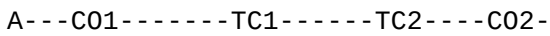
Blue Box courtesy of the Jolly Roger

To quote Karl Marx, blue boxing has always been the most noble form of phreaking. As opposed to such things as using an MCI code to make a free fone call, which is merely mindless pseudo-phreaking, blue boxing is actual interaction with the Bell System toll network.
It is likewise advisable to be more cautious when blue boxing, but the careful phreak will not be caught, regardless of what type of switching system he is under.
In this part, I will explain how and why blue boxing works, as well as where. In later parts, I will give more practical information for blue boxing and routing information. To begin with, blue boxing is simply communicating with trunks. Trunks must not be confused with subscriber lines (or "customer loops") which are standard telefone lines. Trunks are those lines that connect central offices. Now, when trunks are not in use (i.e., idle or "on-hook" state) they have 2600Hz applied to them. If they are two-way trunks, there is 2600Hz in both directions. When a trunk IS in use (busy or "off-hook" state), the 2600Hz is removed from the side that is off-hook. The 2600Hz is therefore known as a supervisory signal, because it indicates the status of a trunk; on hook (tone) or off-hook (no tone). Note also that 2600Hz denoted SF (single frequency) signalling and is "in-band." This is very important. "In-band" means that is within the band of frequencies that may be transmitted over normal telefone lines. Other SF signals, such as 3700Hz are used also. However, they cannot be carried over the telefone network normally (they are "out-of-band" and are therefore not able to be taken advantage of as 2600Hz is. Back to trunks. Let's take a hypothetical phone call. You pick up your fone and dial 1+806-258-1234 (your good friend in Amarillo, Texas). For ease, we'll assume that you are on #5 Crossbar switching and not in the 806 area. Your central office (CO) would recognize that 806 is a foreign NPA, so it would route the call to the toll centre that serves you. [For the sake of accuracy here, and for the more experienced readers, note that the CO in question is a class 5 with LAMA that uses out-of-band SF supervisory signalling]. Depending on where you are in the country, the call would leave your toll centre (on more trunks) to another toll centre, or office of higher "rank". Then it would be routed to central office 806-258 eventually and the call would be completed.

Illustration



A.... you
CO1=your central office
TC1.. your toll office.
TC2.. toll office in Amarillo.
CO2.. 806-258 central office.
B.... your friend (806-258-1234)

In this situation it would be realistic to say that CO2 uses SF in-band (2600Hz) signalling, while all the others use out-of-band signalling (3700Hz). If you don't understand this, don't worry. I am pointing this out merely for the sake of accuracy. The point is that while you are connected to 806-258-1234, all those trunks from YOUR central office (CO1) to the 806-258 central office (CO2) do *NOT* have 2600Hz on them, indicating to the Bell equipment that a call is in progress and the trunks are in use.
Now let's say you're tired of talking to your friend in Amarillo, so you

send a 2600Hz down the line. This tone travels down the line to your friend's central office (CO2) where it is detected. However, that CO thinks that the 2600Hz is originating from Bell equipment, indicating to it that you've hung up, and thus the trunks are once again idle (with 2600Hz present on them). But actually, you have not hung up, you have fooled the equipment atyour friend's CO into thinking you have. Thus,it disconnects him and resets the equipment to prepare for the next call. All this happens very quickly (300-800ms for step-by-step equipment and 150-400ms for other equipment). When you stop sending 2600Hz (after about a second), the equipment thinks that another call is coming towards
--> on hook, no tone -->off hook.
Now that you've stopped sending 2600Hz, several things happen:

1) A trunk is seized.
2) A "wink" is sent to the CALLING end from the CALLED end indicating that the CALLED end (trunk) is not ready to receive digits yet.
3) A register is found and attached to the CALLED end of the trunk within about two seconds (max).
4) A start-dial signal is sent to the CALLING end from the CALLED end indicating that the CALLED end is ready to receive digits.
Now, all of this is pretty much transparent to the blue boxer. All he really hears when these four things happen is a <beep><kerchunk>. So, seizure of a trunk would go something like this:

1> Send a 2600Hz
2> Terminate 2600Hz after 1-2 secs.
3> [beep][kerchunk]

Once this happens, you are connected to a tandem that is ready to obey your every command. The next step is to send signalling information in order to place your call. For this you must simulate the signalling used by operators and automatic toll-dialing equipment for use on trunks. There are mainly two systems, DP and MF. However, DP went out with the dinosaurs, so I'll only discuss MF signalling. MF (multi-frequency) signalling is the signalling used by the majority of the inter- and intra-lata network. It is also used in international dialing known as the CCITT no.5 system.
MF signals consist of 7 frequecies, beginning with 700Hz and separated by 200Hz. A different set of two of the 7 frequencies represent the digits 0 thru 9, plus an additional 5 special keys. The frequencies and uses are as follows:

Frequencies (Hz)	Domestic	Int'l
700+900	1	1
700+1100	2	2
900+1100	3	3
700+1300	4	4
900+1300	5	5
1100+1300	6	6
700+1500	7	7
900+1500	8	8
1100+1500	9	9
1300+1500	0	0
700+1700	ST3p	Code 1
900+1700	STp	Code 1
1100+1700	KP	KP1
1300+1700	ST2p	KP2

1500+1700 ST ST

The timing of all the MF signals is a nominal 60ms, except for KP, which should have a duration of 100ms. There should also be a 60ms silent period between digits. This is very flexible however, and most Bell equipment will accept outrageous timings. In addition to the standard uses listed above, MF pulsing also has expanded usages known as "expanded inband signalling" that include such things as coin collect, coin return, ringback, operator attached, and operator attached, and operator released. KP2, code 11, and code 12 and the ST_ps (STart "primes" all have special uses which will be mentioned only briefly here.

To complete a call using a blue box once seizure of a trunk has been accomplished by sending 2600Hz and pausing for the <beep><kerchunk>, one must first send a KP. This readies the register for the digits that follow. For a standard domestic call, the KP would be followed by either 7 digits (if the call were in the same NPA as the seized trunk) or 10 digits (if the call were not in the same NPA as the seized trunk). [Exactly like dialing normal fone call]. Following either the KP and 7 or 10 digits, a STart is sent to signify that no more digits follow. Example of a complete call:

1> Dial 1-806-258-1234
2> wait for a call-progress indication (such as ring,busy,recording,etc.)
3> Send 2600Hz for about 1 second.
4> Wait for about ll-progress indication (such as ring,busy,recording,etc.)
5> Send KP+305+994+9966+ST

The call will then connect if everything was done properly. Note that if a call to an 806 number were being placed in the same situation, the are code would be omitted and only KP + seven digits + ST would be sent.

Code 11 and code 12 are used in international calling to request certain types of operators. KP2 is used in international calling to route a call other than by way of the normal route, whether for economic or equipment reasons. STp, ST2p, and ST3p (prime, two prime, and three prime) are used in TSPS signalling to indicate calling type of call (such as coin-direct dialing.