COMPUTER FORENSICS CASE FILES

TALES OF MURDER,
PORN,
AND FORENSICS

TYLER HUDAK

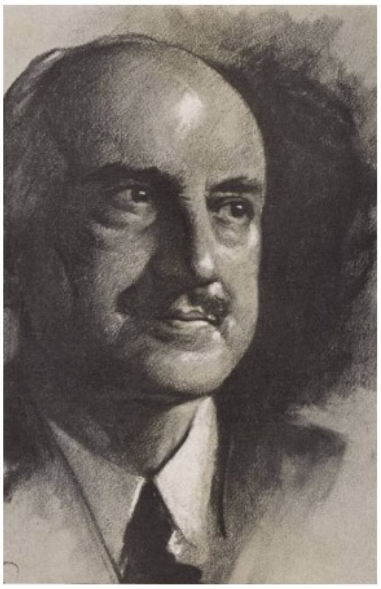
- Practice Lead, Incident Response at TrustedSec
- 20+ years in Info Sec
- Complete geek/nerd

securityshoggoth@gmail.com

@secshoggoth

Tyler.Hudak@TrustedSec.com

Disclaimer: Opinions are my own and not of the views of employer.



GEORGE SANTAYANA

THOSE WHO CANNOT REMEMBER THE PAST ARE CONDEMNED TO REPEAT IT.

TRIGGER WARNING

We will be discussing cases involving murder and porn.

No graphic images will be shown. (Obscene text is present)

If this may still disturb you, feel free to stop watching.

CASE #1:

THE BTK KILLER

Sources:
https://web.archive.org/web/20080529014836/http://www.trutv.com/library/crime/serial_killers/unsolved/btk/25.html
https://web.archive.org/web/20140714151807/http://www.scotsman.com/news/world/btk-strangler-resurfaces-after-25-years-1-519136
https://survivingbtk.weebly.com/
https://handwritinguniversity.com/crime/btkkiller/btk5.html
https://web.archive.org/web/20050305060631/http://www.kansas.com/mld/kansas/news/special_packages/btk/history/8321038.htm
https://web.archive.org/web/20050305025827/http://www.kansas.com/mld/kansas/news/special_packages/btk/
https://www.biography.com/news/btk-killer-meaning-dennis-rader-clues

WICHITA, KS 1974

January 15, 1974

4 members of the Otero family were murdered in their home

MORE MURDERS

April 4, 1974
Kathleen Bright murdered

March 17, 1977
Shirley Vian Relford murdered

December 8, 1977
Nancy Fox murdered

TOYING WITH THE POLICE AND THE LETTERS

- From 1977 to 1991 the BTK Killer murdered a total of 10 people
- Police made multiple attempts to catch him with no luck
- Killer contacted the media/police several times
  - Called 911 in at least one case to notify them of the murders
- One 1978* letter to TV station KAKE ended with the following:

"P.S. Since sex criminals do not change their M.O. or by nature cannot do so, I will not change mine. The code words for me will be... Bind them, toture them, kill them, B.T.K., you see he at it again. They will be on the next victim."

COLD CASE

- Case went cold until 30th anniversary of Otero family murders
- March 17, 2004 BTK contacts media again
- Begins communicating with police and media
- In one message sent to KAKE, BTK asked:

Can I communicate with Floppy and not be traced to a computer. Be honest.

FEB 16, 2005

- Later message contained a floppy disk
- This disk led to the capture of the BTK Killer

RANDY STONE – FORENSIC INVESTIGATOR

- Imaged the disk with Encase
- A deleted Word document was located on the disk
- Opened a copy of the document in Word and went to…

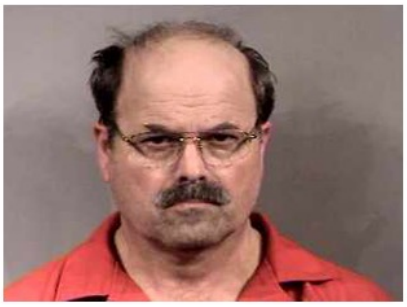
The metadata!

Metadata Information

"Christ Lutheran Church"
Last modified by: Dennis

DENNIS RADER – BTK KILLER

- Quick search led to Dennis Rader
- President of the church council
- Arrested shortly after



WHAT CAN WE LEARN FROM THIS CASE?

- Data is never deleted
- Look everywhere for evidence
- Metadata is powerful
- Learn when to ask for help

RANDY STONE ADVICE

Is there anything you would tell computer forensics/IR analysts today based on your experiences?

Resist the dark side. Staffing, caseload and our current analysis culture will encourage you to shortcut everything and to conduct exams in areas you aren't qualified (I've seen a lot of questions on list serves similar to "I know nothing about [topic] but now I'm investigating one. What should I do?")

CASE #2:

JULIE AMERO

https://web.archive.org/web/20090124121203/http://www.sunbelt-software.com/ihs/alex/julieamerosummary.pdf

JULIE AMERO

- Oct 19, 2004 – Substitute teacher in 7th grade
  - Computer started showing pornographic images to students
  - Presumed she showed them purposely to students
  - Charged with *Risk of Injury to a Minor*
- Jan 5, 2007 – Convicted, but sentencing delayed
  - Faced max sentence of 40 years

MARCH 6, 2007

Hartford Courant Ad - An Open Letter to Kevin Kane

3/6/07 The following open letter to Connecticut's Chief State Attorney appears in today's printed version of the Hartford Courant on page four.

The Julie Amero case has created outrage in internet forums and among computer experts all over the country. Briefly, Julie Amero was seven months pregnant and acting as a substitute seventh grade teacher in Norwich, Connecticut. She left the classroom briefly, and while she was gone some of her students used the class computer to surf the web. When she returned a stream of pornographic pop-up ads began to appear. She panicked and tried to stop the pop-ups but did not turn off the computer because she had been firmly instructed not to do so. She was charged with exposing her students to pornography and convicted in January. She now faces up to forty (40) years in prison.

Many computer experts believe that the stream of obscene pop-up ads were caused by malicious spyware and adware programs which users seldom know have infected their computers until too late - after they have done their evil work. It is most troubling that the computer had no firewall protection - apparently because a vendor's bill went unpaid - and that the prosecution did not make a search for spyware.

An excellent suggestion has been offered by Mark Rasch, former chief of the U.S. Department of Justice's cyber crime unit: "Find an independent investigator with no preconceived notions at all and find out what happened." We the undersigned computer science professors at Yale, UCONN, Wesleyan, Trinity, the University of Hartford, and the State Universities urge you to take up Mark Rasch's suggestion, and to delay sentencing Julie Amero until the investigator has filed his report.

Ad in Hartford Courant published by 28 CS professors

Asked for investigation due to perceived mistakes done on part of forensic investigators

March 21, 2007 - Multiple forensic analysts led by Alex Eckelberry of Sunbelt Software reviewed evidence and published opinion

https://web.archive.org/web/20090202163306/http://blog.state-v-amero.com/2007/03/06/hartford-courant-ad--an-open-letter-to-kevin-kane.aspx

TRIAL INFO

Key testimony from two individuals helped lead to the original conviction.

Norwich Public Schools
IT Manager

Norwich Police
Detective

Purposely not named within this presentation

BASIS FOR CONVICTION BY JURY

- Amero purposely clicked on the links showing porn
- She made no effort to hide it from the students

Fred Stephen Fox (jury) interview:

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

https://web.archive.org/web/20070217032225/http://blogs.pcworld.com/tipsandtweaks/archives/003741.html

EVIDENCE – EVIDENCE OF ACCESSES PORN SITES

Original Claim

- Sites from Temporary Internet Files directory were listed
- Firewall logs examined
- Used to show evidence of access to porn sites AND intent

Refuted Evidence

- Internet Cache does show evidence of access

BUT

- Does not show if it was accessed on purpose
- History file (index.dat) was not examined

https://julieamero.blogspot.com/

EVIDENCE – PORN LINKS WERE CLICKED ON

Q (Prosecution) : Are there any specific characteristics that may occur to a web page when you click on specific link?

A (Detective) : Yes. When you click on a link, again, links are Javascripted, you click on a link, it changes color and then you will get sent to that new address, that new page or site.

Q (Prosecution) : Detective, when you actively clicked on a link from the web page, what are one of the detail signs that it was an active click of a link on a web page?

A (Detective) : Again, it would be a different color, it will change colors.

Links on porn sites were a different color

↓

Therefore, they were clicked on

https://web.archive.org/web/20090124121203/http://www.sunbelt-software.com/ihs/alex/julieamerosummary.pdf

EVIDENCE – PORN LINKS WERE CLICKED ON

Q (Prosecution) : I will take your attention specifically to this, Female Sex Enhancers; anything different about that link as opposed to the other links?

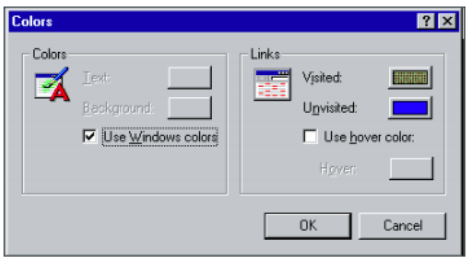
A (Detective) : The color, it's red.

Q (Prosecution) : And to your knowledge, based on your forensic examination of this machine, what may that indicate to you?

A (Detective) : That indicates that that link was actively clicked on and you were then sent to that page.

REFUTED EVIDENCE – PORN LINKS WERE CLICKED ON

- Links that have been previously visited – whether intentional or not – will change color.
- IE was configured to show visited links in green, not red.



- The HTML source of the page had code to color the font of that link red.
- That page was not found in any history or cache files.

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

EVIDENCE – TOOLS UTILIZED

Original Claim

- Detective only used ComputerCop Professional for analysis
- Used it to find HTML pages, images, and a keyword search

Refuted Evidence

- Program not widely used/accepted
- Cannot determine intent
- Cannot determine why data is there (e.g. from malware, user, etc.)
- No other tools/analysis were used

https://web.archive.org/web/20071011231942/http://www.networkperformancedaily.com/2007/01/the_strange_case_of_ms_julie_a_2.html
https://web.archive.org/web/20041014214030/http://www.computercop.com/prof.html

EVIDENCE – MALWARE ON THE SYSTEM

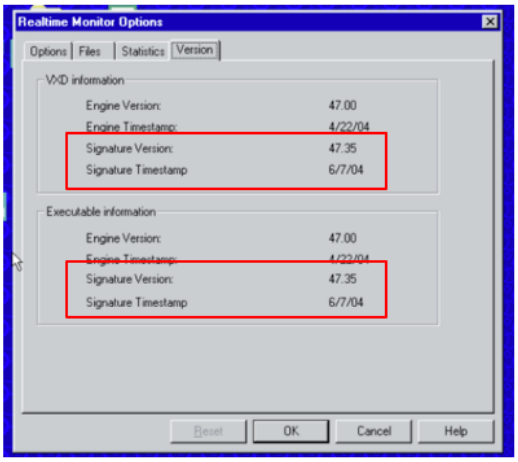
Original Claim

- InoculateIT Anti-virus was up to date
- Malware/Spyware was not capable of spawning pornographic popups
- "Endless loop" popups were not possible
- Malware was not on the system

Refuted Evidence

- AV was no longer supported by vendor
- Last signature update occurred June 2004 (4 months prior)
- Spyware is/was 100% capable of displaying porno popups

AV SIGS AND EXAMINATION



Trial Transcripts

Q (Defense) : Did you examine the hard drive for spyware, adware, viruses or parasites?

A (Detective) : No, I didn't.

NO SPYWARE???

- New analysis found that spyware program "newdotnet" on the system
- Installed 5 days prior to the event (Oct 14, 2004)
  - Installed when a Halloween screen saver was installed
  - "Free Offers from Freeze.com" suite also installed
- Program hijacks search results and sends to other sites
- Evidence that newdotnet hijacked search for "new hair styles" on Oct 19, 2004

Image attribution:
https://upload.wikimedia.org/wikipedia/commons/2/2e/Malware.png

RESULT OF INDEPENDENT EXAMINATION

- June 6, 2007 – Just threw out conviction and Amero granted a new trial
- November 21, 2008 – Original charges dropped*!

* Found guilty of misdemeanor disorderly conduct, paid $100

WHAT CAN WE LEARN FROM THIS CASE?

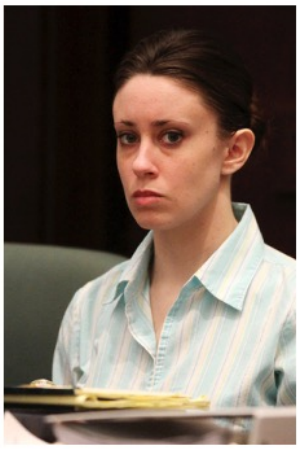
- Don't rely on one tool!
- Look everywhere for evidence
- Verify, and then verify again
- Assume nothing
- Ask for help

CASE #3:

CASEY ANTHONY

CASEY ANTHONY

- Accused of killer her daughter in 2008
- July 16, 2008 – Casey Anthony arrested
- Aug 2008 – Police restore Firefox history file from unallocated space
- May 24, 2011 - Trial begins
- July 5, 2011 - Acquitted

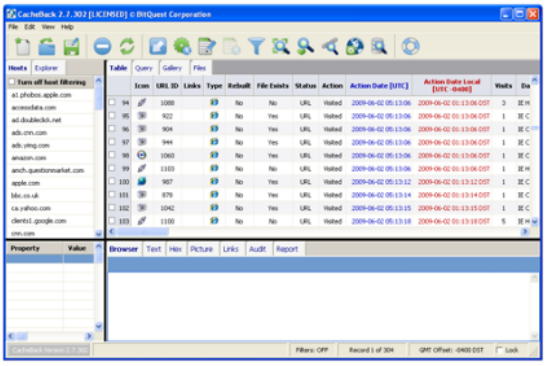


https://belkasoft.com/case_of_casey_Anthony
https://www.biography.com/news/casey-anthony-muder-trial-timeline-facts
http://content.time.com/time/nation/article/0,8599,2077969-1,00.html
https://www.csmonitor.com/USA/Justice/2011/0608/Casey-Anthony-trial-Internet-searches-for-chloroform-take-center-stage
https://www.scribd.com/doc/66346491/Casey-Anthony-Computer-Forensics

Forensic testimony
https://www.youtube.com/watch?v=acQ943U9J24&list=PLZQ8HI-rMK-6vqzUJchX9l9qkp2Prx7K7&index=29
https://www.youtube.com/watch?v=FXZjiZCJEiw&list=PLZQ8HI-rMK-6vqzUJchX9l9qkp2Prx7K7&index=30
https://www.youtube.com/watch?v=jLgecQyLRWw

JOHN BRADLEY FORENSICS TESTIMONY – JUNE 8-9, 2011

- Used CacheBack v2.8 RC2
- Extracted FF history data and gave report to police to analyze
- Testified on:
  - What CB report said
  - The report showed that www.sci-spot.com/chemistry/chloroform.htm was visited 84 times



https://web.archive.org/web/20110803181001/http://www.cfnews13.com/article/news/2011/june/259019
https://jessicaspraggins.wordpress.com/2011/06/09/the-hits-just-keep-coming/
http://caseyanthony-trial.blogspot.com/2011/06/bones-k-9-caseys-computers.html

Notes – June 8 2011 testimony

- This was performed on Anthony's PC; could not determine who performed the search just that the search was performed
- Det Sandra Osborne performed investigation of the system:
  - IE, Mozilla Firefox, and Safari were on the system
  - Two users were on the system – "owner" and "casey"
  - Recovered a complete history file for Firefox from unallocated space
  - Exported history file from system and gave to Sgt Kevin Stenger for analysis; she said he used NetAnalysis for analysis
  - A keyword search for "chloroform" was what led her to finding the deleted history file
- Sgt Kevin Stenger performed the following (NOTE: Video feed was cut so part if his testimony was not viewed by me)
  - Used NetAnalysis and Cacheback for analysis of Firefox history

    - Used both tools bc Cacheback was able to display correct dates (convert from UTC correctly)
    - Provided copy of extracted Firefox history file to John Bradley (creator of Cacheback) provided him with “a statement as to his findings”
- John Bradley – Developer of Cacheback
    - Dec 2009 asked by Sgt Stenger to look at the Firefox history file that was recovered
    - Stenger was not able to decode the whole file with CacheBack
    - Bradley modified CacheBack code to provide additional decoding of the file
    - Was shown a CacheBack report and asked to look at multiple entries
    - Some entries showed google searches for “chloroform” and “chloroform” (sic), access to chloroform Wikipedia page
    - Testified that the report showed that “http://www.sci-spot.com/chemistry/chloroform.htm” was visited 84 times

DEFENSE CONTRADICTION OF EVIDENCE

- NetAnalysis report found 8,878 records in the FF file; Cacheback found 8,557 records
- NetAnalysis report showed 1 visit to www.sci-spot.com/chemistry/chloroform.htm
- Multiple URLs were missing from CacheBack Report

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 FAIRED 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 >

This was brought up during Defense examination of detective on June 16, 2011

NetAnalysis report showed only 1 visit to http://www.sci-spot.com/chemistry/chloroform.htm
NetAnalysis report found 8,878 records in the file while CacheBack found 8,557 records

https://web.archive.org/web/20080709045508/www.sci-spot.com/chemistry/chloroform.htm

WHAT HAPPENED?

- Bug in CB – chloroform site only accessed once
  - Myspace accessed 84 times
- Detective knew about the discrepancy and did not disclose
- Neither tool parsed the FF history file properly (9,075 records)
- Bradley was asked to interpret results on the stand he had never seen


SiQuest

FOR IMMEDIATE RELEASE
Monday, July 11, 2011

Computer Evidence in the Casey Anthony Trial - A Post Mortem

CacheBack 3
ADVANCED INTERNET CACHE AND HISTORY ANALYSIS

In the recent case of the State of Florida vs. Casey Anthony, a recovered Firefox 2 history from Unallocated Space became the focal point of the State's case surrounding arguments of "premeditation". During the course of the trial, two different reports were tendered by members of the Orange County Sheriff's Department (OCSD). One was created using NetAnalysis dated August 2008. The other was created using CacheBack Version 2.8 RC2 in December 2009.

What came out at trial was a discrepancy between the two reports with regards to the Visit Count of 84 visits a "chloroform.htm" at "sci-spot.com". The NetAnalysis report was tendered by the Defense under Direct Examination of OCSD's lead forensic examiner. The CacheBack report had already been tendered by the State during Direct Examination of the developer of CacheBack (me) one week earlier.

As a result of this "discrepancy", a lot of confusion and presumptions have arisen. The first presumption is that NetAnalysis was the "correct report" and CacheBack was faulty. While admittedly true that CacheBack had some issues with the Visit Count and was missing some records, BOTH software products failed to fully parse the entire mork database file by some few hundred records.

On July 11, 2011, Digital-Detective.co.uk posted a public blog to discuss the discrepancy issue and provided a tutorial on the Mork file format in contrast to "the other tool". Since the article refers to the Casey Anthony trial and the issue at hand, the author might as well have simply said "CacheBack" and be straight about it. As a result, I feel compelled to set the record straight once and for all. I therefore need to shed some light on exactly what transpired that led to the issues at hand.

https://www.websleuths.com/forums/threads/lippman-says-cindy-george-may-sue-john-bradley-re-84-searches.145269/page-5#post-6938615
https://i.pinimg.com/originals/28/7b/03/287b03d10a4b0e57afaa227978f9a7ab.jpg
https://www.digital-detective.net/digital-evidence-discrepancies-casey-anthony-trial/
https://marshalla99.wordpress.com/2011/07/12/valid-conclusions/
https://web.archive.org/web/20110723223442/https://www.nytimes.com/2011/07/19/us/19casey.html

The press release was removed shortly after it was posted. However, I was able to reconstruct it from various online sources:

In the recent case of the State of Florida vs. Casey Anthony, a recovered Firefox 2 history from Unallocated Space became the focal point of the State's case surrounding arguments of "premeditation". During the course of the trial, two different reports were tendered by members of the Orange County Sheriff's Department (OCSD). One was created using NetAnalysis dated August 2008. The other was created using CacheBack Version 2.8 RC2 in December 2009.

What came out at trial was a discrepancy between the two reports with regards to the Visit Count of 84 visits a "chloroform.htm" at "sci-spot.com". The NetAnalysis report was tendered by the Defense under Direct Examination of OCSD's lead forensic examiner. The CacheBack report had already been tendered by the State during Direct Examination of the developer of CacheBack (me) one week earlier.

As a result of this "discrepancy", a lot of confusion and presumptions have arisen. The first presumption is that NetAnalysis was the "correct report" and CacheBack was faulty. While admittedly true that CacheBack had some issues with the Visit Count and was missing some records, BOTH software products failed to fully parse the entire mork database file by some few hundred records.

On July 11, 2011, Digital-Detective.co.uk posted a public blog to discuss the discrepancy issue and provided a tutorial on the Mork file format in contrast to "the other tool". Since the article refers to the Casey Anthony trial and the issue at hand, the author might as well have simply said "CacheBack" and be straight about it. As a result, I feel compelled to set the record straight once and for all. I therefore need to shed some light on exactly what transpired that led to the issues at hand.

The following is a timeline of events that took place since the beginning of the investigation through to and including the final days of the trial:

AUG 2008 - NetAnalysis was used to parse the Firefox 2 history file that OCSD recovered from Unallocated Space. This report listed 8,878 records. The actual mork file contained 9,075 records. This report was disclosed as evidence.

DEC 8, 2009 (16 months later) - While attending a CacheBack course in Orlando, members of the OCSD stated that NetAnalysis was NOT able to parse the FF2 file. They also cited issues with Daylight Savings conversion with the tool. CacheBack 2.8 at the time could only parse part of the file so I was asked to try and re-tool the function so that it could fully parse the FF2 file.

DEC 10, 2009 - I completed the updates to the best of my abilities at the time for CacheBack 2.8 RC2 and turned over the results to OCSD. I urged OCSD to manually validate select artifacts in the file since they had the Firefox 2 file format and decoding instructions from the CacheBack course Training Manual. I asked that any issues or concerns be brought to my attention immediately for investigation and/or correction. Since Firefox 2 history (mork) file format was already depricated, I felt at that time that no additional work was warranted on "that specific file format". In hindsight, I should have re-verified the work upon my return to Canada but that was

unfortunately not the case.

OCT 2010 - I was deposed as a witness in the case with the State and Defense counsels present. My line of questioning was completely restricted to my actions from December 2009. At NO time was I ever asked to "analyze" or "investigate" the history data or form any opinions. At NO time in the future was I also asked to analyze or investigate the history file. My sole purpose was to provide a "decoding function" for the investigators.

MAR-MAY, 2011 - I contacted the State Attorney's office on numerous occasions to verify what I was required to testify about at trial. I specifically inquired about whether I needed to examine the data, create any presentations for court, or if I required a laptop. I was told that I did not need to bring anything and that everything was already looked after. I was expected to only be on the stand for a few minutes - that was it.

JUN 8 & 9, 2011 - I was called to the stand by the State to testify about a CacheBack report that I had never seen before and the contents of which I had no foreknowledge of. This report was created by OCSD on June 3rd, 2011! I was only supposed to get up on the stand and say "I decoded the file" and that was it. Instead, I was tediously asked to read directly from the CacheBack report. Since OCSD officers had testified prior to me, and since the State was not affording me an opportunity to 'explain in simple terms' items like "URL" etc., I essentially was just a narrator and assumed that the jury was already educated by OCSD witnesses.

During my testimony, my attention was directed to a URL at "sci-spot.com" and I was asked to read aloud the Visit Count for that entry. As I stated in the courtroom, I said "According to the report...84 times". Personally speaking, a single "chloroform.htm" with a visit count of 84 seemed odd. But, since I did not have any other details about the investigation, and since I did not investigate the evidence, that's all I could say.

JUN 16, 2011 - The supervising OCSD computer forensic investigator (Sergeant) took the stand under direct examination by the Defense. He was shown two reports: the NetAnalysis report from August 2008 (which parsed only 8,878 records) and the CacheBack report, which parsed 8,571 records. OCSD was asked to point out the glaring differences between the Visit Count of 1 for the NA report and 84 for the CB report. In addition, "myspace.com" was missing from the CB report, as were other URLs. Rather than acknowledge this already known issue and address it there and then, the officer chose not to.

From a developer's perspective, this was an obvious "parsing error". By looking for a valid Visit Count attribute, CacheBack skipped over records until it found a valid Visit

Count marker. As I later determined (see below), FF2 infers the first visit count and thereby "omits" the Visit Count attribute altogether. So while terribly damaging, the actual correction to the problem was relatively easy, and obvious to me once I became aware of it.

JUN 16, 2010 (after his testimony) - I called the OCSD Sergeant about his testimony and inquired about the discrepancy. That's when he said that he KNEW about this discrepancy LONG AGO. When asked "What did you do about it?", he replied "that he 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". Despite the obvious and critical flaw in this thinking, he still knew that the NetAnalysis report was still in evidence with a visit count of 1.

According to the OCSD officer, this discrepancy was known LONG before trial. NO attempts were made to contact me, the developer of NetAnalysis or to validate it manually using any other combination third party tools. Validation of "select URLs" (e.g., chloroform) would have taken only 10 minutes. So at this point, there are 2 inconsistent reports before the court and nothing was done about it. Even the prosecutor didn't know.

JUN 16-19, 2011 - I advised the State Attorney of the problem(s) and liased with her and the OCSD officer. During the next 36 hours, I completely retooled the code in CacheBack and successfully matched the proper 9,075 records. An independent tool called "dork.exe" developed by the Mozilla developers corroborated my results. I also used EnCase Version 6 keyword search on the new record marker (a square open bracket) and verified the same results. CacheBack 3.7.11 was immediately released and I prepared an assortment of published results (for OCSD and the State prosecutor) in various file formats to make it easy to disclose and review.

This information was provided to the prosecution and to the OCSD in advance of the State's rebuttal, and the OCSD officer's second appearance (for the State). I even offered to fly down there overnight at my own expense to set the record straight and explain the discrepancy. Since the fate of woman's life could lay in this critical piece of information, I did everything in my power to remedy the situation, or at least mitigate the issue - once I became aware of it.

COMMENTS

Had OCSD informed me that NetAnalysis had indeed been able to parse the Firefox 2 history file in August 2008 (16 months earlier), I would have definitely asked for a copy of the results as a benchmark to my own work in December 2009. This

information was selectively omitted in my discussions with OCSD.

The OCSD had an opportunity and a responsibility to validate the results, in particular, the URLs that were deemed to be the most critical to the State's case. Had I been asked to revisit the results or aid in the examination of the results, the issues would have been discovered and corrected immediately.

In hindsight, I could have (should have) done more upon my return in December 2009 to further review the Firefox 2 parsing routine. Unfortunately, this is a valuable lesson learned. Despite Mork file format being depricated, we should have invested more time to review again the changes made in CacheBack 2.8 RC2.

While NetAnalysis and CacheBack were eventually updated to better parse the Firefox 2 file, neither product's reports tendered in the Casey Anthony trial were entirely correct. It is disappointing that NetAnalysis in this case was somehow held out to be otherwise.

I was not going to post anything herein because I believed that members of the forensic industry would qualify any suspicions by asking involved stakeholders about the matter - directly. Unfortunately and regretably, either for personal gain or for no other reason than to attempt discredit the CacheBack name, certain limited comments have found their way into public venues through posts and blogs that are completely subjective and misleading.

Like anyone other software development company, our software is developed by humans and we have endeavored to correct any and all issues immediately once they are discovered or reported. While we do our best to test, test, re-test and test some more, sometimes that isn't always enough.

My personal thanks to my good friend and colleague Shafik Punja of the Calgary Police Service for pushing me to come forward to define the issues and offer the true perspective on the issues.

CacheBack is a great tool for Internet investigations! I stand behind the product and I stand behind our customers. When a customer reports an issue, we're on it right away and we fix it right away, if required. The Casey Anthony Trial was a good experience for no other reason than to experience the American justice system and to be humbled in acknowledging that "one more test" is never a waste of time.

TO THE MEMBERS OF OCSD:
I am truly sorry that I was unable to refrain from discussing this issue in a less than

positive light. Collectively, we could have done things differently and I know we have all learned from this experience.

Respectfully,

John Bradley
CEO & Chief Software Architect

WHAT CAN WE LEARN FROM THESE CASES?

- Tools can be incorrect
- If it looks wrong, dig deeper
- Don’t presume results
- Be willing to say you don't know

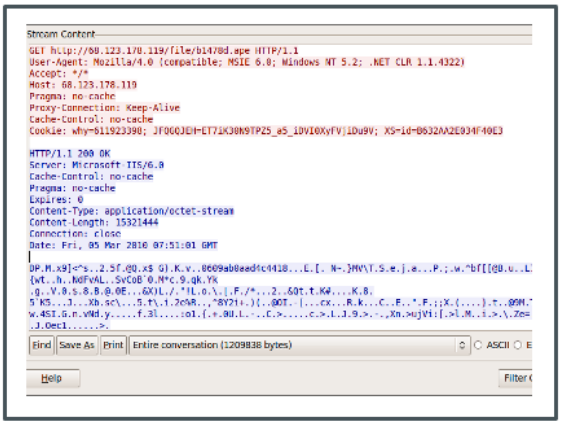
QUESTIONS?

securityshoggoth@gmail.com
@secshoggoth
Tyler.Hudak@TrustedSec.com

CASE #4:

APT

APT BACKDOOR



- Multiple versions existed
- Various C2 protocols used
  - HTTP, FTP, SSL
- Used a custom encryption in C2 traffic

REVERSE ENGINEERING GOALS

01

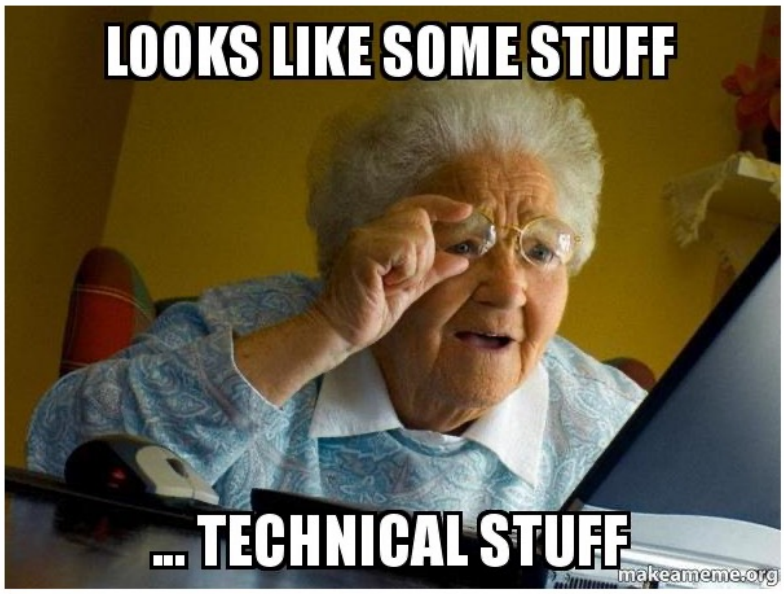
Break the Encryption

02

Determine commands available within

03

Resources were available that had already accomplished some of this


LOOKS LIKE SOME STUFF
... TECHNICAL STUFF
makeameme.org

INITIAL KEY GENERATION

Loop from 0-15

- Loop value multiple by itself + 1
- Increased by 32
- Mod by 256
- Value placed in byte array

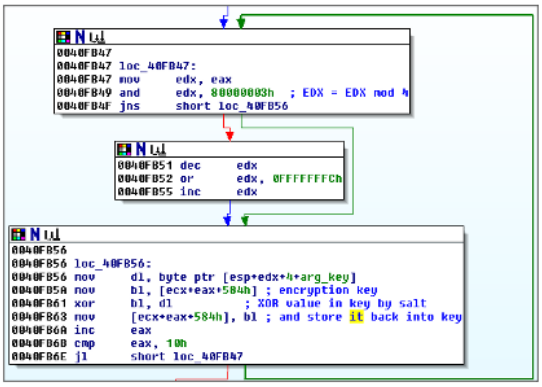
```
0040FAE2
0040FAE2 loc_40FAE2:              ; this loop will initialize the encryption key (0x584)
0040FAE2 mov     al, cl           ; see backdoor-key-init.pl for full code.
0040FAE2                          ;
0040FAE2                          ; for ($i=0;$i < 16;$i++) {
0040FAE2                          ;   $key[$i] = ((($i+1) * $i) + 32) % 256;
0040FAE2                          ; }
0040FAE2                          ;
0040FAE4 inc     al
0040FAE6 imul    cl
0040FAE8 add     al, 20h
0040FAEA mov     [edx+ecx+584h], al
0040FAF1 inc     ecx
0040FAF2 cmp     ecx, 10h
0040FAF5 jl      short loc_40FAE2
```

XOR Key:
0x20,22,26,2c,34,3e,4a,58,68,7a,8e,a4,bc,d6,f2,10

Always starts with the same initial key; no seed.

INITIAL KEY GENERATION #2

- Use a salt value of 0x8034ef12
- Loop thru key and XOR the bytes with the corresponding salt byte



XOR Key:

0xa0,16,c9,3e,b4,0a,a5,4a,e8,4e,61,b6,3c,e2,1d,02

Still getting a static key.

DATA ENCRYPTION

Data is "encrypted" using the 16-byte XOR key for every packet sent.

Data is a variable length.

Two random numbers are used to obfuscate data length and modify the XOR key.

Length Obfuscation:

```
Obf_Length = Rand1 ^ (Length - 4)
Rand1 = Rand1 + 291
```

XOR KEY MODIFICATION

Second random number generated: *rand2*.

↓

Copy first 2 bytes of XOR key as word: *key*.

↓

```
For i = 0 to 7:
    rand2 = rand2 – i
    key = key XOR rand2
```

↓

Copy modified word back into key.

↓

rand2 = rand2 - 1110

HUH?

- Backdoor creates a 16-byte encryption key
- Initial key is a static value
- Modifies the first two bytes of encryption key with a random value
- Obfuscates the length of the data with a random value

ENCRYPTED PACKET LAYOUT

Bytes	Explanation
0-1	Random number used to modify length
2-3	Obfuscated Length
4-5	Random number that modified the XOR key
6-?	Obfuscated Data (bytes 8-9 are the command)

We know how the length was obfuscated so we can reverse the algorithm to get it back

Only the first 2 bytes of the key are modified – the rest is static

We know how the first two bytes are modified and are given the random number used, so we can get the full key back!

PACKET DECODING

```
Packet Decoding #24:
        Time:                   Feb 1, 2010 06:09:38.338556 GMT
        Random Number:          19169   0x4ae1
        Data Length:            4       0x0004
        Random Number 2:        15724   0x3d6c
        XOR key: a0 16 c9 3e b4 0a a5 4a e8 4e 61 b6 3c e2 1d 02
        Command:        Heartbeat

        Decoded packet data:

        00 00           . . . . . . . .

Packet Decoding #27:
        Time:                   Feb 1, 2010 06:10:00.133617 GMT
        Random Number:          41      0x0029
        Data Length:            10      0x000a
        Random Number 2:        18467   0x4823
        XOR key: a0 16 c9 3e b4 0a a5 4a e8 4e 61 b6 3c e2 1d 02
        Command:        Execute:        shell


        Decoded packet data:

        02 00 73 68 65 6c 6c 0a         . . s h e l l .

Packet Decoding #29:
        Time:                   Feb 1, 2010 06:10:00.450814 GMT
        Random Number:          41      0x0029
        Data Length:            109     0x006d
        Random Number 2:        18467   0x4823
        XOR key: a0 16 c9 3e b4 0a a5 4a e8 4e 61 b6 3c e2 1d 02
        Command:        Execute:        Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>
```

HEARTBEAT SIGNATURE

In a heartbeat packet, the data is only the heartbeat command: 0x0000

What is 0 XOR any number?

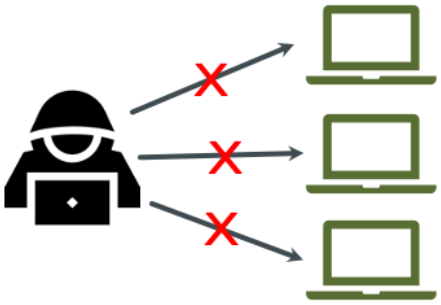
We can exploit the XOR key bug to create a static network signature for it.

```
alert tcp $HOME_NET any -> any $HTTP_PORTS
(msg:"UPS backdoor heartbeat"; dsize:8;
byte_test:2,=,51518,6;
flow:to_server,established;)
```

SO WHAT HAPPENED?!?

One night the heartbeat alert went off…the APT was in the network.

Using real time decoding, saw the attacker connecting to each system (and what commands they were typing)



As the attacker connected to one system, we'd take it down

One by one, the attacker tried to connect to systems

Soon they had no systems left and were kicked out

WHAT CAN WE LEARN FROM THIS CASE?

- Don't roll your own encryption!
- RE is powerful
- Visibility and instrumentation is key
- One person is not an IR **Team**