Sierra Signals

Sierra Foothills Amateur Radio Club
Auburn, CA
An ARRL Special Service Club

November 2008 P.O. Box 1005, Newcastle, CA 95658

Pixels From Space, part 2

(Submitted by Greg, KO6TH)

Last month's announcement that Richard Garriott, W5KWQ, could be operating SSTV from the International Space Station during his visit in October turned out to be an understatement, if you can imagine such a thing. Pixels did, in fact, rain down from outer space, and many Hams on the ground gathered them into stunning pictures. And there was a whole lot more.

As scheduled, Richard launched into orbit on October 12th, 2008, on board a Soyuz rocket. With him were the crew of the next ISS rotation, astronaut Mike Finke, KE5AIT, and cosmonaut Iouri (Yuri) Lonchakov. Their capsule rendezvoused and docked with the ISS two days later, temporarily bringing the total population of the orbiting outpost to six. Richard wasted little time in activating the ham station, using the on-board laptop and its Slow Scan TV software. Several pictures were sent in the Martin-1 format, showing some test patterns and other pre-recorded pictures of the crew.

By the next day, the Kenwood VC-H1 camera was all hooked up, and sending pictures every three minutes. The lens was aimed downward towards Earth out one of the Station's windows, giving Earthbound Hams a view of themselves from orbit. The station's call sign, NA1SS, was automatically

(*continued on page 2)*

OFFICERS

PRESIDENT
Don Hay, WB6LPJ
wb6lpj@arrl.net

VICE PRESIDENT
Casey McPartland, W7IB
w7ib@arrl.net

SECRETARY
Wayne Stilwell, W6DT
dxwayne@juno.com

TREASURER
Leslie Nye, K7NYE
leslie@incite1.com

DIRECTORS
Jim Griffith, KI6AZH
jim griffith@usamedia.tv
Chuck Minton, KG6FFK
chuckminton@wizwire.com
Norm Medland, W6AFR
norm.linda@surewest.net

REPORTERS
Satellites: Greg, KO6TH
History: Gary, KQ6RT
Misc Radio: Fred, K6DGW

RESOURCES

REPEATERS
145.430 (-0.6 MHz/PL 162.2)
440.575 (+5.0 MHz/PL 94.8)
223.860 (-1.6 MHz/PL 100.0)

CLUB NET
Thursdays, 7:30PM, K6ARR/R 145.430

CLUB MEETINGS
Second Friday of the month, 7:30PM at the Library, 350 Nevada St, Auburn CA

CLUB BREAKFAST
Last Sat of the month at Susie's Café, Cirby at Riverside, Roseville – 8:00 AM

NET CONTROL OPS
Dave Jenkins, WB6RBE
Gary Cunningham, KQ6RT
Norm Medland, W6AFR
Casey McPartland, W7IB

EDITOR
Deb Cunningham, KF6LXN
916.663.4143
kf6lxn@sbcglobal.net

2008 Calendar of Events

Nov 1	**VE Session – 8:00 – 10:00am**
	Raley's - Douglas/Auburn Folsom
Nov 14	**Regular Meeting – Elections**
Nov 29	**Club Breakfast – Susie's – Cirby/Riverside**
Dec 6	**VE Session**
Dec 12	**Regular Meeting – Annual Christmas Dinner**
Dec 27	**Club Breakfast**

We encourage members to receive Sierra Signals via email to save the Club the cost of reproduction and mailing

50 Years Ago At The SFARC

(Reported by Gary, KQ6RT)

The November 5th meeting of the Sierra Foothills Amateur Radio Club was brought to order by Jerry Murch, Vice President in absence of the President.

A film on the cathode tube was shown, phone patch schematics were drawn and discussion was held on QSL cards.

The 2 $5.00 certificates donated by Mr. Ted Pantages as door prizes were won by Harry Grieb and Bob Richier.

Refreshments were served and ragchews followed the closing of the meeting.

These minutes are respectfully submitted for correction or approval.

Arlene Murch

Secretary

Bruce Morrow, WA6BLN, member of our club, was injured in and automobile accident A bouquet of flowers were sent to the hospital in the name of our club.

73,

Gary

KQ6RT

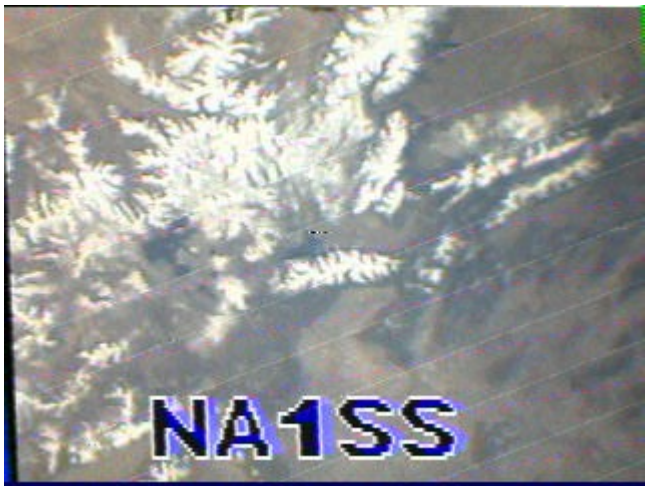
Pixels...

(Continued from front page)

superimposed over the image, clearly displaying the picture's origin as being from out of this world. The ARISS team had set up a web site for Hams to upload and archive the images, and these can still be viewed at:

http://ariss-sstv.ssl.berkeley.edu/SSTV/archive.php

Soon, however, the pictures turned to a deep blue, but still with the callsign clearly visible. It turns out that the Kenwood camera is battery operated, and had been left on all night, still snapping pictures. The camera part takes a bit more power to operate, so under low power conditions, the remaining electronics still functioned, but without a proper video input. Apparently, spare batteries were available, and the situation was soon rectified.



As soon as word was received that the pixels were flowing, I turned on my station. It consists of a Yaesu 736R transceiver and an 8 element beam antenna on 2 meters (among others), with a preamp at the top of the tower. The antennas are on an rotor system that can orient them in any direction in Azimuth (0-360 degrees around the compass dial), and also 0-90 degrees in elevation. Both the transceiver and rotor controller are connected to a PC running the Linux operating system. Software consists of the "qsstv" software for decoding the SSTV pictures, and "predict" for tracking the Station and driving both the rotor controller for direction, and the transceiver for that all-important Doppler shift. With this automation, I was able to leave the PC running while I was asleep or at work. It stayed running all week, and it was a treat to come home from work to see what had been received during the day. All told, I recorded some 32 pictures, not all of which were exactly gallery quality. A few started too late in the pass, and were cut short by, well, the Earth getting in the way. Others just had poor signal quality due to the low elevation of the pass, or the Station dipping behind one of Auburn's hills. But several are crystal clear, and present views of Earth, and of the activities inside the ISS.

Richard's ham activities included much more than just snapping pictures. He had scheduled several school contacts during the flight, including two that used the ham station at Santa Rosa Community College as the downlink, which is close enough to here that both the college and Auburn were in the Station's footprint for much of the pass. My wife and neighbors were able to listen in on one of the contacts, and were amazed at what they were hearing. I was at work, and caught part of another pass with just my HT from the patio outside the building. Richard was talking to a student about decorating the Station for Halloween. (I wonder what they would have done if someone knocked on the hatch, yelling "Trick or Treat"?)

In addition to all that, Richard spent some time talking directly with Hams on the ground. The weekend of October 18 th was the Scout's Jamboree on the Air (JOTA), and several Scout stations were able to make contact. Regular Hams around the world also participated, including me, with a contact Saturday morning. It is reported that Richard made over a hundred random contacts around the globe.

All in all, it was a very memorable week. Thanks go to ARISS, and of course, to Richard, W5KWQ, on board the International Space Station.

73,

Greg KO6TH

October Meeting Minutes

(Reported by Wayne, W6DT)

Minutes of the Meetings of October 10, 2008

Board of Directors Meeting

The meeting of the Board of Directors was called to order at 7:00 PM, a quorum being present.

Expenditures for the backup repeater were reviewed and Richard, WA6RWS, was reimbursed, the authorization being granted at a prior meeting.

Next months election of officers was reviewed.

The meeting was adjourned at 7:18 PM.

Meeting of the General Membership

The meeting was called to order at 7:30 by President Don, WB6LPJ. Flag salute was followed by the introduction of officers and members.

Vice President Casey, K7IB, went over next month's elections, the Christmas Dinner in December as well as mentioned the Club Breakfast, usually held the last Saturday of the month.

Richard, WA6RWS, reminded the club that we were providing communication for a motorcycle enduro on October 25 and extra participation was welcome.

The treasurer, Leslie, N7NYE, advised that we started the month with approximately $2440. We had to pay for the meeting room at $20 a month for 11 months, had PG&E and telephone bills as well as the reimbursement costs for the backup repeater leaving a balance of approximately $1300.

An ARES report was given by Chuck, KG6FFR.

A satellite report was given by Greg, KO6TH, mentioning that the space station was going to be workable in our area.

Richard, WA6RWS, briefed the club on the upcoming club election and encouraged people to get involved. He gave the status of the backup repeater.

The ARRL Auction is this month was a reminder by Al, NI2U.

Frank, N6GP reminded members that the Golden Bear Net is active on 3975 kHz at 7 PM local time.

Dave, NO6NO, has converted the Bylaws to a word document so that they can be more easily kept up to date and so changes from the review can be made.

The White Elephant Sale was conducted by Don, WB6LPJ and Richard, WA6RWS.

The meeting was adjourned at 9:25 PM.

Respectfully submitted,

Wayne Stilwell, W6DT

Secretary

Miscellaneous Radio

Logbook of the World "Certificate Mumbo Jumbo"

If you aren't registered with ARRL's Logbook of the World [LoTW], you might consider doing it. I've been registered for several years now, and I have uploaded 32,248 QSO's, nearly all contest logs. Of those, 11,577 have resulted in QSL matches. When I first applied for DXCC, I was a few short of 100 in LoTW and supplemented them with some cards I had.

Today, I am well past 100 LoTW confirmed DXCC Entities. Getting started is easy, just visit www.arrl.org/lotw/getStartedGuide.pdf

I was helping a friend get set up in LoTW, and he asked about all of the "Certificate" stuff. To prevent fraudulent QSO's being uploaded into the system, LoTW requires that you digitally "sign" your log files using a "Certificate" issued to you by ARRL. This proves to the system that the log you are uploading came from you and not an imposter. This is a huge difference from other on-line QSL services such as eQSL. To understand how this works, we need to take a quick romp through the fascinating world of cryptography.

There are two classes of cryptosystems: Symmetric and Asymmetric. In a symmetric system, you and I agree on a key [let us say a very large number], and using an algorithm [computation rule] that we have agreed on, I use the key to encrypt my message. The message now looks like garbage and I send it to you. You, using the same algorithm and key, process the garbage and my plain text message reappears. The security depends on the secrecy of the key only. The algorithm doesn't matter although some are more robust that others. If the key is long enough, such systems can be nearly unbreakable.

The problem is that you have to physically get the two identical keys to each end of the circuit. In military usage, the keys were typically on special punched cards or small magnetic tapes, and couriers would transport them. If you were an officer heading for some base, it was common that you'd be given a service .45 and a sealed canvas bag which you then delivered at your destination. Kind of cumbersome though, although "cumbersome" has never deterred the military.

Asymmetric cryptosystems operate quite differently. They depend on the existence of a class of mathematical things called "one-way functions." These are functions that are easy to compute in one direction, but nearly impossible to compute in the reverse direction.[1] They involve a pair of related keys. Either key can be used to encrypt a message, however the other key in the pair must then be used to decrypt it back to plain text. Each time I want to generate a key, I actually get two and like multiplication or addition, this is the "forward" direction for the function and it is easy. If all you have is one of the keys however, it is practically impossible to derive the other key in the pair from it because that's the "reverse" direction for the function. Note that the algorithm [function] is public – everyone can know it.

So, I generate a key-pair. I keep one of them secret, and I tell the world about the other one which becomes my public key. Now, Casey decides to send me a secret message. He looks up my public key and uses it to encrypt his message and then sends it to me. I use the secret key of the pair to decrypt his message. It's that simple. How do I tell the world about my public key? The Internet, of course. There are a number of "key servers" scattered around the world and they all chat with each other. You log in to any one, load your public key, it gets passed to all the other key servers, and all Casey has to do is go to a server and search for my key. Go to pgp.mit.edu and search on ["fred c. jensen"]. You'll see the public key I had while still employed, and my current public key which I never use anymore. In fact, I don't think I can find my secret key for it so don't try to send me an encrypted message☺.

But wait! There's more! Supposing I want to send a message to Casey and I want to make it possible for him to verify that it really is from me and that it hasn't been tampered with along the way. One way for me to do this is to encrypt the message using my secret key and send it to him. He looks up my public key and decrypts the message with it. He knows the message is from me because only my public key will decrypt a message that was encrypted with my secret key, and he knows it hasn't been modified enroute or it wouldn't decrypt at all. This is called a digital signature, and is at the heart of the LoTW security system.

A major problem with public key cryptosystems is validating that the public key on the keyservers really is mine. Suppose someone can intercept the messages between Casey and me. He removes my public key on the servers and replaces it with his but leaves my identity associated with it. Casey uses that key [which he believes is mine] to encrypt a message – "Attack at dawn." The interceptor can not only decrypt that message using his secret key, he can modify it, perhaps to "Retreat immediately," encrypt it using my public key that he originally got from the server, and send it to me. There is no way for me to know the message isn't from Casey. One way around this is for me to hand-deliver my public key to Casey. He would recognize me, and know that this really was my public key. This however gets us back into the problem with symmetric cryptosystems … I have to visit him at least once.

In the Big World, this problem is solved by submitting my public key to one of a number of authentication companies. Verisign is one such company [in whom I have no financial interest … anymore]. They physically validate who I am, where I live and/or work, and other information and then they digitally sign my public key with their secret key meaning that they have validated that this really is my public key. That's called a certificate. Verisign's digital signature goes with my public key onto the keyservers and can be validated by anyone using Verisign's public key. Can't someone forge Verisign's digital signature? Not really, the whole world knows their public key [and those of others like Microsoft]. In fact, the public keys of most of the authentication companies are built into your web browser and get updated regularly. And that's the basis for the LoTW certificates.

ARRL provides software [TQSLCert] with which you generate a key pair. You then send your public key to ARRL. ARRL looks up your USPS address in the FCC database and mails you a post card with a special password on it at that address. If you really are the ham who created the key, you'll be expecting this and you'll go into TQSLCert, give it the special password, and it will get your certificate for you. Remember, the certificate is your public key which has been digitally signed

[1] Choose two large prime numbers [numbers divisible only by one and themselves], and multiply them together. Easy, we all know how to multiply. But if I give you their product and ask you to tell me the two primes it came from … not so easy. As of today, no algorithm that will factor arbitrary numbers is known and there is some evidence that none exists. And, if the numbers are really large, the exhaustive search method would take more than our lifetimes, even on the fastest computers. This is one example of a "one-way function."

and vouched for by ARRL using their master secret key. TQSLCert will ask you to assign a password to your new certificate which you'll have to provide every time you want to digitally sign a log for upload.

When you upload a log, you first use TQSL to digitally sign your log with your secret key. It also adds your certificate to the file which you then upload on the LoTW web site. ARRL looks at your certificate, validates that the public key is really yours [they signed it, so if their signature is good, so is your key], and they then validate that you signed the log.

For DX stations, it's a little more complex because they're not in the FCC database. For them, ARRL requires that they submit physical evidence [e.g. copies of licenses] to validate identity. Remember, that's the whole issue– what human being actually belongs to this public key. An ARRL-issued certificate is good for two years. But, if you act before your certificate expires, the renewal process is easy. You use TQSLCert to generate a new key-pair, and you request a new certificate, signing the request with your old certificate. You get a new one good for 2 years, and the old one expires. TQSLCert allows you to manage this process and keep track of your certificates. And, this is a whole lot harder to explain than to do.

While I hope that the on-line Logbook of The World does not totally replace personal, paper QSL cards, it is a huge step forward. Currently ARRL's LoTW supports awards for DXCC and WAS, and, if both you and your rare DX station upload to LoTW, you get confirmation without begging for QSL cards. Most Dxpeditions these days upload their logs. Sometimes it takes a year because they solicit nominal amounts of monetary support for "real" QSL cards. Currently, you can upload computer-generated logs in the Cabrillo and ADIF formats.

So, if you're into puzzles, here's an old one from cryptography: I have a valuable item [say an Elecraft K3] that I want to send to you in a padlocked box, but I have no way to get the key to the lock on the box to you to you without taking the chance that it could be intercepted. You can assume the box cannot be physically broken into. How can I do this? There are cryptographic analogs to this problem when dealing with information, but they are a lot more complex than this simple puzzle.

73,

Fred K6DGW

New Digital Television Channel Plan Explained

(Reported by Dave, NO6NO)

I've overheard and contributed to several discussions on what will happen when TV goes digital. There were lots of theories, but nobody seemed sure what was true. I did a bit of research and this is what I found:

After February 17, 2009, *full-power* television stations in the USA will broadcast in digital only. In Canada, this will happen Aug. 31, 2011.

While the majority of the viewed TV broadcast stations are full-power stations, about 1800 in number, there are three other categories of TV stations that exist:"low-power" stations, "Class A" stations, and "TV translator" stations. There is presently *no deadline* for these stations, about 7100 in number, to convert to digital broadcasting.

New digital television frequency spectrum will occupy 54 Mhz to 699 Mhz or the existing channels 2 to 51.

The existing upper end of UHF 700 Mhz to 808 Mhz or Channels 52 – 69 will be reassigned to new services.

As most of us are aware existing stations are broadcasting in analog and digital at this time. However, some will change to new channels and some will end up where they were.

There appears to be some confusion as to where stations will end up channel and frequency-wise after the transition. Well, some will still broadcast VHF and some will migrate to UHF. The following table will take some of the mystery out of what will most likely happen in the Sacramento area.

Now (Analog) Channel	**Now (Digital) Channel**	**Eventual (Digital) Channel**
3	35	35
6	53	6
10	61	10
13	25	25
29	48	48
31	21	21
40	55	40

I hope this makes it clearer.

Dave Albright NO6NO

Stuff for Sale

The widow of an SK has some Ham Radio gear for sale. For information contact Fred's friend PA, K6DMF – (530)823-9898
