A PROJECT REPORT ON

DUAL BAND CELL PHONE JAMMER

2013-14

SUBMITTED BY

Afzal Ibrahim	11509
Momin Muzammil	11512
Khan Mohammed Khalid	11520
Mohsin Khan	11521

GUIDED BY

PROF.NIYAZ KHAN

Department Of
Electronics and Telecommunication
Engineering

M.H.SABOO SIDDIK POLYTECHNIC
Byculla, Mumbai-400008

M.H.SABOO SIDDIK POLYTECHNIC
Byculla, Mumbai-400008

CERTIFICATE

This is to certify that the project entitled

DUAL BAND CELL PHONE JAMMER

SUBMITTED BY

Afzal Ibrahim	11509
Momin Muzammil	11512
Khan Mohammed Khalid	11520
Mohsin Khan	11521

Have satisfactorily completed the same as a partial fulfilment of the project work of the **Diploma in Electronics End Telecommunication Engineering** as per the curriculum specified by **M.S.B.T.E**. Mumbai during the Academic year **2013-14** for final year diploma engineering,

Prof. Niyaz Khan
(Guide)

Prof. Niyaz Khan
(H.O.D)

Prof. Javed Akhtar
(Principal)

EXTERNAL EXAMINER

Acknowledgement

It is indeed a matter of great pleasure and privilege to be able to present this report on dual band cell phone jammer under the valuable guidance of Prof. Niyaz Khan, professor and faculty of electronics and telecommunication engineering, M.H.Saboo Siddik Polytechnic, Byculla, Mumbai-400008.

We would like to express our deep sense of gratitude to our guide for his valuable guidance, advice and constant to our work. We are also thankful to our honourable principal prof. Javed Akhtar who made all facilities for us in college premises. We are obliged. It has been great fun to work together with the problems related with project, financial support from our parents is gratefully acknowledge.

I would like to thanks my parents for their understanding and support during these days. Many many thanks to our group member for their patience, encouragement among us.

INDEX

Chapter 1

Introduction

1. Introduction

This report presents the design, implementation, and testing of a dual-band cell-phone jammer. This jammer works at GSM 900 and GSM 1800 simultaneously and thus jams the three well-known carriers in India. This project went through two phases:

Phase one: studying the GSM-system to find the best jamming technique, establishing the system design and selecting suitable components.

Phase two: buying all the needed components, drawing the overall schematics, fabricating the PCB layout, assembling the devices, performing some measurements and finally testing the mobile jammer.

The designed jammer was successful in jamming the three carriers in India, as will be shown at the end of this report.

Communication jamming devices were first developed and used by military. This interest comes from the fundamental objective of denying the successful transport of information from the sender (tactical commanders) to the receiver (the army personnel), and vice-versa. Nowadays, mobile (or cell) phones are becoming essential tools in our daily life. Here in Jordan, for example, with a rather low population (around 5 million), three main cell phone carries are available; namely; the first two use the GSM 900 system, while the third uses the GSM 1800 system. Needless to say, the wide use of mobile phones could create some problems as the sound of ringing becomes annoying or disrupting. This could happen in some places like conference rooms, law courts, libraries, lecture rooms and mosques. One way to stop these disrupting ringings is to install device in such places which will inhibit the use of mobiles, i.e., make them obsolete. Such a device is known as cell phone jammer or "GSM jammer", which is basically some kind of electronic countermeasure device.

The technology behind cell phone jamming is very simple. The jamming device broadcasts an RF signal in the frequency range reserved for cell phones that interferes with the cell phone signal, which results in a "no network available" display on the cell phone screen. All phones within the effective radius of the jammer are silenced. It should be mentioned that cell phone jammers are illegal devices in most countries. According to the Federal Communications Commission (FCC) in the USA: "The manufacture, importation, sale, or offer for sale, of devices designed to block or jam wireless transmissions is prohibited". However, recently, there has been an increasing demand for portable cell phone jammers. We should mention that this project, presented in this report, is solely done for educational purposes. There is no intention to manufacture or sell such devices in India, or elsewhere. In this project, a device that will jam both GSM 900 and GSM 1800 services will be designed, built, and tested.

1.2 Jamming Techniques

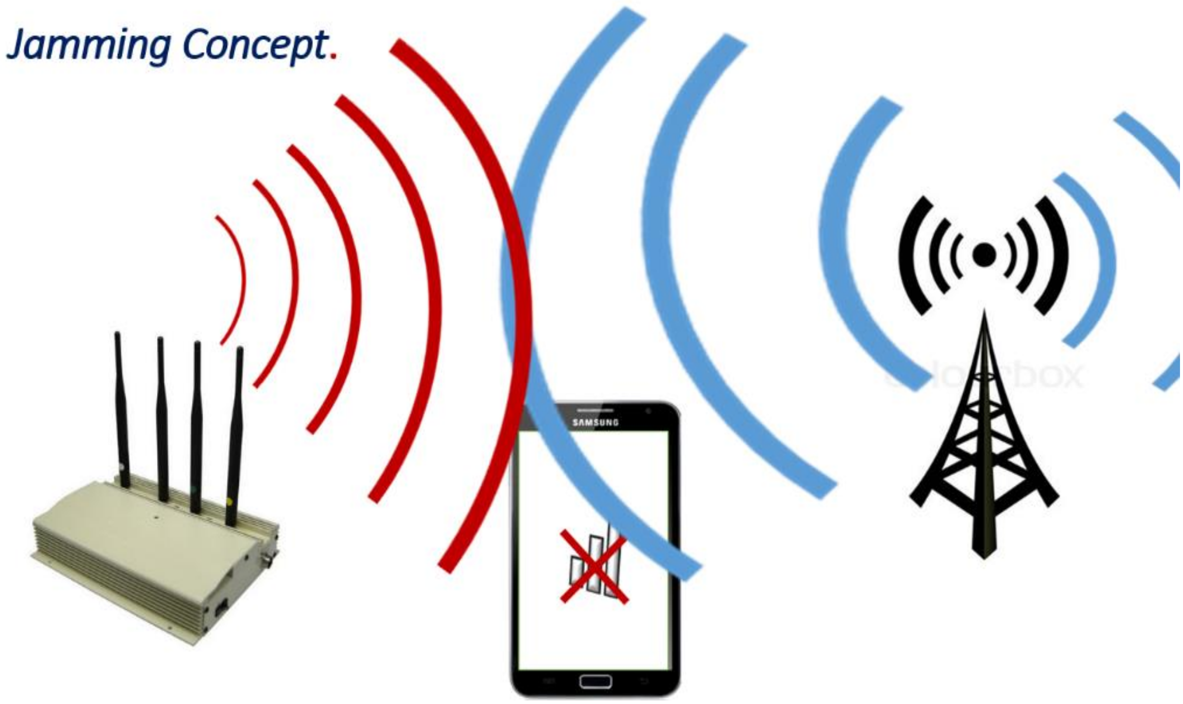
There are several ways to jam an RF device. The three most common techniques can be categorized as follows:

A) Spoofing

In this kind of jamming, the device forces the mobile to turn off itself. This type is very difficult to be implemented since the jamming device first detects any mobile phone in a specific area, then the device sends the signal to disable the mobile phone. Some types of this technique can detect if a nearby mobile phone is there and sends a message to tell the user to switch the phone to the silent mode (Intelligent Beacon Disablers).

B) Shielding Attacks

This is known as TEMPEST or EMF shielding. This kind requires closing an area in a faraday cage so that any device inside this cage can not transmit or receive RF signal from outside of the cage. This area can be as large as buildings, for example.



C) Denial of Service

This technique is referred to DOS. In this technique, the device transmits a noise signal at the same operating frequency of the mobile phone in order to decrease the signal-to-noise ratio (SNR) of the mobile under its minimum value. This kind of jamming technique is the simplest one since the device is always on. Our device is of this type.

1.2 Design Parameters

Based on the above, our device which is related to the DOS technique is transmitting noise on the same frequencies of the two bands GSM 900 MHz, and GSM 1.8 GHz (known also as DCS 1800 band). We focused on some design parameters to establish the device specifications. These parameters are as follows:

A) The distance to be jammed (D)

This parameter is very important in our design, since the amount of the output power of the jammer depends on the area that we need to jam. Later on we will see the relationship between the output power and the distance D. Our design is established upon D=10 meters for DCS 1800 band and D=20 meters for GSM 900 band.

B) The frequency bands

In our design, the jamming frequency must be the same as the downlink, because it needs lower power to do jamming than the uplink range and there is no need to jam the base station itself. So, our frequency design will be as follows:

GSM 900 935-960 MHz

GSM 1800 1805-1880 MHz

C) Jamming-to-signal ratio {J/S}

Jamming is successful when the jamming signal denies the usability of the communication transmission. In digital communications, the usability is denied when the error rate of the transmission cannot be compensated by error correction. Usually, a successful jamming attack requires that the jammer power is roughly equal to signal power at the receiver (mobile device).

The general equation of the jamming-to-signal ratio is given as follows:

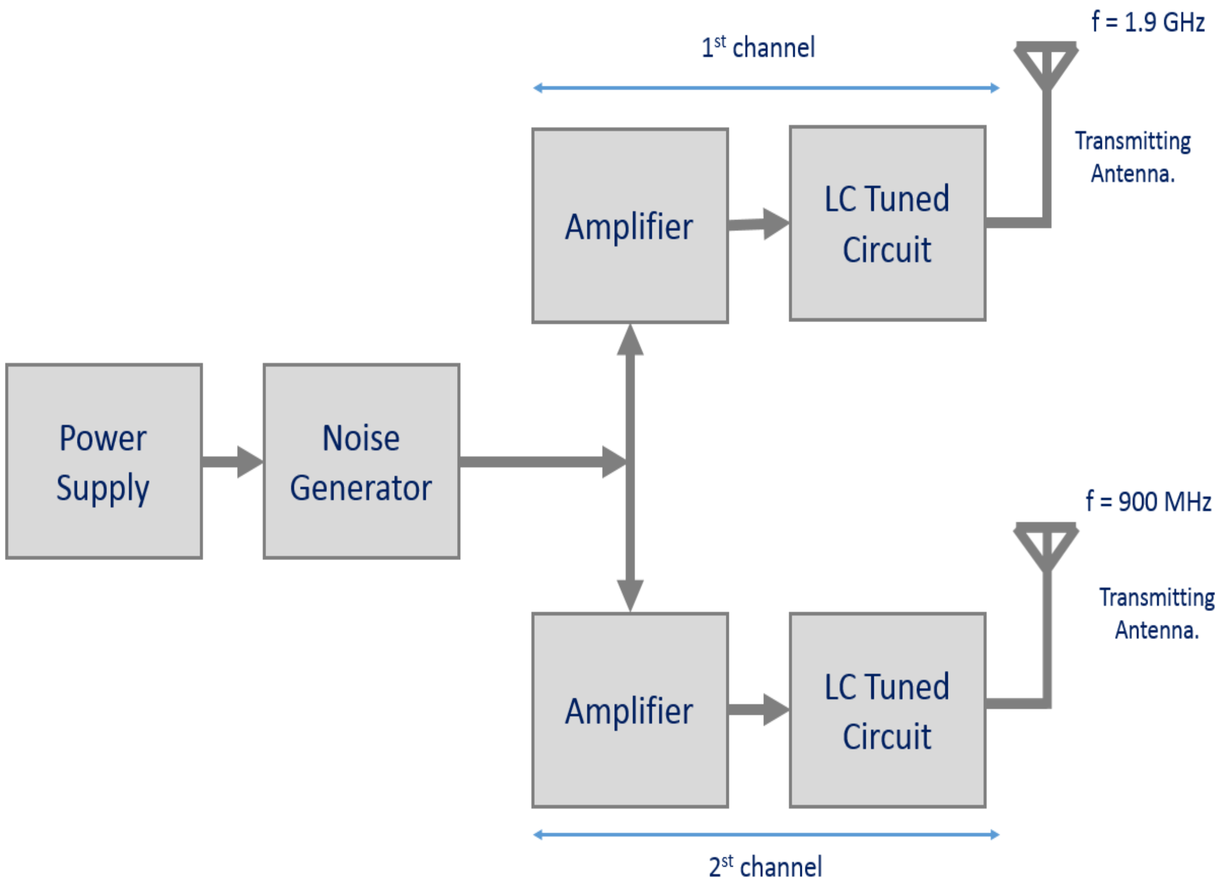
$$\frac{J}{S} = \frac{P_j G_{jr} G_{rj} R_{tr}^2 L_r B_r}{P_t G_{tr} G_{rt} R_{jr}^2 L_j B_j}$$

where: Pj=jammer power, Gjr= antenna gain from jammer to receiver, Grj=antenna gain from receiver to jammer, Rtr=range between communication transmitter and receiver, Br=communication receiver bandwidth,Lr =communication signal loss, Pt=transmitter power, Gtr= antenna gain from transmitter to receiver, Grt=antenna gain from receiver to transmitter, Rjr= range between jammer and communication receiver, Bj=jammer bandwidth, and Lj=jamming signal loss.

For GSM, the specified system SNRmin is 9 dB which will be used as the worst case scenario for the jammer. The maximum power at the mobile device Pr is -15 dBm.

Chapter 2
Block diagram

Block Diagram



Power supply: We Have Used 15V Power Supply, Dc .

Noise generator: It Produce Noise Signal of Frequency Approximately 10MHz, Noise Generator Is Built on IC 555. IC 555 Is In Astable Mode**.**

The output of noise generator is given to two separate channels, each channel consist of an amplifier and lC tuned oscillator.

Amplifier and lc tuned oscillator amplify the resonance frequency.

The first channel as output of frequency 1.9GHz,

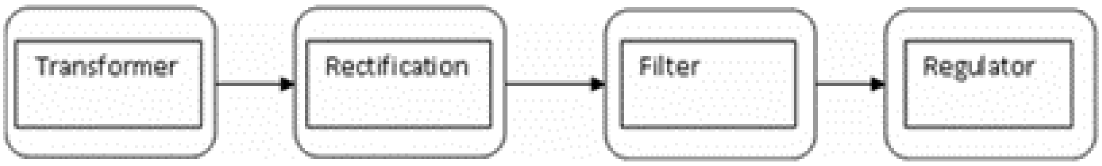
The second channel as output of frequency 900MHz, which is required to jam a signal within specific range. Hence it is a dual band cell phone jammer.

The Power supply

This is used to supply the other sections with the needed voltages. Any power supply consists of the following main parts:

Transformer: - is used to transform the 220VAC to other levels of voltages.

Rectification: - this part is to convert the AC voltage to a DC one. We have two methods for rectification:



A] Half wave-rectification: the output voltage appears only during positive cycles of the input signal.

B] Full wave -rectification: a rectified output voltage occurs during both the positive and negative cycles of the input signal.

The Filter: used to eliminate the fluctuations in the output of the full wave rectifier “eliminate the noise” so that a constant DC voltage is produced. This filter is just a large capacitor used to minimize the ripple in the output.

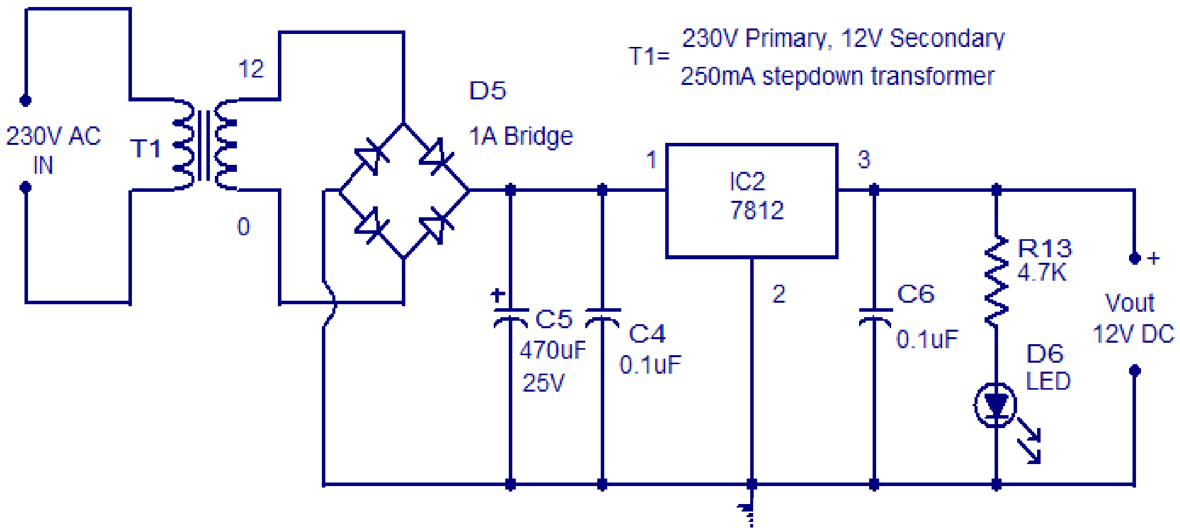
Regulator: this is used to provide a desired DC-voltage. Figure 2 shows the general parts of the power supply.

Specification of Parts Required In Power Supply

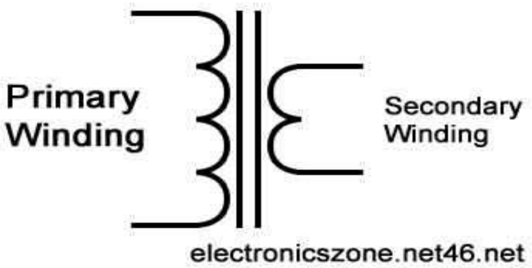
A) Step down Transformer;

What is a step down transformer: is one whose secondary voltage is less than its primary voltage. It is designed to reduce the voltage from the primary winding to the secondary winding. This kind of transformer “steps down” the voltage applied to it’s a step-down unit, the transformer converts high-voltage, low-current power into low-voltage, high-current power. The larger-gauge wire used in the secondary winding is necessary due to the increase in current. The primary winding, which doesn’t have to conduct as much current, may be made of smaller-gauge wire.

We have used a 15V, 1 Amp Step down Transformer



12V DC power supply



B) IC 7815: Positive Voltage Regulator IC.

TheLM78XX series of three terminal regulators is available with several fixed output voltages making them useful in a wide range of applications. One of these is local on card regulation, eliminating the distribution problems associated with single point regulation. The voltages available allow these regulators to be used in logic systems, instrumentation, HiFi, and other solid state electronic equipment. Although designed primarily as fixed voltage regulators these devices can be used with external component s to obtain adjustable voltages and currents.

Specifications

Product Category: Linear Regulators - Standard

Polarity: Positive

Number of Outputs: Single

Output Type: Fixed

Output Voltage: 15 V

Output Current: 1.5 a

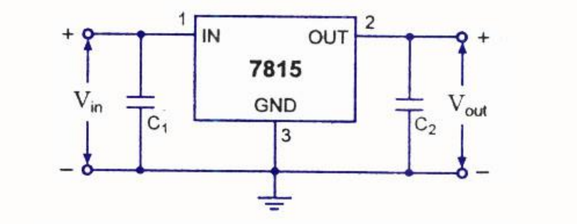
Line Regulation: 300 mV

Load Regulation: 300 mV

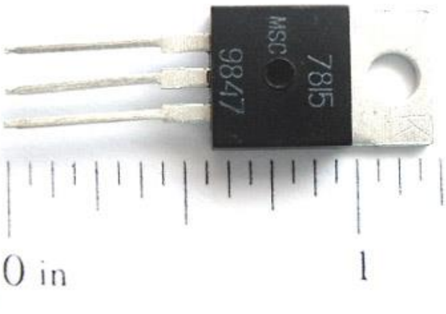
Dropout Voltage (Max): 2.5 V @ 1A

Maximum Operating Temperature: + 150 C

Minimum Operating Temperature: 0 C

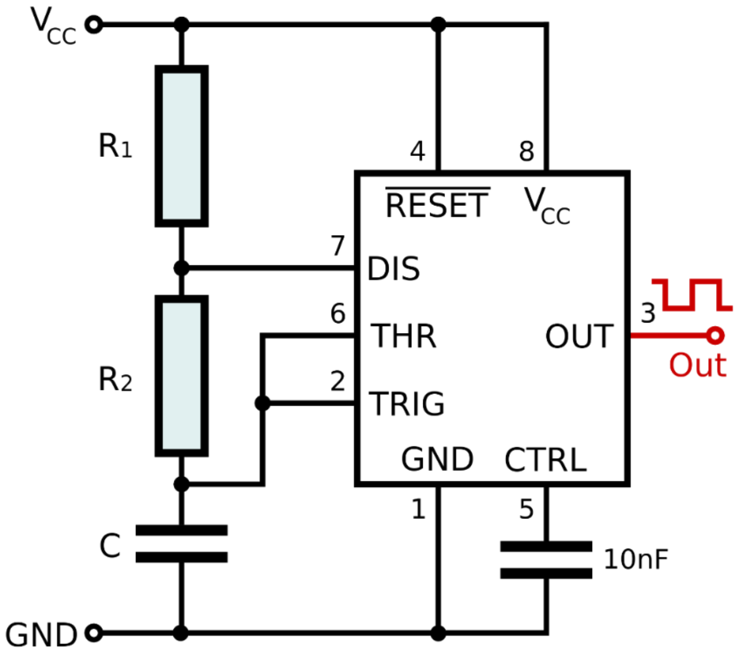


Connection of 7815 Voltage Regulator



Noise Generator Using IC 555.

The IC 555 Is In Astable Mode.



In astable mode, the 555 timer puts out a continuous stream of rectangular pulses having a specified frequency. Resistor R_1 is connected between $V_{CC}$and the discharge pin (pin 7) and another resistor (R_2) is connected between the discharge pin (pin 7), and the trigger (pin 2) and threshold (pin 6) pins that share a common node. Hence the capacitor is charged through R_1 and R_2, and discharged only through R_2, since pin 7 has low impedance to ground during output low intervals of the cycle, therefore discharging the capacitor

In the astable mode, the frequency of the pulse stream depends on the values of R_1, R_2 and C:

$$f = \frac{1}{\ln(2) \cdot C \cdot (R_1 + 2R_2)}$$

Class A Amplifier

Amplifying devices operating in class A conduct over the entire range of the input cycle. A class-A amplifier is distinguished by the output stage devices being biased for class A operation. Subclass A2 is sometimes used to refer to vacuum-tube class-A stages where the grid is allowed to be driven slightly positive on signal peaks, resulting in slightly more power than normal class A (A1; where the grid is always negative[9]), but this incurs a higher distortion level.

Advantages of class-A amplifiers

Class-A designs are simpler than other classes; for example class -AB and -B designs require two connected devices in the circuit (push–pull output), each to handle one half of the waveform; class A can use a single device (single-ended).

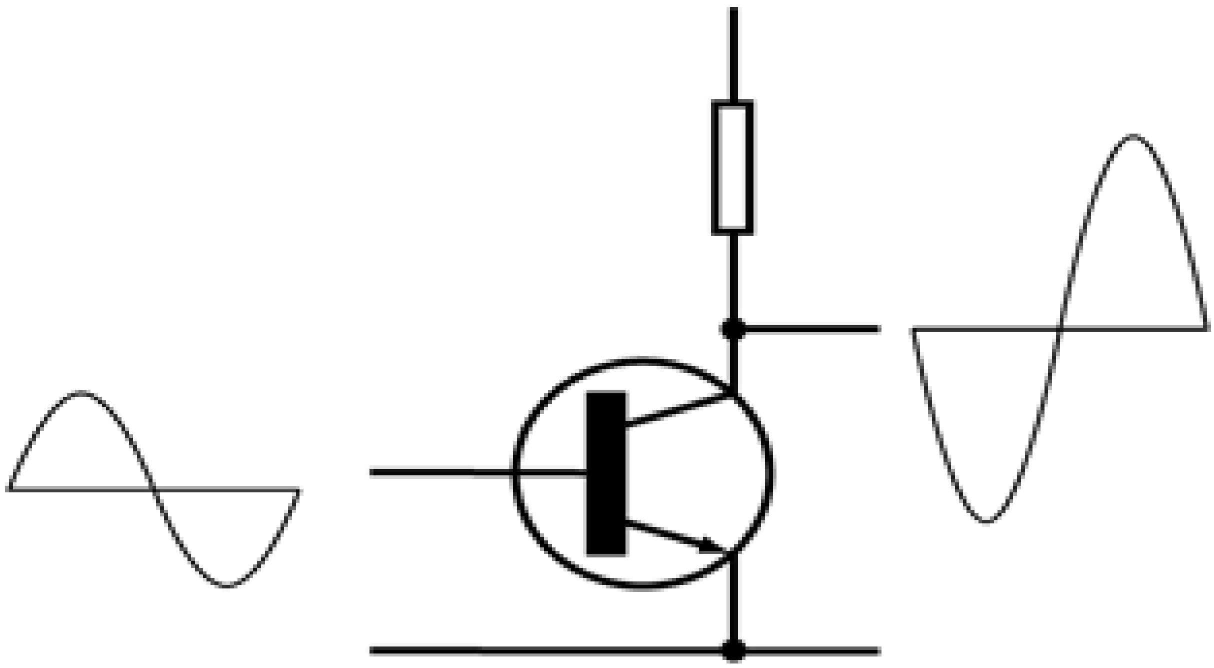
The amplifying element is biased so the device is always conducting, the quiescent (small-signal) collector current (for transistors; drain current for FETs or anode/plate current for vacuum tubes) is close to the most linear portion of its trans conductance curve.

Because the device is never 'off' there is no "turn on" time, no problems with charge storage, and generally better high frequency performance and feedback loop stability (and usually fewer high-order harmonics).

The point at which the device comes closest to being 'off' is not at 'zero signal', so the problems of crossover distortion associated with class-AB and -B designs is avoided

Class-A amplifiers are inefficient. A theoretical efficiency of 50% is obtainable with transformer output coupling and only 25% with capacitive coupling, unless deliberate use of nonlinearities is made (such as in square-law output stages). In a power amplifier, this not only wastes power and limits operation with batteries, but increases operating costs and requires higher-rated output devices. Inefficiency comes from the standing current that must be roughly half the maximum output current, and a large part of the power supply voltage is present across the output device at low signal levels. If high output power is needed from a class-A circuit, the power supply and accompanying heat becomes significant. For every watt delivered to the load, the amplifier itself, at best, uses an extra watt. For high power amplifiers this means very large and expensive power supplies and heat sinks.

Class-A power amplifier designs have largely been superseded by more efficient designs, though they remain popular with some hobbyists, mostly for their simplicity. There is a market for expensive high fidelity class-A amps considered a "cult item" amongst audiophiles [10] mainly for their absence of crossover distortion and reduced odd-harmonic and high-order harmonic distortion.

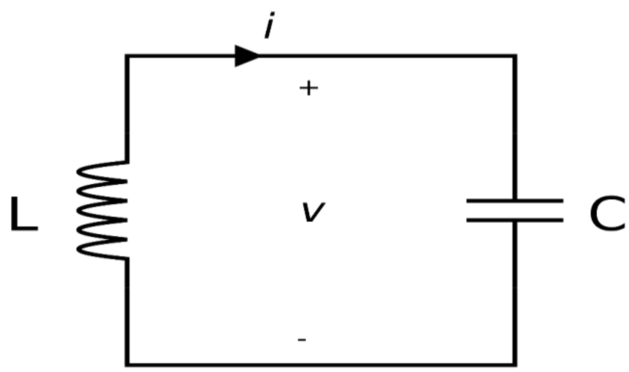


LC TUNED CIRCUIT.

In electronics an LC circuit, also called a resonant circuit, tank circuit, or tuned circuit, consists of two electronic components connected together; an inductor, represented by the letter L, and a capacitor, represented by the letter C. The circuit can act as an electrical resonator, an electrical analogue of a tuning fork, storing energy oscillating at the circuit's resonant frequency.

LC circuits are used either for generating signals at a particular frequency, or picking out a signal at a particular frequency from a more complex signal. They are key components in many electronic devices, particularly radio equipment, used in circuits such as oscillators, filters, tuners and frequency mixers.

An LC circuit is an idealized model since it assumes there is no dissipation of energy due to resistance. Any practical implementation of an LC circuit will always include loss resulting from small but non-zero resistance within the components and connecting wires. The purpose of an LC circuit is usually to oscillate with minimal damping, so the resistance is made as low as possible. While no practical circuit is without losses, it is nonetheless instructive to study this ideal form of the circuit to gain understanding and physical intuition. For a circuit model incorporating resistance,



If a charged capacitor is connected across an inductor, charge will start to flow through the inductor, building up a magnetic field around it and reducing the voltage on the capacitor. Eventually all the charge on the capacitor will be gone and the voltage across it will reach zero. However, the current will continue, because inductors resist changes in current. The energy to keep it flowing is extracted from the magnetic field, which will begin to decline. The current will begin to charge the capacitor with a voltage of opposite polarity to its original charge. When the magnetic field is completely dissipated the current will stop and the charge will again be stored in the capacitor, with the opposite polarity as before. Then the cycle will begin again, with the current flowing in the opposite direction through the inductor.

The charge flows back and forth between the plates of the capacitor, through the inductor. The energy oscillates back and forth between the capacitor and the inductor until (if not replenished by power from an external circuit) internal resistance makes the oscillations die out. Its action, known mathematically as a harmonic oscillator, is similar to a pendulum swinging back and forth, or water sloshing back and forth in a tank. For this reason the circuit is also called a **tank circuit**. The oscillation frequency is determined by the capacitance and inductance values. In typical tuned circuits in electronic equipment the oscillations are very fast, thousands to millions of times per second.

The resonance effect occurs when inductive and capacitive reactance's are equal in magnitude. The frequency at which this equality holds for the particular circuit is called the resonant frequency. The resonant frequency of the LC circuit is

$$\omega_0 = \frac{1}{\sqrt{LC}}$$

where L is the inductance in henries, and C is the capacitance in farads. The angular frequency \omega_0\, has units of radians per second.

The equivalent frequency in units of hertz is

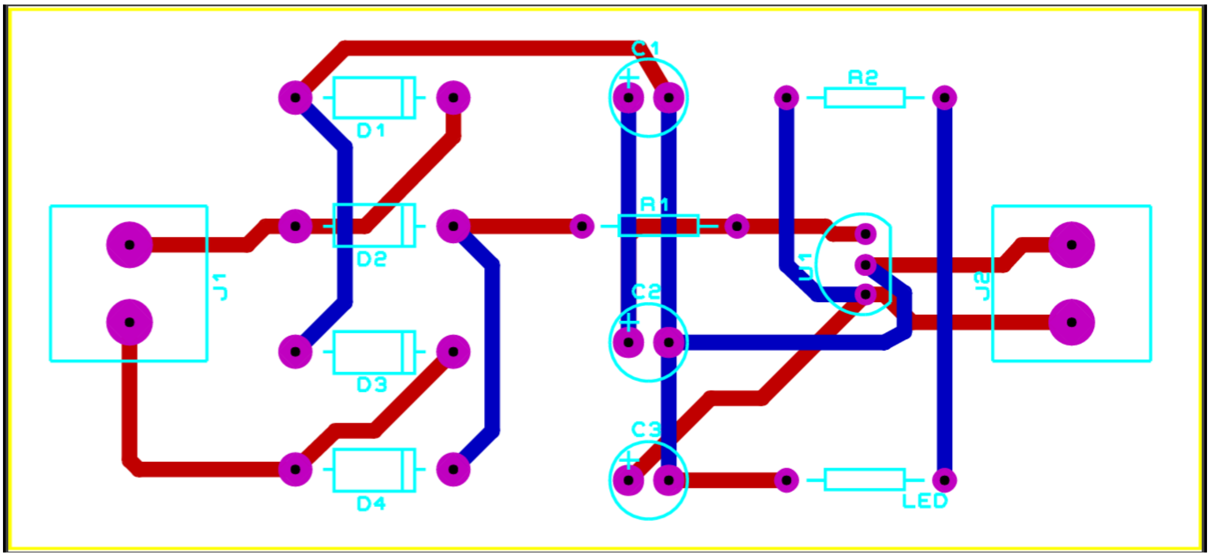
$$f_0 = \frac{\omega_0}{2\pi} = \frac{1}{2\pi\sqrt{LC}}.$$

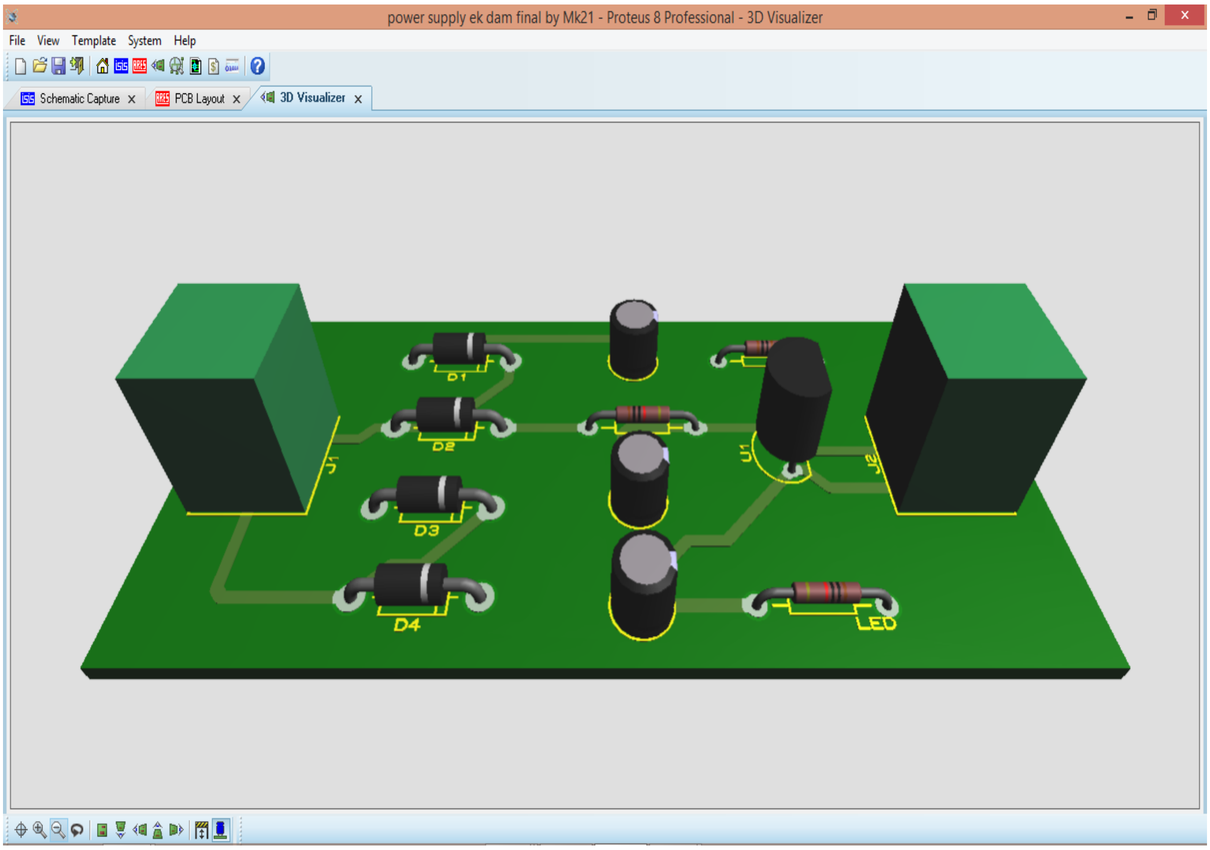
LC circuits are often used as filters; the L/C ratio is one of the factors that determines their "Q" and so selectivity. For a series resonant circuit with a given resistance, the higher the inductance and the lower the capacitance, the narrower the filter bandwidth. For a parallel resonant circuit the opposite applies. Positive feedback around the tuned circuit ("regeneration") can also increase selectivity (see Q multiplier and Regenerative circuit).

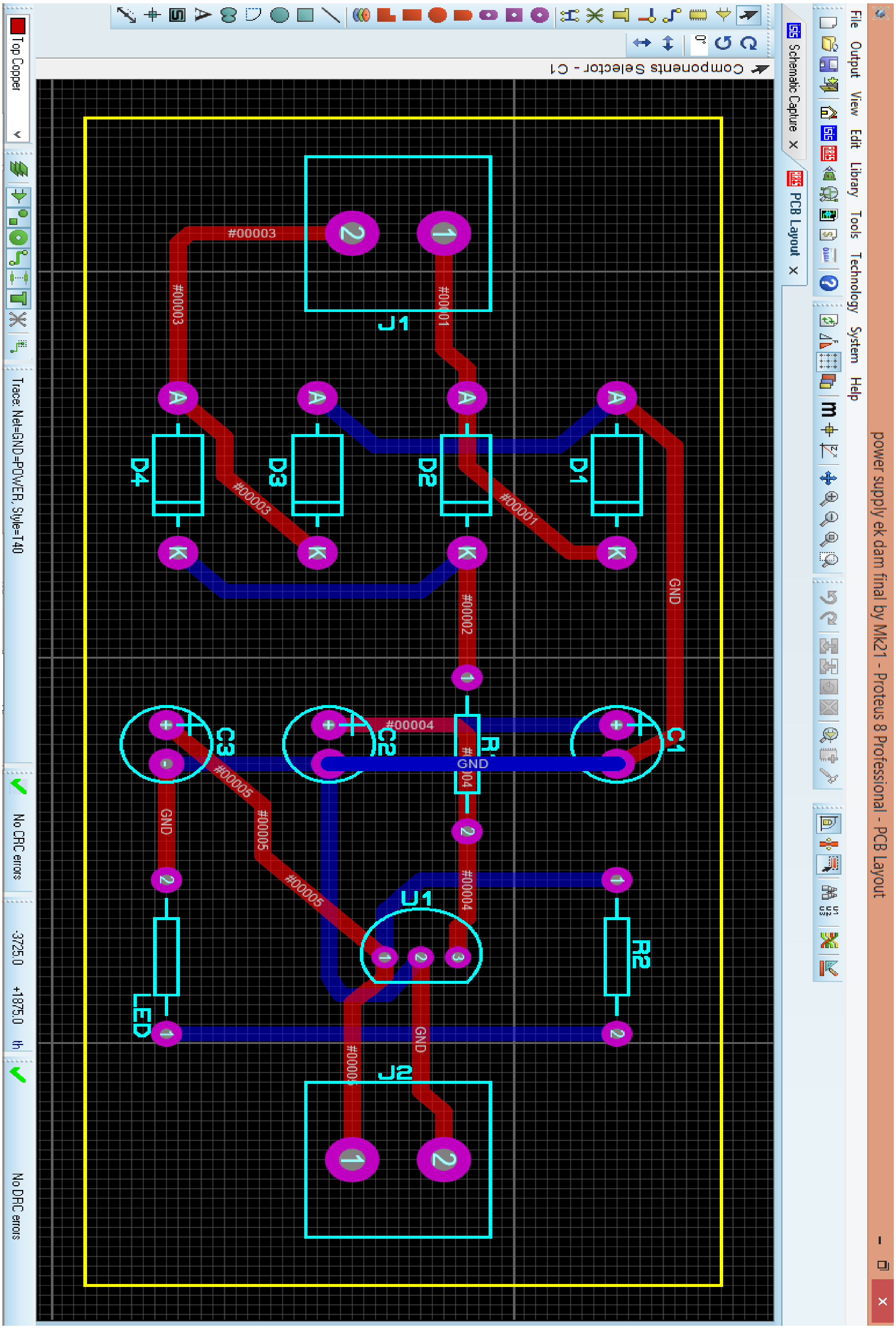
Stagger tuning can provide an acceptably wide audio bandwidth, yet good selectivity.

The most common application of tank circuits is tuning radio transmitters and receivers. For example, when we tune a radio to a particular station, the LC circuits are set at resonance for that particular carrier frequency.

This layout was made on PROTEUS 8 software by our team

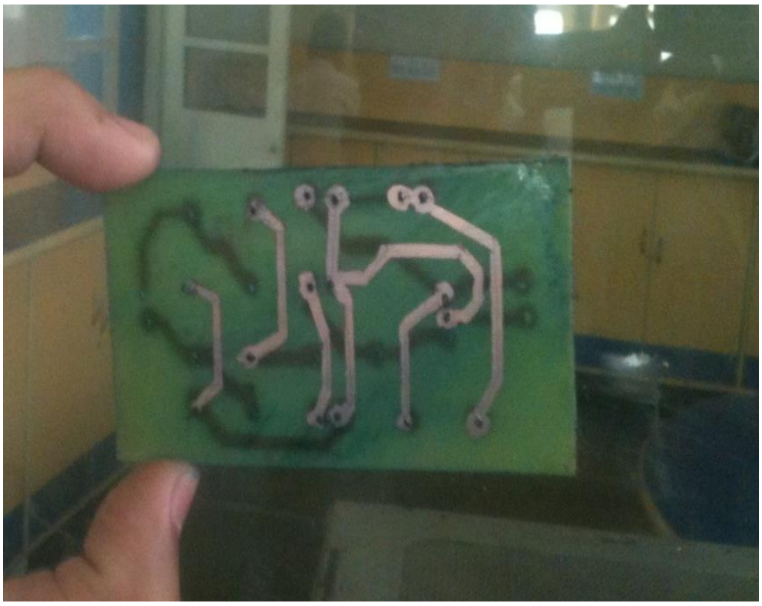


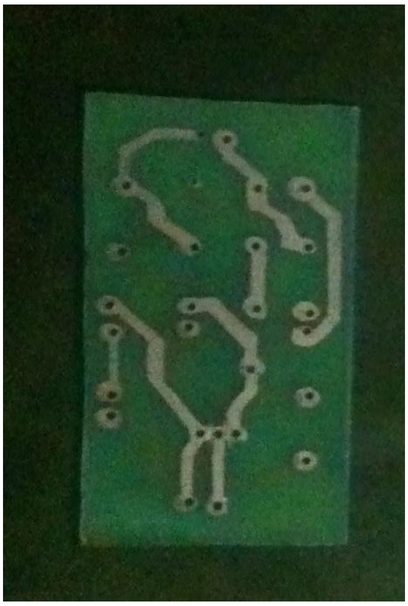


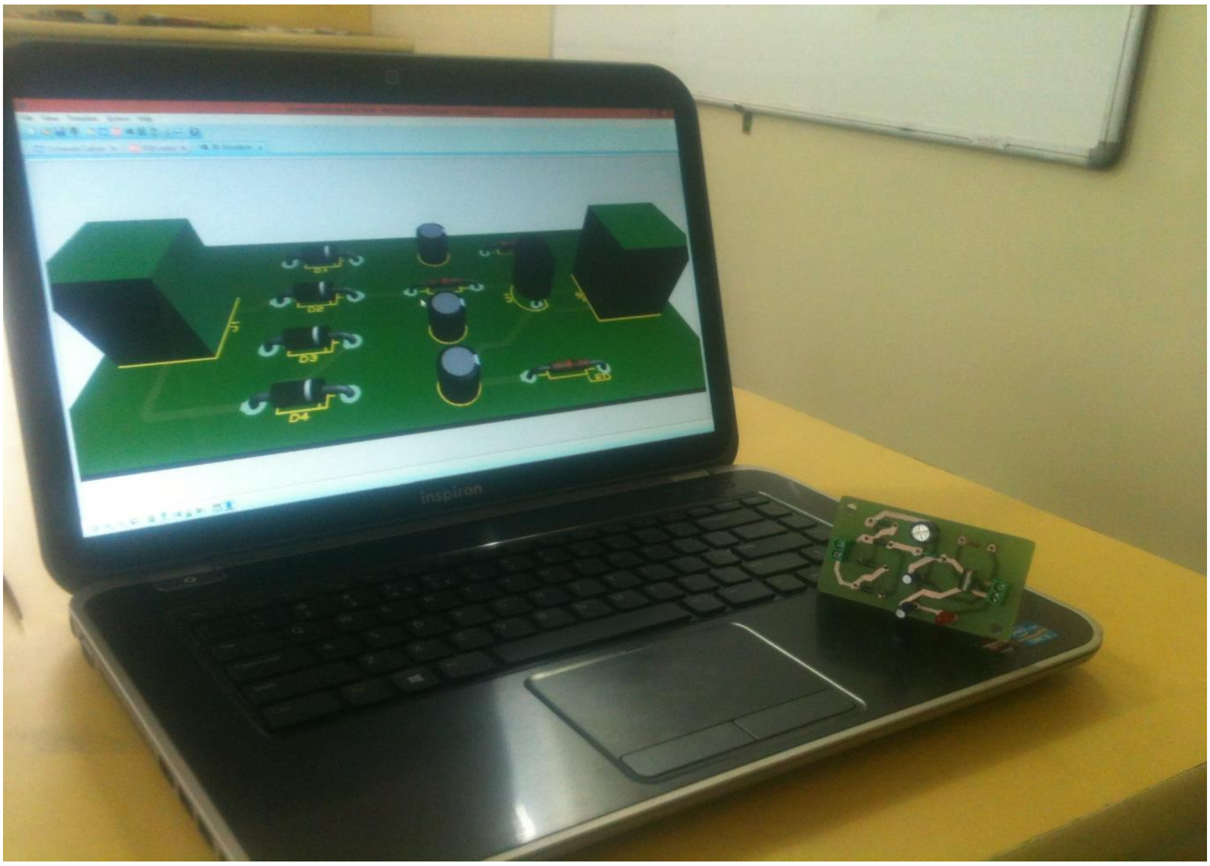

power supply ek dam final by Mk21 - Proteus 8 Professional - PCB Layout
File Output View Edit Library Tools Technology System Help
Schematic Capture
PCB Layout
Components Selector - C1
J1
J2
D1
D2
D3
D4
C1
C2
C3
R2
U1
LED
#00001
#00002
#00003
#00004
#00005
GND
Top Copper
Trace: Net=GND=POWER, Style=T40
No CRC errors
-3725.0 +1875.0
No DRC errors

Making of Power Supply.

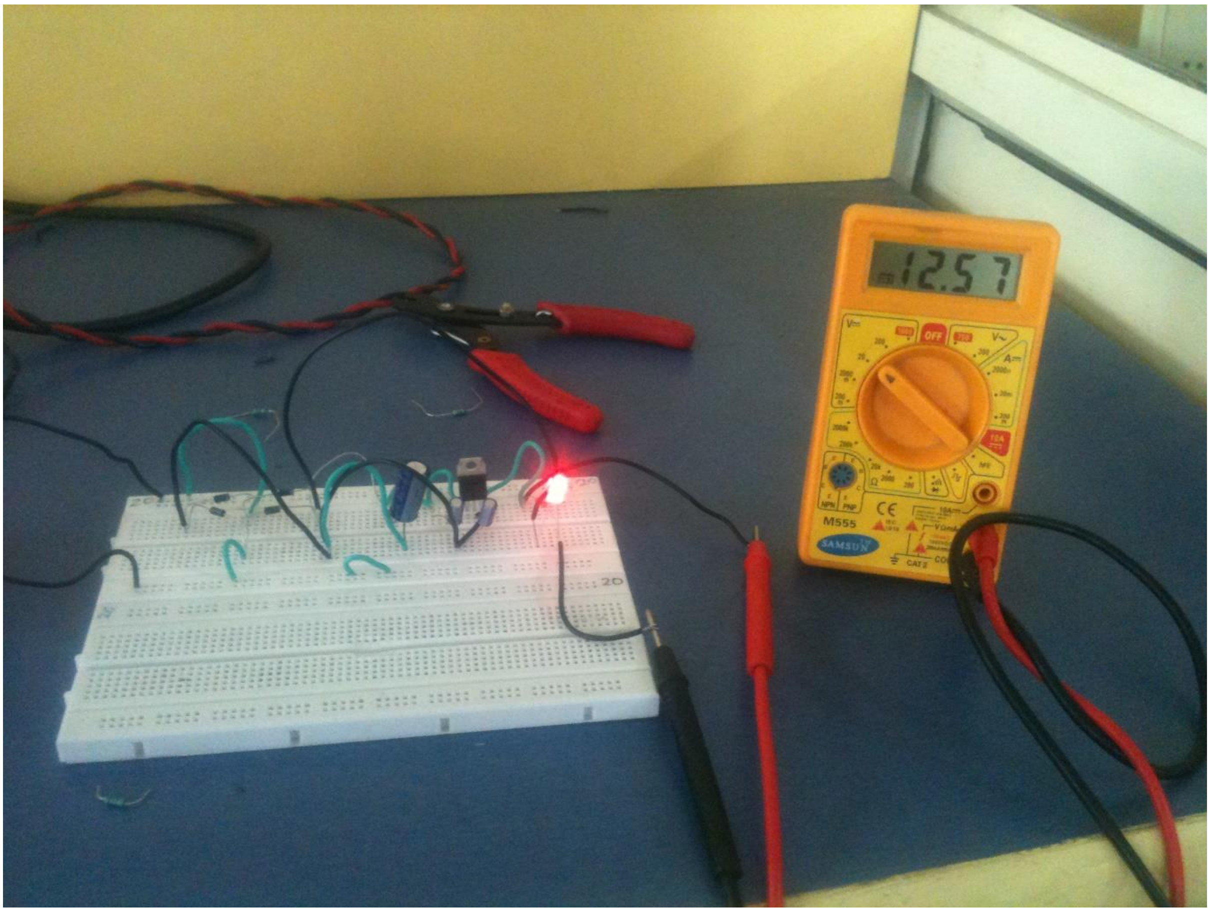
We have Used Dua[redacted]l Side PCB for Making Power Supply.







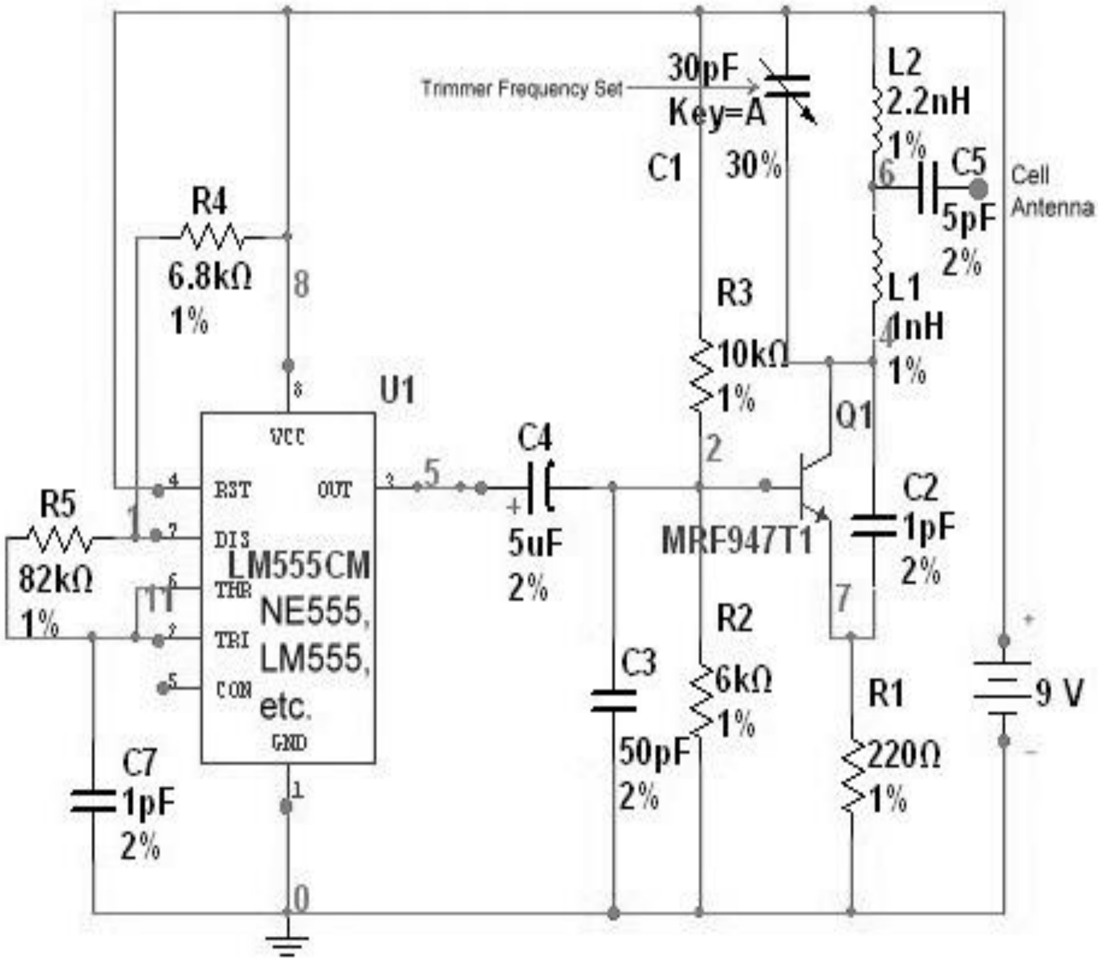
Testing of power supply.



4.2 Cell phone jammer

A "Cell Jammer" is just way of saying "Dirty Transmitter" which happens to transmit within the Cellular Phone Bands. Reality is, the dirtier the better. The 555 timer [8 pin] IC simply makes a noise. It's coupled via C4 [electrolytic] to modulate the MRF transistor oscillator. With C1 set at roughly 1/3rd, you will be close to 900 MHz's by sweeping the C1 trimmer capacitor, you can swing the output frequency from 800 MHz to 2 GHz with the transistor and values shown. You could replace the 555 chip with an electret microphone and listen to yourself talk on a scanner, so the unit could easily couple as a UHF Bug. Instead of a single Tapped Coil, I've used two molded inductors for ease of construction. Values for C1, C2, L1, and L2 are critical for the frequency range. You might want to build the unit into a metal box, add an on/off switch in the batteries + line, and maybe even add a LED. Connect an old 800 MHz cell phone antenna to C5. Would you believe the whole thing can be built on top of the 555 IC itself when using surface mount components, and the lot will fit onto a nine volt battery clip. Output is reasonably good, although the current drain is a bit high, so battery The "Cell Kill Distance" is around 10 – 15 feet, ample for most purposes.

Initial Circuit Diagram.

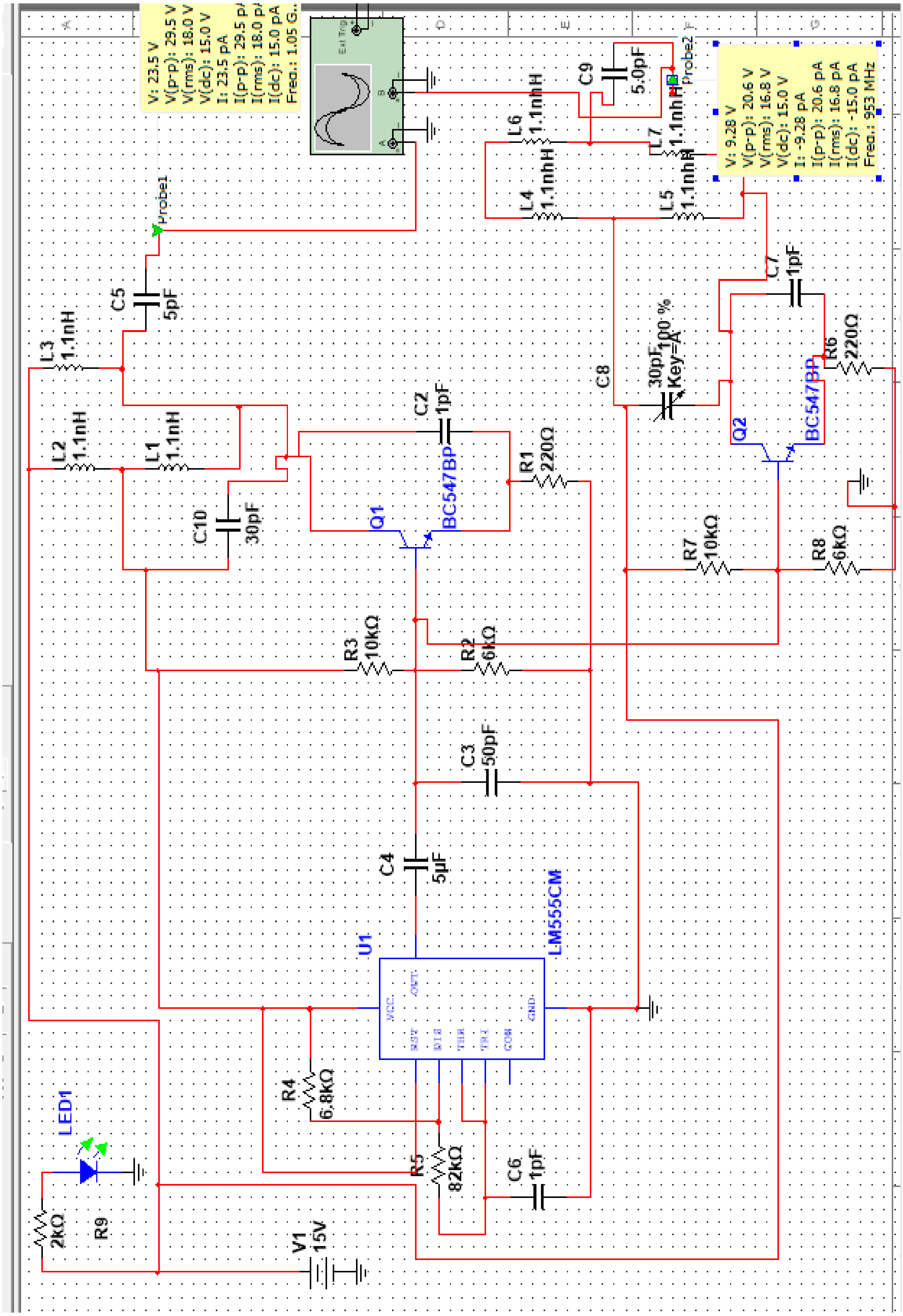


This was the initial circuit diagram which we get from internet, its gives us 900mhz frequency noise signal on simulation .But as we want to build dual band cell phone jammer , so we have modified the circuit to get dual band frequency signal .

First band = 900 MHz

Second band = 1.8 GHz

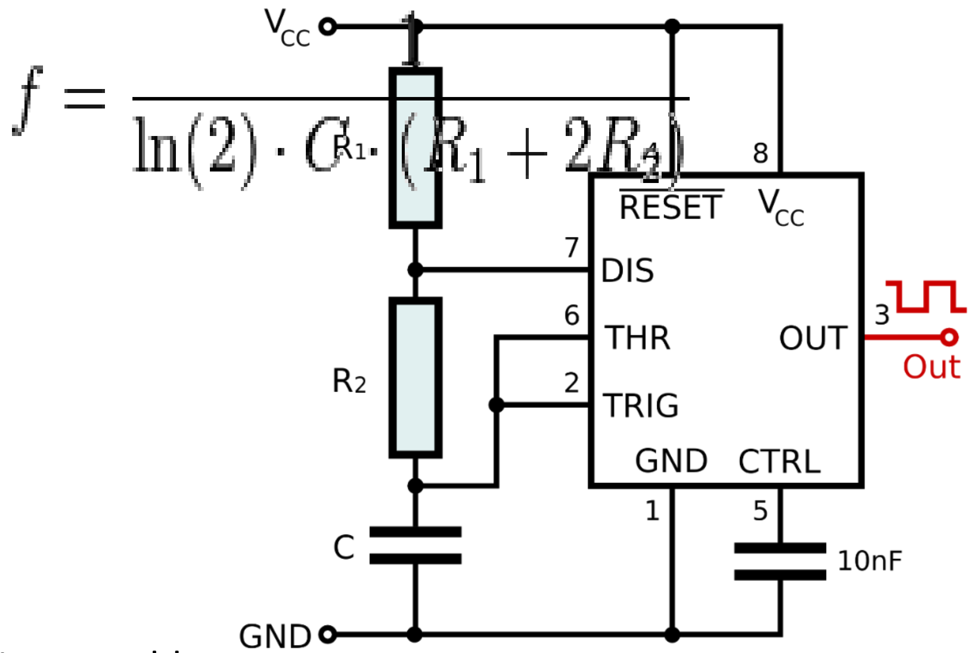
Modified circuit diagram.



Noise Generator Using IC 555.

The IC 555 Is In Astable Mode.

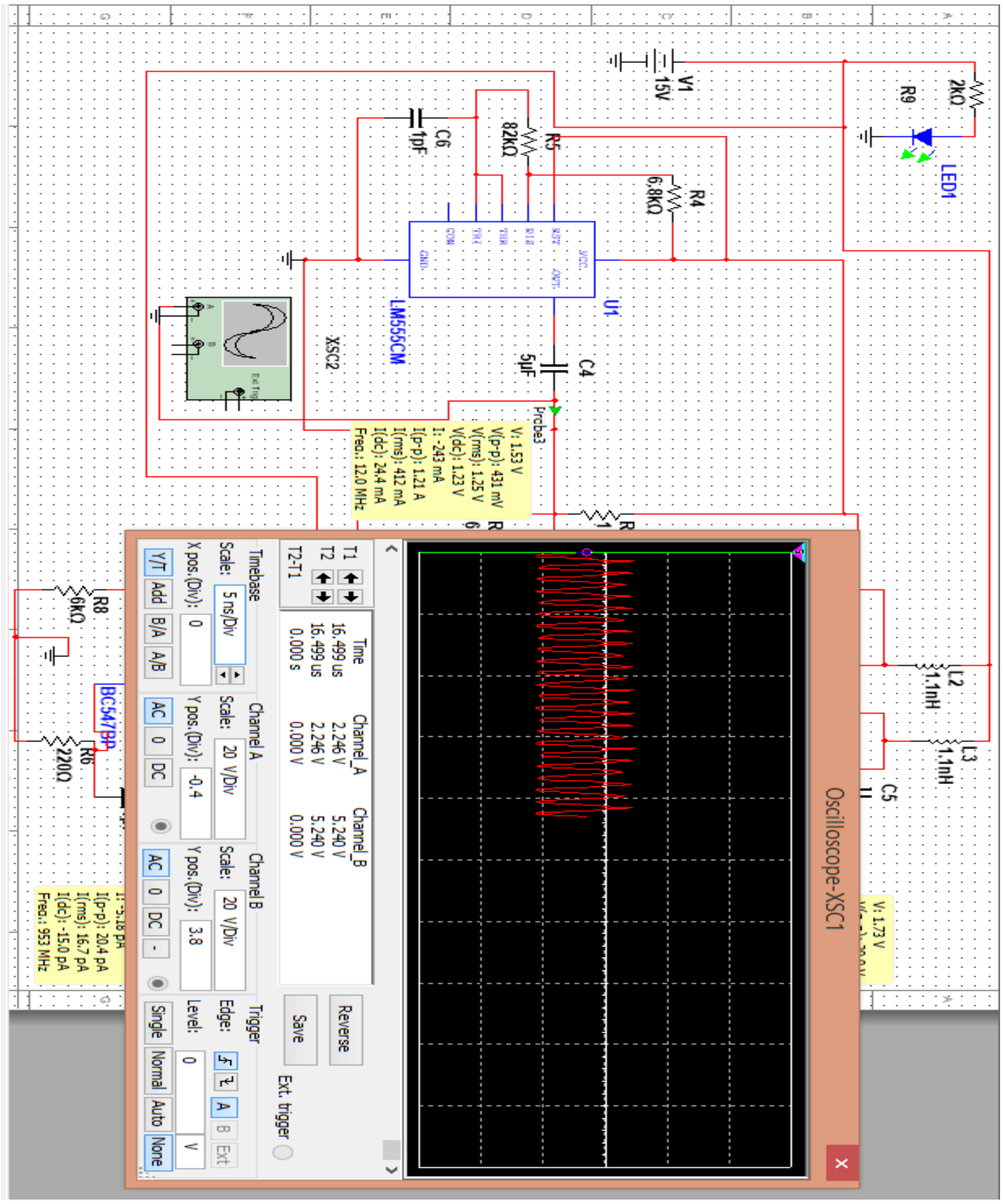
$$f = \frac{1}{\ln(2) \cdot C \cdot (R_1 + 2R_2)}$$



In astable mode, the 555 timer puts out a continuous stream of rectangular pulses having a specified frequency. Resistor R_1 is connected between $V_{CC}$and the discharge pin (pin 7) and another resistor (R_2) is connected between the discharge pin (pin 7), and the trigger (pin 2) and threshold (pin 6) pins that share a common node. Hence the capacitor is charged through R_1 and R_2, and discharged only through R_2, since pin 7 has low impedance to ground during output low intervals of the cycle, therefore discharging the capacitor.

In the astable mode, the frequency of the pulse stream depends on the values of R_1, R_2 and C:

We have getting approximately 12 MHz frequency at the output of noise generator.



We have used an class A amplifier with LC tuned oscillator.