COMPROMISING ELECTROMAGNETIC EMANATIONS OF WIRED AND WIRELESS KEYBOARDS

EPFL/LASEC/USENIX SECURITY'09

Martin VUAGNOUX and Sylvain PASINI

MODERN KEYBOARDS RADIATE COMPROMISING ELECTROMAGNETIC EMANATIONS

THESE EMISSIONS LED TO A FULL OR A PARTIAL RECOVERY OF THE KEYSTROKES AT A DISTANCE UP TO 20 METERS

FULL SPECTRUM ACQUISITION METHOD

FOUR SOURCES OF INFORMATION LEAKAGE FROM KEYBOARDS

EXPLOITATION IN DIFFERENT SCENARIOS

WHY COMPUTER KEYBOARDS?


esc
COMPROMISING delete
tab EMANATIONS
caps lock OFF WIRED return
shift KEYBOARDS shift
control option command ⌘ ⌘ command option control
fn home page up
delete end page down
clear = / *
7 8 9 −
4 5 6 +
1 2 3 enter
0 .

KEYBOARDS

MAIN INPUT DEVICE/PASSWORD

KEYBOARDS

SECURITY IS NOT A PRIORITY

KEYBOARDS

ALICE TYPES ON HER KEYBOARD...

KEYBOARDS

WHY ELECTROMAGNETIC EMANATIONS?

Bell 131-B2
Mar 1, 1944

- Bell 131-B2 mixing devices
- Encrypt teletyperwriter communications with one time pad
- When a key is pressed, a peak appears
- Recover the plaintext at more than 25 meters away.

Markus Kuhn
Dec 1, 2003

Compromising Emanations: Eavesdropping Risks of Computer Displays.

Dmitri Asonov and Rakesh Agrawal
Jan 1, 2005

Keyboard Acoustic Emanations.

Davide Balzarotti, Marco Cova, and Giovanni Vigna
May 28, 2008

ClearShot: Eavesdropping on Keyboard Input from Video.

Markus Kuhn
Dec 1, 2003

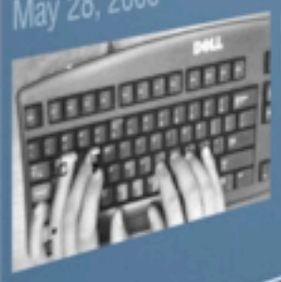
Compromising Emanations:
Eavesdropping Risks of Computer
Displays.

Dmitri Asonov and Rakesh Agrawal
Jan 1, 2005

Keyboard Acoustic Emanations.

ation Theft by
magnetic Radiation
.

Davide Balzarotti,
May 28, 2008



ClearShot: Eavesdropping on Keyboard
Input from Video.

2005
2010
2015
2020

Dmitri Asonov and Rakesh Agrawal
Jan 1, 2005

Keyboard Acoustic Emanations.

Davide Balzarotti, Marco Cova, and Giovanni Vigna
May 28, 2008

ClearShot: Eavesdropping on Keyboard Input from Video.

2005
2010
2015
2020

ELECTROMAGNETIC COMPATIBILITY

CONDUCTIVE

RADIATIVE

ELECTROMAGNETIC COMPATIBILITY

CONDUCTIVE

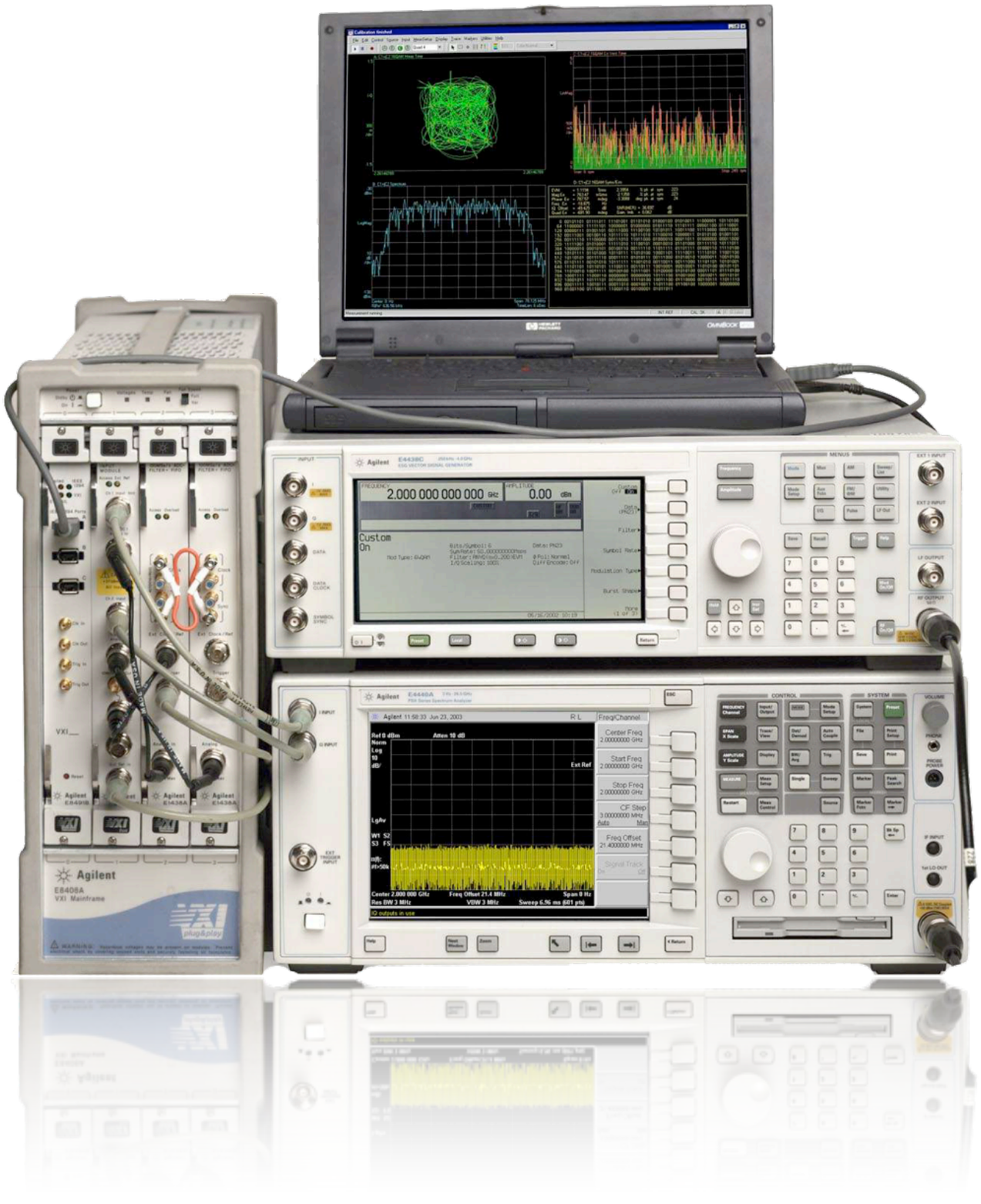
RADIATIVE

ATTACKER'S POINT OF VIEW

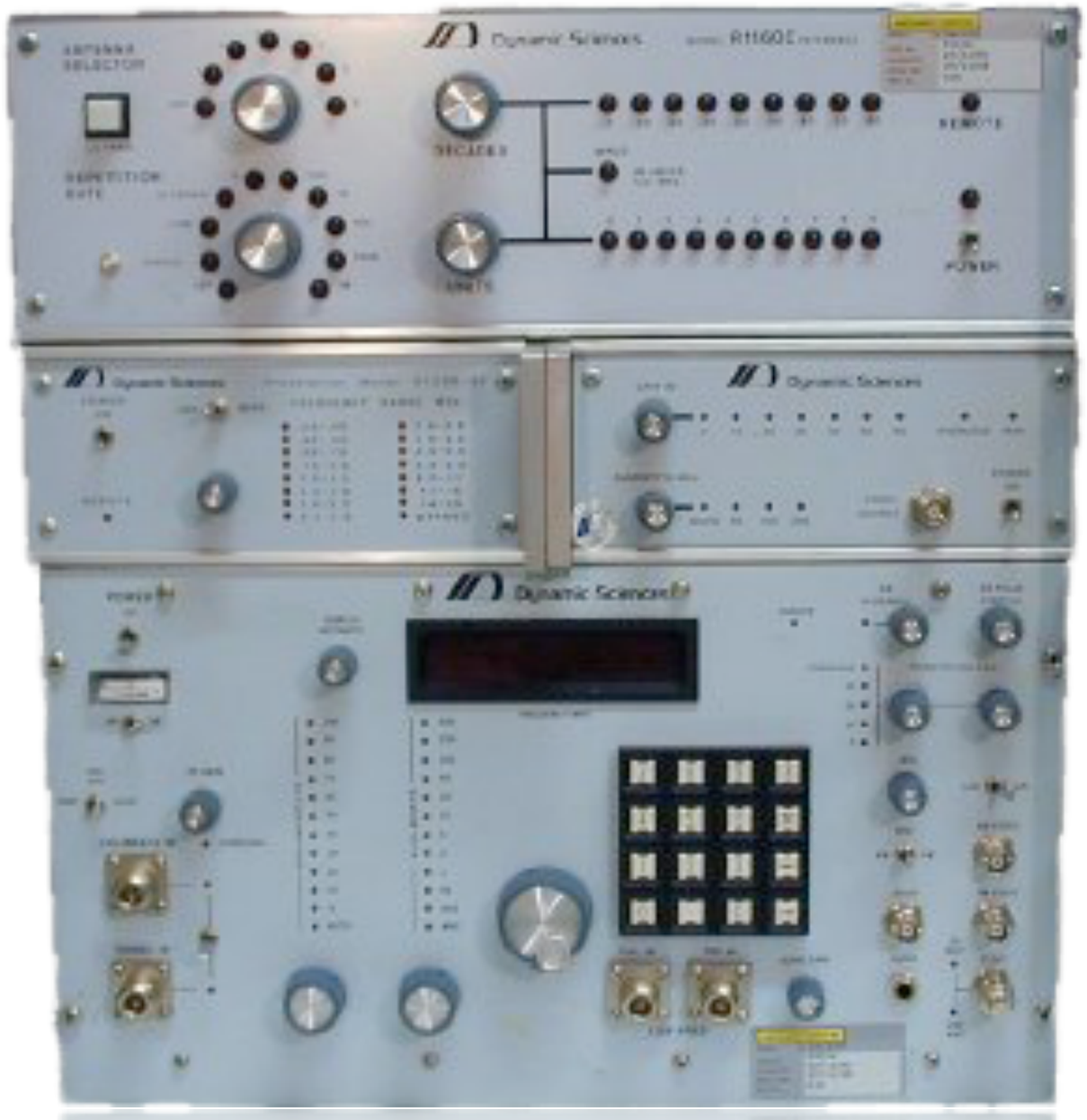
DIRECT EMANATIONS

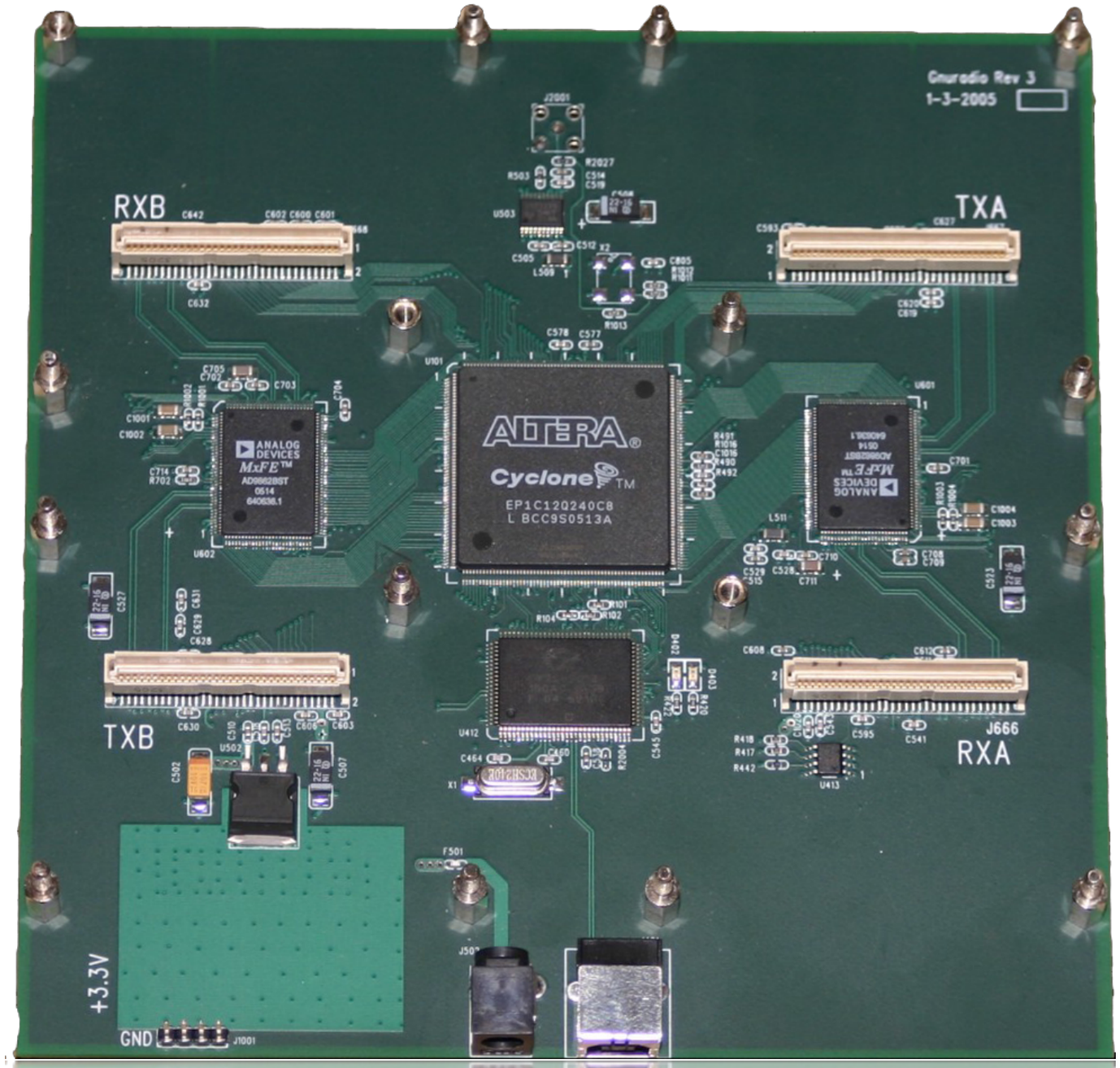
INDIRECT EMANATIONS

HOW TO DETECT COMPROMISING ELECTROMAGNETIC EMANATIONS?


Agilent
E8408A
VXI Mainframe
Agilent E4438C
2.000 000 000 000 GHz
0.00 dBm
Agilent E4440A
Agilent 11:58:33 Jun 23, 2003
Center 2.000 000 GHz
Freq Offset 21.4 MHz
Span 0 Hz
Res BW 3 MHz
VBW 3 MHz
Sweep 6.56 ms (601 pts)
OMNIBOOK


FINE TUNING
SIDEBAND
UPPER
LOWER
A.F. GAIN
POWER
SPEAKER
1814
KC/S
MC/S
R.F./I.F. GAIN
SPEAKER
MONITOR
R.F. TUNE
INCREASE FREQ.
B.F.O. NOTE KC/S
V.F.O.
RACAL
FREE
LOCK
R.F. RANGE MC/S
BANDWIDTH
A.V.C.
LIMITER
POWER
A.F. GAIN
R.F. ATTENUATOR

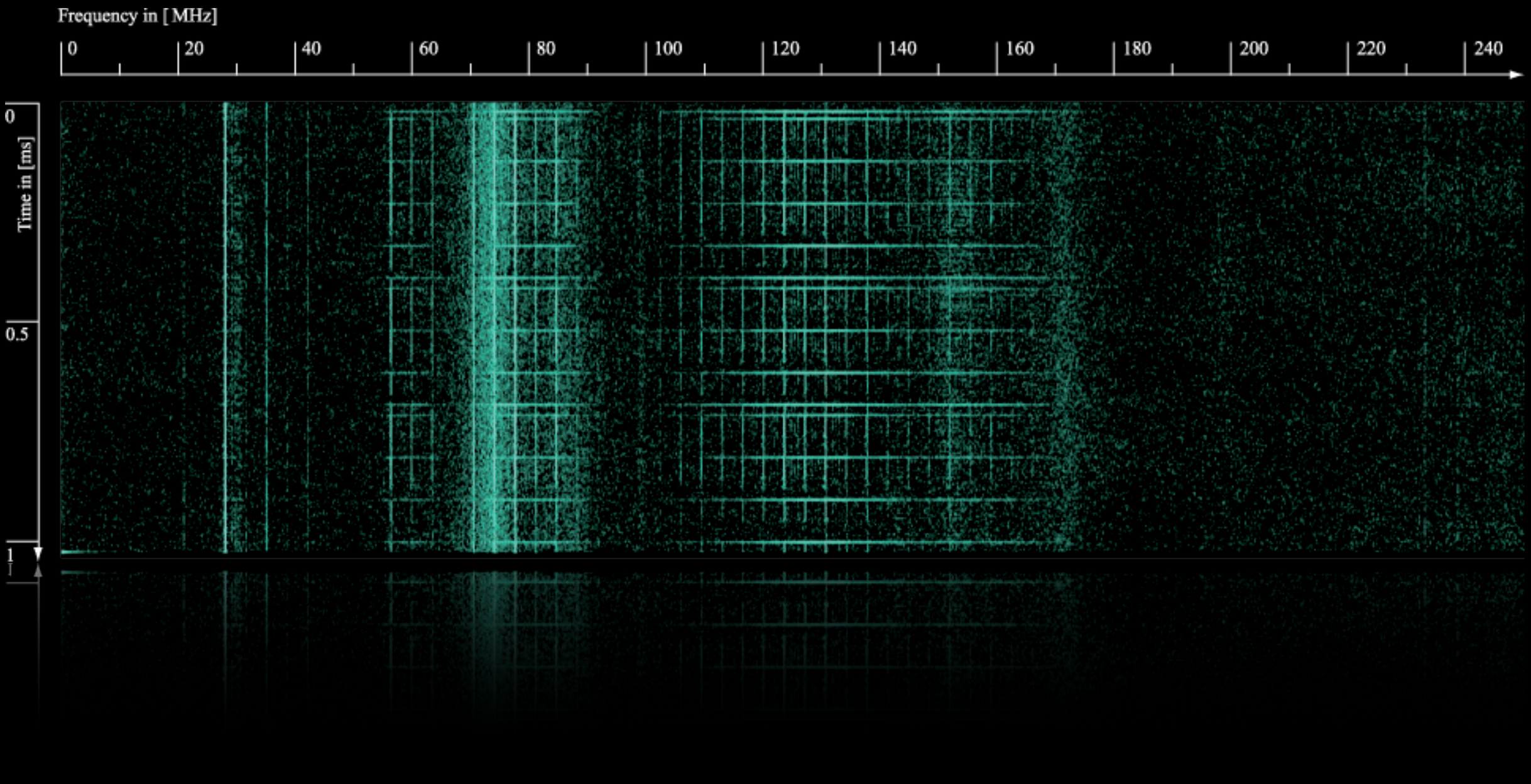

Dynamic Sciences
ANTENNA SELECTOR
REPETITION RATE
SECONDS
UNITS
REMOTE
POWER


Gnuradio Rev 3
1-3-2005
RXB
TXA
TXB
RXA
+3.3V
GND
ALTERA
Cyclone
EP1C12Q240C8
L BCC9S0513A
ANALOG DEVICES
MxFE
AD9862BST
0514
640636.1
J2001
J666
J1001
U101
U412
U502
U503
U601
U602
U413
X1
F501

FULL SPECTRUM ACQUISITION METHOD

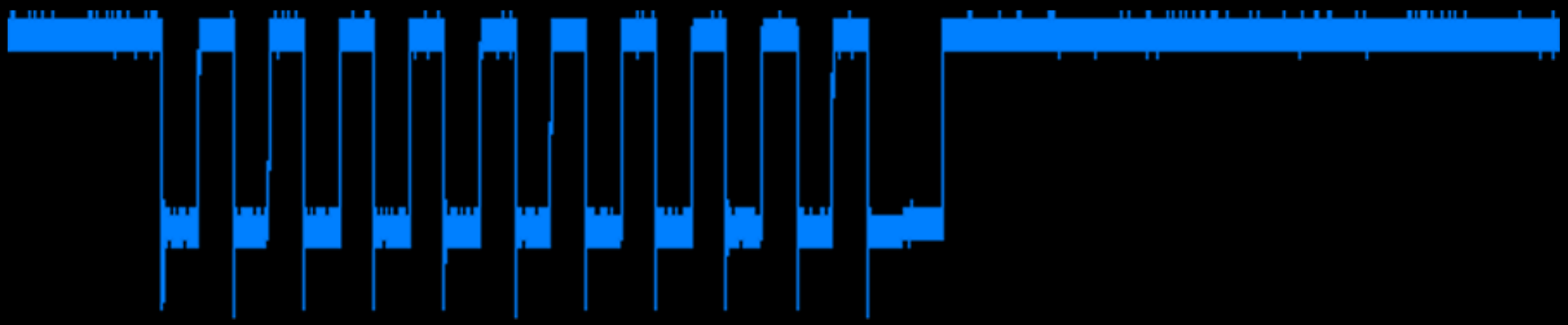

ANTENNA
ADC
MEMORY
COMPUTER


MacBook

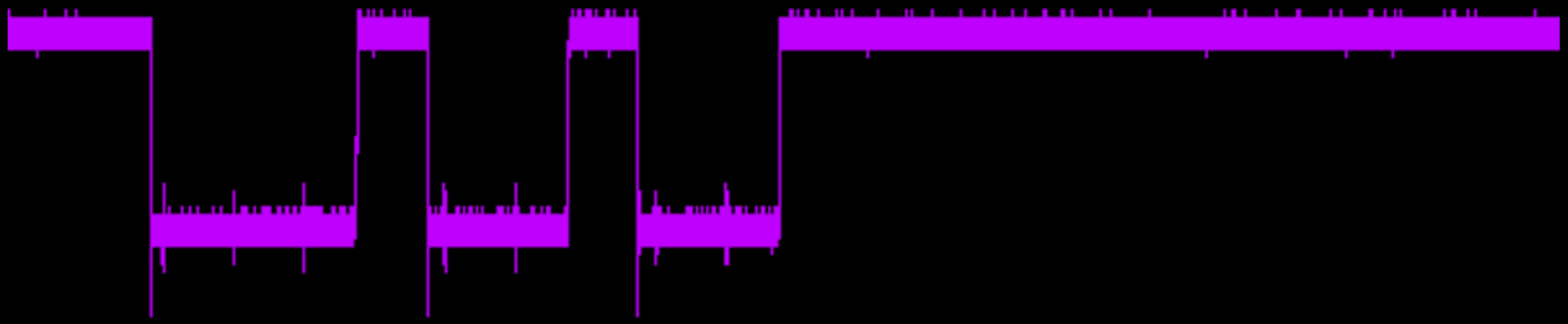

Frequency in [MHz]
0
20
40
60
80
100
120
140
160
180
200
220
240
Time in [ms]
0
0.5
1

HOW TO DETECT COMPROMISING SIGNALS?

DIRECT EMANATIONS

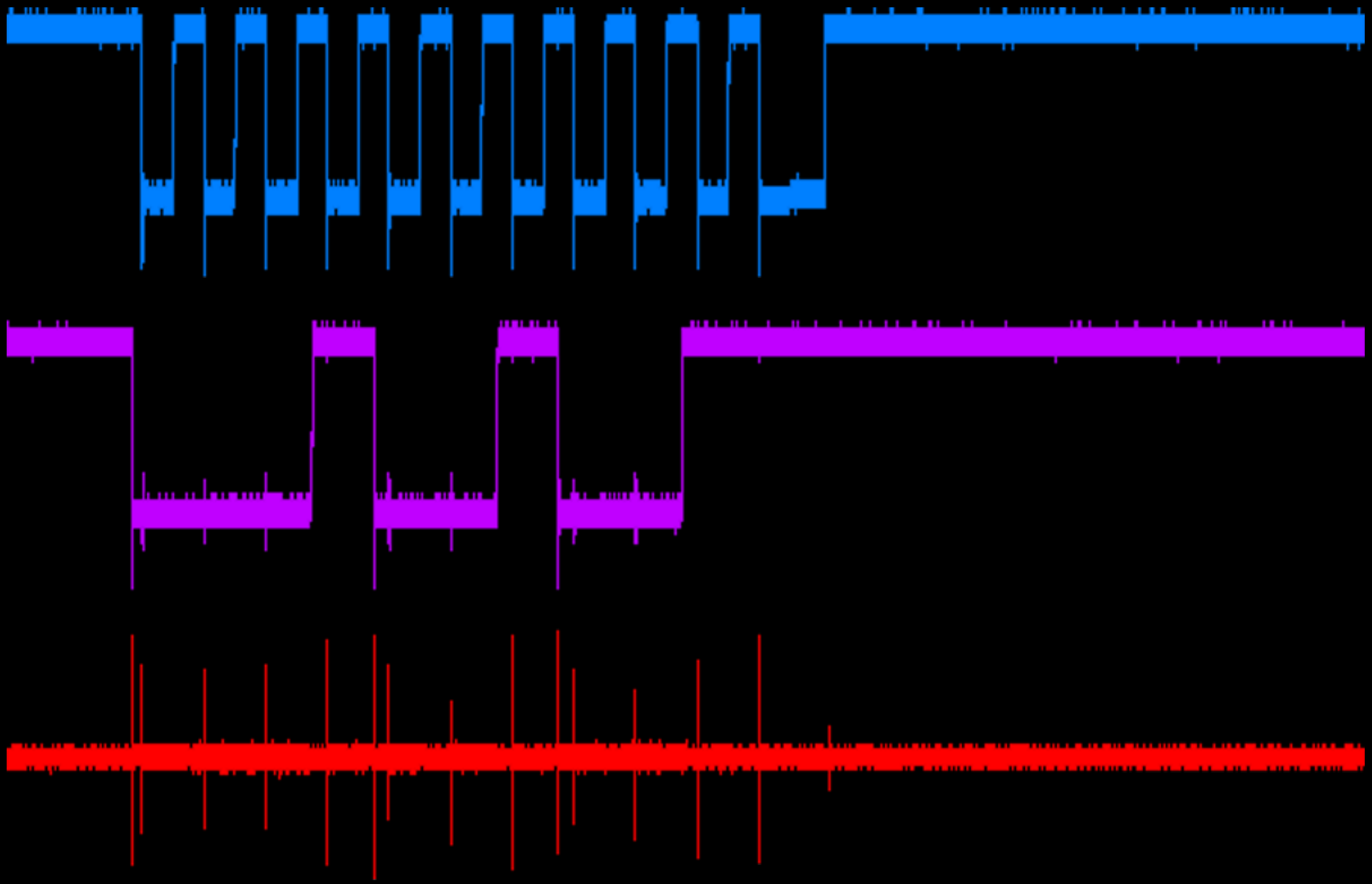


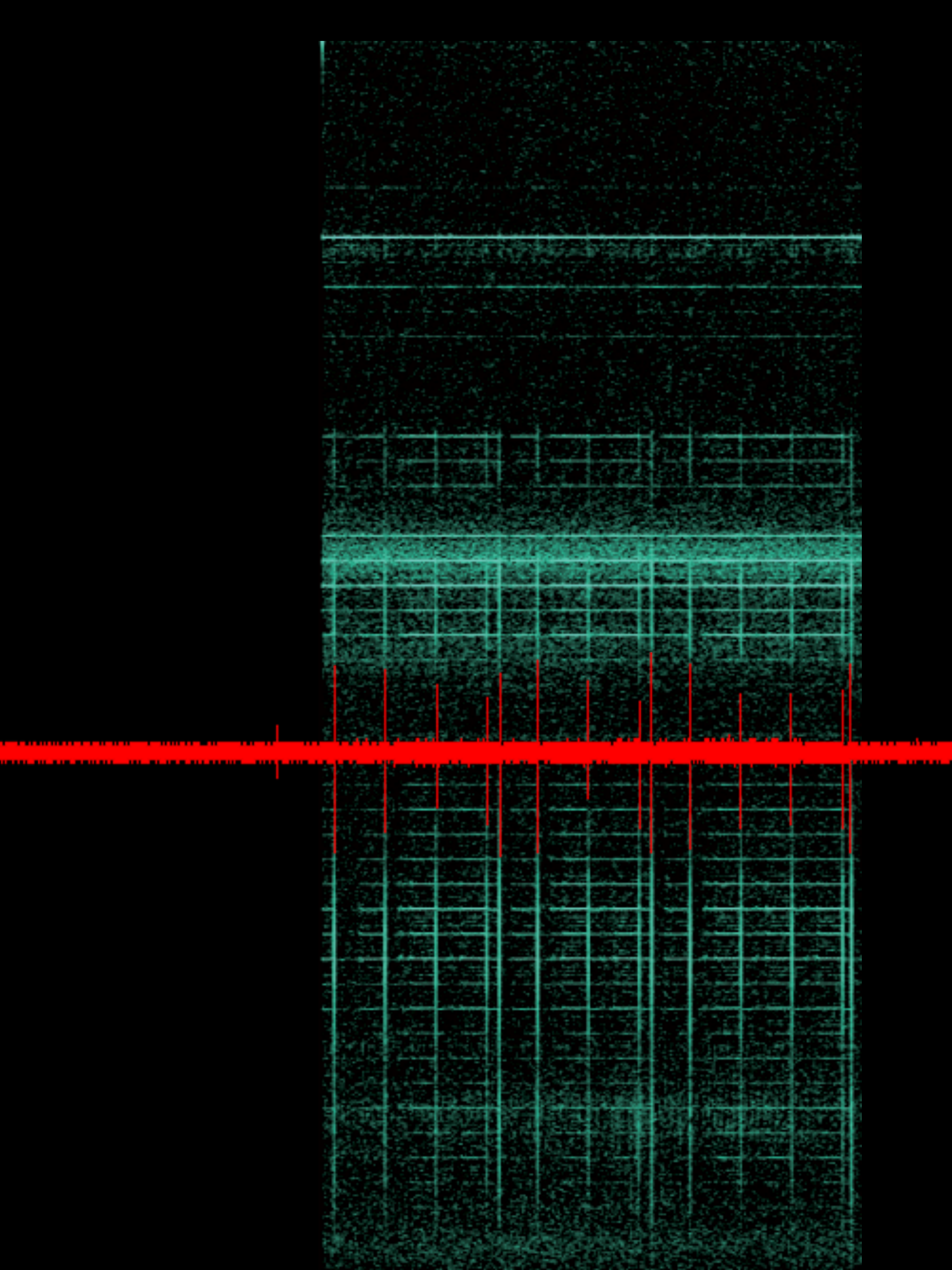
0001001001 1

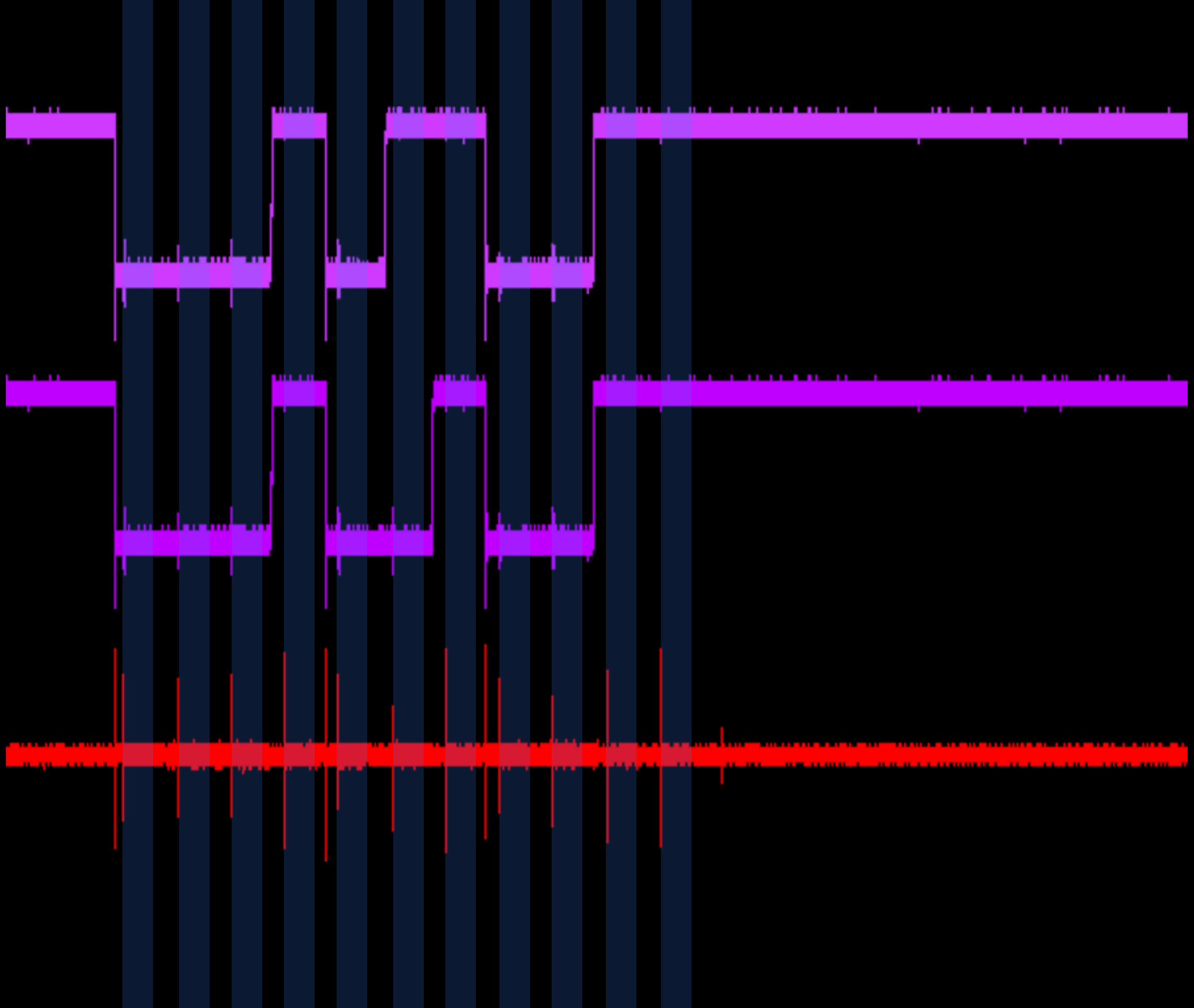



0001001001 1

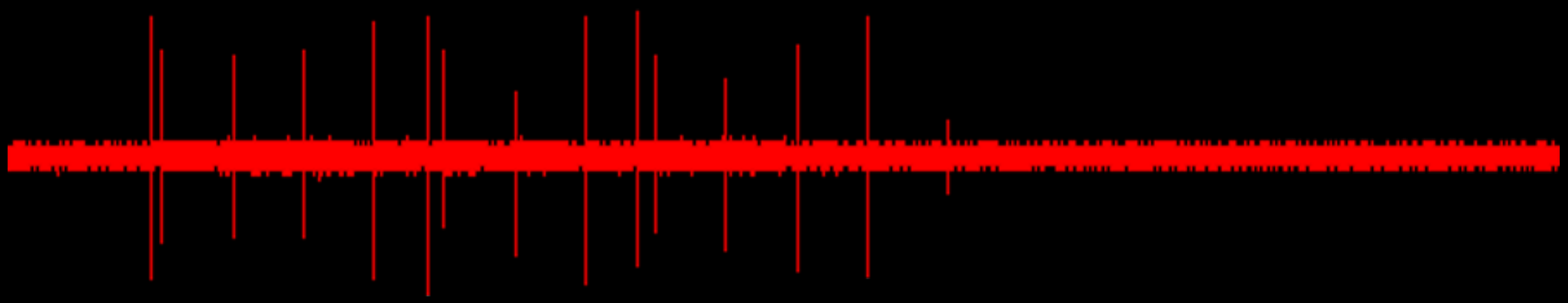
00100100 = 0x24 = E







21112112111 = 3,6,E,G

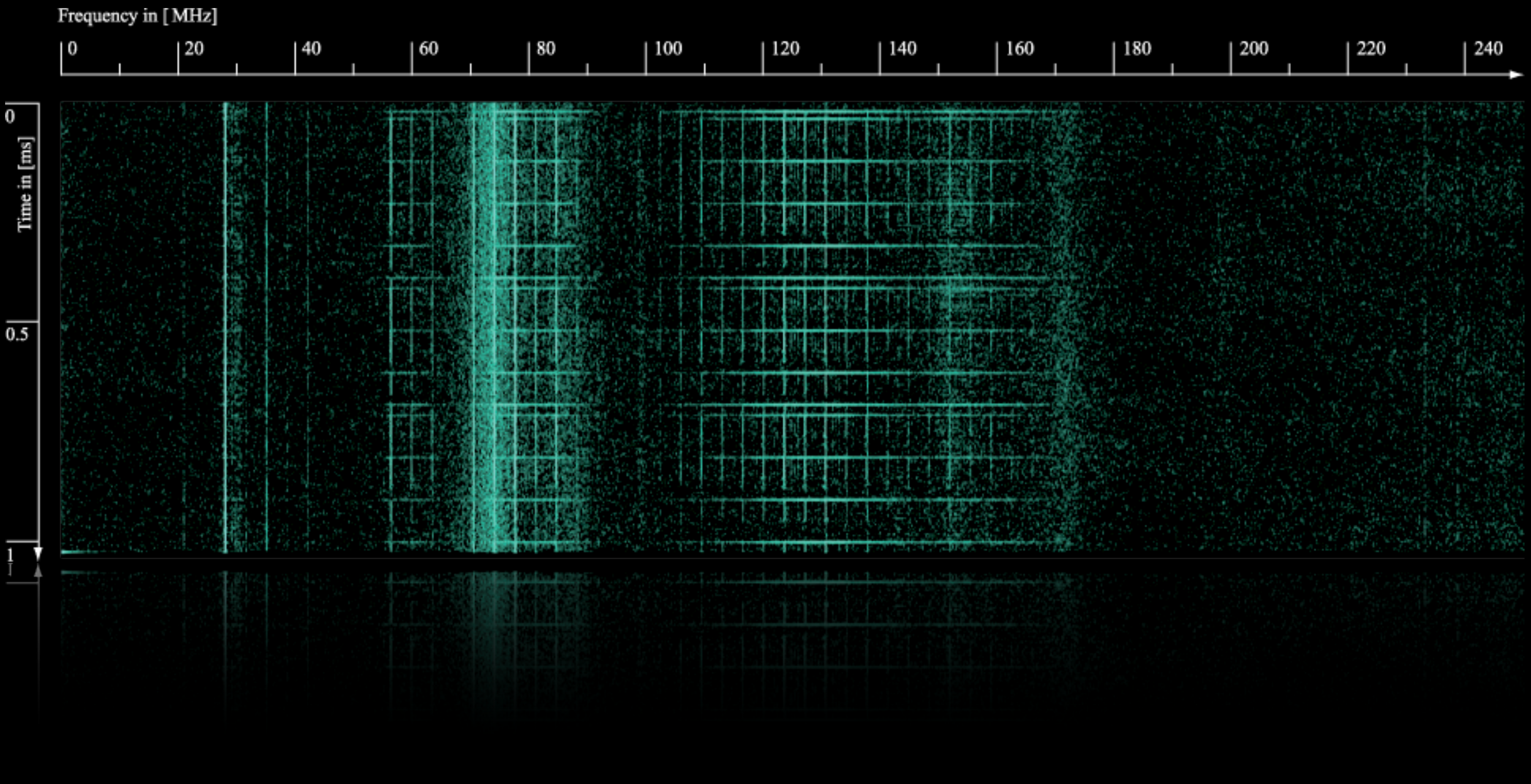


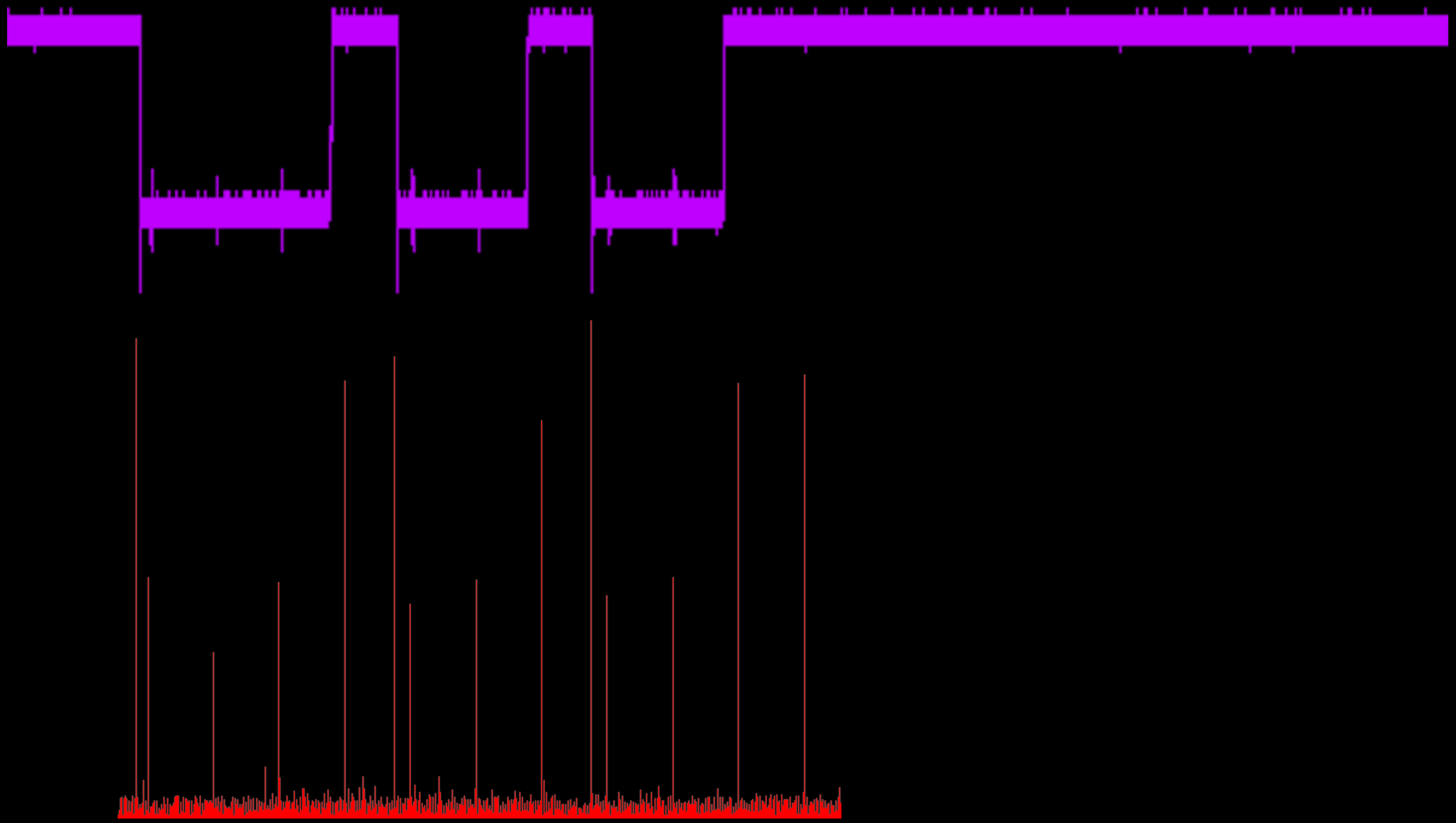
21111111111 <non-US-1>
21111111121 <Release key>
21111111211 F11 KP KP0 SL
21111112111 8 u
21111121111 2 a
21111121211 Caps Lock
21111211111 F4 ‘
21111211211 - ; KP7
21111212111 5 t
21112111111 F12 F2 F3
21112111121 Alt+SysRq
21112111211 9 Bksp Esc KP6 NL o
21112112111 3 6 e g
21112121111 1 CTRL L
21112121211 [
21121111111 F5 F7
21121111211 KP- KP2 KP3 KP5 i k
21121112111 b d h j m x
21121121111 SHIFT L s y
21121121211 ’ ENTER]
21121211111 F6 F8
21121211211 / KP4 l
21121212111 f v
21211111111 F9
21211111211 , KP+ KP. KP9
21211112111 7 c n
21211121111 Alt L w
21211121211 SHIFT R \
21211211111 F10 Tab
21211211211 . KP1 p
21211212111 Space r
21212111111 F1
21212111211 0 KP8
21212112111 4 y
21212121111 q
21212121211 =

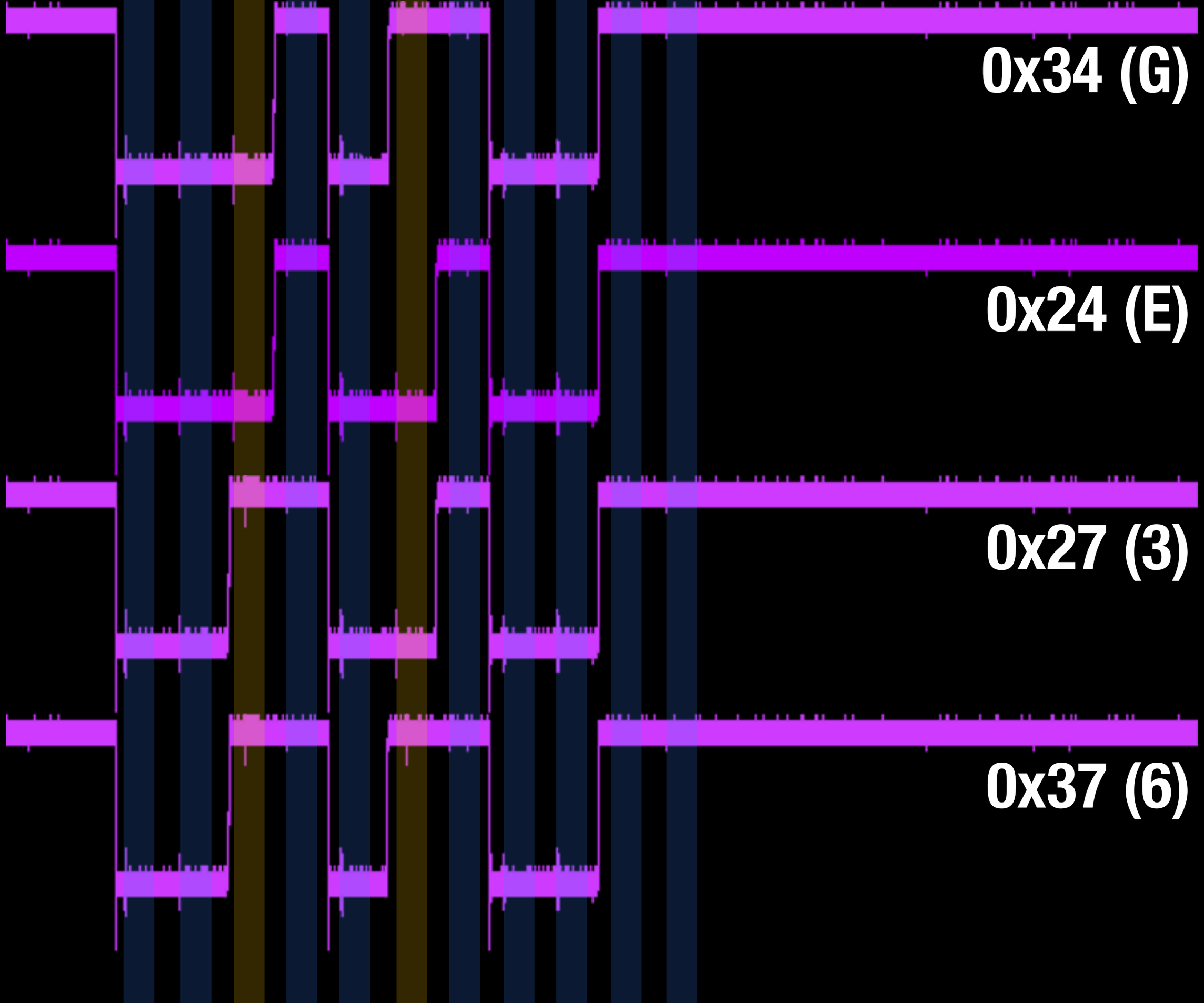
FALLING EDGE TRANSITION TECHNIQUE

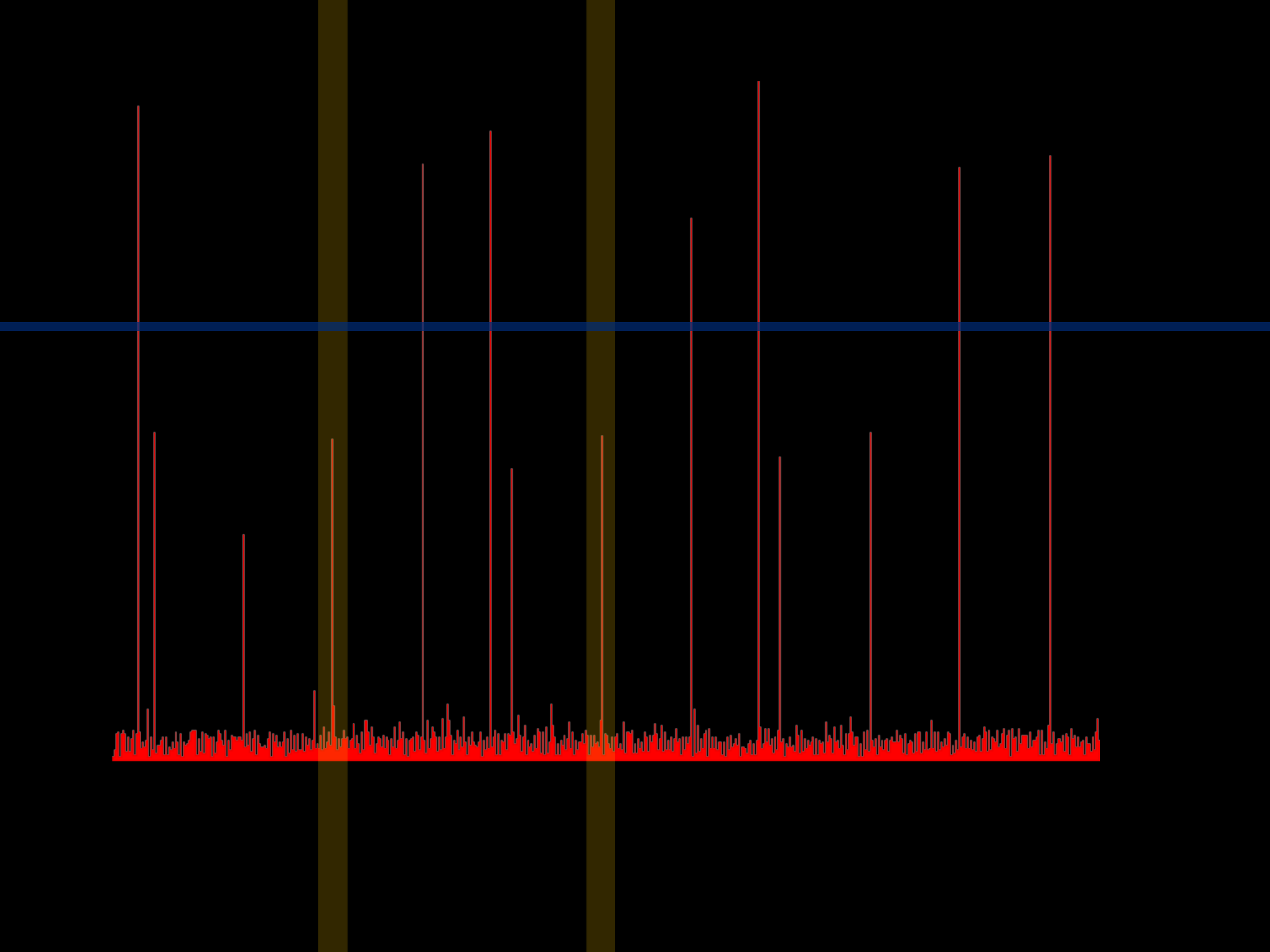
1. PEAK DETECTION
2. TRACE COMPARISON

HOW TO AVOID THESE COLLISIONS?


Frequency in [MHz]
0
20
40
60
80
100
120
140
160
180
200
220
240
Time in [ms]
0
0.5
1




0x34 (G)
0x24 (E)
0x27 (3)
0x37 (6)

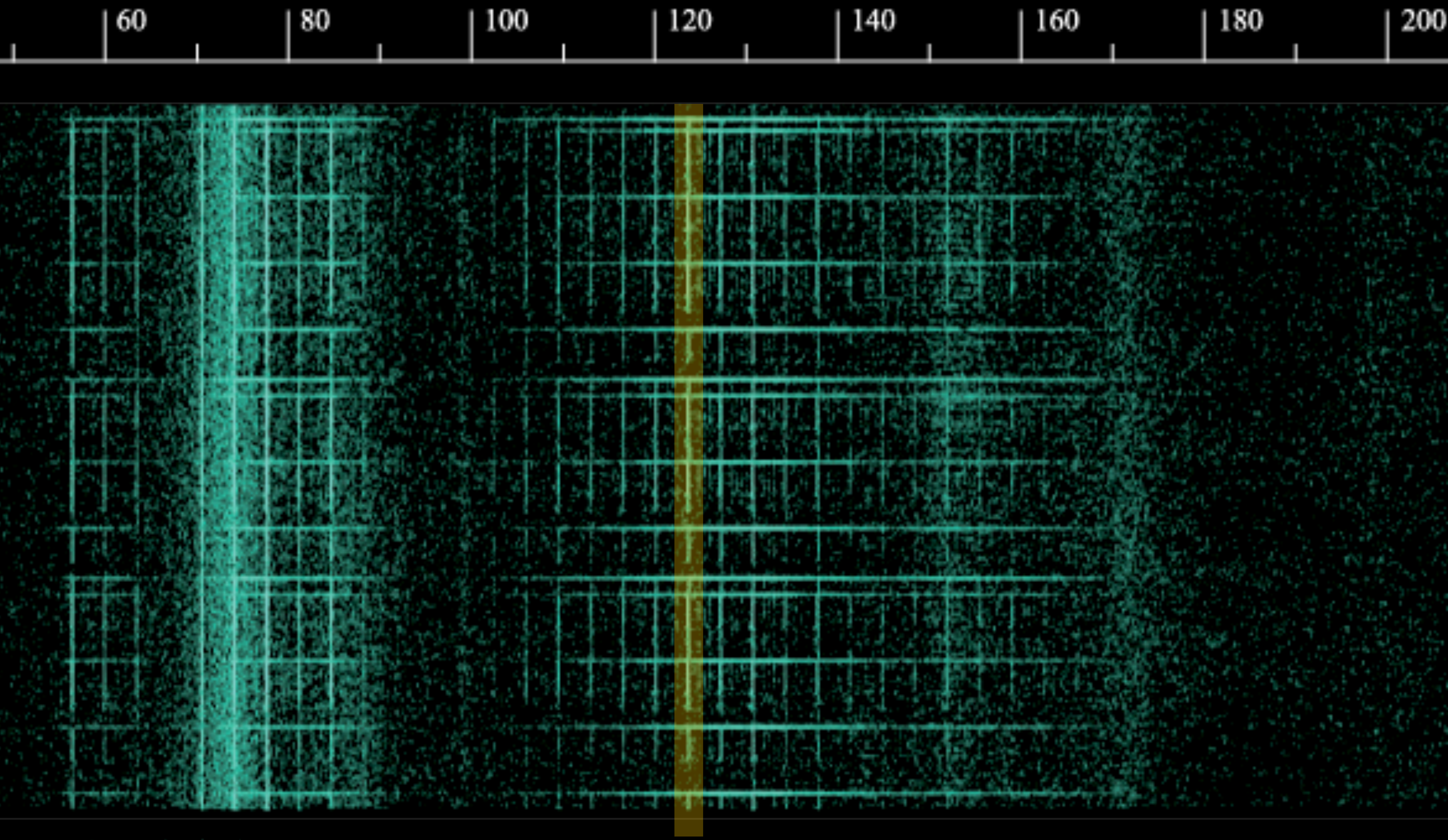


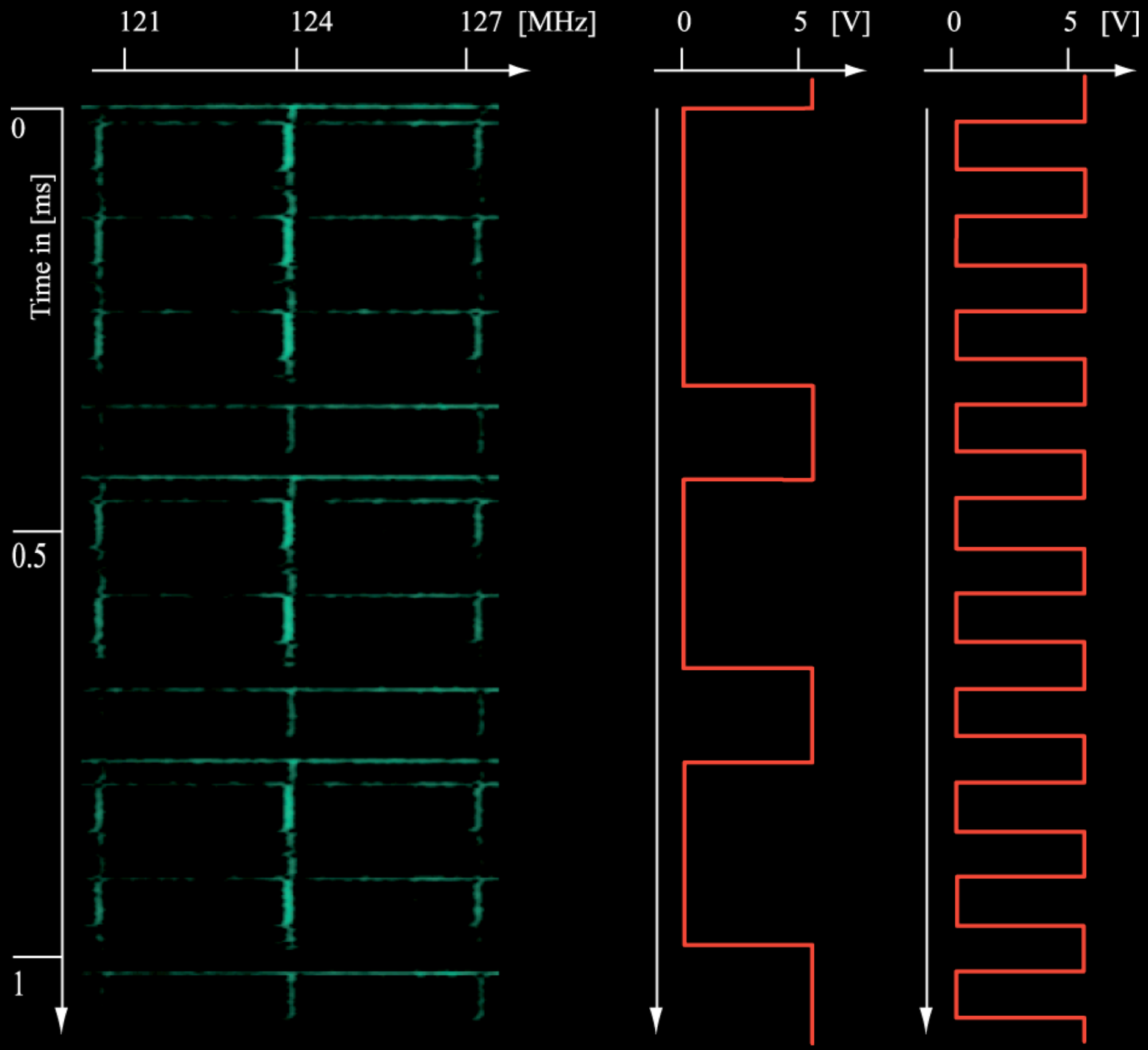
GENERALIZED TRANSITION TECHNIQUE

1. PEAK DETECTION
2. TRACE SUBSET (E,G,3,6)
3. COMPUTE THRESHOLD
4. MEASURE CRITICAL BITS

HOW TO DETECT COMPROMISING SIGNALS?

INDIRECT EMANATIONS

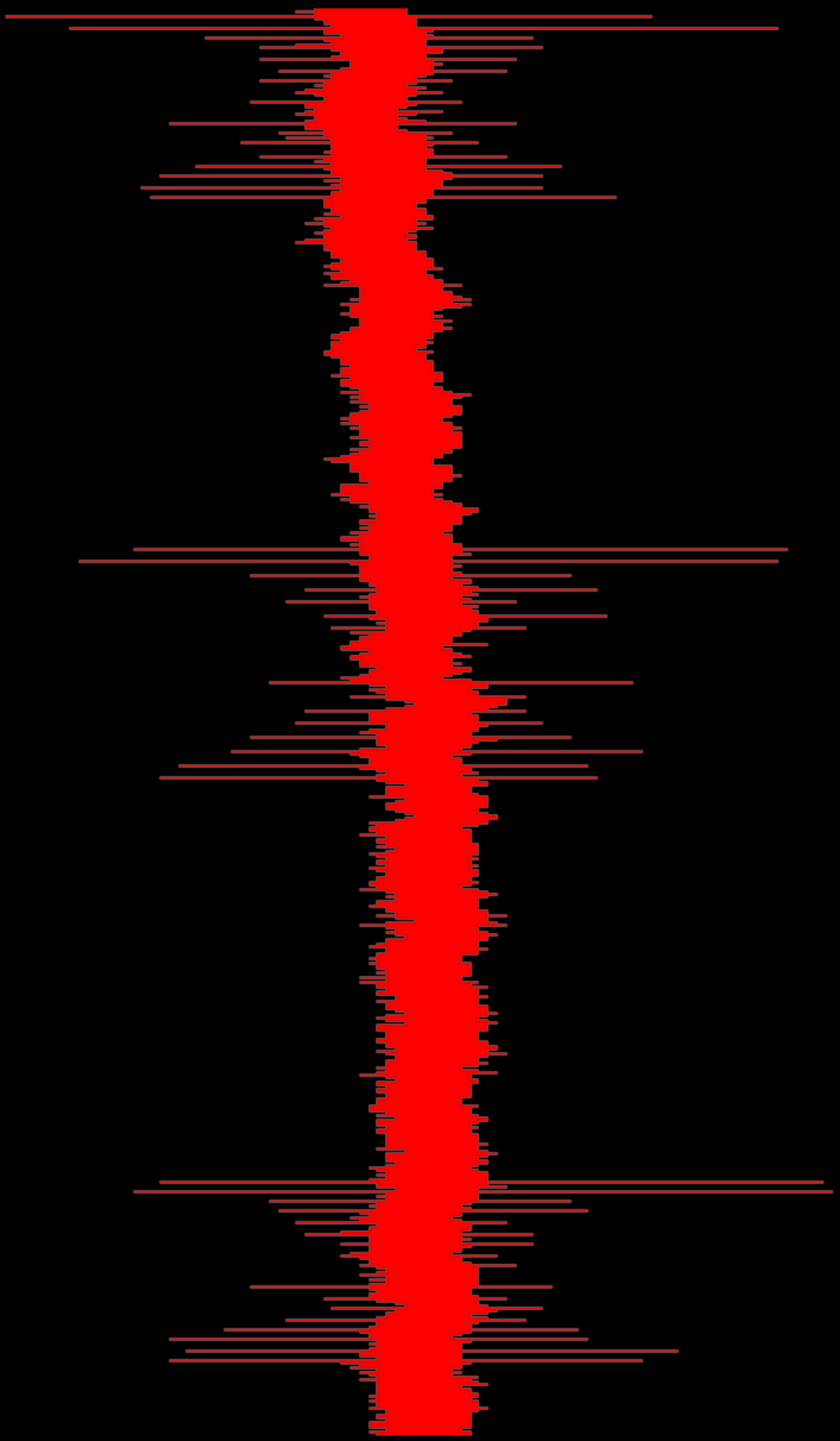

60
80
100
120
140
160
180
200

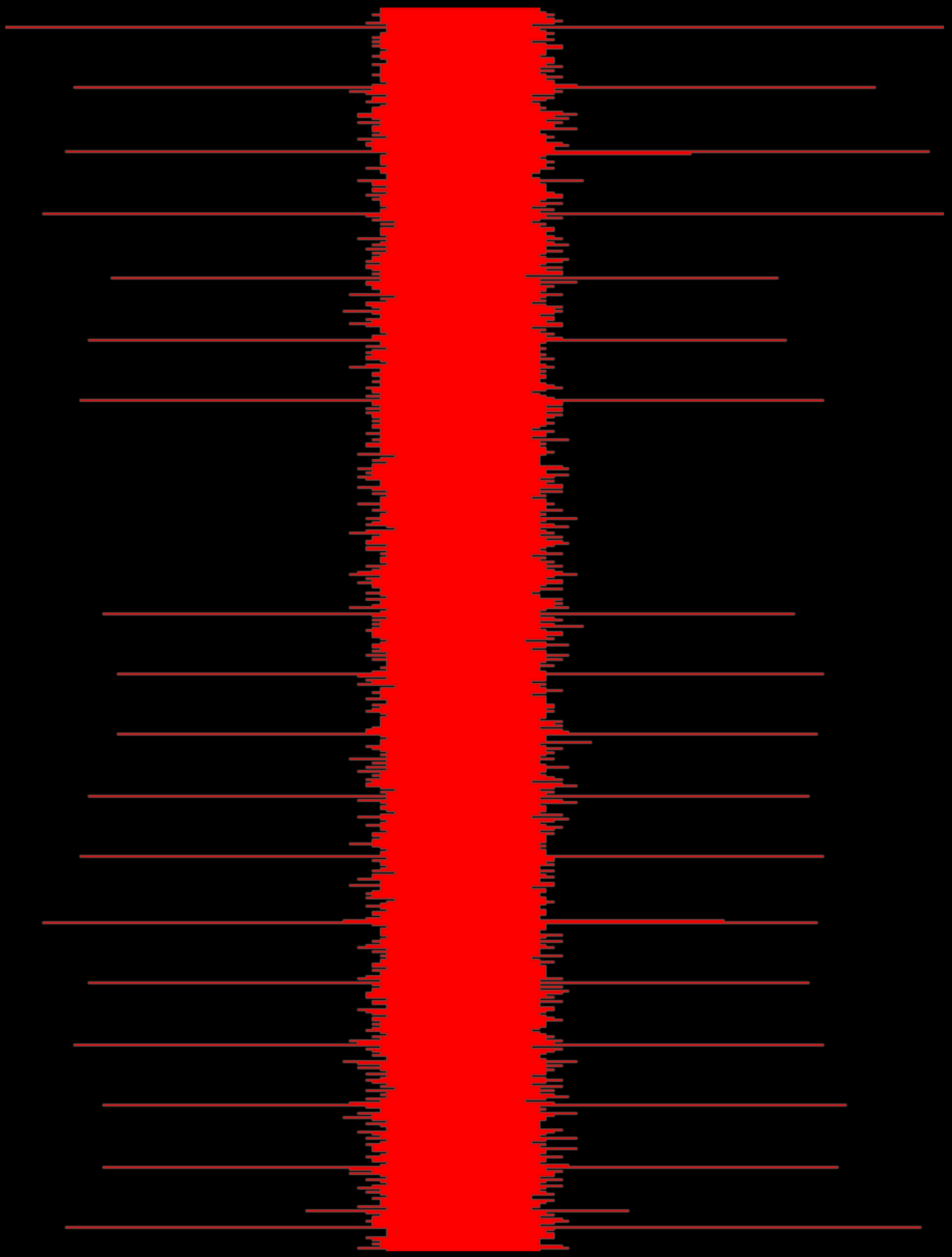

121
124
127 [MHz]
0
5 [V]
0
5 [V]
0
Time in [ms]
0.5
1

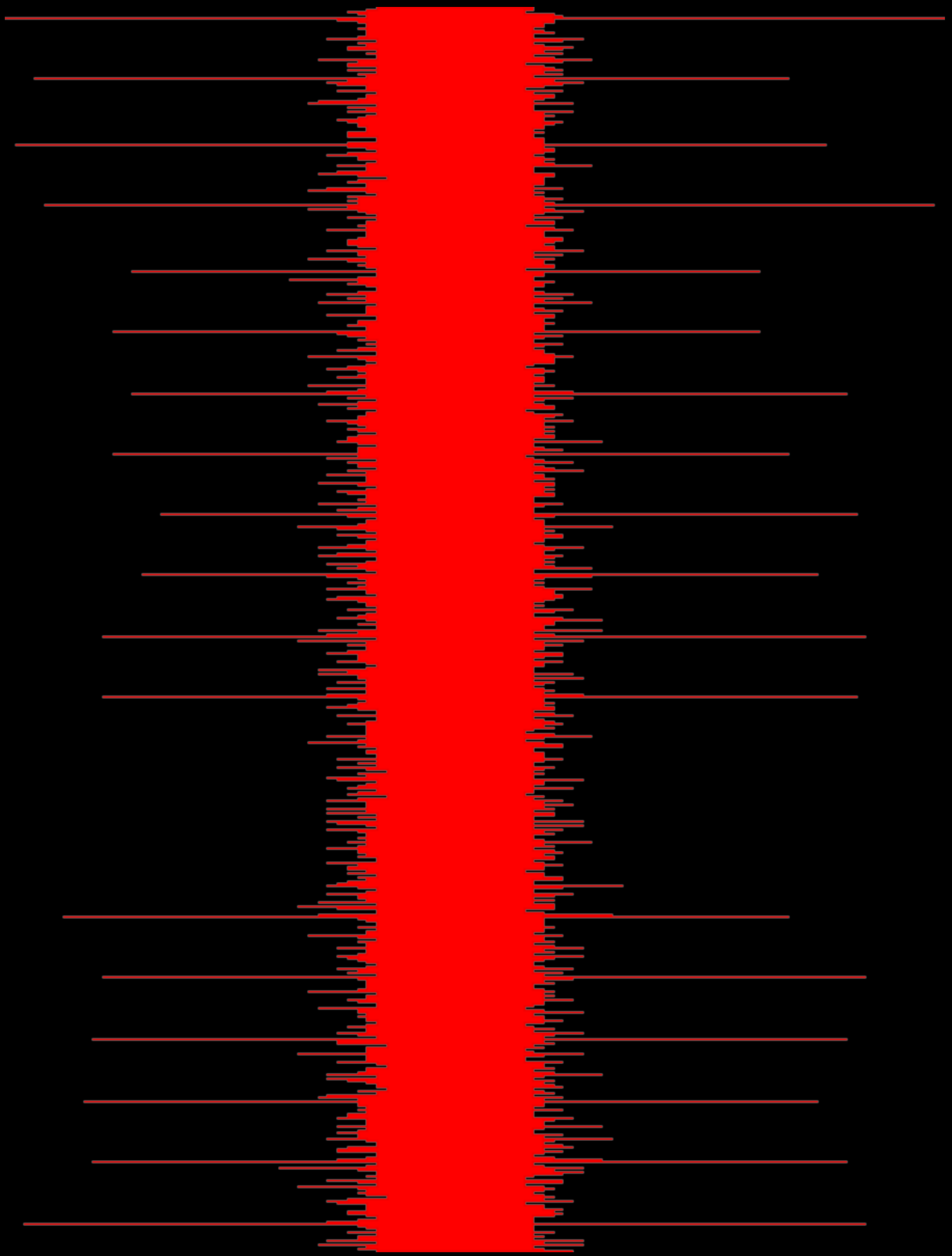
MODULATION TECHNIQUE

1. DETECT CARRIER(S)
2. DEMODULATION (AM & FM)

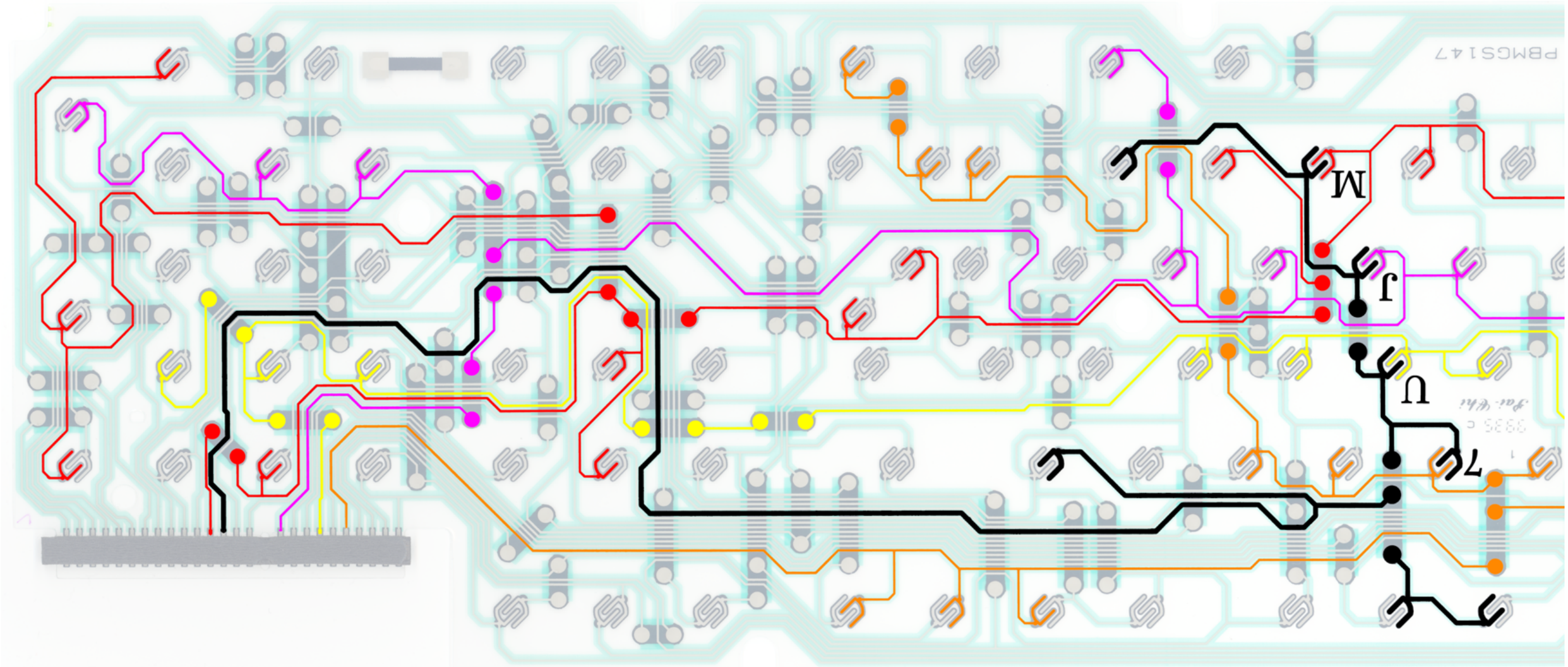
WHAT ABOUT USB AND WIRELESS KEYBOARDS?

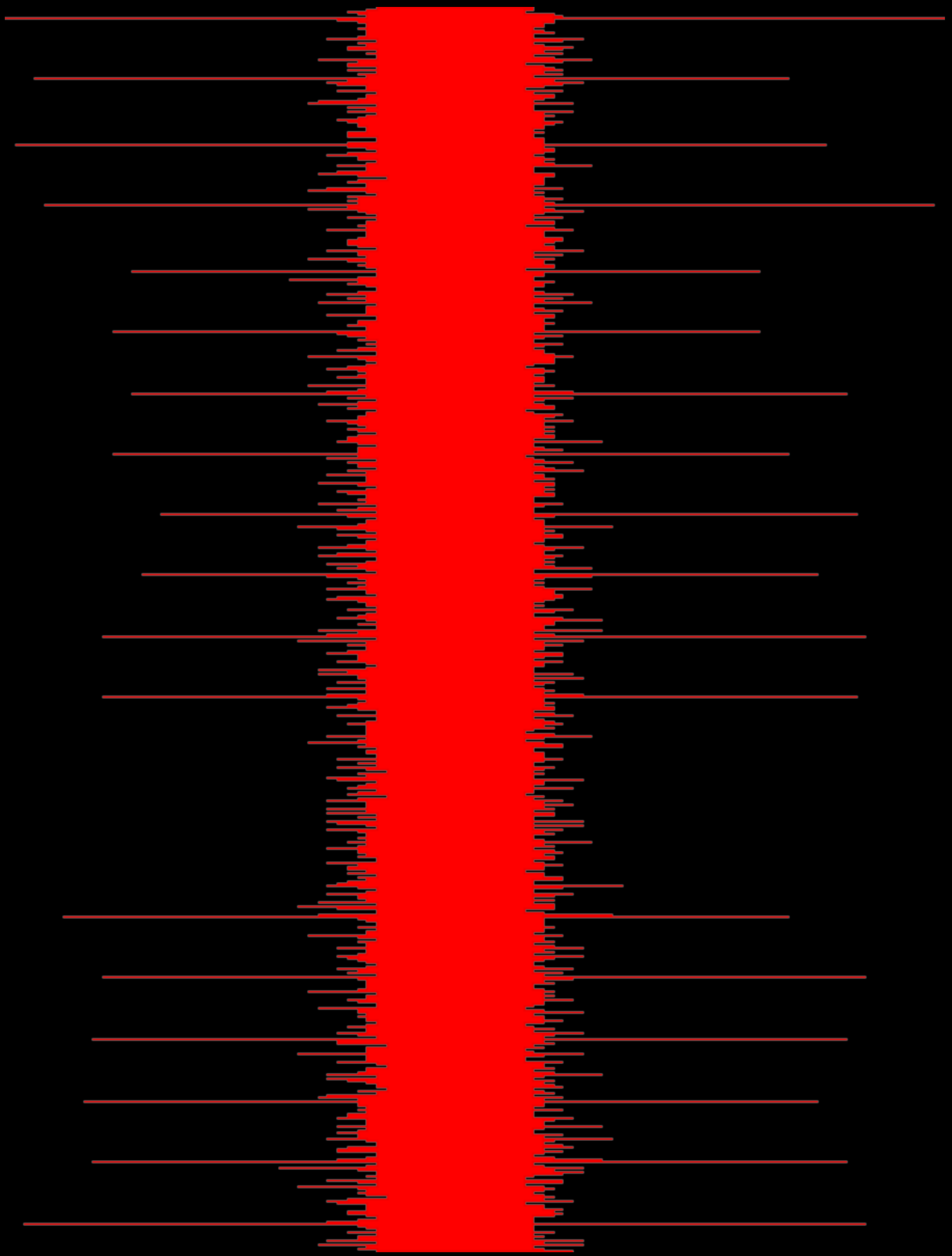






7	6, 7, H, J, M, N, U, Y
8	4, 5, B, F, G, R, T, V
9	BACKSPACE, ENTER
10	9, L, O
11	0, P
12	3, 8, C, D, E, I, K
13	1, 2, S, W, X, Z
14	SPACE, A, Q


M
J
U
11
7



MATRIX SCAN TECHNIQUE

1. PEAK DETECTION
2. TRACE COMPARISON

filtered as in Fig. 7 and the received Tempest signal has vanished except for the horizontal sync pulses.

to its periodic nature, a video signal can easily be separated from other signals and from noise by periodic averaging.

We have identified two more potential sources of periodic signals in every PC, both of which can be fixed at low cost by software or at worst firmware changes [28]. Keyboard controllers execute an endless key-matrix scan loop, with the sequence of instructions executed depending on the currently pressed key. A short random wait routine inside this loop and a random scan order can prevent an eavesdropper doing periodic averaging. Secondly, many disk drives read the last accessed track continuously until another access is made. As an attacker might try to reconstruct this track by periodic averaging, we suggest that after accessing sensitive data, the disk head should be moved to a track with unclassified data unless further read requests are in the queue.

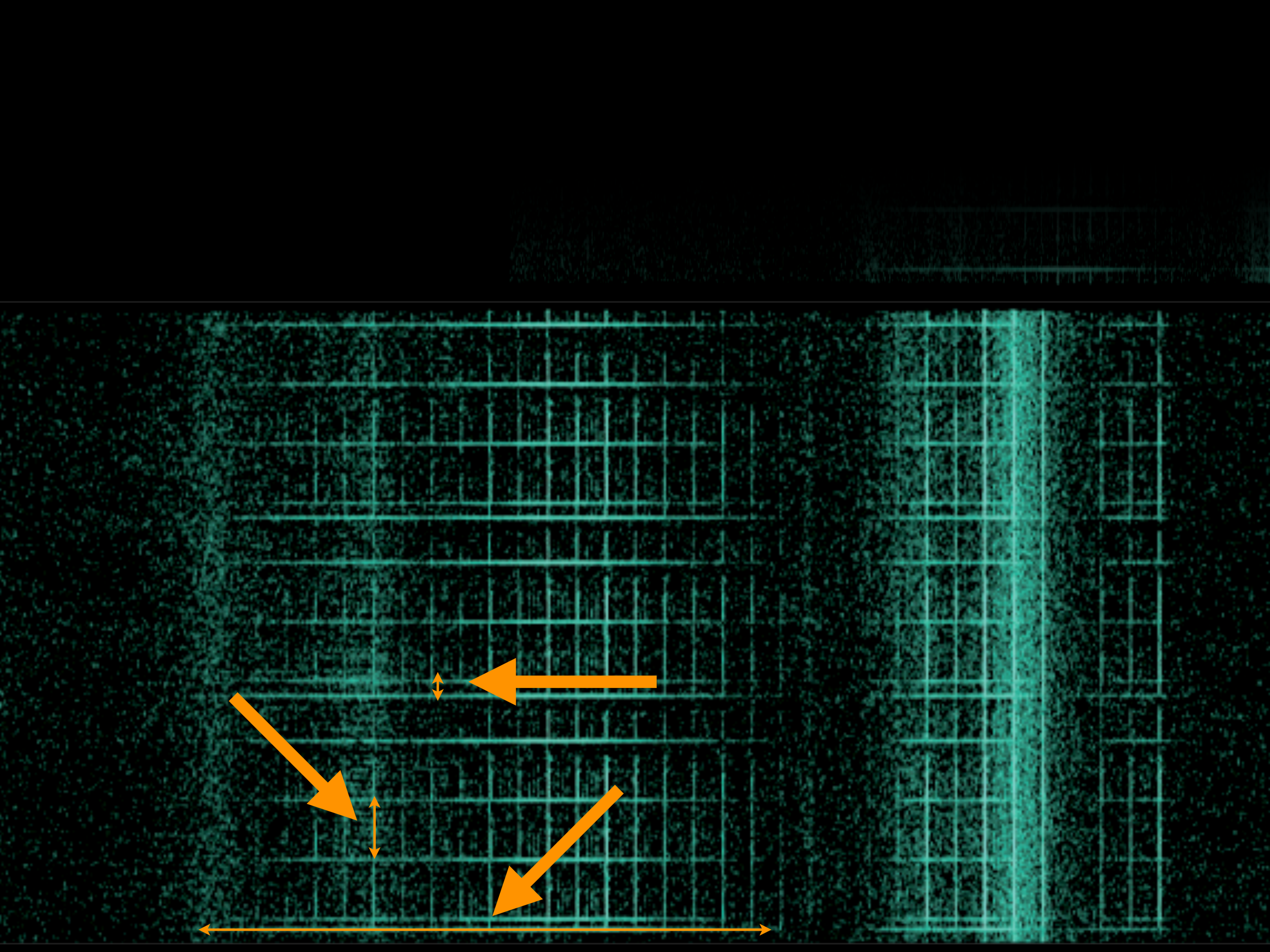
DRAM refresh is another periodic process in every computer that deserves consideration. The emanations from most other sources, such as the CPU and peripherals, usually [illegible] periodically, [illegible] knowledge of the system configuration and the executed software.

We are convinced that our Soft Tempest techniques, and in particular Tempest fonts, can provide a significant increase in emanation security at a very low cost. There are many applications where they may be enough; in medium sensitivity applications, many governments use a zone model in which computers with confidential data are not shielded but located in rooms far away from accessible areas. Here, the 10–20 dB of protection that a Tempest font affords

MARKUS KUHN & ROSS ANDERSON

1998

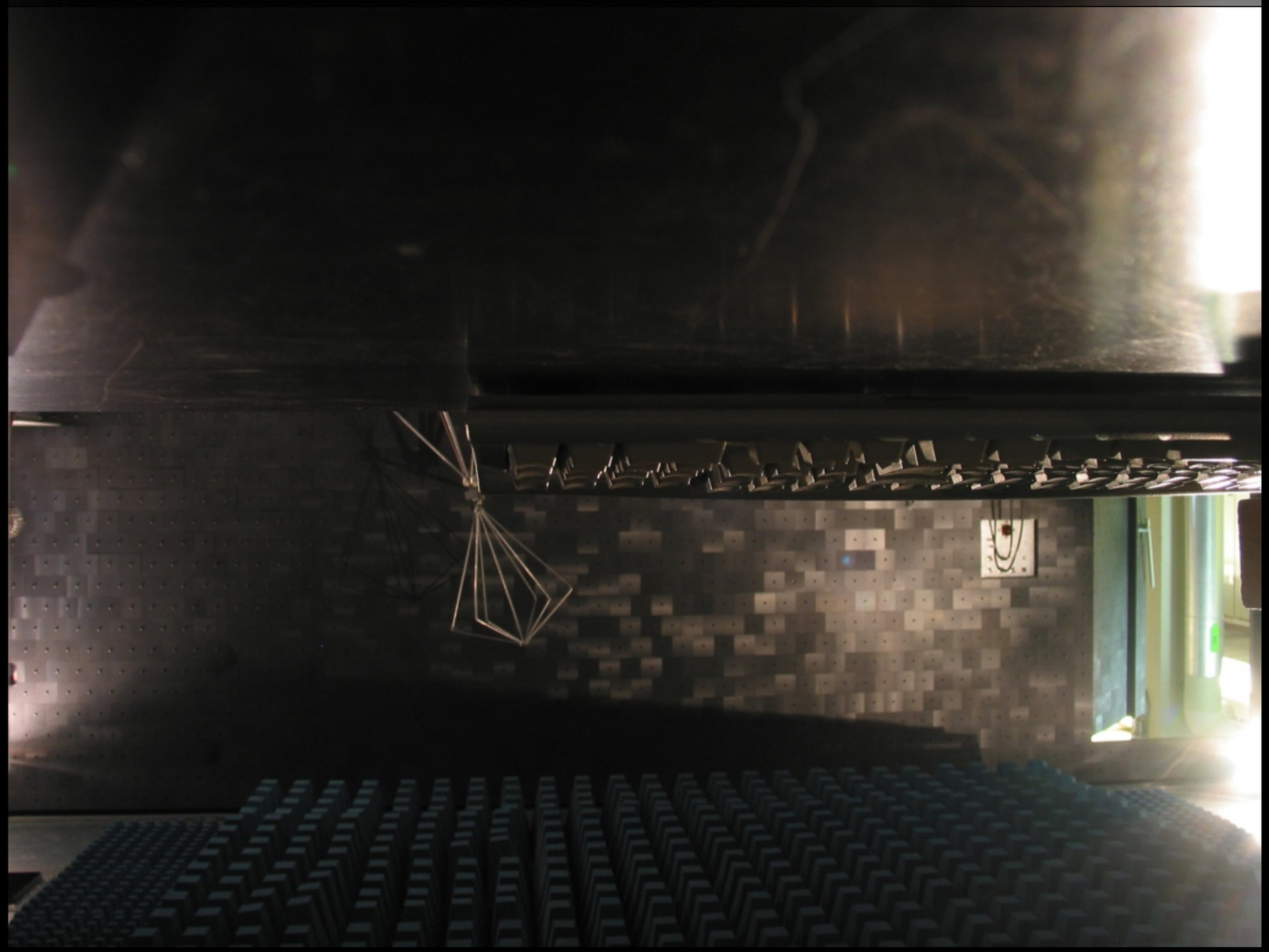
MULTIPLE KEYBOARDS

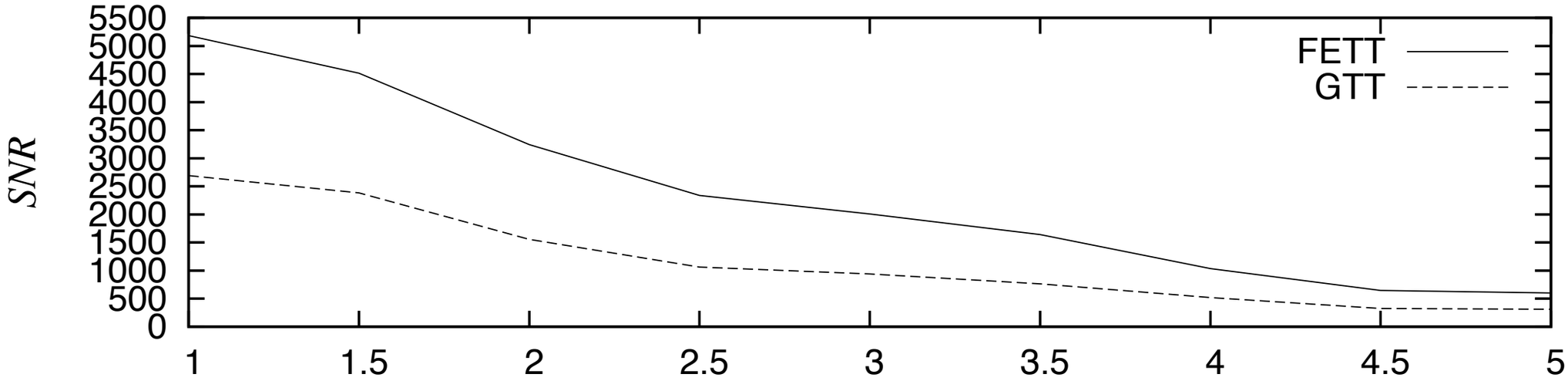


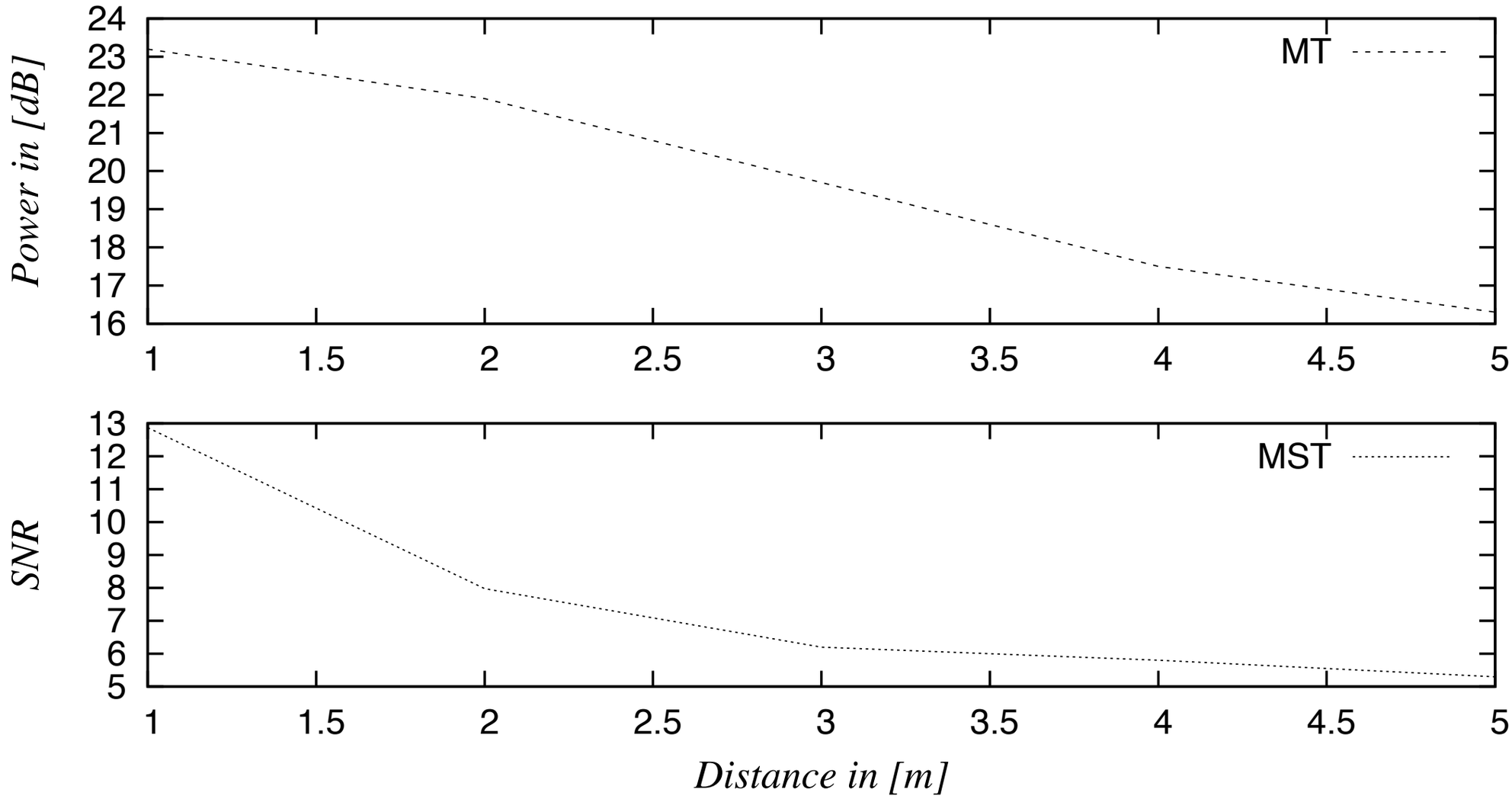
THEORY VS. PRACTICE

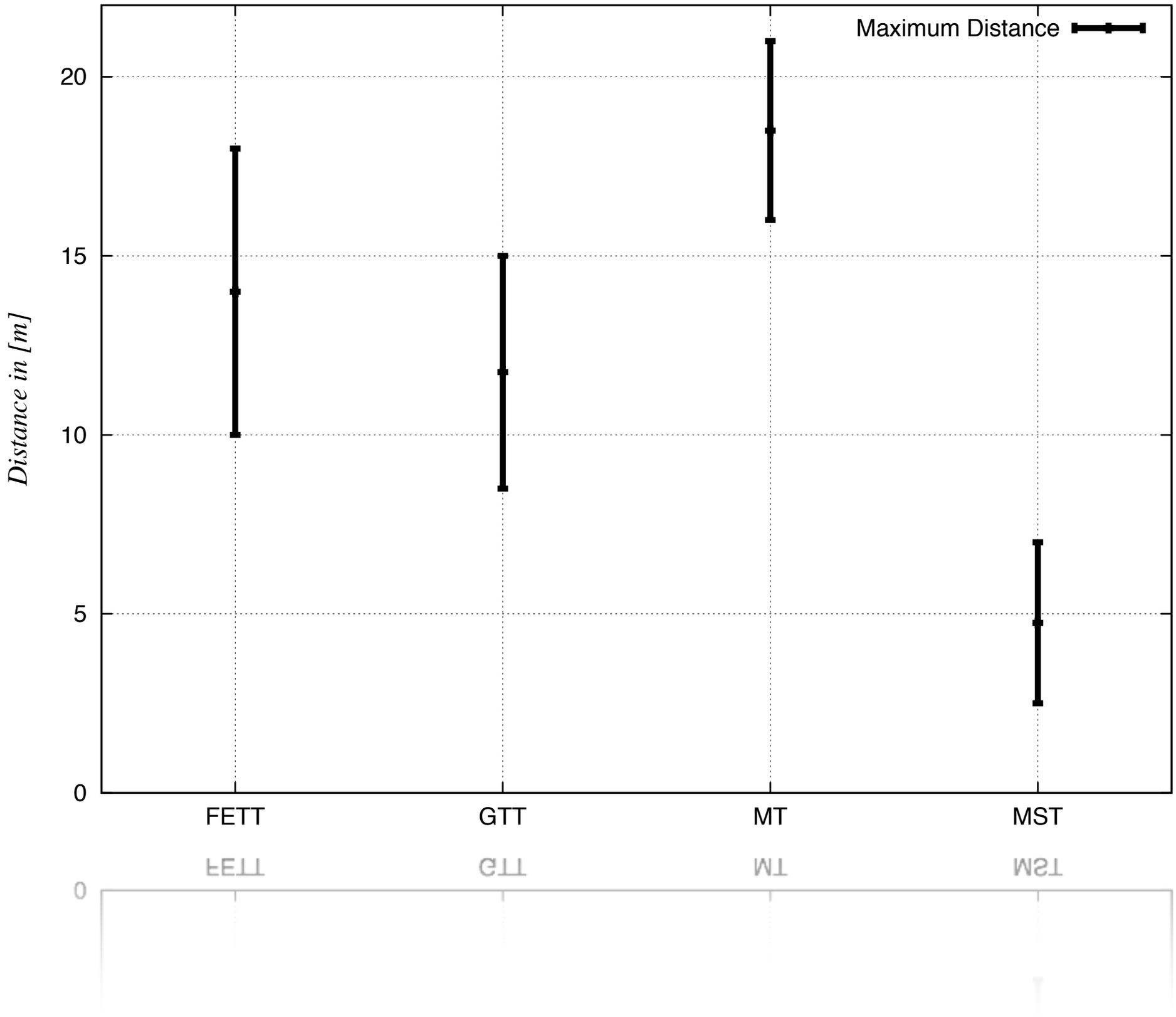
RECOVER 95% OF 500+ KEYSTROKES

SETUP1: A SEMI ANECHOIC CHAMBER

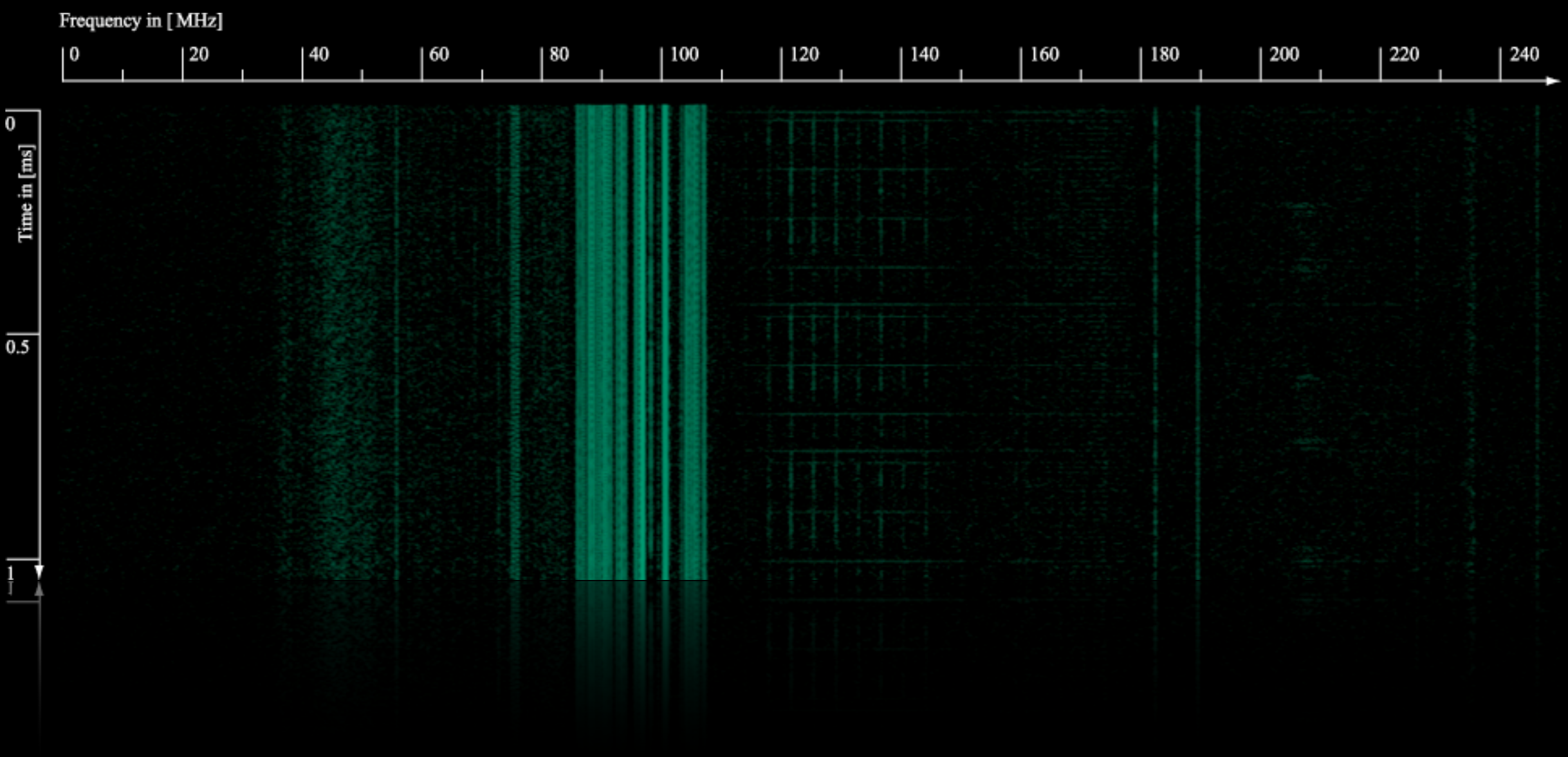


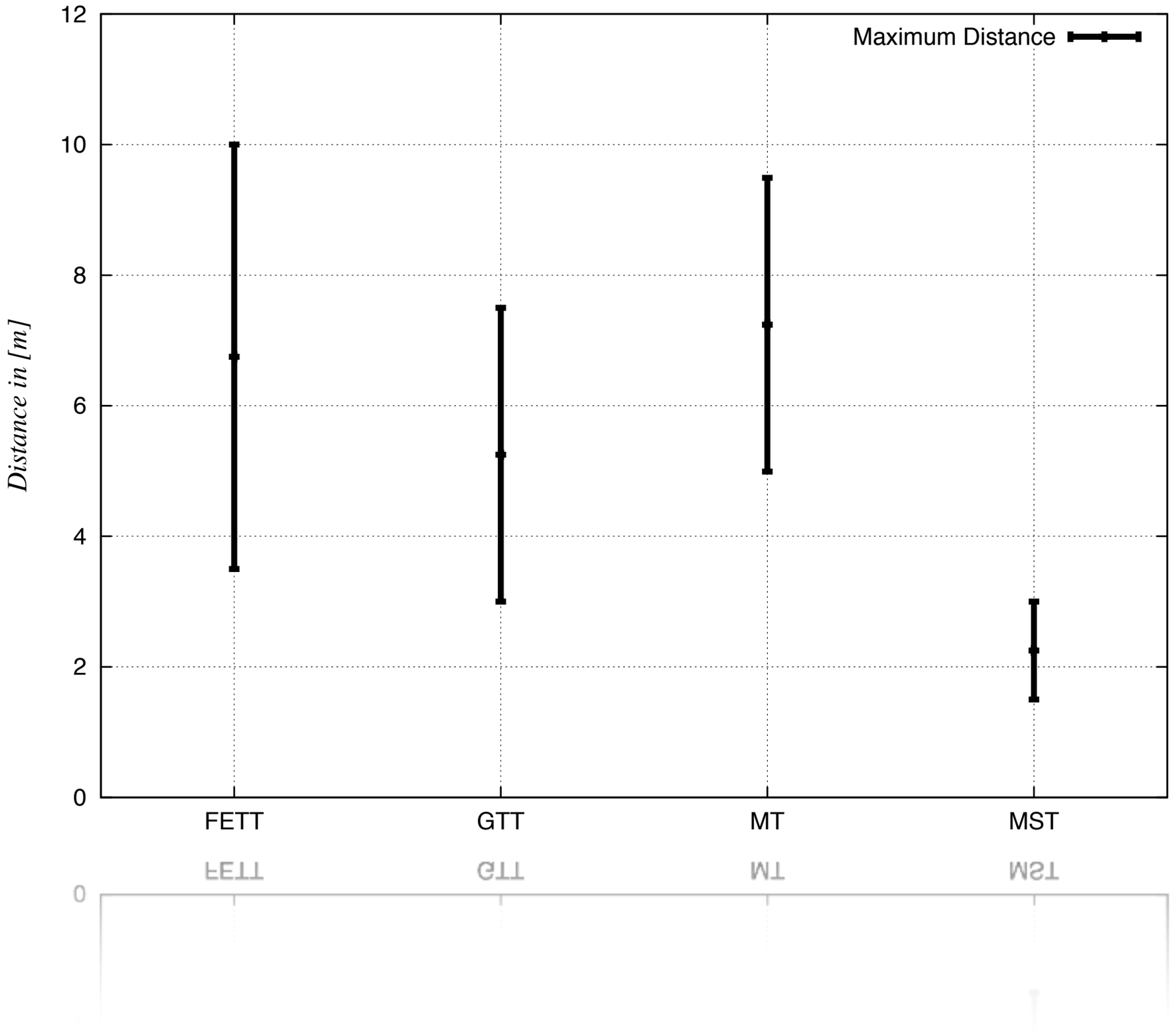

SNR
5500
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
1
1.5
2
2.5
3
3.5
4
4.5
5
FETT
GTT


Power in [dB]
24
23
22
21
20
19
18
17
16
1
1.5
2
2.5
3
3.5
4
4.5
5
MT
SNR
13
12
11
10
9
8
7
6
5
MST
Distance in [m]


Maximum Distance
20
15
10
5
0
Distance in [m]
FETT
GTT
MT
MST

SETUP2: THE OFFICE


Frequency in [MHz]
0
20
40
60
80
100
120
140
160
180
200
220
240
Time in [ms]
0
0.5
1


Maximum Distance
Distance in [m]
12
10
8
6
4
2
0
FETT
GTT
MT
MST

SETUP3: THE OFFICE WITH WALL

VIDEO


Ettus
Research
USRP
Universal Software Radio Peripheral
TRIGGER

SETUP4: A FLAT

ALL THE ATTACKS WORKS WITH THE KEYBOARD AT THE 5th FLOOR AND THE ANTENNA IN THE BASEMENT, 20 METERS AWAY!

SHARED GROUND OF THE BUILDING ACT AS **ANTENNA!**

CONDUCTIVE AND RADIATIVE COUPLING

DISTANCE BETWEEN THE KEYBOARD AND THE SHARED GROUND

+

DISTANCE BETWEEN THE SHARED GROUND AND THE ANTENNA

WATER PIPE OF THE BUILDING CAN BE USED AS WELL:

BETTER SIGNAL-TO-NOISE RATIO SINCE LESS ELECTRIC POLLUTION

THANKS TO

ERIC AUGE
LUCAS BALLARD
DAVID JILLI
MARKUS KUHN
ERIC OLSON
FARHAD RACHIDI
PIERRE ZWEIACKER