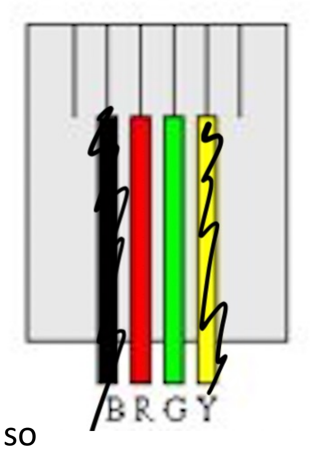
EPQ Add-on

Daniel Rezaie

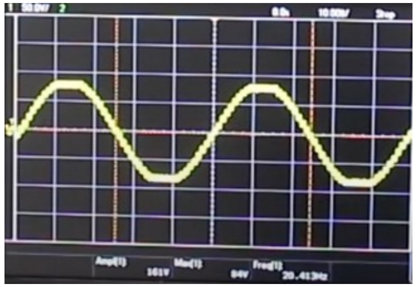
Preliminary Warning

- This project was done with sufficient knowledge of electrical systems, the phoneline and safety.
- All steps were taken to ensure safety
- All tests and presentations were done on a PERSONAL mimic phone network, NOT THE PUBLIC OPENREACH NETWORK, which will be shown later on in the presentation

The phone line

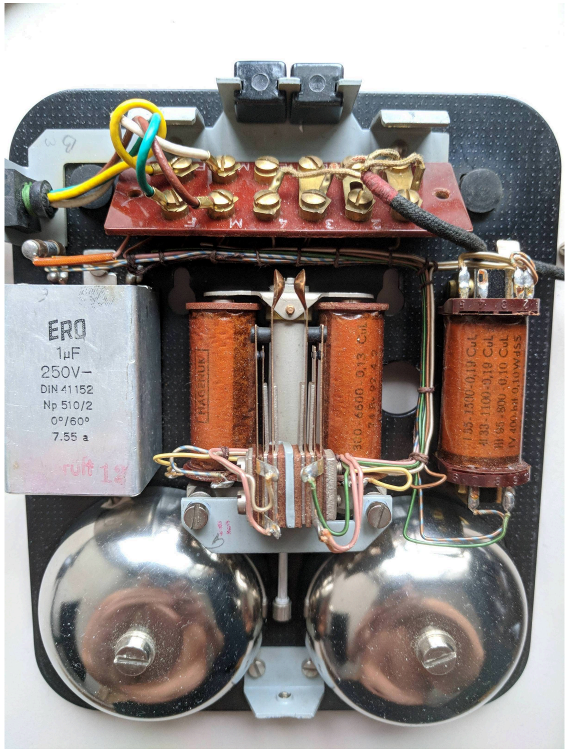


- Firstly, I stripped the end of an rj-14 phone cable and cut off the yellow and black wires as shown in the diagram to turn it into an rj-11 cable
- Before starting I already new that the bare phone lines were going to be relatively harmless so I took the appropriate measures to keep myself safe e.g. having dry hands to increase any possible bodily resistance so that in the case of shock the current will be limited to a safe amperage.
- Then I plugged it in making sure that the 2 conductors could not touch each other.
- The two remaining cables, Green and Red, are know as the tip and ring contacts, respectively.
- Over these 2 wires was a potential difference or voltage of around 48 volts D.C. which is a harmless voltage and relatively safe when in contact with skin
- While testing I saw that voltage jumped to 60 volts R.M.S. when the phone line was ringing. So, I switched my multimeter out for my oscilloscope because it has an AC mode and redialled the line with my mobile phone to simulate a call. On the AC mode my oscilloscope showed a peak to peak of around 160 Volts with a 20 Hz frequency. This voltage is quite high so you must be very careful to not touch either of the bare cable ends or let them touch each other or other items such as grounded equipment as it could possibly damage the telephone exchanges circuitry.



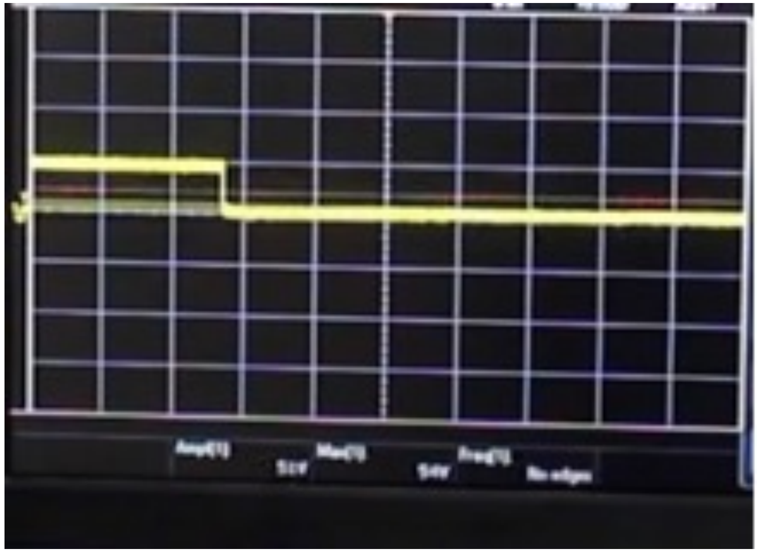
History of the phone lines

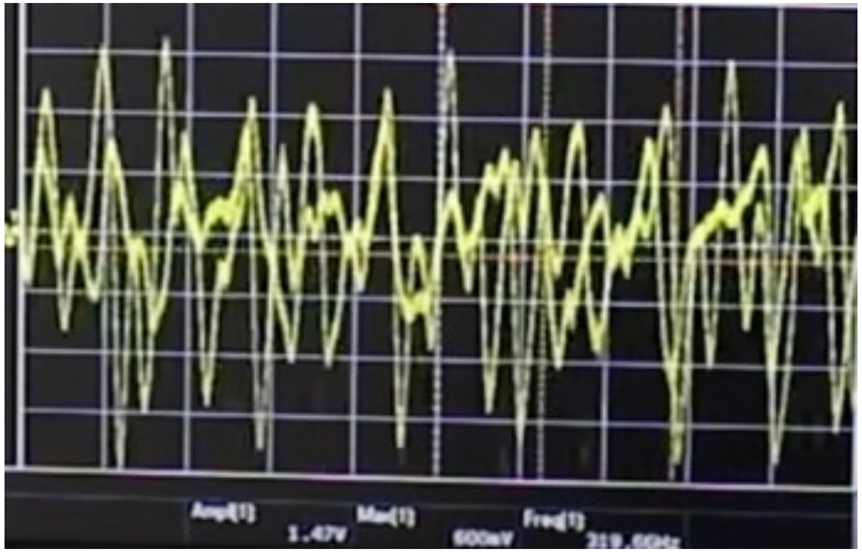
- You may be wondering why there is such a high AC voltage to signal the ringing of the line. This is because the phone lines are maintained in a way to maintain backwards compatibility with older phones such as those ones which had 2 actual bells inside with a hammer attached to a coil of wire which created a magnetic field which in turn struck them 20 times a seconds. (20 Hz). It is calculated that on a normal landline you can have up to 4 of the classic phones ringing at the same time, but if you even add a fifth one, the whole circuit will fail to have the required amperage required to move the hammer on them all so none of them would ring. This number is provided on packaging nowadays as an R.M.S. Value starting at 1 and going as far up to 4 depending on how many milliamps it needs to ring as the telephone exchange can only give as much as 50 mA to each line.

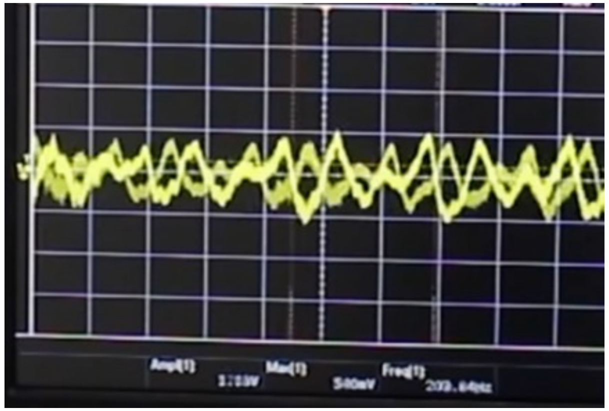


My voice on the line

- So I called the house phone again and this time I picked up and saw that there was a significant voltage drop to 7 VDC because the phone has to load the line with a set resistance of around 390Ω to notify the switching system in the exchange that you've picked up the phone.
- Now after I get rid of the DC signal and amplify the signal a little bit you can see when I speak into the landline side, my voice is show over the lines at around 3 volts Peak-to-Peak, but from the 'mobile' phone side, I get at its highest, 1 volt Peak-to-Peak.

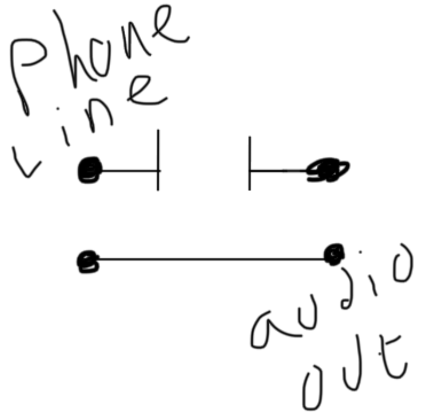






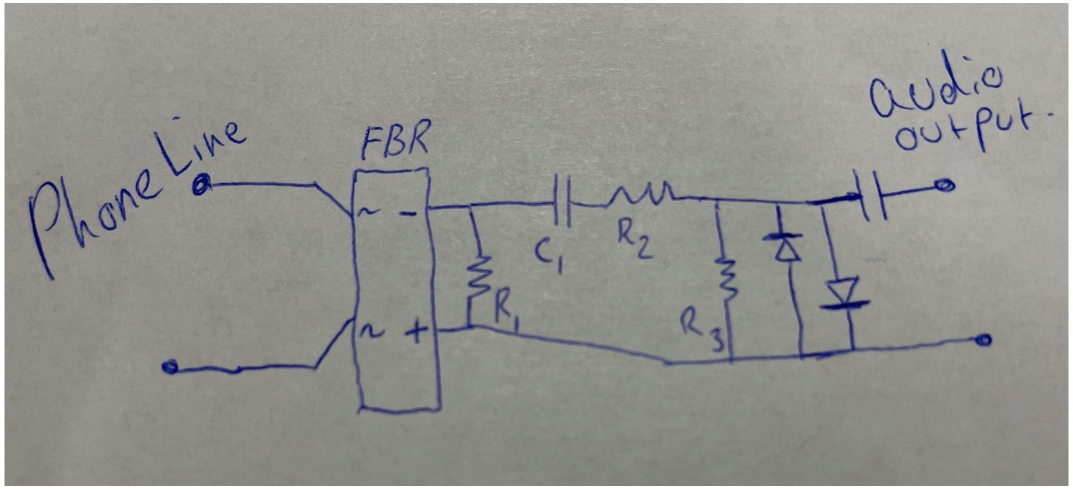
Creating the circuit

- I want to build a circuit that can be outputted to a recorder's audio input or a standard pair of headphones
- It seems to me that if was to plug it in during an active call, then I would only need a single capacitor in series to separate the DC levels on both sides as shown in the diagram.
- So, I connected my phone cable capacitor and a pair of headphones to try it out.
- It was here when I nearly made a huge mistake.
- I had used a 16v capacitor as I thought that I only needed it to be over 7v, so I quickly pulled out the wire but luckily the 48v capacitor didn't blow up due to the low current availability on the line.
- So, to continue to use the 16v capacitor I unplugged the cable, called, picked up and then reconnected it.
- At this point I could hear myself through the headphones



Improving the Circuit

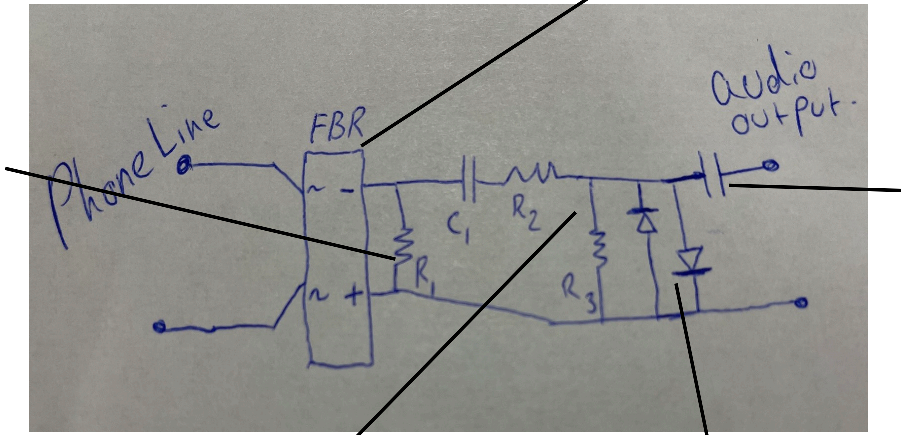
- So now all I need to do is to design a circuit which can protect any recorder or device when plugged in from high voltage, reverse voltage, ringing voltage and can feed the audio safely into any device because the last thing anyone wants is to destroy expensive recording gear
- Testing normal microphones and other general outputs, I saw that the audio signals are about 1 volt Peak-to-Peak up to 10 volts Peak-to-Peak, which are already higher than what I saw on the phone line so its clear to me that its safe just to continue the circuit design like this for use in recorders.
- After taking a couple minutes to design a circuit, I constructed this circuit



Explaining the circuit

The rectifier is usually used to make a DC voltage, but we want the AC signal of the audio to go through so that's where R1 comes in. The full bridge rectifier only outputs current in one direction which would charge the capacitor C1 up to the peak of the AC and DC signal combined. So for any voltage below the peak and the AC signal gets stuck into a falling cycle or the DC signal drops for any reason, the diode will turn off and the AC signal would be cut. Resistor 1 makes sure Capacitor 1 is discharged as the AC voltage goes fluctuates and so the entire AC cycle happens. C1 used to isolate the landline's constant DC voltage from the circuit and to allow only the AC through.

The full bridge rectifier makes sure that if the order of wires is not important as it will make one side positive and the other negative. I couldn't use a single diode to prevent reverse polarity because it would only work half the time due to it being a sine wave modulated signal. I could have alternatively used 4 diodes to create a full bridge rectifier in the event that the electronics shops near me had no stock.

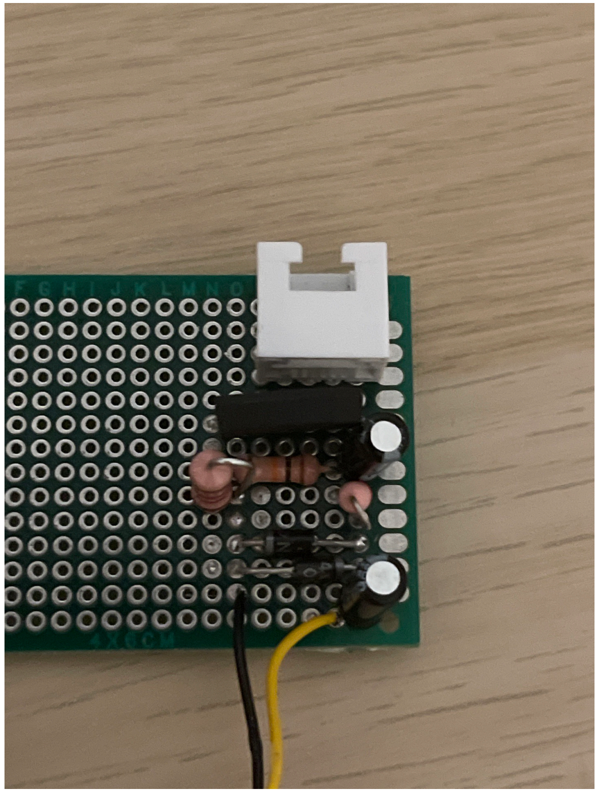


Capacitor 2 isolates the DC voltage which can come from any recorder from the circuit. My recorder gives out approximately 2 volts DC when recording, which will easily clamp to 0.7 volts by diode 2 and pretty much eliminates the AC audio signal as well. Luckily when capacitor 2 is present, clamping never occurs. The DC voltage coming from my recorder is so it can power external microphones and is sometimes also used as an indicator by most mics attached so they can see when the recorder is on.

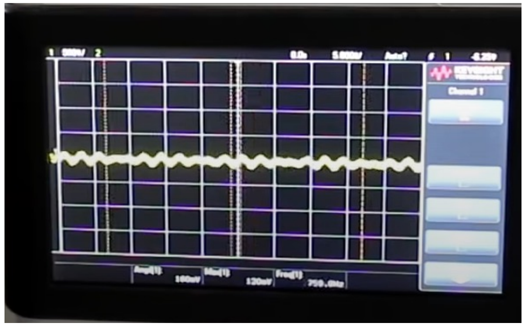
Here, the alternating signal goes through the the two resistors which act as a resistive divider, which divided the amplitude of the signal by a divisor of 3. my measurements showed that the AC signal was at a maximum of 3V ptp or 1.5 volts amplitude. So dividing it by 3 would give a peak voltage of 0.5.

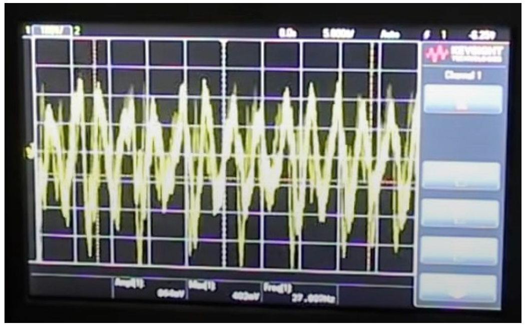
These 2 diodes are here to limit the peak of the AC signal. For peaks above 0 volts, any signal above approximately 0.6 Volts diode 2 would work to clamp the voltage to somewhere between 0.6 and 0.7 volts, and for voltages below 0 volts, diode 1 will do the same. Because of this, the AC signal won't rise above 0.7 volts ptp, which would be safe for any recorder or input device. This is the reason I divided signal using resistor 2 and 3 to a max of 0.5 volts audio level, so that diodes 1 and 2 wouldn't clamp and interfere with the audio. So fundamentally diode 1 and 2 would stop the ringing voltage of the line, in addition to any transients and electrostatic discharge voltages.

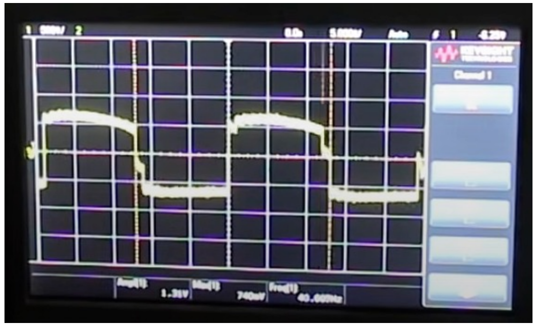
Testing the circuit



This is the circuit I designed. I soldered it together with an rj-11 jack on the input side and a 3.5mm headphone jack wired up in dual-mono.
I plugged in the phone end and I probed the output wires with my oscilloscope. The first thing I noticed was that there was no trace of the 48 volt phone line input and if I pick up the phone, you can see the dial tone mixed with my voice. If I call the phone, I can see the ringing signal which is slightly over 1 volt ptp which is safe to feed straight into any recorder

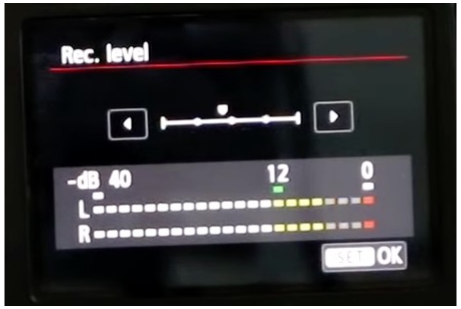


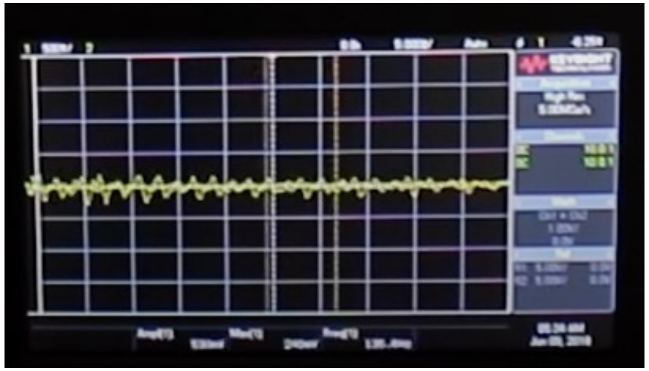


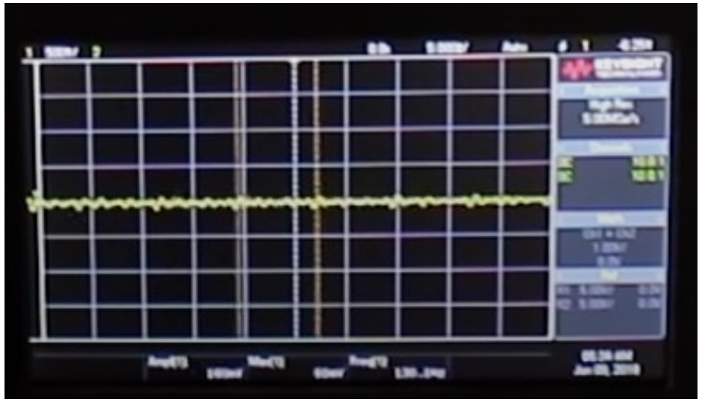


Using the circuit

- Due to the gain of the circuit being fixed, I needed to adjust the gain on my recorder to make sure the audio doesn't clip.
- So now I tested the circuit using 2 phone lines and when I called I got a strong signal from the local side while getting a weaker but still clear signal from the other line. This is great which shows great success from the circuit.

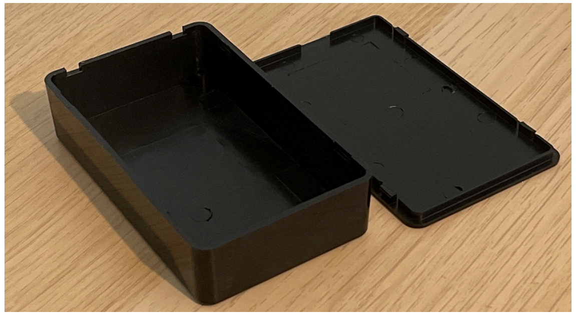






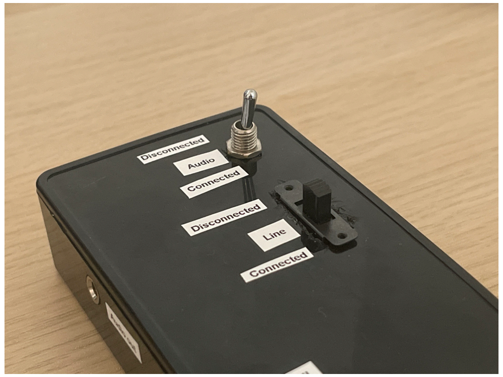
Enclosing the circuit

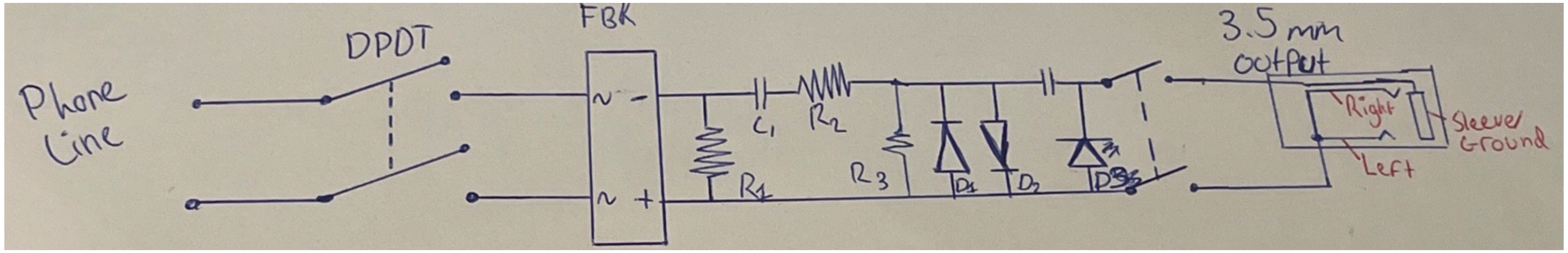
- The circuit should be put into a small black box to avoid suspicion and to be able to be put anywhere without being seen.
- I bought a small box from amazon with the dimensions of 9.9x6.9x4.4cm which has a clip on lid which allows the box to be clamped closed without the need of screws or other items which may draw attention to the device and thus give its location away.
- I secured the board into the box with hot glue and cut out the holes required for the switches, line input and the audio output with a Dremel.
- My circuit board fitted snuggly into the box with plenty of space for the wires and the switches.



Additional features

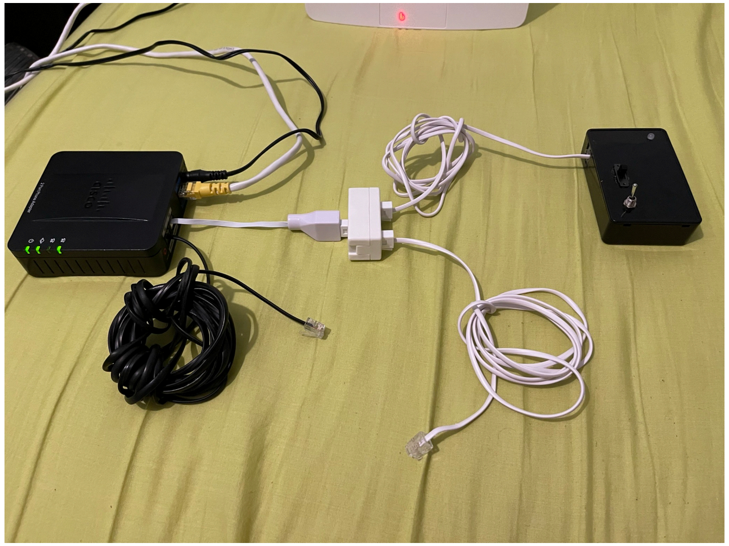
- I have improved the circuit by adding 2 DPDT (double throw double pole) switches, one slide switch and one toggle switch
- The slide switch is being used as a mechanical master switch to completely disconnect the line from the device in the case of a malfunction.
- The toggle switch is being used as a electronic disconnect to the output medium to allow the spy to stop listening to the conversation without making any noise
- I used a slide switch as the master switch because of its low profile which allows it to be harder to mistakenly flip.
- I used a toggle switch to allow for easy switching as the force required to enable it is very low
- I also added a red LED to indicate when a call is present or incoming.



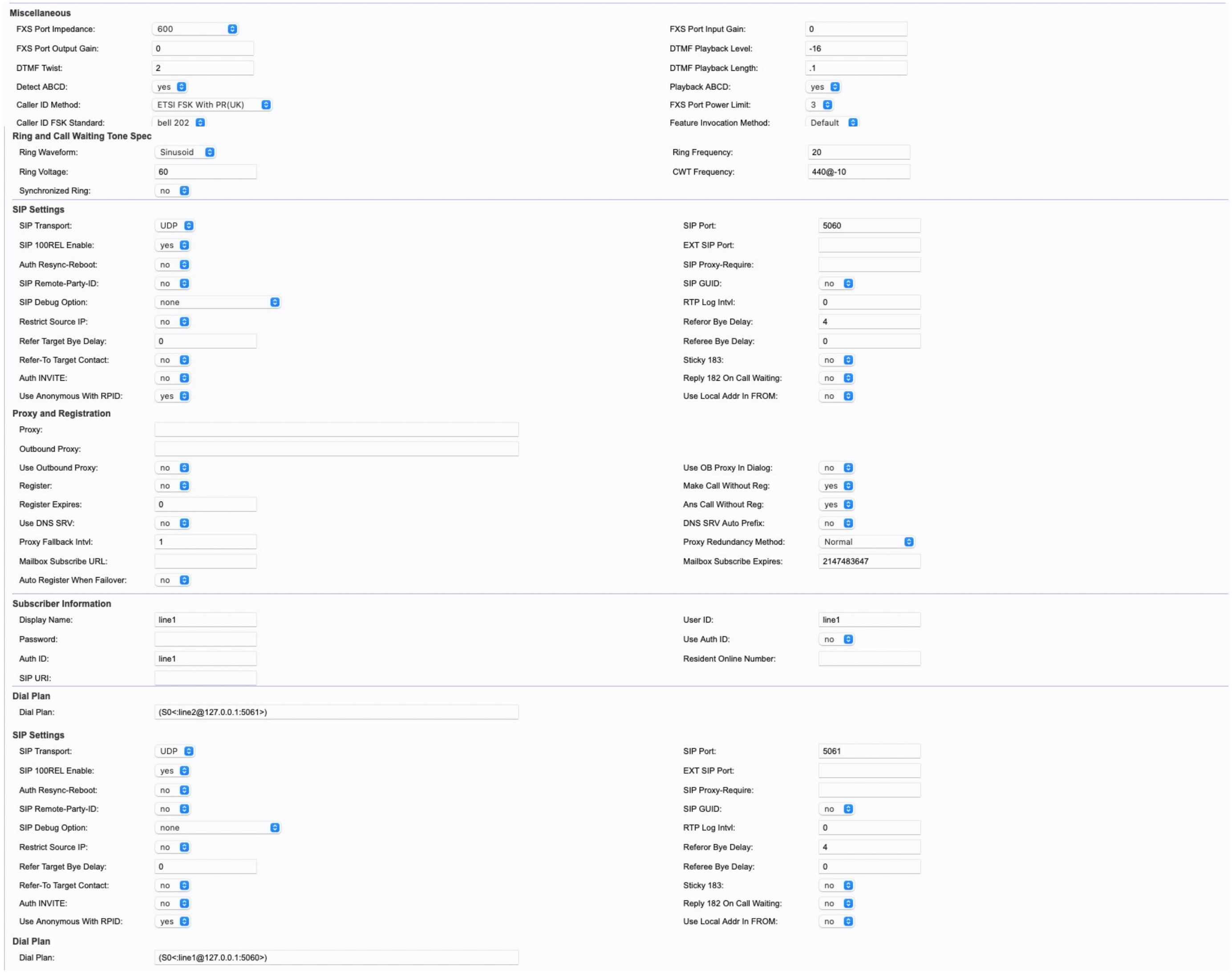


Mimicked Network

- For the mimicked network, I used an old internet router and a Cisco SPA112.
- The SPA112 is a VoIP adapter designed for 2 phones to talk to others over the internet through a SIP provider
- The router and SPA112 were used together to create a loopback line by pointing the dial plan of each phone to the IP address of the SPA112 adapter itself, so whenever you pick up the phone, the SPA112 would initiate the dial plan which would tell the router to call the IP address of the other phone, which in my case I put as the adapter's own IP address so it routes back to the SPA112 through the router and thus rings the other phone.



Mimicked network settings



Miscellaneous

FXS Port Impedance:	600	FXS Port Input Gain:	0
FXS Port Output Gain:	0	DTMF Playback Level:	-16
DTMF Twist:	2	DTMF Playback Length:	.1
Detect ABCD:	yes	Playback ABCD:	yes
Caller ID Method:	ETSI FSK With PR(UK)	FXS Port Power Limit:	3
Caller ID FSK Standard:	bell 202	Feature Invocation Method:	Default

Ring and Call Waiting Tone Spec

Ring Waveform:	Sinusoid	Ring Frequency:	20
Ring Voltage:	60	CWT Frequency:	440@-10
Synchronized Ring:	no		

SIP Settings

SIP Transport:	UDP	SIP Port:	5060
SIP 100REL Enable:	yes	EXT SIP Port:	
Auth Resync-Reboot:	no	SIP Proxy-Require:	
SIP Remote-Party-ID:	no	SIP GUID:	no
SIP Debug Option:	none	RTP Log Intvl:	0
Restrict Source IP:	no	Referor Bye Delay:	4
Refer Target Bye Delay:	0	Referee Bye Delay:	0
Refer-To Target Contact:	no	Sticky 183:	no
Auth INVITE:	no	Reply 182 On Call Waiting:	no
Use Anonymous With RPID:	yes	Use Local Addr In FROM:	no

Proxy and Registration

Proxy:			
Outbound Proxy:			
Use Outbound Proxy:	no	Use OB Proxy In Dialog:	no
Register:	no	Make Call Without Reg:	yes
Register Expires:	0	Ans Call Without Reg:	yes
Use DNS SRV:	no	DNS SRV Auto Prefix:	no
Proxy Fallback Intvl:	1	Proxy Redundancy Method:	Normal
Mailbox Subscribe URL:		Mailbox Subscribe Expires:	2147483647
Auto Register When Failover:	no		

Subscriber Information

Display Name:	line1	User ID:	line1
Password:		Use Auth ID:	no
Auth ID:	line1	Resident Online Number:	
SIP URI:			

Dial Plan

Dial Plan:	(S0<:line2@127.0.0.1:5061>)

SIP Settings

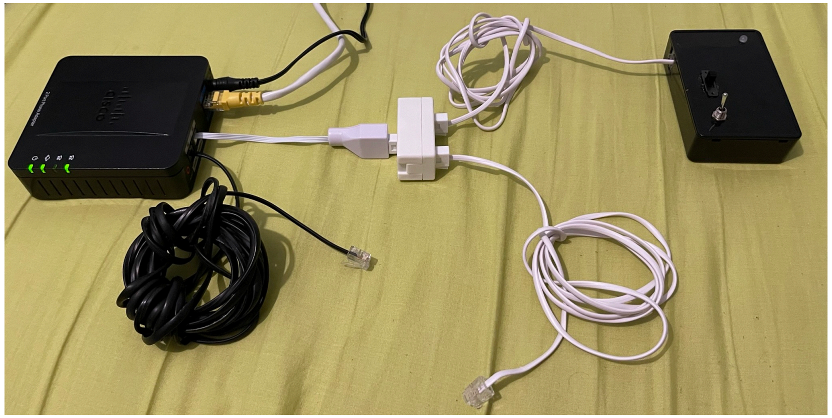
SIP Transport:	UDP	SIP Port:	5061
SIP 100REL Enable:	yes	EXT SIP Port:	
Auth Resync-Reboot:	no	SIP Proxy-Require:	
SIP Remote-Party-ID:	no	SIP GUID:	no
SIP Debug Option:	none	RTP Log Intvl:	0
Restrict Source IP:	no	Referor Bye Delay:	4
Refer Target Bye Delay:	0	Referee Bye Delay:	0
Refer-To Target Contact:	no	Sticky 183:	no
Auth INVITE:	no	Reply 182 On Call Waiting:	no
Use Anonymous With RPID:	yes	Use Local Addr In FROM:	no

Dial Plan

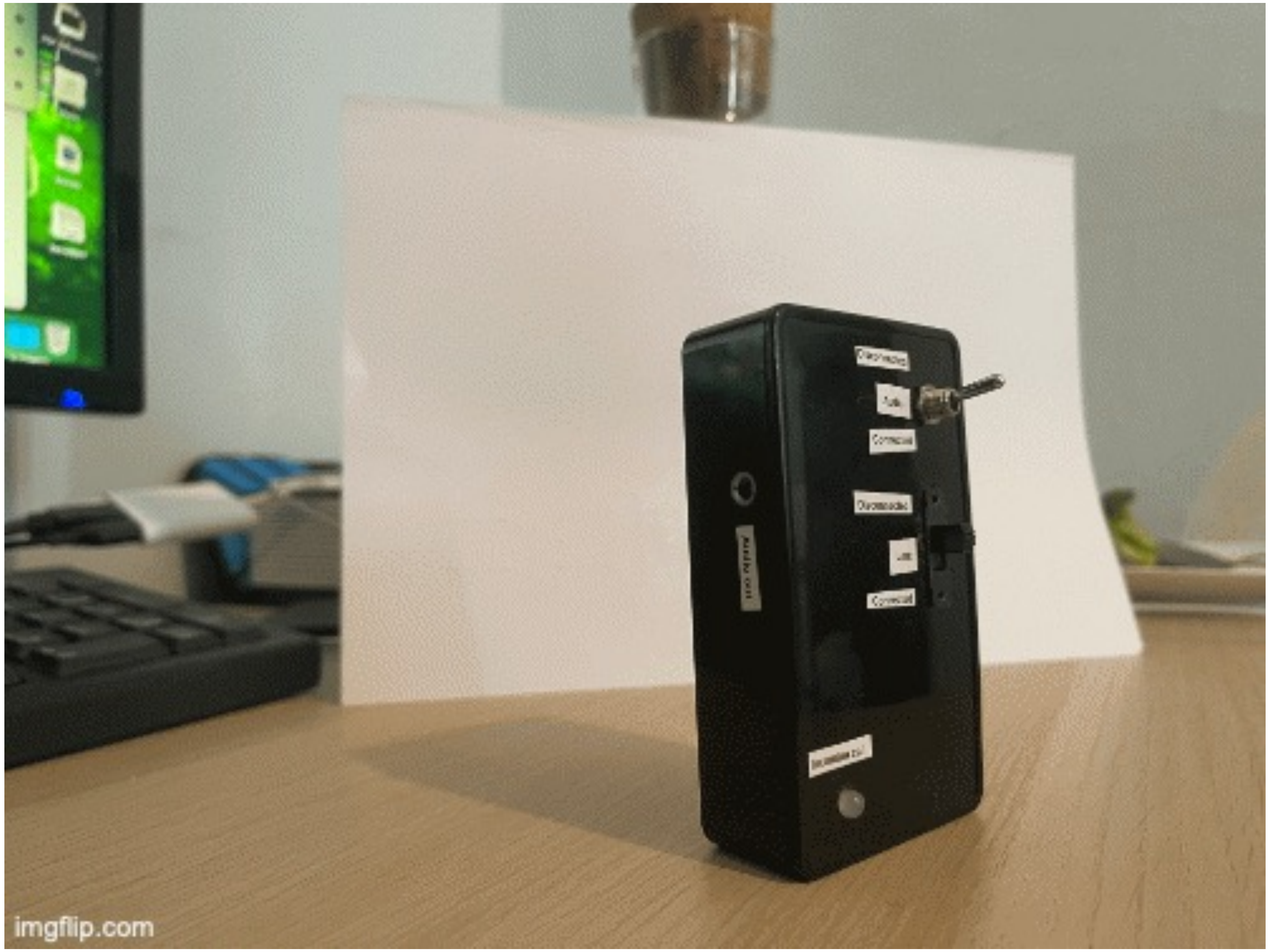
Dial Plan:	(S0<:line1@127.0.0.1:5060>)

Connecting to the mimicked network

- On the mimicked network, each of the 2 ports on the back of the SPA112 is designed to be 2 different households or people
- Port 1 is designed to be person number 1’s house while Port 2 is designed to be person number 2’s house
- Person number 2’s house has more than one port which may be placed around the house, the 3 port adapter is used to mimic the multiport availability you would have in the house.
- According to the shared ports, I plugged the wire tap and a landline telephone into the 3-way adapter plugged into port 2 and then plugged another phone into port 1 of the SPA112, this gave me the infrastructure needed to wiretap the phones

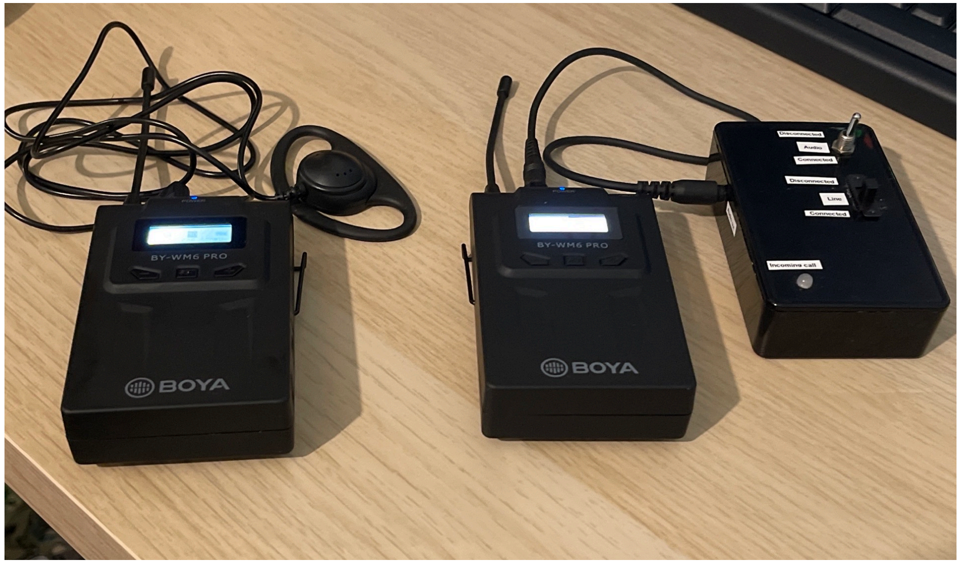


The final product



The final product

- I finally completed the device and labelled it for ease of use so that the people who are allowed to use it don't need extra training.
- Currently the product can only be used relatively close to the mark's house or place of contact.
- As an improvement, I would use an Arduino with a keypad to electronically lock out any unauthorised users from using it.
- I would also make a wireless transmitter and receiver addon which can be plugged into the device and allow the spy to listen from greater distances.
- At the current moment, I am able to listen to conversations by adding a commercial lavalliere microphone set



Demo time!!!

Thanks for listening :)