Poking the Wookie: The Chewbacca Defense in Digital Evidence Cases

Anjali R. Swienton, MFS, JD
Erin E. Kenneally, MFS, JD

AAFS February 24, 2005

Laying the Defense: Computer Forensics v. DNA Forensics

- DNA wars
  - dispute actus reus and mens rea by directly challenging the science and techniques applied to identification via biological artifacts
  - "I didn't do it because that's not my DNA"
- Wookie wars
  - dispute actus reus and/or mens rea by challenging techniques to identify via digital artifacts
  - "I didn't do it because those aren't my packets"

Contrast: Difference with Distinction

- **DNA evidence**
  - source not called into question
    - Don't debate whether Jack Doe's body reliably produces the DNA in his blood
    - Forensics won't change Jack's DNA into Jane's
  - very difficult to transplant DNA, biological set-up costs high
- **Digital evidence**
  - source reliability open to challenge: multiple connection points between Jack → computer → user account → data artifacts transmitted
    - Forensics can change the identifying, correlative, corroborative properties of data
    - My computer and data is not me
  - Digital set-ups more possible, probable, believable

ESSENCE OF ALL FORENSIC SCIENCES

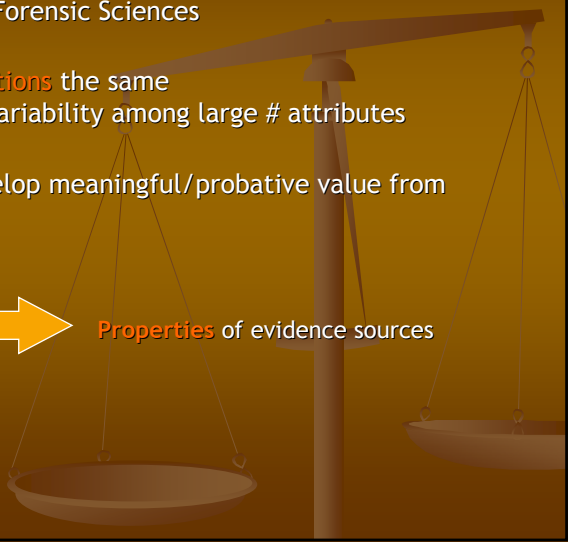
- Principles applied to the
  - Detection,
  - Collection,
  - Preservation,
  - Analysis

  of evidence to ensure its admissibility in legal proceedings

Computer Forensics & Digital Evidence: The 'New' Kid on the Block

- Compare to established Forensic Sciences
  - Fundamental assumptions the same
    …start with intense variability among large # attributes
  - Advances aim to develop meaningful/probative value from variables
    - identifying
    - characterizing
    - correlative

    → Properties of evidence sources



(..Compare to DNA Forensics)

- Techniques to enhance the I/C/C properties :
  - more precisely
  - more accurately
  - faster/less time
  - requiring less evidence

- /ex/ Binary Data v. Biological Data
  - A/B/O typing --> rH factors --> DNA typing via RFLP --> DNA typing via PCR
  - Hash libraries (to ID data); File signature (match name & file type); Mirror imaging software

(...Compare to established Forensic Sciences)

- "What we observe is not Science, but Science's answer to our questions"
  - Question : ~~existence of evidence~~ ability to uncover & contextualize evidence
  - Challenge:
    - Where look ?
    - What technique to make apparent ?
    - Is it admissible ?

Analogize:

::

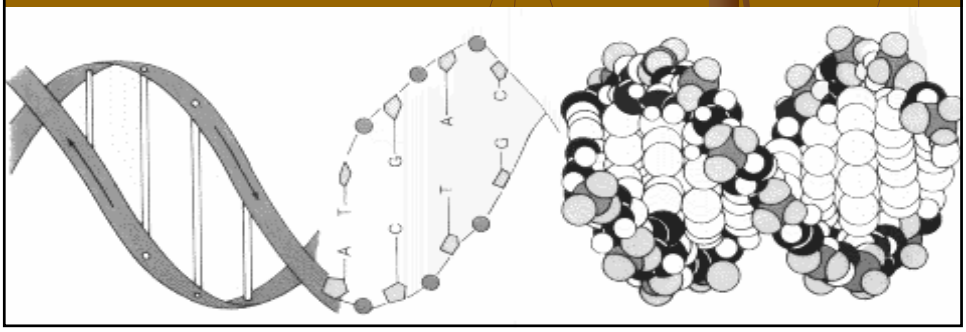
	DIGITAL EVIDENCE	DNA EVIDENCE
WHERE	Media (HD, CD, PDA, DVD) Location (server logs, IDS, firewall logs)	Clothing, cigarette butts, weapon Blood, saliva, hair shaft
WHAT TECHNIQUE	Software / Hardware to recover deleted data, file slack, unallocated space, swap files	PCR RFLP STR
ADMSSBLTY	Technology to recover deleted data → Accepted ↓ SW recovery (inclusiveness) → Challenged	DNA technology → Accepted ↓ STR technique → Challenged

DNA and Digital Evidence; Different Topics, Similar Issues

- Methodologies questioned as "novel"
- Technologies viewed as complex and beyond understanding of average person
- Disagreements within each field on issues of interpretation
- Suspicion of evidence tampering or misrepresentation

The DNA Wars, a Brief History

Although now widely accepted, it was not always so…



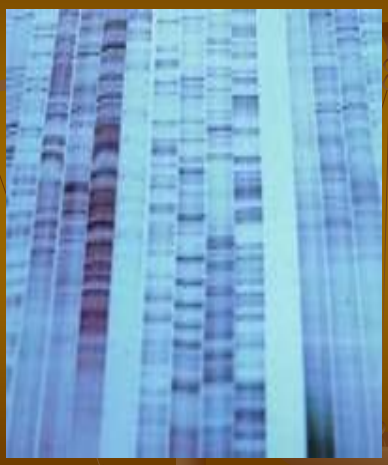
The DNA Wars

Disagreement over the admissibility of statistical calculations assigned to the genetic profiles used for human identification provided valuable lessons for later forensic disciplines

Methodology Challenges

- RFLP testing was subjected to *Frye* hearings when first proffered late 1980's
- Challenges to:
  - Methodology
  - SOPs
  - Whether mistake had been made in the instant case

This was expected

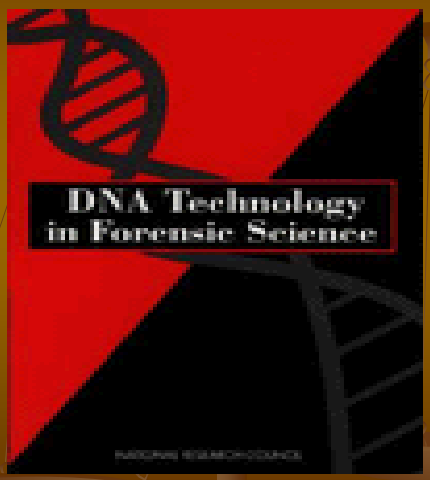


Validity - Counterarguments

- Methods used by DNA analysts are basic molecular biology techniques
- Used for decades for medical and disease research
- Only their *application* to human identification was new

Interim Solution: NRC I

- National Advisory Group convened by National Academy of Science to draft recommendations on testing and reporting to the field
- Issued report in 1992



General Acceptance

- Forensic DNA evidence was offered under the aura of expert testimony and was initially generally accepted
- Eventually, defense attorneys began to challenge it
- Found that there was disagreement over the methods used to calculate statistics assigned to genetic profiles

General Acceptance (cont'd)

- Statistics did not affect the actual methods used to generate the genetic profiles
- They affected the weight the results were afforded at trial
- Scientists agreed that they may have rushed to court too quickly, but only needed to reevaluate the calculations, not the testing itself

Controversy over Statistics

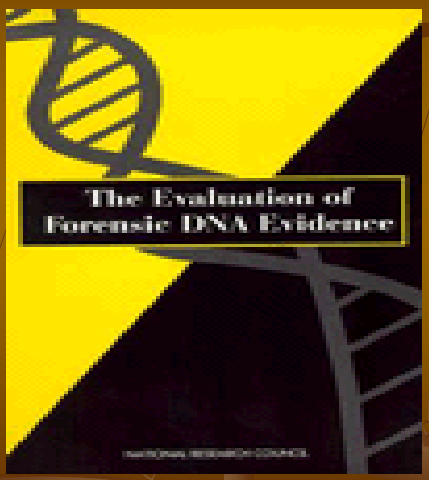
2 sides to the numbers:

- "big is big"
- calculation should be accurate/exact

Scientifically or statistically significant vs. legally significant

Solution: NRC II

- Convened to resolve issues of statistical calculations
- Issued report in 1996 with amended recommendations on calculating statistics to account for potential subpopulation variations



DNA laid the groundwork…

DNA

is grounded in basic principles of genetic Inheritance; is reproducible, verifiable, falsifiable

Digital Evidence

The new "black box" science, mysterious

Not understandable by the average person

Burden of proving and persuading Authenticity, Interpretation, Methodology and application

Forms of Challenges to DE

1. question whether the DE altered, manipulated, or damaged after created?
2. question reliability of program producing – mechanical & human operator
3. question identity of source of data/author

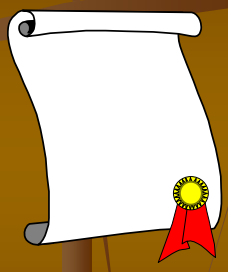
- **1) Authenticity**:
  - Absent specific evidence that tampering, mere possibility of tampering no affect authenticity of a computer record. Whitaker
  - Possibility alter data insufficient to establish untrustworthiness
    - US v. Glasser(11th Cir. 1985)
- **2) Methodology reliability**:
  - SOPs for data autopsies
  - /ex/ Bsnss Rcrds Exception used for documents
- **3) Interpretation**
  - Circumstantial evidence generally provides key

How are Courts Authenticating DE?

- General Rule for Computer Records : same as other records:
  - **witnesses to testify to the authenticity of computer records**
    - **no need not have special qualifications.**
    - **no need to have programmed the computer himself**
    - **no need to understand maintenance / technical operation**
  - **BUT,**
    - Precedent unclear
    - Fluid standards- this is changing as challenges mount

Contrast: Computer Forensics v. Traditional DNA Forensics

- **Qualifying Cyber Experts under Daubert/Kumho**
  - Shifting paradigm
    - What is 'general acceptance'
    - academic credentials
      - CS curricula short academic tradition
      - high academic credentials << commercial/industrial value
    - quantifying experience
      - no certification standards
      - diverse knowledge-base



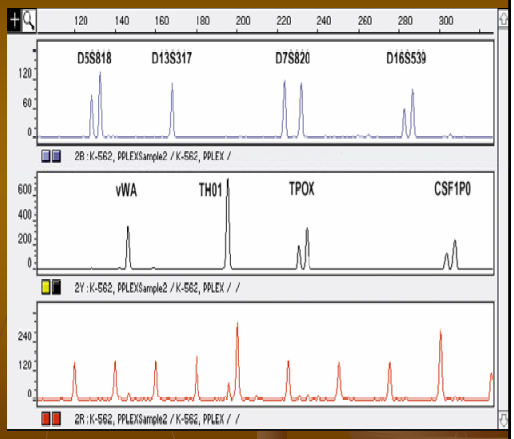
DNA- "New" Challenges

With the statistics issue resolved, and the testing methodologies becoming generally accepted, challenges moved toward individual cases:

- Analysts qualifications
- SOPs
- Potential mistakes in the instant case

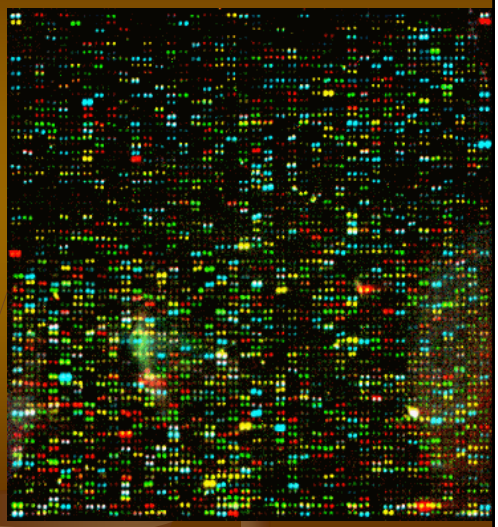
What qualifies as "new"?

- Technology evolves
- Scientific vs. legal definition of what is truly "novel"
- PCR testing was challenged each time new probes were available



PCR Testing cont'd

- As testing became more widespread, more money was put into research to make it better, faster, cheaper, more discriminating
- Each iteration of new tests were viewed by the legal community as "new" and therefore subject to new challenges



Primer Sequences, do they Matter?

- Clever legal argument set DNA testing back
- Commercial entities claimed IP rights, refused to disclose data
- Difficulty of trying to explain complex scientific processes to those with little or no scientific background
- Knowing you're right doesn't matter when someone else is ruling
- Eventually overcame (and rendered argument obsolete)

Authentication

How do you prove that the DNA detected and reported *actually* came from the event in question and was not planted, fabricated or misinterpreted by the analyst?

Interpretation

- In addition to questionable statistics, results can be misrepresented in testimony
- Terminology matters ('consistent with', 'cannot be excluded' vs. 'identity', 'it's him')
  - May mean the same thing to a scientist, but not to a fact finder…

Admissibility

Testimony can be wholly excluded if found to be overly prejudicial, or can be admitted with vigorous cross examination in hopes that the fact finder will afford it less weight.

How do we know we're getting our point across?

Verdicts

Science vs. Junk

- Difficulties – opposing experts willing to take the opposite stance, confuse the issue
- With complex issues like DNA and digital evidence, how is a judge to know which to believe?

Legal Mechanics of Chewbacca & DNA Defenses

- DNA Defense:
  * based on physical impossibility of Def's guilt

- Chewbacca Defense:
  * based on physical possibility that someone else committed bad act

  * conditions ripe for jurors to believe that "the computer did it"
    - relatively easy to manufacture and plant electronic
    - low barrier to entry: skill curve low; point & click tools; tools free and prevalent
    - can be easy to go undetected, anonymity is the default , wiping and hacking tools ubiquity and dual-use

Reality of the Digital & DNA Deniability Defenses

- **Trojan Horse Defense- Aaron Caffrey, U.K.**
  - charged with "carrying out a denial of service attack on the computers of the port of Houston, Texas on September 20, 2001"
  - DoS traced to a computer at Caffrey's home by U.S. police
  - Defense argument: a Trojan horse program opened back door for a hacker; Trojan gave control of the computer to real attacker who launched the DDoS attack; wiping tools removed any evidence of itself (edited the system's log files and then deleted all traces of the Trojan and real intruder)
  - Trojan horse never discovered ; Caffrey acquitted
- **Virus clears man of tax evasion and fraudulent returns**
  - Alabama accountant, Eugene Pitts, acquitted
  - Defense claim errors on tax return caused by a virus; not detected until after revenue investigators alerted him in 2000 of problems with his personal and corporate returns
  - (Side bar….. none of the returns he filed on behalf of his clients were affected by the virus)

<?> Implication for Rebutting Digital Defenses

- **Proving a Negative?**
  - Must the prosecution disprove the possibility the defense has raised beyond a reasonable doubt ??
  - **Traditional rebuttal tactics:**
    - Est. Def's motive to commit the crime and a lack of any plausible alternative suspects
    - Distinguish familiar crime fact finding: notions of reasonableness, probability, possibility have context against which to make judgments
      - jurors can rely on their common sense, knowledge of physical reality, human function and interaction; common sense grounded in empirical reality (own experiences)

Rebuttal Applied: Countering Chewbacca Defense

- **Playing it out:**
  (a) the defendant is charged with launching a denial of service attack;
  (b) he claims the attack was launched by a Trojan horse that was installed on his computer without his knowledge and as to the existence of which he was ignorant;
  (c) prosecution experts found no trace of a Trojan horse on his computer;
  (d) prosecution experts found he had installed a firewall and had up-to-date antivirus software on his computer;
  (e) defendant has formal training in computer science, has worked with computers since he was twelve years old and has been employed in the computer security field for the last five years; so, therefore,
  (f) he, not a Trojan horse, launched the denial of service attack

Rebuttal Applied: Countering Chewbacca Defense

1. Establish Defendant's Computer Expertise
- Show Def. knowledge about computers; digital threats; efforts to secure his computer

2. Negate the Factual Foundation:
show that malware was not responsible for the commission of the crimes charged in this particular case.

1. Via Technical Analysis
2. Via traditional tactics

3. Standard Operating Procedures
- Include initial malware detection methodology
  - shows investigator thoroughness
  - keep burden on Defense to prove otherwise
  - Decrease credibility… favor "probability" over "possibility"

…. The Future is Now

ANDREWS PUBLICATIONS — THOMSON WEST

Lawyer Who Missed Court Date Because of Spam Blocker Won't Be Sanctioned

By Jodine Mayberry
Medical Devices Litigation Reporter

A plaintiffs' attorney in a wrongful-death lawsuit, who missed a court date because his firm's spam blocking software automatically sidetracked the court's e-mail notice, has narrowly escaped being sanctioned for failing to appear at the scheduled status conference.

Attorney Jeffrey J. Stesiak, of Sweeney, Pfeifer, Morgan & Stesiak in South Bend, Ind., who represents the family of Ruthie Barnes, explained in his response to the order to show cause that he did not receive the electronically transmitted notice from the court that the status conference would be held Dec. 8, 2004. Stesiak said he left for a vacation in California Dec. 7 but if he had received the n

Stesiak said that with the help of the court's system administrator, he discovered t high, which blocked the e-mail notification from the court. After the security level

U.S. Magistrate Judge Christopher A. Nuechterlein accepted the explanation and were not warranted.

because his firm's spam blocking software automatically sidetracked the court's e-mail notice

* Don't have to offer evidence of technical controls on DNA to infer Def.'s involvement if their DNA found at crime scene…..

<?> What if it became reasonably possible for DNA to be transplanted like DE?

THANK YOU!!

Anjali Swienton
301-528-5050
aswienton@scilawforensics.com

Erin Kenneally
858-822-0991
erin@sdsc.edu

SciLaw Forensics, Ltd.