Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

Title	**The Bell Telephone System: A Black Box Analysis**
Date	1964-07-14
Author(s)	Mesler, Donald T.
Abstract	Academic paper written by a classmate of Hoyt Stearns describing how Stearns figured out how to build a blue box in 1964. Includes some really great quotes, e.g.: "To be successful, only two attributes are necessary: (1) An intense interest and curiosity about the telephone system, and (2) Time to investigate and piece together all possible sources of information." Or: "The nationwide telephone network was essentially a black box with one pair of terminals accessible for measurement."
Keywords	blue box; Cornell; Ithaca, NY; Hoyt A. Stearns, Jr.; Donald T. Mesler
Source	Hoyt Stearns

The Bell Telephone System
A Black Box Analysis

Submitted to

Professor Green

School of Electrical Engineering
Cornell University
Ithaca, New York

by

Donald T. Mesler

14 July 1964

ABSTRACT

All long distance telephone numbers, whether dialed directly or placed through a long distance operator, are eventually coded into a set of audio frequencies spread between 700 and 1700 cps. The purpose of this project was to uncover the coding process, reproduce the code with experimental apparatus, and to attempt activation of telephone company equipment by such apparatus.

The entire telephone network was treated as a "black box" and all measurements and tests were made from two wires entering this black box from a private telephone. The audio frequencies corresponding to each digit were tape recorded, analyzed, and identified. A multi-frequency key-pulsing system was constructed and successfully used to reach telephone numbers in every part of the country.

Telephone agents stress that it is impossible to fool the telephone equipment. The device was in violation of Section 967 of the New York State Penal Code dealing with attempts to defraud. It did however uncover a shortcoming of the direct distance dialing system whereby billing equipment can be evaded.

INTRODUCTION

For most of us, placing a telephone call consists only of turning a dial. Behind this operation, which is no more than lifting a finger, is a complex of electronic equipment, the function of which is not known even to many telephone men of long experience. However, a person interested in the operation of the telephone system, though working from the outside, can uncover enough data to construct in the laboratory similar equipment on a smaller scale. To be successful, only two attributes are necessary: (1) An intense interest and curiosity about the telephone system and (2) Time to investigate and piece together all possible sources of information.

Hoyt A. Stearns, a junior electrical engineer, has made telephony, the science of telephonic transmission, his hobby for several years. When a basic working knowledge of direct distance dialing was gained, one question inevitably followed. Could direct dialing be accomplished by means of a home-built multi-frequency dialing generator whereby the functions of the central telephone exchanges could be bypassed or overridden and handled completely by the individual placing the call?

BASIC OPERATION OF THE TELEPHONE SYSTEM

When direct dialing long distance from Ithaca, the area code and telephone number must be preceeded by dialing "1". This signals equipment in the Ithaca exchange to route the call to Binghamton, the area distribution point for long

distance calls. At Binghamton, the dialed number is stored in a computer called the "Marker". The call is next transmitted to Albany, the closest tie-in point for the telephone "long lines" which connect to all distant telephone areas. The Marker at Binghamton converts dial pulses into coded audio tones which activate all remaining equipment. At Albany another Marker computer receives the coded telephone number, stores it in memory, selects an open trunk or the shortest possible alternate route, and transmits the number using tones as before. At the receiving end, the pulses are decoded and the proper extension is reached.

THE INVESTIGATION

For duplication of this process, accurate technical information was needed. Several sources were available, including Bell System employees, The Bell System Technical Journal, and tours through telephone exchanges. More productive however, was the pair of wires leading into Mr. Stearns' house to his private telephone. The nationwide telephone network was essentially a black box with one pair of terminals accessible for measurements. The first thing observed was the series of faint audio tones heard in the background when placing any long distance call. It was as though a set of audio oscillators was connected to a keyboard and played in some as yet undetermined sequence. Tape recordings failed to divulge any pertinent information other than to assure the importance of

the tones. The tone signal was too weak for analysis and it was impossible to correlate the tone with the number, if that was indeed the coding procedure.

The next step involved the identification of each particular tone frequency and its associated number. Results were obtained using trickery and the cooperation of the Reno, Nevada information operator. A keyboard as postulated above for use with the audio oscillators does in fact exist and one which had been removed from a switchboard was purchased on the surplus market. The information operator was called by Mr. Stearns and informed that her multi-frequency generator was out of order. The caller was identified as "Test Board", the service division of Bell System. She was instructed to depress each key in sequence for a period of one minute while tests were conducted. She was extremely busy and somewhat dubious, but she did comply by holding each key down for about ten seconds, long enough for a perfect recording to be made. The results are shown in Table I. Note that each tone is a superposition of two tones thus eliminating the possibility that the equipment will be activated accidentally by conversation or music or random noise. Three additional code units also came to light. Their functions were identified by experimentation and by research in The Bell System Technical Journal.

The RELEASE function clears the trunk for a number to be transmitted. The K.P. function is an abbreviation for "key punch". This signals the Marker computer that the first digit

of a complete telephone number will follow. The S.T. function is an abbreviation for "start". It signifies that the last digit of the number has been transmitted. The call is now processed at the receiving end.

TABLE NO. I

Generator Frequencies

Character	Frequency Combination
1	700 & 900
2	700 & 1100
3	900 & 1100
4	700 & 1300
5	900 & 1300
6	1100 & 1300
7	700 & 1500
8	900 & 1500
9	1100 & 1500
0	1300 & 1500
K.P.	1100 & 1700
S.T.	1500 & 1700
RELEASE	2600

CONSTRUCTION OF A MULTI-FREQUENCY DIALING GENERATOR

The general order of events of direct distance dialing was now known. At this point it was pure speculation as to whether or not the same operations could be performed from a private telephone. Several multi-frequency dialing generators were constructed and modified. Details of the prototypes are unimportant. The only major problem was obtaining a stable distortion free sine wave audio oscillator.

In its final form the multi-frequency dialing generator, now called multifreq, consists of seven oscillators of 700,

900, 1100, 1300, 1500, 1700, and 2600 cps, two stages of audio amplification, a power supply, and a loudspeaker. Multifreq is about the size of a twenty-watt high fidelity amplifier. The oscillator circuit was taken from the Radio Amateur's Handbook. This circuit is recommended because it meets stability and waveform requirements. Parts' layout is non-critical. Two test instruments are required for calibration, an audio frequency oscillator and an oscilloscope. Frequency comparisons are made using Lissajous patterns in the standard manner. Each oscillator of the device must be tuned carefully as the majority of incomplete calls were the result of poor alignment. The signal is fed from the multifreq loudspeaker through the telephone mouthpiece. Gain is critical, and the magnitude can be determined by experiment only. More consistant results can be obtained by replacing the loudspeaker with a multi-turn coil 3" in diameter. This was slipped over the telephone receiver earpiece and the signal inductively coupled into the telephone system.

Experience indicates that under no circumstances should a direct tap into the telephone lines be made. Besides interfering with the balance of telephone circuits and making the device easier to trace and locate, it means the difference between a charge of disorderly conduct and misdemeanor or felony when an investigation gets under way.

OPERATION

As described, the device was 95 per cent reliable. At other times the familiar operator's recording was heard saying that we had dialed incorrectly, to hang up and dial again. All calls were placed through information. A distant area code was selected and the information number for that area dialed in the usual manner. Before information answered, the Release key on multifreq was depressed. This disconnected the recieving station but left the long distance trunk open to accept any new number. The desired telephone number was now keyed on multifreq in the following sequence:

K.P. + telephone number + S.T.
(10 digits)

A remarkable feature of the device was its ability to bypass billing equipment. Telephone company policy permits free information calls to most major cities in the country. It was initially assumed, although incorrectly, that no record was being made of the calls since each was being made through an information channel. Although no charge is made for information calls, a tabulation is available giving party number, destination, and length of call. The sudden increase in information calls, numbering dozens, with times exceeding one hour, triggered investigation and action by law authorities.

CONCLUSIONS AND RECOMMENDATIONS

Several similar devices have been reported by news media recently. The details of operation are probably discovered

independently in each case, although dissemination of this information by its discoverers is inevitable. I recommend that the telephone company find a method to prevent external activation of its equipment. Perhaps also, they should publicize laws and penalties regarding attachments to, or fraudulent use of their facilities.

Mr. Stearns paid dearly for his ingenuity. He has reimbursed New York Telephone $276 besides serving a short jail sentence. His personal telephone service was disconnected. I recommend that all experiments along this line be discouraged until such time as it may be authorized by the telephone company.

No effort was made to miniature this model of multifreq or to minimize the number of components. Using semi-conductor devices, the size could be reduced and battery operation would be feasible. Each of the seven audio oscillators required one tube. A better method would consist of a single oscillator whose frequency could be changed by switching tuned circuits. A unit small enough to be hand held and portable would result.