Acoustic Intrusions

Fun and games in audioland

HD Moore

RAPID7

HELLO
my name is

HD Moore

RAPID7

Chief Security Officer

metasploit®

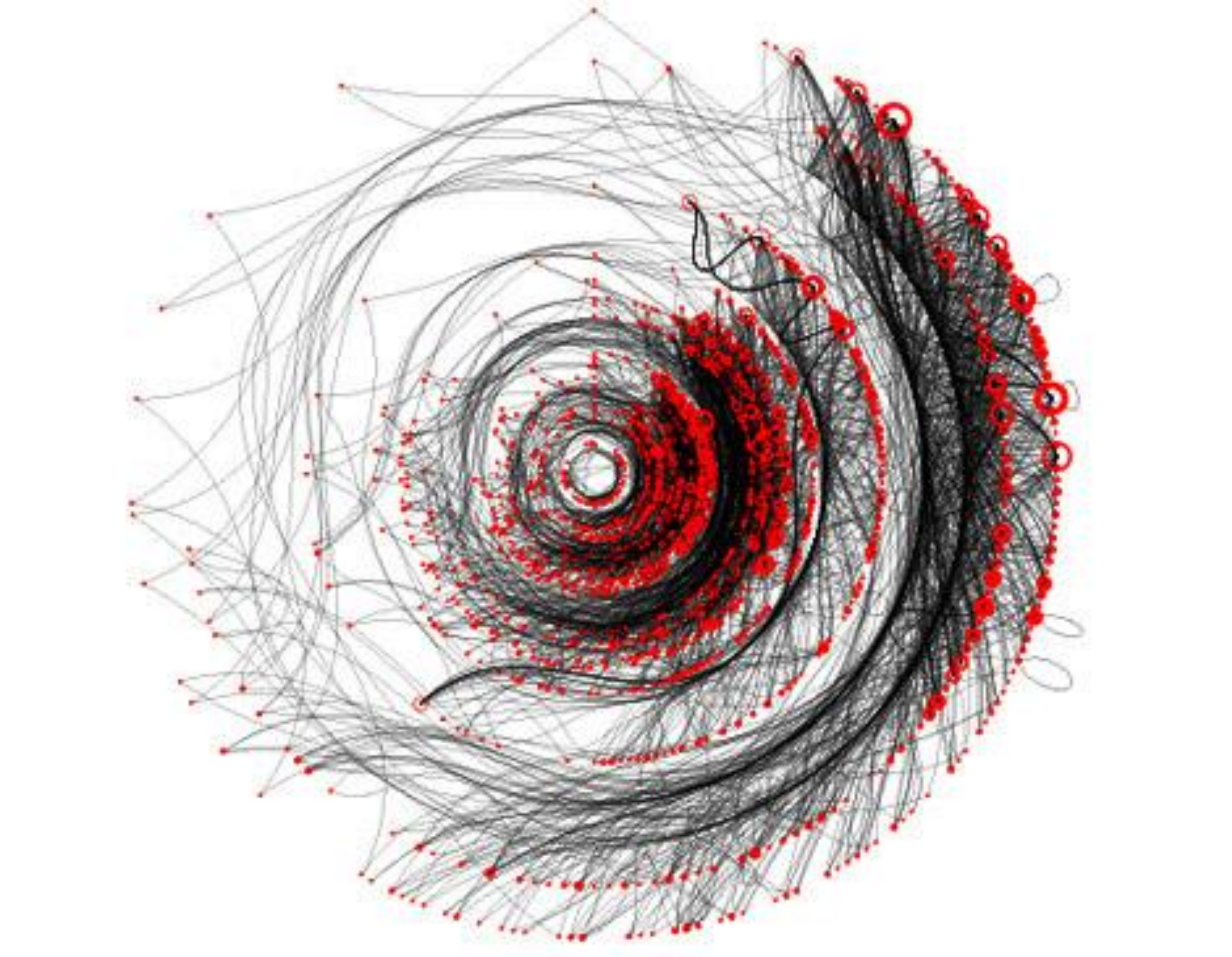
Founder & Chief Architect

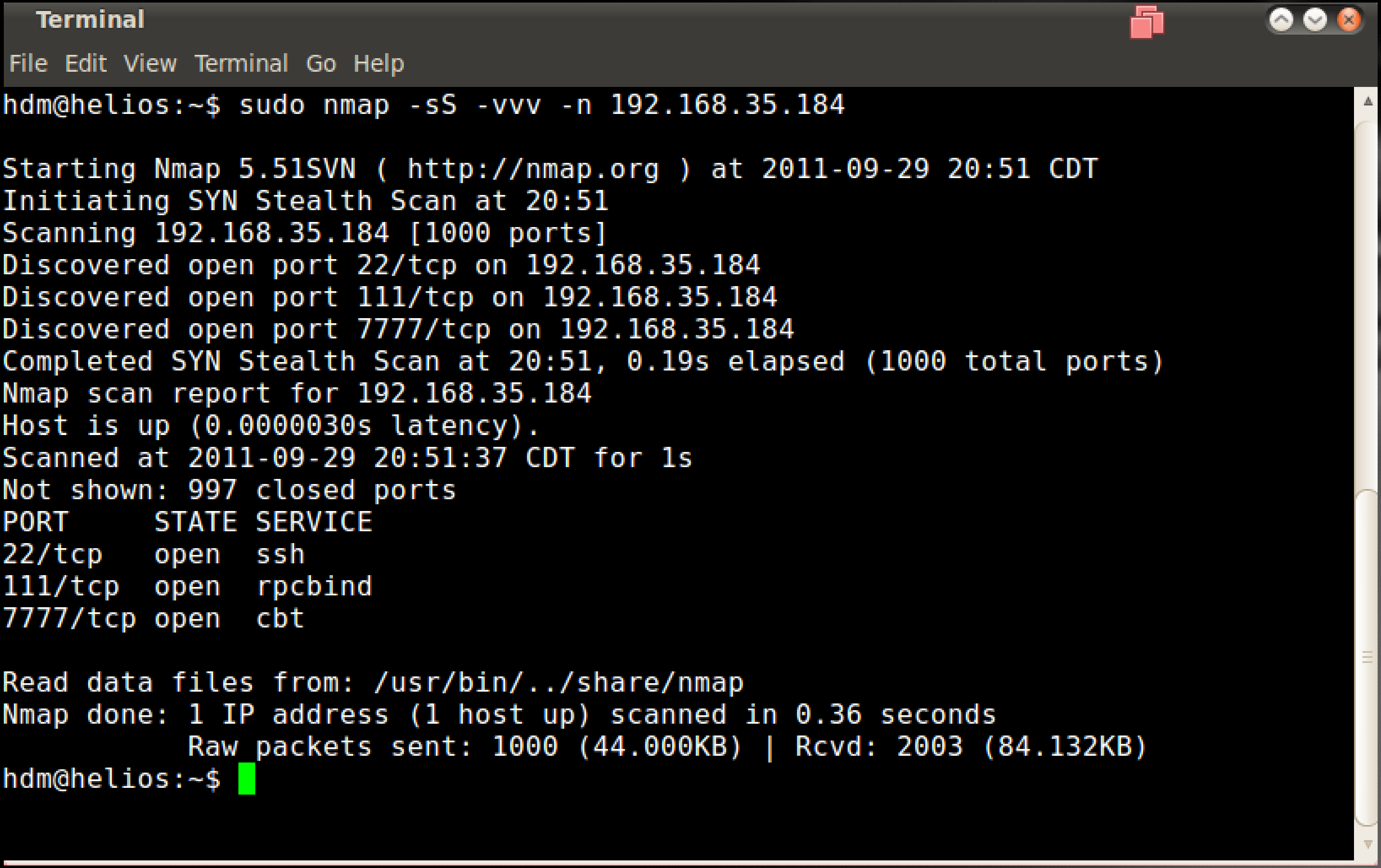
WE

♥

DATA

?





```
hdm@helios:~$ sudo nmap -sS -vvv -n 192.168.35.184

Starting Nmap 5.51SVN ( http://nmap.org ) at 2011-09-29 20:51 CDT
Initiating SYN Stealth Scan at 20:51
Scanning 192.168.35.184 [1000 ports]
Discovered open port 22/tcp on 192.168.35.184
Discovered open port 111/tcp on 192.168.35.184
Discovered open port 7777/tcp on 192.168.35.184
Completed SYN Stealth Scan at 20:51, 0.19s elapsed (1000 total ports)
Nmap scan report for 192.168.35.184
Host is up (0.0000030s latency).
Scanned at 2011-09-29 20:51:37 CDT for 1s
Not shown: 997 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
111/tcp  open  rpcbind
7777/tcp open  cbt

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
           Raw packets sent: 1000 (44.000KB) | Rcvd: 2003 (84.132KB)
hdm@helios:~$
```

Information retrieval

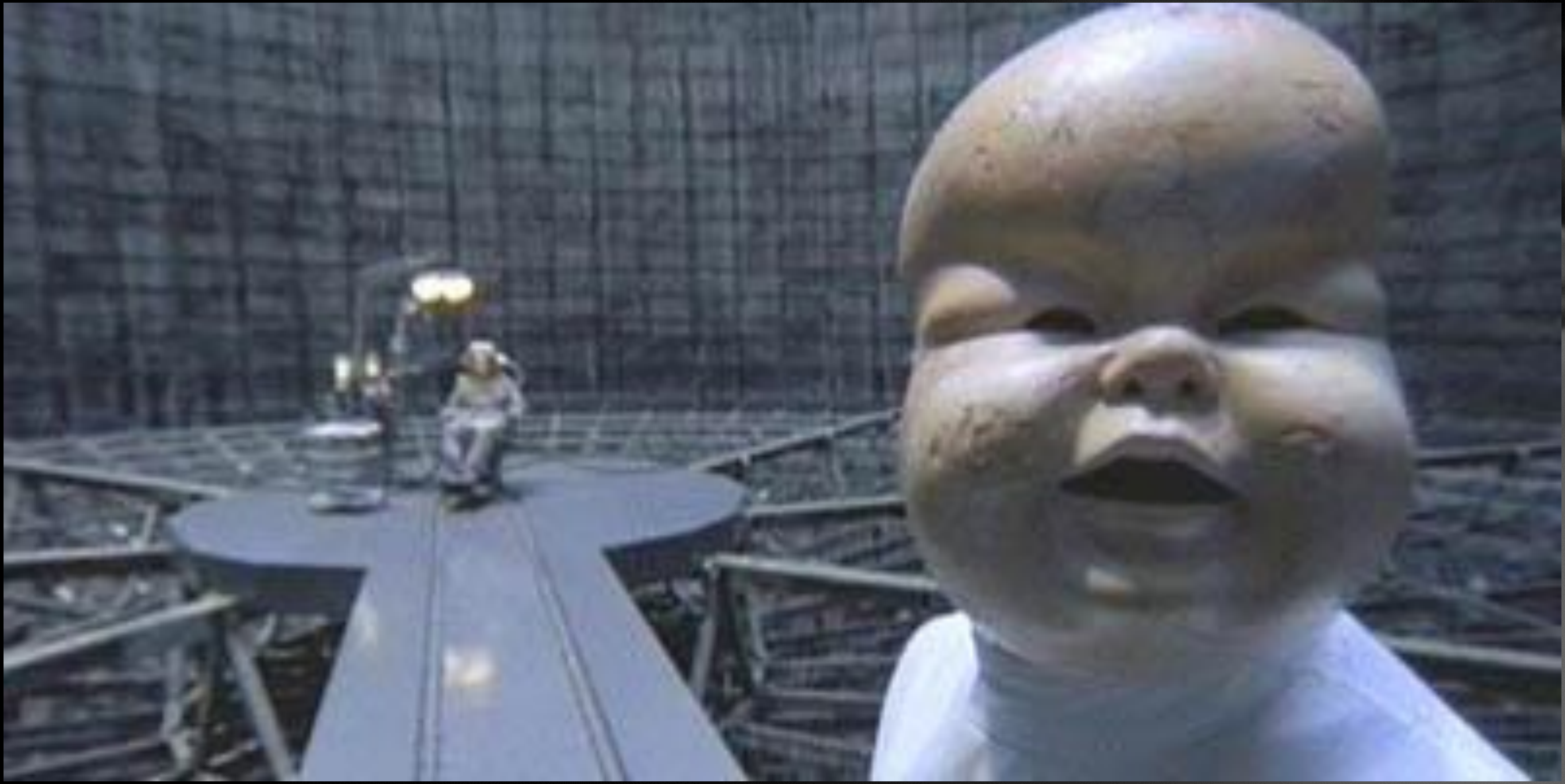
- Information security is all about data collection
- Network range discovery, user identification
- Vulnerability assessments, scanning, sniffing
- Penetration testing, post-exploitation

Three approaches to data gathering

Find a copy already stored somewhere else

Get close to the target and monitor for it

Actively extract it from the target systems



Computer data is easy to collect

- Great searchable public information resources
- Stable monitoring tools for networks
- Mature network scanning tools
- Awesome frameworks (PTES)

Computers are just one avenue

- Data is printed, trashed, scribbled, and faxed
- Shouted by cell phone users at the airport
- Those convenient trash cans near ATMs
- Exposed constantly as background noise

Capturing data isn’t the challenge

- Cataloging, sorting, and indexing is the issue
- OCR is useful in specific cases but not most
- Voice recognition is still just plain awful

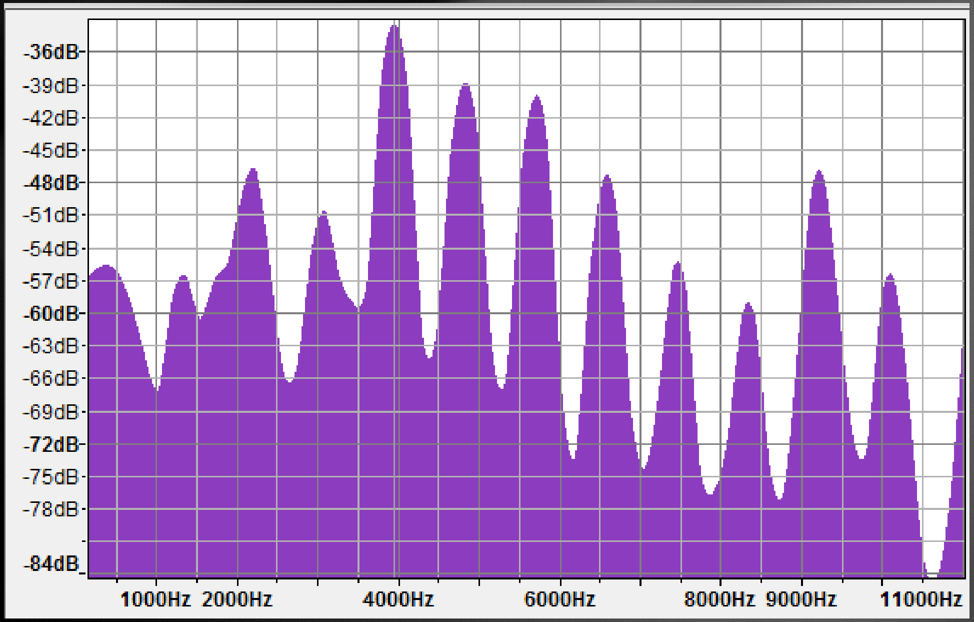
Data leakage through audio

- Moving beyond plain old eavesdropping
- Fingerprint computer OS and applications
- Identify phone vendor via ringtones
- Hang out in the lobby, record, and wait

Las Vegas hotel safe

- Different tone for every touch pad key
- Clearly audible from outside the room
- Recorded through the wall via iPhone

```
#0 = 3962hz  #5 = 4109hz
#1 = 5108hz  #6 = 4352hz
#2 = 3462hz  #7 = 3307hz
#3 = 4701hz  #8 = 4876hz
#4 = 4984hz  #9 = 5189hz
```



Telephones

- Phone systems provide a wealth of information
- Modems, faxes, and interesting gear
- Interactive voice response systems
- Detailed employee directories
- DTMF codes on forwarders
- Entry points into the PBX
- Voicemail boxes
- Dial tones

Voicemail boxes

- Expose huge amounts of data
  - Name
  - Title
  - Cell #
  - OOO

- Identify targets for phishing & impersonation
- Determine organization relationships
- Hijack unused or insecure boxes
- Access stored voicemail

Completely ignored by most audits

- Lack of awareness about the risks of attack
- Rarely covered by compliance regulation
- Not something most auditors know
- Few commercial drivers
- Limited set of tools

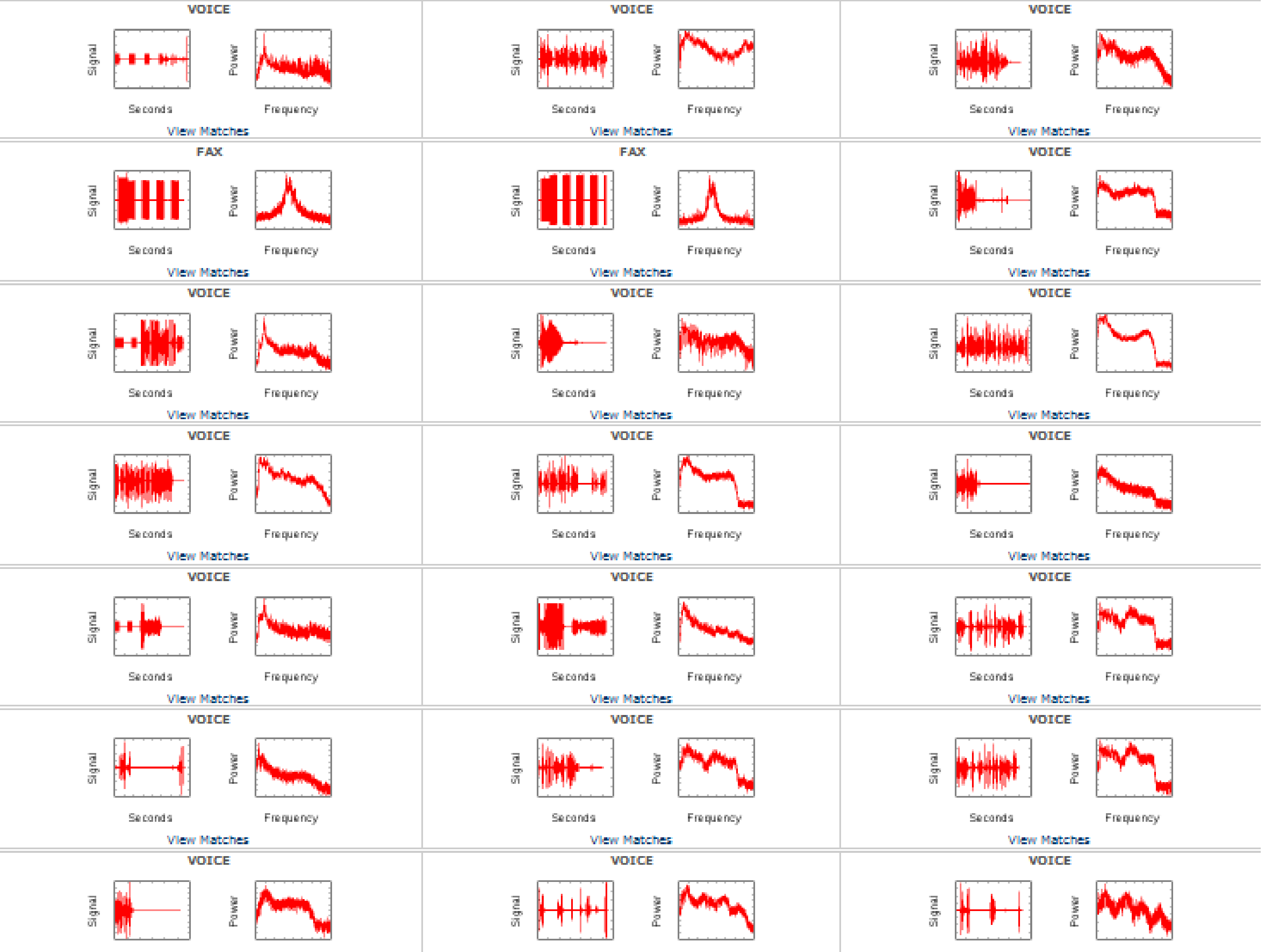
- Lets fix that

waRvox

2.0.0

Re-Introducing WarVOX

- WarVOX is a Ruby on Rails web application
- Makes lots of phone calls over VoIP (IAX2)
- Scales to hundreds of concurrent calls
- Records a set length of audio data
- Post-processes the raw audio
- BSD licensed

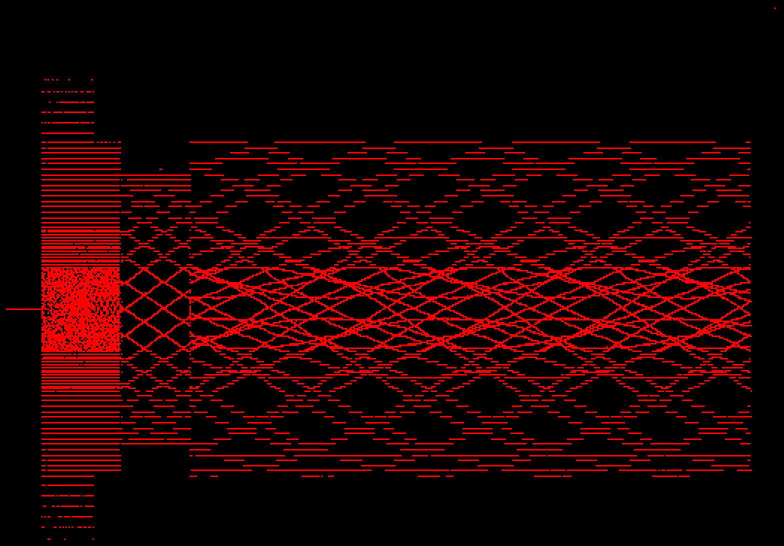


VOICE	VOICE	VOICE
FAX	FAX	VOICE
VOICE	VOICE	VOICE
VOICE	VOICE	VOICE
VOICE	VOICE	VOICE
VOICE	VOICE	VOICE
VOICE	VOICE	VOICE

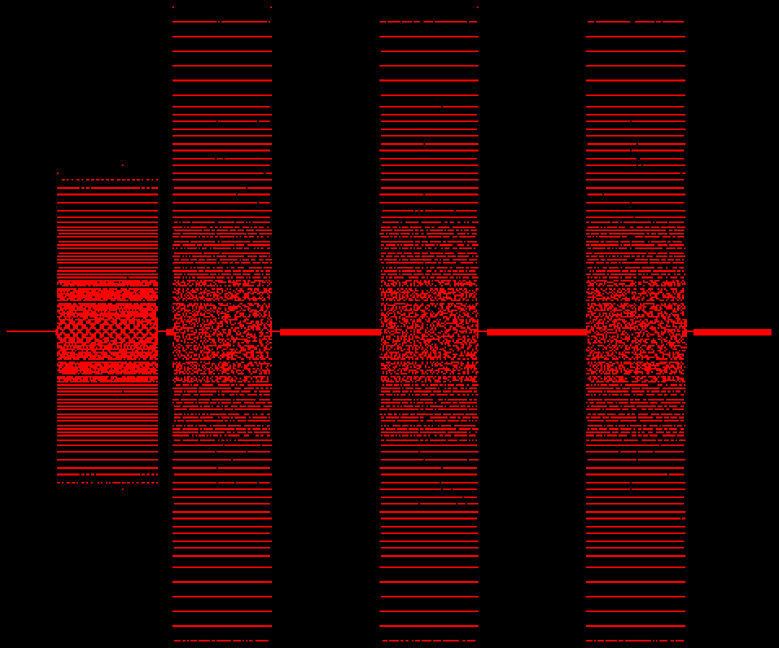
Wardialing for modems in 2011

- Modem hunting used to be incredibly slow
- WarVOX dials over 10,000+ numbers/hour
- However, only ~4% of lines are modems
- Identified through frequency analysis
- Redial with a modem for banners

MODEM

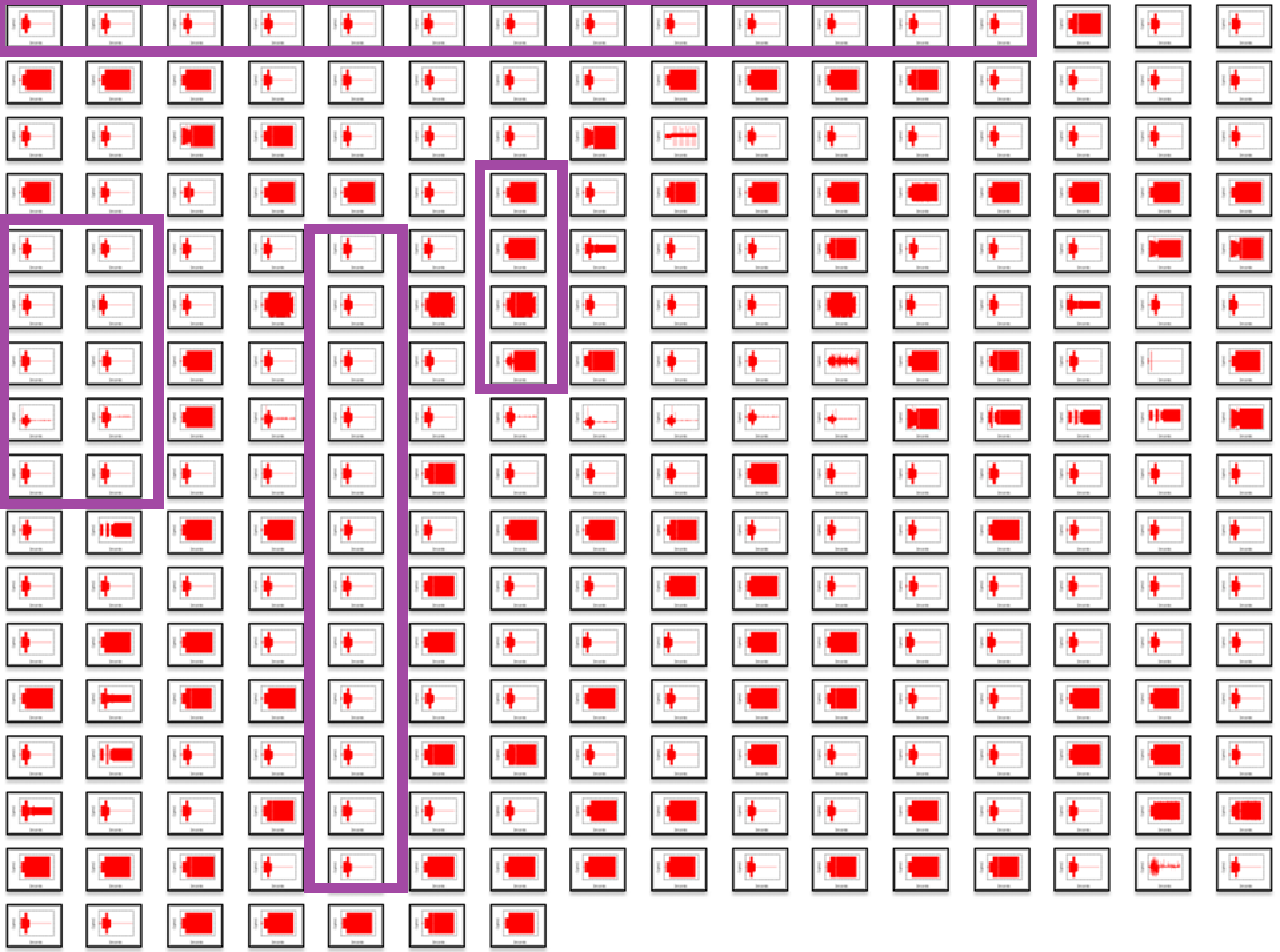


FAX



Modems can be fingerprinted

- Identify specific hardware vendors by audio
- Dialed 400+ ISP lines and plotted waves
- Visual grouping matches hardware



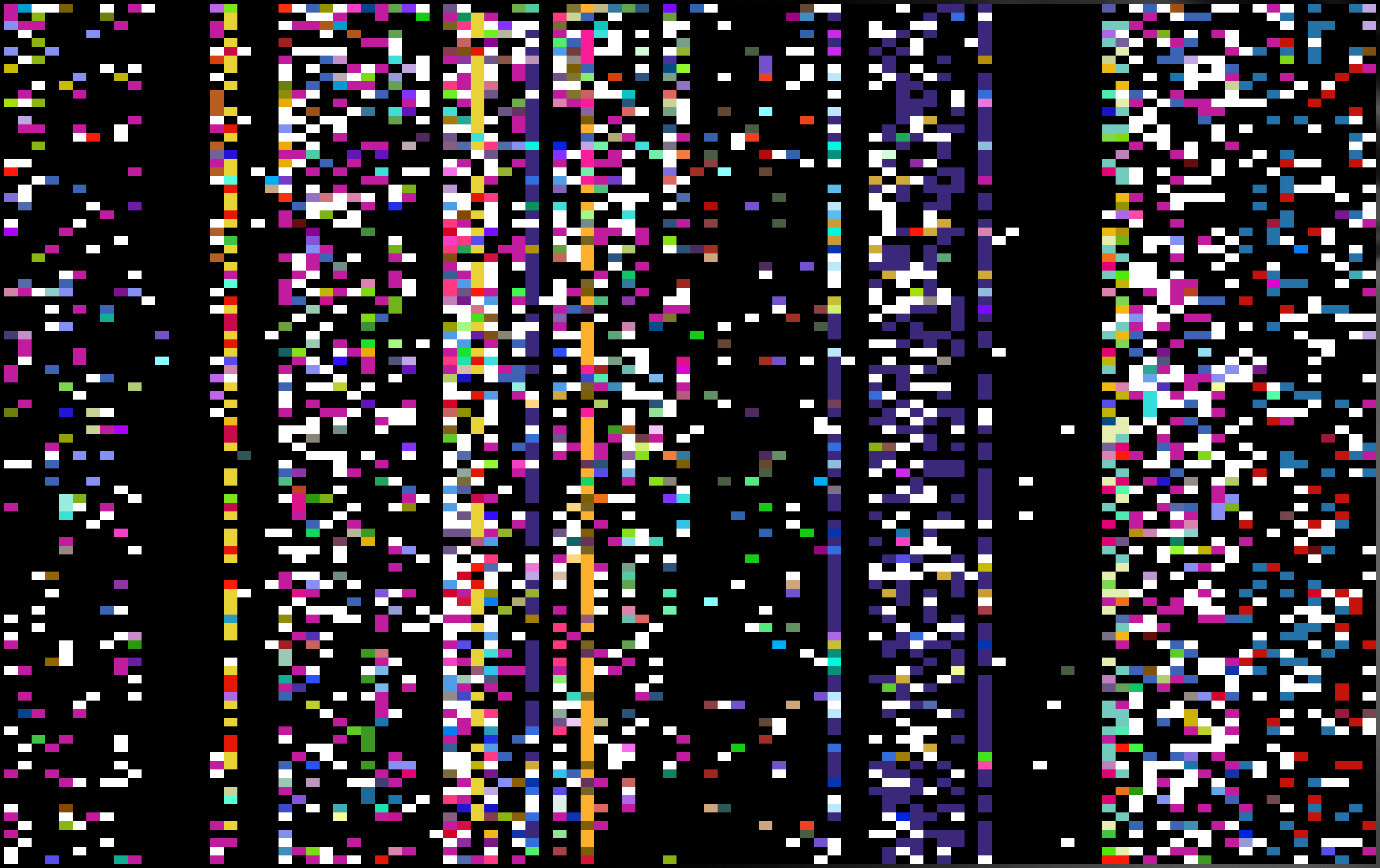
Modems are not that interesting

- Voice numbers are where the data is today
- Processing voice is a significant challenge
- Each sample is ~20 seconds of 8k audio
- Speech-to-text systems failed

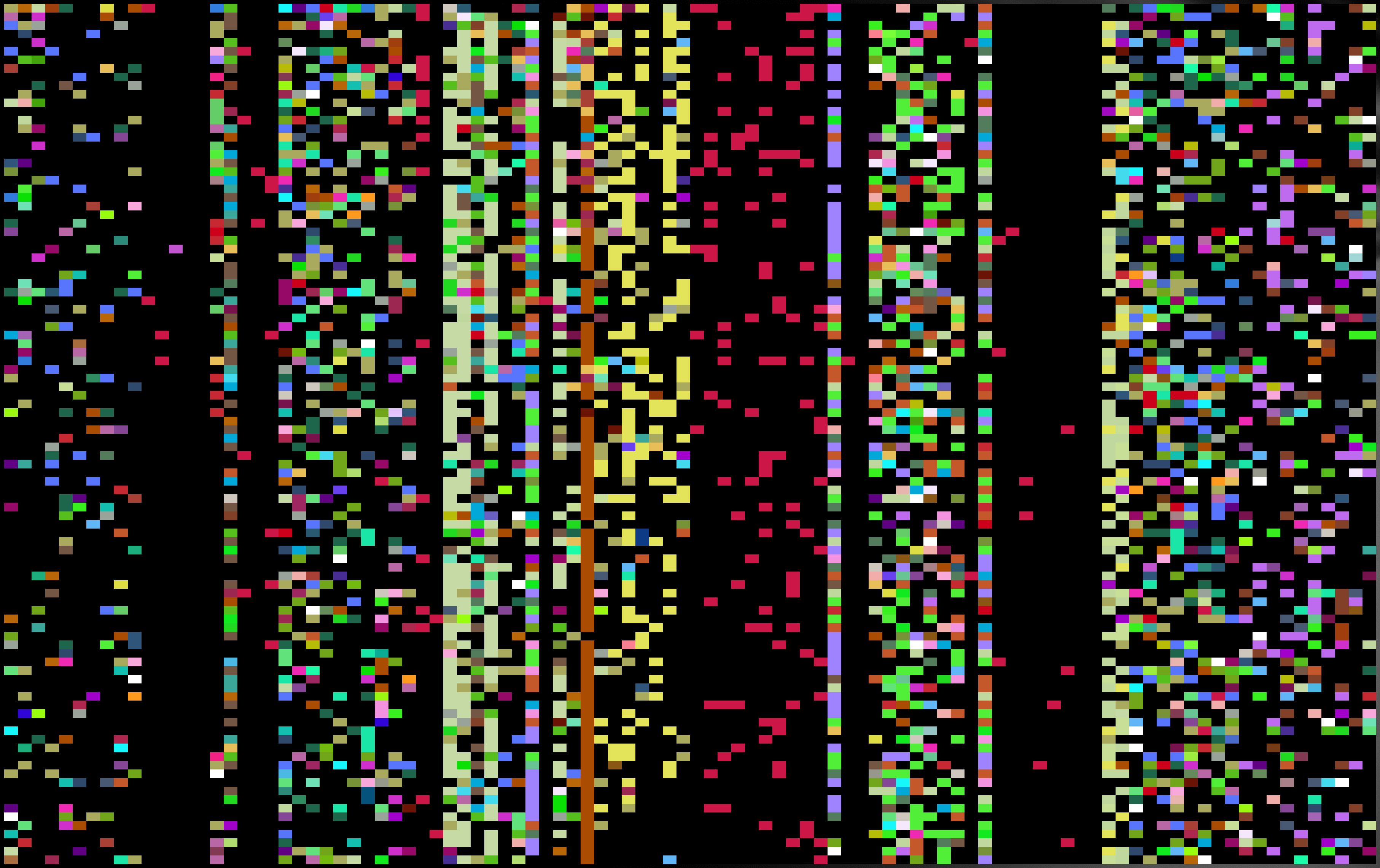
Automatic grouping of sameness

- Sorting is easy when like audio is grouped
- Helps identify patterns and oddities
- WarVOX 1.0 used two different methods

Grouped by Silence vs Noise



Grouped by Peak Frequency



WarVOX 1.0 problems

- Used buggy IAX2 library (libiaxclient)
- Scaled poorly due to SQLite3 backend
- Signatures break due to time shifting
- Hard to find “like” audio easily

2.0: PostgreSQL

- Migrated to PostgreSQL for the database
- Store all media content in the database
- Leverage PG specific features (signatures)

2.0: Ruby IAX2 Library

- Rex::Proto::IAX2::Client (in Metasploit)
- IAX2 protocol is much saner than SIP
- G711 and linear PCM codecs are easy
- Multiple delivery methods
  - VoIP providers with IAX support (Vitelity, etc)
  - SIP providers via Asterisk gateway
  - SIP providers via FreeSwitch gateway
  - Analog via Asterisk + Digium cards

2.0: New Signatures

- Top 5 frequencies of every second of audio
- Frequencies rounded to the nearest 100hz
- Low-power signals (< 100) dropped entirely
- Intervals of 1/20th second over sample
- Expanded into unique 4-second windows
- ~30s of audio is ~500 4-second fingerprints
    - (Sample Length * 20) * 4

2.0: Signature Format

- Each fingerprint looks like: [100, 200, 300, 400]
- Divide each of these by 100: [1,2,3,4]
- Pack these as bytes: “\x01\x02\x03\x04”
- Unpack this as a 32-bit integer: 0x01020304
- Collect all of these integers into an array
  - [0x01020304, 0x02030405, 0x03040506, …]
- Store these in an “int[]” PostgreSQL column

2.0: Signature Matching

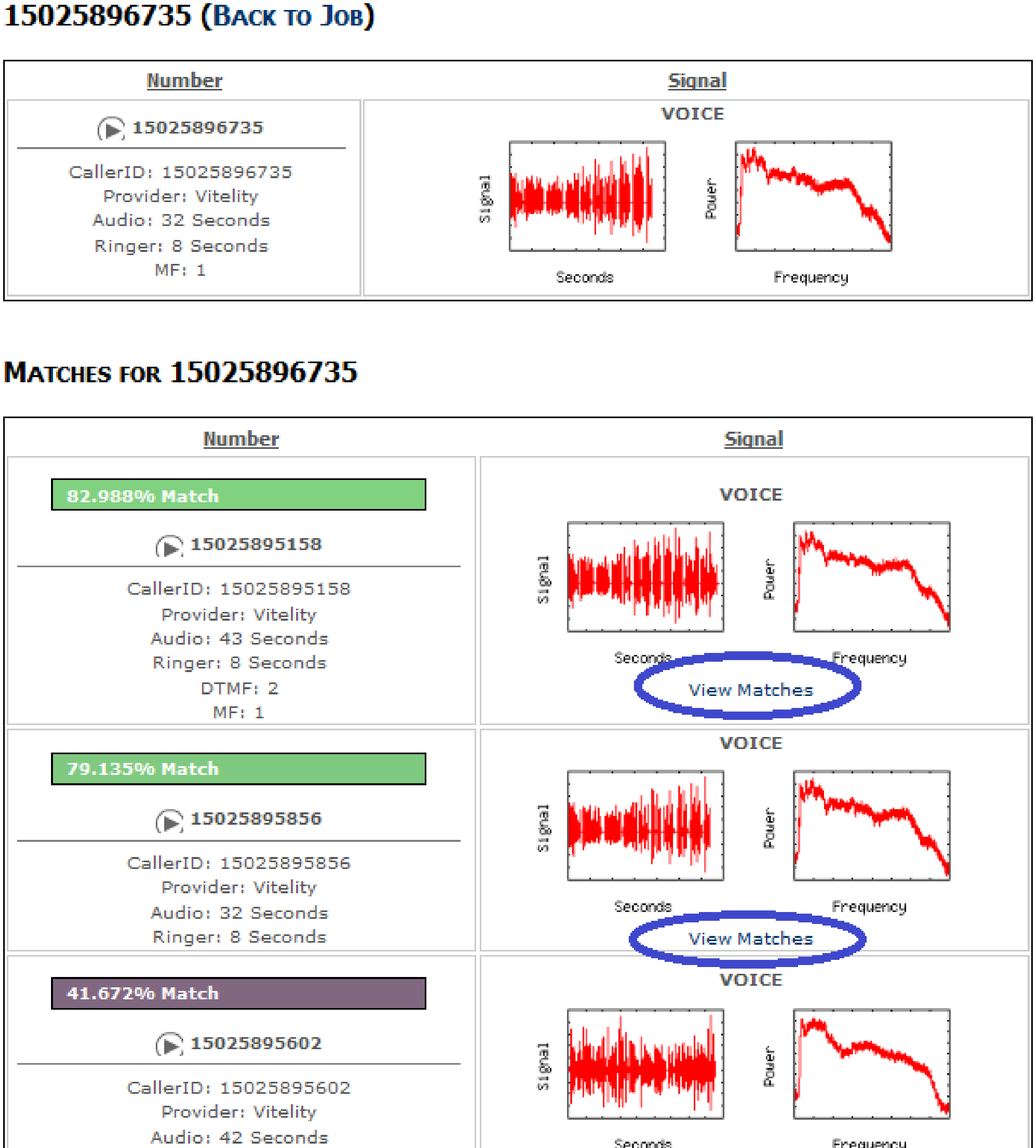
- Every audio sample has an array of integers
- Create a fingerprint of the source to match
- Leverage PostgreSQL integer array intersect (&)
  - **\i /usr/share/postgresql/8.4/contrib/_int.sql**
- SQL query returns the intersection count
- This is the % of the source sample matched
- Relatively fast results**

2.0: Signature Example (SQL)

```
SELECT dial_results.number, ( ( icount('{
0,2,3,4,514,515,516,770,772,1026,1028,2048,2304,131586,131587,131842,131843,132098,132099,197122,197123,197634,197635,262658,
262659,263170,263171,524288,526336,526592,589824,591872,592128,16779264,16779272,16779273,16779520,16779528,16779529,169
08802,16908803,16908804,16909058,16909059,16909060,16909061,16909315,16974338,16974339,16974340,16974594,16974595,169
74596,16974597,16974851,17040130,17040132,33554440,33554441,33556480,33556488,33556489,33556736,33556744,33556745,336204
83,33620736,33620739,33620995,33685504,33685512,33685762,33685763,33685764,33686016,33686017,33686018,33686019,33686020,
33686272,33686273,33686274,33686275,33686276,33686277,33686529,33686530,33686531,33686532,33751040,33751048,33751296,337
51298,33751299,33751300,33751552,33751553,33751554,33751555,33751556,33751808,33751809,33751810,33751811,33751812,33751813,3
3752064,33752065,33752066,33752067,33752068,33752323,33816834,33816835,33816836,33817088,33817090,33817091,33817092,33817
344,33817346,33817347,33817348,33817602,33817603,33817604,50331656,50331657,50333696,50333704,50333705,50333952,50333960,5
0333961,50397192,50397193,50397698,50397699,50397700,50397952,50397954,50397955,50397956,50398211,50462720,50462728,504
62729,50462978,50462979,50462980,50463232,50463233,50463234,50463235,50463236,50463488,50463489,50463490,50463491,504
63492,50463493,50463744,50463745,50463746,50463747,50463748,50528256,50528264,50528265,50528514,50528515,50528516,5052
8768,50528769,50528770,50528771,50528772,50529024,50529025,50529026,50529027,50529028,50529029,50529280,50529281,50529
282,50529283,50529284,50529539,50593800,50593801,50594050,50594051,50594052,50594304,50594306,50594307,50594308,50594
560,50594562,50594563,50594564,50594818,50594819,50594820,50660099,67110912,67110920,67110921,67111168,67111176,6711117
7,67174915,67175171,67175427,67239936,67240450,67240451,67240452,67240705,67240706,67240707,67240708,67240962,67240963,6
7305472,67305986,67305987,67305988,67306240,67306242,67306243,67306244,67306498,67306499,67371522,67371523,67371524,6737
1778,67371779,67371780,67372034,84083456,134217728,134742016,134807552,150994944,151519232,151584768
}' & dial_results.fprint) / 249.0) * 100.0)
as matched from dial_results
order by matched;
```

2.0: Signature Example (Output)

```
15557774938 | 100.0000000000000000000000
15557770000 |  76.92347234911646582340
15557770060 |  36.947791164658634538000
15557770046 |  34.136546184738955823000
15557770099 |  25.702811244979919679000
15557770077 |  22.088353413654618474000
15557770049 |  19.678714859437751004000
15557770079 |  19.277108433734939759000
15557770086 |  18.072289156626506024000
15557770006 |  17.670682730923694779000
15557770002 |  12.449799196787148594000
15557770051 |  11.646586345381526104000
```



15025896735 (Back to Job)

Number	Signal
▶ 15025896735 CallerID: 15025896735 Provider: Vitelity Audio: 32 Seconds Ringer: 8 Seconds MF: 1	VOICE

Matches for 15025896735

Number	Signal
82.988% Match ▶ 15025895158 CallerID: 15025895158 Provider: Vitelity Audio: 43 Seconds Ringer: 8 Seconds DTMF: 2 MF: 1	VOICE View Matches
79.135% Match ▶ 15025895856 CallerID: 15025895856 Provider: Vitelity Audio: 32 Seconds Ringer: 8 Seconds	VOICE View Matches
41.672% Match ▶ 15025895602 CallerID: 15025895602 Provider: Vitelity Audio: 42 Seconds	VOICE

2.0: Signature Tools

- Command-line export and mangling tools
- Create and test signatures from sources

```
$ bin/audio_export.rb data 10
```

```
$ bin/audio_trim.rb 2 data/NNNNNNNNN.raw |
     bin/audio_raw_to_fprint.rb - |
     bin/identify_matches.rb 5 -
```

VoIP now inside of Metasploit

- Dial numbers and record linear PCM audio
- Detect DTMF tones via IAX control packets
- Send linear PCM audio fairly easily
- Borrow WarVOX2 code for analysis
- Use Metasploit modules and mixins

One example module written

- auxiliary/scanner/voice/recorder

Demo

Questions