
# SIGNAL Processing with GNUradio and SDRs

Ateet Kumar

*Senior Security Researcher, Xen1thLabs*

*Digital14 LLC*

# Who am I ?

## Ateet Kumar

Senior Security Researcher, Xen1thLabs, Digital 14 LLC

- The *Signals Guy*
- Electronics and Communication Engineer
- Former DRDO Research Fellow for 3 years

@HyperS0nik ateetkumarofficial@gmail.com

# Content

- PART-1: Basics of EM and RF
- PART-2: Digital Signal Processing Techniques
- PART-3: GNURadio hands-on.
- PART-4: SDRs and RF hacking Hands-on.


# PART 1

# Electromagnetic Spectrum

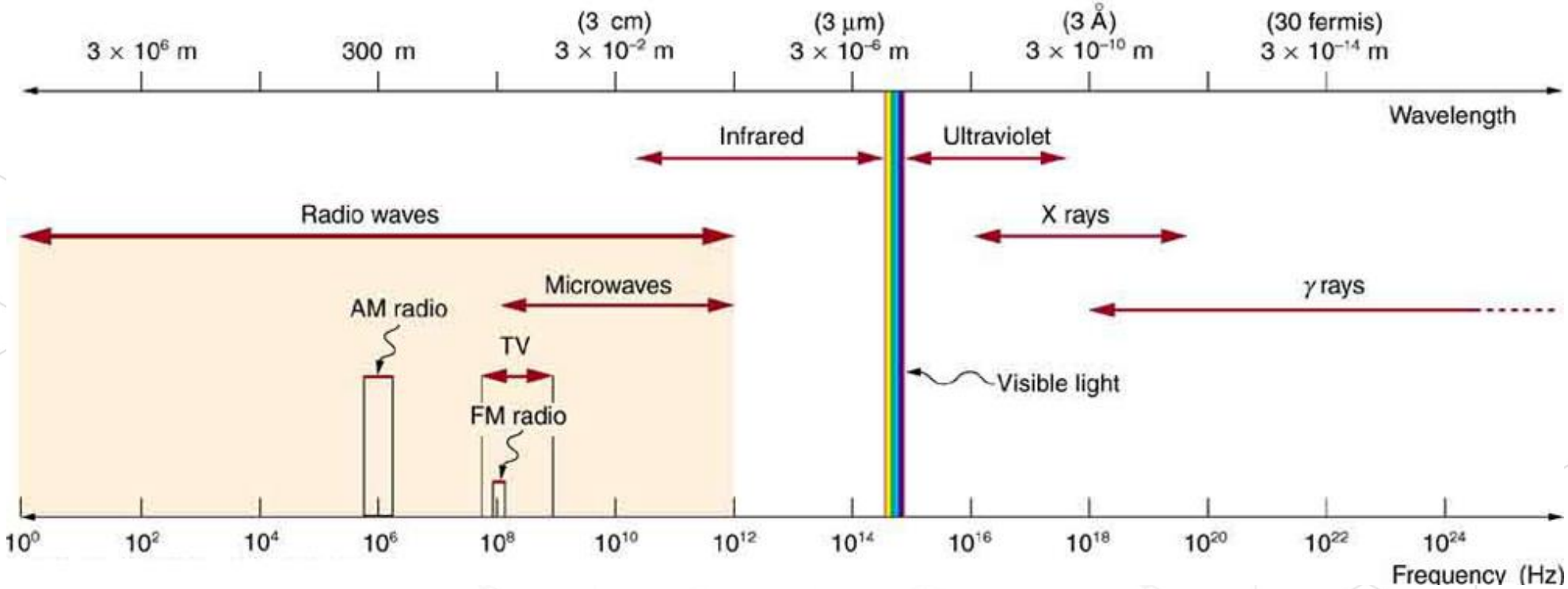



Image source: https://opentextbc.ca/openstaxcollegephysics/chapter/the-electromagnetic-spectrum/

# Frequency Band Designation

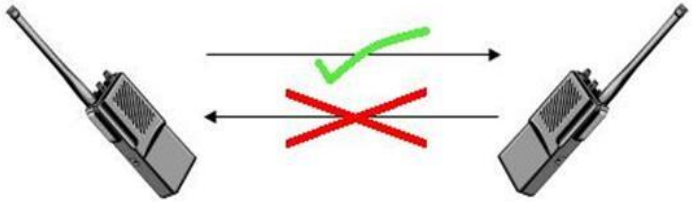
| $f$ | $\lambda$ | Band | Description |
|---|---|---|---|
| 30–300 Hz | $10^4$–$10^3$ km | ELF | Extremely low frequency |
| 300–3000 Hz | $10^3$–$10^2$ km | VF | Voice frequency |
| 3–30 kHz | 100–10 km | VLF | Very low frequency |
| 30–300 kHz | 10–1 km | LF | Low frequency |
| 0.3–3 MHz | 1–0.1 km | MF | Medium frequency |
| 3–30 MHz | 100–10 m | HF | High frequency |
| 30–300 MHz | 10–1 m | VHF | Very high frequency |
| 300–3000 MHz | 100–10 cm | UHF | Ultra-high frequency |
| 3–30 GHz | 10–1 cm | SHF | Superhigh frequency |
| 30–300 GHz | 10–1 mm | EHF | Extremely high frequency (millimeter waves) |

Image source: http://www.ni.com/tutorial/3541/en/

# Radio Waves

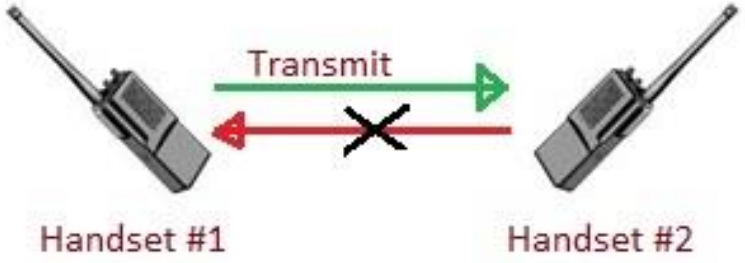
- 30Hz to 300GHz
- Either in terms of frequency or wavelength
- Generated by accelerating electric charges. ( e.g. current)
- Space generates a lot of Radio waves too
- Radio waves are EM waves too

# RF Communication Systems



Simplex

Duplex



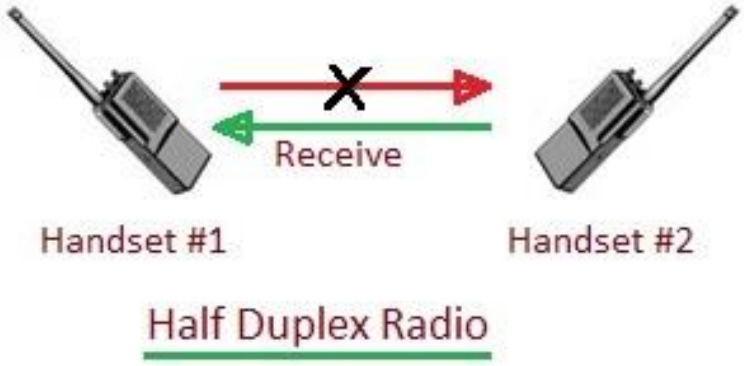
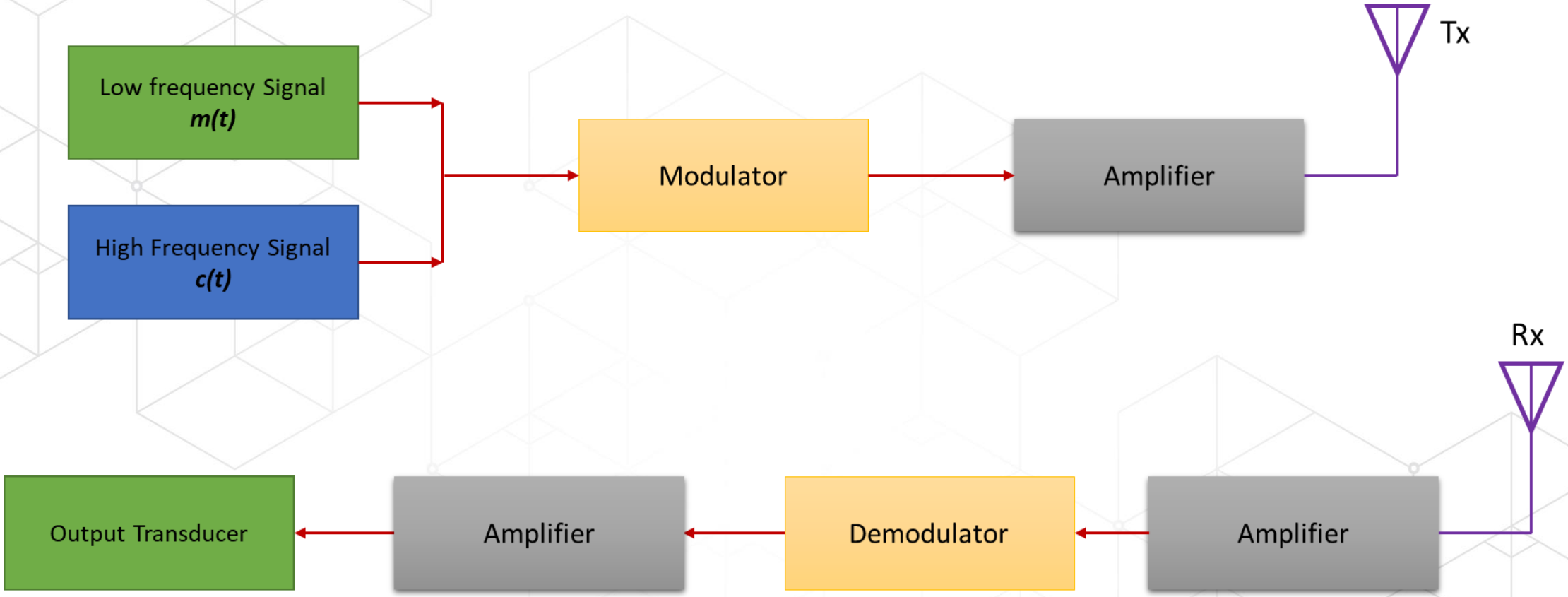




Image source: https://commons.wikimedia.org/wiki/

# Wireless Communication Systems

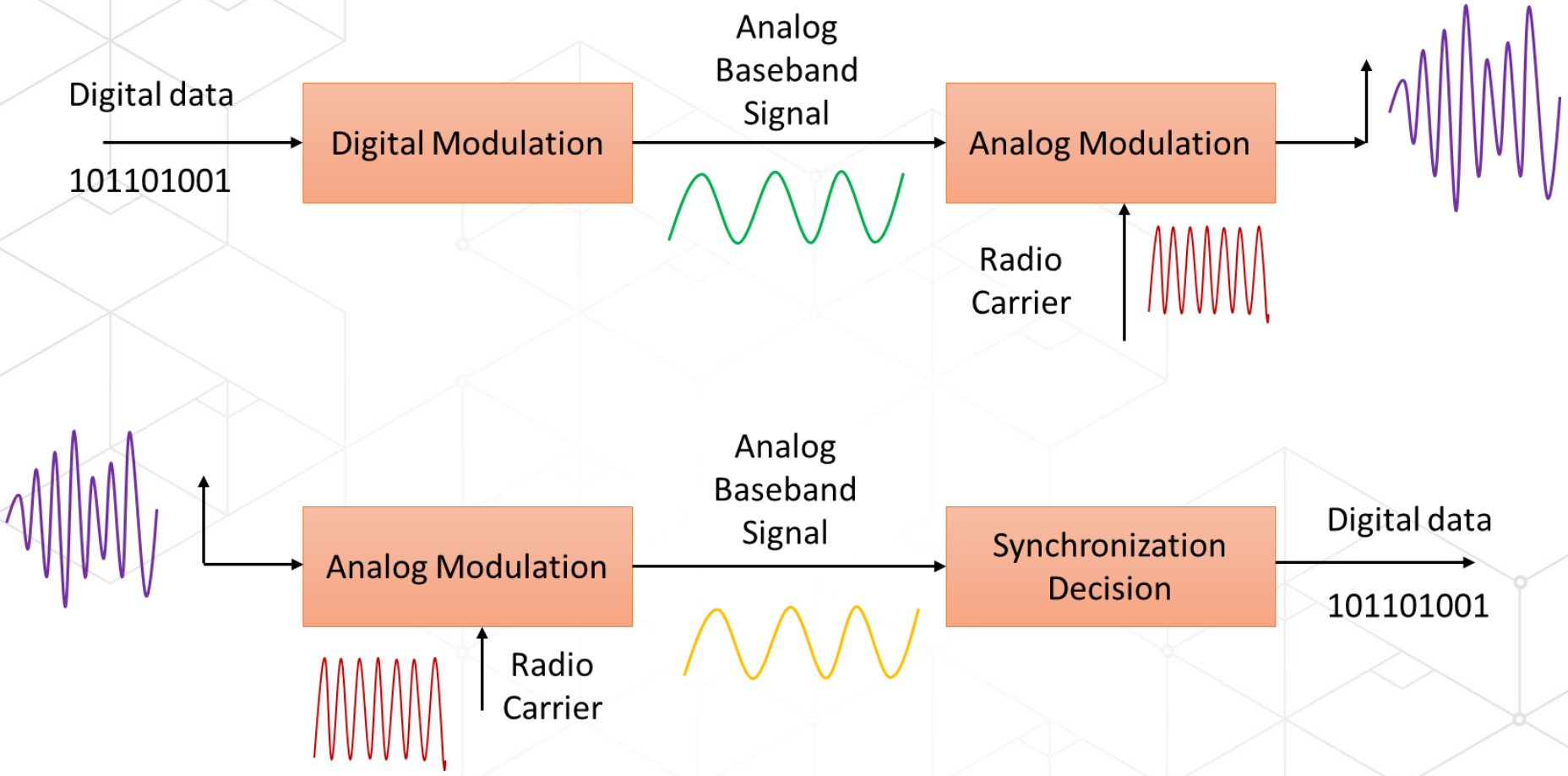


# Types of Modulations

1. Amplitude Modulation (AM): the amplitude of the carrier varies in accordance to the information signal
2. Frequency Modulation (FM): the frequency of the carrier varies in accordance to the information signal
3. Phase Modulation (PM): the phase of the carrier varies in accordance to the information signal

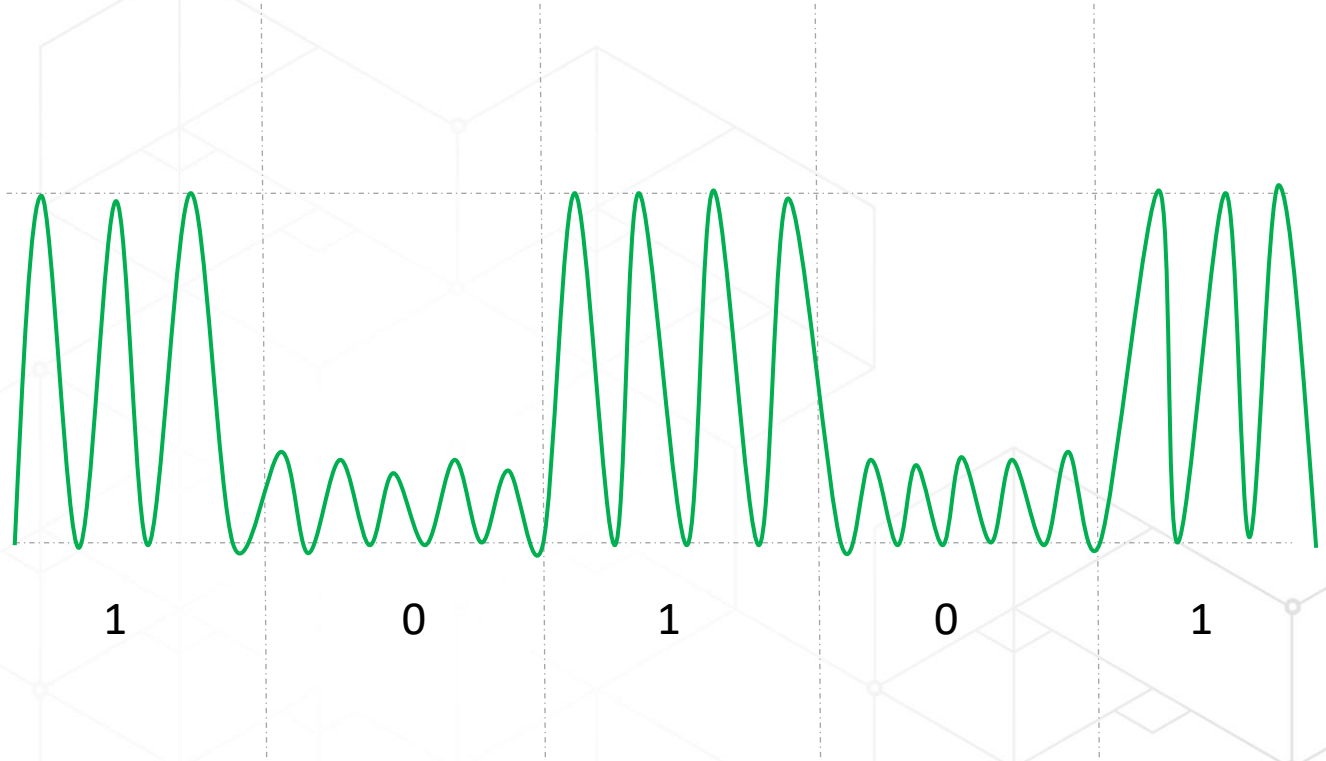
- Carrier signal:- $c(t) = A \sin(\omega c + \varphi)$
- Message Signal:- $m(t) = M \sin(\omega m + \varphi)$
- Modulated O/P signal:- $y(t) = [A + m(t)].c(t)$

# Modulation and Demodulation



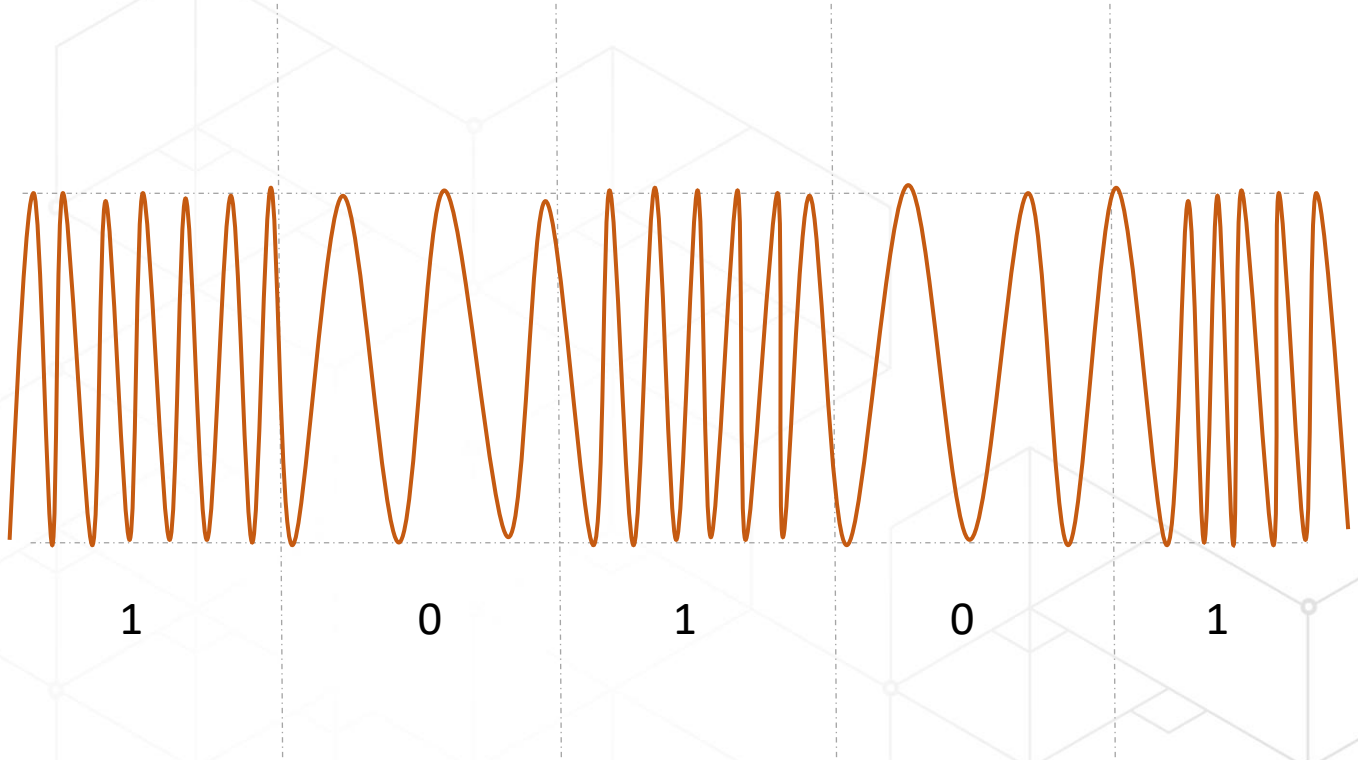
# Digital Modulation

- Shift Keying
  - ASK
  - FSK
  - PSK



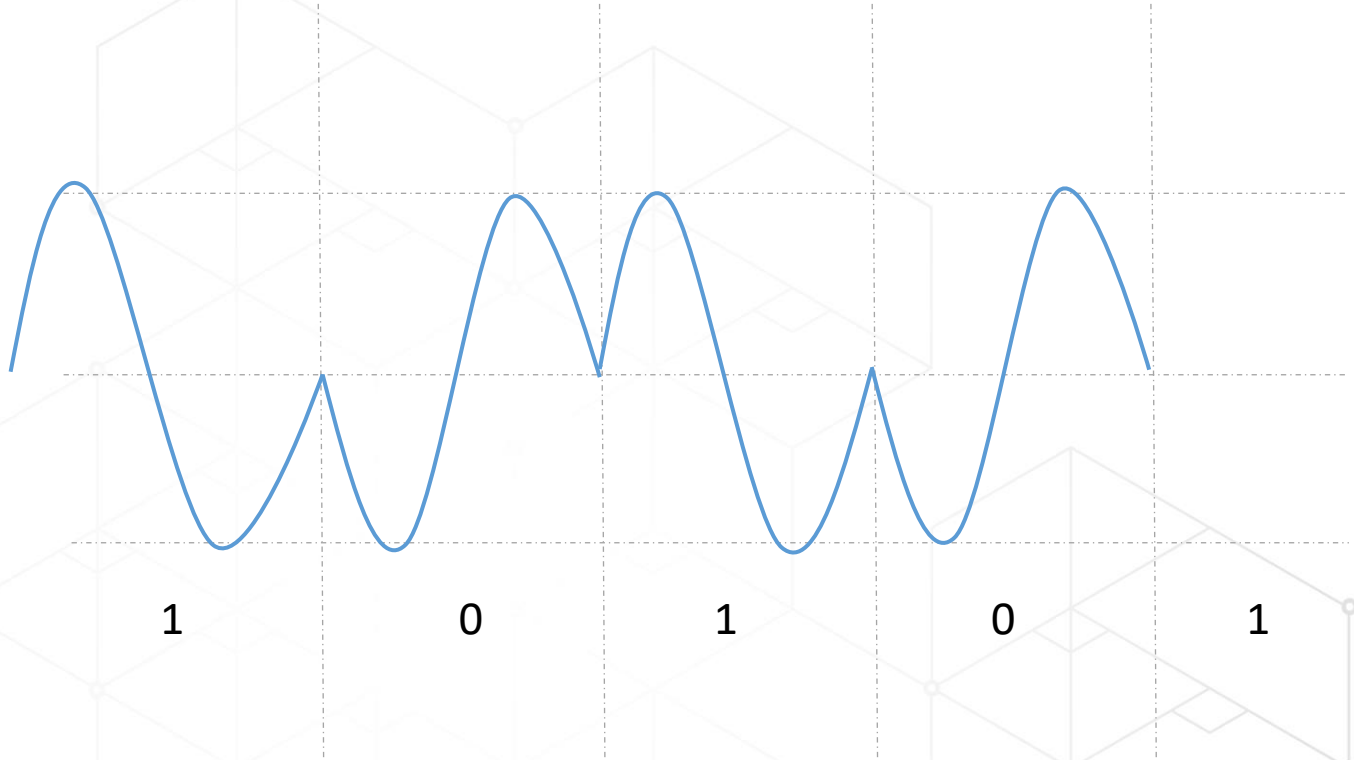
# Digital Modulation

- Shift Keying
  - ASK
  - FSK
  - PSK



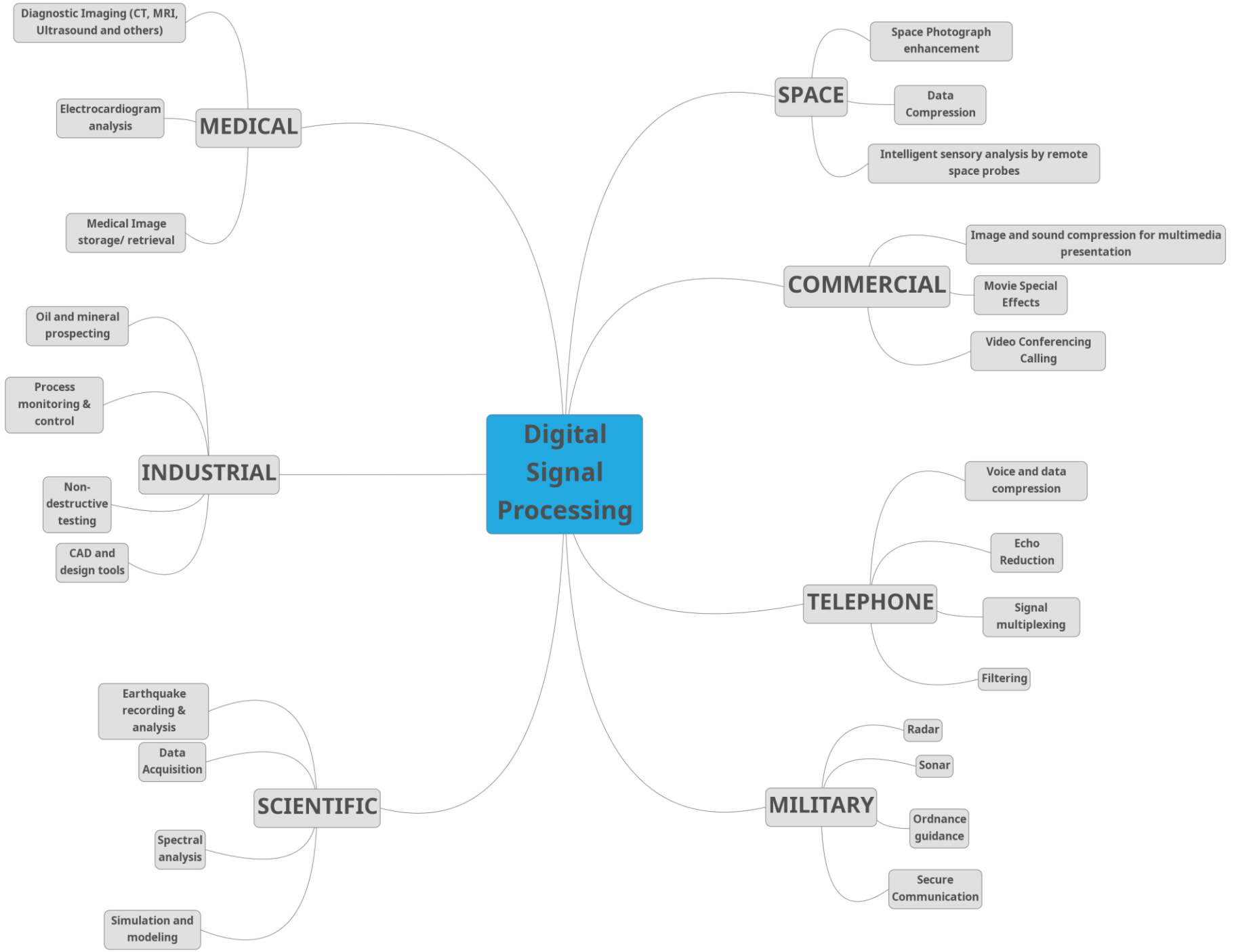
# Digital Modulation

- Shift Keying
  - ASK
  - FSK
  - PSK

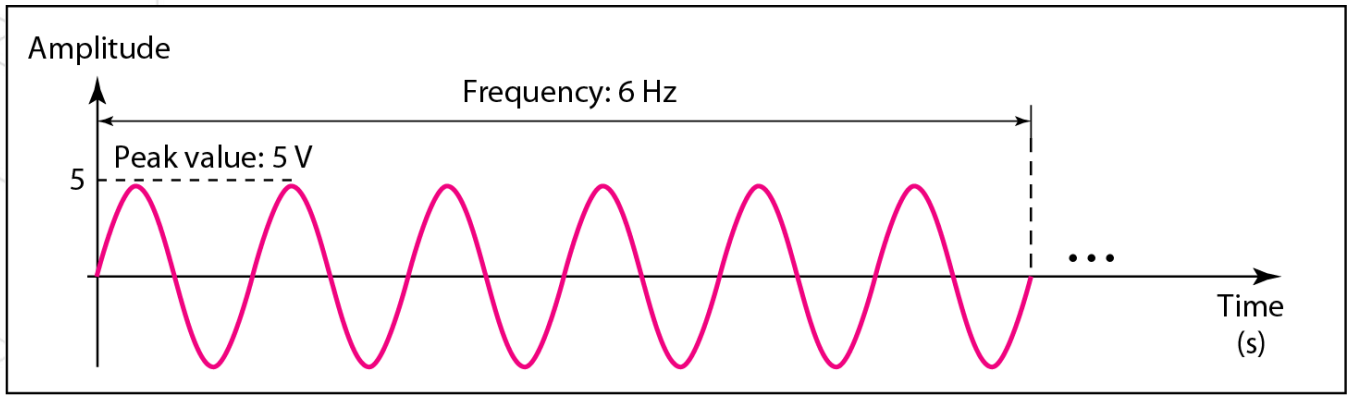



# PART 2

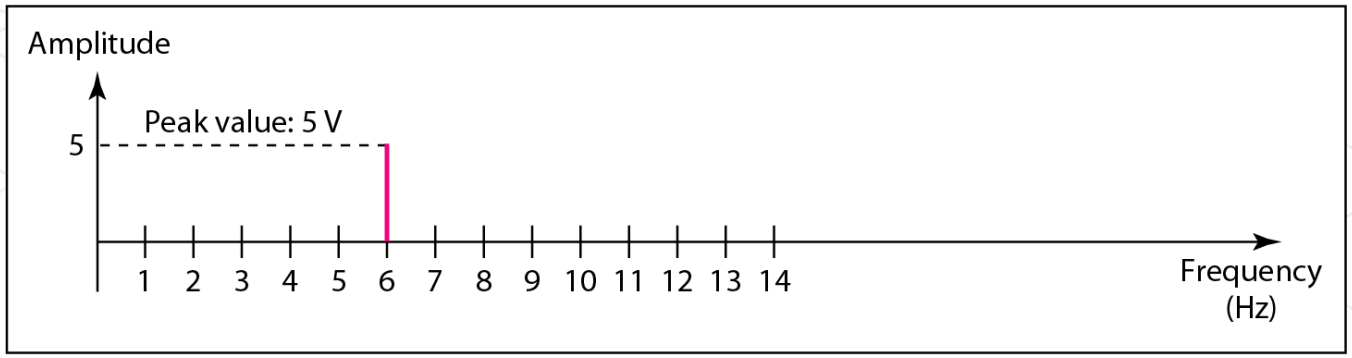
# DSP


Digital Signal Processing
MEDICAL
Diagnostic Imaging (CT, MRI, Ultrasound and others)
Electrocardiogram analysis
Medical Image storage/ retrieval
SPACE
Space Photograph enhancement
Data Compression
Intelligent sensory analysis by remote space probes
COMMERCIAL
Image and sound compression for multimedia presentation
Movie Special Effects
Video Conferencing Calling
INDUSTRIAL
Oil and mineral prospecting
Process monitoring & control
Non-destructive testing
CAD and design tools
TELEPHONE
Voice and data compression
Echo Reduction
Signal multiplexing
Filtering
SCIENTIFIC
Earthquake recording & analysis
Data Acquisition
Spectral analysis
Simulation and modeling
MILITARY
Radar
Sonar
Ordnance guidance
Secure Communication

# Time domain and frequency domain plots of a Sine Wave



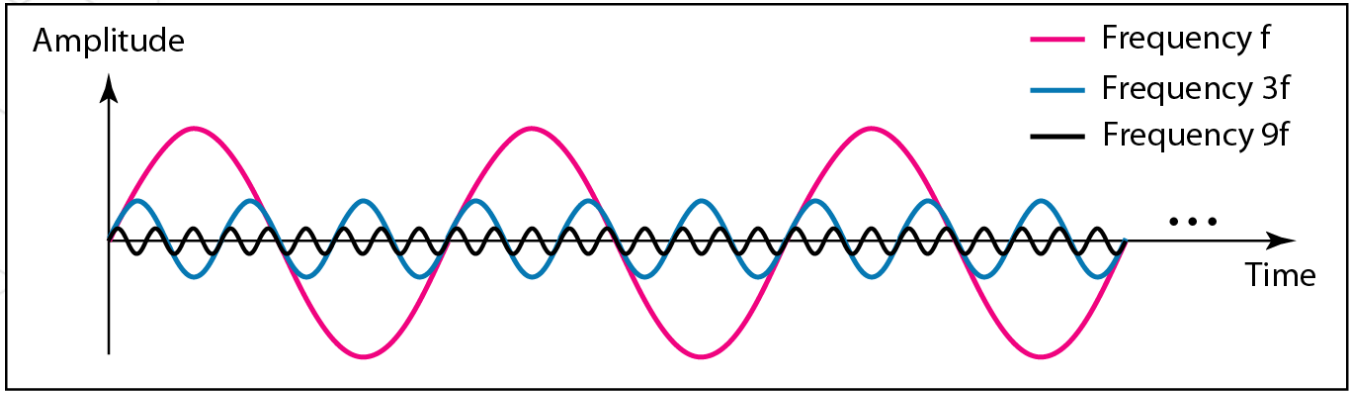

a. A sine wave in the time domain (peak value: 5 V, frequency: 6 Hz)



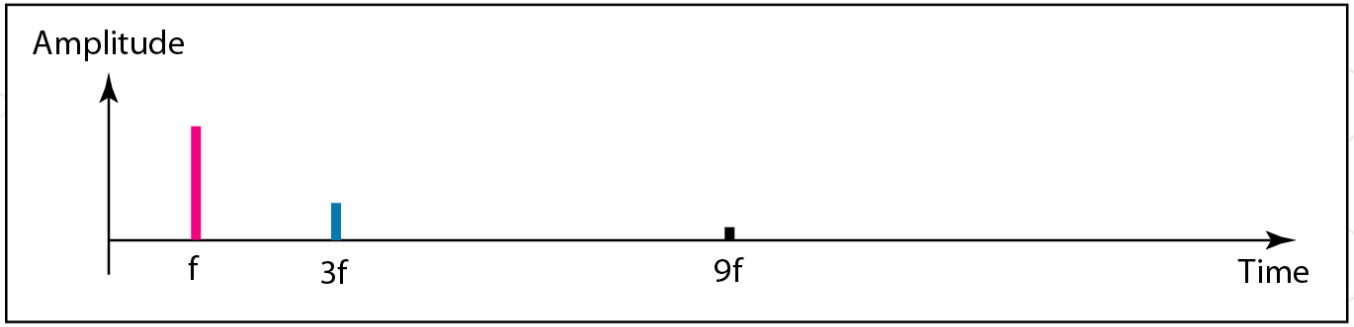

b. The same sine wave in the frequency domain (peak value: 5 V, frequency: 6 Hz)

Image Source: Data Communications and Networking, Fourth Edition, Forouzan

# Decomposition of a composite periodic signal in the time and frequency domains




a. Time-domain decomposition of a composite signal




b. Frequency-domain decomposition of the composite signal

Image Source: Data Communications and Networking, Fourth Edition, Forouzan

*If a signal does not change at all, its frequency is zero.*

*If a signal changes instantaneously, its frequency is infinite.*

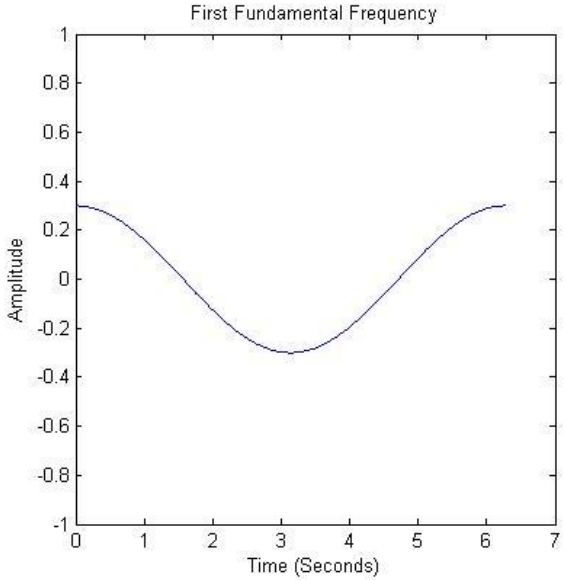
Image Source: Data Communications and Networking, Fourth Edition, Forouzan

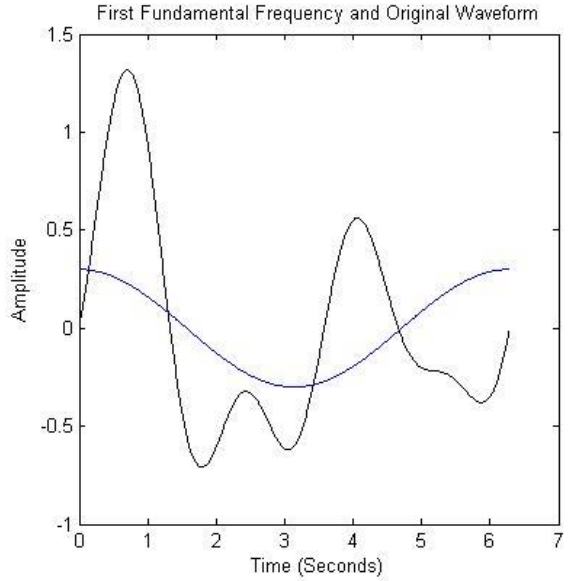
# Fourier Transforms

The Fourier Transform .com

$$\mathcal{F}\{g(t)\} = G(f) = \int_{-\infty}^{\infty} g(t)e^{-i2\pi ft}\,dt$$

$$\mathcal{F}^{-1}\{G(f)\} = g(t) = \int_{-\infty}^{\infty} G(f)e^{i2\pi ft}\,df$$



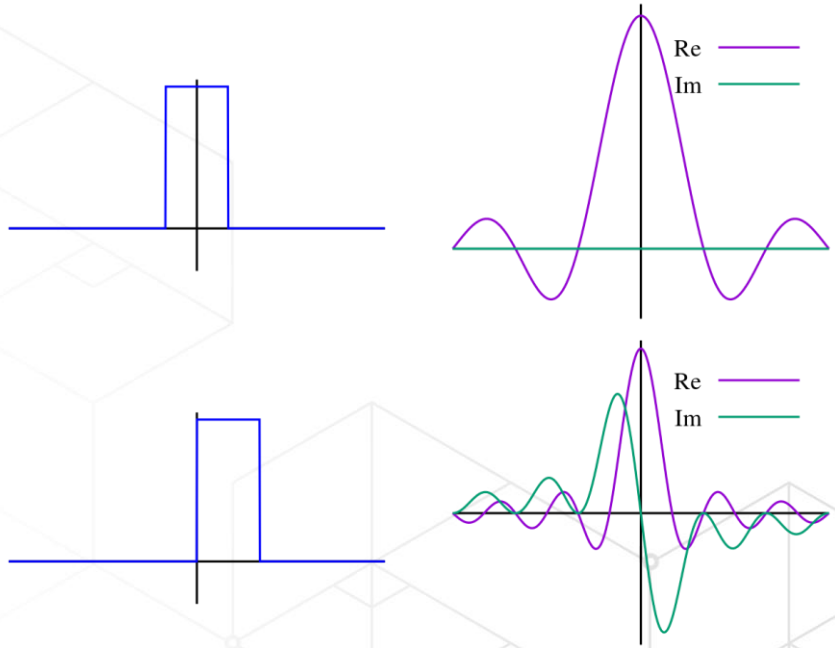
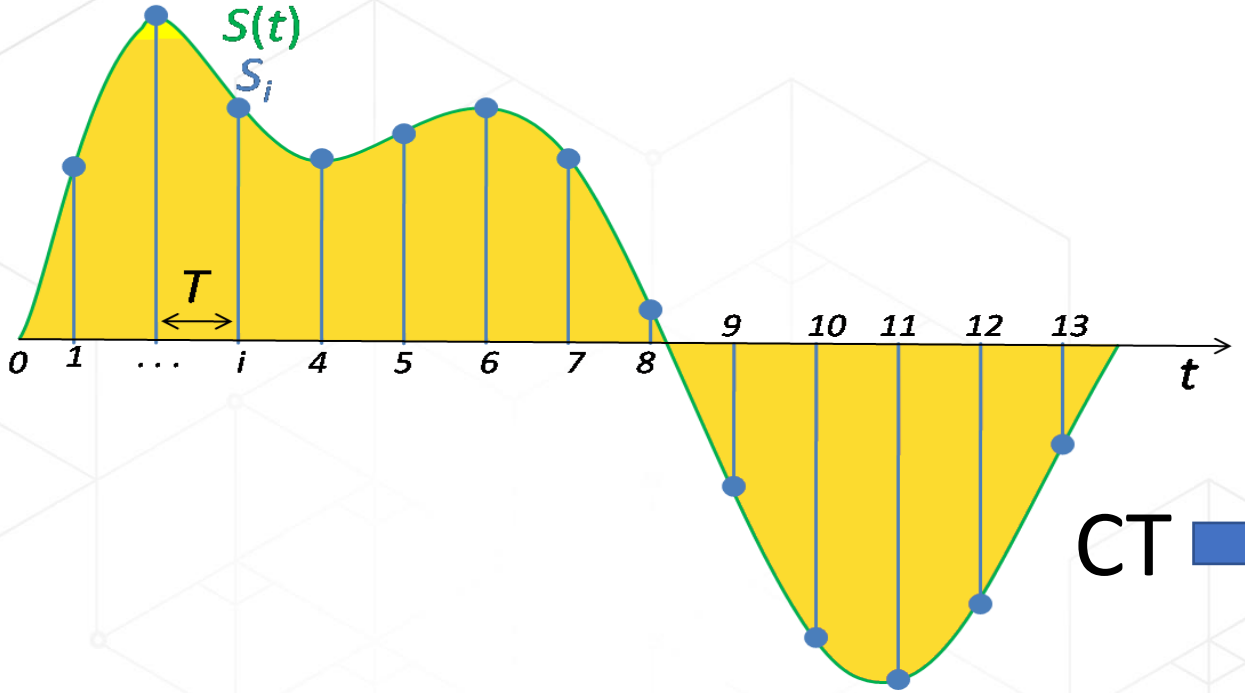




Image source: http://www.thefouriertransform.com/#introduction

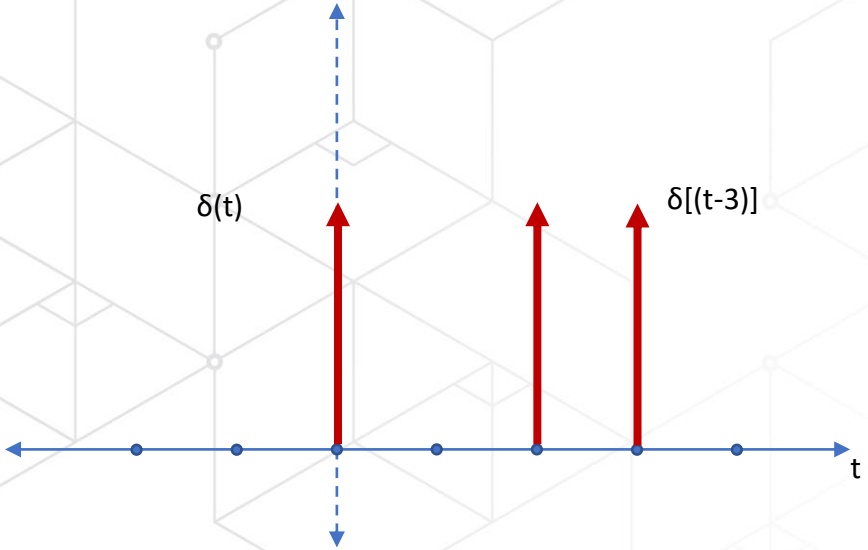
# Sampling

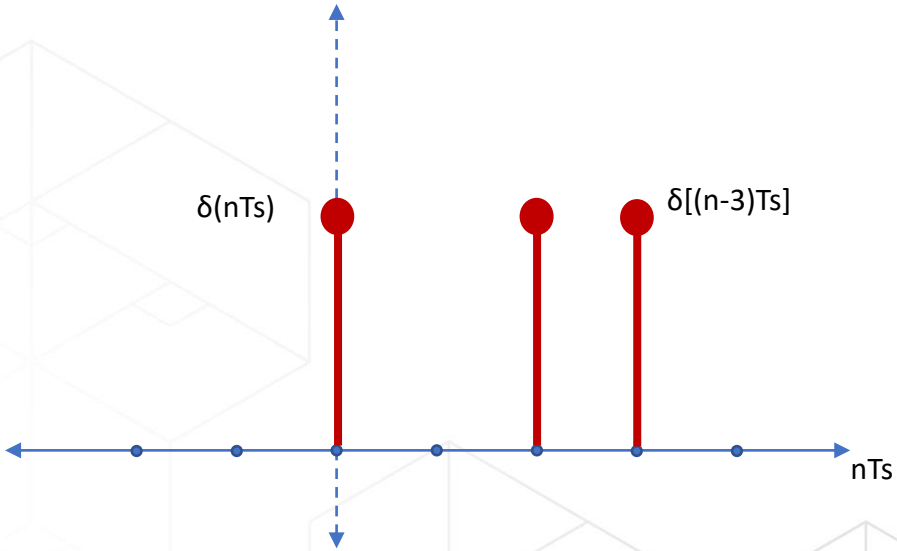



CT → DT

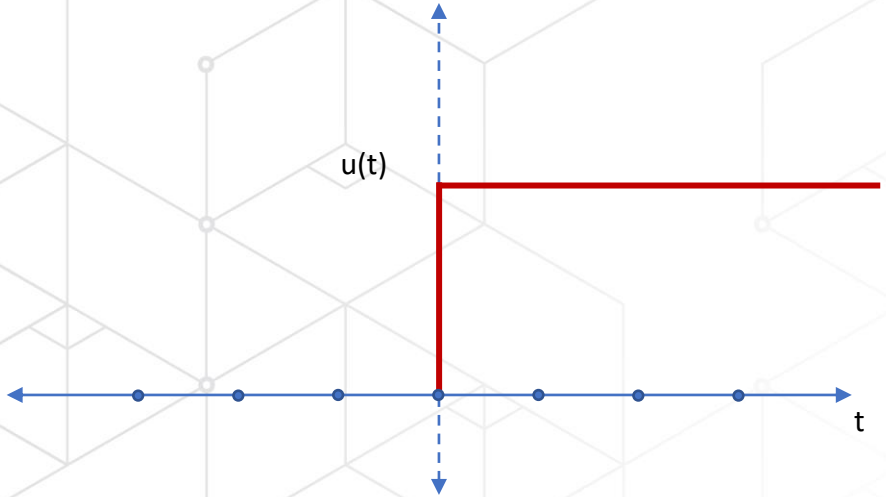
https://en.wikipedia.org/wiki/Sampling_(signal_processing)

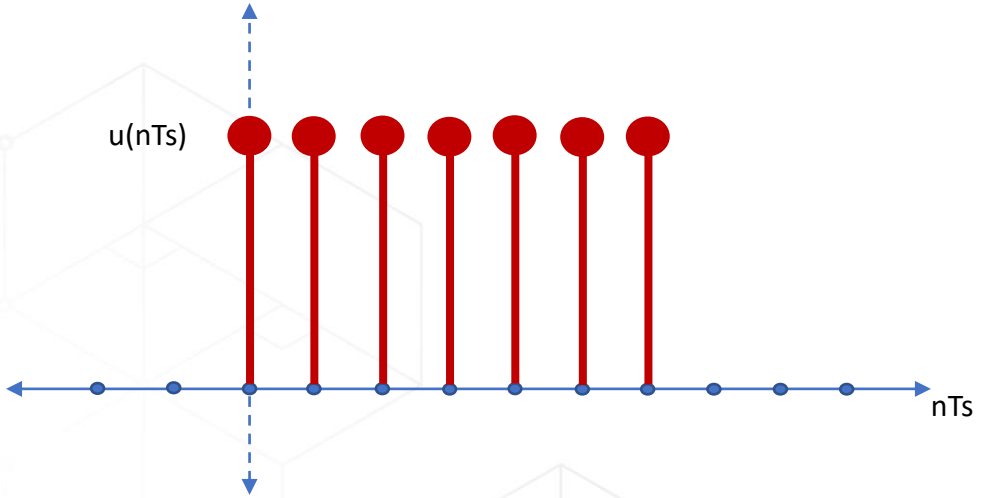
# Impulse Signal



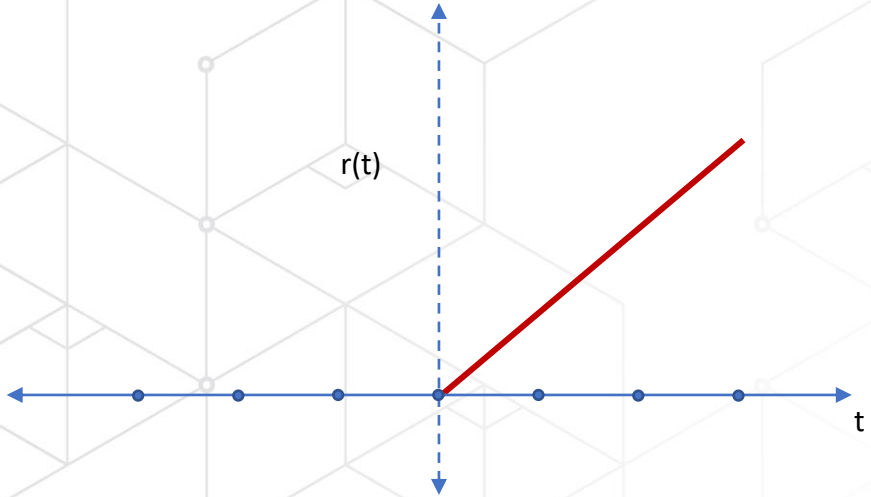



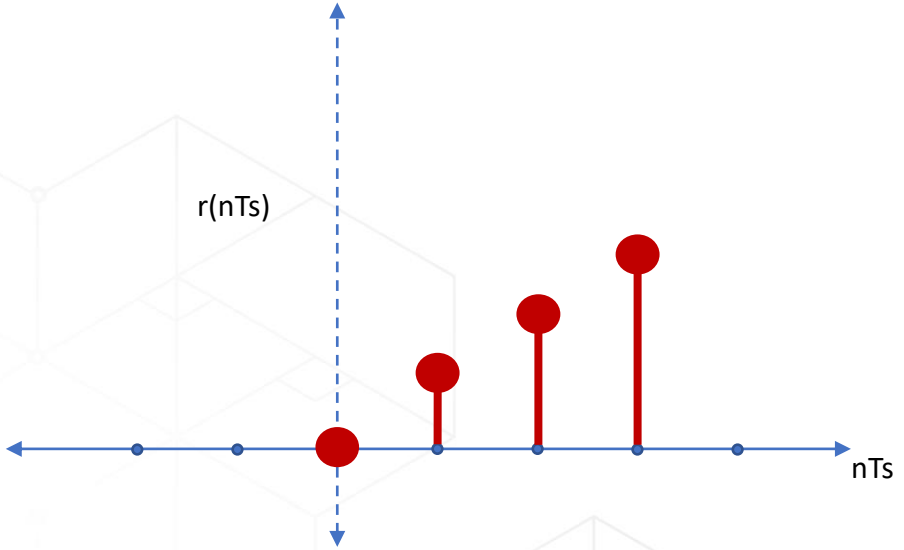
# Step Signal



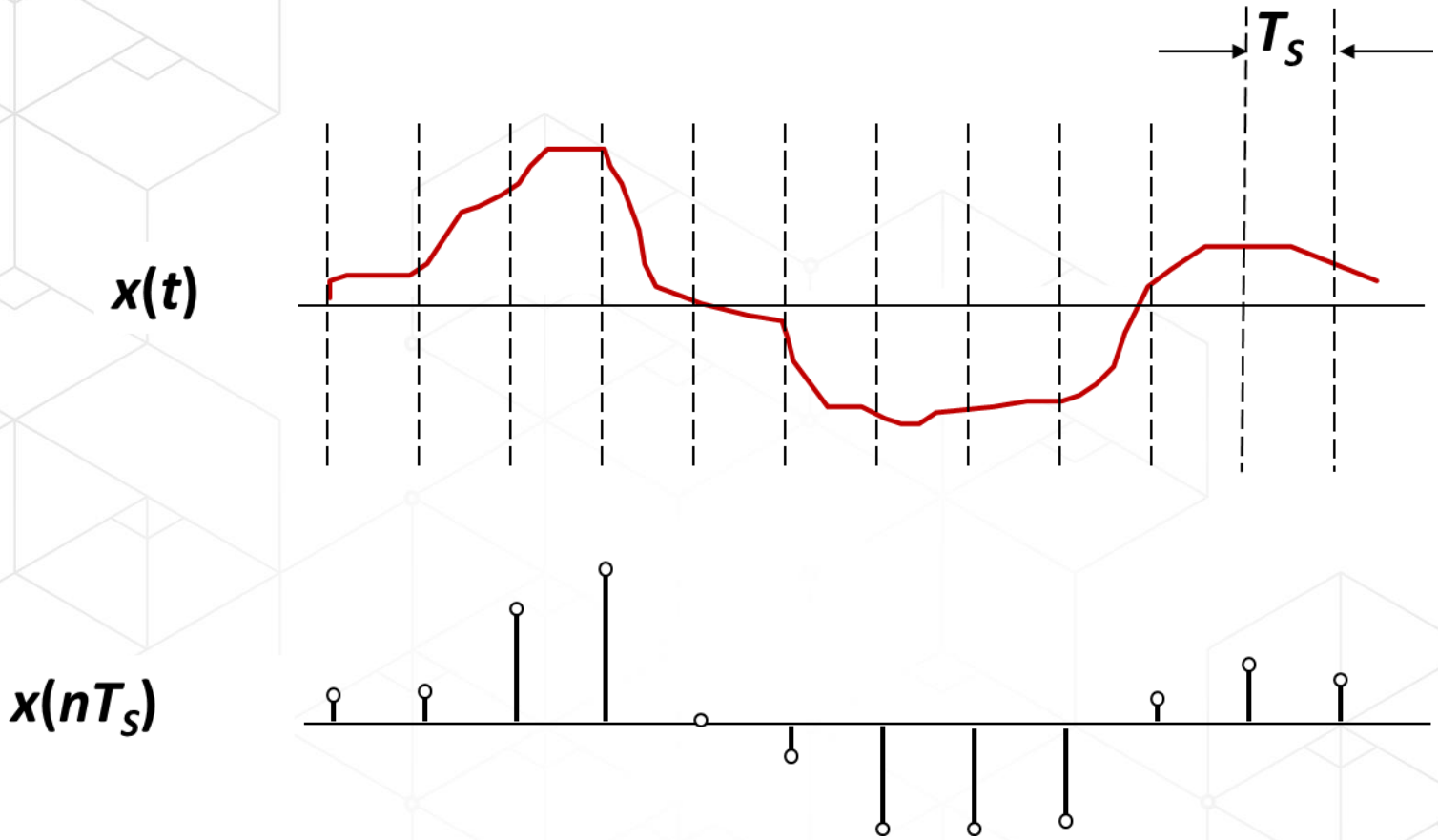



# Ramp Signal



# Sampling




http://www.ee.cityu.edu.hk/~csl/adsp/adsp.html

# Decimation

- Reducing sampling rate
- Simply Low pass filtering
- Also called Downsampling
- The decimation factor is simply the ratio of the input rate to the output rate. It is usually symbolized by “M”, so input rate / output rate=M.
- Why decimate? to reduce the *cost* of processing
- You can only decimate by integer factors; you cannot decimate by fractional factors.
- A signal can be downsampled (without doing any filtering) whenever it is “oversampled”, that is, when a sampling rate was used that was greater than the Nyquist criteria required.

https://dspguru.com/dsp/faqs/multirate/decimation/

# Interpolation

- Inserting zero-valued samples between original samples to increase the sampling rate.
- Zero Stuffing
- Upsampling
- Increase the sampling rate at the output of one system so that another system operating at a higher sampling rate can input the signal.
- The interpolation factor is simply the ratio of the output rate to the input rate. It is usually symbolized by “L”, so output rate / input rate=L.

https://dspguru.com/dsp/faqs/multirate/decimation/


# 5 Minutes Break


# PART 3


- Free and open source SDK
- Signal Processing modules for SDRs
- Source: www.gnuradio.org

***Let's use it to learn it ….***


# 5 Minutes Break


# PART 4

# SDR – Software Defined Radios

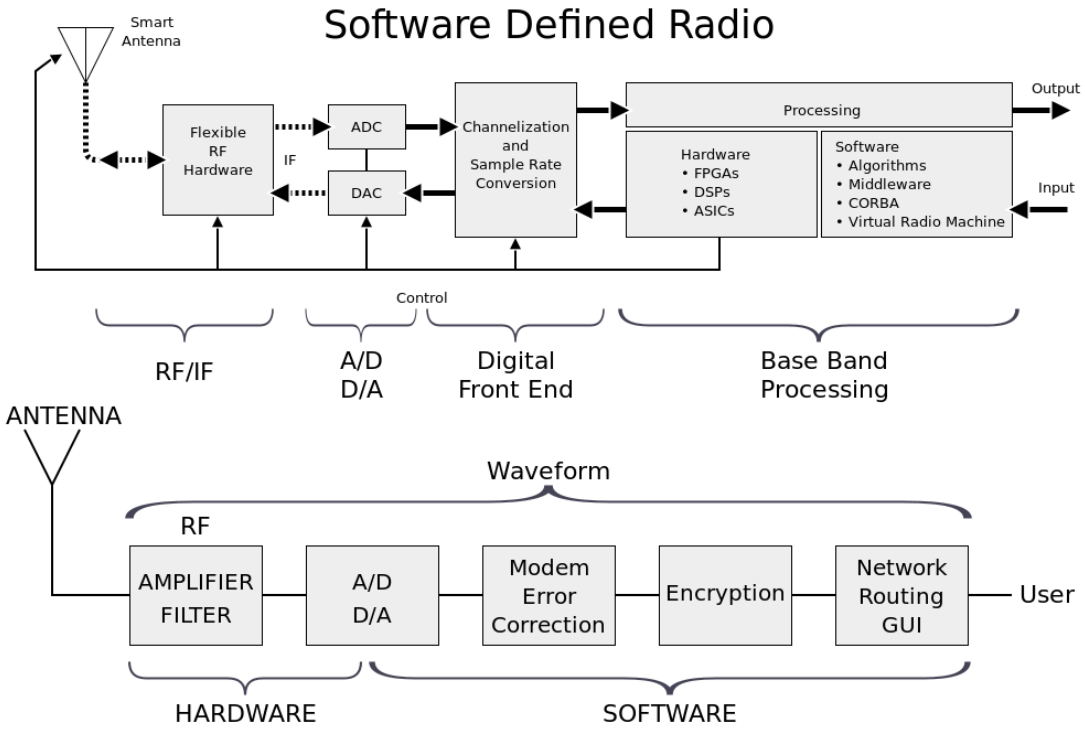



Image source: https://en.wikipedia.org/wiki/Software-defined_radio

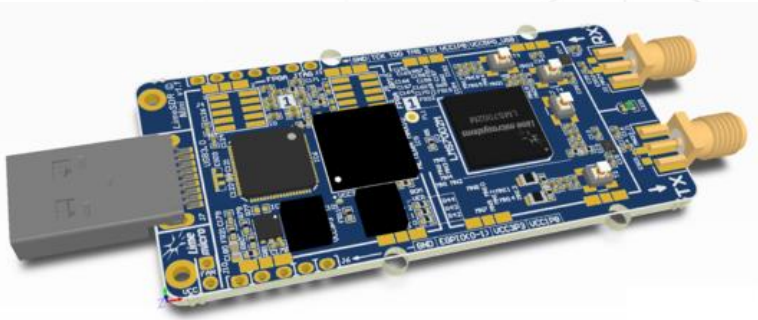
# SDRs


CLK
RX
TX


HackRF One
GREAT SCOTT GADGETS


USRP B210
RF A
RF B
TX/RX
RX2


RTL-SDR.COM
QUICKSTART SETUP GUIDE: RTL-SDR.COM/QSG
DVB-T+DAB+FM+SDR
RTL2832U R820T2 TCXO+BIAS T+HF
V.3



# Other SDRs

- RTL SDR – from RTLSDR blog
- Hack RF One – from Great Scotts Gadget
- Blade RF – from Nuand
- USRP – from Ettus Research
- LimeSDR from Limemicrosystems


# Let’s begin SIGNAL HUNTING ….


# Thank You!

HITB LOCKDOWN 002
livestream

Ateet Kumar, ateetkumarofficial@gmail.com