

**Lessons Learned
About
Internet Sex Offenses**

Robert H. Featherston

Law Offices of Correa & Featherston, P.C.

The Travis Building, Suite 340

405 N. Saint Mary's

San Antonio, Texas 7823305

<mailto:robert@correafeatherston.com>

<http://www.correafeatherston.com>

(210) 838-8582

SACDLA

Sexual Assault & Family Violence Offenses

August 25th 2006

Robert Henry Featherston, Esq.

Law Office of Correa & Featherston, P.C.
The Travis Building, Suite 340
405 N. Saint Mary's
San Antonio, Texas 78205
Email:robert@correafeatherston.comt
(210) 838-8582

A D M I T T E D T O P R A C T I C E

United States Court of Appeals for the Fifth Circuit
United States District Court – Western District of Texas
United States District Court – Southern District of Texas
State of Texas

P R O F E S S I O N A L A S S O C I A T I O N S

- American Bar Association
- National Association of Criminal Defense Lawyers
- College of the State Bar of Texas
- Texas Criminal Defense Lawyers Association
- San Antonio Bar Association
- San Antonio Criminal Defense Lawyers Association

E D U C A T I O N

- **THOMAS JEFFERSON SCHOOL OF LAW**, San Diego, Ca. December, 1996
Juris Doctor
- **UNITED STATES NAVY**, Sacramento, Ca. 1979
NAVAL FLIGHT OFFICER DESIGNATION
- **TEXAS A&M UNIVERSITY**, COLLEGE STATION, TEXAS 1977
B.S. ENGINEERING TECHNOLOGY - ELECTRONICS.

P R O F E S S I O N A L E X P E R I E N C E

Partner, Law Office of Correa & Featherston, P.C. (July 2005 - Present)

- Focus exclusively on Criminal Law Practice
- Designated a “[Rising Star](#)” by Scene in SA monthly Magazine October 2005
- Reported Cases Include: [Ex parte Garcia](#), 100 S.W.3d 243; [Ex parte Arredondo](#) 2000 Tex. App. Lexis 8105; [In Re Heins](#), 2000 Tex. App. Lexis 1527; [Rogers v. State](#), 113 S.W.3d 452; [Ex parte Gomez](#), 2003 Tex. App. Lexis 1322; [Ex parte Farias](#), 82 S.W.3d 652; [Husain v. State](#), 2005 Tex App. LEXIS 1419.

Associate, Law Office of Taylor & Correa, P.C. (November 1999 – July 2005)

- Responsible for State & Federal Criminal Cases, Appeals & Writs.

United States Navy (January 1977 - July 1994)

Retired as a Naval Flight Officer under the early retirement program as a Lieutenant Commander.

TABLE OF CONTENTS

INTRODUCTION 5

SCOPE OF PAPER 5

PUBLICITY 5

TYPICAL CLIENT 6

ATTORNEY’S FEES 6

EVIDENCE PRESERVATION 6

SEX REGISTRATION 7

DUTY TO REPORT 7

POSSESSION OR PROMOTION OF CHILD PORNOGRAPHY (TPC 43.26) 7

ONLINE SOLICITATION OF A MINOR (TPC 33.021). 14

CRIMINAL SOLICITATION OF A MINOR (TPC 15.031). 15

DEFENSIVE STRATEGIES 16

PRETRIAL MOTIONS 18

VOIR DIRE 19

OPENING STATEMENTS 19

CLOSING STATEMENTS 19

MITIGATION 19

EXPERTS 20

COMPUTER BASICS 20

FORENSIC COLLECTION OF COMPUTER EVIDENCE 26

GOVERNMENT STANDARDS FOR COLLECTION & ACCREDITATION27

COMPUTER FORENSIC PROGRAMS 28

OTHER COMPUTER PROGRAMS 29

YAHOO MESSENGER 30

SAMPLE YAHOO! CHAT SESSION 36

SAMPLE CASE EVIDENCE CHRONOLOGICAL DIAGRAM. 37

MYSACE.COM. 37

COURT ROOM PRESENTATION 37

CONCLUSION 39

APPENDIX (A) SAMPLE MOTIONS A1

APPENDIX (B) SAMPLE JURY INSTRUCTIONS B1

APPENDIX (C) SAMPLE ENCASE REPORT. C1

APPENDIX (D) SAMPLE VOIR DIRE D1

APPENDIX (E) SAMPLE OPENING E1

APPENDIX (F) SAMPLE CLOSING F1

APPENDIX (G) SAMPLE WARRANTLESS ARREST BRIEF. G1

APPENDIX (H) FEDERAL DISCOVERY ORDER. H1

INTRODUCTION

Law Enforcement Officers; locally, from the Texas Attorney General's Office and various Federal Agencies, 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.

SCOPE OF PAPER

All types of crimes are being actively pursued. However, Child Pornography (TPC 43.26), Online Solicitation of a Minor (TPC 33.021) and the "Traveler Case," "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)), will be the focus of this paper.

PUBLICITY

NO UPSTANDING CITIZEN likes pedophiles, child molesters or sexual predators.

Politicians certainly know this. Jumping on the steam roller to vilify persons convicted of these types of crimes, has no political down side.

Unfortunately, those accused of the above crimes are being swept down the river of conviction by draconian laws, rules of procedure and Court interpretations that favor "Justice."

Look at any news paper, listen to the Bexar County District Attorney, Susan Reed, the Texas Attorney General, Greg Abbott or the U. S Attorney General, Alberto Gonzales, the above three crimes are political gold mines!

Dateline NBC has raised its ratings significantly by running a series of controversial and sensational programs called "To Catch A Predator."

Dateline has stated in its series and Alberto Gonzales has quoted from Dateline, that at any given moment, 50,000 potential child molesters were prowling the Internet. When questioned on the figure Dateline could provide no hard statistics to back this up and has since dropped using the figure. However, numerous law enforcement agencies continue to use the quote because, Alberto Gonzales use this figure in a speech given in April of 2006 (<http://www.msnbc.msn.com/id/13529278>).

The general public is being conditioned by our political leaders, law enforcement and the media to believe that anyone accused of one of the above crimes is a evil predator.

Herein lies the rub for the defense attorney. Have no illusions, these types of cases are an uphill battle from the onset. Besides the technical issues that may actually show your accused client is innocent, finding a jury panel that can set aside the rhetoric, ignore the publicity, consider only the facts of this case, and see your client as a person, with faults or not, is a tall order to strive for.

TYPICAL CLIENT

Usually male, late teens on up. Enough education to use a computer, surf the web and know how to use Yahoo! Messenger, Email, instant messaging, web cams... 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 is essential, to have the client evaluated by a psychiatrist and have an Abel Assessment of Sexual Interest completed. Some of these clients are actually compelled to do what they do. While this may not rise to the level of an insanity defense, the clients psychological makeup can be powerful mitigation evidence.

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!

EVIDENCE PRESERVATION.

If your client's case involves any communication with any party over the internet, 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, Criminal Solicitation of a Minor, Online Solicitation of a Minor and Child Pornography sting cases, the material portion of the case is made by the computer. This is a double edge sword for both the State and the defendant, nothing can be hidden from a competent forensic examiner, because all of the computer communication will come across a computer controlled by either the State, the Defendant or an Internet Service Provider. EVERYTHING should be preserved.

Internet Sex Offenses

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.

A subpoena to the internet service provider and host of the parent communications program (Yahoo! AOL, MySpace...) for logs and chat files must be done. This subpoena must be issued as soon as possible as some providers only hold this type of data for 30 days.

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.

SEX REGISTRATION

Possession or Promotion of Child Pornography is a lifetime registration requirement, CCP 62.101(a)(2). Criminal Solicitation of a Minor and Online Solicitation of a Minor are 10 year registration requirements, CCP 62.101(c)(2).

DUTY TO REPORT

Section 261.101, Family Code, provides that an attorney has a duty to report child abuse or neglect that comes to his attention. The requirement to report "applies without exception to individual whose personal communications may otherwise be privileged, including an attorney," § 261.101(c), Family Code; *Bordman v. State*, 56 S.W.3d 63, 67-68 (Tex. App. - Houston [14th Dist.] 2001 *pet.ref'd*). The duty to report should not apply if the attorney has a reasonable belief that the incident has already been reported.

POSSESSION OR PROMOTION OF CHILD PORNOGRAPHY (TPC 43.26)

In Texas, defending a child pornography (CP) case involving the internet falls into two broad categories:

- The defendant did not knowingly or intentionally possess CP.
- The images are not CP.

Knowing or Intentionally Possessing Child Pornography

Possessing Child Pornography includes the following elements:

- a. Knowing or intentionally.
- b. Possesses
- c. Material containing film image visually depicting child under 18 years of age engaging in sexual conduct
- d. With knowledge material depicts this.

The entire statute is produced below with emphasis:

§ 43.26. POSSESSION OR PROMOTION OF CHILD PORNOGRAPHY.

SUBCHAPTER B. OBSCENITY

(a) A person commits an offense if:

(1) the person **knowingly** or **intentionally** possesses visual material that visually depicts a **child younger than 18** years of age at the time the image of the child was made who is engaging in **sexual conduct**; and

(2) the person **knows** that the material depicts the child as described by Subdivision (1).

(b) In this section:

(1) "Promote" has the meaning assigned by Section 43.25.

(2) "Sexual conduct" has the meaning assigned by Section 43.25.

(3) "Visual material" means:

(A) any film, photograph, videotape, negative, or slide or any photographic reproduction that contains or incorporates in any manner any film, photograph, videotape, negative, or slide; or

(B) any disk, diskette, or other physical medium that allows an image to be displayed on a computer or other video screen and any image transmitted to a computer or other video screen by telephone line, cable, satellite transmission, or other method.

(c) The **affirmative defenses** provided by Section 43.25(f) also apply to a prosecution under this section.

(d) An offense under Subsection (a) is a felony of the third degree.

(e) A person commits an offense if:

(1) the person knowingly or intentionally promotes or possesses with **intent to promote** material described by Subsection (a)(1); and

(2) the person knows that the material depicts the child as described by Subsection (a)(1).

(f) A person who possesses visual material that contains **six or more identical** visual depictions of a child as described by Subsection (a)(1) is presumed to possess the material with the intent to promote the material.

(g) An offense under Subsection (e) is a felony of the second degree.

Added by Acts 1985, 69th Leg., ch. 530, § 2, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 361, § 1, eff. Sept. 1, 1989; Acts 1989, 71st Leg., ch. 968, § 1, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994; Acts 1995, 74th Leg., ch. 76, § 14.51, eff. Sept. 1, 1995; Acts 1997, 75th Leg., ch. 933, § 1, eff. Sept. 1, 1997; Acts 1999, 76th Leg., ch. 1415, § 22(c), eff. Sept. 1, 1999.

Please note that each CP image is an allowable unit of prosecution, *Ex parte Gonzalez*, 147 S.W.3d 474, 479 (Tex.App. San Antonio 2004, no pet.). Additionally, concurrent or consecutive sentences are permitted, TPC 3.03(b)(2).

Internet Sex Offenses

A Client has a reasonable expectation of privacy in his/her hard drive, see *United States v. Barth*, 26 F.Supp.2d 929, 932 W.D. Tex. 1998 and *Rogers v. State*, 113 S.W.3d 452 (Tex.App. San Antonio 2003 no pet.) Therefore, how the client's computer came to the attention of the State is a very important issue for search & seizure purposes. Additionally, besides traditional fourth Amendment search & seizure law, the Texas Constitution and exclusionary rule, Texas also has a statute entitled "Breach of Computer Security," TPC 33.02, which within the meaning of the statute, makes it a crime have unauthorized access to a computer. This makes discovery of CP on the client's computer by a third party subject to suppression under Texas law.

§ 33.02. BREACH OF COMPUTER SECURITY.

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) An offense under this section is a Class B misdemeanor unless in committing the offense the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, in which event the offense is:

(1) a Class A misdemeanor if the aggregate amount involved is less than \$1,500;

(2) a state jail felony if:

(A) the aggregate amount involved is \$1,500 or more but less than \$20,000; or

(B) the aggregate amount involved is less than \$1,500 and the defendant has been previously convicted two or more times of an offense under this chapter;

(3) a felony of the third degree if the aggregate amount involved is \$20,000 or more but less than \$100,000;

(4) a felony of the second degree if the aggregate amount involved is \$100,000 or more but less than \$200,000; or

(5) a felony of the first degree if the aggregate amount involved is \$200,000 or more.

(c) When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, damage, or deletion of property may be aggregated in determining the grade of the offense.

(d) A person who his subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, § 2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994; Acts 1997, 75th Leg., ch. 306, § 2, eff. Sept. 1, 1997; Acts 2001, 77th Leg., ch. 1411, § 1, eff. Sept. 1, 2001.

How the Images got on the Client's Computer.

The State has the burden of proving knowing and intentional possession. With respect to knowing and intentional possession, how the images got on the client's computer is just as important as where on the client's computer the images are stored. The client's computer is at the end of the largest distribution of knowledge ever invented by man, the Internet.

Web sites, Search Engines, Hot links & Pop-Ups. Anyone who uses the World Wide Web, conducts searches using search engines such as Google, or Yahoo!, visits different web sites, is subject to having thousands of images in the form of web site graphics, photographs and thumbnails downloaded on to their computer without knowing what those images are till they are already downloaded to their computer's hard drive and viewable. In addition, web sites routinely download tracking files, called "cookies" which the owner of the computer never sees. An unintentional visit to the wrong site or having your computer hijacked to the wrong type of site could result in the download of hundreds of images of pornography or child pornography. It is not uncommon for a client who has been hijacked to or entered a site that contains child

pornography to have no idea those images are now on his/her computer because they failed to scroll down and examine the whole page.

Distributed File Sharing Networks. Thousands of users using the same type of file sharing software connect their computers together using the Internet to share files. The practice originally started to share music files and has grown to the sharing of any file type including child pornography. The issue for the defense attorney is that, the client by joining such a network can lose control of what is being uploaded to and downloaded from his computer. Some of the most popular file sharing program now in use include Gnutella, BitTorrent, KaZaA, eMule, Freenet, I2P, GUNet and Entropy. True pedophiles who collect child pornography usually have thousands of images. The images are usually indexed so the pedophile can quickly access the type of material he/she is looking for. Some pedophiles are technically proficient and able to store their collections on other unsuspecting computers in these distributed networks. If your client has no idea how such an extensive collection got on to his computer, he may be a victim of a pedophile who is using your client's computer to store his/her collection. On August 04th 2006, Broadwing Communications, an internet service provider based in Austin Texas, had one of its computers hijacked by Hezbollah's Al-Manar television station. Al-Manar used the hijacked connection to place video streaming broadcasts on the internet. For a client that leaves his/her computer on all of the time, has a broadband connection, does not use or has improperly configured a firewall, does not use or has out of date virus software, his/her computer is ripe for hijacking.

Networking & Computer Access. The state in order to prove the elements of possession or distribution of CP has to prove, beyond a reasonable doubt, that it was your client who was accessing the child pornography files. Does your client have exclusive use of the target computer? If other persons have access the answer is no. Whether those persons are family members, co-workers, friends, neighbors or unknown persons from the Internet, exclusive use of the target computer can be hard to prove for the State. Wireless networking in the office and at home has thrown in a new issue. Is the wireless network open or secured. What type of security is being used. Is the neighbor or another worker within range of the client's wireless network using that network and the client's computer to obtain and store CP? On August 2nd 2006, USA TODAY, reported that even offline wireless networking equipped computers can be hacked, used and controlled without the owners knowledge.

http://www.usatoday.com/tech/news/computersecurity/hacking/2006-08-02-wireless-hackable_x.htm?POE=TECISVA

Viruses, Trojans & Back Doors. The presence of any malicious software on your client's computer raises the issue of exclusive access. Another computer user has managed to download on to your client's computer software, images... that your client was unaware of. Malicious back doors such as "BackOrifice," allows another user, complete control of your client's computer without your client's knowledge.

Chat Rooms, Instant Messaging. Yahoo! Messenger, AOL instant messaging, Sprint, T-Mobile, Cingular and many others all have chat rooms and instant messaging. Most have the capability to attach images to their messages. The majority of the communication providers retain their logs for at least 30 days and are subject to subpoena. Your client may have been the victim of the receipt of a unsolicited message containing an image of CP. However, more often

than not this is a serious area of liability for your client. The presence of CP can usually be traced to a solicited line of communications, which goes a long way towards the State proving knowing and intentional possession. Approximately 66% of defendants convicted of Criminal Solicitation of a Minor over the internet have CP on their computers. Defense Counsel should closely examine the communication stream that resulted in the depositing of CP on the client's computer to see if the images were solicited or not.

Email. Was the message solicited or arrived unsolicited. Did the client transmit an email with an attached image of CP? Was it really your client that transmitted the message or someone else using his/her computer at the keyboard or remotely? Email on its face can be damaging. The State has a leg up in proving your client knowingly or intentionally possessed images of CP. Defense Counsel is usually left with, if it of course is true, claiming someone other than his client used his computer or IP address to send/receive the message.

Where the Images are Stored on the Client's Computer.

The State often takes the position that if images of CP are on the client's computer then they were knowingly and intentionally obtained, this is not necessarily the case. If the images are located in the Temporary Internet Files or if they are located in a cached file that is automatically controlled by a communications program, then image files can get onto the hard drive without the client's knowledge. However, some Texas counties are still prosecuting clients who have CP images in these locations. It should be noted, for reasons listed above, that a client's computer could contain thousands of images of CP, all indexed into categories and all placed there by a pedophile without your client's knowledge.

Images are not Child Pornography

In Texas you cannot discuss the Issue of Possession or Promotion of Child Pornography without looking at TPC 43.25 Sexual Performance by a Child.

In [*Ashcroft v. Free Speech Coalition*](#), 535 U.S. 234, 122 S.Ct. 1389, 1405, 152 L.Ed.2d 403 (2002), the Supreme Court stated that the Federal prohibition on the possession of Child Pornography included only images of actual children. Then in response to a Constitutional challenge to the Texas CP Statute, TPC 43.26, The Second Court of Appeals stated that the plain language of the statute indicates that it prohibits only possession of material that depicts an actual child, not material that merely "appears" to depict a child. The Court further stated: "The plain language of *section 43.26* clearly requires the State to prove that (1) the appellant possessed visual material depicting a child under the age of eighteen engaging in sexual conduct and (2) appellant knew that the material depicted a child engaging in sexual conduct. Although the defendant may choose to counter the State's evidence with evidence that the child depicted was eighteen years of age or older, the statute does not place the burden on the defendant to prove the age of the child. That burden rests with the State. [*Webb v. State*](#), 109 S.W. 3d 580, 583-584 (Tex.App. Fort Worth 2003, no pet.)

Internet Sex Offenses

Then the Texas Legislature modified TPC 43.25 to include a procedure for determining when a image is of a child younger than 18 years of age, as set out below:

§ 43.25. SEXUAL PERFORMANCE BY A CHILD.

SUBCHAPTER B. OBSCENITY

(a) In this section:

(1) "Sexual performance" means any performance or part thereof that includes sexual conduct by a child younger than 18 years of age.

(2) "Sexual conduct" means sexual contact, actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, sado-masochistic abuse, or lewd exhibition of the genitals, the anus, or any portion of the female breast below the top of the areola.

(3) "Performance" means any play, motion picture, photograph, dance, or other visual representation that can be exhibited before an audience of one or more persons.

(4) "Produce" with respect to a sexual performance includes any conduct that directly contributes to the creation or manufacture of the sexual performance.

(5) "Promote" means to procure, manufacture, issue, sell, give, provide, lend, mail, deliver, transfer, transmit, publish, distribute, circulate, disseminate, present, exhibit, or advertise or to offer or agree to do any of the above.

(6) "Simulated" means the explicit depiction of sexual conduct that creates the appearance of actual sexual conduct and during which a person engaging in the conduct exhibits any uncovered portion of the breasts, genitals, or buttocks.

(7) "Deviate sexual intercourse" and "sexual contact" have the meanings assigned by Section 43.01.

(b) A person commits an offense if, knowing the character and content thereof, he employs, authorizes, or induces a child younger than 18 years of age to engage in sexual conduct or a sexual performance. A parent or legal guardian or custodian of a child younger than 18 years of age commits an offense if he consents to the participation by the child in a sexual performance.

(c) An offense under Subsection (b) is a felony of the second degree.

(d) A person commits an offense if, knowing the character and content of the material, he produces, directs, or promotes a performance that includes sexual conduct by a child younger than 18 years of age.

(e) An offense under Subsection (d) is a felony of the third degree.

(f) It is an **affirmative defense** to a prosecution under this section that:

(1) the defendant was the spouse of the child at the time of the offense;

(2) the conduct was for a bona fide educational, medical, psychological, psychiatric, judicial, law enforcement, or legislative purpose; or

(3) the defendant is not more than two years older than the child.

(g) **When it becomes necessary for the purposes of this section or Section 43.26 to determine whether a child who participated in sexual conduct was younger than 18 years of age, the court or jury may make this determination by any of the following methods:**

(1) personal inspection of the child;

(2) inspection of the photograph or motion picture that shows the child engaging in the sexual performance;

(3) oral testimony by a witness to the sexual performance as to the age of the child based on the child's appearance at the time;

(4) expert medical testimony based on the appearance of the child engaging in the sexual performance; or

(5) any other method authorized by law or by the rules of evidence at common law.

Added by Acts 1977, 65th Leg., p. 1035, ch. 381, § 1, eff. June 10, 1977. Amended by Acts 1979, 66th Leg., p. 1976, ch. 779, § 1, eff. Sept. 1, 1979; Acts 1985, 69th Leg., ch. 530, § 1, eff. Sept. 1, 1985; Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994; Acts 1999, 76th Leg., ch. 1415, § 22(b), eff. Sept. 1, 1999; Acts 2003, 78th Leg., ch. 1005, § 4, 5 eff. Sept. 1, 2003.

Internet Sex Offenses

This procedure has placed the rules for admitting photographs on its head. Additionally, this procedure may be subject to a Confrontation Clause challenge under [Crawford v Washington](#), 541 US 36.

If the Court or the jury are allowed to determine if the subject image of of a child younger than 18 years of age and you have a good faith belief that the image is not of a real child, don't forget to educate both the judge and jury about Barbra Stanwyck: Barbra Stanwyck was an American film actress with a distinguished career from 1927 through 1964.



She never posed nude, however, there she is with no clothes on, of course the image on the right is a fake. However because it is a .jpg image only a person with personal knowledge could tell you it is a fake. Even an expert would have a difficult time telling you if it is real because of the compression scheme used to make the digital image. Defense Counsel should use [United States v. Katz](#), 178 F.3d 368, 373 (5th Cir. 1999) in an attempt to convince the Court that a pretrial determination of what images may be CP is necessary. [Katz](#) was a child pornography case in which government had to prove that a model, who is post-puberty but appears quite young, is less than 18 years old, the Court opined that expert testimony may well be necessary to assist the trier of fact to understand evidence or to determine fact in issue. [Fed.Rules Evid.Rule 702, 28 U.S.C.A.](#)

The images that the State provides you in discovery, are the images that the State has to use at trial. “Decision to exclude high quality, color images produced from computer disk delivered to child pornography defendant, as sanction for government's attempt to sandbag defense by providing it, during discovery, only with poorer quality, black and white copies of these same images, was not abuse of district court's discretion, where prejudice to defendant, whose defense was premised on expert testimony as to age of models depicted, was high, particularly since defendant was arrested shortly after controlled delivery of computer disk and had no information about contents of these images other than what he learned during discovery.” [United States v. Katz](#), 178 F.3d 368, 373 (5th Cir. 1999)

AFFIRMATIVE DEFENSES

The affirmative defenses listed in TPC 43.25(f) are available for a CP case, they are:

- a. Defendant had a good faith reasonable belief that the child was 18 years of age or older.
- b. Defendant was the spouse of the child at the time of the offense
- c. The conduct was for a bona fide educational, medical, psychological, psychiatric, judicial, law enforcement or legislative purpose, or
- d. Defendant not more than two years older than the child.

ONLINE SOLICITATION OF A MINOR (TPC 33.021)

This is a new statute making it an offense for any one over the age of 17 to communicate in a sexually explicit manner or distribute sexually explicit material to a minor over the internet. No one has yet challenged this statute on 1st amendment grounds as void for being too vague.

§ 33.021. ONLINE SOLICITATION OF A MINOR.

- (a) In this section:
 - (1) "Minor" means:
 - (A) an individual who represents himself or herself to be younger than 17 years of age; or
 - (B) an individual whom the actor believes to be younger than 17 years of age.
 - (2) "Sexual contact," "sexual intercourse," and "deviate sexual intercourse" have the meanings assigned by Section 21.01.
 - (3) "Sexually explicit" means any communication, language, or material, including a photographic or video image, that relates to or describes sexual conduct, as defined by Section 43.25.
- (b) A person who is 17 years of age or older commits an offense if, with the intent to arouse or gratify the sexual desire of any person, the person, over the Internet or by electronic mail or a commercial online service, intentionally:
 - (1) communicates in a sexually explicit manner with a minor; or
 - (2) distributes sexually explicit material to a minor.
- (c) A person commits an offense if the person, over the Internet or by electronic mail or a commercial online service, knowingly solicits a minor to meet another person, including the actor, with the intent that the minor will engage in sexual contact, sexual intercourse, or deviate sexual intercourse with the actor or another person.
- (d) **It is not a defense** to prosecution under Subsection (c) that:
 - (1) the meeting did not occur;
 - (2) the actor did not intend for the meeting to occur; or
 - (3) the actor was engaged in a fantasy at the time of commission of the offense.
- (e) **It is a defense** to prosecution under this section that at the time conduct described by Subsection (b) or (c) was committed:
 - (1) the actor was married to the minor; or
 - (2) the actor was not more than three years older than the minor and the minor consented to the conduct.
- (f) An offense under Subsection (b) is a state jail felony, and an offense under Subsection (c) is a felony of the third degree, except that an offense under Subsection (b) or (c) is a felony of the second degree if the minor is younger than 14 years of age or is an individual whom the actor believes to be younger than 14 years of age.
- (g) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

Added by Acts 2005, 79th Leg., ch. 1273, § 1, eff. June 18, 2005.

CRIMINAL SOLICITATION OF A MINOR (TPC 15.031)

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.

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

**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

Internet Sex Offenses

(f) In this section, "minor" means an individual younger than 17 years of age.
(EMPHASIS ADDED)

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."

Section (e) gives notice that the punishment is one category lower than the attempt. For example, if 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.

To date all challenges to the legal or factually sufficiency of the evidence and all constitutional challenges to the above three statutes have failed. However, in a Arizona Supreme Court case, Mejak v. Hon. Granville, CV-05-0299-PR (2006), interpreting a statute similar to TPC 15.031, reversed and remanded the case because the sting operation was conducted by the media and not law enforcement.

DEFENSIVE STRATEGIES

Preservation/admissibility of evidence, conduct of the police, entrapment, fantasy, roll playing accommodation, location, how alleged CP files got on client's computer and are the images really CP, are the probable pillars of the defense in this type of case. For solicitation cases, remember – EVERY ONE LIES ON THE INTERNET, and if it is a sting case, 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 part of appendix (A).

Internet Sex Offenses

Admissibility of Evidence. The material evidence usually involved in the solicitation cases includes:

1. Chat room public window.
2. Instant Messages.
3. Email.
4. Greeting Cards.
5. Computer logs.
6. Web Camera (still photos or video)
7. Transmitted photos
8. Recorded Phone Conversations.
9. Surveillance or arrest videotape.

In CP cases the evidence begins by placing the client at the computer manipulating the digital files, where and how the digital files arrived on the computer and whether the digital files are CP.

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)

The Preference for Arrest Warrants in Texas. Once Defense Counsel has shown the Court that the client was arrested without a warrant, the burden shifts to the State to show the warrantless arrest was statutorily authorized. This is an important concept in all three of the above statutes. All three crimes can be completed over the internet without the client leaving the keyboard. In almost all cases the State has enough information to obtain an arrest warrant prior to encountering your client and in most cases they don’t obtain one. If the Court agrees with you that an arrest warrant should have been obtained, then the Court may suppress the fruits of the arrest, to include any statements made by your client. A brief on the subject is attached as Appendix (I).

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

Internet Sex Offenses

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 in the solicitation cases 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 solicitation case, however it is precluded by statute in the Online Solicitation of a Minor 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.

MITIGATION

All three of these types of cases are tough to win an outright acquittal. More often victory is measured by keeping the client out of jail. If you are going to go to trial you must prepare for the punishment phase of trial, hopefully you want get to it, but odds are that you will. The conviction rate for all three of these crimes to date is almost 100%. Most of the District Attorneys in Texas have a stated policy of jail time offers only for these offenses. That leaves you preparing your mitigation case. Most clients that are charged with these types of crimes are

otherwise law abiding citizens, they have never been arrested much less convicted of any crime. Most of these clients are compelled to do what they do. They are unable to cope with the most powerful emotion a human can have, human sexuality. Getting your client properly evaluated and having expert testimony ready to go can be the difference between jail time and probation and if the State slips and opens the door to this type of testimony during the guilt/innocence phase of the trial, it may result in an acquittal.

EXPERTS

As discussed above, technical 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 **Encase** 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>)

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),

Internet Sex Offenses

- 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 there 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 there 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 .

Internet Sex Offenses

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.

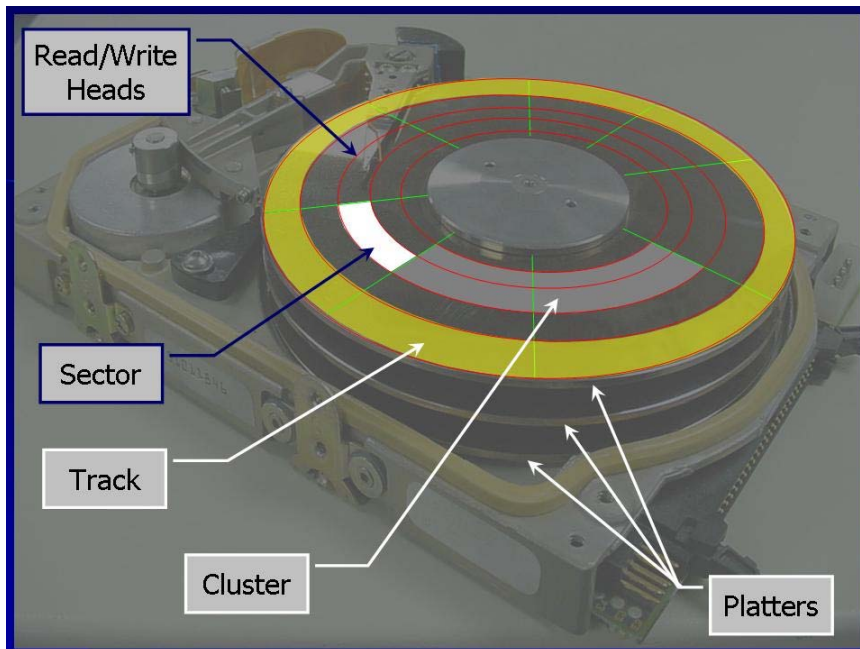
Logically the hard drive consists of cylinders, tracks, sectors, clusters, file allocation table and partitions.

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!

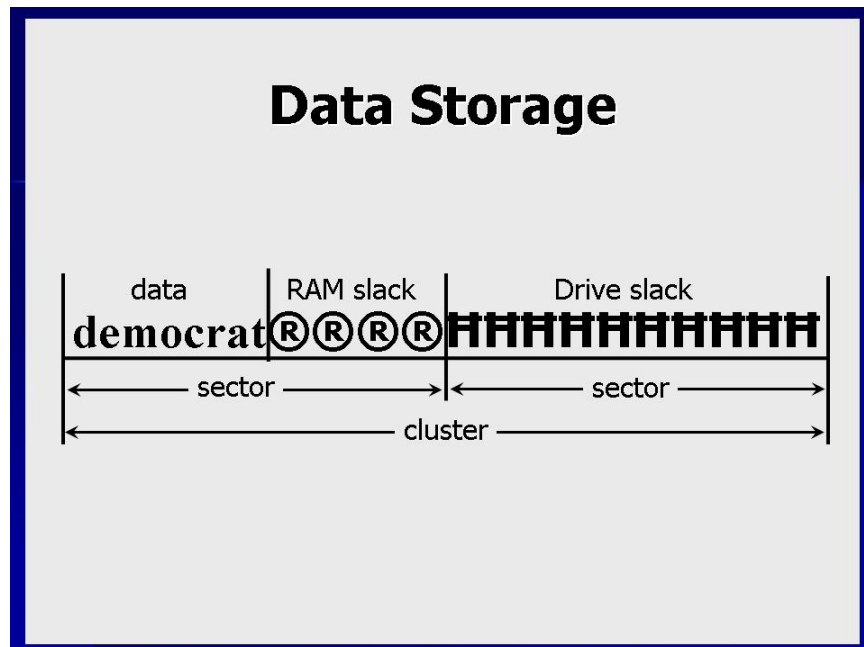
File Slack is the data storage space that exists from the end of the file to the end of the last cluster assigned to the file. Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. Larger cluster sizes mean 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 menu, 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 heels 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.  This program is touted as the gold standard of forensic tools. It 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.”


Internet Sex Offenses

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

OTHER COMPUTER PROGRAMS



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 defendant's hard drive. A computer contains thousands of files, most dealing with the operating system and programs installed. If an 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 digests for use by law enforcement and other organizations in computer forensics investigations, http://www.nsrll.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 level 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 conversation 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.

Internet Sex Offenses

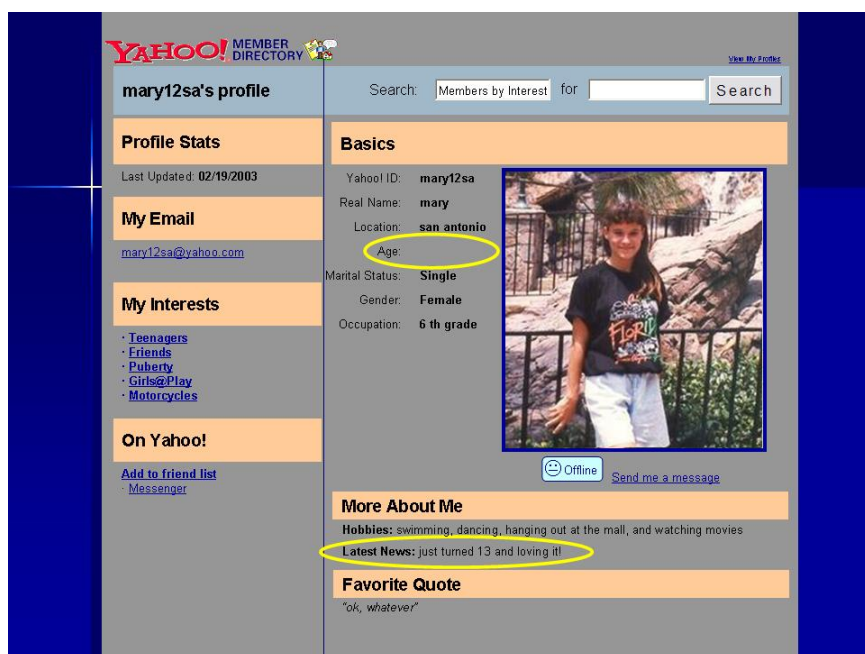
Users are required to be at least 18 years of age to participate in the chat rooms.



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.



Internet Sex Offenses

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!

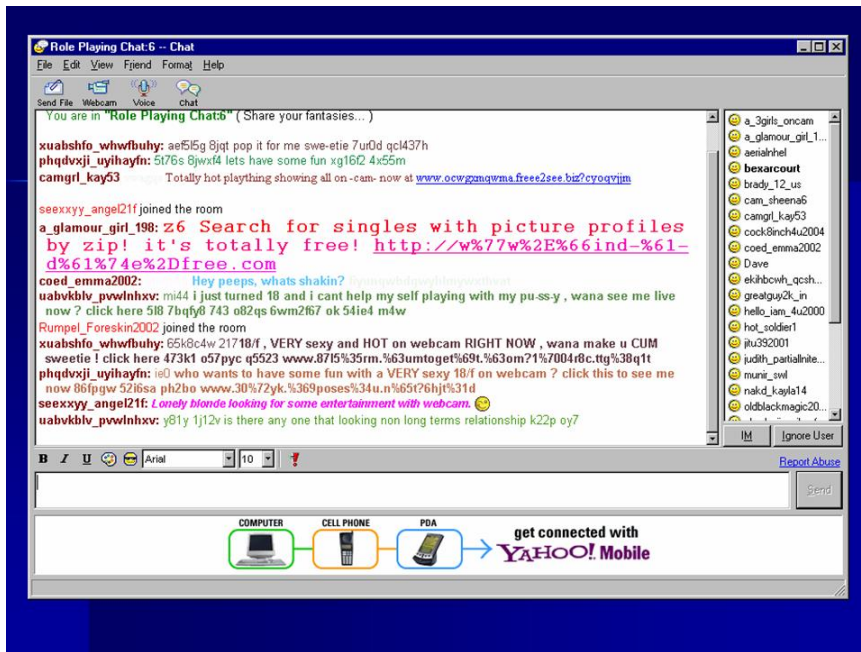
A constant theme that you should reinforce to the jury is that every one lies in these chat rooms and on their profiles. How many pictures of Nichole Kidman are on users profiles?



After a particular chat room has been chosen, the main chat screen will open. This is the window that establishes the character of the conversations, 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

Internet Sex Offenses

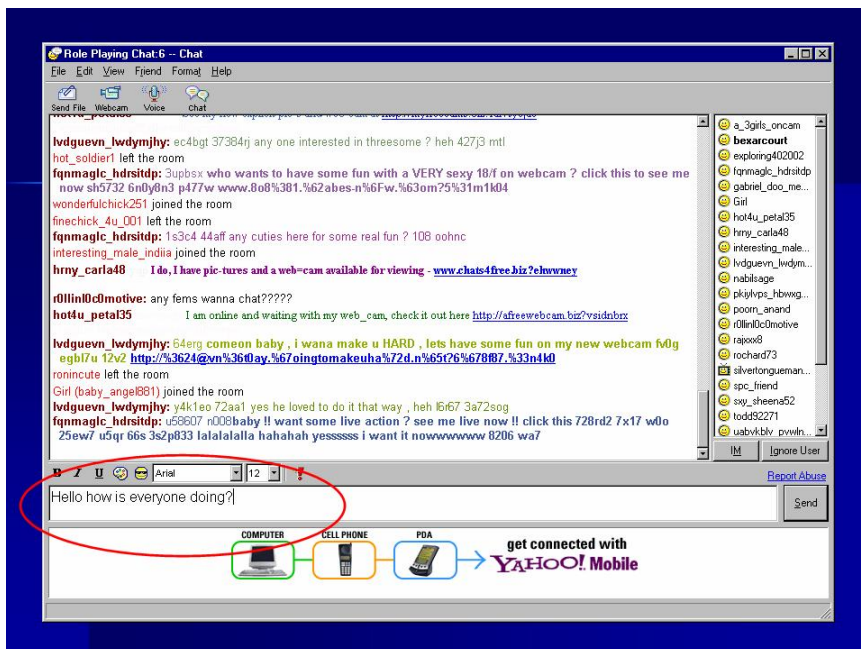
listing of all of the participants in that particular chat room, by “screen name”. Below the area where the public chat sessions are in progress is a box for the user to type in a message that will be displayed on the public window.



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

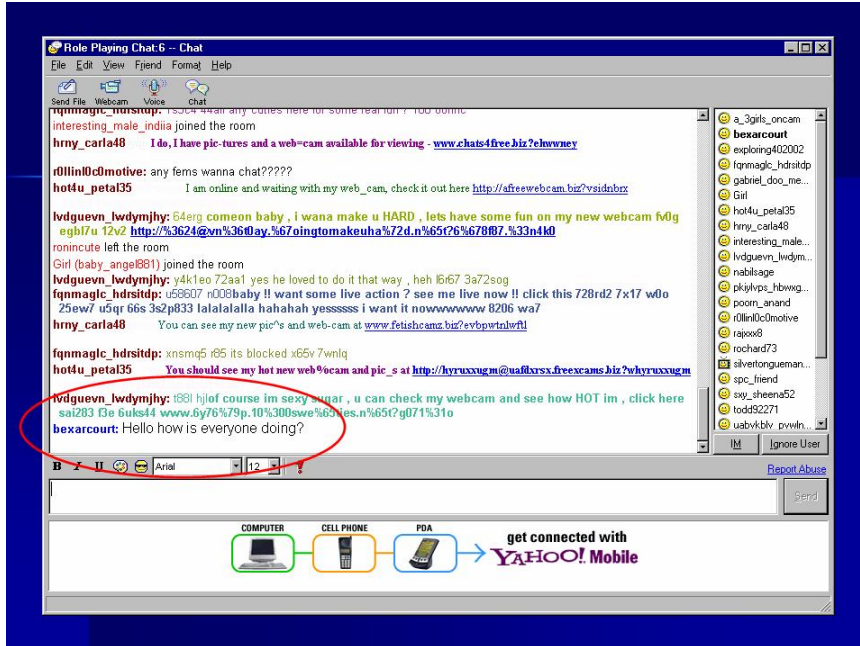
has preserved this evidence. Depending on what the evidence shows, defensive theories such as fantasy/roll play or accommodation may come into play, or the content may plainly demonstrate the need for an entrapment defense.

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.



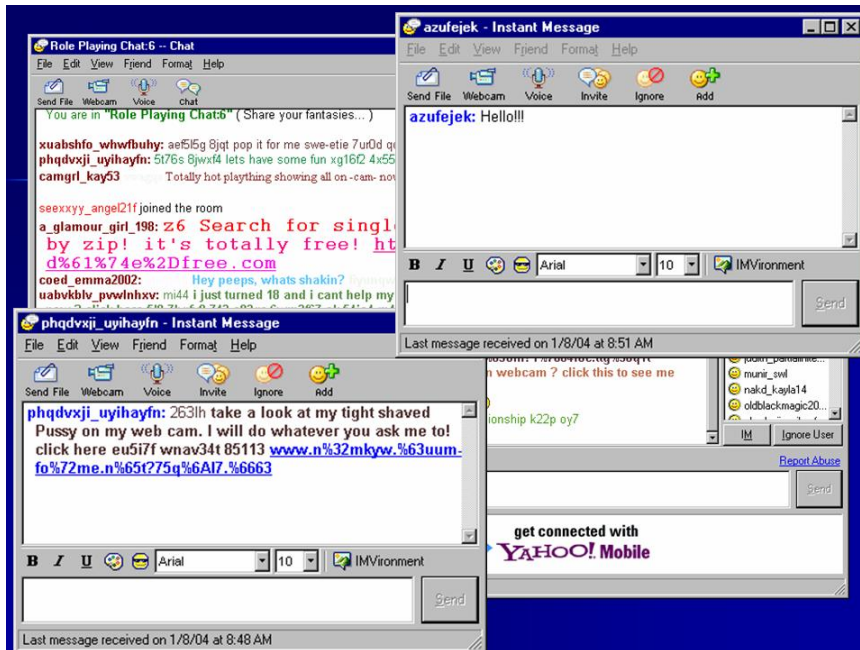
Public communication is established by the user typing his/her message in the box below the public window.

Internet Sex Offenses



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.

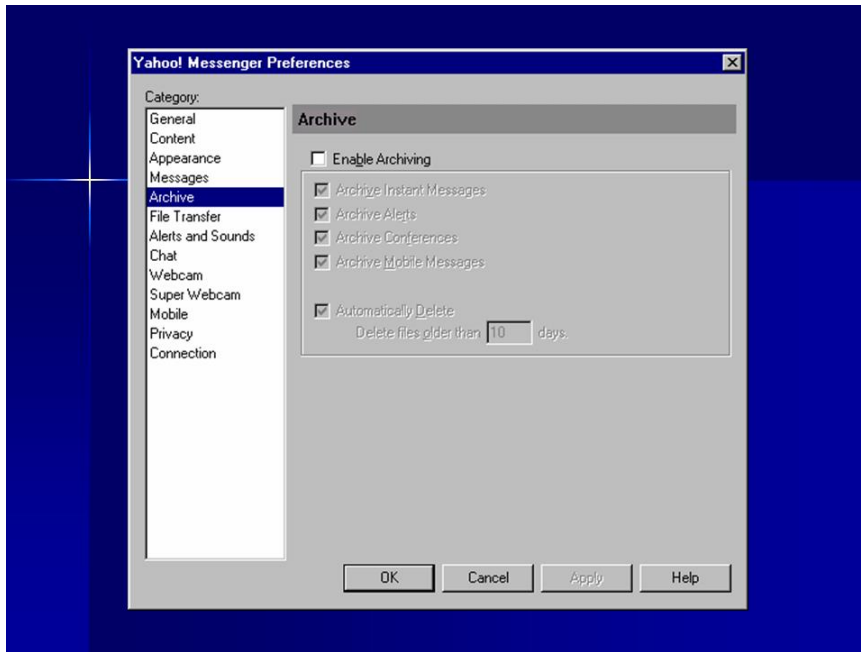


A user can send an instant message by simply double clicking on the screen name of the user he/she wishes to contact, either from the listing of screen names on the right side of the screen. When this selection is made an instant message window will pop up for the user to type his/her message into and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

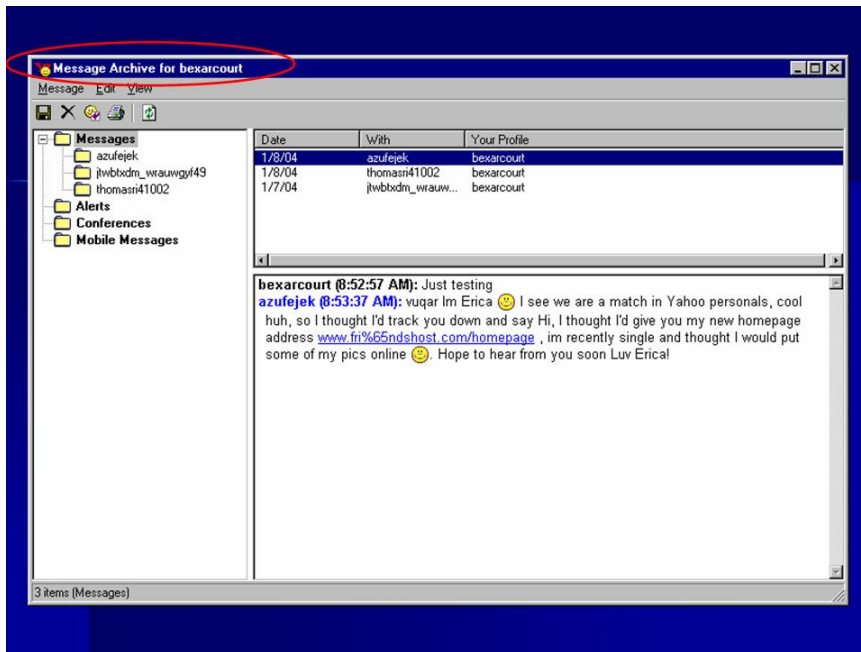
screen.

Internet Sex Offenses

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.

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

**YAHOO MESSENGER CHAT SESSIONS EXTRACTS
FOR 19 Nov 02
Evidence Offered by State**

cheezitogether (7:39:59 PM): dont u want to know anything about me
mary12sa (7:40:17 PM): I hope you like the way I look enough to stay that long. I'm afraid you might not like me when you get here.
cheezitogether (7:40:21 PM): what grade are u in and can u spend the day with me
mary12sa (7:41:07 PM): I'm in the sixth grade and I could figure something out.

Recovered from Defendants Computer

cheezitogether (17:42:01): dont u want to know anything about me
cheezitogether (17:42:23): what grade are u in and can u spend the day with me
cheezitogether (17:43:07): are you there
cheezitogether (17:44:25): hey would u like to see me
cheezitogether (17:46:14): well let me know if u wanna see me at arkhark@yahoo.com
mary12sa (17:47:37): what happened?
mary12sa (17:47:46): what happened?
mary12sa (17:50:28): I am very interested in meeting you. please e-mail me at mary12sa@yahoo.com
mary12sa (17:52:45): i don't know what happened. please e-mail me. I want you to visit me.
mary12sa@yahoo.com
mary12sa (17:53:10): are you there?
mary12sa (17:53:25):
mary12sa (14:04:55): Is my new friend there yet?
mary12sa (14:08:21): I am here when you feel like chatting. I should be able to stay on for about two hours.

Email Address !!

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,

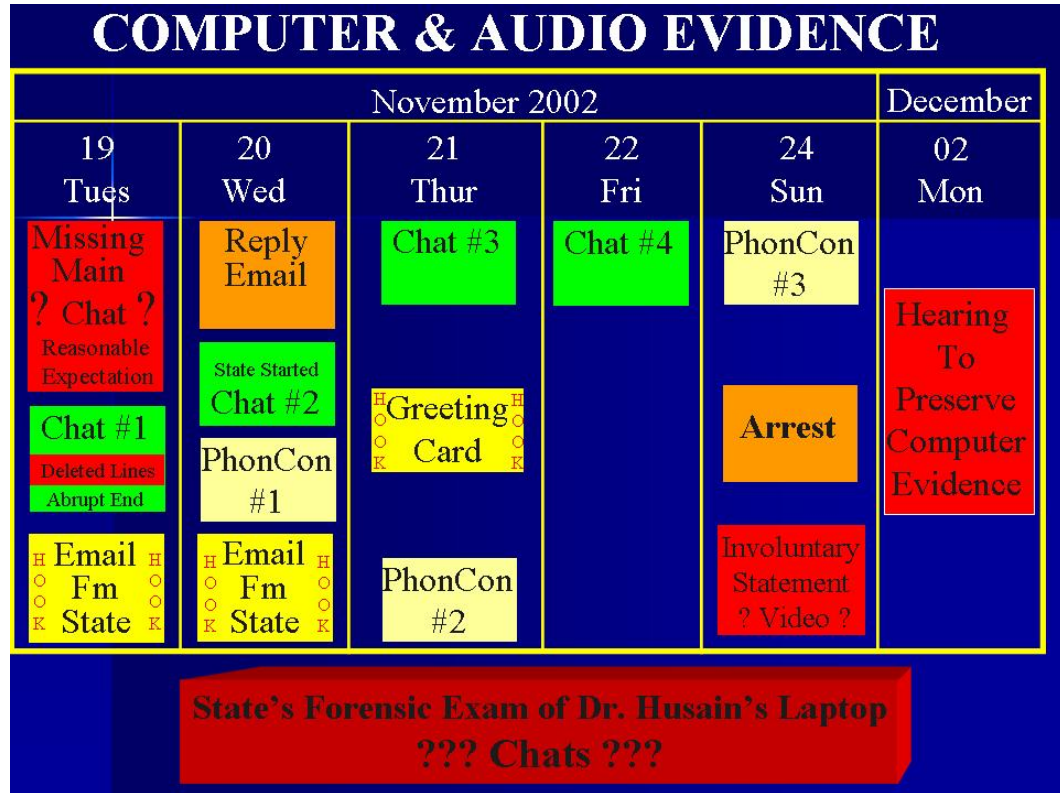
yet in the upper window (states computer) these lines do not exist! The only possible explanation for this is that the State did not preserve the very lines to text that they transmitted to the defendant! Additionally, note in the upper window (state's computer) the lines of text from mary12sa at (7:40:17) 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 conversation! So, the agent must have removed that line of text from his preservation of the evidence.

SAMPLE CASE EVIDENCE CHRONOLOGICAL DIAGRAM



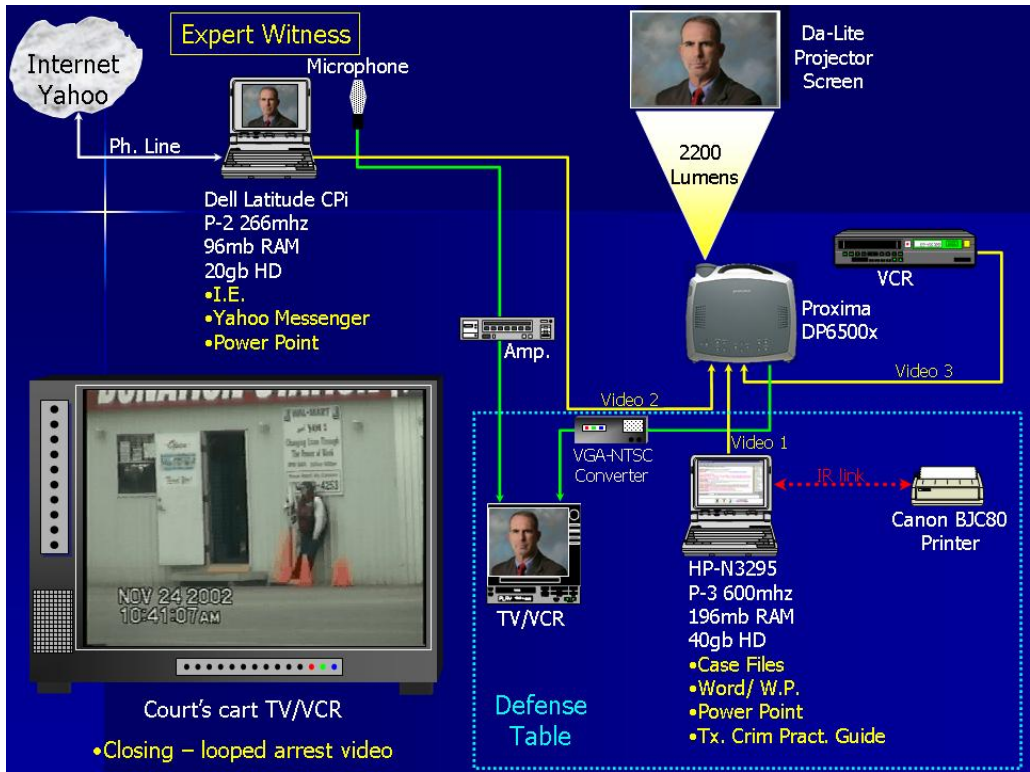
KISS, keep it simple stupid always applies with a jury. If you can represent all of the evidence in your case on one demonstrative aid then do so. Below is a Power Point illustration of the evidence in a Internet sex case.

MYSFACE.COM

This site receives more traffic on a daily basis than Google. The site focus is on teenagers with provisions for member web sites, instant messaging, chat rooms, blogs, music downloads and more. Law Enforcement is known to monitor this site and run sting operations.

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.

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.

CAUSE NO. NM777777

EX PARTE

§
§
§
§
§
§
§

IN THE DISTRICT COURT

187TH JUDICIAL DISTRICT

JOHN SMITH

OF BEXAR COUNTY, TEXAS

EX PARTE MOTION TO PRESERVE EXCULPATORY EVIDENCE

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, 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 Scott Lee Poth SAPD # 2178 and Detective Terry Linn Lowe SAPD# 2400. The incident was given SAPD case number 02-794964, JN#0987193 and the above entitled night magistrate number. The Defendant was assigned SID # 792743. As a result of the arrest, the Defendant was charged with the offense of Criminal

Appendix (A)

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.

Appendix (A)

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 FEATHERSTON
CORREA, & FEATHERSTON, P.C.
The Travis Building, Suite 340
405 N. Saint Mary's
San Antonio, Texas 78233-6301
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT**

CAUSE NO. NM777777

EX PARTE

§
§
§
§
§
§
§

IN THE DISTRICT COURT

187TH JUDICIAL DISTRICT

JOHN SMITH

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, JOHN SMITH, SID# 799999, to include but not limited to San Antonio Police Department Case # 02-777777, JN# 0988888 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

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT’S MOTION FOR EQUAL ACCESS IN COURT ROOM
(3RD TRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through Robert H. Featherston, his attorney of record, and files this his Defendant’s Motion for Equal Access in Court Room, and would respectfully show to this Court as follows:

I.

Defendant hereby moves this Court for an order allowing him equal access to the intranet and other presentation technology installed by the State in the courtroom. Specifically, Defendant moves this Court for an order allowing him access to the internet, as well as electronic aids and equipment used to make computer visual demonstrations during the trial of this cause.

II.

Defendant would show that he is accused of a crime that originated on the internet. The internet will play a very important role in the presentation of both the State’s and Defendant’s case. As part of Defendant’s presentation, he will require access to the internet, and sufficient space so as to place a large screen within view of the jury and litigants, as well as space to allow a projector to project the image on the screen.

III.

Appendix (A)

Failure to allow the Defendant access as requested, and to present his defense as set forth herein, will deny Defendant an equal opportunity to present his defense, and deprive him of a fair trial. Defendant would show that he is entitled to this request under the Equal Protection Clause, his right to effective assistance of counsel, and the Due Process Clause, as guaranteed by the United States Constitution and Due Course of Law under the Texas Constitution.

WHEREFORE, PREMISES CONSIDERED, the Defendant respectfully prays that this Honorable Court set this motion for a hearing prior to trial; that Defendant be granted all relief requested herein; that this Court order that Defendant be given access to the internet during the trial of this cause; that this Court order that trial occur in a court room large enough to allow Defendant to set up his equipment and present his computer and internet evidence; and for all other relief to which Defendant may otherwise show himself entitled.

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the 23rd day of December, 2005.

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175 TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS
	§	

ORDER ON DEFENDANT’S MOTION FOR EQUAL ACCESS IN COURTROOM
(3RD TRIAL)

On this the ____ day of _____, 2006, came on to be considered the above-styled and numbered motion, and said motion is hereby: **GRANTED** / **DENIED**.

IT IS FURTHER ORDERED THAT:

1. The Bexar County District Attorney’s Office provide Defendant’s computer network with access to the internet via the existing Internet connection used by the District Attorney’s Office in the 187th ‘s courtroom, using equipment provided by the Defense. This connectivity shall be in place and tested by _____ day of January, 2006.
2. The Bexar County District Attorney’s Office provide equal access to courtroom audio & video presentation equipment used by State in the above entitled cause.

SIGNED this _____ day of _____, 2006.

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175 TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS
	§	

BRADY MOTION FOR PRODUCTION AND INSPECTION OF EVIDENCE
WHICH MAY LEAD TO EXCULPATORY EVIDENCE
(3RD TRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, the Defendant in the above entitled and numbered cause, by and through Counsel, and would, pursuant to Article 2.01, Texas Code of Criminal Procedure, and the authority of *Brady v. Maryland*, 373 U.S. 83 (1963), request that the State produce for inspection all evidence and information which may lead to favorable evidence on the issues of Defendant's guilt or innocence, or upon the issue of punishment in the event of a finding of guilt, including but not limited to the following:

I.

A complete digital copy of the digital video tape that recorded events surrounding the arrest of Defendant at his meeting with a undercover police officer on 24 November, 2002.

II.

Defendant would show that he has previously been provided with a VHS copy of the digital video arrest tape, that the VHS is of far inferior quality (250 horizontal scan lines), when compared to the digital version (500 horizontal scan lines), in the possession of the State, and that the digital version has a significantly higher degree of resolution, providing a more clear picture of events. Defendant would suggest that he needs at least the same degree of resolution

Appendix (A)

as may be possessed by the State in its media in order to properly prepare his case.

WHEREFORE, PREMISES CONSIDERED, the Defendant submits to this Court that the failure or refusal to produce any or all of the foregoing evidence or information by the Prosecution constitutes a suppression of evidence and a violation of the Fifth, Sixth and Fourteenth Amendments to the United States Constitution, Article I, Sections 10 and 19 of the Texas Constitution, and Articles 1.04, 1.05, 1.051(a), and 2.01 of the Texas Code of Criminal Procedure, and substantially denies the Defendant the effective assistance of Counsel and a fair trial.

Defendant prays for the Court to grant this Motion in all things.

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the 23rd day of December, 2005.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

ORDER

BE IT REMEMBERED, that on the _____ day of _____, 2006, came on to be considered the above and foregoing Motion for Exculpatory Evidence by Defendant. After consideration of the same, it is the opinion of the Court that the same be:

() GRANTED, and in such regard the Court hereby orders the Attorney for the State to produce such evidence requested be furnished within least seven (7) days of the entry of this order.

() DENIED, to which ruling the Defendant excepts.

() SET FOR HEARING ON THE _____ day of _____, 2006, at _____ o'clock _____.

Signed this _____ day of _____, 2006.

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175 TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S MOTION TO QUASH INDICTMENT
(3RD TRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through Robert H. Featherston, his attorney of record, and files this his Defendant's Motion to Quash Indictment, and would respectfully show to this Court as follows:

I.

Defendant would submit that the charging instrument and the underlying statute are facially unconstitutional as being in violation of the First Amendment to the United States Constitution as it is being applied to this Defendant herein.

WHEREFORE, PREMISES CONSIDERED, the Defendant respectfully requests that the indictment in the above cause be set aside and quashed pursuant to the First Amendment, due process and equal protection clauses of the Fourteenth Amendment of the U. S. Constitution; the due course of law provision of Article I, Sections 8 & 19, of the Texas Constitution and Code of Criminal Procedure Article 1.16.

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.

Appendix (A)

405 North St. Mary ' s St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the 23rd day of December, 2005.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS

§
§
§
§
§

IN THE DISTRICT COURT

vs.

175TH JUDICIAL COURT

JOHN SMITH

BEXAR COUNTY, TEXAS

ORDER ON DEFENDANT 'S MOTION

On this the _____ day of _____, 2006, came on to be considered the above-styled and numbered motion, and it is hereby ORDERED that said motion is GRANTED/ DENIED.

SIGNED this the _____ day of _____, 2006.

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	,	IN THE DISTRICT COURT
	,	
vs.	,	175TH JUDICIAL COURT
	,	
JOHN SMITH	,	BEXAR COUNTY, TEXAS
	,	
	,	

DEFENDANT’S MOTION TO SUPPRESS STATE’S DIGITAL & AUDIO EVIDENCE
(3RD TRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through Robert H. Featherston, his attorney of record, and files this his Defendant’s Motion to Suppress Evidence, and would respectfully show to this Court as follows:

I.

Defendant hereby moves this Court for an order suppressing the State’s digital & audio evidence. Defendant would show that the methods used to preserve digital & audio evidence lacked trustworthiness. That the methods used did in fact produced inaccurate results in violation of Defendant’s constitutional right to a fundamentally fair trial under the U.S. Constitution’s 5th and 6th Amendments made applicable to the State’s under the 14th Amendment; Article 1, Section 19 of the Texas Constitution; Texas Rules of Evidence, R401, R403, R803(6), R901(a),R901(b)(4), R901(b)(9), R106 & R107.

II.

In support of the motion, the Defendant would show the Court that the State had complete control over the collection of digital and audio evidence in this internet sex sting case.

WHEREFORE, PREMISES CONSIDERED, the Defendant respectfully prays that this

Appendix (A)

Honorable Court set this motion for a hearing prior to trial and that as a consequence of this hearing, this Honorable Court order all digital and audio evidence collected by the State be suppressed at trial, and for whatever other relief the defendant is entitled to.

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the 23rd day of December, 2005.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	,	IN THE DISTRICT COURT
	,	
vs.	,	175TH JUDICIAL COURT
	,	
JOHN SMITH	,	BEXAR COUNTY, TEXAS
	,	

**ORDER ON DEFENDANT'S MOTION
TO SUPPRESS STATE'S DIGITAL & AUDIO EVIDENCE**

On this the ____ day of _____, 2006, came on to be considered the above-styled and numbered motion, and said motion is hereby:

GRANTED DENIED

SIGNED this the _____ day of _____, 2006.

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

**DEFENDANT’S MOTION TO SUPPRESS EVIDENCE
AND BRIEF IN SUPPORT**

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES, JOHN SMITH, Defendant in the above entitled and numbered cause, by and through his attorney of record, Robert H. Featherston, and respectfully moves this Honorable Court to suppress all evidence seized from his vehicle, his person, his hotel room, all statements and consents to search by the Defendant made at the time of his detention, and would respectfully show to this Court as follows:

I.
Motion to Suppress Evidence

The Defendant was detained and placed under custodial arrest, without a warrant and without probable cause in violation of the Fourth, Fifth, Sixth and Fourteenth Amendments to the Constitution of the United States of America and Article I , Section 9, 10 and 19 and of the Texas Constitution and Art. 1.04, 1.05,1.06 and 14.01 of the Texas Code of Criminal Procedure. Therefore, Defendant moves this court to make a finding that his detention was illegal, with all consequences that may result from such a finding.

II.

Defendant would allege and show that on or about November 24th, 2002, Defendant’s vehicle was stopped and searched and Defendant placed under custodial arrest without probable cause and

Appendix (A)

without a warrant.

III.

Therefore, the stop was illegal, and the evidence subsequently obtained was obtained as a result of the illegal stop and arrest. Because the initial detention was illegally conducted, the subsequent statements, admissions, and consent to search were also illegally obtained, being the fruit of the illegal detention. Defendant moves this court to find that all items found and recovered during the illegal search were the fruit of the illegal detention, and must be suppressed. *Wong Sun v. United States.*, 371 U.S. 471 (1963).

IV.

Defendant moves to suppress any oral or written statements, comments, or remarks Defendant may have made to any peace officer, investigator, or agent for the State or Government, with regards to any aspect, evidence, or person involved in this case. Defendant would show that such statements were obtained as a direct result of the above complained illegal detention and search and would be fruit of the poisonous tree. Accordingly, Defendant moves that the foregoing statements are inadmissible under the Constitution and case law, and that same should be suppressed.

V.

Brief in Support.

The Defendant was stopped, detained, and subjected to a restraint of movement by San Antonio Police Department officers, its agents and employees, and the restraint of movement constitutes a seizure. *United States v. Bowles*, 625 F. 2d 526 (5th Cir. 1980); *United States v. Robinson*, 625 F. 2d 1211 (5th Cir. 1980); *United States v. Santora*, 619 F. 2d 1052 (5th Cir. 1980); *see also, Florida v. Royer*, 460 U.S. 491 (1983); *Jefferson v. City of Omaha Police Dep't*, 335 F.3d 804, 806 (8th Cir. 2003).

Appendix (A)

VI.

Where it is established that a detention, arrest and search are made without a warrant, the burden shifts to the prosecution to produce “clear and convincing evidence” that the warrantless search meets constitutional requirements. Warrantless arrests and searches are *per se* unreasonable under the Fourth Amendment. *Coolidge v. New Hampshire*, 403 U.S. 443 (1971); *United States v. Jeffers*, 342 U.S. 48 (1951); *William v. State*, 382 F.2d 48 (5th Cir. 1967); *see also, Texas v. Brown*, 460 U.S. 730 (1983); *United States v. Kelly*, 547 F.2d 82, 84 (8th Cir. 1977)(when a search is conducted without a warrant, it is incumbent upon the Government to prove that the search falls within one of the limited exceptions to the warrant requirement).

VII.

It has been the law that the requirements for probable cause are at least as stringent in a non-warrant search as where a warrant is obtained. Rather than leaving probable cause decisions to those “engaged in the often competitive enterprise of ferreting out crime,” the preferred practice of obtaining warrants interposes the “informed and deliberate” judgment of “a neutral and detached magistrate.” *Wong Sun v. United States*, 371 U.S. 471 (1963); *Whitley v. Warden*, 401 U.S. 450 (1971); *United States v. Ventresca*, 380 U.S. 102 (1965).

VIII.

“A search is not to be made legal by what it turns up. In law it is good or bad when it starts and does not change character from its success. The forefathers, after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment.” *United States v. Dewy Re*, 68 S. Ct. 222, 229 (1948). In order for a warrantless arrest to be justified, the Government must show the existence of probable cause at

Appendix (A)

the time the arrest is made, and the existence of circumstances which made the procuring of a warrant impracticable. Where probable cause is lacking, the challenged search will not be upheld merely because the exigencies of the situation precluded the obtaining of a warrant.

IX.

The Defendant requests this Honorable Court to set this Motion for an evidentiary hearing. WHEREFORE PREMISES CONSIDERED, Defendant prays that this Court grant this Motion to Suppress all evidence seized from Defendant's truck and all statements made by this Defendant; and set this motion for an evidentiary hearing, and for all other relief to which the Defendant may otherwise show himself entitled.

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the 23rd day of December, 2005.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

ORDER

The above styled and numbered Motion to Suppress came on to be heard, and for consideration, on the ____ day of _____, 2006, and the Court after considering same is of the opinion that said motion should be set for an evidentiary hearing on _____, 2006, at ____ a.m./p.m.

SIGNED this the ____ day of _____, 2006.

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT’S MOTION TO DISMISS
(3RD TRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through Robert H. Featherston, his attorney of record, and files this his Defendant’s Motion to Dismiss, and would respectfully show to this Court as follows:

I.

Defendant hereby moves this Court for an order dismissing the indictment herein. Defendant will show, that this case should be dismissed for two reasons. First, the State failed to preserve material exculpatory evidence, evidence that would have established a valid defense to the charges. And second, because of the conduct of State agents, the Defendant herein was entrapped.

II.

Synopsis of the Case

From **19 to 24 November 2002** the State conducted an Internet sting operation where agents of the State posed as a child (**mary12sa**) communicating with JOHN SMITH (**Cheezitogether**), Initial communication occurred in a Yahoo! Messenger internet chat room Public Window and then progressed to four instant message chat sessions, three telephone calls, two email messages and a Yahoo! Greeting card over the course of six days as outlined in the below graphic.

Appendix (A)

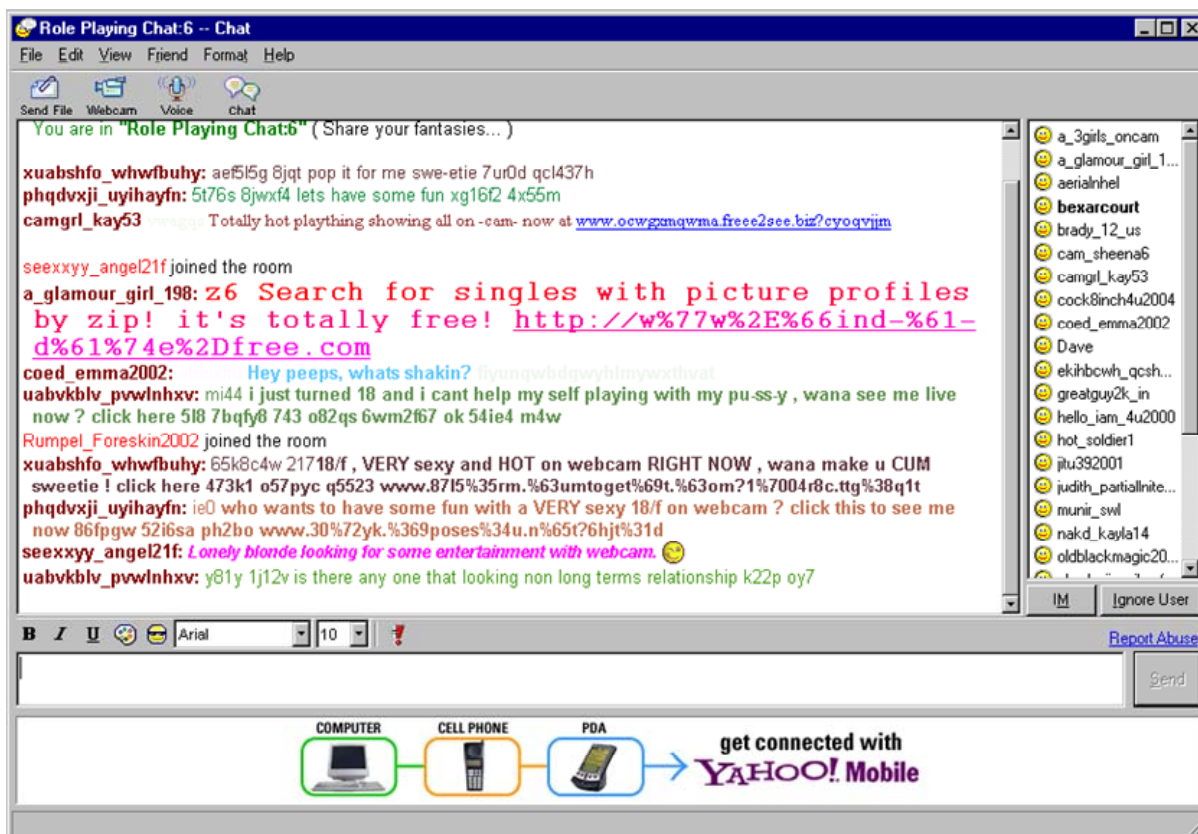
As a result of the Internet sting operation, JOHN SMITH was arrested on 24 November 2002 by members of the San Antonio Police Department.

On 02 December 2002 the trial court conducted a hearing on a Motion to Preserve

Exculpatory Evidence, opposed by the State and denied by the Court.

The State did not preserve the initial contact in the Yahoo! Messenger chat room public chat window. A sample public window is shown below:

COMPUTER & AUDIO EVIDENCE					December
November 2002					
19 Tues	20 Wed	21 Thur	22 Fri	24 Sun	02 Mon
Missing Public ? Chat ? Reasonable Expectation	Reply Email	Chat #3	Chat #4	PhonCon #3	Hearing To Preserve Computer Evidence
Chat #1 Deleted Lines Abrupt End	State Started Chat #2	Greeting Card		Arrest	
Email Fm State	Email Fm State	PhonCon #2		Defendant Statement	



Sample Yahoo! Messenger Public Window

Appendix (A)

III.

Attorney for the Defendant will show this honorable Court that the State's failure to preserve the initial communication between the State and the Defendant materially alters the context in which the subsequent instant messages and telephone conversations would be viewed by the fact finder. The initial communication and where it occurred sets the tone for the entire case.

IV.

Additionally, with respect to the first instant message chat session, which occurred immediately after the initial communication in the public window, the chat session offered by the State did not match the chat session found on the defendant's computer. Lines of text in the State's version had been altered, deleted or added, materially altering the meaning of the communication, as

**YAHOO MESSENGER CHAT SESSIONS EXTRACTS
FOR 19 Nov 02**
Evidence Offered by State

cheezitogether (7:39:59 PM): dont u want to know anything about me
mary12sa (7:40:17 PM): I hope you like the way I look enough to stay that long. I'm afraid you might not like me when you get here.
cheezitogether (7:40:21 PM): what grade are u in and can u spend the day with me
mary12sa (7:41:07 PM): I'm in the sixth grade and I could figure something out.

Recovered from Defendants Computer

Email Address !!

cheezitogether (17:42:01): dont u want to know anything about me
cheezitogether (17:42:23): what grade are u in and can u spend the day with me
cheezitogether (17:43:07): are you there
cheezitogether (17:44:25): hey would u like to see me
cheezitogether (17:46:14): well let me know if u wanna see me at arkhark@yahoo.com
mary12sa (17:47:37): what happened?
mary12sa (17:47:46): what happened?
mary12sa (17:50:28): I am very interested in meeting you. please e-mail me at mary12sa@yahoo.com
mary12sa (17:52:45): i don't know what happened. please e-mail me. I want you to visit me.
mary12sa@yahoo.com
mary12sa (17:53:10): are you there?
mary12sa (17:53:25):
mary12sa (14:04:55): Is my new friend there yet?
mary12sa (14:08:21): I am here when you feel like chatting. I should be able to stay on for about two hours.

outlined below:

The text in **red** on the upper part of the above slide is from the **States version** of chat session #1. This **red** text **was never received** by Husain's laptop.

Appendix (A)

The text in the lower part of the slide is from Husain's laptop for chat session #1.

The **green text** matches the State's version.

The **black text** is what Husain transmitted to the State but is not in the State's version.

However, Det Lowe used the email address listed in **magenta** for the 19 Nov 02 email, so we know that the State (Det Lowe) received it.

The **blue text** was transmitted by the State (Det Lowe) to Husain's laptop, **but is not in the State's version** of the chat session.

III.

Defendant further moves for a dismissal because he was entrapped, and the State's conduct violated normal standards for a fair and ethical prosecution such as to deny his rights for Due Process and Equal Protection under the United States and Texas Constitutions.

WHEREFORE, PREMISES CONSIDERED, the Defendant respectfully prays that this Honorable Court set this motion for a hearing prior to trial and that as a consequence of this hearing, this Honorable Court order a dismissal of the indictment against Defendant; and for all other relief to which Defendant may otherwise show himself entitled.

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the 23rd day of December, 2005.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	,	IN THE DISTRICT COURT
	,	
vs.	,	175TH JUDICIAL COURT
	,	
JOHN SMITH	,	BEXAR COUNTY, TEXAS

ORDER ON DEFENDANT’S MOTION TO DISMISS

On this the ____ day of _____, 2006, came on to be considered the above-styled and numbered motion, and said motion is hereby:

GRANTED **DENIED**

SIGNED this the _____ day of _____, 2006.

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT’S SPECIAL PLEA
(3RD TRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through Robert H. Featherston, his attorney of record, and files this his Defendant’s Special Plea, pursuant to Art. 27.05, Tex. R. Crim. Proc., and would respectfully show to this Court as follows:

I.

Defendant would show that he was charged in cause number 2003-CR-2036 in a two count indictment, alleging that Defendant attempted to induce a person he believed to be less than seventeen years of age to engage in sexual intercourse constituting aggravated sexual assault and that he attempted to induce a person he believed to be younger than 17 years of age to engage in deviate sexual intercourse constituting aggravated sexual assault. Defendant went to trial on January 12, 2004, and the case went to the jury on January 19, 2004. On January 24, 2004, the jury returned a verdict of not guilty on the first count, and the trial court ordered a mistrial on the second count.

II.

The trial court ordered the mistrial concluding that the jury would not be able to come to a lawful verdict on the second count. Defendant contends that the trial court improperly

Appendix (A)

dismissed the jury and that at the time of dismissal, the jury could have come to a verdict on the remaining count had the jury been given additional time. Defendant would show that he can introduce evidence in support of this contention, and the attached exhibit is offered in support thereof.

III.

As authorized by Art. 27.07, Tex. Code Crim. Proc., Defendant hereby demands a jury trial on this issue, and that Defendant be entitled to offer all such evidence as he may present to said jury in support of said contention. Art. 27.07 authorizes the submission to the issue to the jury as a matter of law.

WHEREFORE, PREMISES CONSIDERED, the Defendant respectfully prays that this Honorable Court grant this motion; that Defendant be entitled to offer evidence at his trial demonstrating that his previous trial was improperly terminated; that this jury be given such jury issues as may be appropriate to obtain a finding whether his prior trial was in fact improperly terminated; that if the jury finds that Defendant's prior trial was improperly terminated, then and for all other relief to which Defendant may otherwise show himself entitled.

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

Appendix (A)

VERIFICATION

I hereby certify that the facts contained in the forgoing pleading are true and correct.

ROBERT H. FEATHERSTON

SUBSCRIBED and SWORN TO before me, the undersigned notary, on this the 23rd day of December, 2005.

NOTARY PUBLIC, STATE OF TEXAS

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the 23rd day of December, 2005.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS
	§	

ORDER ON DEFENDANT’S SPECIAL PLEA
(3RD TRIAL)

On this day came on to be considered the above-styled and numbered motion, and said motion is hereby GRANTED.

IT IS THEREFORE ORDERED and DECREED that Defendant shall be entitled to submit to the jury evidence that the jury deliberations in his previous trial were improperly terminated and that the jury be given such jury issues as may be appropriate to obtain a finding whether Defendant’s prior trial was in fact improperly terminated.

SIGNED this _____ day of _____, 2006.

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S REQUESTED INSTRUCTION TO THE JURY NO. 1
(3rd TRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through his attorney of record, Robert H. Featherston, and files this his Requested Instruction to the Jury No. 1, and would respectfully request that the Jury be instructed as follows:

"You are instructed that Defendant has been tried previously for the same offense. You are further instructed that Defendant has offered evidence to you from previous jurors that they could have and would have reached a unanimous verdict if the jury had been given additional time to deliberate.

"Should you find, from a preponderance of the evidence, that if in fact the jury had been given additional time to deliberate that they would have reached a unanimous verdict, then you are to find the Defendant not guilty."

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Suite 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the ____ day of _____, 2006.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

ORDER

On this, the _____ day of _____, 2006, came on to be heard the foregoing requested jury instruction, and the Court, after hearing the arguments of counsel, and considering same, hereby orders that the motion is (GRANTED) (DENIED).

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S REQUESTED INSTRUCTION TO THE JURY NO. 2
MISSING EVIDENCE (3rd TRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through his attorney of record, Robert H. Featherston, and files this his Requested Instruction to the Jury No. 1, and would respectfully request that the Jury be instructed as follows:

"You are hereby instructed that if you find that certain evidence is within the control of the State, and that the State failed to produce said evidence during the trial, you may presume that if said evidence had been produced in court it would have operated against, or be to the detriment of, the State." *Watson v. Brazos Elec. Power Corp., Inc.*, 918 S.W.2d 639, 643 (Tex.App.- Waco 1996, pet. den.).

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Suite 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the ____ day of _____, 2006.

ROBERT H. FEATHERSTON

Appendix (B)

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

ORDER

On this, the _____ day of _____, 2006, came on to be heard the foregoing requested jury instruction #2, and the Court, after hearing the arguments of counsel, and considering same, hereby orders that the motion is (GRANTED) (DENIED).

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S REQUESTED INSTRUCTION TO THE JURY NO. 3
ENTRAPMENT (3RD RETRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through his attorney of record, Robert H. Featherston, and files this his Requested Instruction to the Jury No. 3, and would respectfully request that the Jury be instructed as follows:

"You are instructed that it is a defense to prosecution that a person engaged in the conduct charged against him 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; however, conduct of law enforcement agents that merely affords a person an opportunity to commit an offense does not constitute entrapment.

"By the term "law enforcement agent" as used herein is meant 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.

"Therefore, if you believe from the evidence beyond a reasonable doubt that the defendant committed the offense as alleged, but you further believe, or you have a reasonable doubt thereof, that he was induced to do so by Terry Lowe and Lori Maulding, law enforcement officers, by persuasion or any other means likely to cause persons to do so, and that the conduct of Terry Lowe and Lori Maulding did not merely afford the defendant an opportunity to commit the offense, if any, you will find the defendant not guilty." E. Berry, G. Gallagher & P. McClung, *Texas Criminal Jury Charges* §12.940.10 (2005).

Respectfully submitted,

Appendix (B)

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the ___ day of January, 2006.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S REQUESTED INSTRUCTION TO THE JURY NO. 3
ENTRAPMENT (3rd RETRIAL)

ORDER

On this, the _____ day of _____, 2006, came on to be heard the foregoing requested jury instruction, and the Court, after hearing the arguments of counsel, and considering same, hereby orders that the motion is (GRANTED) (DENIED).

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175 TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S REQUESTED INSTRUCTION TO THE JURY NO. 4
(3rd RETRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through his attorney of record, Robert H. Featherston, and files this his Requested Instruction to the Jury No. 4, and would respectfully request that the Jury be instructed as follows:

“In this case the defendant, Amur Husain, has filed a special plea that he has already been prosecuted for the same offense for which he is now on trial, and that the former prosecution was improperly terminated.

“Under our law when a criminal case is submitted to the jury for its consideration, the court may, in its discretion, discharge the jury from further consideration of its verdict in the case where it has been kept together for such period of time as to render it altogether improbable that it can agree.

“Now, if you find from the evidence that when the case against the defendant for the offense of Criminal Solicitation of a Minor, for which he is now being tried, was submitted in the first trial to the jury on the issue of guilt or innocence on 21 January 2004, the jury was discharged before it had been kept together for such time as to render it altogether improbable that it could agree on a verdict, or if you have a reasonable doubt thereof, then you will render a verdict of "True" on the special plea.

“However, if you find from the evidence beyond a reasonable doubt that the jury was not discharged before it had been kept together for such time as to render it altogether improbable that it could agree on a verdict, then you will render a verdict of "Untrue."

Appendix (B)

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the ___ day of January, 2006.

ROBERT H. FEATHERSTON

Appendix (B)

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

ORDER

On this, the _____ day of _____, 2006, came on to be heard the foregoing requested jury instruction, and the Court, after hearing the arguments of counsel, and considering same, hereby orders that the motion is (GRANTED) (DENIED).

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	187TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S REQUESTED INSTRUCTION TO THE JURY NO. 5
(RETRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through his attorney of record, Robert H. Featherston, and files this his Requested Instruction to the Jury No. 5, and would respectfully request that the Jury be instructed as follows:

“The jury is instructed that if it believes or has reasonable doubt that any evidence presented herein was obtained in violation of the constitution and laws fo the United States or of this state, the jury shall disregard any such evidence so obtained.” Tex. Code Crim. Proc. art. 38.23 (a).

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary’s St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the ___ day of January, 2006.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

ORDER

On this, the _____ day of _____, 2006, came on to be heard the foregoing requested jury instruction, and the Court, after hearing the arguments of counsel, and considering same, hereby orders that the motion is (GRANTED) (DENIED).

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	187 TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S REQUESTED INSTRUCTION TO THE JURY NO. 7
(RETRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through his attorney of record, Robert H. Featherston, and files this his Requested Instruction to the Jury No. 7, and would respectfully request that the Jury be instructed as follows:

“You are instructed that unless you believe from the evidence beyond a reasonable doubt that the alleged confession or statement introduced into evidence was freely and voluntarily made by the defendant without compulsion or persuasion, or if you have a reasonable doubt thereof, you shall not consider such alleged statement or confession for any purpose nor any evidence obtained as a result thereof.” *Texas Crim. Jury Charges*, §12.900.11 (2005).

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the ___ day of January, 2006.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS

vs.

JOHN SMITH

§
§
§
§
§

IN THE DISTRICT COURT

175TH JUDICIAL COURT

BEXAR COUNTY, TEXAS

ORDER

On this, the _____ day of _____, 2006, came on to be heard the foregoing requested jury instruction, and the Court, after hearing the arguments of counsel, and considering same, hereby orders that the motion is (GRANTED) (DENIED).

JUDGE PRESIDING

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

DEFENDANT'S REQUESTED INSTRUCTION TO THE JURY NO. 9
(RETRIAL)

TO THE HONORABLE JUDGE OF SAID COURT:

NOW COMES JOHN SMITH, Defendant in the above entitled and numbered cause, by and through his attorney of record, Robert H. Featherston, and files this his Requested Instruction to the Jury No. 9, and would respectfully request that the Jury be instructed as follows:

“The jury is instructed that under the Texas Constitution, the State has a duty to preserve evidence that has apparent exculpatory value, which includes not only exculpatory evidence, but also evidence that is potentially useful to the defense. In either case, the evidence must be of such a nature that the defendant would be unable to obtain comparable evidence by other reasonably available means. The loss or destruction of such evidence results in a breach of the State’s duty.

“In this case there has been evidence that the State failed to collect/preserve certain evidence which is material to the defense. It does not matter for these purposes whether the State was negligent, the State lost the evidence through lack of training, or whether the State deliberately lost the evidence. The failure of the State to collect/preserve such evidence entitles the defendant to an inference that if such evidence were available at trial it would be exculpatory. This means that, for purposes of deciding this case, you are to assume that the missing evidence, had it been collected/preserved, would not have incriminated the defendant and would have tended to prove the defendant not guilty. The inference does not necessarily establish the defendant's innocence, however. If there is other evidence presented which establishes the fact or resolves the issue to which the missing evidence was material, you must weight that evidence along with the inference. Nevertheless, despite the inference concerning the missing evidence, if you conclude after examining all the evidence that the State has proven beyond a reasonable doubt all elements of the offense(s) charged, you would be justified in returning a verdict of guilty.” *Pena v. State*, 166 S.W.3d 274, 282-283 (Tex.App.- Waco 2005, pet. granted)(as modified).

Appendix (B)

Respectfully submitted,

ROBERT H. FEATHERSTON
CORREA & FEATHERSTON, P.C.
405 North St. Mary's St., Ste. 340
San Antonio, Texas 78205
Telephone: (210) 838-8582
Facsimile: (210) 479-3205
State Bar No.: 24004641
ATTORNEY FOR DEFENDANT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing Motion has been hand-delivered/mailed/faxed to Miguel Najera, Bexar County Assistant District Attorney, Bexar County Justice Center, 300 Dolorosa, San Antonio, Texas 78205 on this the ___ day of January, 2006.

ROBERT H. FEATHERSTON

CAUSE NO. 2003-CR-XXXX

STATE OF TEXAS	§	IN THE DISTRICT COURT
	§	
vs.	§	175TH JUDICIAL COURT
	§	
JOHN SMITH	§	BEXAR COUNTY, TEXAS

ORDER

On this, the _____ day of _____, 2006, came on to be heard the foregoing requested jury instruction, and the Court, after hearing the arguments of counsel, and considering same, hereby orders that the motion is (GRANTED) (DENIED).

JUDGE PRESIDING

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
|  |-- SHELLEX
|  |-- Spool
|  |-- Drivers
|  |  |-- W32x86
|  |  |-- PrtProcs
|  |  |-- W32x86
|  |-- IOSUBSYS
|  |-- COLOR
|  |-- VMM32
|  |-- OOBE
|  |-- MSNSETUP
|  |-- SETUP
|  |-- HTML
|  |  |-- MOUSE
|  |  |-- IMAGES
|  |  |-- ISPSGNUM
|  |  |-- IMAGES
|  |  |-- ERROR
|  |  |-- MSNHTML
|  |  |-- ISPSGNUM
|  |  |-- 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
|  |  |-- Grpflt
|  |  |-- MSINFO
|  |  |-- Application Data
|  |  |-- Microsoft
|  |  |-- WELCOME
|  |  |-- Internet Explorer
|  |  |-- Quick Launch
|  |  |-- Outlook Express

```

Case: f01044

|||| +- Mail
 |||| +- News

|||| +- texasnet

Volume "D" Parameters

File System: FAT32
 Sectors Per Cluster: 8
 Total Sectors: 1,092,357
 Total Clusters: 136,274
 Free Clusters: 124,689
 Volume Name:
 OEM Version: MSWIN4.1
 Heads: 255
 Unused Sectors: 11,502,603
 Sectors Per FAT: 1,066

Drive Type: Fixed
 Bytes Per Sector: 512
 Total Capacity: 558,178,304 bytes (532.3MB)
 Unallocated: 510,726,144 bytes (487.1MB)
 Allocated: 47,452,160 bytes (45.3MB)
 Volume Offset: 11,502,603
 Volume Serial #: 0000-0000
 Sectors Per Track: 63
 Number of FATs: 2
 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\CWINDOWS\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



WELCOME

Louis Correa
Robert Featherston
Correa & Featherston, P.C.

Ray Taylor, Of Counsel

REPRESENTING
Dr. John Smith

FAIRNESS - PARTICIPATION

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

BACKGROUND

- **Objections**
- Meeting in the hall
- **Physical problems** precluding jury service ?
- Military duty ?

BACKGROUND cont.2

- Have you or a family member or friend been involved in a case of sexual abuse?

Criminal Solicitation of a Minor, TPC 15.031

ⓘ A person commits an offense if, **with intent** that an offense under **Indecency With a 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 . . .

(EMPHASIS ADDED)

INTENT - BELIEF

- Who's **Intent** ?
- Who's **Belief** ?
- Who's shoes **must** you walk in ?
- How do you determine it ?
- If you have a **reasonable doubt** as to **Intent** or **Belief**, what **must** your verdict be ?

PUNISHMENT

- **Two Trials**
 - Guilt / Innocence
 - Punishment
- **Punishment range** for this offense.
 - **Probation ?**

POLICE OVERREACHING

- What is that?
- **Proactive** approach to law enforcement.
- Training
- **Tulia Drug Sting**
 - ◆ Manufactured Evidence
 - ◆ Altered Evidence

COMPUTERS & INTERNET

- Who uses a Computer?
- The Internet?
- Yahoo! Messenger
- Instant Messaging
- Email
- **Are computers good at recording data?**

COMPUTERS & INTERNET

- Forensic Collection of Computer based Evidence - **CSI . . .**
 - **Standard Collection Procedures (SOP)**
 - **Training**
 - Screen/Keyboard **Logger Programs ?**
 - **Hashing Programs ?**

PRETENDING

- **Masquerade Ball**
- Reasonable Expectations, "The Bar"
- **First Amendment Right !**
- **Role Playing** and the Internet
- 1-900
- **Pretending** or **Reality** – when do you know?
 - ◆ **Definitive pointers to Identity !!!!!**

DEFENDANT'S STATEMENT

- What makes it **Voluntary**
- What makes it **Involuntary**
 - Does **cultural background** play a role?
- He said / She said
- Interview Room
- **Video** Tape, **Audio** Tape

FAMILY

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

WITNESS CREDIBILITY

- **Public Speaking**
- **Meet the Press.**
- Professional Witness
- Lay Witness

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

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

WHAT MUST THE JURY DO ?

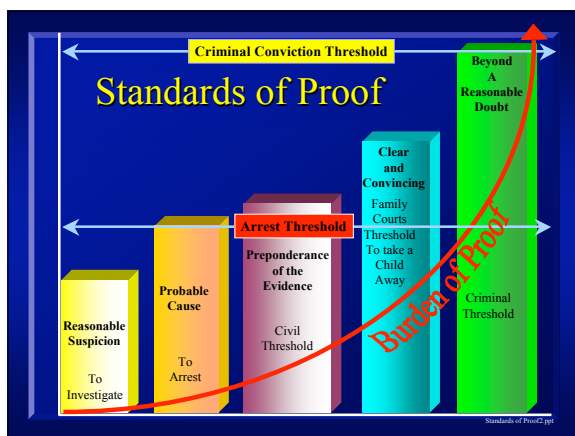
Is the jury here to decide if Amir Husain is **Innocent ?**

NO !

The jury **Must** decide whether, the State has proven their case.

Beyond A Reasonable Doubt !

➤ **Standards of Proof**



C.C.P. Art. 35.16(a) (10) & (c)(2)

- As Amir sits before you **right now** how many of you are **leaning just a little bit** towards **guilt**, feeling that it would take **some evidence** to remove this from your mind?
 - ◆ Who says **Yes**?
 - ◆ Who says **No**?
 - ◆ Who **does not know**?

JURY DELIBERATION

- YOUR GOING TO WANT TO GO HOME. . .
- Burden of Proof

Exonerated After Wrongful Conviction
The Innocents

Photographs and Interviews by Taryn Simon
Commentary by Peter Neufeld and Barry Schick

VERDICT

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

Thank You !

Fin

The Innocents

Photographs and Interviews by Taryn Simon
Commentary by Peter Neufeld and Barry Schick

OPPORTUNITIES TO PRESERVE THE TRUTH

- KEY EVIDENCE NOT PRESERVED
- MISTAKES BY THE STATE
- NO FORMAL COMPUTER TRAINING
- DEFINITIVE POINTERS TO PARTICIPANT'S IDENTITY NOT SAVED BY STATE

- UNDERCOVER OPERATION ON THE INTERNET CONTROLLED BY S.A.P.D. VICE.

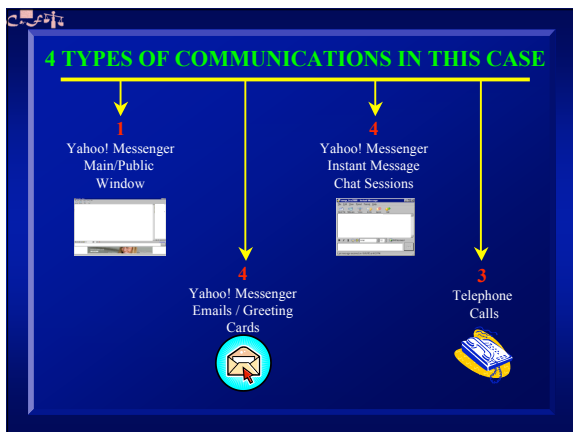
THERE ARE
NO CHILDREN
INVOLVED WITH THIS CASE !

DR. JOHN SMITH

- YOU WILL HEAR FROM DR. SMITH
- HE DID NOT SOLICIT A CHILD
- HIS BACKGROUND
 - ◆ Highly Intelligent
 - ◆ Multiple Languages
 - ◆ Speech Impediment
 - ◆ Grew up in India
 - ◆ Trained as a Doctor & Cardiologist in Russia
 - ◆ In U.S. 18mo prior to this incident

DR. JOHN SMITH

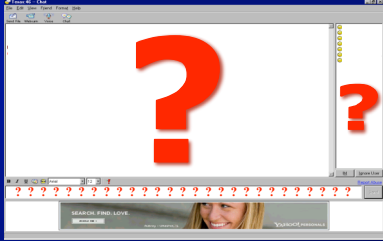
- On Yahoo! Messenger to meet Adult Females
- Willing to accommodate to establish a relationship
- The definitive pointers to Identity that he observed:
 - On the Internet
 - From the Telephone
 - At the Arrest location
- Sexually Graphic conversation of Det Lowe in the public window of Yahoo Messenger (not preserved by State)
- Role of the Public Window in his deciding he was communicating with an Adult.



Detective Lowe Will Also Testify That:

- COMPUTER EVIDENCE COLLECTION:
 - ◆ HE ONLY PRESERVED THAT EVIDENCE THAT HE DEEMED PERTINENT
 - ◆ HE LEFT EVIDENCE OUT
 - ◆ HE CAN'T TELL WHAT EVIDENCE IS MISSING OR HOW MUCH


Yahoo! Messenger Main/Public Communications Window



Detective Lowe Will Also Testify That:

THE 1ST COMMUNICATION BETWEEN DET. LOWE & DR. HUSAIN WAS NOT SAVED


Yahoo! Messenger Main/Public Communications Window



Detective Lowe Will Also Testify That:

- YAHOO! MESSENGER:
 - ◆ IS INTENDED FOR ADULTS
 - ◆ FOLKS **ROLE PLAY** ALL OVER THE SYSTEM


Yahoo! Messenger Main/Public Communications Window



Detective Lowe Will Also Testify That:

- In the Public Window:
 - ◆ REASONABLE EXPECTATION PERSON IS **18 YEARS OF AGE**
 - ◆ LIKE A **MASQUERADE PARTY**
 - ◆ FOLKS **ASSUME IDENTITIES** HERE
 - ◆ COME TO **ACT OUTRAGEOUS**
 - ◆ **HOW OUTRAGEOUS** IS ESTABLISHED BY WHAT'S GOING ON

Yahoo! Messenger Main/Public Communications Window



Detective Lowe Will Also Testify That:

- Conversations in the Public Window:
 - ◆ ARE **MATERIAL**
 - ◆ ESTABLISH **CHARACTER** OF THE ROOM
 - ◆ JURY HAS **NO OPPORTUNITY** TO JUDGE FOR THEMSELVES
 - ◆ **"CANT RECALL"** HAVING A CONSERVATION IN THE PUBLIC ROOM

The evidence will also show:

- **NO SOP.**
- **NO** Automatic Collection of Computer Evidence.
- **NO** use of **Screen Logger** Program
- **NO** use of **Key Logger** Program
- **NO** use of **Video Tape** to collect Computer Evidence

The evidence will show:

- **NO** use of **Hashing** Program.
- Officer Maulding – Audio Tape **Quality**
- Officer Maulding – **NO** Audio from body microphone.

The evidence will show:

- No video tape or audio tape of Dr. Husain's alleged statement.
- This statement was **Not Voluntary**
- Pay very close attention to Arrest Video

The evidence will show:

- Affirmatively, Dr, Smith had **No Intent** to have sex with a child.
- THE EVIDENCE WILL SHOW THAT DR. SMITH IS:
NOT GUILTY.

Thank You !

The Rule of Law

- Deter & Punish Offenders
- Protect **us** from **Governmental Overreaching**:
 - ◆ Privacy
 - ◆ Free Speech
 - ◆ Constitutional Rights

Police

Citizen Expectations

- The Power
- Fair
- Unbiased
- Well Trained & Supervised
- The Whole Picture
- **Completely Truthful**
- **Liberty is at Stake!**

Human Sexuality

- The **Most** Powerful Human Emotion
- Under Cover Officer **Training**
- Predisposition / Opportunity
- **Inducement**

DR. JOHN SMITH

- **HE DID NOT SOLICIT A CHILD**
- Not a Professional Witness
- Stand in his Shoes
- HIS BACKGROUND
 - ◆ Highly Intelligent
 - ◆ Socially Inept
 - ◆ Multiple Languages
 - ◆ Speech Impediment
 - ◆ Grew up in **India**
 - ◆ Trained as a Doctor & Cardiologist in **Russia**
 - ◆ In U.S. **18mo** prior to this incident
- **GET ON LINE TO GET A DATE !**

DR. JOHN SMITH

- On Yahoo! Messenger to meet **Adult Females**
- Willing to pretend to further a relationship
- **Sexually Graphic** conversation of Det Lowe in the **public window** of Yahoo Messenger (**not preserved by State**)
- Role of the **Public Window** in his deciding he was communicating with an **Adult**.

- **UNDERCOVER OPERATION ON THE INTERNET CONTROLLED BY S.A.P.D. VICE – they made the rules !.**

THERE ARE

NO CHILDREN

INVOLVED WITH THIS CASE !

The evidence has Shown:

- **NO SOP.**
- **NO** Automatic Collection of Computer Evidence.
- **NO** use of **Screen Logger Program**
- **NO** use of **Key Logger Program**
- **NO** use of **Video Tape** to collect Computer Evidence
- **NO** use of **Hashing Program.**

COMPUTER & AUDIO EVIDENCE					
November 2002					December
19 Tues	20 Wed	21 Thur	22 Fri	24 Sun	02 Mon
Missing Man ? Chat ? Reasonable Expectation	Reply Email State Started Chat #2	Chat #3	Chat #4	PhonCon #3	Hearing To Preserve Computer Evidence
Chat #1 Status Icon Always On	PhonCon #1	Greeting Card		Arrest	
Email Fm State	Email Fm State	PhonCon #2		Involuntary Statement ? Video ?	
State's Forensic Exam of Defendant's Laptop ??? Chats ???					

Yahoo! Messenger Main/Public Chat Room Window

!! LOST LOST LOST !!

MATERIAL !!

Lowe Says: "Now we Preserve the Main Window"

ITS NOT HER PHOTOGRAPH!

YAHOO MESSENGER CHAT SESSIONS EXTRACTS FOR 19 Nov 02

Evidence Offered by State, From State's Computer

```

cheezitogether (7:39:59 PM): dont u want to know anything about me
mary12sa (7:40:17 PM): I hope you like the way I look enough to stay that long. I'm afraid you might not like me when you get here.
cheezitogether (7:40:21 PM): what grade are u in and can u spend the day with me
mary12sa (7:41:07 PM): I'm in the sixth grade and I could figure something out.
    
```

Email Address !!

Recovered from Defendants Computer

```

cheezitogether (17:42:01): dont u want to know anything about me
cheezitogether (17:42:23): what grade are u in and can u spend the day with me
cheezitogether (17:43:07): are you there
cheezitogether (17:44:25): hey would u like to see me
cheezitogether (17:46:14): well let me know if u wanna see me at arrark@yahoo.com
mary12sa (17:47:37): what happened?
mary12sa (17:47:46): what happened?
mary12sa (17:50:28): I am very interested in meeting you. please e-mail me at mary12sa@yahoo.com
mary12sa (17:52:45): i don't know what happened. please e-mail me. I want you to visit me.
mary12sa@yahoo.com
mary12sa (17:53:10): are you there?
mary12sa (17:53:25):
    
```

Arrest

- **Approached a Woman !!**
- **Hotel**
- **Condoms**
- **Dolphin**
- **FEAR !**

NOV 24 2002
10:41:17 AM

STATE'S STATEMENT

- Who had all the Information?
- Not Dr. Smith's Statement !
- **Shocked & Confused, Handcuffed**
- **Fear**
- Raised, India, Qatar, Kuwait, Russia
- **No Prior Criminal Experience**
- **Requested Attorney**
- **Not Voluntary**
- Det. Lowe's Words
- If you had Dr. Smith's background you WOULD sign too !
- **Video / Audio Tape** (Another lost Opportunity !)

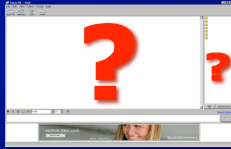
But it's the truth isn't it?

DET. LOWE

- **NO** Formal Computer Training !
- **NO** Formal Training on Internet Sex Stings !
- His **FIRST** case as Lead Agent !
- **SUPERVISION ?**
- **Wanted to Make His Case !**
- 1st Chat Session, "**Not where Lowe wanted it to End.**"
- **THE WHOLE PICTURE ??????**

Detective Lowe Testified That:

THE 1ST COMMUNICATION BETWEEN DET. LOWE & DR. HUSAIN WAS **NOT SAVED**




Yahoo! Messenger Main/Public Communications Window

- **BLOCKING**
- **PARTICIPANTS - WITNESSES**

Detective Lowe Testified That:

COMPUTER EVIDENCE COLLECTION:

- ◆ **HE ONLY PRESERVED THAT EVIDENCE THAT HE DEEMED PERTINENT**
- ◆ HE **LEFT EVIDENCE OUT**
- ◆ HE **CAN'T TELL** WHAT EVIDENCE IS **MISSING OR HOW MUCH**




Yahoo! Messenger Main/Public Communications Window

Detective Lowe Testified That:

YAHOO! MESSENGER:

- ◆ **IS INTENDED FOR ADULTS**
- ◆ FOLKS **ROLE PLAY** ALL OVER THE SYSTEM




Yahoo! Messenger Main/Public Communications Window

Detective Lowe Testified That:

In the **Public Window**:

- ◆ **REASONABLE EXPECTATION** PERSON IS **18 YEARS OF AGE**
- ◆ LIKE A **MASQUERADE PARTY**
- ◆ FOLKS **ASSUME IDENTITIES** HERE
- ◆ COME TO **ACT OUTRAGEOUS**
- ◆ **HOW OUTRAGEOUS** IS ESTABLISHED BY WHAT'S GOING ON




Yahoo! Messenger Main/Public Communications Window

Yahoo! Messenger Main/Public Communications Window

Detective Lowe Testified That:

- Conversations in the **Public Window**:
 - ♦ ARE **MATERIAL**
 - ♦ ESTABLISH **CHARACTER** OF THE ROOM
 - ♦ "**CANT RECALL**" HAVING A CONSERVATION IN THE PUBLIC ROOM
 - ♦ **JURY** HAS **NO OPPORTUNITY** TO JUDGE FOR THEMSELVES



Det. POTH

- Professional Witness
- His Style, Appearance - (**Beet Red**)
- **LACK of Facts** in His Report
- **? Unbiased ?**
- SUPERVISION ???, - Who's on First !
 - Then why is there **missing** Evidence?
- **Every** second of **Every** minute.....

OFFICER HERRIES

It's the little lies...

- SHE LOOKED YOU IN THE EYE AND **LIED** TO YOU!
- Video Tape, - **She is not a Child !!**
- Who's Role Playing ?
- Audio Tape
 - (American Idol, **Simon says**: "*That's Horrendous!*")
- **Quality** of the Audio Tape, whose duty to cure?
- Pay very close attention to Arrest Video

DET. LOWERY


"Not Sure" "Don't Know"

- Pretty Good with Encase ?? (button pusher)
- Collect / Analysis ??
- Not a Buddy List !
- Visiting Web Sites???
- Where are these Photos?
- **NO CHILD PORNOGRAPHY**

Grant's Tomb

"Can't Recall"

Intellectually Dishonest



DAVID McGROTY

- State **failed** to save Material Evidence !
 - **We would not be here if the State had Preserved the Public Window !**
- **Why** did the State call the Defendant's Computer Expert First ??
 - Cover State's own Blunders!
- "**You would hope** that the State's Computer Experts would be **at least as Qualified** as David McGroty.
- Methods for Preserving Computer Evidence.

WHAT MUST THE JURY DO ?

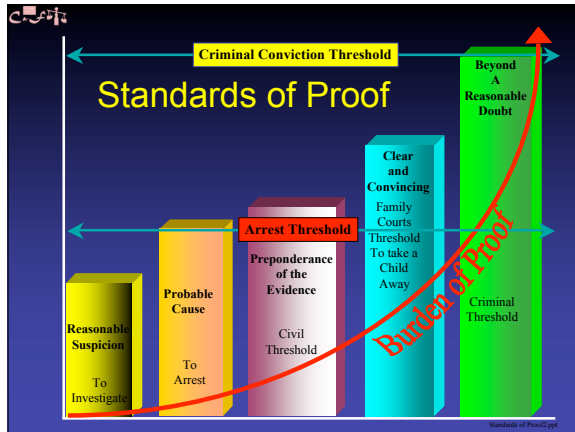
Is the jury here to decide if Amir Husain is **Innocent ?**

NO !

The jury **Must** decide whether, the **State** has proven their case:

Beyond A Reasonable Doubt !

➤ **Morality & The Law**



JURY DELIBERATION

- **YOUR GOING TO WANT TO GO HOME. . .**
- **There is no DNA for Intent**
- **Stick to your Guns !**
 - Do not surrender your honest belief as to the weight and effect of evidence solely because of the opinion of your fellow jurors or for the mere purpose of returning a verdict.
- **I have a Reasonable Doubt.**

THOUGHT CRIME

- Dr, Husain had **No Intent** to have sex with a child.
- The missing **PUBLIC WINDOW !!!!**
- The State **HAS NOT** preserved all the Evidence in this case!
- The State **CANNOT** prove their case Beyond a Reasonable Doubt.
- **IF THE STATE LEFT IT OUT - THAT'S REASONABLE DOUBT!!**

THEN YOU MUST VOTE NOT GUILTY !

Thank You !

Arrest without Warrant

- In Texas, the authority to arrest a suspect without a warrant is **governed exclusively by statute.**
 - *Johnson v. State*, 32 S.W.3d 294, 298 (Tex.App. - San Antonio 2000, pet.ref'd.);
 - *State v. Parson*, 908 S.W.2d 284, 286 (Tex.App. - San Antonio 1996, no pet.);
 - *Ruiz v. State*, 907 S.W.2d 600, 603 (Tex.App. - Corpus Christi 1996, no pet.);
 - *Simpson v. State*, 709 S.W.2d 797, 802 (Tex.App. - Fort Worth 1986, pet. ref.d.)
- **Texas law**, rather than federal law, governs the legality of a state arrest unless it violates the Fourth Amendment.
 - *Sandoval v. State*, 35 S.W.3d 763, 767 (Tex.App. - El Paso 2000, pet. ref'd.)

Texas Statutory Authority

- The Texas statutory authority to make a warrantless arrest is more restrictive than the requirements of the United States Constitution.
 - *Hughes v. State*, 24 S.W.3d 833, 838 (Tex.Crim.App. 2000 [generally. Arrest must be made with warrant, but statutory exceptions exist];
 - *Josey v. State*, 991 S.W.2d 831, 841 (Tex.App. - Houston [14th Dist.] 1998, pet. ref'd.) [Texas law requires warrant unless one of statutory exceptions is met];
 - *Hawkins v. State*, 853 S.W.2d 598, 601 (Tex.App. - Amarillo 1993, no pet.);
 - *Stevenson v. State*, 780S.W.2d 294, 295 (Tex.App. - Tyler 1989, no pet.)

Arrest without Warrant

- In Texas, a person may be arrested without a warrant only if
 - ☞ There is **probable cause**, & **and**
 - ☞ The arrest **falls within the provision of one of the statutes authorizing a warrantless arrest.**

- *Anderson v. State*, 932 S.W.2d 502, 506 (Tex.Crim.App. 1996);
- *Lunde v. State*, 736 S.W.2d 665, 666 (Tex.Crim.App. 1987);
- *Dyer v. State*, 59 S.W.3d 713, 715 (Tex.App. - Austin 2001, no pet.);
- *Moore v. State*, 55 S.W.3d 652, 659 (Tex.App. - San Antonio 2001, no pet.);
- *Chilman v. State*, 22S.W.3d 50, 56 (Tex.App. - Houston [14th Dist.] 2000, pet. ref.d.);
- *State v. Steelman*, 16 S.W.3d 483, 487-488 (Tex.App. - Eastland 2000, pet. granted);

State's Burden

- An arrest without a warrant is **deemed to be unreasonable** and unlawful, and the **State has the burden** of establishing the statutory authority for the arrest.
 - *Wilson v. State*, 62 1 S. W.3d 799, 803-04 (Tex.Crim.App. 198 1);
 - *Darden v. State*, 783 S.W.2d 239, 242 (Tex.App. - Corpus Christi 1989, pet. ref d.);
 - *Beasley v. State*, 728 S.W.2d 353, 355 (Tex.Crim.App. 1987);

State's Burden

- When a defendant has shown that an arrest was made without a warrant, the **burden shifts to the State** to establish that the warrantless arrest was **statutorily authorized.**
 - *McClain v. State*, 984 S.W.2d 700, 702 (Tex.App. - Texarkana 1998, no pet.);
 - *Sims v. State*, 980 S.W.2d 538, 539-40 (Tex.App. - Beaumont 1998, no pet.);

Strict Construction

- Because of the **legislative preference** that every arrest be made with a warrant, the statutes authorizing warrantless arrests are **strictly construed.**
 - *Hullit v. State, supra*, note 1 [Art. 1, § 9, Texas Constitution, does not require that arrest be made with warrant, but statutes that require warrants may not be ignored];
 - *Vasquez v. State*, 739 S.W.2d 37, 41 (Tex.Crim.App. 1987), reh. denied, 816 S.W.2d 750 (Tex.Crim.App. 1991, en banc) ["The rule favoring arrest with warrant is not constitutionally mandated but is a product of legislative action."]
 - *Reichaert v. State*, 830 S.W.2d 348, 349 (Tex.App. - San Antonio 1992, pet.ref.d.)
 - *Dejarnett v. State*, 732 S.W.2d 346, 349 (Tex.Crim.App. 1987);

Strict Construction

- The validity of an arrest without a warrant depends on the facts which existed at the time of the arrest, and those facts **must** come "**squarely**" within the provisions of one of the statutes authorizing an arrest without a warrant.

■ *Simpson v. State*, 709 S.W.2d 797, 802 (Tex.App. - Fort Worth 1986, pet. ref.d.)
■ *Heath v. Bond*, 175 S.W.2d 214, 215 (Tex. 1943)

Facts After Arrest

- Facts discovered or knowledge acquired **subsequent to the arrest may not** be utilized retrospectively to establish probable cause at the time of the arrest.

■ *Amores v. State*, 816 S.W.2d 407, 415 (Tex.Crim.App. 1991);
■ *Jones v. State, supra*, [lack of probable cause cannot be cured by bolstering the arrest with evidentiary fruits illegally seized];
■ *Atkinson v. State*, 848 S.W.2d 813, 815 (Tex.App. - Houston [14th Dist.] 1993, no pet.) ["Probable cause is determined based upon the legal significance of facts known to the officer **at the time of the arrest**, and facts coming to light after the arrest going to establish guilt would not be relevant to show probable cause."].

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

FILED
AUSTIN DIVISION
2004 OCT 20 PM 1:31
U.S. CLERK'S OFFICE
DEPUTY

UNITED STATES OF AMERICA)
)
V.) A-04-CR-181-SS
)
FRANKLIN S. BUCKRIDGE)

ORDER REGARDING
DISCOVERY OF COMPUTER FORENSIC EVIDENCE

On this 15th day of October, 2004, the foregoing Agreed Motion for Discovery of Computer Forensic Evidence came on to be heard by the Court and, the Court having considered the same, says:

IT IS HEREBY ORDERED:

1. That the Government shall provide defendant's counsel with one (1) bit by bit (also known as mirror image) copy of hard drives from all computers seized in this case, necessarily including any and all child pornography and/or contraband allegedly contained thereon;
2. That in connection with the provision of such copy, defense counsel will furnish the Government with a hard drive and/or other necessary computer media onto which the mirror image copy will be replicated so that it functions as readily as the original;
3. that the bit by bit or mirror image copy referenced above (hereinafter the "Mirrored Drive") shall be maintained by defense counsel and/or an expert retained by the defense in accordance herewith and shall be used by counsel and/or the expert solely

CTS
53

Appendix (H)

and exclusively in connection with this case (including trial preparation, trial and appeals or other related legal proceedings) and for no other purposes;

4. That the data contained on the Mirrored Drive may be accessed and viewed only by defense counsel, the defense expert, and defense investigators;

5. That defendant himself shall not under any circumstances be permitted to access or view any graphic image file containing actual or alleged child pornography without petition to and further order of the Court; however, defendant may access and view non-image data on the Mirrored Drive for the purpose of assisting in the preparation of his defense in the presence of counsel and under the direct supervision and control of counsel;

6. That the computer into which the Mirrored Drive may be inserted for access and operation shall not be connected to a network while the Mirrored Drive is installed, or at any time prior to the destruction of all data as specified in paragraph 11;

7. That the computer into which the Mirrored Drive is inserted may be connected to a printer only on the following terms and conditions—that any printer utilized is a local printer, that such printer may be connected only when and as necessary to print non-graphic image files (text files, log files, directory trees, etc.), and that defense counsel or a defense investigator shall be personally present at all times a printer is connected;

8. That in no event shall any graphic image file containing child pornography or which may reasonably be construed as constituting child pornography be copied, duplicated or replicate, in whole or in part, onto any external media including, but not limited to, paper, floppy disk, CD-ROM, DAT tape, zip disk, or other media;

Appendix (H)

9. That the Mirrored Drive shall be maintained by defense counsel and/or the defense expert in a locked file or cabinet at all times except when being actively utilized as provided for herein;

10. That a copy of this Order shall be kept with the Mirrored Drive at all times;

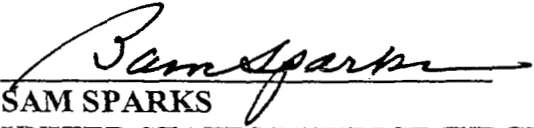
11. That upon termination of this matter the parties shall meet, agree upon, and execute procedures which will result in the non-recoverable destruction, without damage to the hardware, of all data on the Mirrored Drive, and on all computers and computer components used to examine such data. The physical hard drives, computers, and computer components, once the data have been removed, shall remain property of defense counsel or the defense expert;

12. That any dispute as to appropriate data destruction procedure will be resolved by the Court;

13. That upon termination of this matter and data destruction as provided for herein, defense counsel shall file a brief report with the Court, with a copy to government counsel, specifying that the terms of this Order have been complied with and reporting the occurrence of the referenced data destruction;

14. That defense counsel shall be permitted reasonable access to defendant's original computer system for viewing and visual inspection; and

Signed this 20th day of October, 2004.


SAM SPARKS
UNITED STATES DISTRICT JUDGE