enfuse™ 2016

The Five Mistakes You Don't Want to Make when Providing Forensic Testimony

Panelists

Suzanne Widup (moderator), Verizon Enterprise Solutions

David Cowen, G-C Partners LLC

Sheryl Falk, Winston & Strawn, LLP

Christopher Novak, Verizon Enterprise Solutions

Jonathan Rajewski, Senator Patrick Leahy Center for Digital Investigation

James Vaughn, iDiscovery Solutions

Mistake #0.5: Lack of fundamental prep

Everyone preps for the 'tough questions,' but what about the basics?

- Top tech experience ≠ Great Expert Witness & Expert Witness Experience ≠ Great Expert Witness
- Expect all parties will research your background thoroughly (prior testimony, social media, etc…)
- Be prepared for challenges to your experience, especially if your education and certifications are light
- Prepare for deposition the same as courtroom testimony, they are effectively the same.
- Prepare for trial, not settlement…

Mistake #1: The assumed truth question

Anytime you're being asked a question that has an assumed fact be wary.

Sometimes they are just throwing something out there to see if you would actually agree with it, true or not.

Other times it is a setup to trap you in a logical fallacy.

- Examples:
  - Isn't it true that malware could have done this?
  - Are you aware that this was something my client was allowed to do?
  - And you agree with everything in this document?
  - And you would have no way of knowing if X happened correct?
  - Are you an expert on what this is?

Mistake #1: The assumed truth question

Wrong ways to answer the question

Sometimes you'll be asked questions meant to lead you into a logic trap. There are several basic mistakes most experts make when responding.

- Answering yes or no
  - If the question does not have a yes or no answer, don't answer it
- Asking a question back
  - Only the attorney gets to ask questions
- Believing the attorney and agreeing
  - An Attorney can ask you a question they know not to be true just to see if you agree with it
- Getting argumentative
  - You appear biased if you argue and get confrontational

Mistake #1 Case Examples

Case Name	Description
Wells Fargo v Super Future Equities	You are not an expert on web server logging are you?
Suncoast v PT USA	A file put in the recycle bin doesn't really delete it does it?
Lockheed Martin v L-3	So this number reflects how many times the document was opened correct?
Metso Minerals v FLSmidth Excel	So this would mean the CAD drawing was accessed by Joe

Mistake #2: Refusing to answer the question

What happens when you get asked the question you hoped they wouldn't ask

Sometimes you'll be aware of a bad fact, you still have to answer the question. Other times you'll be asked to answer a question you know would mislead the judge and jury.

- Examples
  - Isn't it true FTP connections leave no evidence in the HTTP logs?
  - Why do you get paid more to testify than do analysis?
  - Didn't the IT staff login to the machine before you did?
  - Did your client preserve the evidence you are claiming we should have?
  - Can you say this information was a trade secret?

Mistake #2:

Wrong ways to answer the question

Sometimes you'll be asked questions you can't or don't want to answer because of what it implies. There are several basic mistakes most experts make when responding.

- Refusing to Answer the Question
  - This plain does not work
- Answering the Question you wish had been asked. (Dave Cowen is the only one who can do this well.)
- Over Advocating -Refusing to Concede the Obvious
  - You look Biased
- The Professor - Long, Rambling answer
  - You lose the judge or jury
- Say what? Not knowing the facts
  - Never guess

Mistake #2 Case Examples

Case Name	Description
Suncoast v PT USA	Can you recover data after your client wiped it?
Inventory Locator v Partsbase	After seeing all this evidence, would you agree with Mr. Cowen?
Transfirst v Phillips	Are you aware of a contract clause that wouldn't allow this?
Brinson Benefits v Linda Hooper	Can you say that this was a network drive?

Mistake #3: You know more than they do

Anytime you're being asked a question, listen twice…..

Sometimes they ask the way they were prepped to ask, and sometimes they want to see how you answer the technically inaccurate question.

- Examples:
  - Are you familiar with a MD5 hash tag?
  - So you saw evidence that Mr. Smith deleted the files, then emptied the recycle bin?
  - You are familiar with memory allocation, right?
  - Did you create a forensic image of the files?
  - How do you know the website was visited 14 times?

Mistake #3: You know more than they do

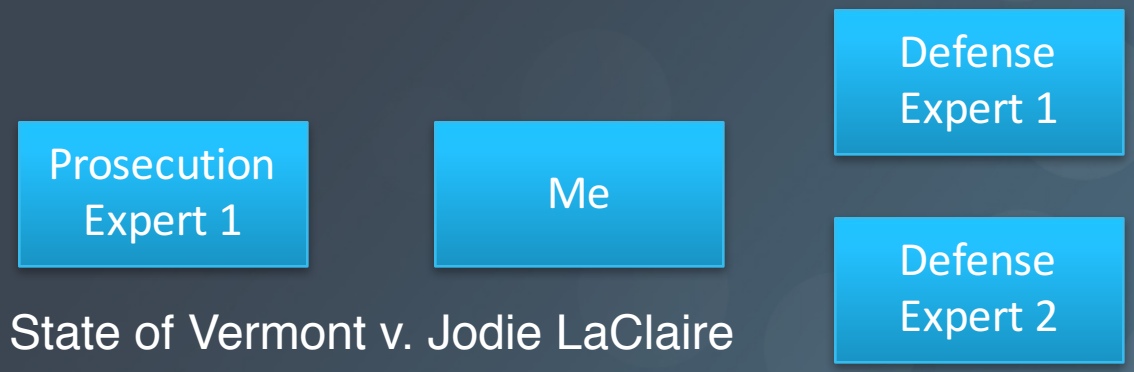
Do not help them formulate the question

Examples:

- Answering yes and stopping to you knowing what a MD5 hash tag is? - This could either way, you could say I know what a MD5 hash value is, or you can say I don't understand the question
- You saw evidence that Mr. Smith deleted files then emptied the recycle bin. YES - Did you? Or did you see who was at the keyboard. Several experts confuse that because Mr. Smith's profile was in use, it was password protected, and you can establish the laptop was physically in his possession, it must have been Mr. Smith. Speculation can cause credibility issues.
- Memory Allocation - Simple answer to how much memory a program needs as a minimum. Do not fall into the game of what if other programs were there, what if other programs were running, etc.
- Forensic image of the files? - If this does not make sense, do not answer the question. If you say no, because you are savvy and you know you imaged the hard drive, or because you used Robocopy to log and capture network data, do not lock yourself into the "forensic image" debate.
- Website visited how many times? – Did you test with more than one tool? This has bitten examiners and came back on them for only relying on one tool, and then found out that 14 website visits or a certain number of searches ended up not being that high.

Mistake #4: You don't know what you don't know…

The "battle of the experts"



Mistake #4: You don't know what you don't know…

What happened on the primary computer on 3/23/2009?

Prosecution Expert 1

1. Someone searched the computer for financials
2. Attempted to accessed a retirement account
   - "Proofing Events"

Mistake #4: You don't know what you don't know…

ProofingEvent

Prosecution Expert 1

Event Timeline – 3/23/2009 (all times EST)
(Timeline details may be found on subsequent pages)

04:16:55	Search (Microsoft Search Assistant) for the term "credit card"
04:18:41	Internet Explorer started
04:18:43	Possible Google.com activity (Internet Explorer homepage)
04:20:09	Possible first usaa.com activity using Internet Explorer
04:21:20	usaa.com proofingEvent15f1a89e
04:22:17	Possible usaa.com logon event
04:22:24	"My Documents" folder opened
05:15:13	usaa.com proofingEvent81328d6e[1]
05:17:03	Possible usaa.com logon event

State of Vermont v. Jodie LaClaire

Mistake #4: You don't know what you don't know…

ProofingEvent

Defense Expert 1

Mobwars was logged into on March 23, 2009 at approximately 5:14 AM by Facebook user [redacted] according to the USAA.com security file proofingEvent81229556[1].htm. This file takes a snapshot of the browser as it exists, including what pages are open in other tabs/windows of the browser, at the time of a login attempt to the USAA website.

Mistake #4: You don't know what you don't know…

ProofingEvent

Defense Expert 1

Q Q Correct.
in A It is something that I'm sure all of us would
Fa love to talk to them about, but it is -- it is a
re file that is used to take a snapshot of who the
person is in the sense of what was open on the
A browser at the time, how fast their connection is,
Q things along that line.
A Q Okay.
Q A And apparently they're using it -- and I use
us the word apparently. Apparently from what I found
A is they're using to more or less profile what the
us user is, what browser they're using, where they
th -- but I think it's used primarily for a security
th reason from what it looks like.

State of Vermont v. Jodie LaClaire

Mistake #4: You don't know what you don't know…

ProofingEvent

Defense Expert 2

proofingEvent81229556[1].htm | Accessed: 3/23/2009 5:14:42 AM

";b:1;s:8:\"fb_frame\";s:7:\"**mobwars**\";s:13:\"is_translator\";b:0;s:14:\"intl_tag_depth\";i:0;s:12:\"translations\";a:0:{}s:17:\"non_underlineable\";a:0:{}}";app_8743457343.data = {**"user":**[redacted],"installed":true}

This excerpt above is the beginning of the event and it displays the game Mob Wars on Facebook, followed by the user number ([redacted]) that is tied with the account. Since this was associated with Facebook, if you enter www.facebook.com/[redacted] into your browser, it will bring up the Facebook profile of [redacted] as shown below.

Mistake #4: You don't know what you don't know…

ProofingEvent

Defense Expert 2

Q Right. And my question for you is were you able to cross reference this information? In other words, did you find any other verification that somebody had indeed logged into this Facebook account at 5:14:42 a.m. anywhere else on the hard drive?

A No.

Q Did you try to do that?

A No.

Q And why not?

A As far as I was concerned, when I saw the two proofing events, one being the USAA website and the proofing event that had a Facebook account logged in under the credentials of [redacted] [redacted] using Mob Wars, I saw that as -- it explains itself really. The evidence explains itself.

State of Vermont v. Jodie LaClaire

Mistake #4: You don't know what you don't know…

Attorney General – Called in another expert

Me

1. Focus on all reports, depositions and confirm/refute findings
2. Essentially help the AG try to determine which side is right and wrong /if they have the right suspect

Mistake #4: You don't know what you don't know…

ProofingEvent

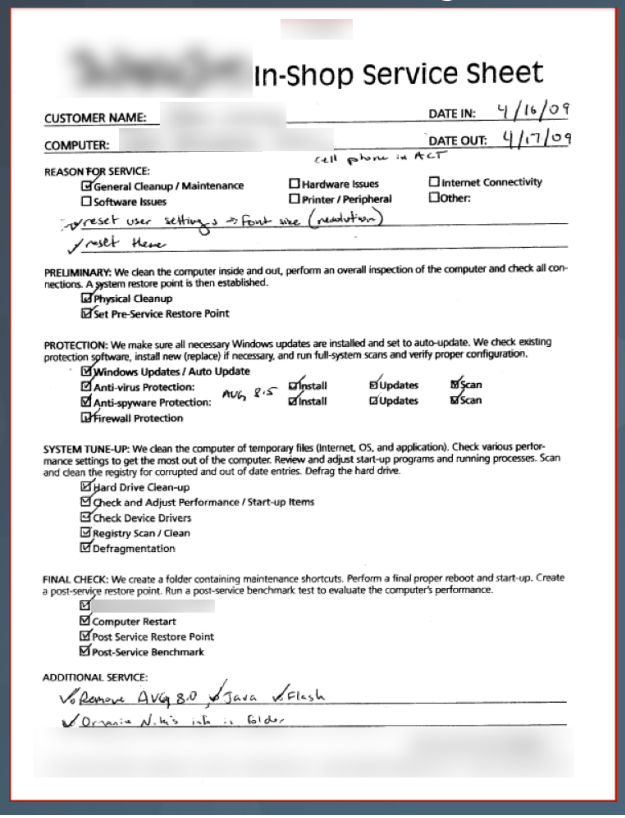
Name	File Created	Last Accessed	Last Written	Entry Modified
proofingEvent81229556[1].htm	03/23/09 05:14:42AM	03/23/09 05:14:42AM	03/23/09 05:14:42AM	04/16/09 06:35:18PM

Cluster Chain – 7001180, 8595034, 709965, 709966, 709967, 709968, 709969, 709670, 709671, 709672, 709673, 709674, 709675 and 709676

We have fragmentation and EnCase reports this file is overwritten.. Can we prove anything about the mobwars activity?

Mistake #4: You don't know what you don't know…

ProofingEvent



[redacted] In-Shop Service Sheet

CUSTOMER NAME: [redacted] DATE IN: 4/16/09

COMPUTER: [redacted] DATE OUT: 4/17/09

cell phone in ACT

REASON FOR SERVICE:

- ☑ General Cleanup / Maintenance
- ☐ Hardware Issues
- ☐ Internet Connectivity
- ☐ Software Issues
- ☐ Printer / Peripheral
- ☐ Other:

preset user settings → Font size (resolution)

✓ reset these

PRELIMINARY: We clean the computer inside and out, perform an overall inspection of the computer and check all connections. A system restore point is then established.

- ☑ Physical Cleanup
- ☑ Set Pre-Service Restore Point

PROTECTION: We make sure all necessary Windows updates are installed and set to auto-update. We check existing protection software, install new (replace) if necessary, and run full-system scans and verify proper configuration.

- ☑ Windows Updates / Auto Update
- ☑ Anti-virus Protection: AVG 8.5 ☑ Install ☑ Updates ☑ Scan
- ☑ Anti-spyware Protection: ☑ Install ☑ Updates ☑ Scan
- ☑ Firewall Protection

SYSTEM TUNE-UP: We clean the computer of temporary files (Internet, OS, and application). Check various performance settings to get the most out of the computer. Review and adjust start-up programs and running processes. Scan and clean the registry for corrupted and out of date entries. Defrag the hard drive.

- ☑ Hard Drive Clean-up
- ☑ Check and Adjust Performance / Start-up Items
- ☑ Check Device Drivers
- ☑ Registry Scan / Clean
- ☑ Defragmentation

FINAL CHECK: We create a folder containing maintenance shortcuts. Perform a final proper reboot and start-up. Create a post-service restore point. Run a post-service benchmark test to evaluate the computer's performance.

- ☑ [redacted]
- ☑ Computer Restart
- ☑ Post Service Restore Point
- ☑ Post-Service Benchmark

ADDITIONAL SERVICE:

✓ Remove AVG 8.0 ✓ Java ✓ Flash

✓ Organize N.h's info in folder

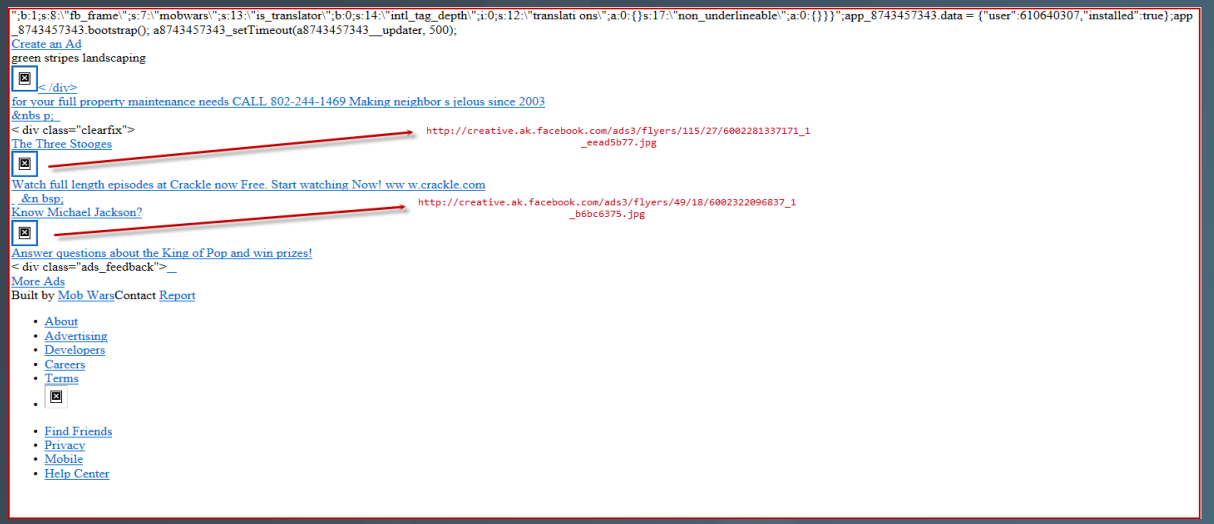
Name	File Created	Last Accessed	Last Written	Entry Modified
proofingEvent81229556[1].htm	03/23/09 05:14:42AM	03/23/09 05:14:42AM	03/23/09 05:14:42AM	04/16/09 06:35:18PM

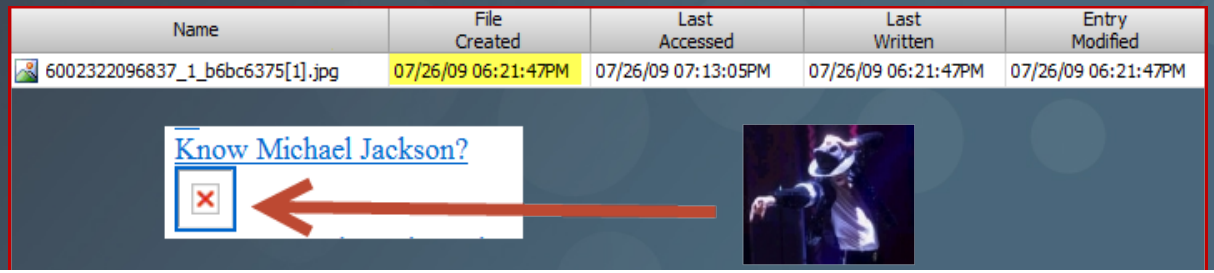
```
";b:1;s:8:\"fb_frame\";s:7:\"mobwars\";s:13:\"is_translator\";b:0;s:14:\"intl_tag_depth\";i:0;s:12:\"translations\";a:0:
{}s:17:\"non_underlineable\";a:0:{}}}";app_8743457343.data = {"user":[redacted]"installed":true};app_8743457343.bootstra
p();
</script>
<script type="text/javascript">
```


Name	File Created	Last Accessed	Last Written	Entry Modified
proofingEvent81229556[1].htm	03/23/09 05:14:42AM	03/23/09 05:14:42AM	03/23/09 05:14:42AM	04/16/09 06:35:18PM

Mistake #4: You don't know what you don't know…

ProofingEvent





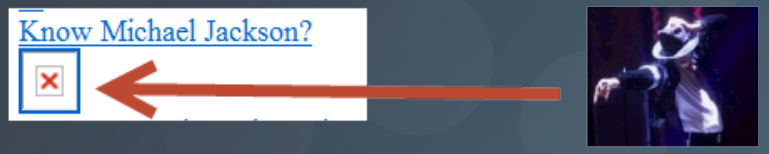
Name	File Created	Last Accessed	Last Written	Entry Modified
6002322096837_1_b6bc6375[1].jpg	07/26/09 06:21:47PM	07/26/09 07:13:05PM	07/26/09 06:21:47PM	07/26/09 06:21:47PM

Name	File Created	Last Accessed	Last Written	Entry Modified
proofingEvent81229556[1].htm	03/23/09 05:14:42AM	03/23/09 05:14:42AM	03/23/09 05:14:42AM	04/16/09 06:35:18PM

Mistake #4: You don't know what you don't know…

ProofingEvent

Name	File Created	Last Accessed	Last Written	Entry Modified
6002322096837_1_b6bc6375[1].jpg	07/26/09 06:21:47PM	07/26/09 07:13:05PM	07/26/09 06:21:47PM	07/26/09 06:21:47PM



"On 7/26/2009 from approximately 5:14:01PM until 7:31:43PM the Facebook website was accessed and a user was interacting with the MobWars application"

07-26-2009 06:10:20 PM	http://apps.facebook.com/mobwars/profile/do.php?action=increase&type=attack
07-26-2009 06:10:24 PM	http://apps.facebook.com/mobwars/profile

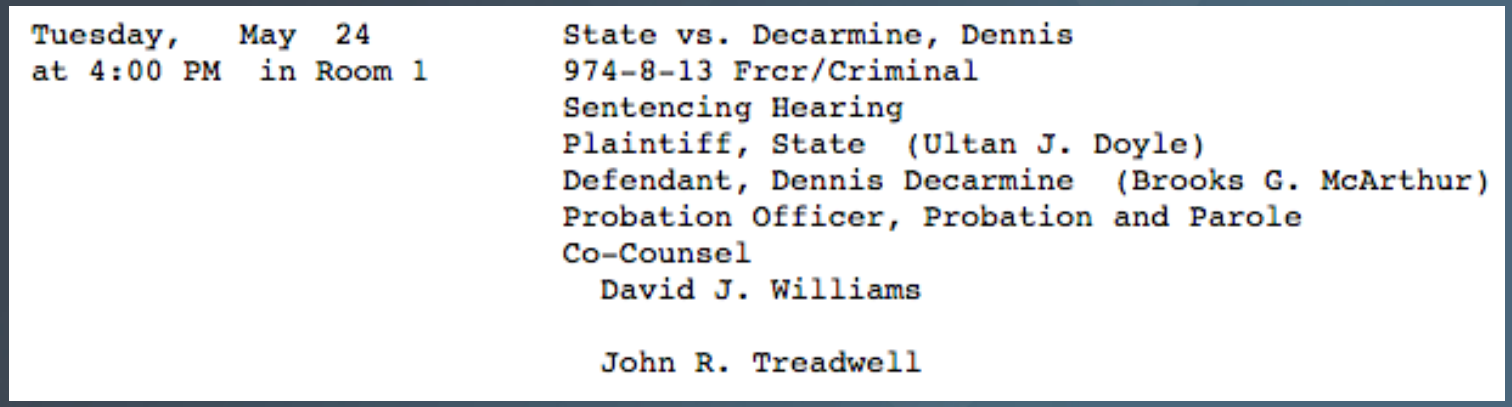
Name	File Created	Last Accessed	Last Written	Entry Modified
proofingEvent81229556[1].htm	03/23/09 05:14:42AM	03/23/09 05:14:42AM	03/23/09 05:14:42AM	04/16/09 06:35:18PM

Tuesday, May 24

1:30PM
2:30PM

The Five Mistakes You Don't Want to Make when Providing Forensic Testimony

James Vaughn, Managing Director, iDiscovery Solutions
Jonathan Rajewski, Director & Digital Forensics Professor, Champlain College
Sheryl Falk, Attorney, Winston Strawn
Christopher Novak, Managing Principal, Verizon
David Cowen, Partner, G-C Partners, LLC / SANS
Suzanne Widup, Senior Analyst, Verizon



Tuesday, May 24
at 4:00 PM in Room 1

State vs. Decarmine, Dennis
974-8-13 Frcr/Criminal
Sentencing Hearing
Plaintiff, State (Ultan J. Doyle)
Defendant, Dennis Decarmine (Brooks G. McArthur)
Probation Officer, Probation and Parole
Co-Counsel
David J. Williams

John R. Treadwell

enfuse 2016

VERMONT

Office of the Attorney General
WILLIAM H. SORRELL

Search here...

Vermont.gov | Home | A to Z Listing | Office Organization | Contact Info

Press Releases

Related News

St. Albans Man Charged with Possession of Child Pornography

Home » Press Releases » St. Albans Man Charged with Possession of Child Pornography

CONTACT: Cindy Maguire, Assistant Attorney General, (802) 828-5512

August 23, 2013

Vermont Attorney General William H. Sorrell announced today that Dennis Decarmine, of St. Albans, Vermont, has been charged with three felony counts and two misdemeanor counts of Possession of Child Pornography. The charges stem from a shared investigation between the Vermont Attorney General's Office, Vermont's Internet Crimes Against Children Task Force, and the St. Albans Police Department. According to documents filed with the court, Mr. Decarmine obtained and distributed child pornography over the internet using publicly available peer-to-peer file sharing programs.

Mr. Decarmine pleaded not guilty today at his arraignment in Franklin Superior Court and he was released on conditions including conditions that limit his access to minors and the internet.

Published: Aug 23, 2013

Mistake #4: Case Example

One of the most important things a forensic examiner/testifying expert should be comfortable with

Case Name	Description
State of Vermont v. Jodie LaClaire	Second Degree Murder Trial

Mistake #5: So you didn't examine the defendant's computer at all?

Timeline | Events

July 2013 – Prosecution Report – Dennis Decarmine's Computer

Registry SOFTWARE Information	
Install Date	3/25/2010 6:56:06 PM +00:00
Product Name	Windows 7 Professional

The remainder of the report provided evidence that supported this system had and distributed child pornography.

Mistake #5: So you didn't examine the defendant's computer at all?

Timeline | Events

September 2014 – Defense Report

June 2014 Computer Forensics Exam

During the week of June 16, 2014, I traveled to Burlington, VT to conduct a computer forensics examination of various computers and hard drives that were retrieved from Mr. Hansen's house.

Upon my arrival at the office of David Williams, Esq., I was presented with three laptop computers and a box containing a variety of hard drives. I set up my computer and forensics software (the X-Ways Forensics suite) and began examining the drives. As I examined each of the hard drives in the laptops and the assorted loose hard drives, I photographed the labels of technical information of each drive. Copies of those photos are available if needed.

Mistake #5: So you didn't examine the defendant's computer at all?

Timeline | Events

September 2014 – Defense Report

Possible Remote Access of Mr. Decarmine's Computer

Mr. Hansen's primary computer was clearly a Dell XPS computer containing two hard drives: a 320 MB Seagate ([redacted]), used primarily for data, and a second 320 MB Seagate ([redacted]), used to store and run the Windows XP operating system.

I examined the contents of the hard drive containing the XP operating system and determined that it contained a file called **mstsc.exe**, which is used to start and run the Microsoft **Remote Desktop Connection**. This program can be used to connect one computer to another at a remote location, and allows the person initiating the connection to run programs and access information on the remote computer. Microsoft provides a brief video describing how the program works on its Web site: http://windows.microsoft.com/en-us/windows7/help/videos/remote-desktop-connection.

Mistake #5: So you didn't examine the defendant's computer at all?

Timeline | Events

September 2014 – Defense Report

Contents of Mr. Hansen's Hard Drives

There are three possible explanations: a) Mr. Hansen in fact only looked at pornography on the Internet when visiting Mr. Decarmine's house; b) Mr. Hansen did in fact use his computer(s) to view pornography on the Internet but was unusually careful and scrupulous in clearing his Internet cache and erasing all traces of his activity; or c) Mr. Hansen used his ability to remotely access Mr. Decarmine's computer to search for pornography, view it, and store it on Mr. Decarmine's computer. Upon information and belief, Mr. Hansen had the requisite computer knowledge to set up the necessary connection, and would have understood that all activity would have occurred on the remote computer and not on his machine.

Mistake #5: So you didn't examine the defendant's computer at all?

Timeline | Events

August 2015 Pre-trial hearing

Defense Expert Verbal Testimony

Q. Now, it's my understanding, based on reading your memorandum, that you don't believe it would be possible to determine whether the defendant's computer ever actually was remotely accessed?

A. Right.

Q. Okay. And is that still your position today?

A. Yes.

Q. Okay. And so, did you ever actually try to determine whether or not the defendant's computer was remotely accessed?

A. No. As I said earlier, I did not take a look at Mr. DeCarmine's computer for this particular software.

Q. And so, are you aware that one of the State's experts, specifically Jonathan Rajewski, thinks that it is possible to check whether or not someone's computer has been remotely accessed?

A. I'm aware of that, yes.

Mistake #5: So you didn't examine the defendant's computer at all?

Timeline | Events

August 2015 Pre-trial hearing

Defense Expert Verbal Testimony

THE COURT: My question wasn't clear. Mr. DeCarmine's computer?

THE WITNESS: No. I did not examine -- I have to double-check to be absolutely sure of this, but I did not examine the image that was prepared from an evidentiary point of view. If I had conducted any examination, it would have been on the forensic image, not the original.

THE COURT: So you examined the image?

THE WITNESS: No, in this particular case, I don't believe -- I'd have to double-check my notes on this. It -- this has been now a couple years. I don't recall whether or not I examined the image of Mr. DeCarmine's computer.

THE COURT: You -- so, you didn't examine the defendant's computer at all?

THE WITNESS: I need to double-check on that, Your Honor, because that I --

THE COURT: Is there something that would refresh your memory about that?

Mistake #5: So you didn't examine the defendant's computer at all?

Timeline | Events

August 2015 Pre-trial hearing

My report

Registry SOFTWARE Information	
Install Date	3/25/2010 6:56:06 PM +00:00
Product Name	Windows 7 Professional

Mr. Decarmine's computer – Remote Desktop logging was enabled

On page 2, paragraph 4, Mr. Lane reports "consumer PCs are not typically equipped with software to record instances of remote access…" Mr. Decarmine's computer was running the Microsoft Windows 7 Operating System, which by default has extensive logging enabled. This logging includes Remote Desktop Connections. I reviewed the Event Logs on Mr. Decarmine's computer and found zero instances of an inbound Remote Desktop Connection. To reiterate, there is no evidence present on the Mr. Decarmine's computer suggesting that a Remote Desktop Connection was established to Mr. Decarmine's computer by any other computer.

Mistake #5 Case Example

Case Name	Description
State of Vermont v. Dennis Decarmine	Possession / Distribution of Child Pornography
#	#
#	#
#	#
#	#

Where to get this deck

Because we finalized it too late to be on the kiosks

This deck is hosted on http://www.encasebook.com under Presentations.

Thank You

From all of us