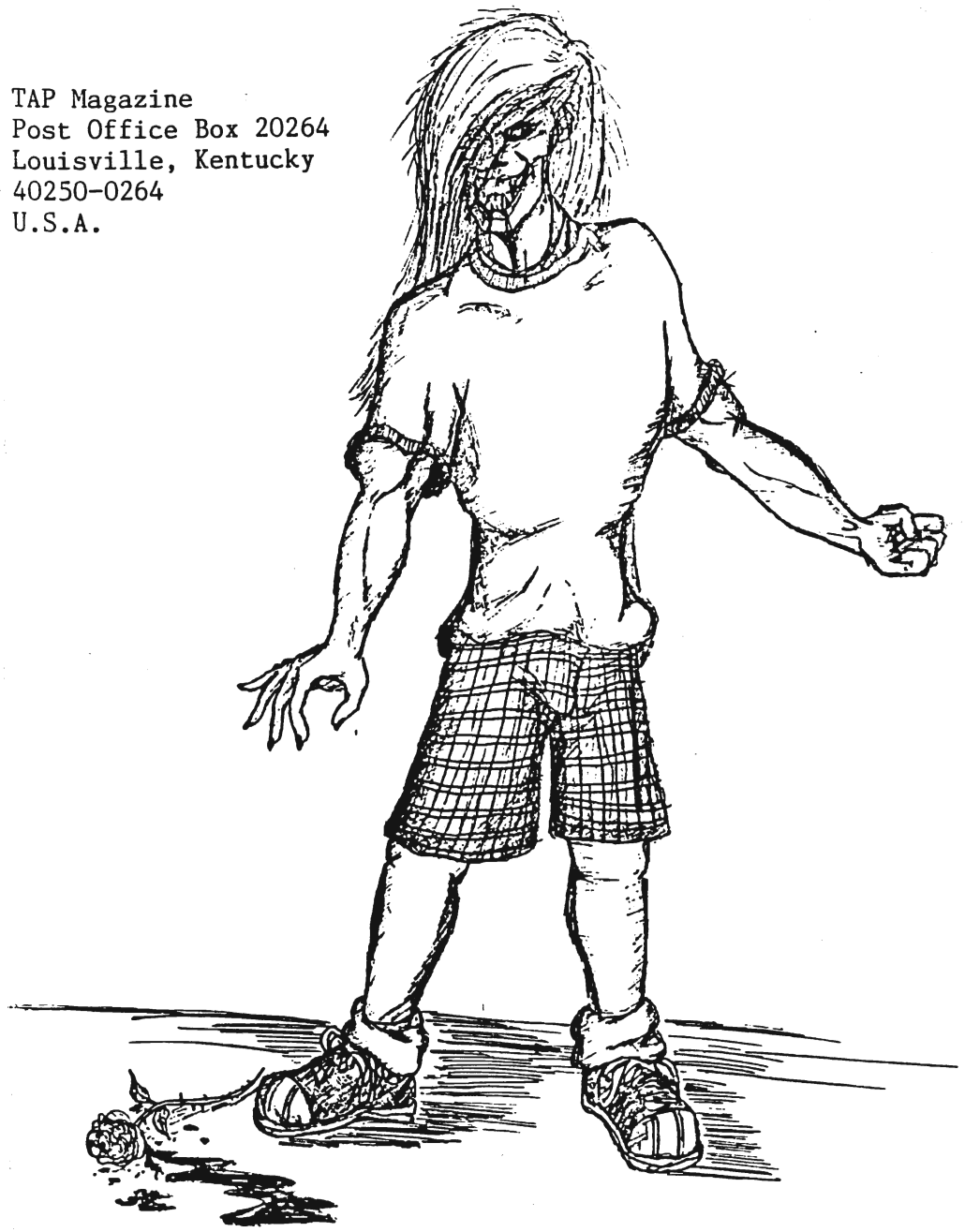
TAP

Issue #103
February 1991
$2.00

TAP Magazine
Post Office Box 20264
Louisville, Kentucky
40250-0264
U.S.A.



TAP Magazine
Post Office Box 20264
Louisville, Kentucky
40250-0264

GEEK ATTACK

NOT FOR HUMAN USE

Contents of Issue #103
-------- -- ----- ----

Contents Page 1
TAP News Page 2
TAP RAP 103 Page 3
DNA Box Part 2 Page 4
The Perfect Wilson by Cthulhu Pages 5-8
The Chronicle Page 9 & 10
The Dictator exposed from CUD Pages 11-13
Bells $100.00 Idea Page 14
WWIV Call Analysis for the BBS Page 15
ATM Fraud by Count Zero Pages 16-18

GRAB!

Frontier technology, glasnost, Jung, Reich, lost history, translations, original prose fiction, graphic arts, video, film, reviews, contact resources, orgone, utopians, Forteans, mail art, millenarians, poetry, philosophy, UFOs, satire, ranters, imported underground periodicals and books from UK, Australia and Canada...

RECEIVE 52-PAGE CATALOG SEND NAME, ADDRESS AND $1.00 TO:

FLATLAND
BOX 2420
FORT BRAGG, CA
95437-2420

*+=+=+=

TAP RAP / Issue 103 by Predat0r

Well here it is, another issue. I have a bunch of random stuff to throw your way so listen up. Thanks go to Reficul for the cover art. Who says hackers can't do anything besides mess with computers? Reficul also did the cover to issue 97. Thanks go to Sinister X for the colored paper used in issue 101 and in 103. The Postal monopoly raised their prices for their Ungodly Snail Paced Service. Twenty nine cents for a stamp. Thats a quarter and four pennies. What kind of stupid price is that? They should have just got another penny out of us and made it an even thirty cents. Here is my $1.16 give me 4 stamps please. What are we paying this increase in price for, even slower service, more lost mail, hell if i know but is has to suck.

TAP has not dealt much with the Operation Sundevil busts or the Phrack case in Chicago. We thought since it was plastered everyplace else we would not force it down your throat too. How many times can you read the same story before it becomes boring? Well i would like to inform our readers that Craig Neidorf the former editor of PHRACK still needs some help in paying his lawyer fees. Since he was molested by Bellsouth and faced false charges for publishing a newsletter most all of us have read i think we owe him a little for his terrible ordeal. Show your support and help out someone who fought the system and won, but doesn't have the bank roll to back him like Bellsouth those corporate bastards.

Neidorf Defense Fund
Katten, Muchin and Zavis
525 West Monroe St #1600
Chicago, IL 60606-3693
Attn: Sheldon Zenner

I have been debating within myself to step up the time of publication from monthly to bi-monthly. I won't know till i see how things shape up during the next couple of months. I can print 20-24 issues a year if i get some articles in here. I have lots of people saying yeah i will write but then i never see anything. I will also be changing TAP around some in its physical layout. As soon as i find a good desk top publishing program i will switch over to it for most of the issues contents. I will start a classifieds page or two in the next issue. If you want something placed in there send it in to me very soon. I might charge for future issues but for now, if you subscribe it's free.

TAP T-shirts might soon be a reality. All i need is a cheap, but good quality place to have them done. If you know of one forward it to me. A complete set of back issues will be ready by spring time. Stay tuned here for details. If your subscription runs out you will not get a fancy reminder in the mail. Just look on the top of your mailing label and it will show you the last issue which you will get. Example if it says 103 on it well this is your last issue. Renew as soon as possible or you will be removed from the mailing list.

Here is a short list of needed items to keep TAP going strong in 91. Articles, hack - phreak - anarchy text files ibm format, new 29 cent stamps, 4 cent make up stamps used with the old 25 cent stamps. IBM bbs or terminal programs for our bbs users. 360k or 720k disks. Copy paper any color is also needed.

THE DNA BOX
Hacking Cellular Phones
by
The Outlaw Telecommandos

P A R T T W O

The previous DNA file discussed the possibility of using Japanese handheld HAM radios and personal computers, or tape recorders to hack Cellular Phone codes, and possible uses for investment & business info obtained by hacking executive and corporate phone calls, and investment info services.

Here I want to mention the obvious idea of simply modifying or replacing the ROMs in a standard Cellular Phone, and disassembling the ROM software that operates the Phone in order to "customize" it for scanning, data monitoring, evesdropping and (of course) making free calls using the codes of registered subscribers.

Simply unplugging the ROMS, putting them on a ROM card for a PC and then copying the software to disk for disassembly is the obvious first step. Use of a logic analyzer to monitor and record activity on the Cellular Phone's digital bus would simplify things by providing a map of where data is stored and which instructions are executed during each period of activity: decoding/sending ID tones, selecting frequencies, dialing, and talking.

Checking the part number on the CPU embedded in the Cellular Phone will tell you which disassembler to use to give a first draft of the ROM code. The next step is to generate a map of the locations of every subroutine call's entry point, any branch & loop locations, and all addresses written to, read, or read-only (to map out any variables and data). Locations incremented, decremented or tested by branch instructions should also be noted, along with their initial and final values.

Each address in the map should be given a symbolic label in your draft of the assembly code. Comments can also be entered with high-level language equivalents that summarize the assembly code as you understand it. Pay special attention to data or loop limits that match elements of the Cellular Phone ID codes (length or contents), or any data locations that are always accessed as a group. This may give you enough info to find the location of the ID code and burn an EPROM with any ID's you've hacked by listening to Cellular Calls.

If you have identified the subroutines that accept phone numbers for dialing, you can patch in a second subroutine that accepts an ID code from the keypad and stores it in RAM before calling out, and modify any routines that utilize ID Codes to use RAM addresses instead of ROM addresses.

Chances are that the software takes up most or all of the available ROM and RAM scratchpad space on the single-chip microprocessor. If this is the case it might be neccessary to piggyback additional memory chips onto the circuit board to hold any new subroutines you want to add.

Suggested new features:
1) Have the Cellular Phone scan for an empty channel and wait for an ID code. Capture the ID code into a table of ID's in RAM and display the captured codes on the liquid crystal display.

2) Program the Cellular Phone to emulate the switching signals and codes sent by PacBell (or your local Cellular carrier), bypassing central switching entirely. This would be useful for making 100% untraceable calls to other

Cellular subscribers within direct radio range. This can be used to do your own routing, emulating a phantom switching cell. This could be used to extend cellular service into an otherwise inaccessible area by coupling your Cellular Phone to a 1.2GHz linear amplifier modified to work in the 800MHz band.

3) Make the Cellular Phone recieve data under one ID/Frequency and retransmit it under another. This would make it impossible to monitor both sides of a conversation. This feature could also be used to implement conference calling by running several calls at once out of one phone.

THE PERFECT WILSON!
by Ctnulhu

It was a cold snowy night. My partner, who's identity shall remain unknown, and I were going door to door. When tried each of the heavy glass pained doors proved to be locked. The campus was closed for winter break. The all the surrounded parking lots were empty. Its was the first time we were able to park so close.

We tried half of the external doors around the building until we reached the loading docks to the sub-levels of University. We were ready to give up when a half hearted yank on a door let me to find it unlocked. It was great! A gentle rush hit us both. This was truly Christmas!

We roamed the halls of the school. Most of the hallways were lit, but we took the long way to the Applied Computer Science offices anyways. On the office doors were taped our keys: the grade reports. Even though I was in my senior year in high school, I felt like I was getting an 'A' for each 'F' I found there. We both stood looking like Charlie Brown, struggling with make shift paper, a pen, and a pencil with a broken lead copying down. All the fail, incomplete, and 'D-' grades with the corresponding students social security number. With a satisfactory amount of them, which was all of them, in hand, we both felt very snug. That feeling grew when we walked in to the unlocked room labled 'MAD VAX' on the other side of the school. Once in the room, we both took off our jackets and got comfortable sitting before the familiar IBM brand ascii terminals. Flipped on our terminals and went to work.

Our plan was to use the login name 'newuser' and enter in as a password our copied social security number from the grade report sheets. This plan was established on the knowledge that all the system users recieve notices that they have an account on the system. This notice tells them to enter 'newuser' as a login name and then to enter their social security number as a password. When we listed the password file we could see who had not activated their account by the 'nopass' entry instead of an encrypted password in the password field. Yet the hardest part was obtaining the social security numbers that corresponded with the target accounts.

To obtain the numbers we tried hopping over false ceilings to get into locked rooms where such lists might be found. We tried getting the numbers from student librarians and student campus security personel. None of the ideas panned out. The the idea of the grade reports came by accident. Just seeing the papers on the walls and doors seemed like a sign. The theory that students with poor, failed, incomplete, or dropped markings might not have gotten on the system to activate their account. So the grade reports were the password keys to UNIX locks.

When we used most of the social security number passwords up, our feelings of grandure began to fade. As the list diminished we felt that it was a waste. But then finally it happened. One of the accounts opened. The system allowed us to become a newuser. We enterec a new password, as directed by the computer, and then viewed the account's files. It was bare except all the default UNIX configuration files. It worked! It fucking plan worked!

I worked on the new account, first real time I have ever been on UNIX, or any mainframe for that matter. I proded around with commands I knew from UNIX manuals then I went back to trying the 'newuser' logins. But, sadly, that was the only one that did work. out of the listing we scribbled down.

So now knowing the plan worked we thought of whom else has access to the system? Math majors did, my partner thought. It sounded good to me. So we proceeded to copy seemingly related mathematics grade results down. Unfortunatly, many of the prime target grade reports only gave a partial social security number. But if only one number more came through it would be worth it. So we ended up copying reports that weren't quite the type a computer science student would be taking. Since other people would be in those classes we felt the odds were against us more. But we headed back to the the VAX terminal cluster named 'MAD VAX'.

In the hallway, we were standing on a glass bridge over looking the road around the inner campus. When we got half way over a trio of cars passed underneatr us. Panic hit us. One was a police car. Now the the rush we felt before was nothing like the one we felt now! Butterflys in the stomach, the random bursts of the words 'fuck' and 'shit', as well as the rest of the symptoms to fear.

Our reactions were instict. Take off! We headed to the lower levels of the building. We stopped on the ground level right before an exit leading out, to the far side of the campus from my partners car, and a door that lead through one of the basement levels of the school. My partner looked out the door and I checked the basement door. The basement was not lit and it was a straight line through for most of way to the otherside, where the car was.

I began to approach the door and then there he was. The man I can now identify as a 'pig', but at the time I identified him as 'Sir'. He possessed the typical traits of his profession: slow, cocky, subserviant, and very armed. He radioed in our capture, location, names, and addresses. The names were the most difficult thing for

CIA Promises:
This Time No Dirty Tricks

him. He gave each letter to the dispatch as the begining of a word. He even had trouble finding words for some of the letters.

This was my worst nightmare. I was freaking out. My partner was pretty calm about the whole thing until someone else arrived to our hallway, his professor, the chairman on every technical aspect of the entire universisty as well as surrounding communities. The seemingly fragile old man was as imposing to my partner as King Kong to the natives. The professor immediatly began to interrogate him as soon as he was with-in sight. I felt as though the Daleks had landed. The professor had no regard for neither the pig nor me. I was pleased, but my partner was not. The professor systematically launched question after question at him. All of which he of course knew the answer to. My partner looked down and replied that the motive was games. When the professor questioned him on the use of the new accounts to get around the restricting policies of the system, my partner was replying with 'it was to play games'.

I thought he was twisted off his gord. He already has access to all the games on the system. Besides that they all suck! What was his problem. I wondered. Then the professor attacked that exact point. That my partner had access to the systems games. To this my partner had no answer besides saying, 'I don t know. I guess...' Then the satisfied professor closed his interrogation with a rapid speech about the signing of documents restricting usage of the system by any user who violate the system's or another user's security on that system. My partner stated to the idea that the signing wasn't anything he knew of ever doing.

The professor started to leave and the officer, whom was standing at attention with me during the Nazi commander's speech, asked to the effect of if he wanted us to be brought to the station. The professor said as simple, 'yes'. His satisfied looking knod and firm posture with hands behind his back stated he wanted much worst. The idea of the professor ranting a continous, "exterminate! exterminate", in a Dalek voice was his modivation but luckly not his style.

We were escorted through the school's hallways. Areas where, when in the dark, I was lost. Stumbling around, in the delerium of my adreniline high's backlash, until we hit the cold outside. The I calmed down some then. The pig frisked us in our heavy winter clothing against the security squad car. After satisfied that we did not have anything like a computer under our jackets he put us in the car. The stiff hard plastic seat froze my spine and head. I felt tired, which was better than scared at the moment.

We drove to the station . Which turned out to be the radio room and lounge for the pigs a half mile away. We were told to sit down in a twin row of plastic molded chairs and to space ourselves far from each other. The pig took my partner into a nearby room. Asked his a bunch of questions softly. My partner answered them in a normal discusion voice so I could hear. He was sticking to the 'hacking for games' story. I failed to see the logic in it but the professor was no where to be seen so I figured the story was good enough. Better than my lack of a story. After a while I was called in and my partner left the room looking at me with a promising face. I sat down in another oversized kindergaroen chair ne't to the pig. He paid more attention to my name and where I lived than to why I was there. He read off my partners report and asked me to elaborate for him on some points. The points had nothing to do with the situation at all. They were mostly about where we got into the campus, why I was on the campus as a non student, and if I had a computer at home. The answers came easily, instead of how I feared they would. Then he had us sit back in the lounge and he gave us his sympatnys. He told us why the university was so uptight about the computers. He told us we would not even begin to understand what they could do and that the professor was just looking out for its safty. The pig even told us how he would probably have tried to same things if was our age because he is a covid Nintendo game player.

So now I thought Oh my God! Its over! These are the closing remarks to this bad movie! Now we go home to our warm beds and forget it all! Right? Wrong!

The soon officer explaned how come it was a minor that I could not be let go with out a guardian present. Shit! Now here comes the real Nazi, my mother! Sure enough he calls my house and wakes my mother up. Gets her out of bed and over to the campus which is way out in the country. I sweat it out and thank God that the pig did not tell her anything on the fone.

My mother came and took me away with out the pig getting a sentence out. Yeah! I forgot my mom hates the pigs! She was a hard core activist in college! My luck is turning. My mom did not say anything until we were near home. Then she gave a short blurb about my number of chances and not blowing it. Cool! I am free to live a life away from computers, for a week or so.

My partner kept the whole things secret from his parents. He just drove home and called me on the fone. He had a meeting with the Dean of Students and the Nazi Professor laster as soon as school resumed. The put him on disciplinary suspension. My partner was already on suspension for poor grades. So he was in deep water, almost too deep. Now a year later he has gotten back into the program mysteriously and pulling a grade point average in the three area.

Now, a year after my first 'Wilson', I intend to make it my last one. Now I have worked my way back up on to a platform of observation. Now its time to dive into the pool and swim. No more forgetting to check for empty pools though!

The...Chronicle

Alaska's only real alternative

Published by **Students for Freedom** at the University of Alaska-Fairbanks

INFORMATION ABSORPTION:

The Disney Conspiracy
UFOs • Mass Murder
Subliminal Messages
Weird Science • Hemp

plus

Movie, Music, Book, Catalog, Cult and **Zine Reviews!**

Reviewed in Mike Gunderloy's
FACTSHEET FIVE
$3.00 from 6 Arizona Ave,
Rensselaer, NY 12144-4502

THE ... CHRONICLE Dec. 1988-Apr. 1989: An alternative student paper that's trying to provide a bit of a reality check under a variety of guises. The December issue was **THE CONSUMER CHRONICLE**, examining some of the ins and outs of greed and what it's doing to the planet. April was **THE CONSPIRACY CHRONICLE**, with everything from mass murderers to those politicians running things behind the scenes.

THE CONTROVERSY CHRONICLE Vol. 4 #2: A very alternative school paper from up Alaska way. This issue is filled with all sorts of wild and wooly stuff from the margins: a conspiracy at Disneyland, firsthand reporting from the Exxon oil spill, Nazis in your home town, Majestic 12, and lots else. Some of the printing is a bit marginal, but overall this is great stuff-- a zine that spits in the face of its elders and dares them to make something of it.

THE CONSTITUTION CHRONICLE Vol. 5 #1: About the best student publication I see these days, one which is not afraid to jump off the margins and see the underbelly of reality. This issue has UFO history, mysterious maps of Antarctica, a guide for the first-time LSD user, drugwars and big business, and tattooing, to name a few topics. Wild Stuff.

Students for Freedom is an organization dedicated to using our First Amendment rights to promote freedom of the press and ideas. We openly oppose the mind control and covert manipulation of the Conspiracy! The vehicle for our cause is **The...Chronicle**. Through the use of a technique known as *information absorption*, the vile effects of the Conspiracy's mind control can be defeated!

Students For Freedom
c/o Nathaniel-M. Naske
P.O. Box 80721
Fairbanks, AK 99706 USA

WE REVIEW ZINES!

The **Campaign** Chronicle.....$1
The **Consumer** Chronicle.....$1
The **Conspiracy** Chronicle.....$1
The **Controversy** Chronicle.....$1
The **Constitution** Chronicle.....$1
The **Commercial** Chronicle.....$1

$3 outside of Alaska

WE'LL TRADE FOR YOUR ZINE!

>From ->THE DICTATOR (#156)
Date ->01/12/90 11:08:00 PM

Hey (name deleted)...whats up?

Ask KL to give me a call and let me in on the details, (602-225-8581), or he can leave me mail on Jolnet. I'd rather him call me, instead of having that message pass through the Jolnet system.

Any ways... Ifits in Louie again this year, Im sure I can make it...let him know..thanks.

The Dictator
The Dark Side BBS

++++++++++End Example ++++++++++++++

The reference to "Louie" is to summercon.
The telephone number listed above was left on a public BBS (in a different message) in the general message section by The Dictator in a public request for another user to call him. It is also the number that others have given us independently as one he gave them for voice contact. Hence, the number appears directly and unequivocally linked to The Dictator. Attempts to contact him through that number, however, reach a machine, and the person who responds to that machine has, for several months, refused to return calls collect or otherwise.

Even after allegations of his apparent role in the video tapes of Summercon '88 surfaced, the dictator made no effort to hide his connection to The Dark Side. He left the following in response to several callers bickering among themselves over a Chicago BBS also known as "The Dark Side." He makes it clear the two are separate entities:

The Dictator of The Dark Side and the above messages as also linked to the Secret Service informant by the nature of the logs he provided to them. We will continue to provide details of the substance of the documents in coming issues. However, messages printed in the Secret Service document allude to private e-mail sent to "CI 404-235," and these can be traced to The Dictator as the recipient by examining existing e-mail logs retained or acquired by others.

The Craig Neidorf trial led to the revelation that the Secret Service had video-taped parts of Summercon '88 in St. Louis surrepticiously. One participant at Summercon who also viewed the tapes indicated that the tape captured the events in The Dictator's room from an adjoining room. If true, it indicated that advance cooperation and preparation were necessary between the participant-informant and the tapers.

Why is it necessary to reveal the identity of the informant? We value privacy and we have no wish to embarrass those who may be coerced into performing unnatural acts for the government. However, if the Secret Service are correct, their informant was a willing volunteer who was paid for his services. Those who find betraying alike the innocent and guilty indiscriminantly for monetary gain are as ethically bankrupt as those who buy the service. Our abridged dictionary doesn't contain the term for those who get paid for performing unnatural acts, but it will come to us eventually.

The informant was on a number of boards, and because he reported *FOR MONETARY GAIN*, we cannot be sure how many innocent people had their logs passed on, how these logs may have been edited or interpreted by law enforcement, or what uses were made of the information once acquired. The strangely creative interpretations and cavalier disregard of "reality" by federal prosecutors and some Secret Service agents are too troublesome to allow presumption of good-faith use. We STRONGLY URGE all persons who have been or currently are on a board with The Dictator to search their logs and consider filing a Freedom of Information Act request (see concluding file).

--Begin Phoenix Project Message---
>
>13/100: the dark side
>Name: The Dictator #115
>Date: 10:42 pm Fri Nov 04, 1988
>
>attention:
> the dark side bbs is up and running...any user that wishes to become
>a part of history...please call..this is yet another hard working system
>that wishes to make its mark in computer history.
>
> give us a call..
>
> the dictator
>
>dark side bbs 602-789-9864
>
>summer con '88 members given imddiate access

The number given is different from the one later identified in SS documents as the sting board number. Perhaps it was typo, or perhaps it was and it was presumably changed shortly after this message was left. An anonymous sysop of a board in the Midwest told CuD that the Dictator personally left the number of The Dark Side on the BBS, and recalls at least one public message in which The Dictator left a public message requesting people call it. This BBS in question was a quasi-open board in that--as most boards, including public ones--after a preliminary log-in, virtually everybody who seemed "non-loony" was validated. The point is that The Dictator was ACTIVELY SOLICITING CALLERS OPENLY, and not simply inviting a "select few" to call the board who "demonstrated an interest in conducting criminal activities." One user who documents participation on The Dark Side from shortly after it's inception states that The Dictator encouraged him to tell his friends to call The Dark Side and, at one time shortly after it "went up after being down" actually "seemed desperate for new users."

According to information from several DARK SIDE users and logs they have provided from The Dictator on his own system and on others, The Dictator took an active role in generating message topics. According to one source, The Dictator would rarely provide information, but would attempt to generate seemingly innocent topics that might, in retrospect, provide the kind of "documentary evidence" (especially if take out of context) that could lead to suspicion or to searches. The following were provided as examples of "typical" ways that a discussion topic might be generated. We observed from the responses to these notes (that we deleted), that the innocent question would elicit a technical or potentially incriminating answer of the type used prejudicially in the sentencing memorandum of the Atlanta Three, or of the type used to justify the raid on Steve Jackson Games. The lesson we take from the following is that the Secret Service, through the use of an informant, seems to have *ELICITED* statements that could be used as evidence.

Drawing from the above information, the following suggests that The Dark Side, The Dictator, and a person identifying as (name deleted) are the sting board, the sysop, and the informant, respectively.

1. We have obtained telephone billings and computer telephone logs for December, 1988 and through mid-1989 indicating that when one called (602) 789-9269, The Dark Side BBS was accessed. This suggests that the sting number and The Dark Side were one and the same.

2. A person identifying himself as "The Dictator" called a number of boards in 1988-1990 (among them The Central Office, The Phoenix Project, Hackers' Den, Ripco, and others) and through 1990 continued to call such boards as Atlantis, Ripco, Face-to-Face, BlitzKrieg, and others. In public and private messages on these boards, The Dictator would typically include in his signature both his name and his association with The Dark Side BBS:

** WHAT'S THE POINT? **

****

When the federal government uses *paid* informants, nobody wins. Officially sanctioned deception and betrayal, as Gary Marx argued in his book "Undercover: Police Surveillance in America," is generally far more detrimental to public order in the long run than whatever "crimes" the deception targets.

When federal agencies set up sting boards and use informants to gather, even generate, diverse information that is in turn given to agents as potential "evidence" of wrong doing, there can be problems. In the 1960s and 1970s, we have seen through various class action suits, congressional hearings, FOIA requests, and other inquiries, how abuse of information by those who collected it resulted in lost employment opportunities and other uncool consequences. In the past year, we have also seen the misuse of information in indictments, sentencing memorandums, and especially in several search affidavits and seizure warrants.

Most of us are concerned if agencies collect information on us against our knowledge, because the potential for harm can be subtle. Many readers of CuD have called a variety of bulletin boards considerated to be "underground." When an agency such as the Secret Service sets up a STING board and PAYS an informant to capture logs, those of us who call these boards have reason to be concerned with how our **LEGAL, LEGITIMATE** posts may be interpreted and used by agents. When we recall that one sysop was liked to a fraud conspiracy because of a two line comment that kermit is a 7-bit protocol used primarily on mainframes, our confidence in agents' interpretive competence diminishes.

Our intent has not been to embarrass The Dictator. If it were, we would include the name he uses when socializing with others.

IT WOULD ALSO BE TOTALLY REPREHENSIBLE IF OTHERS WERE TO ENGAGE IN HARASSMENT OR OTHER RESPONSE AGAINST HIM! The CU has increasingly been united by principles of justice, and to engage in unjust acts because we feel others have done the same to us violates those principles we are working toward.

Calls to the "voice number" The Dictator has left on at least one public post on a public board, and given to others, have gone not received a response. Messages left to him on BBSs have also not generated contact. We continue to invite him to contact us and give his side of the story. There are generally shades of grey in even the darkest images, and if he contacts us we promise either a fair and impartial story, or, he can write his own version and we will publish it unedited.

We also remind readers that the issue IS NOT an individual. At stake in all this is the issue of privacy and police power as we enter the 21st century. When laws cannot keep up with technology, the consequences may be ill-considered strategies for monitoring and punishing alleged wrong-doers. As Gary Marx reminds us in his book "Undercover" (p. 233):

> In a democratic society, covert police tactics, along with many of the other surveillance techniques, offer us a queasy ethical and moral paradox. The choice between anarchy and repression is not a happy one, wherever the balance is struck. We are caught on the horns of a moral dilemma. In
>
> Machiavelli's words: (Never) let any state ever believe that it can always adopt safe policies...we never try to escape one difficulty without running into another; but prudence consists in knowing how to recognize the nature of the difficulties and how to choose the least bad as good." Sometimes undercover tactics will be the least bad. Used with great care, they may be a necessary evil. The challenge is to prevent them from becoming an intolerable one.

This was found in a trashing raid.
Bell propaganda at it's best.

"LET'S GROW BETTER"

DO YOU HAVE A GREAT IDEA

BUT NO ONE WILL EVER LISTEN

????????????????????????????????

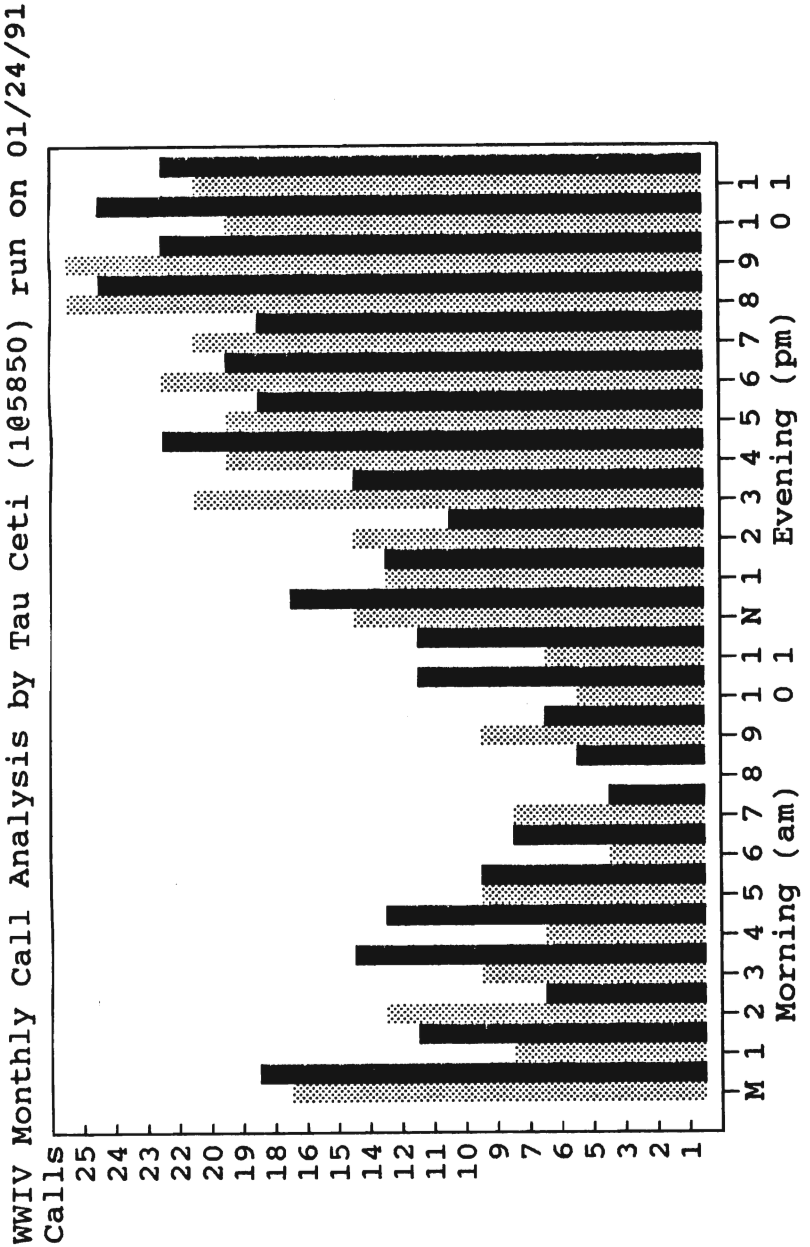
WE'LL LISTEN...AND...WE WILL

PAY $100 CASH FOR IT ! !

NO QUESTIONS ASKED.

ANY IDEA IS WANTED--WHETHER JOB RELATED OR NOT.
ANY ONE CAN ENTER AN IDEA FROM MAY 15 THRU JUNE 15
JUST COMPLETE THE "LETS GROW BETTER" IDEA FORM

I wonder if the guy who thought up caller ID got his hundred bucks worth?



This graph will help you find the best time to call the bbs. The number is 502-499-8933

```
+------------------------------+
|                              |
|  A. T. M.  Fraud Made Easy   |
|                              |
|  summary and research by     |
|        Count Zero            |
|                              |
|  (A CHiNA Info-Net Prod)     |
|                              |
+------------------------------+
```

Have you ever looked longingly upon the sight of your local PULSE machine and thought, "There must be some way that I can make some money REAL easy here."?

Well, there is. But it won't be easy. Protection methods can be overcome, but the technology involved must be understood IN ITS ENTIRETY before an attempt at illegal access is to be made. There are hundreds of people, guests of the state, that figured their plans infallible, only to fall victim to a well-hidden camera.

This article will not be a lesson on HOW to break into the machine, it is merely a summary of the operations involved with a normal ATM transaction. This information is being presented on a "for information's sake"-only basis. I, Count Zero, do not promote nor remotely condone any illegal acts of any sort. So there.

I. MAGNETIC STRIP FORMAT

This would seem to be the most efficient method of trying to access illegal sums of cash. You could:

a. steal somebody's card and PIN code
b. synthesize a card
c. attempt to "jackpot" the system

We will only look at option B. As "A" is up to your own devices and "C" has several good text files written about it already. So "B" it is.

Let's look at the format of the data written to the magnetic strips. This has been taken from a recent HARTWELL, INC manual.

```
[ XX XX XX XX XX XX XX XX ] [ YYYY ] [ - 20 CHARS - ] [ ZZ ZZ ZZ ] [ CC CC ]
 \----------------------/  \------/ \--------------/ \----------/ \-------/
   Your individual acct.      PIN      Name of card     Bank route    CHKSUM
     number/serial code       Code        issuee       code/rem.
                                                       access #
```

For validation, each entry is written twice but not written here for ease of typing. But it is repeated in the form of:
"ACCT NUM" "ACCT NUM" "PIN CODE" "PIN CODE" etc...

These codes may be examined by building a simple code-reader as many have done which can be easily interfaced to your IBM-PC. Full plans to be put into a future CHiNA newsletter.

If you were to attempt to write a magnetic strip or change a currently

existing one, you would need to be using a head-write circuit based on the popular Motorola BCX119221-A...C series of head control chips.

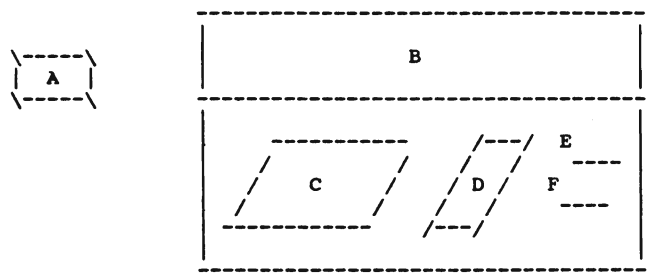
NOTE: Make sure to change the last 2 values! They constitute the checksum of the entry.
Merely add all existing characters written (only the first entry, not both of them) using the following chart:

CHARACTER	VALUE
0..9	0..9
A..Z	10..36
EOL	37
EOT	38
CLR	39
HMX	40
PTT	41
RIA-1	42
RIA-2	43

I doubt anyone in the communications biz needs an explanation of these terms so I'll move on.

II. ATM HARDWARE

Usually consists of:



A. Camera Mount
B. Hidden Voice-Activated recorder & printout link
C. Display Monitor
D. Options buttons
E. Card Slot
F. Receipt Slot

Your machine may vary slightly. But the concept will almost always hold true. Simple rules for each.

A. Wear a paper bag or mask. See also Part II A
B. Do NOT speak. This is the most crucial part! See also Part II A
C. Nothing
D. Wear gloves
E. See Part I
F. TAKE YOUR RECEIPT AND BURN IT!!

One of the neat flaws in many machines made prior to 1989 involved the use of the "CANCEL" button. This button was made to be pressed when the user decided, at any time during the transaction, that he didn't wish to continue. The display would jump immediately to:

"TRANSACTION CANCELLED - CHOOSE ANOTHER?"

This was all well and good, but the machines did not disable this feature between the time your cash was dispensed and you were prompted for your next activity. In effect, you could push the "CANCEL" button after your money has been withdrawn and it would not be added to your account record!

THIS STILL WORKS IN MANY PLACES! OVER 85% OF ALL MACHINES MADE BEFORE MAR. 198 STILL HAVE NOT BEEN UPGRADED.

Although most machines of that period would only work if you were withdrawing amounts larger than $20 (usually $25 is the next possible choice!)
This is ideal if you are using another's card!

II A. CAMERA/SOUND HARDWARE

You can go other routes when dealing with camera systems. You do not have to wear a bag on your head (unless the cosmetic improvement is quite large) Thin alloy metal such as common aluminum/tin foil, which are full of impurities react in a bizarre way when photographed through the special lenses that are commonly used. The effect is to "blur" or "bleed" the image, rendering it indestinguishable from an accident in your local Sherwin-Williams store. Most people prefer to make a "headband" of this metal, lined with copper wire in a sine wave pattern when accosting a machine. You should seriously consider this possibility!
For further reading on this subject, consult:

BANKER'S WORLD - Apr 1989
"Where Have All the Dollars Gone?"
pp 24-29

P. I. - Apr 1989
"The Last Straw"
pp 37-41 (p 38 in particular has a nice diagram. Fig 1)

Sounds, these articles also suggest an indirect method of dealing with the voice-activated recording device. Oddly, a pure square wave tone (roughly around 3100 hz) will cause a major screwup in the sound-sensing abilities of the recorder. It usually will have to be replaced. Suggested volume, given at 6" range is 8.5+ db. Obviously, anything louder will do.

An interesting side-note is that this has become a past-time of suburban teenagers!

Well, hope this gets you started! More will be coming in the next exciting file!