or** written to the disk. Note, then, that if the file was copied from another source, "creation time" would be the time the file was copied rather than the time it was first created, http://www.dmares.com/maresware/articles/filetimes.htm . Typically, when a file is downloaded from the Internet the creation date and time are set to the start of the download time.

Last Written Date and Time. The last time the file was actually changed and then *saved*, http://www.guidancesoftware.com/support/EnCaseForensic/version3/analysis.shtm#date_time.

Last Modified Date and Time. This is only pertinent to NTFS (Windows NT, Windows 2000) and Linux file-system files. It refers to the pointer for the file-entry and the information that that pointer contains, such as the size of the file. So, if you were to change a file, but not alter its size, then the entry modified column would NOT change. However, if the size of a file were changed from eight sectors to ten sectors then this entry would change.
http://www.guidancesoftware.com/support/EnCaseForensic/version3/analysis.shtm#date_time.

Last Accessed Date (FAT files). The last time the file was *viewed*, but not *changed*, http://www.guidancesoftware.com/support/EnCaseForensic/version3/analysis.shtm#date_time .

File size. Indicates in bytes how big the file is. This information in combination with the download time as discussed above can give you an indication of the Internet connection speed.

Additionally, two files with the same name but different file sizes, is a good indication that the two files are different.

File Type or Extension. This usually tells you what type of file it is. For example, a .txt, .doc, .wpd files are text or word processing files, .ppt is a PowerPoint file, .gif, .jpg are image (picture) files. If the file extension has been altered, the State may allege it was done to hide a particular file type, for example 11.jpg file extension is changed to 11.txt in an attempt hide that it is an image. The forensic tools discussed below have the ability to detect this type of alteration.

The date and times as well as the file location on the computer are important, especially if knowledge of their existence by the defendant is an issue, i.e. child pornography.

For example, if you are dealing with files that have been downloaded from the internet, the difference between the file creation date and time and the last written date and time may indicate how long the file took to download into the computer, when compared to the file size this could indicate the type of internet connection, i.e. dial up or broadband. If the time difference between the file creation date/time and the last written date/time are large, this usually indicates a modification to the file. More importantly, if the creation, last written, last accessed and modification dates are all the same this might indicate that the file was just looked at once or maybe not at all. If that file is also located in the temporary internet files folder then an argument exists that the file was not knowingly and intentionally possessed.

STORAGE

Random Access Memory (RAM). The computers involved with the case will have some form of RAM installed. RAM is the hardware location in a computer where the operating system, application programs, and data in current use are kept so that they can be quickly reached by the computer's processor. RAM is much faster to read from and write to than most other kinds of storage in a computer (the hard disk, floppy disk, and CD-ROM). However, the data in RAM stays there only as long as it has power. When the computer is turned off, RAM loses its data, http://www.rose-hulman.edu/Class/ee/yoder/ece332/Papers/RAM%20Technologies.pdf . What is important to note about RAM is that a portion of it is used as "**RAM slack**" to even out files for storage on a hard drive. RAM slack is discoverable by forensic collection tools and is further defined below.

The Hard Drive.

This is the main storage device for the computer. It contains a number of magnetic storage platters and read/write heads for each platter.

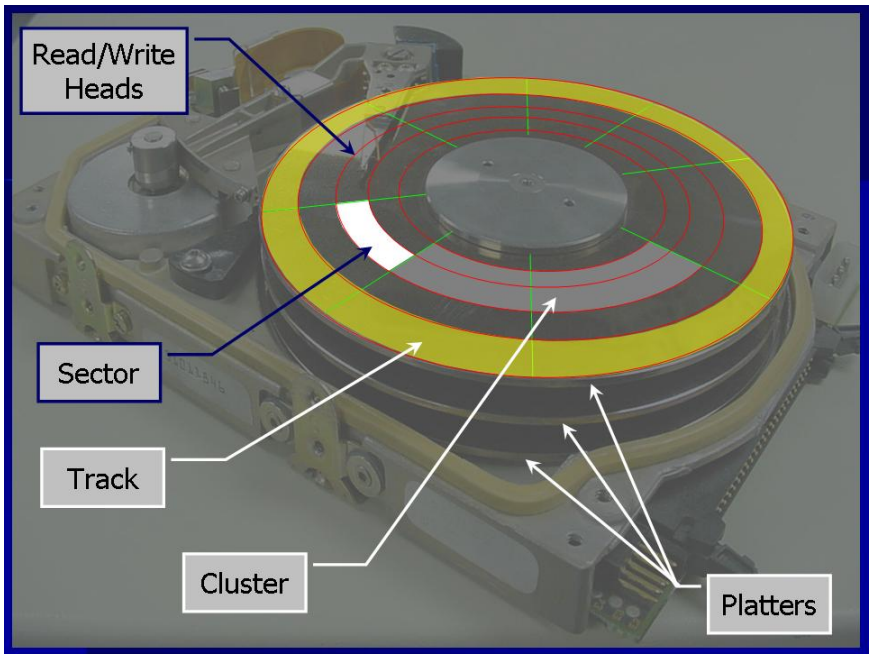
Logically the hard drive consists of cylinders, tracks, sectors, clusters, file allocation table and partitions.

If a hard drive is **partitioned**, into two or more "logical drives" such as drive "C" and "D," then the computer treats each partition separate and apart from the other. This is important because, as far as the computer is concerned, there are two different drives in the system. Each of these "logical drives" operate independently of the other. Different operating systems could be

installed on each partition as well as different application programs. When a forensic examination of the hard drive is performed, the number of partitions are identified.

Tracks are thousands of concentric rings expanding out from the center of the magnetic platters to the edge of the platter. Each track is divided up into **sectors**. Each sector can hold 512 bytes of data as discussed below. There is one track on top of the platter and one on the bottom of the platter. For a particular physical track location on the hard drive, if the hard drive has four platters then their would be eight tracks at that physical location. These eight tracks are referred to as a logical **cylinder**.

If for example a disk had 10,000 tracks on the upper platter, then the entire hard drive would have 10,000 cylinders.



Cylinders, tracks and sectors are the book shelves in the library, where the books (data) are stored, however, without a guide to the library (hard drive) we could not find these books. Much like a library has a card index for locating books within the building, a hard drive uses a "File Allocation Table," (FAT) to locate data on the hard drive.

The FAT is the index for all the data on the hard drive. When a particular file uses up more than one sector for storage, then the FAT will automatically group sectors into "**Clusters**" to simplify the storage process.
So, files are stored in **sectors** and **clusters** which are located on **tracks** and **cylinders** all of whose locations are known to the **FAT**.

Almost always a file will not completely fill up the sector or cluster assigned to it; this is known as "**file slack**," however, there are no voids on a hard drive. When a file fails to completely fill up a particular sector or cluster then the computer will obtain random data from either RAM or the hard drive to write a full sector or cluster. This procedure is know as using "RAM slack" and "Drive slack", as described below.

It is important to note that when a user deletes a file from his/her computer, you do not really delete the file, only the entry in the FAT is removed, (this is the same as removing the index card from the library card file, the book is still in the library, but now no one knows where to look), the data remains on the drive till it is overwritten by the FAT. For large hard drives that could be

a long time. Forensic analysis tools will look for these deleted files and can sometimes recover the whole file!

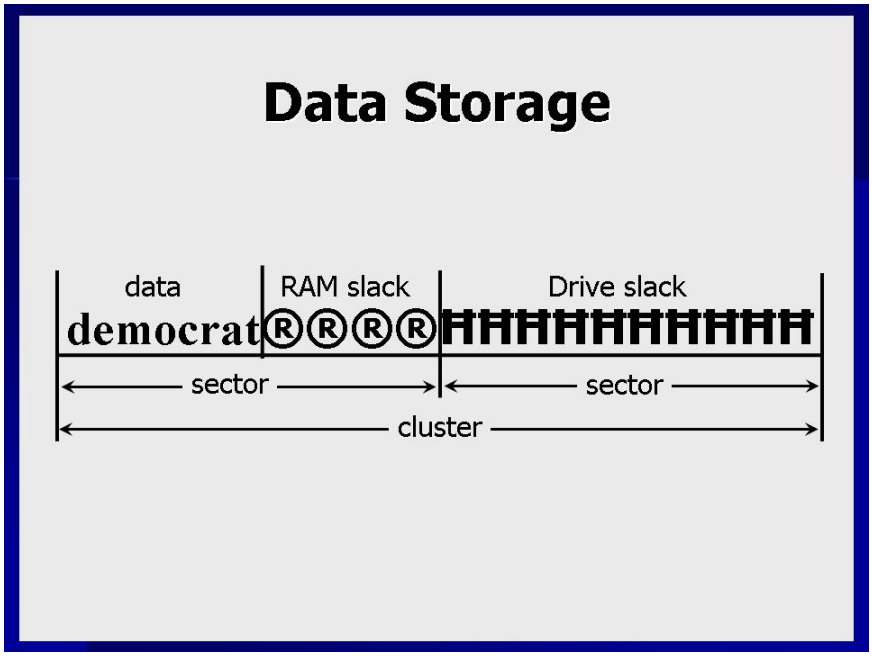
File Slack is the data storage space that exists from the end of the file to the end of the last cluster assigned to the file. Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. Larger cluster sizes mean more file slack and also the waste of storage space when Windows 95 systems are involved. File slack contains randomly selected bytes of data from computer memory. This randomly selected data is called **RAM Slack** because it comes from the volatile memory of the computer.

RAM Slack can contain any information that may have been created, viewed, modified, downloaded or copied during work sessions that have occurred since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past.

Drive Slack. RAM slack pertains only to the last sector of a file. If additional sectors are needed to round out the block size for the last cluster assigned to the file, then a different type of slack is created. It is called **drive slack** and it is stored in the remaining sectors which might be needed by the operating system to derive the size needed to create the last cluster assigned to the file. Unlike RAM slack, which comes from volatile memory, drive slack is padded with what was stored on the storage device before. Such data could contain remnants of previously deleted files or data from the format pattern associated with disk storage space that has yet to be used by the computer.

If the examiner is properly trained and knows what to look for, file slack is a significant source of evidence and leads.

Example. Let's say that a file is created by writing the word "**Democrat**" to a file. Assuming that this is the only data written in the file and assuming a two sector cluster size for the file, the data stored to disk and written in **file slack** could be represented as follows:



File Slack is created at the time a file is saved to disk. When a file is deleted under DOS, Windows, Windows 95, Windows 98 and Windows NT/2000/XP, the data associated with RAM slack and drive slack remains in the cluster that was previously assigned to the end of the 'deleted' file. The clusters which made up

the 'deleted' file are released by the operating system and they remain on the disk in the form of **unallocated storage space** until the space is overwritten with data from a new file.

It is important that you to understand the significance of file slack in computer-related investigations. Because file slack potentially contains data dumped randomly from the computer's memory, it is possible to identify network logon names, passwords and other sensitive information associated with computer usage. File slack can also be analyzed to identify prior uses of the subject computer and such legacy data can help the computer forensics investigator. File slack is not a trivial item. On large hard disk drives, file slack can involve several hundred megabytes of data. Fragments of prior E-Mail messages and word processing documents can be found in file slack. From a computer forensic standpoint, file slack is very important as both a source of computer evidence and security risks. http://www.forensics-intl.com/def6.html

Swap file
A swap file is a space on a **hard disk** used as the **virtual memory** extension of a computer's real memory (**RAM**). Having a swap file allows your computer's **operating system** to pretend that you have more RAM than you actually do. The least recently used files in RAM can be "swapped out" to your hard disk until they are needed later so that new files can be "swapped in" to RAM. In general, Windows and Unix-based operating systems provide a default swap file of a certain size that the user or a system administrator can usually change. http://whatis.techtarget.com/definition/0,289893,sid9_gci213077,00.html

Unallocated Space
When files are erased or deleted in DOS, Windows, Windows 95, Windows 98 and Windows NT, the content of the file is not actually erased. Data from the 'erased file' remains behind in an area called unallocated storage space. The same is true concerning **file slack** that may have been attached to the file before it was deleted. As a result, the data remains behind for discovery through the use of data recovery and/or computer forensics software utilities.

Unallocated file space and file slack are both important sources of leads for the computer forensics investigator.

Until the first file is written to the data storage area of a computer storage device, the clusters are unallocated by the operating system in the File Allocation Table (FAT). These unallocated clusters are padded with format pattern characters and the unallocated clusters are not of interest to the computer forensics specialist until data is written to the clusters.

As files are created by the computer user, clusters are allocated in the **File Allocation Table (FAT)** to store the data. When the file is 'deleted' by the computer user, the clusters allocated to the file are released by the operating system so new files and data can be stored in the clusters when needed. However, the data associated with the 'deleted' file remains behind. This data storage area is referred to as unallocated storage space and it is fragile from an evidence preservation standpoint. However, until the unallocated storage space is reassigned by the operating system, the data remains behind for easy discovery and extraction by the computer forensics specialist.

Unallocated file space potentially contains intact files, remnants of files and subdirectories and temporary files which were transparently created and deleted by computer applications and also the operating system. All of such files and data fragments can be sources of computer evidence and also security leakage of sensitive data and information. http://www.forensics-intl.com/def8.html.

COMPUTER LOGS.
The computer, depending on the operating system and software installed, maintains a number of logs of computer activity that the normal user is unaware of. Logs can be a rich source of information for the forensics examiner.

The next time you are at your computer, go to the start menue, select find files and type in *.log in the named section then select your C drive to look in and have the computer run a search. You will find at least 50 entries for different types of logs!

For Internet sting operations over a modem to Yahoo!, two logs are very important. They are the modem log and the ypager log. Both logs are text based and can be opened with any word processor. The modem log will usually have “modem” in the name. This log contains connect times to the Internet. The “ypager” log contains connecting information through yahoo and can reveal the screen names of users who have communicated to the target computer. These logs should be examined to see if there are sessions involving the undercover agent for the State and the defendant that the State has not revealed.

FORENSIC COLLECTION OF COMPUTER EVIDENCE
This section is merely an overview. When you know which operating systems, programs, storage media and forensic tools are involved in your case then its time to use an Internet search engine such as Google, http://www.google.com, to find more out about these programs and search for experts.

The term "Computer Forensics" was coined back in 1991 in the first training session held by the International Association of Computer Specialists (IACIS) in Portland, Oregon. Computer Forensics deals with the preservation, identification, extraction and documentation of computer evidence. Like any other forensic science, computer forensics involves the use sophisticated technology tools and procedures which must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer evidence processing. Computer forensics has also been described as the autopsy of a computer hard disk drive because specialized software tools and techniques are required to analyze the various levels at which computer data is stored after the fact. http://www.forensics-intl.com/def4.html.

GOVERNMENT STANDARDS FOR COLLECTION & ACCREDITATION
The organization that seized the defendants computer and collected the evidence off of it, and/or collected the evidence through a State computer off the Internet should have a standard operating procedure for the collection of that evidence. Defense counsel should subpoena this document and compare it to the guides put out by the United States Secret Service and Department of Justice. Below are listed the links to sites containing these guides. In addition there are links to test results for two popular disk imaging tools and the results of their accuracy.

- Best Practices for Seizing Electronic Evidence, Unites States Secret Service,
- Electronic Crime Scene Investigation: A Guide for First Responders, NIJ Guide, June 2001
- Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations; Computer Crime and Intellectual Property Section, Criminal Division United States Department of Justice, July 2002
- State and Local Law Enforcement Needs to Combat Electronic Crime, Research in Brief, August 2000
- Test Results for Disk Imaging Tools: EnCase 3.20, NIJ Special Report, June 2003
- Test Results for Disk Imaging Tools: SafeBack 2.18, NIJ Special Report, June 2003

Certification and Accreditation of Computer Forensics (or Digital Evidence) Labs

The principal organization for the certification of forensics labs, including the collection of digital evidence is the International Organization of Standardization (ISO). All forensics labs are moving towards ISO certification. Government and private labs are eligible for this certification. Digital evidence collection falls under ISO 17025.

Close on he heals of ISO is the American Society of Crime Laboratory Directors, ASCLD who have recently added digital evidence collection to their lab certification process. This certification was developed by the Scientific Working Group on Digital Evidence and is available to law enforcement only. ASCLD is in the process of integrating ISO 17025 into their accreditation scheme.

Individuals can be certified by the International Association of Computer Investigative Specialists, IACIS, as either a Certified Electronic Evidence Collection Specialist or a Certified Forensic Computer Examiner; however these certifications are only issued to law enforcement personnel.

A plethora of vendor specific certifications are also available for the operation of specific software. Some limit their certifications to law enforcement only. The defense attorney should be able to cross examine the State's expert on certification and compliance.

An area that currently has no case law and is ripe for a challenge is Texas Code of Criminal Procedure Article 38.35, Forensic Analysis of Evidence; Admissibility. The statute appears to be broad enough to cover the forensic collection of computer evidence and may be a ground for suppression. The following is a list of certification organizations:

- The International Organization for Standardization-(ISO)
- ISO/IEC/EN 17025, -Forensics Lab Certification and Accreditation program.
- American Society of Crime Laboratory Directors, ASCLD, - Forensics Lab Certification and Accreditation program, .
- ASCLD, Scientific Working Group on Digital Evidence, SWGDE
- **International Association of Computer Investigative Specialists (IACIS)** - IACIS is a nonprofit corporation composed of law enforcement professionals who have been trained in the forensic science of seizing and processing evidence from computer systems. This website contains membership information, training opportunities, and special announcements from IACIS.

Defense access to properly certified experts is extremely limited, with most experts raising moral issues in assisting the defense team. However, there is one Government agency who will assist the defense if the issue deals with the proper operation of a forensic collection tool. This agency is the United States Commerce Department, National Institute of Standards and Technology, (NIST), Computer Forensics Tool Testing (CFTT) Project, http://www.cftt.nist.gov. They will provide a defense attorney with an "unbiased" analysis of a particular forensic investigative tool, if of course its in their data base. If the tool is not in their data base then there presents an argument that that particular tool is not peer reviewed. If the tool is in the data base then any issues dealing with that tool will be their.

Some experts that are willing to work with the defense are identified below.

COMPUTER FORENSIC PROGRAMS

The legal issues involved with forensic programs revolve around their reliability. Most are not accredited by any national or international agency, nor have they been subjected to peer review. File a motion to suppress the results of a forensic examination of your defendant's hard drive and make sure one of the grounds is the scientific unreliability of the program used to conduct the search.

Examiners, usually due to lack of training, often do miss material evidence involved with a case, if the methodology they use to preserve evidence is suspect, then the results of their collection may be subject to a Rule 901(b) (9) objection for the State's failure to use a collection procedure that would produce an accurate result.

ENCASE. is user friendly and menu driven. The program takes a lot of the guess work out of data extraction, however it is no substitute for a trained and certified examiner. NIST has certified version 3.2 for disk imaging only. The web site is a good source of information on the software and they usually list case law that supports its use. http://www.guidancesoftware.com/index.shtm. Attached as appendix (A) is a "Sample EnCase Report."

ILOOK. The ILook Investigator © toolsets are computer forensic tools used to capture and analyze images created from computer systems hard drives and other external storage media.

ILook is provided free to qualifying agencies throughout the world. Eligible users **must be** involved in computer forensics and employed by one of the following:

1) Law Enforcement agency whose employees are sworn law enforcement officers.
2) Government Intelligence agency.
3) Military agencies with authority in criminal and or counter intelligence investigations.
4) Government, State or other Regulatory agencies with a law enforcement mission.

http://www.ilook-forensics.org/.

SAFEBACK. Is a DOS-based disk imaging utility used to back up and restore hard disks. SafeBack picks up every last bit of data-unused

and erased data included-on the original disk and stores it in a tape or disk file (or series of files). SafeBack can take that same backup file and re-create the original disk on your own system. SafeBack does not write or otherwise modify the original system and can (and should) be started from a boot diskette. http://www.forensics-intl.com/safeback.html.

MARESWARE. Mares and Company Provides an essential set of tools for investigating computer records and securing private information. It is highly flexible to meet the needs of all types of investigators including: law enforcement, intelligence agency, private investigator, corporate security officers, and human resources personnel. Used within a forensic paradigm, the software enables discovery of evidence for use in criminal or civil legal proceedings. http://www.dmares.com/maresware/software.htm.

These are the main forensic tools available; however the list is not exclusive. Discover from the State what software was used by the forensic examiner in your case then investigate grounds for suppression of its results

EVIDENCE PRESERVATION. The day the client walks into your office file and have a hearing to preserve evidence! The defense attorney cannot lose with this type of hearing.

The hearing forces the State to commit to the Court, on the record, that all of the evidence has been preserved in this case, or admit that it has not. Even without an order, you win. The defense attorney now has a record and if it turns out that evidence has been altered, or not preserved, a motion to dismiss may be appropriate. If the motion to dismiss fails, the jury may view the State's failure in a light more favorable to your defendant.

In Internet sting operations, the material portion of the case is made by the computer. This is a double edge sword for the State, nothing can be hidden, because all of the computer communication is coming across a computer the State controls. EVERYTHING should be preserved.

If the defendant is telling you there were more chat sessions, emails or greeting cards than the State has produced, then examination of the State's computer for modem logs, ypager logs, emails and the un-produced chat sessions or fragments of chat sessions is material to your case.

The methodology used by the State to preserve all of the evidence in the case is material and relevant. This methodology should be closely examined.

As a base line you should expect and the jury shall expect, the State to have a methodology in place that preserves all evidence associated with the case and preserves it so that alterations to the evidence can be detected.

The case agent conducting the sting should not be primarily responsible for the preservation of the evidence. This job should be accomplished by the Information Systems Administrator (ISA). In fact, the case agent should not even have access to the data from the computer he/she is working on until after the data/evidence has been preserved. The ISA can set up screen and

keyboard loggers to automatically capture everything occurring on the computer and to then preserve the data without the case agent having to intervene.

SCREEN/KEYBOARD LOGGERS. These programs record every keystroke and all activity that comes across a monitor on the computer they are installed on. The programs run in the background, in other words the user of the computer does not have to deal with it and in most cases may not even know the logs are being generated. For preservation of evidence purposes they are ideal. A search of the Internet will reveal numerous vendors of these products, such as Guardian, http://www.guardiansoftware.com .

HASHING. Is a program for computing a condensed representation of a message or a data file. SHA-1 is the most current hashing standard, http://www.arid.us/cs/sha.html. The program produces a unique series of alphanumeric to represent a particular file. This unique alphanumeric is referred to as a message digest and is considered a finger print for a particular file.

For example, the State's computer receives a Yahoo! Messenger Instant Message, (as described below). The computer can be configured to automatically save the message and to automatically hash the file using a hashing program, all without user intervention. Now the file is preserved with a hash. If a year from now you wish to access the file, but want to know if it has been altered since the original hash, you rehash the file and compare the two message digests, if they are the same then the file has not been changed since the original hash.

Beware, hashing a file after it has been altered will not detect the alteration! An illustration of a hash is in the attached "Sample EnCase Report."

Besides being used to authenticate a file, hash message digests are also used to speed up the search of a defendants hard drive. A computer contains thousands of files, most dealing with the oprating system and programs installed. If a examiner has a known set of message digests for the operating system and program files, he/she can hash the files on the target computer and compare the resulting message digests to the known digests. If no alterations to the files have been made, the message digests will match, thus eliminating a great number of files from the investigation task. Where does the examiner get a good set of message digests? The Government maintains a data base.
The National Software Reference Library (NSRL) provides a repository of known message digenst for use by law enforcement and other organizations in computer forensics investigations, http://www.nsrl.nist.gov/Project_Overview.htm .

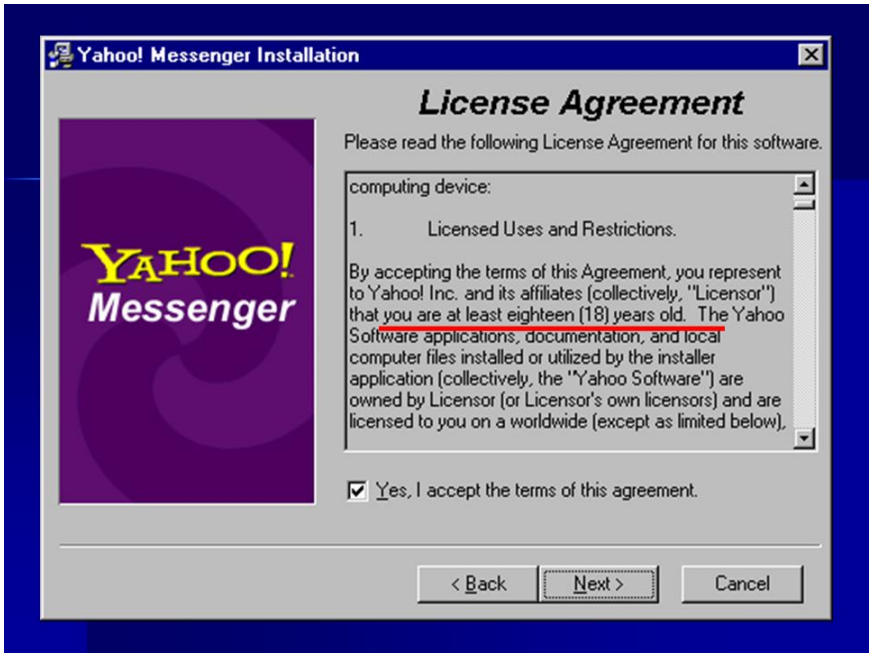
YAHOO! MESSENGER.
This program, along with AOL Instant Messenger are the preferred law enforcement hunting ground for undercover sting operations. This paper will give you an introduction to Yahoo! Messenger.

At this site users have access to "chat rooms," where they can go to discuss common interests, email each other, send greeting cards, use web cams, and voice over the Internet. Each of these communication tools have a different levels of reliability with respect to accurately identifying the end user. For example, if all of the communications between two users occur through Yahoo Messenger's public chat window and instant messages, with only profiles to look at, then knowing who is really on the other end of the conservation is impossible.

Why? – EVERY ONE LIES ON THE INTERNET! Make this a theme of your case.

The Yahoo! Messenger program allows users who access the Internet to automatically connect to the Yahoo! Messenger web site.

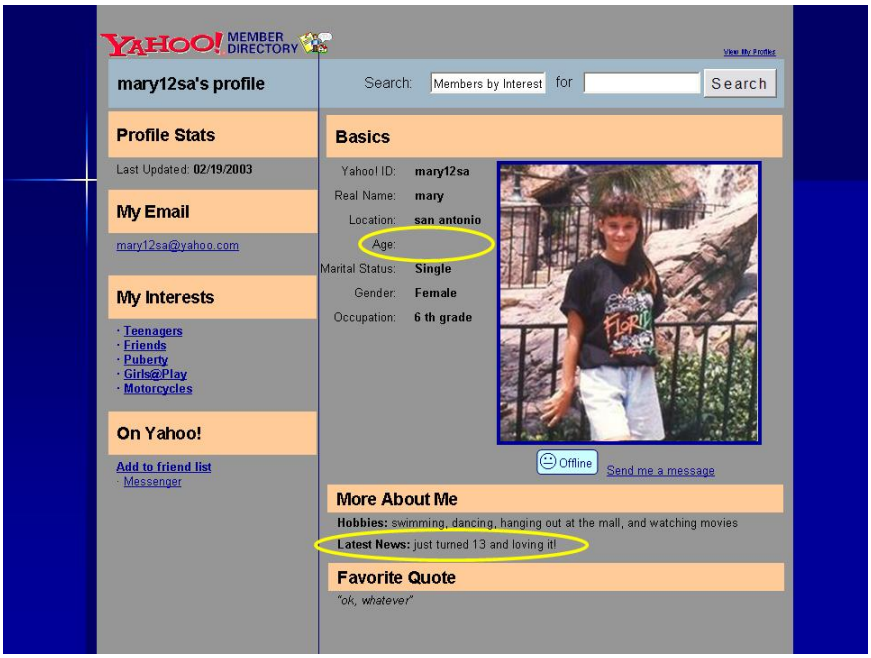
Users are required to be at least 18 years of age to participate in the chat rooms.



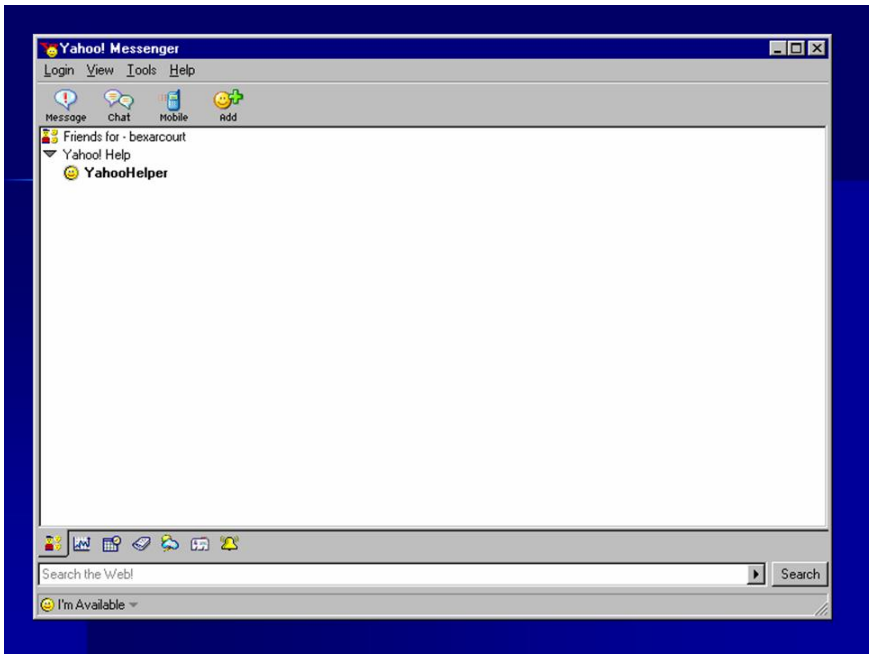
When a potential user is setting up the service, the program will not allow you access if your age is under 18. Law enforcement agents will circumvent this requirement by listing a false age in the sign up page and then listing an age of below 17 on the profile page.

The profile page can be accessed by right clicking on the "screen name" of the user.

THERE IS NO CHILD IN THIS TYPE OF CASE. The profile is a complete lie, a construct for law enforcement purposes. Carefully examine the profile page used in your case. Note when the page was last updated. Ensure that the profile the State is sponsoring is the one in existence at the time of the communications with the defendant.



The main Yahoo! Messenger window is the location from where the chat rooms are accessed. Clicking on the Chat icon allows the user to view a list of all chat rooms.



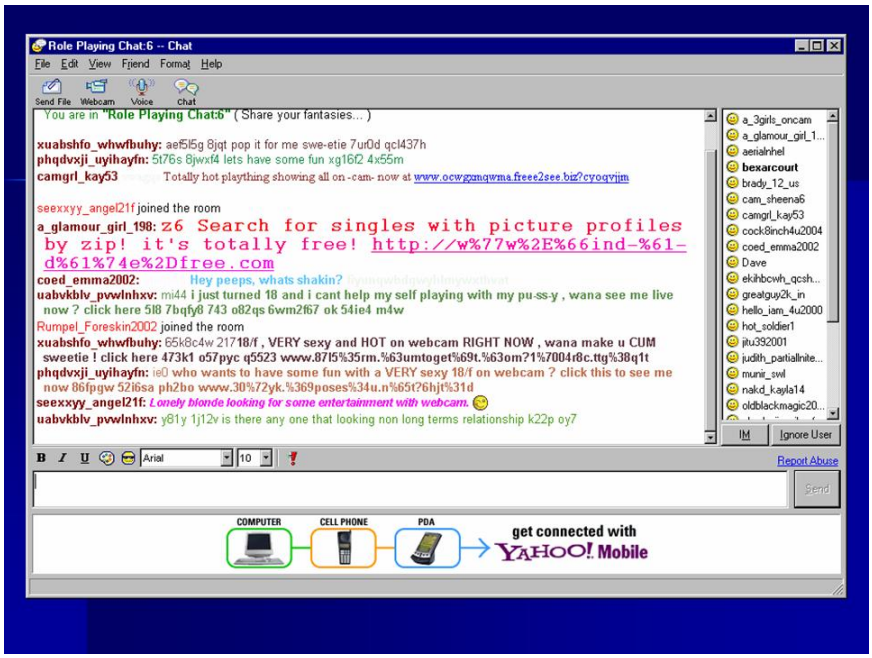
The Join Room page lists all of the categories of chat rooms available. None of these chat rooms are designed for children. Most contain graphic sex talk, even those not listed as adult.

Depending on which chat room is involved in your case, a reasonable expectation as to what the user can expect to find in the chat room is first established by the name of the chat room. For example, it is more probable that adult sexual role playing is being conducted, if that is the chat room the user goes to. Remember, there are no chat rooms designed for children in Yahoo! Messenger!

A constant theme that you should reinforce to the jury is that every one lies in these chat rooms and on their profiles. How many pictures of Nichole Kidman are on users profiles?

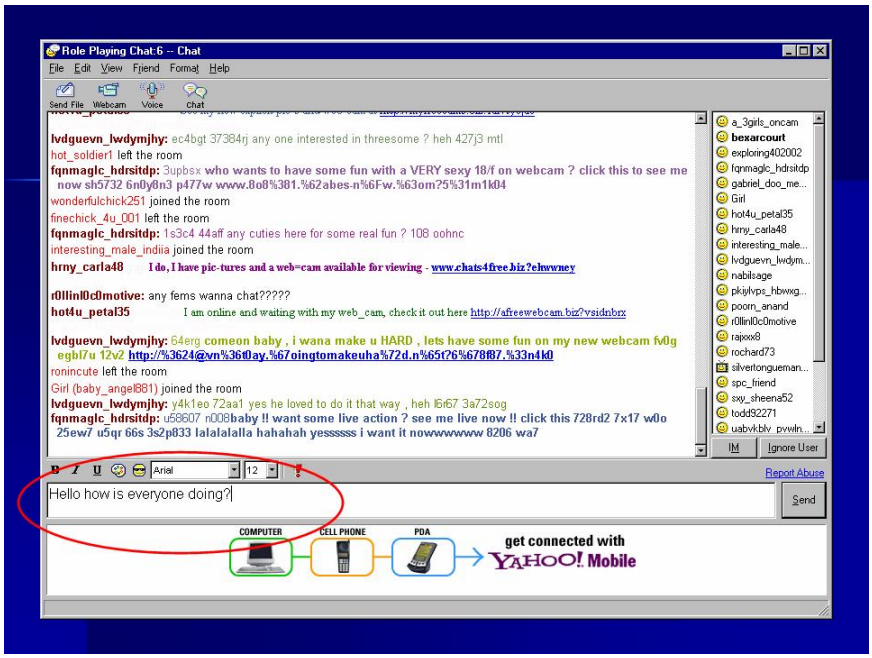
After a particular chat room has been chosen, the main chat screen will open. This is the window that establishes the character of the conservations, the defensive themes of your case. The main screen is organized into three principal areas. The largest area contains the content of the public chat sessions in progress and will scroll as participants trade communications. On the far right of the screen is a listing of all of the

participants in that particular chat room, by "screen name". Below the area where the public chat sessions are in progress is a box for the user to type in a message that will be displayed on the public window.

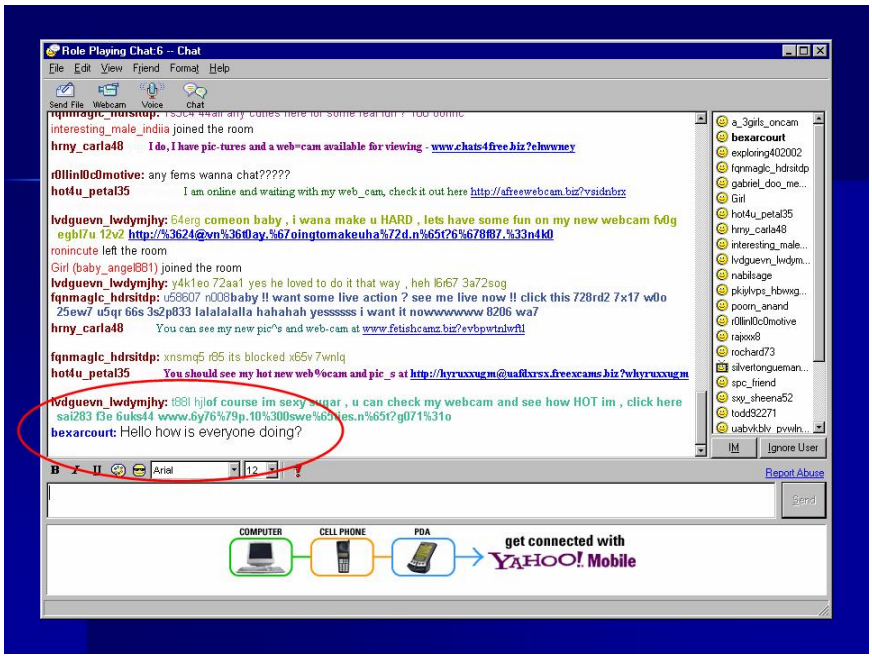


Preservation of the messages in this window are material to your case! Without them you cannot establish the character of the room. Are you at a church social or a frat party? Is the content sexually graphic or are the users discussing sports? Is the undercover agent for the State participating in the public chat sessions or just staying on the sidelines? None of these questions can be adequately answered unless the State has preserved this evidence. Depending on what the evidence shows, defensive theories such as fantasy/roll play or accommodation may come into play, or the content may plainly demonstrate the need for an entrapment defense.

This main window establishes the playing field. A user has two choices for communicating with other users. Use this public forum or send an instant message directly to the other user that the rest of the participants do not see.

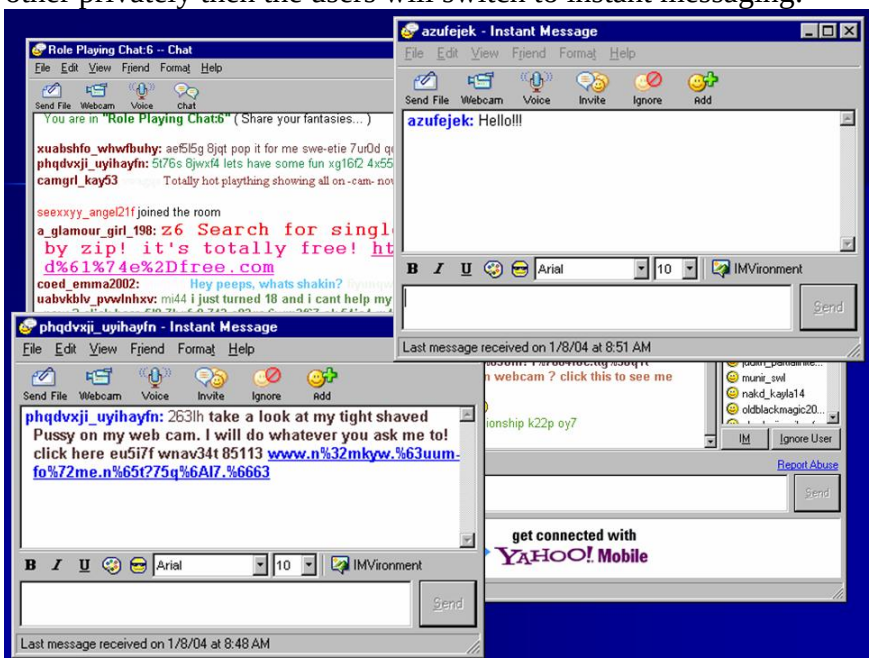


Public communication is established by the user typing his/her message in the box below the public window.



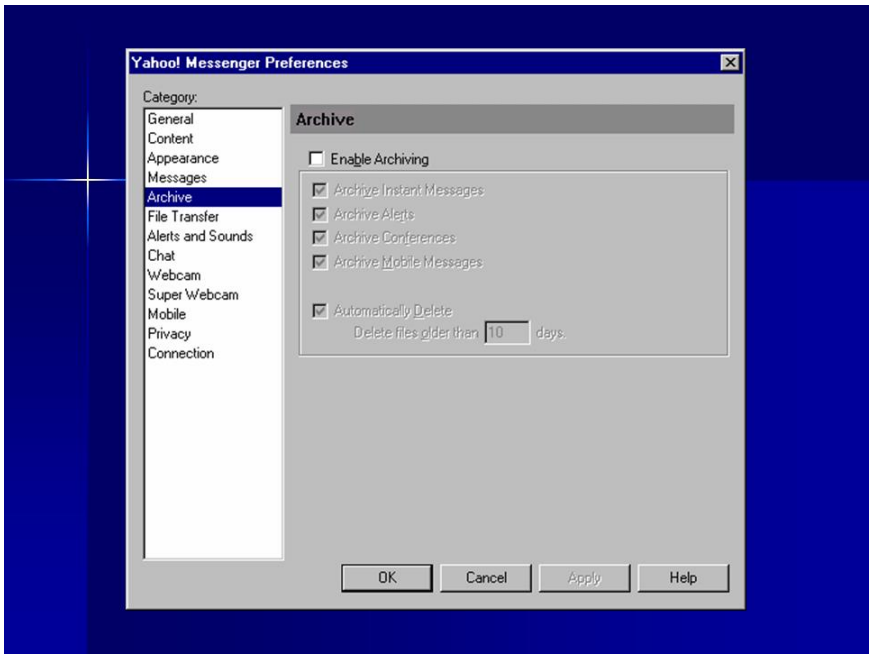
When the user selects the enter/return key or selects the send button, the message is transmitted and displayed on the main screen.

Initial contact is almost always made from the main window. If two users decide to contact each other privately then the users will switch to instant messaging.

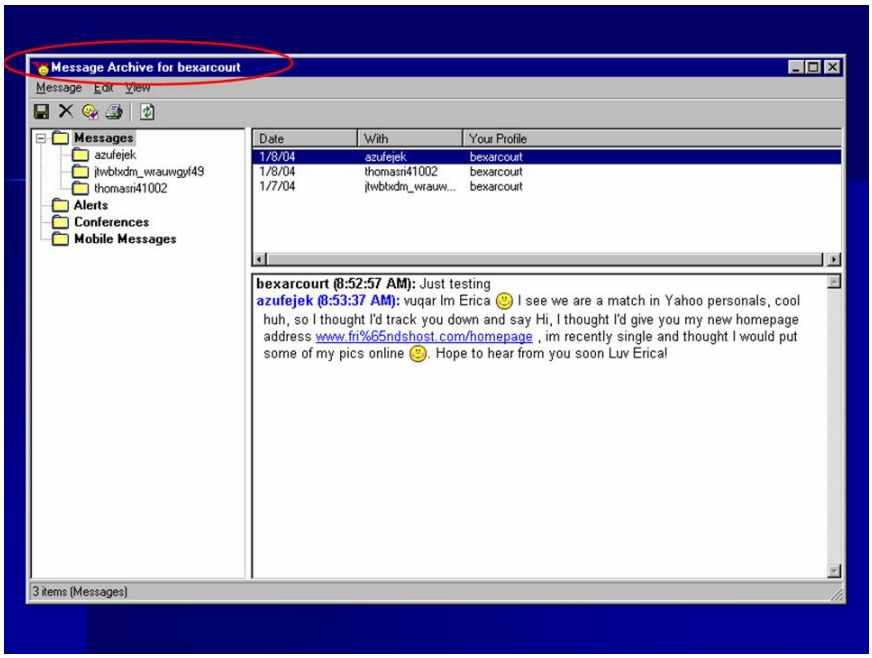


A user can send an instant message by simply double clicking on the screen name of the user he/she wishes to contact, either from the public window or from the listing of screen names on the right side of the screen. When this selection is made an instant message window will pop up for the user to type his/her message into and send to the other user. The other user, when they receive this message, will have an instant message window appear on their screen.

Yahoo! Messenger has the ability for the user to archive their messages by selecting enable archiving in the Yahoo! Messenger Preferences window. Once selected, all IM messages will be archived.



When a user wants to see their archived messages they can go to tools on the main window and select archiving. The window below will appear with all of the instant messages in it.



The above procedure requires the user to activate archiving in order to retrieve the user's instant messages. Most users don't activate this function and some users would not want their sessions archived.

What most users and forensics examiners don't realize is that, irrespective of whether archiving is selected by the user, those instant messages are already saved to the user's hard drive in a format that the user can't directly access and that the most popular forensic tools will not decode. This file is not hard to find, if you know it exists. It is probably the only evidence on the defendant's computer that can be used to refute the State's offered evidence of what constituted the entire computer conservation

with the defendant. If what is on the defendant's computer is different than what the state is offering, then the foot is in the door for an argument about the loss/omission of evidence.

CRIMINAL STATUTE

CRIMINAL SOLICITATION OF A MINOR

The legal vehicle to which the State will hitch its horse is Texas Penal Code Section 15.031, Criminal Solicitation of a Minor, the statute is as follows:

Sec. 15.031. Criminal Solicitation of a Minor.

(a) A person commits an offense if, with intent that an offense listed by Section 3g(a)(1), Article 42.12, Code of Criminal Procedure, be committed, the person requests, commands, or attempts to induce a minor to engage in specific conduct that, under the circumstances surrounding the actor's conduct as the actor believes them to be, would constitute an offense listed by Section 3g(a)(1), Article 42.12, or make the minor a party to the commission of an offense listed by Section 3g(a)(1), Article 42.12.

(b) A person commits an offense if, with intent that an offense under Section 21.11, 22.011, 22.021, or 43.25 be committed, the person by any means requests, commands, or attempts to induce a minor or another whom the person believes to be a minor to engage in specific conduct that, under the circumstances surrounding the actor's conduct as the actor believes them to be, would constitute an offense under one of those sections or would make the minor or other believed by the person to be a minor a party to the commission of an offense under one of those sections.

(c) A person may not be convicted under this section on the uncorroborated testimony of the minor allegedly solicited unless the solicitation is made under circumstances strongly corroborative of both the solicitation itself and the actor's intent that the minor act on the solicitation.

(d) It is no defense to prosecution under this section that:

(1) the minor solicited is not criminally responsible for the offense solicited;

(2) the minor solicited has been acquitted, has not been prosecuted or convicted, has been convicted of a different offense or of a different type or class of offense, or is immune from prosecution;

(3) the actor belongs to a class of persons that by definition of the offense solicited is legally incapable of committing the offense in an individual capacity; or

(4) the offense solicited was actually committed.

Criminal Solicitation of a Minor, TPC 15.031

(b) A person commits an offense if, **with intent** that an offense under Indecency With a Child, Sexual Assault, Agg Sex Assault or Sex Perform Child, be committed, the person by any means requests, commands, or attempts to induce a **minor** or **another whom the person believes** to be a **minor** to engage in specific conduct that, under the circumstances surrounding the actor's conduct **as the actor believes them to be**, would constitute an offense under one of those sections or . . .

(e) An offense under this section is one category lower than the solicited offense.

(f) In this section, ``**minor**'' means an individual younger than 17 years of age.

(EMPHASIS ADDED)

Attempted Indecency With a Child – under 17
Attempted Sexual Assault – under 17
Attempted Sexual Performance of a Child – under 17
Attempted Aggravated Sexual Assault – under 14

(e) An offense under this section is one category lower than the solicited offense.

(f) In this section, ``minor'' means an individual younger than 17 years of age.
(EMPHASIS ADDED)
Legislative History
Leg.H. Stats. 1995 74th Leg. Sess. Ch. 262, effective January 1, 1996; Stats. 1999 76th Leg. Sess. Ch. 1415, effective September 1, 1999.

In an Internet sex solicitation case involving an undercover agent and NO CHILD, the operative paragraphs of the above statute are (b), (e) and (f).

"Whom the person believes," "as the actor believes them to be," is very important language in this statute. With respect to Internet sex solicitation cases; this wording virtually turns the statute into a "thought crime."

This may be a First Amendment issue as applied, no one to date, that the author could discover, has pursued this issue.

Section (e) gives notice that the punishment is one category lower than the attempt. For example, it the attempted crime is aggravated sexual assault, a 1st degree felony, then the punishment will be for a 2nd degree felony.

The age allegations is important because of the age differences between aggravated sexual assault (under 14), indecency with a child (under 17) and sexual performance of a child, which is normally under the age of 18, but if used as an attempt, within the solicitation statute, its under the age of 17.

DEFENSIVE STRATEGIES
Preservation/admissibility of evidence, conduct of the police, entrapment, fantasy, roll playing and accommodation are the probable pillars of the defense in this type of case. Remember – EVERY ONE LIES ON THE INTERNET, and THERE IS NO CHILD INVOLVED WITH THIS CASE!

Defense counsel should endeavor at all times to look more professional and better prepared than the State in front of the judge and jury.

Preservation of Evidence. As discussed above start immediately! At the hearing to preserve evidence, your goal should be to get the State to image all of the hard drives involved with the case, both the State's and the Defendant's. Defense counsel's goal here is not to obtain a copy of the State's hard drives, access to the State's images of the State's computers will probably require a Brady motion after indictment, at a pretrial discovery hearing. Defense counsel merely wants to preserve the status quo at this hearing. See motion attached as appendix (B).

Admissibility of Evidence. The material evidence usually involved with these types of cases include:

1. Yahoo! Messenger chat room public window.
2. Yahoo! Messenger Instant Messages.

3. Email.
4. Greeting Cards.
5. Computer logs.
6. Recorded Phone Conservations.
7. Surveillance or arrest videotape.

Best Evidence. It is important to note here that the evidence on the computer is electronic in nature; a printout of this evidence is not really evidence, but a product of that evidence. When asking for discovery from the State or obtaining a discovery order from the Judge obtain a bit-stream image of the evidence. A bit-stream image will preserve the file parameters as discussed above.

This is the field of "Digital Evidence." A great deal has been written about it, most civil, but it does apply to your case. If the State tries to give you only a printout of the digital evidence, raise a best evidence issue under Rule 1002 and cite the following cases:

- *Broderick v. State*, 35 S.W.3d 67 (Tex.App. – Texarkana 2000, pet.ref'd).
- *Gates Rubber Co. v. Bando Chem. Indus.*, 167 F.R.D. 90 (D.C. Colo. 1996), *affirmed in part, vacated in part*, 9 F.3d 823 (10th Cir. 1993)

Conduct of the Police. Jurors want to know that their police officers are competent, unbiased and professional in the pursuit of their cases. In cross examination of the police officer, start with the officer's training, education, experience and certifications to operate a computer and preserve evidence in the internet environment. Examine the laboratory setup used by law enforcement to collect their digital evidence. What methodology was in place to ensure the system would produce an accurate result. Use Rule 901(b)(9) to challenge inadequate methods.

Entrapment. Appears attractive on its face and as a issue before the jury has some appeal, however, from a legal definition stand point the defendant must admit to committing the offense to take advantage of this defense. The statute reads:

> Sec. 8.06. Entrapment.
> (a) It is a defense to prosecution that the actor engaged in the conduct charged because he was induced to do so by a law enforcement agent using persuasion or other means likely to cause persons to commit the offense. Conduct merely affording a person an opportunity to commit an offense does not constitute entrapment.
>
> (b) In this section ``law enforcement agent'' includes personnel of the state and local law enforcement agencies as well as of the United States and any person acting in accordance with instructions from such agents.

It is probably better on voir dire to discuss circumstances leading to entrapment, but let the actual word be spoken by a panel member.

Fantasy/Roll Playing. Usually this is the lynch pin to your case. The Internet is a stage, a masquerade party that user attends to live out their fantasies. The key is, did the user know he/she was dealing with a minor? The jurors have to enter the mind of the defendant to determine this. What clues were present in the case that would lead the jury to decide that the

other user was a minor. What clues are present that the other user was not a minor, which, by the way, IS the truth in Internet sting operations!

Accommodation. This is another spin on fantasy/roll playing. Here, the user is accommodating the other user fantasy, encouraging him/her/it in the hope of meeting that individual for a sexual liaison.

Chat Sessions. This digital evidence will usually be the featured smoking gun by the State. Embrace it, go through it line by line with the defendant in front of the jury. Show the jury what the defendant's mental thoughts were to each message line. If the jury believes that the defendant thought he was dealing with an adult then actual content of the chats becomes irrelevant!

PRETRIAL MOTIONS

Motion to preserve evidence. Discussed above with a sample motion as attachment (B)

Motion to quash. The indictments generated by this statute may be subject to a **motion to quash**. Besides the language of the above solicitation statute, if the State wants to allege an attempted aggravated sexual assault of a child or an indecency with a child by contact/exposure, the elements of those crimes must also be included. Look specifically for the right ages with the appropriate attempted crimes, i.e. under 14 for agg sex assault, under 17 for indecency with a child. Also look for the proper mens rea for each attempt.

Discovery motion. CCP Art. 39.14 does not help much with discovery. However, allege fundamental fairness under the 5th amendment (Brady) for pre trial discovery of all of the digital evidence and scientific reports (EnCase, ILook…) in the possession of the State.

Motions to suppress. When computers are involved, whether they belong to the defendant or the State, suppression issues will be present. For the defendant's computer start with how the State obtained the computer. Search and seizure issues apply to computers as well as any other evidence. The defendant does have a reasonable expectation of privacy in their hard drive. See *United States v. Barth*, 26 F.Supp.2d 929, (D.C. W.D. Texas 1998), *Rogers v. State*, 113 S.W.3d 452, (Tex. App. San Antonio 2003).

If, the evidence came from the State's computer it could be subject to a motion to suppress/dismiss. Grounds could include: CCP Art. 38.35, the lab was not certified to collect the forensic evidence, the methodology used to preserve the evidence was not reliable, material exculpatory evidence was not collected, evidence was tampered with.
Defense counsel will have to make a tactical decision about filing these motions, depending on the judge and the prosecutor involved you may gain an advantage by waiting till trial to raise admissibility issues. Warning, this tactic must be very carefully considered so as not to waive any issue!

VOIR DIRE
Use Power Point or another presentation software to bring your themes to the panel. Outline what you wish to discuss and then refer to this outline on the screen to jog your memory as you conduct voir dire. A sample general voir dire for this type of case is attached as appendix (C).

OPENING STATEMENTS
Use Power Point! Any time Defense counsel has the opportunity to get in front of the jury, consider doing it! If only to echo what the State has already stated in their opening, with a defensive spin of course! Enclosed as attachment (D) is a sample Power Point opening.

CLOSING STATEMENTS
As above, use Power Point. Organize your bullets as you go through the trial. Present only the high points then use the bullets as a foundation for you closing. Enclosed as attachment (E) is a sample closing.

EXPERTS.
As discussed above, experts are difficult to find.

- Jason Velasco with Renew Data Corp. jvelasco@renewdata.com does disk imaging and analysis. He is familiar with EnCase and has testified in both criminal and civil cases.
- David McGroty with Sahara/Digital, mac@saharadigital.com (210) 366-8771, is a data security expert. He is familiar with computer operation, forensic collection of computer evidence, EnCase, Internet and Yahoo! He has testified in criminal cases.

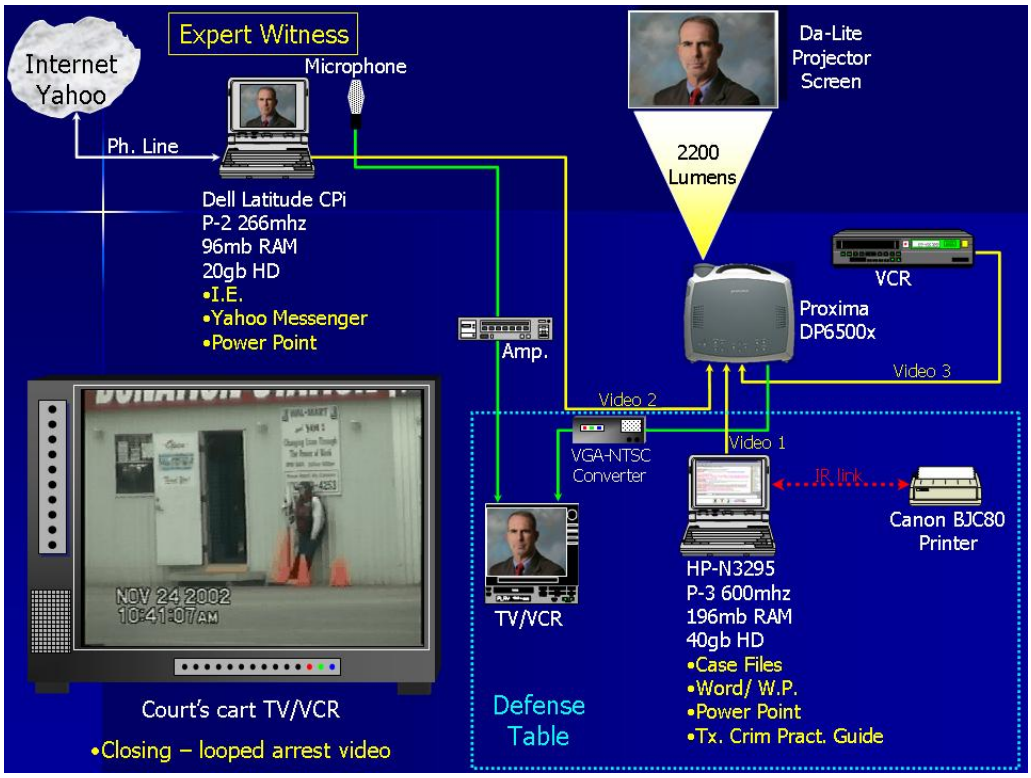
The following persons are all **EnCE** certified and are willing to work with criminal defense attorneys:

- Larry Leibrock Ph.D. eForensics LLC, Leibrock@eForensics.com. Dr. Leibrock has done over 100 cases.
- Rey Anzaldua, rey@genxforensics.com, http://www,genxforensics.com
- Michael De La Cruz, Michael@genxforensics.com, http:/www.genxforensics.com
- Richard Dorough, richarddorough@yahoo.com

Another possible source on computer experts and internet operation are local computer clubs.

- Alamo PC Organization, (http://www.alamopc.org/about/clubs.shtml)

COURT ROOM PRESENTATION
The ability to present evidence in a clear and concise format, the ability to advocate with graphics to illustrate your points is critical to your case. You should map out a plan for the presentation of evidence in your case.

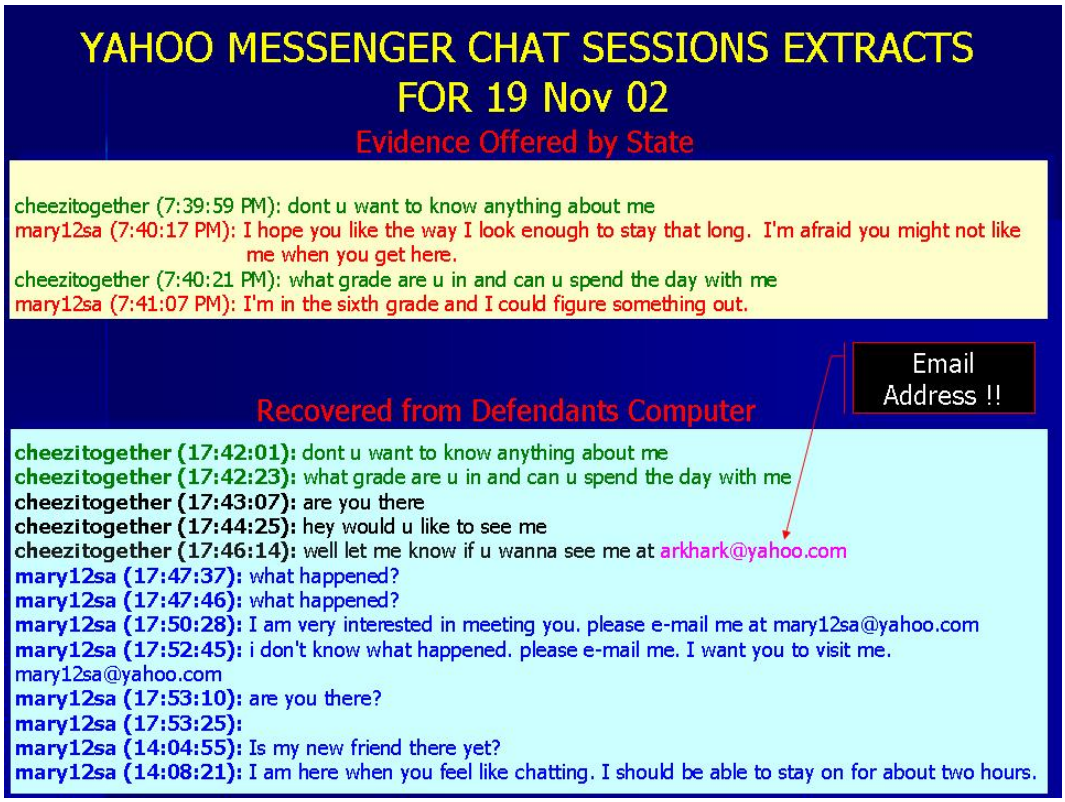


Presentation of a typical internet sting case will start with the lead defense counsel's **laptop computer**. If the laptop has been purchased in the last three years, it is probably powerful enough for static presentations, such as **PowerPoint**. If you desire to play video through the laptop then it should at least be a Pentium III class machine. This computer should be loaded with presentation software such as PowerPoint or **Sanction II**, word processing software such as **Word** or **Word Perfect** and an encyclopedia of law such as the **Texas Criminal Practice Guide**. PowerPoint or Sanction II should be used for Voir Dire, Opening, at trial presentation of evidence, out of the presence of the jury legal arguments to the judge and closing. A **printer** should be available to provide a print out of any legal point the judge may need. The lead counsel's laptop should be connected to a **computer projector** for court room display. This projector should have at least 2000 lumens of light intensity output and a resolution of at least 1024 by 768 pixels. Multiple inputs on the projector are desirable. If your case has an arrest video or other video a **VCR** should be attached to the projector. Most District court rooms have **projector screens**. Check with court personnel on the availability of a screen. If you have to bring your own screen, Da-Lite, http://www.da-lite.com , makes a good line. These types of cases cannot be won without expert testimony on evidence preservation and the medium of communication, Yahoo! Messenger. Consider providing the expert witness with a **laptop** and **internet access** for a live demonstration of Yahoo! Messenger on the computer projector. What the expert testifies to and what he is doing on the computer needs to be preserved for the record. Most court reporters are not set up for preserving this type of testimony. A **microphone** attached to an **amplifier** which is attached to a **TV/VCR** and a **video feed** from the computer projector will preserve the testimony for the record. Finally, a cart mounted **TV/VCR** may be required to play video tapes during closing while the computer projector is displaying your closing argument.

SAMPLE YAHOO! CHAT SESSION

The extracts below are from an actual case.

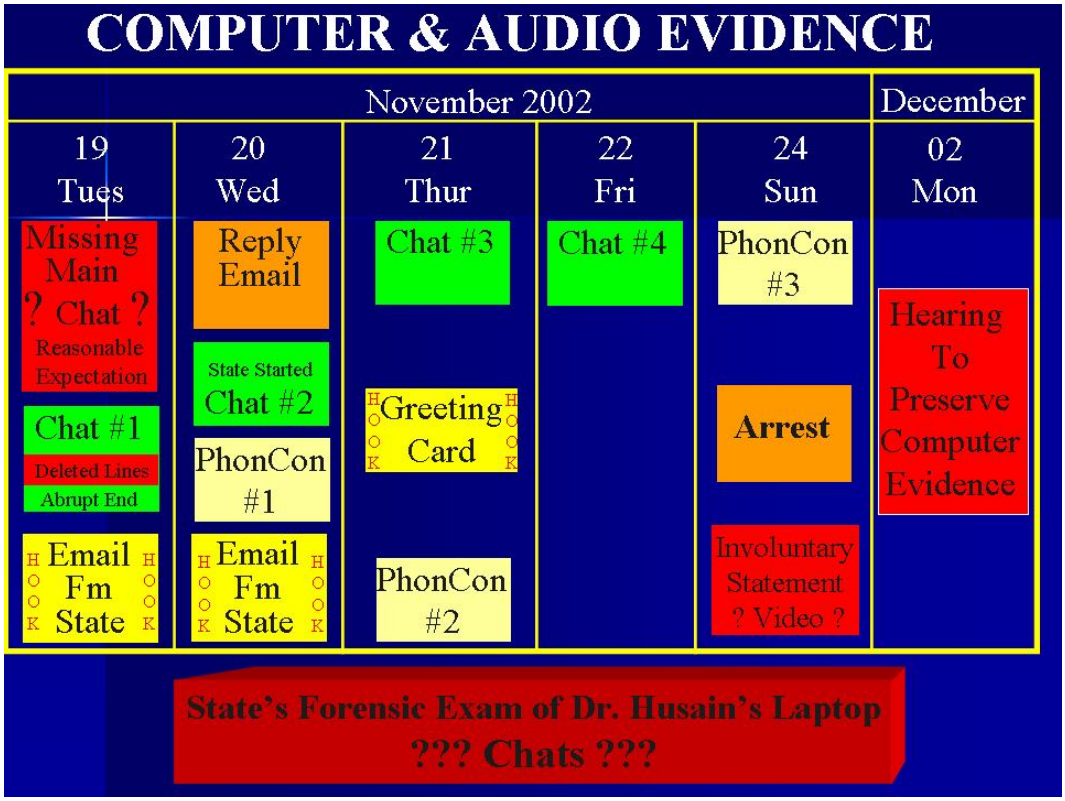
The upper window is what the State offered into evidence, the lower window is what was recovered from the defendants computer for the same time frame! Cheezitogether is the Defendant, mary12sa is the State. Look at the lower window (defendants computer) starting with mary12sa (17:47:37) and below. All of those lines of text were transmitted to the defendant's computer from the state's computer, yet in the upper window (states computer) these lines do not exist! The only possible explanation for this is that the State did not preserve the very lines to text that they transmitted to the defendant! Additionally, note in the upper window (state's computer) the lines of text from mary12sa at (7:40:17) and (7:41:07), now look in the lower window (defendants computer), the defendant never received those lines of text!



In the eyes of the jury these "changes" materially altered the meaning of the chat session. Were these deletions and additions of text intentional?

Note in the lower window (defendant's computer) the line of text at 17:46:14, the email address listed in this text line is present no where else in this case. The defendant's profile did not list this email address. The State's agent would not be able to discover this email address unless the defendant gave it to him/her. Look in the upper window, the State told the jury that they never received that line of text. However, the agent for the State used that very email address to send an email to the defendant within hours of this conservation! So, the agent must have removed that line of text from his preservation of the evidence.

SAMPLE CASE EVIDENCE CHRONOLOGICAL DIAGRAM



KISS, keep it simple stupid always applies with a jury. If you can represent all of the evidence in you case on one demonstrative aid then do so. Below is a sample of a Power Point illustration of the evidence in a Internet sex case.

CONCLUSION

Know your case better than the State, take each piece of evidence and analyze it for admissibility. Decide tactically whether to file a motion or raise the issue at trial. Defense counsel must raise reasonable doubt with the jury that the defendant thought he was dealing with a minor. Be concise, professional and more knowledgeable about technical issues before the jury and an acquittal will follow.

Evidence Number "F01044-A" Alias "WD 36400"

File "E:\F01044\F01044.E01" was acquired by Roger Rabbit at 08/30/01 11:32:37AM.
The computer system clock read: 08/30/01 11:32:37AM.

Acquisition Notes:
SN 420 218 6575.

File Integrity:
Completely Verified, 0 Errors.
Acquisition Hash: 5698D7A0A90ED1DEEA0DF255C91335C2
Verification Hash: 5698D7A0A90ED1DEEA0DF255C91335C2

Drive Geometry:
Total Size 6.0GB (12,594,960 sectors)
Cylinders: 13,328
Heads: 15
Sectors: 63

Partitions:

Code	Type	Start Sector	Total Sectors	Size
0B	FAT32	0	11502540	5.5GB
0B	FAT32	11502540	1092420	533.4MB

Volume "C" Parameters

File System:	FAT32	Drive Type:	Fixed
Sectors Per Cluster:	8	Bytes Per Sector:	512
Total Sectors:	11,502,477	Total Capacity:	5,877,760,000 bytes (5.5GB)
Total Clusters:	1,435,000	Unallocated:	2,930,176,000 bytes (2.7GB)
Free Clusters:	715,375	Allocated:	2,947,584,000 bytes (2.7GB)
Volume Name:		Volume Offset:	63
OEM Version:	MSWIN4.1	Volume Serial #:	0000-0000
Heads:	255	Sectors Per Track:	63
Unused Sectors:	63	Number of FATs:	2
Sectors Per FAT:	11,222	Boot Sectors:	32

Volume "C" Folders

+-🗀 WINDOWS
| +-🗀 SYSTEM
| | +-🗀 SHELLEXT
| | +-🗀 Spool
| | | +-🗀 Drivers
| | | | +-🗀 W32x86
| | | +-🗀 PrtProcs
| | | +-🗀 W32x86
| | +-🗀 IOSUBSYS
| | +-🗀 COLOR
| | +-🗀 VMM32
| | +-🗀 OOBE
| | | +-🗀 MSNSETUP
| | | +-🗀 SETUP
| | | +-🗀 HTML
| | | | +-🗀 MOUSE
| | | | | +-🗀 IMAGES
| | | | +-🗀 ISPSGNUP
| | | +-🗀 IMAGES
| | | +-🗀 ERROR
| | | +-🗀 MSNHTML
| | | | +-🗀 ISPSGNUP
| | | | +-🗀 MOUSE
| | | +-🗀 MSNERROR
| | | +-🗀 MSN
| | | +-🗀 PASSPORT
| | +-🗀 MACROMED
| | | +-🗀 DIRECTOR
| | | | +-🗀 XTRAS
| | | +-🗀 FLASH
| | | +-🗀 SHOCK7
| | | | +-🗀 XTRAS
| | | +-🗀 Shockwave
| | | +-🗀 XTRAS
| | +-🗀 WINMODEM.101
| | +-🗀 QuickTime
| | +-🗀 ShellNew
| | +-🗀 sfp
| | +-🗀 ie
| +-🗀 INF
| | +-🗀 INFBACK
| | +-🗀 CATALOG
| | +-🗀 OTHER
| | +-🗀 QFE
| | +-🗀 STIDRV
| +-🗀 COMMAND
| | +-🗀 EBD
| +-🗀 SYSTEM32
| | +-🗀 DRIVERS
| +-🗀 CATROOT
| | +-🗀 {F750E6C3-38EE-11D1-85E5-00C04FC295EE}
| | +-🗀 {127D0A1D-4EF2-11D1-8608-00C04FC295EE}
| +-🗀 HELP
| +-🗀 CURSORS
| +-🗀 JAVA
| | +-🗀 CLASSES
| | +-🗀 Packages
| | | +-🗀 Data
| | +-🗀 TrustLib
| +-🗀 VCM
| +-🗀 FONTS
| | +-🗀 Corel
| +-🗀 WEB
| | +-🗀 Wallpaper
| +-🗀 DRWATSON
| +-🗀 CONFIG
| +-🗀 MSAGENT
| | +-🗀 INTL
| +-🗀 MEDIA
| +-🗀 PIF
| +-🗀 SAMPLES
| | +-🗀 WSH
| +-🗀 TEMP
| | +-🗀 cometdt
| | +-🗀 _ISTMP1.DIR
| | +-🗀 _ISTMP2.DIR
| | +-🗀 _ISTMP3.DIR
| +-🗀 SYSBCKUP
| +-🗀 APPLOG
| +-🗀 ShellNew
| +-🗀 spool
| | +-🗀 PRINTERS
| +-🗀 MsApps
| | +-🗀 Grphflt
| | +-🗀 MSINFO
| +-🗀 Application Data
| | +-🗀 Microsoft
| | | +-🗀 WELCOME
| | | +-🗀 Internet Explorer
| | | | +-🗀 Quick Launch
| | | +-🗀 Outlook Express
| | | | +-🗀 Mail
| | | | +-🗀 News
| | | +-🗀 texasnet

Volume "D" Parameters

File System:	FAT32	Drive Type:	Fixed
Sectors Per Cluster:	8	Bytes Per Sector:	512
Total Sectors:	1,092,357	Total Capacity:	558,178,304 bytes (532.3MB)
Total Clusters:	136,274	Unallocated:	510,726,144 bytes (487.1MB)
Free Clusters:	124,689	Allocated:	47,452,160 bytes (45.3MB)
Volume Name:		Volume Offset:	11,502,603
OEM Version:	MSWIN4.1	Volume Serial #:	0000-0000
Heads:	255	Sectors Per Track:	63
Unused Sectors:	11,502,603	Number of FATs:	2
Sectors Per FAT:	1,066	Boot Sectors:	32

Volume "D" Folders

+-🗀 RECYCLED
+-🗀 AOL30
| +-🗀 SPOOL
| +-🗀 ORGANIZE
| +-🗀 CCL
| +-🗀 IDB
| +-🗀 MPM
| +-🗀 TOOL
| +-🗀 WINSOCK
| +-🗀 TOD
| +-🗀 TODBKUP
| +-🗀 CACHE
| | +-🗀 USR00101
| +-🗀 AOLTEMP
| +-🗀 AOL4095
| +-🗀 download
+-🗀 America Online 4.0
| +-🗀 csl
| +-🗀 idb
| +-🗀 modems
| +-🗀 tool
| +-🗀 download
| +-🗀 organize
| | +-🗀 CACHE
| +-🗀 spool
| +-🗀 net
| | +-🗀 win98
| +-🗀 TOD
| +-🗀 AOLTEMP
| +-🗀 todbkup
+-🗀 NCDTREE
+-🗀 Unallocated Clusters

Bookmarks

A

1) Full Path: WD 36400\C\WINDOWS\Desktop\Agent\!spring2k_ibi_lilmodix.jpg
File Creation Date: 02/17/00 04:48:18PM
Last Written: 02/17/00 04:49:16PM
Last Accessed: 08/15/00
Modification Date:
Deletion Date:
Logical Size: 56,000
File Type: JPEG

2) Full Path: WD 36400\C\Program Files\NewsRover\Projects\277\files\0027.jpg
File Creation Date: 08/02/00 03:26:38PM
Last Written: 08/02/00 03:26:40PM
Last Accessed: 08/09/00
Modification Date:
Deletion Date:
Logical Size: 57,001
File Type: JPEG

3) Full Path: WD 36400\C\WINDOWS\Desktop\Agent\009aa_u3.jpg
File Creation Date: 02/17/00 04:31:20PM
Last Written: 02/17/00 04:32:02PM
Last Accessed: 08/15/00
Modification Date:
Deletion Date:
Logical Size: 33,788
File Type: JPEG

4) Full Path: WD 36400\C\WINDOWS\Desktop\Agent\2310dgx.jpg
File Creation Date: 11/05/99 03:15:52PM
Last Written: 11/05/99 03:15:54PM
Last Accessed: 08/15/00
Modification Date:
Deletion Date:
Logical Size: 44,210
File Type: JPEG

Appendix (B)

CAUSE NO. NM000000

EX PARTE	**§**	**IN THE DISTRICT COURT**
	§	
	§	
	§	**187TH JUDICIAL DISTRICT**
	§	
	§	
DEFENDANT	**§**	**OF BEXAR COUNTY, TEXAS**

EX PARTE MOTION TO PRESERVE EXCULPATORY EVIDENCE

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES AMIR HUSAIN, Defendant herein, by and through his attorney of Record, ROBERT FEATHERSTON, under the Fourth, Fifth and Sixth Amendments to the Constitution of the United States, made applicable to the States by and through the Fourteenth Amendment to the Constitution of the United States, and under Texas State Constitution Article I Sections 9 & 10, pursuant to the United States Supreme Court decisions in *Brady v. Maryland*, 373 U.S. 83, 83 S. Ct. 1194, 10 L. Ed 2d 215 (1963), *California v. Trombetta*, 467 U.S. 479, 104 S. Ct. 2528 (1984), and *Ake v. Oklahoma*, 470 U.S. 68, 76-77, 105 S.Ct. 1087, 84 L.Ed.2d 53 (1985) and files this Motion to Preserve Exculpatory Evidence. The Defendant respectfully requests this honorable Court to issue an order requiring any and all state agencies to preserve certain computer generated evidence in this case and for cause would show the Court as follows:

I.

The Defendant was arrested on 24 November 2002 at or about 10:35 a.m. by Officers of the San Antonio Police Department, to include but not limited to Detective Freese SAPD # 22222 and Detective Loose SAPD# 22221. The incident was given SAPD case number 02-000000, JN#0000000 and the above entitled night magistrate number. The Defendant was assigned SID #

000000. As a result of the arrest, the Defendant was charged with the offense of Criminal Solicitation of a Minor – Aggravated Sexual Assault, (pre-indictment). Additionally, Law enforcement personnel on 24 November 2002 seized a lap top computer alleged to have been used by the Defendant.

II.

On 25 November 2002 the Defendant and all members of his family withdrew consent to search any property seized by the State of Texas in the above case.

III.

The State will allege that the Defendant participated in online communications with an undercover police officers facilitated by the use of computers and the Internet.

IV.

It is the Defendant's position that the computers used by the State in this alleged solicitation contain exculpatory evidence. To wit, chat room/electronic messaging files, both saved and deleted and that the only way to properly preserve this exculpatory evidence is to secure/seal the use of the subject computer(s) until a forensic clone of the State's hard drive(s) can be obtained.

The forensic clone of the State's hard drive(s) is necessary because under the Windows operating system any time the computer is booted in the Windows environment and the subject data is accessed, it is altered by the computer. Additionally, the Windows environment constantly overwrites sections of the hard drive that contain data that has been deleted but not erased. Continued use of the State's computer in the Window's operating environment will result in this deleted data becoming unrecoverable.

Alterations that occur to the data file upon access include resetting of the last access dates

and possible corruption of the modification and creation dates of subject exculpatory evidence files, in addition to an outright manipulation of the underlying data.

The only way to preserve this information is to forensically clone (copy) the hard drive, preserving the data as is and examine it using a forensic evidence gathering tool such "Encase."

V.

The Defendant is not asking this honorable Court to rule on the release of this data to the defense at this time. The Defendant is merely asking the Court to preserve the evidence. The Defendant will file the appropriate motions for discovery of exculpatory evidence (*Brady* material) during the course of this case if the Defendant is indicted.

VI.

The Defendant further requests that any and all computers seized or voluntarily turned over to the State of Texas in the above case be sealed pending a determination by this honorable Court on the method to be used to examine the subject computers.

WHEREFORE, PREMISES CONSIDERED, the Defendant respectfully prays that this Honorable Court grant his Motion to Preserve Exculpatory Evidence as requested above.

Respectfully submitted,

ROBERT H. FEATHERSTON
TAYLOR & CORREA, P.C.
4718 Camino Dorado
San Antonio, Texas 78233-6301
Telephone: (210) 656-3711
Facsimile: (210) 590-1544
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

Appendix (B)

CAUSE NO. NM000000

EX PARTE	**§**	**IN THE DISTRICT COURT**
	§	
	§	
	§	**187TH JUDICIAL DISTRICT**
	§	
	§	
DEFENDANT	**§**	**OF BEXAR COUNTY, TEXAS**

ORDER

On this _____ day of November A.D. 2002, came on to be heard Defendant's Motion to Preserve Exculpatory Evidence and the evidence and argument of counsel having been heard by the court, and it appearing to the court that said motion should in all things be

GRANTED:

or

DENIED, to which action of the court the defendant excepts.

It is HEREBY ORDERED that the District Attorney's Office immediately notify any state agency that has a computer used to communicate with the above Defendant, SID# 000000, to include but not limited to San Antonio Police Department Case # 02-000000, JN# 0000000 and under an unknown case number with the Sugarland Police Department, to immediately seal said computer(s) until by order of this court a forensic clone of said computer's hard drive(s) is/are produced using a process ordered by this Court.

All State agencies in possession of the subject computers shall identify with specificity, the computer(s) to the court and certify the time at which the computer was sealed.

All computers seized from the Defendant are to remain sealed pending a determination by this honorable Court on the method to be used to examine the subject computers

_____

Judge Presiding

WELCOME

Louis Correa
Robert Featherston

Taylor & Correa, P.C.

REPRESENTING

Donald Duck

PARTICIPATION

- There are no Right or Wrong Answers, we are only trying to understand your views.
- Who can be FAIR.

Before I Become a Judge, I Think You Should Know …

Embarrassed ? Ask

to approach the Judge.

BACKGROUND

- Know the Judge, attorneys, court personnel or witnesses ?
- Any one in law enforcement ?
- Prior jury experience ?
- Membership in civic organizations ?
- Military duty ?
- Physical problems precluding jury service ?

BACKGROUND cont.1

- Publicity involving this case ?
- Who does not want to serve on this type of case ?
- Do you know any of the other panel members ?
- Interest in law or employment in legal field ?

BACKGROUND cont. 2

- Prior accusations of criminal conduct by or against you ?
- Know anyone accused of a crime ?
- Objections
- Meeting in the hall

FAMILY

- Who has children?
- Are they computer literate?
- Surf the internet?
- Chat rooms?
- Parental Responsibility.
- NO MINOR INVOLVED IN THIS CASE!

SOCIAL BACKGROUND

- What's in a name?
- Muslim religion.
- Any one grow up in or visit India?
- Russia?
- Familiarity with police conduct in the above countries?

CRIMINAL SOLICITATION

- Has any one work professionally or as a volunteer with rape victims?
- Any involvement with CPS ?
- Any one a victim of sexual abuse?
- Close family member or friend involved in a case of sexual abuse?

CRIMINAL SOLICITATION cont.

- Discussed sexual matters or allegations of sexual abuse with a child ?
- Difficulty sitting and listening to testimony on this subject ?
- Punishment range for this offense.

INTENT

- Who’s Intent?
- How do you determine it?
- Who’s shoes must you walk in?
- If you have a reasonable doubt as to intent what is your verdict?

POLICE OVERREACHING

- What is that?
- Proactive approach to law enforcement.
- Tulia Drug Sting.

FANTASY

- Masquerade Ball
- Reasonable Expectations, "The Bar"
- First Amendment
- Roll Playing and the Internet
- 1-900
- Fantasy or Reality – when do you know?

DEFENDANT'S STATEMENT

- What makes it Voluntary
- What makes it Involuntary
- He said / She said
- Video Tape, Audio Tape

COMPUTERS & INTERNET

- Who uses a Computer?
- Professionally?
- The Internet?
- Internet Explorer
- YaHoo! Messenger
- Instant Messaging
- Email
- Are computers good at recording data?

COMPUTERS & INTERNET

- Screen/Keyboard Logger Programs?
- Hashing Programs?
- WebCam?
- Chat Rooms?
- Are you anonymous on the Internet?
- Collection of Computer based Evidence

COMPUTERS & INTERNET

- Any one feel intimidated by computers and the internet?
- Who has never used a computer or logged on to the internet
- Who feels they cannot sit on this type of case because of the technology involved?

EXPERTS

- What makes a person an expert ?
- Would you expect a police officer to be an expert?
- Would you believe an expert witness over a regular person ?
- Can an expert be wrong ?
- What would you think of an expert who derives all of their income from the State ?

EXPERTS cont.

- How do you feel about evaluating expert testimony ?
- Can an expert have a bias or motive to testify like any one else?
- Do you know any one who has testified as an expert ?
- Would you accept an expert's testimony just because they are an expert ?

WITNESS CREDIBILITY

- Meet the Press.
- Has anyone here ever had occasion to evaluate the truthfulness of someone's story?
- What observations make a witness more, or less credible to you?

CHARGE OF THE COURT

- This is your Bible.
- You will swear an Oath to follow the law in the Charge.
- You must follow the law.
- Who agrees with this. – Raise your hand.

THE LAW – FACT JUDGES

➢**You are the exclusive judges of the facts proven, of the credibility of the witnesses, and the weight to be given to their testimony, but you are bound to receive the law as stated in these instructions and to be governed thereby.**

(CCP Art 36.13, 38.04)

THE LAW – WHO'S BURDEN

- The law does not require an accused person to prove his innocence or produce any evidence at all.

THE LAW - TESTIFYING

- **A decision by an accused person not to testify cannot be considered as evidence or as a circumstance against the accused person and cannot be held against the accused person.**

- **No conclusion of guilt can be based solely or in part upon an election not to testify.**

- **You are not to consider, discuss, or even refer to this matter during your consideration of this case.**

(clos2)

JURY DELIBERATIONS

- In the jury room a person starts to talk about Defendant not testifying, what is your sworn duty?

Should the Citizen Accused be Required to prove his/her Innocence ?

- **NO! - PRESUMPTION OF INNOCENCE**
- Fundamental !

THE LAW - PRESUMPTION

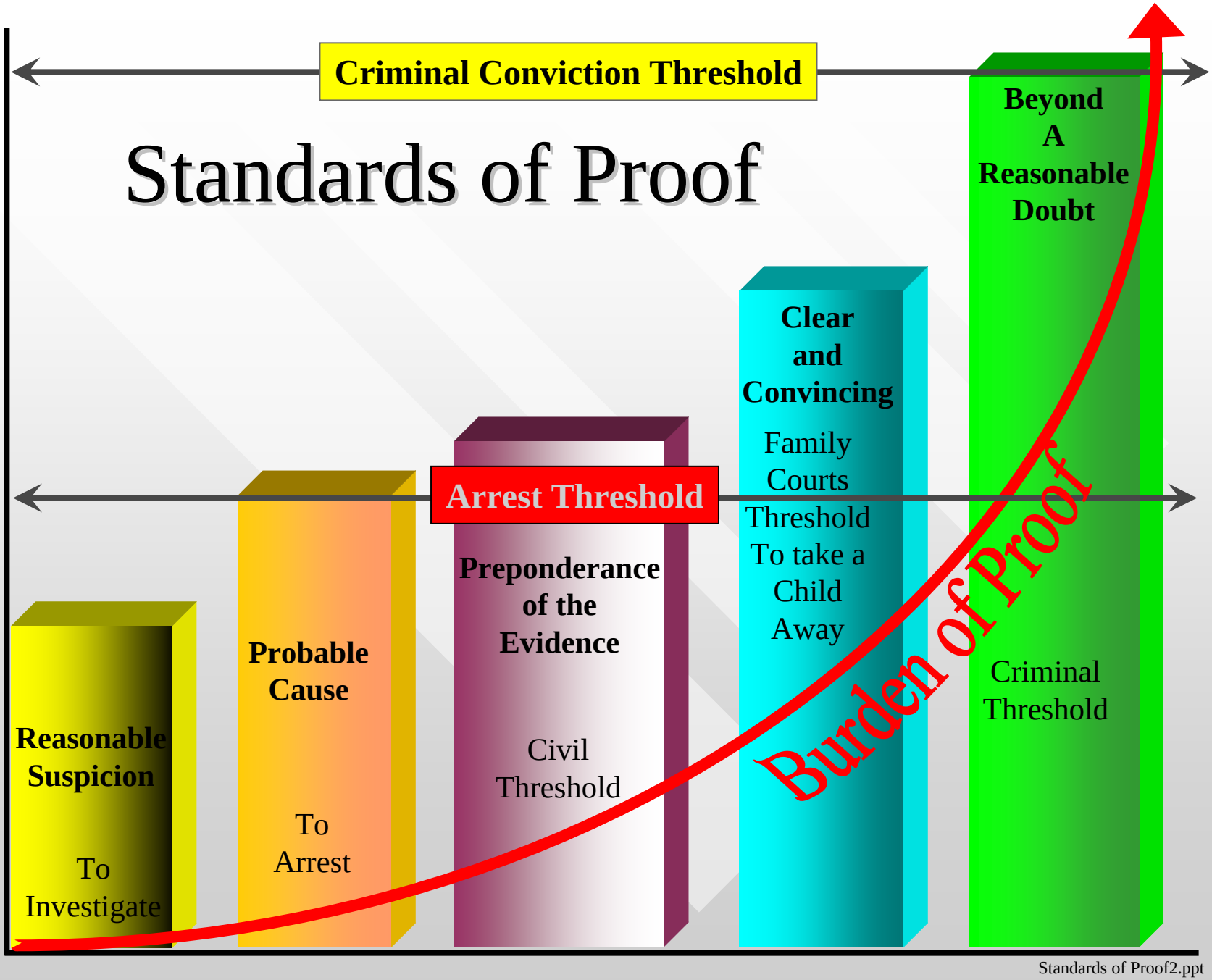
- **All persons are presumed to be innocent and no person may be convicted of an offense unless each element of the offense is proven beyond a reasonable doubt.**

- **The fact that a person has been arrested, confined, or indicted for, or otherwise charged with an offense gives rise to no inference of guilt at his trial.**

(CCP Art. 38.03, PC Sec. 2.01)

TRAFFIC TICKET

- Justified ?
- Nervous ?
- Fumble for drivers license ?
- Trouble finding insurance papers?
- Level of proof ?


Criminal Conviction Threshold
Standards of Proof
Beyond A Reasonable Doubt
Clear and Convincing
Family Courts Threshold To take a Child Away
Arrest Threshold
Preponderance of the Evidence
Civil Threshold
Probable Cause
To Arrest
Reasonable Suspicion
To Investigate
Burden of Proof
Criminal Threshold

PLAUSIBILITY

- If the State's facts are plausible and the Defendant's facts are equally plausible what would be your verdict?

IS DEFENDANT INNOCENT ??

Is there a difference between a jury finding of innocence,

AND

A jury finding that the State has not proved their case beyond a reasonable doubt ?

VERDICT

- After looking at ALL of the evidence, if one piece of evidence raises in your mind a single doubt as to guilt, what is your duty as to your verdict ?
- NOT GUILTY

Thank You !

Fin

REASONABLE SUSPICION

- The reasonableness of a temporary detention must be examined in terms of the totality of the circumstances and will be justified when the detaining officer has specific articulable facts, which taken together with rational inferences from those facts, lead the office to believe that the detained person actually is, has been, or soon will be engaged in criminal activity.

Woods v. State, 956 S.W.2d 33, 38 (Tex.Ct.App. 1997)

PROBABLE CAUSE

- Probable cause for an arrest requires that, at the moment of arrest, the facts and circumstances within the knowledge of the arresting officer and of which the officer has reasonably trustworthy information would justify a reasonable and prudent person in believing that a particular person has committed or is committing a crime.

McCray v. Illinois, 386 U.S. 300, 304, 87 S.Ct. 1056, 18 L.Ed.2d 62, 66-67 (1967)

PREPONDERANCE OF THE EVIDENCE

- As a standard of proof in civil cases, means the greater weight and degree of credible evidence admitted in the case. That degree of proof that, when taken as a whole, shows that a fact sought to be proved is more probable than not.

Lackey v. State, 819 S.W.2d 111 (Tex.Crim.App. 1991)

CLEAR & CONVINCING

- This is an intermediate standard, falling between the preponderance standard of ordinary civil proceedings and the reasonable doubt standard of criminal proceedings.
- It is defined as:
- "That measure of degree of proof that will produce in the mind of the trier of fact a firm belief or conviction as to the truth of the allegations sought to be established."

Edwards v. Texas Department of Protective and Regulatory Services, 946 S.W.2d 130 (Tex.App. – El Paso 1997)

THE LAW – REASONABLE DOUBT

- **The law does not require an accused person to prove his innocence or produce any evidence at all.**

- **It is not required that the prosecution prove guilt beyond all possible doubt; it is required that the prosecution's proof excludes ALL reasonable doubt concerning the defendant's guilt.**

(clos2)

Opening

- The evidence will show:

- THERE IS **NO CHILD** INVOLVED WITH THIS CASE
- **Fantasy**, **Role Play**

The evidence will show:

- No Standard Operating Procedure was used for Forensic Collection of Computer Generated Evidence.
- No Automatic Collection of Computer Evidence.
- No use of Screen Logger Program
- No use of Key Logger Program

The evidence will show:

- No use of Hashing Program.
- No Collection of Main Chat Room Conservations
- Det. Goofey – Audio Tape Quality
- Donald Duck childhood / early adulthood – India, Qatar, Kuwait, & Russia
- Donald Duck licensed Medical Doctor – India & Russia

The evidence will show:

- Donald Duck – Research Scientist for M.D. Anderson Hosp. Houston
- No video tape or audio tape of Donald's alleged statement.
- This statement was Not Voluntary

The evidence will show:

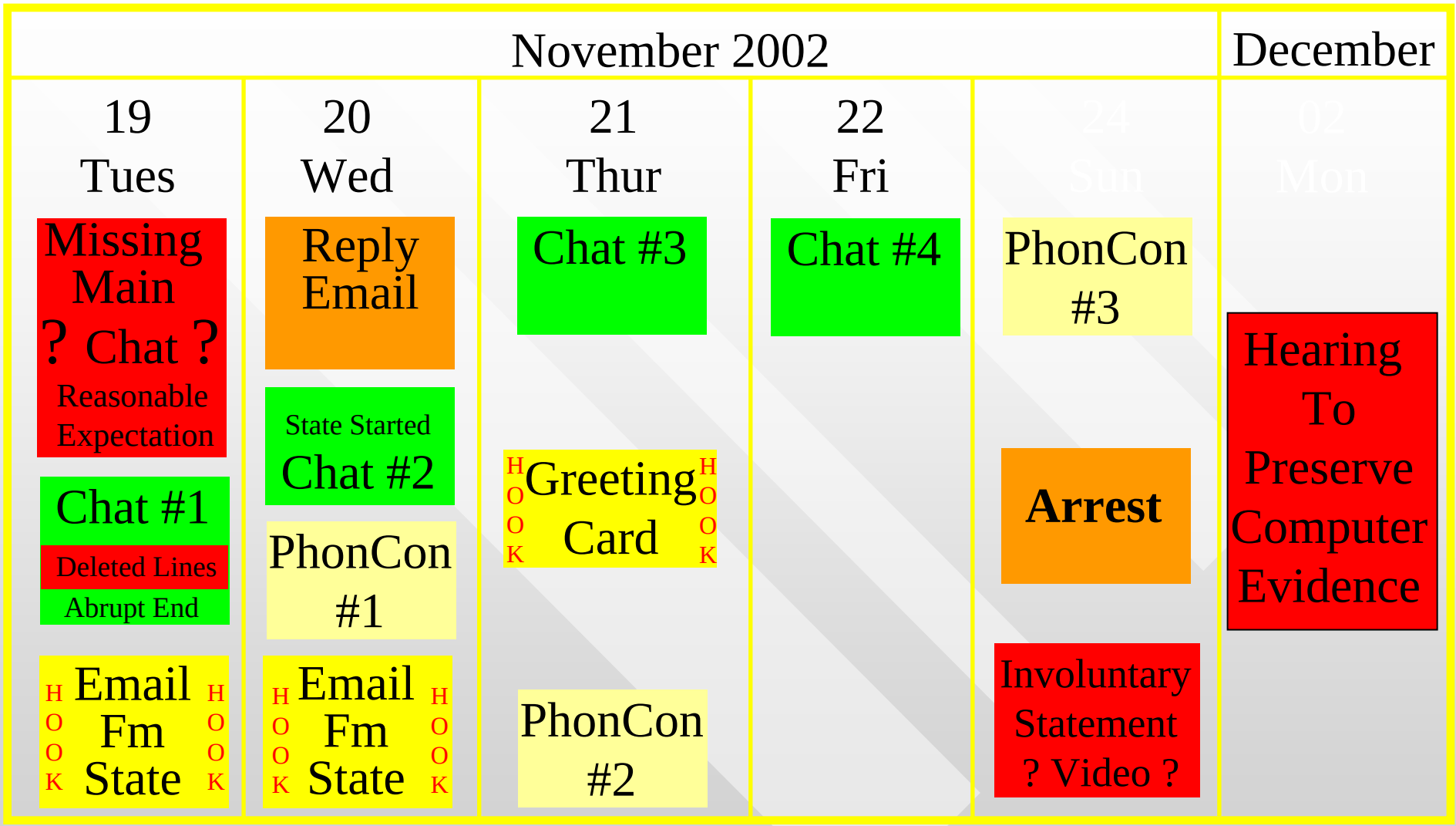
- Affirmatively, Donald Duck had No Intent to have sex with a child.
- THE EVIDENCE WILL SHOW THAT DR. Donald Duck IS NOT GUILTY OF THESE CHARGES.

Thank You !

THOUGHT CRIME

- **THERE WAS NO CHILD INVOLVED IN THIS CASE !!**
- **Who's Role Playing here – Lowe, Herries**
- **Facilitating Role Play & Fantasy**
- **You Must Place Yourself in Dr. Husain's Shoes.**
- **CIRCUMSTANCES SURROUNDING**
  - **". . . as Amir Husain believed them to be, . . ."**
- **1984**

COMPUTER & AUDIO EVIDENCE



DET. LOOSE

- Computer Skills
- **All** the Evidence is here!
- Well I guess I did miss something !
- Email Address!!
- Well, I used my discretion ? ! ? ! ? !
- **!! Intentional Destruction of Evidence !!**
- **Bad Faith !!**
- Facts in the Statement
- If he Left It Out – its **Reasonable Doubt !!**

OFFICER DAFFEY

- Video Tape, She is not a Child !!
- Role Playing
- Actress on the Witness Stand
- Two Octaves down
- Quality of the Audio Tape, whose duty to cure?

Det. PONSE

- His Style, Appearance
- Professional Witness
- Motion to Preserve Evidence
  - “Its all here Judge”
- ? Unbiased ?
- Facts in the Statement
- If he Left It Out – its **Reasonable Doubt !!**

STATE'S STATEMENT

- Not Donald Duck's Statement !
- Shocked & Confused, Handcuffed
- **Fear**
- Raised, India, Qatar, Kuwait, Russia
- No Prior Criminal Experience
- **Requested Attorney**
- Not Voluntary
- Det. Loose's Words
- If you had Donald Duck's background you sign too !
- **Video / Audio Tape**
- When the State Leaves it Out – its **Reasonable Doubt !!**

DAVID McGROTY

- “I would hope that the State’s Computer Experts would be more Qualified than I am.”
- Methods for Preserving Computer Evidence
- **Intentional Destruction** of Computer Evidence!
- Omissions of Material Evidence by the State
- If the State Left It Out – its **Reasonable Doubt !!**

CHARGE OF THE COURT

- This is your Bible.
- You have sworn an Oath to follow the law in the Charge.
- You must follow the law.
- Everyone has agreed to this.

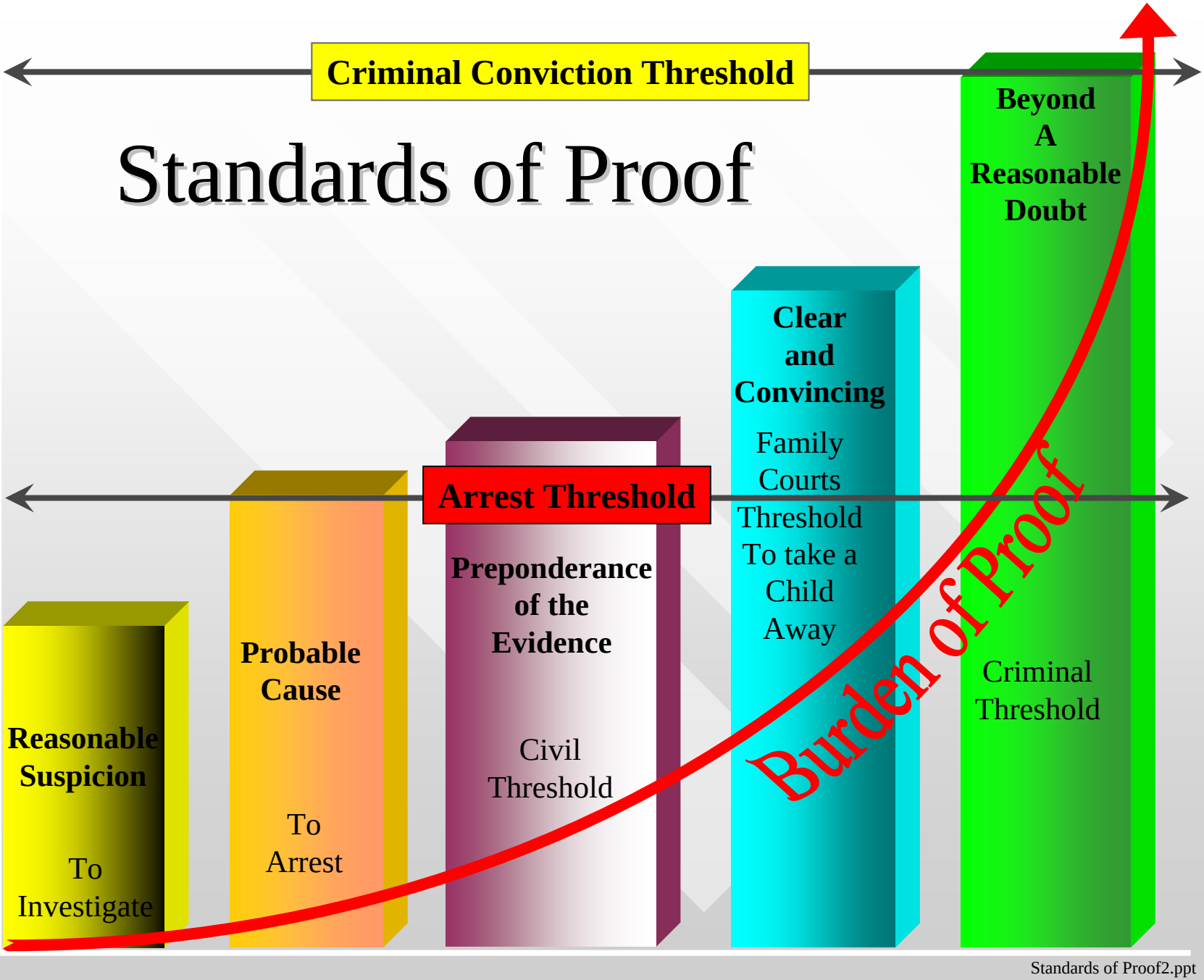
CHARGE OF THE COURT WHO'S BURDEN

- "THE **PROSECUTION** HAS THE **BURDEN** OF PROVING THE DEFENDANT GUILTY AND IT MUST DO SO BY PROVING EACH AND EVERY ELEMENT OF THE OFFENSE CHARGED **BEYOND A REASONABLE DOUBT** AND IF IT FAILS TO DO SO, YOU MUST **ACQUIT** THE DEFENDANT."

CHARGE OF THE COURT

- "You are the exclusive judges of the facts proved, of the credibility of the witnesses and of the weight to be given to the testimony, . . ."

- THE STATE HAS **ROBBED** YOU OF YOUR ABILITY TO SEE ALL OF THE FACTS !
- JUDGE THE CREDIBILITY OF DET LOWE & POTH IN LIGHT OF THE **MISSING EVIDENCE !**
- **IF THE STATE LEFT IT OUT – ITS REASONABLE DOUBT!!!**


Criminal Conviction Threshold
Standards of Proof
Beyond A Reasonable Doubt
Clear and Convincing
Family Courts Threshold To take a Child Away
Arrest Threshold
Preponderance of the Evidence
Civil Threshold
Probable Cause
To Arrest
Reasonable Suspicion
To Investigate
Burden of Proof
Criminal Threshold

CHARGE OF THE COURT JURY DELIBERATIONS

- ". . . **NO** JUROR SHOULD SURRENDER HIS HONEST CONVICTION AS TO THE WEIGHT OR EFFECT OF THE EVIDENCE SOLELY BECAUSE OF THE OPINION OF HIS FELLOW JURORS, OR FOR THE MERE PURPOSE OF RETURNING A VERDICT."

VERDICT

- After looking at ALL of the evidence, if one piece of evidence raises in your mind a single doubt as to guilt, what is your duty as to your verdict ?
- **NOT GUILTY**
- When the State Leaves it Out – THAT'S **REASONABLE DOUBT** !!!