MORE FORTRESS FUN!

Last week, I met with "CJ" and "The Professor" and told them how much I would like a Fortress Fone of my very own to play with. About 1/2 hour after they left, they returned with one and gave it to me to open. "The Professor" was able to pick the upper lock after removing the shroud around it. It's only 4 levers. I immediately went to work on it while "CJ" bashed open the coin box. After he opened it we made the following discoveries:

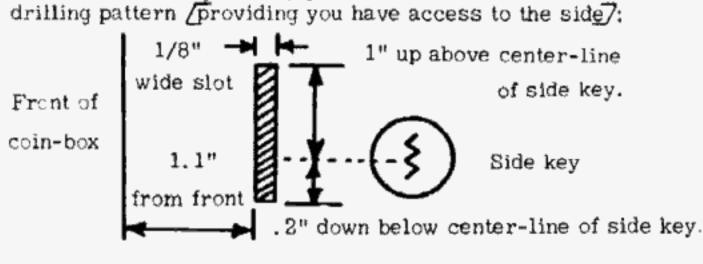
it, we made the following discoveries:

1. The drill pattern you published in #30 for the front plate would make it almost impossible to get the box open, because the bolts go thru double sets of slots before going into the outer shell of the phone. When the rotary plate is drilled as in #30, it should rotate and retract the bolts. 7

2. The right-hand bolt is really wide and protects the

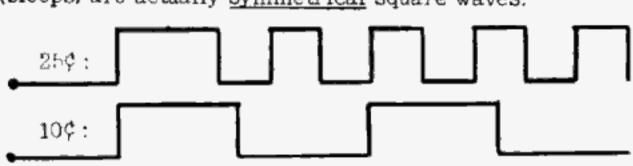
side lock (interlock).

3. The following cutting pattern would be better than a



The cut should be 1.2" long, 1/8" wide, and 1" deep. It can be done with a special grindstone drill bit, and will shear off the interlock mechanism as well as cut the spiral front plate free so it can turn. We are checking reports of a puller for the cover. If there is such an animal, and if it does work, you'll hear about it first in TAPIT

4. The tones' intervals are not generated by the coins pushing levers on the red box mechanism (like everyone thinks) but by a little relay which reverses the direction of the wheel that the levers cock. In other words, when a coin is dropped, the coin pushes a lever which cocks a wheel. The coin then drops into the drop chute, and the red box goes thru a 70ms delay to allow the coin to clear the mechanism. After that, a unijunction-timer circuit pulls in a relay which unwinds the wheel until it is back where it started. The number of times the relay ticks, pulling the wheel, is the number of beeps. If the wheel went 5 notches forward, a switch drops, telling the unit to do 35ms bleeps (for a quarter). However, the first bleep will always be the same as the above-mentioned 70ms pre-bleep delay, because the coin will just be clear, and all of the pulses (bleeps) are actually symmetrical square waves:



I will restate the specs on these tones because they are <u>very</u> important and must be known by all TAP readers. The 25¢ tones are 70ms on, 35ms off, 35ms on, 35ms off, 35ms on, 35ms off, 35ms on, The dime is 80ms on, 80ms off, 80ms on. These can be fudged to 70ms if needed, and better be generated digitally, because they'll fuck up with analog timers, "windows", and analog delays. Then I made a few discoveries myself:

1. Coin Drop Mechanism - In my last letter, I asked about the "coin-sense relay" but couldn't figure how Bell knew about the money. Now I know! First, they use a low current (20ma) high voltage (50v) relay to release the money. Second, the relay resets a vane which senses the presence of the money. This vane cannot be checked by the operator. However, she can see the current drain caused by the drop relay pulling in. If the vane hasn't been hit by money, the coin-drop relay won't pull in even when the operator tries to make it. The good part is that she can't check the vane until she drops the money. So it doesn't matter when you drop your nickel, as long as you drop one before each time she collects. Also, she can't check it on

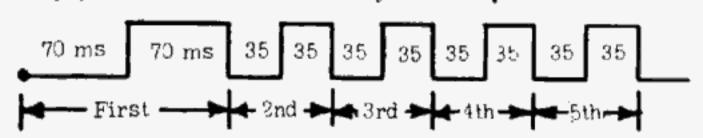


MAR-APRIL 1978 NO. 49

the initial three minutes because that drops automatically, and so you can talk for at least three minutes for free.

2. The pay phone red box tones drift with the outside temperature. So...before boxing away, make sure the payphone frequencies match your red box frequencies or you'll get screwed when you drop your 5¢.

3. As I told you last time, the 25¢ set of tones are 5 beeps, the first one twice as long as the rest:



All of the above info is confirmed by an in-depth experiment which can be done on any phone without taking it out of the booth!

1. Drop 5¢ into a pay phone. Listen to the side and hang up. The relay will pull the wheel back once and click.

2. Drop two nickels into the phone, one at a time. Listen to the receiver or the side of the phone. When the second nickel is dropped, two clicks of the relay are heard - as if a dime had been dropped.

3. Now for some fun: Drop a nickel, and then a dime. There are three clicks! Amazing, a 15¢ piece!
4. Now try dropping two dimes right together and you'll hear both dimes hit the bottom of the coin holding chute before you hear four clicks! a 20¢ piece!

5. Try a nickel and a quarter and get six clicks (30¢).
6. If you're fast enough, this will work too: Drop a nickel. Then two dimes together and you'll hear the familiar quarter sequence and not five nickel bleeps.
Whether you are listening to the bleeps thru the receiver

or clicks on the side of the phone, you'll find these experi-

ments interesting.

If you don't believe me about the timing of the tones on
the 25¢ bleeps, try tape recording them (have a friend call
you from a pay phone and drop money) at 7 1/2 ips on a
reel-to-reel recorder. Slow down the tape on playback to
as slow as possible and mark the tape at the beginning and
end of each bleep. When done marking, measure the marks
and you can determine the tone durations. You will find
most phones adjusted perfectly, whether single tone or mf
phones, so the first bleep is twice as long as the rest.

If you should ever have access to a phone in a relatively private place, and wish to record the tones interference-free, get a phone pickup coil from someplace like Radio Shack (bletch!) and place it 3" behind the top keyhole on the right side of the Fortress Fone. It picks up the tones fine there.

Computer Wizard

Some Fortresses must have a mechanism defect. It seems that they will take two dimes or two nickels - a 50% savings! Please advise readers to deposit two nickels first and listen for second dial tone. This is for a 20% local call area.

Mugs

© Youth Hot Line Reports, Inc. 1978 - Do not make checks out to Youth Hot Line Reports, PLEASE! Movement groups may reprint without permission with TAP's address given with all credits. Please send us a copy of reprinted work. WARNING: We will prosecute copyright violators.

THE PRINCIPLES OF TWX PHREAKING

by Cheshire

INTRODUCTION

IN 1971, THE WESTERN UNION TELEGRAPH CO BOUGHT THE TELETYPENRITER EXCHANGE (TWX) NETWORK FROM THE AMERICAN TELEPHONE & TELEGRAPH CO UNDER THIS AGREFMENT, ATAT COULD NOT ENTER CATA COMMUNICATIONS UNDER 300 BAUD 30 CHARECTERS PER SECOND, UNTILL APRIL 1966 MEANWHILE, WHY WOULD ANY OF THE INDEPENDENT TELCOS BUILD WHOLE NEW EXCHANGES FOR THIS PA BELL PLAYTOY? THEY WOULDN'T, OF COURSE THEY TRANSLATE FROM FUNNY TWX AREA CODES TO NORMAL TELEPHONE EXCHANGES FIND THE

RIGHT EXCHANGE, AND WIN THE TWX NETWORK

TRANSLATING THE EXCHANGES

ANNO THE MEHER MODELS.

THERE IS AN EASY WAY OF TRANSLATING A TWX EXCHANGE THAT'S WHEN IT IS "GIVEN" TO YOU IN THE TWX DIRECTORY. TWX AREA CODES ARE USUALLY 510, 710,810, & 910 IN THE UNITED STATES, AND A10 IN CANADA SOME TWX MACHINES HAVE REGULAR TELEPHONE NUMBERS, BECAUSE THEY WERE INSTALLATIONS BEFORE THE MODEL 33 TELETYPE BECAME THE STANDARD OF OF THE TWX NETWORK. THESE OLDER MACHINES HANDLE THEIR OWN LIMITED SPEED CONVERSION, AND COMMUNICATIONS IS POSSIBLE BETWEEN THESE OLD MACHINES,

ANYONE WITH A MODEL 33 (OR EQUIVILENT COMPLITER TERMINAL SUCH AS A COMPUTER DEVICES 1103, TI SILENT TOAL OR TERMIFLEX HT-2> CAN SEND TO A TWX TERMINAL A TWX MACHINE ANSWERS WITH THE SAME "CARRIER" TONE AS A COMPUTER SOES, SO YOUR TERMINAL WILL I IGHT ITS CARRIER LIGHT (IF IT HAS ONE) EACH MODEL 33 HAS A PROGRAMMED "ANSWERBACK" WHEEL IN IT IT IS PROGRAMMED WITH AN IDENTIFIER OF 20 CHARECTERS OR LESS. THE FIRST THREE CHARECTERS ARE HISUALLY CARRAGE RETURN (CR), LINE FEED KLEY- PUB OUT (ROY) THE LAST THREE ARE USUALLY, CP, LF, CONTROL Q. THE CONTROL Q CHARECTOR WILL TURN ON THE PAPER TARE PEADER OF THE DISTANT TERMINAL IF IT IS PROGRAMMED TO DO SO. WHICH MOST ARE: THIS LEAVES 14 CHARECTERS LEFT FOR IDENTIFICATION AN EMAMPLE WOULD BE! NHLWINGSPR DET THIS IS THE ANSWERBACK OF THE DETROIT WINGS OF THE

NATIONAL HOCKEY LEAGUE, AND WOULD FURTHER

SEEM TO BE THEIR PR DEPARTMENT

THE THX NUMBER OF THE WINGS IS 810-221-5033. AS WE LOOK DOWN THE LISTINGS FOR DETROIT IN A 1974 OR EARLIER TWX DIRECTORY (LATER ONES LUMP A WHOLE STATE TOGETHER) WE FIND LISTINGS FOR OLDER INSTALLATIONS. THE EXCHANGES FOR THESE OLDER MACHINES ARE 212-538, 313-222, 213-342, AND 313-755. WHEN WE HIT 222-5032, WE FIND THE AMSWERING TONE OF A TWX MACHINE. OTHER TWX MACHINES IN DETROIT ARE 810-221-5127. DETROIT PO DETA: 810-221-9458 (UNIPOYAL DETA: AND 810-221-5121. MED EXAM DET.)

DET 19. OF COURSE THE CITY CODE OF DETROIT OTHER CITY CODES

ARE NYW FOR NEW YORK. LSA FOR LOS ANGELES,
SEO FOR SAN FRANSISCO. AND
CGO FOR CHICAGO SMALL COMMUNITIES
HAVE FOUR LETTER CITY CODES I DON'T KNOW THE TWO TRANSLATIONS FOR ALL THE AROME CITIES BUT THOSE SENDING
TWO TRANSLATIONS TO TAR WILL GET A LIST OF THE FEW CITIES TRANSLATIONS
ARE AVAILABLE FOR, I HAVE TRANSLATED CITIES WITH TRUCK STOPS. AND SENT MYSELF MESSAGES WHEN TRAVELING.

ANOTHER POSSIBILITY IS TO MAKE FRIENDS WITH SOMEONE WHO WORKS IN A SMALL OFFICE OF A LARGER COMPANY AND USE THEIR TWO MACHINE. THE TRICK THEN IS TO CALL A TWO NUMBER THAT DOES NOT EXSIST AND LET THE PHONE COMPANY COMPUTER TELL YOU WHAT NUMBER IT THINKS YOU DIALED. THIS WORKS FOR YERY FEW CITIES.

EXAMPLE: THE WESTERN UNION TELEGRAPH CO IN UPPER SADDLE RIVER NJ IS 710-988-2251. IF WE DIAL 910-988-2253 ON A THE MACHINE. WE'LL HEAR A RECORDING SAY "THE NUMBER YOU HAVE DIALED: 279-2253. " WHICH TELLS US THAT BY DIBLING 201-279-2251 WE CAN PEACH NU SALES UPSR IF HE THEN LOOK CLOSELY AT THE NUMBER GIVEN FOR THE FYI NEWS SERVICE OFFERED TO TWO SUBSCRIBERS, THE NUMBER GIVEN IS 910-988-5956 BY DIALING 201-279-5956 AND THROWING THE HAND-SET INTO THE ACCOUNTIC COUPLER. OUR TERMINAL TYPES OUT "NU FYI MANA" THE ANSWERBACK OF IBM SYSTEM 7 COMPUTER LOCATED IN MAHMAH NJ THIS MACHINE IS UPDATED ONCE AN HOUR BY UP! OVER DEDICATED BACKED UP LEASED LINES. AS THE COMPUTER SENDS ITS ANSWERBACK, IT TRANSMITTS CONTROL E CONTROL E SHOULD TRIP THE ANSWERBACK OF THE CALLING THE MACHINE. SINCE THE COMPUTER WILL GO NO.

FURTHER UNTILL IT RECIEVES SOMTHING.

TYPE IN ANY PANDOM CHARECTERS * "DOXXXX" *

AND IT WILL LET YOU IN TYPE CATALOG

OR TUST "CATA" AS IT ONLY "SEES" THE FIRST

FOUR CHARECTERS AFTER A SPACE YOU

CAN TYPE "NEWS WERT SPOR * CR * " AND IT

WILL GIVE YOU THE LATEST NEWS, WEATHER

FOR 20 CITIES, AND SPORTS, THE

CATALOG GIVES INSTRUCTIONS AND TELLS

YOU WHAT INFORMATION IS AVAILABLE. THIS

IS A "DIAL-A-JOKE" TYPE SERVICE, PAID

FOR BY THE LINE CHARGES OF THE LONG

DISTANCE CALL IN REACHING IT

IT SHOULD BE NOTED THAT YOUR TERMINAL SHOULD BE SET FOR 110 BAUD, AND EVEN OR NO PARITY HAVE FUN, HAPPY

TWX R4 PHREAKS

ATTN: MILO FONEBILL

HACKING, AND REMEMBER,

Please get in touch with me through the TAP office.

Tom Edison

COMING NEXT ISSUE!!!

Our next issue, #50, marks the 7th anniversary of TAP. To mark the occasion, issue #50 will be a special double edition with color pages. I want this to be the best fuckin issue of TAP that we've ever put but! I'm asking all of our readers, especially those who have sat on their fat asses and done nothing to help out over the past years, to send in information, newsclips, articles, and adjumns. I want i pages just bursting with technical knowledge. Lets show Bell that we DO care!

LETTERS FROM READERS

Dear TAP,

Perhaps some of your readers would like to chat with ships on the high seas. This is now possible through a satellite called Marisat. Actually there are two currently operational: Atlantic and Pacific, and in a very short time there will be one for the Indian Ocean too. Enclosed is a list of most of the ships that you can contact and the list continues to grow. To place a call: engage your favorite 800 or 555 number, then box off to 800-243-3640 (or 264-9090 in Conn.). This gets you the Marisat operator. She will ask you billing information, so you should have a story made up as to who (what individual/or company) is calling and give her a number to bill it to (like IBM or Continental Bakery, or whatever). She doesn't have any way (presently) of knowing where the call is coming from. (It's going to cost somebody 10 bucks a min-

a number to bill it to (like IBM or Continental Bakery, or whatever). She doesn't have any way (presently) of knowing where the call is coming from. (It's going to cost somebody 10 bucks a minute!) And be a good guy and give her the ship's number (like SS Jonsson #1560201) and tell her you want to speak with.... oh, what the hell, the chief stewart or cabin boy - anyway, the radio operator will get the call and you can bullshit with him. Sparks can tell you where the ship is, courses, speed, destination, etc. Comsat has some other numbers that might prove fruitful if somebody knows how to exploit them: (203) 264-9030 is Data Test (associated digits 1800-922-4646, which may be a computer entry code?), 264-9040, 264-9050 (data set), and 264-9060. You might

Has anybody ever "boxed" calls through TWX? I don't know if it's it's a usable system. (See article on TWX phreaking by Osbert Kilgallen in this issue of TAP.) Anyway Marisat has Telex capability too: 710-581-5920 (toll free). Additionally, AT&T long lines is 914-682-8252 and the United Nations language bank (free translations?) is 212-686-3061.

May the force be with you,

Greetings,

also try 264-4091/4092.

In Missouri, Southwestern Bell has forced itself upon an unwilling public. They now charge 20¢ per directory assistance call (after the first five free ones per month).

Well, in a burst of insight it came to me--and it has

Call the 555-1212 number, using the 1 code, omitting the area code (as in calling directory assistance for another town in your area code). When the operator asks you "What city please?" just say the name of your town (in my

"What city please?" just say the name of your town (in my case St. Louis) -- and she says "go shead." They have no way of knowing what town you are disling from! And there is no charge for the 55501212 number.

I also, note that Kansas City, Mo 555-1212 info uses computers to retrieve telephone numbers. When will I be able

Back Issues are 50¢ each.

Sucscriptions - 10 issues - US Bulk rate 35.
US First Class in plain sealed envelope 37.

Janada & Mexico First Class \$7.

Fireign \$8.

IMPORTANT! Include mailing label or Xerox copy when writing to TAP about your subscription.

Birk - Manopoly \$1.23.

Electronics Courses - \$0¢ each. A - DC Basics,
B - AC Basics, C - Phone Basics, D - Amplifiers.

TAP mugs - \$4.50.

TAP T-shirts - \$4.50. Specify size and color: Small Mailing of Firest Lance.

TAP T-shirts - \$4.50. Specify size and color: Small, Medium, Large, Extra Large. Black or red T-shirt with white TAP logo.

TAP "Ma Bell is A Cheap Mother" T-shirts - \$4.50.

Specify size and color: Medium, Large, Extra Large.

Blue, tan, or yellow.

Blue, man, in yellow.

Send CNLY theck or miney order (No Cash) to:

TAP, Romatil the Mest 42 Street, New York, N.Y. 10036

This is a small then also.

THIS I THE Broadway. Romatile. New York, N.Y. 10001

HOURS: WEDNESDAY, Joe & pm.

Shipboard Terminal installations:

At blass time, the to twing vesses were equipped with shipboard terminals which have been commissioned for operation with the Marisat System.

Telegnone

Telex Number

Answerback

Country of

Registration

Al Hasa Panama 1330701 HCWD 1330701 Alaskan Star #GPJ 1531511 United States American Ace #F09 1500101 United States 1500101 AQuatru's united States WSKS 1500*12 Arco Anchorage 1501104 WORD INSTITUTE Arco Faribanius United States WGWB 1501103 Arco Juneau #S8G 1501102 Umied States Arco Prushoe Bay #PFD 150110 United States Altevida Denmark. 2VR2 26:011 Son Ocean Lancer United Kingdon GUUU 24404 Cable Venture GUNZ 2440112 United Kingdom Chevron Haway MINED 156040 United States WBGF 1501576 1501516 University States Donghae Ho HYSA 3743101 Sauch Arabia Duchess Diane MGNA 1501574 United States Esso Banghon Panama 1330101 HPXD 1330101 Esso Copennagen 1240102 ELSJ 1240112 HPDA 1330112 Esso Maiacca 1330102 Essa Philippines HPKW 1330103 Panama Esso Wilhelmshavin ELVX 1240 1240:01 Fred H Moore United States 1500602 MOBL 1500502 Golden Bear United States 1500501 WE20 1500501 Indian Seal 1503201 United States SEAL 1503201 2370101 Sweden SLAT 2370101 Jonsson Canada VYXD 1560201 KDO Maru 3203177 JGCC 3203177 King Öscar United States WYVC 1501201 Kurama-Maru JDDG 3200112 LASH Atlantico United States WEZU 1500271 LASH Italia United States WJAY 1500204 LASH Pacifico United States WIEE 1500202 LASH Terhiye United States WMIG 1500223 John A. MacDonald Carrada CG8K 1560101 Mercury 2440101 United Kingdom GJXH 2440101 Messiniahi Chara Greece SXRN 2130101 Moon Aero United States WLBY 1500601 Monnucstar United States 1500301 KGOF 1500301 Nai Maria Amena ISBry (BFR 2150201 United States 1501575 KPKV 1501575 Ocean Range Panama HENB 1330702 Portobello Panama 1330402 HPBJ 1330402 Phaedra United States 1501573 WPSH 1501573 Puerto Frica United States MFJK 1503202 United States Li S Olympic 1503216 WYZO 1503216 Paceseller III United States WD8T 1501477 Post Enterprise United Kingdom GUNL 2440201 United Kingdom Queen Enzabeth 2 2440301 GBTT 2440301 Royal Villing Sea Norway 2310101 LECK - 2310101 Sedca-709 United States KBCG 1500603 Seamic Explorer United States 1501478 WRHC 1501476 Texaco Georgia United States WLDW 1502111 Wild Gannett United Kingdom GWAQ 2440202

Dear Thr:

I understand that at some point in the recent past your readers, or your magazine itself were interested in knowing the frequencies for those digits that come after 9.

* (11) 941.0 + 1336.0 * (11) 941.0 + 1209.0 * (12) 941.0 + 1477.0 (13) 697.0 + 1633.0 (14) 770.0 + 1633.0 (15) 852.0 4 1633.0 (16) 941.0 + 1633.0 (17) 350.0 + 440.0

this information is available through many publications e.g. branco Controls Division, Ledex Inc., College and South Streets, siqua Chio -5356, (513) 773-8271. I trust this information will not be used for anything illegal or foolhardy. Branco's booklet could give you more information.

one lonely Canadian



Phone Call Is Rated X Scattle (UPI) — It may work for Superman, but changing your clothes in a public telephone booth can mean trouble for the rest of us Iluber Martin, 31, stepped into a glass phone booth next to a public park and exposed himself while changing trousers, police said. He was arrested for changing into

blue denim cutoffs while 25 to 30

persons of both sexes looked on.

When I posed for the picture that accompanied the interview article in The Village Voice, reprinted in TAP #48, I had no idea that so many readers and friends would write in to ask where those "Ma Bell Is A Cheap Mother" T-shirts could be bought. The original shirt was made up special for me by a real Bell employee! I find it refreshing to know what Ma Bell employees REALLY think of Ma. As a result of all this reader interest, TAP now has a supply of "Cheap Mother" T's. This T-shirt is available in three colors, yellow, blue, and tan. Sizes - Medium, Large, and Extra Large. Cost: \$4 plus 50¢ postage. Total: \$4.50. Be the first on your block to show Ma what YOU really think of HER!

GET MUGGED!!!

That's right, get mugged!!! Start off the New Year right by getting your TAP mug. The mug is white with black TAP logo, 11 onces, and stackable. Excellent for coffee, juice, beer or for using as a planter for your Columbian Gold! Cost: \$4 plus 50¢ for postage. Total: \$4.50. If you're a cheap mother yourself, stop by the TAP office on Wednesdays to pick up your mug and save the 50¢ postage charge.

AT&T's Profits Up 17% in Qtr

American Telephone & Telegraph Co posted its fifth consecutive billiondollar quarter yesterday, reporting profits in the three months ended Aug. 31 climbed 17% to \$1 19 billion. AT&T's revenues in the period rose 10% to \$9.15 billion. John D. deButts, chairman, said that while earnings show sustained improvements there are still a number of states "where earnings fall alguificantly below the level required to support continuing growth and modernization of Bell System facilities ' In these areas, the company will continue to seek rate increases, he said, adding: "in the main, however, our aim is to increase earnings without raising

HELP ROLL BACK PAY PHONE COSTS!

Please do not use this telephone unless your call is of an emergency nature. For more information write: Committee For A Five Cent Phone Call — P.O. Box 30669 — Seattle, Washington 98103.

FLASH! LATE REPORT

KON-KLAVE KANCELLED

by Cheshire

There was to be a Phone Phreak Konklave at the New York Coliseum running concurrently with the Personal Computing Expo (PCX) over the Halloween weekend. About 1/4 of the TAP mailing list (those in the "Bos-Wash" and a few west-coasters) got the word a week or so before the event. The evening before the event was to begin, I was approached by people from Byte magazine, a co-sponsor of PCX. It should be explained that all negotiations had been handled by H A Bruno Associates in New York, who had arranged to rent the Coliseum for the show. I had already checked that no nearby hotel had function rooms (I didn't bother checking the Central Park South hotels), and approached Bruno Assoc. as a representative of a Communications Hobbyist Group wishing to rent function space. When the folks from Byte came into town, they had a fit.

In June 1975, 73 magazine published the schematic diagram for a Blue Box. Pa Bell came down hard, and sued The Magazine, The Publisher, and The General Manager. The judgement that each one signed stated that none of them would ever again aid, abet, or otherwise help Phone Phreaks again, etc. If the Phreaks held their meeting, it might be construed that Byte, and in particular, Byte's Publisher (then General Manager of 73) was aiding Phone Phreaks, and Byte magazine would no longer exist. This was not designated a goodness.

The meeting was cancelled, flyers were printed up to state this, but we were requested not to release details until after the weekend. This request was also honored. However, as we handed the flyers out, we informed the recipient that we intended to cry into our beer over the cancellation at 4PM at the cafeteria.

Oh yeah, why did we try to have a konklave? Because any Phreak worth his whistle knows that digital is the way of the future. We expected a lot of our friends would be attending anyway and wanted to get together.

We'll see you soon.

Published for informational purposes only by Youth Hot Line Reports, Inc.

Address all mail and checks to:

TAP,ROOM 418, 152 W.42ST, NY 10036

Employes Find Ways To Steal

There are 415 known ways to steal money and/or goods from employers and new methods are being discovered almost every day,according to a recent study by the Dale System, Inc. "A clerk in a busy New York City candy store under-rings every sale by one penny and takes home \$5 a day - for 22 years A supermarket manager in Oklahoma City sets up his own cash register at peak periods and in three months collects \$75,000 his employers never knew about," noted Dale statisticians.

49

Downloaded from www.artofhacking.com