Technical review of the Trial Testimony
State of Connecticut vs. Julie Amero

March 21, 2007

Contributors (alphabetical order):

Alex Eckelberry
Glenn Dardick, Ph.D.
Joel A. Folkerts
Alex Shipp
Eric Sites
Joe Stewart
Robin Stuart

Introduction

We have prepared this document as a technical review of the testimony in State vs. Julie Amero, a case involving a substitute teacher (Julie Amero) who has been convicted of 4 felony counts of "Risk of Injury to a Child in violation of Connecticut General Statute 53-21(a)(1)".

Each of us has various levels of professional experience in the field of computers and technology. We have reviewed the transcripts of the trial (docket number CR-04-93292), as well as evidence supplied to the defense by the prosecution.

This document does not deal with our forensic analysis of the physical evidence (namely, a copy of the disk drive itself). Rather, it is a review of the technical information presented at the trial, and in some cases compares what we know of the physical evidence against the testimony presented.

We are offering this document as additional information which we believe should result in a re-examination of the physical and circumstantial evidence. We have performed this analysis on a purely voluntary basis, outside of our normal work. Our opinions and findings are ours, not of our employers.

It should also be noted that we found inconsistencies in the trial transcript when compared against the police reports and other information which did not fall into our mandated purview of technology and technology concepts. Others qualified in legal or investigative matters may contact us for further information.

Glossary of terms

At the end of this document, we have provided a basic glossary on some of the concepts used in our analysis. We would urge that anyone unfamiliar with technical concepts should review that section before continuing, as a number of critical pieces of information rely on a basic understanding of the terms used.

Summary of findings

Our findings lead us to believe that incorrect information was supplied in court. In addition, we are concerned as to the possible lack of a thorough forensic examination on the physical evidence by both the defense and the prosecution.

The physical evidence

A disk image was provided by Herb Horner, the defense's expert witness, to Eric Sites of Sunbelt Software. The disk was imaged from Mr. Horner's copy using Ghost, a disk replication product (Mr. Horner had similarly received a Ghost image from the Norwich police).

It should be noted that to forensic experts, Ghost is not typically considered the first tool of choice for copying a disk drive. While it can be customized to some degree[1] to provide a forensically-acceptable match of the original system, other forensic imaging tools such

[1] http://service1.symantec.com/SUPPORT/ghost.nsf/pfdocs/1999110813413225

as Linux's dd or EnCase Forensic are generally the preferred method of copying media. Furthermore, these image files can be verified to be an exact duplicate of the original media through a process called hashing. Also, a "write blocker" should also be used copy a drive image, in order to insure that the source drive has not been altered in any way (it is unknown whether or not a write blocker was used in this instance). Failure to adhere to strict standards in the imaging of forensic data can potentially render it inadmissible in a court of law[2].

Hence, we are unable to complete a full forensic examination on the drive in question without having a bit-for-bit copy of the hard drive, as well as the complete firewall logs for that day (or at least for the morning of October 19th, 2004).

Nevertheless, the disk image offered enough information to provide a basic review of the system's state and activities conducted on October 19, 2004. We would recommend any future forensic analysis to be done using industry-standard methods, as mentioned above.

Environment

Our analysis of the physical evidence showed that the system was running Windows 98 (4.10.1998, original version) running Internet Explorer 6.0.2800.1106IC. The system had previously been a Windows 95 system that had been upgraded to Windows 98.

The system's antivirus software was a trial version of Cheyenne AntiVirus ("Cheyenne AntiVirus for Windows 95 v4.00- Live trial build 048"). The antivirus definitions were at least three months out of date[3]. Furthermore, the antivirus definitions were themselves not updated regularly. The last attempt at an update was August 31st, 2004. This was of course a "do-nothing" update, because no new definitions had been available for some time.

[2] And: http://www.ncjrs.gov/pdffiles1/nij/199408.pdf "Examination is best conducted on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence." In Chapter 3, Evidence Acquisition, it states: "Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination. For these reasons special precautions should be taken to preserve this type of evidence. Failure to do so may render it unusable or lead to an inaccurate conclusion." An additional reference: http://www.krollontrack.com/newsletters/cybercrime/aug06.html "...steps a forensic expert should take to prevent data from being altered or damaged through improper handling: Secure the computer system to prevent it from being tampered with by investigators, third parties or automated processes. Avoid analyzing data on the machine from which it was collected. Do not run programs on a computer under investigation. Exercise minimal interaction with original evidence. Make exact, forensically sound copies of data storage devices. Protect extracted data from mechanical or electromagnetic damage. Do not change date and time stamps or alter data itself. Do not overwrite unallocated space, which may happen when rebooting. Establish and maintain a proper chain of custody. Failure to adhere to strict industry standards regarding data preservation can result not only in the loss of critical data, but also can impinge upon the credibility of any data that is recovered, potentially rendering it unreliable or inadmissible in a court of law."

[3] Support for the Cheyenne version by Computer Associates (also known as Inoculan) officially ceased on March 17th 2004 (Cheyenne was purchased by Computer Associates in 1996 and users of the Cheyenne product were gradually moved over to the Computer Associates equivalent, eTrust Antivirus.) However, Computer Associates unofficially continued support until June 30th, 2004, when they released their last signatures, version 47.35.

Antispyware or client firewall software was not found on the system. In addition, there was no popup blocking technology. Finally, as was testified at the trial, the school's content filter's subscription had expired (reportedly for several months[4]).

Analysis disclosed that on October 12, 2004, an adware program, newdotnet, was installed onto the system[5].

[4] http://www.norwichbulletin.com/apps/pbcs.dll/article?AID=/20070124/NEWS01/701240317

[5] See glossary for further description. The newdotnet Spyware program was installed at 14-Oct-2004 15:35. At this time, no browsing activity was detected. The program suite "Free Offers from Freeze.com" was installed at the same time. It appears that newdotnet was installed as a result of installing a Halloween screen saver. It is likely that newdotnet was unintentionally installed at the same time as this program, which is a common practice in spyware.

Analysis of testimony

We have analyzed statements made by both the prosecutor and the prosecutor's witnesses for significant technical issues.

Testimony of Bob Hartz, IT Manager for Norwich Public Schools

Bob Hartz made potential misstatements in his testimony, both in actual fact as well as possibly misleading statements which may have been interpreted incorrectly by the jury.

i. Use of the Temporary Internet Files directory and firewall logs as testimony[6].

During his testimony, the prosecutor and Hartz referred to the Temporary Internet Files directory, which was subsequently shown by the prosecution on a large screen in the courtroom, showing various adult-themed websites.

It is our belief that the listing of the Temporary Internet Files directory, by inference, suggested that Amero intentionally accessed websites whose contents were cached in the directory. The Temporary Internet Files directory does not necessarily indicate which websites were intentionally viewed by the user. It is merely one component forensic examiners analyze to determine how the computer was utilized. Additional analysis is performed on several components including the index.dat file. This file is used in several ways including the tracking of web browsing history, cookie tracking, and the correlation of cached pictures to the corresponding website.

To the uninitiated user, a listing of sites in the Temporary Internet Files directory can be quite misleading. However, used in context and with the correct forensic analysis, a damning website can be found to be, in fact, simply a popup.

The prosecutor and Hartz also discussed Hartz's analysis of the school's firewall logs. It should be noted that these logs merely provide a listing of sites accessed, whether intentionally visited or not.

Isolated analysis of the firewall logs and Temporary Internet Files directory lack critical context and in our opinion, should not be solely used as forensic evidence. Hartz's testimony did not establish Amero's intention to access inappropriate sites; however, this subtle point may have been lost on the jury.

ii. Incorrect testimony to existing virus protection

Hartz testified that the computer had updated virus protection and that it was updated weekly.

> "Anti-virus updates, Inoculate IT was updated I want to say weekly. It would have been updated no later than October 12th, the week before that and probably sometimes towards the middle of the week." [7]

[6] Trial testimony, pages 68-79

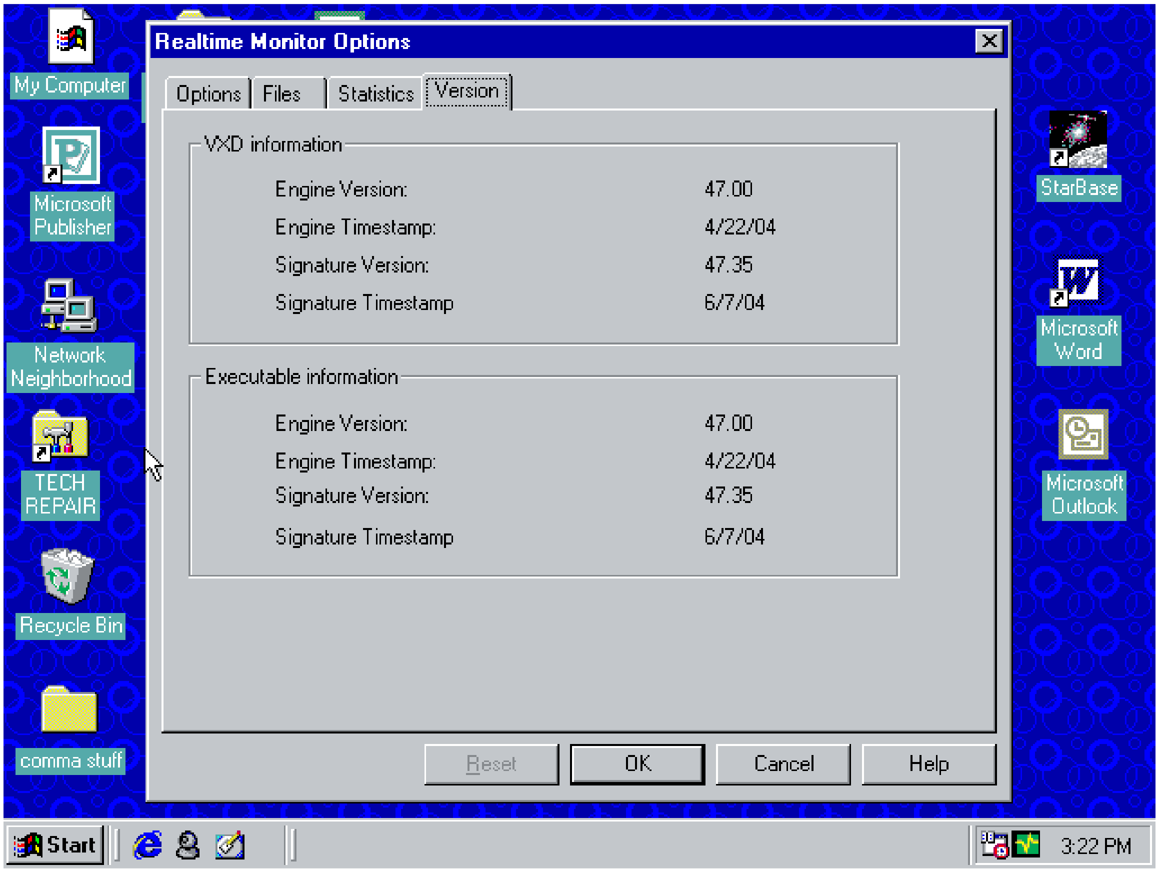
[7] Ibid. page 92

This statement would give the impression that the machine was protected against, at least, certain types of malicious threats.

However, according to the system's antivirus update log[8], the virus signatures were last updated on 8/31/2004 at 11:46:57 am. The signatures themselves were from June 30th 2004, which was the last update Computer Associates ever made for this product.

As stated by the company, "CA has dropped support for InoculateIT/Inoculan v 4.x for Windows (including signature updates and localized versions) effective March 17, 2004." [9]

As an example, the following is a screen shot of the version numbers of the Cheyenne product taken from the hard drive in question:



Realtime Monitor Options

VXD information

Engine Version: 47.00
Engine Timestamp: 4/22/04
Signature Version: 47.35
Signature Timestamp 6/7/04

Executable information

Engine Version: 47.00
Engine Timestamp: 4/22/04
Signature Version: 47.35
Signature Timestamp 6/7/04

In other words, Hartz's statement that the antivirus engine was updated weekly is physically impossible.

iii. The IT manager was unaware that adware was on the system and testified that adware/spyware is not capable of spawning pornographic popups.

[8] C\Program Files\Cheyenne\AntiVirus\AVUPD95.LOG
[9] http://www3.ca.com/securityadvisor/newsinfo/collateral.aspx?cid=52311

From his testimony[10]:

> *Question*: Were any of these viruses on the computer?
> *Answer:* I don't know of any viruses that were on the computer nor do I know if any adware or spyware was on the computer.
>
> *Question*: Does spyware and adware generate pornography?
> *Answer:* Not to the best of my knowledge.

Forensic analysis disclosed that adware program "newdotnet" was installed on the system. In addition, adware programs have been well documented to generate popups containing pornographic material.[11]

iv. Hartz testifies as to "endless loop" pornographic popups

From the trial testimony[12]:

> *Question*: Is it possible to be in an endless loop of pornography?
> *Answer:* I've never seen that, so I would have to say probably not.

Popups that continually inundate a user may be referred to as "popup bombs" or "mouse trapping" and are a common occurrence on pornographic websites. These popups can easily be created manually or by using a simple program such as Nuclear Bomb[13].

[10] Trial testimony, page 86

[11] Sample references include Ben Edelman, http://www.benedelman.org/news/062206-1.html and SunbeltBlog http://sunbeltblog.blogspot.com/2007/01/so-you-want-to-see-what-porn-spyware.html

[12] Trial testimony, page 88

[13] http://scripts.filehungry.com/product/php/ad_management/nuclear_bomb_-_hidden_popup_windows_generator

Testimony of Detective Mark Lounsbury
We found a number of misstatements in Mr. Lounsbury's testimony

i. Lounsbury solely relied on ComputerCop Professional.

Lounsbury testified that he solely relied on ComputerCop Professional for his forensic analysis[14]. By the company's own admission, the program is incapable of determining whether a site was visited intentionally or accidentally[15]. It is our understanding that ComputerCop searches a hard drive for suspicious terms and images, and in the professional version, provides export capabilities of the findings into a "Case Manager" component.

While we have not evaluated this program, we believe the use of only one program, such as this one, does not constitute an exhaustive and rigorous forensic evaluation. A proper forensic examination should do many other things, including looking at the firewall logs, which contain the complete history of all pages visited, and also of blocked pages[16]. We are also not clear if any attempt was made to piece together how the PC went from site to site.

It's worth noting that, to our knowledge, ComputerCop is not a program that is widely used in expert forensic circles, despite intimations otherwise on the company's website[17]. While it may be useful as one aspect of an investigation, as we have seen, the Norwich Police Department used it exclusively for investigation Julie Amero. The idea that ComputerCop would be used *solely* for the prosecution of individuals is of concern: it is our belief that this program does not replace careful, manual forensic examination, using a number of different tools.

ii. Pornographic images were displayed from the websites in question for the jurors

On multiple occasions during Lounsbury's testimony, pornographic images apparently captured through ComputerCop were displayed on the screen[18], which were ostensibly taken from the Temporary Internet Files directory. These were simply displayed as pornographic images for the jurors, which may have lead the jurors to believe that Amero intentionally displayed pornographic material to students. In fact, we found that the images displayed had little relevance to the images actually seen by the children.

iii. By his own admission, Lounsbury performed no examination of the computer for adware

From the trial testimony**[19]**:

[14] Trial testimony, pages 119-120

[15] http://www.networkperformancedaily.com/2007/01/the_strange_case_of_ms_julie_a_2.html

[16] The files on the PC itself only log the last visit to pages which were visited successfully. The firewall logs can therefore be used to determine the browsing patterns, giving a much more detailed insight into what happened.

[17] From the company's website (http://www.computercop.com): "ComputerCOP is the developer of a suite of computer monitoring and forensic tools for home, corporations and a wide-range of law enforcement and law enforcement-related agencies."

[18] Trial testimony, pages 125-127

[19] Ibid. page 134

Question: Did you examine the hard drive for spy ware, ad ware, viruses or parasites?
Answer: No, I didn't.

iv. Lounsbury falsely claims that a "red" link indicates a site has been visited. Lounsbury testified that a change in link color (specifically, the color red) indicates that someone *intentionally* viewed a site. This was further heavily emphasized by the prosecutor in the closing arguments.

From the trial testimony[20]:

Question: Are there any specific characteristics that may occur to a web page when you click on specific link?
Answer: Yes. When you click on a link, again, links are Javascripted, you click on a link, it changes color and then you will get sent to that new address, that new page or site.

[Authors' note: JavaScript has nothing to do with links in this regard.]

Question: Detective, when you actively clicked on a link from the web page, what are one of the detail signs that it was an active click of a link on a web page?
Answer: Again, it would be a different color, it will change colors.

Question: That is based on -
Answer: They do that so that you know where you are now. If you have a number of links, they are all the same color, you click a link, it sends you somewhere else. You still have your list of links. You see the one that is highlighted, that's where you are now.

Question: I'm going to come down here and read a couple of website pages. Could you tell me what those are?
Answer: Bring Her To Climax, Give a Girl An Orgasm, Orgasm Machine, Pussy Orgasms, Female Sex Enhancers, Ask Our Doctors.

Question: Are those indicative of other website pages that originally existed on the computer?
Answer: Those are all links.

Question: I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?
Answer: The color, it's red.

[20] Trial testimony, pages 288-295

Question: And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?
Answer: That indicates that that link was actively clicked on and you were then sent to that page.

Question: Okay. So a person would actually have to click on the Female Sex Enhancers link to go to another page, correct?
Answer: Yes.

And upon cross-examination by defense attorney Cocheo, Lounsbury stands by this incorrect notion:

Question: Detective Lounsbury, you indicated that, I guess, the coloration in the photograph shown to you by Mr. Smith indicates that links were clicked on, is that correct?
Answer: Yes, sir.

Question: When you say indicated, you are not saying a hundred percent?
Answer: I've never seen anything other than that.

Question: But you're not saying a hundred percent?
Answer: In my mind it is.

Question: Are you saying you're positive?
Answer: Based on my knowledge of how it works, yes.

Question: What about the science of it also?
Answer: Which is based on my knowledge of the science.

The prosecutor then discussed this information theme in his closing arguments [emphasis added]:

> I think it's very clear that that just didn't happen, pop-ups randomly popping up over and over and over during the course of the day…
>
> What I point out is that the defense's own expert indicated that if redirects were to come through, it would not leave an address on the computer. I believe he stated it up there.
>
> <u>You have to type it in, and that is when the address comes in. You don't get a mark in the temporary Internet folder unless you actively go to that site. I believe I made that clear with him.</u>
>
> I would ask that you look at State's Exhibit 4, the Internet sites visited on the log, and you will see specific sites about masterbation.com, or orgasm.mystery.com, store.sex-superstore.com. I believe there is also later in the day

> vaginalcumshots.com. Based on the testimony of the defense's witness, that information could only get there if she actively accessed those sites.
>
> *[Author's note: The prosecutor's reference to the "defense's witness" making these various claims may cause some confusion to the reader. In fact, we have found no such claims having been made.]*
>
> …You would have to actively click to get at these sites. Femalesexual.com, cheatinglesbians.com. I would ask you to go through that, correlate that with the time, correlate that with what their witness said about you have to actively physically click on it to get to the site.
>
> Exhibit 6 hopefully is trying to explain the difference in color as to the JavaScript elements which he clicked on. Some of us using our common sense understand this; when you click on a web page it transfers you over. And that changes to show that you actually accessed that page. Take this into account for intent; that the defendant purposely accessed those websites.
>
> I think the evidence is overwhelming that she did purposely access those websites and she should be found guilty of all of those counts by the information the state put forward.

It is not difficult to see how testimony shaped the jury's perception of the day's events. A juror on the case, Fred Stephen Fox, recently contacted a journalist and wrote[21]:

> "Finally she was pronounced guilty because she made no effort to hide or stop the porno, not just because she loaded the porno onto the machine. Going to the history pages it was obvious that the paged were clicked on they were not the result of pop-ups. Each web page visited showed where links were clicked on and followed to other pages. Pop ups go to sites without change link colors, as in used links."

However, this claim made is incorrect, for a number of reasons.

a. All websites visited are always in a changed color.
Visits, whether intentional or not, are always shown in a changed link color. For example, a popup is shown as "visited" (usually, in the color red), as does an intentional visit[22].

b. On the system in question, the link color had actually been changed from the default red to green.

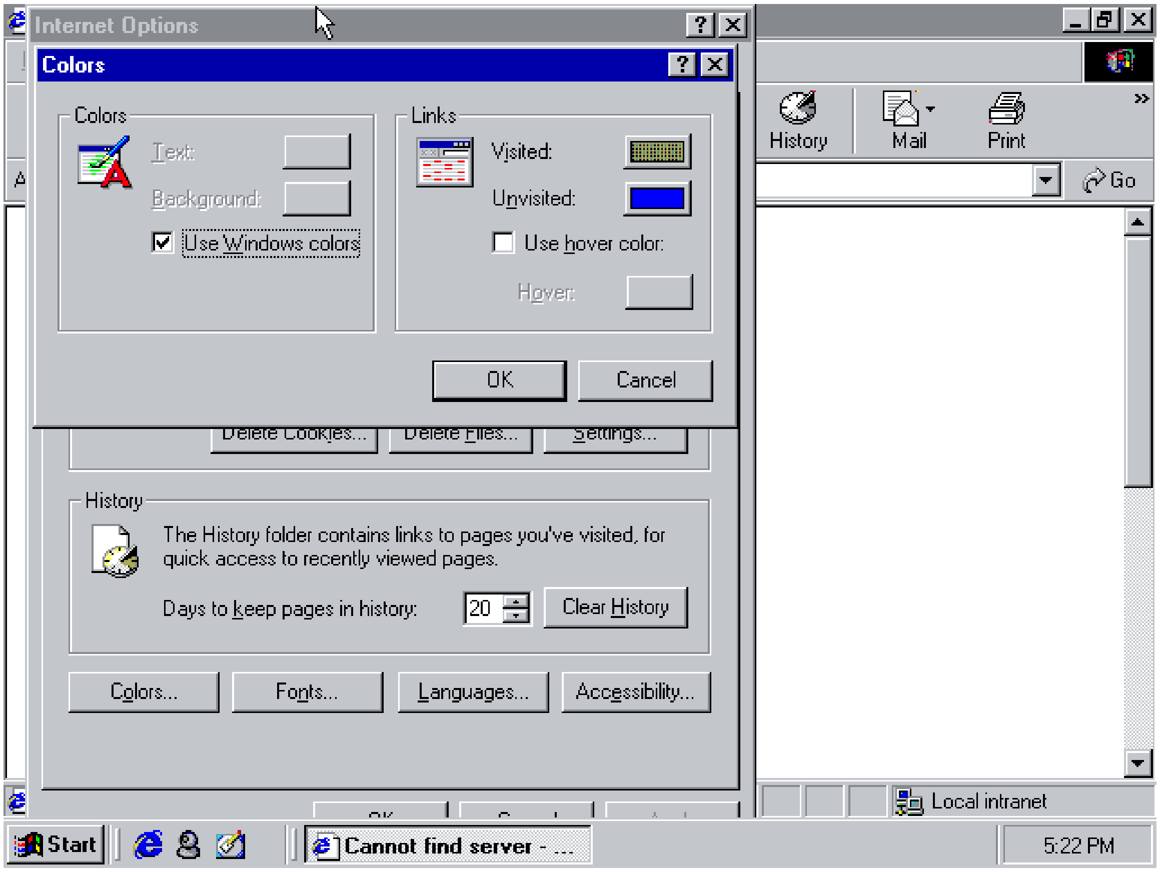
[21] http://blogs.pcworld.com/tipsandtweaks/archives/003741.html

[22] A change in the link color would generally only indicate that the page referenced by the link had been visited. This means that while the link may have been actively clicked on, it could also be the result of the page being called by another page through a script file. For an example, see http://www.joestewart.org/visitedlinkdemo.html

One of the features of Internet Explorer is the ability to change the visited link color – perhaps for cosmetic reasons, or to assist someone with color-blindness.

We found in our analysis of the hard drive that the default link color for visited web pages on the computer used by Ms. Amero was not actually red, as testified to by Mr. Lounsbury, but actually a greenish-grey color.

By opening the browser and performing a simple check, it was revealed that the link color was not red, as can be seen by this screen shot.



Colors

Text:

Background:

☑ Use Windows colors

Links

Visited:

Unvisited:

☐ Use hover color:

Hover:

History

The History folder contains links to pages you've visited, for quick access to recently viewed pages.

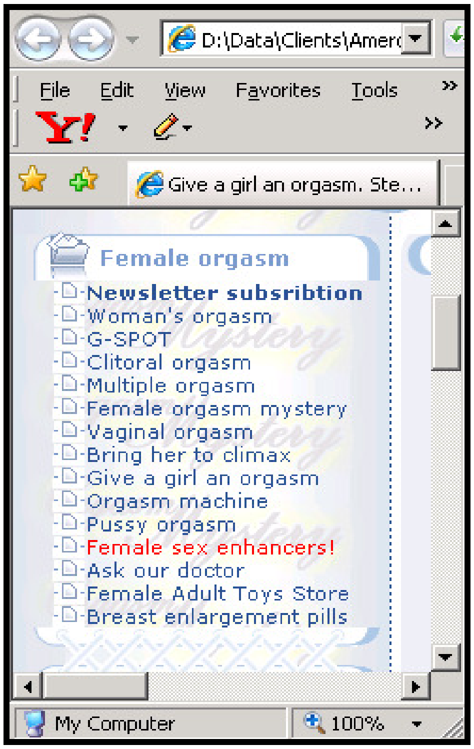
Days to keep pages in history: 20

Indeed, by checking the registry, we were able to verify that the default color of visited links was defined in the registry as "96,100,32", a greenish-gray color, by the registry entry "\Software\Microsoft\Internet Explorer\Settings\Anchor Color Visited" found in the USER.DAT registry within the Windows directory[23].

c. The html source of the page in question actually had a command in it to change the font color to red.

[23] While the default color for previously visited pages on those specific pages could have been determined by the style sheet, sr.css (also found in the Internet cache) that was incorporated into the webpage, it was not - instead the default color of visited links was defined in the registry as “96,100,32”.

By comparing the testimony to the contents of the hard drive, we were able to determine that the page mentioned in the testimony appeared to be from a website called "orgasm-mystery.com". The screen shot below shows the text that was apparently referenced by Mr. Lounsbury and the prosecutor:[24]:



Examining the HTML source of that page, we determined that, in fact, the text "Female sex enhancers" was colored red through the <font color="#FF0000"> tag. Specifically:

```
        <img src="images/folder_25a.gif" width="18" height="12" align="absbottom"><a
        target="_blank" href="viagra-cream-for-woman.htm"><font color="#FF0000">Female
                sex enhancers!</font></a>
```

Hence, it is clear that the text in question was *colored* red, as opposed to being red due to having been visited.

d. That page referred to that particular link does not appear in any of the caches or Internet History files

Lounsbury testified that the link was visited at "9:54:32 a.m" on the 19th"[25]. In fact, we found no evidence that such a visit had ever occurred. The link on the page in question

[24] The page was found in the Temporary Internet Files Content.IE5 cache folder "49armrul" and stored as "give-a-girl-an-orgasm[1].htm". The page originally came from the URL, "http://www.orgasm-mystery.com/give-a-girl-an-orgasm.htm". The page might have also come from the one that was found in the Temporary Internet Files Content.IE5 cache folder "49armrul" and stored as "clitoral-orgasm[1].htm". The page originally came from the URL, "http://www.orgasm-mystery.com/clitoral-orgasm.htm". Both pages contain the links referred to by Mr. Lounsbury. The links are located in the orgasm-mystery.com top-left column menu which is identical on both pages. In both cases the menu has one link which is highlighted in red as testified to by Mr. Lounsbury.

[25] Trial testimony, page 292

refers to a page, “viagra-cream-for-woman.htm”, which appears nowhere in any of the Internet Files caches. References to the “viagra-cream-for-woman.htm” also do not appear anywhere in the Internet History “DAT” files.

These facts are exculpatory evidence showing that the link was never clicked on by the defendant, or for that matter by anyone else, as there was no recorded attempt to ever access or retrieve the page.

We are concerned that Lounsbury’s and the prosecutor’s inaccurate claims swayed the jury’s opinion of Amero’s actions and intention on October 19, 2004.

Further inconsistencies and concerns

“Uncontrollable popups”.
From the trial testimony, Lounsbury claims that there were no uncontrollable popups on the system.

> *Question:* Was there any indication that there were uncontrollable pop-ups?
> *Answer:* There was no evidence.

In fact, we did find evidence of what could be described as “uncontrollable pop-ups” on that system. (Generally, “uncontrollable pop-ups” might be described as popups that occur in a very rapid fashion, and which upon being closed, create more popups. In this case, however, we are merely focusing on rapidity of popups. More analysis can be done upon request.)

For example, from an analysis log created by Joe Stewart, we find this:

```
Cache entry created: 2004-10-19 09:19:26
File mtime: 2004-10-19 09:19:28
Last access by IE: 2004-10-19 09:19:26
File path: whur4da3\a@Position3[1]
http://network.realmedia.com/RealMedia/ads/adstream_jx.ads/hairnews/1x1pop/r
on/wmn/ss/a@Position3
```

Glenn Dardick then performed an analysis using X-Ways Trace (a computer forensics tool) and found that this page was loaded 21 times in one second.

In another case, we find this:

```
Cache entry created: 2004-10-19 09:32:46
File mtime: 2004-10-19 09:32:48
Last access by IE: 2004-10-19 09:32:46
File path: xyq0akc4\openwindow[1].htm
http://www.aboutmasturbation.com/javascript/openwindow.php?hlpfile=
```

Using the same methodology, it was determined that the page was loaded 16 times in one second.

Spyware was not installed after visiting pornographic web sites.
From the trial testimony:

> *Question:* Subsequent to that, to your knowledge, if you had gone to pornographic websites, could spyware have been installed after that fact?
> *Answer:* Once you go to the site, that is most probably the time that you would get infected.
> *Question:* After you go to the pornographic website?
> *Answer:* Yes.[26]

In fact, we see that the spyware installed came on October 12th, after a Halloween screen saver is installed.

We are confused as to the use of "Javascript" describing a link.
There were references to Javascript somehow being related to links: "When you click on a link, again, links are Javascripted" [27] and "Exhibit 6 hopefully is trying to explain the difference in color as to the JavaScript elements which he clicked on."[28] We admit to some confusion as to these statements, as JavaScript itself has nothing to do with links.

Inconsistencies about the computer
Our analysis of the disk image shows clearly that the system in question is a Dell PC. Herb Horner, the defense's witness, maintains that the machine that he saw stored as evidence at the police station was, in fact, a Gateway PC, Lounsbury insists in his testimony that the system in custody was the original computer seized Kelly Middle School[29]. However, Office Belair claims he seized the computer[30], but in his actual police statement he implies only the drive is seized.

Hartz testified that the system was turned off within days of October 19th, 2004; that he took the computer out of the classroom by the 22nd to the principal's office and got Mr Napp another PC. However, our analysis shows that the system was actively in use until approximately 1:43 PM on October 26th, 2006 (on the second third of testimony, the October 26th date was made clear by Detective Lounsbury). This use included internet browsing, which potentially overwrote elements in the browser cache and history files. This means that evidence has been irretrievably lost which could be used to piece together a fuller picture.

[26] Trial testimony, page 294
[27] Trial testimony, page 288
[28] Ibid. 316
[29] Ibid. pages 117-118
[30] Ibid. page 95

Furthermore, Matthew Napp states that he came in one day “probably a couple of weeks afterwards” and the computer hard drive was gone[31]. This contradicts Hartz’s statement that the whole computer was removed to the office for safe keeping.

This issue must be cleared up: Having the original PC in question is critical for checking the system clock in order to determine the correct time. It is also considered professional practice to maintain the PC in its original state, as it is effectively a “crime scene”.

Julie Amero was her own worst witness.

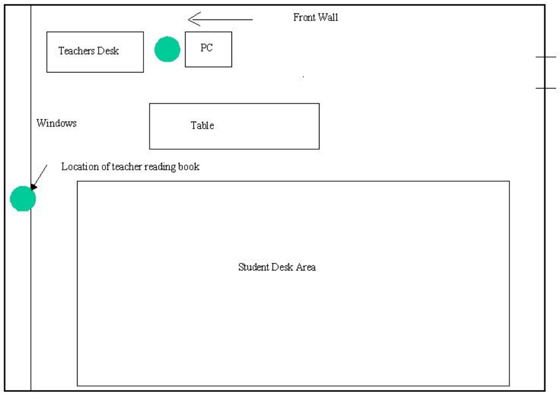
One thing we observed was that Julie Amero had a far worse recollection of the events that day than one can surmise from the evidence to hand. Julie says the pop ups were appearing all day. In fact, logs show the last porn appeared at 11:13am. The police report substantially agrees with this, stating that the porn ends at 11:11am. No children in classes after 11:11am report seeing porn (despite some reports that the computer was showing porn “all day”).

In other words, the entire incident in question occurred over a space of less than two hours.

Location of the computer in question

While some reports may indicate that the pornographic popups in question were available for the children to see, we have some doubt as to whether or not the children were actually able to even see the monitor from their seats.

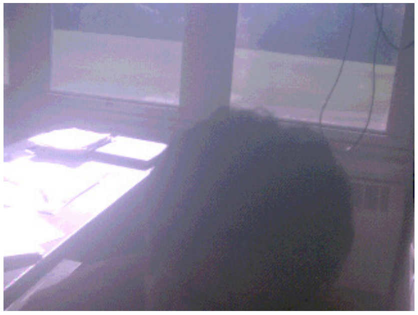
For example, we have this diagram which was produced by consulting Ms. Amero[32].



Also, that system had a webcam and we were able to find an image saved on the system which was apparently a shot from the computer[33], indicating that the monitor was facing toward the window. The image show the computer table is against the front wall instead of in-line with the teacher's desk (and is therefore even further from the students than the

[31] Ibid. page 43
[32] http://region19.blogspot.com/2007/02/drawing-evidence-missing-in-amero-trial.html
[33] Amero drive image, C:\My Documents\QuickCam\Album\Pictures\Picture 1.jpg

above drawing). This would make sense, given the need for various cords to be out of the way. Notice that even though the webcam seems to be angled toward the room somewhat, one isn't able to see any student desks from where it sits.



Obviously, it would be necessary for a site check and further interviews with witnesses in order to resolutely determine the actual position of the computer.

Possible accidental evidence tampering

We did notice that drive was altered somewhat after 10/19/2004. For example, we noticed that the screensaver.com entry for the "haunted house screensaver" is still in the registry, but the whole directory seems to be missing from the hard drive, where it was installed into C:\Program Files\ScreenSaver.com\Haunted House. We were not able to ascertain if an uninstall process would remove the entire ScreenSaver.com directory, or if someone deleted the whole directory tree because they recognized it might be adware.

We also found that on the day after, 10/20/2004 at 15:19:18, http://store.sex-superstore.com/favicon.ico was stored in the cache. Generally, Internet Explorer 6 will only request the favicon when adding a site to the Favorites folder. But the sex-superstore entry is no longer present in the Favorites on the copy we have. So it is apparent that this bookmark was removed the day after the 19th.

Finally, we found the entire temporary internet files directory had been copied to another directory[34], and a deleted index.dat file was also found which provided additional evidence (this file was likely deleted automatically by Internet Explorer, but this fact highlights the need for an accurate bit-copy of the drive, not a Ghost copy).

Pictures shown out of context

From the trial transcript it appears at least 13 pictures were shown to the jury. We believe that these pictures may have been inflammatory for the following reasons:

- What was actually seen: We believe there may be inconsistencies between what pictures were shown in court versus what the children stated they actually saw; this should be examined thoroughly.

- Size of the pictures: The pictures were displayed on a large screen in the court room, at a far larger size than normal.

[34] The directory C:\stuff was created on October 21st, and contains a copy of the Temporary Internet Files directory.

- Out of context: When a page is actually displayed, the pictures loaded may be buried at the bottom of the page or can even be resized depending on the HTML code in the page. We question whether the images shown in the court were ever actually visible on the screen; it is actually possible that the majority of the pictures found on the hard drive never actually displayed on the monitor of the computer (because the images would have required someone to scroll down the page to see them).

- Timeline: Apparently, there was no correlation of pictures to the timeline of when the children saw them. There were four charges, and different minors were in the classroom at different times. Hence, without knowing which charges relate to which possible pictures, we believe it would be impossible for the jury to correctly decide on the charges.

Browsing habits in class
Our analysis of the evidence shows that the system in question was used for a variety of tasks prior to 10/19/2004, much of it school-related, but in some cases, not related directly to school activities. These sites include:

ESPN.com
CBS Sportsline
ffch.football.sportsline.com/standings
football.fantasysports.yahoo.com/
eharmony.com (dating site)
Peoples.com (online banking)

It should be noted that accessing dating sites has been shown to add to the risk of installing malware on the computer. While eharmony.com is a harmless dating site which has no history of installing any malware, accessing dating sites in general can possibly cause spyware and tracking software (not of the type that was loaded on the class computer) to think the user of the computer is interested in pornography – and serve these advertisements specific to that “interest”.

Biographies

Alex Eckelberry is the CEO of Sunbelt Software, a developer of antispyware, antivirus, firewall and other security technologies. He has over 20 years of experience in technology and related areas, having worked for Borland International, Quarterdeck Corporation, Mijenix Software and Ontrack Data. In 2005, both he and Alex Shipp were recognized by Google, Inc. for their contributions to Google's security and product safety.

Dr. Glenn S. Dardick, Ph.D. is the editor-in-chief of the Journal of Digital Forensics, Security and Law as well as the chair and founder of the annual ADFSL Conference on Digital Forensics, Security and Law. Dr. Dardick is a partner in the digital forensics and consulting firm of Integrity-ICT as well as a member of the faculty of Longwood University responsible for its Digital Forensics, Security and Law program. Dr. Dardick has been working with computers since the 60's and was on the original IBM PC development team. Dr. Dardick has been admitted in Federal, State and Sectarian courts as an expert witness in Digital Forensics as well as various IT and Internet matters.

Joel Folkerts studied Computer Engineering at Iowa State University. After graduating college, Joel was commissioned as an officer in the United States Air Force and was assigned to the Air Force Office of Special Investigations (AFOSI) where he was stationed in Germany. As an AFOSI Special Agent, Joel specialized in investigating computer crimes involving criminal and counter-intelligence investigations. Since leaving the Air Force, Joel conducts computer forensic investigations for ManTech SMA supporting national level interests.

Alex Shipp started his career writing memory-resident programs and terminal emulation systems. He was later the lead architect and programmer for one of the world's first internet level anti-malware systems and then invented the first commercial heuristic-only anti-malware scanner. In 2006 he was lead architect for an internet level anti-malware system scanning HTTP web traffic for malware. He holds ten patents, mostly related to heuristical ways of detecting malware. He is recognised as a leading anti-malware researcher, and regularly speaks at conferences around the world, including RSA, Virus Bulletin, AusCERT and AVAR. He has been an expert witness in two cases involving malware, and has been involved with providing help and assistance with malware related incidents and education to law enforcement officials around the world. He has a BA in computer science from Cambridge University.

Eric Sites is the vice president of research and development for Sunbelt Software. An expert in a wide range of programming languages, as well antivirus and antimalware technologies, he has worked for over 20 years in software development. He was previously the chief technology officer for AskSam Systems, a leading developer of database technology.

Joe Stewart, GCIH is the director of malware research with SecureWorks, and specializes in reverse-engineering malware. He has been a SANS GIAC Certified Incident Handler since 2002, and has written numerous articles on malware and cybercrime.

Robin Stuart is a digital forensics specialist with Fortune 100 financial services and ecommerce experience, and a contributing author to the Handbook of Information Security (2005 John Wiley & Sons) on the subject of digital evidence handling. Ms. Stuart is also the founder and Chief Mad Scientist for RCS Security, a forensics consulting and software company.

Glossary

Cache: In computers, an area where data is stored in order to increase performance. For example, there are several caches on a computer which store information on web pages visited. The next time the page is visited, the information can be loaded from the cache, as opposed to downloading it all over again.

HTML: The language used to create web pages. You can view the HTML in a page by choosing "View Source" in your internet browser.

Index.dat file: One of several hidden cache files stored on a Windows system that contains a detailed record of activities performed by Internet Explorer. There are a number of Index.dat files on any system, and the location varies depending upon which version of Windows is used. One of the most critical elements in a forensic examination involving internet usage are the index.dat files on a system.

JavaScript: A programming language used to perform various advanced actions inside of a web page. JavaScript is used to add rich, dynamic functionality to a web page, but it is not required. For example, to have a web page create a new web page (a popup), one would use a JavaScript command.

Newdotnet: A type of adware. Newdotnet itself is a company that sells websites that are not named in a conventional manner (such as websites ending with .shop, .family, .tech, etc.). Normally, Internet browsers don't accept these types of names, but newdotnet has made agreements with various organizations to enable their recognition. However, since not all of the necessary parties recognize these types of names, newdotnet markets a free program, called the "New.net Domain Software", which forces the Internet browser to recognize these unusual names. This software it is often marketed by "bundling" with other applications (such as screensavers). Furthermore, in order to make additional money, newdotnet "hijacks" search results when a user enters keywords directly into their browser address bar. For example, when a user enters a search term directly into the browser address bar (the area where you would typically see "yahoo.com" or other websites), the browser gets confused and produces an error page. This error page is taken over by the newdotnet program and the user is instead directed to a search page with results that ostensibly have a financial benefit to newdotnet (find.reliableresults.info). This particular activity occurred on the morning of October 19th, where someone typed in "new hair styles" into the browser address bar, and then was presented with search results from find.reliableresults.info, which presented the user with the rogue new-hair-styles.com.

Popup: A web page that is displayed without the user's intention. Popups can come from a web site (by the simple act of visiting it) or through spyware.

Spyware (also adware): A term, generally interchangeable with the word "adware", that denotes a type of program which resides on a person's PC, tracks usage and then performs various marketing based on the user's habits. For example, a spyware program may track that a person visits a site about babies, and then spawn a popup about baby bottles. Or, a spyware program may display its own preferred results in a search engine when a person searches for a term. In some cases, spyware can be quite malicious, stealing personal information or performing other dangerous activities. Generally, however, spyware/adware programs are used to market products or to increase traffic to a website, effectively turning a person's pc into a sort of advertising kiosk.

Tags: In HTML, tags are instructions which tell the web browser how to display a page. Tags are enclosed in these symbols: <>. As an example, to create a text in boldface, one enters the tag <b>, writes the text, and ends it with the tag </b>.

Temporary Internet Files folder: A cache folder that contains a record of visits made by Internet Explorer, and stores various elements downloaded from a web page. The purpose of the Temporary Internet Files is to increase the performance of a web browser (as files already in the cache can be loaded from the PC, instead of downloading them again).

Web page: A document connected to the World Wide Web and viewable with a web browser (such as Internet Explorer or Firefox). A web page is what you see when you go to "Yahoo.com" or other sites.

World Wide Web: A part of the Internet, consisting of sites that offer text, graphics, and other resources, all shared through HTTP (HyperText Transfer Protocol).