Digital Signals On Your Scanner

Discover What They Are

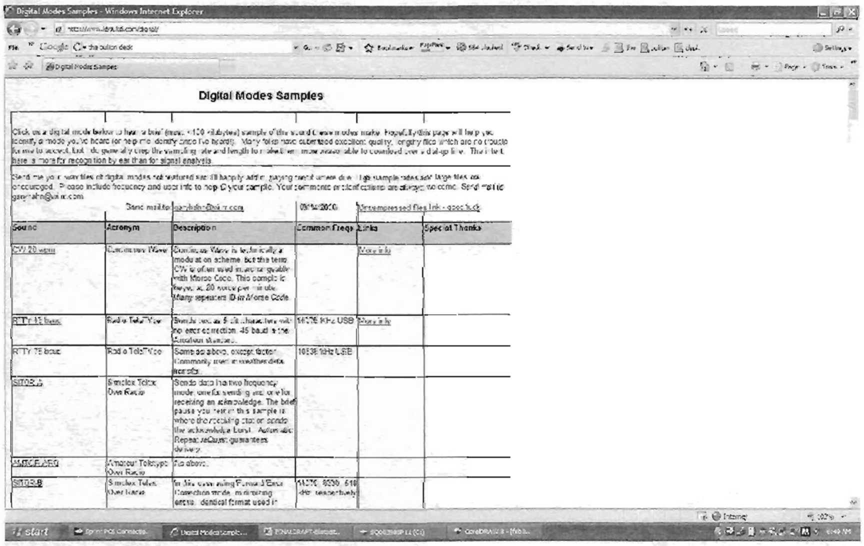
Text by John Bolduc

Have you every tried monitoring non-verbal communications on your scanner. Do you wonder where those funny sounding computer generated voice messages come from? Granted for the most part you won't be able to understand the data communications, but you can log and perhaps identify what you are receiving.

The shortwave bands are filled with blitz and blaps, dits and dats, but the world above 30 MHz, in the typically scanner bands are filled with similar buzz. Some higher end scanners will also let you monitor below 30 MHz giving you a greater variety of data signals to tackle.

Mobile Data terminals are used regularly by Police and increasingly by Fire Departments. Manchester NH has just switched over the MDT usage in all their apparatus. If you monitor them now, you will hear the initial dispatch for a call, and little else, unless the incident gets big and involves mutual aid.

Just what does a Mobile Data Terminal sound like? On the internet there is a fine site dedicated to the various data modes. Each mode has a high quality audio sample. These make a good reference to determine just what type of data "blatz" is coming across your scanner.



Digital Modes Samples - Windows Internet Explorer

Digital Modes Samples

Click on a digital mode below to hear a brief (max. <100 kilobytes) sample of the sound these modes make. Hopefully this page will help you identify a mode you've heard (or help me identify ones I've heard). Many folks have submitted excellent quality, lengthy files which are no trouble for me to accept, but I do generally crop the sampling rate and length to make them more reasonable to download over a dial-up line. The intent here is more for recognition by ear than for signal analysis.

Send me your wav files of digital modes not featured and I'll happily add in, giving credit where due. High sample rates and large files are encouraged. Please include frequency and user info to help ID your sample. Your comments or clarifications are always welcome. Send mail to [illegible]

Send mail to: [illegible] [illegible] Uncompressed files link - good luck

Sound	Acronym	Description	Common Freqs	Links	Special Thanks
CW 20 wpm	Continuous Wave	Continuous Wave is technically a modulation scheme, but the term CW is often used interchangeably with Morse Code. This sample is keyed at 20 words per minute. Many repeaters ID in Morse Code.		More info	
RTTY 45 baud	Radio TeleTYpe	Sends text as 5-bit characters with no error correction. 45 baud is the Amateur standard.	14075 KHz USB	More info	
RTTY 75 baud	Radio TeleTYpe	Same as above, except faster. Commonly used in weather data transfer.	10536 KHz USB		
SITOR-A	Simplex Telex Over Radio	Sends data in a two frequency mode, one for sending and one for receiving an acknowledge. The brief pause you hear in this sample is where the receiving station sends the acknowledge burst. Automatic Repeat reQuest guarantees delivery.			
AMTOR-ARQ	Amateur Teletype Over Radio	As above.			
SITOR-B	Simplex Telex Over Radio	In this case using Forward Error Correction mode, minimizing errors. Identical format used in	14070, 8030, 618 KHz respectively		

Digital Modes Samples web page

These digital mode samples can be found at: http://www.kb9ukd.com/digital/.

From these samples we figured out the Nashua NH's old UHF Police frequency was now using RD-LAP (Radio Data - Link Access Protocol) data protocol at 19200 baud. Nashua had gone to an 800MHz Trunk Radio System many years ago. The old UHF frequencies were still licensed but remained silent for years. Low and behold, about a year ago one of the old channels came alive with data. It appears that Milwaukee WI Police also use this protocol on their 800 MHz system.

Now this begs the question. Why doesn't Nashua have their MDT's integrated into their Motorola Trunked System. The only thing I can figure, based on what a fire dispatcher told me, is when the 800 MHz system was installed many of the so called bells and whistles were specifically excluded from the system in order for the total system cost to come within budget. Later on, UHF remedy apparently was more cost efficient than retrofitting the system. Given the topography of Nashua, the UHF also is probably much more reliable than 800 MHz in terms of coverage. The city is far from flat and the undulating evergreen laden hills are not always kind to 800 MHz signals.

Common in my part of the world and often noticed in my many travels up and down the eastern states are water pumping/control stations. These very small masonry buildings typically have a highly direction Yagi antenna mounted aside them, pointing towards the main fresh water, or waste water pumping plants. Some of the local towns have half a dozen or more easily visible such control stations, and there are usually more off the beaten path.

In Derry NH, 453.8875/458.8875 MHz is the frequency pair to monitor. Through casual observation I've noticed that one frequency is the main plant and will transmit data for a second or two. On the other frequency one of the outlying stations with transmit its data back. Whether that data is just a handshake, an acknowledgment of message I don't know. It could be an *I'm still alive* indicator, or actually measurement data. The signal strength will appear to vary from the outlying station as it transmits different segments of data. It is soon realized that each of the stations in various parts of town take turns replying to the data sent by the "home" station.

This particular frequency can be quite annoying in my town. Even though the transmit power into the antenna is a matter of watts, the beam antenna causes signal splatter on adjacent channels if you happen to be in the path of the signal. Bedford NH fire is on 453.875 with a DPL of 723. Even though I have Bedford on tone squelch, the data signal on the adjacent channel split channel still come through when Bedford is transmitting. If you don't have a tone squelch scanner and live in the wrong part of town, monitoring not too distant Bedford could be annoying.

If pumping water does not sound to exciting to you, how about F1 race cars. The Yahoo Group http://groups.yahoo.com/group/f1scanner/ has provided several telemetry signals to the Digital Mode Audio Samples page at the kb9ukd.com site.

Searching through VHF High Band I've come across a strange type of data/voice combination. On 151.925 MHz is a signal that sometimes sends a tiny bit of data followed by a verbal message such as, "Test, Test, Test". Rarely will you hear others messages such as "Battery Power Engaged" or "Water Level Low Alert". The most unusual message heard was "Bring home a loaf of bread", just kidding!

At search at FCC.gov gives us the most likely user is WQDT422, the Gregg Falls Hydroelectric Associates. The actually show two bases at two locations running 25 and 40 watts respectively. The mode shown is your run of the mill analog FM. Stated use is for security and maintenance. I never heard anything here that would indicate a live human being was communicating.

Back in 1980's many professionals commonly carried voice pagers. Some of these voice pages were sent by answering services and were initially a useful tool, especially for the medical profession. However, many of these pagers could be accessed by a dedicated not so hard to figure out telephone numbers. Several unscrupulous scanner listeners turned this feature/weakness in a game of pager tag. These "hobbyists" would have identified several local paging frequencies that could be monitored in plain language over the any scanner. They would scan local classified and display ad sections of the newspaper for advertisements containing a paging access number as a contact phone number. It was obvious that many of the phone numbers were very close. For example 555-1700, 555-1726, 555-1749.

A game ensued whereby one monitor would "try" a number leave a message such as "Pager Tag #43, got ya!" and record which frequency they heard it one. Often these were tape recorded as part of the contest. Other monitors would try to outdo each other and get the most tags. Sometimes it would be more like a real game of tag. Two or more contestants would tag each other via a high jacked voice page until a set tag. The last person tagged when time expired lost.

A variation of this would be to monitor the access tones preceding a voice page and match it to somebody very important. If they heard pages, for instance for Mayor Sullivan, they would keep pinging phone numbers until they tripped the correct access tones as heard over the air. They would then take shots at leaving the Mayor inappropriate messages. One funny, but not to the person receiving the page, message I heard was some girl pretending to be the mayor's mistress. At least I think she was pretending.

As paging system operators got smart, those users who were getting harassed or could be possible targets had access PINs added to the telephone access. Therefore, even if you got the correct number for Doctor Swartz, you could not send a voice page without a passcode.

A much cleaner solution to voice pages came in the form of text capable pagers. Even if you knew a block of access telephone numbers, it would be much harder to hack and attack somebody. At least if you got a rude message, it was sent to your eyes and not everybody's ears in the vicinity of the pager.

POSCAG, A Common Paging Protocol

Most text paging systems use a protocol called POCSAG. Post Office Code Standardization Advisory Group. In Europe, and in this case England, Post Offices not only delivered mail but also ran the telephone and telegraph until deregulation came into being.

Trying to figure out the POCSAG coding protocol can be quite involved. From the Paging Information Resource Page here is just a taste of what's involved.

Rules when requiring two POCSAG codes:

Every pager must have a Code A. Code A and Code B must be in the same frame.

Rules when requiring three POCSAG codes:

Every pager must have a Code A. Code A and Code B must be in the same frame. The frame of Code A and Code B must be less than the frame of Code C.

Rules when requiring four POCSAG codes:

Every pager must have a Code A. Code A and Code B must be in the same frame. (Formula provided below) There must be a Code C to have a Code D. Code C and Code D must be in the same frame. The frame of Code A and Code B must be less than the frame of Code C and Code D.

Okay I see a pattern here, but this looks like it could be tough to figure out in just one evening!

Formula to find the frame number:

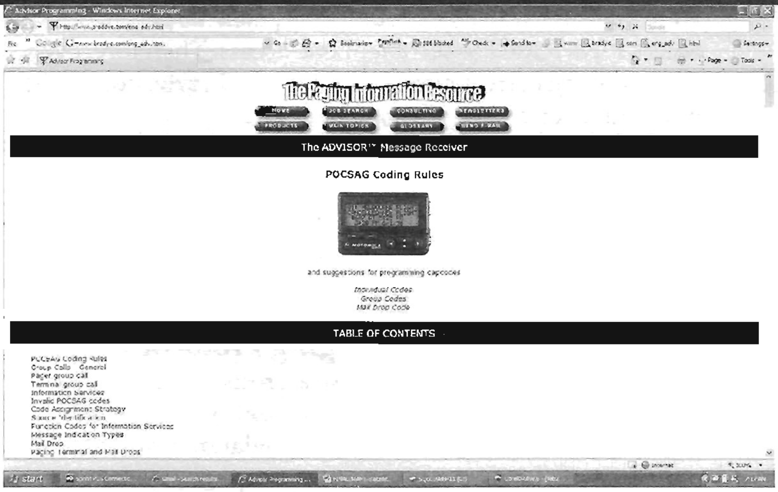
Divide each Capcode by 8. Take the decimal remainder and multiply by 8. The result is the value of the frame (or frame number).

Example:
Code A = 2013670 ÷ 8 = 251708.75
or
Code B = 1657614 ÷ 8 = 206701.75

.75 x 8 = 6
Therefore Frame = 6

The much more very full details are available on the Internet at: www.braddye.com/eng_adv.html.

POCSAG has three different transmission rates, 512, 1200, and 2400 bps. The 1200 bps rate is the most common among users who have their own paging terminals. Pages through telephone service provider terminals are typically sent at 2400 bps. Industrial in house paging systems most



The ADVISOR™ Message Receiver

POCSAG Coding Rules

and suggestions for programming capcodes

Individual Codes
Group Codes
Mail Drop Code

TABLE OF CONTENTS

POCSAG Coding Rules
Group Calls General
Pager group call
Terminal group call
Information Services
Invalid POCSAG codes
Code Assignment Strategy
Source Identification
Function Codes for Information Services
Message Indication Types
Mail Drop
Paging Terminal and Mail Drops

often use the slowest rate, 512 bps. You will sometimes see the three rates listed as 512, 1024, and 2048.

Text pagers generally have a group call and an individual call mode reception. All pagers within a "group" need to have a common *Capcode* if the group page is to be sent out simultaneously in an efficient manner. The destination pagers however must be capable of containing more than on Capcode, the others being for individual or sub-group messages.

An older inefficient way of sending group pagers was with the Terminal Group Call Method. A page is sent to a paging terminal which contains all the individual Capcodes for each member of the group. The terminal then sends one page at a time to each group member. This takes up quite a bit of airtime can be expensive.

A common model of pager, the ADVISOR, can have up to four Capcodes that can be programmed into it. Each of the Capcodes must have a relation to each other as shown in the POCSAG rules above. Depending on which of the Capcodes was accessed in the pager, a different *alert* or *function* could be triggered in the pager. One alert for a group call could simply be for the pager to vibrate. An individual page could cause the pager to beep loud and long. Another page could cause the pager to give one short beep. Another method is to use the same Capcode, but also include a single character origin code.

Capcodes, what are they?

Capcodes are like a serial number for your pager. When a message is sent through a terminal destined for a pager, it is put in a queue. Here many, many messages are broadcast over radio signals in a stream containing "frames". When your pager sees a frame with its CAP Code embedded, it captures that data and performs the appropriate functions, such as beep twice and display a message.

CAPcode, is it an acronym?

Just what does CAP code mean. Well, I have a theory; I have yet to prove it. Here goes! When motion pictures for the commercial movie industry (Hollywood) was being affected by illegal copies of its movies being made, the leader section of the film and edges of certain "frame" were embedded with a series of punch dots that indicated the original and copy number of each movie print. The CAP code was inserted every so many frames apart in a particular pattern. Even if the CAP code was correct, the positioning among the frames was also critical. In this case the C-A-P stood for Copyright Anti Piracy. When you think about it the frames of a motion picture are organized similar to the frames of a data stream.

POCSAG decoder software is able to display pager messages by using a normal radio scanner, a computer and a soundcard. The 512 and 1200 rates can be decoded using just the "clean signal" audio output of a scanner fed into a computer sound card. For 2400 rate, you will need to take the signal of the scanner decimator. This involves a scanner mode which is beyond the scope of this article.

Caveat Number One

My Symantec/Norton Internet security software blocked many of these software and modification sites from my access because they were branded *criminal.* I suspect the ECPA (Electronics Communication Privacy Act) of 1986 would address whether of not the decoding of these messages is the proper thing for the proper scanner enthusiast to be doing. However, the ECPA is another article for another time.

Caveat Part Deux

A very fast processor is also needed or you'll find yourself decoding one message and missing unknown subsequent messages.

Less popular alternatives to PSCSAG are FLEX and GOLAY.

FLEX is typically heard in the 900 MHz range and can use up to 6400 baud.

GOLAY can be annoying as Motorola DPL also uses this protocol as a sub carrier transmitted at 134.5 Hz. This often causes analog radios to falsely open squelch if they are using a CTCSS of 136.5. In New Hampshire, 136.5 Hz seems to be the default CTCSS tone to use. If you are in an area where intermodulation from strong signals occurs, a P25 digital transmission can cause some distorted sounding signals on your favorite scanner frequency.

Common Voice Pager Frequencies:
152.010 - 152.210
453.025 - 453.125
454.025 - 454.650
462.750 - 462.925

Common Non-Voice Paging Frequencies:
35.020 - 35.680

43.200 - 43.680
152.510 - 152.840
157.770 - 158.070
158.490 - 158.640
459.025 - 459.625
929.0125-931.9875

The 72-75 MHz band, between North American analog television channels 4 and 5 is used by paging companies as a link from terminal to transmitter. However the mode used here is Audio Frequency Shift Keyed. At the transmitter the mode is converted to FSK. You may also hear this on some of the old mobile telephone frequencies.

In POCSAG, FSK or Frequency Shift Keying, modulation is used with a 4.5 kHz shift of the carrier frequency. A plus shift represents a data zero and a negative shift represents a data one. Data words are 32 bits in length. A word in this case can either be data or an address. Much of each word is made up of 10 bits dedicated to data validation and error correction. A sync, address or idle word is followed by 16 data words. The pager typically only need to be awake to receive the sync word, and if necessary stays awake for the next sixteen words. This helps extend battery life. Before each set of data burst, there is additional synchronization going on. A preamble of approximately 576 alternating zeros and ones are sent to make sure the receiving pager is in sync with the transmitted signal timing.

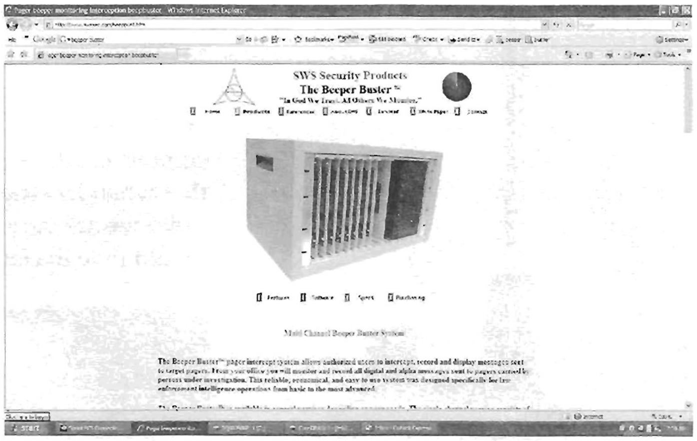
```
08/05/07 6:21:51 B=1024, A=0012863, F=1, msg = FOXTV
SEE NEWS TONIGHT*

08/05/07 6:21:52 B=1200, A=0024833, F=3, msg =  09
W704240796 CUSTOMER REPORTS CHEESE ON PIZZA
ALL SLID INTO CORNER OF BOX* CD12 xxx27548 4663-
2431- network:cd12 800 679-3536 21 N
08/05/07 6:21:53 B=1200, A=0026255, F=4, msg = BRING
HOME A LOAF OF BREAD NOW*
08/05/07 16:21:54 B=2048, A=0012379, F=2, msg =  05
W704240717 1 1 24 MAIN STREET REAL ESTATE* ACTIVE
ITEM 4G83 xxx61354 5185-5231- network 800 702-2256 65
08/05/07 16:21:54 B=512, A=0886135, F=0, msg = 620900091
```

You might notice that the A indicates the Capcode, B indicates baud rate, and F indicates function (beep, buzz, display text, display number, etc…)

RTTY - Radio Teletype

Another mode using FSK (Frequency Shift Keying) RTTY - While not inhabitants of the world above 30 MHz, some scanners do trek down to the frequencies below 30 MHz. RTTY, short for Radio Teletype, became an increasing popular mode of operations for Amateur Radio operators on February 20, 1953. On this date the use of FSK, became legal for use in the Ham bands.

In an FSK RTTY system the operator can send either characters or functions. Depending on what is sent the transmitter frequency is shifted by 170 or 425 Hz and this is detected by the appropriate receiving apparatus. You can recognized these transmission by their starting and ending with a high pitched tone. A popular frequency is 3602.5 KHz, best heard in the evening. RTTY has lost considerable popularity as transmissions rates are typically set a 45 baud or equivalent of 60 words per minute. Weather related RTTY heard in the 10 MHz band is sent at 75 baud. However RTTY with FSK is quite impervious to static and is almost as reliable under bad conditions as CW Morse Code.


Pager beeper monitoring interception beepbuster - Windows Internet Explorer
Features
Software
Specs
Purchasing

SWS Security Products
The Beeper Buster™
"In God We Trust. All Others We Monitor."

Multi Channel Beeper Buster System

The Beeper Buster™ pager intercept system allows authorized users to intercept, record and display messages sent to target pagers. From your office you will monitor and record all digital and alpha messages sent to pagers carried by persons under investigation. This reliable, economical, and easy to use system was designed specifically for law enforcement intelligence operations from basic to the most advanced.

Big Brother

Searching the internet researching this article, I came across an interesting device called the *Beeper Buster*. It is a device available to law enforcement agencies produced by SWS Security Products. This is a pager intercept system that allows authorized users to intercept, record, and display intercepted messages from targeted pagers. Targeted pagers are those devices carried by suspects and other persons under surveillance.

The simple single radio channel model can monitor up to 200 capcodes, and implement 50 search strings simultaneously. The system can also build a searchable database for each capcode being monitored. More advanced models can include seven additional modules to monitors seven additional radio channels. The system is designed in a manner to help identify a previously unidentified target pager for inclusion in the interception model. The system can also detect the origination of a page, such as a payphone number. You can target your recordings to trigger on a given phone number rather than a capcode. The system uses an ICOM PCR100 as the receiver.

Editorial Note: *Monitoring data signals that are private* ***and not intended to be read by others using these devices or software found on the Internet is a violation of federal law. While there is nothing illegal in understanding how paging systems work or how pagers receive this data, scanner hobbyists will want to make sure they abide by all laws.***