Screen Gleaning

Receiving and Interpreting Pixels by Eavesdropping on Video Signals without a Line of Sight

February 25th, 2021

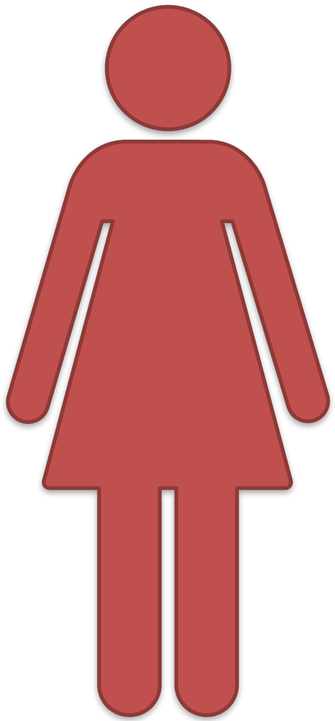
Dirk Lauret, Zhuoran Liu and Léo Weissbart

LASER 2021

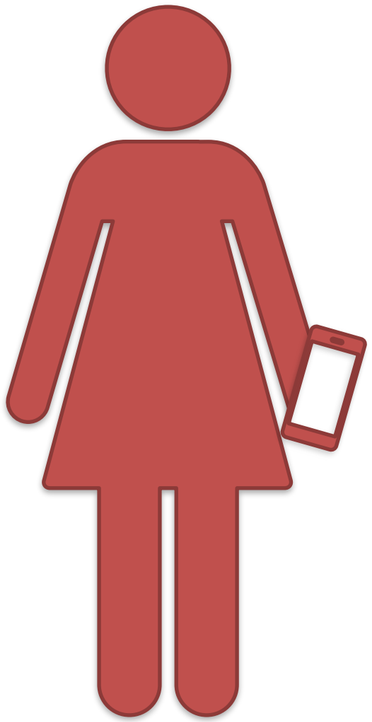
Radboud Universiteit

Imagine…

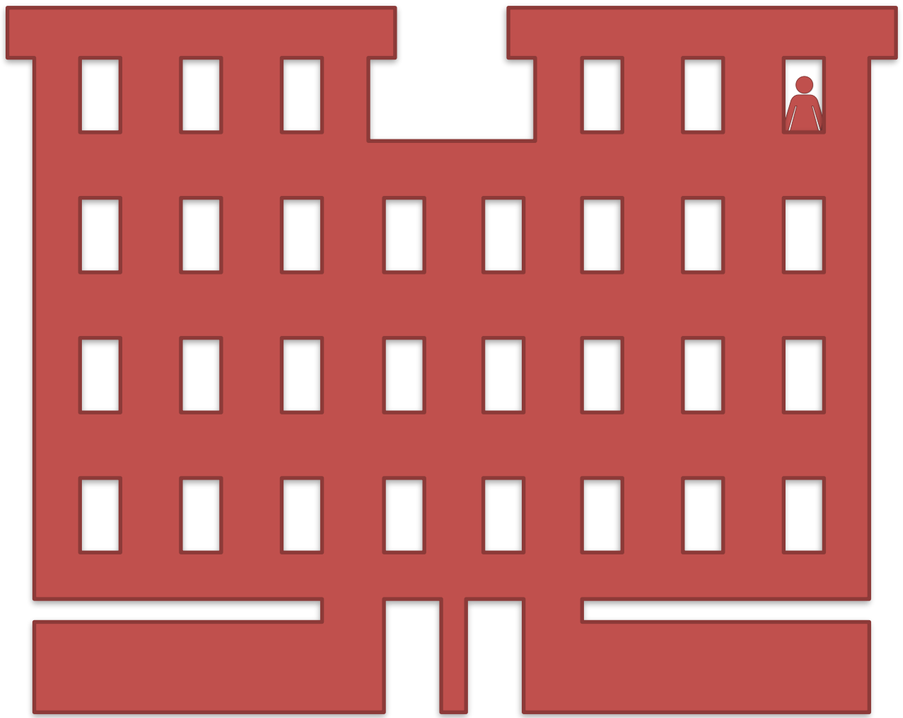
Imagine…



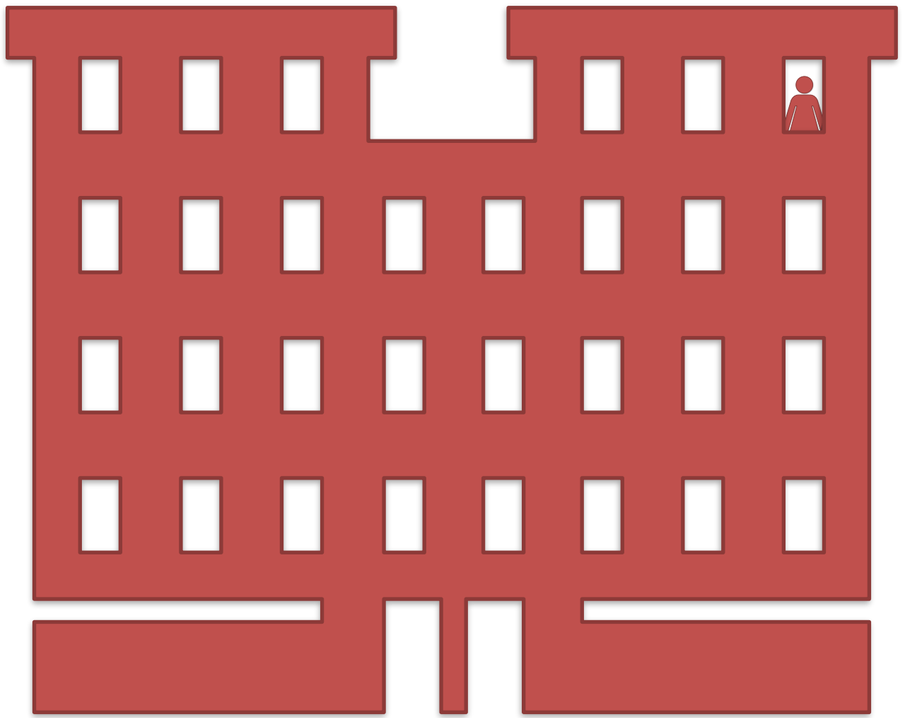
Imagine…

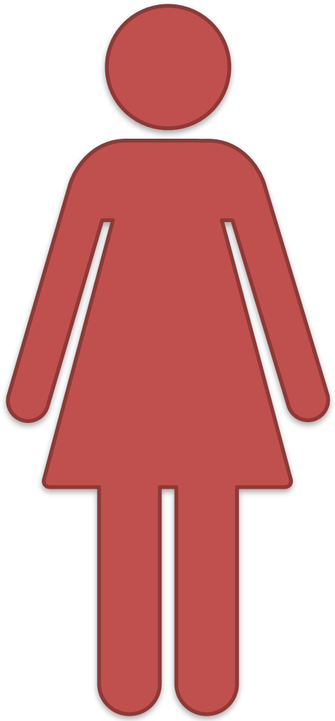


Imagine…

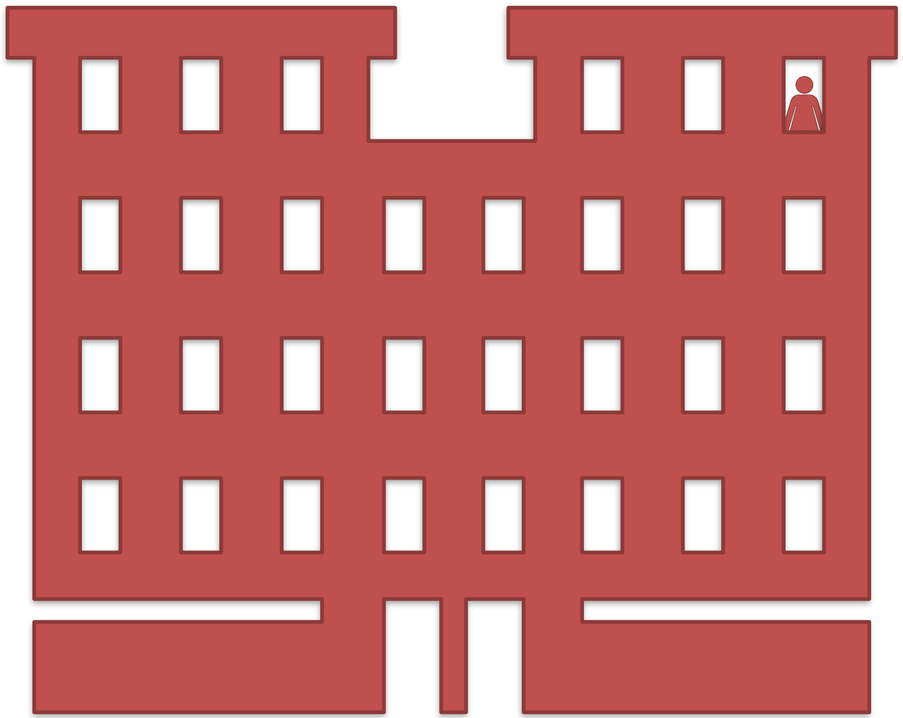


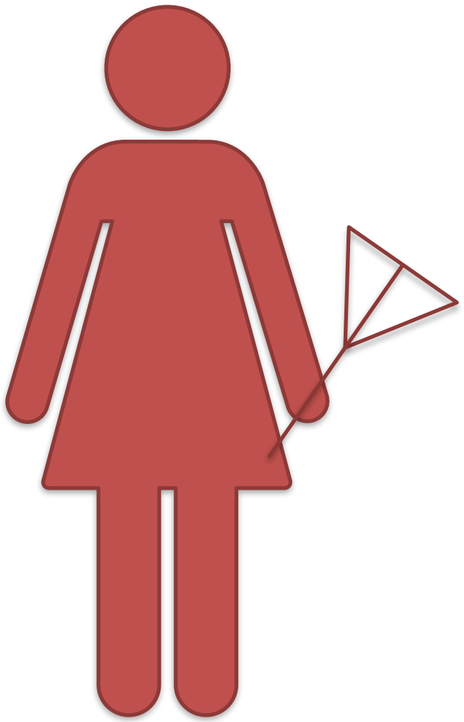
Imagine…



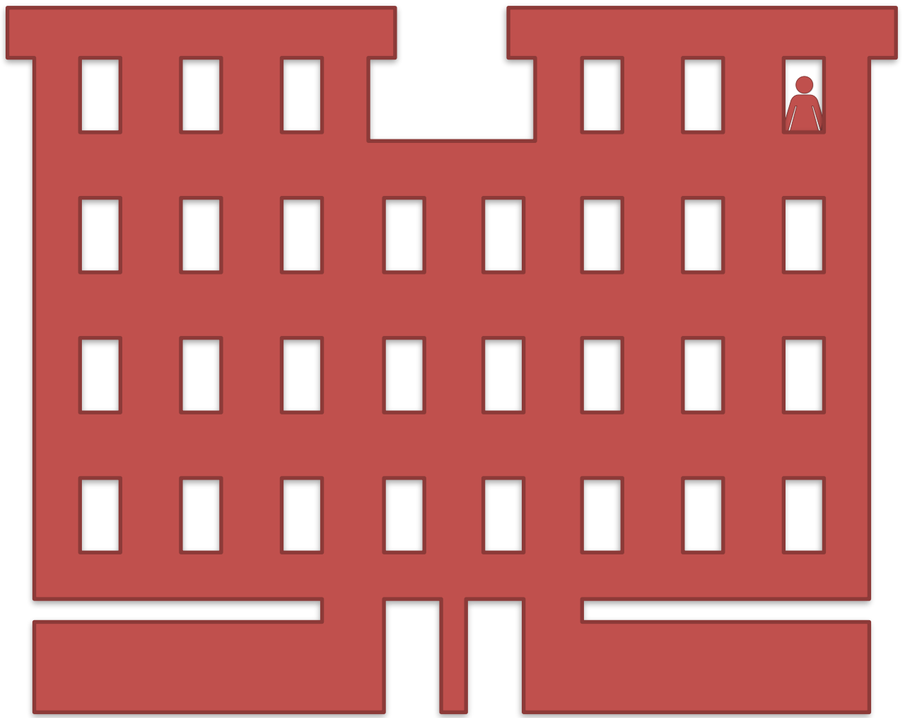


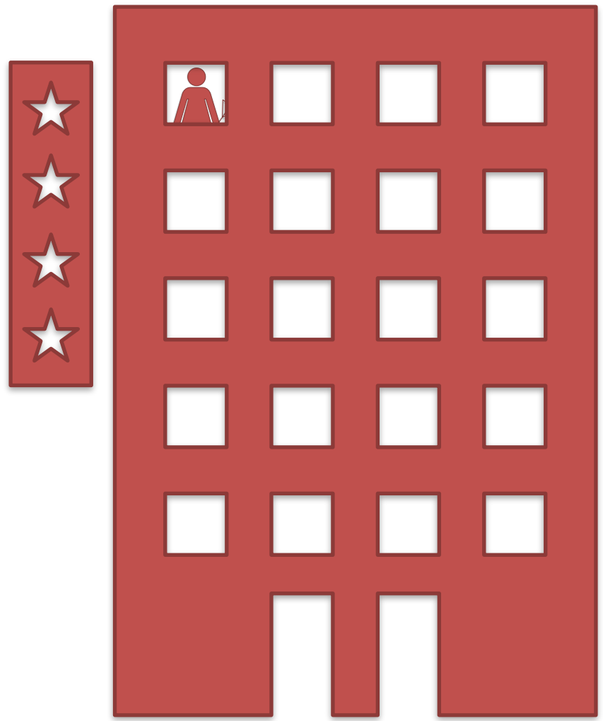
Imagine…





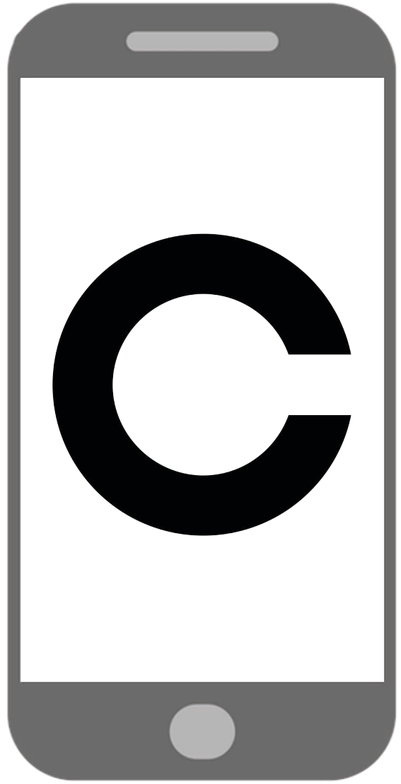
Imagine…



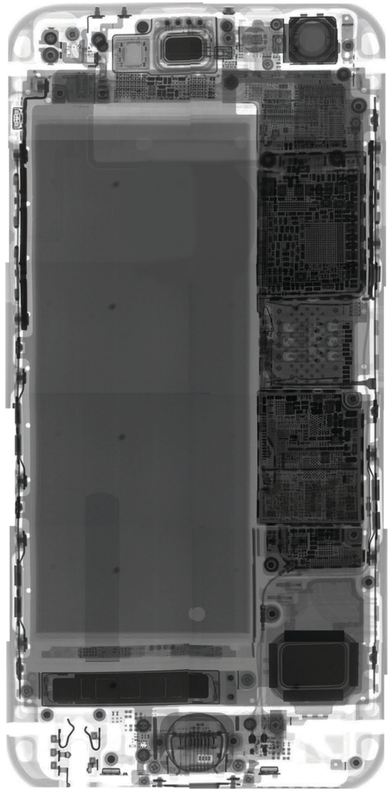


The Setup

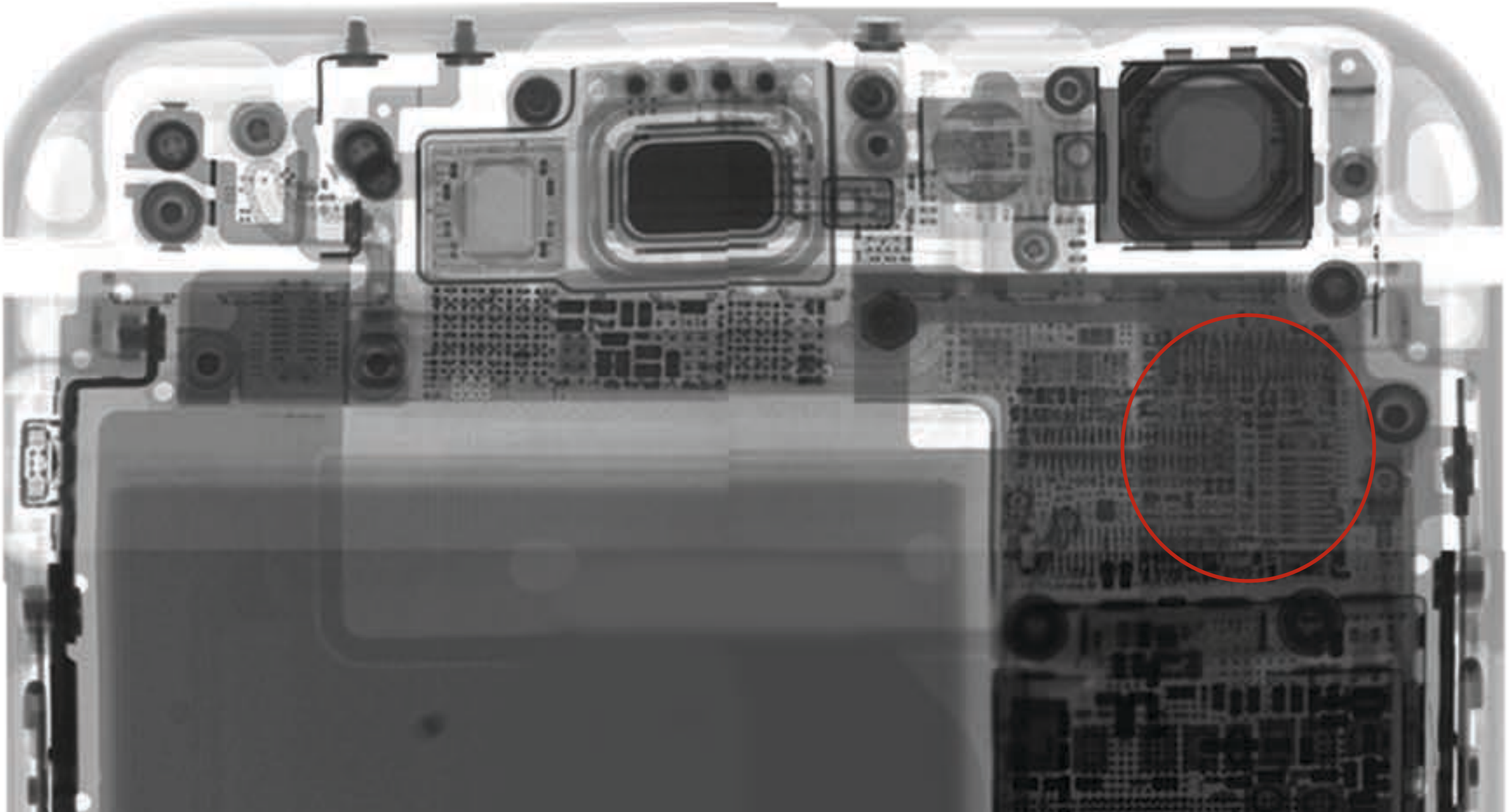
The Setup



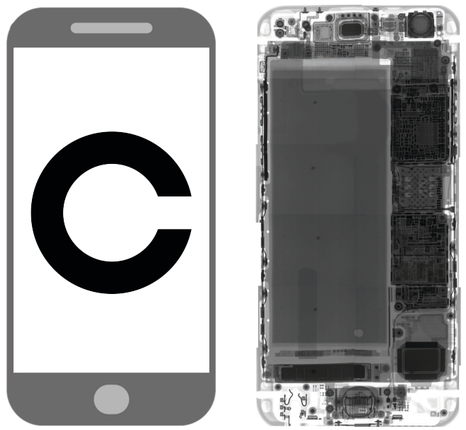
The Setup



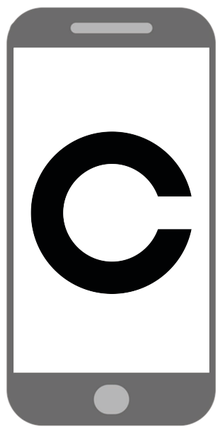
The Setup

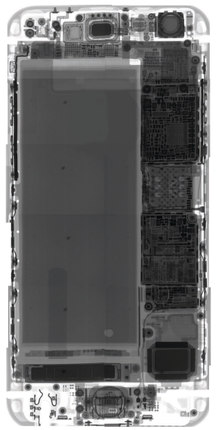


The Setup

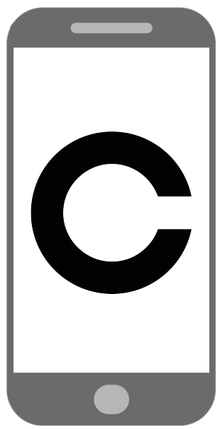


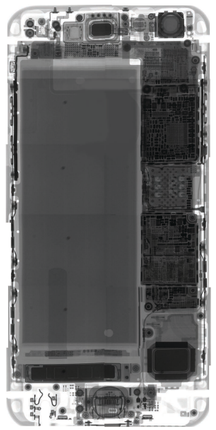
The Setup



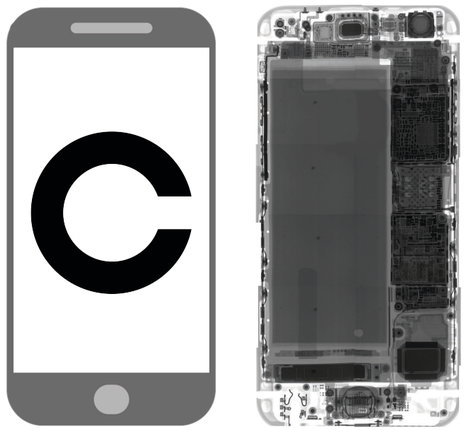


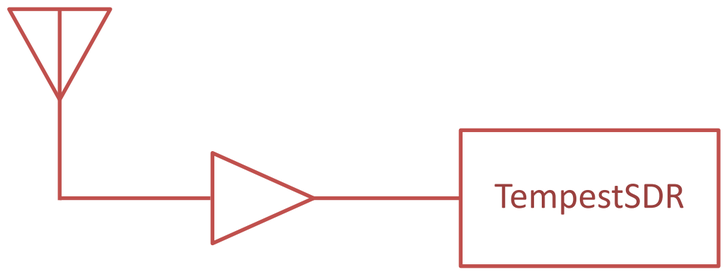
The Setup



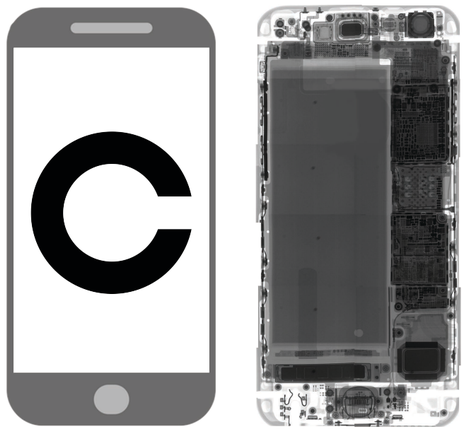


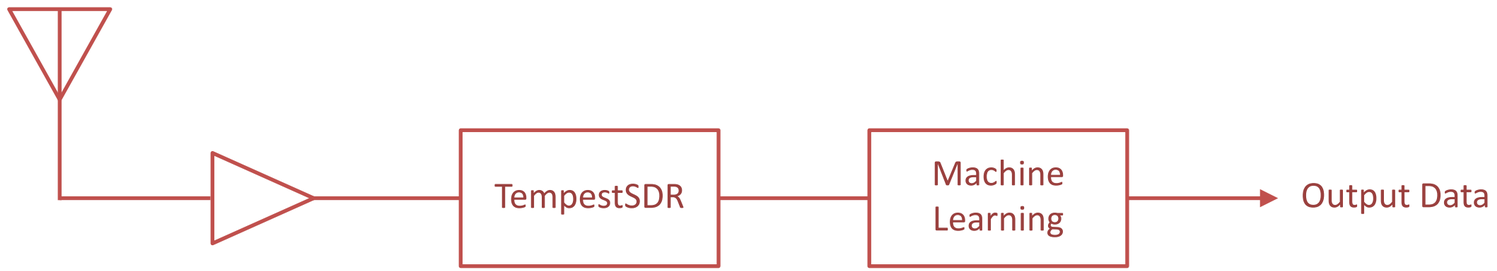
The Setup





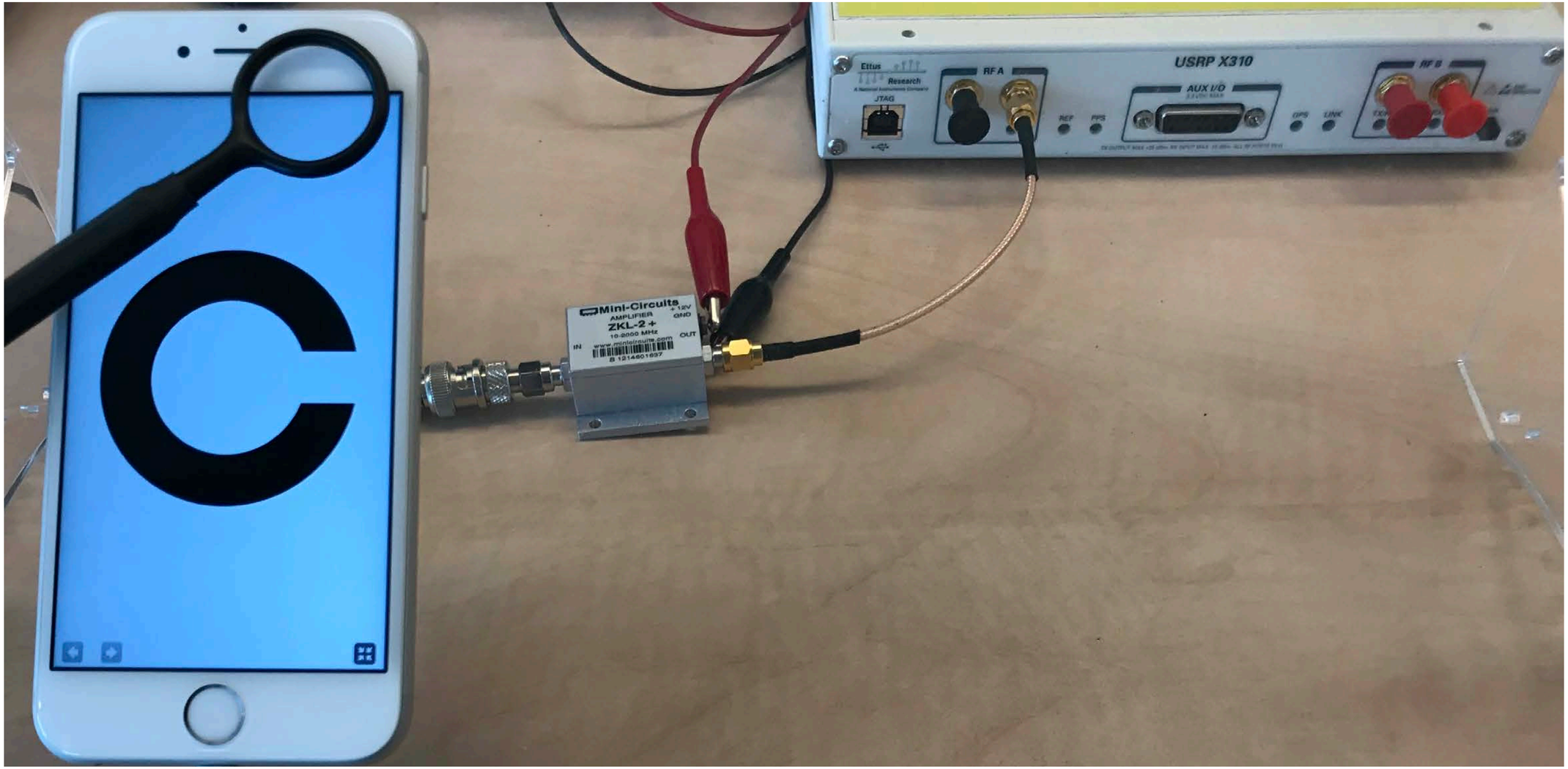
The Setup



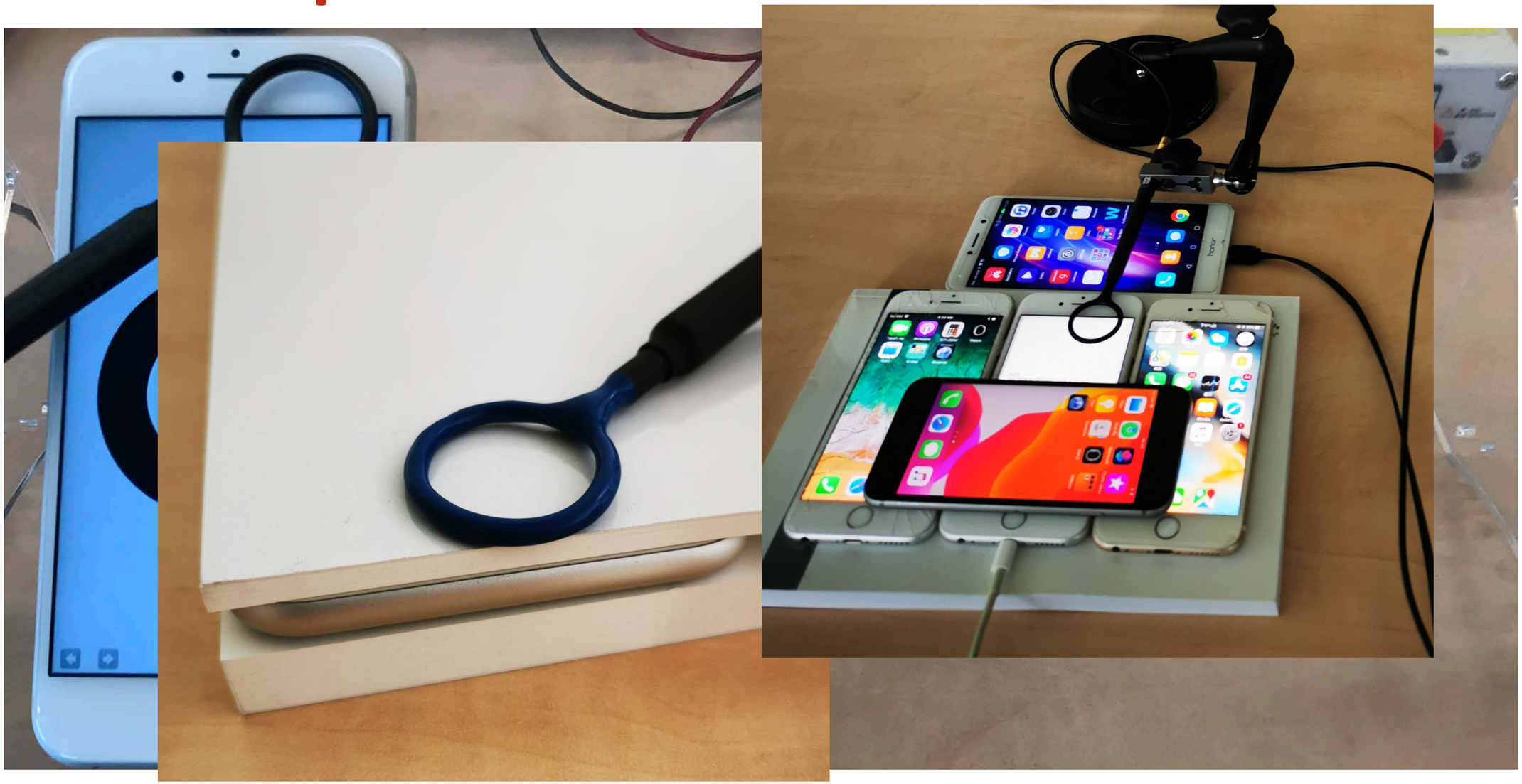


Used Setup

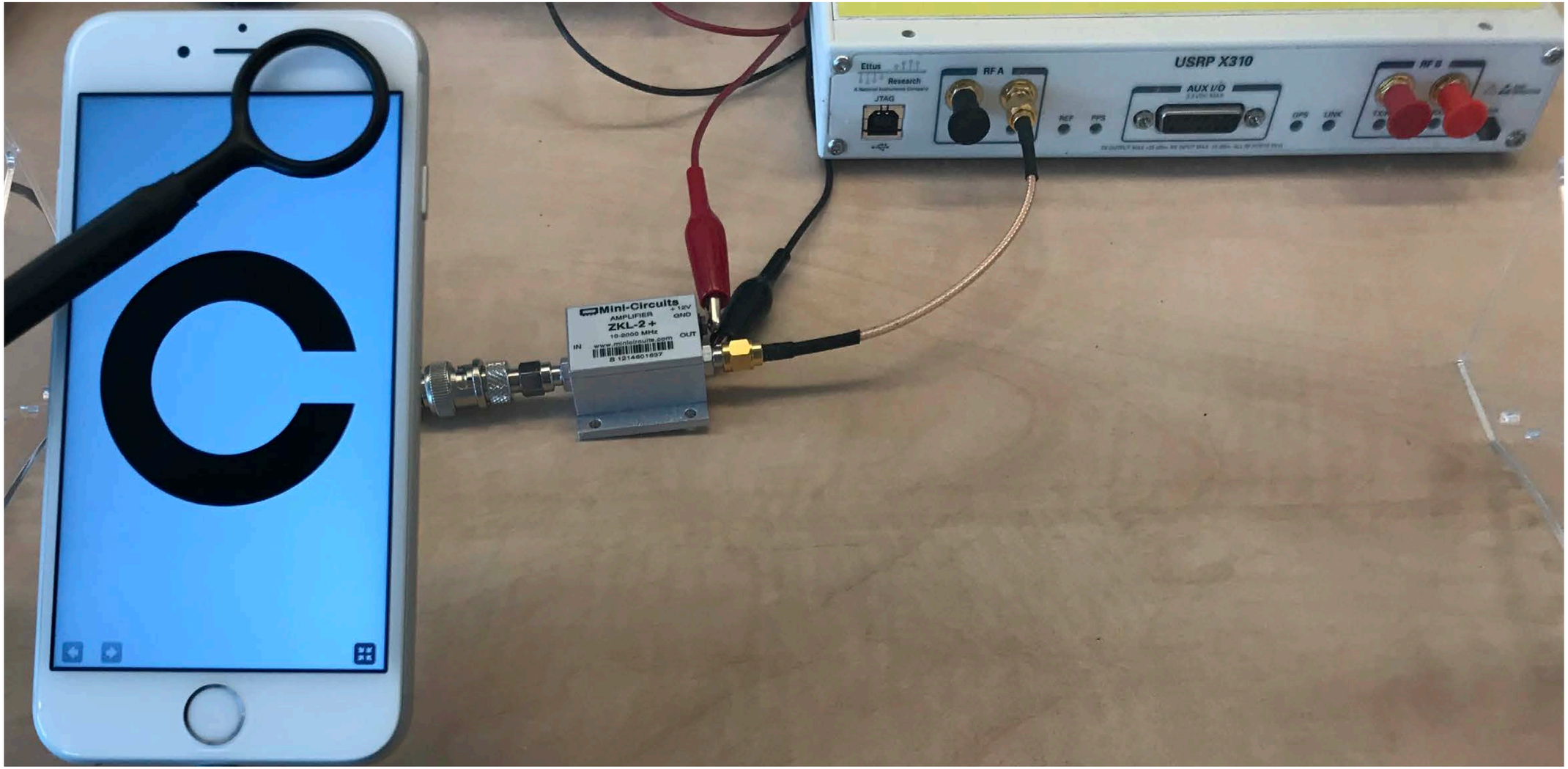
Used Setup


Ettus
Research
JTAG
RF A
USRP X310
AUX I/O
RF B
REF
PPS
GPS
LINK
Mini-Circuits
AMPLIFIER
ZKL-2+
10-2000 MHz
+12V
GND
IN
OUT

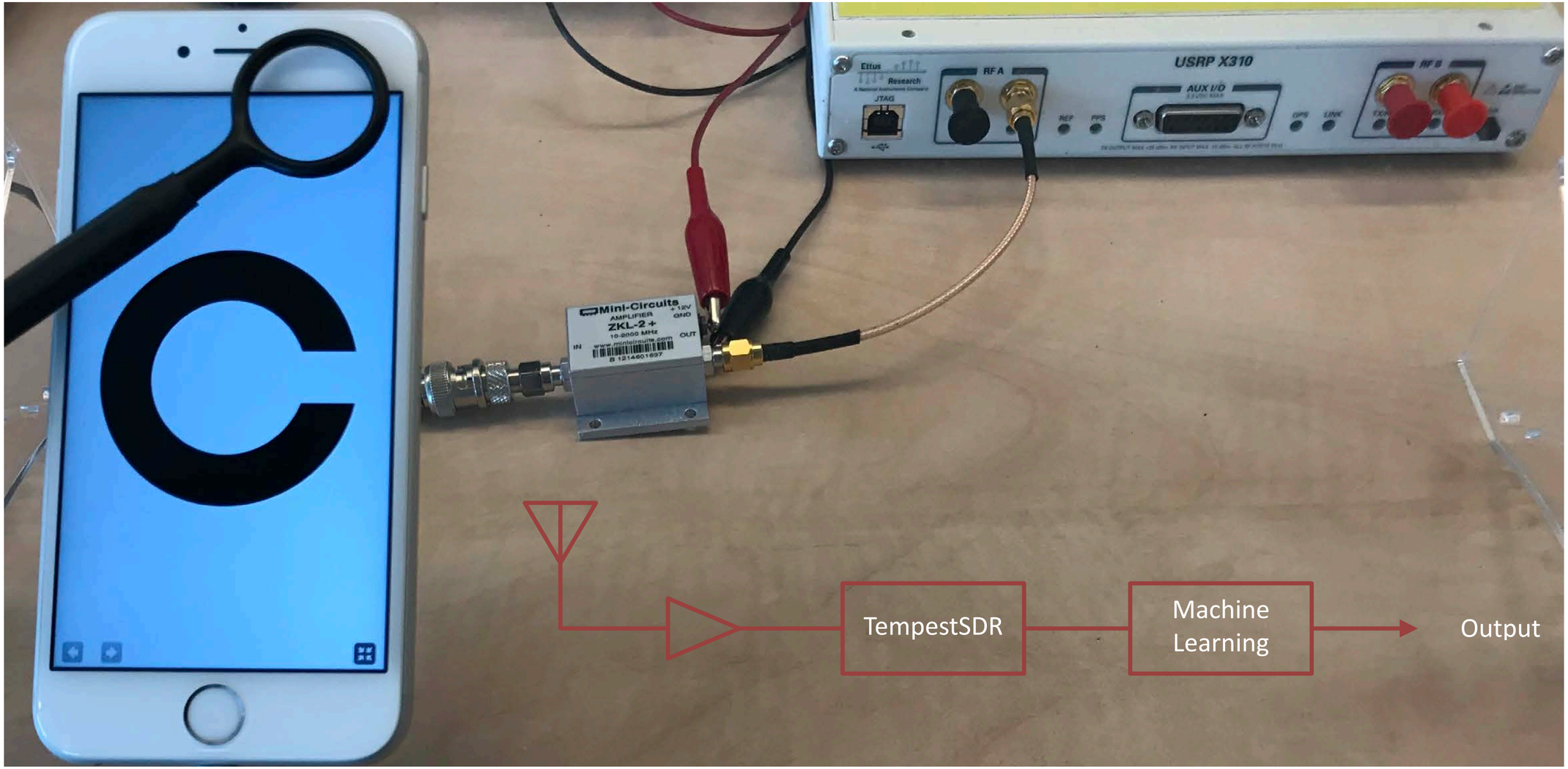
Used Setup



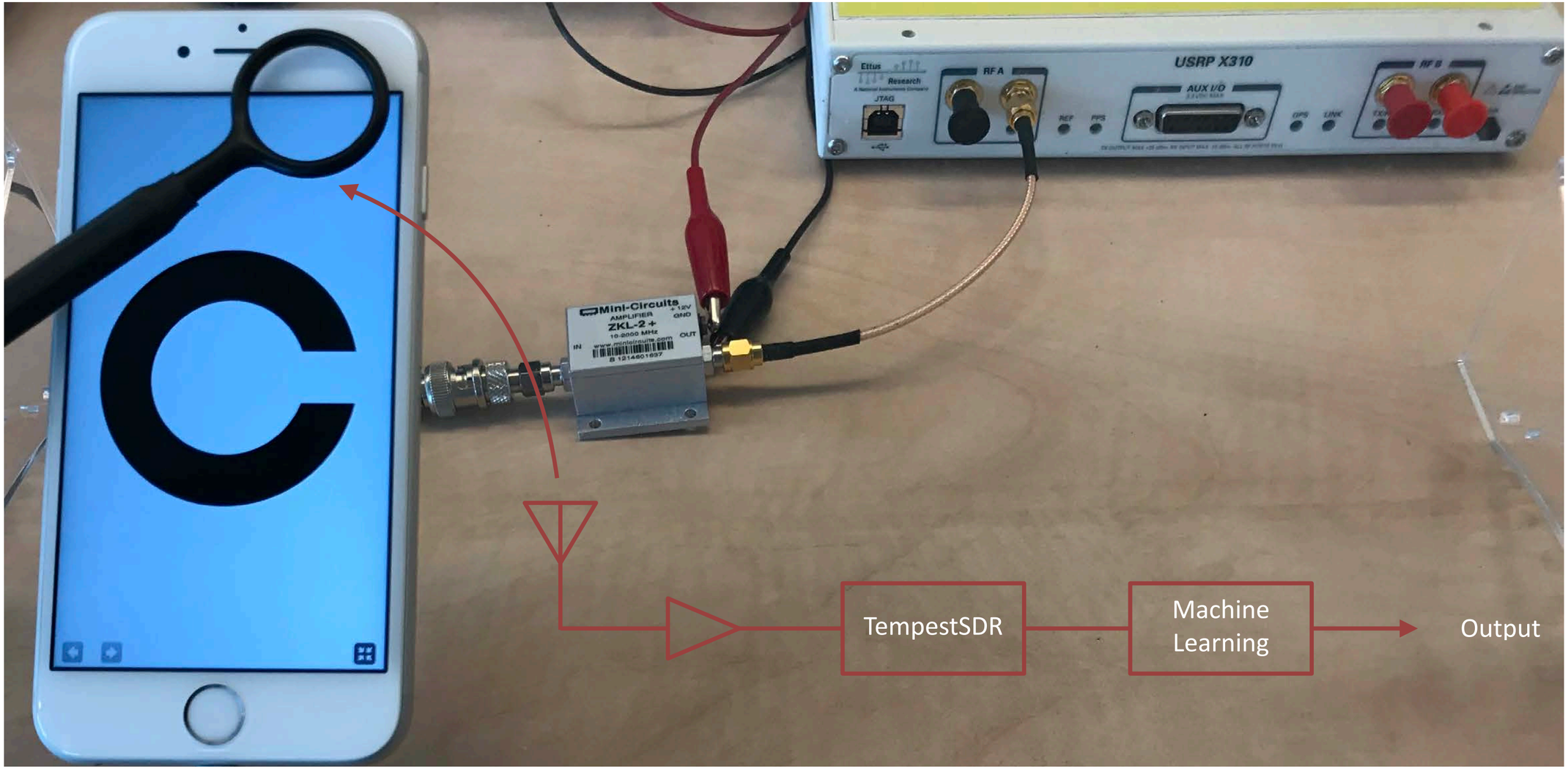
Used Setup


Ettus
Research
JTAG
RF A
USRP X310
AUX I/O
RF B
REF
PPS
GPS
LINK
Mini-Circuits
AMPLIFIER
ZKL-2+
10-2000 MHz
+12V
GND
IN
OUT

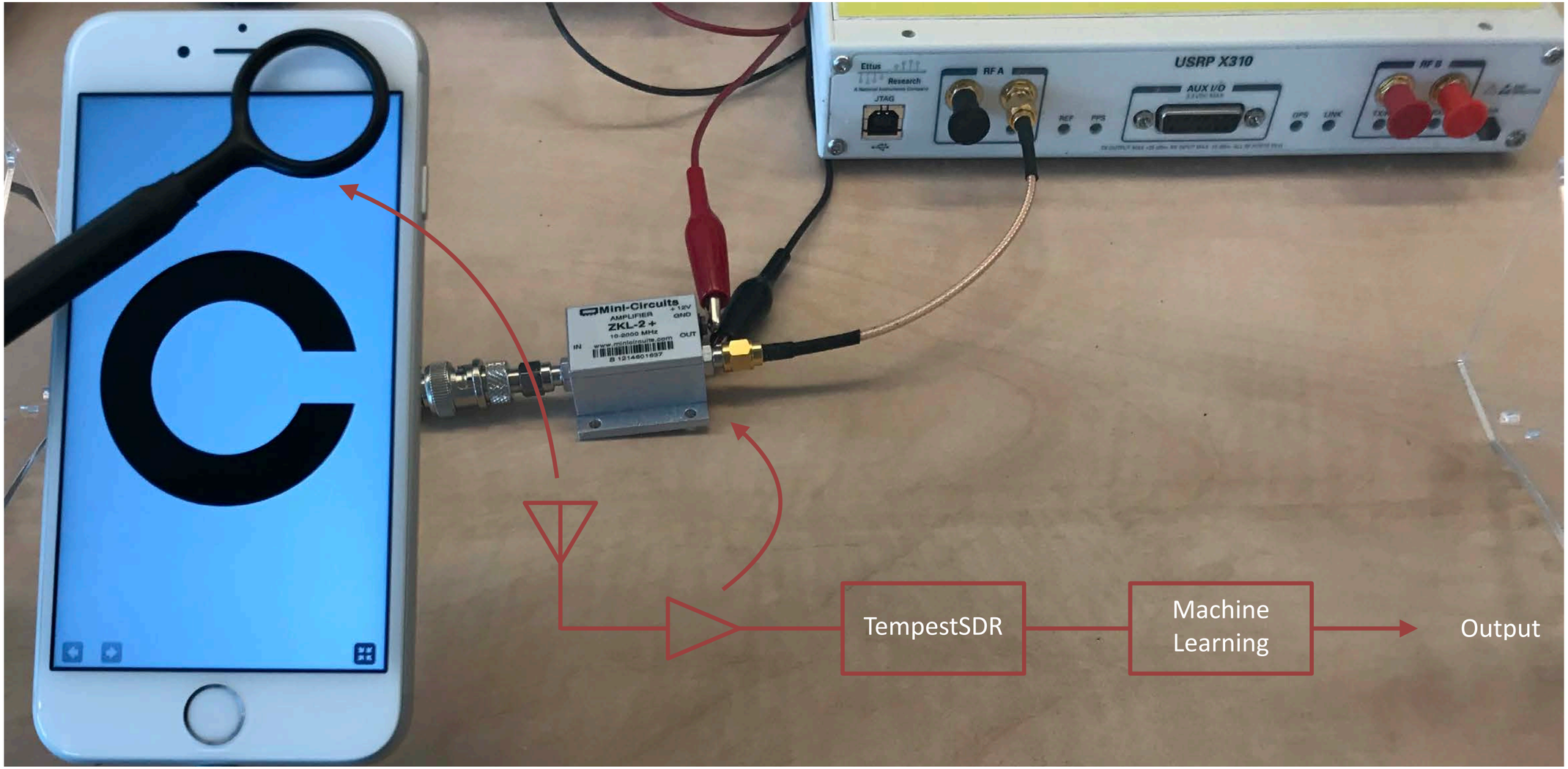
Used Setup


USRP X310
RF A
AUX I/O
Mini-Circuits
AMPLIFIER
ZKL-2+
10-2000 MHz
TempestSDR
Machine Learning
Output

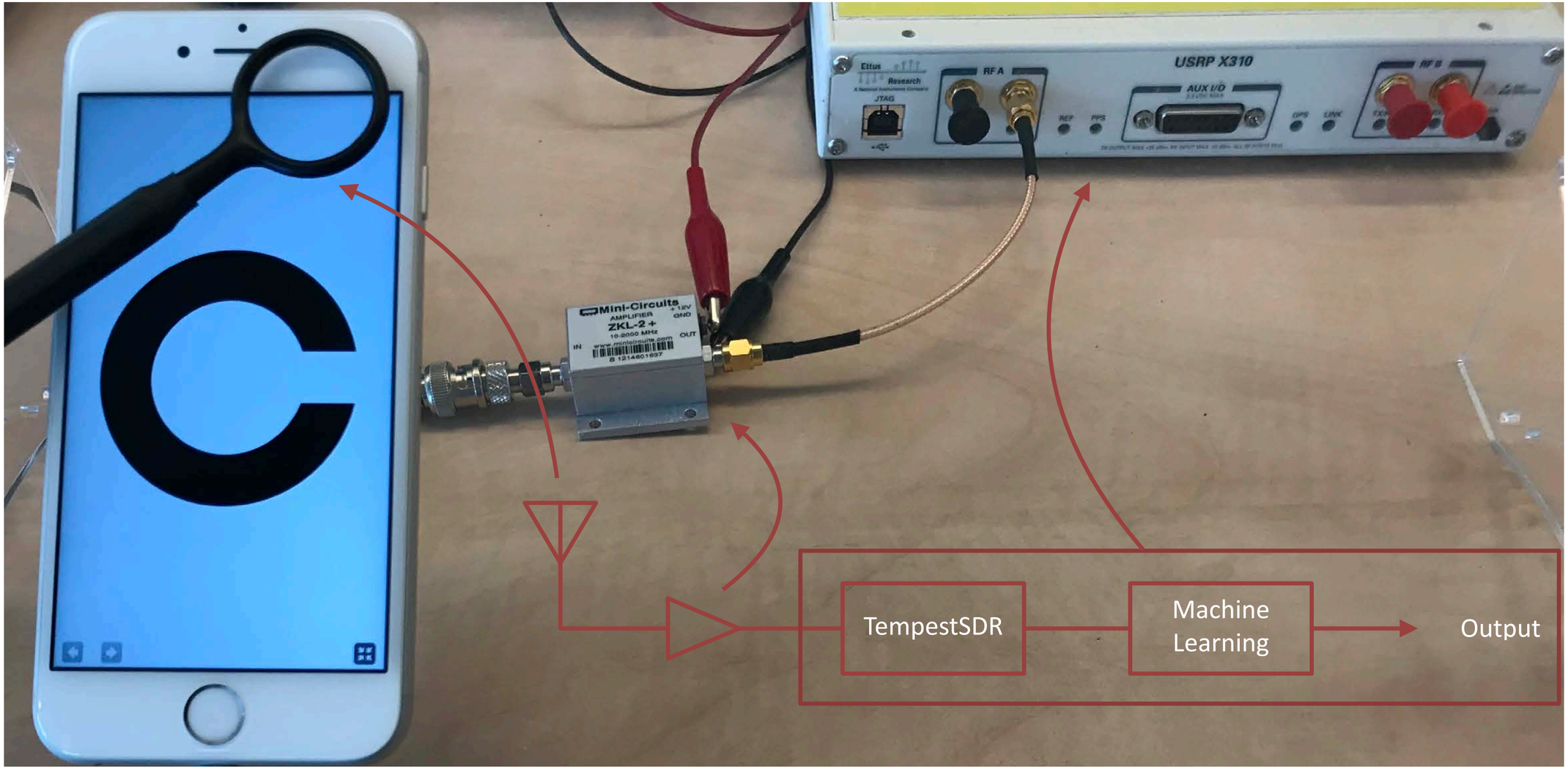
Used Setup


USRP X310
Mini-Circuits
AMPLIFIER
ZKL-2+
10-2000 MHz
TempestSDR
Machine Learning
Output

Used Setup


USRP X310
RF A
AUX I/O
Mini-Circuits
AMPLIFIER
ZKL-2+
10-2000 MHz
TempestSDR
Machine Learning
Output

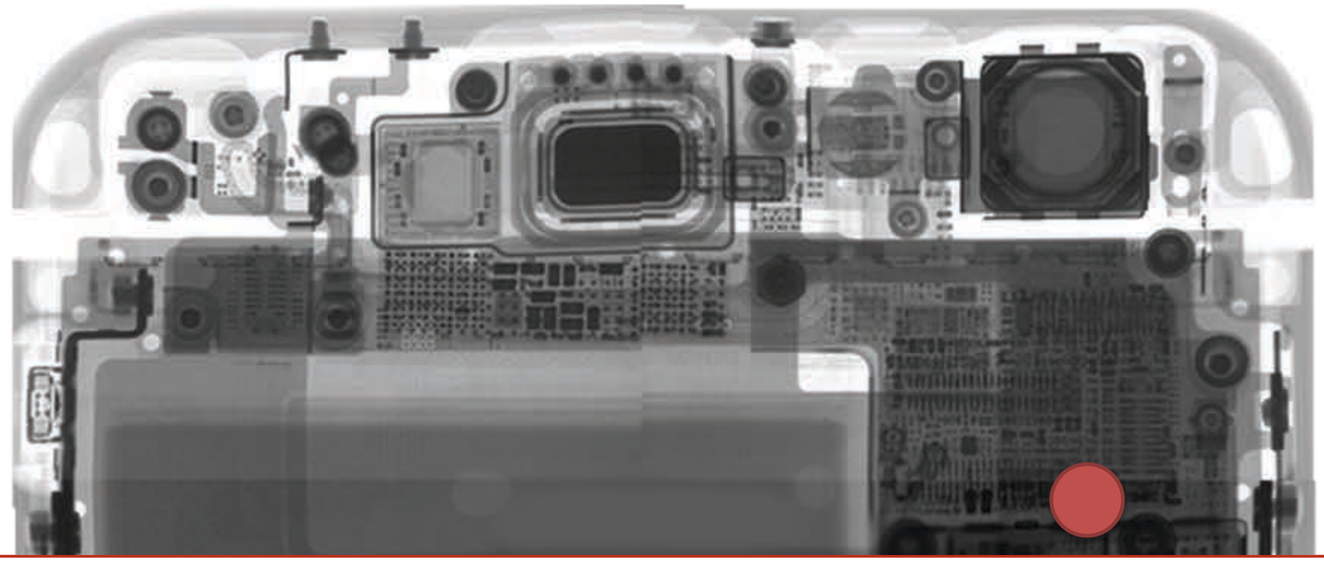
Used Setup


USRP X310
RF A
AUX I/O
Mini-Circuits
AMPLIFIER
ZKL-2+
10-2000 MHz
TempestSDR
Machine Learning
Output

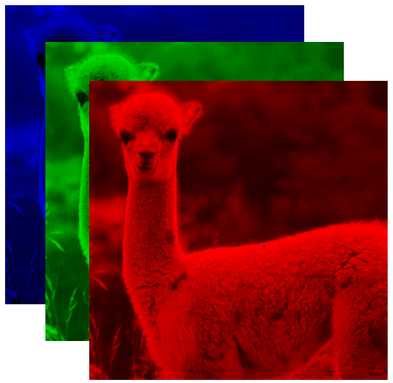
Video Transmission

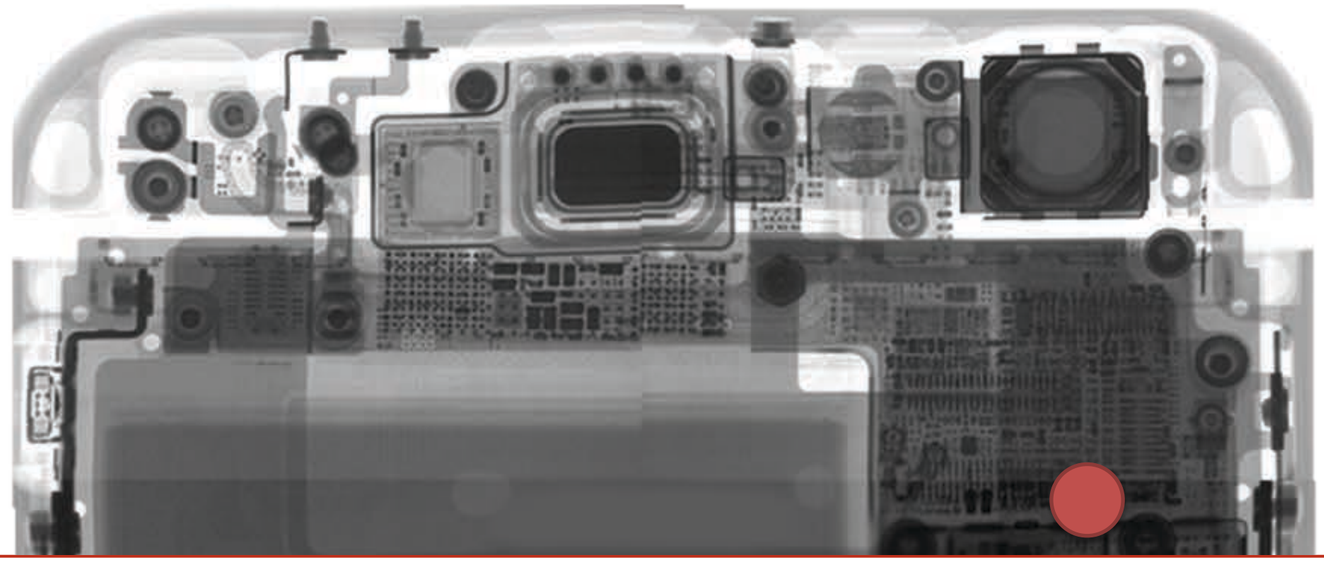
Video Transmission

Video Transmission

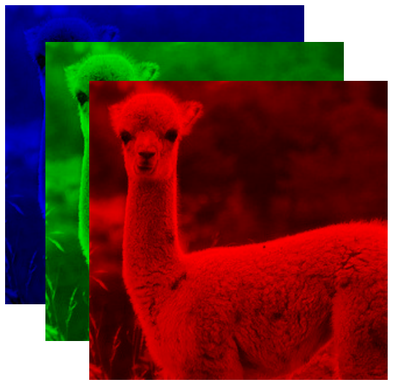


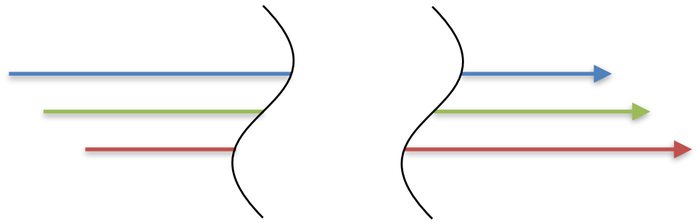
Video Transmission

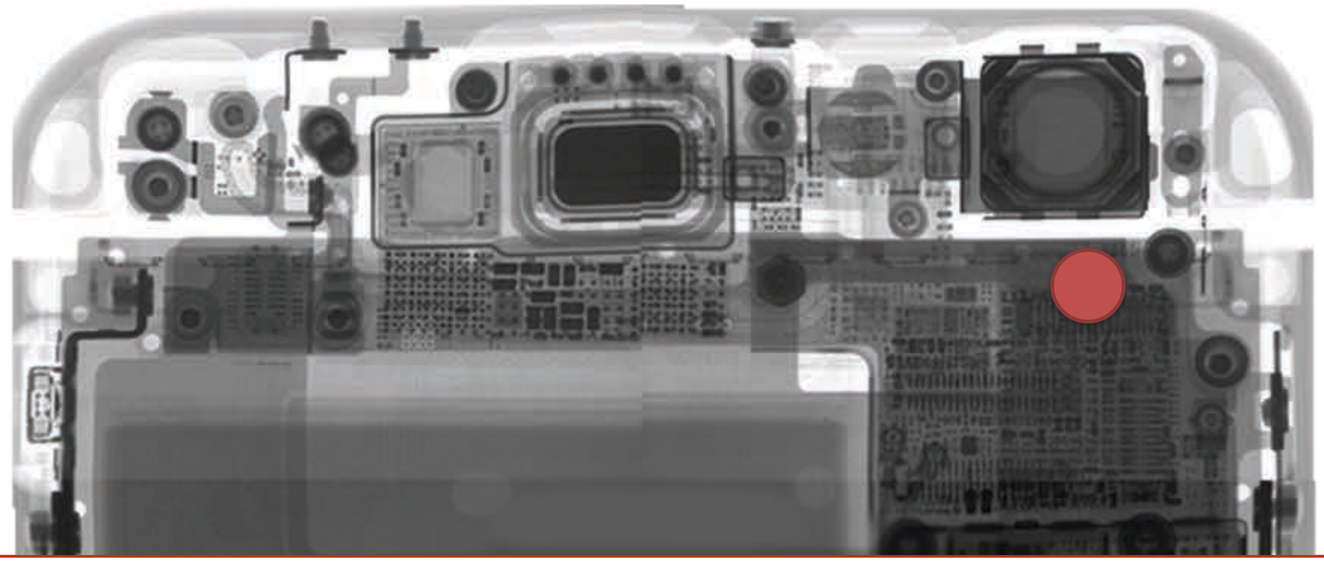




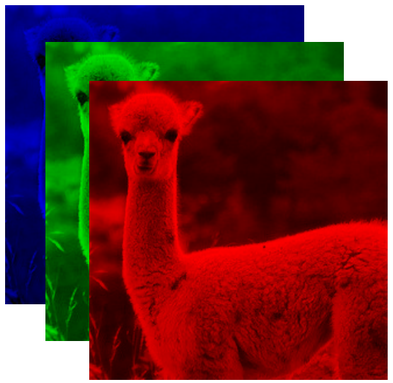
Video Transmission

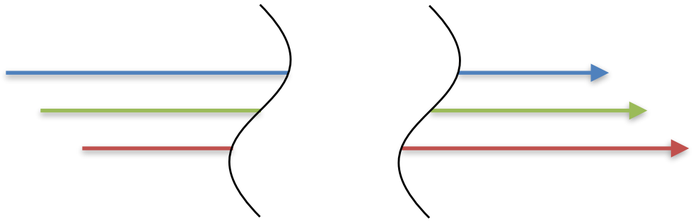


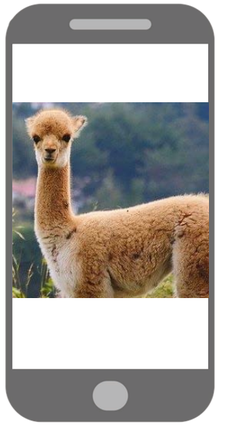




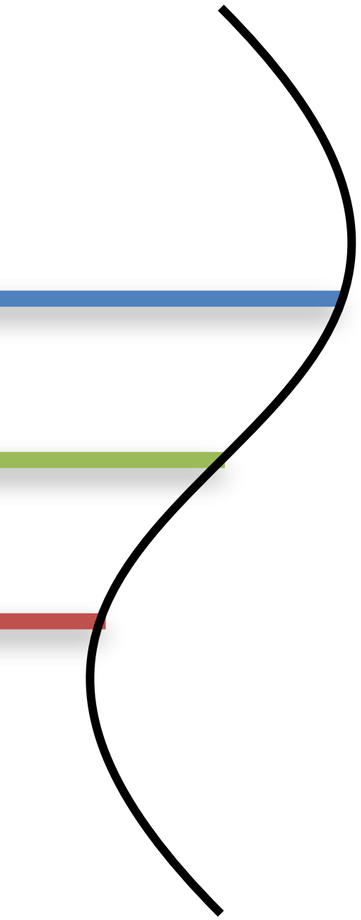
Video Transmission

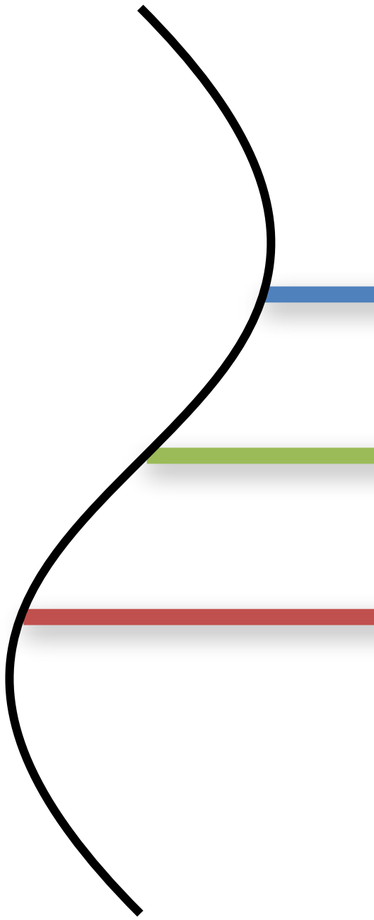




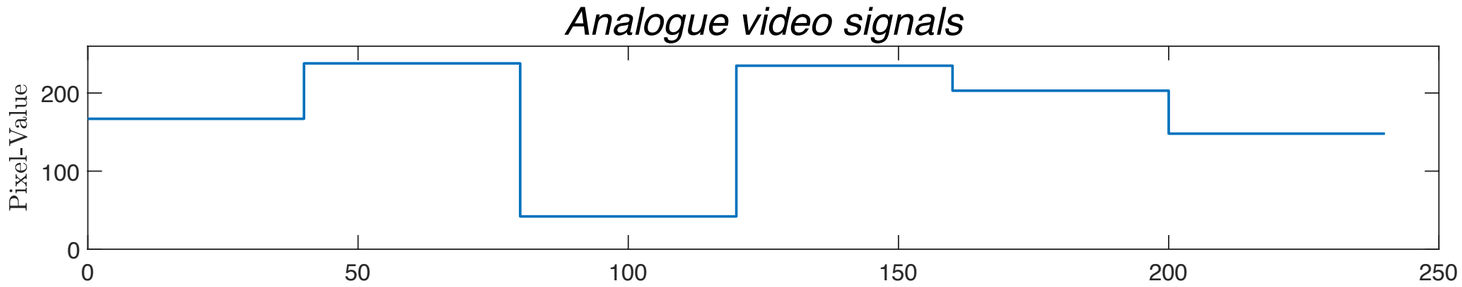


Video Transmission

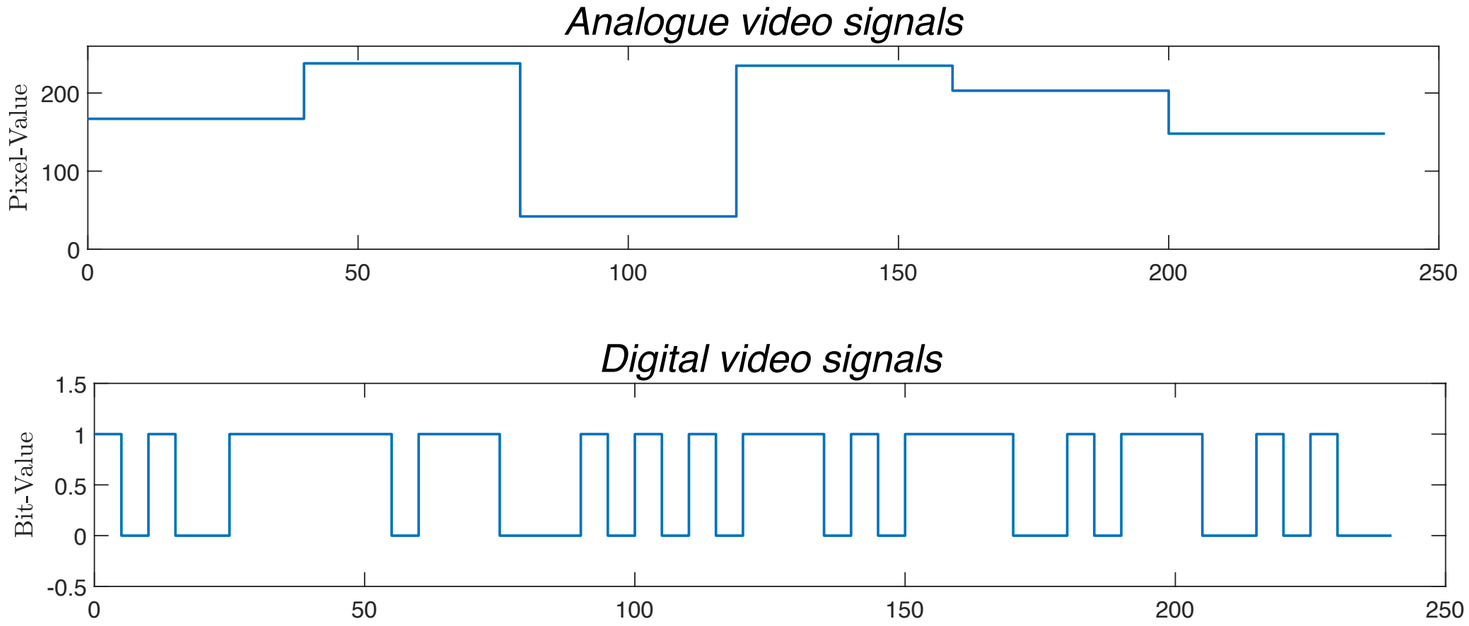




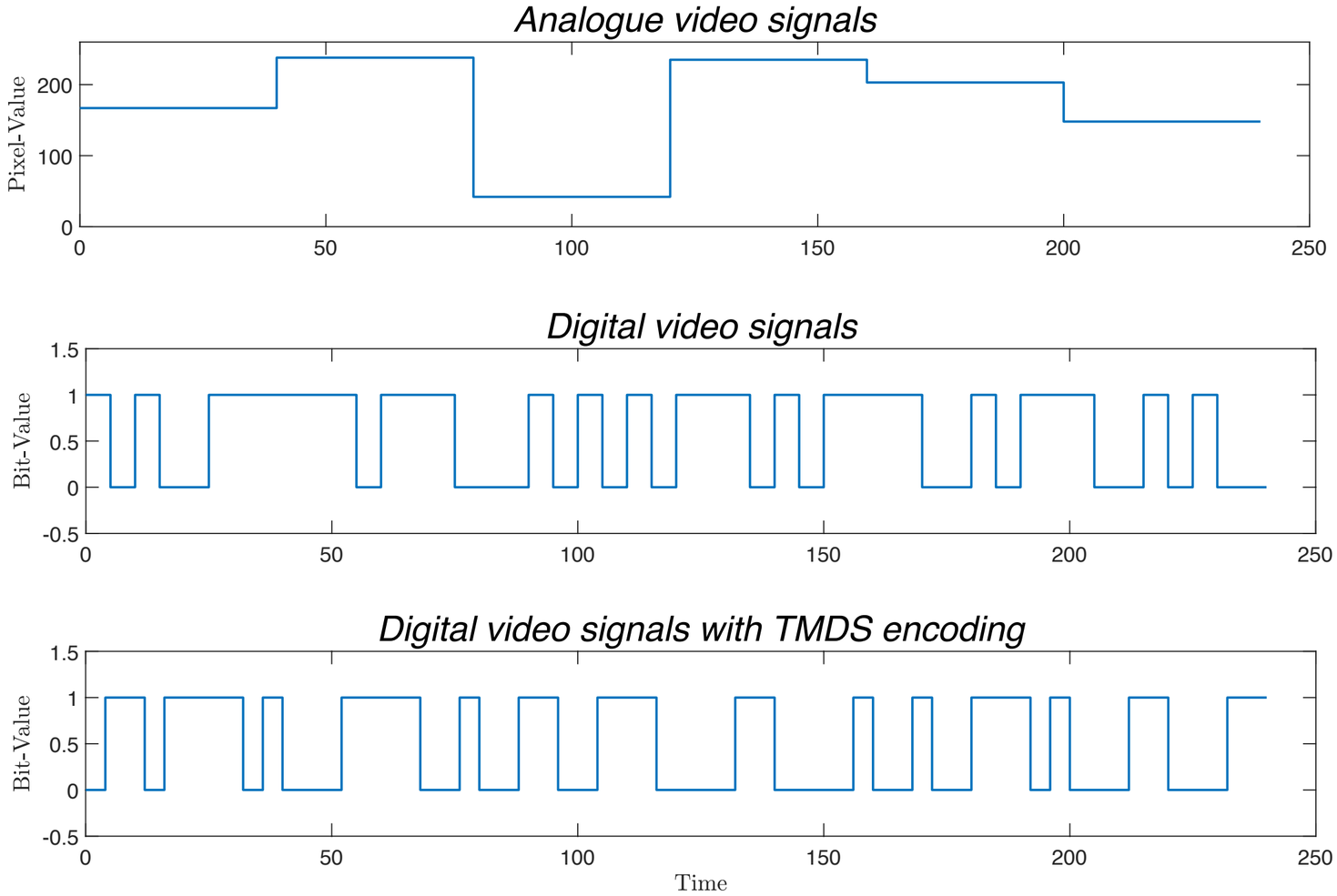
Video Transmission



Video Transmission

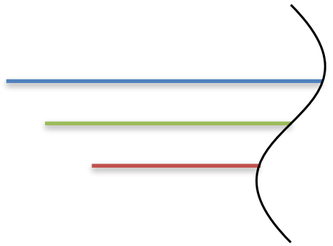


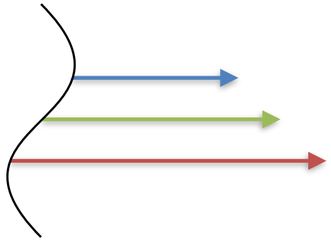
Video Transmission

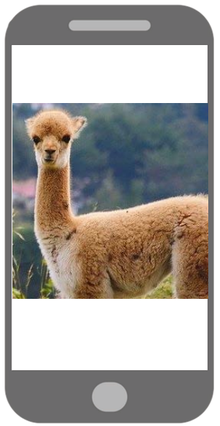


Electromagnetic Emanations

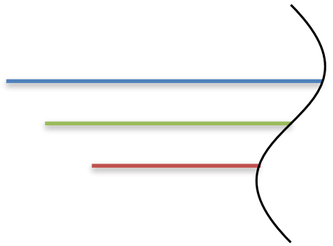
Electromagnetic Emanations

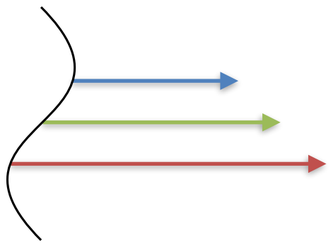


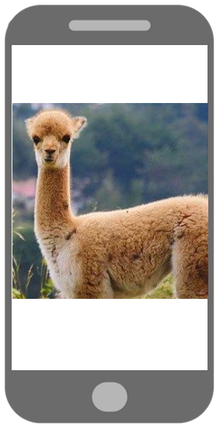


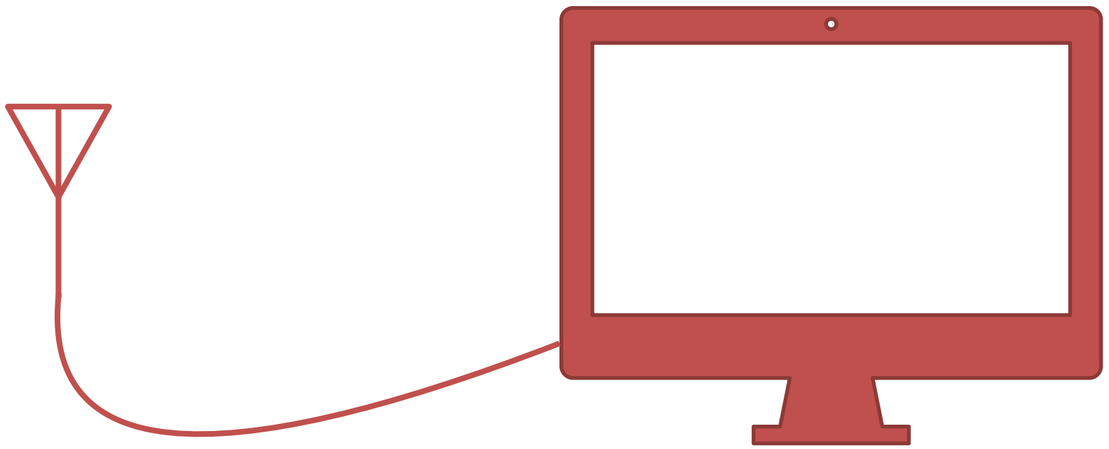


Electromagnetic Emanations



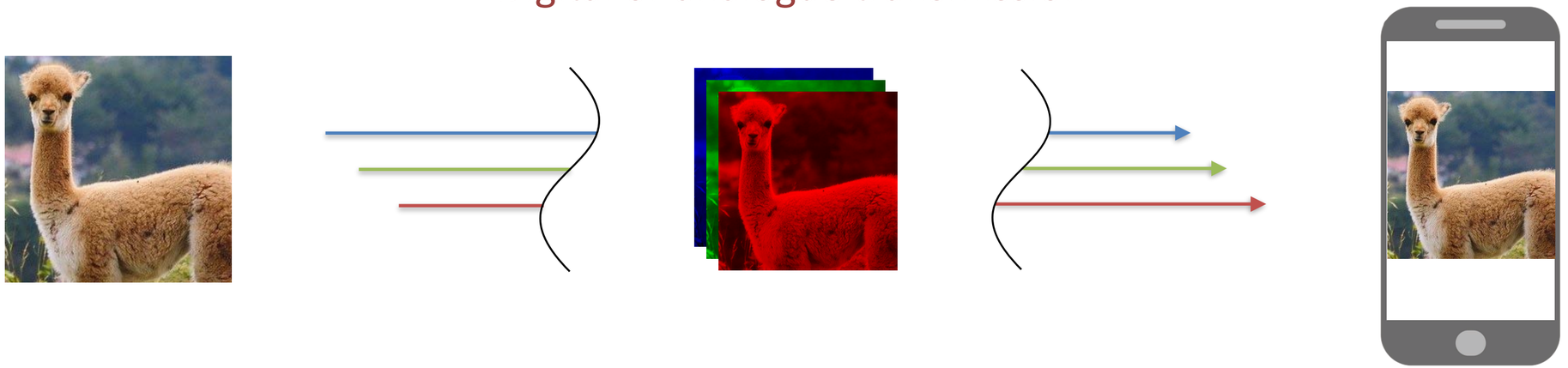


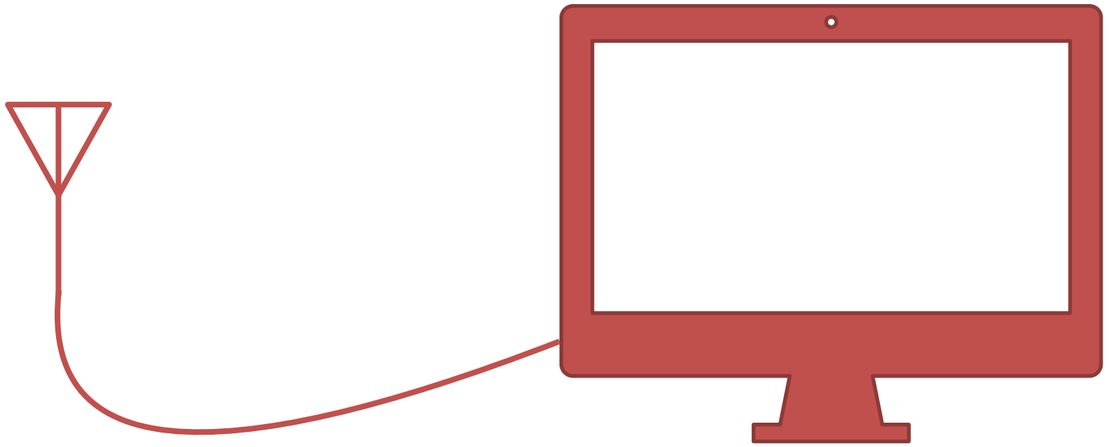




Electromagnetic Emanations

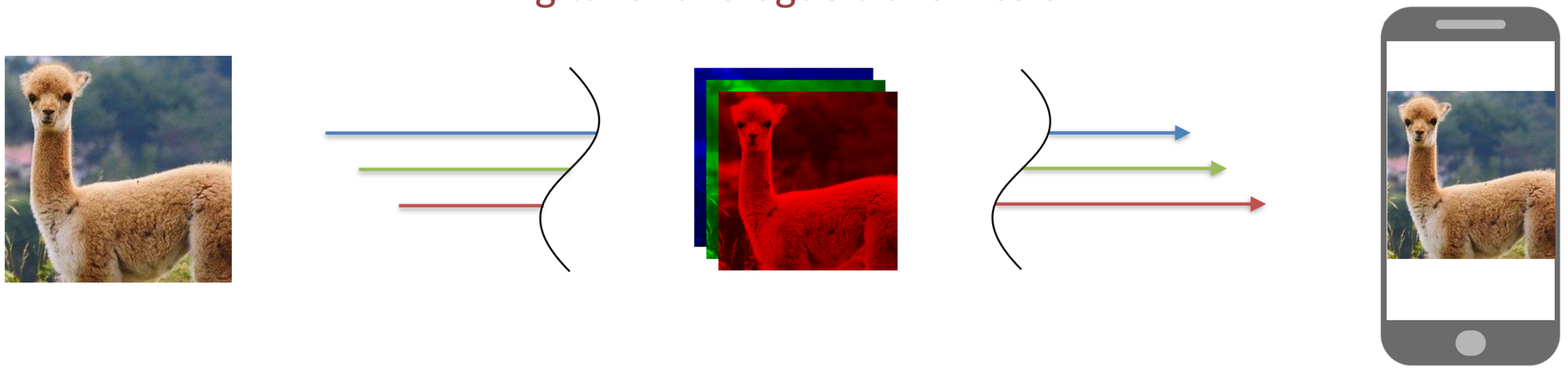
Digital or analogue transmission

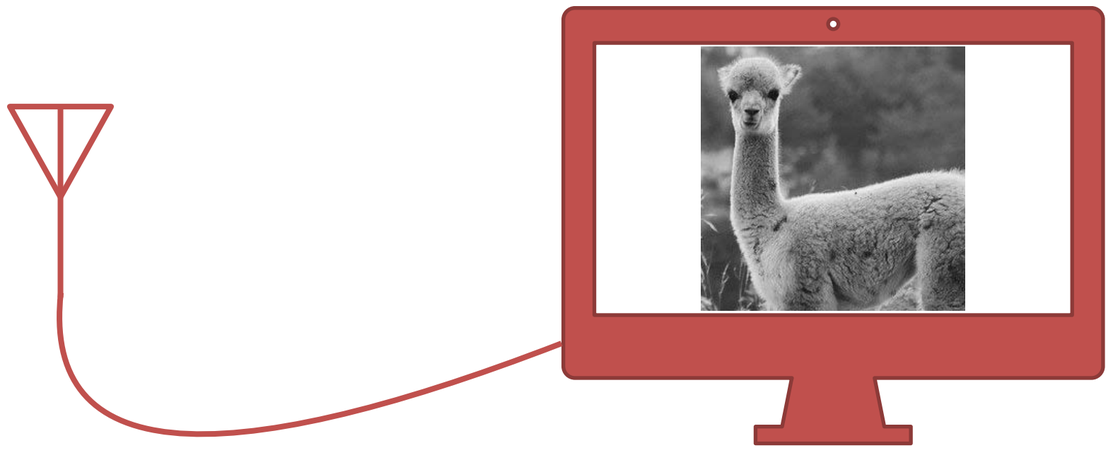




Electromagnetic Emanations

Digital or analogue transmission





CONTENTS

Table of Contents

Table of Contents

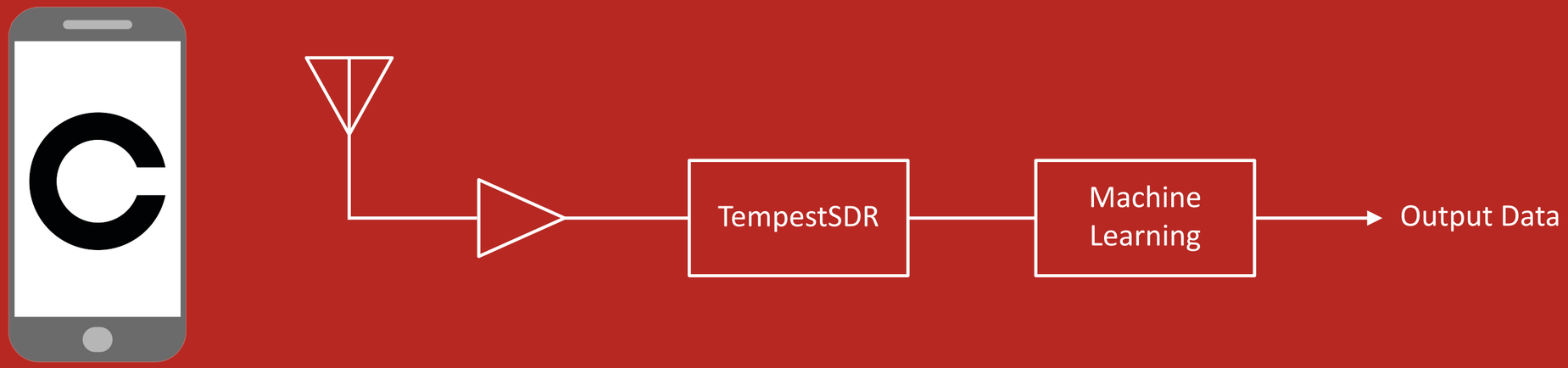
Table of Contents

Table of Contents

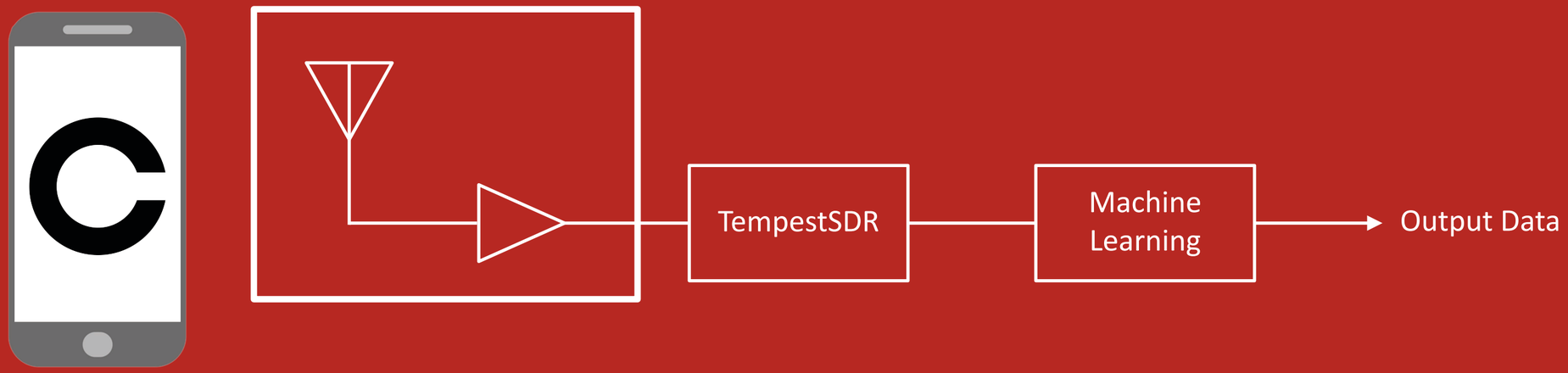
Table of Contents

Table of Contents

Antenna Design

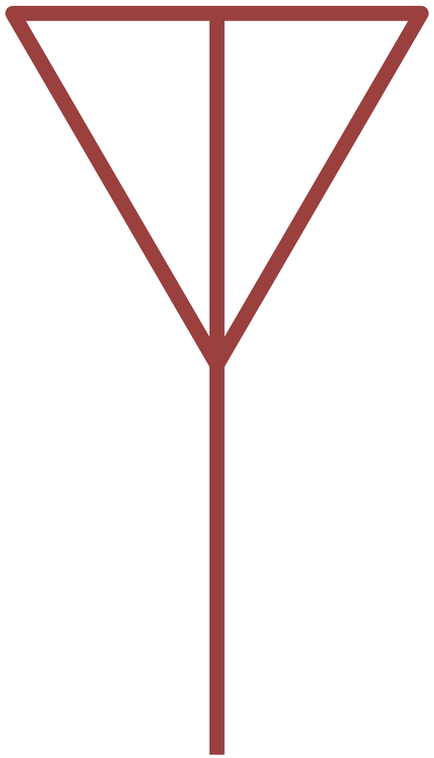


Antenna Design



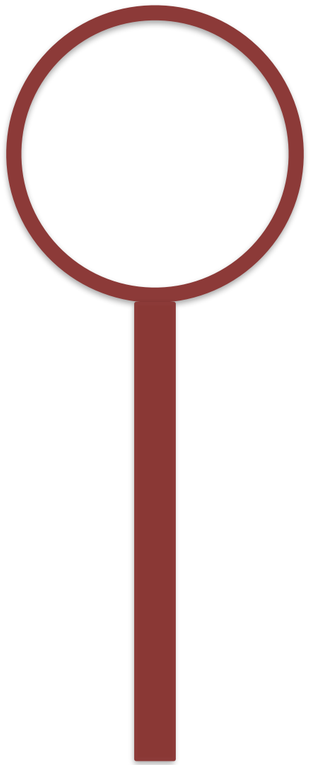
Antenna Positioning

Antenna Positioning



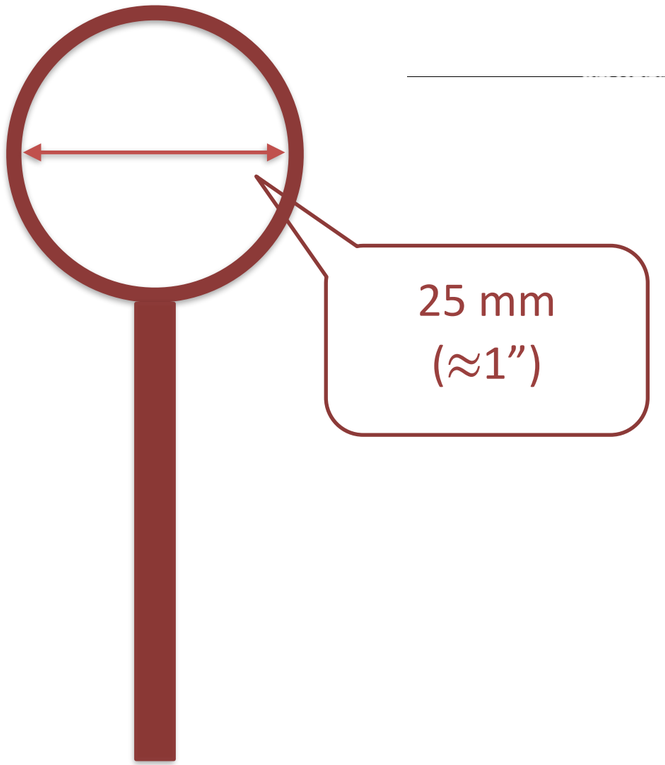
Antenna Positioning

Langer RF-R 400



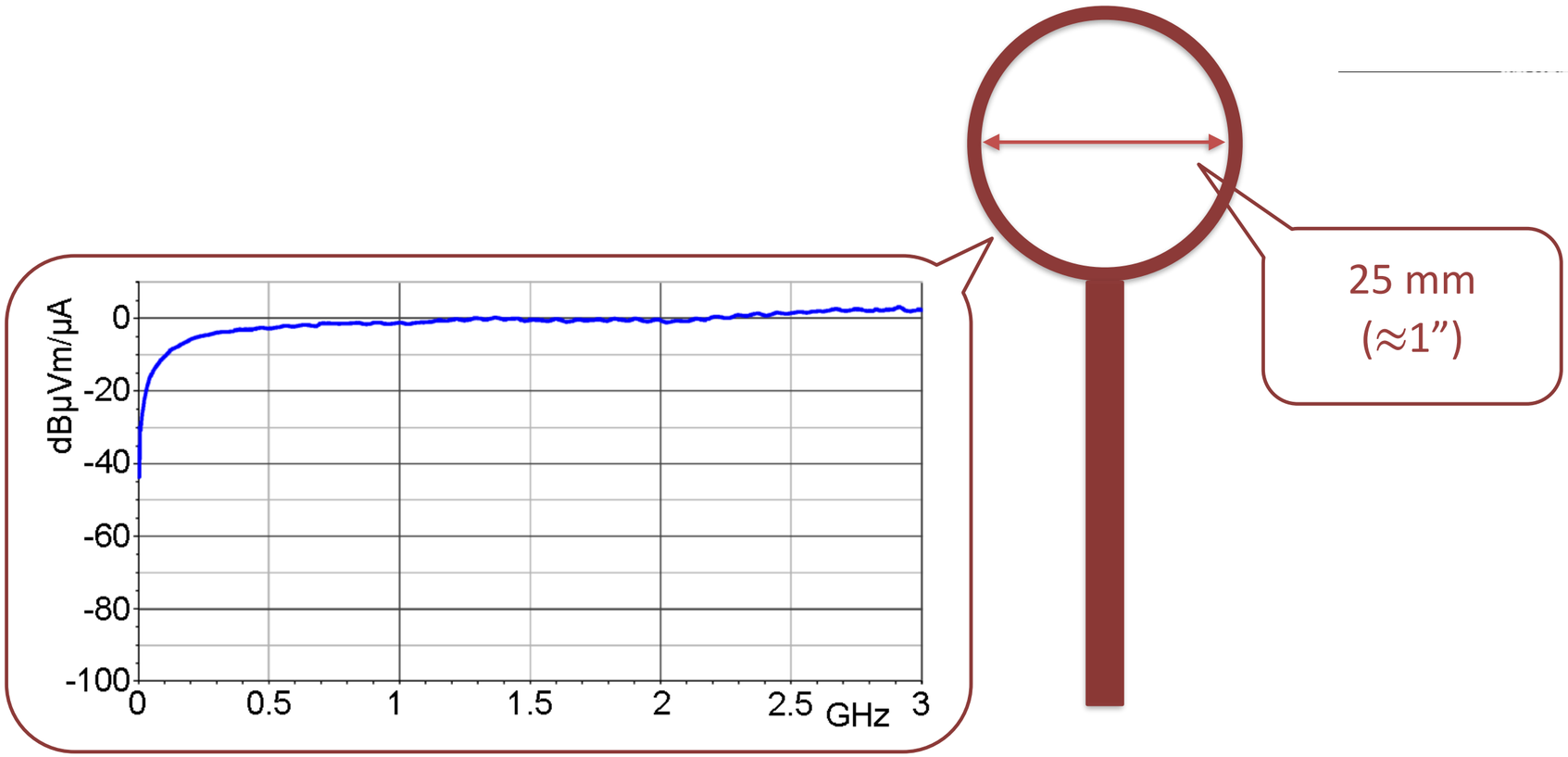
Antenna Positioning

Langer RF-R 400



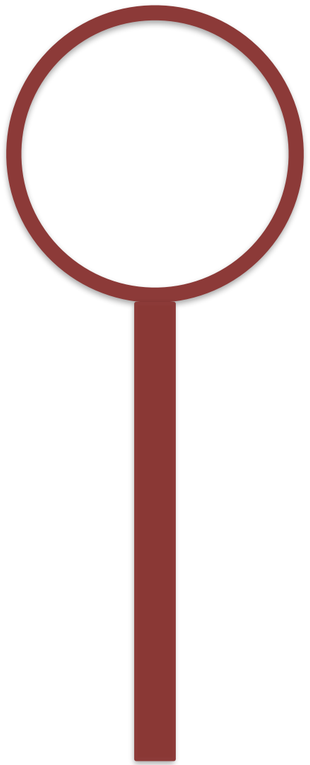
Antenna Positioning

Langer RF-R 400

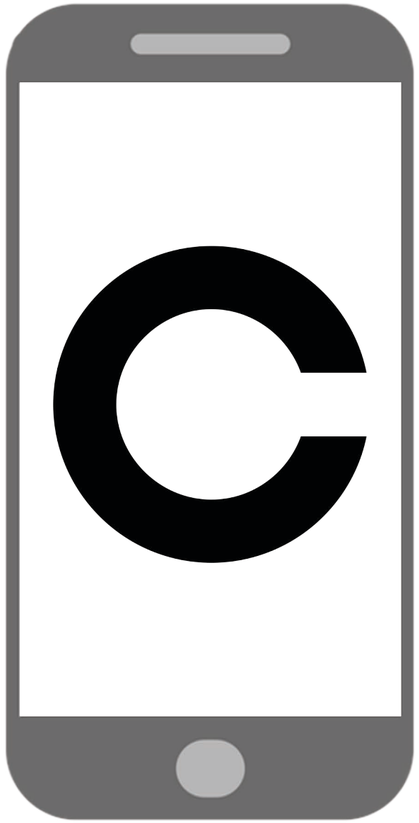


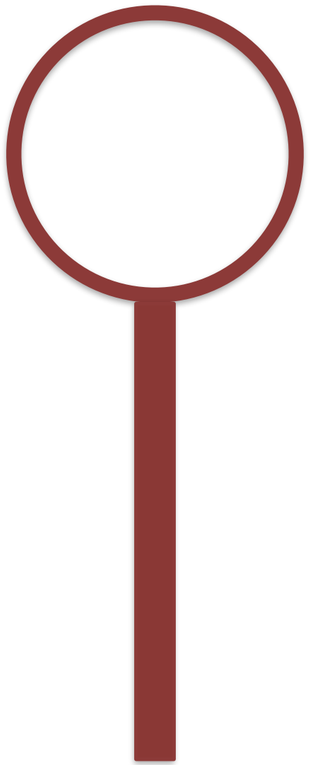
25 mm
(≈1”)

Antenna Positioning

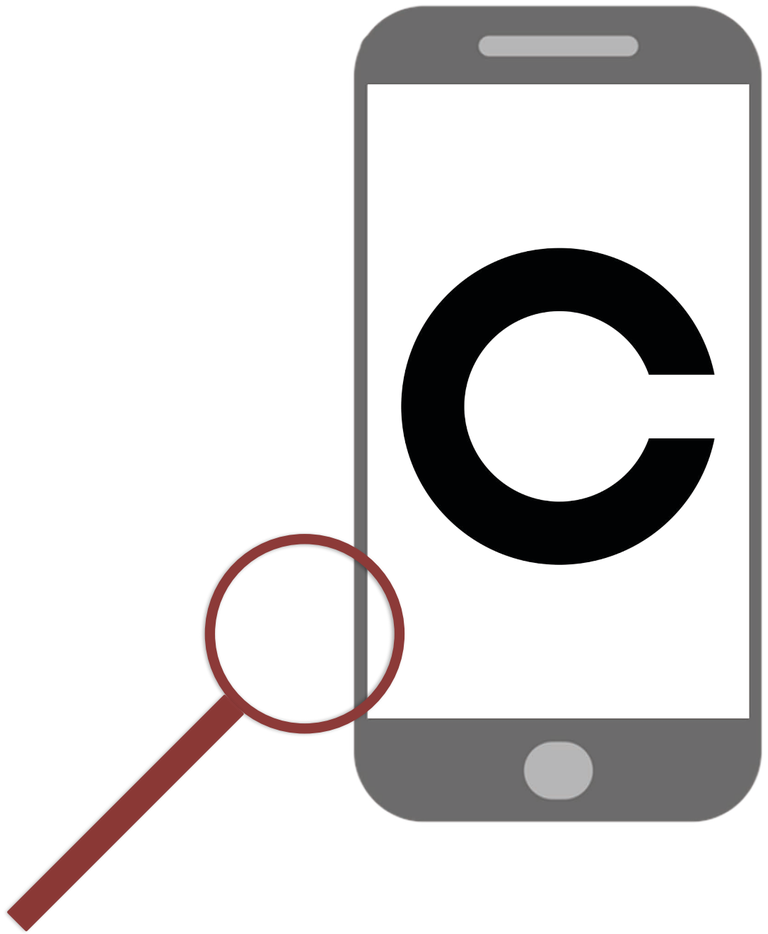


Antenna Positioning

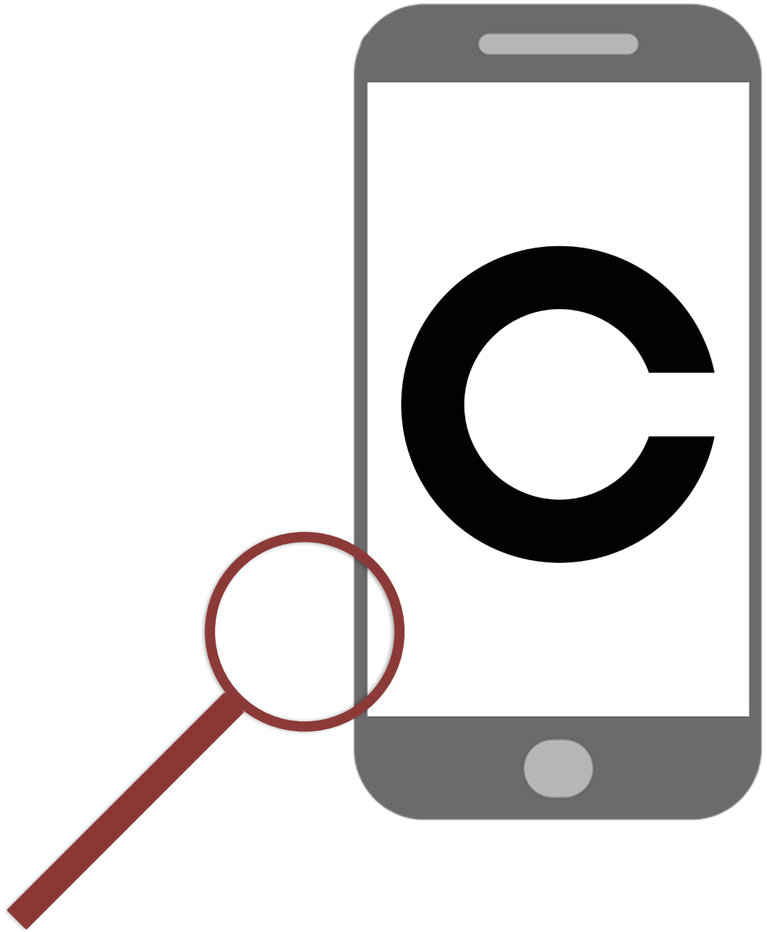


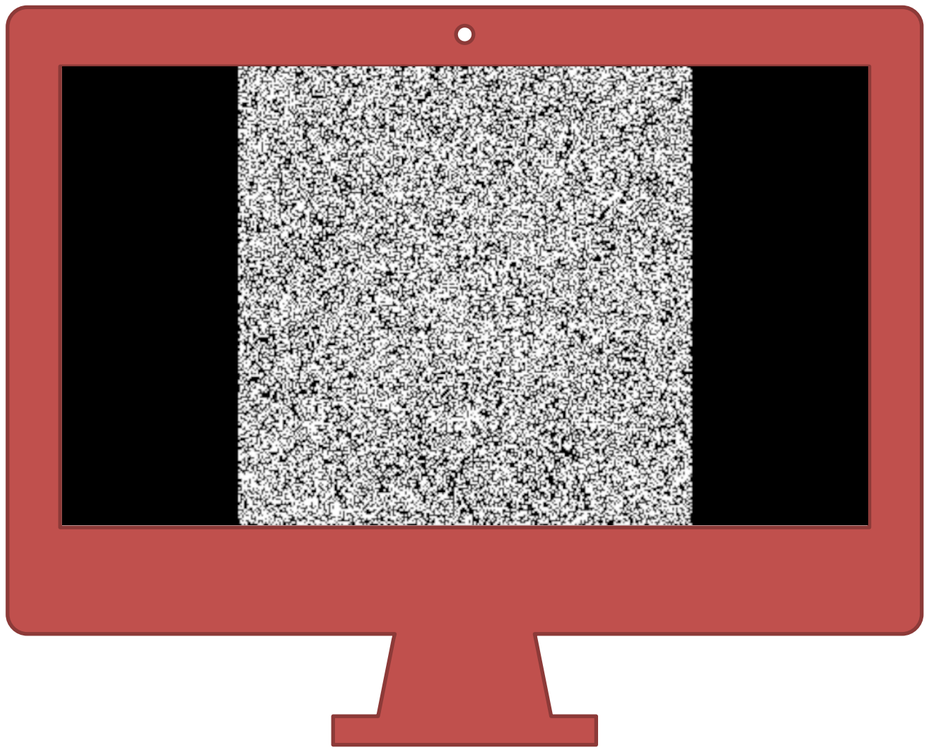


Antenna Positioning

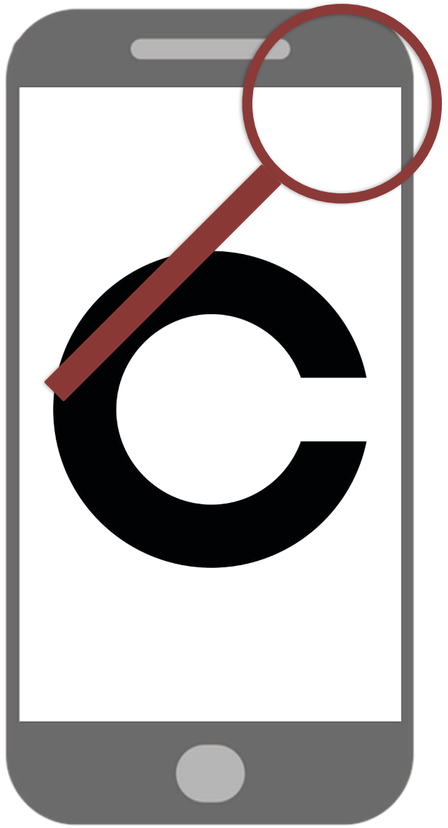


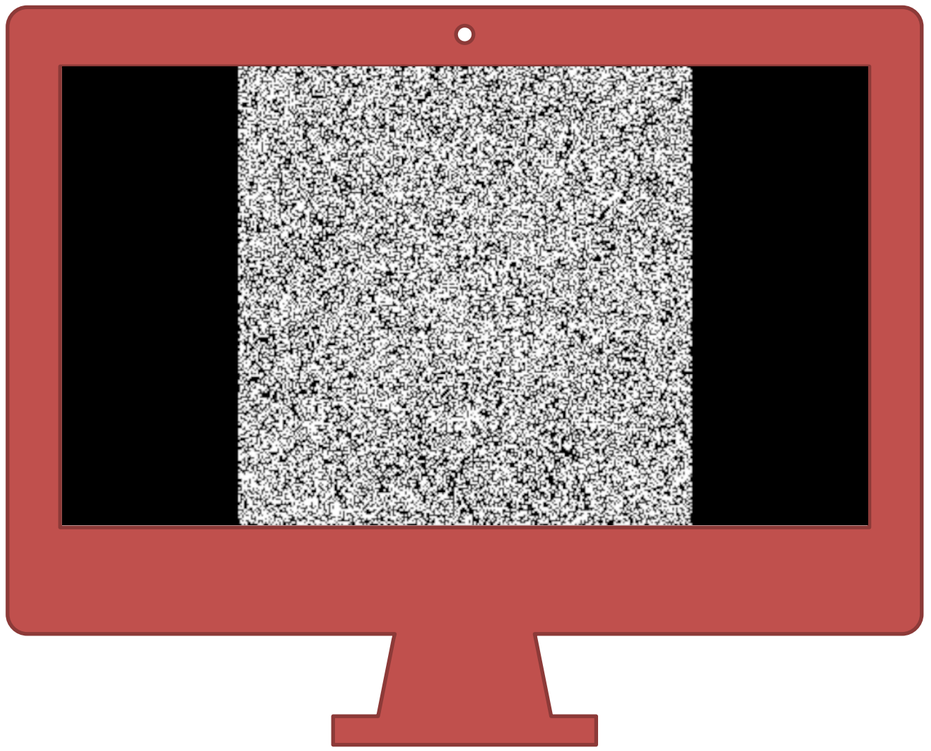
Antenna Positioning





Antenna Positioning





Limitations

[1] Nathan Ida. Engineering electromagnetics. Springer, 2000.

Limitations

- Near-Field probes

[1] Nathan Ida. Engineering electromagnetics. Springer, 2000.

Limitations

- Near-Field probes
  - Only for showing proof of concept

[1] Nathan Ida. Engineering electromagnetics. Springer, 2000.

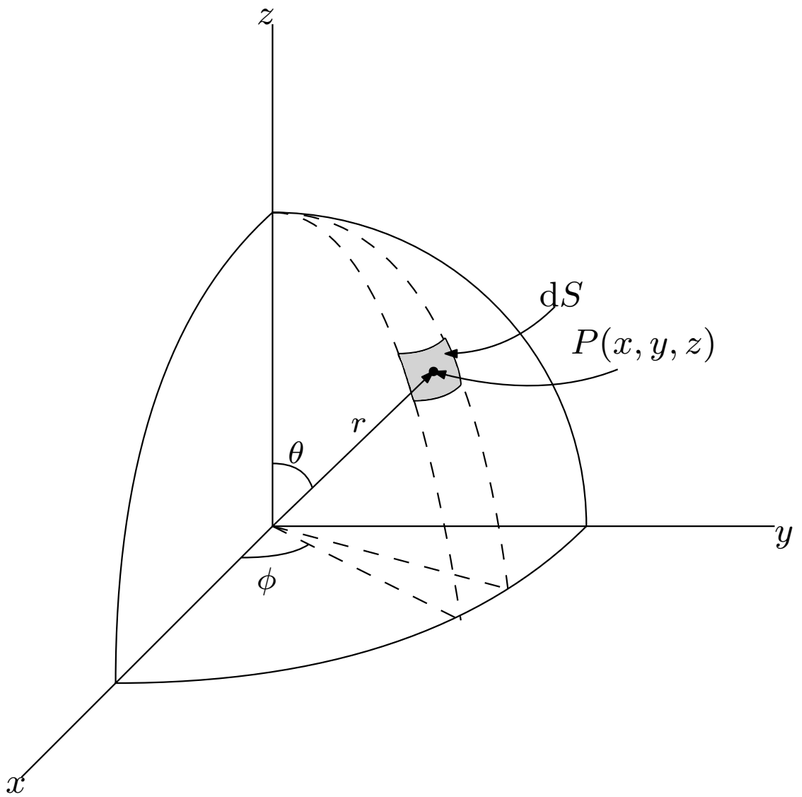
Limitations

- Near-Field probes
  - Only for showing proof of concept
  - Inefficient for distances $>$ 2 cm

[1] Nathan Ida. Engineering electromagnetics. Springer, 2000.

Limitations

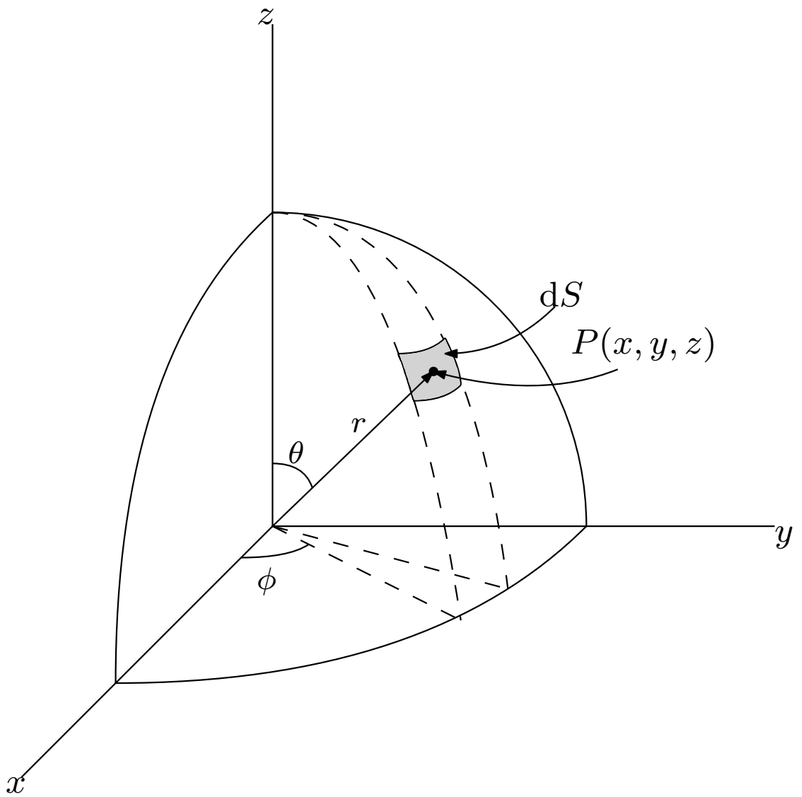
- Near-Field probes
  - Only for showing proof of concept
  - Inefficient for distances $>$ 2 cm



[1] Nathan Ida. Engineering electromagnetics. Springer, 2000.

Limitations

- Near-Field probes
  - Only for showing proof of concept
  - Inefficient for distances > 2 cm

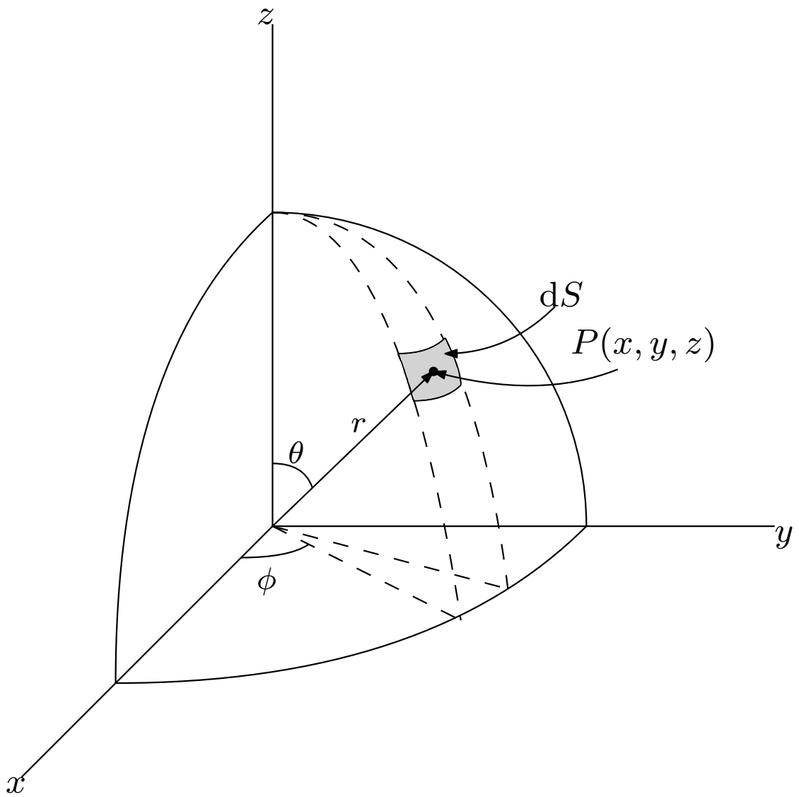


$$\mathscr{P}_{av} = \overrightarrow{e_r}\frac{j\omega\mu m^2}{16\pi r^5}\sin^2\theta - \overrightarrow{e_\theta}\frac{j\omega\mu m^2}{8\pi r^5}\sin\theta\cos\theta$$

[1] Nathan Ida. Engineering electromagnetics. Springer, 2000.

Limitations

- Near-Field probes
  - Only for showing proof of concept
  - Inefficient for distances > 2 cm



$$\mathscr{P}_{av} = \overrightarrow{e_r}\frac{j\omega\mu m^2}{16\pi r^5}\sin^2\theta - \overrightarrow{e_\theta}\frac{j\omega\mu m^2}{8\pi r^5}\sin\theta\cos\theta$$

$m :=$ magnetic moment of loop

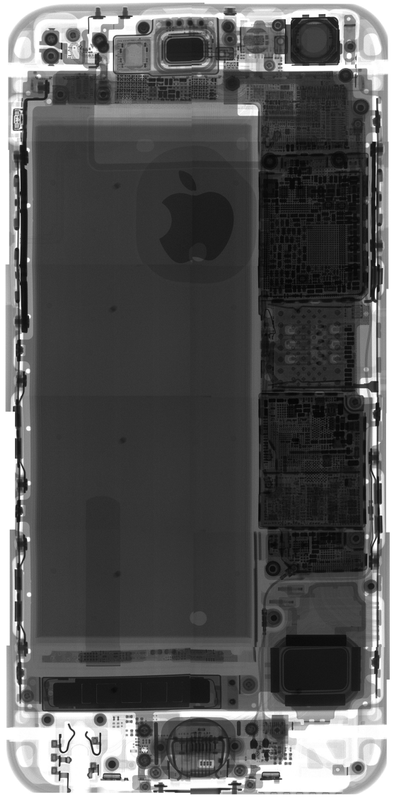
$\mu :=$ magnetic permeability

$\omega :=$ angular frequency (i.e., $\omega = 2\pi f$)

[1] Nathan Ida. Engineering electromagnetics. Springer, 2000.

Signal Strength

Signal Strength

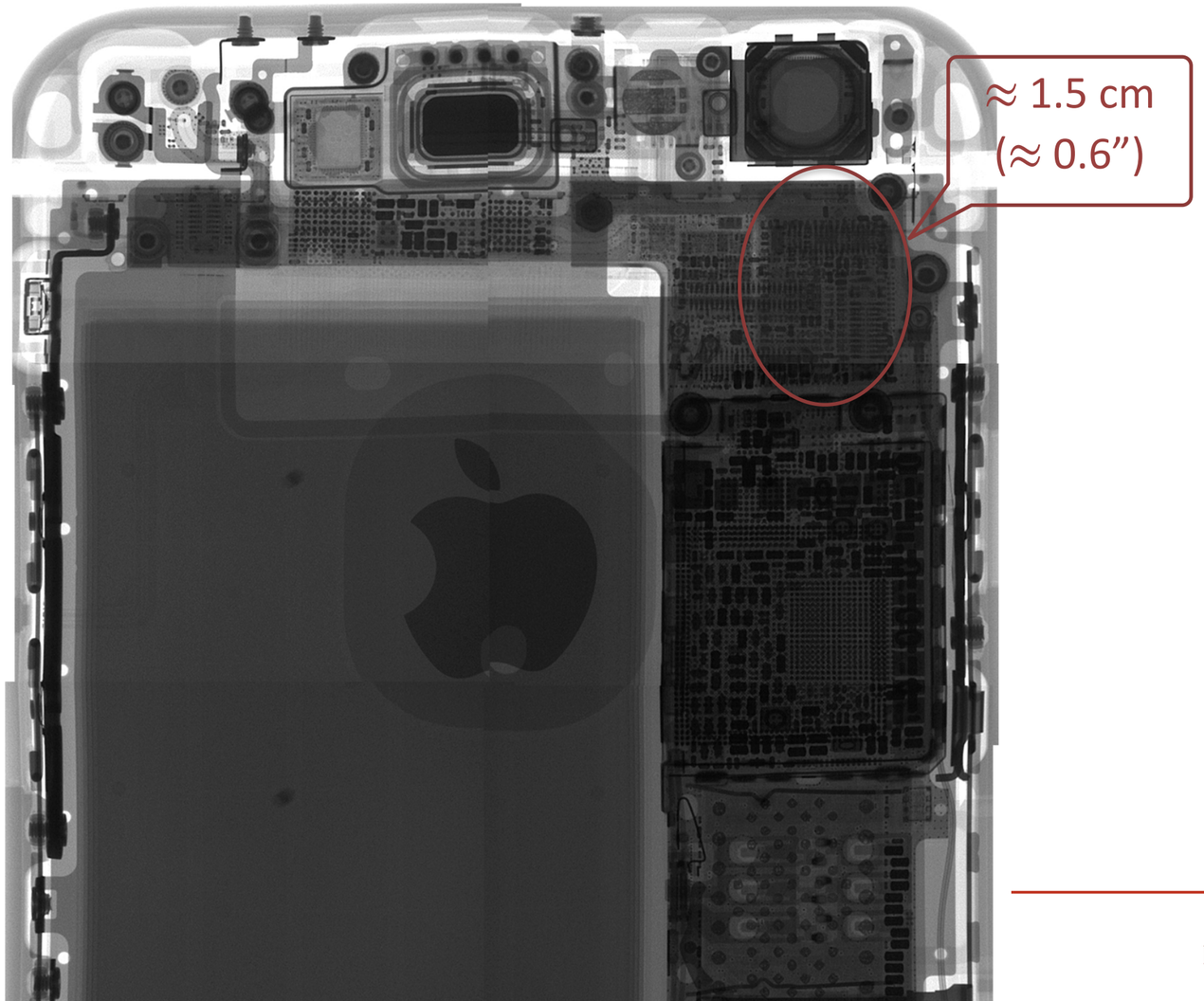


iPhone 6(s)

Signal Strength

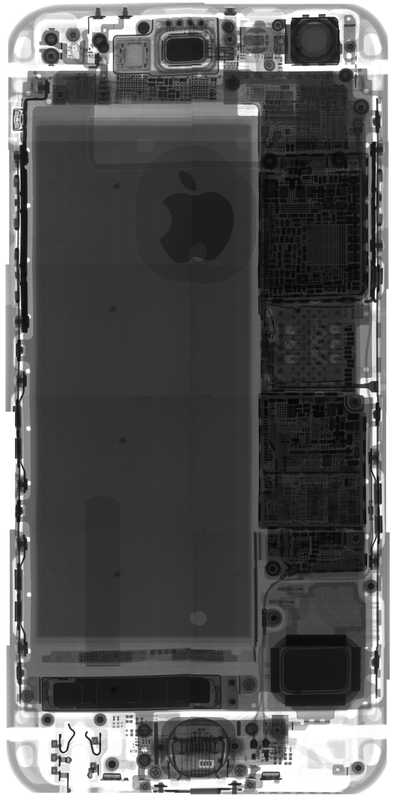
iPhone 6(s)

Signal Strength



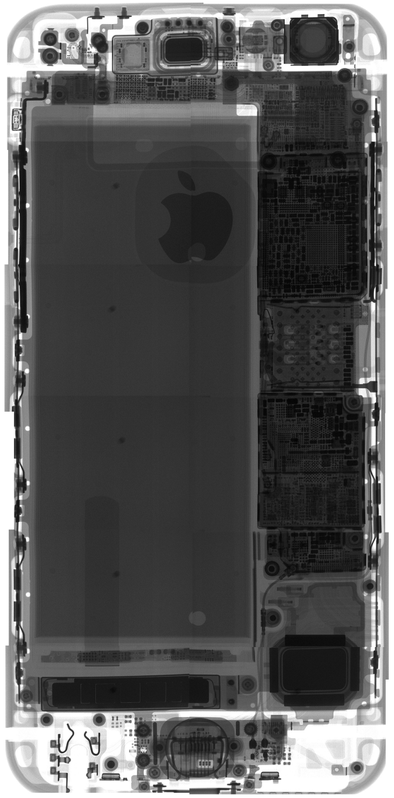
iPhone 6(s)

Signal Strength

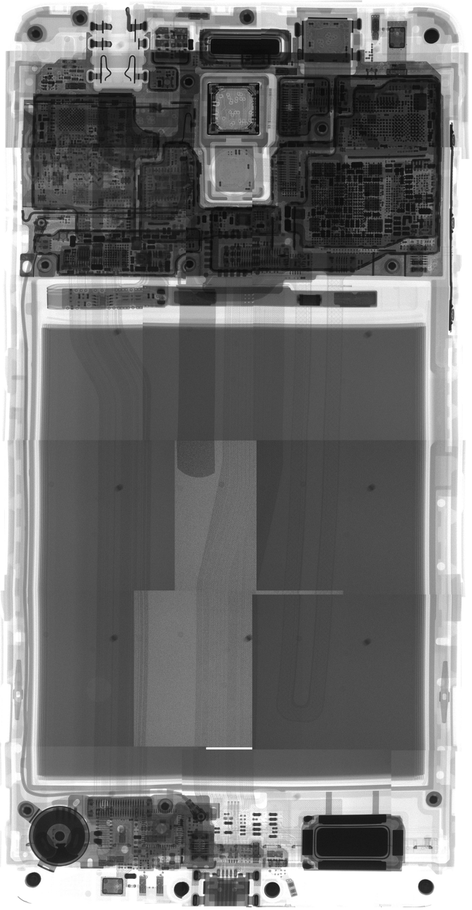


iPhone 6(s)

Signal Strength

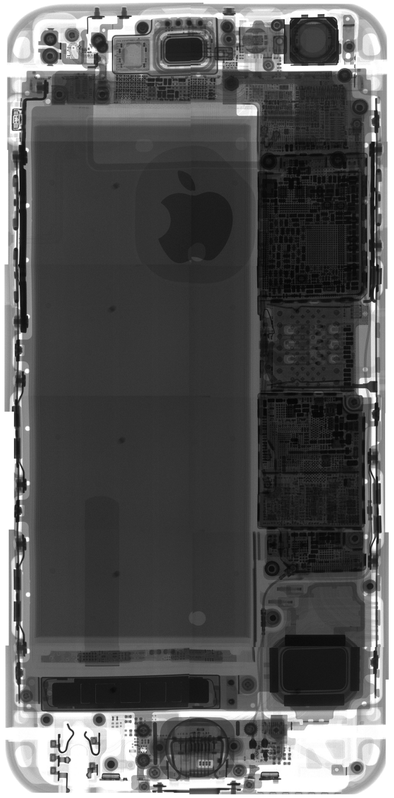


iPhone 6(s)

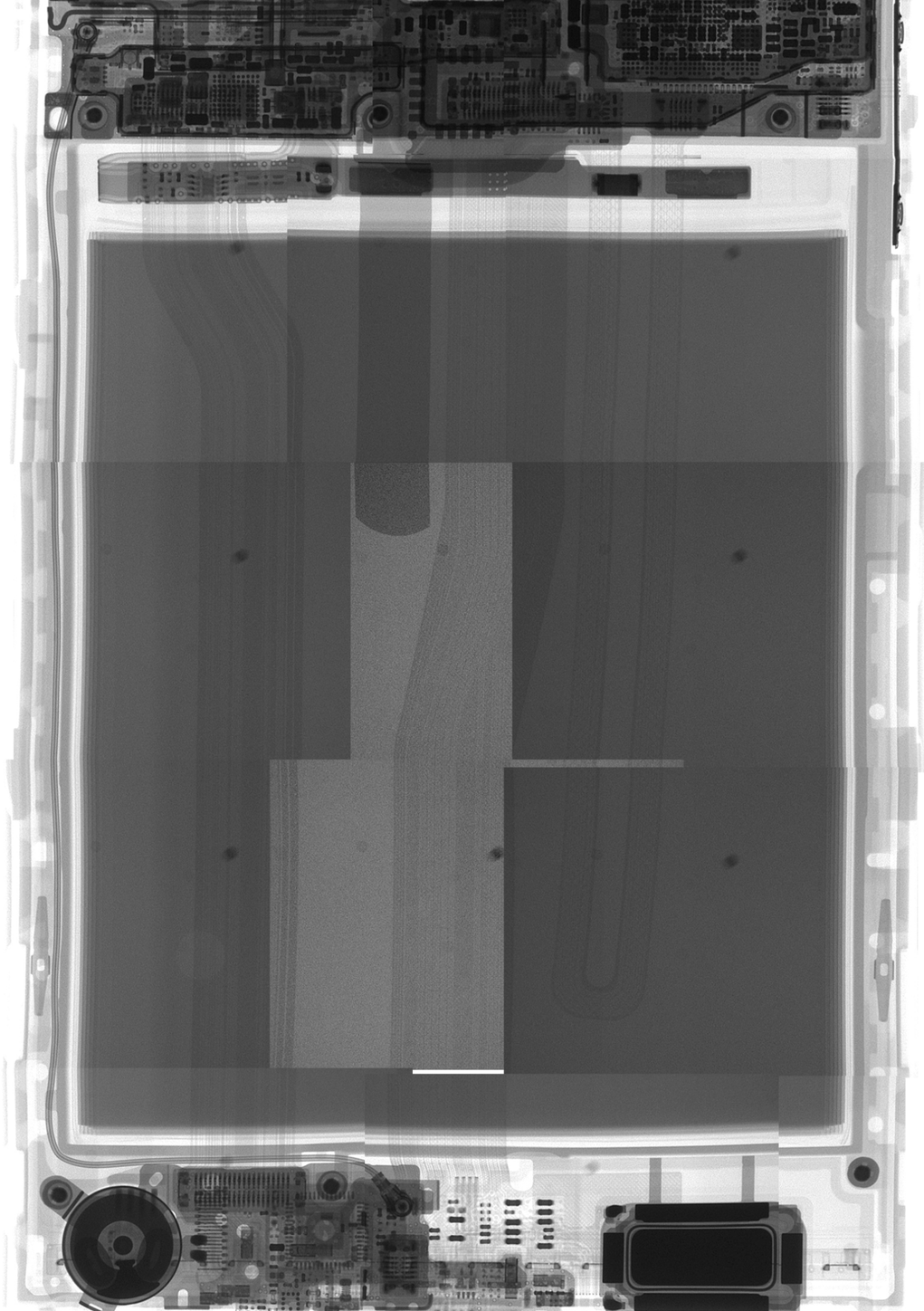


Honor 6X

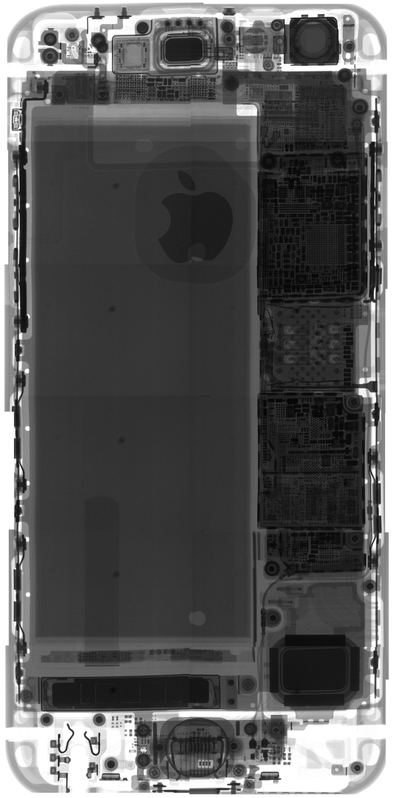
Signal Streng



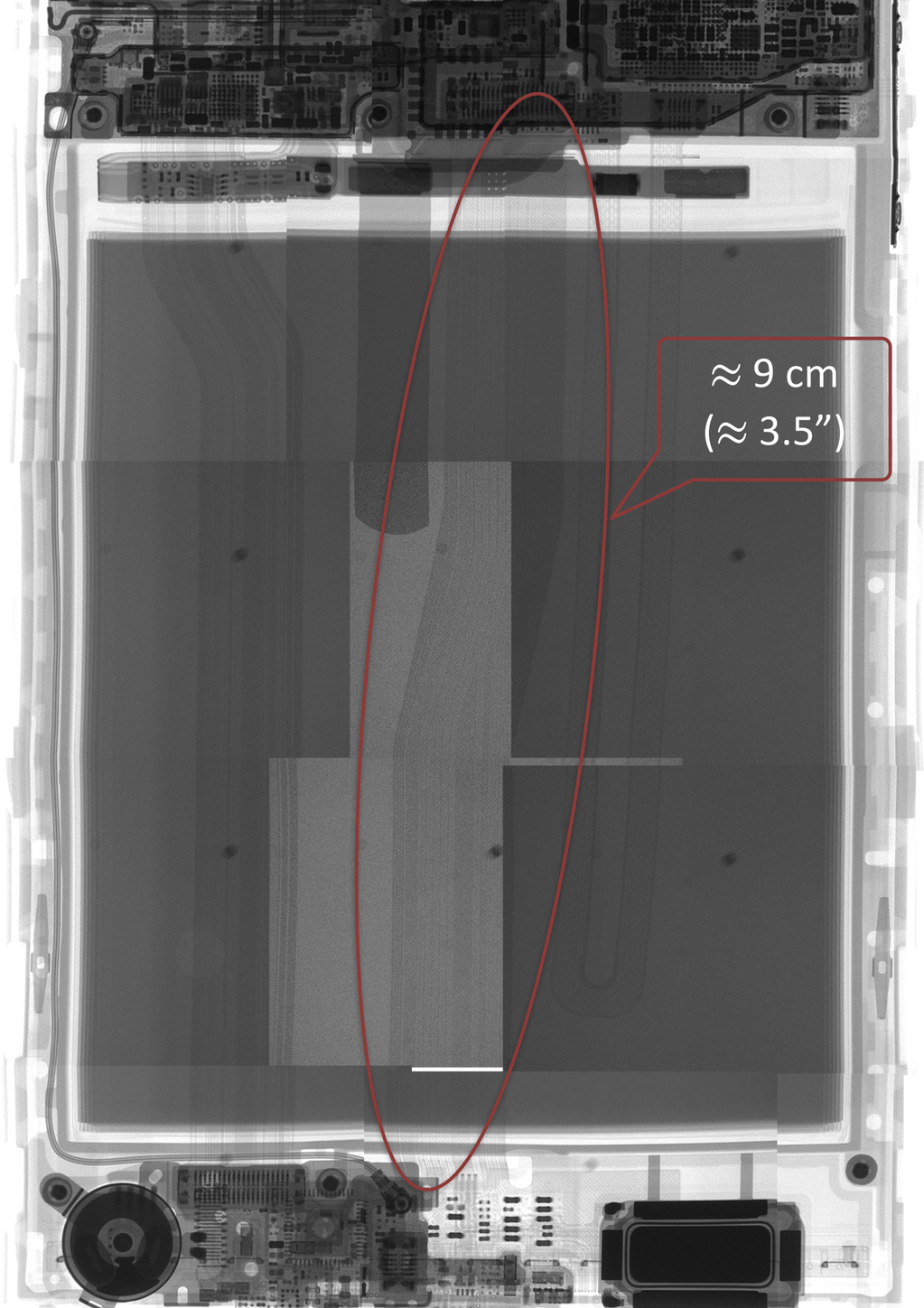
iPhone 6(s)



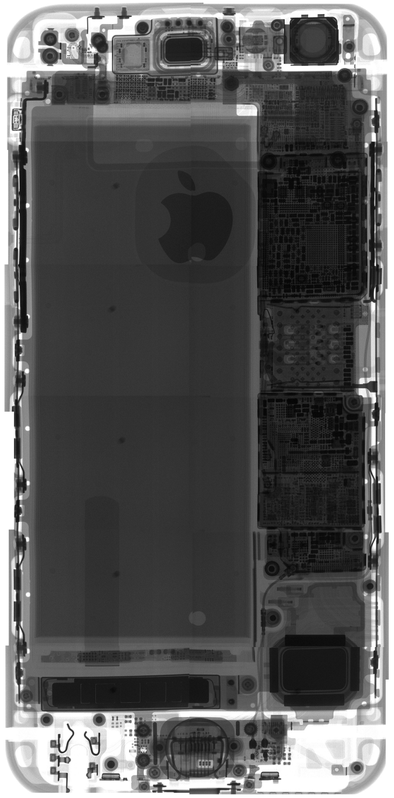
Signal Streng



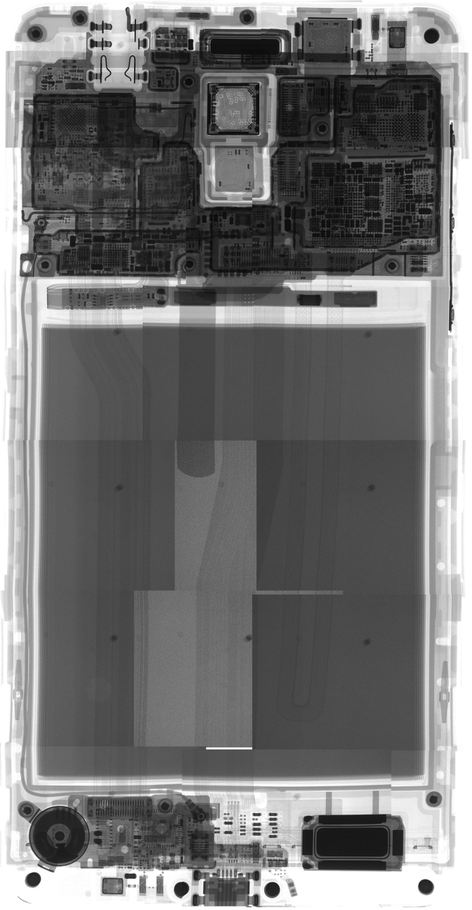
iPhone 6(s)



Signal Strength

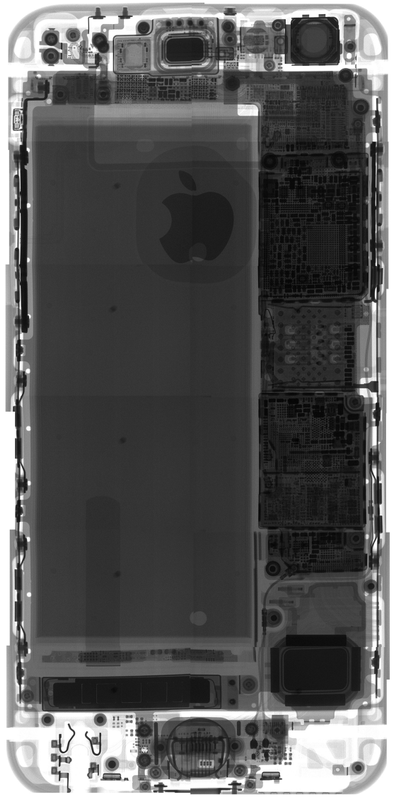


iPhone 6(s)

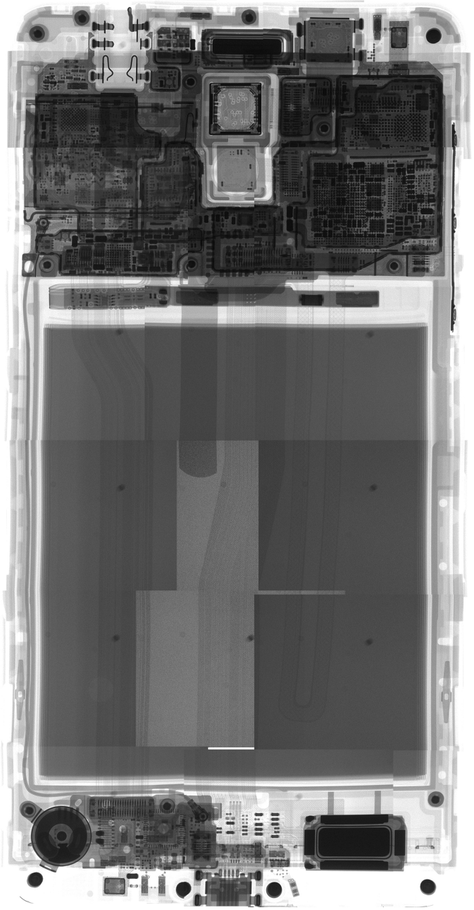


Honor 6X

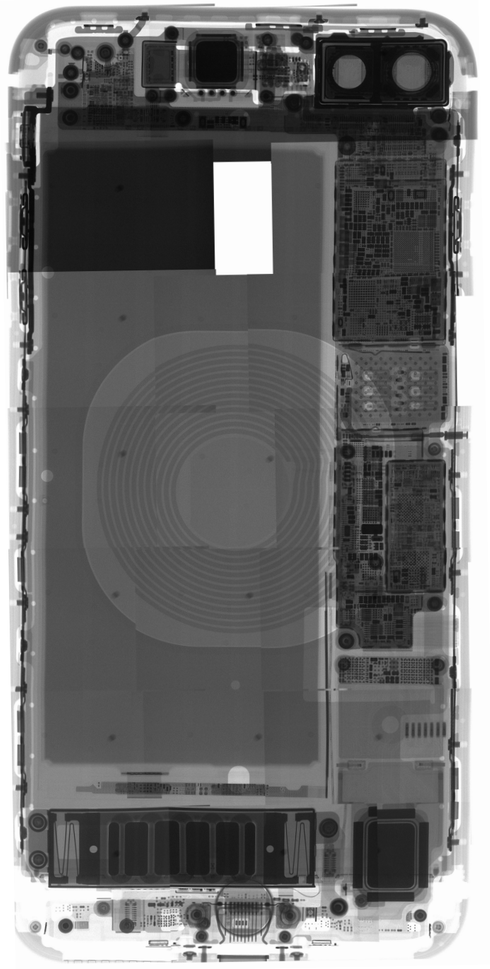
Signal Strength



iPhone 6(s)

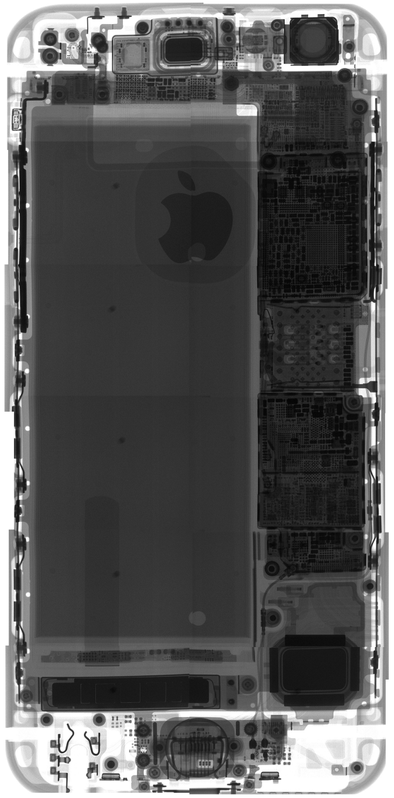


Honor 6X



iPhone 8 Plus

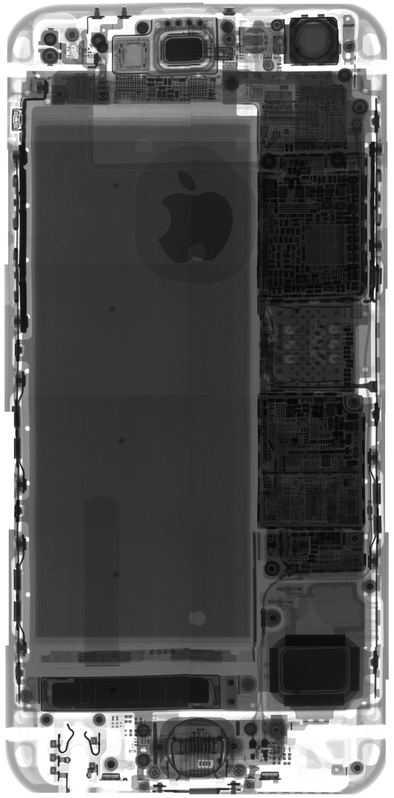
Signal Streng



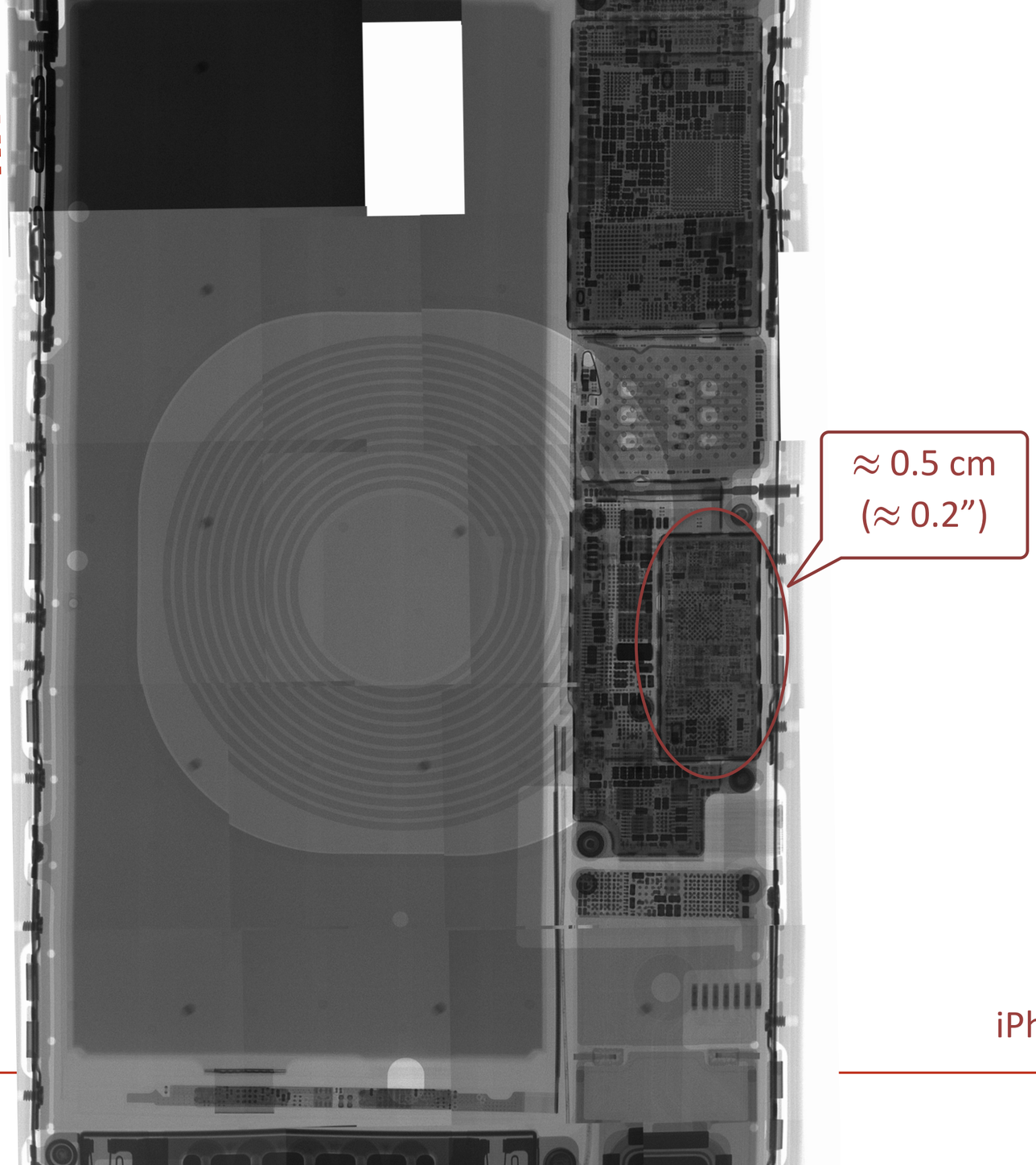
iPhone 6(s)

iPhone 8 Plus

Signal Streng



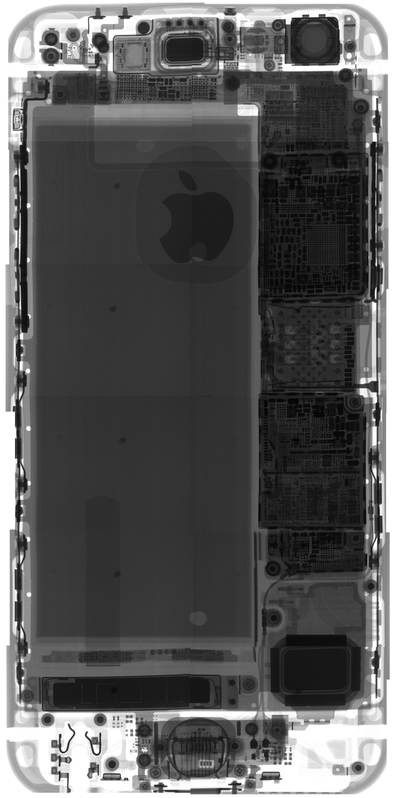
iPhone 6(s)



iPhone 8 Plus

Signal Streng

Better shielding
(More power to X-ray)

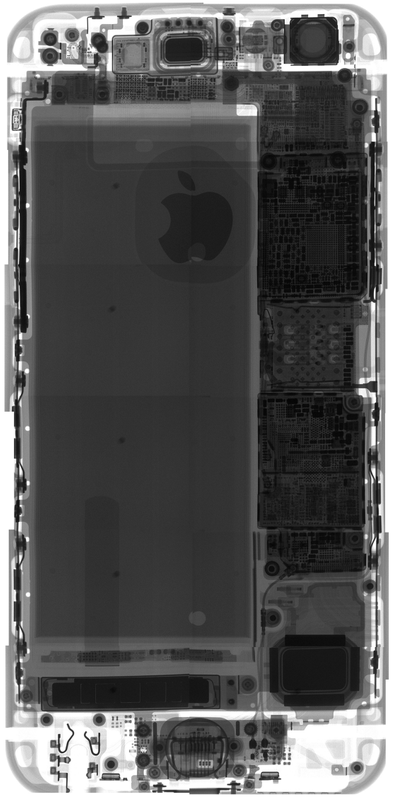


iPhone 6(s)

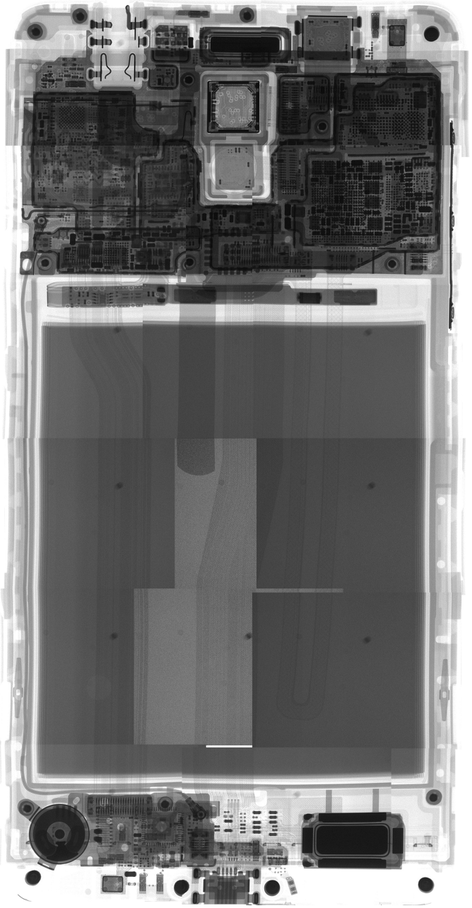
≈ 0.5 cm
(≈ 0.2”)

iPhone 8 Plus

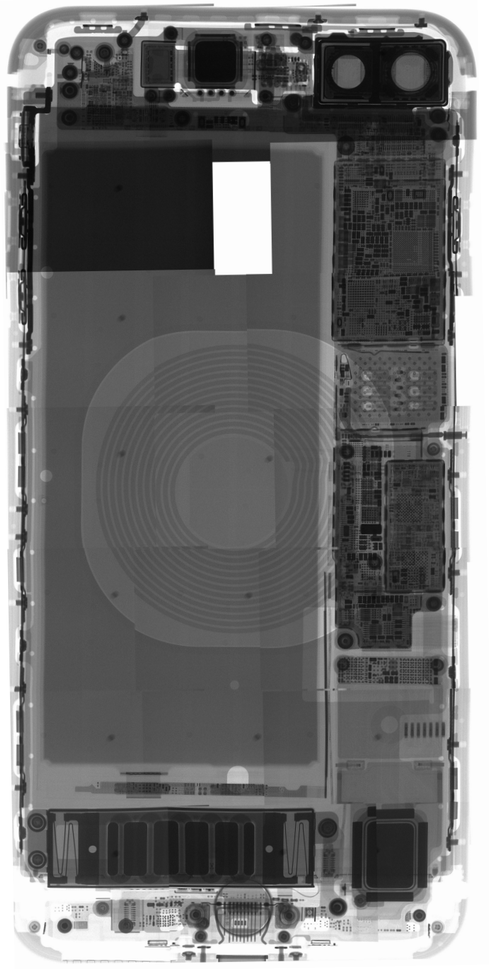
Signal Strength



iPhone 6(s)



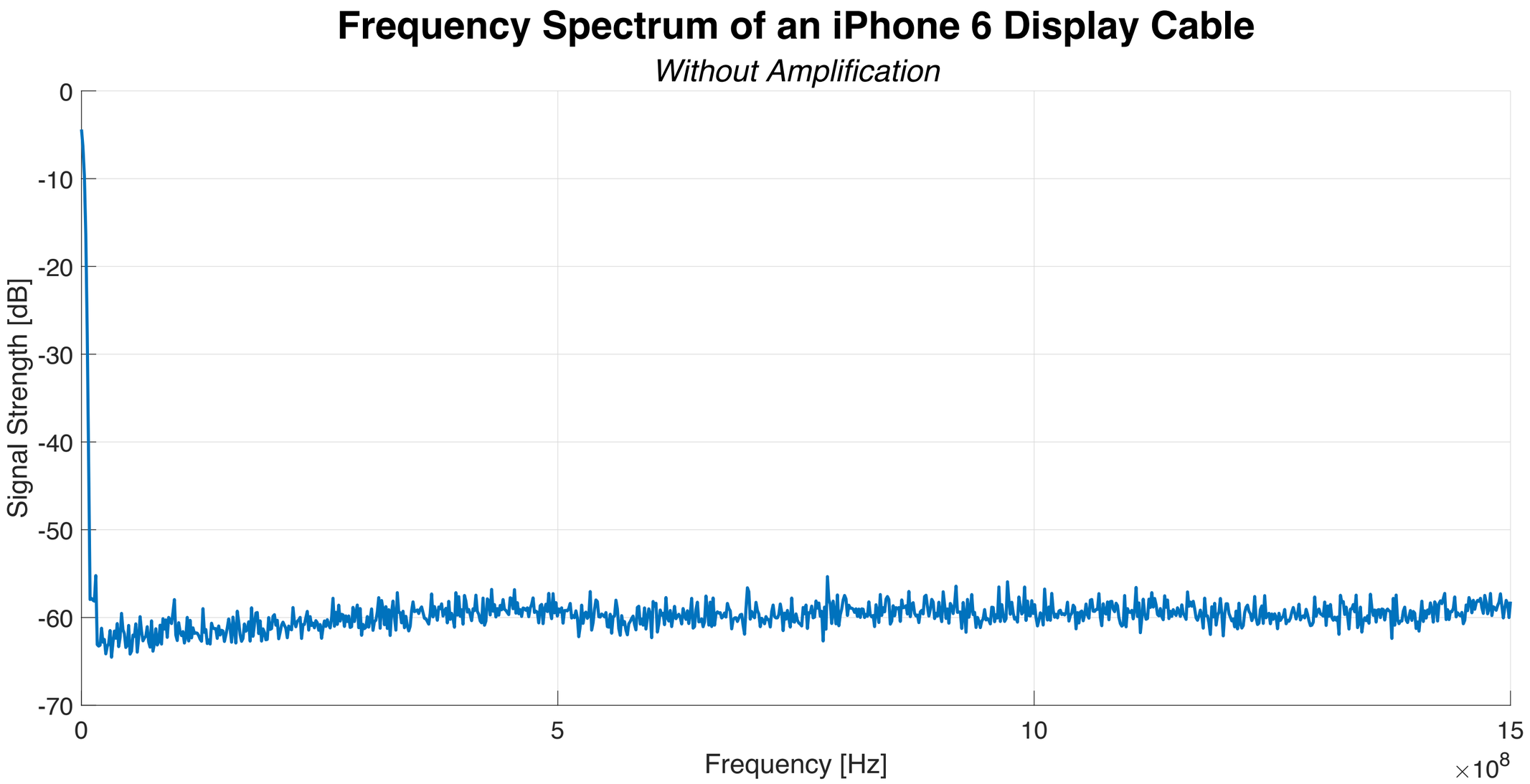
Honor 6X



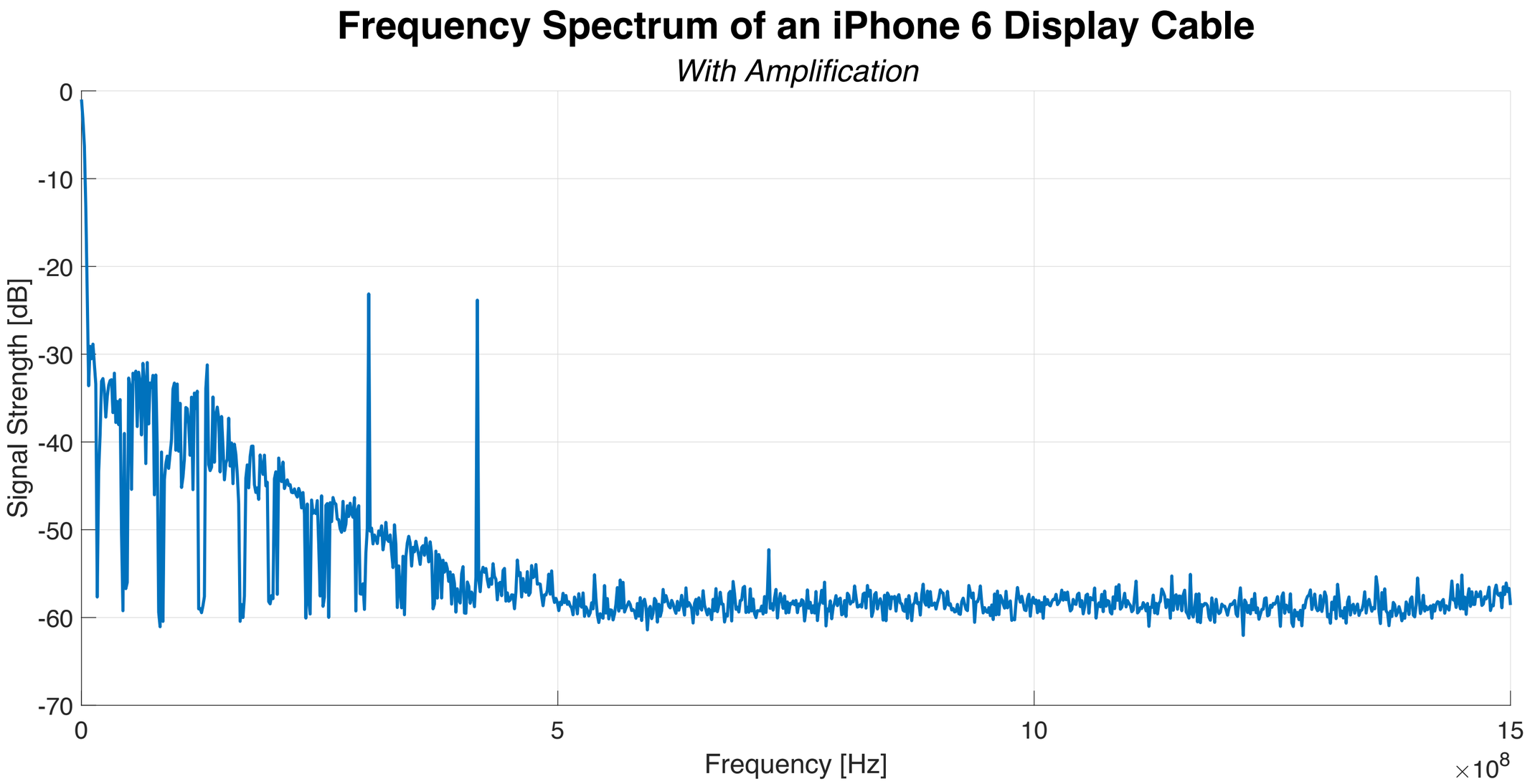
iPhone 8 Plus

Amplification

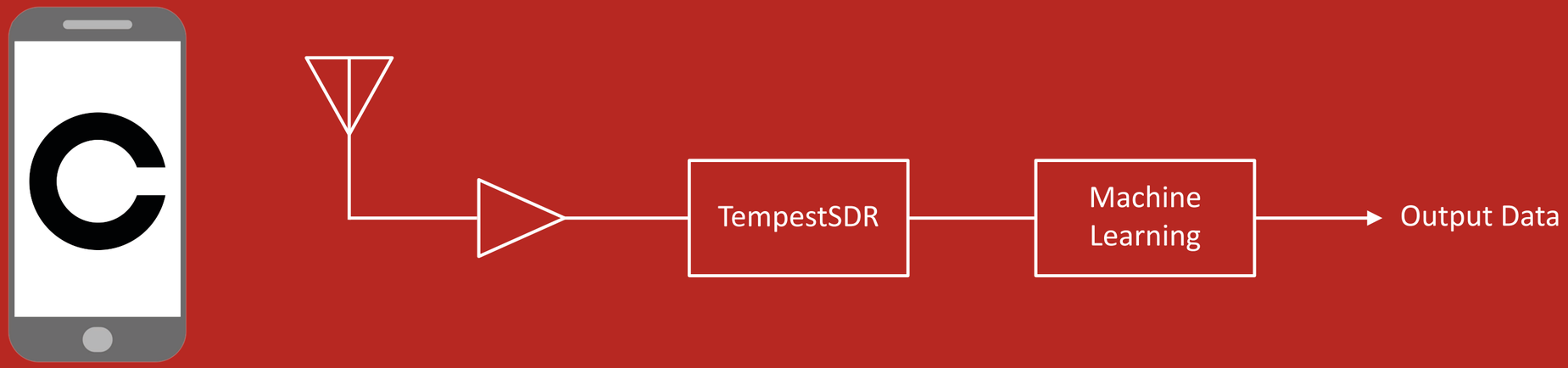
Amplification



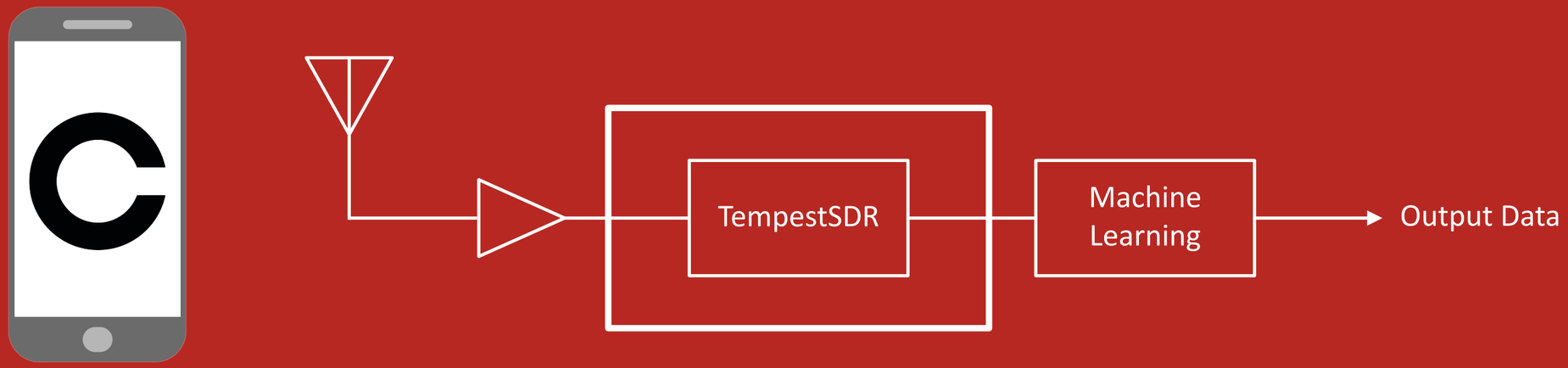
Amplification



TempestSDR

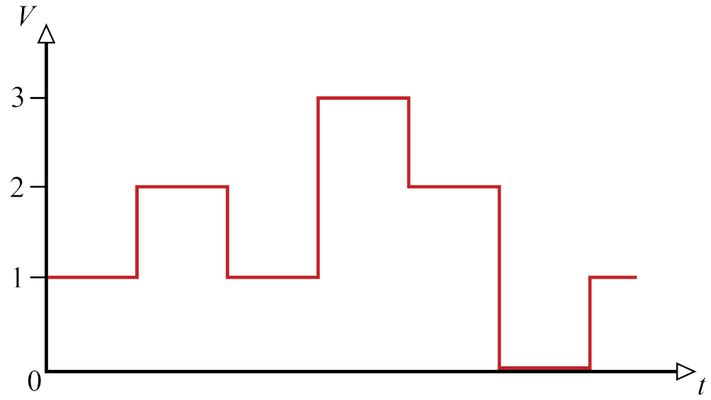


TempestSDR

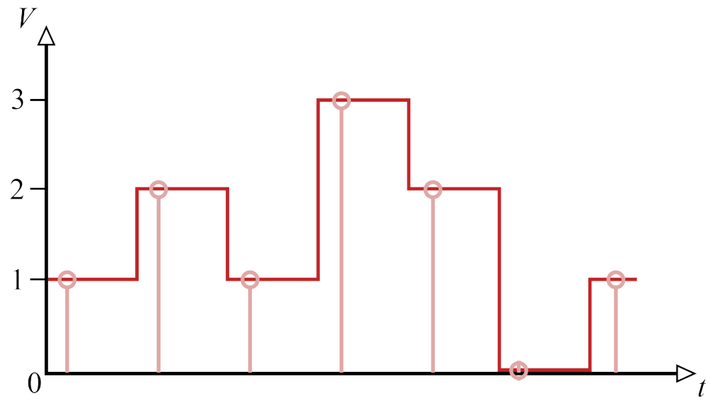


Schematic Design

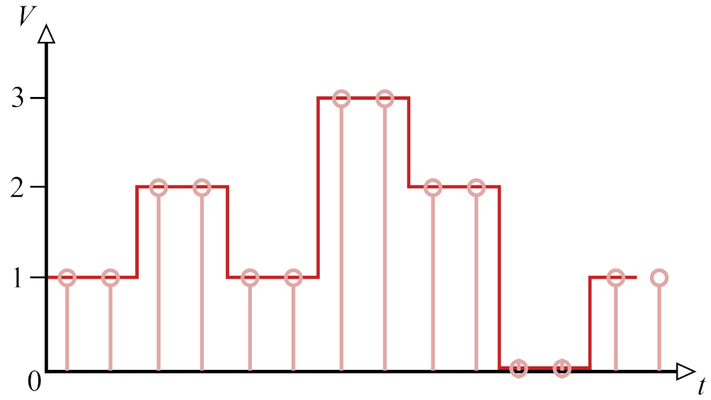
Schematic Design



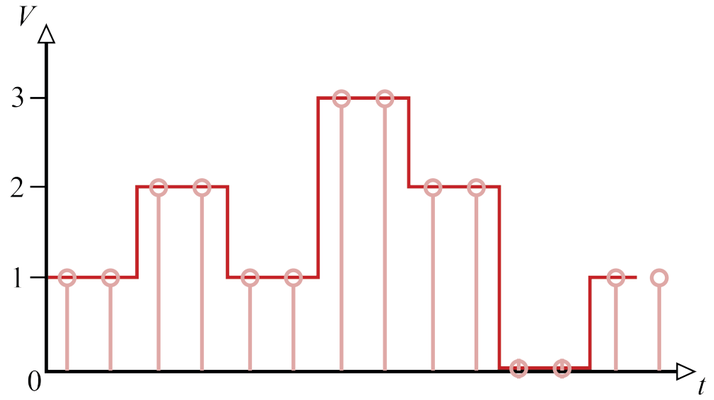
Schematic Design



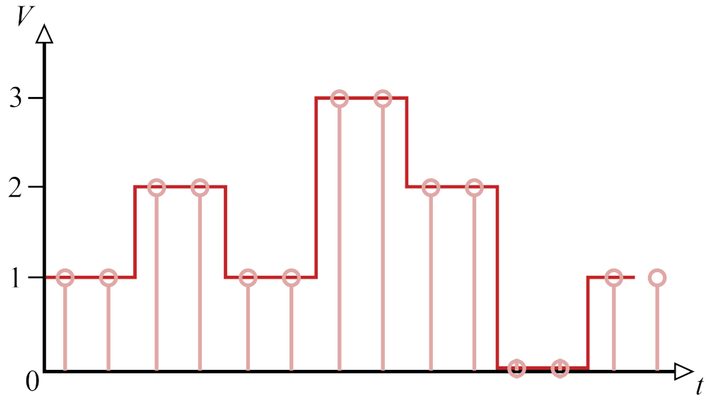
Schematic Design



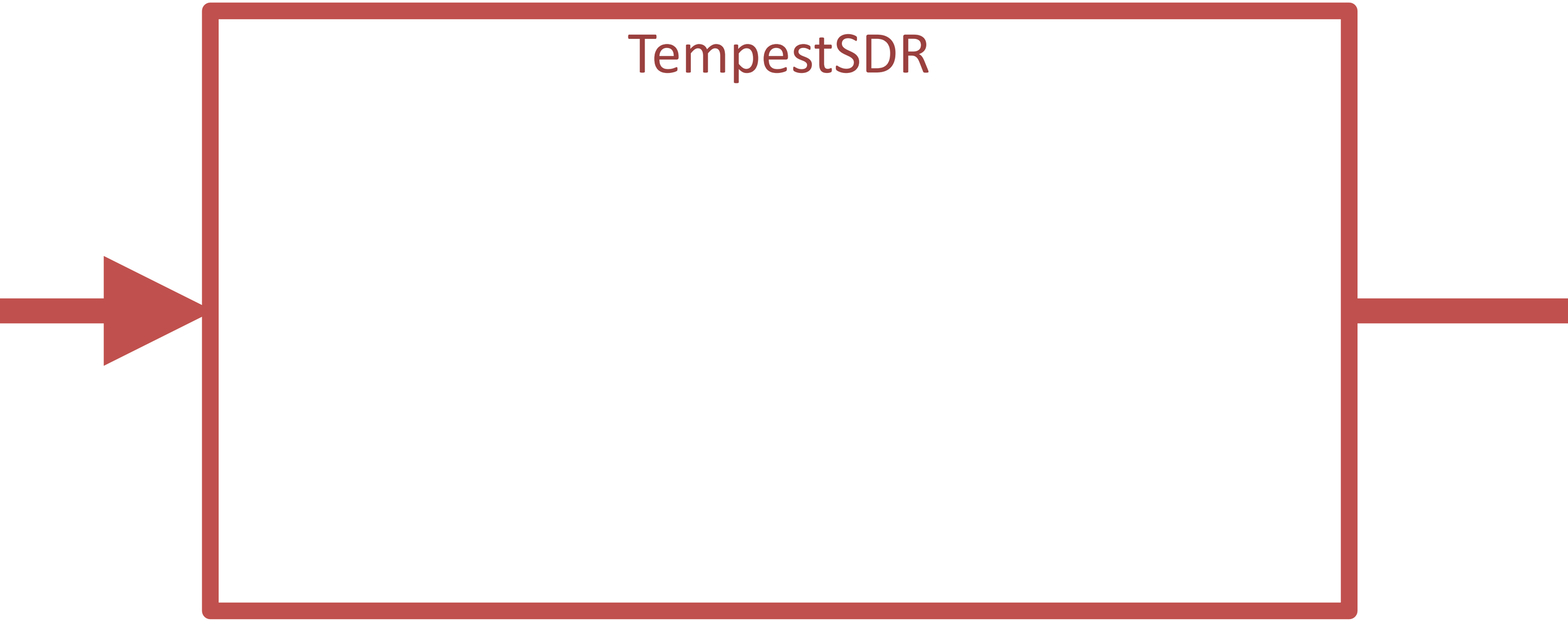
Schematic Design



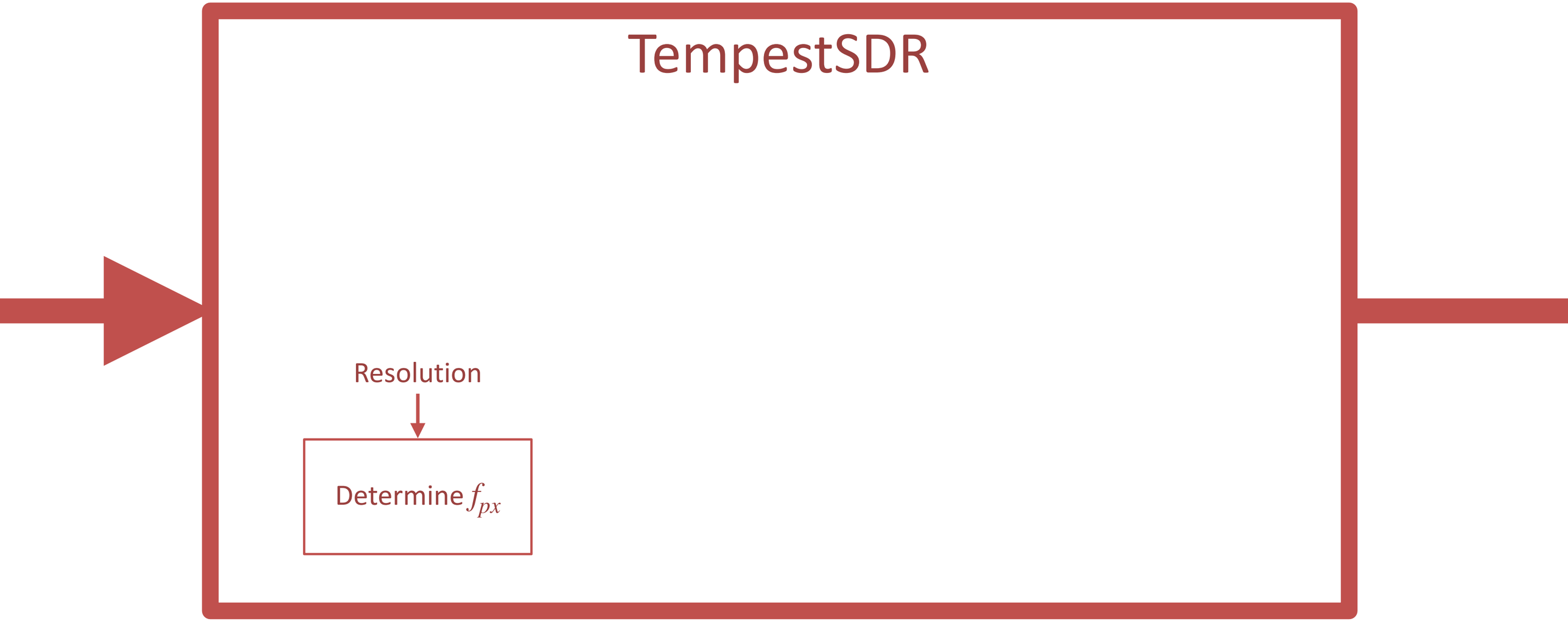
Schematic Design



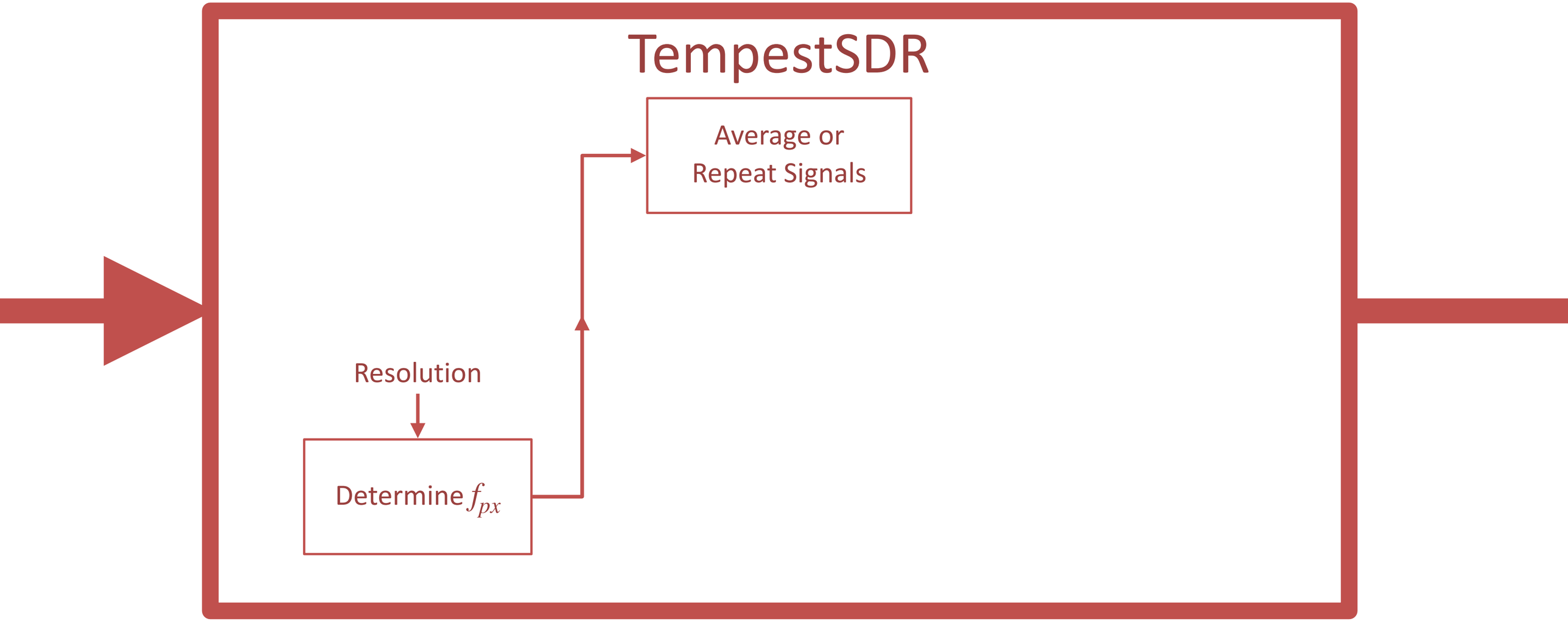
Schematic Design



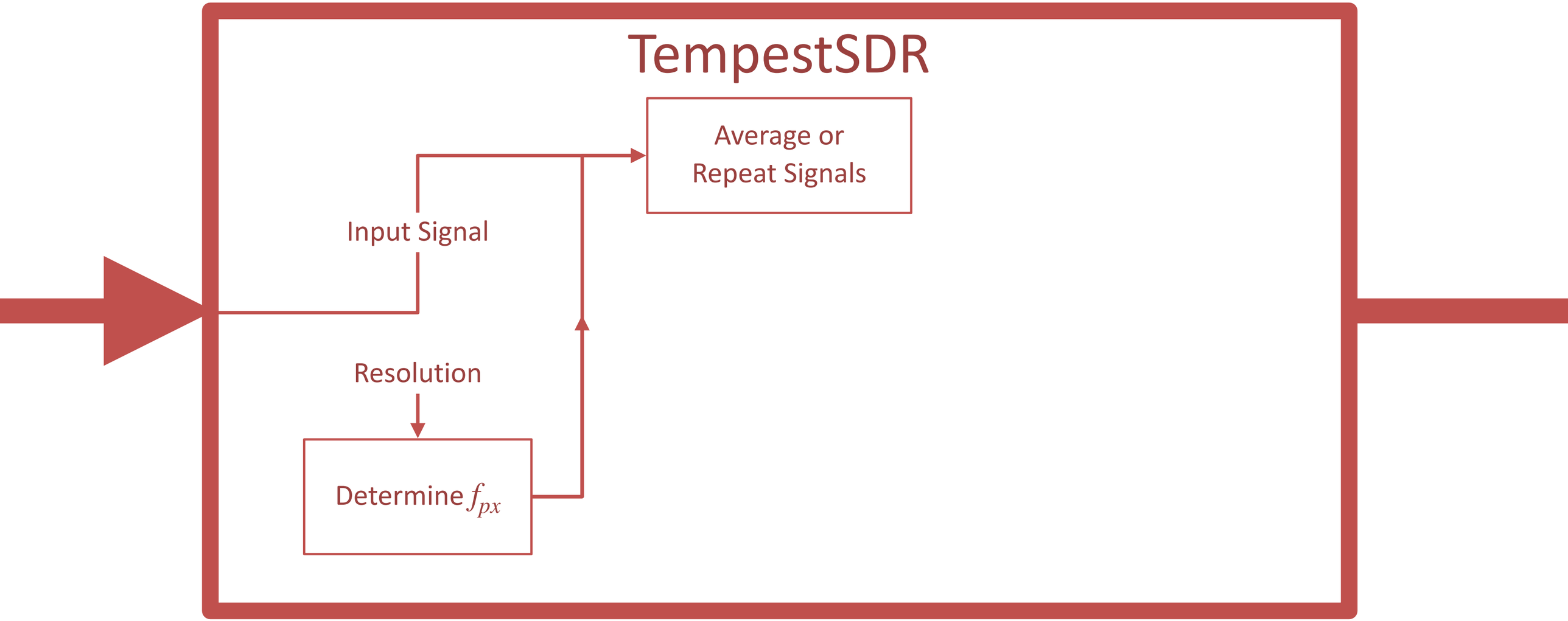
Schematic Design



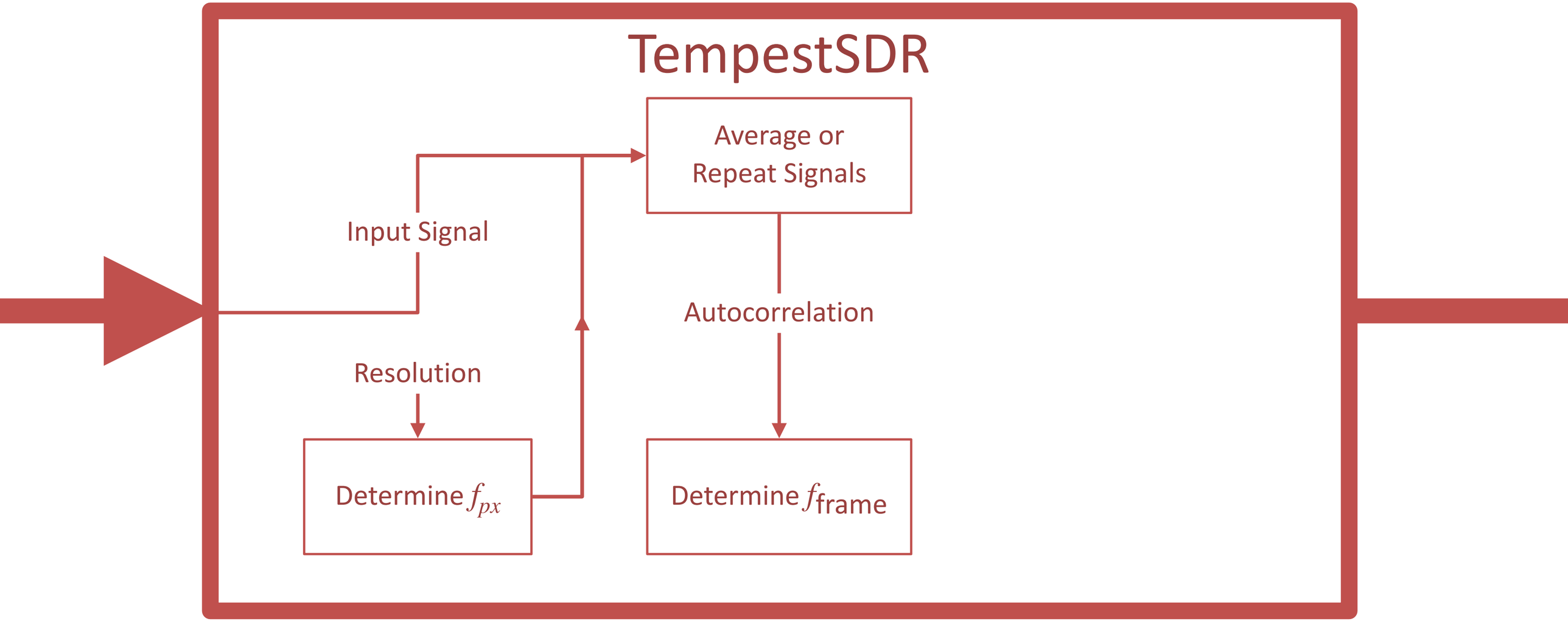
Schematic Design



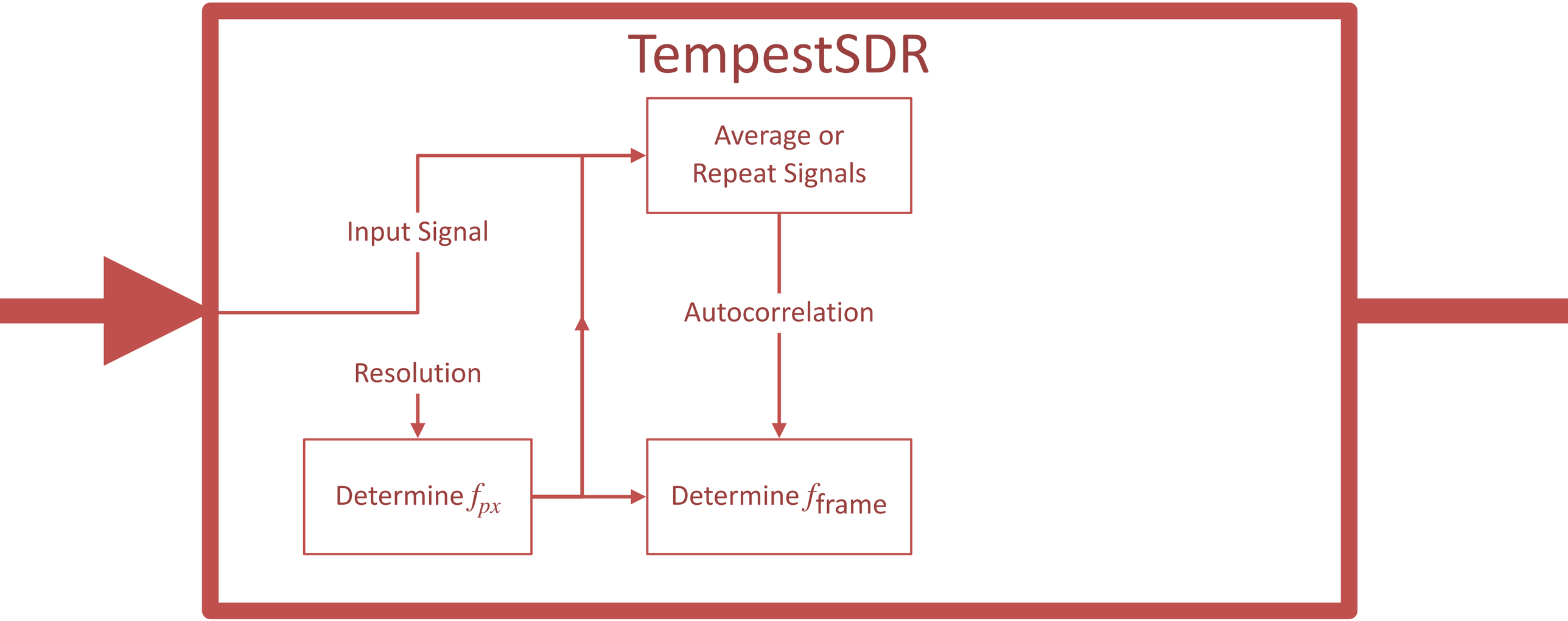
Schematic Design



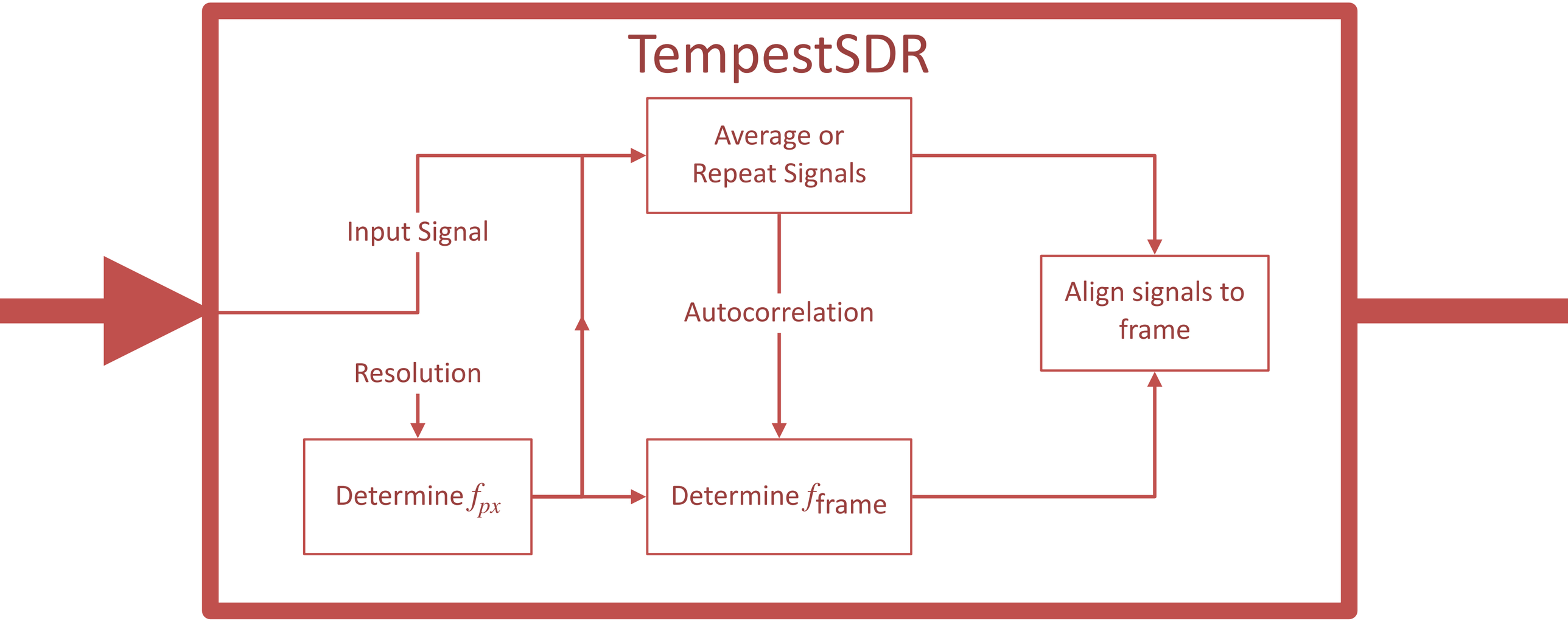
Schematic Design



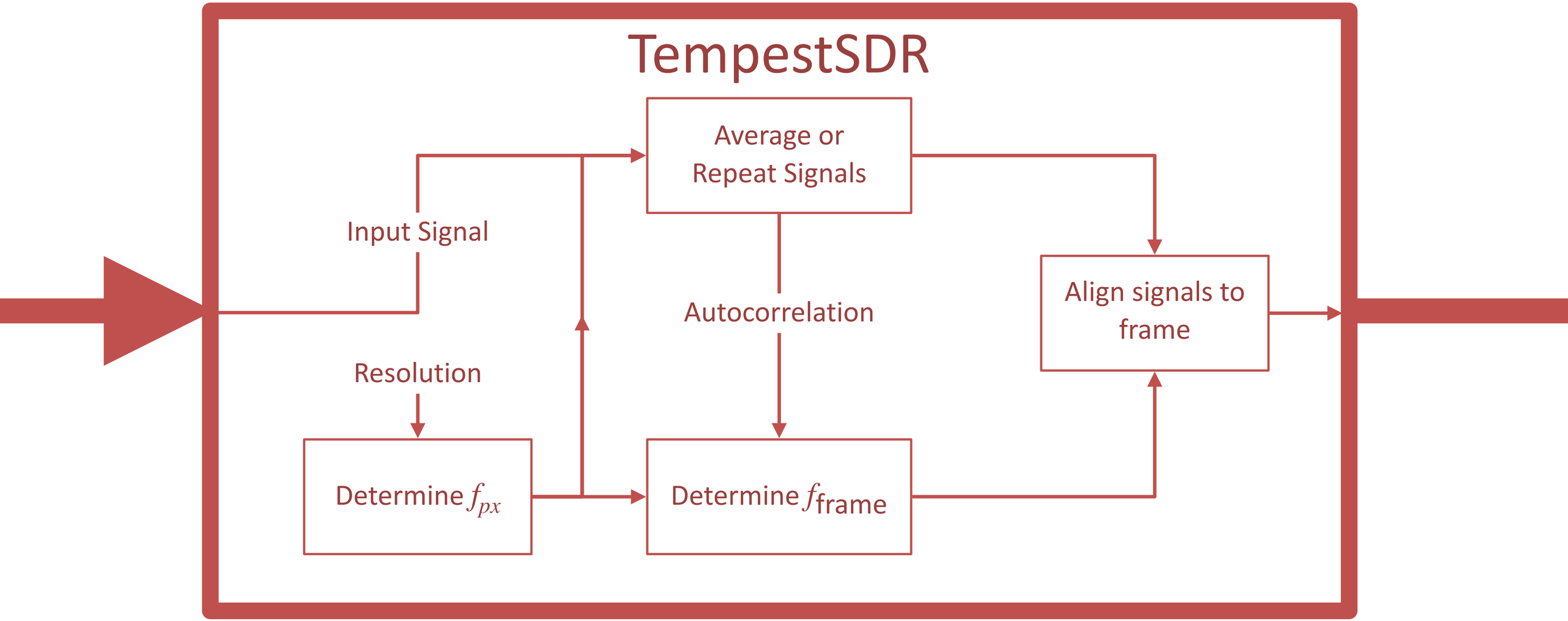
Schematic Design



Schematic Design

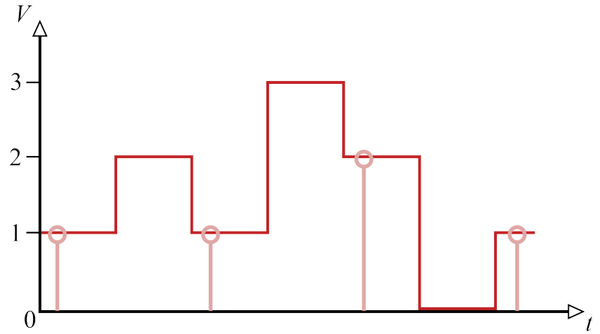


Schematic Design

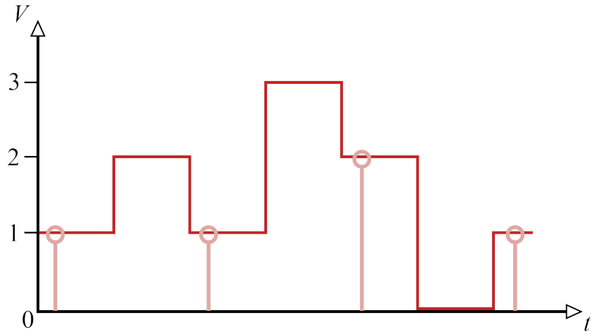


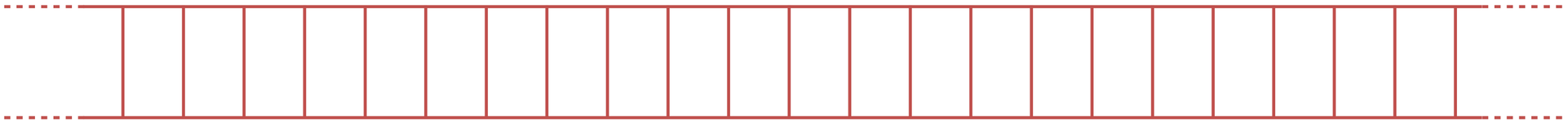
Distinguishing Pixels

Distinguishing Pixels

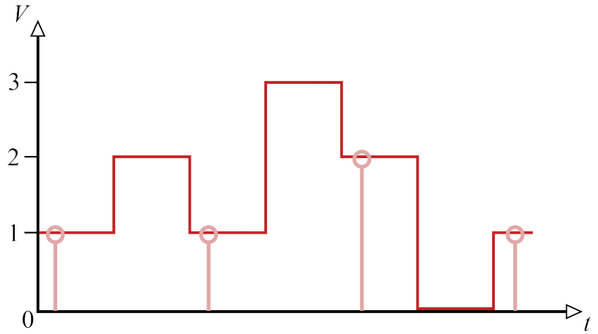


Distinguishing Pixels

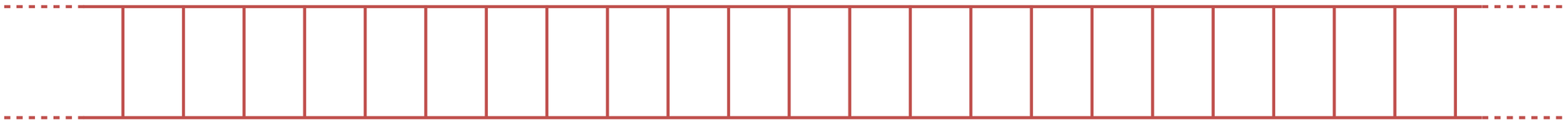




Distinguishing Pixels

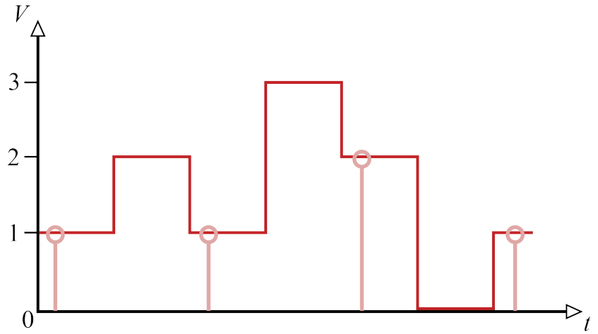


Input Signal

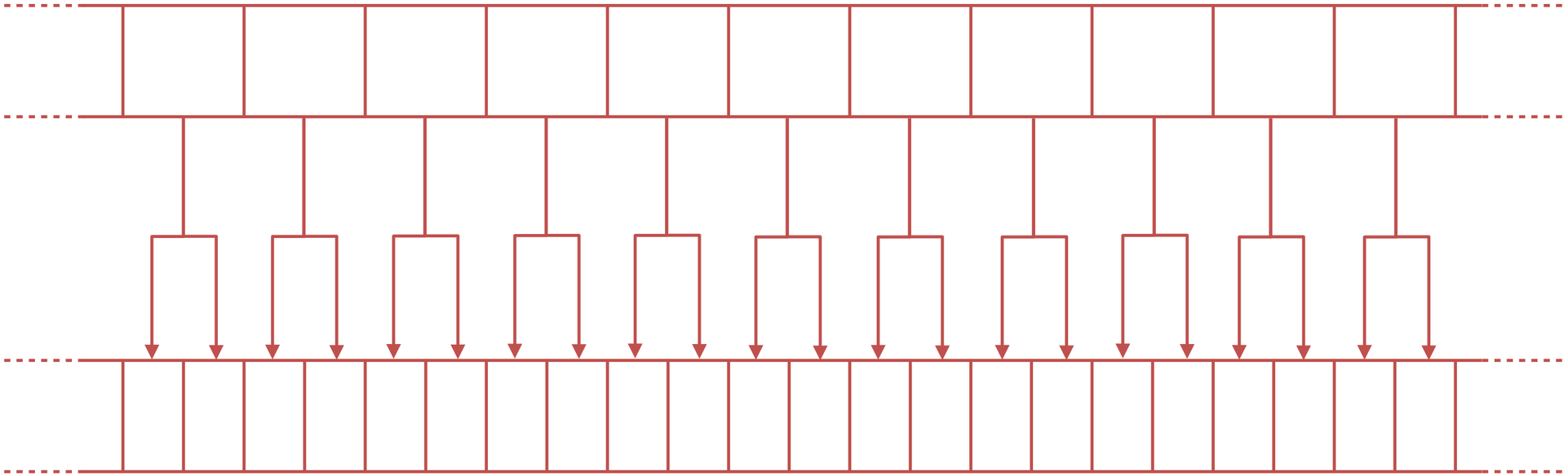


Pixel Component
(Bits or Steps)

Distinguishing Pixels

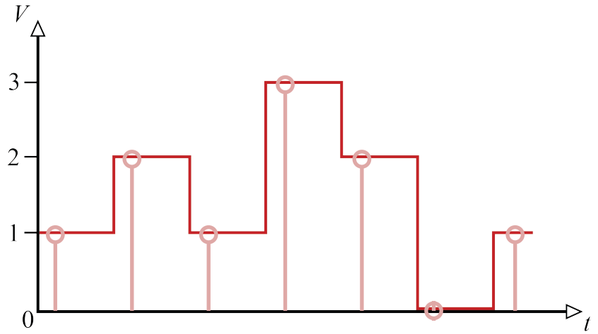


Input Signal

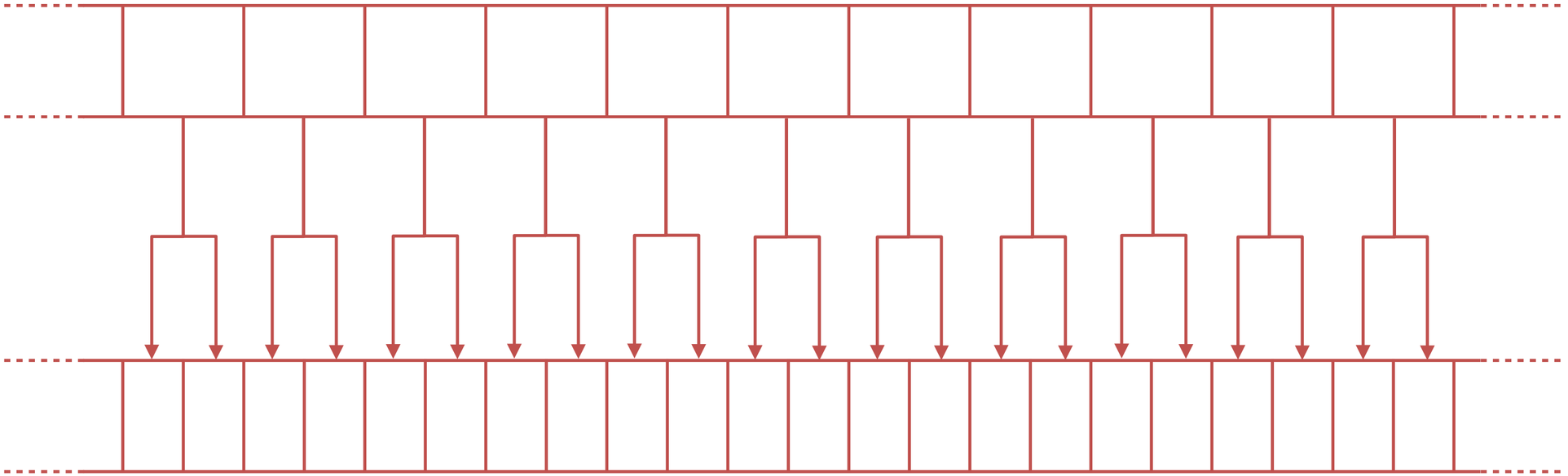


Pixel Component
(Bits or Steps)

Distinguishing Pixels

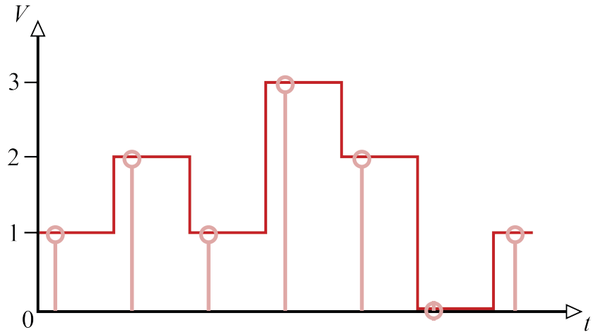


Input Signal

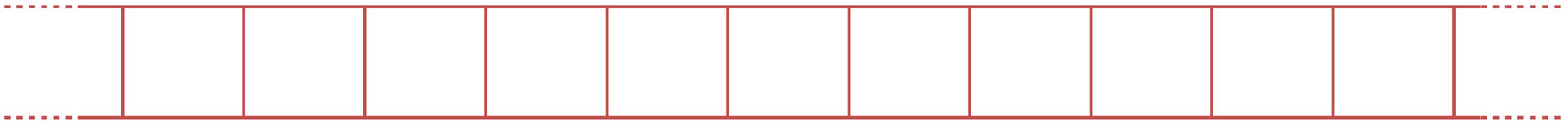


Pixel Component
(Bits or Steps)

Distinguishing Pixels

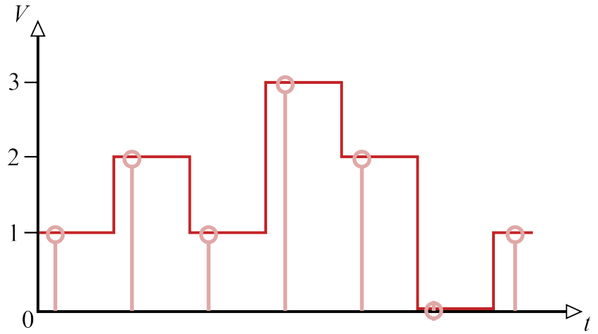


Input Signal

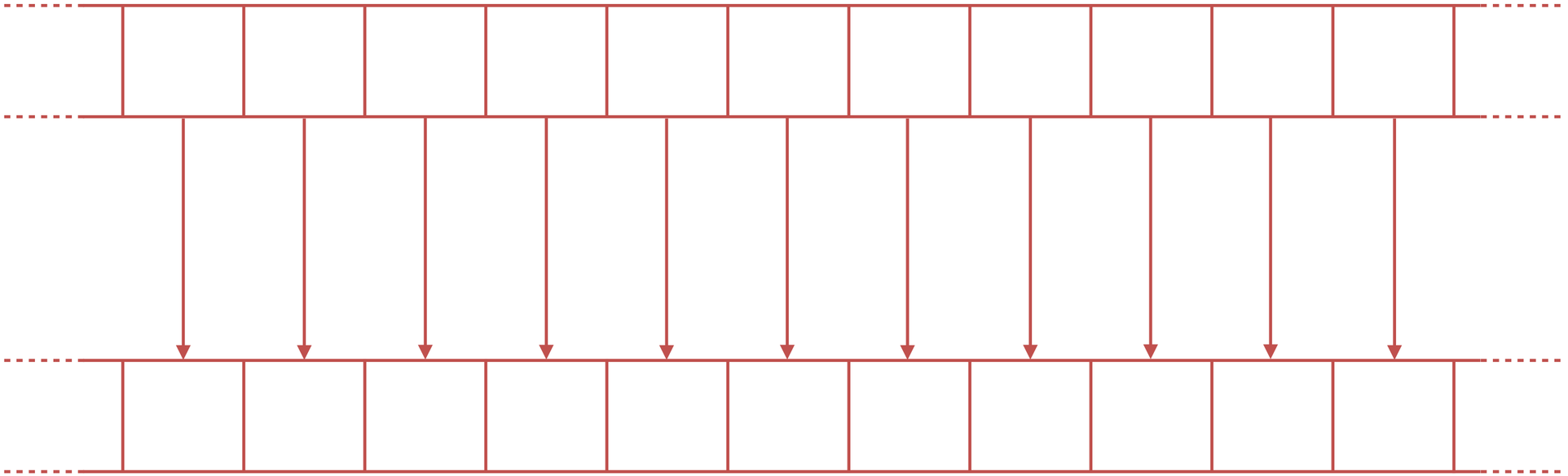


Pixel Component
(Bits or Steps)

Distinguishing Pixels

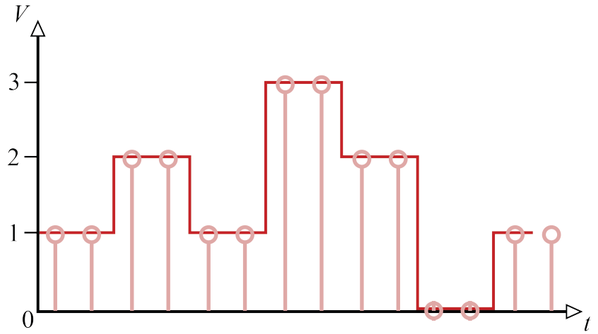


Input Signal

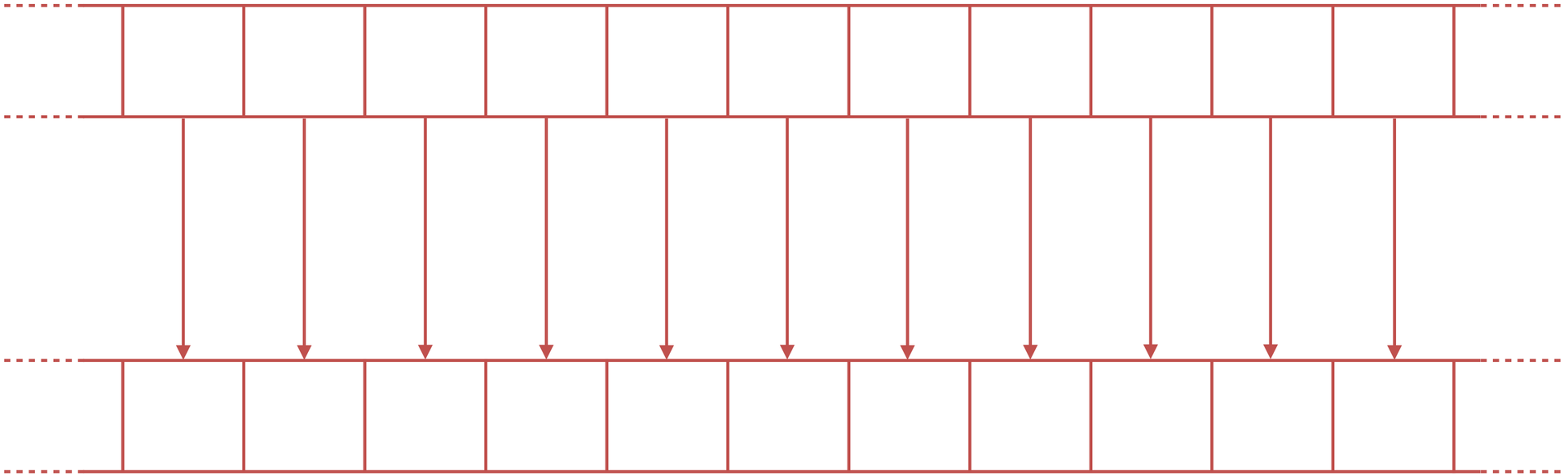


Pixel Component
(Bits or Steps)

Distinguishing Pixels

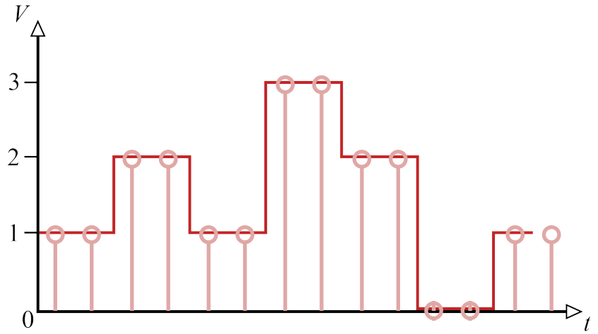


Input Signal



Pixel Component
(Bits or Steps)

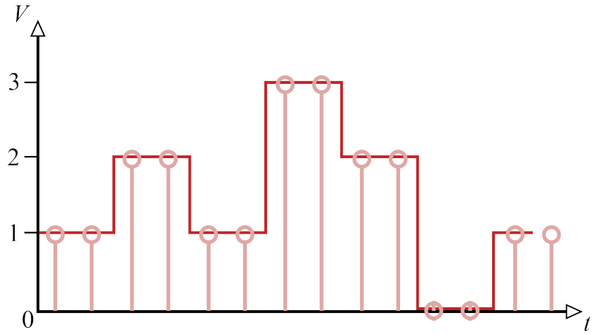
Distinguishing Pixels

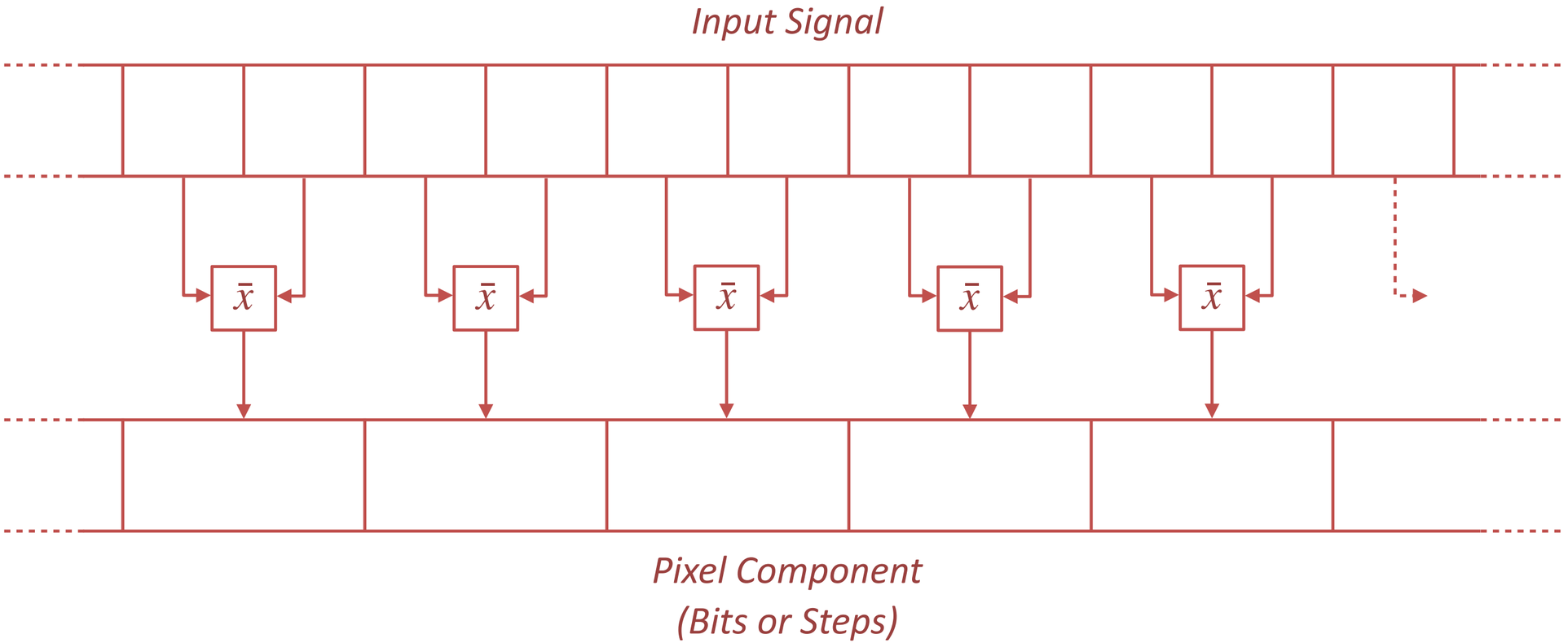


Input Signal

Pixel Component
(Bits or Steps)

Distinguishing Pixels

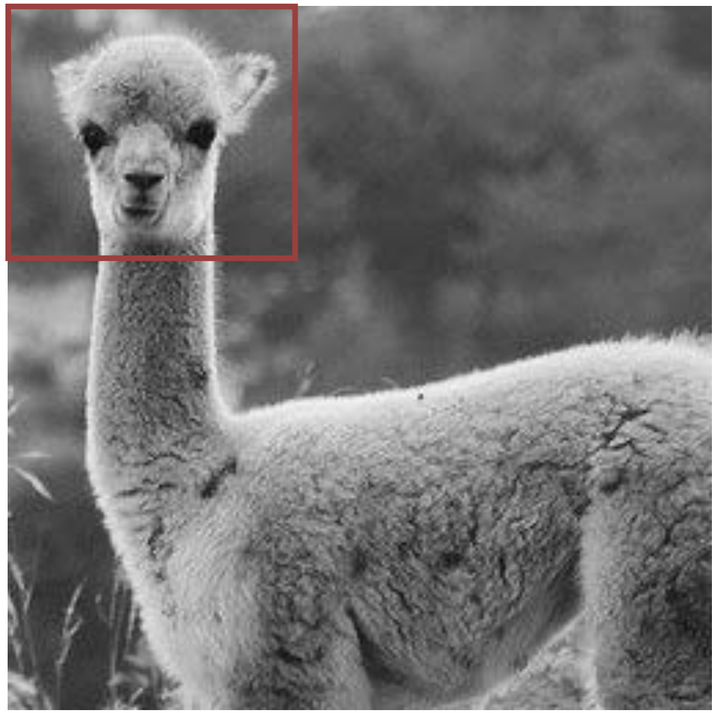




Distinguishing Frames

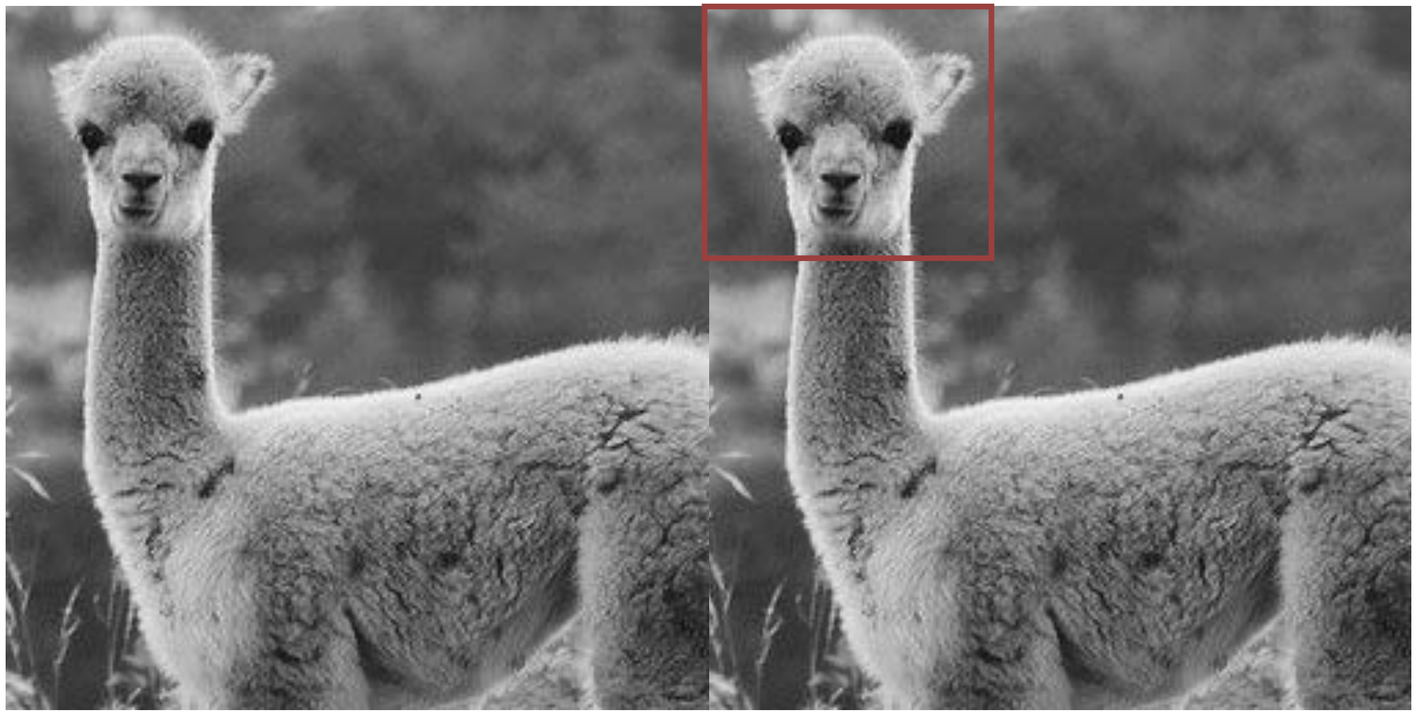
Distinguishing Frames

Distinguishing Frames



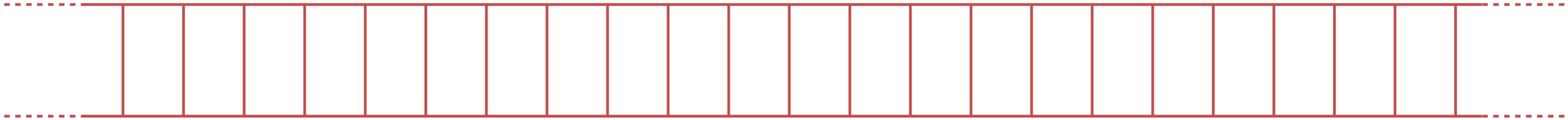
Distinguishing Frames

Distinguishing Frames

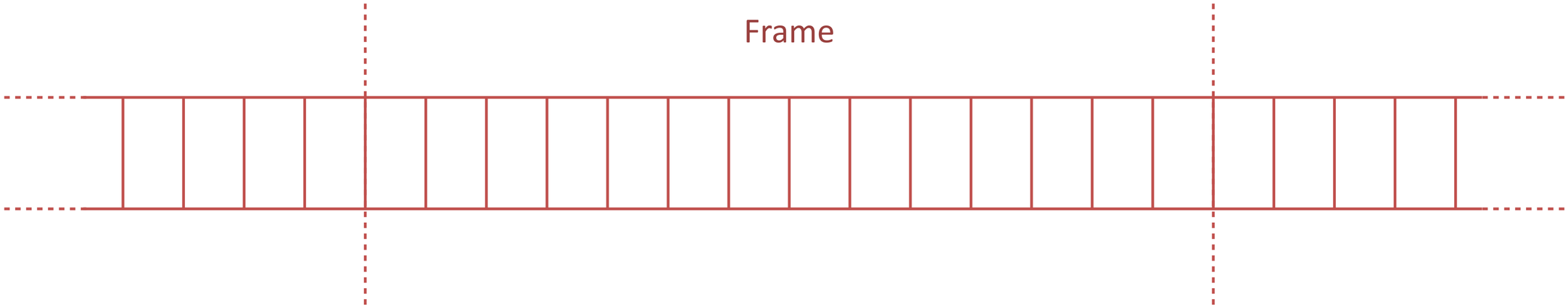


Alignment

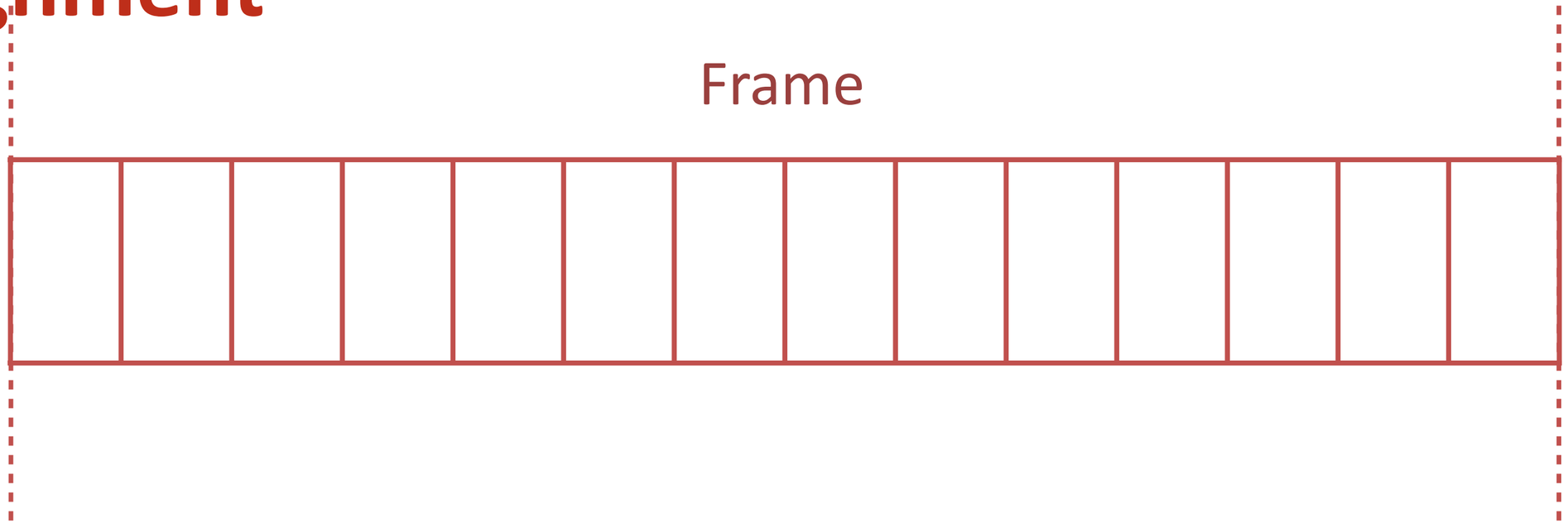
Alignment



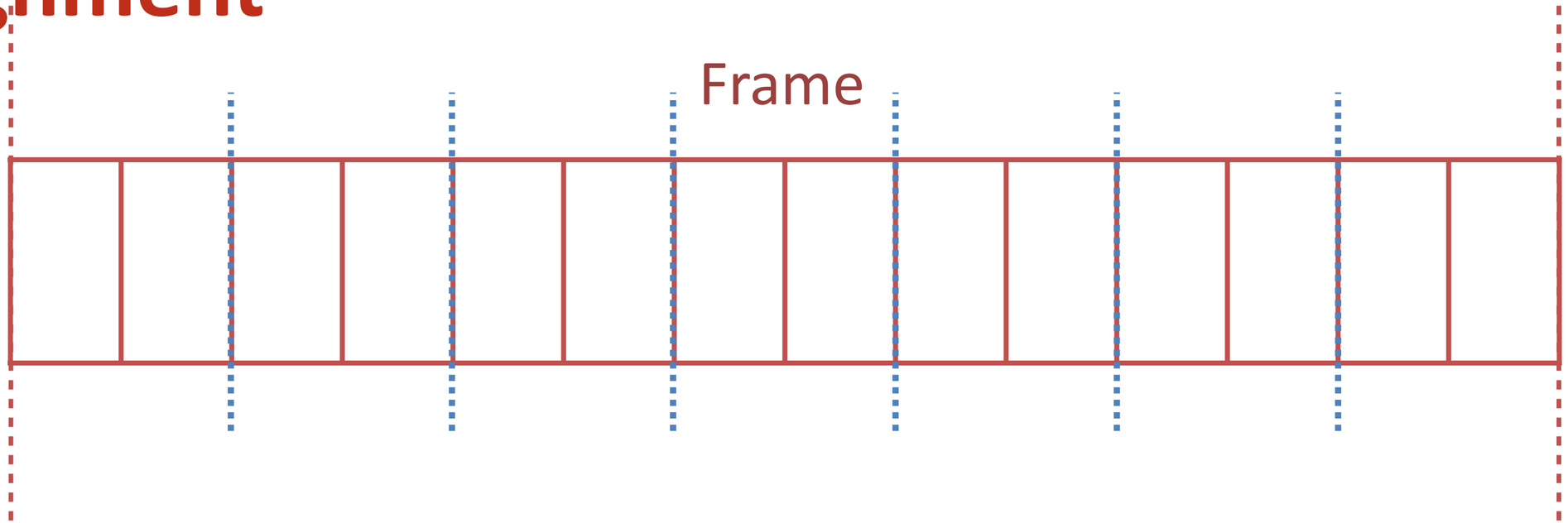
Alignment



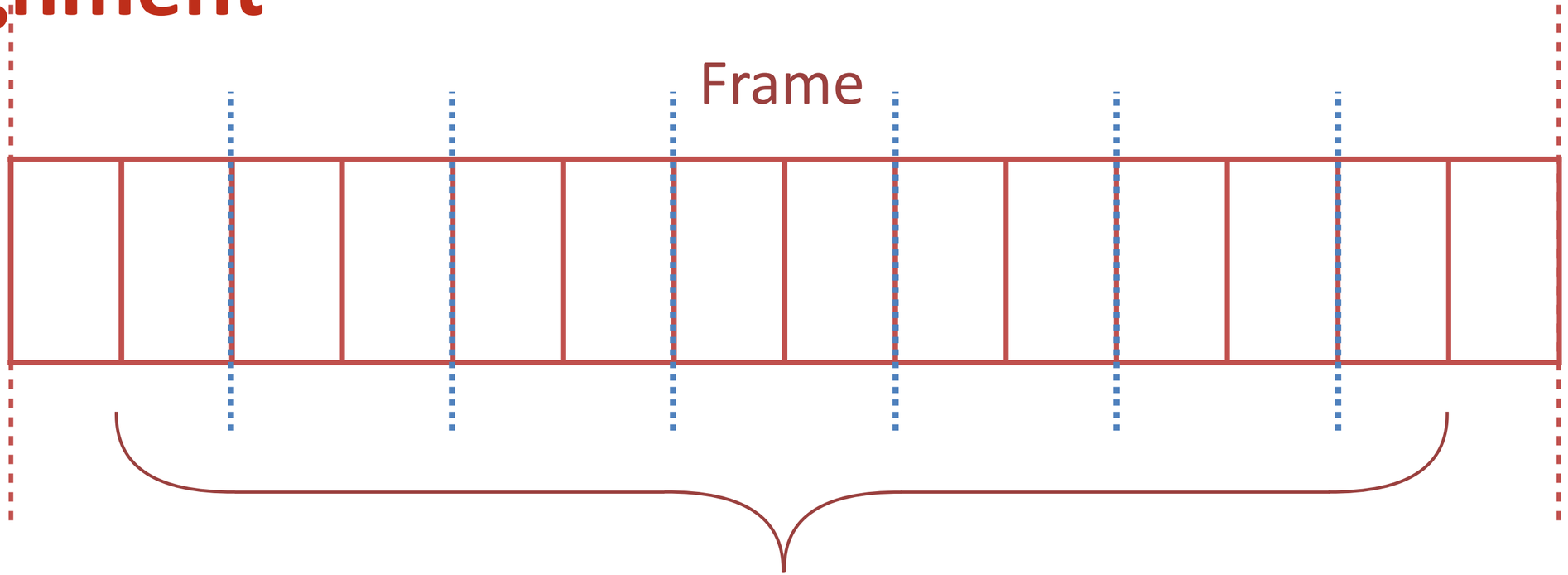
Alignment



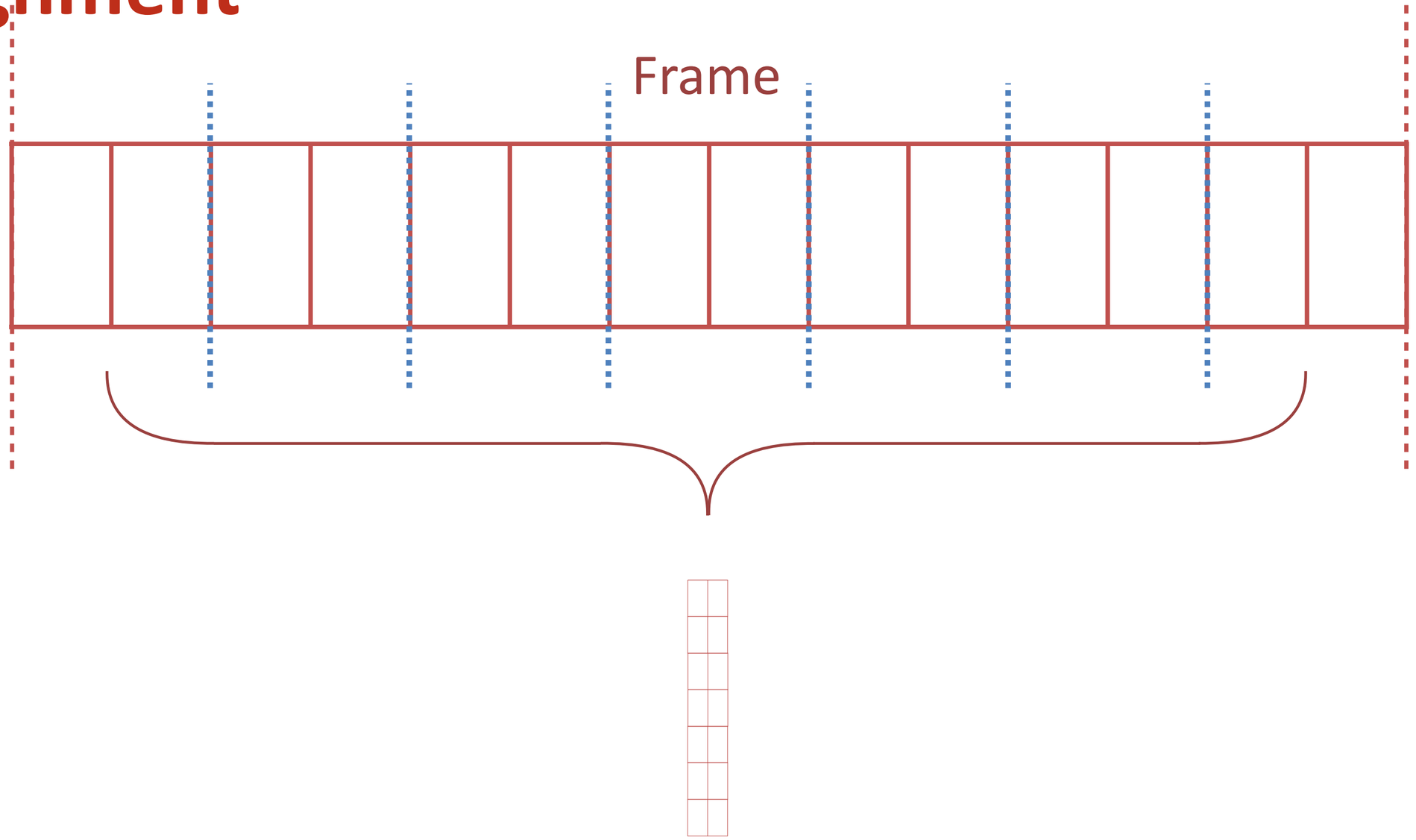
Alignment



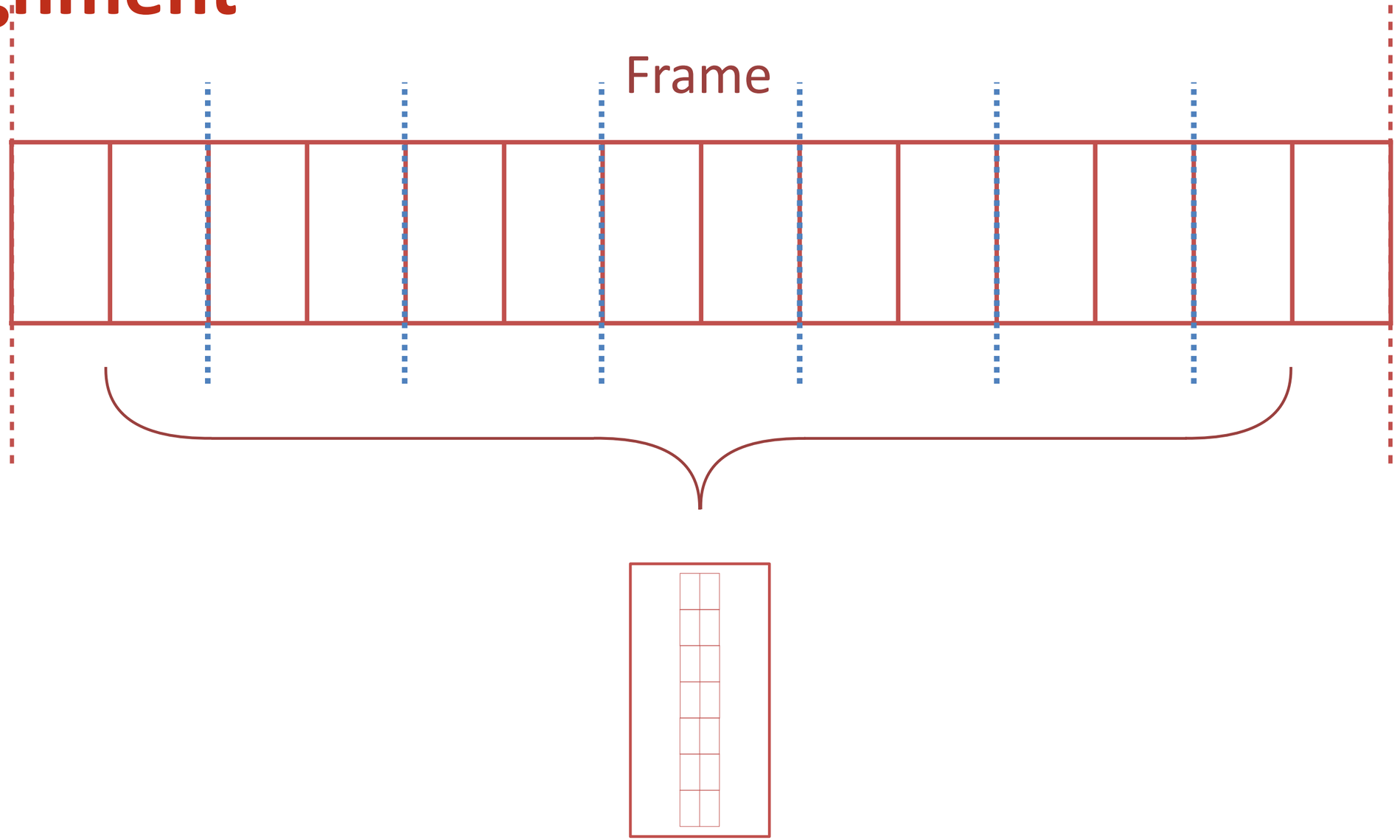
Alignment



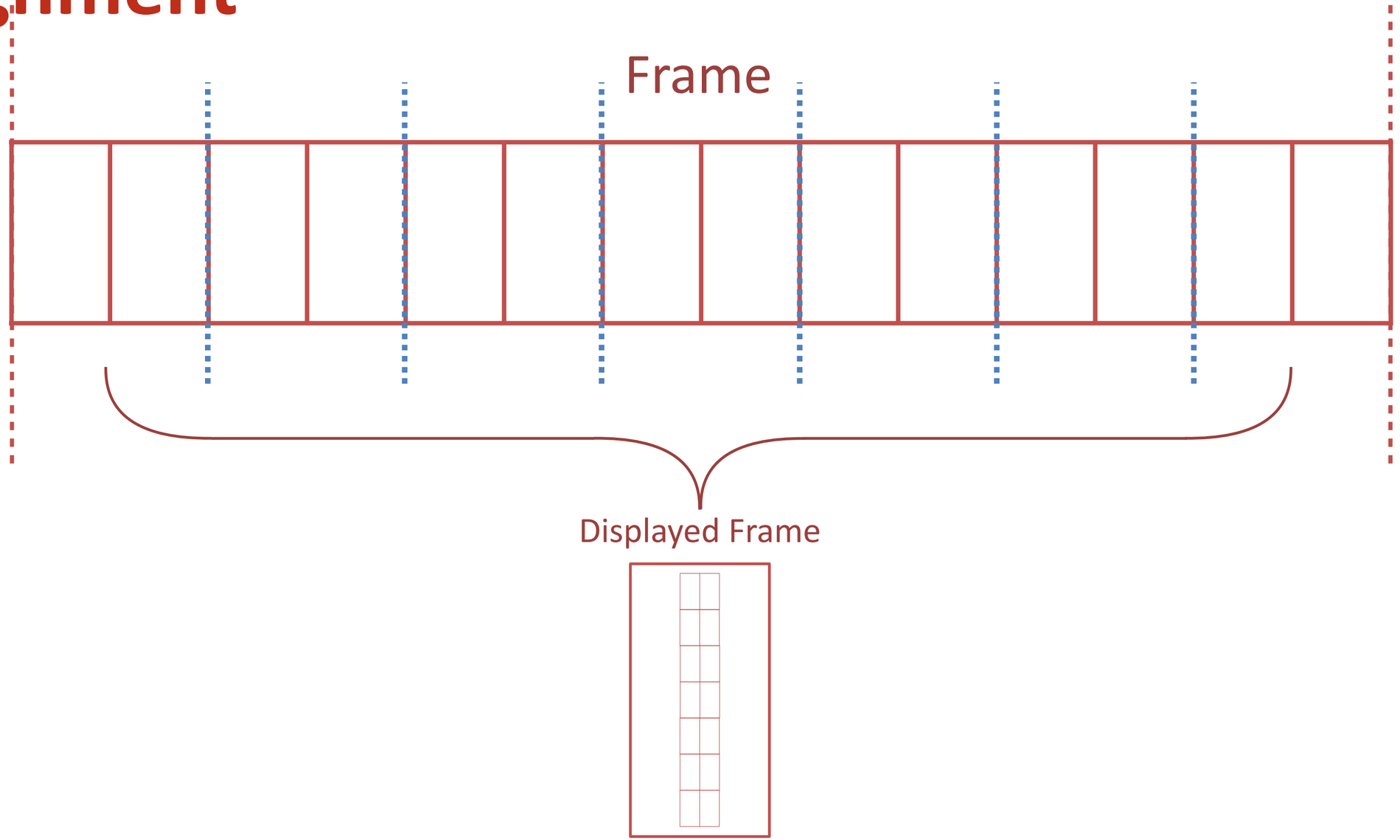
Alignment



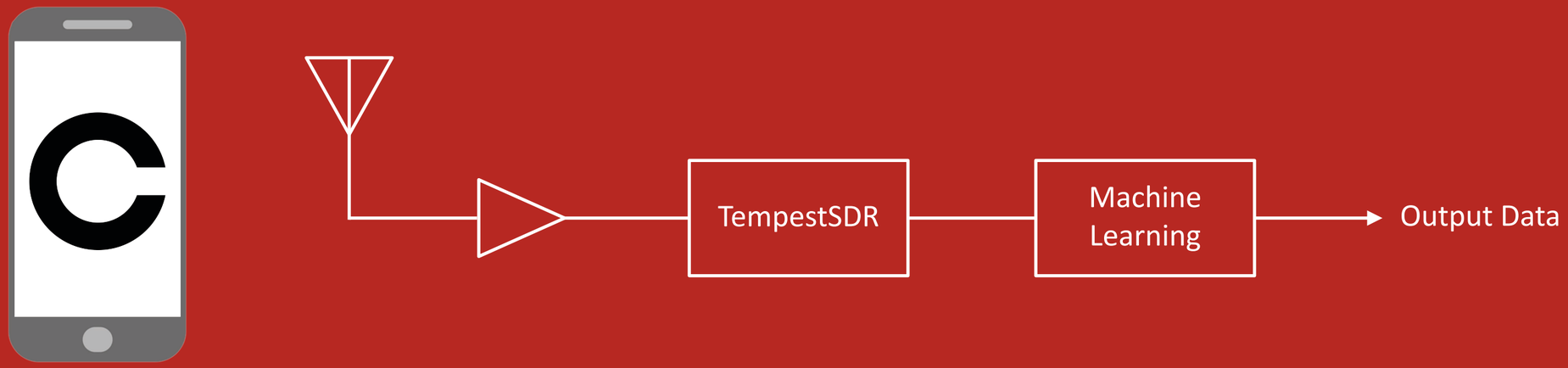
Alignment



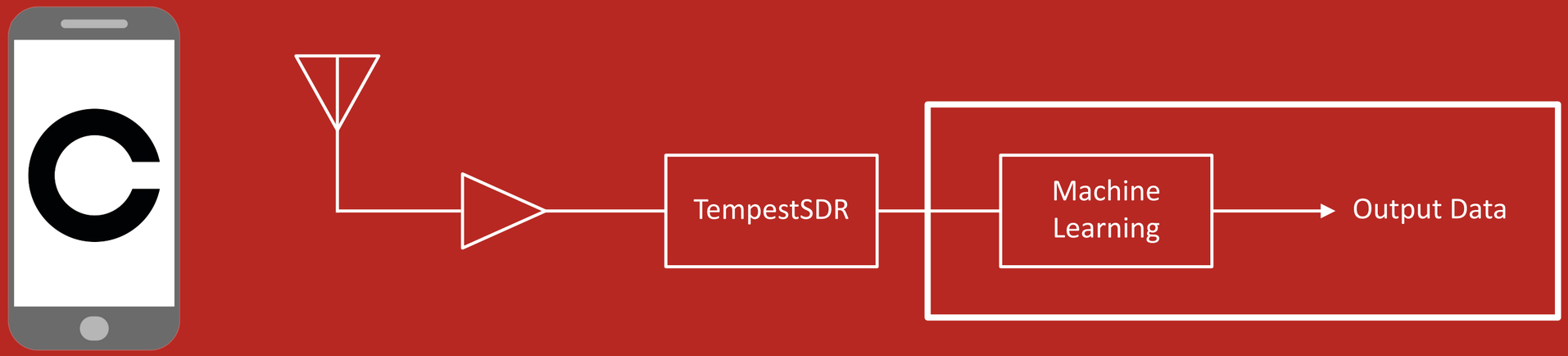
Alignment



Machine Learning

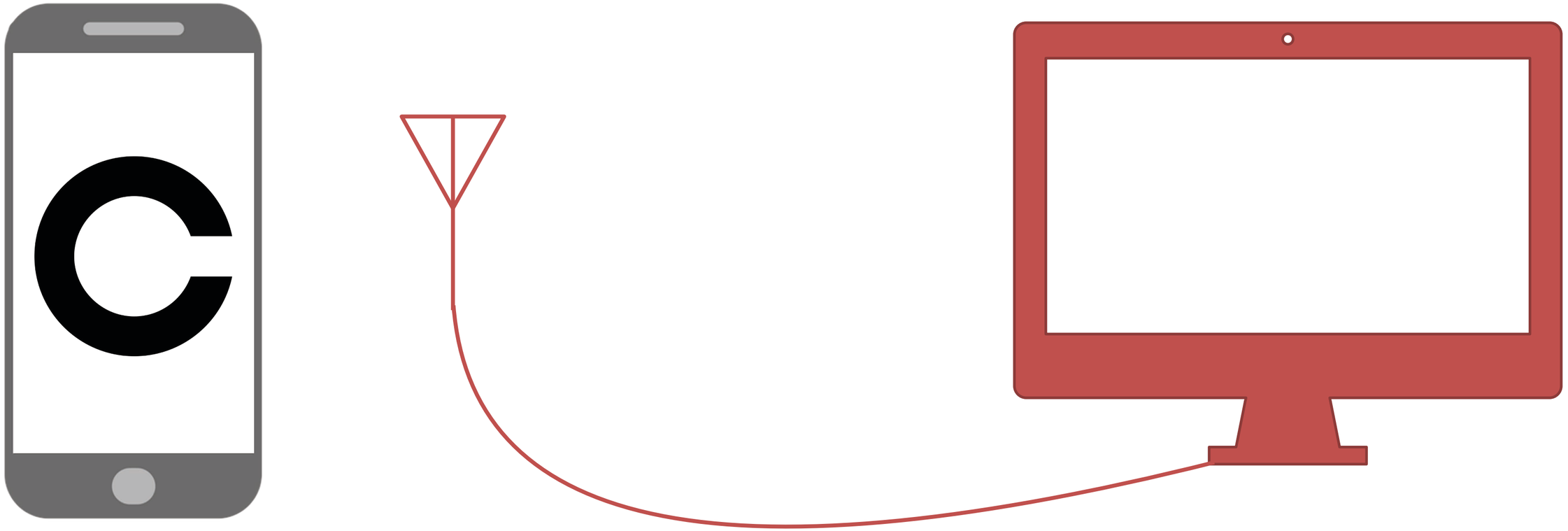


Machine Learning

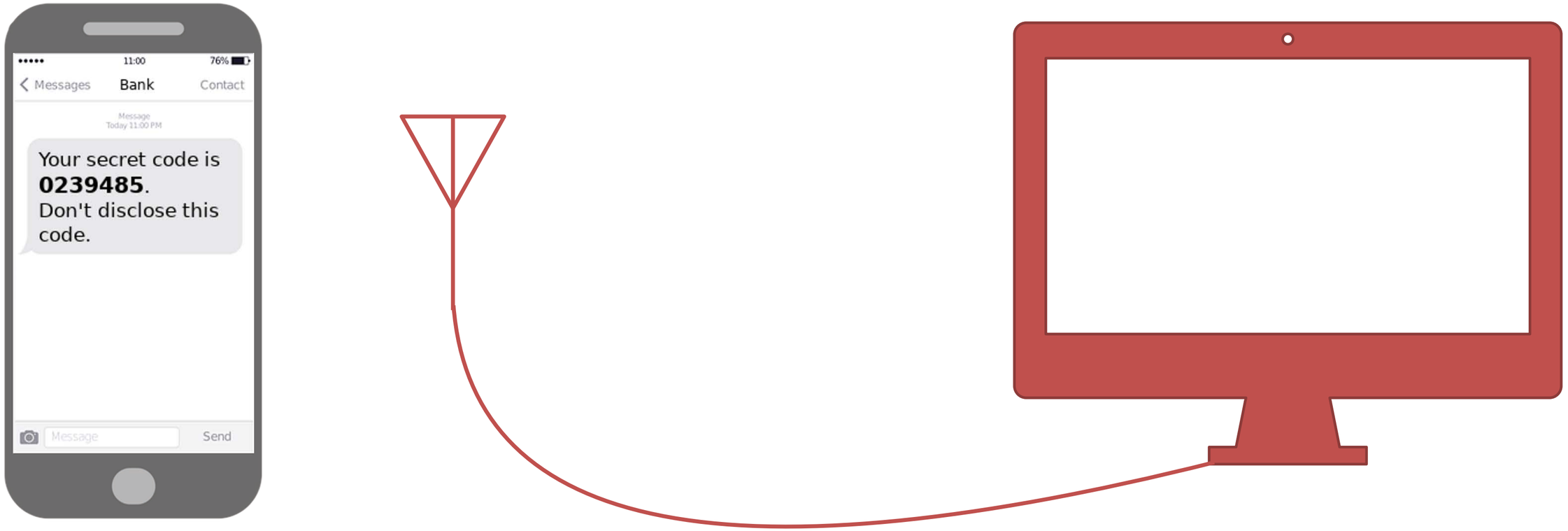


Use Cases

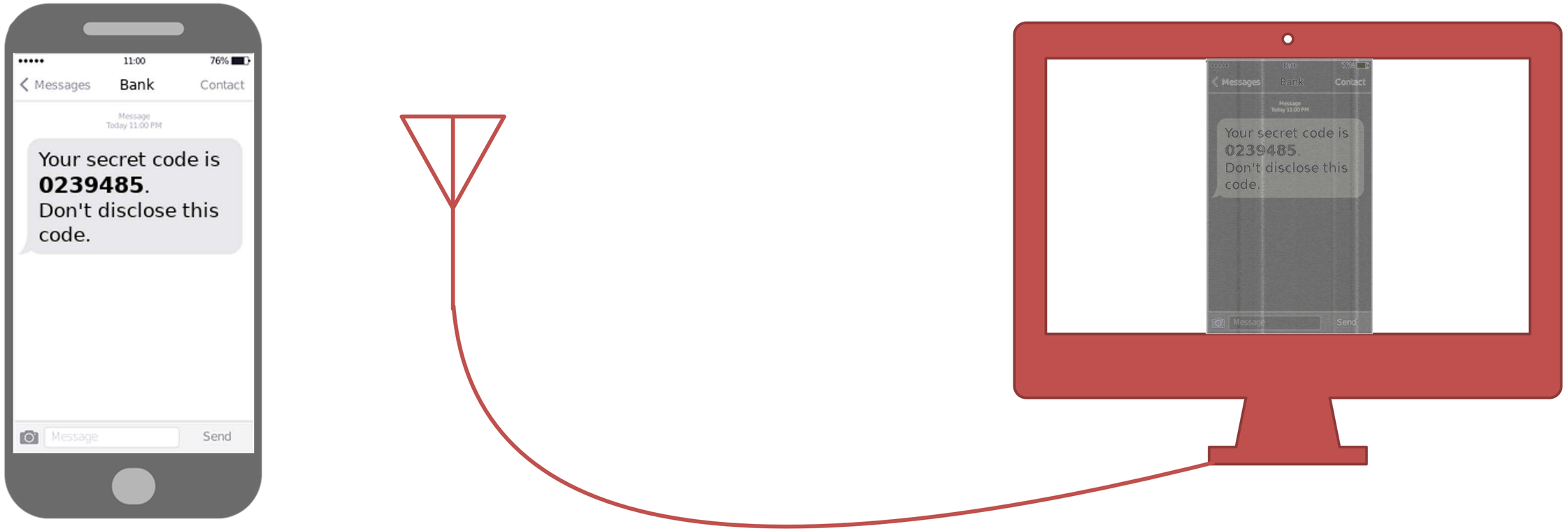
Use Cases



Use Cases

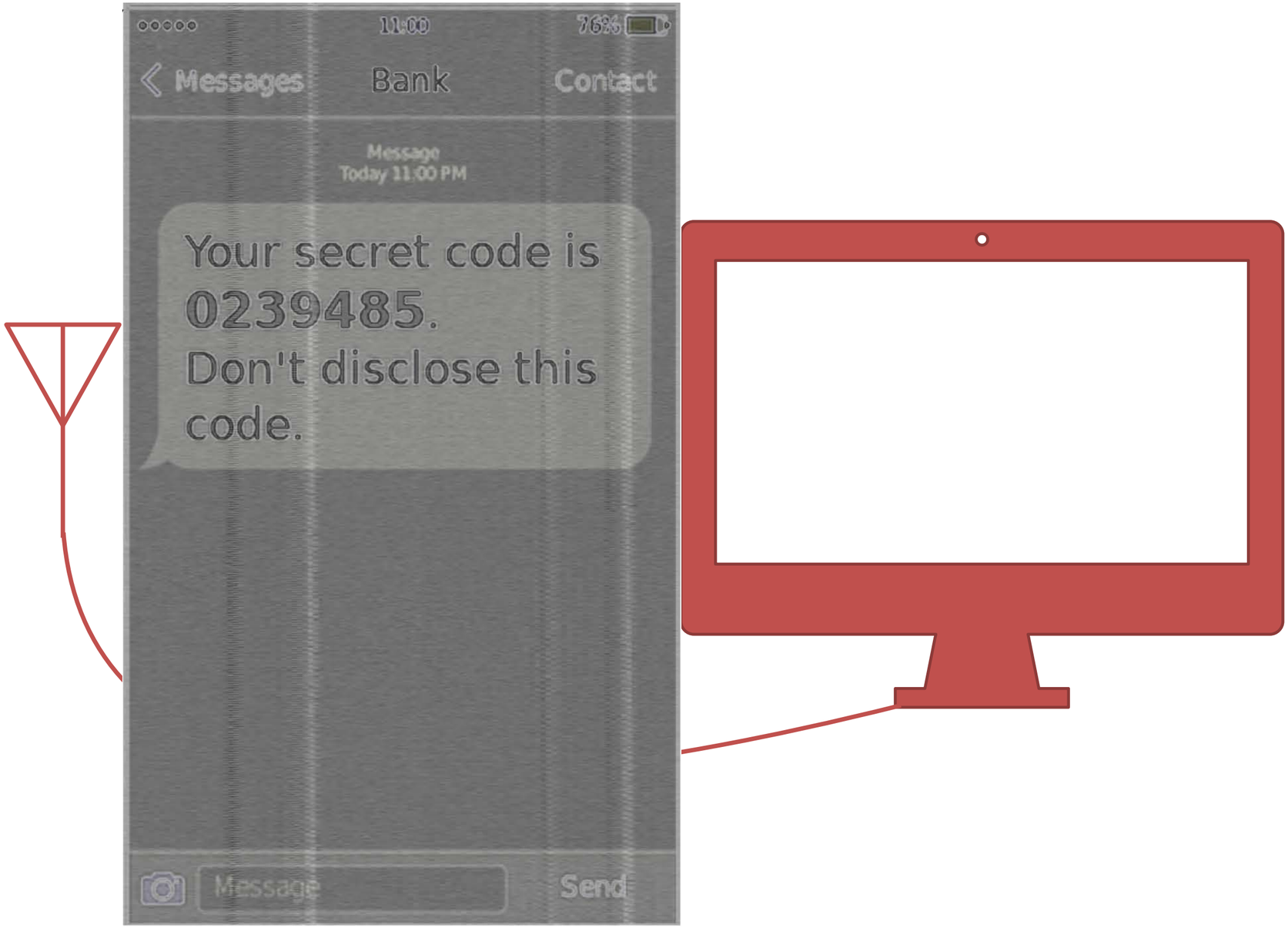

11:00
76%
Messages
Bank
Contact
Message
Today 11:00 PM
Your secret code is
0239485.
Don't disclose this
code.
Message
Send

Use Cases

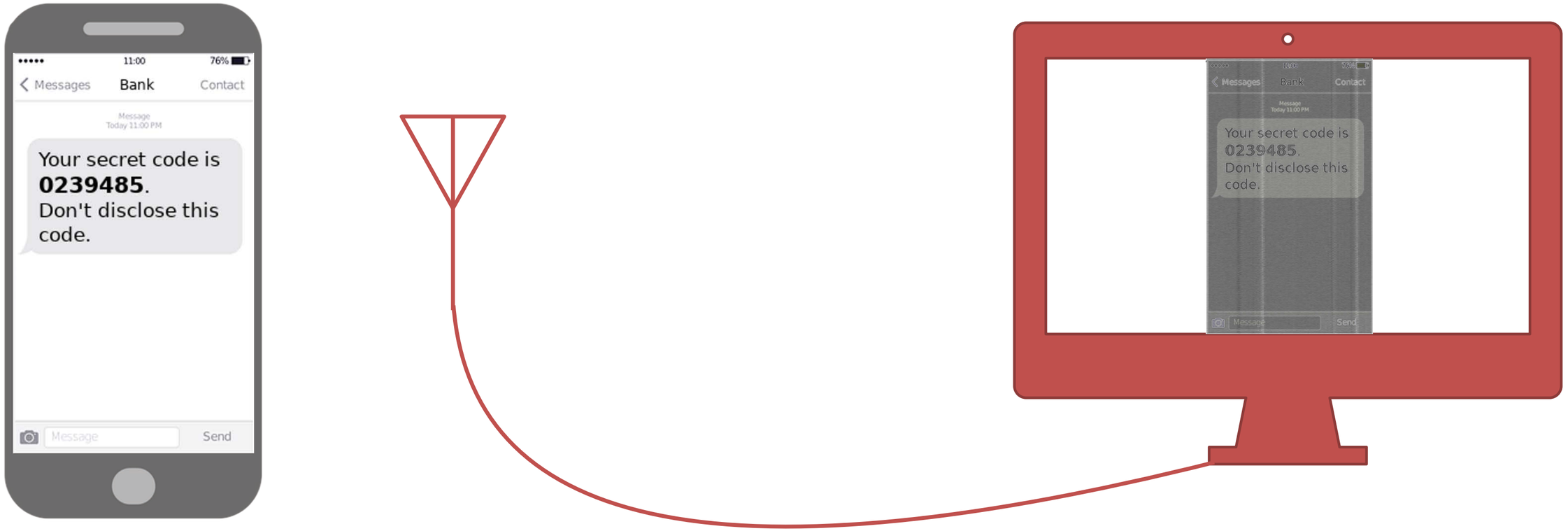

11:00
76%
Messages
Bank
Contact
Message
Today 11:00 PM
Your secret code is
0239485.
Don't disclose this
code.
Message
Send

Use Cases

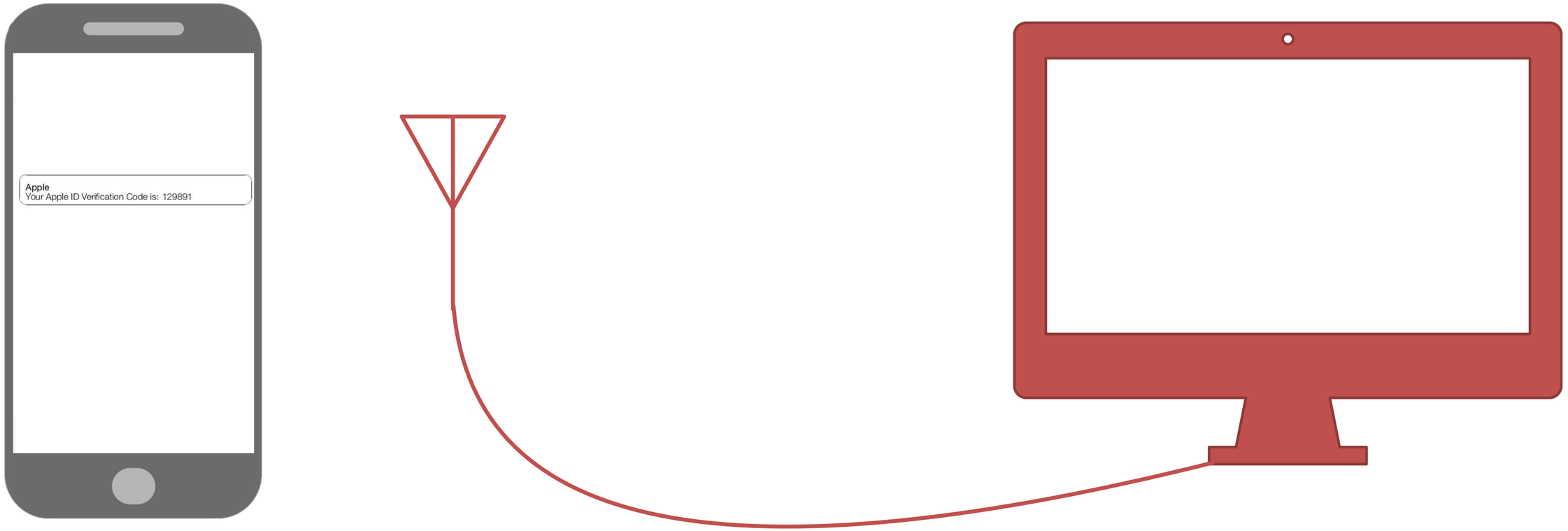

11:00
76%
Messages
Bank
Contact
Message
Today 11:00 PM
Your secret code is
0239485.
Don't disclose this
code.
Message
Send


11:00
76%
Messages
Bank
Contact
Message
Today 11:00 PM
Your secret code is
0239485.
Don't disclose this
code.
Message
Send

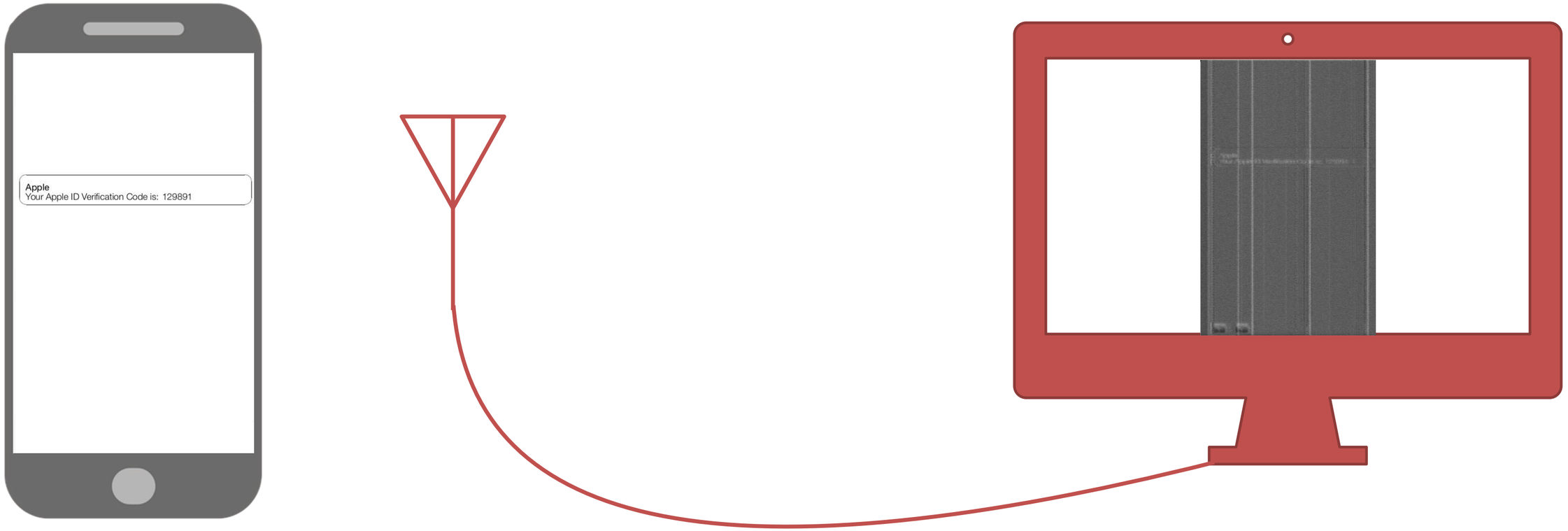
Use Cases


11:00
76%
Messages
Bank
Contact
Message
Today 11:00 PM
Your secret code is
0239485.
Don't disclose this
code.
Message
Send

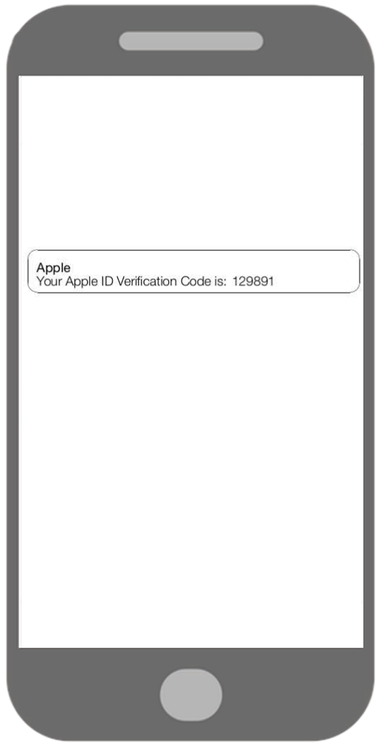
Use Cases

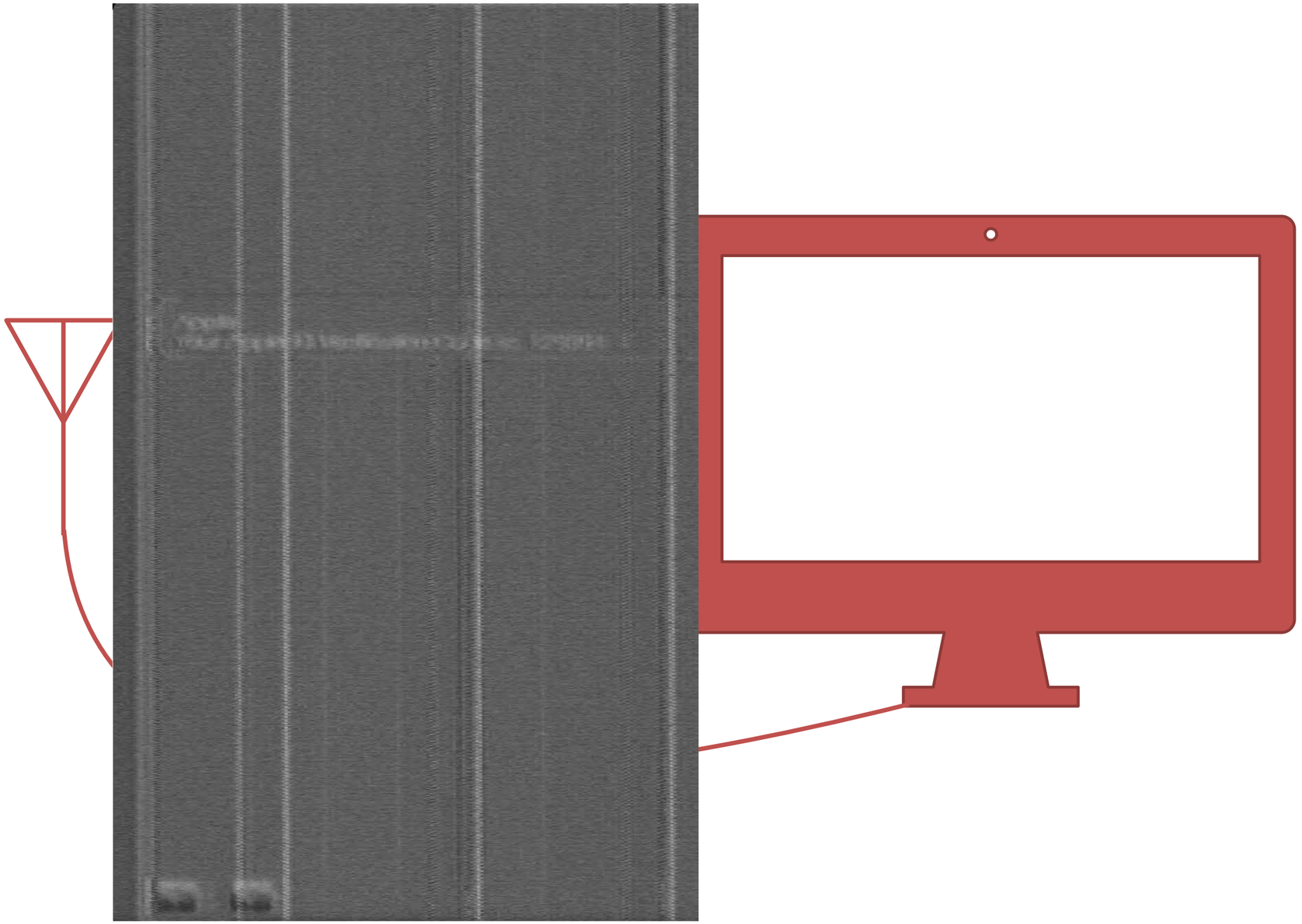


Use Cases



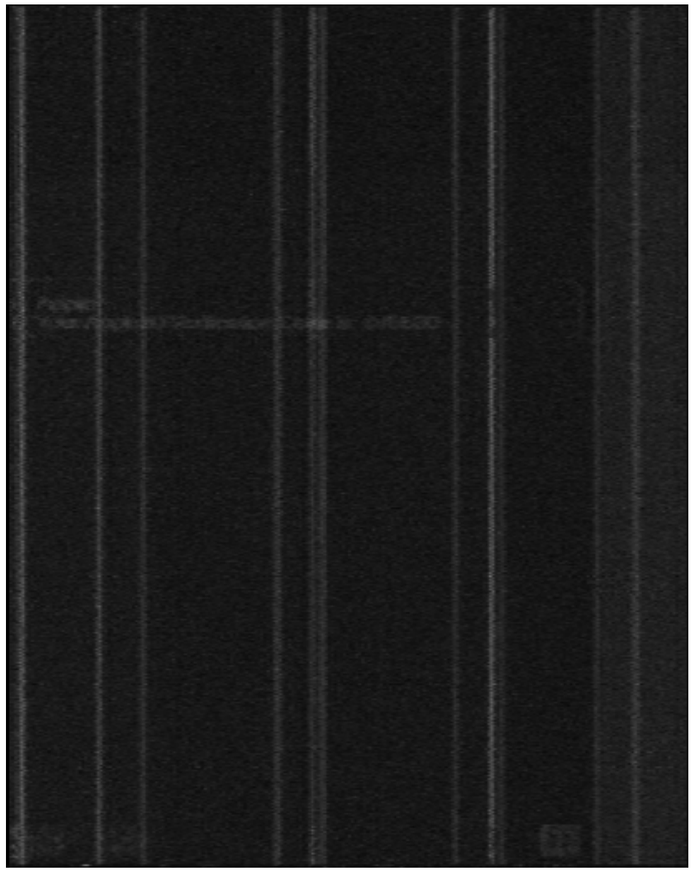
Use Cases



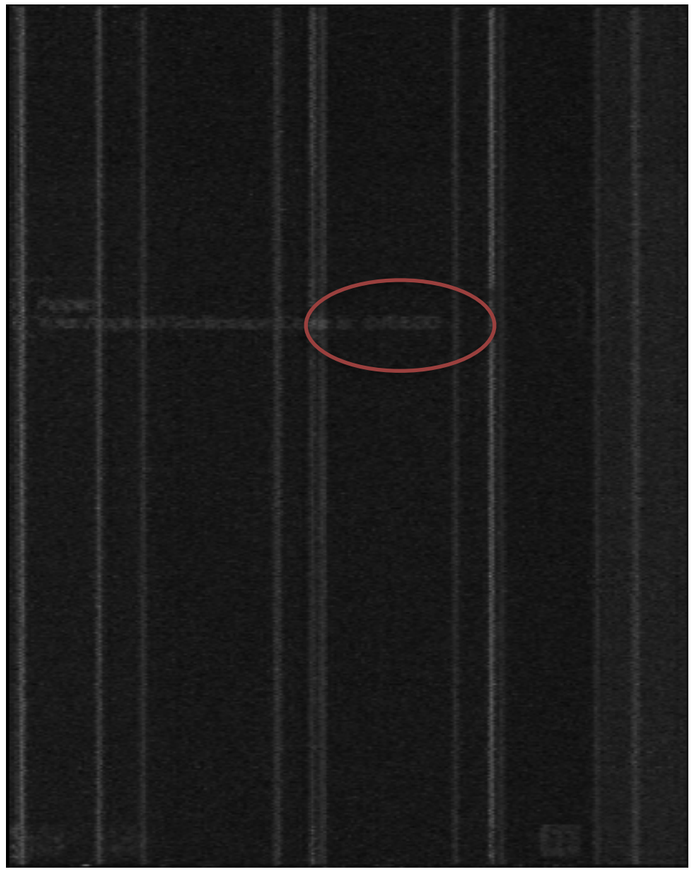


Finding the Security Code

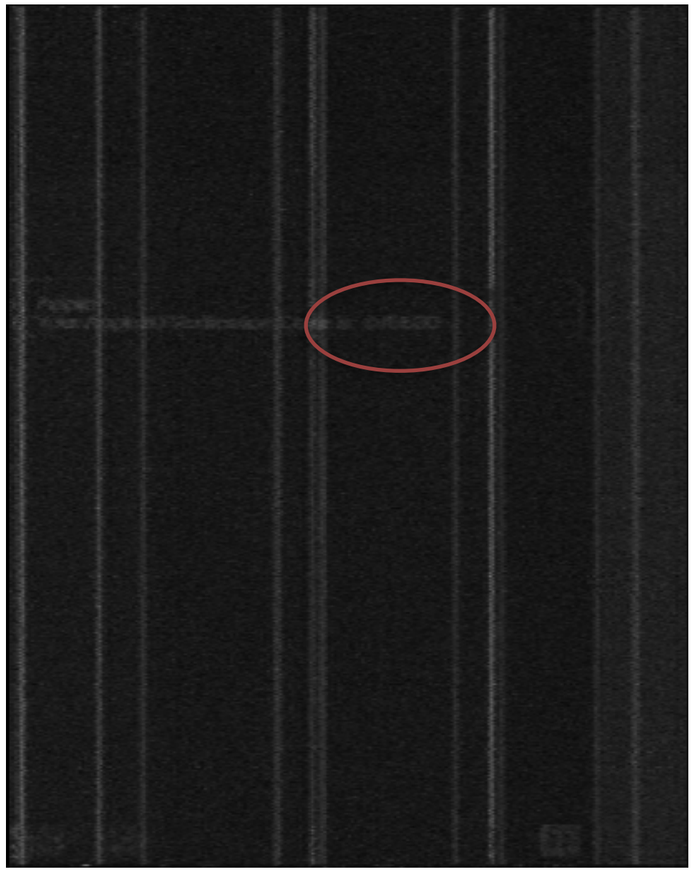
Finding the Security Code



Finding the Security Code

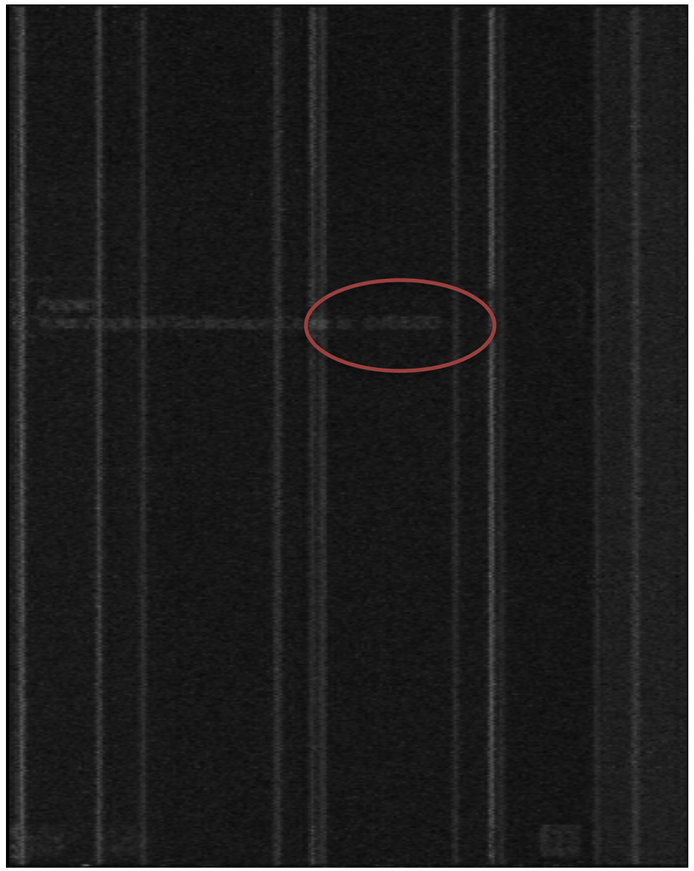


Finding the Security Code

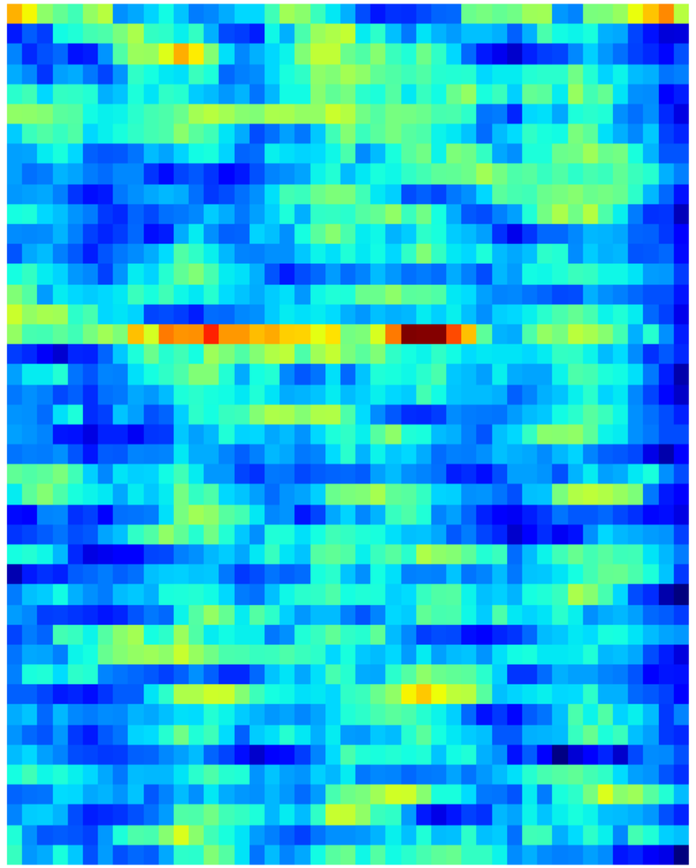


Sliding Window

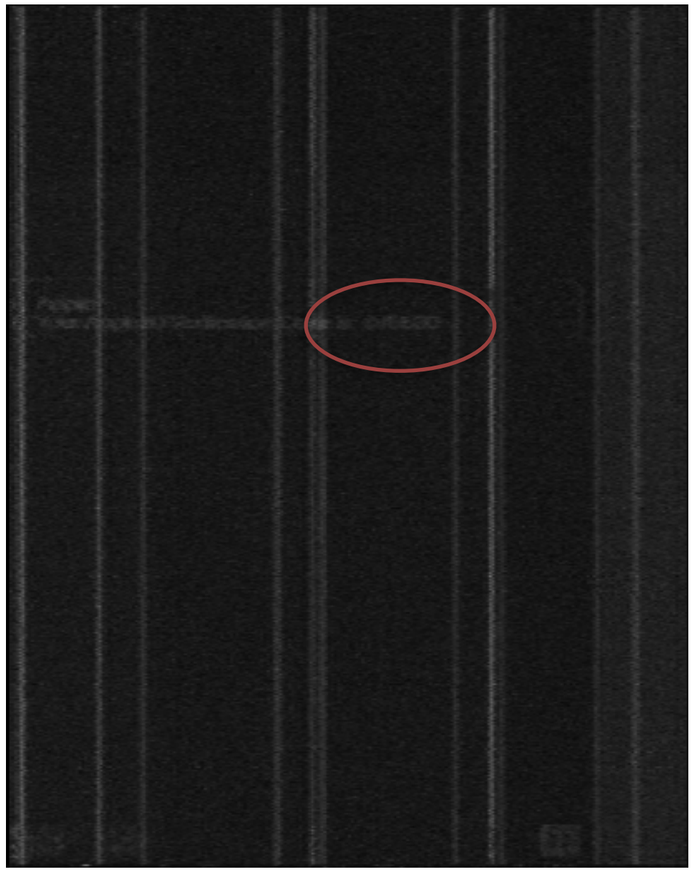
Finding the Security Code



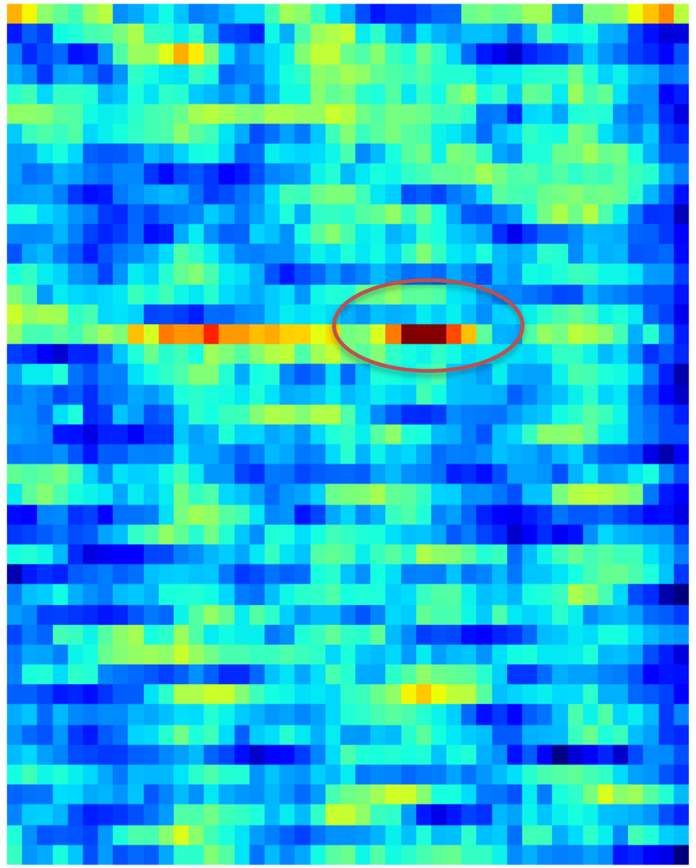
Sliding Window



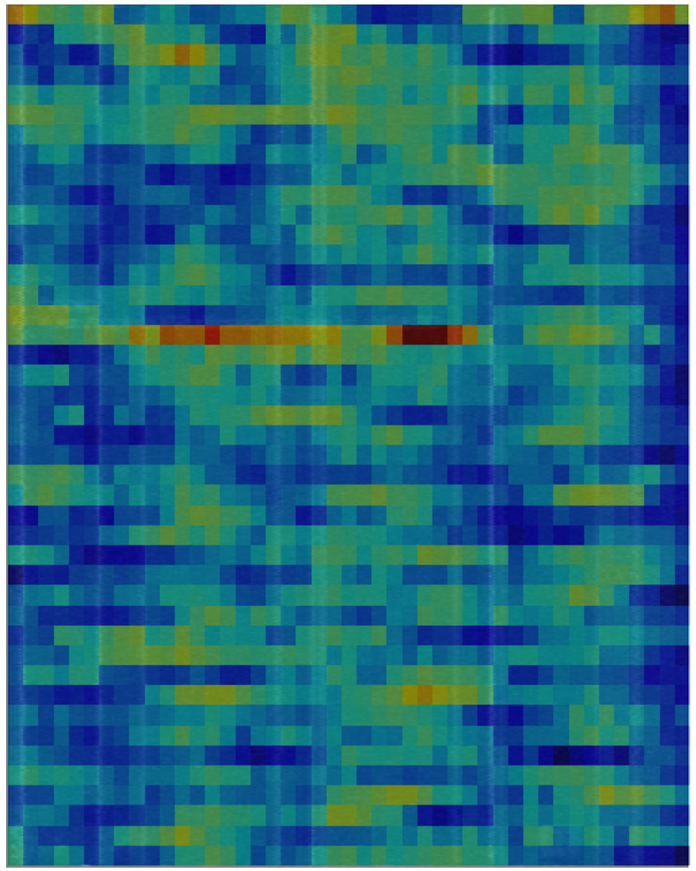
Finding the Security Code



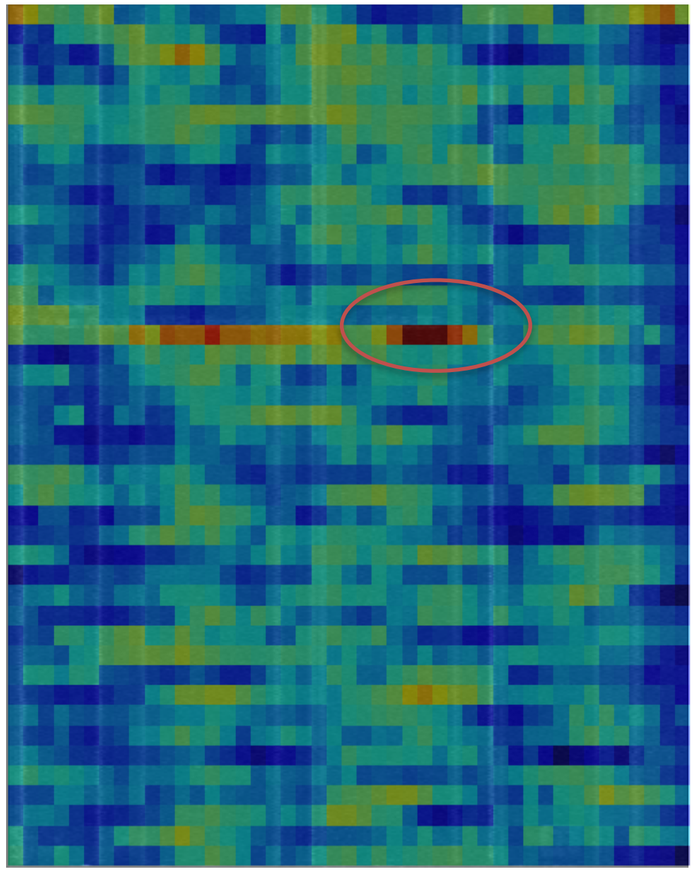
Sliding Window



Finding the Security Code

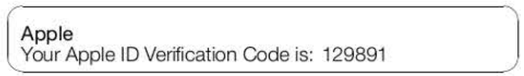


Finding the Security Code

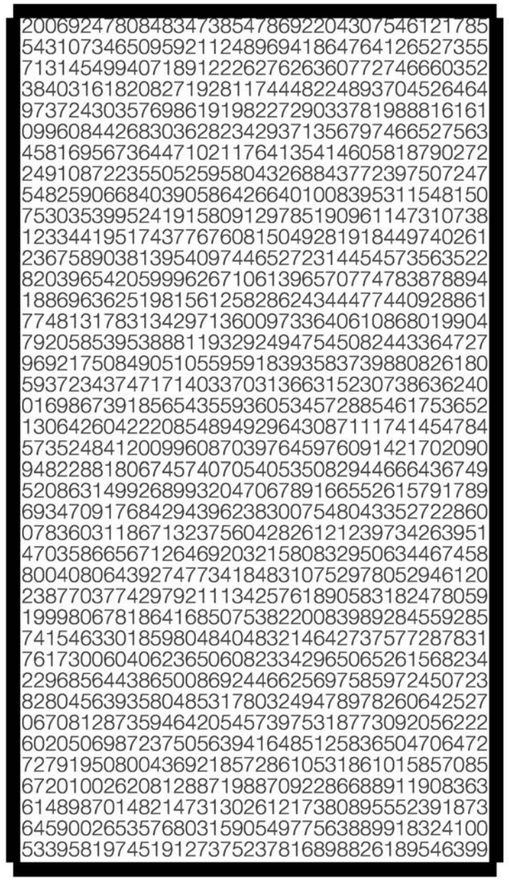


Obtaining Training Data

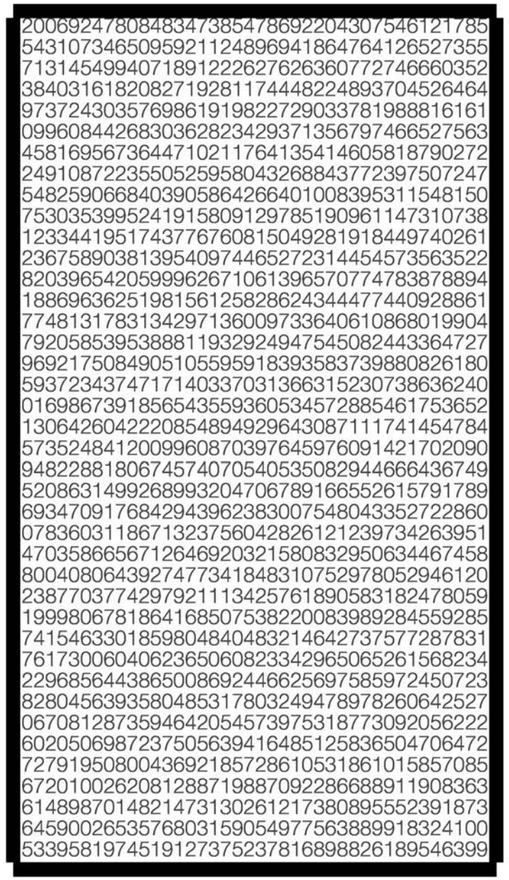
Obtaining Training Data

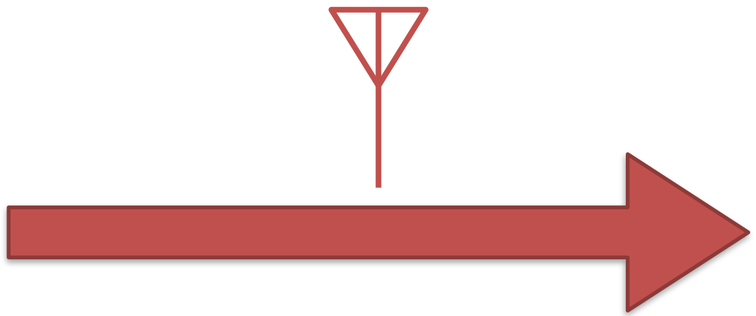


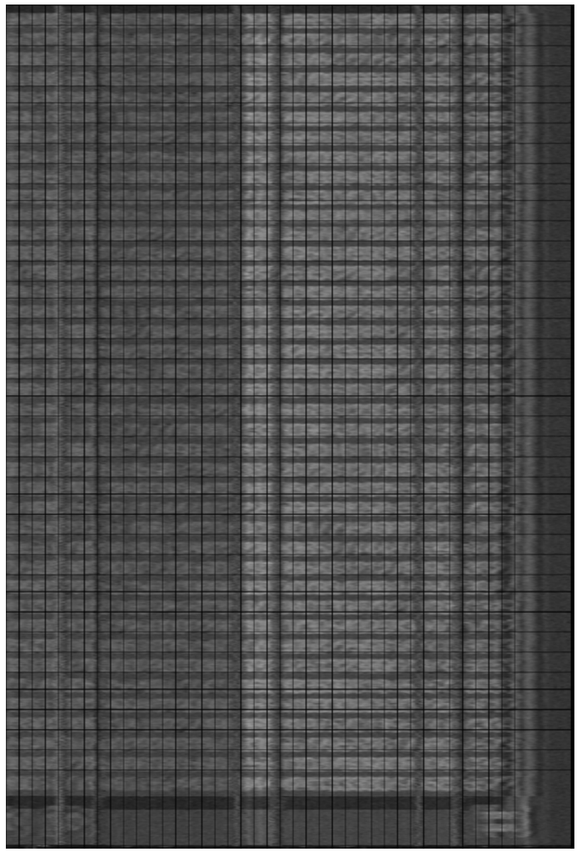
Obtaining Training Data



Obtaining Training Data

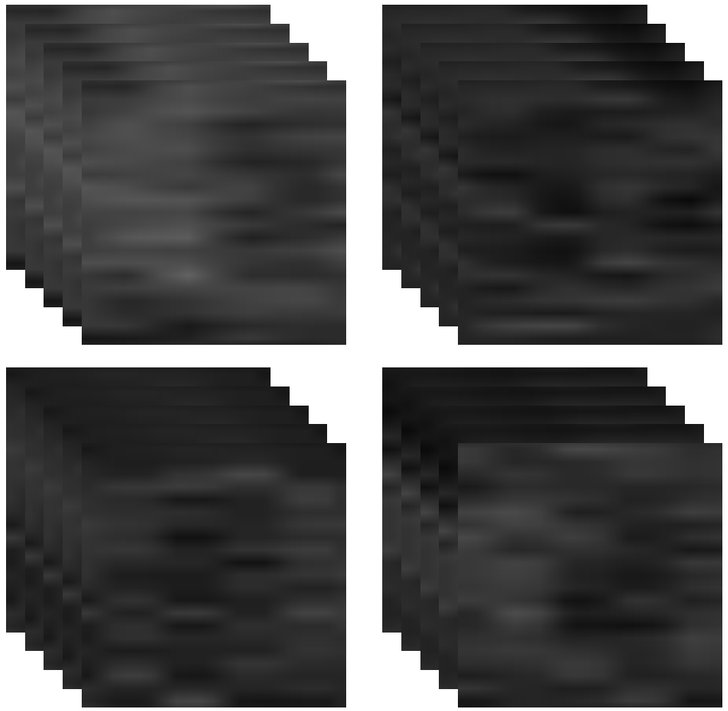






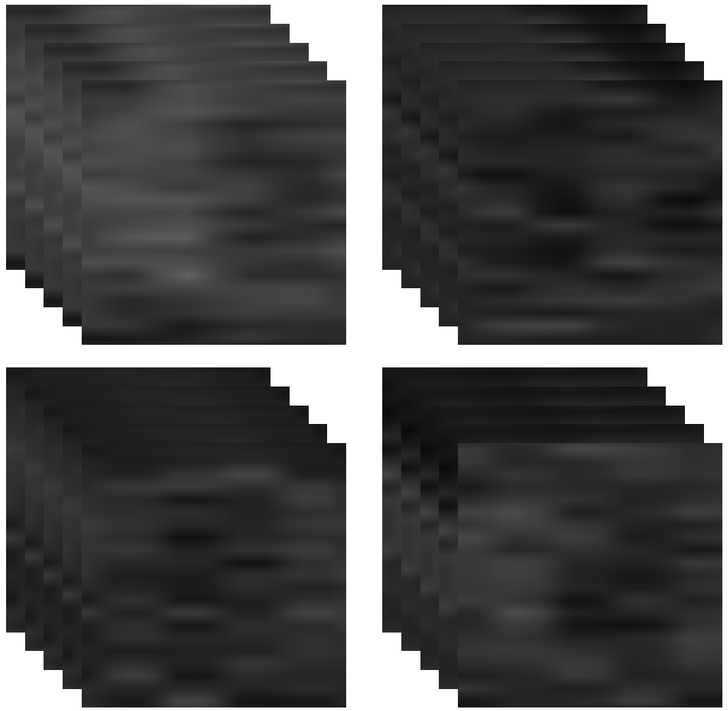
Machine Learning Training

Machine Learning Training



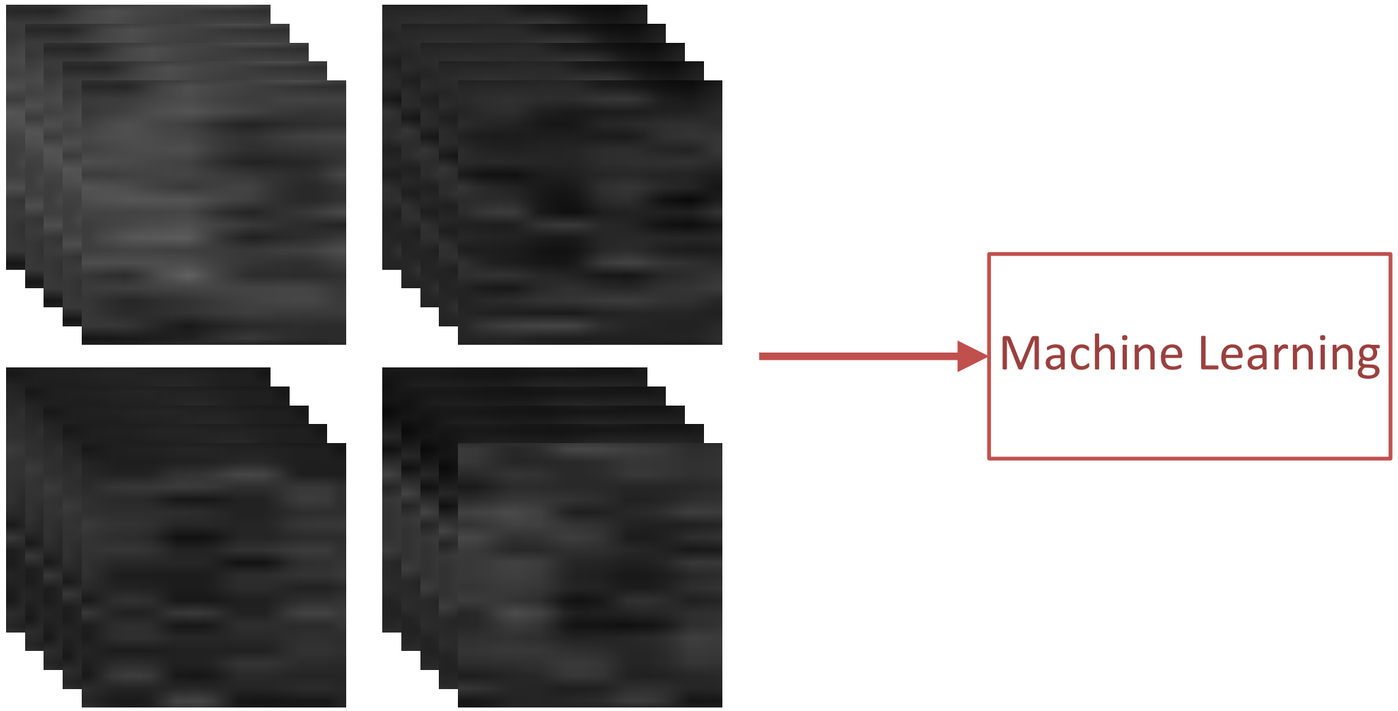
Machine Learning Training

“This is a digit 0”

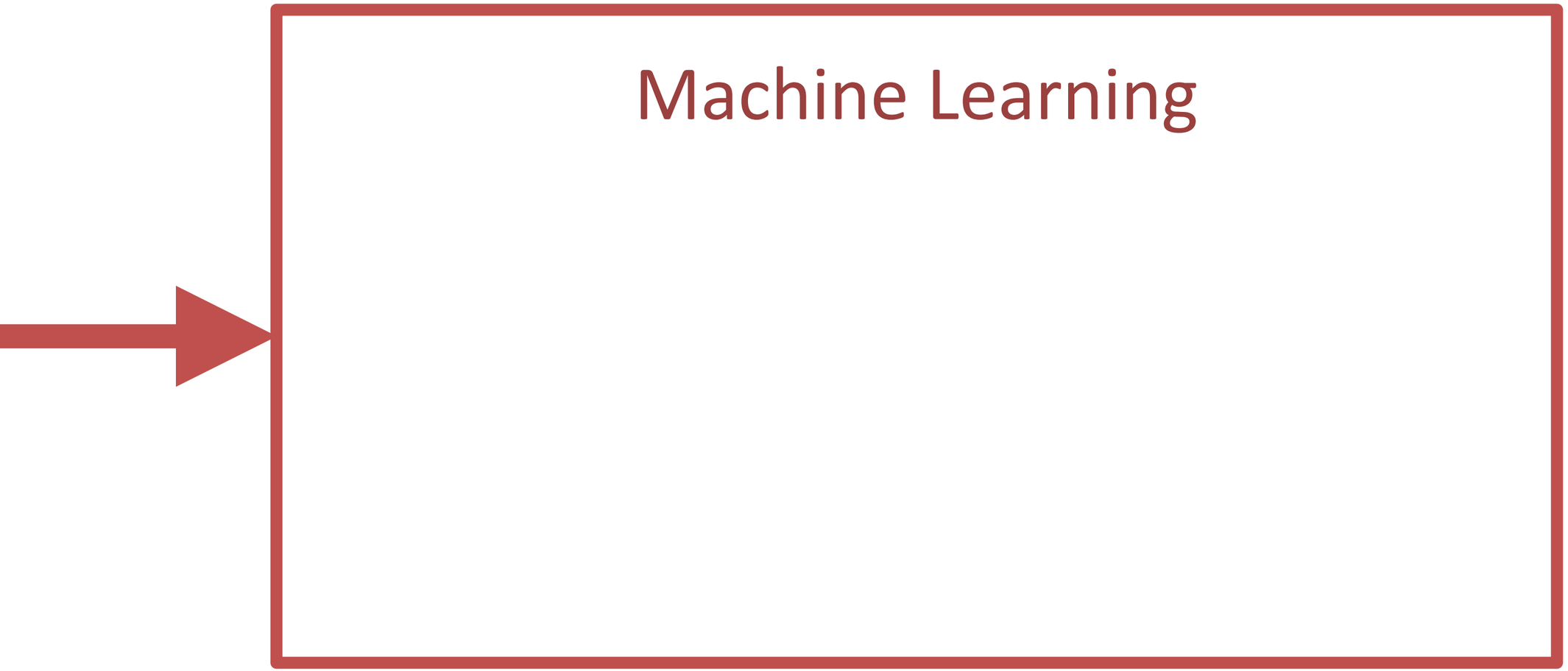


Machine Learning Training

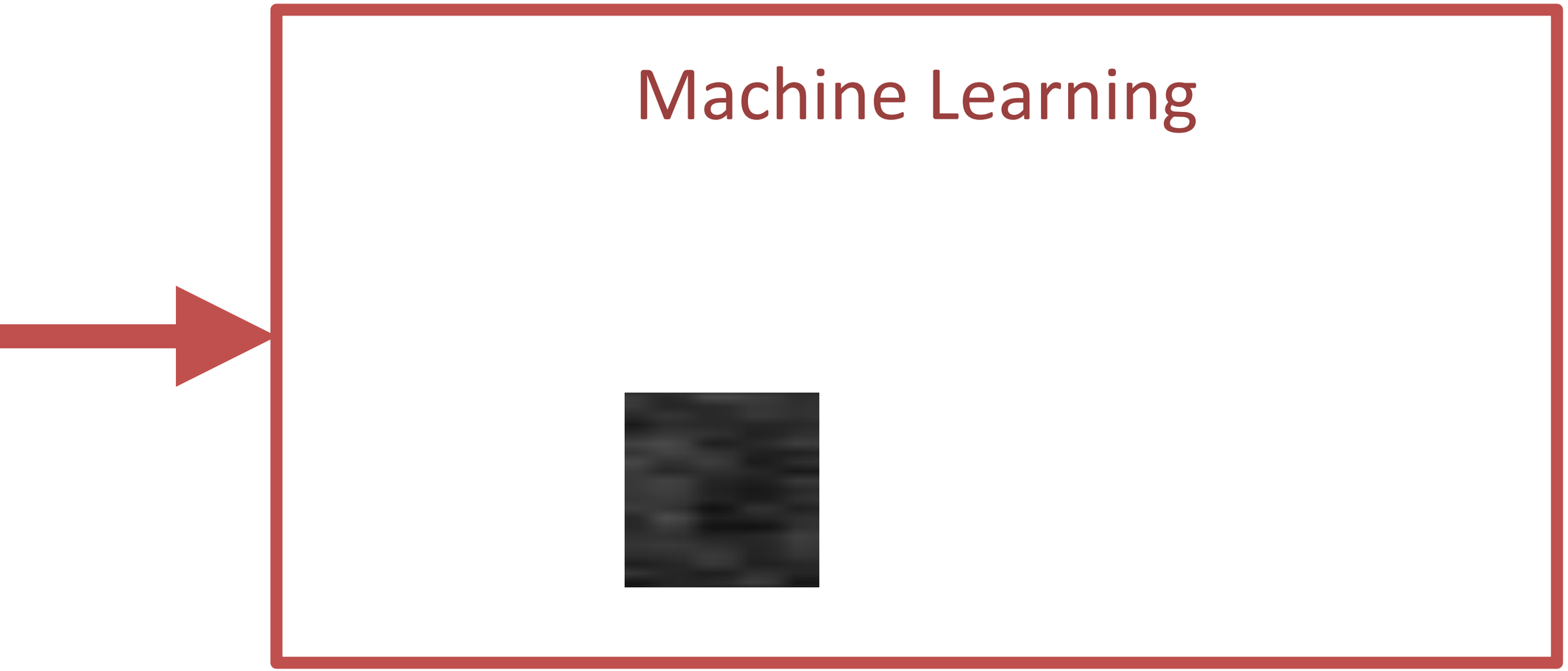
“This is a digit 0”



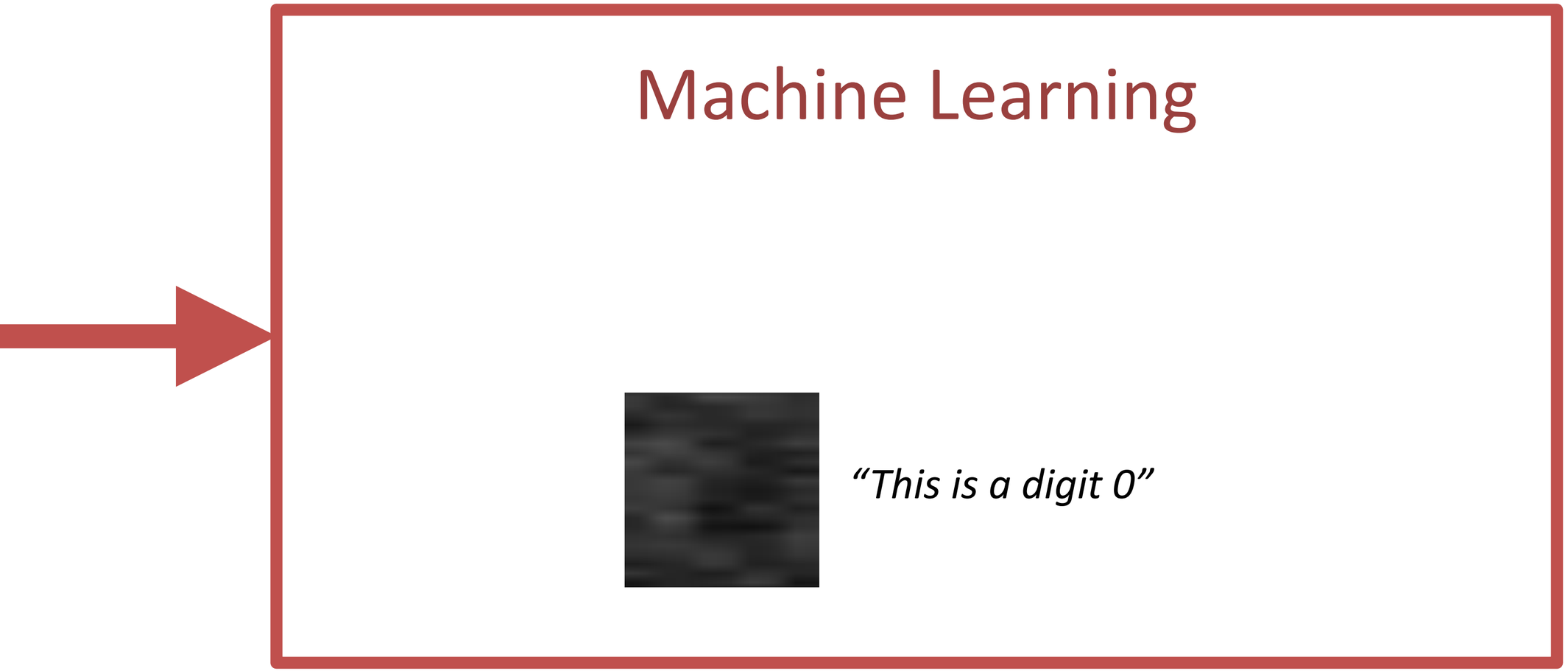
Machine Learning Training



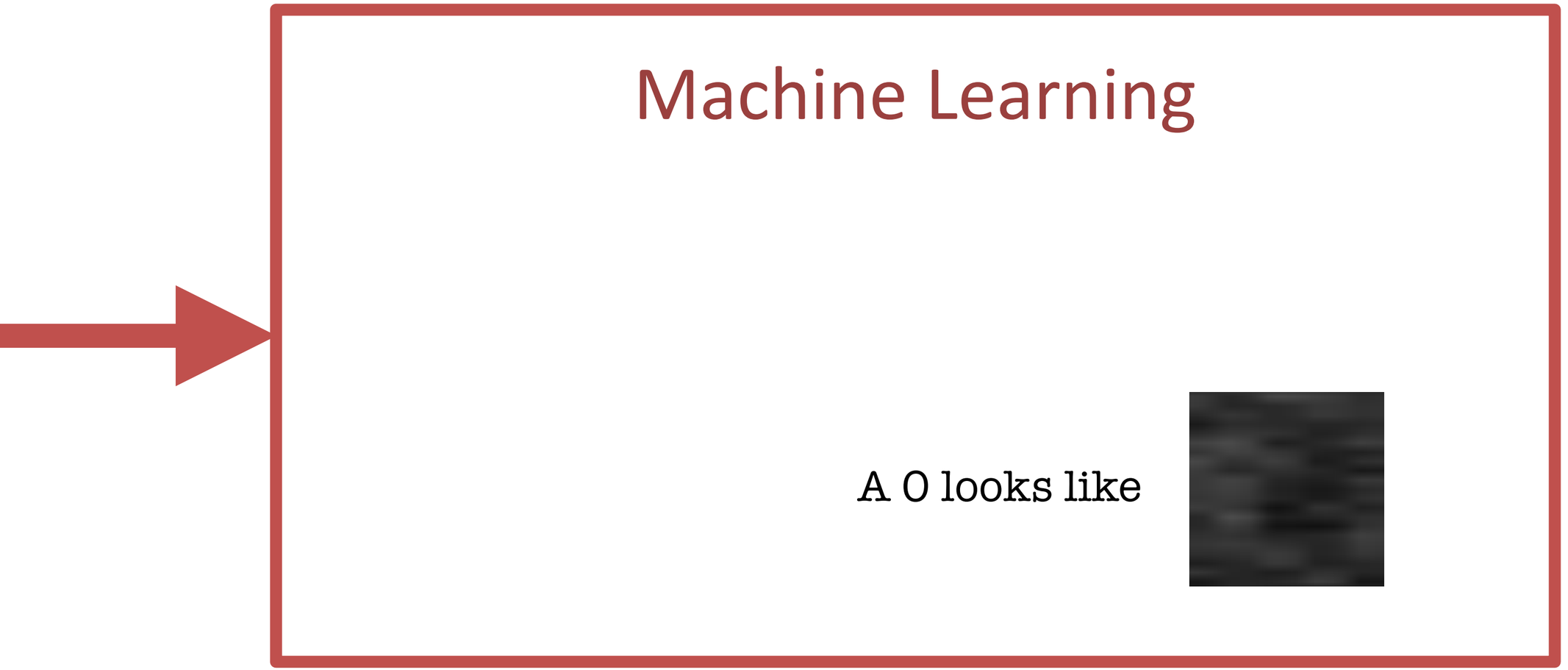
Machine Learning Training



Machine Learning Training

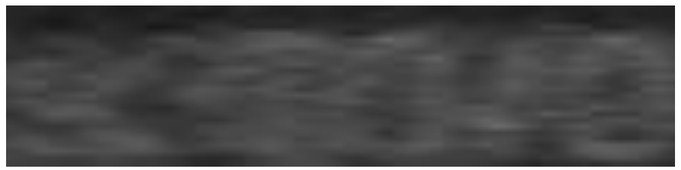


Machine Learning Training



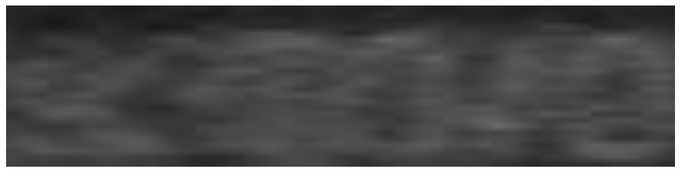
Machine Learning Classification

Machine Learning Classification



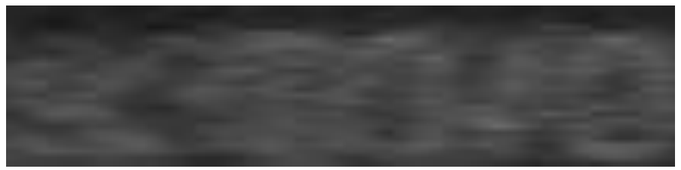
Machine Learning Classification

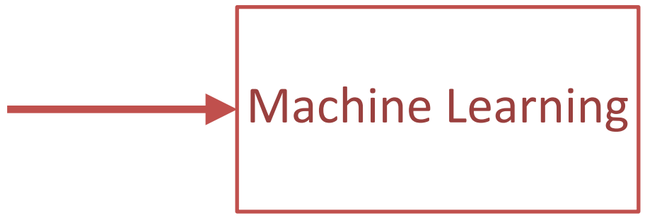
“What does this say?”



Machine Learning Classification

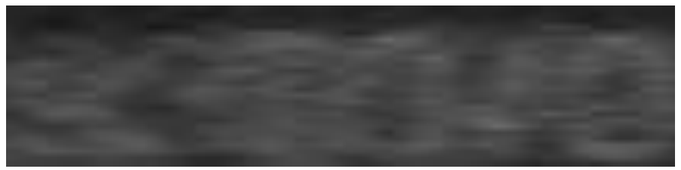
“What does this say?”





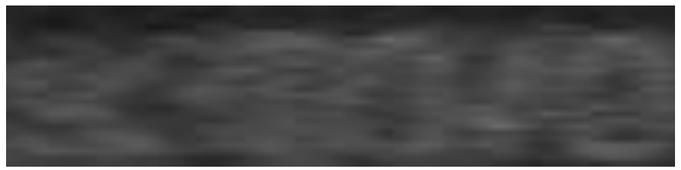
Machine Learning Classification

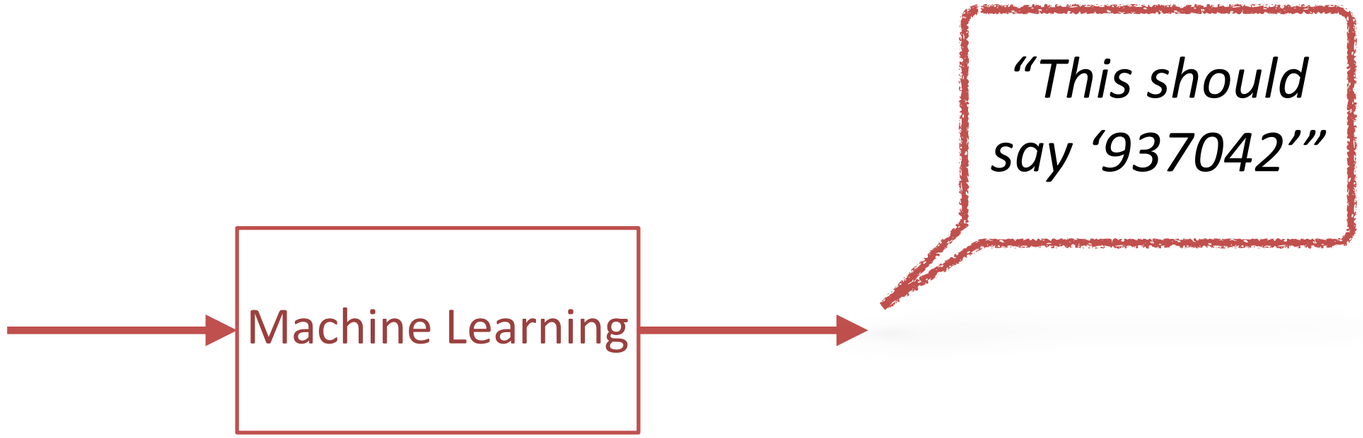
“What does this say?”



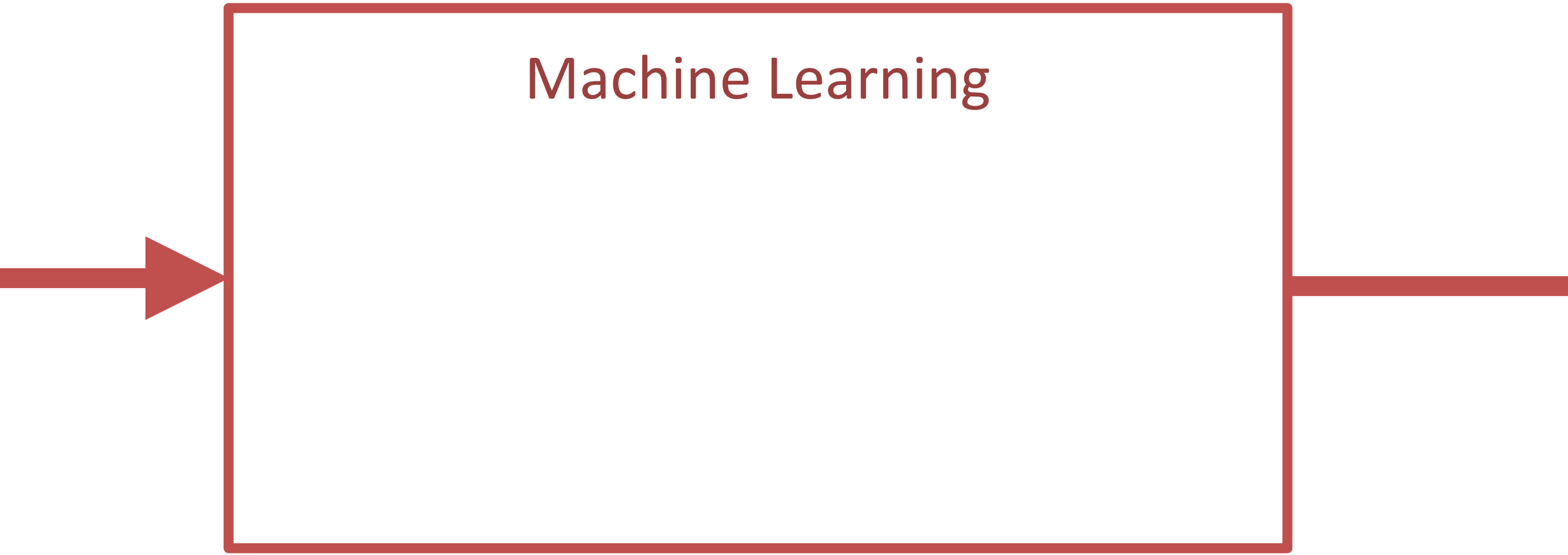
Machine Learning Classification

“What does this say?”

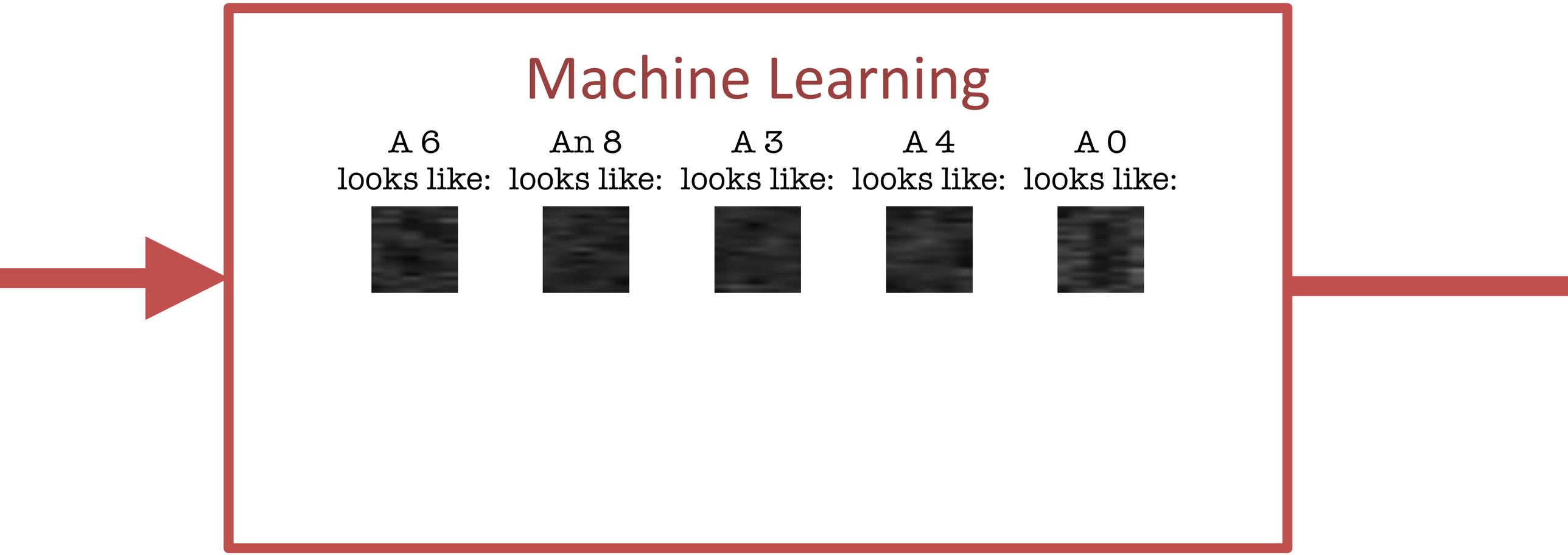




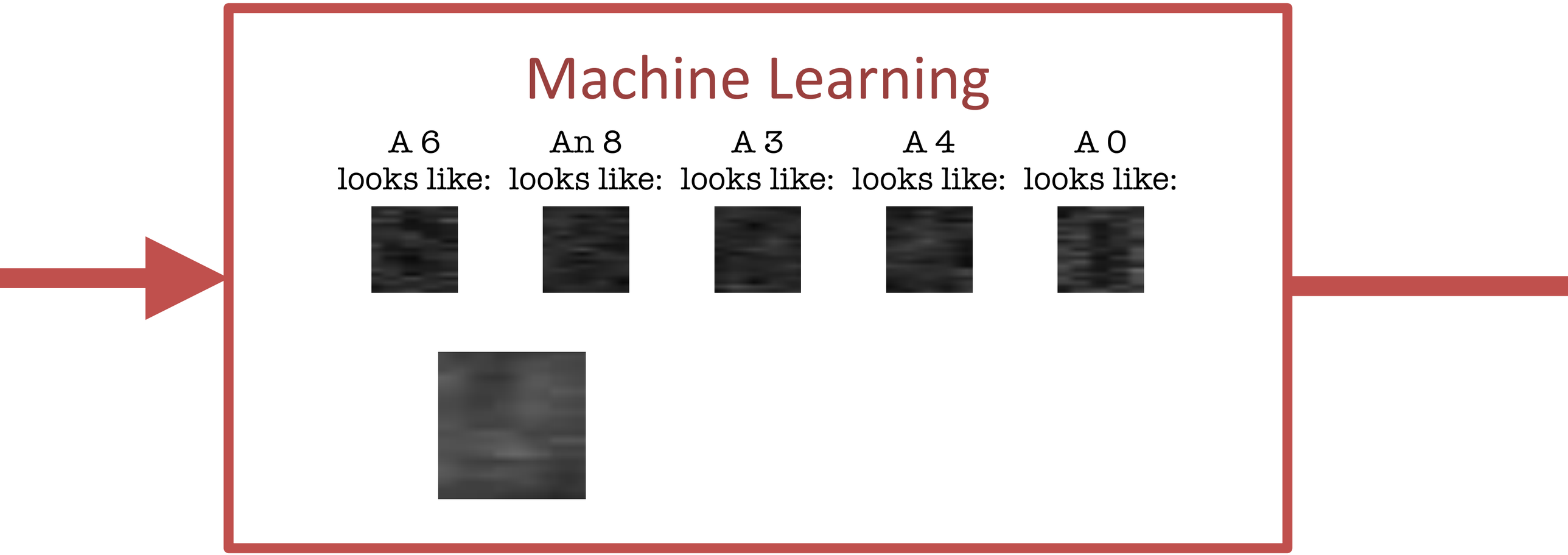
Machine Learning Classification



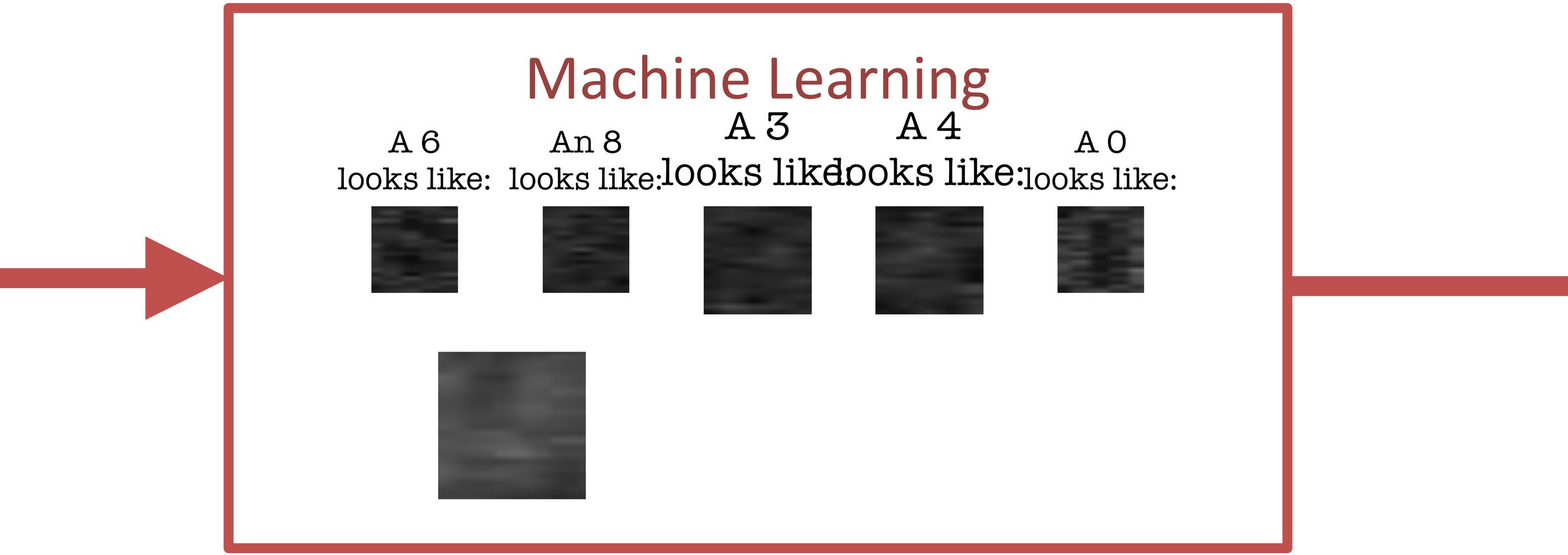
Machine Learning Classification



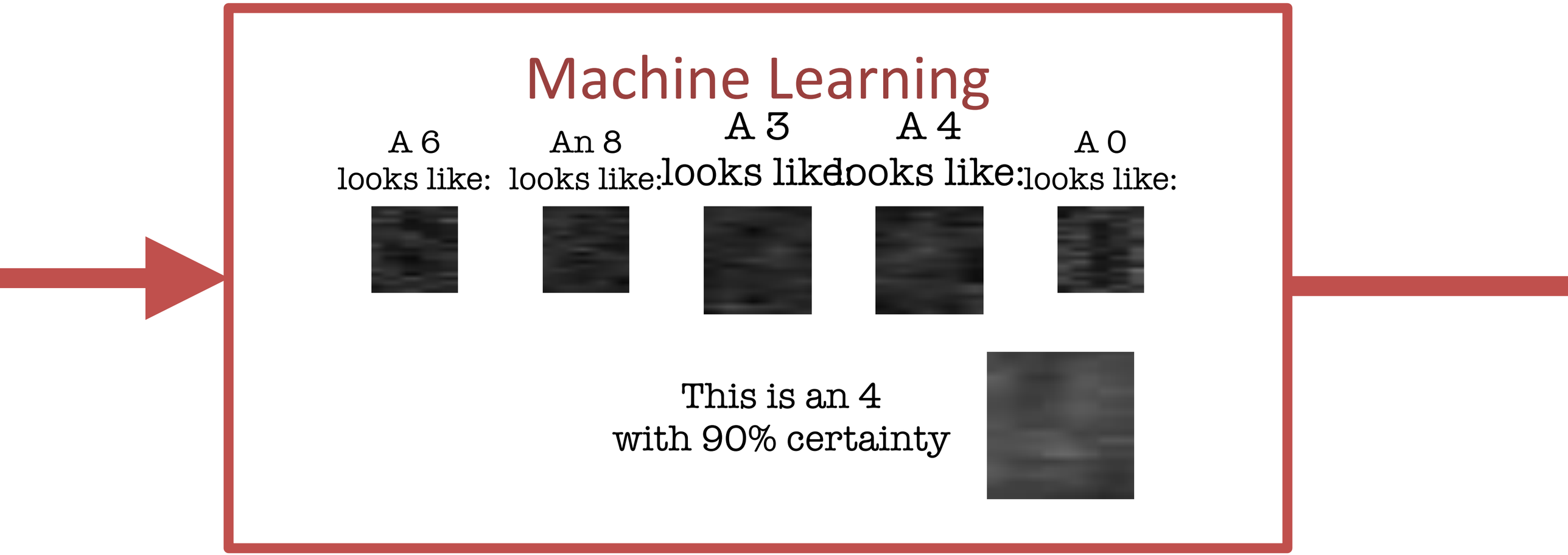
Machine Learning Classification



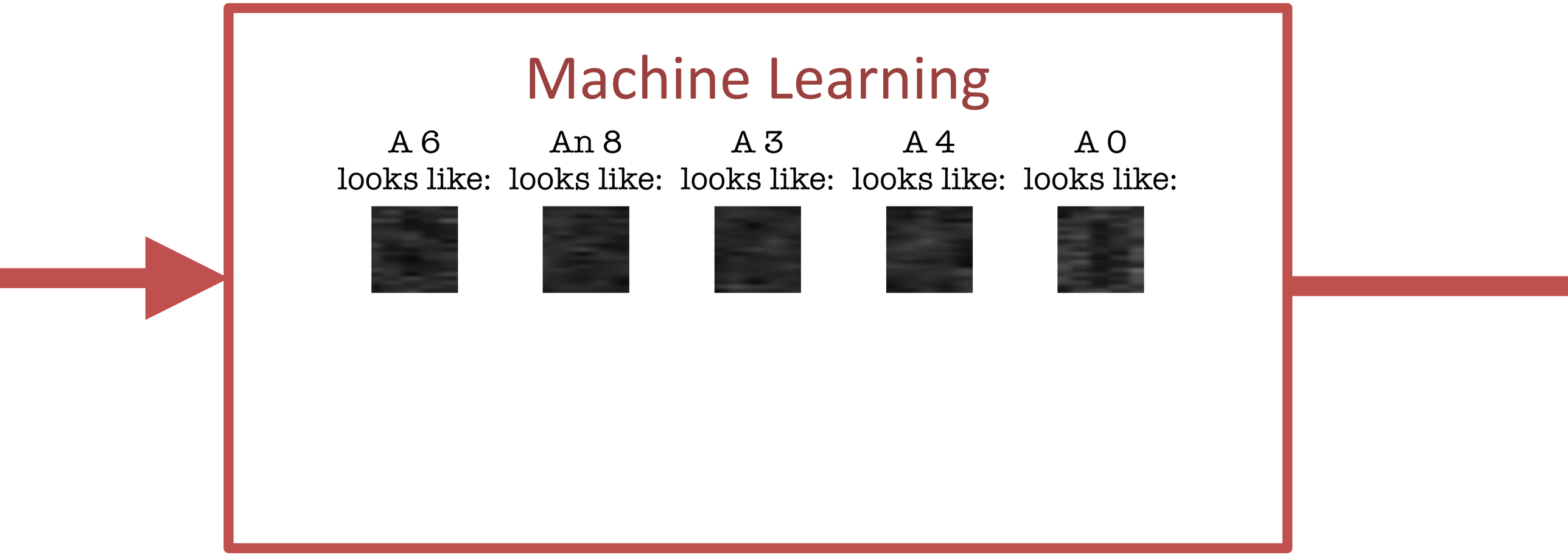
Machine Learning Classification



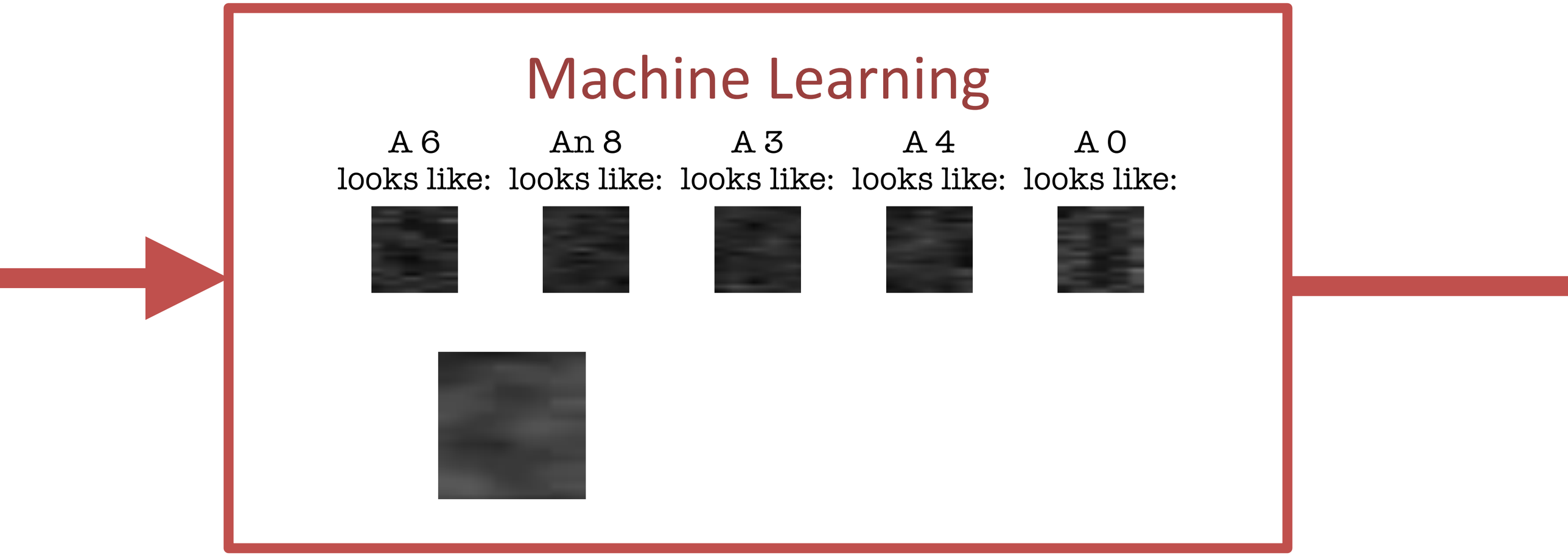
Machine Learning Classification



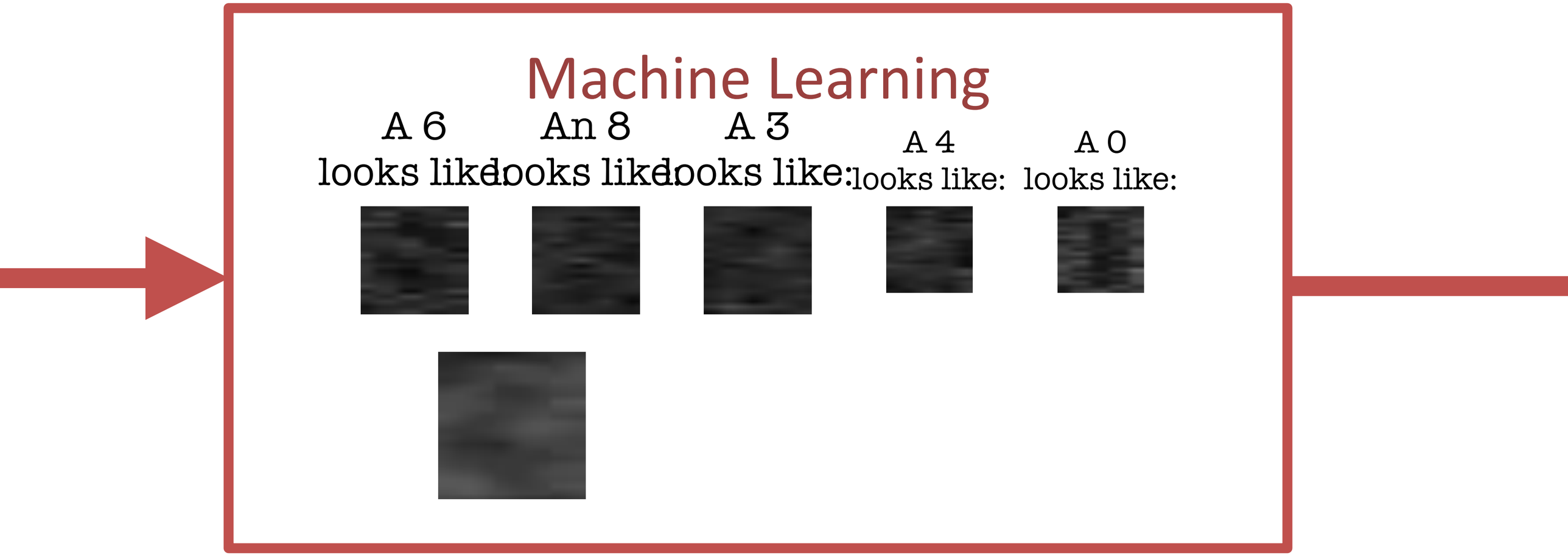
Machine Learning Classification



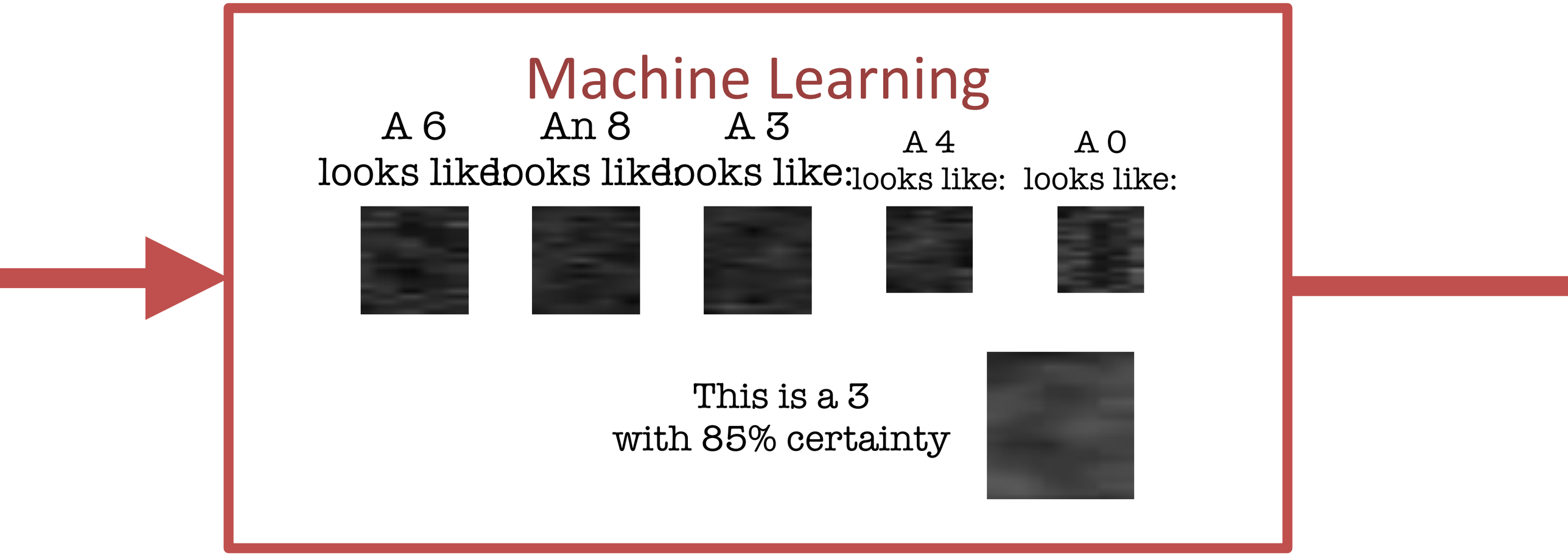
Machine Learning Classification



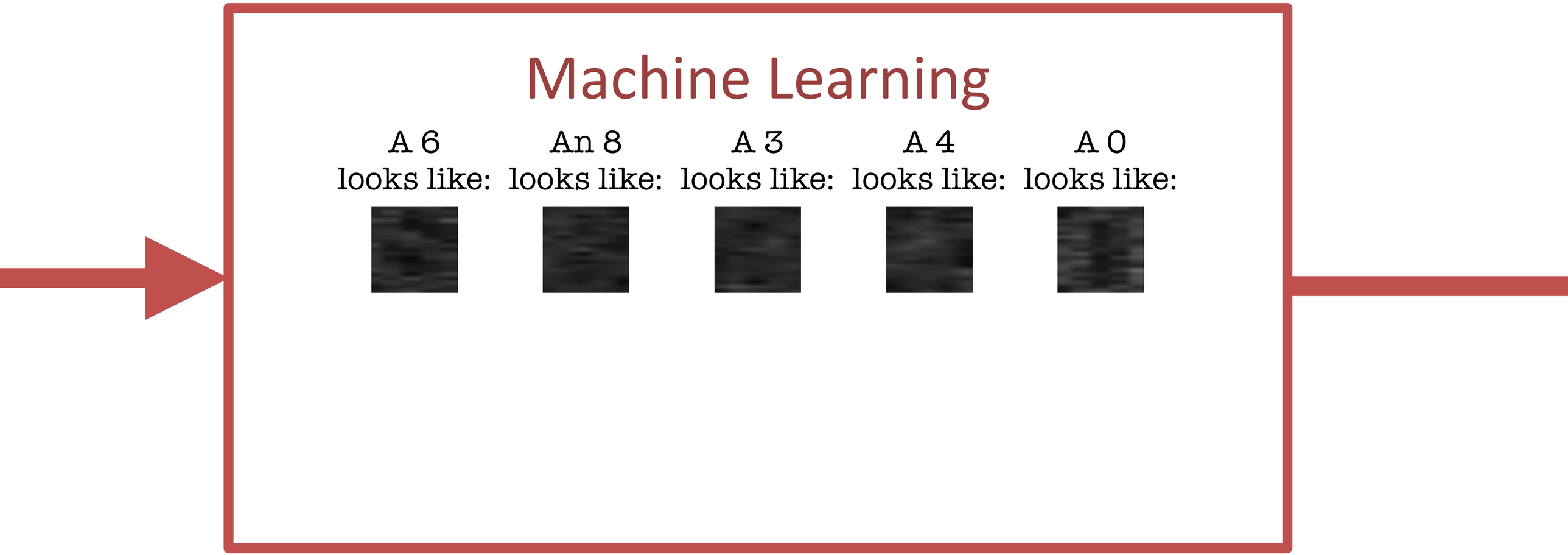
Machine Learning Classification



Machine Learning Classification

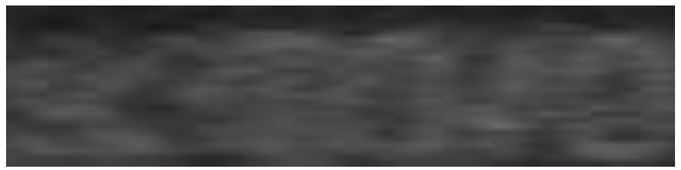


Machine Learning Classification



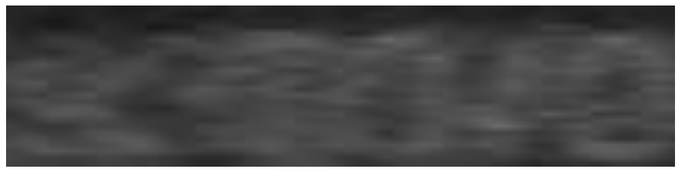
Machine Learning Classification

“What does this say?”



Machine Learning Classification

“What does this say?”



I am 90% sure
it is “937042”.

OUTLOOK

Outlook

Outlook

- Non-ideal antenna

Outlook

- Non-ideal antenna
  - Want to measure greater distances

Outlook

- Non-ideal antenna
  - Want to measure greater distances
  - Want to measure every phone

Outlook

- Non-ideal antenna
  - Want to measure greater distances
  - Want to measure every phone
- SDR setup requires optimizations

Outlook

- Non-ideal antenna
  - Want to measure greater distances
  - Want to measure every phone
- SDR setup requires optimizations
  - Higher sample rates

Outlook

- Non-ideal antenna
  - Want to measure greater distances
  - Want to measure every phone
- SDR setup requires optimizations
  - Higher sample rates
  - Other measurement methods

Outlook

- Non-ideal antenna
  - Want to measure greater distances
  - Want to measure every phone
- SDR setup requires optimizations
  - Higher sample rates
  - Other measurement methods
- New testbed for machine learning

Take Home Message…

Take Home Message…

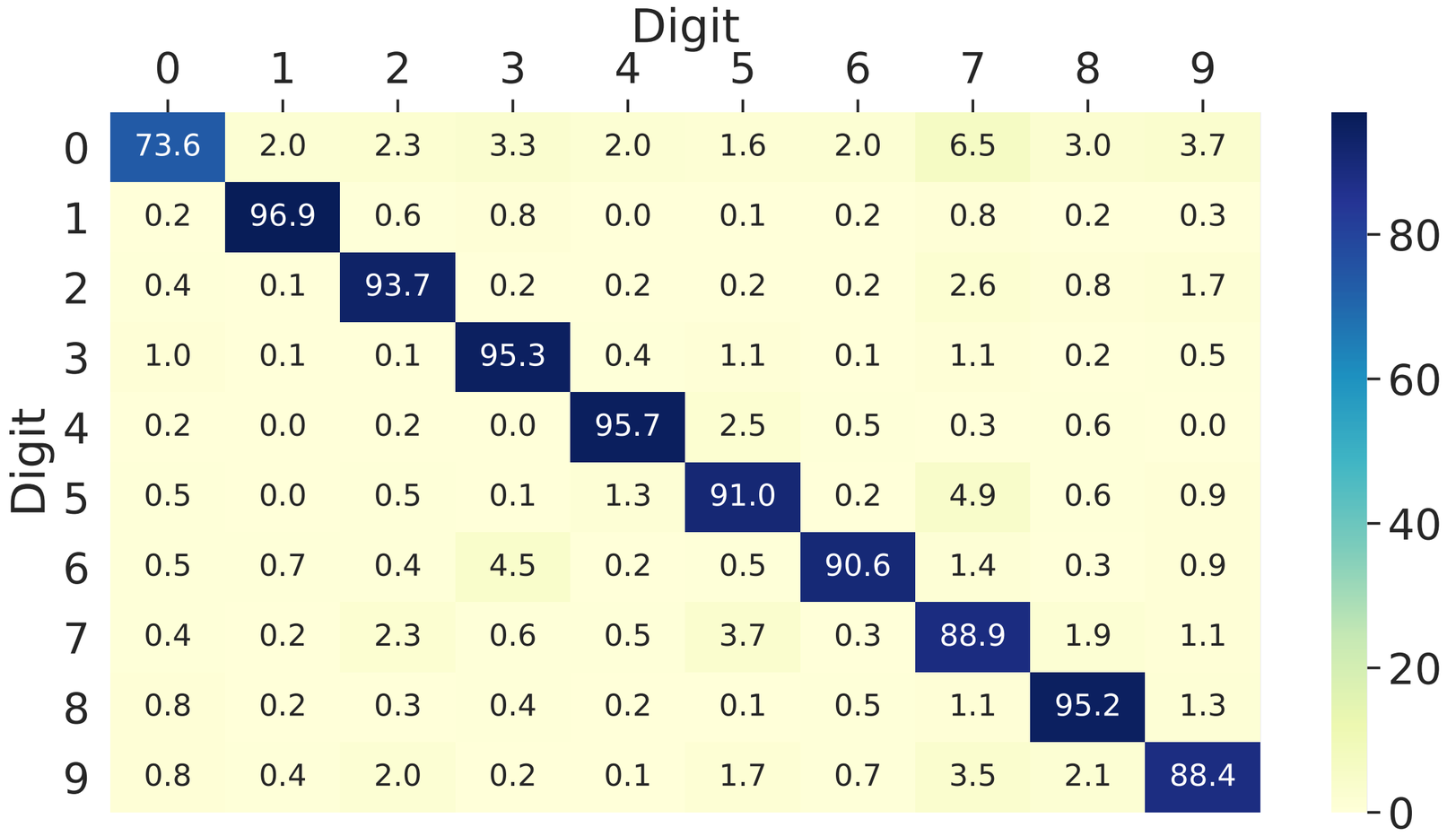
Screen Gleaning works!

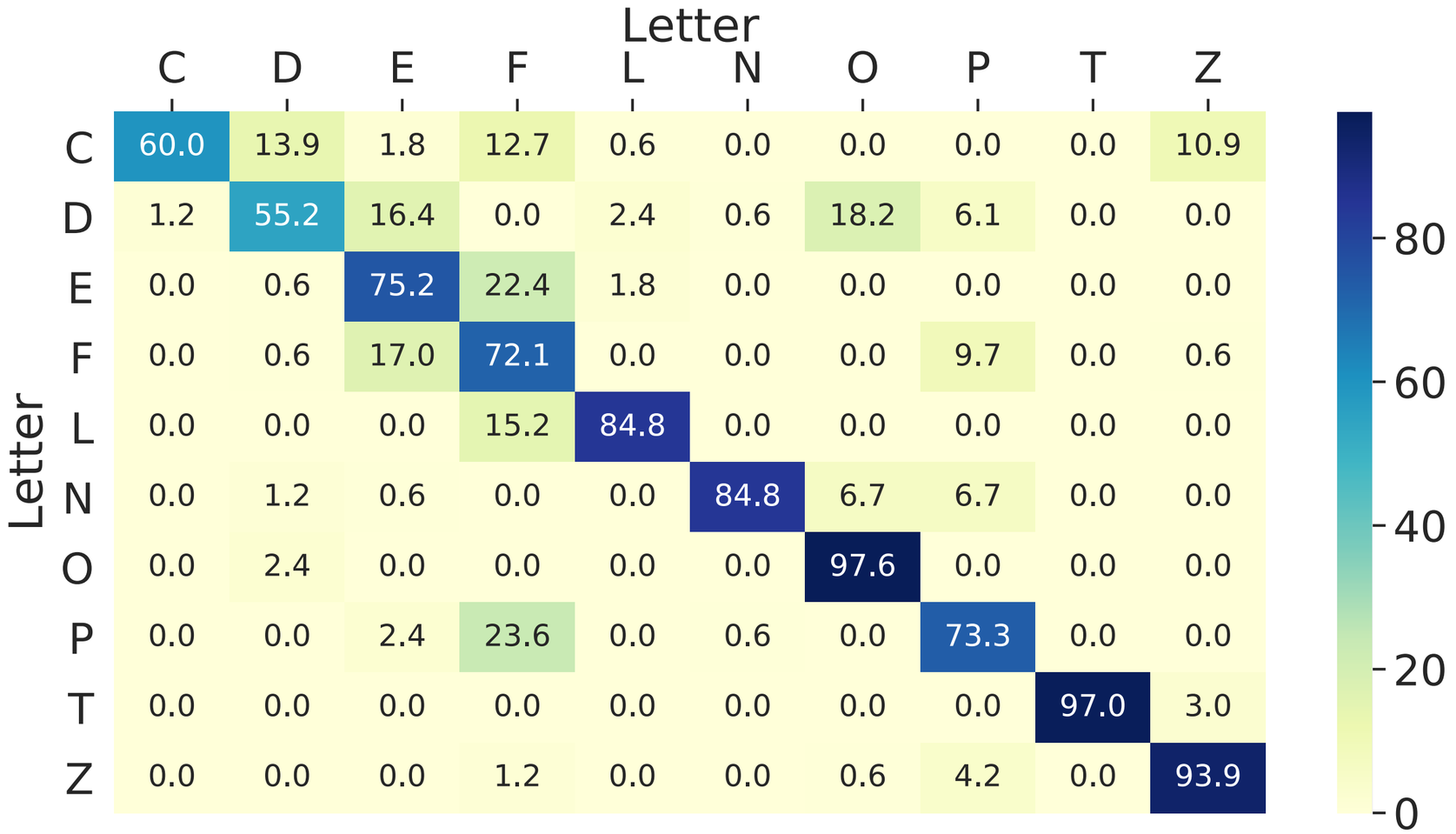
Take Home Message…

Screen Gleaning works!

Be careful with what you read on your phone…

DISCUSSION


Digit
0 1 2 3 4 5 6 7 8 9
Digit
0 73.6 2.0 2.3 3.3 2.0 1.6 2.0 6.5 3.0 3.7
1 0.2 96.9 0.6 0.8 0.0 0.1 0.2 0.8 0.2 0.3
2 0.4 0.1 93.7 0.2 0.2 0.2 0.2 2.6 0.8 1.7
3 1.0 0.1 0.1 95.3 0.4 1.1 0.1 1.1 0.2 0.5
4 0.2 0.0 0.2 0.0 95.7 2.5 0.5 0.3 0.6 0.0
5 0.5 0.0 0.5 0.1 1.3 91.0 0.2 4.9 0.6 0.9
6 0.5 0.7 0.4 4.5 0.2 0.5 90.6 1.4 0.3 0.9
7 0.4 0.2 2.3 0.6 0.5 3.7 0.3 88.9 1.9 1.1
8 0.8 0.2 0.3 0.4 0.2 0.1 0.5 1.1 95.2 1.3
9 0.8 0.4 2.0 0.2 0.1 1.7 0.7 3.5 2.1 88.4
80
60
40
20
0


Letter
C D E F L N O P T Z
Letter
C 60.0 13.9 1.8 12.7 0.6 0.0 0.0 0.0 0.0 10.9
D 1.2 55.2 16.4 0.0 2.4 0.6 18.2 6.1 0.0 0.0
E 0.0 0.6 75.2 22.4 1.8 0.0 0.0 0.0 0.0 0.0
F 0.0 0.6 17.0 72.1 0.0 0.0 0.0 9.7 0.0 0.6
L 0.0 0.0 0.0 15.2 84.8 0.0 0.0 0.0 0.0 0.0
N 0.0 1.2 0.6 0.0 0.0 84.8 6.7 6.7 0.0 0.0
O 0.0 2.4 0.0 0.0 0.0 0.0 97.6 0.0 0.0 0.0
P 0.0 0.0 2.4 23.6 0.0 0.6 0.0 73.3 0.0 0.0
T 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 97.0 3.0
Z 0.0 0.0 0.0 1.2 0.0 0.0 0.6 4.2 0.0 93.9
80
60
40
20
0