
waRvox

H D Moore <hdm [at] metasploit.com>

metasploit

Project lead

BreakingPoint Systems

Director of Security Research

Telephone Fun Time

Way back when...

- Modems were how you got access to things
- Modems were poorly protected, easy to find
- Nights were spent in front of TONELOC

Found all sorts of interesting things

- UNIX machines, remote access, PPP/SLIP
- Routers, switches, various data services
- HVAC, SCADA, power mgmt, radio gear

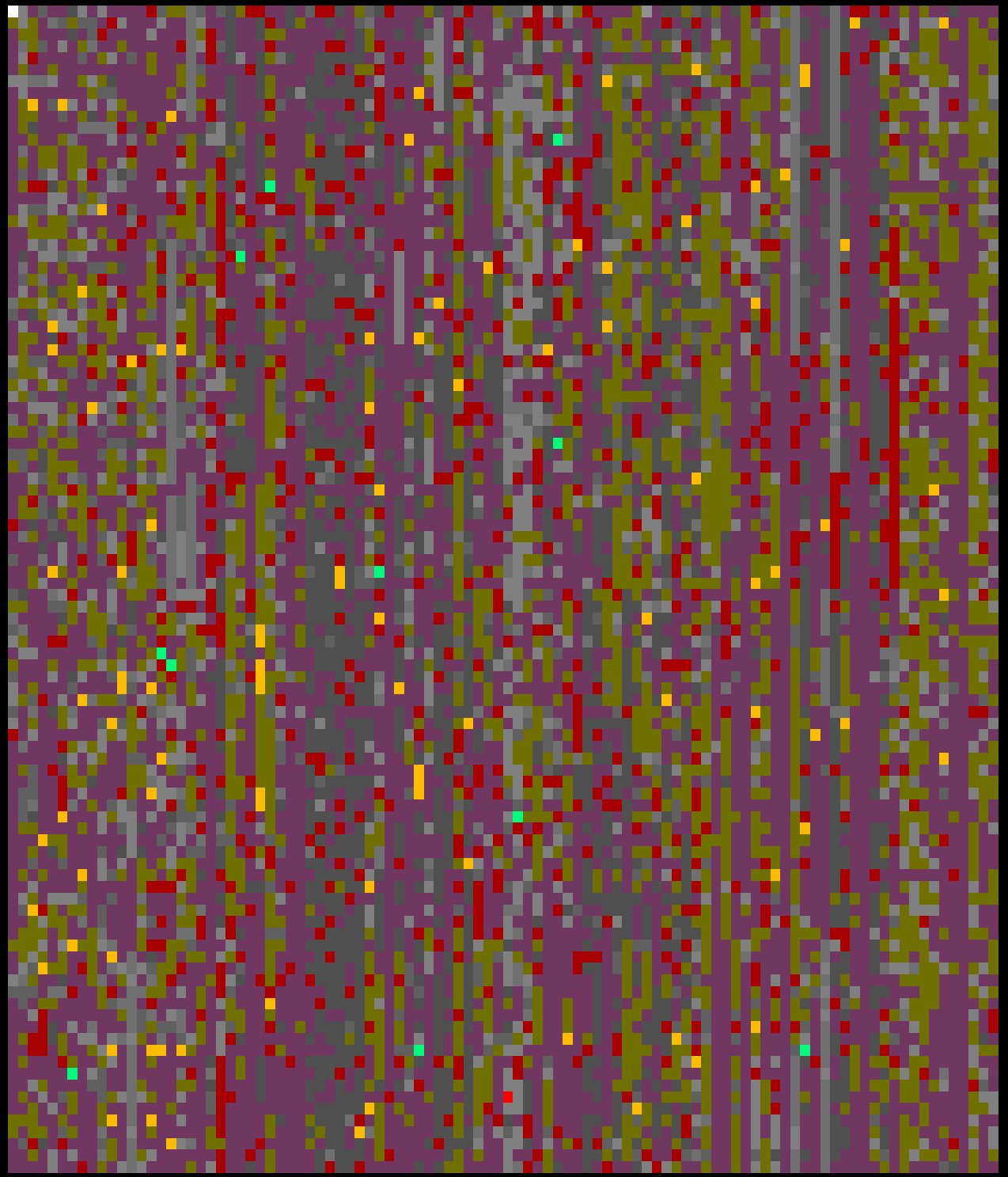
TONELOC Maps

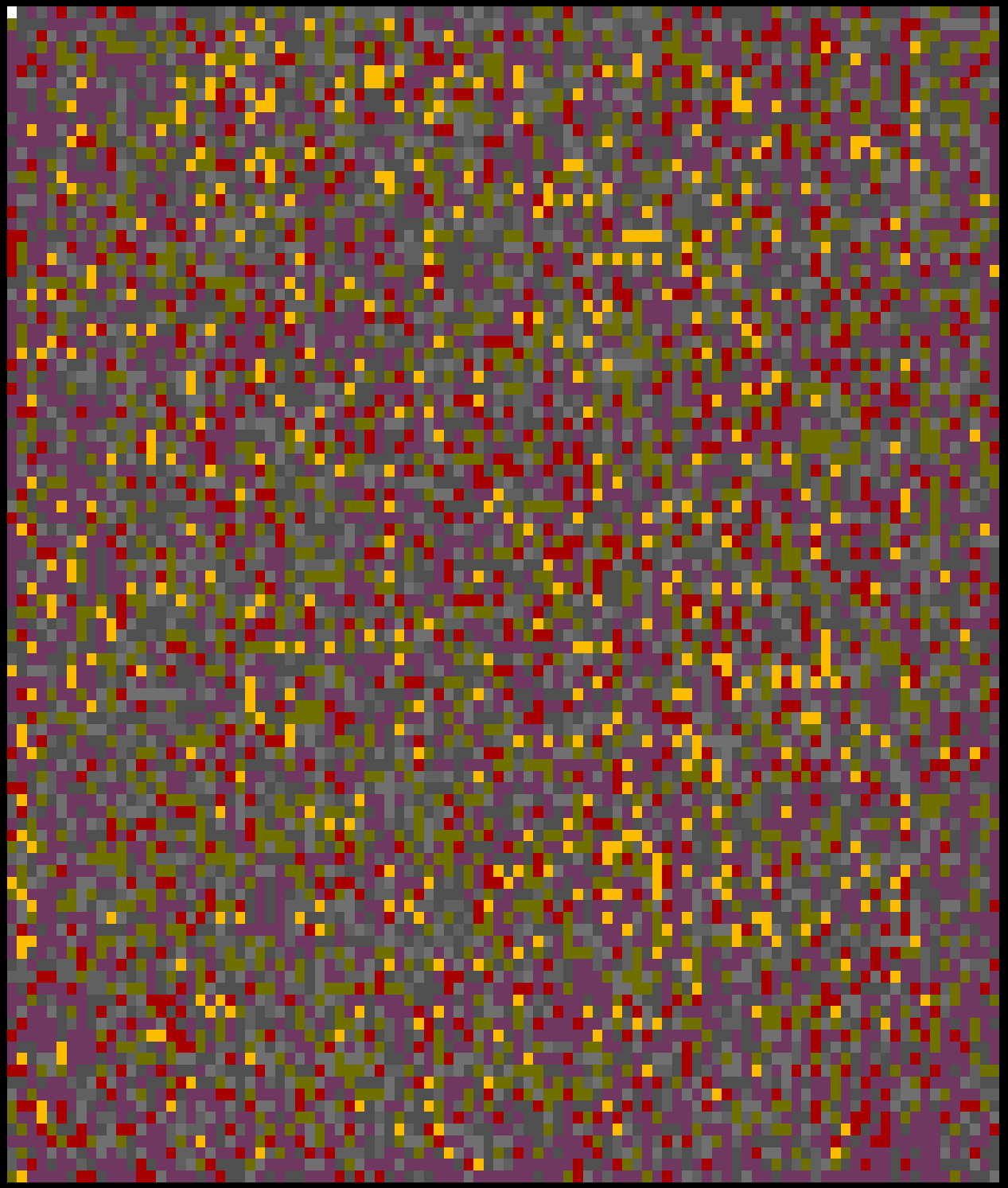
Displays 10,000 number blocks

- Dial an entire exchange: 123**-456-XXXX**
- Plot as a 100x100 grid colored by type
- Vertical rows are sequential numbers

Number classification

- CARRIER, BUSY, VOICE, FAX,TIMEOUT
- Manual classification (GIRL, AHOLE, etc)


SAMPLE6.DAT
Tone
Carrier
Undialed
Dialed
Timeout
Ringout
Busy
Voice
Noted
Fax
VMB
Girl
Asshole
Aborted
Blacklist
Omitted
Excluded
0000
Busy
(0)


SAMPLE10.DAT
Tone
Carrier
Undialed
Dialed
Timeout
Ringout
Busy
Voice
Noted
Fax
VMB
Girl
Asshole
Aborted
Blacklist
Omitted
Excluded
0000
Voice (0)

Wardialing Today

Wardialing

- Search for modems, faxes, and tones
- Still effective against large organizations
- Connect modems to phone lines
- Dial until you find something

Slow and inefficient

- Requires hardware and line investment
- Commercial software is expensive

Commercial Tools

Sandstorm's PhoneSweep

- **PhoneSweep Basic** starts at **$1,186.00**
  - Limit of one modem, not included
  - 60/calls per hour
- **PhoneSweep Plus 16** starts at **$35,600.00**
  - Includes 16 modems, rackmount server
  - 1000/calls per hour

FREE! SecureLogix's TeleSweep

Open Source Tools

MS-DOS (WinXP & DOSEmu)

- **TONELOC**
- **THC-SCAN**

UNIX Systems

- **iWar**
- **PAWS**
- **Metasploit**: I)ruid's wardial module
- **Others:** ShokDial, ward.c, etc

Wardialing + VoIP

Required hardware investment

- Modem + IAXY + Asterix + SIP provider
- Modem + SIP ATA + SIP provider
- Modem + Time Warner ATA

Software is not quite there yet

- iWar does not handle VoIP properly
- iaxmodem can only handle fax machines

Wardialing with metasploit

Hardware setup

- US-Robotics USB modem (v.90)
- Generic dual-stack SIP/IAX ATA

Software

- Checkout latest Metasploit SVN snapshot
- `use auxiliary/scanner/telephony/wardial`

Find a VoIP Service Provider...

Wardialing with VoIP

Reality check on “unlimited” ISPs

- Common rate is $40 USD/mo
- Limited to one outgoing call
- Limited to 250 total destination numbers
- Aggressive auto-dialer policies
- Contract locks

Wardialing with VoIP

Per-minute ISPs are much nicer

- Common rate is $0.01 per minute
- Better protocol support (IAX and SIP)
- Multiple outgoing calls (~10 is normal)
- Happy as long as they get paid

Still some hidden fees (vitelity.net)

- Minimum of one minute, rounded ~6 secs
- Include **ring time** in the count...

Wardialing is Boring

Dialed for 48 hours straight

- Covered approximately 2000 numbers
- Lots of **300 BAUD** mangled carriers (faxes)
- Approximately ~45% answer rate
- Approximately ~4% carriers

Dialing results

- Found close to 100 carriers (most 300B)
- Bill from vitelity.net was **$13.25**

OCD + Impatience

Limited by the hardware

- Only one modem, only one ATA device
- Limited to one outgoing call at a time

Software modems are limited

- Requires real codec/DSP in software
- iaxmodem, but it does FAX only
- iWar is a nice idea, but not implemented

Stepping Back

Modern wardialing misses the point

- Only ~4% of numbers are modems
- Dialing these with a modem is a waste
- What about the rest of the numbers?

TONELOC

- Half the fun was listening to the audio
- Manual classification of interesting lines
- Found strange and insecure things

War Voicing

WarVOX is the solution

- Call each number using VoIP
- Record an audio sample (~20 secs)
- Process the audio later on

Benefits over traditional dialing

- Scalable and cheap using VoIP
- Opens the door to new attacks
- Archival audio data

WarVOX Implementation

Softphone that records audio

- **iaxrecord**: dial over IAX and save raw samples

Ruby on Rails Web UI

- Configure VoIP providers
- Launch a new dial job
- Analyze the audio
- Classify the lines
- Visualize the data

WarVOX Speeds

VoIP ISP allows ~50 concurrent calls

- Scan over 3,000 numbers/hour
- Scan ~10,000 numbers in 3 hours
- 45% pickup == **$45.00** in VoIP fees

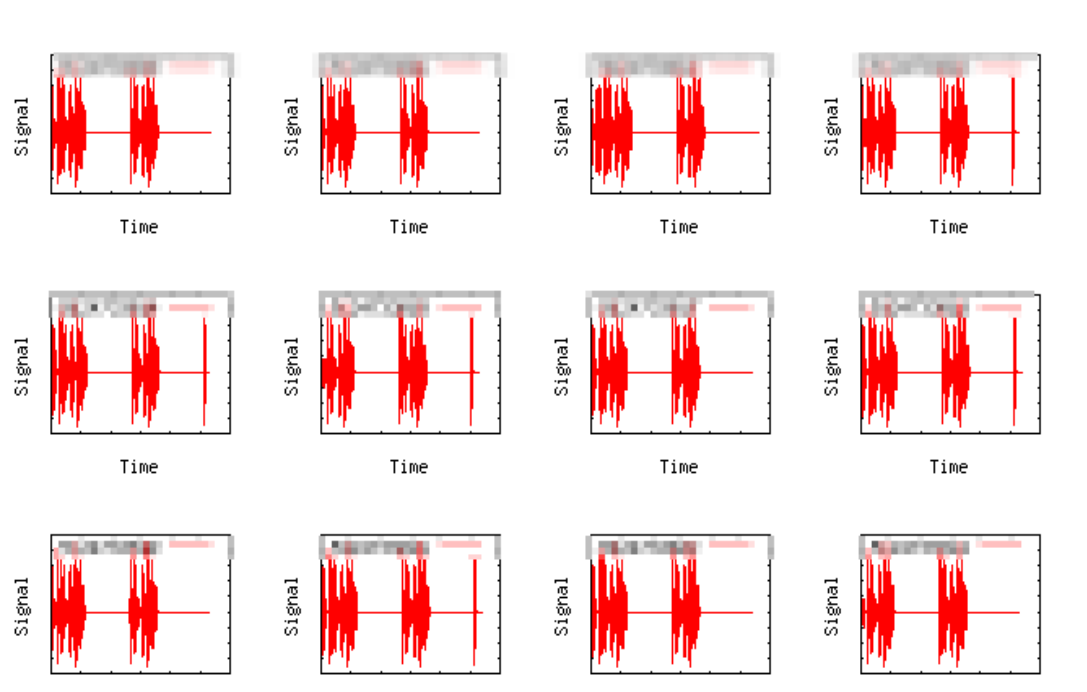
Analysis is resource intensive

- Lots of processing (mp3, png, fft, etc)
- Averaging ~20 seconds per audio sample
- Can use multiple CPU cores :-)

Call Analysis

Generate a simple signal graph

- Scripted through GNUPlot
- Visually identify similar lines



Call Analysis

Ghettotastic signature generation

- Developed with Efrain Torres of Metasploit
- Look for silence vs noise patterns

Format is Type, Length, Average

L,16194,16 **H,1380,3096**

L,320,8 **H,29822,3096**

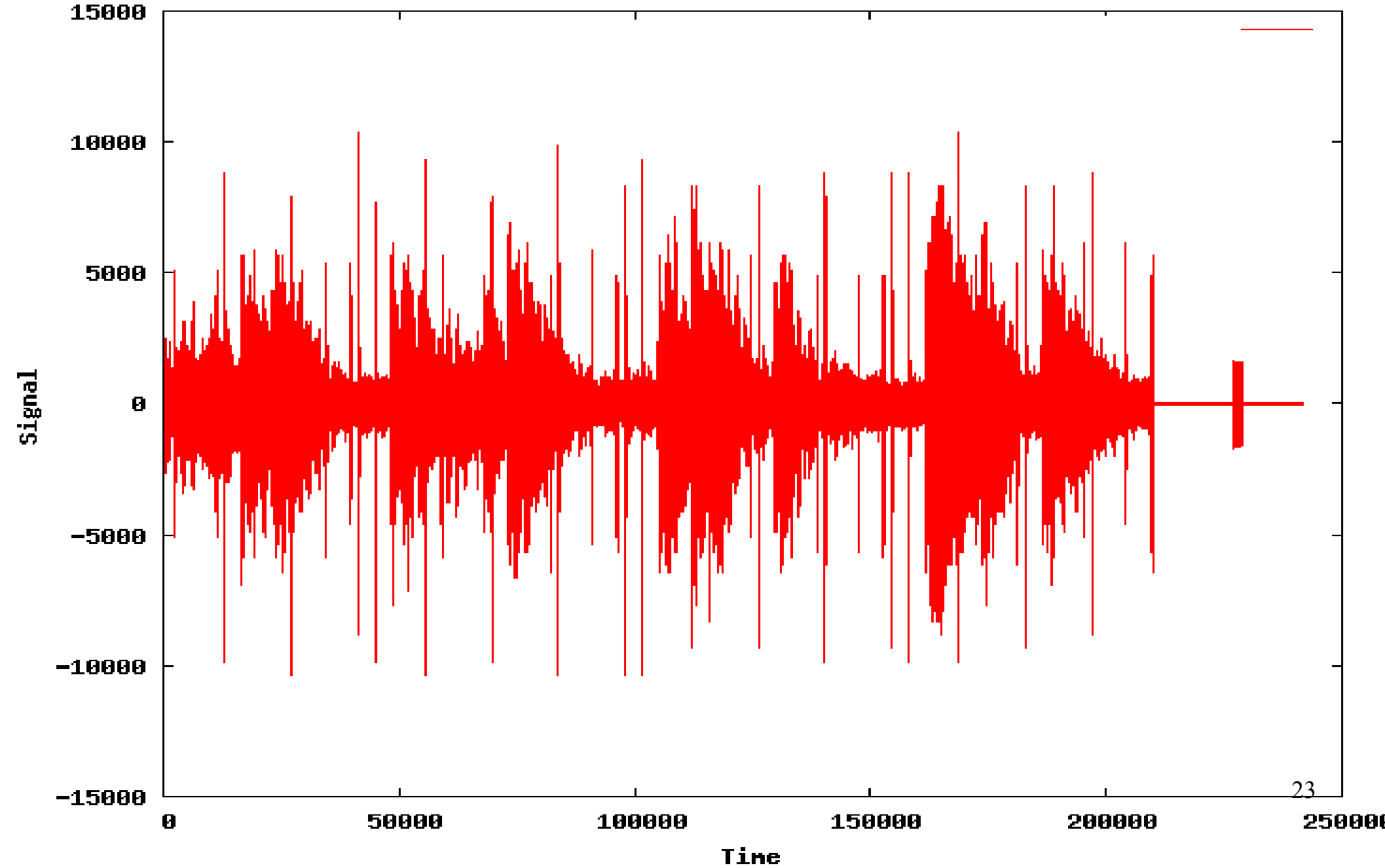
L,569,18 **H,739,2549**

Call Analysis

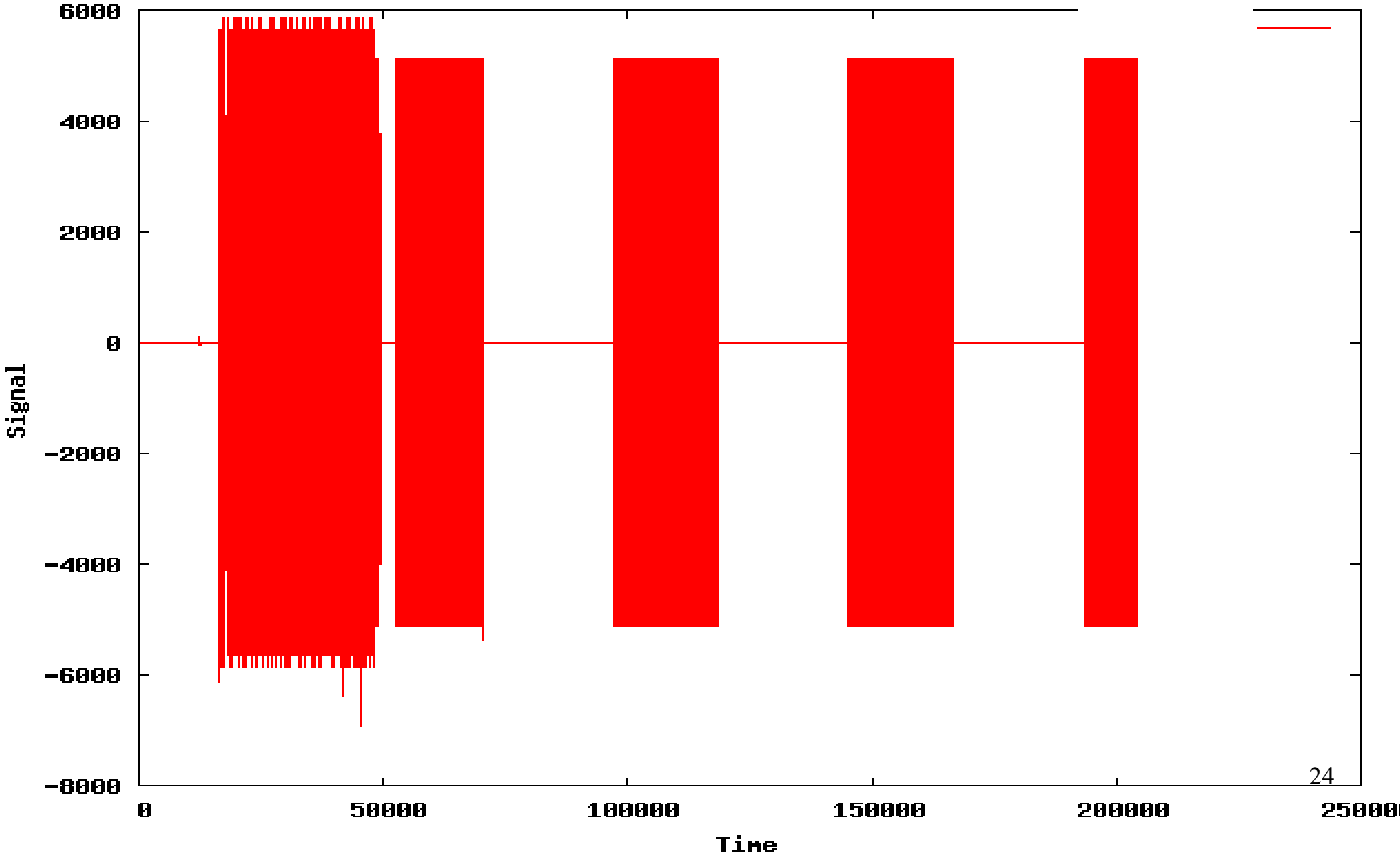
Noise vs Silence signatures

- Carriers and tones are “small”
- Voice systems are “long”
- Humans are mostly silence

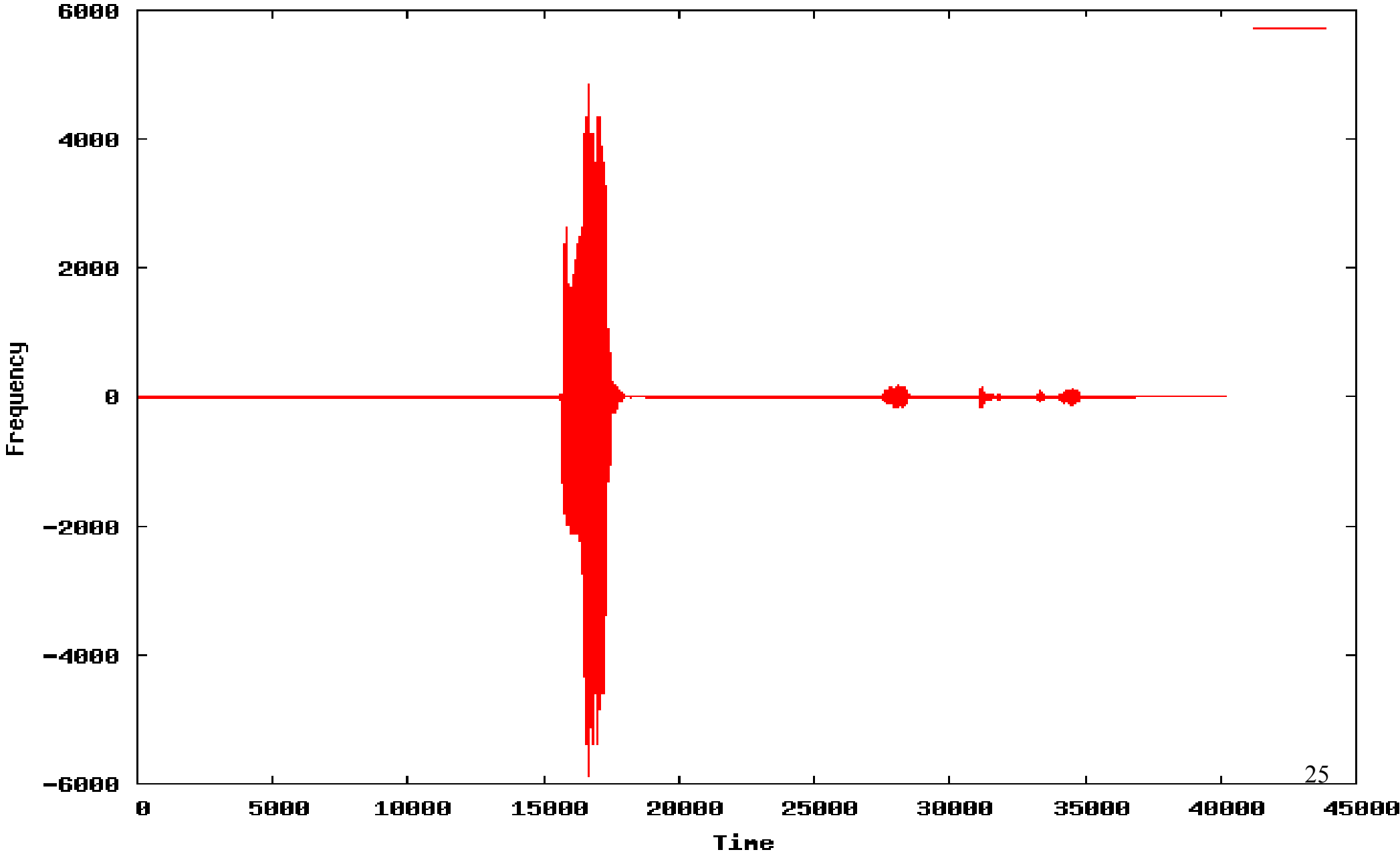
WarVOX (voice)



WarVOX (fax)


6000
4000
2000
0
-2000
-4000
-6000
-8000
Signal
0
50000
100000
150000
200000
250000
Time

WarVOX (human)



Automatic Grouping

Match each sample against the rest

- Fuzzy matching of Silence vs Noise signature
- Automatically group similar calls
- Group up the faxes and modems

Find similar sounding audio

- **“This call is being answered by Audix”**
- **“Welcome to Cisco Unity Call Manager”**
- **“This ABC Internal Number is not in service”**

Practical Uses

Identify similar voice greetings

- Find all incoming lines for a company
- Target specific PBX vendors

The outliers are interesting

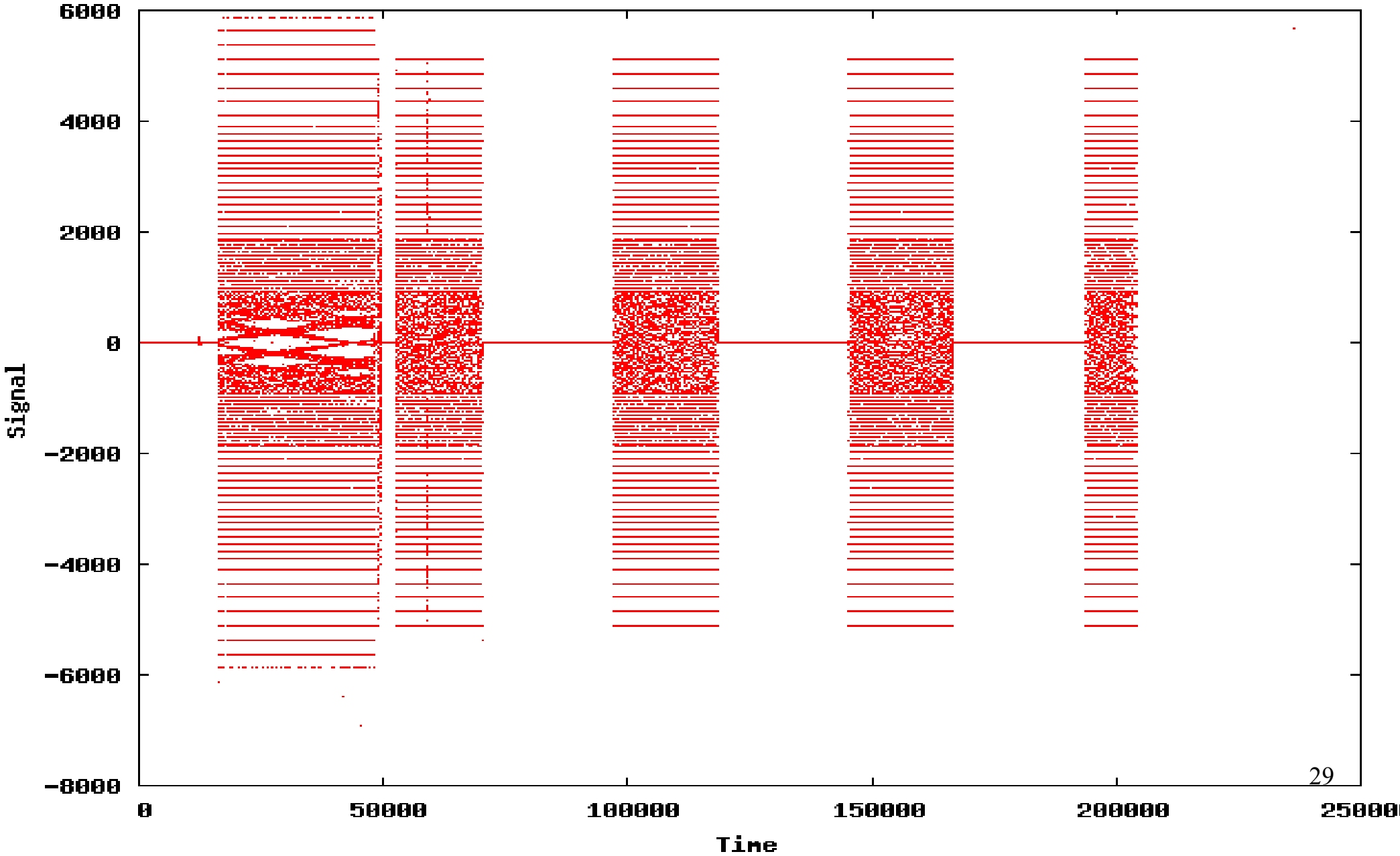
- Corporate phones forwarded to mobiles
- International forwarding (UK ring tones)
- Teleconferencing systems
- Lots of weird stuff

Modems vs Faxes

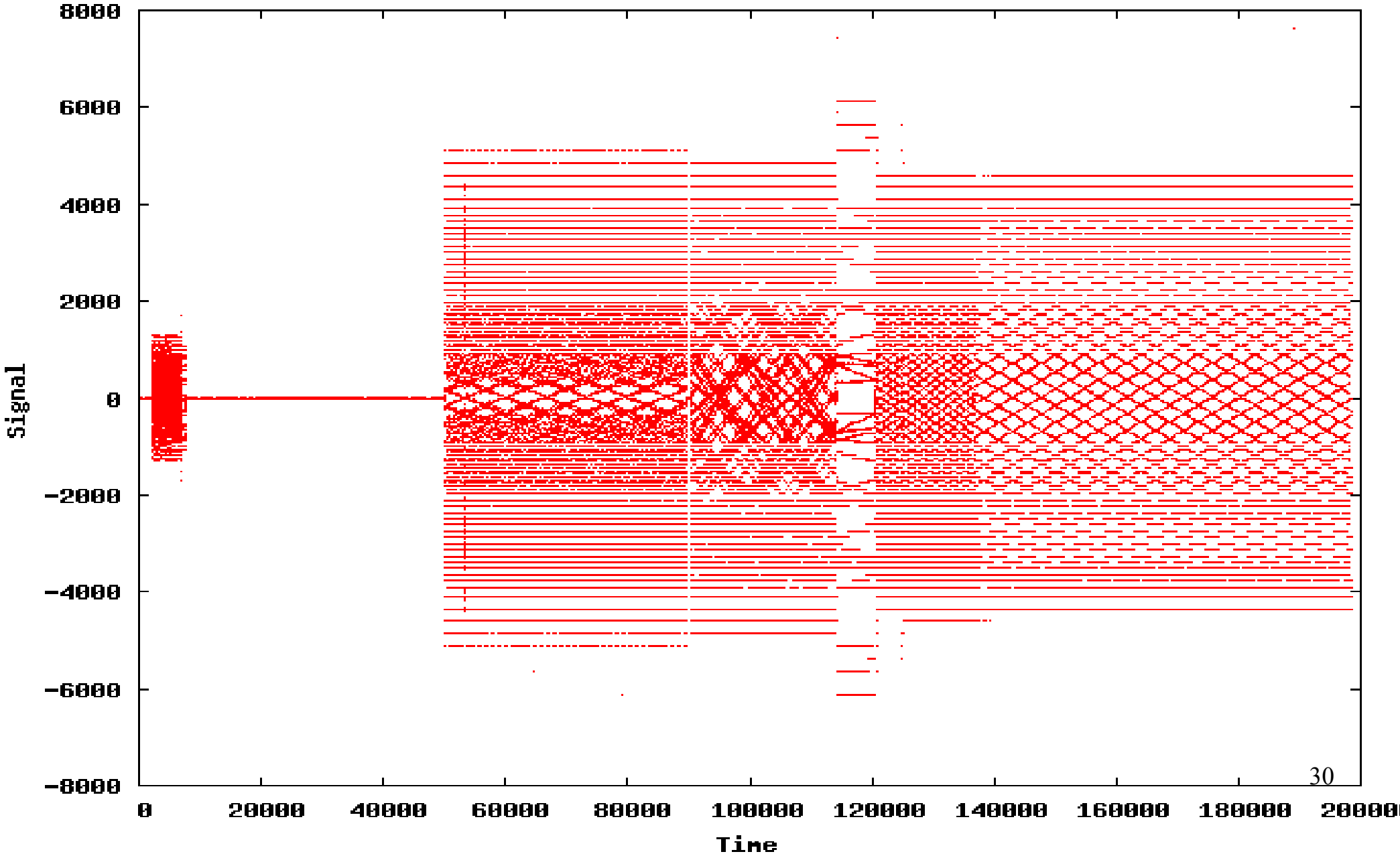
Modems sound a lot like faxes

- The signal graphs look very similar
- Some people can tell them apart by ear
- Noise vs Silence signatures fail
- Lets look closer...

WarVOX (fax)


6000
4000
2000
0
-2000
-4000
-6000
-8000
Signal
0
50000
100000
150000
200000
250000
Time

WarVOX (modem)



Modems vs Faxes

Determine difference by frequency

- Require spectrum analysis of the audio
  - Hacked up **Ruby-KissFFT** for WarVOX

Fax Machines

- **2100hz** + 1625hz, 1660hz, 1850hz...

Modems

- **2250hz** + 1625hz, 1850hz, 2000hz...

Automatic Grouping

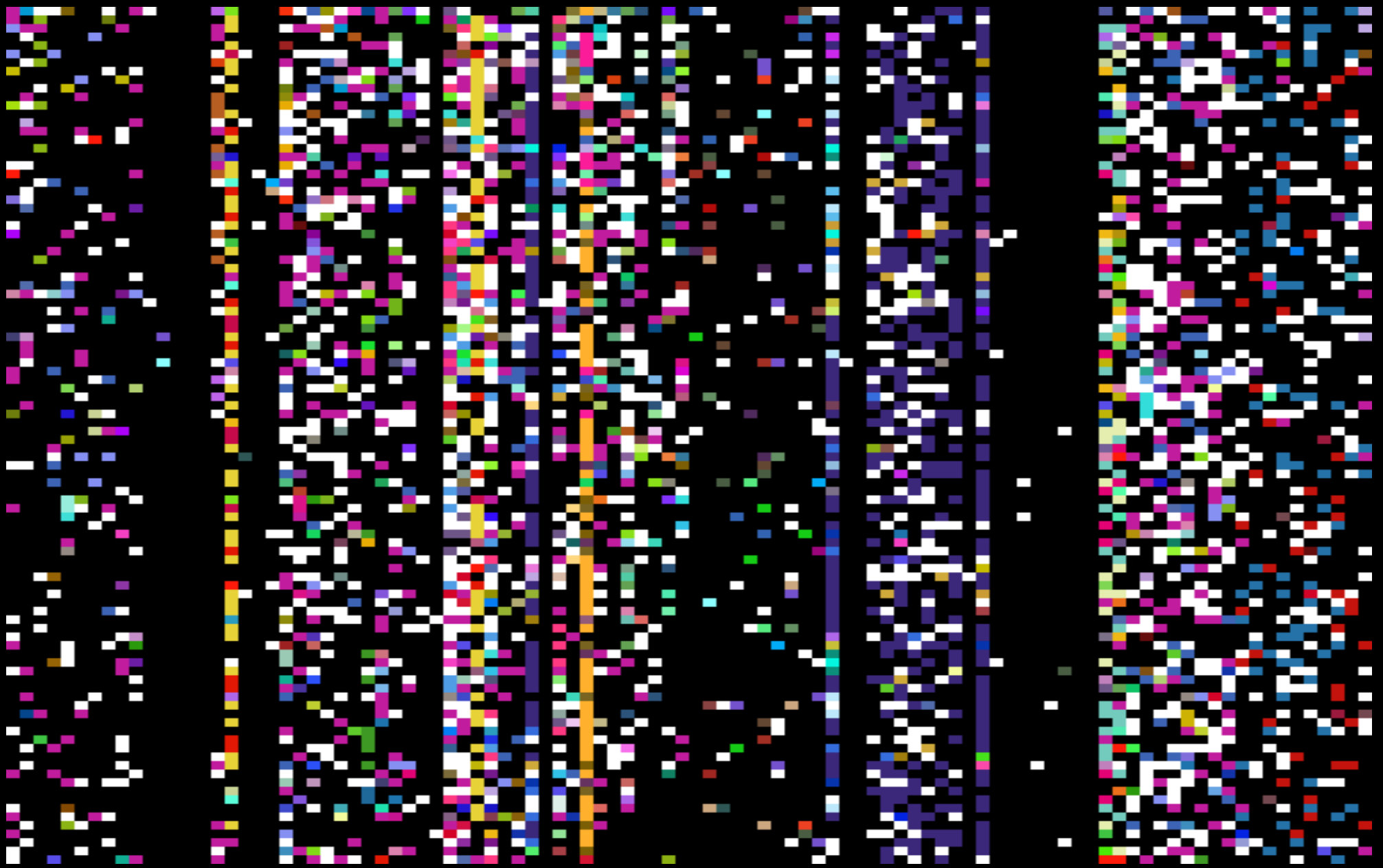
Browsing the groups

- Use HTML5 Canvas object to TONEMAP
- Plot 100x100 numbers by group
- Each group its own color

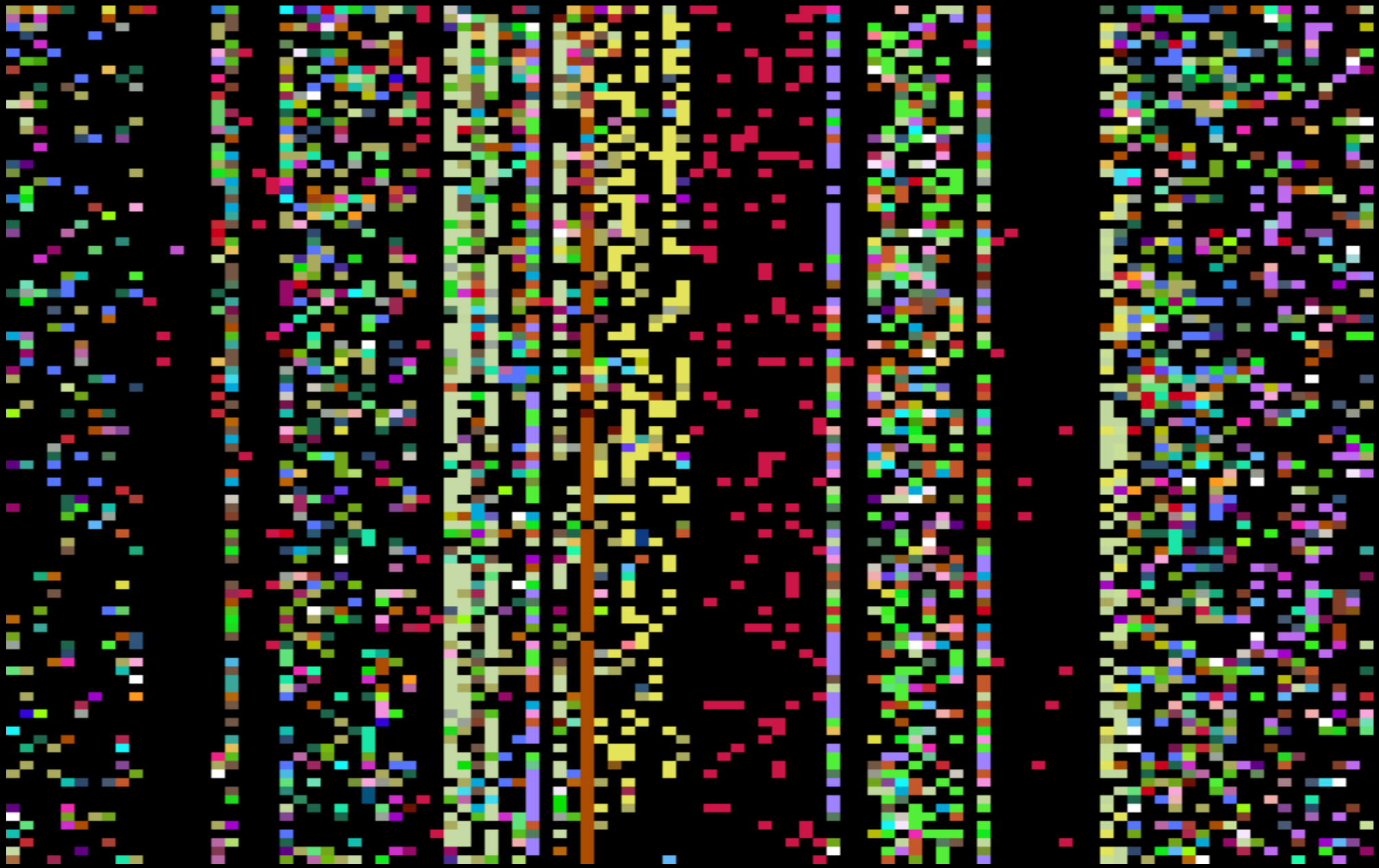
Drilling down into groups

- Click to select any group
- Hide other groups
- Link MP3 + graphics

Grouped by Silence vs Noise



Grouped by Peak Frequency



Spectrum Analysis

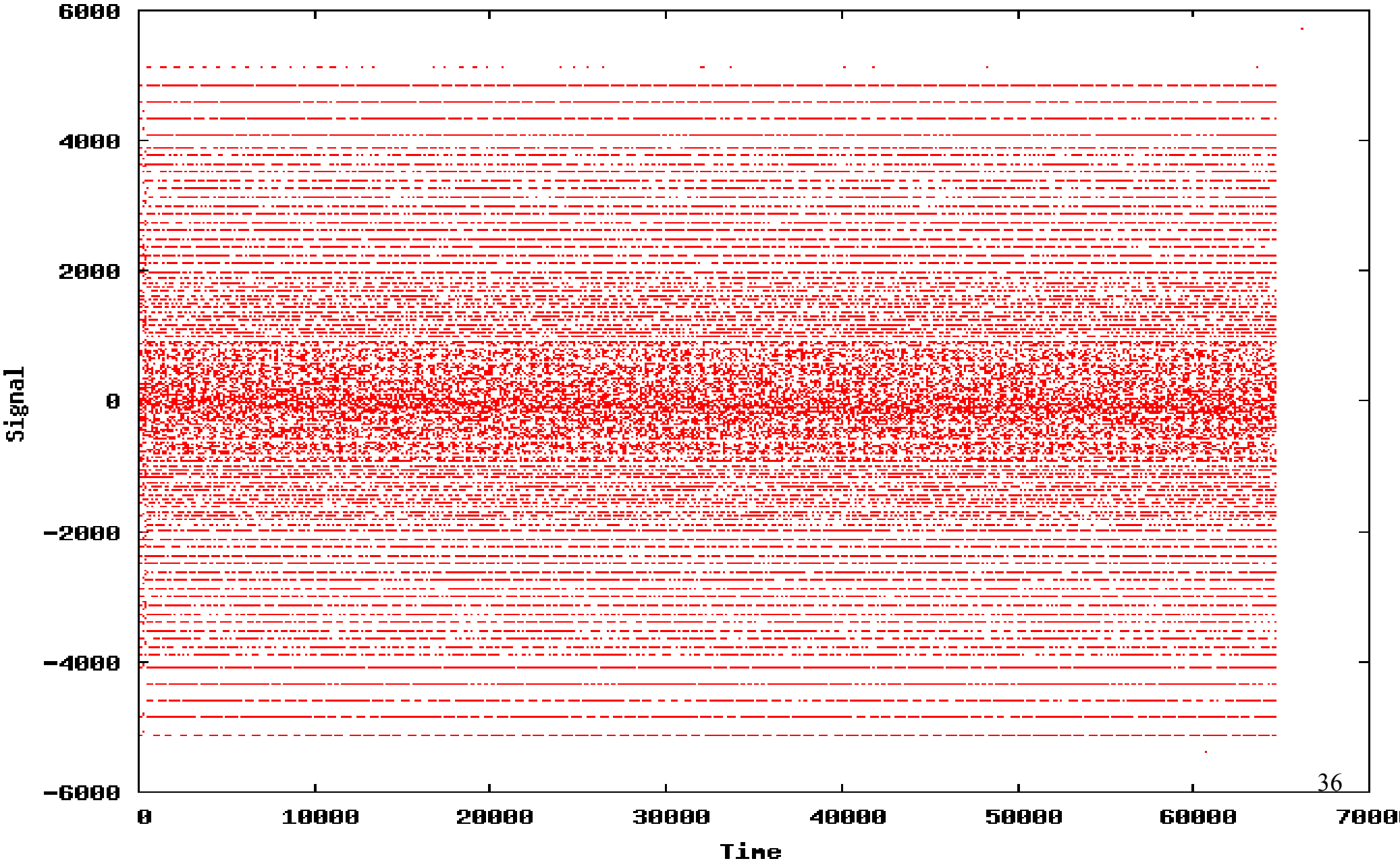
Provides us with tone detection

- Signature specific BEEPs and tones
- Group phone systems by BEEP
- Find loops and other oddness

A quick frequency challenge

- What is the following signal?

WarVOX (350hz + 440hz)



Moving Forward

Latest online at WARVOX.ORG

- Version 1.0.0 is now public!
- Limited documentation

Features coming in 1.0.1..

- Import and export calls by type
- Browser-based TONELOC maps
- Integrated auto-grouping
- Tons more :-)

Legal Aspects

Fax.com ruined it for everyone

- Wardialed every # for fax machines
- Spammed them with advertisements
- Settled for $6.5 million

TCPA amended in 2003...

- Prohibits calling for “fax vs voice detection”
- Could easily apply to most wardialers
- More at http://warvox.org/legal.html

Demonstrations

questions ?