Exploding The Phone

www.explodingthephone.com

Bibliographic Cover Sheet

db485

Title	**Cap'n Crunch Comments on the Esquire Article**
Publication	*well.com*
Date	1998-00-00
Author(s)	Draper, John T.
Abstract	Draper's comments on the technical accuracy of the Esquire article.
Keywords	John Draper; Cap'n Crunch; blue boxes; Esquire
Notes	Claimed to have been published on the Well in 1998; this is unconfirmed. Now hosted on several sites.
Source	Web

Cap'n Crunch comments on the Esquire Article

For a very long time, I've had to answer many questions about some of the claims made in the Esquire article on some of the things I did, so here, I've included my comments on the article. I recently found a copy of the article on the WEB, and have read it again, so here are some of my comments... I hope this answers once and for all the myth behind some of the claims in the article.

"Calling around the world several times, ringing the pay phone next to you" - Well, this was true. It worked like this... In the UK, we were able to switch a call through the UK, and from there, go to Australia (Using different set of tones), then back to SF and the pay phone. This worked, because in the UK, they used 2280 Hz signaling which didn't interfere with the USA signaling frequency of 2600 Hz. The Australian signaling frequency was 600 Hz followed by 770Hz I believe. It's been such a long time ago, but I'm sure someone will come forth and set me straight. As to calling myself clockwise then counter clockwise, that was also true to a point.

By then, I was just learning the intricacies of Tandem stacking using guard-banding. Very new people other than me were successful at this. First, let me explain "Guard Banding". It becomes necessary for the phone company to install circuitry that prevented disconnection's when a high pitch voice has 2600 Hz component in their voice, otherwise, old Auntie would trip the call and disconnect. So, this circuitry was designed so that if there were OTHER frequency components OTHER than 2600 on the line, it wouldn't trip the call.

It turns out that if you selected a "Guard" frequency that is slightly higher than the upper frequency limit (Around 3200 Hz was optimal), this means that on the first leg of the connection, one had to boost the 3200 component in such a way that when they arrived at the other end, BOTH would have identical levels and the call wouldn't trip off. On the 2nd leg, the 3200 component would be attenuated BELOW the guard threshold, and the line would trip off, not all the way back to the first trunk, but land you on the 2nd trunk. Instead of getting the "Ker-cheep" sound, you would hear "Ker-cheep-cheep", two distinct beeps. One coming from the first, and the other coming from the 2nd. With this new concept, it was possible to hop-scotch and zig zag just about anywhere up to about 8 or 10 hops. With this, one would certainly cause massive headaches for anyone wanting to "trace" a call.

When the Esquire article came out, Guard banding hadn't been "Invented" yet, but the article mentioned zig zagging. In THAT case, tandem hopping was a little different. Back then, the long distance circuits used a number-1 crossbar switch for long distance switching, instead of the more common 4A switches. Fresno and Bakersfield had TTC codes of 042 and 044 respectively. For instance, these codes distinguished the cities in the same area code. For instance, to reach a Fresno operator, one had to dial kp 209-042-121-st. The 042 was a "Routing code" which routes the call to Fresno. Stockton which had a 4a was a main switching center for the 209 area code.

For testing purposes, it was possible to do kp-042-st (from a 209 area code trunk). This caused a rather interesting thing to happen. The number-1 crossbar switch would just drop you right onto a Fresno trunk. One could then do kp-044-042-st This would route first to Bakersfield (044) then back to Fresno (042). Then by repeating it (kp-044-042-st) over and over, resulted in hopping back and forth. Eventually, this would result in either the blue box tones being so weak that you couldn't go any further, or the trunk lines would all be busied out. Well, at that time, about 30% of the ATT system was using the number-1 crossbar switches. All one had to do was to go out and find them. I did, and found just about all of them in the USA and mapped them. Through this, one could zig-zag as mentioned in the article. On those round the world demonstrations, the delay times weren't 20

seconds. It was more like about 3 seconds, and with an amplified line tie, it was possible to actually create an "Echo chamber", A mighty long one at that :-)

A lot of the cities and names used in the Esquire article was false to protect the people involved.

The description of the procedures outlined in the article were accurate, but some of the tones given in the article were FALSE. This, of course was to protect the phone company, but SOME students would make the connection and find a source for the actual blue box frequencies which were published in a Bell System technical journal and was available in any University library, as Woz soon discovered after he read the article. It's not known how many people actually figured out how to Blue Box from the article, but Woz was the first one I encountered.

The overseas access code KP-182-ST was accurate. That was the code for the UK. KP-183-ST was Europe, and eventually KP-186-ST was for Japan and the Pacific. Eventually, that was phased out, and a more standard overseas access was employed, where one would dial KP-011-044-ST would translate to KP-182-ST. These were the trunk codes for overseas calls. Because the tandem registers only had the capability of storing 11 digits, one had to first call through a device called a "Sender" The KP-182-ST was the code for the overseas sender. After dialing that, one would hear a tone, not unlike a dial tone, then upon hearing that tone, would dial KP-04412220666 -ST for "Dial a Disc" which would pipe the latest London pop tune hit through the phone. Then, London code was (01). Dropping the "0", would be the "1" for London.

0 - Send call through Satellite or
1 - Send call through Cable
44 - Country code for UK
1 - code for London (I think it's 071 now)
222-0666 London's Dial-a-disc number

Now, here's the real ironic thing... Back in the early 60's when the ATT long lines had just developed "Multi-Frequency", there were ads placed on TV, which explained this. REAL tones were actually given out in their ads. "Now we can switch calls 10 times faster to speed your call to Granny by using pairs of tones" the ads would hype. Tsk Tsk - Little did they know... I mean, it was quite clever for ATT to use this method of signaling. It meant that it was possible to use only ONE trunk for BOTH signaling and TALKING. My My, they saved heaps of $$$ doing it this way, SO THEY THOUGHT!!

It was possible to record the tones on a good tape recorder and play them back. Those old Panasonic mono portable cassette recorders worked best. Most people would use simple organs to record the tones for their favorite numbers. So blue boxes weren't really necessary. Countless times, I was asked by my blind colleges to hook up their recorders to my Blue box.

The description and theory behind the principles of the Blue box was very well explained in the Esquire article.

The only way one would get caught using blue boxes was to dial an excessive amount of 800 numbers to places where the duration of the calls are quite short. For instance, a call to the US Army Recruiters for 4 hours might be noticed.

Now to clear up another myth. 800 numbers DID get registered on the AMA tape (Automatic Message Accounting). These tapes are fed into big mainframes to collate people phone bills. NORMALLY, 800 numbers won't get transferred to a person's phone bill. It took someone to program their computers to "Look" for unreasonable length calls to 800 numbers, but this practice didn't happen until AFTER the esquire article. People got caught by dialing (then) toll free information numbers, and dialing off those. Back then, ALL information calls (909-555-1212) would NOT register an "Off hook" signal. But if you used a blue box from them, when your party answered, you would get that DREADED off hook signal and that would CERTAINLY cause attention.

That's how "Gilbertson" mentioned in the Esquire article, got caught.

The mention of a conference number in Canada was true. That was the (in)famous 2111 conference in Vancouver. I explain it in more detail in my stories.

The quote: "Captain Crunch is one of the older phone phreaks," Gilbertson tells me. "He's an engineer who once got in a little trouble for fooling around with the phone, but he can't stop"

THAT'S NOT TRUE!! Back then I had NEVER gotten into any kind of trouble. The trouble started BECAUSE of the esquire article, which spawned massive grand jury investigations in MANY cities all over the USA as a result of that article.

The Article quoted...."Well, the guy drives across country in a Volkswagen van with an entire switchboard and a computerized super-sophisticated M-F-er in the back. He'll pull up to a phone
booth on a lonely highway somewhere, snake a cable out of his bus, hook it onto the phone and sit for hours, days sometimes, sending calls zipping back and forth across the country, all over the world...."
NOT TRUE... But it certainly sold a lot of copies of Esquire... I did have an "Automatic Box" as it was called, because the tones were pulsed out at exactly the same specification as the automatic senders, making detection harder to notice. AS far as having an entire switchboard in my Van, that's a bit far-fetched. I did drive a VW Van. Had a separate bank of about 4 car batteries in the back which operated a 110 volt inverter for my radio equipment. Which was a 2 meter FM Ham Transceiver and an FM Broadcast transmitter, mixer console, and turntables.

As far as snaking a cable out the van, THAT'S not true, but I did pull up to those "Phone from car" type pay phones, which in my area were too few to be used very frequently. I DID go on a lot of "Phone trips" where we would go out to the most remote places to see if it was possible to Blue box from them. Often I would find special codes that permitted me to access long distance numbers. I remember going to "Grasshopper Junction, Az" where all they had was those old Crank phones, and I was able to "Twiddle" a call from one of them. Reports got back to my friends back home and it was quite a feat. "Hi Denny, Guess where I'm calling from?" I would say.. then told him I was using an old crank phone. I strived to find the strangest places to call from... The Space Needle in Seattle, a train from Philadelphia to New York, and just about every landmark in the USA.

After repeated urging, I did demonstrate to Ron Rosenbaum the art of tandem stacking by calling his hotel phone and letting him hear the call "taken down" as I hung up. This produced a cacophony of chirps as the connection was torn down. It was quite a spooky sound.

By the way, I DID call the US Embassy in Moscow. Ron was quite impressed with that.... Had to go through Canada of course, because the USA wasn't on speaking terms with the USSR. I just did KP-187-ST to get the Montreal sender, then KP-07-095-252-0011-ST - I remember that number well....

07 - Country code for USSR
095 - city code for Moscow
252-0011 - US Embassy's phone number in Moscow

The super computer Blue Box was quite amazing back in its time. The esquire article explained it quite well... It used MIL-SPEC components (Which came in handy when I was up in BC in the winter time). If I were to tabulate how much money I saved using it, I would guess about $10, because I used it to dial codes not accessible from subscribers phones.

Although I had the ability to "tap" into conversations, using the "Verify" lines, it was rather risky and for me, somewhat unethical, and I only did it WITH PERMISSION of the two parties talking, for instance when the 2111 conference was being torn down, I "Jumped" on Fred's line via the Verify trunks to the amazement of both parties. The quote where the article

mentioned me tapping into my girl friends line as true SOMEWHAT but was over sensationalized.

The MF Boogie Blues was a song composed by an organ, a bunch of phone freaks and was quite funny. It was played on the 2111 conferences as well as other conferences.

The Esquire mentioned Guard banding, but it mentioned using 1700 plus 2600. This was the early intro. to Guard banding, but long after that, 3200 Hz was determined to work far better.

A lot of the quotes that Ron had claimed I made were not really true. My ears being $20,000 piece of equipment just meant that I have perfect pitch and can hear a tone and can determine within 1 % of the actual frequency, but MOST people with perfect pitch can do that.

A lot of my conversations with Ron (according to the article) made it seem like I was bragging. But a lot of information Ron got was from my younger blind friends who looked up to me as someone much older and more experienced, especially my electronic experience. But when I talked to Ron, I let him know in no uncertain terms that to publish this would cause MAJOR PROBLEMS, not for just me, but for the phone company and all parties concerned, and did everything in my power to convince him NOT to publish this information, even if he mislead readers on the actual frequencies and names involved, it was still to easy to get the correct ones, not to mention the problems for the Phone company officials and the authorities as well. However, Ron's Greed for a killer article and the money and fame he got from it reigned, and (sigh!) it was published. After that, phone hacking was never the same again.

I think that "Gilbertson" (The dude that got caught for stupidly using "long distance Information") and selling the boxes to the Mafia definitely had MONEY on his mind, and because HE got caught, he thought that he should "BLOW THE LID" and screw it up for everyone. I hate to admit, he was very successful.

This quote "Many phone phreaks pick up spending money by MF-ing calls from relatives to Vietnam G.I.'s, charging $5 for a whole hour of trans-Pacific conversation." is FALSE... In almost ALL the phone freaks I've ever known (With the exception of Steve Wozniak) NONE have had ANY financial incentive to use their skills to make money. Woz sold a number of Blue boxes to some pretty unscrupulous duds which helped him through college and partially payed for the Apple I boards that helped start Apple Computer. He put in a note "He's got the whole world in his hands" inside each one. With all the fame I've accumulated, I've never accumulated one red cent for all the hassles I've endured in all of this 25 year fiasco. Pretty much ALL book offers have fizzled, but other people have gotten filthy rich off my story (Sneakers, the movie was based somewhat on my story), where in the movie, the dude that went to jail held phone freak classes for the prisoners, and other things related to the computer accesses in the 60's. I'll no doubt cover THAT in some future entry in my WEB pages. I'm only scratching the surface right now, using just a few exerps from my memoirs.
Then I appeared on CBS's "This Morning" TV program back in 1992 during the release of "Sneakers", I said "My story is a lot more complex and interesting".

The legendary 2111 conference was explained very well in the esquire article. We found NO LIMIT to the number of people who could get on that thing. One thing the Esquire article didn't mention, was that the BC Phone company actually wired it up to it's OWN TTC code. kp-604-059-2111-st could access SOME of the lines for many many years to come (Probably 7 - 8 years longer) before the plug was pulled for good, sometime in 1980. According to reports, only 20% of the phone system still used in-band signalling. By 1982 only 5% and now today, very few circuits will respond to in-band tones, and these are watched very carefully.

The quote: "Later that evening Gilbertson finished telling me how delighted he was at the flood of blue boxes spreading throughout the country, how

delighted he was to know that "this time they're really screwed." says a lot about Gilbertson's attitude on the phone system, and Gilbertson was the person who made the initial contact with Ron to write the article in the first place. Gilbertson WENT DOWN, and wanted to take the phone company with him. I talked with him briefly (through a blind phone freaks "Line tie") this man was BITTER...

Anyway, after that article, many many people got arrested (including me), even long after I stopped doing the blue box experiments. Article came out late September, 1971, I was arrested in May of 1972..

So, these are my thoughts on the article, read it yourself, it's still very fascinating, very informative, made quite sensational, and no doubt made SOME people a lot of money. I just wish some money would have come to me for all the hassle this caused me.