OFFICE OF THE MARICOPA COUNTY ATTORNEY
ANDREW P. THOMAS

MEMORANDUM

State of Arizona v. Matthew Bandy
CR2005-014635-001 DT
February 2, 2007

Factual and Forensic Report

On January 12, 2007, an episode of the ABC show *20/20* included a report about a case prosecuted by this office, *State v. Matthew Bandy*. This summary will provide facts, not suppositions or wild conclusions, conveniently left out of the story resulting in a complete distortion of the true events surrounding this case.

Initiation of the Investigation

In November of 2004, internet service provider Yahoo!, as required by federal law, reported to the National Center for Missing and Exploited Children's CyberTipline that on November 7, 2004, images of child pornography were uploaded to a location on one of their servers that was determined to contain a Yahoo! group "beth_lard9." The screen name of the user posting the images was "mrbob1980hoopdu." The Phoenix Police Department's detectives assigned to the Internet Crimes Against Children Task Force continued the investigation.

To understand the nature of these images, it is instructive to review by example the description of one of the image files as described by one of the assigned detectives:

> "This is a color image of a young nude female. The young nude female has blond hair and is sitting on a green couch. The young nude female has her legs apart and is spreading her vagina open with her hands in an exploitive manner. This young nude female is less than fifteen years of age."

It is also important to note that this image was later viewed by a forensic pediatrician who works at ChildHelp in Phoenix, who made the following findings:

> "SMR I (sexual maturity rating, Tanner Stage 1) pubic hair development, SMR I breast development. Estimated Age of Person(s) Depicted: Based on her young facial appearance, her childlike body habitus and her immature sexual characteristics this girl is less than 13 years old."

What the doctor is describing is a pre-pubescent child - not a young-looking adult, not even a young teenager - a child.

One of the detectives then applied for and received a subpoena which was provided to Yahoo! and requested the subscriber information for the person using the screen name "mrbob1980hoopdu." Yahoo! then provided the subscriber information and recent log in times for this user. It is important to note that subscriber information is supplied by the user at the time the account is created and the accuracy of the information is not verified, thus law enforcement will simply be provided with the subscriber information that is input by the user. Interestingly, the user in the case made the following entries in the various fields:

Full name:	"Ms. Joe Bean"
City:	"Phoenix"
State:	"AZ"

The detective also noted that "mrbob1980hoopdu" created the account on November 5, 2004, using the IP address 68.98.62.49 owned by Cox Communications. This same IP address was used by "mrbob1980hoopdu" to log in from November 5 to November 8. Another subpoena was served on Cox to determine who was assigned the IP address during these times. Cox responded that this IP address was being used by an account registered to a Greg Bandy at 1425 E. Desert Broom Way in Phoenix. Other conventional methods of investigation were conducted in order to verify who was living at this address.

Based on this information, the detectives applied for and were issued a search warrant for the Bandy residence that directed them to search for and seize any evidence of violations of Arizona law related to child pornography. It is important to keep in mind that up to this point, the detectives are not targeting any person or persons, only the computer evidence that might lead them to a potential suspect. On December 16, 2004, the warrant was served at the Bandy residence. No persons were injured and no property was damaged any time during or after the service of the warrant.

The detectives explained to Mr. and Mrs. Bandy and their son Matthew that they were investigating a report of someone posting child pornography to a Yahoo! group from their residence. The family was directed to a couch were they sat while the search was conducted. One of the detectives heard Matthew Bandy tell his mother that he had accessed Yahoo! groups. A short time later, after being advised of his constitutional rights against self-incrimination, Matthew Bandy agreed to speak with the detectives. He admitted that he had created the screen name "joebean1988hoopdu" to access Yahoo! and he denied any knowledge of the screen name "mrbob1980hoopdu." He stated that he did indeed join several groups so he could view adult pornography, but claimed he never downloaded any of the images he viewed. Mr. and Mrs. Bandy denied utilizing the computer for improper purposes. Investigation concluded that they did not engage in illegal conduct. Therefore, Mr. and Mrs. Bandy were not considered suspects.

While the interviews were taking place, Det. Larry Core of the Maricopa County Attorney's Office, a computer forensics investigator certified by the International Association of Computer Investigative Specialists (IACIS), was conducting a forensic

preview of the computer that Matthew Bandy admitted using. Det. Core has nine years of experience in computer forensics and over 400 hours of training. He investigates an average of 40 computer crimes a year. He has been a police officer and detective for 35 years. A text search of the Bandy's computer revealed approximately 80 hits for the screen name "mrbob1980hoopdu" and approximately 500 hits for the Yahoo! group "beth_lard9." Det. Core also found thumbnail images of child pornography. The computer equipment, including homemade compact discs, were seized as directed by the warrant so that a full forensic analysis could be completed. Clearly, there existed at that time probable cause to arrest Matthew Bandy for multiple counts of Sexual Exploitation of a Minor. Instead, exercising an abundance of caution, charges were not filed against Matthew Bandy until the investigation had progressed further.

Forensic Investigation

Detective Core conducted his forensic analysis of the computer equipment in June of 2005. Using the latest version of the forensic software program EnCase, Det. Core examined the hard drive of the computer Matthew Bandy admitted to using, as well as the homemade compact discs that were seized from the same table. His 100+ page report revealed the following with respect to Matthew Bandy's HP desktop computer:

1. BIOS date was correct and the time was fast by ten minutes.

2. The HP Pavilion contained a 120-gigabyte Seagate hard drive (serial number 3JT1CK22).

3. The product name is Microsoft Windows XP.

4. There was no registered owner listed.

5. Located on the hard drive was an "Owner Folder". Located under "Owner folder" was a subfolder called "Homework". Located under "Homework" was a subfolder called "English". Located in the "English" folder was a document listing "MatthewBandy" dated 11/14/2004.

6. Located in "D\documents and Settings\Owner\My Documents\My eBooks" was a folder called (‘). Located under (‘) was a subfolder called "kid". Located under "kid" was a subfolder called "Lolita" that contained images of child pornography. Located under "Lolita" was a subfolder called "good ones" that contained 72 images of child pornography. The images received by Detective Curley in his complaint did match almost all of the images on the CD.

7. Searching for the word "mrbob1980hoopdu" received 299 hits.

8. Searching for the word "beth_lard9" received 949 hits.

9. Located in the “Temporary Internet Files” were deleted images of adult and sexual cartoons pornography.

10. Text fragments were bookmarked that did show the pornography sites were visited.

11. Located in the “Recycler Folder” were images of young children and sexual cartoons.

12. Located in the “Recycler Folder” were link files to pornography.

13. Deleted from the “Recycler Folders” were various pornography files.

14. Located on the hard drive was the profile of “mrbob1980hoopdu”.

15. Located on the hard drive was the e-mail address of “mrbob992000”.

16. Located on the hard drive in unallocated clusters was the following.

    [Basic User Info (EReg)]
    firstname=matt
    middle initial=G
    lastname=Bandy
    company=none
    address=1425 Youdontneedtoknow lane
    address2=
    city=Phoenix
    Country=UNITED STATES|USA
    state=Arizona|AZ
    zip code=15489
    phone=000-867-5309
    phone extension=
    dialout prefix=
    use dialout prefix=
    email=mrbob1980hoopdu@yahoo.com
    email2=
    Gender=MALE
    Address Type=HOME
    Phone Type=HOME
    Use=PERSONAL

Det. Core next performed a forensic examination of the CDs that were seized. One of these CDs plays perhaps the most significant role in the case. It contained the same child pornography images that were located on the hard drive of the computer. The Bandy’s would later claim, and still maintain, that this CD was a backup of the entire computer system and that when it was reloaded onto the computer, these images were again inadvertently put back as part of the installation. As described below, and as will be described later based on yet another examination, it is impossible that the entire system

was on this CD, for the CD had a storage capacity of 650 megabytes while the computer contained more than 100 gigabytes of files.

The examination of the removable storage media revealed the following.

1. Located in item 505 were four CDs.

2. On one TDK CD were numerous images of child pornography and sexual cartoons.

3. Located in a folder named "kid/lolita/goodones" were images of child pornography. Several of the images were saved to the CD on November 11, 2004. This is the date the uploads were reported to Phoenix Police Department Detective Curley. The images received by Detective Curley in his complaint did match some of the images on the CD.

Thus, the forensic evidence in the case pointed to only one possible user – Matthew Bandy. The defense offered different theories of why this conduct should not be attributed to Bandy, including the malicious virus theory, however a second examination conducted by Det. Core on September 28, 2006, for the purpose of testing the defendant's theories discredited the attempts to shift blame away from Matthew Bandy.

Second Forensic Examination

The second examination of the hard drive revealed that the operating system was first installed on April 9, 2003 at 4:06 pm. Further examination revealed that the operating system was reinstalled on December 4, 2004 at 05:41:52 pm, mostly likely in an attempt to rid the computer of the viruses which had been downloaded. Examining the folders and files that contained the child pornography revealed that the file creating date was December 4, 2004 at 05:48:15pm to 05:48:24 pm. Approximately seventy-two files were installed on the hard drive on December 8, 2004 at 03:57 pm in "My Documents Folder". The images that were charged on this case were located on the hard drive and the CD. The MD5 hash (digital fingerprint) matched all of the images. Image "felich-13.jpg", "e788.jpg", and "00001113(1).jpg" were also located in unallocated clusters.

Conclusion: It would be impossible for a malicious virus, Trojan, worm, or a hacker to do the following:

1. Create the screen name of "mrbob1980hoopdu@yahoo.com" with the user information of Matt G. Bandy.

2. Download child pornography on November 11, 2004.

3. Burn the child pornography to a CD.

4. Reinstall the operating system on December 4, 2004.

5. Insert the CD into the CD drive and create folders in "D:\Documents and Settings\Owner \My Documents\My eBook\'\kid\Lolita\good ones" and then transfer images from the CD back to the hard drive.

6. On December 8, 2004 approximately seventy two files were created at the same time on the hard drive in "My Documents Folder".

7. Thirty-two animated child pornography images were created between 5:48:29 pm and 5:48:32 pm on December 12, 2004 in a folder named "Animated".

8. In a folder named "Tight" were one hundred twenty images that were created on December 4, 2004 between 5:47:42 and 5:47:49.

9. The document "Matt/English 10/Mrs. Brown" dated November 14, 2004 was created on December 8, 2004 at 3:58:47pm on the hard drive.

Once again, the attempts to deflect the blame in this case to anyone but Matthew Bandy fail.

The Prosecution

It was only after the Phoenix Police Department received the results of Detective Core's examination that the case was submitted to the Maricopa County Attorney's Office for review. On November 10, 2005, Matthew Bandy was indicted by a Maricopa County Grand Jury on nine counts of Sexual Exploitation of a Minor, all class 2 felonies and Dangerous Crimes Against Children because the children in the images were all prepubescent and thus well under fifteen years of age. Some were identified as under age 10. Mr. Bandy received a Summons through his attorney and to this day has not spent any time incarcerated. If convicted at trial, Bandy would have been required to serve at least ten years on each count to be served consecutively. This office never sought nor intended such a result.

The County Attorney's Office reviews each case solely on its own merit in an effort to seek a just result. Investigation revealed that Matthew Bandy was 16 years old at the time these crimes were committed and had no prior criminal record. Under these circumstances a 90 year prison sentence would not be appropriate. It was determined to seek a result that would impress upon Matthew Bandy the significance of his conduct, hold him accountable, afford him supervision while at the same time not destroying his future. To accomplish this result he was offered the opportunity to plead guilty to a class 6 felony and be sentenced to a probationary term. He and his family accepted this result.

This offer was in no way an admission by this office that the case against Bandy was not strong nor that the State did not believe it could prevail at trial. The offer recognized Bandy's age and a reasonable likelihood that he could be rehabilitated.

Not satisfied with a just result, the Bandy's hired a publicist and crisis management team and commissioned the services of a self-proclaimed computer forensics expert to advance conclusions so absurd that they continue to baffle true experts in the field. Detective Core has now, for the third time in this case, reviewed the actual evidence seized from Matthew Bandy. His findings are set forth below and reach the same inescapable conclusion – Matthew Bandy is solely responsible for the crimes with which he was charged and indicted.

Third Forensic Examination

In response to the attack on the prosecution that began with an episode of ABC's 20/20 regarding the Bandy case, this office has again re-examined the evidence in light of the claims made by the defendant, his family, and the people they have engaged to further their account of this case. In the 20/20 report, Tami L. Loehrs, President of LAW2000 Inc., who has little more than 32 hours of forensic training and only on one software program, stated that a hacker corrupted the hard drive in Matthew Bandy's computer by using backdoor Trojans to save their child pornography on his hard drive. Ms. Loehrs stated that this is common for a person that views child pornography to store the images on an innocent person's computer. The viruses that Ms. Loehrs listed in her forensic report revealed that they are associated with file sharing programs. Ms. Loehrs listed backdoor Trojans designed to cause a number of problems, such as slow performance, loss of data or leaking private information. They are distributed by network sharing and file sharing. These are viruses attach to a file, and when accessed on the Internet, are downloaded to your computer with the file. Ms. Loehrs stated in her forensic report: "I noted a significant number of suspicious executable files that began running on or about November 6, 2004 and continued through December 3, 2004". "I was unable to determine the purpose of these files; however, they appear to be related to one or more of the backdoor Trojans identified on the system".

Ms. Loehrs' statements demonstrate a fundamental misunderstanding of the nature of backdoor Trojans. The Trojan tries to make itself hard to remove. For Back Orifice, it uses a file with a name that usually shows up as ".EXE". Sometimes, it uses a name like "MSGSRV32.DRV". Windows prevents deleting the Trojan file while it is active. The viruses attach to Rundll32.exe, systray.exe, scanregw.exe, taskmon.exe, mstask.exe. There are also some other files that are legitimate parts of the registry. The Trojan will usually be in the Windows or Windows\System folder. Trojans are designed to take over a hard drive and steal passwords, screen names, and private information about the user. Attached as Exhibit 1 is basic information on "malware", or malicious software such as viruses, worms, Trojans, and spyware.

Recall that on approximately November 8, 2004, Yahoo! reported to the National Center for Missing and Exploited Children, images of child pornography were uploaded from a group called "beth_lard9" by a person using the screen name of "mrbob1980hoopdu". It should be noted that Yahoo will report the information to the National Center for Missing and Exploited Children (NCMEC) several days after the site is shut down. During the service of the search warrant at Bandy's home, a CD was found

on the desk next to the computer that contained numerous folders of child pornography, animated child pornography, and nudists. The forensic evidence shows that this CD was burned on November 4, 2004 at 10:31 p.m., and that the operating system was reinstalled on the computer on December 4, 2004 at 5:41 pm. On December 4, 2004 at 5:49 pm, there were folders installed on the hard drive that contained images of child pornography, animated child pornography, and adult pornography. The folders were installed in "D\Documents and Settings\Owner\My Documents\My eBooks\'\. The folder "'" was created by the user and was created under the folder of "eBooks" to hide it. Some of the folders on the hard drive contained the same files on the CD and the images contained the same MD5 hash, or digital fingerprint.

Attached as Exhibit 2 are screen shots of the file structures of the CD that was created on November 4, 2004 at 10:31 pm and the folders that were created on the hard drive on December 4, 2004 at 5:49 pm. Attached as Exhibit 3 is a screen shot of an HTML page showing that "mrbob1980hoopdu@yahoo.com" was approved for membership to the "beth_lard9" group on November 6, 2004.

The following question was posted on the International Association of Computer Investigative Specialists (IACIS) list server. The people who subscribe to this list are all certified forensic computer examiners. "A defense computer forensic examiner recently made a public statement that it is well known that a person that views child pornography will hack into a personal computer belonging to an innocent party and store their child pornography on that person's hard drive without the owner's knowledge. Has anyone heard of this defense or had a case where this occurred"? In a span of less than 48 hours, a dozen responses were received all indicating that the scenario described by Ms. Loehrs was simply unheard of. The responses received are attached as Exhibit 4.

The Forensic Facts of the Case

- On November 4, 2004 at 10:31 pm, a CD was created with fifty-one folders that contained over 2,800 images of child pornography, adult pornography, and animated child pornography. This CD was created by Roxio DVD and CD burning software. Roxio was on the hard drive in the Bandy's computer when this CD was burned.

- On November 8, 2004, Yahoo reported to the National Center for Missing and Exploited Children that a person using the screen name of "mrbob1980hoopdu" was uploading images of child pornography to a group called "beth_lard9". The National Center for Missing and Exploited Children reported this to the Phoenix Internet Crimes Against Children Task Force. An HTML page was located on the hard drive where "mrbob1980hoopdu" was approved to be a member of "beth_lard9" on November 6, 2004. See Exhibit 3.

- At approximately the same time, the child pornography was uploaded and the viruses appeared on the hard drive, according to Ms. Loehrs' report.

- On December 4, 2004, at 5:41 pm, the operating system was reinstalled on the hard drive of the Bandy's computer. See Exhibit 5.

- On December 4, 2004 at 5:49 pm (eight minutes later) a subfolder named "**'**" was created by a user under the folders "My Documents/My eBooks". There were fifty-eight subfolders in that directory that contained over 3,000 images of child pornography, adult pornography, animated child pornography, and nudists. The folders listed as "Lolita" and "good ones", where the child pornography was located, contained almost all of the same images that were located on the CD that was created on November 4, 10:31 pm. A MD5 hash was run to compare the images and they were the same. The images that were sent to the Phoenix Internet Crimes Against Children Task Force from the National Center for Missing and Exploited Children were located on the CD and hard drive. See Exhibit 6.

- On December 5, 2004 at 4:56 pm, folders containing pornography were created. On December 11, 2004, between 11:43 pm and 12:43 am, these folders were deleted. See Exhibit 7.

- On December 8, 2004 at 3:58 pm, a number of personal documents, relating to school work, were created on the hard drive that were initially created as far back as September 16, 2004.

- Under the homework folder were subfolders named "Bible", "Biology", "English", History", "Math", and "Spanish". The creation date was December 8, 2004 at 3:58 pm. The only folder that contained a file was the "English" folder. The file was titled "Piggy forever.doc". At the top of the document was "MatthewBandy", "English 10", Mrs. Brown", "Lord of The Files Leadership Essay" dated 11/14/2004. This file was last accessed on December 11, 2004 at 12:31 pm.

- In the "Recent" folder was a link file to the folder "**'**". The last access time was December 11, 2004 at 12: 32 pm. See Exhibit 8.

- In the "Recent" folder were six link files to "Jesus Journals". The access time was December 11, 2004 at 12:32 pm. This was the same time that the child pornography was viewed. See Exhibit 8.

- In the "Recent" folder was a link file to the folder "kid" folder. The last access time was December 11, 2004 at 4:23 pm. This is the folder where the child pornography was saved. <u>The essay and the link files to the child pornography were accessed on the same date (December 11, 2004) and one minute apart.</u> See Exhibit 8.

- In the "Recent" folder was a link file to "good stuff" folder. The last access time was December 11, 2004 at 11:45 pm. This folder contained the child pornography. See Exhibit 8.

- Located in unallocated clusters was a URL path to "Visited: Ownerfile:///C:/Doctments and Settings/Owner/My Documents/**i**/pix/kid/Lolita/good ones/tnPICT0008.jpg. This child pornography was viewed on October 25, 2004 at 12:56 am. A child pornography image of "vika09" was viewed on November 3, 2004 at 4:55 pm. There were other child pornography images viewed dating as far back as February 11, 2004 at 9:51 am. Ms. Loehrs reported in her forensic report that the viruses were present between November 6, 2004 and December 3, 2004. These files were viewed before the viruses were found on the hard drive. See Exhibit 9.

- A second CD recovered during the search warrant was also created by Roxio DVD and CD burning software on July 24, 2004 at 10:39 am. This CD contained a story written by Matthew Bandy. See Exhibit 10. Thus, on this date and time, the Roxio software program was on the computer. Recall that when the CD containing the child pornography was burned on November 4, 2004, the same software was used.

In the seven page forensic report submitted by Ms. Loehrs, she only reports finding "Trojans and viruses" on the hard drive. She does not show any evidence that a hacker had taken over the hard drive and saved his child pornography to view at a later time. Ms. Loehrs states in her forensic report that she received a CD marked as evidence and a separate envelope that contained a password. Interestingly enough, she did not provide any forensic report on the evidence found on the CD. Ms. Loehrs states on her forensic report on page five, "In addition, I noted a significant number of suspicious executable files that began running on or about November 6, 2004 and continued through December 3, 2004.

All files had similar naming conventions (ie: Aooo4696.exe., A0009921.exe, A0007346.exe, etc.) I was unable to determine the purpose of these files: however, they appear to be related to one or more of the backdoor Trojans identified on the system." This is simply not the case. The viruses relate to spyware and adaware. They are not back door Trojans. See Exhibit 11.

On January 23, 2007, Det. Core was provide a report that listed those items Ms. Loehrs reported as viruses. See Exhibit 9 attached. This list was not part of the original forensic report given to our office but was only recently provided by Matthew Bandy's defense attorney at our request. Listed on the report were restore points from the "System Volume Information" folders and subfolders. A virus checker was run against the folders and no viruses were located. What Ms. Loehrs listed as viruses were located in the folder "System Volume Information" restore points, and they are simply not viruses. See Exhibit 12.

Ms. Loehrs identifies six Trojans, however our investigation found only two of them on the hard drive, which were not capable of permitting someone to remotely control the computer. The virus "instsrv.exe" is the "bargain buddy" adware program which is not capable of remotely controlling a computer. The virus divx.exe, which was ironically created to target users downloading child pornography and illegal software, showed up with the error message "failed to download url;" it was unable to control Bandy's computer. The other Trojan and adware files listed by Ms. Loehrs in her report were not found on the computer: backdoor.w32.rbot, backdoor.rbot.gen, trojanproxy.win32.bobax.c., and win32.winshow.g.

Ms. Loehrs' report states that she could not determine whether antivirus protection was updated or running. In fact, the Norton Antivirus on Bandy's hard drive was running and the "Auto-Protect" was on, "Email Scanning" was off, "Script Blocking" was on, "Automatic LiveUpdate was on, and the system was scanned on December 10, 2004. The virus definitions were updated on December 15, 2004. See Exhibit 13. A memory run was completed on the Bandy's hard drive and the examination of the files did not show any Trojans running. See Exhibit 14. Lastly, the hard drive was run against an updated version of Norton Antivirus and no Trojans were located, only spyware and adware. See Exhibit 15.

Conclusion

The entirety of the evidence in this case shows that no remote user ever controlled Matthew Bandy's computer, as the Bandy's and their entourage now claim. Rather, the evidence clearly shows that Matthew Bandy is responsible for the manipulation of the folders and files on the computer and the storage media.