Software on the witness stand: what should it take for us to trust it?

Sergey Bratus & Anna Shubina, Dartmouth
Ashlyn Lembree, Franklin Pierce Law

Why we are here

- You are experts on which kinds of software can be trusted, and which kinds are not trustworthy
- Courts of law ponder these issues now, increasingly faced with software-generated evidence
- This is a community call to action

Outline

- What should we demand of a computer program/platform to regard its output as trustworthy evidence?
- Case study: computer-generated evidence in a "p2p file sharing" lawsuit
- Legal practice & precedent

Latest "p2p" cases:

- Purported evidence of wrongdoing is a long print-out from a computer program
- Generated autonomously, not via interactive human decision-making & action (e.g., an EnCase forensic session)
- Software written and run by a 3rd party company retained by the plaintiffs

"Robotic investigator"?

- Software is the only entity to "witness" alleged violations and produce an account of them for the court
- Software automatically & autonomously:
  - finds targets for investigation,
  - decides wrongdoing,
  - takes & records investigative actions.

This is not Sci-Fi!

- UMG v. Roy (this case study)
- many other RIAA cases across the US
  - http://recordingindstryvspeople.blogspot.com
- a new wave of cases in EU and the US?

Purported evidence

- ISP subpoenaed for : IP address at
  date hour:minute:second
  (and any e-mail and billing e-records,...)
- ISP disclosed: IP addr, account owner
- No MAC address present in records or
  "registered" with the ISP
- About 940 pages of PDF output

Purported evidence (1)

```
4/24/2007 5:49:32 AM EDT (-0400 GMT)    Initializing analysis of user 75.68.28.28:6346
(ArchiveID: 760387)
4/24/2007 5:49:32 AM EDT (-0400 GMT)    Rule Name: Rec 2 Gnutella c
4/24/2007 5:49:32 AM EDT (-0400 GMT)    System Build Version: 1.30.3560
4/24/2007 5:49:32 AM EDT (-0400 GMT)    Scanner Name: DC014 (agent ID 323)
4/24/2007 5:49:32 AM EDT (-0400 GMT)    Total Recognized Audio: 218
4/24/2007 5:49:32 AM EDT (-0400 GMT)    Total Recognized Video: 19
4/24/2007 5:49:32 AM EDT (-0400 GMT)    Total Recognized Software: 1
4/24/2007 5:49:32 AM EDT (-0400 GMT)    Total Recognized Documents: 1
4/24/2007 5:49:32 AM EDT (-0400 GMT)    Total Recognized Files Being Distributed: 480
4/24/2007 5:49:32 AM EDT (-0400 GMT)    ================================================

4/24/2007 5:49:44 AM EDT (-0400 GMT)    Connection Type: Direct

4/24/2007 5:49:44 AM EDT (-0400 GMT)    Attempting to match files
4/24/2007 5:50:04 AM EDT (-0400 GMT)    Found Match: Lionel Richie - Hello.mp3
4/24/2007 5:50:11 AM EDT (-0400 GMT)    Found Match: Happy Hardcore - Eminem - Without me
(techno remix).mp3
4/24/2007 5:50:12 AM EDT (-0400 GMT)    Found Match: Eminem - Drips.mp3
```

```
4/24/2007 6:14:52 AM EDT (-0400 GMT)    Successful download of Jay-Z - Vol.1 In My Lifetime - 11
- Real Niggaz.mp3

                                         First Packet Received: 4/24/2007 5:54:27 AM EDT (-0400
                                         GMT)
                                         First Download Packet Received: 4/24/2007 5:54:27 AM
                                         EDT (-0400 GMT)
                                         Last Download Packet Received: 4/24/2007 5:56:28 AM EDT
                                         (-0400 GMT)
                                         Last Packet Received: 4/24/2007 5:56:22 AM EDT (-0400
                                         GMT)
                                         Bytes Completed: 4,948,606
                                         Copying file: Jay-Z - Vol.1 In My Lifetime - 11 - Real
                                         Niggaz.mp3
                                         Logging Jay-Z - Vol.1 In My Lifetime - 11 - Real
                                         Niggaz.mp3
```

Purported evidence (2)

- This is a packet:

```
RECEIVED CONTENT PACKET: 4/24/2007 5:51:57 AM EDT (-0400 GMT)
Packet Source: 75.68.28.28
Packet Destination: xxx.xxx.31.78
Packet Data: (bytes 0-1459)
ÿû°•••••••i••••••
 Ã•••••¤•••••••4ƒ€••LAME3.87 (beta 1, Sep 27 2000)
 UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUULAME3.87 (beta 1, Sep 27 2000)
 UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
 UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
 UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
 UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
 UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
 UUUUUUÿû²•ÿ•ð••i••••••
 ••••••¤•••••••4€•••
 UUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUULAME3.87 (beta
 1, Sep 27 2000)
```

- This is a packet log:

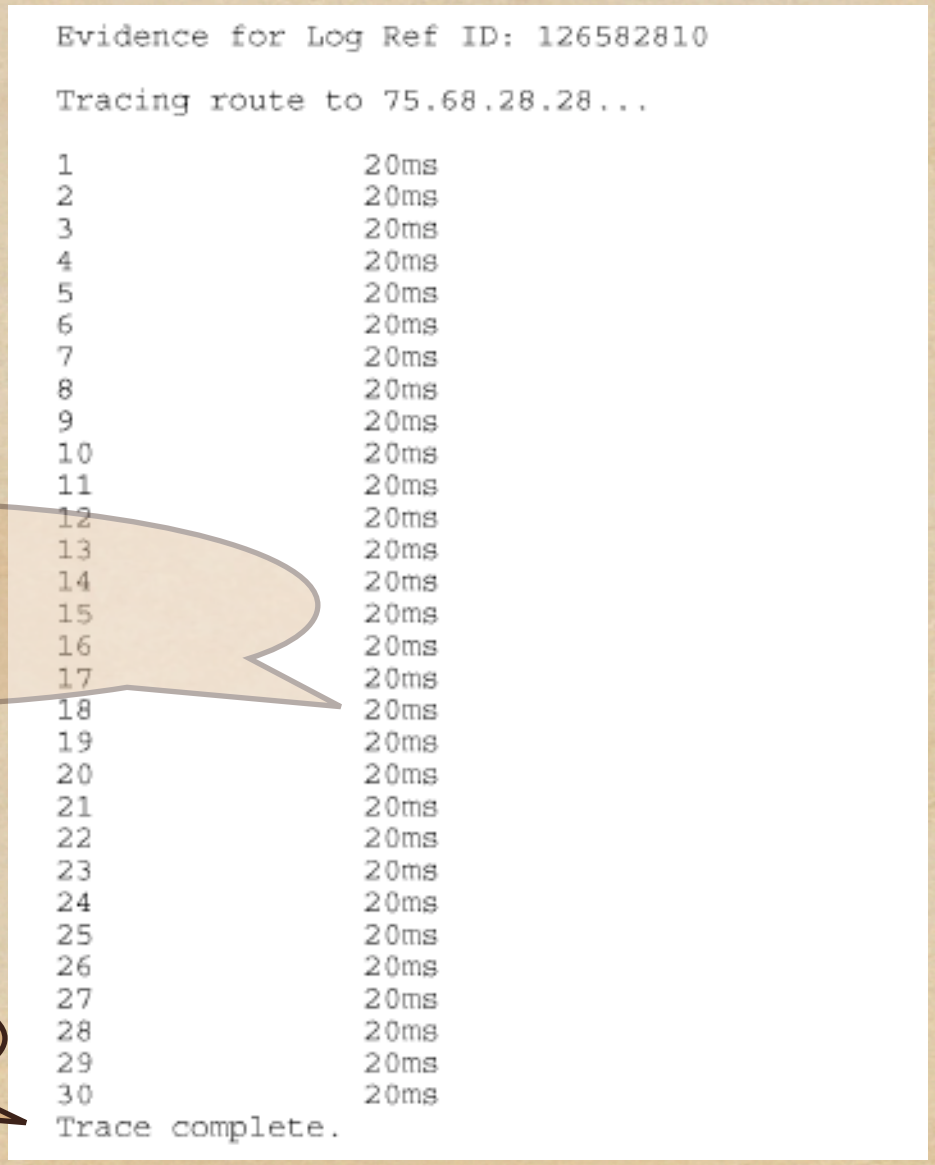
```
Title: Jay-Z - The Blueprint - 09 - Never Change.mp3

IP Byte Log for user at address 75.68.28.28 for file: Jay-Z - The Blueprint - 09 - Never
Change.mp3
4/24/2007 5:51:57 AM EDT (-0400 GMT), StartByte, 0, EndByte, 1459, TotalBytes, 1460
4/24/2007 5:51:57 AM EDT (-0400 GMT), StartByte, 1460, EndByte, 1778, TotalBytes, 319
4/24/2007 5:51:57 AM EDT (-0400 GMT), StartByte, 1779, EndByte, 3238, TotalBytes, 1460
```

Purported evidence (3)

- This is a traced network route:

"20 ms"

"Trace complete"



```
Evidence for Log Ref ID: 126582810

Tracing route to 75.68.28.28...

1                20ms
2                20ms
3                20ms
4                20ms
5                20ms
6                20ms
7                20ms
8                20ms
9                20ms
10               20ms
11               20ms
12               20ms
13               20ms
14               20ms
15               20ms
16               20ms
17               20ms
18               20ms
19               20ms
20               20ms
21               20ms
22               20ms
23               20ms
24               20ms
25               20ms
26               20ms
27               20ms
28               20ms
29               20ms
30               20ms
Trace complete.
```

Purported evidence (4)

```
Log for User at address 75.68.28.28:6346 generated on 4/24/2007 5:51:55 AM EDT (-0400 GMT)
Total Recognized Files Being Distributed: 480
------------------------------
Total Recognized Audio Files: 218
Total Recognized Video Files: 19
Total Recognized Software Files: 1
Total Recognized Document Files: 1
------------------------------

File Name: 02-busta_rhymes-touch_it__dirty_.mp3 (4,674,820 bytes)

File Name: 04-50_cent-the_ski_mask_way-whoa.mp3 (4,242,342 bytes)
```

```
Log for User at address 75.68.28.28:6346 generated on 4/24/2007 5:51:55 AM EDT (-0400 GMT)
Total Recognized Files Being Distributed: 480
------------------------------
Total Recognized Audio Files: 218
Total Recognized Video Files: 19
Total Recognized Software Files: 1
Total Recognized Document Files: 1
------------------------------


File Name: 02-busta rhymes-touch it  dirty .mp3
        Sha1: 2HVBST4FHJ3RCSAKI6RRRUSKQHLRCRW3

File Name: 04-50 cent-the ski mask way-whoa.mp3
        Sha1: STYQXPSR7WUOYONP2RGNZO73BA6KBW4M
```

Purported evidence (4)

xxx:	Purport	Description	Page count
054	"Download Info For <filename>"	ASCII printout of IP packets with IP addresses decoded	124
178	"IP byte log for user at address <IP> for <filename>"	One line per packet: "timestamp, StartByte, %d, EndByte, %d, TotalBytes %d"	785
963	"Shared file matches for user at address <IP:port>"	Filename, length, checksum	1
964	"RECEIVED PACKET <timestamp>"	ASCII printout of IP packet	9
973	"Initializing analysis of user <IP:port>"	Log of actions such as "Attempting to match files", "Choosing files to download", "Initiating download of <filename>"	4
977	"Tracing route to <IP>", "DNS Lookup for <IP>"	Failed traceroute	1
978	"Log for User at address <IP> generated on <timestamp>"	File name and SHA1	11
989	"Total Recognized Files Being Distributed"	File name and size	8

Table 1. Evidence materials in Roy case

How trustworthy is this?

- Software is notorious for bugs, even lethal ones (e.g., the RISKS digest); platforms have misconfigurations
- Software entrusted with such an important function must be held to special, higher standards of trustworthiness

Is software objective?

- Humans' testimony is not by default assumed to be impartial, objective, or trustworthy
- Cross-examination addresses biases and conflicts of interest, under oath
- Software merely implements behaviors designed by humans

"Illusion of infallibility"

- Long-standing court practice: trusting lab results/device tests/software evidence by default
- Popular perception of computer as a "machine", an "idiot savant"
- Computers assumed to inherently add trustworthiness to human activities

Courts & tech evidence

- In criminal cases, some recent steps to question technology:
  - State v. Chun (source code/device/operator review ordered by court)
  - Melendez-Diaz v. Massachusetts
- Civil cases lag behind
  - UMG v. Lindor (software evidence assumed "objective")

From the bench...

"The software, source code, or algorithm ... is irrelevant to ... whether the screen shots [software-generated evidence] accurately depict copyright violations [internet account activity] that allegedly took place"

- Judge Levy (E.D.NY) in UMG v. Lindor

From the bench...

"Release of this information [source code, algorithm, technical data, or detection method] would harm [software vendor] with no discernible benefit to defendant's case"

- Ibid.

The reality

- Software is perfectly capable of expressing bias and conflict of interest:
  - in algorithm (e.g., bias to over-detect, no awareness of context)
  - in code (logic flaws, contrary to programmer's belief)
  - in configuration (network view, timing)
- Speed camera conspiracies ("short yellow")
  - Italy: 70 municipalities, 63 municipal police, 39 govt officials, managers of 7 companies

Confrontation Clause

- Constitutionally, criminal defendants have the right to confront accusers (U.S. Const. Amend. VI)
- If software is the accusing agent, what should the defendant be entitled to under the Confrontation Clause?
  - source code, machines, operators, makers of machines?

Testimonial or not?

- Some material is testimonial (involves a human making a solemn affirmation of some fact), some isn't
- Is output of software testimonial?
  - is it signed by a human?
  - what technological measures should be mandated to assure software/ platform trustworthiness?

Our position

- Interpret Daubert criteria to mean:
  - for transient events (such as Internet actions), methodology and software must be pre-verified & pre-tested by independent experts (cf. Crawford v. Washington)
  - (for non-transient events, apply several competing methods, compare results - requires aggressive defense)

Our position

- Code of software used as witness must be made available for detailed examination by experts
- Code must be measured and attested
  - A case for trusted hardware
- Platform configuration must be examined, measured, and attested

Beyond the algorithm

- Time synchronization is an open problem!
  - Accurate timeline is forensically critical
  - All timestamp sources must be attested (both at the ISP and the plaintiff)
- Network configs must be attested:
  - DNS resolver, Whois server, Routes, network paths

Research Challenges

- Can the software be relied on to operate as expected? (CS & security experts)
- Trier-of-fact perceptions -- Do judges and juries believe software to be accurate, unbiased, and impartial?
- Witnesses are sworn in and cross-examined to expose biases & conflicts -- what about software as a witness?