Downloaded from www.artofhacking.com

TAP has changed both its name and address. We are now the:

Technological Assistance Program

TAP's new address is:

TAP
ROOM 603
147 W. 42 ST.
NEW YORK 10036

TAP

SEPT - OCT 1979 **No. 59**

A name change was appropriate because with this issue of TAP we begin a new era in publishing. For the last year we were crippled by a lack of mailing labels, caused by Al Bell's screw up. It has taken this long to reorganize the master subscription list but the task is finally done. On August 8, 1979 I mailed out issues 57 & 58 and on September 1, 1979 I mailed out 59 & 60. We will continue to run on schedule. TAP will be mailed out on Jan. 1, May 1, and Sept. 1. All submitted work MUST be typewritten with a 5 inch type column width. There will be NO exceptions!!! Deadline for all submitted articles is one month before publication dates. The same deadlines apply to ads for our new classified sheet (Dec. 1, April 1, and Aug. 1). Speaking about our new ad sheet, I hope that you will take advantage of our low rates. If this sheet cannot become self-supporting, I will be forced to cancel it.

On April 22, 1979 TAP sponsored our annual convention, THC-79, at the Diplomat Hotel in New York City. A large crowd gathered to hear seminars on topics ranging from the use of MF tones in signaling to the use of atomic power. Bell training films on ESS were shown. Available at the convention for both group and private discussion were: Al Mundy, Mr. Phelps, Cheshire Catalyst, Ted Vail, Sam Tobe, Agent MDA, the Litchfield Larcenist, Computer Wizard, Peter Piper, and of course yours truly, Tom Edison. If you would like to help plan the next TAP-Con or you would just like the opportunity to rap with the TAP staff, we "meat" every Friday night at DIONYSIA, Jones & W. 4th St., Greenwich Village, New York City from 5:00 PM to 8:00 PM.

The following letter from John Draper (a.k.a. Capt Crunch) was distributed at THC-79. I thought you'd all like to read it.

GREETINGS---

Since I am not attending THC-79, I have prepared this letter to be read so that my current status and intentions can be clearly made known to those individuals who may be interested.

The most important thing I have to say is that, for several reasons, I have permanently retired from phone phreaking. This is not the result of any personal dispute with phone phreaks themselves (although we are all aware of those individuals that play both sides), but rather a realistic decision that it's time to move on to new areas of legitimate interest, such as professional computer programming. So to preserve my personal privacy and freedom, I have chosen to remain as far removed from any and all phreaking activities as possible, and wish to have no further contact with phreaks or other individuals who may have similar interests.

While I am currently serving a sentence for my third conviction under the toll-fraud laws (in this instance, for violating conditions of my probation due to the Pennsylvania arrest), with a release date set for late summer of this year, my main purpose now and in the future is to pursue those goals, like programming, which I now find more rewarding in both personal and economic ways. Besides, computers are fun, too! So, in parting, remember to stay free, take care, and get high (as in technology, that is)!

Sincerely yours,

John Draper

Editor's note: John was recently released from the California slammer.

"Number please, Your Majesty?"

THE EXISTENCE of numerous special procedures designed to give government officials and VIPs special facilities in the public phone system has now been disclosed.

The *Operating Handbook*, the bible of Post Office telephone operators, gives full details on how to handle *Royal*, *Exercise*, *Pool*, and many other special calls, as well as special procedures like call tracing and checking the numbers of phone users. A copy of the *Operating Handbook* was sent anonymously to a London based magazine recently.

Government officials, the army, and royalty all have their own special priority service, which may be used merely by phoning the operator and saying the right thing. 'We should like a royal call to...' is all, surprisingly, that is necessary. Royal calls can be made 'by members of the British Royal Household', and are 'URGENT... (and) cannot tolerate any delay that might be in force'.

Officials of the government, public corporations, and the armed forces can get the same treatment by demanding a Government urgent, civil urgent or service urgent call. Exercise calls, the handbook goes on to say, are made by members of the Home Office and the Armed Services sometimes in co-operation with the local Police Force' – presumably with the intention of setting up a police/military communications system during exercises.

Part of the public long-distance network, it is revealed, are separated as a 'Trunk Pool' which can be taken over at whim by Government Departments – and 'selected subscribers'. Trunk pool lines and the trunk subscribers together are believed to form the core of the Post Office's top secret Defence Network Emergency Manual Switching System. If even the simple procedures for disconnecting 'unimportant' telephones in case of war are not sufficient, then carefully selected operators will retreat to fallout protected emergency switchboards underground, in the basement of large telephone exchanges.

Mischievous subscribers could, it appears, wreak havoc by using the *Prolonged Uninterrupted Telephone* call system. If anyone claiming to be a government department asks an operator for a *PUT* call, the call is set up indefinitely – operators are not allowed to monitor or disconnect the call once set up. Only supervisors are allowed to disconnect and if asked by both callers. Or perhaps, after the call has passed its first birthday!

Undercurrents #16

Due to space limitations, this article and the letter below addressed to Jim Phelps were not in the last issue.

Dear JP,

The P O is considering stopping collect calls as fraud from people calling pay phones collect has soared to "alarming proportions". Germany has already discontinued this service.

Another simple method of fraud is the "booked call" procedure, where you book a call for a certain time to any national or international #. All you need to do is to book the call from a domestic phone to a payphone for whatever time you want to make the call and make sure you're at the payphone at the right time to receive it.

Please reprint the Undercurrents article "Number please, Your Majesty". All you have to do to make a free call in the U K is to say to the operator "This is the Post Office here, can I have a service call please (or a 'service urgent call' if you're in a hurry). The operator will ask your number and the number you're calling, but since engineers on customers' premises often call engineers on other customers' premises there is never any comeback. Bell engineers must also use the same kind of method. Just listen the next time you have an engineer around who wants to call his base.

Botheinternational and national telegrams and calls can be sent and made via the operator by giving as your # the # of a multi-line business on your exchange. As I mentioned in #43 there is no way these can be checked or that you can be caught (unless your phone is tapped). Please choose #s of multinational corps. that can afford it.

For those of you who may not have understood all the terms in #43, CCITT v.24 (not volume) modems (data sets) are used in Western Europe and the data tones used here are incompatible with RS232 (Bell standard) modems. When I said the P O stinks, it's because it rents 300 bits per second modems at £100 per annum (which can be bought outright elsewhere for $80 or so). Of course the P O has a total monopoly of these here. If you're interested KP0441278606IST gives a demo of all the data tones used in the U K.

"TKO'ing" is Trunk Offering by which the operator or Feds use special lines to intercept calls in progress and to check if the caller has given a true own #.

Depravo

VIDEO VISIONARY by The Wizard

WHAT??? RENT A BOX TO WATCH MOVIES??? FOR $15+ A MONTH??? HERE'S HOW TO BUILD YOUR OWN...

If you are living in the New York vicinity, you are probably receiving entire, uncensored, and unedited fairly recent movies right at your antenna terminals. To watch them, all you need to do is add this circuit to your T.V. and buy some popcorn.

The decoding process itself is very basic, but building one that works is moderately involved. You will qualify as an active filter expert after you complete it.

Tuning channel 68 (or 60 for New York) during Pay T.V. broadcasts (8 PM to 2 AM) will bring in a dark picture with a white pedestal that tears with the picture. To "decode" the picture, the pedestal must be offset back into the black region where it belongs. Your T.V. will now sync on it, the color burst will retyrn, and the AGC will properly limit again. The decoder box will provide movie audio output to your amplifier and speaker.

The transmitted audio portion of the station's signal is very similar to that of an FM stereo broadcast station. There is a pilot tone and a subcarrier for the rest of the audio. The pilot tone is at 15.738 KHz (in phase with the horizontal sync of the picture) and the movie audio is single-sideband which requires a 31.476 KHz injected carrier for product detection. Notice that the carrier frequency is double the horizontal sync frequency.

I recommend that you install a DPDT switch on your T.V. and use it to switch the detected audio from your T.V. to the decoder box, the other half of the switch to remove the de-emphasis cap from the circuit. The first thing you must achieve is to pick off the pilot tone with a peak/notch filter. This filter is tuned to 15.738 KHz with a gain and Q of about 10. The notch output will be discussed later. The peak output will feed your PLL (I used a Harris HA-2825), and a buffer (7438) is attached to the PLL output to boost the current for both the return loop and audio carrier. A /2 (7490) and a sharp filter (Q of 50) is used in the return loop to cause the oscillator to run at 31.476 KHz. The filter is extremely important to reject noise. The output from the 7490 will be a clean sync signal with which you can now easily drive another buffer (the 7438 contains four buffers, so that you still have two spare buffers). This second buffer is used for isolation purposes only. The buffer's out put is now ready to trigger a pulse generator composed of a dual timer (74221 or equivalent). The first half is to be used as a delay. It should be variable over the duration of ½ cycle, or from 0 to 30 usec. The first timer's output triggers the second timer which corresponds to the pedistal offset time, or about 6 usec. A simple circuit can be rigged in your T.V. to offset the pedistal using this +5 volt pulsed signal.

The input to your first video amplifier can be loaded at the proper interval by an externally variable negative voltage on the gate of an FET (the SK3112 is perfect and very conservatively rated for this application). During normal T.V. viewing or during periods between the pedestals on Pay T.V. transmissions, the gate should be driven even more negative so that it pinches off the transistor's effect on your T.V. Minus 4 volts and more negative will pinch it off totally. The less negative voltage will allow leakage from the FET's source (chassis ground) to the drain (attached to your first video amplifier's input). Vary this voltage to give the proper loading offset (too little offset will cause picture tear and too much will cause vertical roll). If the offset bar cannot be located over the pedestal, just invert the input to the first timer by using a third buffer.

The sound recovery is much easier. We will make use of the notch output of the first filter for this. The output was notched at the pilot tone frequency to assure that this would not be detected by the product detector. Another bandpass filter is used to filter out noise from the rest of the spectrum. The audio is upper sideband so tune this filter for a response between 32 and 42 KHz. This signal (along with a greatly attenuated square wave signal from the PLL output buffer as the carrier) will produce good quality audio using a 1496 IC as the product detector, to be passed along to your audio amplifier.

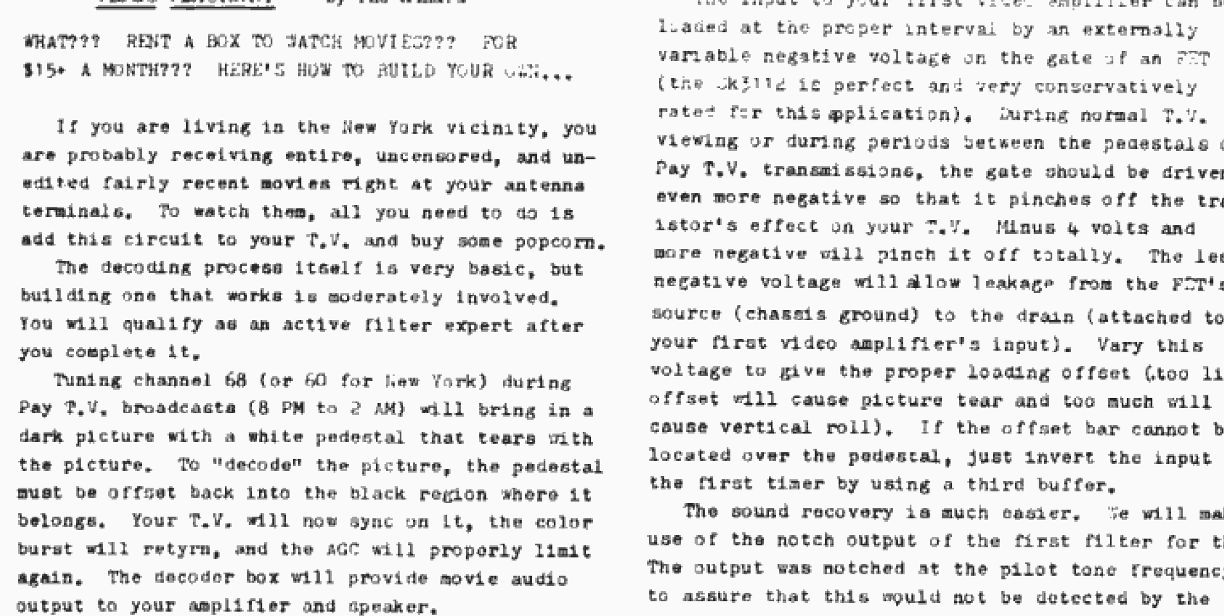
A few cautions regarding active filters; any DC offset voltage on the filter's input will give very disappointing results, so use a .1 uF cap before all filter stages of the circuit. The stability of the filters is also of primary importance. The 3401 (3900) IC is an excellent quad op amp for filters which can be driven with a power supply from 6 to 26 volts or more. Another area of concern is the stability of the dual timer. Drift in the timing caps will create an annoying drift of the pedestal offset delay adjustment. Insufficient filtering in the phase lock loop return will cause picture break-up during action scenes. Inadequate skirts on the 32-42 KHz audio bandpass filter will allow a high degree of video noise residing in the lower sideband area to be detected since the 1496 doesn't know the difference.

All the information necessary for construction of the stages was provided in the IC manufacturer's data books.

I have heard that some cable companies have a movie channel that looks similar to that of channel 68, except that the audio is already provided. Perhaps the audio is not on a subcarrier to keep the signal bandwidth within normal limits. The pilot tone may still be part of the audio signal, or it may be at some other frequency. I would be very interested to learn more about this from anonymous sources. Please pass any info directly to TAP and it will be passed on to me.

Good luck and don't hog the popcorn.

DECODER BLOCK DIAGRAM



A very interesting item is the United States Congress, Title 47, Communication Act. This act is what has been used to have the bans on radar detectors struck down in court. An excellent article on this appeared in the classic issue of Car and Driver September 1977. What this Act of Congress does is to give the right to receive all radio transmissions "to all the people of the United States". What this has the effect of doing is preventing any local, state, or federal government from suppressing your right to reception. It should be noted that Title 47 defines the nature of the signals in a very broad scope. Title 47,Sec 153 (b) "Radio communication or communication by radio of writing, signs, signals, pictures and sounds of all kinds". One other important point is that Sec. 605 of this same act can be used against you in federal court. It states "no person not authorized by the sender shall divulge or publish the existance, contents, substance, purport, effect, or meaning of such intercepted communication to any person". One other item that is interesting is that the regulations for CB radios REQUIRE the license to be posted in a clearly vissible place and if a copy is posted it MUST indicate the location of the origional. So if the man (bear) stops you and you find out he has a CB VERY POLITELY inquire of the license, if there is one and where it is. Also have on hand a copy of Part 95 which lists this rule. Then if he issues you a ticket, etc. POLITELY ask if he will accompany you to the headquarters since you understand he was only doing his job, and you would like to file a complaint about the improperly licensed transmitter. If you are POLITE and not high strung and know the facts exactly, chances are the entire matter on his side and yours may wash out and you may never see the desk sargent. If you do then stick to the EXACT FACTS.

Enough of the preliminaries already. The entire point of this is that you can legally receive ANYTHING if you keep it to yourself. This brings up one point of interest in the TAP office area. WOMETCO home movies, which is on UHF Channel 68. They scramble the signal and for $14.95 a month or $179.45 a year you can get a little box and small UHF antenna which decodes the picture and sound. Now the request WHAT IS THE BOX and WHAT IS THE METHOD OF SIGNAL ENCODING. With this information you can construct your own box (possible not for resale since it may be patented if so the patent office has the details and a copy can be obtained from them). AND ITS ALL LEGAL the US Congress gave us ALL the right. So get busy with the info and contact TAP. There are those of us who can construct the unit with enough details and make up a PC board which can be printed. A couple of ideas are that the sync pulse is inverted or otherwise changed, and the audio is shifted in frequency within the transmitted bandwidth, since you receive a 'tearing' picture but with an anouncers voice telling you how to get the service. There maybe other areas in the US and World with similar systems. IT IS VITAL THAT INFORMATION BE FOWARDED FOR THIS LEGAL ACTIVITY since TAP is one of the only medias that can pass it along to other interested parties.

One other interesting LEGAL idea is that atleast one and possibly several nationwide networks are being set up or operating that use satellites to provide coast to coast service for relaying cable TV movies etc. What an interesting idea, to receive this info, decode it and display it at no user fee. But there is one slight draw back, most microwave equipment is very expensive, so home brewed ideas are a must.

Tom Edison ...... Editor-in-Chief

Staff Writers.....
Cheshire Catalyst, Jim Phelps, Alexander Mundy, Computer Wizard,

Feature Writers .....
Agent MDA, Oz Y. Mandias, Sam Tobe, Ted Vail, The Magician

Contributing Writers .....
Dr. Charles A. Forbin, Robert Neville, Nickolai Testicle, Peter Piper

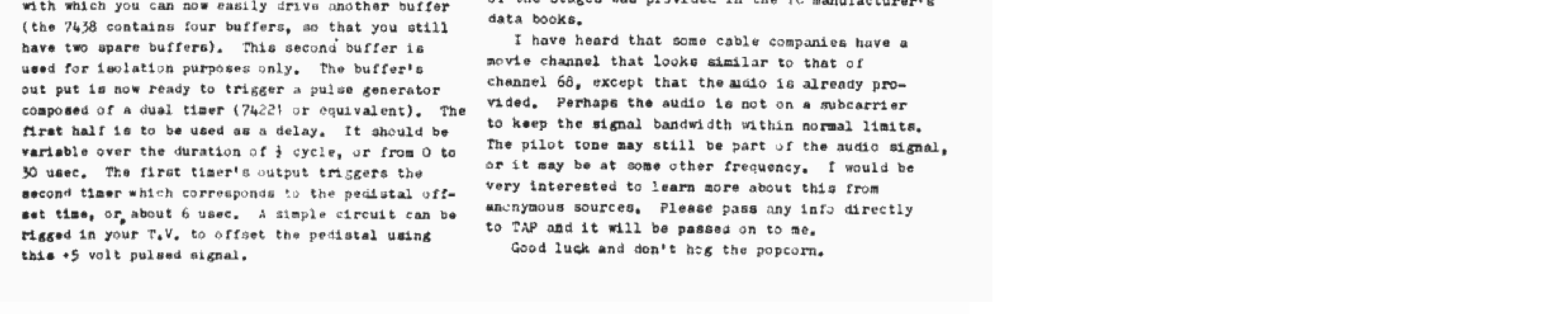
Consultation, Syntax, and Complaints .....
Jim Phelps

TAP is published bi-monthly for informational purposes only by Youth Hot Line Reports, Inc. Address all mail and checks to: TAP, Room 603, 147 West 42nd Street, New York, N.Y. 10036.

Back Issues are 50¢ each. Issue #50 is $1.00.
Subscriptions - 10 issues - $5 Bulk rate $5.
US First Class in plain sealed envelope $7.
Canada & Mexico First Class $7.
Foreign $8.
IMPORTANT! Include mailing label or Xerox copy when writing to TAP about your subscription.
Electronics Courses - 50¢ 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, Medium, Large, Extra Large. Black or red T-shirt with white TAP logo.
TAP "Cracked Bell" Button - 50¢ each.
TAP Cassette Tape - $3.50. Hear Capt Crunch, Al Bell, Joe Engressia, and Bell Security Chief John Doherty.
TAP "The Telephone #1" artist print - $3.50. Mounting instructions for Box concealment included.
TAP "Ma Bell Is A Cheap Mother" Patch - $1.50.

Send cash, check, or money order to:

TAP
Room 603
147 West 42nd Street
New York, N.Y. 10036



TAP, Room 603, 147 W. 42 St., NY 10036

59

Downloaded from www.artofhacking.com