DIGITAL FORENSICS IN CHILD EXPLOITATION CASES

LARS DANIEL, ENCE, CCO, CCPA, CTNS, CTA, CWA, CIPTS

ENVISTA FORENSICS

ENVISTA FORENSICS

GUARDIAN DIGITAL FORENSICS

Special Issues

- Adam Walsh Child Protection and Safety Act
  - Federal crime to allow child porn to be given to anyone outside of law enforcement for any reason
  - Contains language of re-victimization based on viewing images
    - Civil lawsuits for known victims

The Players

- Internet Crimes Against Children Task Force (ICAC)
  - Over a billion dollars in funding by congress in 2008
  - Tens of thousands of trained law enforcement and prosecutors
    - From the website:
      - ***The Internet Crimes Against Children Task Force Program*** is a national network of 61 coordinated task forces *representing over 3,500 federal, state, and local law enforcement and prosecutorial agencies*. These agencies are continually engaged in proactive and reactive investigations and prosecutions of persons involved in child abuse and exploitation involving the internet

The Players

- Genesis if the agency ICAC examiner
  - Grant money is received by the agency
  - Officer gets a couple weeks of training on computer forensics
  - Focus on peer to peer and solicitation cases
  - Receive forensic software and hardware
  - Required to do child exploitation cases
    - Often do other types of cases as well, but limited experience and training outside of sexual exploitation cases.

The Players

- NCMEC (National Center for Missing and Exploited Children)
  - Maintains a database of known child pornography victims.
  - Can provide statements from victims for trial.
  - NYC Trace-Route Case
    - 3 FBI Agents flown in to testified to knowing the picture series.

How do people get caught?

- Peer to peer investigations
- Child porn found subsequent to other computer forensic examinations
- Reported by someone using their computer
- Reported by third party
  - Computer repair shop
  - Librarian
- Devices seized as part of a sex crime investigation

Law Enforcement Examiners

- Count on not being challenged
  - "it's either there or it's not" what is there to investigate?
  - No motivation to perform full examination
    - Where did it come from?
    - When did it get here?
    - User attribution?
    - intent or accident?

Too Common Scenario

- How it often goes down…
  - Law enforcement locate child porn on device
  - Submit images to prosecutor
  - Charges are files
  - Suspect is arrested
  - Defense attorney reviews images
  - No expert is hired for the defense
  - Defendant takes a plea
- It doesn't have to always be like this:
  - These cases are defensible.

Skeptical?

- Case Example 1:
  - Three charged images

The following files were noted as potential child pornography in the [redacted] forensics report.

Name	File Deleted	File Created	Last Written	Entry Modified	Evidence File	Full Path
169_160x220[1].jpg	Yes	03/09/12 01:42:26PM	03/09/12 01:42:26PM	03/09/12 01:42:26PM	[redacted]	[redacted] D\Lost Files\169_160x220[1].jpg
259_160x220[1].jpg	Yes	03/09/12 01:42:24PM	03/09/12 01:42:25PM	03/09/12 01:42:25PM	[redacted]	[redacted] \D\Lost Files\259_160x220[1].jpg
54320202[1].jpg	Yes	03/09/12 01:40:52PM	03/09/12 01:40:52PM	03/09/12 01:40:52PM	[redacted]	[redacted] D\Lost Files\54320202[1].jpg

Skeptical?

- Case Example 1:
  - Link them to Internet History
    - Basic question: Where are they from?

The following internet history records relate to the three images noted by the [redacted] as potential child pornography:

URL (Website Address)	Last Checked by Local Host Date/Time - (UTC-5:00)	Source
http://www.teeniesland.com/crtr/thumb/169_160x220.jpg	03/09/2012 01:42:26 PM	[redacted] Partition 2 (Microsoft NTFS, 74.45 GB) (Unallocated Clusters)

URL (Website Address)	Last Checked by Local Host Date/Time - (UTC-5:00)	Source
http://www.teeniesland.com/crtr/thumb/259_160x220.jpg	03/09/2012 01:42:25 PM	[redacted] - Partition 2 (Microsoft NTFS, 74.45 GB) (Unallocated Clusters)

URL (Website Address)	Last Accessed Date/Time - (UTC-5:00)	Source
fhgzone.com/tm/forcedtowitness2/*/54320202.jpg	03/09/2012 01:40:52 PM	[redacted] - Partition 2 (Microsoft NTFS, 74.45 GB) (All Files and Folders) - [ROOT]\Documents and Settings\public\PrivacIE\index.dat

Skeptical?

- Case Example 1:
  - Websites registered to Moniker Services LLC

Moniker Online Services LLC

Moniker Online Services LLC prohibits activites related to Child Pornography. The following is from their registration agreement under the section *Prohibited Conduct:*

1. Uploading, posting or otherwise transmitting any content that is unlawful, harmful, threatening, abusive, harassing, tortious, defamatory, slanderous, vulgar, obscene, libelous, invasive of another's privacy, hateful, embarrassing or racially, ethnically or otherwise objectionable;

2. Activities designed to encourage unlawful behavior by others, such as hate crimes, terrorism and child pornography;

The web address from the registration agreement is as follows: http://www.moniker.com/legal/registration-agreement

Skeptical?

- Case Example 1:
  - Conclusion
    - They don't expect to be challenged!

Conclusion

1. No evidence related to the websites of origin for the three images give any indication that the images are child pornography.

2. Upon visual inspection of the images all three appear to be adult pornography images.

Skeptical?

- Case Example 2:
  - Ares alone contraband prove not!
    - Law enforcement claimed that since Ares was installed c that the defendant was downloading child porn
      - Defendant has been in prison for two years when I performed

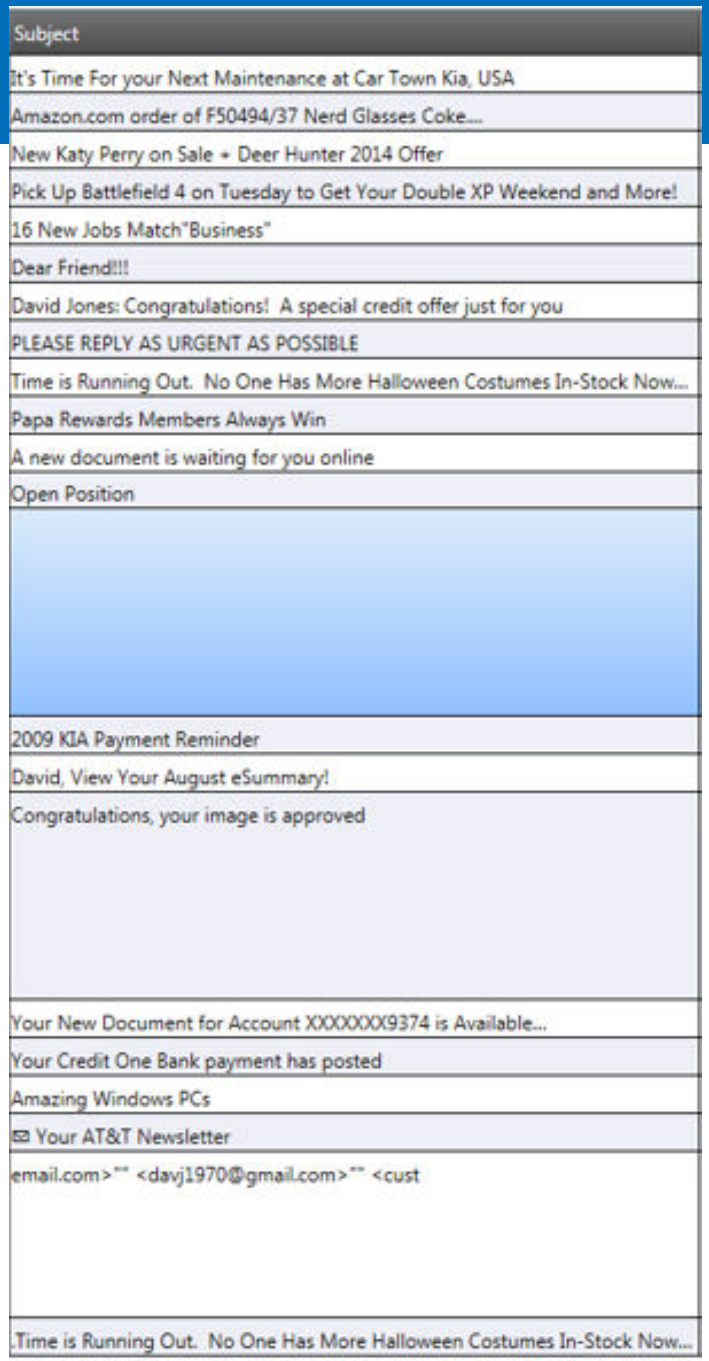
Skeptical?

- Case Example 2:
  - Cell Phone Examination
    - Searches
      - The search terms used by the defendant were examined. No evidence of any search term related to child pornography, child erotica, or any kind of child exploitative content exists on the phone. The searches the user performed are as follows:

Timestamp	Value	Source
10/20/2013 7:52:49 PM...	video chat	Play Market
10/20/2013 7:52:00 PM...	skype	Play Market
10/20/2013 7:46:19 PM...	skype for android	Play Market
10/20/2013 7:43:57 PM...	hangouts	Play Market
10/15/2013 6:06:37 PM...	att radio	Play Market
9/22/2013 11:44:21 PM...	bible king james version	Play Market
9/22/2013 9:57:19 PM(UTC...	algebra 1 in 24 hours	Play Market
9/21/2013 1:59:00 AM(UTC...	Samsung	Play Market
9/18/2013 8:36:15 AM(UTC...	powerball lottery	Play Market
9/12/2013 11:12:20 PM...	craigslist	Play Market
9/11/2013 10:24:19 PM...	ekudirect	Play Market
9/11/2013 10:22:56 PM...	eku	Play Market
8/27/2013 12:49:58 AM...	miley cyrus vma 2013	Youtube Application
8/24/2013 10:42:43 PM...	pop evil	Youtube Application
8/11/2013 11:12:16 PM...	funny video	Youtube Application
8/9/2013 3:53:52 AM(UTC+0)	bobaflex	Youtube Application
8/8/2013 11:56:41 PM(UTC...	devil is a woman charm city devils	Youtube Application
8/8/2013 11:52:29 PM(UTC...	man of constant sorrow	Youtube Application
8/8/2013 11:52:25 PM(UTC...	hail to the king avenged sevenfold	Youtube Application
		Play Market
	g	Play Market

Skeptical?

- Case Example 2:
  - Cell Phone Examination
    - Emails
      - The emails on the phone were examined. No evidence of any email related to child pornography, child erotica, or any kind of child exploitative content exists on the phone. The information concerning the emails on the phone is as follows:



Skeptical?

- Case Example 2:
  - Cell Phone Examination
    - Other Cell Phone Evidence

SMS Messages

522 Short Message Service (SMS) messages, often referred to as text messages, were recovered from the cell phone. All of these messages were examined. No evidence of any text message related to child pornography, child erotica, or any kind of child exploitative content exists in the text messages. These messages are provided in a separate document included with this report due to length.

MMS Messages

19 Multimedia Message Service (MMS) messages were recovered from the phone. All of these messages were examined. No evidence of any multimedia message related to child pornography, child erotica, or any kind of child exploitative content exists in the text messages. These messages are provided in a separate document included with this report.

Web Bookmarks

All of the website bookmarks, or "favorites" were examined on the phone. No evidence of any web bookmark related to child pornography, child erotica, or any kind of child exploitative content exists in the web bookmarks. The web bookmarks are as follows:

Skeptical?

- Case Example 2:
  - Cell Phone Examination
    - Web Bookmarks
      - No contraband

Title	URL	Timestamp
Amazon	http://www.amazon.com/	1/1/2012 12:01:57 AM(UTC+0)
AT&T Mobile Web	http://home.att.com	1/1/2012 12:01:57 AM(UTC+0)
AT&T Wi-Fi Hot Spots	http://attwifi.knowwhere.com/attwifiw/	1/1/2012 12:01:57 AM(UTC+0)
BBC	http://www.bbc.co.uk/	1/1/2012 12:01:57 AM(UTC+0)
Bluegrass Community &...	http://bluegrass.kctcs.edu/	8/18/2013 12:13:00 AM(UTC+0)
CNN	http://www.cnn.com/	1/1/2012 12:01:57 AM(UTC+0)
Credit One	https://m.creditonebank.com/	8/4/2013 9:19:18 PM(UTC+0)
eBay	http://www.ebay.com/	1/1/2012 12:01:57 AM(UTC+0)
ESPN	http://espn.com/	1/1/2012 12:01:57 AM(UTC+0)
Facebook	http://www.facebook.com/	1/1/2012 12:01:57 AM(UTC+0)
Google	http://www.google.com/	1/1/2012 12:01:57 AM(UTC+0)
Home	Page | Eastern Kent	
Home Page | Eastern...	http://www.eku.edu/	8/18/2013 12:13:00 AM(UTC+0)
Jo	bs & Job Search Advice, Employment & Careers |	
Jobs & Job Search Advice,...	http://www.careerbuilder.com/?cbRecursionCnt=1	8/18/2013 12:13:00 AM(UTC+0)
MSN	http://www.msn.com/	1/1/2012 12:01:57 AM(UTC+0)
NY Times	http://www.nytimes.com/	1/1/2012 12:01:57 AM(UTC+0)
Picasa	http://picasaweb.google.com/	1/1/2012 12:01:57 AM(UTC+0)
Twitter	http://twitter.com/	1/1/2012 12:01:57 AM(UTC+0)
Weather Channel	http://www.weather.com/	1/1/2012 12:01:57 AM(UTC+0)
Wikipedia	http://www.wikipedia.org/	1/1/2012 12:01:57 AM(UTC+0)
Yahoo!	http://m.yahoo.com/?tsrc=samsungbm	1/1/2012 12:01:57 AM(UTC+0)
Yahoo!	http://www.yahoo.com/	1/1/2012 12:01:57 AM(UTC+0)
Your Retirement Plan – Wells...	https://www.wellsfargo.com/retirementplan/wrs	8/18/2013 12:13:00 AM(UTC+0)

Skeptical?

- Case Example 2:
  - Cell Phone Examination
    - Web History – no contraband

Last Visited	Title	URL	Visits
10/26/2013 11:30:44 PM(UTC...	AT&T Device Help for the Samsung Galaxy S III	http://simplyinteractiveguides.com/att_mobile/?pa=70726f6a656374	16
10/26/2013 11:30:43 PM(UTC...	Messages	https://m.facebook.com/messages/?folder=other&_rdr	12
10/24/2013 10:04:47 PM(UTC...	Messages	https://m.facebook.com/messages/?folder=other&refsrc=http%3A%2F%2Fm.facebook.com%...	2
10/24/2013 10:04:30 PM(UTC...	Welcome to Facebook	https://m.facebook.com/login.php?next=http%3A%2F%2Fm.facebook.com%2Fmessages%2F%...	2
10/24/2013 10:04:08 PM(UTC...	Welcome to Facebook	https://m.facebook.com/login.php?next=http%3A%2F%2Fm.facebook.com%2Fmessages%2F%...	4
10/24/2013 4:16:24 PM(UTC+0)	Police and Detectives : Occupational Outlook Handbook : U.S. Bureau of Labor Statistics	http://www.bls.gov/ooh/Protective-Service/Police-and-detectives.htm	1
10/23/2013 9:33:29 AM(UTC+0)	http://adtrack.king.com/modules/adTracking/adClicked.jsp?...	http://adtrack.king.com/modules/adTracking/adClicked.jsp?...	2
10/22/2013 10:30:35 PM(UTC...	Winchester, KY 40391 Tomorrow's Weather Forecast - AccuWeather.com	http://m.accuweather.com/en/us/winchester-ky/40391/daily-weather-forecast/333329?...	10
10/20/2013 8:41:06 PM(UTC+0)	Winchester, KY 40391 Daily Weather Forecast - AccuWeather.com	http://m.accuweather.com/en/us/winchester-ky/40391/daily-weather-forecast/333329?...	2
10/20/2013 8:40:49 PM(UTC+0)	Winchester, KY 40391 Daily Weather Forecast - AccuWeather.com	http://m.accuweather.com/en/us/winchester-ky/40391/daily-weather-forecast/333329?...	2
10/18/2013 11:15:03 PM(UTC...	http://www.accuweather.com/m/details2.aspx?p=samand&lang=en-us&loc=cityId%3A333329	http://www.accuweather.com/m/details2.aspx?p=samand&lang=en-us&loc=cityId%3A333329	1
10/18/2013 11:14:57 PM(UTC...	Winchester, KY 40391 Tomorrow Afternoon's Weather Forecast - AccuWeather.com	http://m.accuweather.com/en/us/winchester-ky/40391/afternoon-weather-forecast/333329?day=2	1
10/18/2013 12:03:16 PM(UTC...	Kroger - Win An XBOX ONE	http://kroger.softcoin.com/programs/kroger/oneaday/?...	2
10/16/2013 8:15:24 AM(UTC+0)	http://m.facebook.com/l.php?u=http%3A%2F%2Fwakeupcallnews.blogspot.com%2F2013%...	http://m.facebook.com/l.php?u=http%3A%2F%2Fwakeupcallnews.blogspot.com%2F2013%2F10%...	1
9/2/2013 6:17:41 PM(UTC+0)	http://m.accuwe□2□< □□□KWinchester, KY 40391 Tomorrow's Weather Forecast -...	http://m.accuweather.com/en/us/winchester-ky/40391/daily-weather-forecast/333329?...	2
9/2/2013 6:17:41 PM(UTC+0)	Winchester, KY 40391 Tomorrow's Weather Forecast - AccuWeather.com	http://m.accuweather.com/en/us/winchester-ky/40391/daily-weather-forecast/333329?...	2
	http://www.thecastlejewelry.com/Women-s-Rings-s/273.htm	http://www.thecastlejewelry.co□□□□ □□K□Khttp://m.ac	1
	http://m.accuwe□2□< □□□KWi	nchester, KY 40391 Tomorrow's Weather Forecast - AccuWeather.comhttp://m.accuweather.com/...	115
	Wi	nchester, KY 40391 Tomorrow's Weather Forecast - AccuWeather.comhttp://m.accuweather.com/...	115
	http://login.microsoftonline.com/logout.srf?ct=□□□ □□□https://m.facebook.com/...	folder%3Dother&refsrc=http%3A%2F%2Fm.facebook.com%2Fmessages%...	117
	http://login.mi	crosoftonline.com/logout.srf?ct=□□□ □□□https://m.facebook.com/login.php?next=http%3A%...	61
	https:	//m.facebook.com/login.php?next=http%3A%2F%2Fm.facebook.com%2Fmessages%2F%3Ffolder...	0

Skeptical?

- Case Example 2:
  - Cell Phone Examination
    - Videos
      - Also no contraband

Name	Created	Modified	Accessed	Path	Size
AndroidInSpace.240p.mp4	6/28/1970 10:45:39 PM(UTC+0)	8/1/2008 12:00:00 PM(UTC+0)	8/1/2008 12:00:00 PM(UTC+0)	/Root/media/video/AndroidInSpace.240p.mp4	193567
AndroidInSpace.480p.mp4	6/28/1970 10:45:39 PM(UTC+0)	8/1/2008 12:00:00 PM(UTC+0)	8/1/2008 12:00:00 PM(UTC+0)	/Root/media/video/AndroidInSpace.480p.mp4	1506932
arrow.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	38814
arrow_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	45647
car.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	157691
car-circle.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	2095
classic.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	77425
classic_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	69442
convertable.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	84228
convertable_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	72667
LOGO.mp4	5/1/2013 10:41:46 PM(UTC+0)	5/1/2013 10:41:46 PM(UTC+0)	5/1/2013 10:41:46 PM(UTC+0)	/Root/media/gameloft/games/GloftUFHM/...	397368
miniVan.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	79168
miniVan_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	99301
monsterTruck.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	77876
monsterTruck_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	96633
motorCycle.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	80464
motorCycle_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	74939
muscleCar.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	74802
muscleCar_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	93756
oldSchool.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	81115
oldSchool_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	71221
smallCar.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	79057
smallCar_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	98395
spaceShip.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	74243
spaceShip_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	99299
sportsCar.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	78810
sportsCar_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	98512
Sunset.240p.mp4	6/28/1970 10:45:39 PM(UTC+0)	8/1/2008 12:00:00 PM(UTC+0)	8/1/2008 12:00:00 PM(UTC+0)	/Root/media/video/Sunset.240p.mp4	388748
Sunset.480p.mp4	6/28/1970 10:45:39 PM(UTC+0)	8/1/2008 12:00:00 PM(UTC+0)	8/1/2008 12:00:00 PM(UTC+0)	/Root/media/video/Sunset.480p.mp4	1598754
SUV.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	78506
SUV_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	68661
tank.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	83245
tank_grey.mod	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	10/12/2013 8:13:37 AM(UTC+0)	/Root/data/...	70879
triangle.mod	10/12/2013 8:13:38 AM(UTC+0)	10/12/2013 8:13:38 AM(UTC+0)	10/12/2013 8:13:38 AM(UTC+0)	/Root/data/...	263195
triangle_gray.mod	10/12/2013 8:13:38 AM(UTC+0)	10/12/2013 8:13:38 AM(UTC+0)	10/12/2013 8:13:38 AM(UTC+0)	/Root/data/...	4984

Skeptical?

- Case Example 2:
  - Conclusion

1. No evidence of any kind of movie, image, or any other type of media containing child pornography, child erotica, or other child exploitative content exists on the defendant's cell phone.

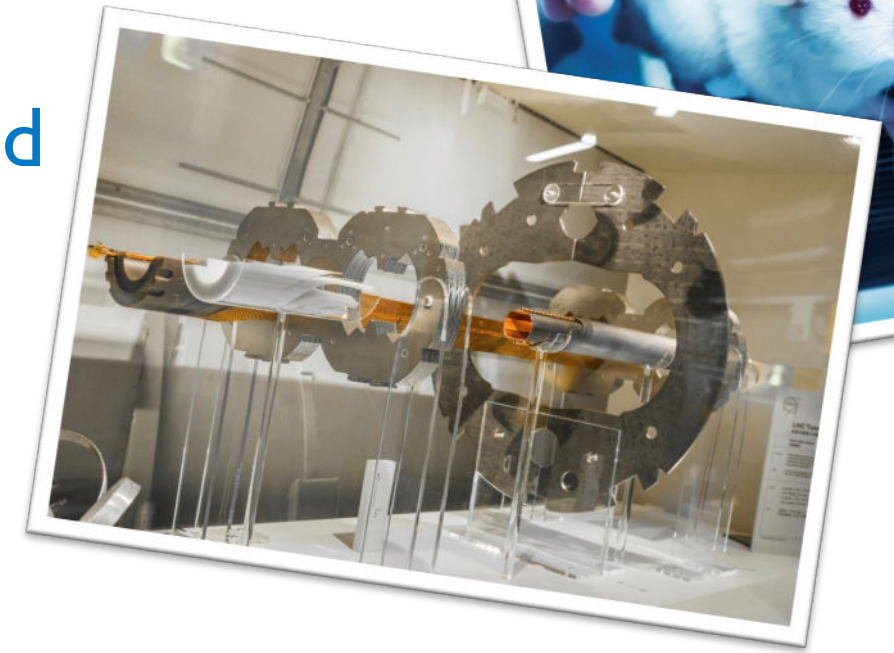
2. No evidence of any kind of movie, image, or any other type of media containing child pornography, child erotica, or other child exploitative content exists on the defendant's computer.

3. No evidence has been located in my examination, or in the law enforcement examination, showing that any of the defendant's devices were used to share the child pornography video downloaded by [redacted].

4. No evidence was located in my examination, and according the discovery documents that have been provided to me, no evidence was found in the law enforcement examination showing that the defendant ever used a peer to peer file sharing program such as Ares, ever accessed, possessed, or shared child pornography, or engaged in any illegal activity whatsoever related to child pornography, child erotica, or child exploitative content.

Why Use an Expert?

- Verify opposing experts work
  - We have seen examples of this already
- Sentencing mitigation
  - Compound files
    - Image reduction
  - Searches
- Get the charges reduced
  - Distribution?



Sentencing Mitigation Example

- Images by Category
  - Defendant charged with "enhanced" images

Category	Statistics	Number of Images
1	Child Pornography - Sadism and Masochism	864
2	Child Pornography - Under 12 Years of Age	16,069
3	Child Pornography - Over 12 Years of Age	16,666
4	Child Erotica	370,433
5	Child (Not Pornographic, Non-Sexual)	216
6	Adult Pornography	77,062
7	Obscenity	139
9	NCMEC Identified	3,121
10	ProjectVIC	51,826

Sentencing Mitigation Example

- Images by Category
  - Searches don't fit enhanced charges
    - Consistent with defendant statements

Search Keyword				
11y	daniela	magazine fashion	ptsc	torrent
11y	daniela	marinat	S00	torrent model
12y	darkology	mfg	S00	torrent pt
12y	dmetry	mirna	showstar	trixie
15y	emulecollection	model	showstar	trixie
15y	evelyn	model alice	showstars	trixie model
agency model	evelyn	model gabe	showstars	ttl
agency models	eyecan	modelring	SILVIYA	ttlmodel
all pics	flo	modsl alice	site	ttlmodels
angelripper	flo busty	multi model	smile model	underage
bella model	gabe	multi model	smile model	unearthly
bella model	gingrrsnaps	nerea	SOO	unearthly
btm	gtm	nerea	SOO	vladmodels
cam girls	gtm	organ	special set	w001
camfrog	hussyfan	organ	stef	w01
camfrog girl	jamie	patti model	stef	webcam
camfrog girls	jamie model	patti model	stickam	webcam cuties
cammslave	kidz	patty	stickam girls	webcam kid
candydoll	kiki	perfectflex	sweet kitty	xam
candydoll vip	kiki	pipe organ	sweet lil	xam
candydoll anjelika	kitty	pipe organ	sweet mixed girls	xara
candydoll laura	lena model	playtoy	syuzanna	xara
candydoll laura vip	lollipop	playtoy	teens agency	y001
candydoll maya	lollipop	polska	teens agency	y01
candydoll.tv	lolmag	prmodels	teensagency	y107
charming models	ls models	prmodels	teensagency	young horny
charming models	m001	ptsc	tinymodel	young horny kidz

Reduction in Charges

- Distribution
  - *KNOWING* Distribution? - MT Frostwire Case

Narrative

The following excerpts are from the [redacted] interview dated July 10, 2013 (Case No. [redacted])

On Page 313, Agent [redacted] and the defendant say the following:

> GS: On a scale of one (1) to ten (10), one (1) being very low and ten (10) being very high how would you rate yourself as a computer user?
>
> EH: In the winter more often, and in the summer very rarely,

This is a common question asked in the interview of suspects by law enforcement agents. It is clear from the defendant's response that he did not accurately understand the question, as it relates not to the amount of computer usage during a particular season, but instead to the capability and knowledge of a person related to computers on a scale of one to ten.

Reduction in Charges

- Distribution
  - *KNOWING* Distribution? - MT Frostwire Case

Further on page 313, the following is said:

GS: Oh okay. Um, so do you know how to save files?

Eh: Not…

GS: On a computer?

EH: Really just on my desktop.

GS: Do you know how to create a folder and put stuff into it?

EH: As in…

GH: Like just create a little folder and name it somethin' and then put files into it, do you do anything like that?

EH: That's, I, that I don't know much about.

Why use an Expert?

- Get the charges dismissed
  - Alabama – Barlow Case

Why use an Expert?

- Get the charges dismissed
  - NC v Jones

Expert Testimony

- Boston Case
  - Possession, Distribution, Receipt of Child Porn
    - Yahoo Messenger Chat
      - Roleplay is real.
    - Adult vs. Child Porn
      - Amount and source matter.

Expert Testimony

- Boston Case
  - Tens of thousands of adult porn files and only a few child porn files.
    - In this case, search terms unrecoverable

Like "*sex*" Or Like "*porn*" Or Like "*pussy*" Or Like "*suck*" Or Like "*hor*" Or Like "*dick*" Or Like "*nude*" Or Like "*tranny*" Or Like "*shemale*" Or Like "*ass*" Or Like "*rape*" Or Like "*fuck*" Or Like "*teen*" Or Like "*lesb*" Or Like "*cock*" Or Like "*anal*" Or Like "*incest*" Or Like "*cum*" Or Like "*girl*" Or Like "*tit*" Or Like "*BDSM*"

The following are the 10 files that were not located using the adult search terms:

From the Saved Folder

Number	Limewire Saved_File Exam For Content.Name
1	Jerry Springer - uncut.avi
2	We Live Together - Lexi (full).mpg
3	Pedo (Pthc) - Little 6yo and dad (Hussyfan) (r@ygold) (babyshivid) - sound, heavy crackling.mpg
4	Jerry Springer Too Hot For Tv 5.mpg
5	Jerry Springer - I Refuse To Wear Clothes 5.mpg
6	eva mendas.mp3
7	Da Ali G Show - Borat Tries To Buy A Slave.mpg

Expert Testimony

- Boston Case
  - Tens of thousands of adult porn files and only a few child porn files.
    - Law enforcement later determined all chat partners were adult

Further, a screenname such as "judy12_needdaddy" (File 1 in "IM's Of Interest from [redacted] report) no more informs someone that Judy is 12 years old than "cute_molly81" informs someone that cute_molly is 81 years old. Numbers in a screenname can mean something, or they can be entirely meaningless. Even if the numbers do have some sort of meaning, it does not necessarily mean that another person would know the significance behind the numbers.

Due to the anonymity of the internet, it is common knowledge in the forensics community that chat rooms, and in particular sexually oriented chat rooms, are commonly used by persons for the purpose of roleplay. This roleplaying can come in the form of various sexual fetishes, and given Yahoo's policies concerning the age restriction of 18 years or older to access Yahoo Messenger chat services, someone claiming to be underage could be determined to be of age and roleplaying by a user of Yahoo Messenger when chatting with that person.

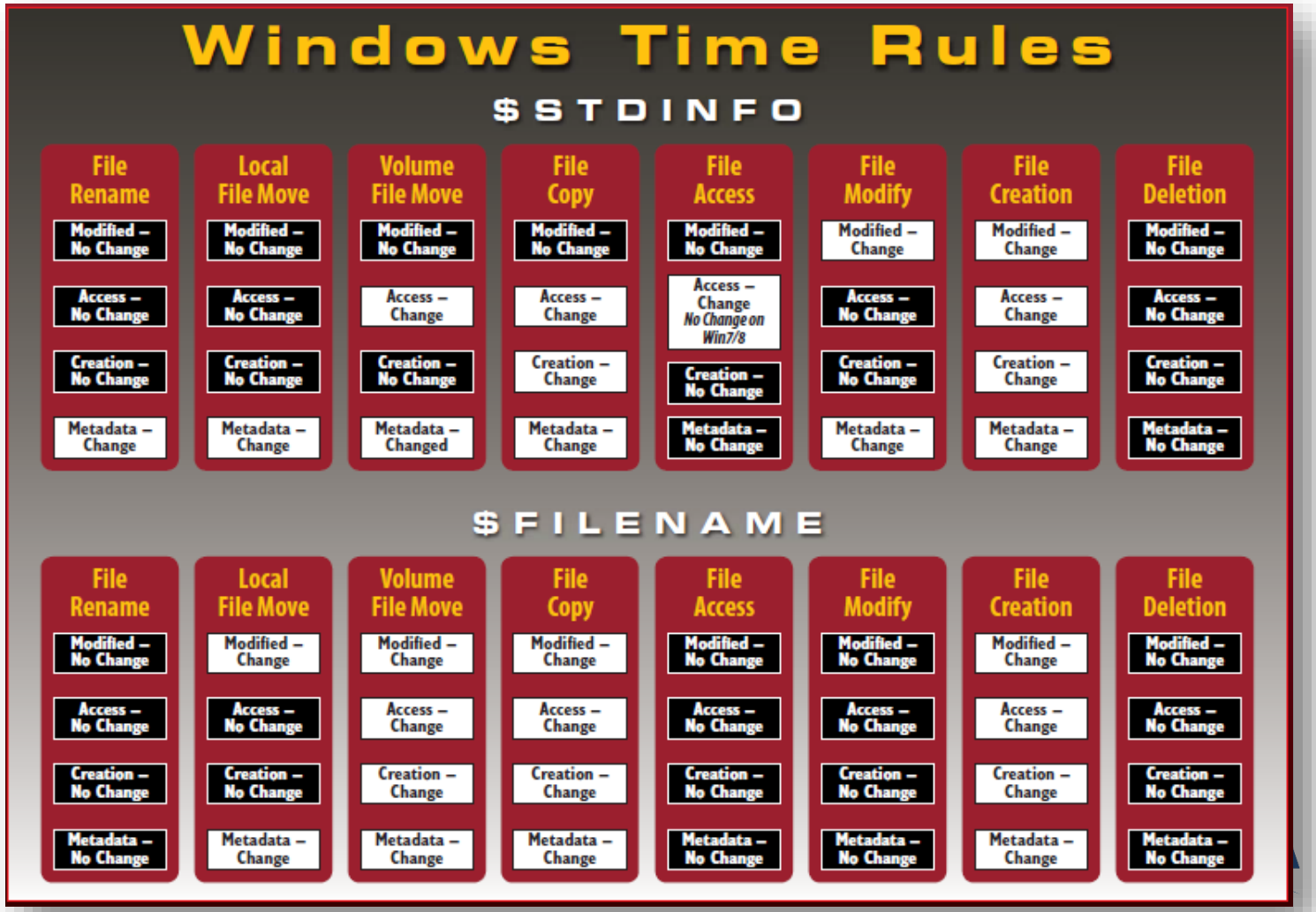
Expert Testimony

- Boston Case
  - Download times match chat records?
    - Affidavit about computer times
    - Law enforcement examiner could not testify as expert

Expert Testimony

- Fact Witness vs. Expert Witness
  - Affidavit about computer times
  - Law enforcement examiner could not testify as expert

- SANS Forensics Windows Forensic Analysis Poster, www.sans.org



Expert Testimony

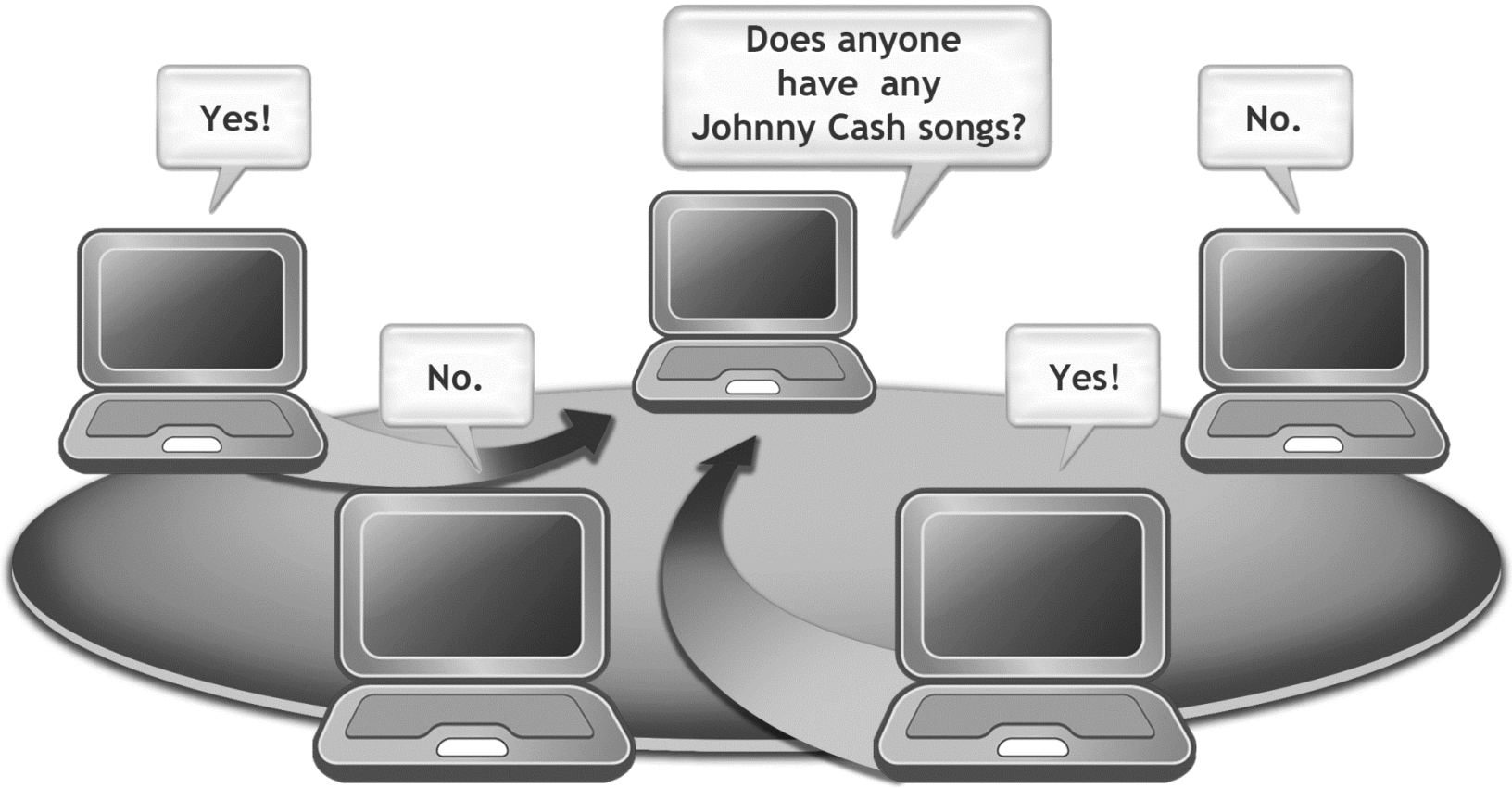
- Boston Case
  - Download times match chat records?
    - Affidavit about computer times
    - Law enforcement examiner could not testify as expert

18. The basis for Detective [redacted] "looking at times that the videos were created and looking at other items that occurred around that time" is also based upon a basic misunderstanding of the computer file system and how the peer to peer file sharing software Limewire works. The created date of the video file *does not* relate to user activity. The created date of the video file would indicate the time the file *finished* downloading. The date the file finishes downloading can be hours or even days after any actual user activity took place. This renders the examination of Limewire video created dates to "other items that occurred around that time" nonsensical.

Peer to Peer Investigations

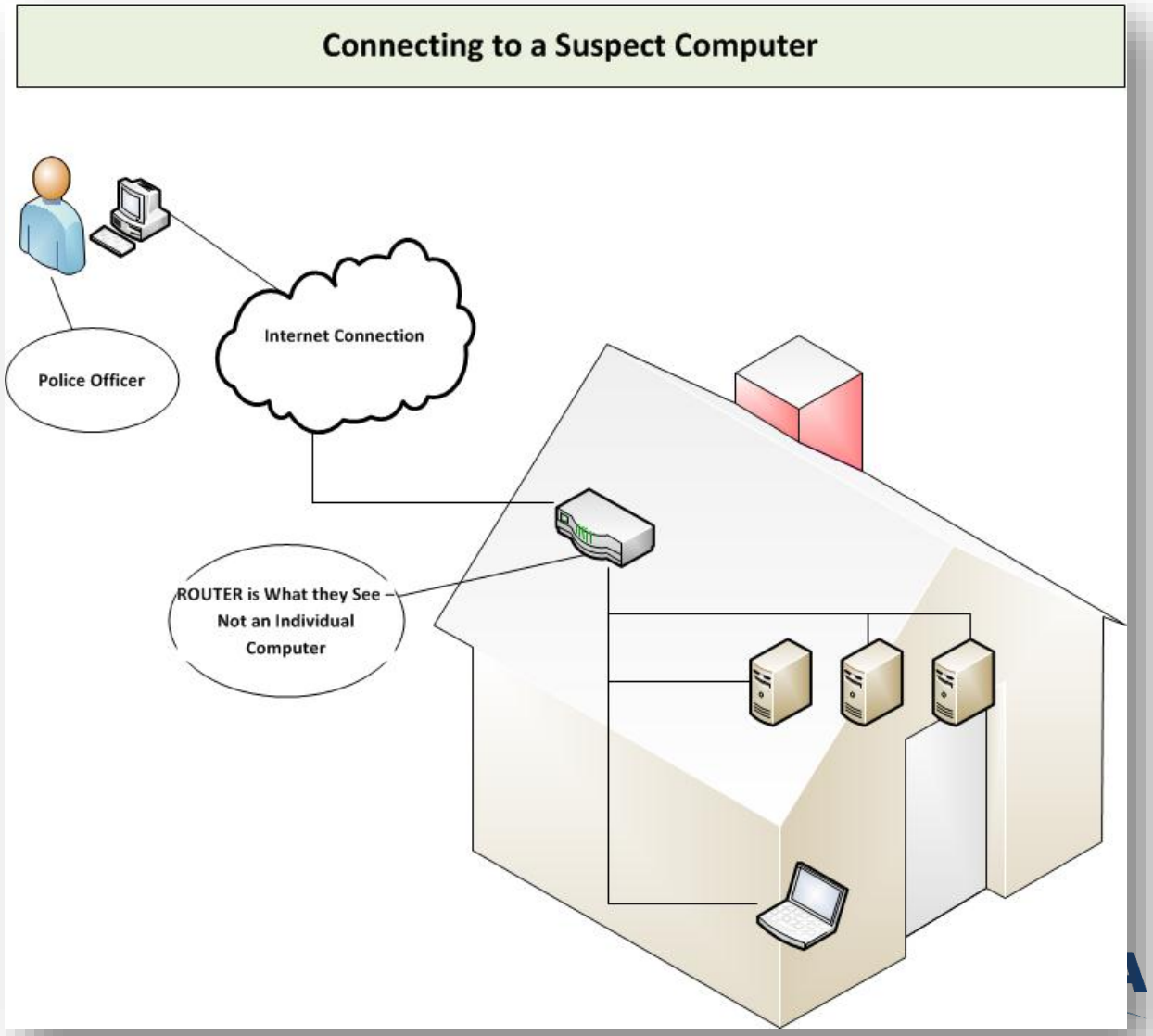
- How They Work
  - Special law enforcement only software
    - Peer Spectre, GNUWatch, etc.
  - Can "see" child porn being transferred via peer to peer networks
  - Can see IP of ***router*** sharing or downloading
  - Direct connect to suspect computer on the network
  - WHOIS lookup to see where IP is located
  - Subpoena the ISP for Subscriber info
  - Captures list of files being shared or downloaded
  - Progress to a warrant from there

Peer to Peer Investigations



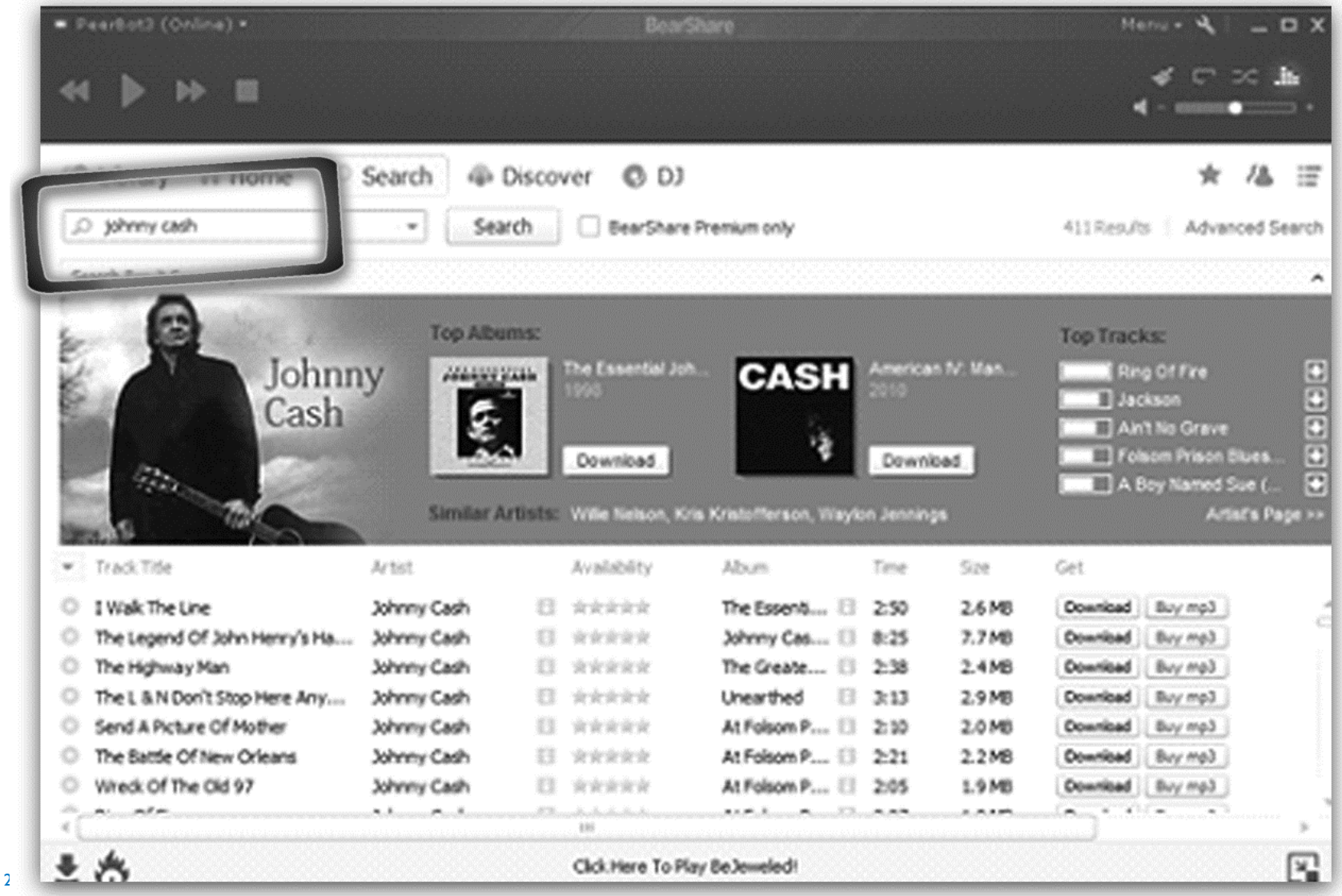
Peer to Peer Investigations

- Cannot see behind router!



Peer to Peer Investigations

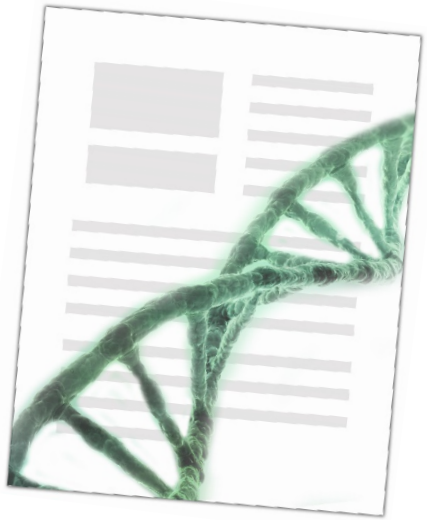
- Search box



Peer to Peer Investigations

- Search Returns
  - SHA1

File	Sharing Host	SHA1
Copy of Johnny Cash - The Devil Came Back To	213.58.202.86:22881	YK32F75GKWIXT6M7XNJ7HGBZAUTNU5OI
Dick Dale & His Del-Tones - Ring of Fire [Johnn	79.42.130.89:6346	2NVZULSRGOOCPSHIXDUICSKF6SR3TJSJ
George Jones & Johnny Cash & Willie Nelson -	173.72.181.134:15102	OKZHPFIRUGQFYEQFZE4WJWMUYQJMJGPU
Jason Aldean - Johnny cash.mp3	64.239.218.155:40305	RJAM57ML7RHKJUPAYAKXGKQADZLV6ELD



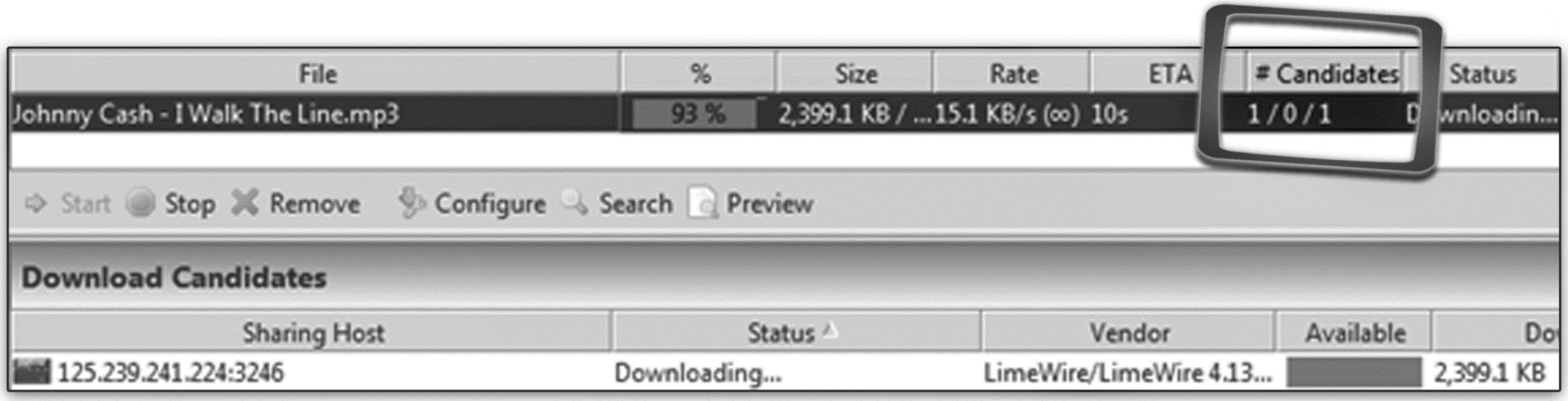
Peer to Peer Investigations

- Direct Connect

File	SHA1	Sharing Host
Jonas Brothers - Tonight.mp3	WWIIPFJ574A2NKDBXXE7LH6D3TXNJDY4	125.239.241.2
Jonas Brothers - Paranoid.mp3	O2EH5PGE2DHO4AMPK33EF3UAKEEPAOSY	125.239.241.2
Jonas Brothers - Burning Up .mp4	27NNINZTJG5EVD7L64LRGXUOOBSCVKBH	125.239.241.2
Jon Lajoie - Show Me Your genita	36JTILMPPPLT7AH7O4N2OCD4YPOCNRJY	125.239.241.2
Jon Lajoie - Show Me Your Genita	OP3QYEYJXMRMLBIWSCWPUYSZRHBK7SJ5	125.239.241.2
Johnny Cash - I Walk The Line.mp	ULKZTRCAISYEOLGZFAEMEUFIZMDAQXBP	125.239.241.2

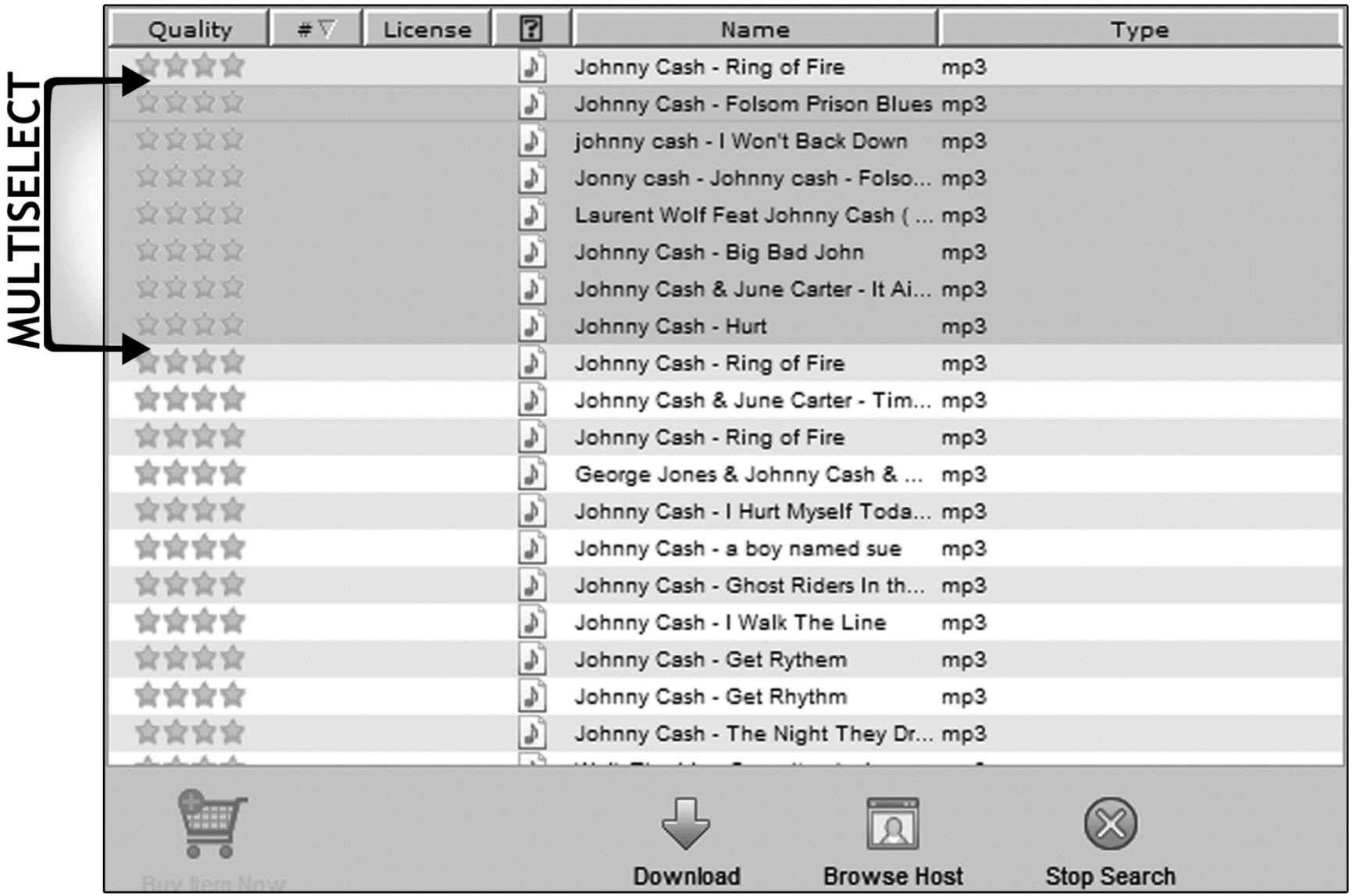
Peer to Peer Investigations

- Single source download



Peer to Peer Investigations

- Multiselect



Why use an Expert?

- Assist client with understanding the merits of their case, or lack thereof.
  - Sometimes the best option is to have a conference call or sit down meeting with the attorney and client.
  - Sometimes the defendant has significantly more technical experience than their attorney
  - They need to know the case government is going to bring
  - The cat didn't do it.

The Questions

- General Categories
  - What is present?
  - Where is it?
  - When did it get there?
  - How did it get there?
  - Who put it there?

Case Example: Questionable Downloads

- Microsoft Flight Simulator…for free?

ENVISTA FORENSICS

Case Example: Virus?

- A virus did it….once.

The Questions

- General Categories
  - What is present?
    - Pictures
      - Thumbnails
      - Full size
    - Movies
      - CP embedded in middle
      - Movies complete or incomplete
      - User have software to open the movie

The Questions

- General Categories
  - Where is it?
    - Logical, "deleted", or unallocated space
    - In a database
    - Compound file
    - Is it on external devices
      - External drives
      - Thumb drives
      - DVDs, CDs Media Players
      - Cloud storage
      - Email accounts

Case Example: The Collector

- Complete and archive.

The Questions

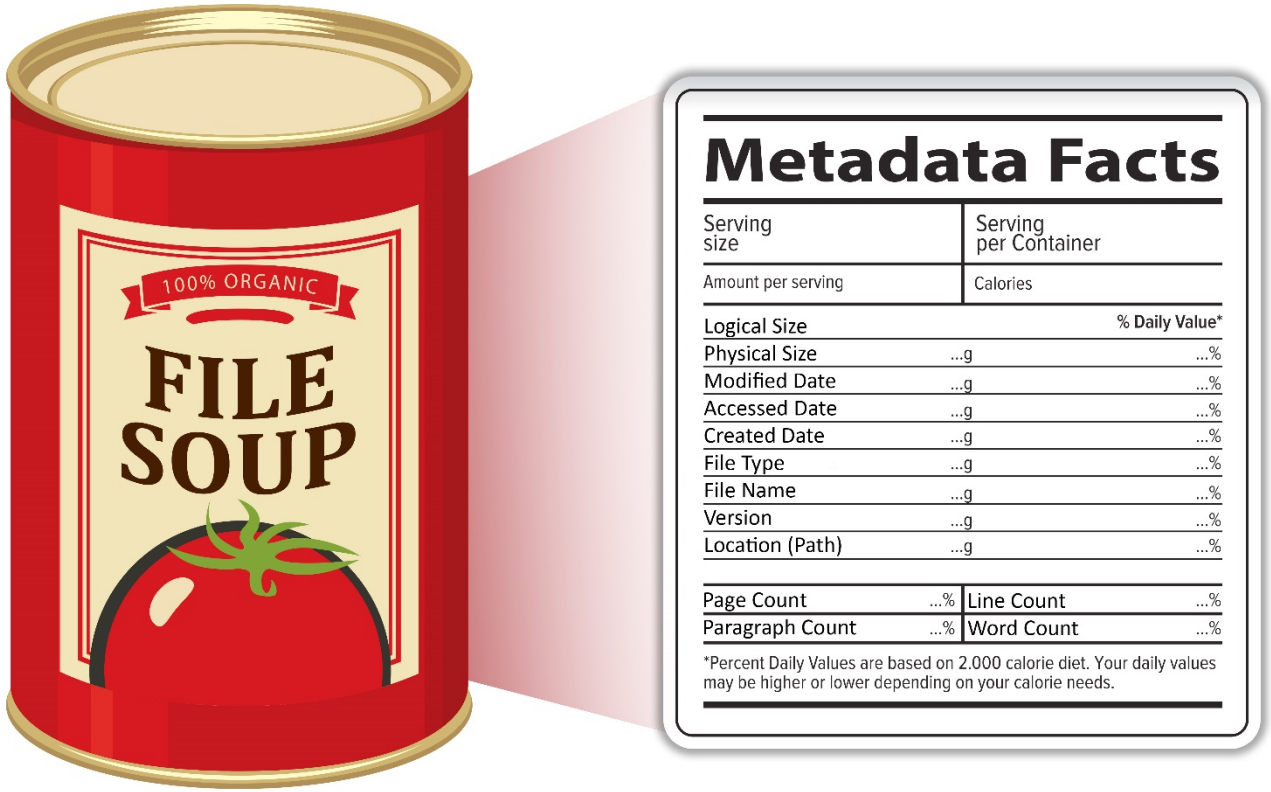
- General Categories
  - When was it put there?
    - Defendant at work
    - Others have access to the device
    - How many "locked doors"
      - Physical locks
      - Passwords

The Questions

- General Categories
  - How did it get there?
    - Downloaded and in the internet cache only
    - Via a file sharing program
    - Shared via a chat room or message board
    - Inside of a text message or email
    - Copied to the computer from an external device

Case Example: Cell Phone Picture

- Photo Editing and Metadata



Metadata Facts

Serving size	Serving per Container
Amount per serving	Calories

		% Daily Value*
Logical Size		
Physical Size	...g	...%
Modified Date	...g	...%
Accessed Date	...g	...%
Created Date	...g	...%
File Type	...g	...%
File Name	...g	...%
Version	...g	...%
Location (Path)	...g	...%

Page Count	...%	Line Count	...%
Paragraph Count	...%	Word Count	...%

*Percent Daily Values are based on 2,000 calorie diet. Your daily values may be higher or lower depending on your calorie needs.

The Questions

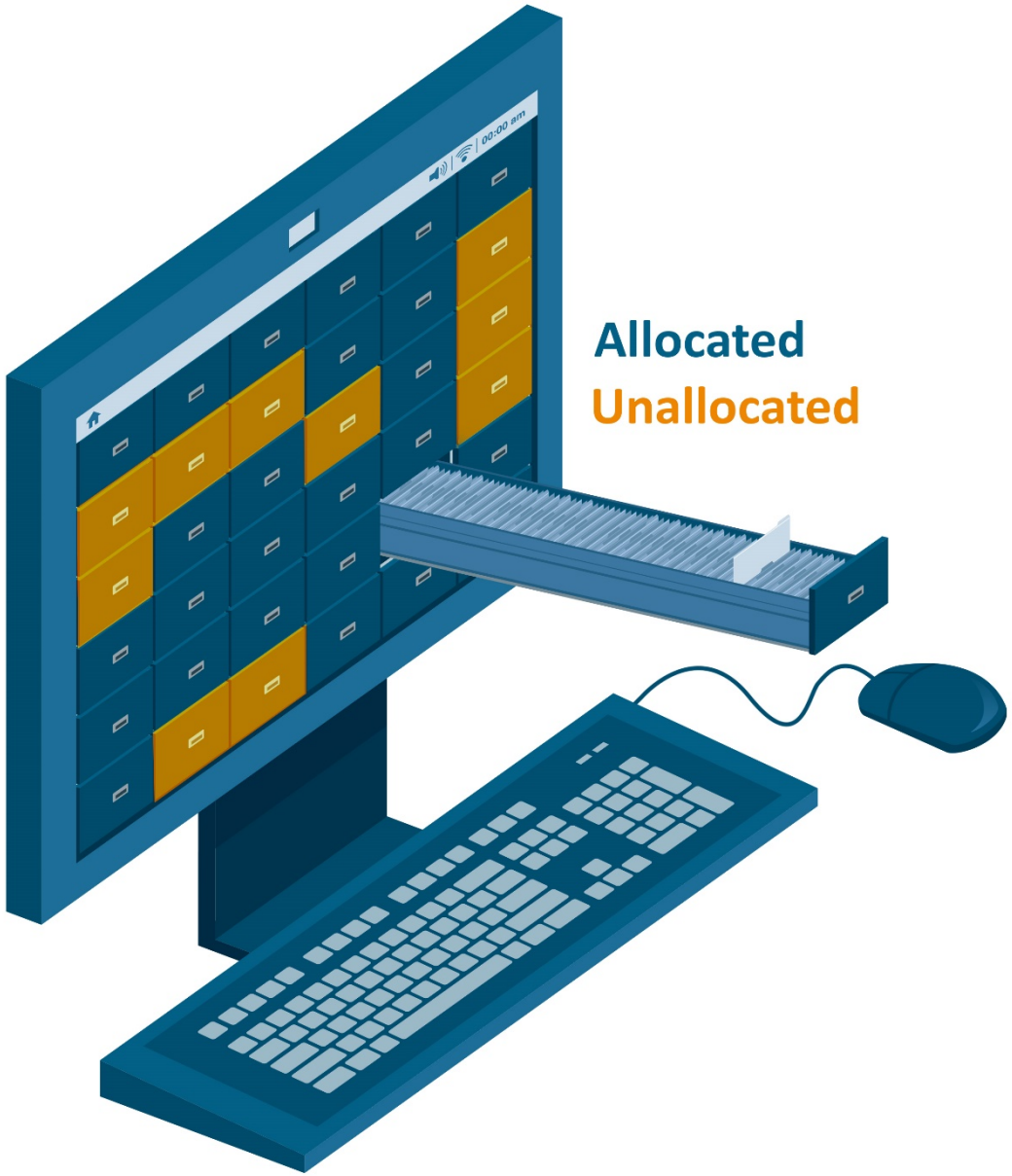
- General Categories
  - Who put it there?
    - Who owns the computer
    - What profile is it stored under
    - Secure activity around download times
      - Social media activity and logins
      - Bank and financial activity and logins
    - Others have access to the defendant's accounts
    - Anyone ever see the defendant viewing or downloading child porn

Other Issues

- Browser Caching
  - US v Kuchinski 469 F. 3d 853 (9th Cir. 2006)
    - Where a defendant lacks knowledge about the cache files, and concomitantly lacks access to and control over those files, it is not proper to charge him with possession and control of the child pornography images located in those files, without some other indication of dominion and control over the images.
    - To do so turns abysmal ignorance into knowledge

Other Issues

- Unallocated Space
  - US v Flyer (February 2011)
    - Users have no method for accessing files in unallocated space.
    - But deletion of an image alone does not support a conviction for knowing possession of child pornography on or about a certain date within the meaning of § 2252(a)(4)(B) (2004). No evidence indicated that on or about April 13, 2004, Flyer could recover or view any of the charged images in unallocated space or that he even knew of their presence there. Accordingly, the district court committed plain error, and we reverse Flyer's conviction on Count Three



Case Examples

- Challenging the Evidence
  - Signed, sealed, delivered.
    - Technology argument
      - Intent to possess contraband?

Case Examples

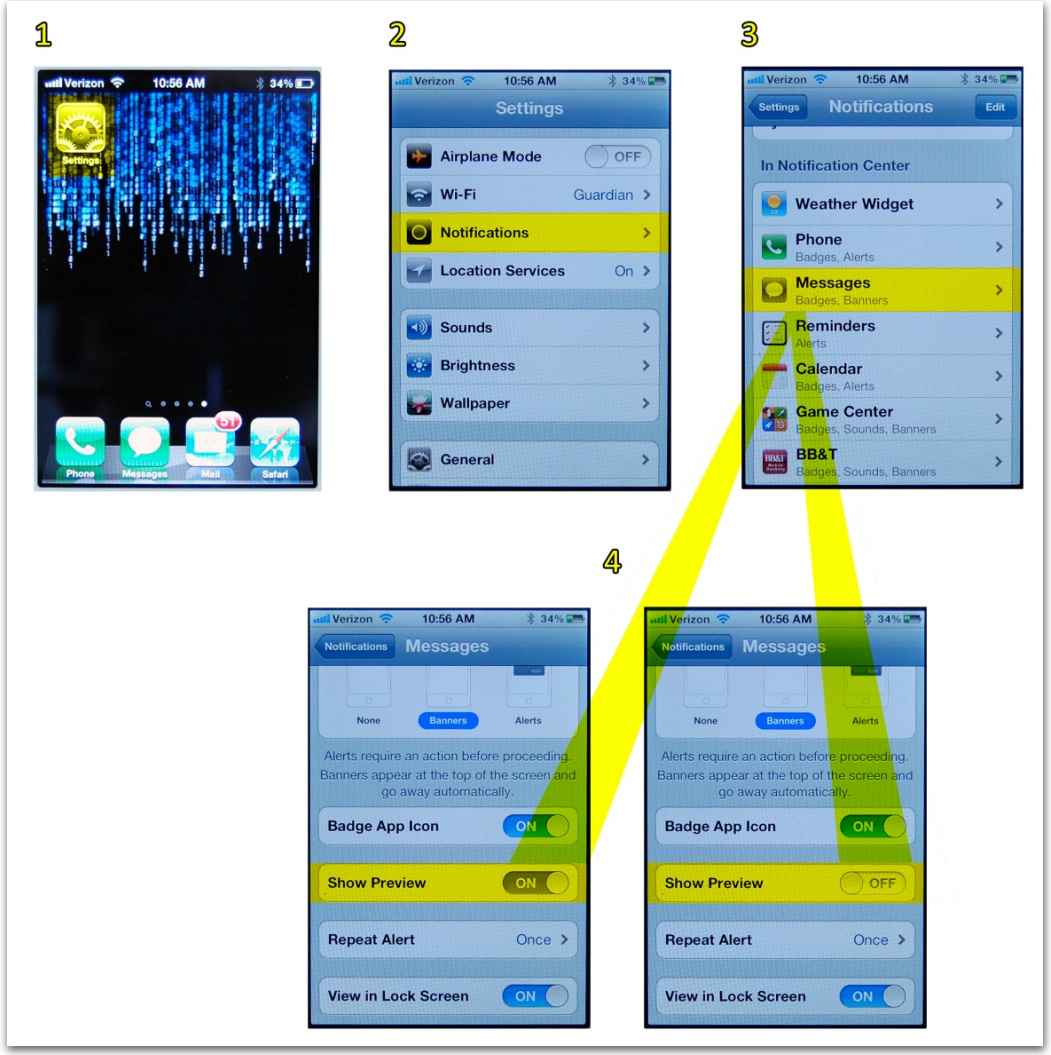
- Challenging the Evidence
  - Signed, sealed, delivered.
    - When receiving a MMS or SMS message on an iPhone, the recipient of the message cannot determine the contents of the message until it has already been received and viewed. Further, with a SMS or MMS message, the user does not have the ability to prevent the reception of the message.

    - If a person sends a SMS or MMS message to someone else, that message is automatically delivered to the other person ***regardless of their consent*** or intent to receive that message.

    - The delivery and receiving of MMS and SMS messages is an ***automated*** process carried out by cellular service providers and cell phone hardware that does not allow for a user to determine what SMS or MMS messages they receive. The only way to determine what the contents of SMS and MMS message are is to view the message. This description of the sending and receiving of MMS and SMS text messages is not isolated only to iPhones, but is the normal operation of almost all cellular phones.

Case Examples

- Challenging the Evidence
  - Signed, sealed, delivered.
    - Preview on, or off.



Case Examples

- Challenging the Evidence
  - Signed, sealed, delivered.
    - Preview on, or off.

Case Examples

- Challenging the Evidence
  - Signed, sealed, delivered.
    - When an MMS message containing a picture is received on an iPhone, ***it will only exist within the SMS folder of the file system on iPhone***. The picture is ***automatically saved*** there upon receipt of the message without any input or preservation steps taken by the user. An image existing within the SMS folder of an iPhone file system will have file path that is consistent with the following example:

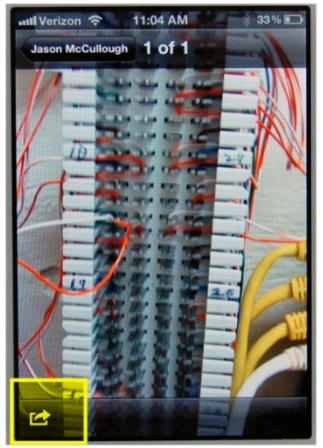
- **Library/SMS/Parts/35/05/55555-5.jpg**

Case Examples

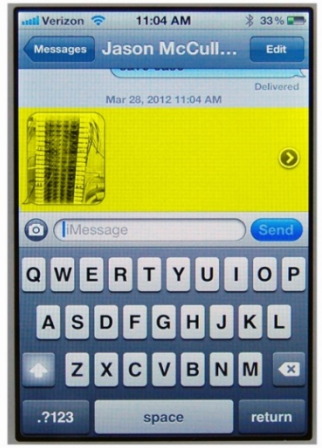
- Challenging the Evidence
  - Signed, sealed, delivered.
    - For a user to intentionally preserve that image, it has to be saved to the *Photos* application on the iPhone by selecting the image, then viewing it in full screen mode, selecting the *Share* icon, and then selecting *Save Image* option in the pop-up dialogue box.

1

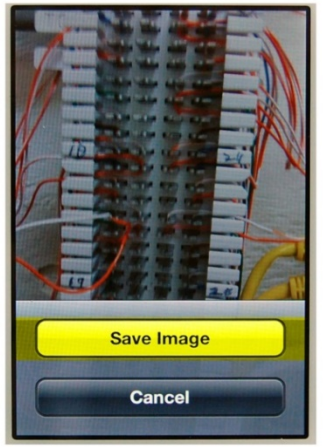
2



3



4

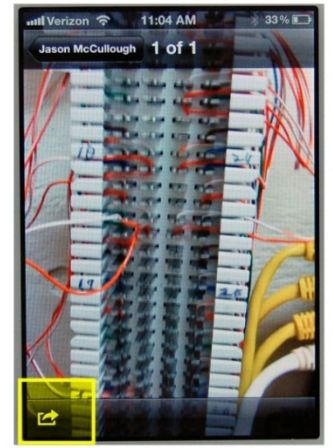


Case Examples

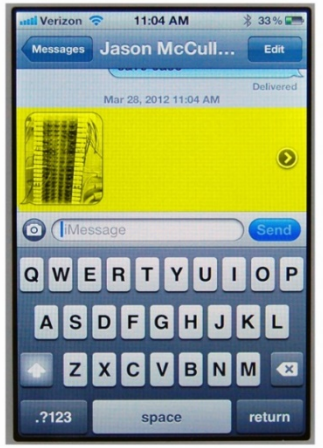
- Challenging the Evidence
  - Signed, sealed, delivered.
    - For a user to intentionally preserve that image, it has to be saved to the *Photos* application on the iPhone by selecting the image, then viewing it in full screen mode, selecting the *Share* icon, and then selecting *Save Image* option in the pop-up dialogue box.

1

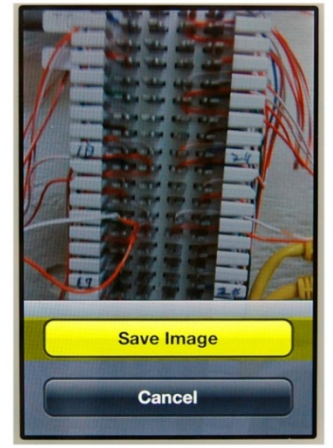
2



3

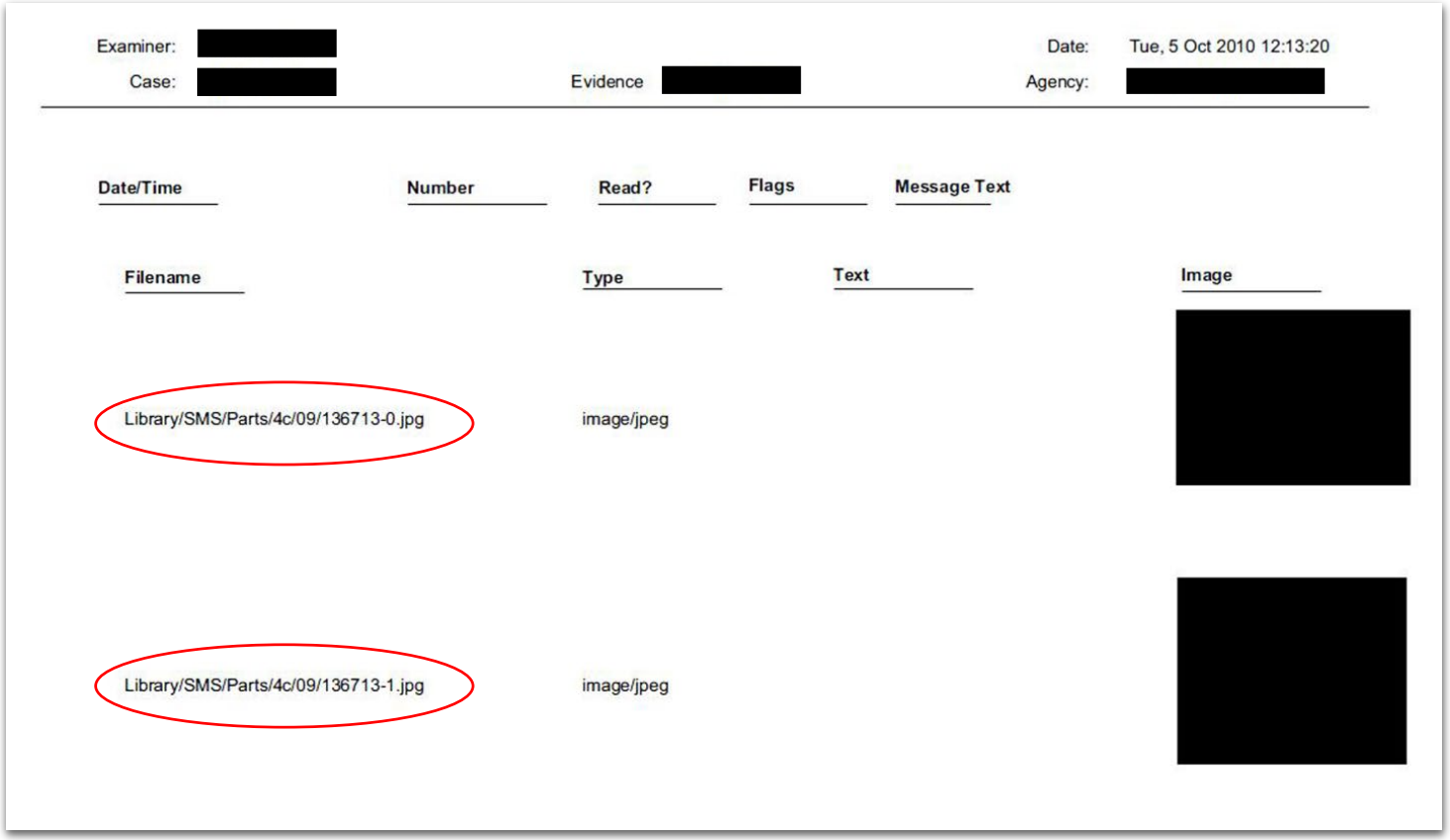


4



Case Examples

- Challenging the Evidence
  - Signed, sealed, delivered.
    - Images only existed in the SMS folder of the iPhone file system.



Examiner: [redacted]
Case: [redacted]
Evidence [redacted]
Date: Tue, 5 Oct 2010 12:13:20
Agency: [redacted]

Date/Time	Number	Read?	Flags	Message Text

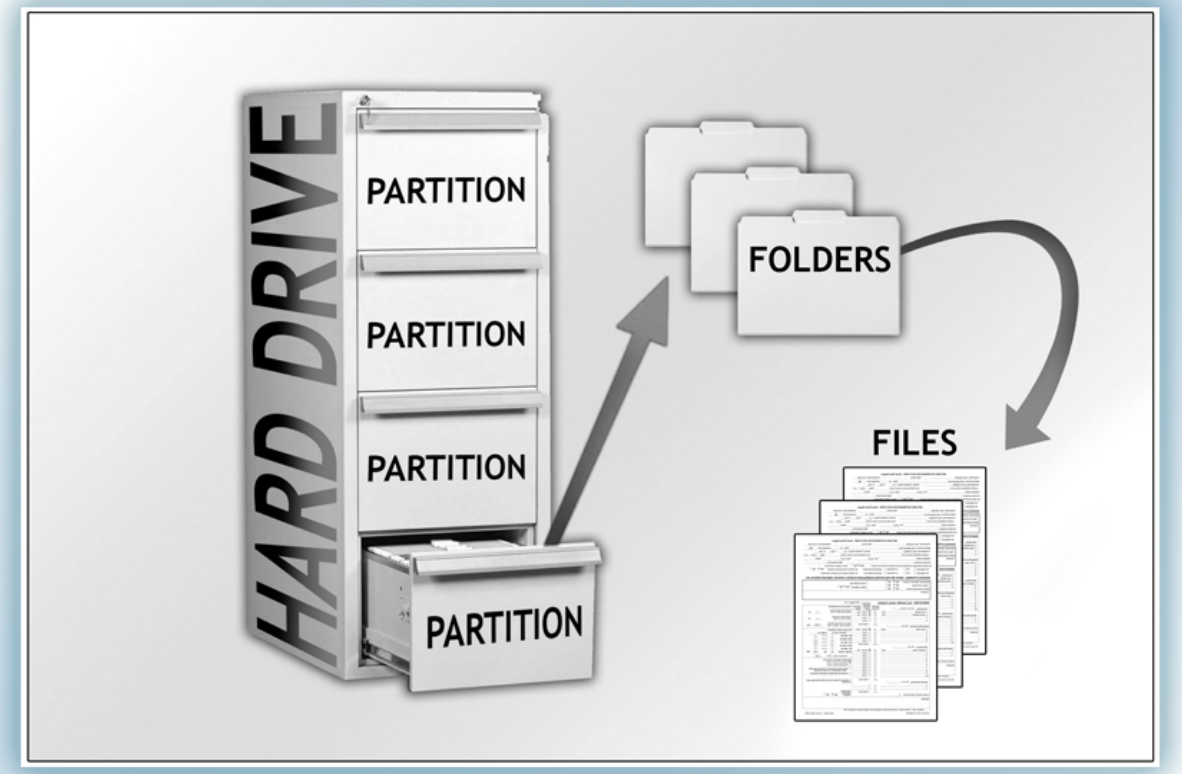
Filename	Type	Text	Image
Library/SMS/Parts/4c/09/136713-0.jpg	image/jpeg		[redacted]
Library/SMS/Parts/4c/09/136713-1.jpg	image/jpeg		[redacted]

Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Data Types

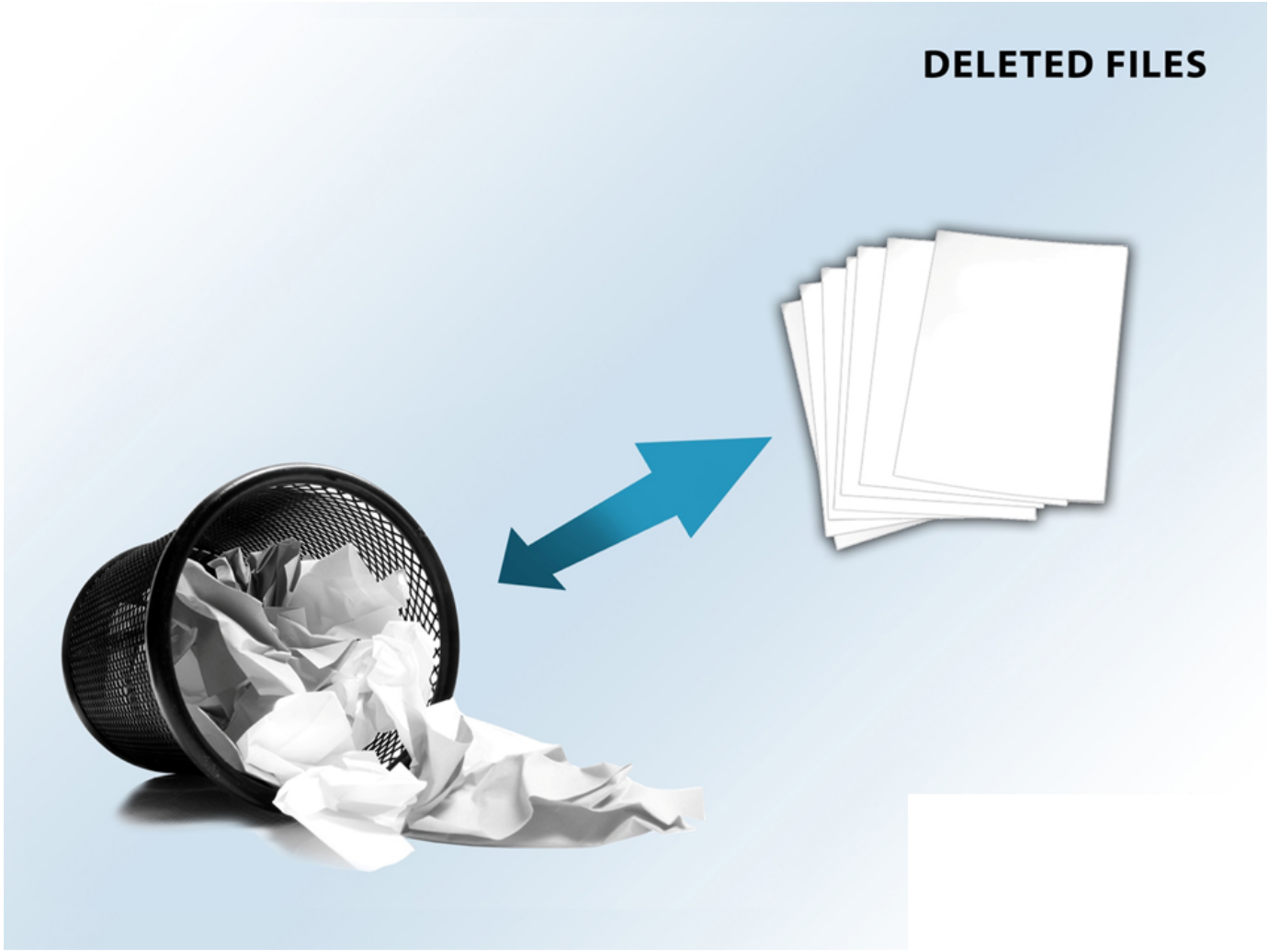
Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - How data is organized



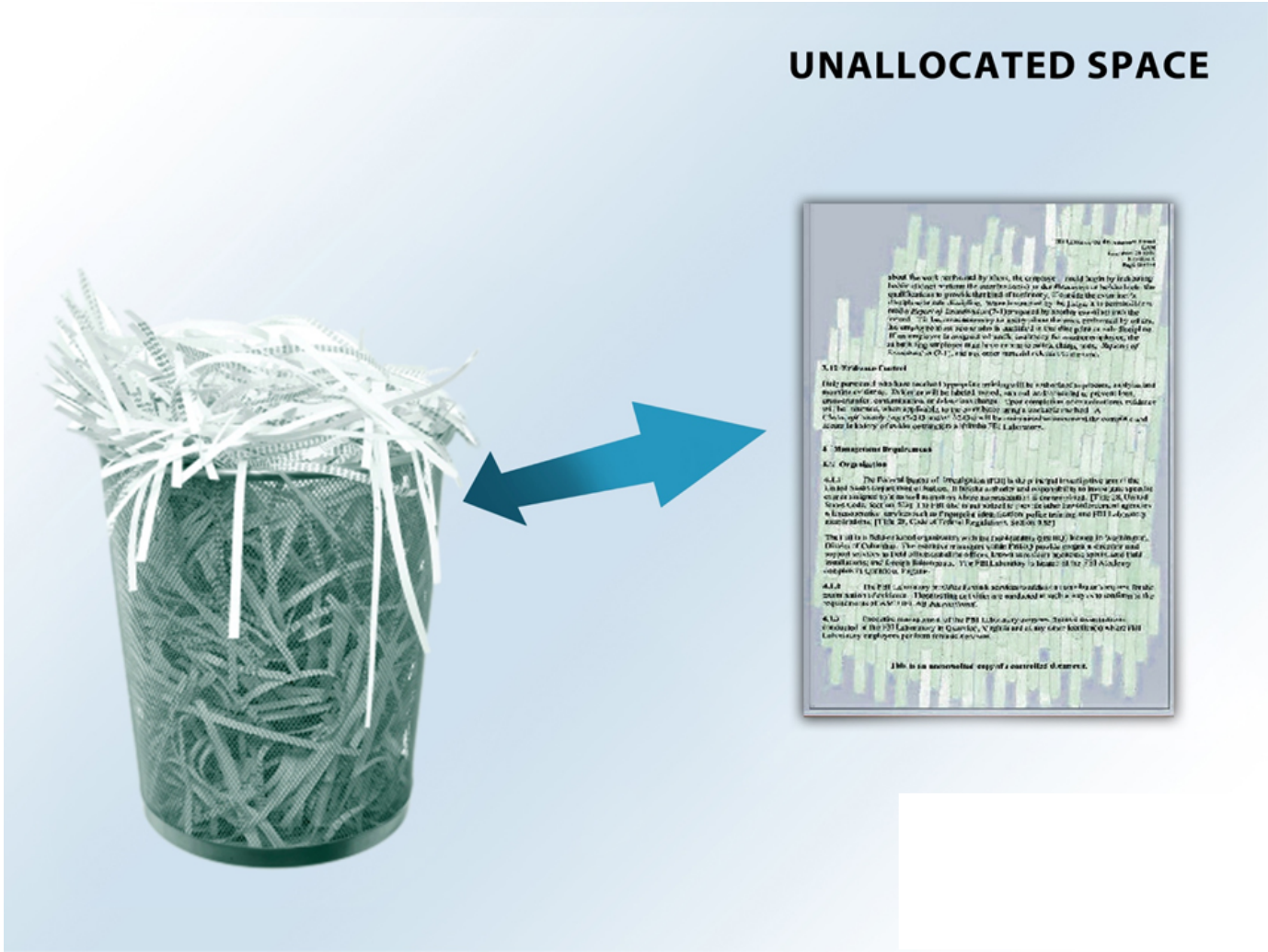
Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Deleted files



Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Unallocated space

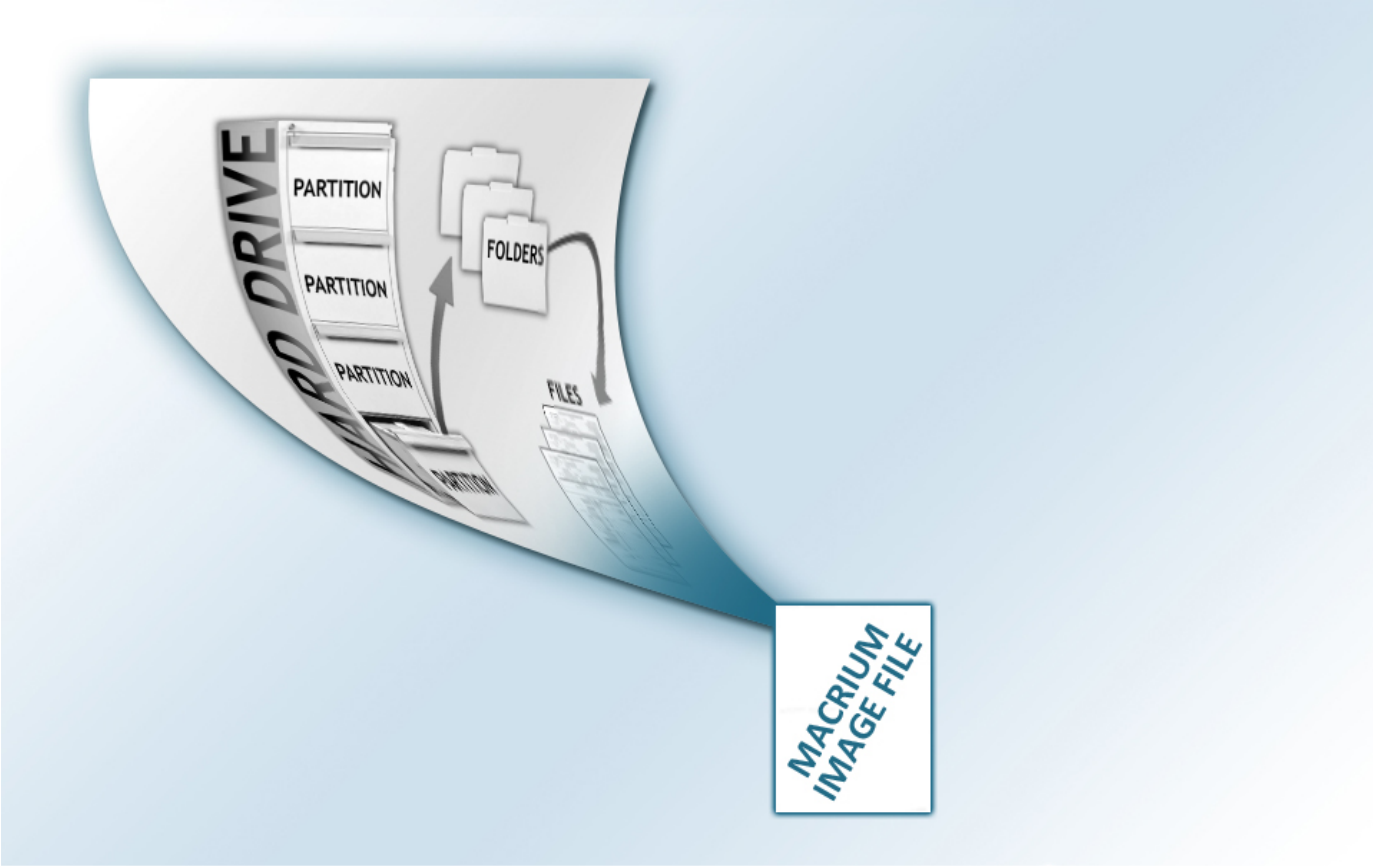


Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Compound files

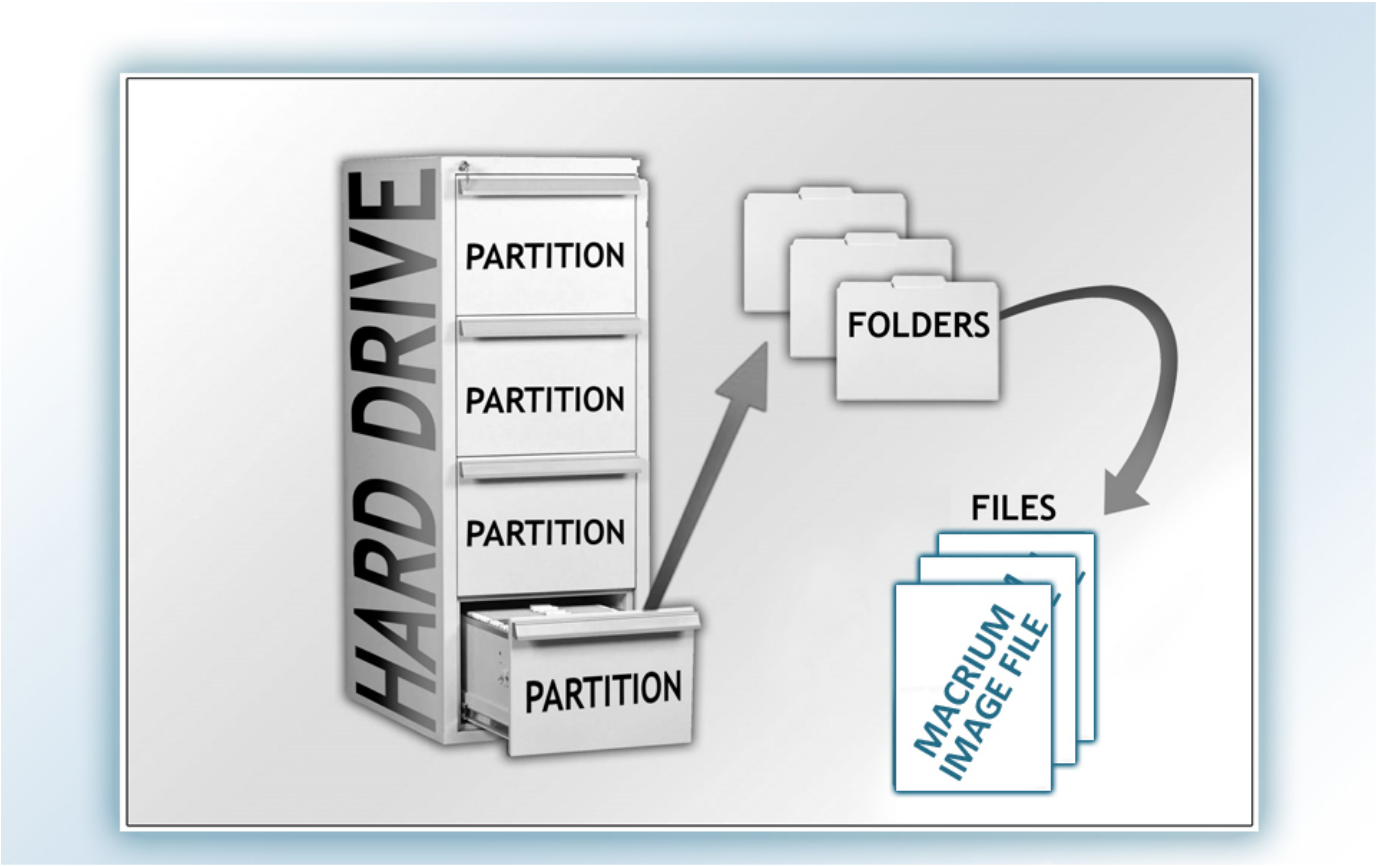
Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Macrium images



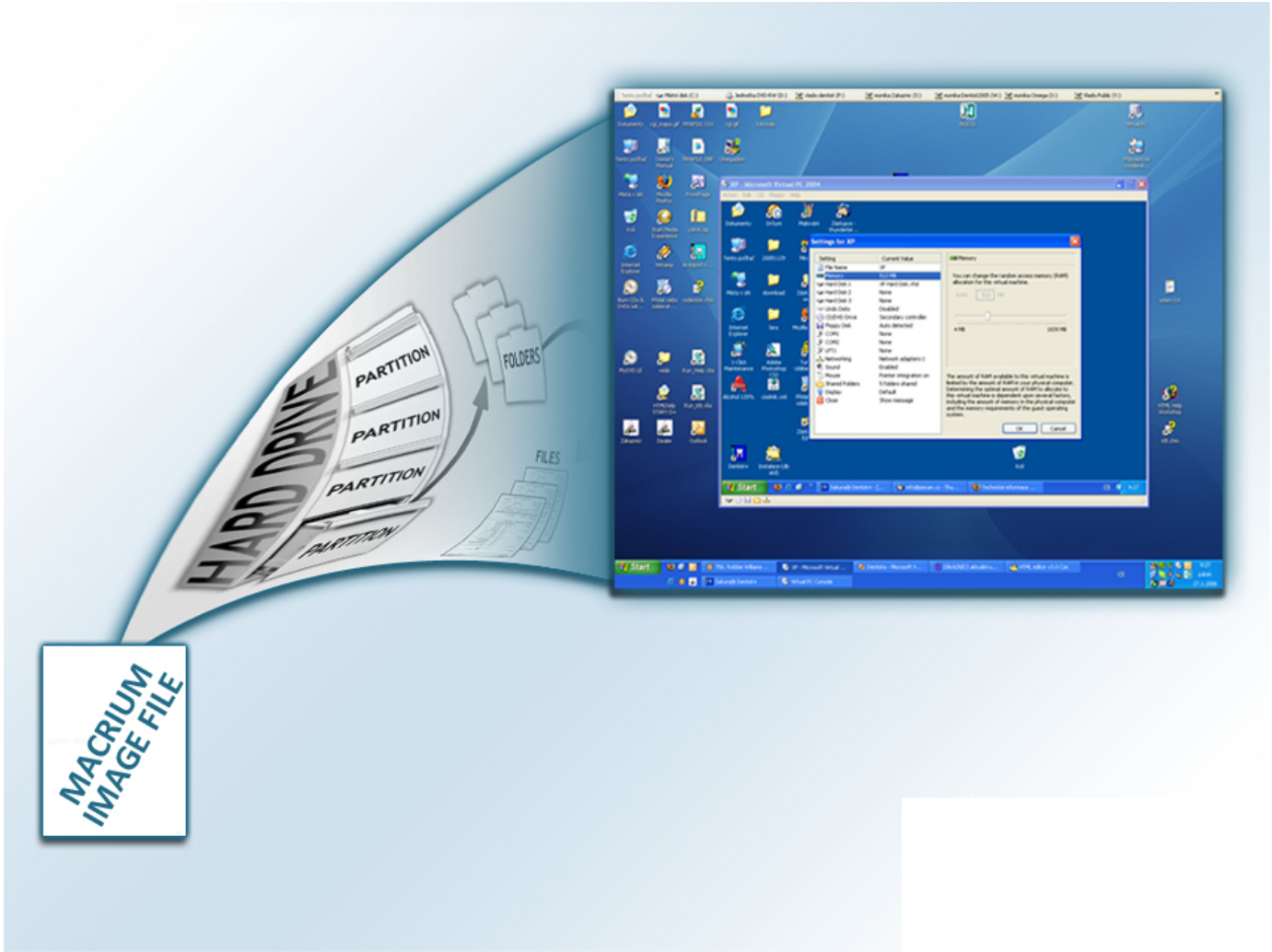
Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Computers in a computer



Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Macrium – cant open as a virtual hard drive with Defendant's version



Case Examples

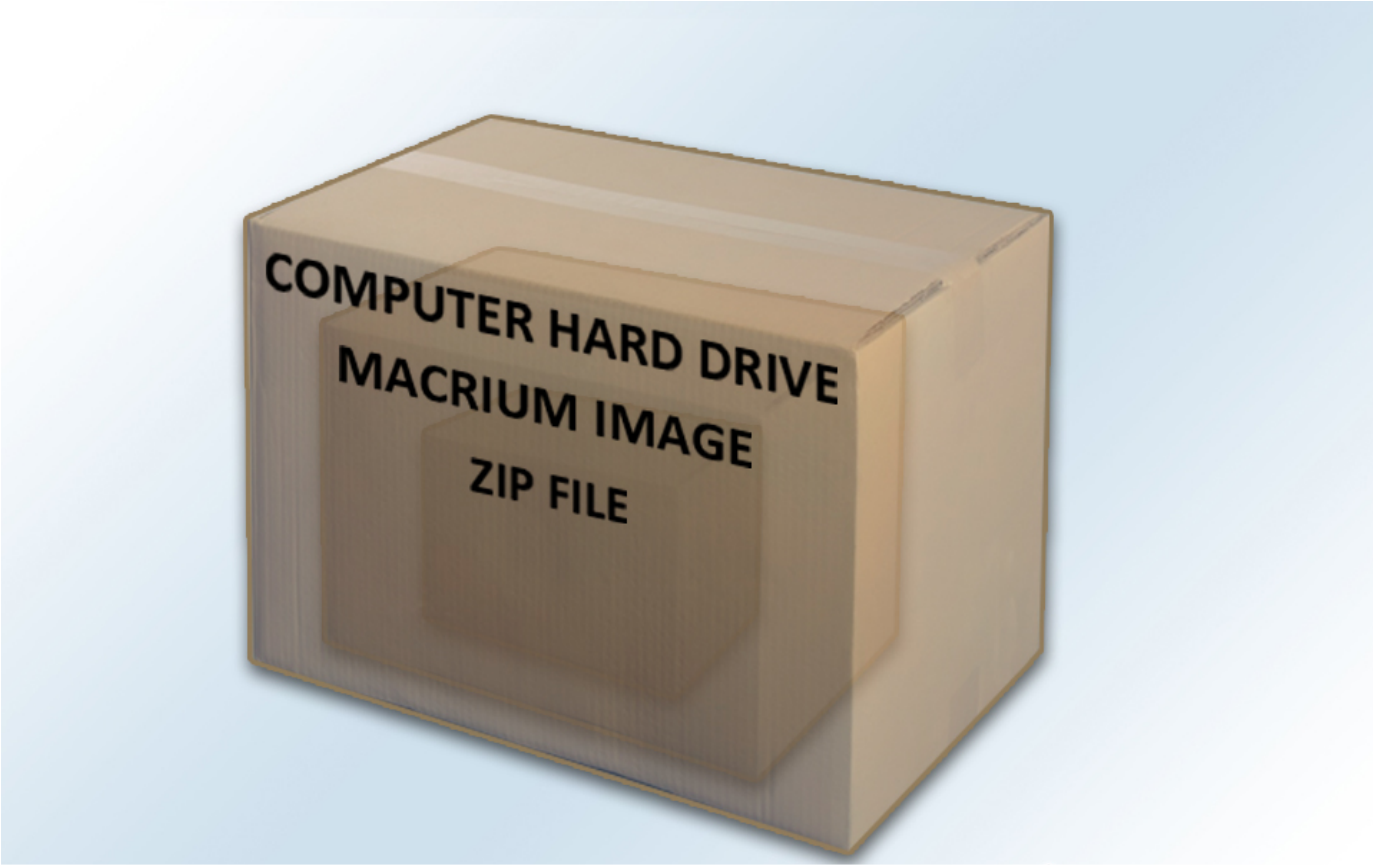
- Kansas – Macrium Image Case
  - Court Presentation
    - Must restore Macrium image to computer

Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - layers

Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Buried inside



Case Examples

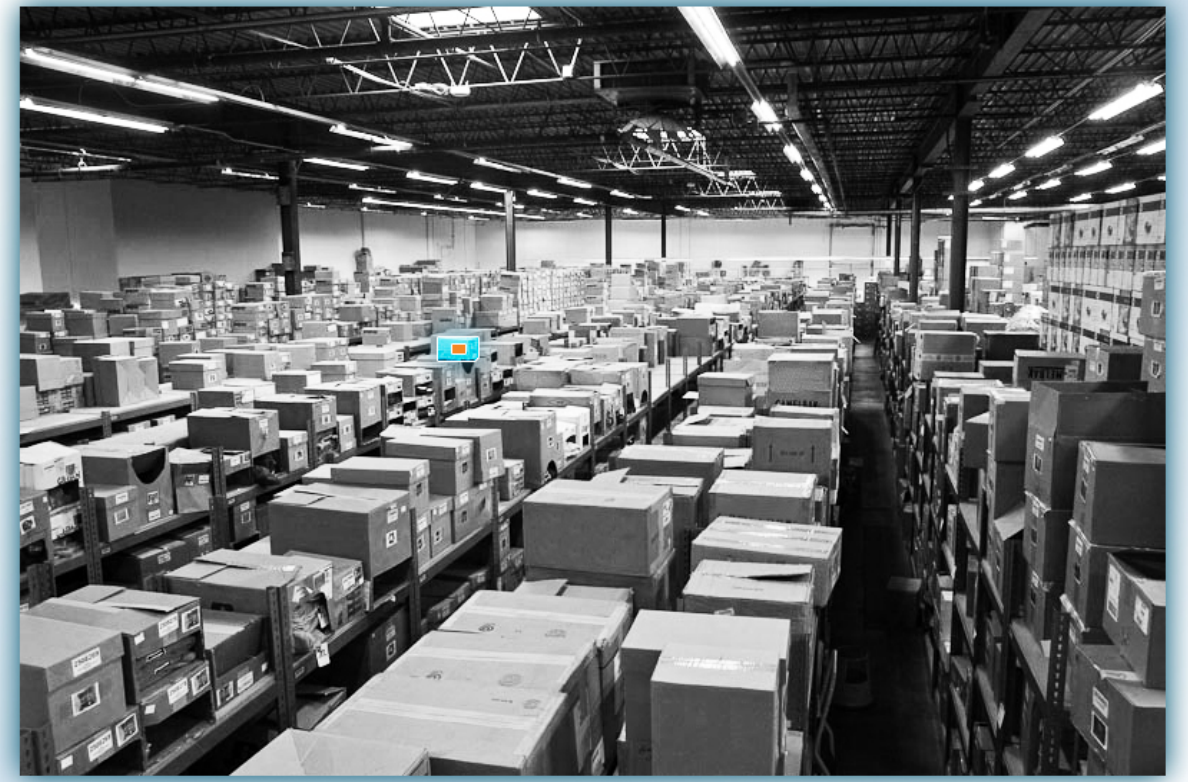
- Kansas – Macrium Image Case
  - Court Presentation
    - Big haystack

Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - There's another haystack

Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Needle in a haystack, inside of a haystack.



Case Examples

- Kansas – Macrium Image Case
  - Court Presentation
    - Warehouse inside of a warehouse which contains a compound file, which contains a handful of contraband images

Questions?

- Lars.Daniel@envistaforensics.com
- 919-621-9335