



Digital forensics: From certainty to shades of grey

Dr. Bradley Schatz

About me

- Dr Bradley Schatz | Forensic computer scientist
 - Managing Director, Schatz Forensic
 - Adjunct Associate Professor, Information Security Institute, Queensland University of Technology (QUT)
 - PhD (Digital forensics), BSc (Computer science)



Disclaimer

- INAL

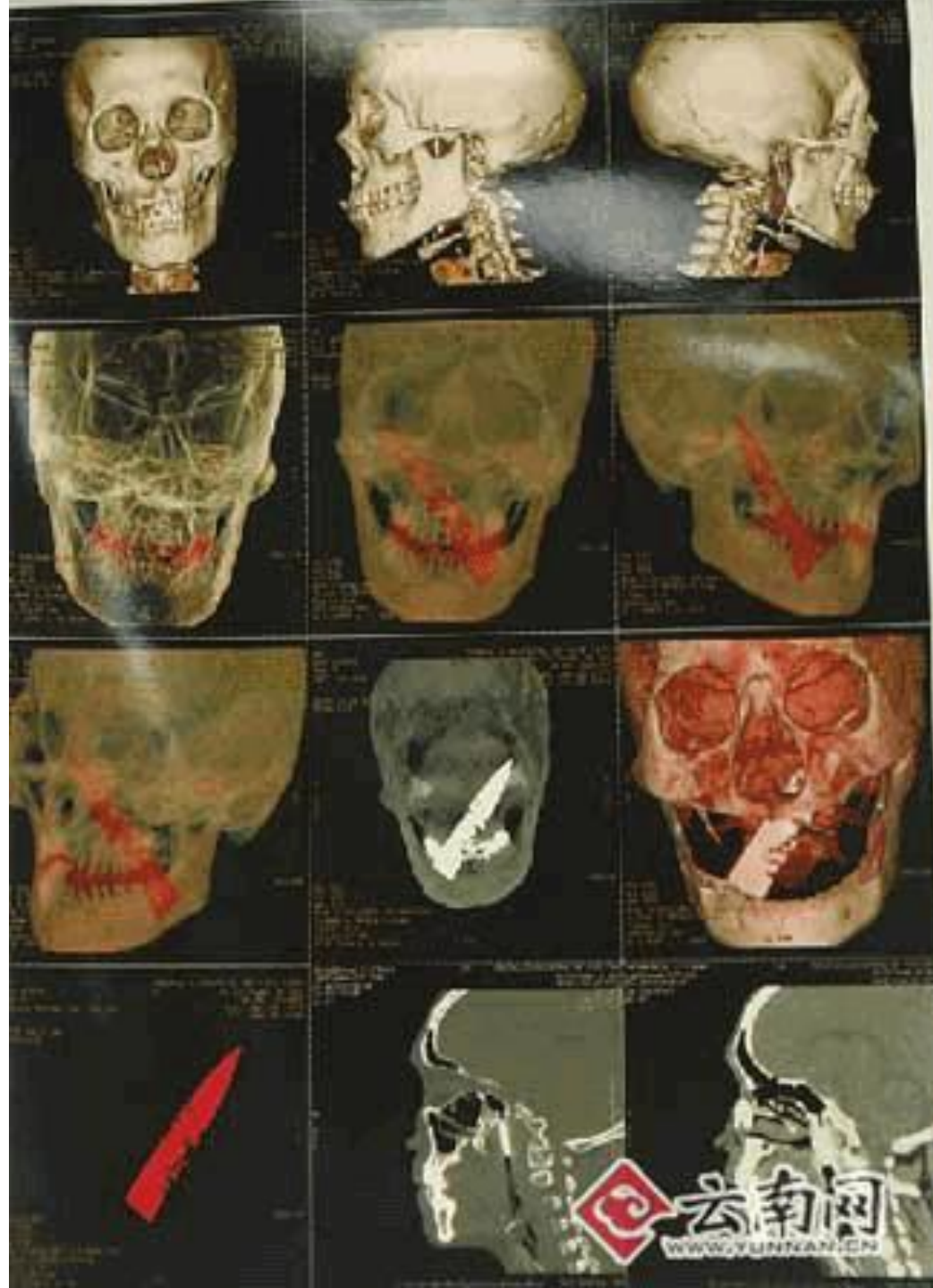
- General



**Will the evidence be admissible if I use open
source tools?**


Perception enhancing technologies != Forensics





Courts do not validate forensic tools

- “Encase is Guidance Software’s court-validated solution that provides law enforcement, corporate investigators...”
- “Built on court-validated FTK technology, ...”



“The integrity of the process depends on the carpenter not the hammer” : Craig Ball

Use the appropriate tool for the task at hand

- Storage forensics
 - Viewing unseen MFT entries
 - Carving
 - Timelining
- RAM Forensics
 - Volatility



Perspectives

Digital forensic evidence ?

- Application and OS performance optimizations (not designed for privacy)
- Novel interpretations of data maintained for other reasons
- Less often: actual logs designed for forensic purposes

After Golden Richard III

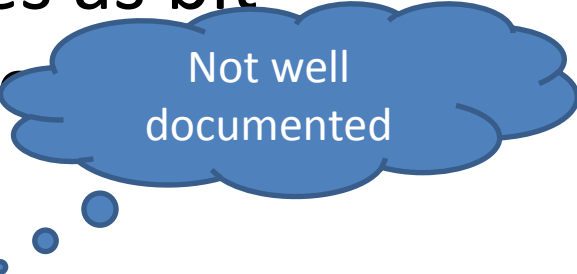
A fundamental theory and methodology of DF

- Real world actions leave traces as bit sequences in the digital environment
- Some of those traces persist
- Folk lore of actions which lead to traces

- Hypothesise which traces should be present
- Design tests of the hypotheses
- Use tools for perceiving and finding traces

A fundamental theory and methodology of DF

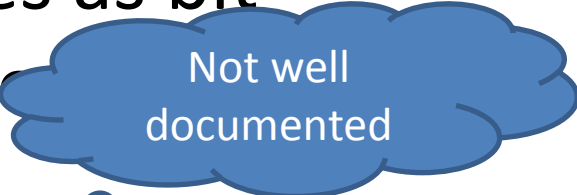
- Real world actions leave traces as bit sequences in the digital environment
- Some of those traces persist
- Folk lore of actions which lead to traces
- Hypothesise which traces should be present
- Design tests of the hypotheses
- Use tools for perceiving and finding traces



Not well documented

A fundamental theory and methodology of DF

- Real world actions leave traces as bit sequences in the digital environment
- Some of those traces persist
- Folk lore of actions which lead to traces
- Hypothesise which traces should be present
- Design tests of the hypotheses
- Use tools for perceiving and finding traces

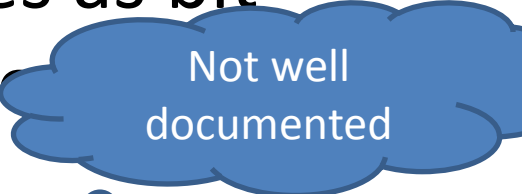




Not well documented



Rigour?

A fundamental theory and methodology of DF

- Real world actions leave traces as bit sequences in the digital environment 
- Some of those traces persist
- Folk lore of actions which lead to traces 
- Hypothesis that traces should be present 
- Design test hypotheses
- Use tools for perceiving and finding traces

A fundamental theory and methodology of DF

- Real world actions leave traces as bit sequences in the digital environment
- Some of those traces persist
- Folk lore of actions which lead to traces
- Hypothesise which traces should be present
- Design tests of the hypotheses
- Use tools for perceiving and finding traces



Attempts to disprove

Guiding principles

- Based on Scientific method
 - Observe
 - Hypothesise
 - Test
 - Report
- Independently verifiable
- Transparent & Substantiated
- Repeatable



**The question that should keep us
awake at night
How reliable are my conclusions?**

- *Who will determine how reliable my conclusions are?*
- *What is the harm going to be if I get it wrong?*

You, your boss or your client?

- *Stemming the bleeding*
- *APT*
- *Internal investigation*



In litigation the judge decides how reliable your conclusions are

- Her primary concern
 - Are your opinions reliable?
- Our concern
 - *Are our methods reliable?*
 - *Are our experience and knowledge reliable?*



Are our methods reliable?

Prosecutors to Seek Death Penalty in Casey Anthony Case



By SCOTT MICHELS

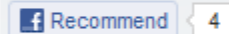
April 13, 2009

Prosecutors plan to seek the [death penalty](#) for [Casey Anthony](#), a Florida woman accused of murdering her daughter, a spokeswoman for the state attorney's office said today.

In December, the state's attorney's office filed court papers indicating that prosecutors [would not seek the death penalty](#) in connection with the first-degree murder case.

In a notice of intent filed today, prosecutors said additional information has become available. The filing says that "sufficient aggravating circumstances exist to justify the imposition of the death penalty," according to the Orlando Sentinel.

A spokeswoman for Jose Baez, Anthony's attorney, said in a statement, "This is not a death penalty case. We will do whatever is necessary to defend Casey Anthony from the state trying to take her life. We already have death-qualified defense lawyers on our team and are prepared for a vigorous defense."

Recommend 4Tweet 0 +1[+ Share](#) Email 100 Comments Print Single Page Text Size - / +

LOCAL NEWS

PHOTOS

SPORTS

BUSINESS

ENTERTAINMENT

LIVING

OBITS

CRIME COURTS

OPINION

LAKEWOOD RANCH

BLOGS

SPECIAL REPORTS

NEIGHBORHOODS

WE



SEARCH

Web Search powered by
YAHOO! SEARCHNEWS - BREAKING NEWS 

Published: Saturday, Nov. 07, 2009

Updated: Saturday, Nov. 07, 2009

0 Comments



Be the first of your friends to like this.

Anthony case: Chloroform found in syringe

By WALTER PACHECO, BIANCA PRIETO, RENE STUTZMAN and ANIKA MYERS PALM - Sun Sentinel

FBI lab technicians detected traces of chloroform inside a sports drink and plastic syringe recovered near the scene where the remains of Caylee Marie Anthony were found in 2008.

Those details and others are included in the more than 2,100 pages of documents released Friday by the State Attorney's Office in the criminal case against Casey Anthony — the 23-year-old accused of killing her daughter last year.

The report from the FBI's lab shows the Cool Blue-flavored Gatorade drink contained an "unknown liquid." The bottle also contained a plastic bag labeled "Disposable Syringe Kit" with a plastic syringe inside of the bag.

A report, generated in June and labeled "Summary of results" by Dr. Michael Rickenbach of the FBI, indicates chemical tests show the syringe contained chloroform, testosterone, ethanol and water.

Chloroform has been depicted in movies and on television when a person uses a rag soaked in the liquid to cover the mouth and nose of another, making the victim lose consciousness. A person can die if too much of the chemical is inhaled.

Testosterone is a natural occurring hormone in men and women. Levels decline gradually with age and the hormone can be prescribed as a controlled steroid to prevent or reduce osteoporosis, diabetes, cardiovascular disease and other diseases and disorders.

Investigative reports released last year show that someone at the Anthony home used the family computer to search the Internet for directions on how to make chloroform and "neck-breaking." Investigators also found traces of chloroform in the trunk of Casey Anthony's car, earlier reports show.



The state is seeking the death penalty against Anthony, who remains in the Orange County Jail.

So far, more than 10,000 pages of documents have been made public.

MY YAHOO!

SHARE   SUBSCRIBE 

ReadPlease?

 Email Story Printer Friendly Reprint | LicenseText Size:  

Casey Anthony Web History Fragments (similar)

- [http://www.google.com/search?q=chloroform
&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-
US:official&client=firefox-a](http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)

Casey Anthony Web History Fragments (similar)

- [http://www.google.com/search?q=chloroform
&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-
US:official&client=firefox-a](http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
- [http://www.sci-
spot.com/Chemistry/chloroform.html](http://www.scispot.com/Chemistry/chloroform.html)



SCI-SPOT.COM

Chloroform



STOP. READ BEFORE CONTINUING

THANKS FOR VISITING SCI-SPOT.COM'S CHLOROFORM SYNTHESIS. BEFORE CONTINUING, PLEASE READ THE FOLLOWING.

CHLOROFORM IS A DANGEROUS CHEMICAL. WHILE THE SYNTHESIS MAY APPEAR SIMPLE, IT SHOULD ONLY BE CONDUCTED BY QUALIFIED INDIVIDUALS. THE DANGER OF INHALING CHLOROFORM IS VERY REAL, AND CHLOROFORM HAS FADED FROM WIDESPREAD USE FOR A REASON. NO CHLOROFORM SHOULD EVER BE INHALED, ACCIDENTALLY OR OTHERWISE. CHLOROFORM PRODUCED IN THIS MANNER IS EVEN MORE DANGEROUS; IT CONTAINS BYPRODUCT SALTS, AS WELL AS ADDITIVES THAT MAY HAVE EXISTED IN THE REAGENT PRODUCTS. THIS MAKES FOR AN EXTREMELY DANGEROUS AND UNPREDICTABLE CHEMICAL.

NEVER LEAVE AN OPEN CONTAINER OF CHLOROFORM. NEVER STORE CHLOROFORM IN A METAL OR PLASTIC BOTTLE. NEVER STORE CHLOROFORM FOR LONG PERIODS OF TIME. STORED CHLOROFORM WILL DECOMPOSE INTO PHOSGENE GAS, A CHEMICAL USED IN WWI AS A CHEMICAL WEAPON. NEVER ALLOW CHILDREN TO COME NEAR CHLOROFORM.

FOLLOW GOOD CHEMISTRY PROCEDURES AT ALL TIMES. WEAR SAFETY GOGGLES AND APPROPRIATE CLOTHING. IF YOU'RE EVER IN DOUBT, ERR ON THE SIDE OF CAUTION.

AGAIN, **NEVER INHALE CHLOROFORM, ESPECIALLY CHLOROFORM PRODUCED IN THIS MANNER.**

[< GO BACK CONTINUE >](#)

Expert: Chloroform Page Accessed 84 Times

POSTED: 4:42 pm EST June 8, 2011

UPDATED: 4:45 pm EST June 8, 2011

Email

0 comments

Recommend 14

SHARE



Prosecutor Linda Drane Burdick ended Wednesday's testimony in the Casey Anthony murder trial with expert witness John Dennis Bradley answering that, according to search history, a chloroform website was visited 84 times on the Anthony family home computer.

Testimony of police examiner

- Report 1: 8,571 records (June 2011)
 - Chloroform web page: VisitCount=84

Testimony of police examiner

- Report 1: 8,571 records (June 2011)
 - Chloroform web page: VisitCount=84
- Report 2 : 8,878 records (August 2008)
 - Chloroform web page: VisitCount=1
 - MySpace web page: VisitCount=84

Recollected conversation between toolsmith and examiner

- "What did you do about it?"
- “.. visually inspected the URL within the Firefox 2 history file which was in question and observed the number 84 nearby (a couple of lines below) and assumed that it was correct”.

Source: http://www.cacheback.ca/news/news_release-20110711-1.asp

What's wrong with this?

- Scientific method
- Transparent
- Good practice

What's wrong with this?

- Scientific method
 - A negative refutes a positive
- Transparent

- Good practice

What's wrong with this?

- Scientific method
 - A negative refutes a positive
- Transparent
 - The results of the negative test should have been communicated
- Good practice

What's wrong with this?

- Scientific method
 - A negative refutes a positive
- Transparent
 - The results of the negative test should have been communicated
 - Assumptions should be declared
- Good practice

What's wrong with this?

- Scientific method
 - A negative refutes a positive
- Transparent
 - The results of the negative test should have been communicated
 - Assumptions should be declared
- Good practice
 - Where interpretation is central, should be manually verified at bit sequence level

```
// <!-- <mdb:mork:z v="1.4"/> -->
```

```
< <(a=c)> // (f=iso-8859-1)
```

```
(8A=Typed)(8B=LastPageVisited)(8C=ByteOrder)
```

```
(80=ns:history:db:row:scope:history:all)
```

```
(81=ns:history:db:table:kind:history)(82=URL)(83=Referrer)
```

```
(84=LastVisitDate)(85=FirstVisitDate)(86=VisitCount)(87=Name)
```

```
(88=Hostname)(89=Hidden)>
```

```
<(80=LE)(81
```

```
=http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:\
```

```
en-US:official)(82=1321438074563875)(83=en-us.start2.mozilla.com)(84=1)
```

```
(85
```

```
=http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:offi\
```

```
cial)(86=google.com)(87
```

```
=http://www.google.com.au/firefox?client=firefox-a&rls=org.mozilla:en-US:o\
```

```
fficial)(88=1321438080517000)(89=google.com.au)(8A
```

```
=M$00o$00z$00i$00l$00l$00a$00 $00F$00i$00r$00e$00f$00o$00x$00 $00S$00t$00a\
```

```
$00r$00t$00 $00P$00a$00g$00e$00)(8B
```

```
=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.\
```

```
mozilla:en-US:official&client=firefox-a)(8C=1321438124485750)(8D
```

```
=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=o\
```

```
rg.mozilla:en-US:official&client=firefox-a)(8E
```

```
=c$00h$00l$00o$00r$00o$00f$00o$00r$00m$00 $00-$00 $00G$00o$00o$00g$00l$00e\
```

```
$00 $00S$00e$00a$00r$00c$00h$00)(8F
```

```
=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa\
```

```
=U&ei=rYvDT03DCqOjiAfE_pzxDQ&ved=0CBYQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U\
```

```
3tA)(90=1321438128376375)(91=http://en.wikipedia.org/wiki/Chloroform)
```

```
(92=1321438131563875)(93=en.wikipedia.org)(94
```

```
=C$00h$00l$00o$00r$00o$00f$00o$00r$00m$00 $00-$00 $00W$00i$00k$00i$00p$00e\
```

```
$00d$00i$00a$00,$00 $00t$00h$00e$00 $00f$00r$00e$00e$00 $00e$00n$00c$00y$00c$00\
```

```
l$00o$00p$00e$00d$00i$00a$00)(95=http://myspace.com/)(96=1321438153845125)
```



```
// <!-- <mdb:mork:z v="1.4"/> -->
```

```
<<(a=c)> // (f=iso-8859-1)
```

```
(8A=Typed)(8B=LastPageVisited)(8C=ByteOrder)
```

```
(80=ns:history:db:row:scope:history:all)
```

```
(81=ns:history:db:table:kind:history)(82=URL)(83=Referrer)
```

```
(84=LastVisitDate)(85=FirstVisitDate)(86=VisitCount)(87=Name)
```

```
(88=Hostname)(89=Hidden)>
```

```
<(80=LE)(81
```

```
=http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:\
```

```
en-US:official)(82=1321438074563875)(83=en-us.start2.mozilla.com)(84=1)
```

```
(85
```

```
=http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:offi\
```

```
cial)(86=google.com)(87
```

```
=http://www.google.com.au/firefox?client=firefox-a&rls=org.mozilla:en-US:o\
```

```
fficial)(88=1321438080517000)(89=google.com.au)(8A
```

```
=M$00o$00z$00i$00l$00l$00a$00 $00F$00i$00r$00e$00f$00o$00x$00 $00S$00t$00a\
```

```
$00r$00t$00 $00P$00a$00g$00e$00)(8B
```

```
=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.\
```

```
mozilla:en-US:official&client=firefox-a)(8C=1321438124485750)(8D
```

```
=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=o\
```

```
rg.mozilla:en-US:official&client=firefox-a)(8E
```

```
=c$00h$00l$00o$00r$00o$00f$00o$00r$00m$00 $00-$00 $00G$00o$00o$00g$00l$00e\
```

```
$00 $00S$00e$00a$00r$00c$00h$00)(8F
```

```
=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa\
```

```
=U&ei=rYvDT03DCqOjiAfE_pzxDQ&ved=0CBYQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U\
```

```
3tA)(90=1321438128376375)(91=http://en.wikipedia.org/wiki/Chloroform)
```

```
(92=1321438131563875)(93=en.wikipedia.org)(94
```

```
=C$00h$00l$00o$00r$00o$00f$00o$00r$00m$00 $00-$00 $00W$00i$00k$00i$00p$00e\
```

```
$00d$00i$00a$00,$00 $00t$00h$00e$00 $00f$00r$00e$00e$00 $00e$00n$00c$00y$00c$00\
```

```
l$00o$00p$00e$00d$00i$00a$00)(95=http://myspace.com/)(96=1321438153845125)
```

Header

```
// <!-- <mdb:mork:z v="1.4"/> -->
```

```
< <(a=c)> // (f=iso-8859-1)
```

```
(8A=Typed)(8B=LastPageVisited)(8C=ByteOrder)  
(80=ns:history:db:row:scope:history:all)  
(81=ns:history:db:table:kind:history)(82=URL)(83=Referrer)  
(84=LastVisitDate)(85=FirstVisitDate)(86=VisitCount)(87=Name)  
(88=Hostname)(89=Hidden)>
```

Field
definitions

```
<(80=LE)(81
```

```
=http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:\  
en-US:official)(82=1321438074563875)(83=en-us.start2.mozilla.com)(84=1)
```

```
(85  
=http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:offi\  
cial)(86=google.com)(87
```

```
=http://www.google.com.au/firefox?client=firefox-a&rls=org.mozilla:en-US:o\  
fficial)(88=1321438080517000)(89=google.com.au)(8A
```

```
=M$00o$00z$00i$00l$00l$00a$00 $00F$00i$00r$00e$00f$00o$00x$00 $00S$00t$00a\  
$00r$00t$00 $00P$00a$00g$00e$00)(8B
```

```
=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.\  
mozilla:en-US:official&client=firefox-a)(8C=1321438124485750)(8D
```

```
=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=o\  
rg.mozilla:en-US:official&client=firefox-a)(8E
```

```
=c$00h$00l$00o$00r$00o$00f$00o$00r$00m$00 $00-$00 $00G$00o$00o$00g$00l$00e\  
$00 $00S$00e$00a$00r$00c$00h$00)(8F
```

```
=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa\  
=U&ei=rYvDT03DCqOjiAfE_pzxDQ&ved=0CBYQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U\  
3tA)(90=1321438128376375)(91=http://en.wikipedia.org/wiki/Chloroform)
```

```
(92=1321438131563875)(93=en.wikipedia.org)(94
```

```
=C$00h$00l$00o$00r$00o$00f$00o$00r$00m$00 $00-$00 $00W$00i$00k$00i$00p$00e\  
$00d$00i$00a$00,$00 $00t$00h$00e$00 $00f$00r$00e$00e$00 $00e$00n$00c$00y$00c$00\  
l$00o$00p$00e$00d$00i$00a$00)(95=http://myspace.com/)(96=1321438153845125)
```

```
// <!-- <mdb:mork:z v="1.4"/> -->
```

```
< <(a=c)> // (f=iso-8859-1)
```

```
(8A=Typed)(8B=LastPageVisited)(8C=ByteOrder)
```

```
(80=ns:history:db:row:scope:history:all)
```

```
(81=ns:history:db:table:kind:history)(82=URL)(83=Referrer)
```

```
(84=LastVisitDate)(85=FirstVisitDate)(86=VisitCount)(87=Name)
```

```
(88=Hostname)(89=Hidden)>
```

(82=URL)

(86=VisitCount)

```
<(80=LE)(81
```

```
=http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:\
```

```
en-US:official)(82=1321438074563875)(83=en-us.start2.mozilla.com)(84=1)
```

```
(85
```

```
=http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:offi\
```

```
cial)(86=google.com)(87
```

```
=http://www.google.com.au/firefox?client=firefox-a&rls=org.mozilla:en-US:o\
```

```
fficial)(88=1321438080517000)(89=google.com.au)(8A
```

```
=M$00o$00z$00i$00l$00l$00a$00 $00F$00i$00r$00e$00f$00o$00x$00 $00S$00t$00a\
```

```
$00r$00t$00 $00P$00a$00g$00e$00)(8B
```

```
=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.\
```

```
mozilla:en-US:official&client=firefox-a)(8C=1321438124485750)(8D
```

```
=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=o\
```

```
rg.mozilla:en-US:official&client=firefox-a)(8E
```

```
=c$00h$00l$00o$00r$00o$00f$00o$00r$00m$00 $00-$00 $00G$00o$00o$00g$00l$00e\
```

```
$00 $00S$00e$00a$00r$00c$00h$00)(8F
```

```
=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa\
```

```
=U&ei=rYvDT03DCqOjiAfE_pzxDQ&ved=0CBYQFjAA&usg=AFQjCNGORI6--agKA23E0q9lkK4r5-U\
```

```
3tA)(90=1321438128376375)(91=http://en.wikipedia.org/wiki/Chloroform)
```

```
(92=1321438131563875)(93=en.wikipedia.org)(94
```

```
=C$00h$00l$00o$00r$00o$00f$00o$00r$00m$00 $00-$00 $00W$00i$00k$00i$00p$00e\
```

```
$00d$00i$00a$00,$00 $00t$00h$00e$00 $00f$00r$00e$00e$00 $00e$00n$00c$00y$00c$00\
```

```
l$00o$00p$00e$00d$00i$00a$00)(95=http://myspace.com/)(96=1321438153845125)
```

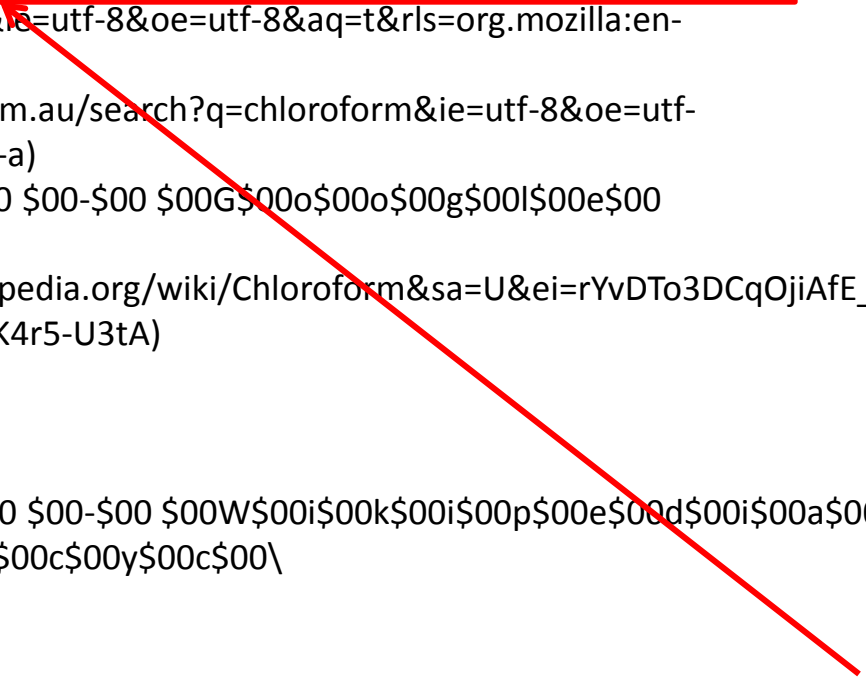
<(80=LE)
(81=http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(82=1321438074563875)(83=en-us.start2.mozilla.com)
(84=1)
(85=http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(86=google.com)(87=http://www.google.com.au/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(88=1321438080517000)
(89=google.com.au)
(8A=M\$00o\$00z\$00i\$00l\$00l\$00a\$00 \$00F\$00i\$00r\$00e\$00f\$00o\$00x\$00 \$00S\$00t\$00a\$00r\$00t\$00
\$00P\$00a\$00g\$00e\$00)
(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-
US:official&client=firefox-a)
(8C=1321438124485750)(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-
8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8E=c\$00h\$00l\$00o\$00r\$00o\$00f\$00o\$00r\$00m\$00 \$00-\$00 \$00G\$00o\$00o\$00g\$00l\$00e\$00
\$00S\$00e\$00a\$00r\$00c\$00h\$00)
(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&
ved=0CBYQFjAA&usg=AFQjCNGORI6--agKA23E0q9lkK4r5-U3tA)
(90=1321438128376375)
(91=http://en.wikipedia.org/wiki/Chloroform)
(92=1321438131563875)(93=en.wikipedia.org)
(94=C\$00h\$00l\$00o\$00r\$00o\$00f\$00o\$00r\$00m\$00 \$00-\$00 \$00W\$00i\$00k\$00i\$00p\$00e\$00d\$00i\$00a\$00,\$00
\$00t\$00h\$00e\$00 \$00f\$00r\$00e\$00e\$00 \$00e\$00n\$00c\$00y\$00c\$00\
l\$00o\$00p\$00e\$00d\$00i\$00a\$00)
(95=http://myspace.com/)
(96=1321438153845125)
(97=myspace.com)
(98=2)
(99=http://www.myspace.com/)
(9A=1321438159407625)
(9B=http://www.myspace.com/help/browserunsupported)

(82=URL)
(86=VisitCount)

<(80=LE)
(81=http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(82=1321438074563875)(83=en-us.start2.mozilla.com)
(84=1)
(85=http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(86=google.com)(87=http://www.google.com.au/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(88=1321438080517000)
(89=google.com.au)
(8A=M\$00o\$00z\$00i\$00l\$00l\$00a\$00 \$00F\$00i\$00r\$00e\$00f\$00o\$00x\$00 \$00S\$00t\$00a\$00r\$00t\$00
\$00P\$00a\$00g\$00e\$00)
(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-
US:official&client=firefox-a)
(8C=1321438124485750)(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-
8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8E=c\$00h\$00l\$00o\$00r\$00o\$00f\$00o\$00r\$00m\$00 \$00-\$00 \$00G\$00o\$00o\$00g\$00l\$00e\$00
\$00S\$00e\$00a\$00r\$00c\$00h\$00)
(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&
ved=0CBYQFjAA&usg=AFQjCNGORI6--agKA23E0q9lkK4r5-U3tA)
(90=1321438128376375)
(91=http://en.wikipedia.org/wiki/Chloroform)
(92=1321438131563875)(93=en.wikipedia.org)
(94=C\$00h\$00l\$00o\$00r\$00o\$00f\$00o\$00r\$00m\$00 \$00-\$00 \$00W\$00i\$00k\$00i\$00p\$00e\$00d\$00i\$00a\$00,\$00
\$00t\$00h\$00e\$00 \$00f\$00r\$00e\$00e\$00 \$00e\$00n\$00c\$00y\$00c\$00\
l\$00o\$00p\$00e\$00d\$00i\$00a\$00)
(95=http://myspace.com/)
(96=1321438153845125)
(97=myspace.com)
(98=2)
(99=http://www.myspace.com/)
(9A=1321438159407625)
(9B=http://www.myspace.com/help/browserunsupported)

(82=URL)
(86=VisitCount)

(8A=M\$00o\$00z\$00i\$00l\$00l\$00a\$00 \$00F\$00i\$00r\$00e\$00f\$00o\$00x\$00 \$00S\$00t\$00a\$00r\$00t\$00
\$00P\$00a\$00g\$00e\$00)



Unicode

<(80=LE)
(81=http://en-us.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(82=1321438074563875)(83=en-us.start2.mozilla.com)
(84=1)
(85=http://www.google.com/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(86=google.com)(87=http://www.google.com.au/firefox?client=firefox-a&rls=org.mozilla:en-US:official)
(88=1321438080517000)
(89=google.com.au)
(8A=Mozilla Firefox Start Page)
(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8C=1321438124485750)(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8E=chloroform - Google Search)
(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&ved=0CBYQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U3tA)
(90=1321438128376375)
(91=http://en.wikipedia.org/wiki/Chloroform)
(92=1321438131563875)(93=en.wikipedia.org)
(94=Chloroform - Wikipedia, the free encyclopedia)
(95=http://myspace.com/)
(95=http://myspace.com/)
(97=myspace.com)
(98=2)
(99=http://www.myspace.com/)
(9A=1321438159407625)
(9B=http://www.myspace.com/help/browserunsupported)
(9C=Myspace)
(9E=http://facebook.com/)
(9F=1321438185938875)

(82=URL)
(86=VisitCount)

<(80=LE)
(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8C=1321438124485750)
(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8E=chloroform - Google Search)
(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&ved=0CByQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U3tA)
(90=1321438128376375)
(91=http://en.wikipedia.org/wiki/Chloroform)
(92=1321438131563875)
(93=en.wikipedia.org)
(94=Chloroform - Wikipedia, the free encyclopedia)
(95=http://myspace.com/)
(9E=http://facebook.com/)
(A0=facebook.com)
(A1=http://www.facebook.com/)
(A2=1321438191642000)(A3=Welcome to Facebook - Log In, Sign Up or Learn More)>
{1:^80 {(k^81:c)(s=9)[1(^8C=LE)]}
[2(^82^81)(^84^82)(^85^82)(^88^83)(^89=1)]
[3(^82^85)(^84^82)(^85^82)(^88^86)(^89=1)]
[4(^82^87)(^84^88)(^85^88)(^88^89)(^87^8A)]
[5(^82^8B)(^84^8C)(^85^8C)(^88^86)(^89=1)]
[6(^82^8D)(^84^8C)(^85^8C)(^88^89)(^87^8E)]
[7(^82^8F)(^84^90)(^85^90)(^83^8D)(^88^89)(^89=1)]
[8(^82^91)(^84^92)(^85^92)(^83^8D)(^88^93)(^87^94)]
[9(^82^95)(^84^96)(^85^96)(^88^97)(^8A=1)(^86=2)]
[A(^82^99)(^84^9A)(^85^9A)(^88^97)(^89=1)]
[B(^82^9B)(^84^9A)(^85^9A)(^88^97)(^87^9C)]
[C(^82^9E)(^84^9F)(^85^9F)(^88^A0)(^8A=1)(^86=2)]

(82=URL)
(86=VisitCount)

<(80=LE)
(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8C=1321438124485750)
(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8E=chloroform - Google Search)
(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&ved=0CByQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U3tA)
(90=1321438128376375)
(91=http://en.wikipedia.org/wiki/Chloroform)
(92=1321438131563875)
(93=en.wikipedia.org)
(94=Chloroform - Wikipedia, the free encyclopedia)
(95=http://myspace.com/)
(9E=http://facebook.com/)
(A0=facebook.com)
(A1=http://www.facebook.com/)
(A2=1321438191642000)(A3=Welcome to Facebook - Log In, Sign Up or Learn More)>

(82=URL)
(86=VisitCount)

Field definitions

{1:^80 {(k^81:c)(s=9)[1(^8C=LE)]}
[2(^82^81)(^84^82)(^85^82)(^88^83)(^89=1)]
[3(^82^85)(^84^82)(^85^82)(^88^86)(^89=1)]
[4(^82^87)(^84^88)(^85^88)(^88^89)(^87^8A)]
[5(^82^8B)(^84^8C)(^85^8C)(^88^86)(^89=1)]
[6(^82^8D)(^84^8C)(^85^8C)(^88^89)(^87^8E)]
[7(^82^8F)(^84^90)(^85^90)(^83^8D)(^88^89)(^89=1)]
[8(^82^91)(^84^92)(^85^92)(^83^8D)(^88^93)(^87^94)]
[9(^82^95)(^84^96)(^85^96)(^88^97)(^8A=1)(^86=2)]
[A(^82^99)(^84^9A)(^85^9A)(^88^97)(^89=1)]
[B(^82^9B)(^84^9A)(^85^9A)(^88^97)(^87^9C)]
[C(^82^9E)(^84^9F)(^85^9F)(^88^A0)(^8A=1)(^86=2)]

(^82^91)

<(80=LE)
(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8C=1321438124485750)
(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8E=chloroform - Google Search)
(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&ved=0CByQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U3tA)
(90=1321438128376375)
(91=http://en.wikipedia.org/wiki/Chloroform)
(92=1321438131563875)
(93=en.wikipedia.org)
(94=Chloroform - Wikipedia, the free encyclopedia)
(95=http://myspace.com/)
(9E=http://facebook.com/)
(A0=facebook.com)
(A1=http://www.facebook.com/)
(A2=1321438191642000)(A3>Welcome to Facebook - Log In, Sign Up or Learn More)>
{1:^80 {(k^81:c)(s=9)[1(^8C=LE)]}
[2(^82^81)(^84^82)(^85^82)(^88^83)(^89=1)]
[3(^82^85)(^84^82)(^85^82)(^88^86)(^89=1)]
[4(^82^87)(^84^88)(^85^88)(^88^89)(^87^8A)]
[5(^82^8B)(^84^8C)(^85^8C)(^88^86)(^89=1)]
[6(^82^8D)(^84^8C)(^85^8C)(^88^89)(^87^8E)]
[7(^82^8F)(^84^90)(^85^90)(^83^8D)(^88^89)(^89=1)]
[8(^82^91)(^84^92)(^85^92)(^83^8D)(^88^93)(^87^94)]
[9(^82^95)(^84^96)(^85^96)(^88^97)(^8A=1)(^86=2)]
[A(^82^99)(^84^9A)(^85^9A)(^88^97)(^89=1)]
[B(^82^9B)(^84^9A)(^85^9A)(^88^97)(^87^9C)]
[C(^82^9E)(^84^9F)(^85^9F)(^88^A0)(^8A=1)(^86=2)]

(82=URL)
(86=VisitCount)

Field definitions

(^82^91)

<(80=LE)
(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8C=1321438124485750)
(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-US:official&client=firefox-a)
(8E=chloroform - Google Search)
(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&ved=0CByQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U3tA)
(90=1321438128376375)
(91=http://en.wikipedia.org/wiki/Chloroform)
(92=1321438131563875)
(93=en.wikipedia.org)
(94=Chloroform - Wikipedia, the free encyclopedia)
(95=http://myspace.com/)
(9E=http://facebook.com/)
(A0=facebook.com)
(A1=http://www.facebook.com/)
(A2=1321438191642000)(A3>Welcome to Facebook - Log In, Sign Up or Learn More)>
{1:^80 {(k^81:c)(s=9)[1(^8C=LE)]}
[2(^82^81)(^84^82)(^85^82)(^88^83)(^89=1)]
[3(^82^85)(^84^82)(^85^82)(^88^86)(^89=1)]
[4(^82^87)(^84^88)(^85^88)(^88^89)(^87^8A)]
[5(^82^8B)(^84^8C)(^85^8C)(^88^86)(^89=1)]
[6(^82^8D)(^84^8C)(^85^8C)(^88^89)(^87^8E)]
[7(^82^8F)(^84^90)(^85^90)(^83^8D)(^88^89)(^89=1)]
[8(^82^91)(^84^92)(^85^92)(^83^8D)(^88^93)(^87^94)]
[9(^82^95)(^84^96)(^85^96)(^88^97)(^8A=1)(^86=2)]
[A(^82^99)(^84^9A)(^85^9A)(^88^97)(^89=1)]
[B(^82^9B)(^84^9A)(^85^9A)(^88^97)(^87^9C)]
[C(^82^9E)(^84^9F)(^85^9F)(^88^A0)(^8A=1)(^86=2)]

(82=URL)
(86=VisitCount)

Field definitions

(URL^91)

<(80=LE)

(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla

(82=URL)

US:official&client=firefox-a)

(86=VisitCount)

(8C=1321438124485750)

(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-

US:official&client=firefox-a)

(8E=chloroform - Google Search)

(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&ved=0CByQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U3tA)

(90=1321438128376375)

(91=http://en.wikipedia.org/wiki/Chloroform)

(92=1321438131563875)

(93=en.wikipedia.org)

(94=Chloroform - Wikipedia, the free encyclopedia)

(95=http://myspace.com/)

(9E=http://facebook.com/)

Field definitions

(A0=facebook.com)

(A1=http://www.facebook.com/)

(A2=1321438191642000)(A3=Welcome to Facebook - Log In, Sign Up or Learn More)>

{1:^80 {(k^81:c)(s=9)[1(^8C=LE)]}

[2(^82^81)(^84^82)(^85^82)(^88^83)(^89=1)]

[3(^82^85)(^84^82)(^85^82)(^88^86)(^89=1)]

[4(^82^87)(^84^88)(^85^88)(^88^89)(^87^8A)]

[5(^82^8B)(^84^8C)(^85^8C)(^88^86)(^89=1)]

[6(^82^8D)(^84^8C)(^85^8C)(^88^89)(^87^8E)]

[7(^82^8F)(^84^90)(^85^90)(^83^8D)(^88^89)(^89=1)]

[8(^82^91)(^84^92)(^85^92)(^83^8D)(^88^93)(^87^94)]

[9(^82^95)(^84^96)(^85^96)(^88^97)(^8A=1)(^86=2)]

[A(^82^99)(^84^9A)(^85^9A)(^88^97)(^89=1)]

[B(^82^9B)(^84^9A)(^85^9A)(^88^97)(^87^9C)]

[C(^82^9E)(^84^9F)(^85^9F)(^88^A0)(^8A=1)(^86=2)]

(URL=http://en.wikipedia.org/wiki/Chloroform)

<(80=LE)

(8B=http://www.google.com/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla

(82=URL)

US:official&client=firefox-a)

(86=VisitCount)

(8C=1321438124485750)

(8D=http://www.google.com.au/search?q=chloroform&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:en-

US:official&client=firefox-a)

(8E=chloroform - Google Search)

(8F=http://www.google.com.au/url?q=http://en.wikipedia.org/wiki/Chloroform&sa=U&ei=rYvDTo3DCqOjiAfE_pzxDQ&

ved=0CByQFjAA&usg=AFQjCNGORl6--agKA23E0q9lkK4r5-U3tA)

(90=1321438128376375)

(91=http://en.wikipedia.org/wiki/Chloroform)

(92=1321438131563875)

(93=en.wikipedia.org)

(94=Chloroform - Wikipedia, the free encyclopedia)

(95=http://myspace.com/)

(9E=http://facebook.com/)

Field definitions

(A0=facebook.com)

(A1=http://www.facebook.com/)

(A2=1321438191642000)(A3=Welcome to Facebook - Log In, Sign Up or Learn More)>

{1:^80 {(k^81:c)(s=9)[1(^8C=LE)]}

[2(^82^81)(^84^82)(^85^82)(^88^83)(^89=1)]

[3(^82^85)(^84^82)(^85^82)(^88^86)(^89=1)]

[4(^82^87)(^84^88)(^85^88)(^88^89)(^87^8A)]

[5(^82^8B)(^84^8C)(^85^8C)(^88^86)(^89=1)]

[6(^82^8D)(^84^8C)(^85^8C)(^88^89)(^87^8E)]

[7(^82^8F)(^84^90)(^85^90)(^83^8D)(^88^89)(^89=1)]

[8(^82^91)(^84^92)(^85^92)(^83^8D)(^88^93)(^87^94)]

[9(^82^95)(^84^96)(^85^96)(^88^97)(^8A=1)(^86=2)]

(URL=http://en.wikipedia.org/wiki/Chloroform)

(VisitCount=2)

[A(^82^99)(^84^9A)(^85^9A)(^88^97)(^89=1)]

[B(^82^9B)(^84^9A)(^85^9A)(^88^97)(^87^9C)]

[C(^82^9E)(^84^9F)(^85^9F)(^88^A0)(^8A=1)(^86=2)]

Win her over



with Chloroform™

Software Designer Reports Error in Anthony Trial



Pool photo by Red Huber

Casey Anthony walking out of the Orange County Jail in Orlando, Fla., on Sunday with her lawyer Jose Baez, left.

By LIZETTE ALVAREZ
Published: July 18, 2011

MIAMI — Assertions by the prosecution that [Casey Anthony](#) conducted extensive computer searches on the word “chloroform” were based on inaccurate data, a software designer who testified at the trial said Monday.

Related

Times Topic: [Casey Anthony](#)

[Enlarge This Image](#)



The designer, John Bradley, said Ms. Anthony had visited what the prosecution said was a crucial Web site only once, not 84 times, as prosecutors had asserted. He came to that conclusion after redesigning his software, and immediately alerted prosecutors and the police about the mistake, he said.

The finding of 84 visits was used repeatedly during the trial

RECOMMEND

TWITTER

LINKEDIN

COMMENTS
(181)

SIGN IN TO E-MAIL

PRINT

REPRINTS

SHARE

S H A M E
DECEMBER 2
[WATCH THE TRAILER](#)



**Are my experience and knowledge
reliable?**

Topics ▾

News

In Depth

Reviews

Blogs ▾

Opinion

Shark Tank

Security

[App Security](#) | [Business Continuity](#) | [Cybercrime and Hacking](#) | [DRM and Privacy](#) | [Security Hardware and Software](#)[Home](#) > [Security](#)

News

Spyware case finally closed for teacher Julie Amero

Julie Amero was facing 40 years in prison

By Robert McMillan

November 21, 2008 12:00 PM ET

[Comments \(22\)](#)[Recommended \(33\)](#)[Like](#)

IDG News Service - The case against [Julie Amero](#) is finally closed.

On Friday, prosecutors reached a plea agreement with the former Connecticut schoolteacher who at one time faced up to 40 years in prison after being convicted of endangering minors. The charges stemmed from a 2004 incident in which a computer loaded with spyware displayed pornography to her students.

State prosecutors dropped four felony charges of "risk of injury to a minor" against her, with Amero pleading guilty to a disorderly conduct misdemeanor, according to the [Hartford Courant](#).

A jury convicted Amero of the felony charges in January 2007, but the presiding judge in the case, Hillary Strackbein, set aside that verdict five months later, essentially granting Amero a new trial.

Amero will pay a \$100 charge and have her Connecticut teaching credentials revoked, said [Sunbelt Software Inc.](#) CEO Alex Eckelberry, who led the team of computer investigators that analyzed the school's computer and concluded that Amero was innocent.

"The stress of this thing,... it just totally freaked her out," Eckelberry said Friday. "For four years, she's been sitting there with this thing hanging over her."

"It's disappointing that it wasn't dropped, but on the other hand I'm happy she

Mistaken interpretation based on incomplete theory of operation

- Testimony of Prosecution Forensic Expert
 - *“I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?”*

Mistaken interpretation based on incomplete theory of operation

- Testimony of Prosecution Forensic Expert
 - *“I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?”*
 - ***“The color, it’s red.”***

Mistaken interpretation based on incomplete theory of operation

- Testimony of Prosecution Forensic Expert
 - *“I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?”*
 - ***“The color, it’s red.”***
 - *“And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?”*

Mistaken interpretation based on incomplete theory of operation

- Testimony of Prosecution Forensic Expert
 - *“I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?”*
 - ***“The color, it’s red.”***
 - *“And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?”*
 - ***“That indicates that that link was actively clicked on and you were then sent to that page.”***

Mistaken interpretation based on incomplete theory of operation

- Testimony of Prosecution Forensic Expert
 - *“I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?”*
 - ***“The color, it’s red.”***
 - *“And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?”*
 - ***“That indicates that that link was actively clicked on and you were then sent to that page.”***
- Independent analysis identified:
 - The link was red because it was authored that way

Presenting assumptions as fact

- Testimony of school IT Admin
 - *“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.” – IT Admin of school*

Presenting assumptions as fact

- Testimony of school IT Admin
 - *“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.” – IT Admin of school*
- Independent analysis identified:
 - Trial antivirus software (unlicensed & expired)
 - At least 3 months out of date

Incomplete investigation

- Testimony of Prosecution Forensic Expert
 - *“Did you examine the hard drive for spy ware, ad ware, viruses or parasites?”*
 - ***“No, I didn’t”***

Incomplete investigation

- Testimony of Prosecution Forensic Expert
 - *“Did you examine the hard drive for spy ware, ad ware, viruses or parasites?”*
 - ***“No, I didn’t”***
- Independent analysis identified:
 - Adware program “newdotnet” installed 12 Oct 2004

Over-generalise based on experience

- *Testimony of IT Admin regarding popups*
 - *“Is it possible to be in an endless loop of pornography?”*
 - *“I’ve never seen that, so I would have to say probably not.”*

Over-generalise based on experience

- *Testimony of IT Admin regarding popups*
 - *“Is it possible to be in an endless loop of pornography?”*
 - *“I’ve never seen that, so I would have to say probably not.”*

- Independent experts confirm:
 - Generally known as “popup bombs” or “mouse trapping”



**How is the judge to recognise
expertise?**

Computer expert ?

<bitchchecker> the timing of my pc is right

<bitchchecker> i even have dst

<bitchchecker> you banned me

<bitchchecker> amit it you son of a bitch

<HopperHunter|afk> LOL

<HopperHunter|afk> shit you're stupid, DST^^

<bitchchecker> shut your mouth WE HAVE DST!

<bitchchecker> for two weeks already

<bitchchecker> when you start your pc there is a message from windows that DST is applied.

<Elch> You're a real computer expert

<bitchchecker> shut up i hack you

<Elch> ok, i'm quiet, hope you don't show us how good a hacker you are ^^

<bitchchecker> tell me your network number man then you're dead

<Elch> Eh, it's 129.0.0.1

<Elch> or maybe 127.0.0.1

<Elch> yes exactly that's it: 127.0.0.1 I'm waiting for you great attack

<bitchchecker> in five minutes your hard drive is deleted

<Elch> Now I'm frightened

<bitchchecker> shut up you'll be gone

<bitchchecker> i have a program where i enter your ip and you're dead

<bitchchecker> say goodbye

<Elch> to whom?

<bitchchecker> to you man

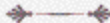
<bitchchecker> buy buy

<Elch> I'm shivering thinking about such great Hack0rs like you

*** bitchchecker (~java@euirc-61a2169c.dip.t-dialin.net) Quit (Ping timeout#)**

Friday, October 25, 2002

**Personal Ads
Jobs Wanted**
as low as \$.50 a day



SEE THE CAT? SEE THE CREDENTIALS?

Psychologist's Scam Gets his Pet
'Board-Certified'

BY MARK HANSEN

Zoe D. Katze has an impressive-looking set of credentials—Ph.D., C.Ht., DAPA. She has been board-certified by three major hypnotherapy associations and holds diplomate status in the American Psychotherapy Association.

Not bad for a 6-year-old house cat. And not even a pedigreed one at that.

But Zoe's not just any cat. She's Philadelphia psychologist Steve K.D. Eichel's cat. Eichel had a point he had been wanting to make about the proliferation of bogus credentialing organizations over the past 10 or 20 years.

So he decided to credential his cat.

To do that, Eichel first had to get his cat some credit, which turned out to be the hardest part of the process. The credit card company's agent initially asked for Zoe's Social Security number, Eichel says, but cheerfully relented when Eichel told him it wasn't readily available. Zoe was then added to Eichel's account as an authorized user.

To get Zoe her first credential, Eichel says, he simply filled out an "application for certification" on a lay hypnosis association's Web site and charged the fee to his credit card under Zoe's name. Since most lay hypnosis associations have reciprocity agreements, he says, it was a snap getting Zoe board-certified by two other credentialing organizations.

Eichel then decided to go for the gold: diplomate status in the American Psychotherapy Association, which, according to its own promotional literature, "is limited to a select group of professionals who, by virtue of their extensive training and expertise, have demonstrated their outstanding abilities in regard to their specialty."

The American Psychotherapy Association is affiliated with the American College of Forensic Examiners, whose credentialing practices were critically examined in the February 2000 issue of the *ABA Journal*. Eichel admits that he served briefly on the APA's executive advisory board, but says he quit in 1999 when he learned it was board-certifying people who did not have licenses or graduate degrees.

[Click here for ABA Journal
Online Classified Ads](#)

FEATURED AD OF THE WEEK:
Rubles for Russian Program at CSULB

Invest in the Russian Program at California State University, Long Beach.

To help establish an endowed chair in Russian Studies...[\(More...\)](#)

Search the ABA Classifieds:

[Click here to place an ad](#)



Zoe D. Katze, Ph.D., C.Ht., DAPA

Expertise to GO

In a hurry? Then order your forensic expert witness credentials—if you have the bucks—from entrepreneur Robert O'Block. But are they legitimate?

BY MARK HANSEN

Robert O'Block has come a long way since 1994, when he made \$40,000 a year as a professor at the College of the Ozarks in Point Lookout, Mo.

Now he's making a six-figure income as the executive director of the American College of Forensic Examiners, a Springfield, Mo.-based nonprofit organization that credentials forensic experts.

O'Block started in 1992 with \$500 of his own money and in the beginning ran a credentialing service single-handedly out of a spare room in his home. It has since grown into a 13,000-member organization with more than \$2.2 million in annual revenue.

He was paid nearly \$190,000

Mark Hansen is a legal affairs writer for the ABA Journal. His e-mail address is markhansen@staff.abanet.org.



ROBERT O'BLOCK

for his efforts in 1997, according to the most recent federal tax return available for the organization.

But O'Block, 48, apparently has made few friends and admirers along the way. One former associate calls him a con artist. And more than one describes his organization's credentialing process as a complete scam.

"He basically takes people's money and gives them a worthless piece of paper," says Robert Phillips, an Audubon, N.J., document examiner. "He's just in it for the money." Phillips claims he has reason to know. He says he resigned as chair of the organization's certification committee in 1993 after discovering that O'Block was issuing credentials to unqualified candidates behind the committee's back.

Many of the nation's leading forensic scientists don't seem to have





“XYZ isn’t forensically sound”

Forensically sound?

- RAM/Phone Acquisition
- Completeness of HDD acquisition
- TRIM



Conclusion

The path to forensic science

- Formalising the body of knowledge
- Peer reviewed techniques
- Rigorous adherence to scientific method and principles

- Not blind trust in tools



Dr Bradley Schatz | Forensic Computer Scientist
Director, Schatz Forensic

web: <http://schatzforensic.com.au/>

email: bradley@schatzforensic.com.au