A Cyber 'Zine How-To

LISTENING IN ON CELL PHONES

Monitoring of cellular phone calls is by far easier than you ever expected. Although it will require some specialized equipment, you will have no trouble finding it or operating it

First, you must understand the laws. After April 26, 1994 it became illegal for manufacturers to make scanners that are capable of receiving cellular phone calls or making scanners that are easy converted to receive the cellular bands. You may, however, modify your scanner to receive these bands LEGALLY (it is only ILLEGAL to listen to cellular phones).

Equipment that you need is quite simple. First you will need a scanner. If you don't know what these are, go to Radio Shack and ask to look at them. They will be more than happy to help you. The average price will be between $200 and $400. I recommend the Realistic PRO-2006 or the Uniden Bearcat 890XLT. This is because when the cellular bands are restored, the tuning steps are changed to 30 KHz steps. This is NEEDED for any serious monitoring. The others are O.K. but the tuning steps will be 12.5 KHz, so you will miss half of the transmissions. Also, buy a good cellular phone antenna (magnetic mobile mounts are best). They will actually increase signal strength. These can be bought almost every where so you should have no problems with that. Cellular phones use coax connections called TNC. In order to hook the cellular phone up to your scanner, which uses a BNC or Motorola connection. Again Radio Shack will help. (aren't they nice?) Remember, these are just the basics, you can get as fancy as you want.

Now you must learn how cellular phones work. The phone transmits on its own frequency, chosen by the phone, between the frequencies of 823.98 to 850.98 MHz. These are the frequencies transmitted by the phone to the nearest "cell" site. During cellular phone calls, the call is actually routed through several different cell sites in order to keep the cells open and the transmission clear. It will sound like a loud buzzing noise, and then the transmission will suddenly stop, when cell sites are switched. This is a major disadvantage to cellular phone monitoring but can easily be overcome with a little work of the search function on your scanner.

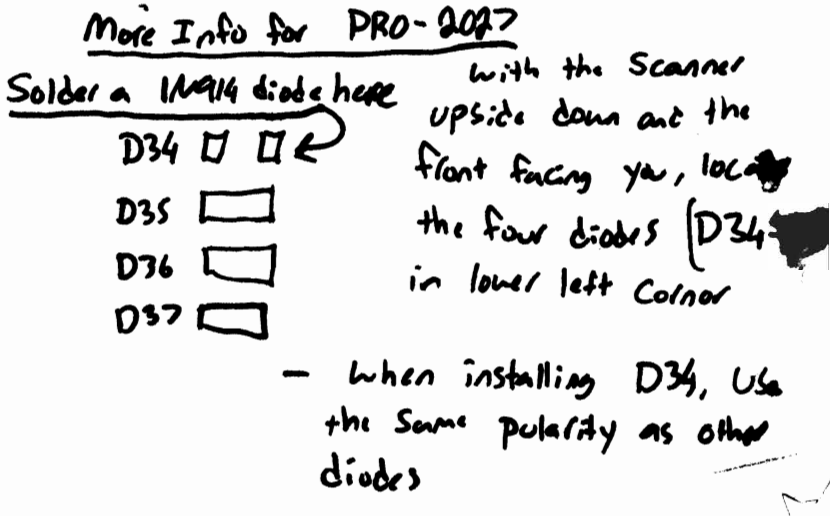
Since you want BOTH sides of the transmission, your going to monitor the 868.98 to 895.98 MHz range. These are the frequencies that the cell sites use. Most of the activity will be in this range, so you don't really have to worry about the other range. You may also find private businesses in this range, like the phone company, and others. The FCC allows private use of some freqs.

Now for the fun part, thanks should go out to all the scanner hackers out there for their knowledge (like Bill Cheek and the Monitoring Times staff).

I will show you how to modify your scanner to receive those bands with simple instructions. I highly recommend Realistic scanners for there ease of manipulation.

PRO-2006 and PRO-2005 scanners:	Cut diode number 502. It is located directly behind the numeral "3" on the scanners keypad.
PRO-2022:	Cut diode number 44. It is located out in the open and you'll find it easily (behind the display) This may also work on the new PRO-2032, I'm not sure, they are basically the exact same scanners.
PRO-2027:	Find the group of diodes in the left, front corner. Take a small signal diode, 1N914, and solder it on the top empty pad. The diodes will be surface mount, i.e. very small.
Uniden 890XLT:	Kinda messed up, see diagram.

When I say cut the diode just cut one leg of it and split it apart. You don't have to unsolder the whole thing.

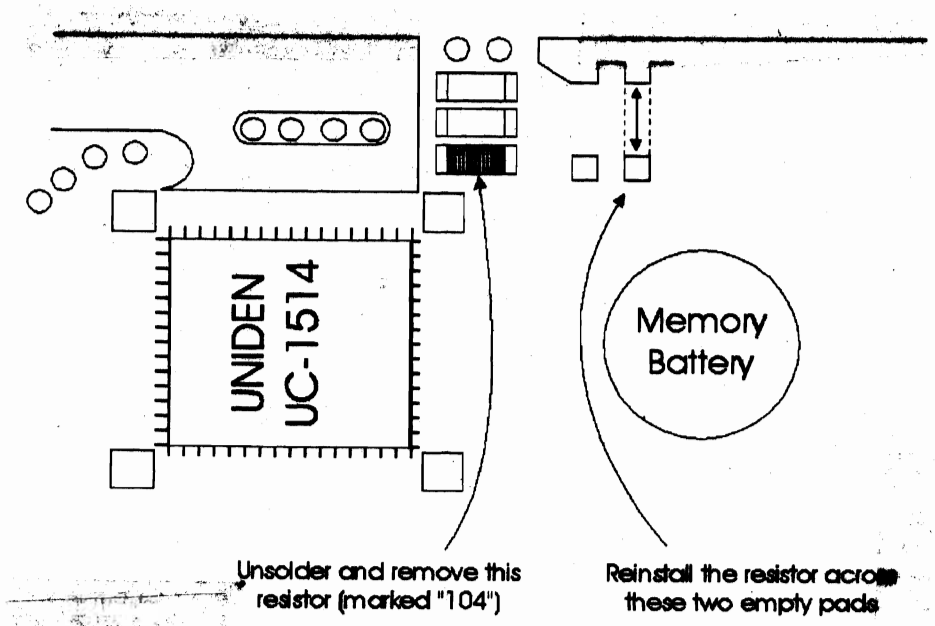


Cellular restoration in the Uniden 890XLT

1. Remove all ten cabinet screws, and carefully separate the halves. Be careful to unplug the speaker wire.
2. Remove the four faceplate screws and the one bracket screw at the center of the main board to loosen the faceplate. Carefully depress the outside edges of the metal faceplate shield and tilt the faceplate downward toward you, exposing the logic board.
3. Unplug connectors J4 and J5 (white and blue wires), and ribbon connectors J501, J502 and J503 (Carefully pull them out). Remove the faceplate and logic board together.
4. Position the circuit board shown in Figure 1, and locate the microprocessor chip (Uniden UC-1514)and the three resistors by the chip's upper right hand corner. Carefully unsolder the closest of the three (marked "104") and reinstall it between the two empty pads closest to the memory battery as shown.
5. Plug in all the connectors, and test it by entering the frequency of 871.2 MHz. That will complete your restoration in the proper 30 KHz steps.

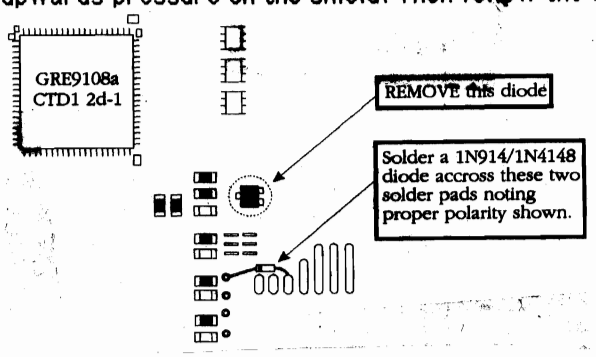
Special thanks goes to Larry Wiland.

Figure 1



JUST IN!! *Cell Modifications For The New PRO-2032*

To do this modification, remove both covers of the scanner. Turn it upside down, with the back facing you. Locate the chrome metal sheild just behind the volume and squelch controls. Unsolder this by using soldering wick and applying gentle upwards pressure on the shield. Then follow the instructions shown below.



Note Polarity!

The diode is available from Radio Shack - Part # - 276-1122 You get 10 for $1.19

Remember to resolder the sheild back on. Its important

Types of computer systems and their default settings

This article will cover some of the more popular operating systems that are found today. I will also include some of the default/common account settings that are normally left open for maintenance access. These are holes used by maintenance personnel to check out the system. Sometimes they are left in, but some times they are taking out. Most of them are not password protected so you can just drop right in.

VMS- This is the VAX computer system made by Digital Equipment Corporation (DEC). It runs the Virtual Memory System (VMS) and has a prompt that looks like this- Username: It will not tell you if you have entered a valid username, and will disconnect after three bad login attempts. Since it is one of the more secure operating systems, the computer will keep track of all failed login attempts and display them to owner of the account on his login. The VAX also has help files available to all users. Just type HELP.

Accounts	Default Passwords
SYSTEM	OPERATOR or MANAGER or SYSTEM or SYSLIB
OPERATOR	OPERATOR
SYSTEST	UETP
SYSMAINT	SYSMAINT or SERVICE
FIELD	FIELD or SERVICE
GUEST	GUEST
DEMO	DEMO
DECNET	DECNET

UNIX- It seems like everything is running UNIX these days. For more information on it, go to your local library or college. They will have tons of stuff on this system for you. The login prompt will look like this- login: or an @ or even sometimes a . It usually does not keep track of bad login attempts. Also note that some systems are case sensitive, so use lowercase when your not sure.

Accounts	Default Passwords
root	root
admin	admin
sysadmin	sysadmin or admin
uucp	uucp
rje	rje
guest	guest
demo	demo
daemon	daemon
sysbin	sysbin
unix	unix

Unresponsive Systems

Here is a list of things you should do if you encounter an unresponsive computer system.

1. Change parity, lengths, or bits. Try parity of SPACE or MARK if you have it.

2. Change baud rates. Try something wierd if your program will let you.

3. Hit RETURN a lot.

4. Send some \'s along with some RETURNs.

5. Send a series of periods.

6. If your getting garbage, hit the i. Tymnet responds to this.

7. Send control characters starting from ^A to ^Z.

8. Change terminal emulation

9. Type LOGIN, HELLO, LOG, ATTACH, CONNECT, DISCONNECT, START, RUN, BEGIN, LOGON, GO, JOIN, HELP, etc...

10. Social engineer the system administrator

11. Disconnect from it! People have been caught this way already. If the system administrator notices someone trying to hack their system, they will set up dead terminals connected to modems, and will let you play with them long enough for the phone company to trace the call.

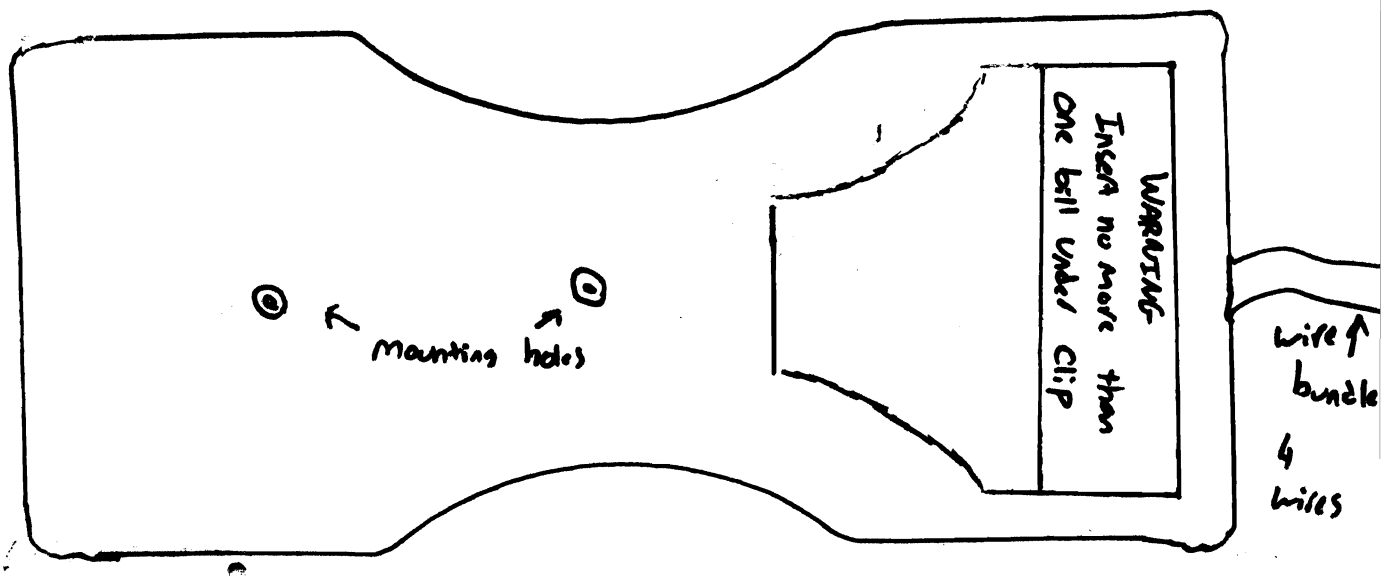
HOPE

Bank Hold-Up Alarms

People just love it when we publish stuff on their alarm systems. Here is another interesting thing we stumbled upon.

Inside the tills at banks, there is a little holder and a switch. The bank employees insert a bill into the holder that closes off the switch. If someone tries to rob the bank, all the teller has to do is pull the bill out from underneath the holder. Since robbers always ask for ALL the money in the till the teller pulls out all the money, setting off the alarm.

Their are some even more advanced versions of this alarm. One style has a capacitor built into the circuit to store charge. IF the robbers happens to be smart enough and turn off the alarm system (all alarms operate on DC) the capacitor will hold enough charge to set off the alarm is the system. Whoa- Advanced.



The bill will get inserted underneath the clip where that warning sticker is located. The switch is no more than spring pushing against a little metal pad. When the bill is inserted, it closes the circuit.

SHOWN ACTUAL SIZE (we had to rob a bank to get one)