Volume Thirty-Eight, Number Three
DIGITAL EDITION

2600

The Hacker Quarterly

DEAR PUBLISHERS,
YOU HAVE BEEN
"RANDOMLY" SELECTED FOR
EXTORTION. ALL YOUR
FILES ARE BELONG TO US
& ARE ENCRYPTED VERY BAD!
YOU ARE BEYOND HOPE,
UNLESS YOU SEND 25% OF
TOTAL INCOME [LINE 22 TWO 22
OF YOUR LATEST Form 1040] TO:

BTC: bc1qp64s77fke2e7ca6tadjd19r384ymvw2gxqfc67

-PUCK (HE/HIM)

Foreign Payphones

Australia. From Brunswick, Melbourne, where payphones are now free for domestic calls (meaning that message on the screen is outdated). This, incidentally, is the smartest thing we've seen done with payphones in ages: keeping them in service and making them more appealing.

Photo by Jacqui A'Vard

Northern Ireland. Technically an emergency phone, but this one really caught our eye, seen near Giant's Causeway. No matter how many times we look at it, it seems to give the appearance of being upside down.

Photo by Trevor Pour

China. The city of Chongqing, where this phone was found, has more than 31 million people in it, yet most of us have never heard of it. This tiny phone in a big booth was seen on the way to Hongya Cave.

Photo by Sam Pursglove

Austria. This is a bit of time travel. Found at the foot of the Grossglockner (the tallest mountain of Austria), this is not only a working phone, but a well maintained booth, complete with a phone book. And to complete the trip into the past, calls cost 30 euro cents a minute.

Photo by Robert van den Breemen

Got foreign payphone photos for us? Email them to payphones@2600.com. Use the highest quality settings on your digital camera! (Do not send us links as photos must be previously unpublished.) (more photos on inside back cover)

Affidavits

Amplification Gone Wrong	4
Wherever You Go, There You Are	6
Using “DeepChecksum” to Ensure the Integrity of Backups	9
I Thought the Cyberpunk Dystopia Would Be a Hacker Paradise	10
Where Have All the Tor Sites Gone?	12
TELECOM INFORMER	13
The FBI Communications Breach of 2010: Applications and Perspectives	15
Book Review: *Press Reset: Ruin and Recovery in the Video Game Industry*	17
The Phreak’s Field Guide to Identifying North American Phone Switches, Part One	18
Empty Houses	23
The Art of the Troll	24
HACKER PERSPECTIVE	26
Exploring Old MS Paint Formats	29
Keyspace Iterator in AWK	33
LETTERS	34
EFFECTING DIGITAL FREEDOM	46
Hacking NYC MTA Kiosks	47
What’s With This Username Stuff, Anyhow?	48
The Matrix Is Real: How to Hack Humans for Fun and Profit	49
ARTIFICIAL INTERRUPTION	52
Why TikTok Activism Made *Actual* Hacktivism Harder	54
Reply to: “Normalizing SASsy Data Using Log Transformations”	55
Thoughts on “Verified Badges for Everyone?”	56
The Lost Art of Windows 9x Pranking	57
An Atavistic Freak Out, Episode Two	58
HACKER HAPPENINGS	61
MARKETPLACE	62
MEETINGS	66

Amplification Gone Wrong

We've all been through some trauma lately. Whether it's due to the pandemic or the increasingly polarized atmosphere our society continues to experience, things just aren't as they used to be. We're not saying that everything was so great before. But at least we weren't as divided. At least common sense was something that transcended politics.

The consensus seems to be that social media plays a big part in this toxic atmosphere. As we've been saying for decades, any form of technology can be used for good or for evil. It's foolish to condemn new technology by default, but it's even more foolish to blindly accept it. This goes for implements of surveillance, smartphones, "convenient" services that collect and share our personal information, or even computers in general. They all can help us in significant ways. But they can also change the dynamics in a manner that's unhealthy. And, as always, the greatest danger is the perception by those growing up in such an environment that this is what's considered normal.

Social media networks need to be subjected to this same scrutiny. As social beings, we embrace the options they afford us. Even the most passionate of privacy advocates can be found using their services. There's no hypocrisy there; social media can be a great way to reach people, as well as a very effective means of organizing. Ironically, it's one of the best ways to help spread the word about the *problems* with social media.

It's hard to believe that people could really be surprised by the existence of social media's dark side. Anyone who's ever been on an IRC channel or used a bulletin board system back in the day knows what can happen when people on opposing sides of an issue dig in their heels. While there's great freedom in the relative anonymity one gets from being behind a keyboard, this only lasts until someone else uses *their* freedom to tear you down. Then it can become a serious matter, often far *too* serious in our belief. Even when there was a significant difference between the online world and "real life," it proved difficult for many to break away and not allow an online slight to ruin their entire day.

Fast forward to the present and we can see how much more harm can be achieved with improvements in technology and a far greater reach. Today, you're considered the oddball if you're *not* on social media, and anonymity is far less of an option. By finding out how many others share similar beliefs, people no longer feel they have to hide, even while possessing the most reprehensible of viewpoints. It's the polar opposite of the beneficial empowerment we can achieve from social networks, simply by realizing we're not alone. But racists, predators, criminals, and fascists can all experience the same thing by using this all-encompassing tool.

When people realize they're not unique in their beliefs, they gain confidence - and power. Societies change as a result. And what we all wind up seeing is what's been there all along. It was simply hidden beneath the surface. Again, nobody should really be surprised by this.

All of this realization is what we're currently confronting. And confronting it is *exactly* what we should be doing. Sure, we can push for legislation and restrictions to stop the hatred and keep false information from dominating our timelines. But that doesn't really work when elected officials are part of the problem. We're more likely to wind up with laws that *protect* misinformation or that push for nonsensical regulations, such as forbidding health decisions that are based on scientific conclusions or embracing wild conspiracy theories. Sure, good laws can help, but we don't trust many of the people currently in power to come up with those. The pressure must come from us directly and be aimed at those social networks currently helping to foster hate and spread blatantly false information. These companies cannot survive without the support of its users and without the support of its own staff, many of whom have ties with the hacker community.

We believe companies like Twitter and

Facebook have the right to determine the rules for their networks and decide who gets booted for violating them. And we as the end users, designers, and technicians get a big say in determining what those rules are. Government simply needs to respect the will of the people. And right now, the people are raising their voices because continuing down this path means turning ugliness into a catastrophe.

Robert Steele 1952-2021

Robert Steele was not only our first HOPE keynote speaker - he was our very first speaker, period. Look at the opening moments of the first Hackers On Planet Earth conference in 1994 and it's him you'll see talking to the audience while the rest of us were still trying to figure out how to register an unprecedented mob of attendees. This was classic Steele: stepping in at a moment's notice to engage with the crowd and tell stories.

Even at that time, people asked why we had someone with CIA ties addressing a bunch of hackers. The very simple reason was that Steele served as a bridge between worlds. Often, he would invite hackers to attend and speak at "fed" conferences and reach an audience that people like us would never encounter otherwise. Most importantly, he "got" who we were and why hackers were so valuable and precious. Sure, he sometimes came up with some wild and crazy theories, but they were entertaining to listen to and fairly innocuous.

We will always remember his dynamic style, his embracing of mischief, and his all-night spy sessions at HOPE. That is always who he will be to us.

Robert Steele died of COVID-19 on August 29th. In recent years, Steele became more and more drawn into the not-so-harmless conspiracies that we've all seen spreading everywhere through social media. He embraced far-right speaking points and was seen by many as one of the key Q-Anon proponents. One conspiracy seamlessly flowed into another: secret societies, sex trafficking on Mars, Holocaust denial, 2020 election fraud, and, finally, COVID-19 denial. It's the latter that you probably read about in stories reporting his death, as Steele refused up until the end to believe that the disease was real and insisted that the whole thing was conjured up as part of some master plan.

Many found humor in the irony. And we get that people believe he brought this on himself. A number of us feel the same way. But that doesn't mean we can't take a moment to reflect on the tragedy that this time hit close to home. It's not just the COVID-19 horror. We have become almost irreparably fractured and divisive in our beliefs and our actions. What the pandemic is doing is illustrating in short order the human toll of working to destroy one another.

The moment COVID-19 became a political issue in this country was the moment hundreds of thousands of avoidable deaths were guaranteed. In a society where half the people don't trust the other half, and even the most logical choices become suspect if they're embraced by the other side, the inevitable toll is nothing short of staggering.

The potential for ugliness and lies peddled as truth exists with or without social media. We can't ever forget that. But the amplification that these networks bring is what influences too many of us to fall for all sorts of non-trustworthy sources. But the power that we as individuals have is what will make the difference and it's what scares the hell out of anyone who thinks they're in control. We have never mattered more.

Wherever You Go, There You Are

by Mr. Icom ticom.new.england@gmail.com

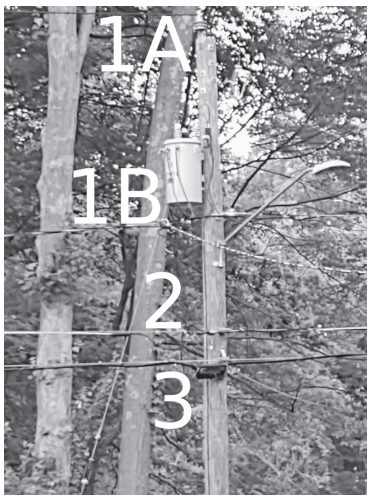
It was the early 1980s when you started seeing personal "microcomputers" in Radio Shack and in department stores such as Sears, Caldor, and Service Merchandise. The stores fiendishly placed demonstrator models in their consumer electronics departments so unsuspecting children, such as the author, could get hooked on the digital gateway drug known as Beginners All-Purpose Symbolic Instruction Code (BASIC). You start typing and, if you are of a certain ilk, the whole megillah hits you like a ton of bricks and you realize that you have the power to do almost anything with sequences of ones and zeros, and all you have to do is learn the language. It was 1982 when I received my first computer, and I got my first modem in late 1983. I quickly found Private Sector BBS, and from there learned about *2600 Magazine*. I had already become familiar with the terms "hacker" and "hacking" from reading Steve Levy's book, and from there realized two things: one did not need a computer or modem to hack, and that there was an actual word for what I had been doing ever since conscious memory. Getting notions, asking questions like "What is this?" and "How does this work?," doing research, exploring, and experimenting. You get the idea.

One of my first, and probably least successful at the time, notions was noticing a rail line, now known as the "Old Put" that ended at the lumber store where my parents used to shop, and deciding it would be a neat thing to explore. This was in the 1970s and I was about four or five at the time. This was about ten years before I learned from reading Steve Levy's book that the original hackers at MIT in the 1960s started with model railroads, and used surplus telephone equipment to do switching. A book I have on the "Old Put" showed it was abandoned a few years before I discovered it, and later I remember the railroad pulling the tracks up. The old right of way remained mostly intact for a number of years, and I explored it thoroughly looking for something I still can't quite put words to. These days it's a rail trail and much more accessible than it was in the 1980s. What's interesting about these former rail lines is that telecommunications infrastructure was, and in many cases still is, often run underground along the same right of way. One active rail line in my area still has standing utility poles marked "WUT" (Western Union Telegraph). Another former right of way turned rail trail has AT&T underground cable signs every few hundred yards or so. The underground cable markings all have fairly recent dates on them, and they are often near manholes.

My next notion involved the phone system. Keep in mind this was still during the late 1970s and early 1980s when one had to pay for any calls outside those of your local area. Running up the parents' phone bill was an ill-advised course of action, as was doing anything on a line traceable to you, but around town were these public phones that recently started providing you with a dial-tone without having to put a dime in first. You still had to pay for most calls, except for 800 numbers. It was right around this time that personal microcomputers began showing up at places where mundane parents would normally shop, and I discovered them along with modems. Then one day my friend Jim, who moved to a neighboring school district a few years earlier, introduced me to his friend Jason who was a hacker and told me about the late *TAP* magazine and this new one called *2600*.

Playing around in BASIC and early eight-bit assembly language was fun, but for me, hacking was more about networks, the lines of communications and travel that connect everything together. Computers and modems were simply tools to learn about the network, and I discovered that learning about networks whatever they may be, was and still is more about the journey than it is the destination. The destinations can be cool (and often are), but the fun was in getting there. You can start this journey without leaving home, because where you live is at the terminus of at least one network you can explore, and may be along the lines of communications of a few others. As a bonus, most of your initial exploratory efforts can be passive and/or legal. The former is good because passive exploration generates no signature for the most part. The latter is good because you don't want to get your ass in a sling and have to hire a lawyer to get you undone.

Go outside for a minute and take a look at the utility pole in front of your home. It should look something like what you see in the picture. The two sets of wires labeled 1A and 1B are electric. Number 1A is the primary at 10,000 plus volts in the U.S.

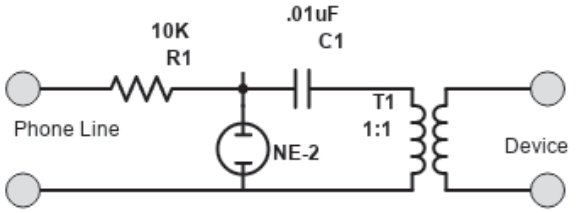


From there it goes through a transformer which is the can below the primary wires to a nominal 220/110 volt feed to your house, labeled 1B. Don't fuck with those, because they will kill you in a painful and demonstrative manner. Number 2 is the feed from the cable TV (CATV) company. It probably looks silver in color. That's a radio frequency feed, and probably the most interesting of the lot due to the bandwidth that's coming down to your house if you have the service. It potentially has both broadcast audio/video and Internet service on it. Number 3 belongs to the phone company. It's probably black in color. In most places it's a bundle of copper wire pairs, or maybe a fiber optic line. It used to be that you could get a dial tone off it, but it's just as likely to be a digital VDSL signal instead, with the dial tone provided by your VDSL modem instead of telco switching equipment at the CO or RT.

Now look on your roof. Back in the days before CATV was ubiquitous, people put antennas on the roofs of their homes to receive broadcast TV signals. This is now called "over the air" (OTA) TV, and is still a thing among some people because it is free. Last time I looked at OTA signals, I was in central Wyoming, one of the most remote places in the continental USA, and still managed to find 15 OTA channels with little more than a hunk of coat-hanger wire stuck above the roof line of a ranch house, maybe 10 to 15 feet off the ground. If you have an antenna on the roof, there is still probably some feedline going down into your home somewhere, and there still might be a working directional rotor system that lets you aim the antenna in different directions. Note this for later because that TV antenna probably has a frequency coverage range of about 50-900 MHz. and may be useful in future explorations.

What I've just pointed out to you are a few avenues of exploration that don't require you to do anything but observe and pay attention to what you discover, and take notes. This passive observation is undetectable, and for the most part totally legal. Finally, it shows you firsthand how things work in the real world.

Let's start at the bottom, and take a look at the phone line coming into your house. If your dial tone is provided by the black box hooked up to a VDSL or FiOS line, then there probably isn't much you can do. If, however, you still have a POTS local loop going to an SLC or RT down the road, or perhaps all the way to the CO, there is an opportunity to hear all sorts of interesting things while your phone is on-hook. The condition of your cable pair might be poor enough that you can hear crosstalk. You might hear a technician borrowing your line to make a phone call. You will also be able to hear any testing going on with your phone line, and anyone who decides to "beige box" off your pair.



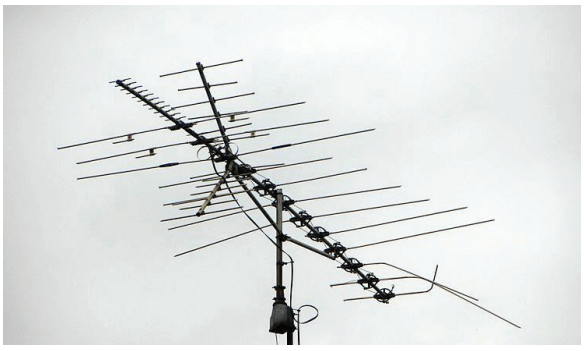
The easiest and safest (for your equipment) way to do this is to build a telephone recording interface as shown here. This schematic will allow low-level AC (audio) to pass through to the recording device, while blocking the nominal 48V and 90V line and ring voltages. A low enough DC resistance on the line will cause it to go off-hook, and the ring voltage might damage any experimental equipment you have connected to the line. For under $50 you can buy a voice-activated digital recorder that'll give you over 60 hours of recording time, or you can feed it into your soundcard input for recording to your PC. Software and stand-alone electronic devices exist that will allow you to decode DTMF tones. Recording your telecom experimentation (provided you're not otherwise breaking the law) and monitoring your line for service trouble is generally legal within certain guidelines that vary state to state. Decoding the DTMF data that's being sent on a phone line you pay for is also legal. Recording someone else's phone conversations is generally not legal.

Going further up the pole, the CATV feed gets more interesting. That coaxial cable feed coming into your residence contains RF signals from 7 MHz. to 1 GHz. The frequency range from 54 MHz. - 1 GHz. is the downstream side going from the head-end to your residence, and 7-50 MHz. is the upstream side for signals going back to the head-end. Depending on the CATV system, the signals on the feed may be analog, digital, or a combination of both. Also, depending on the level of CATV service your residence subscribes to, there may be filters on the CATV feed to block certain frequency ranges used by services/channels that are not in your subscription. If you don't have any service, the CATV provider may have installed a filter that blocks all RF from coming down your coax feed. Depending on the weather or how busy the tech was that particular day, a filter may not have been installed after service was discontinued. Filters such as these were mostly a thing back in the days of analog television when you could just hook a TV up to your CATV feed and get a nominal level of service. CATV service providers who are up to date are all digital and fully encrypted. They rely on the encryption to prevent theft of service. In this case your mileage may vary, and the only way to find out is to plug into the system and give it a look.

I purchased a Wavetek SAM (signal analysis meter) at a hamfest (amateur radio swap meet) a

few years ago for $20. This receiver was used by TV technicians to check the signal strength at a customer's residence when installing a feed and troubleshoot system problems. My SAM has a frequency range of 0-300 MHz., but some go up to 890 MHz. for UHF over-the-air television. When TV went digital, the older analog SAMs started getting sold for pennies on the dollar. These days, the older SAM units are popular with FM broadcast band radio enthusiasts. I hooked mine up to a disconnected Comcast CATV feed to discover what I could hear. The only things I heard were a couple of local AM broadcast band stations, and the digital buzz of the TV channel signals. The latter was to be expected, and I'm guessing the former was due to the length of the coaxial cable feed from the pole acting as an antenna. A TV receiver was then attached to the system and, not surprisingly, I discovered that the system was 100 percent encrypted. Regardless of the outcome, you don't know what you might find on a communications cable feed unless you explore and go look. I'm an old-school analog hardware hacker type, and prefer gear like the Wavetek SAM that I can easily take apart, work on, and modify if I so desire. Getting that kind of gear involves visiting places like hamfests and surplus stores looking for older gear cheap. If this is not for you right now, you can duplicate the previous exercise with an RTL-SDR. You will likely need an RF adapter to connect the male F-connector on your CATV coax to whatever your RTL-SDR is using, probably either an SMA or BNC female.

So far you've looked at the terminus of two different communications networks that feed into your home. Depending on the age of your telecom and CATV infrastructures, you might have discovered some interesting things or nothing at all. Whatever you found, you were still limited by the bandwidth of the media and the equipment on the other end. Now you get to expand your reach into the aether. Earlier in this article, I asked you to look on the roof of your residence to see if an OTA TV antenna was still there from the days before CATV. You should check even if you live in an apartment building complex. When I moved out of my parents' house in the mid 1990s, my first apartment had a TV antenna feed despite also being wired for CATV.



Twenty-five years later I checked Google Street View, and there is still an antenna on the roof of the building. If you have a modern (digital) TV, plug it into the cable coming down from the antenna, and do a channel scan. See what OTA channels you can receive, and research the location of the stations' transmitter sites on the FCC web page. If the antenna and cabling to it is still serviceable, you should be able to pick up something. OTA TV might be interesting for a little while if you can get PBS or an independent station that's not affiliated with the big four (ABC, NBC, CBS, and Fox), but if the OTA feed is working you should connect an RTL-SDR to it and see what else is out there. If the antenna system has a rotor on it (many home systems did), you will want to find the controller, hook it up, and see if the rotor still works. Point the antenna in different directions and note how the reception changes. Start by pointing it in the directions where the horizon is lowest, and then try pointing it at the highest elevation on the horizon. Enter in your location at `www.heywhatsthat.com/` to find these.

When investigating the airwaves, you will find a host of signals across the spectrum that your RTL-SDR covers. You will discover analog and digital voice signals that are easily demodulated and decoded if unencrypted. You will also discover data signals. Some data signals will be easy to decode, others may be proprietary and a little more difficult, and a few might be encrypted. You will also notice what are known as non-communications emitters. You will initially have no idea what these are, but you can still investigate them and find out what they belong to. CPU frequencies from the lowly 33 MHz. Intel 486 to the 1+ GHz. Intel Core models are worth noting for future reference while checking out the airwaves. RF exploring, aka aether surfing, is a subject worthy of its own article, and I'll talk about it in detail in my next one.

No matter where you go, you will find opportunities for hacking. You just need to look for them, and you can start where you are right now. It doesn't matter what you find, if anything, because this is really more about the journey than the destination, and what you learn in the process. I can recall, during my early hacking days in the 1980s, reading on BBSes about the exploits of other hackers who lived in more populated areas than I did, and finding that a lot of it didn't apply to me in the suburbs. I did, however, discover equally interesting things when I started looking around and observing where I was, and I tailored my experimentation accordingly. You may find yourself in a similar situation. Don't be afraid to wing it, and just start hacking with what you have and can find.

Using "DeepChecksum" to Ensure the Integrity of Backups

by 75ce8d3ff802ff42

The U.S. Department of Defense describes five pillars of information security:

- Confidentiality
- Integrity
- Availability
- Authenticity
- Non-repudiation

When dealing with messaging systems, we take great pains to use platforms and services that provide all five pillars, but many of us (including me until recently) don't take "integrity" into account when dealing with data *backups*. If you're like me, you worked hard at making sure that no one could *read* your backups, but didn't give much thought to someone *adding* invalid data to your backups. After all, why would someone want to plant malicious data into a backup set full of files that they can't even read? Several reasons:

- Adding illegal content to a backup could get you in a whole world of legal trouble (depending upon your jurisdiction).
- Adding content deemed "inappropriate" by your local culture/family/circle-of-friends could cause significant loss-of-face.
- If your backup contains executable software, a malicious actor could overwrite an executable (that they cannot read) with malware that your machine will execute when the backup is restored.

Now that we've established that backup integrity is important, let's talk about how you can protect yourself with a cryptographic record of what files were included in the backup.

Note: If you're using an automated backup system or backing up to an encrypted drive (which you should be doing) then this system might be unnecessary/overkill/redundant. If that's the case, consider this a safety-net/airbag/extra-protection/fun-exercise.

The goal of this mini-project (which I call "DeepChecksum") is to create a text file containing the cryptographic hashes of the entire directory tree of the directory being backed up. We can then store that file somewhere safe or (better yet) sign it with your PGP key. Fortunately there's a Linux utility for this! Enter: "hashdeep" (originally called "md5deep").

From the man page: hashdeep *"[c]omputes multiple hashes, or message digests, for any number of files while optionally recursively digging through the directory structure"*. That's exactly what we want! Note: "hashdeep" may be called "md5deep" in your distribution's repository.

The "hashdeep" package should contain several executables that do the same operations but with different hashing algorithms ("sha256deep", "whirlpooldeep", etc). Use whichever version you prefer. Read the man pages for syntax details.

Being a *2600* reader, I prefer to automate whatever I can, so I created a simple "fish" function to automate the entire process for me. ("fish" is an alternative terminal that I prefer to "bash". "Translating this script to 'bash' is left as an exercise for the student.") Just name this file "deepchecksum.fish" and drop it in "~/.config/➥fish/functions/" to make the "deepchecksum" command available anywhere.

```
function deepchecksum
➥--description="Uses hashdeep
➥tools to create checksums of
➥the current directory"
    set DATE (date +%F_%A)
    set BASEDIR (basename $PWD)
    set BASEDIR (string replace
➥-a ' ' _ "$BASEDIR")
    set HASH_FUNCTIONS md5deep
➥sha1deep sha256deep tigerdeep
➥whirlpooldeep
    set SIG_DIR Signatures_for_
➥{$BASEDIR}

    mkdir -p $SIG_DIR

    for HASH in $HASH_FUNCTIONS
        "$HASH" -rl . > "$SIG_
➥DIR"/"$BASEDIR"_"$HASH"_"$DATE"
    end

end
```

Now if you're in the directory "/➥home/1337haxor/Documents/Hacking_stuff/" and run "deepchecksum" you'll get the directory "/home/1337haxor/Documents/Hacking_stuff/➥Signatures_for_Hacking_stuff/" with text files containing hashes for all files in "Hacking_stuff" hashed with md5, sha1, sha256, tiger, and whirlpool. The files have their date of creation in the file names, and, as an added bonus, each file contains the hashes of all hash files created before it. Just sign these files and compare them to later runs of "DeepChecksum" using "diff" to detect any modifications!

Happy hacking! Stay safe out there.

I THOUGHT THE CYBERPUNK DYSTOPIA WOULD BE A HACKER PARADISE - I FAILED TO HEED THE CAUTIONARY TALE

by Johnny Fusion =11811=

What was old is new again. Cyberpunk was a literary genre that gained steam in the mid 80s, especially with the 1984 publication of William Gibson's *Neuromancer*. By the time the 90s came around, it had morphed into a subculture that attracted your typical nihilistic technofetishist. There were hackers in the cyberpunk subculture (I was one of them), but many saw it as just an aesthetic of the obligatory black leather jacket and mirrorshades. (At the time, I would say that the cyberpunk subculture was for hackers with bitchin' fashion sense.) There was even a cyberpunk ethic - a slight change from part of the hacker ethic. Where the hacker ethic says information *should* be free, the cyberpunk ethic anthropomorphizes it by saying "information *wants* to be free." At the time I wrote a shrill essay about the distinction, where the cyberpunk ethic would allow inaction, and those like me who subscribed to the hacker ethic would get off our ass and do something about it. Information was not going to free itself, and it was up the hackers to liberate it.

With the recent release of CD Projekt Red's *Cyberpunk 2077* and associated media to the same, the cyberpunk genre is having a bit of a resurgence. And in a fit of a nostalgia, I have been revisiting the media of my misspent youth when I was consuming this stuff and participating in both the cyberpunk and hacker subcultures. I understand that once upon a time (and maybe today) there was a bit of animosity between the two groups, and I understood this, but I was always poly in many respects. Polyamorous, polysexual, polytheist and so on. I never let artificial barriers, or gatekeeping, or tribal loyalty prevent me from enjoying whatever I wanted. But even so, the two subcultures were always linked. Let's not forget the days of Operation Sundevil, where in 1990 there was a massive crackdown on hackers by the United States Secret Service, and around that time, Steve Jackson Games had their offices raided illegally and equipment seized because it was believed by the feds that *GURPS Cyberpunk,* a tabletop role-playing game, was a manual for computer crime. Never mind that the technology in the game didn't even exist in the real world. The feds were scared of it and they seized all the work in progress for the product. Ironically, Steve Jackson Games later came out with a card-based game called *Hacker* that actually *did* simulate computer crime after winning their court case against the Secret Service where there First Amendment rights as a publisher were upheld.

In the late 80s through the 90s, I was a competent hacker but never did anything that made the news or caught the attention of an enterprising journalist trying to make a name for themselves with sensationalist reporting. I did the usual things. I cracked games, I wardialed and gained illicit access to systems I found in my explorations. I checked my email at the public library from terminals that had a large sign over them saying that they were not capable of checking email. I built a red box from plans in this magazine (though finding a payphone it would work on was another challenge as the phone company had gotten pretty savvy about such things back then). I dumpster dived at the phone company and computer stores. And I had been coding since writing my first program in 1978 when I was six years old.

It was my explorations as a hacker that led me to the cyberpunk genre. It started when rtm released his Internet worm in 1988 and it was reported that he was inspired by John Brunner's novel, *The Shockwave Rider*, having found a very worn copy of the book in his belongings. After reading this, I was hooked and soon I started consuming other cyberpunk literature and enjoyed it immensely. These books painted a world where if someone had the technical acumen, they could do pretty much anything they wanted. And as someone who had technical skills and no qualms about breaking what I saw as unjust laws, I thought the future predicted would be a hacker paradise and I would do very well in that world indeed. I saw the worlds portrayed in cyberpunk literature as something aspirational - where if I had enough "edge," I could get away with daring exploits, help the oppressed, and make my own justice where the legal system just dealt with oppression.

Like any misguided youth, when reading these stories and playing these games, I saw myself as the hero: a console cowboy using their elite skills to right wrongs and stick it to the man. I thought that in a connected digital future that was right around the corner, I would be prepared to be free, living as a digital outlaw and outsmarting those that chose to do me ill. I mean, I was already living that life, but I thought by the second or third decade of the 21st century the toys would be so much better.

Looking back, I see now that I was pretty much a digital version of a doomsday prepper: those nuts that stockpile food and weapons in preparation for when society goes to shit, and they would be prepared and able to survive and live like kings (relatively) in a post-apocalyptic hellscape because they have assault rifles and anything they don't have they can take. They think that when disaster hits, they will be the ones in charge. If the real 2020 (as opposed to the cyberpunk 2020) taught us anything when a real disaster hit, it's that the way through it was to be compassionate and think of others. They found themselves woefully unprepared. Believing the lie of rugged individualism, they found themselves incapable of thinking about others and over half a million people died in the United States alone because you cannot fight the coronavirus with a gun and canned food. I thought the cyberpunk dystopia would be a place where I and people like me (and the readers of *2600*) would thrive. But now that we are living in the predicted cyberpunk dystopia where tech is everywhere, the reality is that multinational corporations have undue influence over governments, and the surveillance state goes hand in hand with tech companies that treat us (or at least the data we generate) as a commodity and our privacy is bought and sold to make the richest people in the world richer, and all we get for it is intrusion into our lives, targeted advertisements, and walled digital gardens as the main way of connecting with our social circles and navigating our online lives. Sure, we can opt out of many of these things, but at what cost? Those that do opt out often live as second-class citizens in our increasingly digital world.

Our world today does resemble in many ways the 2021 predicted by cyberpunk authors and what the readers of *Mondo 2000* and posters to alt.cyberpunk on Usenet were anxiously awaiting (and me with them) in the 90s. But things are far from a hacker paradise. The closest thing I have to a cybernetic implant is a port in my chest where I receive lifesaving medication every four weeks. Instead of a cyberdeck, we have smartphones that connect us to the store of all human knowledge and nearly anyone on the planet; it just cost us intrusive spyware just to get the functionality to make it worth it, and we still have people thinking the Earth is flat and vaccines cause autism or are a means to track you via 5G signals (ironically, these people post this shit to Facebook using their smartphones and are actually being tracked, but, sure, the vaccines are the problem). The net is ubiquitous, and more and more things are being connected to it, but now your personal home network can be pwned because of shitty security in a light bulb. We can have an entire library on a tablet, but the books are riddled with DRM, and we don't even own them. Remember when Amazon removed copies of Orwell's *1984* from all their Kindle devices? Irony is far from dead.

Capitalism drives everything. The reason why this digital oppression is so widespread is because it is profitable. I remember the days when the Internet was noncommercial. I remember the first advertisement on Usenet and the uproar it caused. But the genie was out of the bottle. Instead of an Internet for the free exchange of information and ideas, it became a tool to make money.

The digital pioneers on this electronic frontier wanted a free network. It was in this environment that open-source software and hardware was born. Lest we forget, software *was* free originally. But as soon as Bill Gates started charging money for Altair BASIC and writing nastygrams to the Homebrew Computer Club about the evils of copying software, the writing was on the wall.

People fail to understand that altruism is actually in our own best self-interest, and the need for free software, open design hardware, and the free flow of information is needed today more than ever. Yes, we live in a cyberpunk dystopia, the power is centered on the rich and powerful, but time is ripe for a digital resistance. Big Brother will brand us as criminals, but that is nothing new. What have we got to lose except our chains?

Where Have All the Tor Sites Gone?

by CSCII

When I was in middle school, I stumbled upon a curious piece of anarchy in an increasingly-authoritarian world: the TOR network. Tor (short for the onion router) is an Internet protocol that relies on private exchanges between many nodes to serve information to Tor clients, like your browser. Originally built for the military, the private way to browse the Internet quickly became a haven for criminal activity. It was in the golden age of this era that I began to explore "The Dark Web."

Tor's side of the Internet was not nearly as horrifying as news articles and cringe-inducing YouTube horror videos suggested, but it was not the cleanest part of the Internet. I do not know why my goody-two-shoes self kept coming back to Tor. I was horrified by pornography and have never tried illicit drugs (though it was readily available), but it was thrilling.

Since the browser was readily available, I had no illusions about its exclusivity, but it still felt like a secret club. I dabbled in cryptocurrency tumbling and message boards, but in general I kept to lurking: looking in on the speakeasy through the peephole. Eventually, new priorities came into my life and I stopped going on Tor. After all, I had more important things in my life to waste time on, but Tor would still come into my mind from time to time, but from a more "adult" perspective of improving the protocol and contributing to the project (which I never got around to).

When I bought my laptop for college, one of the first things I installed was Tor, but I never used it, even though I majored in computer science. That changed a few months ago when I updated and ran the Tor browser for the first time in a long time. I wanted to see how the marketplaces were doing. I remembered Silk Road being taken down by the feds, but surely other markets took its place, right?

The first marketplace I visited loaded up fine, but something was different. The front page, which in years past was full of illicit drugs like weed, ketamine, and Adderall (but mostly weed), was now dominated by supposed COVID vaccines and fake vaccine cards. This was strange, but somewhat made sense, however, something else didn't feel right. It didn't feel dynamic.

There were no live conversations going on between illegal ads or fretting about the marketplace's management scamming vendors/buyers out of their crypto. The community was dead. I had no plans to do anything illegal then, but I could almost feel the boomer federal agent meme "watching me through the screen."

I went to another marketplace, but was greeted by a full screen image full of government agency seals from various countries, most prominently a German police bureau. I went to another old marketplace, and this time was greeted by the seal of the FBI detailing the site's seizure.

I googled .onion addresses of more current marketplaces and each time was greeted by taunting government entities, even the Department of Homeland Security. The overall feeling was irony, as Tor was more-or-less created by the U.S. military, and now its domestic partners were cleaning up its mess, years late to the party. However, I felt more than anything else an overwhelming sadness.

This reaction may seem childish to most readers 0f *2600*. You would probably call me a LARPer. That's fine;

I would admit as much, but the health of such a liberating (imperfect) tool such as Tor should cause concern in all *2600* readers. It is up to us to hack our way through the new barriers to ensure privacy for all. An easy way we can do this is by providing computing power. Blockchains (I know- controversial), Internet archiving teams, and the Tor network all rely on a distributed network of servers. It is not terribly difficult for many in our community to start serving these networks, and a Tor bridge requires even less. *2600* contributors generally have a healthier-than-normal distrust of corporations and governments, so let's put our money where our mouths are by supporting these decentralizing entities. And thank you, to those who already do.

TELECOM INFORMER

by The Prophet

Hello, and greetings from the Central Office! It's a typical late autumn day in the Great Northwest, raining cats and dogs and maybe hamsters too. It's cold and windy, tree branches are down all over town, and the outside plant crews are out having the kinds of days that make them question their careers. And as miserable as it is outside, and as impossible as it is to get icky-pic out of my clothes, I'd far rather be working with them than doing what I'm tasked with today.

Earlier this week, the legal department received roughly a truckload of subpoenas. Someone is suing one of our customers, and their lawyers are demanding call detail records. This customer has specially configured lines of service, running on an ancient legacy system. The tools that the legal department ordinarily uses to pull this information unfortunately don't work in the ancient system that serves this customer.

Fortunately for the legal department, and unfortunately for me, I wrote the most comprehensive set of internal documentation for this particular legacy system, so guess who they called when they couldn't find anyone else? And that's how I ended up here in the Central Office, operating under a very strict deadline, and trying to figure out how to re-ink the ribbon on a dot matrix printer. There is no easy way to output the records from this system electronically (we do have electronic output for billing, but that doesn't show call details for any local calls), and I don't have time to figure it out, given the strict timelines. Legal didn't specify the required format, so they're getting the call detail records printed - in ASCII - on dusty tractor feed paper! I'll send it to them via interoffice mail in a large sized banker's box.

Most people don't realize the level of granular detail that call detail records contain about who they call, when they're calling, for how long, and from where (both virtually and physically). Our records contain everything that engineering teams need to troubleshoot a problem circuit - trunk, circuit, etc. Mobile phone records go far beyond the level of detail that we have here in the Central Office; they can include the IP address issued to the handset, the physical location of the towers that handled the call, and even the physical location of the handset (when 911 calls are made). They additionally contain details of text and picture messages sent and received - sometimes even including the content. These can be maintained for an exceptionally long period of time - up to seven years!

That's why attorneys love call detail records, and often seek to subpoena them. "Oh, you claim you weren't cheating?" a divorce attorney might say. "Then why was your phone making calls to your wife from the neighborhood where the woman you were cheating with lives, and the side of the tower that picked up your call is the one pointed at her house?" It's "smoking gun" evidence like this that attorneys are seeking when they subpoena these records and, of course, law enforcement makes extensive use of call detail records too. While access isn't guaranteed in civil cases, very broad access is granted in criminal cases. A law called 18 USC § 2703 outlines the rules under which law enforcement is granted access to these "business records," and they aren't very strict.

The process starts with a "letter of preservation," where an attorney demands that records be preserved. This must be for a specifically defined period of time, and typically includes the following data for a mobile phone carrier:

- Subscriber billing and account information (typically name, address, and other subscriber contact details such as email address, other phone numbers, etc.).
- Any details that the carrier has on when and where the service was set up, whether the phone is an individual, commercial, or family subscription, and any associated telephone numbers on the account.
- ESN, MEID/IMEI, and IMSI information

of the device.

- Call detail records for telephone calls, SMS text messages, MMS picture messages.
- Records of data sessions, including IP addresses, amount of data transferred, and URLs of websites visited.
- Metadata for all stored voicemail messages. Typically, they'll request the content too, and carriers have to preserve that. But in the end, courts often only grant access to the metadata.
- Cell tower location information.
- RTT/PCMD data (this is diagnostic data used to troubleshoot call quality; attorneys like to have this so they can push back on unreliability claims).

At the time a preservation request is received, phone companies don't provide any information to the requesting party. In most cases, the legal department will typically use an automated internal tool (written by a consulting company they hired) to gather all of the information that is requested. They store it in a case management system (creating a new file for each case), and in theory, we never need to be involved or even know that any of this is happening. In many cases, an information preservation request is filed, but no subpoena materializes so the data never leaves our systems. If the court approves a subpoena, the legal department will use a secure managed file transfer service to deliver the records to the court (and only the specific records approved by the court, which doesn't always match what we were requested to preserve).

Of course, there is "in theory" and "in practice" and you probably know where I'm going with this. In practice, the legal department hired the cheapest offshore vendor they could find to build their glitchy automated tool (presumably out of chewing gum, string, and a discarded tennis shoe). It is buggy and breaks a lot, and it throws inscrutable error messages, so we often get involved to help troubleshoot. Having learned through experience why the tool breaks, we can usually manage to adjust our systems around the tool's expectations in order to help the legal department get the information they need. Occasionally, it entirely breaks. In this case, we'll pull the records manually and drop them in a folder on their unreliable document management system I'll call "SwearPoint" for no particular reason. We can work with them to try to fix it, but the engineers are in Bangladesh and the vendor doesn't allow us to talk to them, so we have to hope that their "technical" project managers actually understand the problem and can get it fixed. You can imagine the hilarity that ensues.

And then, of course, there are legacy systems like this one, which was deployed in the early 1980s. Two corporate entities ago, business decisions were made to replace aging legacy systems with new, modern ones. And then, there were new corporate owners with a new corporate strategy whose playbook was largely "raise rates as much as possible while running the network into the ground." The new owners have more or less the same "harvest" strategy. Because the systems are still technically slated for retirement, no new investments are being made into them. This includes compatibility work for internal tools, such as those used by the legal department.

And with that, it's time to ink this dot matrix printer ribbon again. I found an ancient inking kit in storage, which still somehow works! Naturally, though, when I opened the bottle I managed to spill ink all over my hands. I'm going to be here all night listening to a nine pin chorus, and dealing with paper jams in the tractor feed. But I'll meet the legal department's deadline, and might even be named Employee Of The Month! Have a wonderful Thanksgiving, and I'll see you again in the winter.

References

Sample Letter of Preservation: www.➥irisinvestigations.com/➥wp-content/uploads/2019/06/T-➥Mobile-Letter-of-Preservation-➥Template-11-20-18-1.pdf

Mobile carrier records retention policies: www.➥irisinvestigations.com/wp-➥content/uploads/2018/06/IRIS-➥LLC-Cellular-Service-Provider-➥Retention-Schedule-6-22-18.pdf

How police and investigators use call detail and cell site evidence: www.irisinvestigations.➥com/wp-content/uploads/2019/06/➥CALL-DETAIL-CELL-SITE-06-11-19.pdf

THE FBI COMMUNICATIONS BREACH OF 2010: APPLICATIONS AND PERSPECTIVES

by Marc J O'Connor

This article explores the "FBI communications breach," first reported in 2019, as an application of publicly known and researched vulnerabilities of P25 communications systems and considers them in an operational and intelligence context with possible tactics employed and as exploration of open source technologies and literature.

This article assumes the Russian Intelligence Service (RIS) targeted Federal Bureau of Investigation (FBI) land mobile radio (APCO P25) and cellular telephony (4G LTE) employed by FBI counterintelligence activities in order to develop intelligence on FBI counterintelligence operations directed against the RIS.

Overview

P25 Land Mobile Radio systems is the communication technology employed by law enforcement and emergency first responders by over 38 countries, including the U.S., Canada, Mexico, and Russia. In the United States, it is the result of a decades-long transition from analog single channel radio systems to networked digital radio systems, beginning sometime in the 1990s and reaching some degree of completion in the mid-2000s.

APCO P25 Land Mobile Radio (LMR) systems are digital radio systems that provide narrowband data, voice encryption, and addressable and trunked (like a subnet) communications. The P25 LMR can have 9,999,999 individually addressed subscriber units organized into talk groups. P25 can be trunked and transported over Internet Protocol networks.

The FBI maintains the largest P25 land mobile radio system in the world, providing nationwide coverage to federal law enforcement operations, and inferred in this article, their counterintelligence surveillance teams. The FBI maintains this system for the Department of Justice, and the customers are the DoJ appendixes: DEA, BATFE, and U.S. Marshals Service. It is not solely an FBI resource.

From public news services, it was found that the RIS employed an operation to develop intelligence from FBI telecommunications in 2010. These telecommunications are inferred to be the nationwide Land Mobile Radio (LMR) network developed by DoJ for federal law enforcement, and exploitation of the backup telecommunications system, provided in public sources as LTE, or Long-Term Evolution, a cellular service more presently known as 4G, with an additional push-to-talk capability to act as a two-way radio.

Technical Background

An individual APCO P25 radio carried by a person or installed in automobiles is a "subscriber unit." Each subscriber unit must be programmed with a unique unit identification in order to participate in trunked or networked communication. Each unit must also be programmed with a group unique talk group identification to participate in talk groups.

Cellular telephony selectors are better known: the IMSI or telephone number and the IMEI, which is the electronic serial number of many cellular devices. These two selectors, known as "the pair," are emitted constantly as the cellular device seeks an available base station to associate to the network. It is these selectors that are collected using IMEI catchers like the popular Stingray and Do-It-Yourself (DIY) systems.

P25 research has been performed using Software Defined Radio and open source software, notably, Ettus Research Universal Software Radio Peripheral (USRP) , GNU radio software, and Wireshark.

It would appear axiomatic that an APCO P25-using country, like Russia, would have firsthand knowledge of vulnerabilities that would come to the attention of its intelligence services in addition to a large pool of talent and networks to develop technical exploits.

Operational-Technical Games

An actionable intelligence requirement for a clandestine intelligence officer is their surveillance status. Intelligence officers employ surveillance detection tactics, techniques, and procedures to determine hostile surveillance status.

Based on known P25 and cellular handset vulnerabilities, it is possible to develop actionable intelligence to satisfy this requirement using only signal externals: the peculiar metadata accompanying each transmission that is necessary to implement the communications service, but does not include content, per se.

Here the presence of certain telecommunications metadata could aid in the surveillance determination. The "fact of" peculiar metadata in vicinity of the intelligence officer would strongly indicate hostile surveillance activity. That peculiar metadata may be envisioned as a "tag cloud" of selectors where each tag is a metadata element from some electronic device.

In this scenario, these metadata are the IMSI/

IMEI from the PTT cellular devices, the unit identification, and talk group identification from the inferred use of P25 radios by the FBI - and these metadata form part of the tag cloud surrounding the FBI counterintelligence activity. These tag clouds are observable, unique, and sufficiently unchanging.

RIS surveillance detection would take the FBI surveillance from the surveillance pickup point and maneuver on foot or vehicle to sift the collection of signal externals in order to isolate FBI peculiar selectors. That media reporting implicated California, New York, and Washington DC RIS activities, then a better opportunity is presented for differentiation of selectors. In this, FBI tag clouds were observable at these locations, but the extraneous tag clouds unique to these locations would be eliminated, being peculiar to these geographic areas.

Over time, repetition of this sifting would refine the tag cloud collection - the same tag clouds in vicinity of an intelligence officer despite distance, observed and integrated over a long baseline. If one can envision that surveillance detection is a type of maneuver warfare, then the use of surveillance detection is limited by creativity and here it is likely used to provide a sifting/filtering mechanism.

The use of surveillance detection augmented with signals monitoring provided by COTS hardware and software would provide supporting data to confirm/deny the presence of FBI personnel in the area based upon presence of selectors and traffic analysis of unit ID and talk group ID emitted from the APCO P25 handsets and IMSI/IMEI radiating from the PTT cellular handsets.

Once an RIS intelligence officer was certain they were under surveillance, this information may be correlated to observed selectors (the tag cloud) also at that point. Similarly, the absence of that metadata would inform perspectives as to an RIS officer's surveillance status.

The use of traffic analysis and pattern observation from physical and technical surveillance is the crux of the exploit. Operational sophistication stems from this and its fusion with tradecraft to produce military effects.

History

The use of SIGINT-enhanced surveillance detection has precedents. In 1977, the CIA employed a specialized radio receiver to detect KGB surveillance of CIA officers stationed in Moscow. Such a receiver was discovered with CIA officer Martha Peterson after her capture by the Soviet KGB while she was engaged in a high-risk operation in Moscow. KGB and East Bloc officers employed similar technologies with the *Kopchik* surveillance receiver. This communications breach is part of that historical and technical continuum.

Timeline of the Reported Breach in Relation to P25 Security Research and News

2019 - Yahoo breaks story. This is the first public reporting.
2016 - Russian diplomats expelled.
2012 - FBI "full gravity" of breach realized.
2011 - P25 papers at Ruxcon and SecureComm.
2010 - FBI "first breach" detected; DES Research, first public P25 vulnerabilities made public.
2009 - Development of Open Source P25 research platform.

Between 2010 and 2012, there was an investigation of the breach, given the publicly reported outcome was "full gravity of hack realized." Such an investigation likely supported the expulsion of Russian diplomats and was a component of a larger counterintelligence effort.

Application in Open Source Warfare

In this scenario, military effects - deny/degrade - were induced by one state actor upon another, but noteworthy that the technologies involved and the tactics needed to employ them are available as open source information and are developable and deployable by non-state actors.

Such application further distorts the symmetrical relationships and capabilities between state and non-state actors and develops a cognitive and perceptual terrain within that distorted space. Here, the non-state actor may develop counterintelligence that can compete with the state actor security services and use this (formerly) advanced SIGINT capability in competition with other groups, as in a fourth-generation warfare (4GW) environment.

A perspective may be taken that this exploit was successfully tested between two technically and operationally sophisticated adversaries - probably the most rigorous laboratory available for such an application.

Postface

This article focuses on a plausible scenario of communications exploitation that would produce actionable intelligence using open source technologies. The thesis was developed from well-known security research that was operationalized in these exploits. It does not include specious and sensational narratives of vague "backdoors," and "broken encryption."

Bibliography

1. Zach Dorfman, Jenna McLaughlin and Sean D. Naylor. "Russia carried out a 'stunning' breach of FBI communications system, escalating the spy game on U.S. soil." Yahoo! News, 16Sep2019. www.yahoo.➥com/now/exclusive-russia-carried-out-

➥a-stunning-breach-of-fbi-
➥communications-system-escalating-the-
➥spy-game-on-us-soil-090024212.html
2. William Jackson. "Project 25: The Long And Winding Road To Radio Interoperability." GCN, 09Apr2013. gcn.
➥com/articles/2013/04/09/project-25-road-
➥to-radio-interoperability.aspx
3. Stephen Glass, Vallipuram Muthukkumarasamy, Marius Portmann, Matthew Robert. "Insecurity in Public Safety Communications: APCO P25. Security and Privacy in Communication Networks." 7th International ICST Conference," SecureComm 2011, 7-9Sep2011. eudl.eu/
➥pdf/10.1007/978-3-642-31909-9_7
4. Sandy Clark, Travis Goodpseed, Perry Metzger, Zachary Wasserman, Kevin Xu, Matthew A. Blaze. "Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System." www.
➥mattblaze.org/papers/p25sec.pdf, 10Aug2011.
5. Matt Robert. "APCO P25 Security Revisited." RUXCON 2011. paper.seebug.org/papers/old_sebug_
➥paper/Meeting-Documents/Ruxcon2011/
➥RUXCON_2011_slides.pdf. 19Nov2011.
6. Sandy Clark, Perry Metzger, Zachary Wasserman, Kevin Xu, Matthew A. Blaze. "Weaknesses in the APCO Project 25 Two-Way Radio System." repository.upenn.edu/cgi/viewcontent.
➥cgi?article=1990&context=cis_reports. 18Nov2010.
7. Chris Paget. Practical Cellphone Spying. DEFCON 18. www.defcon.org/html/links/dc-archives/
➥dc-18-archive.html 30Jul2010.
8. Steve Glass, Portmann Marius, Vallipuram Muthukkumarasamy.
"A software-defined radio receiver for APCO Project 25 signals." publications.csiro.au/
➥publications/publication/PInicta:1710
➥2009
9. www.cryptomuseum.com/people/peterson/
➥index.htm
10. www.cryptomuseum.com/covert/radio/
➥srr100/index.htm
11. www.cryptomuseum.com/covert/radio/
➥kopchik/index.htm
12. Davey Winder. "Russian Spies Breached FBI Encrypted Communications" Forbes. www.forbes.com/sites/
➥daveywinder/2019/09/18/russian-spies-
➥breach-fbi-encrypted-communications-
➥no-backdoor-needed/?sh=41366592128d
➥18Sep2019.
13. Mike Masnick. "You'd Think The FBI Would Be More Sensitive To Protecting Encrypted Communications Now That We Know The Russians Cracked The FBI's Comms." *Techdirt*. 17Sep2019.

Marc J O'Connor is the author of "Electronic Warfare for the Fourth Generation Practitioner."

Book Review

***Press Reset: Ruin and Recovery in the Video Game Industry*, Jason Schreier, Grand Central Publishing, 2021, ISBN 9781538735497**

Reviewed by paulml

This book is all about the video game industry as seen from the inside. It's not pretty

The job may sound like a dream come true. The game will sell a million copies in its first weekend. The lines outside the video game store will be like those when a new iPhone is released. The game is made for a big-screen movie, a TV series, and many game sequels.

A year or so later, there is an all-hands meeting where everyone is told that the company is closing - today. Some companies may offer severance policy, but don't count on it. The employee is forced to move across the country to some other company that has an opening - until *they* abruptly close. After several such moves, any luster the video game industry may have had is gone.

The book also talks about crunch time (with Release Day approaching, all employees are expected to put in 80-100 hour weeks to get the game finished). It also talks about Curt Schilling's 38 Studio in Rhode Island: they were going to create a game that would be more popular than *World of Warcraft*. Things did not end well. This is an eye-opening book about the video game industry - for those of us on the outside. It is highly recommended.

WRITERS NEEDED!

There are so many topics in the hacker world that capture our interest. And everyone reading this has their own story to tell involving technology and their adventures with it. We need more of you to send us those stories so we can keep capturing and inspiring the imagination of many readers to come!

Send your articles to us via email at **articles@2600.com**

We prefer ASCII but can read any format. Most articles are between 1000-2000 words, but we have many that are fewer and a bunch that are more. What's important is that you add your voice to those who have written for *2600* over the years. (We've never heard anyone say they've regretted it.)

For those without Internet access,
our editorial department can be snail mailed at:
2600 Editorial, PO Box 99, Middle Island, NY 11953 USA

All writers whose articles are printed will receive a one year subscription (or back issues) plus a t-shirt of their choice.

The Phreak's Field Guide to Identifying North American Phone Switches, Part One

by ThoughtPhreaker

Whether you're just bored and looking for some trivia, want to learn how to identify a switch from a mile away, or just want to obsess and compulse over tiny details, get comfortable! One of the things that makes phreaking way more fun is being able to know exactly what equipment you're hitting, and this article is stuffed to the brim with plenty of crap to let you do just that. So, er, enjoy!

Identifying Switches Through Ringing Numbers

One of the best kept, hiding-in-plain-view secrets of the modern phone switch is that no two model types ring alike. The difference is pretty simple; when the ring is generated, something (probably a DSP chip) is looping a pre-rendered waveform with ringback on it. These loops are all slightly different in tiny little ways: some are shorter, some are smoother sounding, and so on. So while it might sound absolutely insane, with a little practice you can be the guy who squeezes blood from rocks at a party! Er, well, if you go to the sort of parties where people talk about phone switches.

Before we start, just make sure you're using a decent phone. If you're using something like a DECT phone that compresses the call as ADPCM, that's fine. A basic WECo desk phone on a POTS line in a quiet room or something that sounds equally good is probably the best starting point, though. Linear predictive codecs, such as the ones cell phones, Skype, etc. use take out way too much data to be useful. Things like Google Voice like to superimpose fake ring over unsupervised audio (though JCSwishman has noticed the mobile Hangouts dialer doesn't do this. The drawback though, is they use some weird codec to compress the call with this client), and since most rings don't go offhook, obviously that's out for this sort of technique as well.

With that out of the way, let's start with an example that you'll probably come across a lot; 5ESSes and DMS-100s. These are actually two of the easiest to tell apart, coincidentally. Nice how these things work out. So go ahead and call 202-986-9992. If you're like the other phreak I gave this to, your first question is probably "Uhh, is this a queue recording or a porno?" By the time you're done asking yourself that, the recording will probably have stopped, and you'll be sitting on a trunk that just plays ring forever.

Get a good sense for what it sounds like. The 5ESS ring is really smooth sounding - there's no clear noise it makes when it loops, but the phase of the ring slowly changes, like a warbly tape. If it helps, don't just hold the receiver flush against your ear. With one end of the earpiece resting against your ear, let the other end fall (the left part if you were to hold it straight up, facing you) ever so slightly so there's a gap between your ear and the receiver. Or if you're a little fuzzy on what I mean, just pull it half an inch away from your ear or something.

Sounds good? Great! Now try calling one of the DMS-100 ringout numbers. Unlike the 5ESS, whenever the sample loops, you can very clearly hear it repeating over and over. I don't think there's a lot of ways to describe different rings, but the audible looping gives it a very rough sound when you're comparing it.

Some rings, like the AXE-10's, are so distinct sounding that it's almost cheating to compare it to anything. Then there's the Redcoms, the DMS-10, and type two EWSD. Actually, try calling them right now. Really tough to tell apart, aren't they? Don't feel too bad - I have trouble with these too sometimes. If you're ever in a position to call them frequently (I'd say scan, but they typically don't ring to error recordings. Maybe pick an exchange with weird stuff on a lot of analog lines if you know of one), it'll make it much easier.

5ESS

The result of 20 years and 100 million lines of source code, the 5ESS is Western Electric's take on a digital switch. Though it wasn't always this way, the 5ESS in its current state seems to have an answer for everything; most of my experiences trying to give the 5ESS some form of unorthodox input seem to end with it giving the most normal possible responses. This contrasts starkly with the DMS-100, which seems to love behaving strangely at any given opportunity. In all fairness, the DMS-100 also has been explored far more thoroughly.

- 5ESS line cards are pretty distinct sounding. They'll make weird noises whenever you go offhook, have a slightly higher noise floor than most line cards, and a very strange frequency response. This doesn't necessarily apply if you're using a line served out of a channel bank or something, but the line cards can give a very different experience on the phone network sometimes. According to Aloha, the noises are a result of the 5ESS setting up a link through an analog switching fabric. Though the 5ESS is a digital switch, an analog cross point switch is used to connect your line to a codec instead of having one permanently associated with your line.
- Supports revertive pulse trunks, a signaling system designed in the 20s to directly drive DC motors in panel switches. To this day, the reports on a ROP (read only printer) include a spot for the number of revertive pulse calls placed on the switch, in spite of the hardware to do this probably only existing in a dust-covered box near some of the oldest 5Es, having not even existed until the twilight days of these systems.

- Supports both drum and AIS-style announcements, but the vast majority use drum-style; where recordings play in a continuous loop, and the switch routes you to the transmit timeslot when it comes back to the beginning. For that reason, you'll see some very strange arrangements sometimes. AT&T CLEC/Teleport for example, rolled out APMaxes for their 5Es, but configured them in drum mode (they also have Cognitronics MCIASes in AIS mode, so they definitely know how to do it). This is the only place in the network where you'll hear error messages ring for an absurdly long time (with TTYs, the recording is pretty long) before starting up.
- If you make a large number of unsuccessful call attempts (can be something as simple as just picking up and hanging up, but partial dial works too), it'll pull your line out of service for 100 seconds, and if you're not on loop carrier, remove power from your line as well. Assuming you don't have voicemail, the 5ESS will spit back an unusual SS7 disconnect message at anyone calling you under this condition. Use your best judgment with this; the switch will print a message on the console saying your line is having trouble if you do it. Probably not an issue, but a responsible operating company (read: none of them) might call you and ask if everything is okay if it happens multiple times.
- Has an unusually large, 16-bit internal frame size on its TDM bus; the most significant eight bits are the content from the corresponding channel (digitized output from a POTS line, a T1 timeslot, etc.), followed by four signaling bits (likely meant to transparently send the A/B/C/D bits associated with E1s and ESF-framed T1s; D4 framing only contains A and B bits), a supervisory (off-hook/on-hook) bit, a TMS buffer bit, followed by framing and parity.
- With the exception of the VCDX, which emulates the administration module on a SPARC machine, the 5ESS has become perhaps the champion of custom architectures, being the last known switch to use a custom CPU for any components. In this case, the administration module, largely a terminal to manage the switching and communication modules (though some systems use it for SS7 as well), runs on a 3B21D, utilizing the bizarre WE32100 processor.
- Earlier switching modules - largely what you interact with at dial tone - are based on Motorola 68K processors. Newer SMs were redesigned to use PowerPC CPUs, and support a greatly expanded capacity.
- Some 5ESSes will terminate a call immediately if it sees the slightest blip of on-hook supervision from a trunk, like for example, the Redcom supe test later in this article. Strangely, using a vertical service code like *67 will make it wait a bit longer for off-hook supervision before deciding it should tear down the call.
- Known to, at least in one specific instance, drop you directly onto the trunk to an ANAC with nothing dialed! You can feed it MFs. Try KP + 3 (other digits get more interesting behavior) + 7 digits + ST. I've seen another 5ESS (the Teleport one in Omaha specifically, OMAHNEXODS0) exhibit this behavior too.
- Was known in early generics to have some very amusing bugs; one allowed you to cause an ANI fail on outgoing calls, another let you "service observe" someone's line by creating a notest trunk via a management terminal, and forwarding it to a victim.
- Allows you to mix touch tone and rotary dialing on the same call, but once you start rotary dialing, it'll lose its ability to hear * and #. For example, if you dial 1167 with mixed tone/pulse, they won't even break the new dial tone.
- Gives short burst of dial tone after dialing a rotary digit, but *only* after dialing a vertical service code. Straight from the dial tone, there's no burst.
- Some RBOC 5ESSes (mostly non-ex-US West ones) allow you to originate calls onto the 0110 carrier access code, a workaround code that places calls onto the trunk group for local calls. RBOC DMS-100s on the other hand, never, ever do this.
- Seemingly incapable of giving any sort of DISA to anyone outside the switch without external hardware. This changes the dynamics of things you'll find in the wild when hand scanning a 5ESS.
- While this is far rarer than on a DMS-100, some 5ESSes can enter a condition that resets you back to dial tone without hanging up. Most switches in incumbent AT&T regions will demonstrate this behavior with a CAC + 0-710 and any seven digits. For example, 101-0288-0-710-222-2222. A strange recording from hardware that doesn't typically play announcements on that switch should start up. In theory, resetting to dial tone without hanging up is a really serious security hole when dealing with PBXes, COCOTs, or other things that are supposed to log/restrict/bill/whatever calls that go out on POTS lines. And on a DMS-100, it is since there's nothing to tell whatever sits on the phone line that the call is done. Unfortunately for anyone fixing to do some security "audits" (the 0+ example call should be programmed as free in most things), the 5ESS pulls battery on its lines for a second before giving you dial tone again. Anything listening for that (and not everything is) will accurately see the interruption in loop current as the end of the call.
- Trmg, one of the core members of the National Questionable Telephony Foundation, discovered a bug in the 5ESS; when calling someone with call waiting and no call forward on no answer (i.e., voicemail, etc.), if the called person hangs up, the 5ESS won't ring their phone back, yet the person calling will still get ringback. In spite of being able to pick up the phone and get dial tone, anyone calling the called party will get a busy signal so long as the person that made the initial

call is still getting ringback. This is believed to only work on intra-office calls.
- From a signaling perspective, the 5ESS' ability to handle fuckery is as admirably (but regrettably) good as it is when sitting on the business end of an analog line. For example, PBXes and other things of the sort tend to be pretty regularly vulnerable to a Heartbleed-esque misuse of a byte counter in ISDN and H.323. If you were to send, say, a display information element (basically, Caller ID Name), it might look something like this: 28 02 48 69, where 0x28 indicates a display element, 0x02 is an unsigned 8-bit integer conveying it's two bytes (sorry, I mean octets) long, and 0x48, 0x69 just says "Hi" in ASCII. Naturally, if you're in a position to manipulate any of this, you might be tempted to tell the switch you're sending more bytes than you actually are. And usually this is a great way to suck up all manner of uninitialized data from previous calls; especially since a lot of q.931 implementations ignore the 82 octet limit of a display IE and let you make it as long as you want, so long as your invisible data isn't going past the length of an LAPD frame (260 bytes). Not so on the 5ESS; any inconsistencies in the length return an ever so disappointing release complete message with cause 100: invalid information element contents.

Remote call forwarding prompt: 608-819-0018
Ringout via some sort of call queue script: 202-986-9992 . This also serves as an example of the all-too-common 16A announcement system in nearly every 5ESS owned by an RBOC. Its distinct sound is caused by the use of an ISD chipcorder, an IC that stores sampled analog values in non-digital form on flash memory.
ANAC trunk, goes offhook and waits for MFs: 503-697-0053
Something to do with ANAC? Gives high tone (480 hz) if call comes in via external trunk, quickly heads to reorder: 813-386-9170

DMS-100/200/250/300/500

One of the most popular switches in the U.S. and Canada, this thing was Nortel's love child for pretty much the company's entire existence. As a consequence, it holds the title of being not just one of the most feature packed, but one of the funnest to play with - or maybe just the most explored.

Though it's been around for decades, the DMS-100 hardware has evolved considerably since it was first made. For example, the original processor was something Nortel (Northern Electric at the time) concocted themselves; an NT-40 core made out of discrete logic chips, also used in their SP-1 processor-controlled crossbar switch. In the 1980s, they ported the software to a redundant pair of 68000s. By the next decade, that became a pair of 88000s. Finally, around 2000, the new processor cards began operating with three PowerPC 604s (XA-Core as they call it for some reason) and only contain a single spare, with a final evolution to G4 chips not long after.

So why all the different names, you might ask? Marketing mostly; they're all DMS-100 family switches with software to do different things. 100 is an end office, 200 is a local tandem, 250 a toll tandem, 300 an international gateway, and 500 combination end office/toll tandem.
- Supports revertive pulse trunks.
- EDRAMs. What the hell is an EDRAM, you ask? The EDRAM is Nortel's crazy announcement machine, or Enhanced Digital Recorded Announcement Machine as they call it. As far as underground (or just plain questionable) telephone scientists can determine, Nortel went out of their way to make their own ADPCM format for these things. Information, as well as the stock announcement set (complete with Nortel's weird container format) are available in random places on the Internet. These are an evolution of the DRAM, which perform more or less the same function, but have lower capacity and took up a whole shelf instead of a single card.
- Ringout conference bridges (internally called MMCONF).
- Able to give DISA dial tone via software! This is very frequently used to give remote access to Centrex and other non-standard dialplans, along with other goodies in test ranges. Being done in software, people who set these up tend to forget about them once they're there.
- In cases where the switch is bridging together multiple calls, such as three-way or an MMCONF, the DMS-100 uses some sort of secondary, different sounding source for all its tones. It's still not known why this is, or where the primary or secondary tone sources are coming from. The DRAM/EDRAM cards are capable of generating some of them however, such as milliwatt and offhook. The offhook tone's susceptibility to this has been confirmed, but other DRAM generated tones such as SITs don't seem to be affected by this. Maybe the DRAM is the secondary source? Very old offices had actual hardware oscillators on a card for offhook, milliwatt, etc. While these are rarely if ever still in use, a DMS still using these cards could potentially answer this.
- Some offices will occasionally have very strange sounding reorders.
- Some lines on some switches will make a soft tick sound when the switch stops waiting for digits, and start processing a call. No correlation is known yet, but I think this may only be done on lines using loop carrier arrangements. Newer generation DMSes possibly don't do this altogether?
- Late in its development life, Nortel wound up porting the Linux kernel to the DMS-100.
- Internally, the system likes to send data in a format called DS-30 and DS-512. Basically, just a lopsided E-carrier format (E1 and E3) that uses ten-bit frames instead of the traditional eight-bit ones. The first and 16th channel of a DS-30, like an E1, are reserved for signaling purposes.

The eight most significant bits are passed transparently from the source channel, while the last is used to indicate parity, and the second to last supervision on every sixth frame conversion.
- On analog E&M trunks (namely the one your ANAC is on if it doesn't just read off digits with the EDRAM), you can flash at just the right time, flash back, and hold the unit up indefinitely.
- As a consequence of possibly the exact same bug, you can stop another caller from flashing on intra-office calls by flashing; the other line won't be able to use it until you return to its call. Great for Centrex auto-attendants? Some ex-GTE regions (most notably, parts of Ziply and Frontier territory) run voicemail on a uReach Oryx system sitting on analog Centrex lines. Unsurprisingly, in almost all cases except a few in Florida, it flashes when it transfers you to something. How the system reacts to this is a question I'm itching to answer.
- Some (most notably, historically independent DMS-100s, like the ones operated by United Telephone, Alltel, GTE, etc. - ex-Bell switches typically won't do this) have dialplan errors; they'll let you dial 0xx and 1xx codes, nine-digit numbers, and other weird things if a CAC is put in front of the destination. For example, 101-0288-1-208-038-1152 will go through, but 1-208- 038-1152 gets an error recording. In that particular case, while 0288/AT&T is capable of routing 0xx traffic, you'll probably just get a recording from a tandem switch instead of from a normal phone line (the Bell Canada network will put up with this behavior just fine - use that to your advantage if you can). If your DMS is cool enough to allow this, there's ways to use that to your advantage, but that's a whole other topic.
- Pacific Bell, and possibly Nevada Bell DMSes are set up in a particularly funny way; if you dial * as one of the last three digits, it'll stop in the middle of the intercept recording, and give you reorder. Alternatively, if it's generating SIT tones (the EDRAM units loop uLaw PCM samples to do this instead of play ADPCM) or a reorder when it stops, you'll just go to dead silence.
- Always has a burst of dial tone after dialing the first rotary digit.
- Some SS7 disconnect messages have q.850 cause codes that make most DMS-100s reset back to dial tone. If the number listed at the bottom doesn't work for you the first time, try it again. On some offices, the likelihood of working is less than others for whatever reason. It might have something to do with the hardware handling the call.
- Standard busy/reorder always go for exactly 30/60 impulses.
- Occasionally you'll run across a DMS that, for whatever reason, has a different pitch in its reorder tone, but also weird timing.
- Will often, but not always send back an all circuits busy message via SS7 when disconnecting after a recording. Some long distance carriers respond to this by assuming the route is busy and, if there are any, cycling through to the next route in the least cost routing list. Though it's definitely not sending an all circuits busy message back, a switch in Washington DC will send something just as strange after playing three bursts of dial tone.
- Like the CS-2000, has I/O processors capable of encapsulating data over ATM delivered via OC-3 links.
- DMS-100 call forwarding translations are quite literal. For example, if 1-958 and your last seven digits will forward you to the ringback program, calling your own number will still get it for you. Consequently, this means other good fun can be had though; if you have a silent switchman test (plays a distinct tone - in the case of a DMS, a slow busy tone, and then pulls your line out of service temporarily) on a seven-digit number, you can forward your calls to that, and anybody on the same switch calling you *will* get their line yanked for 100 seconds. Sadly, this behavior only lasts until the DMS-100 releases your line from the great void. Perhaps even better though, selective call forwarding can be established on a permanent basis to these things. And it'll still give your phone a single ring to inform you when someone has been unfortunate enough to have taken the bait.
- Flashing during SIT tone generation on your local switch (even when you have another call ready to be three-wayed in) *will* make it dump all your calls.
- Flashing during some local announcements, even if you have a line without three-way calling (it usually won't let you get a stutter dial tone at all if this is the case. Some DMSes only allow this without three-way when dealing with certain cause codes when a call releases), will get you a stutter dial tone you can't get rid of. Not much is known about this exception, but vertical service codes (*67, *82, etc.) never, ever work on it. With a little further observation, this looks to be a completely separate dialplan! The most obvious thing to indicate this is on resold lines. Resold POTS on AT&T switches are locked down in a way that prevents people from using ringback for whatever reason. When on the mysterious stutter dial tone, this restriction goes away!
- Many SBC-derived DMS-100s are programmed to reset to dial tone when 101-9017-0 is called. 9017 is a workaround CAC similar to 0110 on some switches. Any calls originated using this will only go over the local network.
- From a protocol perspective, trying an out of spec q.931 IE (say, 0x28, 0xE0 rather than 0x02, 0x48, 0x69) that would get slapped down by a 5ESS returns an incredibly strange response: nothing! As in, it completely ignores, for example, a setup message with this in it. Just ignoring messages, even bad ones, is something a switch isn't supposed to do. For that reason, most ISDN boxes trying this will freak out when

this inevitably makes one of the response timers expire (T.303 if you spend too much time reading ITU docs), and send a disconnect message to reflect that. Even more strangely, the DMS will act as if the identifier your ISDN box made for the call - the call reference value - never existed in the first place! When this is tried on a PRI with other calls on the same circuit, none of the other calls drop, so it's unlikely that this is making any sort of message processor crash. What effect this is having, if anything, needs to be looked at way more thoroughly.

DMS-500 with 480 hertz reorder: 702-310-0012

DMS-100 with weird reorder timing: 303-781-0008, 336-789-0000

MMCONF bridge/ringing number: 510-940-0102

Remote call forwarding prompt: 707-539-0099

Custom IVR: 414-227-0033 (if you press nothing, it'll give you an electromechanical low tone recording)

Unknown, but consistently on DMS-100s: 415-622-0000. (Some noises will make this circuit go offhook. For whatever reason, this only accepts one simultaneous call.)

Unknown: 386-364-1103

No audio, immediately sends dial tone resettable SS7 disconnect message back: 866-202-9985

DISA dial tone: 212-889-9998 (New York City centrex)

EDRAM announcement, disconnects with all circuits busy SS7 message: 434-975-9999

EDRAM generated milliwatt: 801-578-0012 (normally milliwatts are as interesting as dry paint, but one of the EDRAM cards on this switch mixed up its offhook and milliwatt tone samples. Give it a call a few times for ear-piercing lulz.)

Three bursts of dial tone, and unknown (47?/ resource unavailable, unspecified) SS7 disconnect reason: 202-484-0000 (this makes sketchy long distance routes act really weirdly)

DMS-10

This is one of the long-standing champions of phone lines in rural America, having withstood even Nortel's attempt to kill it in favor of small DMS-100s. Despite the similar names however, the two systems have led a lifetime of nearly no common hardware or software and, not surprisingly, sound completely different.

- A direct descendant of the SL-1 PBX; some of the cards are even interchangable.
- Can support drum and AIS-style announcements. Older installations tend to have a DMS-10 DRAM (not to be confused with the DMS-100 DRAMs/EDRAMs; they're much lower capacity - only four simultaneous channels, only support shorter announcements, and are all around less sophisticated) stashed in them somewhere. These cards have a very distinctive feedback noise to them during recording/ playback - really cool to listen to, and sometimes given they're just cards, can sit in the switch forgotten for many years, even after something like an APMax is supposed to have replaced it. That's often the case; a lot of DMS-10s have been fitted with more modern announcement devices (the 68k/pSOS-based Cognitronics MCIAS is still common in some installations, mostly by larger companies; tiny, cooperative telcos use the PowerQUICC/Linux- based Innovative Systems APMax almost exclusively), so you might have to hunt around in test ranges or dial something unusual from the dial tone itself to get these.
- One of the few switches to support looparound test lines in software. Possibly for this reason, most of those in service today will be on DMS-10s.
- Occasionally has test numbers for all of its call progress tones.
- Starting in the 500 series of releases, Nortel began porting the DMS-10 software to ChorusOS 3.2.1. Most switches (even the CS-1500s) in service today run a generic with this OS. The lion's share of DMS-10s running pre-ChorusOS releases are owned by the Citizens Communications (think: rural Minnesota) arm of Frontier, and possibly some ex-Centurytel or Embarq (as opposed to ex-US West; those are all recent releases) Centurylink exchanges.
- DMS-10 offhook tone has a strange, modulated sound to it.
- Stutter dial tone from the switch is considerably slower than other models. See the remote call forwarding number for an example.
- Like the DMS-100, uses DS-30/DS-512 internally.
- Licensing for the switch is based on thousand blocks. For example, a rural phone company serving a town of 500 people might have bought a software license that lets them assign 311-555-0xxx and 1xxx numbers, but nothing else. Because independent telcos can be slippery, unpredictable bastards, this can save you a lot of trouble. If a thousand block is locked, you'll typically get a "cannot be completed as dialed" recording (or sometimes a reorder) on literally every number in the block instead of the standard not in service one.
- On some DMS-10s, flashing on lines without three-way calling might make it throw you onto a permanent signal recording. Or a reorder. Or other weird things.

Loop line: 904-845-1104/1106. 1106 is reorder via the DMS-10 until 1104 is called. Hanging up on 1106 when on 1104 will get rid of the tone for the duration of your call, but still accept new callers on 1106.

Remote call forwarding prompt: 207-657-9999

DMS-10 DRAM: 641-394-1255

High tone: 303-652-0020

Low tone: 303-652-0080

Dial tone: 303-652-0035

Offhook tone: 303-652-0039

Double ringback: 303-652-0042

Solid ringback: 303-652-0043

Empty Houses

by Jared (沼モンスター)

Sometimes, you don't want things arriving at your house. Maybe you're trying to hide something from a family member, or you bought an illicit substance. Perhaps you scammed your way into an online item and need it shipped somewhere that doesn't lead back to you. You might even just be paranoid.

There's a simple solution: Empty houses!

Zillow.com is a website used for finding houses that are for sale within a specified area. You just type a zip code in, and you have a map of all the houses in that zip that are currently unoccupied.

So why not just go on zillow.com, choose a house nearby, and send it there? Additionally, USPS doesn't actually care what name is on the package. Carriers follow a rule: "when in doubt, deliver." They need the package to go to the destination.

It does not matter what name you decide on, just don't make it your real one. If you put "John Smith," they'd still deliver it to the address specified. Just choose a fictitious name. You can keep it simple with names like:

- John Smith
- David Johnson
- Mary Anderson
- Kevin O'Brien
- Emmanuel Goldstein

Or you could mix it up and make it interesting with names like these:

- Mary Ann Marie Smith Johnson Hernandez
- Riko Nikolai
- अरे बहुभाषी पाठक
- Meursault Pierre
- Emmanuel Goldstein

It doesn't have to be a full name either! USPS will still deliver to:

- Richard

They're not worried about whether or not the person on the package lives there. So when you want something shipped *not* to your house, you would go on zillow, put whatever fictitious name you came up with, creative or simple, and ship it to that address. When the package is delivered (you can check with the tracking number), dash over there and pick it up. You would just want to make sure you time it so nobody's there.

USPS is one of the largest distributors of drugs in the United States and they don't even know it. Well, technically they do know, but they can't prove it. FedEx and UPS are allowed to search your packages if they believe there is something suspicious in them. USPS, on the other hand, is legally not allowed to look inside of your mail. A lot of people know this, and utilize it very cunningly. Pounds of marijuana go through USPS and across the country every single day. So when that package comes to the empty house, they also have no idea what's inside.

This whole thing sounds pretty illegal, so let's go over two scenarios.

Let's say you did a bad thing, and used a stolen credit card to buy a new pair of black Air Force 1s so you can rob people better. You decide to go over to zillow, find an open house, and then send it there with the name being "John Cena" so they can't see you. You run onto the front porch, snatch it, and ride off into the sunset. That is illegal. In fact, it's so illegal you'd face credit card *and* mail fraud charges.

But what about this? Alice lives with her fundamentalist parents. Alice feels that she was meant to be male. From now on, I will refer to Alice as Alex. Alex wants to buy a book about people in his situation, but if his parents see it in the mail, they'll disown him. So Alex calls his friend Gus and asks if he can have his mail sent there. Gus says yes, and the mail is sent there. No crime is committed.

But let's switch out Gus's house for a zillow house. Alex decides to mail it to an unoccupied house, but pays for it legitimately. Is this still illegal? From my understanding, yes. However, the police are not going to bother hunting Alex down over a book he legitimately paid for that he just happened to send to an empty house. And even if they do apprehend him, any charges Alex faces will most likely be dropped due to the innocent nature of the situation, regardless of whether or not it's illegal. He'd

probably only face a mild reprimand or warning, if anything at all. One might consider this to be a gray area.

Shipping information is only really a big deal in logistics. They want to get the package there, and fast. You could get packages shipped to a house under a different name, as long as someone consents to have their mail shipped there. When you take away the idea of getting consent to send mail to a specific address, it becomes something of a crime. However, it's only a really significant problem (IMHO) if it involves any kind of fraudulent activity. At that point, it becomes mail fraud, and that's the bad one. If you just want to ship a t-shirt you like to a zillow house, and they do somehow catch you for that, you're most likely not going to face any real consequences. Please keep in mind that I am not a lawyer, and this is just my understanding of it.

In case you couldn't tell, it's pretty damn difficult to get consent to send mail to an unoccupied house. Unless the real estate agent magically decides she'll let you get your mail sent there, you won't have consent, making it illegal. But what about Alex's situation? I wouldn't really call that a crime, but the system may beg to differ.

It can be beautiful or it can be ugly. Take the information I give you and make it beautiful.

The Art of the Troll

by aestetix

A preface: The moniker "Internet troll" has acquired a bad reputation, due to mean-spirited comments on "social" media and other antics. I think it's important to show that a well crafted troll, rather than simply spitting out racial slurs and other nonsense, can be powerful, and indeed, a method of bringing positive change.

Trolling has been around for a long time. In ancient Greece, the birthplace of tragedy and comedy, the playwright Aristophanes was a brilliant troll. Consider his 423 BC play *The Clouds*, in which he mocks Socrates, the famous philosopher. A man named Strepsiades has fallen into debt and decides to enroll in the Thinkery, the school Socrates runs. After all, he reasons, if Socrates is able to use his magic logical "reasoning" to piss off the ruling class, surely he could teach Strepsiades how to trick his creditors into forgiving all his debts. The entire play serves as a massive lampoon on the emerging school of philosophy for which ancient Greece is now so famous. It also shows us an example of how trolling can be done well.

Let's break down the "art of trolling" into a few short and simple rules. First, troll concepts, not people. Second, when we create a troll, make sure the point is clear. Third, our troll needs to be credible, or at least within the realm of possibility. Finally, know the limit, and don't go past it.

One of my favorite trolls, Mark Twain, was a master of using dark comedy to further political ideas, including hitting on topics that might otherwise be taboo. While most are familiar with the famous "whitewashing the fence" scene, in which Tom Sawyer tricks his friends into doing his chores for him, one of my favorite trolls comes from his first novel, *The Gilded Age*. The book, published in 1873 at the dawn of an age in American politics where corporations like Standard Oil ruled over Congress, was so impactful that we have since borrowed the book's title to describe that era. One character from the book comes to mind: Colonel Sellers, who is described as an eternal optimist, but in reality is a hustling serial entrepreneur. In one scene, where the narrator encounters the colonel with his family, desperately poor after yet another failed get-rich-quick scheme and left with nothing to eat but turnips, the colonel preaches about how lucky they are to have these fantastic turnips and how great turnips are for the health. I'm sure readers can see a faint resemblance to a certain recent American politician.

Twain was able to examine obvious failures in the political system of the time, nail down

the precise problem (in this case, corrupt politicians), and create a perfect caricature of the "ideal" corrupt politician, while placing him in increasingly ridiculous situations that the audience would find hilariously absurd. Twain makes no direct personal attacks and uses pointed humor so well that even the target(s) of his jokes would be hard pressed not to laugh.

Sometimes a troll is crafted to clearly show why a rule or policy is bad. In 2016, filmmaker Charlie Lyne was upset that the British Board of Film Classification (BBFC) was serving as an effective censor against films they considered "controversial" or "indecorous." This mattered because a film could not be released in British cinema without a BBFC certificate, which costs around £1000. To protest against this, Lyne created a Kickstarter to produce a "film" that was literally watching paint dry. Every new pledge to the Kickstarter added time to the final movie. By the end of the Kickstarter, the film grew to ten hours and seven minutes, and the BBFC censors were forced to watch the entire thing. Because Lyne considered the BBFC a bad organization with a bad policy, he pushed their policies to the extreme to demonstrate his point, at the same time making a mockery of the process. For those curious, the film obtained a "U" rating, for "unlikely to offend or harm."

While a good troll will clearly be humorous and designed to mock, their points should also be within the realm of possibility. At its top form, the troll should begin with a reasonable premise, and then turn a corner that makes the reader start to ask questions. One of my favorite examples of this in recent years is Lulzsec. Formed in 2011, one of their first targets was PBS. They hacked into the website, and added a fake news story that Tupac Shakur and Biggie Smalls were still alive and living in New Zealand. While this is clearly absurd, it's also hilarious, and just sufficiently within reason that many people had to check other news sources to verify. If the story were posted on a less credible outlet, it would not have been nearly as effective.

Finally, everything has a line, and we should never cross it. A master troll will create a scenario that makes people uncomfortable (but doesn't hurt anyone), and forces hard questions into the public discussion. Two very different examples come to mind. The first is a classic story within the art world: Marcel Duchamp, a French artist, was upset at the snobbery and elitism within the art community in New York City. So in 1917 he created a unique exhibit: he took a Bedfordshire urinal, turned it on its side, and wrote the phrase "R. Mutt" on it. He then entered it as an art piece called "Fountain" in an exhibition. As expected, it created a schism in the community, half the people saying it was a joke and should be thrown out of the show, and half the community pointing out that there was no clear standard that separated this toilet from other "art" pieces. The impact was so powerful that it prompted an entire movement, Dadaism, in the art world, and it continues to inspire today.

A more contemporary troll, one of the masters of stand-up comedy, is Dave Chappelle. He is an expert at taking complex, heated topics in American culture (such as race relations), and presenting them with a framing that forces us to ask difficult, often uncomfortable questions, while couching it in brilliant humor that helps to soften the blow. Like Duchamp, his work splits communities, because he comes so close to the line of what is socially acceptable that the line becomes blurry. With both Chappelle and Duchamp, their success lies in the fact that when someone claims they have gone too far, they can't point to a specific reason why. The reality is that they came up to the line, and it *feels* like they went too far, but they simply expanded the scope of what is open for discussion.

To summarize, trolling can be quite powerful and effective if there is a method to the madness. While the ease of access to the Internet allows amateurish banter to flourish in forums like YouTube commenters, a deeper art, when properly understood and exercised, can be harnessed to a more sophisticated effect. With well calibrated goals, means to these goals, and clarity of purpose, trolling can be the best, and sometimes only, way to further the conversation.

The Hacker Perspective

by MRLN

My perspective as a hacker has changed quite a lot over the years. Computers, for all intents and purposes, haven't even been around for 100 years, making them one of the newest, most powerful, and most complex inventions out there. Computers have changed everything. Don't take my word for it, ask your grandparents. Computers wildly changed *everything* in a relatively short period of time. Computers are everywhere now - from the gas pump to your car and even in the hands of seemingly every person on the planet in the form of a cell phone. Here is a story of my journey through technology and how my perspective on what a hacker truly is has changed over the years.

I remember the first time I saw a computer. It was in a computer lab at my elementary school. It changed my life. It could play games, print out homework papers, play games, browse "The Net," play games, and had a neat little mouse with a metal ball you could take out and throw at classmates. And did I mention you could play games on it??! *Kid Pix* and *The Oregon Trail* were the highlights of my school day. I was also exposed to HTML in elementary school even though, unfortunately, I wasn't interested in it at the time and found it boring and hard. The concept of hacker back then, at least in my corner of the world, was little known and usually reserved as a synonym for criminal. Society perpetuated this concept that a hacker was a criminal that used computers.

Around middle school, I wised up and learned what you could really do with computers. Personal websites were huge at that time and I was learning how to code HTML from Angelfire tutorials and books the size of three bibles. I found it fascinating that you could design your own part of the web, mark your space, and put anything on it you wanted. Share it with friends, view their sites, and sign a guestbook or two. I still considered a hacker to be the same thing as the caricature of a hacker the media perpetuated at that time. Think *The Matrix* and *The X-Files'* "The Lone Gunmen." It was the lone 13-year-old in his parents' basement that was realigning government spy satellites for fun, penetrating government agencies to impress peers in their favorite IRC channel, and consuming endless amounts of soda and Hot Pockets. OK, at least the last part was correct, but at that time it was Bawls soda and pizza... no offense to the Hot Pocket enthusiasts out there. Even though my narrow view of what a hacker was changed little, unbeknownst to me, I was progressing - I was learning how it all worked. The wires that connected to the modem. What a modem did. How to "program" a web page. How routers and switches connected multiple devices. What an intranet was. After all, isn't a hacker someone who is learning a system in order to make it work in a certain way that it may not have been designed for or even thought to be capable of? Gotta start somewhere....

Through high school, we caused all types of Ferris Bueller chaos. Getting out of school, viewing student records, and so on. Let's just say after I found out they didn't confirm doctor notes with the doctor or staff, it was all smoking doobies with chicks in hot tubs from there. I had more "doctor appointments" during school hours than a cancer patient. IT wasn't all good, though. Rest assured the school faculty and administrators knew me and my nerd friends by name (we wore nerd as a badge of honor since our school didn't have many cliques and we all hung out for the most part). The principal even had a post-it note of my personal website address on their desk (it was popular amongst my surprisingly wide group of friends that had various mp3s, ROMs and AIM hacks to download back when that was cool and a lot of them used the site to get games on school computers and I assume it was hitting the firewall pretty hard and got someone's attention), which was right next to the post-it note of their Bess Web Filter! No more proxies for the cool kids, ahem, sorry, nerds, I mean. We kept that nugget to ourselves.

And it was good times up until a friend started "net send"-ing messages to the entire school and one of his friends made a batch file "virus." They gave up the goods when

questioned, and the post-it note with the password vanished. All good things come to an end. Hackers around this time were "cool" and people were realizing they might not be so malicious, but highly technical users that could make computers do unimaginable things. To me this was like magic... actual magicians, casting cryptic code-spells into the ether, and producing seemingly impossible things out of nothingness. To me, hackers were the masters of this black box that no one seemed to understand. Admittedly, this was the more immature version of what I thought a hacker was. While we did in fact find holes in systems and ways around security controls, we rarely added much value and, in our immaturity, caused more problems than we solved. Our entire view was using our knowledge to do whatever we wanted: if you said something we didn't like in chat, then we crashed your computer; if we wanted to play games online, then we'd bypass the school filter; if we wanted to mess with a friend; then we'd hit a few keys and turn their desktop upside down on their monitor. Proof our moral compass hadn't quite developed yet.

In college, my view of what a hacker was matured. My past insecurities of not being smart enough to be one was quelled when I finally realized that a hacker is a technology lover who enjoys learning about it and makes new things possible, stretches the limits of technology, benefits humanity by using technology (hacktivism was big back then), or finds creative ways to fix issues. The ego-driven ways of the past were dead to me. I no longer cared about getting the approval of random people on the Internet. Joining a group to glad-hand ourselves on how l33t we were is hilariously lame. I now was concerned with learning about technology for the love of it! I wanted to know how it worked and, sure, sometimes that may require getting around something in order to make it do what you need it to do, but that doesn't have to be nefarious. As technology started to mature, so did I. I realized that you could still learn the blackhat stuff. In fact, companies will pay big for that type of knowledge in order to protect their systems. As long as you are using what you learn legally, you can do anything you want to your own devices - much like Neo in *The Matrix*... it's *your* playground. Do what you want with it.

After college, I would say my perspective changed the most. Not because college guided me or even provided acceptable levels of education, but because it re-ignited my love of learning. I realized that learning on your own is one of the best ways to learn... there are few good teachers out there and they will only teach you what they are required to - and may not even have the same level of enthusiasm as you. I had the time and knowledge base to start learning the fun stuff. I also came out of my shell a bit and started to try to meet and learn from real hackers out there.

There's no crime in learning. Some of these people were college students while others were what I assume were shady career criminals. The latter taught me a few important lessons: fuck the fancy stuff and just do what works; you can accomplish a goal without fully understanding it; sometimes that comes later and doesn't cheapen it since technology is a huge field and you won't always know everything all the time. After all, not everything has documentation, and since hackers are on the bleeding edge of what's possible, they usually write the rules, so to speak. Hackers are the ones that will tell you where the limits are and then break right on past them. Hackers are those who love learning. Hackers are "do-ers" and value practical experience. Hackers are the types of people that click around in dark rooms of video games and find the hidden Easter Egg. Some do it for the lulz and others do it for the pleasure of solving an incredibly complex puzzle. Some use it for good and others use it for bad. Some want to impress people and others want to satisfy their insatiable quest for knowledge. What all hackers have in common is their love of exploration and using creativity to solve problems.

As I have grown in the community, I have truly realized how little I know about technology. Ironically, this excited me. There is so much to learn. You can learn a little about a lot or specialize in some niche field. You will always have something new to learn with computers and technology.

Enter - The Job. *Dun-Dun-Dunnnnn*. They always said "Do what you love and you'll never work a day in your life" and I have to agree with them. Growing up, I had little direction aside from "go to school and get good grades" and "don't get in trouble." (Can you guess what a kid is going to do, given that advice? I think we all know how well that advice was taken - in one ear and right out the other.) Anyway, as I started to enter the work force, I leaned into technology. It's what I was comfortable with. It's where all my friends were. It's what I did all the time anyway. Even if I couldn't think

of a way to monetize what I was learning or doing at the time in tech, I filed it away as "one of those things that may help make some type of connection later" or at least "one of those things that can give you a bigger perspective." I mean, after all, jack of all trades are quite valuable people to have around.

I started out my tech career fixing computers at various computer repair shops. Then computers became so cheap, Anti-virus software was gaining in popularity and everyone had a tech guy in the family, which meant these shops rarely lasted long. Nowadays, finding a computer repair shop is as hard as finding a TV and vacuum repair shop. Oh, and they aren't hiring. I started coding web pages to supplement my income and found that the Indian market was just crushing the American market. I mean, why even bother competing with someone who will code a page exactly like you want, add forms and databases for cents on the dollar? They even work with graphics artists in-house... how can you compete with that? I was at a loss and had to start looking elsewhere in technology to afford to live.

I started learning networking, which sounded fun, and obtained my CCNA, CCSA, and was working towards my CCDA certification. Almost immediately after my CCNA cert, I had a job in tech. I made my way into networking and worked there for several years. I found out I don't like it. It's repetitive and boring to me. ISP went down, link is flapping, QoS needs tweeking, bank employee unplugged the 5506 at a remote location for Earth Day to save electricity. *sigh*

Lucky for me, networking is a preferred jump-in point for security, which is what I was focusing on getting into. I started learning about that, studying for the Security+ cert, and ended up in a very low-level security position with the company I was at and got my foot in the door. After a few years, I got into another security position, got a security clearance, and have been hacking away ever since.

Slowly but surely, little by little, progressing towards my goal of making what I love my career... and I love it! Security is a dynamic field. It provides you an opportunity to learn a wide variety of topics and technologies. After all, security is a small part of everything and simultaneously an illusion that doesn't exist in this world.

Nothing is 100 percent secure. That's just how it is. Computers weren't invented for security. They were invented to be connected and share information with each other. That makes it challenging and keeps someone like me engaged and not getting easily bored. There's also many aspects of security. You can be the corporate firewall guy, the at-home bug hunter, the freelance coder/auditor, the red teamer/penetration tester, or learn a wide variety of skills working in a Security Operations Center.

Working with hackers has widened my eyes to the variety and personality types, backgrounds, and interests of hackers. We all share certain characteristics; creativity, curiosity, technical prowess, strange interests, and the like. However, we are quite a diverse group: men and women of all nationalities and backgrounds. Some are laser-focused on technology and have no other interests, while others enjoy gardening when not behind the keyboard.

I expect the future to change what a hacker is. Pretty soon, we will all be hackers because technology will be so ubiquitous and secondhand nature that the term hacker will encompass any tech lover and hacking will be an activity we all engage in... whether it's to be productive or just to get that ancient MP3 file format to play on your brand new Generation 2099 floating iPod/teleporter.

MRLN is now living the dream as a security analyst in Colorado while developing his security skills and growing his Linux beard. He won't be found on Facebook, but is an active member of numerous online forums/ communities related to his eccentric hobbies.

HACKER PERSPECTIVE
submissions have closed again.

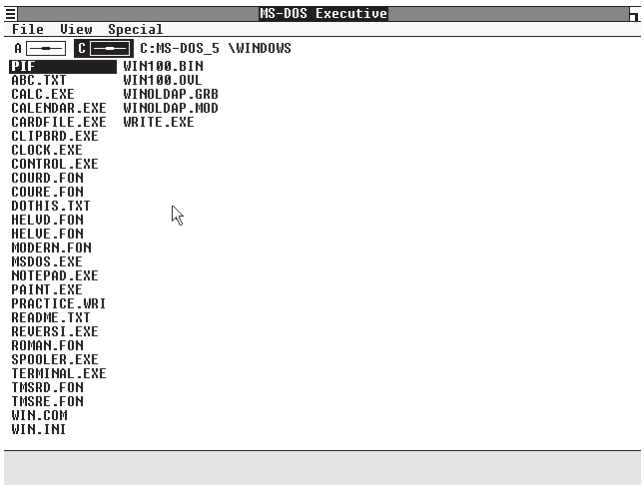
We will be opening them again in the future so write your submission now and have it ready to send!

Exploring Old MS Paint Formats

by MrAureliusR

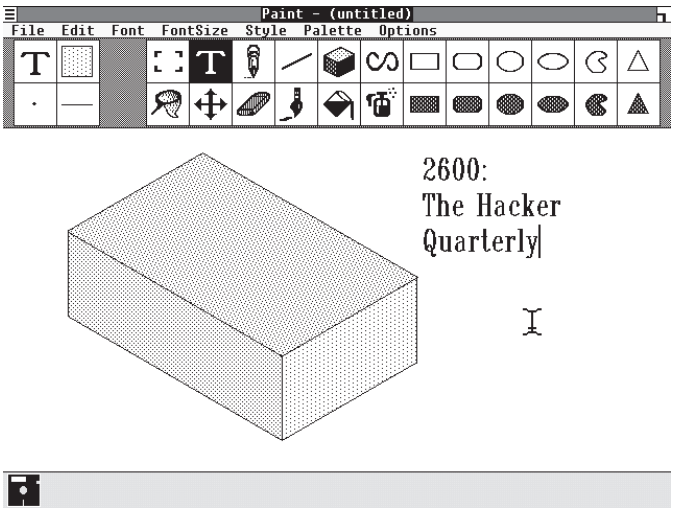
I've recently been hanging out with the crew from WinWorldPC - you know, that website that hosts a huge archive of old software and operating system images. It's a great place to find obsolete software, especially for Windows 9x, DOS, OS/2, and even old Macintosh stuff. On the Discord and IRC channels they use to hang out, I met some interesting characters. We started spending a few hours each day streaming ourselves installing and playing around with all the software on the website. I decided to play around with Windows 1.04 and see what the very first Windows was really like.

I installed DOS 3.3 and then Windows 1.04 on a VirtualBox VM. I was immediately struck by how similar Windows 1 is to the "MS-DOS Shell" that came with DOS 5. However, it includes quite a few applications, including the original Calendar, Clock, Notepad, Write, and our focus: Paint.



The Windows 1.04 interface after install

This version of Paint was actually just a licensed version of ZSoft's PC Paintbrush. It has some unique features that were not incorporated into the version of Paint created by Microsoft for Windows 3, such as the 3D Cube tool (pictured). The interface is very simple, but for the time it was actually quite a decent tool, especially when included as part of the OS. Making simple diagrams which could be printed or even inserted into text documents was quite easy to do.



Microsoft Paint version 1.04 with a beautiful piece of art

This first version of Paint uses a very simple black-and-white format. Pixels are either on or off. There's no grayscale, and there's definitely no color support! I started off just messing around with the tools, but then I started trying to make interesting images that could be used as avatars for modern chat programs. I discovered that the fill tool could create some basic fill patterns which gave the images a lot more texture and depth. The 3D object tool made creating cubes or rectangular prisms very easy, which I used to great effect. The selection of fonts is quite limited (that's a whole other story - this is before TrueType fonts and so Windows used a proprietary .FON format which is quite complex), but despite the limitations it's fun to create retro-looking one-bit art!

I then ran into a problem. I wanted to be able to export these files so I could potentially edit them with GIMP or another modern tool to add a few finishing touches. I could have taken a screenshot of the VM, but that was sure to lose some detail. This version of Paint does not use bitmaps; it uses an earlier proprietary format which is the subject of this article, simply called MSP for Microsoft Paint. Unfortunately, GIMP cannot read MSP files directly. I took a quick look online to see if there were any conversion tools available, but most of them were designed for Windows and were quite obsolete. I run Manjaro and really wanted a simple solution that would make it easy to convert to a modern format.

Whenever I've had to work with simple image data in the past, I've tended to use the X BitMap (XBM) format. This is a very primitive file format that was designed to hold icons and small images for the original X Window System. The format is actually just a C array with some variables to describe the width and height, and so it's very easy to generate programmatically and edit by hand. It also happens to be a bit-per-pixel format, just like MSP. And best of all, GIMP can directly import XBM files and then export them as PNG or any other modern format. So my plan of attack was to go from MSP to XBM to PNG.

```
1: nano FLOPPY_converted.xbm
  GNU nano 5.6.1                                  FLOPPY_converted.xbm

#define FLOPPY_width 560
#define FLOPPY_height 774
static unsigned char FLOPPY_bits [] = {
0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xf, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0xff, 0xff, 0xff, 0xff, 0xff,
0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0x7, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0,
0x0, 0xfe, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff, 0xff,
```

XBM-format image data is just a C array

First I had to figure out the MSP file format. Thankfully, the ArchiveTeam website has a wiki dedicated to documenting file formats, and their entry for MSP had a link to a page with the full format in good detail: `www.fileformat.info/format/mspaint/egff.htm`. This is when I discovered that there are actually two versions of MSP: Version 1 was used with Windows 1, and Version 2 was used with Windows 2. The difference is that MSP Version 2 uses some simple run-length encoding to compress files, whereas Version 1 is just the raw data preceded by a header.

With the format specification in hand, I spent a couple of minutes deciding which language to use to write the converter. I have a lot of experience with C/C++, but when it comes to anything involving text and file manipulation I tend to use Python. The algorithm is so simple that it would be trivial to re-implement in pretty much any language. I've written it as a Python 3 script.

The script checks which version the MSP file is - thankfully, they included a magic four-byte value in the file header to make this easy - and then gets the height and width from the next few bytes. If it's Version 1, it simply copies the data directly into an XBM-format file. My first attempts resulted in some output that looked vaguely like the original file, but something was clearly wrong. It took me a while to realize the MSP format stores each byte with the most significant bit first, but XBM is the other way around! So while the bytes were all in the correct order, each byte was reversed. A quick hack to flip each byte around fixed this!

I decided that I may as well add support for Version 2. The run-length encoding is very simple: read the first byte. If it's 0, the next byte is the length of the run, and the following byte is the byte to be repeated. So you just copy that byte x times. If the first byte is non-zero, it's telling you the next x bytes are to be copied over exactly. Here's a simple example:

```
00 09 FE 04 AA 52 80 14
```

The first byte is zero, so the next byte is the run length. In this case it's nine. The next byte (FE) is the byte to copy. So the start of this data is:

```
FE FE FE FE FE FE FE FE FE
```

It's taken nine bytes and compressed them into three! The next byte is 04, which is telling us the next four bytes are to be copied directly. So the above bytes would be added, and we end up with:

```
FE FE FE FE FE FE FE FE FE AA 52
80 14
```

Pretty simple, right? The Version 2 file also includes a "map" which tells you where each row of image data starts, in case you want to just read part of the file. However, since we're converting the entire file at once, we just start at the top of the image data and continue until we're done. If you get to the end of a Version 2 file and there seem to be bytes missing, it means the remaining bytes are all FF. For example, a 16x16 pixel image should have 256 bytes. If you read all the image data and find you've only read 200 bytes, that means you need to add 56 bytes of FF at the end.

Oh, and one last wrench thrown in the mix: all the bits are inverted in XBM as compared to MSP! So in GIMP, if you want the original image back, you need to do an invert on the image. However, I actually like how they look inverted in some cases, which is why I didn't end up adding the inversion into the script itself.

An avatar made for user Toxidation in MS Paint v2

The script is below and in a GitLab repo located

at gitlab.com/mraureliusr/mspconvert and it has instructions on how to use it. Note that this script uses a new operator (:=) introduced in Python 3.8 and so you need at least that version to run it. If you want to add any improvements or modify the source, go ahead! It's licensed under the Mozilla Public License v2.0. Issues and pull requests are appreciated.

Have fun drawing some retro images in Windows 1 and be sure to Tweet or Toot them at me on Twitter or Mastodon (@MrAureliusR on Twitter, and @amrowsell@mastodon.sdf.org on Mastodon!)

```
#!/usr/bin/env python3

# This Source Code Form is subject to the terms of the
# Mozilla Public License, v. 2.0. If a copy of the MPL
# was not distributed with this file, You can obtain
# one at https://mozilla.org/MPL/2.0/.

import sys

print("MS Paint file converter utility v0.1")
print("Written by A.M. Rowsell, MPL Version 2.0 license\n")
if len(sys.argv) < 2:
    print("Please provide filename (without extension)!")
    print("Example usage:\n./mspconvert.py DONUT")
    sys.exit(255)

filename = sys.argv[1]
width = 0
height = 0
# The output file follows the very simple XBM format
# which is just a basic C syntax array variable
outputString = '''
#define {0}_width {1}
#define {0}_height {2}
static unsigned char {0}_bits [] =
'''

# Output data starts as an empty bytearray
outputData = b''

try:
    with open(filename + ".MSP", 'rb') as f:
        versionString = f.read(4)
        if versionString == b'\x4c\x69\x6e\x53':
            version = 2
        elif versionString == b'\x44\x61\x6e\x4d':
            version = 1
        else:
            print("The given file {0}.MSP is not a valid Microsoft
Paint file!".format(filename))
            sys.exit(255)

        if version == 2:
            print("Version 2 Paint file detected...")
            width = int.from_bytes(f.read(2), "little")
            height = int.from_bytes(f.read(2), "little")
            size = int((width * height) / 8)
            f.seek((height * 2) + 32) # seek to the start of image
data
            while(byte := f.read(1)):
                if(int.from_bytes(byte, "little") == 0): # RLL-encoded
                    rllLen = int.from_bytes(f.read(1), "little")
                    rllValue = f.read(1)
```

```
                    for i in range(0,rllLen):
                        outputData += rllValue
                        size -= 1
                else:
                    rllLen = int.from_bytes(byte, "little")
                    for i in range(0,rllLen):
                        outputData += f.read(1)
                        size -= 1
                        print("Remaining size: {0}".format(size))
            for i in range(0, size):
                outputData += b'\xff'

            with open(filename + "_converted.xbm", 'w') as f:
                print("Writing output file...")
                f.write(outputString.format(filename, width, height))
                f.write(" {")
                q = 0
                for byte in outputData:
                    result = int('{:08b}'.format(byte)[::-1], 2)
                    f.write("0x" + '{:x}'.format(result) + ", ")
                    q += 1
                    if q >= 16:
                        f.write("\n")
                        q = 0
                        f.write(" };")
                        print("Done!")
                        sys.exit(0)
        elif version == 1:
            print("Version 1 Paint detected...")
            width = int.from_bytes(f.read(2), "little")
            height = int.from_bytes(f.read(2), "little")
            f.seek(28)
            q = 0
            outputString = outputString.format(filename, width, height)
            outputString += " {\n"
            while(byte := f.read(1)):
                result = int('{:08b}'.format(int.from_bytes(byte,
➥"big"))[::-1], 2)
                outputString += "0x" + '{:x}'.format(result) + ", "
                q += 1
                if q >= 16:
                    outputString += "\n"
                    q = 0
                    outputString += " };"

            with open(filename + "_converted.xbm", 'w') as f:
                print("Writing output file...")
                f.write(outputString)
                print("Done!")
                sys.exit(0)
except FileNotFoundError:
    print("{0}.MSP does not exist! Quitting...".format(filename))
    sys.exit(255)
except PermissionError:
    print("Unable to open {0}.MSP -- insufficient permissions!
Quitting...".format(filename))
    sys.exit(255)
except Exception:
    print("Something went wrong! Quitting...")
    sys.exit(255)
```

Keyspace Iterator in AWK

by Justin Parrott

I wrote a little keyspace iterator in AWK. The first two uses for something like this that I've thought of are brute force password cracking and groping a web server for hidden files (by combining this script with something that can fetch from a URL). AWK probably isn't going to be the fastest language, but performance may not be such a concern as the real bottleneck is in the application of the string to the situation at hand (the encryption or URL fetch, for example). The first one I wrote was in C, but I'm submitting the AWK version because I think it's a little more interesting (even though it's basically the same implementation of a recursive function).

```
#!/usr/bin/awk -f

# A keyspace iterator for brute force, etc. This can be used, for example,
# in conjunction with a tool like curl to fetch https://site.com/*.html
# - Justin Parrott
#
# usage: ./ks [minlen [maxlen [string]]]
#
# Tested with nawk and gawk

function f(keyspace, kslen, prefix, count, i) {
        if (count > 1) {
                for (i = 1; i <= kslen; i++) {
                        newpfx = sprintf("%s%c", prefix, keyspace[i])
                        f(keyspace, kslen, newpfx, count - 1)
                }
        } else {
                for (i = 1; i <= kslen; i++)
                        printf "%s%c\n", prefix, keyspace[i]
        }
}

BEGIN {
        minlen = 3
        maxlen = 8
        keyspacestr = "abcdefghijklmnopqrstuvwxyz"

        if (ARGC >= 2)
                minlen = ARGV[1]
        if (ARGC >= 3)
                maxlen = ARGV[2]
        if (ARGC >= 4)
                keyspacestr = ARGV[3]

        if (minlen > maxlen) {
                print "Minimum length is greater than maximum length"
                exit
        }

        n = split(keyspacestr, ksary, "")

        for (len = minlen; len <= maxlen; len++)
                f(ksary, n, "", len)

        exit;
}
```

Affirmations

Support

Dear *2600*:

I have been buying this magazine in stores for over 20 years now, semi-consistently. I am going to start a subscription in response to the letter in 38:1 where 6NdLXzc2 whined about the "political bias" of the magazine. Since there are so many people so eager to complain about the alleged political messaging with their own extreme political beliefs, allow me to explain why I am going to negate this loss with starting my own subscription. I hope this consistent subscription will help support people who truly believe in science, truth, morality, and rationality. The apologists for bigots, pseudo-authoritarians, and conspiracy theorists will not be "on the winning side of history."

It's much easier for the angry minority to be heard over the positive and hopeful majority, as they have no reason to raise their voice. The editors are right, as I have experienced in my personal life many times, that these radical idealogues cannot be convinced of anything that goes against their zealous belief. Whether it's trying to convince them that the vaccine does not have alien DNA, microchips, or demon reproductive material; or trying to explain to them that rational and science-based public health messaging will change as new information is presented; or insisting that an attack on the nation's Capitol was not simply equivalent to a tour group, nothing seems to be enough. As they say, you cannot reason someone out of positions that they were not reasoned into.

There seems little reason in responding to all the points in the feedback, as the editors have clearly got that covered. All I can do is hope that this subscription can reflect my support for what *2600* was and still is: a magazine keeping alive the hacker spirit. The hacker spirit is not sophism and conspiracies. The hacker spirit is not hatred and apologism. The hacker spirit is not false equivalencies and bad faith. Instead, it is progress. As is humanity. Pushing the envelope and improving. So, consider this my vote for *2600*.

Shocked998

Wow. Thank you so much for those eloquent words of support. You touch upon a very interesting point. We hear the anger over the positivity even when it doesn't represent the majority - or even reality. Similarly, we tend to get more letters attacking us than supporting us, ostensibly for the same reason: we all feel there's no need to raise our voices to defend what's obvious and rational to us. This can be the right move, but it can also help foster the perception that more people stand for a particular view when in actuality it's a tiny but vocal minority. People need to think for themselves and not reach conclusions before hearing the facts. And it's vital to be able to recognize facts from knowledgeable origins versus misinformation from sources that don't hold up to scrutiny.

Anyway, your support matters. Thanks again for thinking this through as an individual.

Dear *2600*:

I have a subject to laugh about. How do you read any part of this magazine and ever infer the writers and community would ever be about locking kids in cages, hate crimes, and all that other goofball Q-denial of reality Facebook spam?

Speaking on another subject that comes to mind. Any interest in a write-up on Church of Satan submissions for membership? Full Disclaimer: I am a registered card carrying member of The Satanic Temple, particularly due to them seeming more openly anti-bigot and LGBTQ+ supportive and inclusive.

Also, I wanted to share that I learned something new on domain registrations: If you register a .us domain, it will not qualify for whois protection and crappy companies will cold call you in real life, trying to phish you into services. This was my experience on namecheap. I replied I have no business, but a likely C2 (command and control) for a botnet or some other project. Those calls stopped after a few days, yay! Turns our telling people how they got your info takes the wind out of the scam sails.

Thank you all for shining on.

pic0o

We do try to keep religion out of our pages, Satanic or not. That said, we're open to all sorts of perspectives and interpretations. It says a lot when the Church of Satan is more concerned with human rights than many of the more established religions.

Regarding .us privacy policies, your conclusions are indeed correct. This is what they say: "No registrar, nor any of its resellers, affiliates, partners and/or contractors shall be permitted to offer anonymous or proxy domain name registration services which prevent the Registry from having and displaying the true and accurate data elements contained in Section 3.3 for any Registered Name."

Dear *2600*:

Reading feedback letters in issue 38:1 and it's upsetting to see how many readers feel like you're the enemy for writing "Errors in Freedom." I respect *2600* enough to hold different opinions on the route and see that we still agree on the destination. It seems like some people disagree without ever hearing you.

Anyway, I just wanted to say thank you for being *2600*.

proximacentauri

Always good to hear. Thanks for the thoughts.

Dear *2600*:

I got my blue box t-shirt, and I've got to say that it's so good looking and top quality as print and cotton. It gets dry after cleaning very fast.

Please, please, revive the Michelangelo source code t-shirt!

Best regards from Greece.

Emmanuel

Surely there's other source code besides

Michelangelo that would be good on a t-shirt. We're always open to new ideas and designs.

Dear *2600*:

Hello, I just wanted to write and say that I appreciate your publication.

Thank you!

Kryptographik

That one bit of effort on your part brightened the office mood for nearly a full day. We do appreciate our readers.

Dear *2600*:

Thanks for the lower price of the digital version. I prefer to send more money your way. Hopefully you see a greater return on the PDF versions. As much as I like a physical copy, I assume you folks see more profit with the PDF. Thanks for the great work - keep it up.

Antone

The digital version works if people buy it. If they just copy it from someone else, not so much. And while the paper version is something we're quite passionate about - as are many of our readers - there are an incredible amount of challenges involved in putting it out. Having stores close for the better part of a year in 2020 due to the pandemic could easily have wiped us out. Now there's a critical pandemic-related paper shortage, which is skyrocketing the cost of printing and adding more delays. We just can't seem to catch a break. But even with all that, we don't regret a thing. Thanks for the support.

More Meetings

Dear *2600*:

I've tried reaching out on Twitter a couple times and not gotten a response. I am interested in hosting a meeting in my area and wanted to open a line of communication to discuss what I need to do or if it's possible. I meet the required qualifications.

Josh

You should have received a response by now but it's always possible something went wrong somewhere along the line. We're in the process of restoring meetings worldwide in places where the risk of infection has been reduced due to the prevalence of vaccinated people. This is all subject to change as viruses aren't the most predictable things in the world. Further and updated info can always be found in the meetings section of the 2600.com website.

Dear *2600*:

I can't find the meeting times for the locations listed. Is it that people are always there?

Carmel

No, people aren't always at our meeting sites, although that would solve a lot of problems.

There may have been a brief period where the day and time of our meetings wasn't listed. We hope that didn't cause too much confusion. Fortunately, most readers have the default times burned into their DNA: first Friday of the month, 5 pm local time. If the starting time is different, it should be noted next to the entry.

Where We're Going Wrong

Dear *2600*:

Ahoy. Sadly, I too am writing to commiserate with others about the degradation in the quality of *2600*, not from an article side, but from the editorial side. I have been reading *2600* for over 30 years and listening to *Off The Hook*. I even met some of you and helped carry some servers long, long ago. I have been published over 13 times under various aliases, so I have something invested in my sincere critique of a magazine I have come to think of as my own.

First, the "Letters" section. In the old days, the letters section was chock full of criticism of articles by readers, some of it very sharp. This was a good thing, as it kept up quality and helped writers improve. For the past several years, this has practically vanished. The trademark snarky-hacker *2600* replies to letters used to be justified and based on intelligence, but for the past several years they seem stale, forced, and often unjustified. Like you are only pretending to be smart and snarky, but really you are not. Also, as a writer, I can tell you that every early article I wrote with an email address attached received lots of replies from readers. This also has dried up. Is it just a culture change?

Second, concerning *Off The Hook* (because this has a direct bearing on your editorials): In the old days, Emmanuel had a peer named Jim who represented conservative political views on the show and, though Emmanuel disagreed with him always, he at least had his say as he was of an age with Emmanuel, a peer, and so at least afforded respect. Nowadays, *Off The Hook* is filled with sycophants who dare not disagree with political views, no matter how misguided, or he will scream at them. Literally. The only personality brave enough to even attempt to disagree and reason with him at times is Alex (whom I applaud), but even his attempts are half-hearted and shouted down. This breakdown of egalitarian reasoning has weakened the purpose behind *2600*: to remain objective and scientific.

Third and finally, your recent politically partisan editorials. I know you have already heard from plenty of people about this as you damn well should. I am neither right nor left, but the appearance of progressive politics in my magazine stinks! You say *2600* has always spoken out against wrong political things and that's true. But now you are speaking out against entire political *groups of people* and that is ignorant and false. Even your "scientific" assertions are not really all based on science, as this has already been pointed out by many readers and I read your blind-sheep replies proving that you didn't even hear a word that they said. You have been 0wn3d by political brain-washers and it is very sad.

Emmanuel, whom I love for everything he did for us, has turned into the inevitable dictator. His power has gone to his head and apparently there is no one around with the power to reason with him. If *Off The Hook* and *2600* is any indication, he has surrounded himself with a young echo-chamber. God help us all. Maybe the true hacker ethic is dead. There is no going back in time. You cannot fake genuine snark and you cannot fake partisan politics as disinterested scientific opinion. The idea that apologizing makes you weak and so you should always stand your ground only works if you are always right. As soon as you start being wrong

and still refuse to apologize or rethink your position is the moment you have stopped being an authority and started becoming propaganda.

How sad, how very, very sad.

Yours Very Truly,
J.X.

Your issues seem to be more with personalities than what people are or aren't espousing. We see a lot of accusations here, but no specific points on which to disagree. Please show us evidence of this dictatorship you believe exists within our organization or even an example of someone who disagrees being shouted down. (It shouldn't be very difficult, as all of our on-air programs are recorded and made available online unedited.)

We don't know how to respond to accusations of fake snark. Clearly, saying something snarky isn't going to work here, which is a loss for all of us. We can agree that there are less specific criticisms of articles being sent in to the letters section, but that appears to be, as you say, a "culture change" where less people write letters in general. But our readership has done better than most. We know of no other publication with the level of engagement we continue to see here. But we always want more.

Getting back to disagreements, we encourage them, as we always have. But that doesn't mean accepting premises that are demonstrably false. Surely you have noticed that in today's society, it's become a strategy in putting forth an argument: simply make up facts that support one's position. The media hasn't helped by giving equal time to people who are spreading outright lies.

Consider for a moment that with all of the unpleasantness, disagreements, and accusations being hurled around that it isn't us at the magazine who have changed, but rather the world around us. It would be wrong not to react. We wish it were all our fault, but there's a lot more going on out there that you seem to not want to acknowledge.

We don't believe we are being politically partisan. We stand up for certain values and ideals, as we always have. We embrace science and technological advances while fighting for the rights of individuals. We oppose bullying, oppression, and lies on all levels. None of that has changed, but many of these things have turned into political issues, which is unfortunate and self-defeating for those fighting against reality. We don't intend to shy away from the issues that have always mattered to us simply because it makes certain people uncomfortable. Remember that we have always existed to make the right people uncomfortable. It just seems that lately there are many more of them than there used to be.

Dear *2600*:

I am writing to you to address a specific word, which I believe I have firm scientific evidence from experts that you have been using incorrectly. Other letter writers have referred to your use of this word as spreading propaganda or disinformation, but none have yet supplied the science or expert opinions as regards to why they believe that. I hope that this letter will correct your error and that you will see that the sources I cite are unimpeachable, unbiased, nonpartisan, and that this will lead you to a realization on your part not only about the misuse of this word and the damage it causes, but perhaps about your current attitude in general (though I have little hope of that). Admitting when you are wrong is not "weak," it is "strong," and I hope you will role-model this fact for others.

I have been an avid reader of *Foreign Affairs*, the premier magazine of The Council on Foreign Relations, for many years, as mentioned in my *2600* article "Twitter the Enemy." This magazine is unarguably the foremost in political science expertise in the United States. It features only the highest qualified writers, many of whom have served in presidential administrations of both parties. It strives to be neutral as far as partisanship goes.

What I have noticed this past year is that *Foreign Affairs* never, ever, refers to the January 6th event as an "insurrection." It is always called a "riot" or a "mob." Since I have been noticing this, I have had cause to wonder "why?" CFR has not responded to my inquiries, but I have a theory. The dictionary typically defines "insurrection" as: "a usually violent attempt to take control of a government." This word is commonly used in regards to countries run by dictators, where all that is required to take control of the government is to install a new dictator.

The government of the United States of America has three branches: the executive (the president), the legislative (Congress), and the judicial (the courts). Destroy any one of these in a "violent attempt to take control of the government" and there is no successful "insurrection," nor even an "attempted insurrection," because the other two remain and thus there is still a government. This redundancy was carefully designed like this on purpose. Had the rioters of January 6th killed every member of Congress, it still would not be an "insurrection," because our government would still exist and there are procedures and plans in place to replace those members of Congress.

All the research I have seen shows that, at most, the rioters wished to "stop the vote-counting," which is also not an "insurrection." The dictionary can be argued with, but really, *Foreign Affairs* cannot. I submit this to you out of the great regard I have for *2600* and the sadness I share with others at some of its current unapologetic behavior.

Michaleen Garda

We went to Miriam-Webster for the definition of insurrection. They say it's "an act or instance of revolting against civil authority or an established government." Other dictionaries say basically the same thing. As summarized in the Washington Post *analysis "Yes, It Was An Insurrection" by senior reporter Aaron Blake on July 13, 2021, "an 'insurrection' isn't defined by the level of violence; it's defined by its purpose." And to go to what you see as an unimpeachable source,* Foreign Affairs *had an article titled "The Insurrection Hiding in Plain Sight," published January 14, 2021, where the word is used multiple times and very definitely when describing what happened on January 6th.*

This seems a strange thing to call us out for; pretty much every legitimate news outlet in the world agrees

on this.

Dear *2600*:

The oldest and greatest hacker magazine is now trash because it's inundated with right-wing hacktivists who have forgotten what hacking has always been about. Politics was never the focus for hackers - it was about information. The magazines now for hacking are pushing a right wing agenda and it's disgusting, not for being right wing, but for betraying what being a hacker - regardless of what hat you wear - has always been about. That is the ethos that information is free and open to everyone and no one should change any information to fit a narrative other than that which the reader determines for themselves.

Eric

The only thing we can figure is that we're not "the oldest and greatest hacker magazine" since you never actually mention our name and since we're having a hard time understanding how you could have ever reached such a conclusion. We do have people from all different backgrounds and beliefs who write in our pages. But we don't espouse one political belief over another. We confront issues head-on, which some believe makes us political. The conclusions we reach cause us to be labeled as being on one side or another. But it's not always that simple. There are people who will do whatever they're told if the instructions come from someone or something they follow and trust. We don't believe in that. We reach conclusions based on logic, history, science, and documented evidence. In today's society, that's often enough to get you labeled as being on a particular side. We don't control that part of things. But if people want to define their entire political party as being anti-science, racist, and/or anti-democracy, we have no problem at all condemning that party.

Dear *2600*:

I have been buying and reading the magazine since the 1980s. Recently I have signed up for a lifetime subscription. It was great to attend HOPE X and The Eleventh HOPE (and HOPE online in 2020). From time to time, I have listened to the radio show and have pitched in money.

I continue to be impressed with the efforts to speak out and encourage people to do the morally right thing. Be it politics, business, or society at large, immorality should be exposed and challenged. Calling attention to unethical politics, questionable business practices, and sleazy behavior is an important and admirable endeavor.

I now find it disturbing that *2600* is turning away from the moral issues regarding Bitcoin. It is a supportable viewpoint that Bitcoin is wrong on many levels. The insane price makes Bitcoin the greatest financial fraud of modern history. Using unregulated and nonaccountable "exchanges," Bitcoin went from ten dollars to a high of 60,000 over the years. Even presently, the price at around 30,000 is a sham erected by the big holders, miners, and exchanges. The Bitcoin propaganda has told the lies of safety from theft while people have lost thousands... the fairness of decentralization while being quiet on the required fee for every transaction. The hype also flouts the store of value principal while many have lost money due to the price volatility from the pumping and dumping hustle.

I will let someone else talk of the great waste of computer power and electricity used in mining something that is practically useless.

Bitcoin does have one use. It is a convenient and secret means of payment between criminals and bad actors. What is further evidence of the fraud is that blockchain technology is open source. This means anyone needing a cryptocurrency can make their own or get one basically for free. So why the crazy price? Criminal price manipulation? Heaven's, no.

I encourage *2600* staff, hackers, and all people to seriously look at the immorality of Bitcoin and work in defeating this one evil thing in the world.

Old Crow

What exactly did we do to warrant this accusation? We've printed articles that both condemn and praise what Bitcoin is. We didn't create it and nothing we do will fix its many issues. But what we can *do is have a dialogue and spread information, which may help result in some positive changes. We hope to see more pieces that present ideas, evidence, solutions, and more.*

Dear *2600*:

Shortly after I sent you my last letter detailing why I believed that you were using the word "insurrection" incorrectly, I came upon the news that the FBI agrees that there was no insurrection. Now you have The Council on Foreign Relations, the dictionary, and the FBI telling you that there was no "insurrection." If this does not lead you to the conclusion that you have been using this word incorrectly, I do not know what would. The use of this word is inflammatory and spreads unnecessary hate and division in our, and all, communities.

Now if you are intelligent and enlightened enough to admit your error, I am sure the readers of *2600* would be happy to generously accept your apology. I would be remiss not to point out that this is only one of many indications in your verbiage that you are nonpartisan, biased, and *not* on the side of "science." This would be a good moment for you to reread all of your recent opinions with an eye towards discovering if you can find any other areas of error.

Michaleen Garda

Hard pass. We will continue to use the word because it's the correct word to use (not that we plan on continuing to dwell on this). An insurrection does not have to be successful, nor does it need to be well organized to be defined as such. We don't know when you thought the dictionary moved into your corner, but we can assure you they all support our usage. As mentioned in our previous reply, The Council on Foreign Relations' publication has also used the word in this manner. The links you sent that were not avid right wing publications or columnists correctly report that the FBI claims not to have found evidence of an organized plot prior to January 6th. Of course, saying otherwise would make them look rather incompetent, but regardless, such a plot is not an essential part of this. At no point did the FBI say there was no insurrection. In fact, what they did say before Congress was: "That siege was criminal behavior,

pure and simple. It's behavior that we, the FBI, view as domestic terrorism." Perhaps if we had referred to the insurrection as a terrorist act all along, this whole debate could have been avoided.

Dear *2600*:

In the Marketplace section of 38:1, a post from an inmate made it to print. A quick Google of his self-doxxed name and city reveals that he is a convicted pedophile, served time, and looks like he is going back to prison again for the same horrific behavior.

I would advise the community to avoid this person altogether - and for *2600* to exercise better judgment when something sketchy gets submitted to the classifieds.

Hack the planet.

fuX0r

[Note: we removed identifying information, as we don't feel anything is accomplished here by pointing the spotlight at a specific person's crimes.] We understand and respect your concern. We do advise people of the risks of contacting anyone through ads. And, as you say, you were able to easily find this info through Google. It doesn't take much effort. Readers can then make the decision as to whether or not they want to contact a particular person.

Even individuals who have committed crimes have the right to communicate with others. We all should encourage people to be careful when contacting strangers anywhere. After all, there are lots of bad people outside the walls who you won't find out much about through Google.

And now for a look from the other side....

Inside the Walls

Dear *2600*:

Vincent had a problem with multiple issues coming into the prison he's at (Letters, 37:4), and you asked if policies regarding envelope color are common. To answer simply: yes, such policies are very common. What's more, from reading a national corrections journal years ago, state DoC admins carefully structure rules regarding mail to make it more difficult for prisoners to get publications. Many states require manila envelopes while others require white. Some reject anything with stamps or stickers or labels.

Wisconsin DoC will soon be requiring all incoming mail to be photocopied and the copies forwarded to the prisoner. This has already been instituted in one prison. *2600* already has a hit or miss chance for it coming through the mailroom. Almost every publication with "hack-" in the title is prohibited out of hand, and if they start actually paging through an issue of *2600*, it will most likely be denied.

I've been a prisoner for 23 years and our access to computers has only become more restricted over that time. Early in my incarceration, I completed an office vocational program, became the tutor, and taught myself VBA programming and database development. I was called all over the prison to fix problems, build waiting lists, and make tutorials for staff. Now I'm tagged as a security threat, barred from working at the main office building, school, or maintenance.

Books and magazines covering topics regarding computers, robotics, DIY, survival skills, or independent living are commonly denied. The reasons given are crafted to be non-specific: presents threat to security, promotes illegal behaviors, etc. It's a form with check boxes. They deny books because they have scratches on the covers, weigh too much, or are too long. Books over $75 are banned by policy. Property staff recently told me all publications may soon be prohibited. F'ing brilliant.

I thank you for the work you guys put into *2600*. Be well.

Jason

There's only so much we can do with such an insane and inconsistent system. But we do try. And, as the following letter attests, sometimes it works out.

Dear *2600*:

Just wanted to give you guys a *massive* thanks for re-sending the 1998 set of back issues to me in separate manilla envelopes. They arrived all at once with no problems whatsoever at my correctional facility and have been a joy to read. Again, thank you! This made my day and then some.

Interestingly, I thought you might enjoy the irony of one of your responses to a letter about cover photo submissions in the Summer 1998 issue: "Also, we require original photos. Pictures off the net or from digital cameras (anything less than 600 DPI) *are not acceptable*."

The times sure do change! Please continue to do what you guys and gals do as the world and society are better off with *2600* around.

Hack the planet.

Vincent

Yes, it's mostly the technology that has changed for the better. Those early digital cameras were really terrible.

Memory Lane

Dear *2600*:

Does anyone remember a publication called *Life At 300 Baud*?

HC

We weren't able to find such a publication, but we were able to find quite a few people who actually lived through that era. Imagine a time where you could read a line of text as fast as it displayed (or printed), where there were no graphics to speak of, and when audio or video online were science fiction fantasies? It was also a time where those with such access were infinitely superior to the 110 baud mainstream.

Dear *2600*:

Is anyone familiar with HAL2000, the home automation kit? I bought one many years ago and never installed it. I'm just wondering if it's a collectible now? It's the first publicly available voice recognition to automation system, the grandfather of modern Alexa and Google, etc. It used a modem in the PC to utilize the phone lines for TX/RX audio. You would just pick up a phone in the house and tell it to do something. Alternatively, you could wire a house with speakers and microphones in each room.

MN

People were fairly enamored with it when this came out in the 1990s, but the voice recognition didn't exactly get high reviews. It was definitely a pioneer in the field.

But here's something you may not have known: it's still around! The folks at www.automatedliving.com have been keeping this going for over 25 years now. They take great pride in it not being in the cloud, but controlled locally over the phone. Perhaps our readers can let us know if they run such a system and if it's worthwhile.

Scams

Dear *2600*:

Is this scammy? I don't know if this really fits under hacking, but it is suspicious. I never put a car for sale on Facebook Marketplace before, but I have an old minivan, asking $1200. In two hours, I had over a dozen asking "Is this still available?" As soon as I answer Yes, I either get no response or they ask for an address. I started asking where they were coming from and either I didn't get an answer or I got a very unlikely part of town they claim to be coming from. My phone number is not listed in the ad.

Frank

Yes, Facebook Marketplace is infested with scam artists. They work in both directions, being both "sellers" looking for victims and "buyers" who don't actually have the item they're advertising. In your case, they may be trying to get information out of you so that they have an address associated with a name which can then be used for future scams. Of course, since Facebook has a button for people to press to send the "Is this still available?" message, it could be nothing more than curious people who like hitting buttons and don't really intend on doing much more than that. Not giving out personal info to anyone but serious buyers is always the best approach.

Dear *2600*:

How do those so called "dark web scanners" by Experian work? How exactly is something clandestine with no search engine indexing supposed to be scanned? Or is it just a psychological tool?

RE

It's basically a way for a company like Experian to cash in on fear and use the dark web for profit. You give them your Social Security Number, email address, and phone number and they look through various places to see if these things pop up anywhere. If they do, then they can sell you more fear. If they don't, well, you've just given them your private info, so there are all sorts of possibilities.

Mostly, the info they find is already available on other sites and has been for years. It's also misleading to say that your email address has been compromised because it shows up in a listing of breached accounts for some trivial shopper loyalty club or equivalent. If you use the same password for everything, then you would have reason to be concerned. But you certainly don't need Experian to tell you that.

We recommend sites like haveibeenpwned.com, which provides basically the same info for free.

Dear *2600*:

AM AN ANONYMOUS HACKER I BRING GOOD NEWS FOR YOU FACEBOOK PASSWORD HACKING GMAIL HACKING GAMES HACKING INSTAGRAM HACKING ETC SEND ME FREIND REQUEST OR SEND TEXR MESSAGE OR COMMENTS BELOW I WILL TEXT YOU? THANK YOU.

Cash App

And to think there are people who would jump to conclusions and not trust a message like this.

Clarification

Dear *2600*:

I understand people in China are hacking Microsoft. I'm not involved.

HC

Good to know.

Dear *2600*:

There was an interesting bit of shell published recently which mentioned in the comments that getting a new IP from Tor wasn't possible.

This isn't so. Tor has a control API, generally on port 9501. Almost everything can be set from this API. It's a relatively simple text API that is authenticated with a password. Sending the command SIGNAL NEWNYM will do just that.

You can also control entry and exit nodes with ExcludeNodes, ExcludeExitNodes, ExitNodes, EntryNodes statements in torrc. Entries can be countries, node names, address patterns. Config items can also be set via the API.

As far as SIGNAL NEWNYM goes, oh look, a simple API utility exists: github.com/GIJack/tor-util.

GI Jack: All American Zero

Dear *2600*:

I just bought the PDF version of the summer issue, and it surprised me how much personal information I have to give away to buy a digital download using Bitcoin.

I'm not too paranoid about sharing my information, but still. Shouldn't my email address be plenty enough for a digital delivery?

A physical delivery address, billing address, and phone number had to be entered during checkout. It's like the PDFs are marked up as physical goods in Shopify.

Or maybe I'm just doing it wrong?

Of course, this is a minor annoyance. I still love you; keep up the good work!

Sven

We agree it shouldn't be like this. We certainly don't need all that info. We believe this is because we're using the Shopify interface which is set up to treat every purchase like a credit card purchase where such info is required for verification. That's not the case with Bitcoin though, so this shouldn't be happening. We'll try to have a talk with them and see if we can make this not occur - or try and find another way of doing it.

You can also try entering fake info in those fields and see if it causes any problems. (Now, what other magazine would encourage readers to enter fake info when buying its own issues?)

Dear *2600*:

I am excited to see that you chose my photo for your summer issue! However, I never received any correspondence regarding how to claim my free t-shirt and one-year subscription. Please advise.

r

"Never" is such a strong word. In actuality, we have already been in touch. It sometimes takes us a few weeks to make these arrangements after a new issue comes out.

Dear *2600*:

I am reaching out to you to share my story about how I personally suffered from false accusations on the Internet, and how I was blackmailed to delete my information which led me to create the Committee Against Defamation, Discrimination, and Persecution on the Internet.

A law about the regulation of the Internet in the U.S. must be changed. Google, Facebook, Twitter, and other search engines and social media aren't responsible for the content that they show. Fake news resources, forums dedicated to radicalism - all are available online. Millions of people in the world suffer from fake and dangerous information on the Internet. None of the search engines will be held accountable because they are protected under the stupid 230 section that was approved by Congress in 2006. The Tsarnaev brothers bombed people in Boston because they read radical literature on the Internet. There is a threat of terrorism again in the U.S. because of the situation in Afghanistan. Trump promised to change the outdated law, but unfortunately, he did not keep his promise. In his election campaign, Biden also promised to revise section 230, but it was an empty promise. You can't confuse free speech with crimes on the Internet.

The U.S. needs a new law immediately. U.S. authorities must think about the security of people. Below I suggest the following changes that should be included in a new law about the regulation of the Internet: 1) Making social networks and search engines such as Facebook, Instagram, Twitter, YouTube, Google, and others have departments specifically dedicated to filtering what is fake news and what is not. As soon as they identify something as fake news, they need to delete this content and these accounts, these fake sites as well. The criteria of what is fake news is public information. Bigger companies need to have this department. 2) If a person has a court decision from a foreign government about something being fake news, these social sites need to recognize this as valid. There needs to be an understanding of a global court law about fake news. 3) When contacting search engines about fake news being published, they have to respond promptly, for example, in three days. Fake news being spread can do damage very quickly and by the time the platform responds, the harm is already done. This requires a quick response. 4) If Google and other search engines do not delete this false information, then there need to be large fees that they will have to pay. This will serve as an incentive for them to delete wrongful information, as they will be motivated to not pay a large sum.

As an expert in this field, I would like to share and spread exclusive information about cybercrime groups that own these fake news sites and about our investigation of them. Thank you so much.

Yury

Section 230 of the Communications Decency Act has been referred to by the Electronic Frontier Foundation as "the most important law protecting Internet speech." That should be enough to warrant a closer look at calls to get rid of it.

Section 230 says that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." There are exceptions for things like copyright infringement and blatant criminal activity, but this basically protects online services (from social media networks to Internet Service Providers) from being held accountable for each and every thing its users say. Imagine every YouTube video and every comment made about each video, every Craigslist ad, every Facebook post, every Tweet, and so much more, all potentially putting the companies hosting this content at risk. The result would be far less content being posted in the first place and anything controversial being avoided at all costs. Ironically, the people pushing for this the most are Trump's minions who would likely find themselves the first ones locked out if this protection ceased to exist for providers and hosts.

This is not to say that everything is working perfectly. Clearly, that's not the case. The lies and misinformation that spread throughout the net can be frightening and even deadly. We believe a certain level of standards isn't an unreasonable expectation for any company hosting content. These standards should be defined by the communities being served, experts in the fields that are being discussed, as well as historical facts that can't be changed to suit a false narrative. This should not be thought of as an attack on free speech, as anyone still has the right to say whatever they want on their own sites. But massive networks that encourage the spreading of public messages have the right to (and should be expected to) impose standards that prevent demonstrably false info from being spread. And all of this can be done without imposing restrictive laws, which is almost never the answer and probably the last thing we need.

Enthusiasm

Dear *2600*:

I am writing to you today to talk to you about Unix! I am reading about Unix and have discovered that it is much better to use! I recently just bought a book called *Unix for FORTRAN Programmers*. I got the book from eBay. It dates back to 1990. I like the Unix command "sudo rm -r *" which clears all cache! Also, "ls rm -r" and "cat" plus "man". Lots more to learn! Don't forget the "login" and "logoff" command! Thank you so much for your support!

Blair

"Lots more to learn" is putting it mildly. Be very careful with those commands you're enamored with, as they can be very dangerous. "rm -r .cache" is more likely what you would type to get rid of cache, assuming you had the right permissions. It's good to see this level of enthusiasm, but it's so important to know what you're doing - or to at least have a backup in place in case you don't.

Dear *2600*:

Hi all. I ran across this picture in Keystone, South Dakota. The Mount Rushmore artwork above the

receiver (you might have to zoom in) with the busted receiver hanging upside down and a faded plastic enclosure seems like some sort of modern social commentary.

Josh

This description was good enough to print, even though we never got a photo to go along with it. Let us all imagine.

Misbehavior

Dear *2600*:

Good morning. In our most recent street furniture audit, we found that *The Hacker* newspaper box at 3415 N Southport Chicago IL was in poor condition with moderate rusting, graffiti, and/or stickers. As it is our mission to create a welcoming and resilient environment, we kindly ask that you improve the condition of this box or remove it.

I hope this email is finding the right person to talk about newspaper distribution maintenance. If not, would you please point me in the right direction? Let me know if there's any way we can help. Thank you in advance.

Riley Kelly
Urban Planning Intern
Lakeview Roscoe Village Chamber of Commerce

Well, this is certainly interesting. There must have been some sort of publication in Chicago with the name "hacker" on it that actually had newspaper boxes around town. Somehow, the folks in this office assumed they belonged to us. We wish they had sent us a picture - all we could find was a Google image of the area from years ago when no cars were parked in front of the newspaper boxes. If anyone in that area can tell us what this might have been about, we'd sure like to know more.

Dear *2600*:

PayPal thinks I'm violating international sanctions by buying an English-made "Persian rug" mouse mat from Etsy. My account was suspended and, in an email which mistook me for the seller, it informed me I was advertising PayPal as a method of payment for items that may originate from Iran. I was warned that my account would be terminated unless I provided evidence of where the mat was made. It's amusing that PayPal thinks I'm illegally selling rugs instead of improving my desk decor!

CR

Now we really want to buy an actual Persian rug from Iran.

Dear *2600*:

Why does the USPS monitor social media to tip off three-letter agencies about civil unrest? Seems a bit beyond their charter....

DG

We're glad we're not the only ones who felt that way. The program is called iCOP, or Internet Covert Operations Program, and it was revealed earlier this year.

Here's an interesting quote: "Analysts with the United States Postal Inspection Service (USPIS) Internet Covert Operations Program (iCOP) monitored significant activity regarding planned protests occurring internationally and domestically on March 20, 2021" according to a government bulletin issued on March 16 and labeled "law enforcement sensitive." "Locations and times have been identified for these protests, which are being distributed online across multiple social media platforms, to include right-wing leaning Parler and Telegram accounts."

While the target here appears to be violent white supremacists and people who see democracy as the enemy, this type of surveillance is deeply disturbing. Obviously, it can be used on anyone and when this is done en masse, the potential privacy violations for all of us go through the roof.

We believe there are plenty of ways to go after violent thugs. We don't need the post office turning its eye on everyone. There's mail to be delivered, after all.

Dear *2600*:

Hello. Just following up on this request. If we do not hear back from you by September 13th, we will proceed with disposing of these newspaper boxes.

Riley Kelly
Urban Planning Intern
Lakeview Roscoe Village Chamber of Commerce

Note how the box is now boxes. We would have contacted them directly, but we didn't read the email until after the deadline and they already seemed pretty angry. We probably would have felt guilty about something we know nothing about. Typical.

Mischief

Dear *2600*:

If you have an Amazon Echo in the bathroom, you've gotta do this. It's great. Add the skill called Fantastic Farts ahead of time. Then, when someone goes into the bathroom, either do this or make a routine to do this automatically. By using a routine, you'll be able to silently adjust the volume to like 75 to 85 percent. 1) Open the Alexa app on your phone; 2) Go to Skills and find Fantastic Fart; 3) Press the *launch* button; 4) A list should appear from the bottom of the screen giving you a list of your Echo devices, so press the one that is in your bathroom; 5) Wait about five seconds for sound and probably the scream and then the laughter from everyone else in the house. The reason I said to use the Fantastic Farts skill is because it is the first one I've found that you can launch manually like this and not have Alexa ruin the surprise by saying something before the sound

like "here is a wet fart." It just blasts a fart over that speaker. And yes, I might be a five-year-old, but I have 43 years of experience at being a five-year-old!

Mike

"Add the skill called Fantastic Farts." That's as far as we got.

Proposals

Dear *2600*:

Hi there, My name is Dean and I'm a political science student. I came across 2600.com while I was preparing to write my thesis. I found your page https://www.2600.com/dvd/docs/2000/0610-replies.html to be a great resource, which has helped me narrow down my thesis topic (how the Internet is used for censorship by governments). Other than your site, I've only found a few other helpful articles, like this one: https://www.privateinternetaccess.com/blog/internet-freedom-around-the-world-in-50-stats/ which had a good amount of information highlighting the Internet as a tool for censorship around the world. Maybe you'd care to add this to your page, too? It would make for a great inclusion on your site and provide a more complete resource on the subject of Internet freedom/censorship. Thanks again for your helpful site - it's been great for students like me (I've been sharing it with my peers).

Dean Williams

This sure seems like an actual suggestion from a real person. But it's phrased like one of those automated requests to add a link to a site for some unknown purpose. What's odd here is that our page that was cited is simply a transcript for one of the days of our DeCSS trial in 2000. It seems unlikely that this one day of testimony was so inspirational as to help decide someone's thesis. It also didn't help that this was sent from a digital marketing company. What we'd like to know is how this works, assuming it isn't an actual person. (And if it is, we'll feel absolutely terrible.)

Dear *2600*:

I'm writing this letter as a periodic contributor to this journal. As most of you know, hacking is a state of mind that allows us to see the world and its systems for their strength and weakness. I can hear you say "get to the point."

During the COVID pandemic, the world watched in wonder as GameStop stock went through the roof. Hedge fund managers were hitting themselves in the head while the little guy made a profit. The best part: it was legal! Now anybody who's read this journal knows that from time to time we've picked on GameStop, but it was all in good fun. However, this time around we helped a lot of ordinary people.

Can this hack work again? Yes. Let's prove it. There's a band named Life and a Day on soundcloud.com. They've been in prison for over 30 years, but were able to release 46 tracks of original rock and metal music.

They made this music with almost nothing. Simply amazing! If you like rock, you've got to hear these guys. The guitar work is off the hook! There is something for everyone.

Here's the challenge. If the band Life and a Day can get one million downloads or streams, it would place them at Platinum status, and could put them in contention for a Grammy. Yes, I'm aware that only pop stars get Grammys, but if enough people stream Life and a Day's music, we could turn that system inside out, and isn't that the point? Wouldn't it be crazy if they awarded a Grammy to a couple of guys in chains instead of a pop princess? All the band needs to achieve this outcome is a little help from the same community that drove up the stock price of GameStop. Fire up your botnet and see what happens. If nothing else, maybe Life and a Day will make the *2600* Inspirational Music list on the staff page.

Tweakie

This is definitely a longshot but at the very least readers can hear music from people with an interesting back story. We did enjoy watching what happened with GameStop this year. It's always nice to see the underdog bite.

On Deplatforming

Dear *2600*:

While I don't have access to "Errors in Freedom," reading the dialogue about it and the other articles in 38:1 has given me a clear enough picture. I want to say that I completely agree with you that platforms have a right and perhaps an obligation to deplatform truly harmful content. At the same time, however, I worry when that single act of deplatforming contributes to a broader culture of it. For example, if someone is simultaneously removed from Facebook, Instagram, Twitter, and YouTube (not naming any names here *cough*), they really don't have much of a platform in today's centralized era. Similarly, if a certain kind of speech is near-universally considered harmful, it will be very hard for someone to try and publish that speech. I do wonder how hard it would be for gay people to publish online in the 60s, had today's Web existed back then.

And I bring up homosexuality because there are currently people who are persecuted in much the same way: minor-attracted persons, aka pedophiles, nepiophiles, and hebephiles. Before I continue, I'll just say that the majority of them have never committed child sexual abuse and the majority of child sexual offenders are not MAPs. Say what you will about them, but they have the right to free speech and certainly the right to respect, compassion, and a healthy existence, just as much as anyone else. Yet finding companies that will host my MAP/paraphile sites has been very difficult (self-hosting is not an option in my case). I have been suspended or outright refused at least six times now, even by a supposedly free-speech domain reseller named Njalla. There are still some TLDs I can't find a good registrar for, and I only know of two good hosting companies anymore. And those that are left could easily vanish.

Needless to say, this whole experience has changed my perspective on free speech; I used to be like a lot of leftists who see it as less valuable than it once was. But it's easy to say that until it's you being censored.

Kay Faraday

Well, we all learned a few new words, but this really isn't going to do anything but bolster our opinion

that companies have every right to decide who they want to have on their platforms. You may indeed have points concerning unfair persecution of people who have never actually harmed someone else. And yes, everyone does have the right to free speech. But that doesn't mean anyone should be forced to provide a platform for something that violates their standards. This is very different from banning someone because of their race, religion, or sexual preference.

There is always the potential for abuse. Imagining how this would play out in the past or simply looking at what's going on around the world will provide more than enough examples. And when this happens, it needs to be fought. But that doesn't mean the overall premise of removing content society finds abhorrent isn't a sound one. It simply means we have to constantly be vigilant. And occasionally upgrade societies.

Additional Data

Dear *2600*:

In performing the due diligence expected of all readers of your magazine, that is, looking for "2600" in every possible place, it suddenly occurred to me that it was not enough to simply search for the string "2600". This is only the expression of the value in base 10. Realizing that its expression on other bases must be considered, I made a list. Perhaps this has been mentioned previously in your pages, but if not, below is a representative part of the list. Frequently, the value in the other base has a rich significance or pleasing form.

2600 = 101000101000 (base 2)
= 10120022 (base 3)
= 220220 (base 4)
= 40400 (base 5)
= 20012 (base 6)
= 10403 (base 7)
= 5050 (base 8)
= 3508 (base 9)
= 1608 (base 12)
= 1250 (base 13)
= A28 (base 16)
= 808 (base 18)
= 440 (base 25)
= 208 (base 32)

With all best wishes for your work!

ex nihilo nihil fit

Neat. We've now attached our name to three area codes (Hawaii, Cleveland, and Idaho!) and one zip code in Washington DC using this method. Not to mention the A28 highway in Kent and East Sussex, England.

Random Impression

Dear *2600*:

Is it just me or is Facebook's coronavirus vaccine notification as annoying as Clippy was back in the day?

Scott

Well, one was designed to offer tips on how to use Microsoft Office while the other encourages people not to send misinformation on COVID-19 that could prove deadly. Sometimes annoyances are worth it. Other times, they're just annoying.

Advice

Dear *2600*:

What do you think is best to learn for the future? I am 17 and I will finish high school in two years. At school, I'm learning C++ . We learn algorithms and mathematical problem solving. I was talking to my uncle who is into tech and he recommended that I should start learning something that is not very popular hut will be in the next five or ten years. Like a niche. I would love to read some tips, like what do you think about the future or what programming language I should focus on. Some of my interests are crypto, AI, and electric vehicles.

DD

Your uncle's advice is great, but you'd need to be a fortune teller to follow it. Imagine what we could accomplish if we knew of something that wasn't popular now but would be in the future. Obviously, that's something that would pay off, but since there are no guarantees, the first thing to tackle is to find something that you're happy with. That way, whether or not you make a ton of money at it, at least you won't be miserable. All of the interests you list clearly have a bright future, so by all means pursue them to the best of your ability and then see what doors open as a result. We also advise people to branch out a bit, particularly if they're attending college, and learn about things that may not have an immediate practical use. Knowledge has a way of coming back and serving you down the road. It's really impossible to predict, which is why you should never turn down the opportunity to broaden your horizons.

Dear *2600*:

I have received five issues now of *2600 Magazine* and I have really been enjoying it. I must have willed 38:1 into existence, as my excitement about the next issue felt as if it was growing exponentially for the past few days. W00t, it showed up today!

The reason I am writing is that I am perpetually confused and angered by the media. As a teenager, I simply repeated whatever the last argument was that I heard on an issue as if it was my own opinion. Even if it was a completely contrasting argument. Throughout my adult life, much of which has been spent in prison, I have become painfully aware of how easily people will believe anything, and make up absurd explanations for things they don't understand. Or worse, things they don't want to understand.

With this newfound awareness, I try to develop my own opinions about things, but it is difficult without a connection to the outside world. I try to watch both CNN and Fox, but I feel like both are equally full of shit. And occasionally I find myself getting angry about something they say, and I have to stop myself and remember that I'm often literally being given no information about whatever is being reported.

Take the Fauci email "scandal" that's going on. I had my father go online and read the initial *BuzzFeed* report, along with some other digging (including the "Tucker Carlson meltdown," as he put it). As far as he can find, there's not much there beyond his affiliation with some people in Wuhan makes him look kind of bad. But there's sure as shit no smoking gun. So when I watch these news channels, I say to myself (and sometimes to the TV), "Show me the fucking emails!" Or to give an example from the other side,

show me the fucking Georgia voting bill! You know? I'm not interested in what someone has to say about a bill or law or whatever, I just want to read the bill or law or whatever myself. Does that make sense? I feel like that's the right thing to do, and that I am literally the only person here that is interested in signing up for advance copies of Senate/Assembly bills from the Office of Legislative Services in my state.

I ask you this because you seem to be fact-oriented people, and obviously have extremely strong opinions on the matter. I have equally as strong opinions about facts, however they specifically apply to the political matters you frequently discuss where I generally hold no opinion. I can't bother my dad to fact check every little thing I hear, which drives me nuts. But what I don't understand is how everything is just so fucking divided right now. I swear it's being done on purpose by both sides. And that just makes me sound like a conspiracy theorist, but then I find myself rationalizing it by saying, "Well, if (fill in the blank) happened, who the fuck knows? I'd believe anything!" And then invariably the next insane thing happens.

I would also like to state respectfully that I do become frustrated sometimes with the level of political talk, particularly on *Off The Hook*.- though I feel my frustration is perhaps of a different nature than the angry letter writers that disagree politically. I become frustrated because realistically you probably get about 45 minutes of content during the show, and when a significant percentage is allocated to political discussion, I might only be able to hear 20 minutes of hacker content. In such a restricted environment, I am starved for content, and even a full hour weekly coupled with quarterly issues just doesn't cut it.

I get that my life circumstances aren't really your problem, though. I'm paying for and getting help for something pretty terrible that I did, so I guess this is part of the deal. But I wouldn't be saying it if I didn't think you guys were open-minded enough to deal with it.

So maybe it's about time I sum up what I'm asking here:

- Any advice for developing my own opinions?
- Can you point me to any truly objective fact-checking sources that cite primary documents in a concise manner? My father will print anything I ask for.
- Am I way off here?

I think that covers it.... I know you guys probably get an unmanageable amount of letters, but hopefully some day eventually I'll hear back. I really appreciate your time spent reading this; the issues I've described are extremely important to me and my deepest core values.

James

Your perception of the mass media is fairly accurate. But remember that this is what the mass media is designed to do. We do believe there are degrees of distortion that are being peddled and that lumping them all together is basically a victory for the worst elements. There are plenty of sites and organizations dedicated to dispelling myths and verifying facts. FactCheck.org, Snopes, and PolitiFact are three that come to mind. And publications like The New York Times, Washington Post, The Economist, *and* Politico, *while far from perfect, have a much better reputation than many others insofar as reporting the full story. If you have access to broadcast media and are lucky enough to receive BBC World News or C-SPAN, you can bypass much of the personality-driven bullshit. It's hard for broadcast or print media to provide access to full documents, but this is often provided as links at online outlets.*

We sympathize with the frustration you feel listening to our radio shows, which admittedly have spent more time dealing with issues that have been in the headlines. We do always try to tie them into technology, hacking, or free speech issues, as these are key values we all understand. To not devote time to the history that's unfolding around us would be tantamount to existing in a bubble, which is how you wake up one day to a world you don't recognize. We all have a voice and we encourage everyone to use theirs and not just follow blindly or speak through anger. You're doing the right thing by trying to get as much info as possible. This is a challenge no matter what side of the wall you're on.

Opportunities

Dear *2600*:

Cyber Extortion: What the low level approach looks like. The email claims to have video of you doing something incriminating. The email claims that it has access to your passwords. The email claims that if you do not send money to a Bitcoin addresss that they (the extorter) will send evidence to your family, business associates, and other people in your social circle. While some of the claims are fake, the real damage is happening behind the scenes. These emails are distractions for more coordinated cyber extraction activities for your clients and/or your loved ones. *It's not an email you should ignore*. If you get one of these emails frequently, drop me a DM or Signal me. We fix the holes that you left open.

JahSun

Here we go. A scam to protect you against a scam. First of all, these claims of video evidence of some untoward activity are nearly always complete bullshit. They're designed to make your imagination run rampant as to what they might have on you. It's the same sort of illogical thought that people use when thinking about what hackers might be capable of doing. Secondly, it's old news that there are massive lists of compromised passwords, some of which are associated with specific email addresses. So if you're someone who uses the same password for everything, you might panic when you see it displayed after the database of your drug store loyalty card is compromised. But for those who use any degree of security when using passwords, it'll just be a disposable password that means nothing to any of your other accounts.

What you're doing here is relying on people to panic when things like the above happen instead of simply relaying the facts so they don't get taken in yet again by someone like you trying to take advantage of the situation.

Dear *2600*:

I am a 42-year-old Asian American man who has

been interested in hacking and the culture since the mid 90s. Do you think getting into hacking in my early 40s is too late to acquire a good skillset?? Also, how do you handle frustration in learning new skills? I get frustrated when learning things at times.

Chuan

Your ethnicity, age, and sex aren't relevant when it comes to learning. Frustration comes from pressure, which is often related to expectations that aren't met when desired. So consider this an adventure where you don't actually know what skillset you'll develop. You've already achieved the part that most people don't: having a genuine interest in the hacker culture. We can't say where it will take you, but the more you learn, the more possibilities will emerge. If you don't overthink it, we believe you'll have a fresh perspective in the not-too-distant future. Good luck.

Dear *2600*:

Hi there, hope all is well. Thought to check if you might be available for a quick call today/tomorrow.

I ask since my company Mechdroid is offering unlimited calling VoIP plans in New York starting from $19.95/month: We can slash your phone costs by up to 35 percent while boasting industry-leading features your company needs.

Lance

Yes, Lance, all is well, except our spam filter isn't working as well as it should. Do you offer this product? As for our phone bills, no need to worry about us. We mastered that system decades ago.

Dear *2600*:

I accepted the job offer that's breaking me into infosec! Posted not long ago in regards to imposter syndrome because a friend was trying to get me into the consulting company he's a manager at. Just wanted to follow up and mention it because I'm glad I didn't let the haters I work with or imposter syndrome hold me back. I feel like shouting it from a mountain top or some shit. This is my dream job! I'll be pen testing, doing managed services and forensics. Thanks to the *2600* community as a whole because all of the posts on the Facebook group and the actual zine encouraged me as well.

Jay

We always knew you could do it.

Dear *2600*:

Until today, ransomware and data espionage were under the rug affairs. The companies you trusted with your deepest secrets, like law firms, have been keeping secrets from you. When a law firm gets hit with ransomware, their entire legal practice is compromised. From case files to investigation recordings, all is exposed. Each week, we leverage our Darknet Intelligence Collector to scan the darkest corners of the darknet for companies who have been hit by ransomware. If you want to know if a company you are about to do business with has secrets on the darknet, or would like your company to be sanitized from these data stores, call us.

JahSun

You again. So your thing is to prey on people's fears and suspicions, use a bunch of catch phrases and headlines, and make a quick buck off of someone else's scam or misfortune? And you expect us to help you spread the word? Without even offering us a cut?!

Poor Tech

Dear *2600*:

Really infuriated - between my Metro PCS "meh" network and my phone's flaking out on getting my Wi-Fi signals, I do *not* have a reliable "moment's notice" phone in my apartment. Considering VOIP for 911. *Trying* to research the possibility of getting a copper wire landline, but finding out that it's nearly impossible and that the infrastructure (mostly the electricity to keep it running) is going extinct. Thoughts?

Daniel

It's about as dire as you present it and a perfect example of how new technology sometimes makes things less efficient. True, there is much less demand for copper wire landlines these days, but making them obsolete is a mistake and an indication of how little the phone companies actually care about the "service" part of their existence. Copper lines serve a purpose in situations like yours or in emergencies when power and/or cell service goes out. Hurricane Ida recently made that painfully clear in Louisiana and other states. Old and new technology can work alongside each other and ensure that there is never a complete outage. There are numerous examples of this in both the hardware and software world.

Dear *2600*:

My friend was ordering from this web page and it auto-populated the entry boxes with data from another *totally* unrelated customer from a city four hours away from her address, email, phone numbers, etc. 1) Why is one-step checkout considered "secure checkout" and 2) What exactly caused this, and what can we do? We have contacted them for support and gotten nowhere.

Xochitl

This is just poor programming, plain and simple. We've come across it many times on web forms as well as forms on terminals in stores, etc. If you've already contacted them to tell them about this problem and they have yet to do anything, it's time to let the world know exactly who they are. That will get it fixed.

Dear *2600*:

Yesterday, Facebook told me this: "You're temporarily restricted from joining and posting to groups that you do not manage until December 4, 219250468 at 10:30 AM." Since I'm posting this today, either I had so much fun that a quarter billion years went by seemingly overnight, or something went wrong.

Nick

We can't help but be impressed by the fact that many bulletin board systems run by kids back in the 1980s were better managed.

WE WANT YOUR LETTERS!

Please send us your comments on articles, technology, privacy, or whatever else is on your mind.
As you can see, we're open to a wide amount of opinions.

letters@2600.com or 2600 Letters, PO Box 99, Middle Island, NY 11953 USA

EFFecting Digital Freedom

by Jason Kelley

When We Fight, We Win

In September, EFF announced that we were planning to put our ten-year-old browser extension, HTTPS Everywhere, into maintenance mode. This wasn't giving up - this was a victory. As we had hoped when we launched the project, HTTPS, which encrypts website traffic, has become essentially ubiquitous. HTTPS is, actually, everywhere, offering protection against eavesdropping and tampering with the contents of a site or with the information you send to a site. This provides protection against a network observer learning the content of the information flowing in each direction - for instance, the text of email messages you send or receive through a webmail site, the products you browse or purchase on an e-commerce site, or the particular articles you read on a reference site.

Since we started offering HTTPS Everywhere, the battle to encrypt the web has made leaps and bounds. The vast majority of the web is now encrypted. In 2017, half of all web traffic was encrypted - by 2019, nearly 90 percent was encrypted. And the relatively recent addition of a native setting to turn on native HTTPS-only mode in Firefox, Chrome, Edge, and Safari has made our extension, which ensures that users benefit from the protection of HTTPS wherever possible, redundant. This is a win for all users and a clear signal that encryption matters.

But despite the overwhelming recognition that encryption benefits users and its wholesale adoption by tech companies, encryption is still, incredibly, under attack. Technologists, privacy activists, and everyday users were shocked when one of the largest providers of end-to-end encrypted messaging, Apple, announced in August that it would be adding two scanning features to its devices. The first feature would search for "explicit" photos sent to or by young people via Messages if they were on Family plans that enabled it. Separately (and using different technology), Apple is also planning to pilot scanning for their iCloud photos backup service, to look for matches against a database of known child sexual exploitation material, on every device that uses the iCloud service.

Both of Apple's plans are what we call "client-side scanning." Proponents maintain that if the device scans an encrypted message after or before it's been delivered, then end-to-end encryption - where only the sender and the recipient have the keys to unlock the message - remains unbroken. This is wrong. These privacy-invasive proposals work like this: every time you send a message, software that comes with your messaging app first checks it, whether using hash matching or applying an on-device machine learning classifier. "Hash matching" checks the message against a database of "hashes," or unique digital fingerprints, usually of images or videos, and machine learning uses software trained to recognize similar images.

In either case, if it finds a match, it may refuse to send your message, notify the recipient, or even forward it to a third party, possibly without your knowledge. Apple's plan is to scan the photos sent by or to some young people via Messages for "explicit" content, and potentially notify parents if it is sent or received. Apple's other plan is to use client-side hash matching to scan iCloud photo libraries, and if the iCloud photo scanning matches enough photos to the hashed database of known child exploitation material, then a manual review will take place, and Apple may eventually send the information to the National Center for Missing and Exploited Children.

Though these plans differ in intent and technology, they are both extremely dangerous. A backdoor by any other name is still a backdoor. Client-side scanning, like many proposals to infiltrate secure messaging before it, would render the user privacy and security guarantees of encryption hollow. Adding a backdoor that is only accessible by the good guys is impossible, and it fundamentally breaks the promise of encryption. It would offer not only an incentive but a ready-built system for authoritarian governments to scan for additional content from all users - such as protest imagery or even LGBTQ content in countries where it is outlawed. Creating a system to scan photos that are uploaded to the iCloud service or those sent to other users isn't a slippery slope; it's a fully built system just waiting for external pressure to make the slightest change.

As we have for decades, EFF and our allies jumped into action after Apple's announcement, delivering a petition with nearly 60,000 signatures to Apple in under a month, leading protests at Apple stores, and even flying a banner over Apple's headquarters during their September iPhone launch event. We also wrote nearly a dozen different explanations of why the plan was dangerous, many of which have been translated into multiple languages and quoted by hundreds of news sites. Due to this massive criticism, which not only came from EFF and our allies, but from human rights groups, heads of state, and users like you, Apple announced they would delay the launch of these features. This isn't sufficient, of course - the company must wholly commit to protecting encryption and user privacy - but for now, encryption continues to thrive. When cryptographer and cybersecurity expert Bruce Schneier was asked whether backdoors to Apple's iPhones were inevitable during the press conference where we delivered our petitions, he was blunt: "Client-side scanning is the solution du jour. If you go back through the decades, there were different ones: there was key escrow, weakening algorithms... an update mechanism to push hacked updates. In every time period, a different solution becomes the one that is favored. Inevitably, in the past, none of those have been implemented. So, I don't think this is inevitable either. So far, we're doing well here in not getting a backdoor into our devices."

Encryption has become standard over the web, and the number of users who rely on encrypted messaging and encryption generally has grown. Even as the government and law enforcement have pushed tech companies for decades to find backdoors into encryption and encrypted devices, smartphones have become both more important and more secure. They are in the pocket of elected officials and heads of state, CEOs and power plant operators, judges and police officers. We rely on encrypted messaging in ways that many don't even realize.

Apple famously denied the FBI's request to add a backdoor into the device of a suspected terrorist in 2016, which is part of what makes their client-side scanning plan such a slap in the face. We believe the company will find its way to the correct, secure decision in this case as well. There's no guarantee that we'll win the war, but so far, we've won the battles - and EFF will continue to fight to protect the growing number of users who rely on safe, secure communications, whether that's on the web, on phones, or anywhere else. The contours of the fight may have shifted, but when we fight, we win.

Hacking NYC MTA Kiosks

by enbyte

Unfortunately, the technology described in this article is no longer around, possibly because it is hackable. I didn't know *2600* existed when I found out about this, but I would've written in if I knew it did.

A couple of years ago, the New York City MTA (Metropolitan Transportation Authority) started putting kiosks inside subway stations. These would do various things, such as find the next train coming to the station, show you how to get to a station you keyed in, display a map, etc.

The way it was laid out, the bottom half of the screen was an ad, presumably to pay for the kiosks, and the top half had the thing you wanted to see, along with some buttons that changed if you were looking at the maps, directions, or whatever. One of the buttons was "Wheelchair Accessible," which meant that the top of the display became an ad and the bottom showed the UI.

Anyway, one of the tabs was the "Maps" tab, perhaps the seemingly least hackable. All it displayed was an image of the subway map for the five boroughs, with the train lines running through them. However, on the side of the map box, was a little tiny "Microsoft Gray" rectangle, maybe three by 10 pixels. If you tapped on this, a tiny box with a stylus and post-it appeared where the rectangle was. Pressing on this opened a yellow box at the bottom of the screen where you could scribble and the computer would try and fail to guess what you wrote.

I'm not sure what the purpose of the notepad was, but that wasn't the interesting part. On the top of the little box with the writing pad was a keyboard icon. This put a touch keyboard where the pad was. I typed all kinds of random stuff, but nothing happened.

A week later, I was with my dad in the same subway station, and was showing him how to open the keyboard. He suggested that I should try to press keyboard shortcuts and see if that did anything. I discovered that upon pressing (Fn) + Ctrl + Shift + F12, the kiosk would open Intel Graphics Settings! Shortly after opening the settings, the UI behind the graphics settings (and the ad) would change to a screen that said "There was a problem with this kiosk, maintenance is coming." However, the Intel Graphics Settings window didn't disappear!

Inside the settings, you could mess with stuff like saturation and the color profile. All this accomplished was changing the maintenance screen from gray with white text to slightly lighter gray with white text. After messing around with settings for a while, I discovered a help menu with links to Microsoft for support! Clicking on one of these opened some browser window at the given link.

The browser wasn't locked down at all, though. You could type in a URL, and do whatever you wanted. I discovered it could play web games perfectly fine, despite being something like Internet Explorer 2 on Microsoft Windows Kiosk.

Unfortunately, I was eight when I found all of this stuff, and so was content showing my friends and playing various web games while waiting for my train. I didn't do anything like trying to type in a drive letter, trying to open other applications, or messing around in the browser settings.

The new kiosks were installed maybe a month after I did all of this, so the MTA probably knew what I was doing. Despite many attempts, the new kiosks did not conveniently have a "Hack Me" button like the previous ones did. They also had a much slicker UI, and showed you things like the MTA's Twitter feed, or whatever. So unfortunately, I haven't hacked these yet, and probably won't, since I haven't been on the subway in two years.

Shouts: dexrey4 and spaceman.

What's With This Username Stuff, Anyhow?

by dcole

"Dude, I need a handle, man! I mean, I don't have an identity until I have a handle," Joey says to Phreak in the cult classic movie *Hackers*. The anxiety of picking the perfect handle was too much for Joey and he was asking for help. While the perfect handle should obscure your identity online to the authorities, it should also be an extension of your personality within the hacker community. At least, that is what I have come to know over time.

A handle, username, hacker name, alias, whatever you call it, everyone has one online. For some people, this name is an extension of their personality. Everything they do is tagged with this name as a graffiti artist may tag their art. Growing up in the rural prairies of Canada, I never experienced this naming convention. I did not learn of the movie *Hackers* and the whole hacking culture around computers until well into my twenties. As a kid, computers were a solitary hobby for me.

The first computer system I had a user account on was at my high school. The computer administrator set up all the new students' usernames much like any other computer administrator would, the first letter of your first name and the rest was your last name. At this time (the mid 1990s), the eight-character limitation was in place for usernames. Luckily, my whole last name was four letters long, so it fit nicely within this limitation. As I continued my high school career and moved on to post-secondary education, this stock username followed me around as it does with most people. This is how I came to be known (not really) as `dcole`.

In those early days, I was unaware of hacker culture or people choosing handles online that had no direct relation to their offline identity - purposeful anonymity. Being a small-town kid who knew everyone around, it never dawned on me that you could be anonymous. So, as I moved to the online world unaware of the hacker culture, I used the username I had already been provided throughout my school career. This led to a funny misunderstanding one day online.

At the time I was on the SDF public access UNIX server in the chat section. A fellow member online mentioned that they found my username humorous. Rising to the bait, I asked why that was. The member proceeded to write this out; `dcole = dekhole = dick hole`. I was flabbergasted! I'd never had anybody try to make that connection before, but this member clearly had. After picking myself up off the floor from a good laugh, I proceeded to tell this particular member that my username was not nearly so clever as that.

Now let's suppose you, the reader, are a young up and coming hacker looking for a cool handle. How might you choose one? An article posted to `hackernoon.com`[1] suggests opening a dictionary at random and choosing the first noun you come across. Next, close the dictionary, open it at random again, and choose the first adjective you come across. These two words could then become your handle. Not having a dictionary at hand, I asked Google to provide me with a random noun and adjective, this is what I received: `Walking Null`. Not the best alias, but not the worst as well.

The above-mentioned method utilizes randomness to provide a username that is not representative of one's self. This might be a good thing if you are looking to remain anonymous. What if you would like to have a more personalized alias? Hackernoon suggests picking a few different things you like and mashing them all together into one username: `pok3manLover69`. Who wouldn't want a username such as this? Either way, one has to be creative nowadays with their username as there are so many people online compared to 25 years ago. You don't want to be known as `joey61854`, do you?

If you aren't a total n00b and want to be an 31337 H4X0R, another method you could use is 13372 or leetspeak. Leetspeak consists of replacing certain characters in your username with other characters that look similar. For example, the letter "e" can be replaced with the number "3" or the letter "o" can be replaced with the number "0." Using this method, you could easily change a username like `Walking Null` into `Wa7k1ng Nu77`. This instantly makes you a more proficient hacker with the coolest alias on the block (or network). You'll be pwning servers in no time!

As I am not a hacker in the sense of cracking into computer networks, I never felt the need to be anonymous online. This may come across as a naive view, but it is the one I hold. My username is a direct link to who I am in the real world. I will not do or say anything on the Internet that I would not do in real life. I have always tried my best to apply the morals I have learned in the offline world to my online interactions. None of this is meant to look down on those who choose cool online handles like `CRASH OVERRIDE` or `ACID BURN`. In the end, I just wanted to add my two cents to the conversation.

References

[1] `hackernoon.com/how-to-choose-your-next-username-7-creative-ways-to-hack-a-great-handle-l71f73yzp`

[2] `en.wikipedia.org/wiki/Leet`

The Matrix Is Real: How to Hack Humans for Fun and Profit

by dohp az

A mind is inhibited from critical thinking and rational thought during an emotional reaction. When we decide through our emotions, particularly during a reaction, logic does not apply - feelings instead, do. Using emotional cognition when making decisions is the opposite of critical thinking. Emotional triggers are environmental stimuli (such as a picture, word, phrase, etc.) that trigger an emotional response. In the past, each individual had unique emotional triggers based on their life experiences. However, the consumption of centralized content is centralizing humanity's life experiences, and thus centralizing these specific triggers of emotional reaction. After these emotional triggers form in individuals over time, with repeated consumption of content, they are then available for triggering. At a time of a person's or content creator's choosing, otherwise critically thinking individuals can be triggered into an emotional reaction and thus momentarily prevented from logical thought. When combined with confirmation bias, emotional triggers inhibit long term critical thinking and education in general.

Let us begin with an example from an unscientific and informal survey. When unaware of the author, the vast majority of individuals, regardless of political affiliation, agreed with a specific pragmatic description/solution to a problem designed by a popular but polarizing political person. However, a majority of those with opposing political views no longer agreed if they were informed of the author after the problem/solution was presented, but before the reader responded to questions. Most tellingly, if the person was informed of the author ahead of the pragmatic presentation, the respondents of the opposing political view also failed questions regarding the content, as if they were unable/unwilling to listen once emotionally triggered by the polarizing political figure. This self censorship or rational inhibition is an example of an emotional trigger at work.

Images can be as effective triggers as popular personas, but even simple words and phrases have become common targets of emotional trigger programming. Non-organic emotional triggers are often designed around a particular subject, genre, or phraseology and can be triggered on-demand as a means to inhibit logical thought. Once programmed, an emotion is experienced whenever the trigger is encountered, potentially inhibiting the logical thought of an individual on demand.

To scale this to societal control, individual emotional responses to images/ideas are being meticulously recorded and stored in the cloud. This emotional trigger database is a core feature of Big Data. Individualized and applied society-wide simultaneously through centralized media, these triggers are being used today to short circuit the will of the people by interfering with their organic social behavior, thought, and consciousness through the triggering of emotions. A.I. from an advertising use case is best described as the technology to create strong emotional reactions for a brand and is rooted in emotional triggers. Time and endless application of this technology have morphed humanity into a sort of hive mind or assimilated mind. Since the implementation technique (i.e., emotional trigger programming) only inhibits intelligence, the emotionally anxious mind is a more accurate description.

Emotions, and more specifically human reactions to emotions, are a natural and vital element of cognizant beings. Ignoring our emotions is not a healthy or viable means to thwart emotional trigger programming. However, when being bombarded with emotional trigger programming at all times while consuming media content, it is prudent to train our brain to identify and reject this programming.

It is difficult to estimate the amount spent a year by both government and corporations to embed emotional triggers into individuals for future use. Much research, and current corporate expenditures, are done for benign purposes such as advertising and awareness campaigns. However, since COVID-19 in particular, there has been a quiet transition between embedding these triggers to activating previously embedded triggers in order to manipulate individuals and thus society in general. Do not be surprised by observing that the centralized media is coordinating the activation of emotional triggers in order to drive political, ideological, and potentially nefarious agendas. As advertisers, this is their bread and butter. The root problem is not marketing (i.e., emotional trigger programming). The problem is centralization and no transparency. The merger of corporate and government agendas only increases the intensity and spread of media-based psychological attacks that are designed to drive acceptance of an agenda by preventing critical thinking.

Under careful control of Big Data algorithms and orifices, social engineering the human population is now the new business model of Big

Tech and Big Media. But there are more dangers than the obvious ones.

The embedding of diametrically opposed emotional triggers can foment hatred between people with the same triggers but differing emotional responses. People of differing emotional responses to the same trigger can never agree, as emotional responses are not subject to debate or reasoning. If not subjected to emotional trigger programming, these same people could easily communicate and reach a compromise, and at least agree to disagree. But if what they are arguing about is an emotion, there can be no agreement unless the emotion is in agreement. Once an emotion is triggered, an individual can no longer think logically (until emotion subsides), so if both parties are triggering differing emotions from the same trigger there can never be any agreement as the discussion is now an emotional one, not a logical one.

Without knowledge/transparency regarding the AI algorithms used and/or transparency/reverse engineering, we as a society cannot know the future that the corporate and government funded emotional programmers planned for humanity. One thing is very clear, however. Our society is being emotionally triggered at an alarming rate. Are the centralized content creators that currently orchestrate these emotional trigger storms within humans the same as those who programmed the emotional triggers within humanity months/years/decades ago? Does it matter?

Programming emotional triggers into others is itself a form of emotional attack that results in emotional discomfort (or even physical trauma if resisted - "discipline," etc.) among the subjects being programmed. To avoid discomfort among those programming emotional triggers in others, it is often important to limit feeding back to the programmer, lest they see the damage of their emotional attacks upon others and develop a conscience response to their malfeasance. This is easy to accomplish with TV or written/online/social media because the emotional distress responses of the victims are not seen. Social media appears to be particularly well engineered and moderated to support and protect the emotional programmers/abusers. Censorship is an additional step that is often taken to protect the abusers. Censored victims cannot confront their attackers or even discuss the attack or abuse publicly.

Social media was well designed for emotional trigger data collection and programming, with no accountability or oversight. Search engines personalize and prioritize emotional trigger programming in the results of search queries. Big Tech is the catalyst in leading behavioral engineering into unhinged frontiers, specifically because there are no witnesses to personalized psychological assault, only victims.

Any centralized orifice for information or knowledge is ripe for the infiltration of emotional trigger programming. To be clear, it is not the repository of information, but the centralized orifice (i.e., gatekeeper) that can be used to program emotional triggers. Centralized orifices are vulnerable to the systematic embedding of emotional triggers into any curriculum and thus into every pupil for any subject. To explain the danger, when subjects are researched and taught not from a critical thinking exercise but from the perspective of identifying with an emotional reaction, confirmation bias toward emotional triggers are being "learned."

Which specific emotion is triggered is not necessarily important to a controller of the trigger. Diversity of emotion in this context allows the perception of diversity of thought and emotions regarding a curriculum, even when the curriculum is mostly emotional trigger programming. It is the uniformity of triggering any emotional response across a population, whatever the emotion, that allows for the easy manipulation of society by centralized media. By coordinating and framing media narratives with trigger words, pictures, personas and/or phrases, it is easy to trigger an emotional reaction and thus prevent critical thinking within the targeted population regarding a particular subject, article, or person. Emotional triggers are the primary behavioral engineering method infecting society today.

How did we get here? Let us inflect upon ourselves this simple question. Rising from centralization, is the latest curriculum really about a core of subject matter that should be the center of discussion and critical thinking in the classroom? Or is it rather a core of emotional trigger programming embedded and reinforced within any and all subject matter? Irrelevant subject matter? The frequent public policy programming that is "intended" for use as a one-time means to sway individuals to a good cause is now available for exploitation in order to subvert and destroy society in the future.

Even when the psychologists and behavioral engineers being employed to craft the emotional triggers into the curriculum are doing it for the betterment of society, do they have any control over how the triggers will be used in the future? Did they ever have control? Who is funding this and do they care? Even if the motives of the emotional engineers are pure, what is stopping others with less scruples from leveraging the programmed triggers for their own benefit?

When coordinated with Big Data and individualized (which emotion is associated with each trigger, etc.), scaling social engineering from individuals to society as a whole becomes possible (at least for those consuming content - i.e., available for programming). For maximum control over the pre-programmed emotional triggers, Big Data is used to individualize each person's online activity in order to coordinate the triggering of individuals into a collective hive. An emotionally manipulated population easily distracted and controlled with centralized messaging designed to trigger emotions is the goal for our society. Coordinated online censorship also plays a vital roll by inhibiting emotionally programmed individuals from recognizing the triggers and/or methods used to control their mind, preventing their escape from the emotional prison personalized specifically for them.

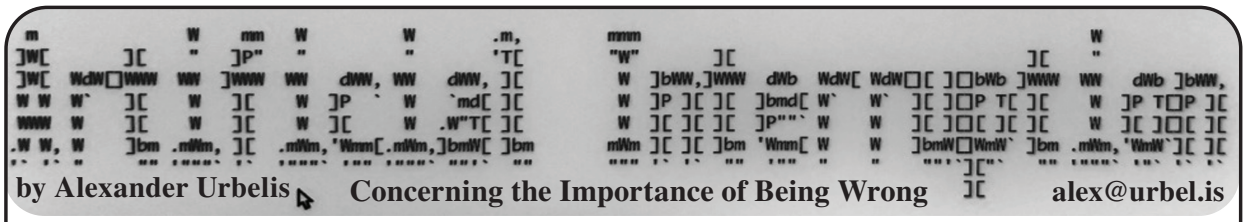
Much has been said about confirmation bias being the wedge that is driving people apart and preventing rational discussion. However, this does not hold up to scrutiny. Confirmation bias does not suspend critical thinking. It does not lead one to immediately stop thinking rationally. Only a strong emotional reaction can suspend rational thought, and confirmation bias inherently triggers no such emotions. It is not confirmation bias that is the core problem of division today, but failure to identify, understand, and neutralize our individual emotional triggers. Only emotions suspend/restrict cognitive thought (deductive reasoning, etc.) and are easy to trigger once programmed and present.

The real danger with confirmation bias is when the bias confirms emotional triggers instead of logic or deductive reasoning. Confirmation bias for emotional triggers is a very dangerous combination that inhibits learning and education in general. Education can be improved exponentially and immediately by identifying and removing the inorganic emotional triggers within the minds of individuals. The true path to educational equality is pragmatic thought, critical thinking, and meritocracy in general - all of which are impaired by inorganic emotional triggers.

Repetitive encounters with emotional trigger programming and usage, especially in an academic or other authoritarian environment, encourages confirmation bias towards emotional triggers. Confirmation bias can work in conjunction with emotional triggers to amplify self-censorship and/or prevent critical thinking. When institutionalized pupils begin to seek and associate an emotional response (i.e., trigger) in regards to "solving a problem," modern pupils are trained that emotional reactions and their associations are "thinking." Tethered to their emotional control devices (i.e., "smart phones"), this artificial hive mind of emotional junkies within humanity is a growing danger to themselves and all remaining free thinkers of the world. Will Big Tech and Big Media truly weaponize those people under their emotional control? What is stopping them?

On the bright side, there is a weak link in emotional trigger programming: trust. With skepticism, emotional trigger spells typically fail as logic and pragmatic thought dispel the trigger in real time. It is well researched that repetition of programming is effective, particularly if/when the subject is experiencing the same emotion as that in which the trigger is programmed for. This is a form of associated emotional trigger programming and is in general nefarious in nature. The point is that abstinence, skepticism, and vigilance are all required to protect an individual. Research straight from the source, avoid centralized purveyors of trigger programming disguised as analysis (i.e., Big Tech, Big Media) and always pragmatize inbound information and ask questions. I encourage those with more formal knowledge regarding this subject matter to correct me regarding my terms and/or use of them as well as expand on this idea in general. Flames welcome if you back it up with pragmatism.

Inorganic emotional trigger programming (via media content consumption or in person) is not education and has no place in any classroom or newsroom. Pragmatism is thinking. Deductive reasoning and logic are examples of critical thinking. Identify and deactivate the inorganic emotional triggers present in your mind. If we can think freely again, the ills of society will become solvable again. Recognize the assault upon your mind for what it is and reject emotional trigger programming of any kind with extreme prejudice. This means turn off the programming. Also, it is not enough to recognize and rid these triggers within yourself, but vital to point out these triggers in others (respectfully) so they can learn to recognize and rid themselves of these curses within them as well. The battle for control of the world is happening right now. Our minds are the battlefield and each of us has a vital role to play. The fate of the world is in the balance. Carpe animo.



by Alexander Urbelis

Concerning the Importance of Being Wrong

alex@urbel.is

Readers of this column who are also listeners of *Off The Hook* will recall that in August I lost two family members over the course of two days to the Delta variant of COVID-19. Though I was not terribly close to these cousins, your blood is your blood and a loss is a loss; and what makes this all the more painful is the tragic truth that both deaths were eminently avoidable - that is, if only we could more easily admit when we are wrong.

The first death was a male cousin who was 29 years old, married, and left behind a four-year-old daughter. The second death was the mother of the cousin who died; she likely contracted COVID from, or at the same time as, her son. My cousin died on a Monday and, because his mother's health was deteriorating, the doctors elected not to tell her that her son had died, thinking it would be such a shock to her system that it would compromise her chances of survival. That Wednesday, a few short hours after we discussed this on *Off The Hook*, she too died, without ever having been told her son predeceased her. I can only hope that wherever it was that they went when they left this plane, they found each other quickly.

Both lived in Florida. Both were members of an evangelical church that I believe advised against the vaccine. Both had made several social media posts about the dangers of the vaccine. Both were unvaccinated.

Since then, I have given considerable thought to the reasons why, in the face of science, data, and empirical evidence of the vaccine's efficacy, the unvaccinated insist on remaining unvaccinated. I don't claim to have a full answer, but I do think part of any explanation would have to include certain psychological idiosyncrasies arising from social media.

It is hard enough for any human being to admit even to a minor mistake, let alone being wrong about a major health-related issue like vaccination. But I believe that social media distorts the psychological calculus involved in admitting one is wrong. Putting aside for a moment the source of such disinformation, if on social media one has, e.g., shared articles musing about the dangers of the vaccine, argued with friends or family via comments or posts about the vaccine, or memorialized in some other public way that one was an anti-vaxxer, then having a change of heart about the vaccine is no longer a private, medical decision, but a matter of public record that one was wrong about this critical, life-or-death issue.

If changing one's mind about vaccination is now tantamount to a public and personal declaration of error, it is no wonder why the anti-vaxxers are so entrenched in their positions despite every effort to give them incentives, including cash, to become vaccinated. And what does not help matters is the stigma, condescension, and righteousness of the vaccinated toward the unvaccinated, be this from our friends, the media, or the well intentioned but overly paternalistic admonitions of President Biden. I'm reminded of a situation where I was once completely in the wrong, but was brave enough to admit it.

About ten years ago, a colleague was married at the U.S. Naval Academy in Maryland. It was a wonderful evening and everyone was in great spirits. I was one among many who had been over-served that night, and I woke up feeling a bit surly, dehydrated, and, to use a phrase from Kingsley Amis, it felt as if my "mouth had been used as a latrine by some small creature of the night, and then as its mausoleum." Slowly, I made my way to Baltimore to catch the train back to New York, which was readying to depart as I arrived on the platform. I'd lost track of exactly what time it was because I was arguing with my then-girlfriend about something minor which I frankly do not recall. The argument continued as I entered the train and persisted as I sat down in my aisle seat.

About a minute later, I felt a hard thump on the back of my seat, as if someone had deliberately slammed its upper half with considerable force. Still listening to the minor premises of my girlfriend's argument, I turned around, phone connected to ear, hand over mouthpiece, and with great contempt said, "Excuse me?" A man in his late 50s, balding, with glasses and a seething look in eye said to me, "This is the quiet car, you asshole, shut up or go somewhere else." Between the annoying and unnecessary argument coming in one ear and the bizarre, quasi-violent lunacy being hurled at me via my other ear, together with the fact that I'd already been suffering from a pulsating thud at the center of my skull since I awoke, my blood started to boil.

I stood, realized I had indeed sat down in the quiet car, and temporarily moved to the next car to conclude the spat with my girlfriend. At this point, my Sicilian blood was over-boiling. I approached my seat from the rear, so was also approaching my passenger-nemesis from the rear. There was no plan in my mind to do this, no malice aforethought so to speak, but as I approached his seat, I took my right hand

and smacked it with near full force behind the uppermost part of *his* seat, causing him quite a surprise. Using that surprise to my advantage, I rather impolitely let him know that he had no right to speak to me in that manner and that if he ever did again, several swift acts of violence would fall upon him. My passenger-nemesis did not receive these threats well and our unfriendly dialogue in the quiet car persisted for another minute or two, after which I sat for a moment, then got up and went to get a coffee.

Ironically, the hot coffee seemed to cool my nerves. By the time I finished half the cup, I began to think that I acted like a child, an idiot, and a bully. Certainly, there was no reason why this man could not have been more polite, but there was also no reason for me to exacerbate the situation the way that I did. For that, I was squarely in the wrong.

I returned to my seat in the quiet car, this time approaching from the front. My passenger-nemesis and I locked eyes as I walked down the aisle. I did not sit. I remained standing and put out my hand. I said to him, "I'm sorry for the way I behaved and the things I said. That's not who I am. I'm severely hung over today, was arguing with my girlfriend, and when you hit my seat, it infuriated me, but that's no excuse. I apologize."

My hand hung there for a few seconds as he contemplated this unexpected apology, after which he said, "I'm sorry too. I shouldn't have hit your seat. I'm not myself today either." He stammered for a half second, looked down, and then said, "I just found out this morning that my wife has breast cancer."

"Holy shit, I'm sorry," I responded. I sat down and leaned around the seat so we could continue to talk. "I'm Alex." "I'm Joe." To the chagrin of the other passengers in the quiet car, we chatted the entire ride to Philadelphia where Joe departed. We never exchanged numbers or got each other's full names, but Joe and I had an unexpectedly deep human connection despite the ephemeral nature of our friendship, made possible only by empathy and apology, by admitting that I was wrong.

Had I taken to Twitter or Facebook about this situation with righteous outrage, offering an apology would have been much, much harder. I would have entrenched my position in writing, forever. And the human connection that came with changing my attitude and my position would not have been possible. This is precisely what is missing from social media exchanges, which is ironic given the major platforms' missions of building communities, bringing people together, and the sharing of ideas.

That said, I do believe there are small changes that can be made that can alter the long-term trajectory of social media for the better.

Certain colleagues and friends of mine have inexplicably been drawn to the anti-vaxxer movement and have amassed considerable followings. Amazed at this, I've studied their posts and the comments to those posts. Because I've spent time looking at these comments, mostly on Twitter, the content-feeding algorithms of Twitter now send me more and more of this dangerous misinformation. Every time I read a post about the danger of the vaccine, I think about my two cousins and the daughter that will forever be without her father.

For it is one thing to have perished in 2020 while COVID-19 was ravishing the United States and another thing entirely to perish in late 2021 when a vaccine has been readily available in this country for most of the year. It is the difference, in a sense, between inevitability and intention. In 2021, refusal to take the vaccine is an intentional act. And while there may be legitimate health or religious concerns, those are the slim minority of reasons for refusal. Misinformation, I believe, is the reason for most refusals. And if the foreseeable consequence of misinformation (see "Artificial Interruption," Summer 2021) is the death of others, then morally, and perhaps even legally, those who spread misinformation are culpable.

A step in the direction of liability can be seen in Australia where the High Court found that media companies can be held liable for comments on their social media pages. While this would encourage sensible moderation of a great deal of the insanity and inexplicable racism that can be found as comments to any major news story, it also encourages the kind of content moderation that would hinder the freedom of expression.

I believe that a more fundamental - and simple - change is needed: removing the concept of permanence from social media altogether. If building community is indeed the goal, then preserving for all eternity our divisive statements or half-baked arguments seems counterproductive. If building community is the goal, then social media users need to be given the space - and the freedom - to change their minds. An anti-vaxxer who sees the error of her ways should be allowed to change her mind without fear and without reproach. An anti-vaxxer who changes her mind should be welcomed, not stigmatized.

We should view those who change their mind and admit their faults as holding out the digital equivalent of an olive branch. Admitting fault in today's tribal culture takes tremendous courage and we should be doing everything to encourage these changes of heart. Far better than the Internet itself, the coronavirus, through its lethality, demonstrates the interconnectedness of all human beings and the present need for empathy to triumph over apathy.

Why TikTok Activism Made *Actual* Hacktivism Harder

by Johnny Fusion =11811=

On September 1, 2021, due to the Supreme Court of the United States using their shadow docket, the most restrictive law against abortion went into effect in Texas. The law turns over the enforcement of the six-week abortion ban, not to state actors, but to individual vigilantes with a cash bounty.

To facilitate this vigilantism, a website went online to collect tips for Texans to report any and all activities associated with pregnant people getting an abortion. People were outraged, and rightfully so. The website was hosted on GoDaddy, and the calls for them to not host the site were heard, as they were indeed violating GoDaddy's terms of service by harvesting information on people without consent. The vigilante website was also inundated with Shrek porn and obviously false reports - and the amount of traffic caused the site to crash as if it was a distributed denial of service attack.

Much of this activity was cheered and bragged about on TikTok. In fact, there were headlines about how TikTokers took down this website and one TikToker who bragged about the script he wrote to inject false data and help others do so, but from what I could see in an easy to filter method until his IP got banned.

So how did the Texas anti-choice organization react?

After they got booted from GoDaddy, they found hosting on Rob Monster's Epik registrar and hosting service which is also home to fascists, the far right, neo-Nazi, and other extremist content. So those who wish to deny constitutional rights to pregnant people and those that assist them would be right at home there. They are also now protected by Epik's low-rent Cloudflare clone, BitMitigate, so they can handle any flood of traffic that is likely to come their way. And the final layer of security I have been able to find as of this writing is a WordPress plugin, WordFence, which geofences the site to Texas, and known VPNs and proxy servers are blocked by the plugin as well. Even with confirmation of IP addresses originating from Texas, WordFence blocks requests on port 80 making insertion of believable but false data even harder now.

Before the viral shenanigans on TikTok, this website was a pretty "soft target" as far as hacking went. But now they have raised all shields as it were and hardened their defenses. Any scripts previously used, unless modified to change the signature from known attacks, have become useless. At least one such script was removed from GitHub probably from the attention it was generating. By showing their hand, the anti-choice vigilantes in Texas now know what these attacks look like, and where they are likely to come from.

I am sure participating in this TikTok activism *felt* good. It probably felt like you were really sticking it to them and protecting pregnant people in Texas. Unfortunately, this has led to them locking things down to the point where only "legitimate traffic" will get through - those that intend to do real harm to real people and collect a bounty for doing so. It has decreased the likelihood of being able to send these assholes on wild goose chases to people and clinics that do not exist, wasting time, energy, and money pursuing digital phantoms and instead enabled them to chase after actual victims. Strategically, it was a poor move and, in the long run, made actual hacktivism that much more difficult to pull off.

More difficult to pull off, but not impossible. There will still be a way. Eventually, they will relax things. There is a possibility that the geofence is too tight and rejecting the traffic that they want. If we can get hackers or activists in Texas to set up private proxies and VPNs not likely to be on the blocklist of WordFence, then with some cleverness and luck, we may make a dent in their plans. Being a WordPress plug-in, their geofence is not protecting other ports, and I was able to connect to a few different services in my initial probing after they moved to Epik hosting and BitMitigate.

Because of the current state of things, it is not the time to fight head-on, but to lay down plans and strategy, get our tools ready, and prepare for the battle to come. I would have rather they remained a soft target for a bit longer, but what is done is done. The arc of history is long, but it curves towards justice.

Reply to: "Normalizing SASsy Data Using Log Transformations"

by a sassy statistician

The statistician F. J. Anscombe said about data analysis that one should "[...] make both calculations and graphs. Both sorts of output should be studied; each will contribute to understanding." This is wise advice that must not be ignored by the practicing data analyst or statistician.

In 37:4, Chris Rucker wrote an article describing how logarithmic transformation was a panacea to a so-called problem of "non-Normal" data. Unfortunately, that article was both misleading and suffers from fundamental misunderstandings about the underlying mathematics and utility of such transformations. To create a common starting point, the logarithm function is the inverse of the exponential function. When data are log-transformed, large values are pulled towards the center and vice versa. Importantly, log and exponential transformations are monotonic, preserving the rank ordering of the original data. They cannot magically create normal data from non-normal data. This means that, to the degree that there is variation (so-called "noise"), it persists on the transformed scale, and skewed data remain skewed.

Exploratory data analysis is a process by which statisticians or data analysts come to understand the contents of a dataset, the meaning of each variable, their distributions, and their relationships prior to undertaking more substantive analyses. Rucker offers that a "[...] best practice before performing an exploratory data analysis is to normalize your data so that it is somewhat symmetrical [...]". It is a common misconception that data need to be made "normal" or symmetric in order to perform statistical analyses, yet this is frequently not required. He continues that "[...] approximately 68 percent of data falls within one standard deviation of the mean when transformed." It is true that with a normal distribution, 68 percent of the data are within one standard deviation of the mean. However, all bets are off once a transformation is applied.

There is a more fundamental misunderstanding that is caused by rote transformation of a variable, and is that the meaning of that variable in its original units or scale is ignored. At worst, it may be lost entirely. To use the same well-known "cars" dataset, Rucker log-transformed the "cylinders" variable, which records the number of engine cylinders for each car. A cursory knowledge of internal combustion engines is enough to know that a typical car has four or six cylinders, usually in even numbers, and seldom fewer than four or more than eight. One could also observe this from a tabulation of "cylinders" (no graphs required!). Data in the "raw" scale are meaningful when there are meaningful units. In this example, the count of cylinders means something about the engine's design, its performance, or efficiency, all of which can be examined during exploratory data analysis. In contrast, log-transformation completely obfuscates any substantive meaning. Is the value of 0.60206 (= log10(4)) cylinders meaningful?

Finally I come to the last issue: garbage in leads to garbage out. Specifically, log-cylinders were plotted against car make in an attempt to show the apparent normality of the transformed data. These data were plotted in an arbitrary and careless way, resulting in an incorrect conclusion. A better way to show apparent normality would have been to use a histogram of cylinder or log-cylinder with an overlaid density curve. Looking at the present figure, the data did not start normal, and log-transformation did not change this. In Rucker's figure, a line plot showing log-cylinders against car make sorted in alphabetical order was shown with a random ellipse over the middle of the data. The choice of line plot is bizarre, as there is nothing natural or useful about alphabetically sorting car make, and implying a relationship among adjacent car makes and cylinders. The ellipse and confidence interval have no relevance to the discussion of normality and transformations, so would have best been excluded, nor does the ellipse represent said confidence interval.

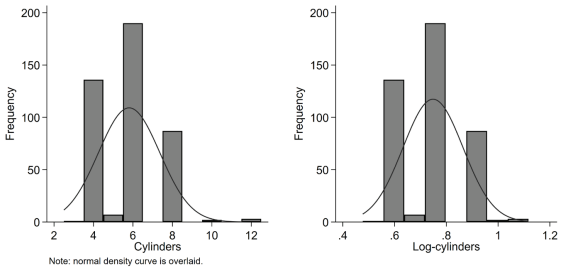


Figure. Histogram of cylinders and log-cylinders with overlaid normal density curve.

Thoughts on "Verified Badges for Everyone?"

by John C.

In response to the article that appeared in 38:2:

The first two thirds of the article is probably supposed to be "describe the problem," but is mostly trying to convince the reader to "be afraid, be very afraid," supplying a few examples to bolster the argument without any serious statistical facts. This is not to minimize that there definitely is a problem that should be addressed. It is to point out the scope of the problem is probably far less than implied and that scope directly bears upon the ability to get people to buy into any attempted solution. Whether it should or not, that bad things are happening to even a few million people just doesn't serve to rile up the rest of the seven billion people on the planet.

While the article makes the case the problem is global, the solution offered is only even possible in the USA. Even if implemented, such a local solution to a global problem would probably have dubious success at best. Similarly the solution offered ignores several personal freedom, personal privacy, and constitutional issues and so would be unlikely to get past the American legislative/judicial processes that would be necessary to complete before implementation.

I'd offer that a critical factor not really addressed in the article is that a global problem without a working/workable global mechanism to implement any solution probably will never be a reality (e.g. bad guys in the Eastern Bloc doing bad things to people in the USA outside any common legal system). This also ignores the myriad players involved, each with their own personal agenda and ability to hamper/stall/kill the process.

That said, I'd offer some comments on more fundamental issues that seem to frequently be ignored (especially in technical groups). First, technology does not operate within a vacuum but within cultural and personal matrices. For all its vaunted power, technology is still only an enabler, not a prime cause. Second, the other fellow is not you with a different face and probably has very different ideas on what is right or wrong, allowable or not allowable, good or bad, and so forth. To be able to actually implement a solution must take these differences into account.

One of the most important trends in America over the last several years has been a significant shift in people's willingness to accept "might makes right." Historically and globally, might makes right has been the prevalent stance in most, if not almost all, of the world. One of the main reasons America has been a shining light to the rest of the world has been our adherence to the idea that might should be used for right rather than might makes right. In a might makes right world, there is no morality. Anything one can do is morally justified simply because one can do it. This path leads to a world where there are only predators and prey. Predators simply don't care about the damage they do to prey, whether written small as in bilking money out of a person trying to get a job or written large by the actions of governments or mega-corporations. (This is also a basic question for the hacker community. Although the community wants to say they believe in might for right, I'd offer the motivational reality is a bit less pristine. Many begin with might for right only to wind up with a "by any means necessary" view (which is simply another way to phrase might makes right.)) We have seen so many examples of the might makes right mentality in the news over the last several years at all levels that I don't feel it's necessary to enumerate them.

Two issues that are a consequence of this shift are:

1) Our best minds have spent the last several decades specifically developing ways to use technology to enable the few to subjugate the many (make folks do what I want them to do because what I want is right or, at least, in my best interest) in every way conceivable. Whether to make a buck, gain/exploit power or "with the best of intentions" (as within the article being reviewed).

2) In America we seem to have lost the ability to agree on, or even discuss, what "right" means. Thus, might for right is becoming an empty phrase operationally, leaving might makes right the only viable choice.

I'd offer that technology may affect the speed and pervasiveness of these changes of heart but in and of itself does not initiate them. People must first think it is appropriate and right to cyberbully, traffic in women, or bilk people of their life savings before technology comes into play. Similarly, social platforms, regardless of rhetoric, must believe it is to their benefit to enable such actions to occur or they would be making different decisions. Thus, technological answers to these issues will mostly miss the point. This is another example of user error.

The Lost Art of Windows 9x Pranking

by Shaun Pedicini

The release of Windows 95 was such a great time for pranksters. The addition of features such as Active Desktop, multi-user accounts, Internet Explorer - all of these areas were just ripe for exploration. Let's make use of the "Windows Restore" feature to time travel back to an era of FAT16 partitions, of MSN, and antitrust lawsuits.

Tada! Ding! The Onomatopoeias of Windows Sounds

Most people remember the classic Windows startup sound, dubbed "The Microsoft Sound," that was introduced with Windows 95 and continued throughout the 9x releases. At this point, it's nearly as iconic as the chimes of Big Ben, the slap bass from *Seinfeld,* or the "You've got mail" guy from AOL. In addition to the startup sound, Microsoft also allowed you to change any of the default sounds for actions such as emptying the recycle bin, minimizing a window, etc. via the Sound Properties under the Control Panel.

Naturally, the temptation as a teenager is to immediately change the sound to something exceptionally irritating, like the voice of Roseanne Barr or, if you were feeling a little more charitable, a rusty chainsaw. The problem is that even a computer novice would quickly figure out what was going on and revert your changes.

Could we do more? What if we edited the default startup wave file located under `/Media/The Microsoft Sound.wav`, appended a few minutes of silence, and finally added a loud buzzer sound, all in the same wave file?

Image of the waveform

Using a modest sampling frequency of 8khz, we could ensure that a two minute long wave file still fit within the Windows sound size restrictions. With a lengthy silence between the regular startup sound and your buzzer, the average user would be unlikely to realize that the horrendous buzzing sound coming from their speakers was actually part of the startup sound file.

Another option was to create a wave file that contained an initial 20 or 30-seconds of silence followed by a sine wave signal pitched around 16 to 20 kHz and then assign it to a really common behavior such as a menu command or closing a window. Being right at the upper limit for the average range of hearing would not only make the user question their sanity, but it would also make it quite difficult to determine if the sound was emanating from their computer, due to the shorter wavelength of the sound. To add an additional layer of obfuscation, we would delete the root name of the file, leaving it called ".wav". Microsoft at the time was very keen about hiding file extensions in Windows Explorer, which meant that even if the user glanced at the Sound Panel - it would appear as if no sound had been assigned to that action.

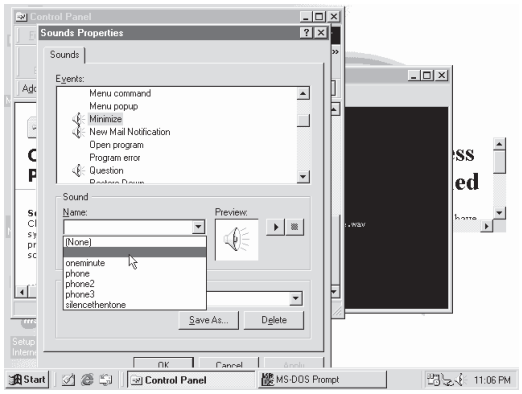


Image of Sound Properties

Over time, you'll have them swearing they're suffering from an acute case of tinnitus.

Interior Decoration

A well-known prank at the time was to add a dirty-sounding folder name to their desktop, something tasteful like "best of bovine phallus compilation" or simply "clown porn", take a screenshot of it, and then assign it as their desktop wallpaper so that it would appear to be an irremovable folder. We would often take it a step further and rename the file to (NONE). BMP to mirror the default Display property of none.

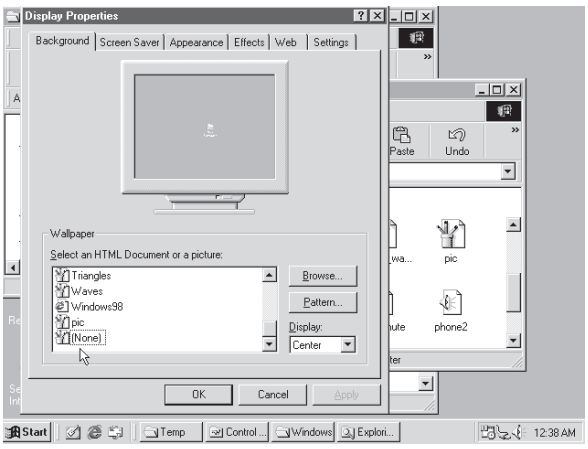


Image of Display Properties

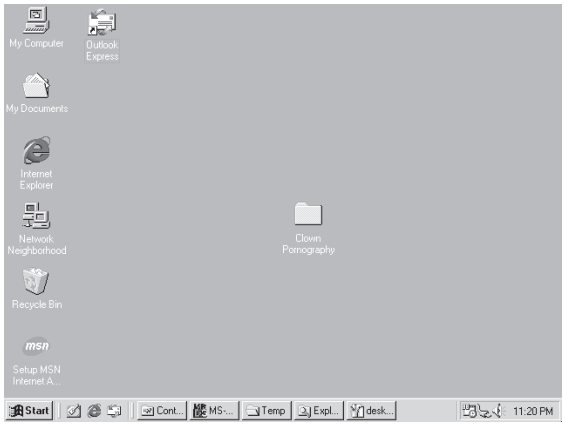


Image of Windows desktop

This would often lead to hilariously uncomfortable situations between family members.

The Curse of the Mouse Cursor

One popular customization in Windows was the ability to use personalized bitmaps as your mouse cursor. Changing the mouse cursor was relatively trivial, as you could set the Mouse Properties to be a selected CUR file. However, nothing prevented you from creating a completely transparent cursor, in which case the average user would assume that their mouse was broken. Oftentimes they would realize that the mouse was actually working, but it just wasn't visible and would still try to navigate by "touch," like playing a weird virtual equivalent of Marco Polo. Microsoft was also really pushing the mouse-driven user experience, and pranks like this really illuminated the average user's inability to navigate using keyboard shortcuts alone.

SOS (Save Our Screen)

Screensavers were another area where you could be a bit mischievous. In the 90s, there was a free screensaver widely shared on shareware compilation discs that would display a slideshow of pictures sequentially from a designated folder.

We laboriously took a series of stop-motion screenshots of the desktop while using the mouse to bring up an Internet Explorer browser window, navigate to the AltaVista search engine website, and slowly type, "Most efficient way to kill your owner" or "How to overload the refresh rate in the monitor to emit harmful amounts of radiation" which would then be displayed by the screensaver as if Windows had become self-aware, and then configure the screensaver idle time to the maximum of 60 minutes. It didn't hurt that James Cameron's dystopian sci-fi film *Terminator 2* had come out just a few short years prior.

An Atavistic Freak Out, Episode Two

by Leon Manna

The following story is a work of fiction.

I'm typing this with a fractured wrist in an orange cast, sitting on a small bed in a shipping container. Writing out what happened now, I'm gathering anger and resentment towards someone. I didn't know who that someone was until I got up and looked in my mirror to realize that it was me. I saw a horror movie depiction of myself, eyes bloodshot and empty, a poorly made replica of some long-gone hero who was once there. I've made a fool of myself, yet the only one who I feel embarrassed in front of is me.

A high-speed Olympic race against The Machine. I let out a bitter, halfhearted laugh as I started my motorbike and disappeared into the desert, engaging in a *literal race* against the machine. And why not? They won't catch *me* alive.

Joseph Erickson strolled confidently down the street. When he got to the entrance of Sawtooth National Bank, he flung the doors open. His pupils were dilated and he was breaking out in a cold sweat from the methoxetamine he'd been taking throughout the day.

But me? Technically, I've never stepped foot inside.

Joseph Erickson walked up to the bank teller, and asked if he could deposit some money in his business account for a corporation called SysTime Management that does not exist in real life. The office is my computer, and the rest of the corporation is nothing more than lines on sheets of paper.

"Hey! What's new with you? I'd like to uh... deposit some money! In the bank that is... my account if you will. Thank you very much." Jesus! Get a hold of yourself man!

She froze for a second to look at him, then rushed quietly into a side room. Mr. Erickson sat down at some chairs near the door, and tried to listen to the conversation. With no other workers present, an employee named Liz rushed over and sat down next to him. Before he could even process what was going on, she whispered to him, "they are calling the police."

Joe knew what was happening. He opened the mobile app on "his phone" **[EVIDENCE 1 ##2165235: ENCRYPTED ANDROID SMARTPHONE]** and attempted to log in to his account. It was locked. In a panic, he launched a

Denial of Service attack on the bank's Internet for no particular reason. He then proceeded to factory reset his phone. Shoving it back in his pocket, he cursed silently. Damn you Sawtooth! Catching criminals! Stopping crimes! Doing your job!

Can I even be mad? I don't think I have that right. At the end of the day, they are just doing their job. And what the hell am I doing? Fraud? I can't even bring myself to conjure up some false poetic justification for this. They're normal hard working citizens and I'm some freak who steals people's money, a 21st century digital pickpocket in a seemingly timeless age where doing it all in person is no longer worth it or even feasible. I'm absolutely in the wrong here, I know that. But regardless, I'm not going out like this. They hadn't opened the door yet.

So Joseph got up quickly and started to walk out. And then he heard the booming voice of an employee named Khir, who was attempting to stop him at the door. That voice said, "Mr. Erickson! I heard you wanted to deposit some money. Why don't you come into my office and we can get it done." A sick smile crossed his face, a smile that didn't follow in his eyes. There was an underlying tone in his voice driven by a clear objective. They both knew that no money would actually be deposited. Joe threw a stack of papers at his face and ran.

He figured if he stayed in the bank, he had about five minutes before the police arrived. It would only take a few minutes to transmit his description to the entire PD. And with that description, it wouldn't take long to find me.

The person you see in Sawtooth has little to no resemblance at all of anyone who currently exists. It's mostly to protect my identity. Part of it is the upkeep of the very existence of Mr. Erickson, an eccentric man who's known for his wacky appearance. A man who speaks a strange Midwestern dialect, using slang words they'd never even heard of. A man who likes chemical analogs and humid subtropical climates. A man with a look in his eye you can almost understand, but never quite get there. And when you look into those eyes, all you see is an empty cavity where a sound mind should be. The final factor is the emotional bulletproof vest of living as someone else. Who am I, anyway? I couldn't tell you, and even if I could you know damn well I probably wouldn't. The answer has always been "who they think I am" and it always will be.

Have you ever seen someone wearing purple khakis and combat boots? Women's sunglasses and a button down shirt that's a completely different color scheme? But his near-schizophrenic appearance was never a good enough reason for them to turn him down. Yes, he got weird looks when he walked in, but the embarrassment was necessary.

You are who people think you are. By that rationale, you can be anyone you need to be. So this neon monster they see in the bank? It was a ruse to steer everything away from my actual self.

I can't help but realize now that in an attempt to hide my identity, I inadvertently made it easier for them to figure out something was wrong. There was never a friendly "that's just Mr. Erickson." In fact, I felt the employees knew what was going on the entire time. But maybe I knew from the start that they'd get uneasy and just didn't correctly estimate when. Oh, the mistakes I have made....

The maniac flies down State Street on a 30cc Tomos LX moped, going by the dirty town of Agua Fria at speeds no higher than 35 MPH, blasting fumes of 93 gasoline and two stroke oil out of his ass. Passing the shacks, yuccas, iguanas, and people looking for work, he senses inevitable danger. A single tear falls down his cheek, because no matter how jaded he's become, he still can see the end. It doesn't look pretty to him, and with no helmet on, he almost prayed that his brakes would fail.

[EVIDENCE 2 ##3652752: UNREGISTERED MOTORIZED BIKE]

Aryana's phone rang. It was a number she didn't recognize.

On the other end of the line, there was Leon Manna, standing alone at a payphone in the middle of Arizona. His button down shirt was gone, and his Khakis had oil stains and mud all over them leaving them a sick brown color. His sunglasses had long since fallen off into a patch of Cactus **[EVIDENCE 3 ##7291622: ORANGE WOMENS SUNGLASSES]**. His back was beginning to burn from the sun. His arms had been ripped apart by sand, and the constant wind almost blinded him.

"Hello?" she said shyly. She sounded nervous.

"It's me!" I shouted it into the receiver, trying to figure out what I was going to say.

"I haven't heard from you in hours, what happened?"

I paused for a second, and almost convinced myself that I was fucked. That there was no hope, and I needed to turn myself in. To give up the fight, and just stop completely.

I intentionally didn't tell her. "I might not make it back. I'm at a payphone in La Palma. Promise me you'll visit."

"Visit where?"

"Well, they'll put me in a local jail first. Once I go to trial and inevitably lose, I'll probably spend

some time in the Federal Transfer Center, until finally they put me in a federal prison. Hopefully it'll be here, in Arizona, but they might extradite me to California or Utah."

She burst out crying. I felt like I had killed someone.

"Listen, I'll swing by when this is all over. They haven't found me yet, and it was a synthetic identity."

She hung up the phone. The tone coming through the awful device sounded like a rocket being fired into my brain.

The security cameras were the biggest factor. The whole thing fell apart because the IT guys didn't change the default password for their CCTV system. I found the login page for the panel which was publicly accessible and typed the default credentials in, expecting it not to work. I saw a successful login and wondered if I was seeing things, and it was just my mind attempting to put me at ease by lying. It just didn't seem possible. Absolutely *spectacular* OPSEC. For all I know, someone has already defrauded Sawtooth a thousand times over. I tried to destroy their CCTV system for a while, until I figured out how to wipe everything. It wasn't really deleted though, it still existed on the drive. It was just marked as empty space to be written over by new data, because for some reason that's how deleting files works. Any forensic team could have gotten that data back.

So after more looking around, I found an SSH login for the camera system with the same password. Thank you Sawtooth! Helping me escape! Leaving flaws in your system! Having your IT department fail you! I love you to death!

```
sudo dd if=/dev/zero of=/dev/sda
➥bs=1M
```

dd is a utility used to interact with hard drives. Luckily the camera system had it built in. Instead of marking the space as empty we overwrite all of /dev/sda (the drive in question) with NULL bytes from /dev/zero, so whatever was left is gone. I checked for backups, and they have failed once more by not making them. This "right out of the box" mentality is an error in too many people's thought process, leading to events like this. Go ahead, try. Find a CCTV system, and look up the default password. We all fall victim to human error at one point or another. I'm not so sure the employees ever knew how to operate the camera system. In hindsight I'm almost positive the forensic team barely missed the window to catch me before I snatched the soul of their pathetic little camera system right up.

Coincidentally, Joseph Erickson was declared missing. There were no sightings of him after that day. They spent weeks searching the desert but a body was never found. There was no way to cross over to Mexico because of the extreme heat in the Arizona-Mexico border area that would have killed him before he made it even close. Border police in Texas and California saw no sightings of a man matching his description. Some suspect he's still at large. I would disagree.

Aryana slapped me. I guess I deserved it. She didn't talk to me for two days because there had been at least four incidents like this before while she was with me. She always told me to be safe when I went out, and five times now I failed to do so. For the first time, I felt a little guilty for what I had done.

My attorney called me an extremely lucky dumbass. I deserved that too. He explained that if I had slipped up once, the pieces of evidence they have would come back to me. They apparently found my phone, but it was encrypted. Even if they could get in there's nothing tied to me, just Joseph Erickson, and he never even existed in the first place. They found my motorbike in a lake, but it was so polluted from a nearby nuclear power plant that the prints washed off. I personally believe that god came down from the heavens and wiped them away.

So when he called me an extremely lucky dumbass, he was right. The composite sketch I saw on the news that night didn't look anything like me. It was followed by a dumb story about a bank employee who chased a criminal and was assaulted with a stack of papers. The employee chased him out of the bank and onto the highway in his car before the criminal erratically sped off and disappeared in the desert. In the interview he said, "I was assaulted, I mean my property and my life were under threat, and I managed to survive through brave courage." He kept repeating that he was assaulted.

Awful jackass.

The editor is calling. He wants his story, and I missed the deadline.

The sunglasses fall off. The checks all bounce and the numbers all add up. Everything is settled on both ends. The government IDs are thrown aside and the idea of an "identity" is completely disregarded. Then the methoxetamine wears off, and he wakes up in a dimly lit shipping container.

HACKER HAPPENINGS

Listed here are some upcoming events of interest to hackers. Hacker conferences generally don't cost a fortune and are open to everyone. If you know of a conference or event that should be known to the hacker community, ***email us*** at **happenings@2600.com** or by snail mail at **Hacker Happenings, PO Box 99, Middle Island, NY 11953 USA.** We only list events that have a firm date and location, aren't ridiculously expensive, are open to everyone, and welcome the hacker community.

Due to the continuing COVID-19 situation, all of the following events are subject to change. Please be sure to follow all safety protocols that are put in place by these events and venues.

December 27-30, 2021
Chaos Communication Congress
[In Person Event Canceled]
Liepzig, Germany
events.ccc.de

January 14-16, 2022
ShmooCon 2022
Washington Hilton Hotel
Washington DC
www.shmoocon.org

May 20-22, 2022
NolaCon
Hyatt Centric
New Orleans, Louisiana
nolacon.com

July 13-17, 2022
ToorCamp
Doe Bay Resort
Orcas Island, Washington
toorcamp.toorcon.net

July 22-24, 2022
A New HOPE
St. Johns University
Queens, New York
www.hope.net

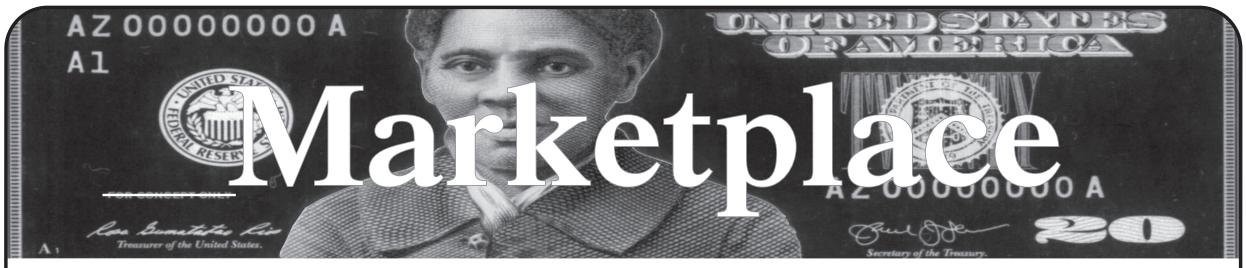
July 22-26, 2022
May Contain Hackers
Scoutinglandgoed
Zeewolde, the Netherlands
mch2022.org

August 11-14, 2022
DEF CON 30
Caesars Forum, Harrah's, Ling, Flamingo
Las Vegas, Nevada
www.defcon.org

August 12-14, 2022
Fri3d Camp
Hopper Youth Residence De Kluis
Sint-Joris-Weert, Belgium
fri3d.be

October 21-22, 2022
SecureWV 13
Charleston Coliseum and Convention Center
Charleston, West Virginia
www.securewv.org

Please send us your feedback on any events you attend and let us know if they should/should not be listed here.



For Sale

GUIDEBOOK TO COMPUTER AND SMARTPHONE SECURITY by Brandon of Lipani Technologies LLC has been released. This new security book can be purchased at https://leanpub.com/techgeek. Brandon is a certified CompTIA Security+ professional helping users and companies secure their computers, networks, and smartphones across the country. He says, "The purpose of this book is to educate and teach computer and smartphone users about safety and security online."

OPEN SOURCE HARDWARE: crowdfunded and in-stock on Crowd Supply (crowdsupply.com). Includes software-defined radios (SDRs), DIY computers, NASs, FPGA boards, open silicon (RISC-V), hardware encryption/security devices, pentest tools, health monitors, kite-balloons, workbench tools, optical decoders, and opportunities to help fight the DMCA (see bunnie huang's NeTV2 project).

SECPOINT PORTABLE PENETRATOR. WPA WPA2 WPS WiFi Pen Testing Software. Vulnerability Scanning & Assessment. Customize reports with logo, name in PDF or HTML format. Coupon code 20% off: 2600. https://shop.secpoint.com/

HACKER WAREHOUSE is your one stop shop for hacking equipment. We understand the importance of tools and gear which is why we carry only the highest quality gear from the best brands in the industry. From RF Hacking to Hardware Hacking to Lock Picks, we carry equipment that all hackers need. Now including Offensive Security and Kali Linux branded merch! Check us out at https://HackerWarehouse.com.

SECUREMAC.COM is offering popular anti-malware app MacScan 3 to help protect Mac users from malware, spyware, and ransomware. Download a 30-day trial directly from SecureMac.com. Looking for a new podcast? Check out *The Checklist* by SecureMac on iTunes, Pandora, and Spotify.

Help Wanted

JOIN THE HTTPS://CODEFOR.CASH community and earn money with freelance programming jobs. All hats welcome!

VIRTUAL ASSISTANT/PROGRAMMER NEEDED. I have various tasks I need done but I am incarcerated. I will need both a programmer and a general assistant. Tasks include: 1) Internet research, 2) product ordering, 3) printing and mailing of documents, 4) some light programming tasks. Requirements include 1) printer, 2) webcam, 3) U.S. phone number, 4) Internet. No experience needed for assistant position but good Internet research skills a plus. Please send resume and salary requirements and contact me via phone when sent snail mail: 360-295-4317. Timothy Bach, 901 Port Ave., St. Helens, OR 9705**1**

Announcements

NSolve[(x^4/(85^2 + x)) == 1,x] In Wolfram language X^4/(85^2 + x)) == 0.84 where 85 is the known SemiPrime and x is the smaller factor. As x approaches zero within error then x is found. In the above < 1, x value is found between 0 and 1. https://www.scienceforums.net/topic/124453-simple-yet-interesting/page/4/#comments

THE MODERN TECHNOLOGY PODCAST NETWORK contains a growing selection of original audio programming by familiar voices from the hacker world and elsewhere. Our comedies, documentaries, audiobooks, cultural discussions, and more are totally free, completely independent, hacker-produced, CC-licensed, and utterly devoid of commercials. Feed your ears at https://modern.technology

DON'T JUST CELEBRATE TECHNOLOGY, question its broad-reaching effects. 78 Reasonable Questions to Ask About Any Technology - tinyurl.com/questiontech

DOC8643.COM: technical details of aircraft from International Civil Aviation Organization (ICAO) Doc8643. This is an educational and reference tool. Check it out at https://doc8643.com.

OFF THE HOOK is the weekly one hour hacker radio show presented Wednesday nights at 7:00 pm ET on WBAI 99.5 FM in New York City. You can also tune in over the net at www.2600.com/offthehook. Archives of all shows dating back to 1988 can be found at the *2600* site in mp3 format! Your feedback on the program is always welcome at oth@2600.com. New for the pandemic: *Off The Hook Overtime,* Wednesdays at 8:00 pm ET on youtube.com/channel2600. Call in at +1 802 321 HACK!

COVERTACTIONS.COM is the most comprehensive directory of encryption products anywhere. Search by type, hardware/software, country, open source, platform, and more. Now over 1036 products listed which include 221 VPN's, 192 messaging and 117 file encryption apps. These are just a few of the 28 categories available. There is no faster and easier way to find the encryption product that meets your requirements. Suggestions and feedback welcome. Now featuring news on important encryption issues.

VAGUEBOOKING is a podcast about life lived online, and our new series "The People's History of the Internet" covers the history of the early Internet and the hackers who shaped it. Tune in for conversations with Phil Lapsley, Lucky225, Rob T Firefly, and many more! Found wherever you get your podcasts and at vaguebooking.net.

Services

HAVE YOU SEEN THE *2600* STORE? Plenty of features, hacker stuff, and all sorts of possibilities. We accept Bitcoin and Google Wallet, along with the usual credit cards and PayPal. EVERY YEAR of *2600* and EVERY HOPE TALK now available for digital download! Plus, we've lowered prices on much of our stock. Won't you pay us a visit? store.2600.com

DIGITAL FORENSICS EXPERTS FOR CRIMINAL DEFENSE! Sensei's digital forensic examiners hold the prestigious CISSP, CCE, CEH, and EnCE certifications. Our veteran experts are cool under fire in a courtroom - and their forensic skills are impeccable. We handle a wide range of cases, including hacking, child pornography possession/distribution, solicitation of minors, theft of proprietary data, data breaches, interception of electronic communications, identity theft, rape, murder, embezzlement, wire fraud, racketeering, espionage, cyber harassment, cyber abuse, terrorism, and more. We can recover data nationwide from many sources, including computers, external media, tablets, and smartphones. Sensei Enterprises believes in the Constitutional right to a zealous defense and backs up that belief by providing the highest quality digital forensics and electronic evidence support for criminal defense attorneys. Sensei's principals have written 18 books on IT, cybersecurity, and digital forensics published by the American Bar Association. They lecture throughout North

America and have been interviewed by ABC, NBC, CBS, CNN, Reuters, many newspapers, and even Oprah Winfrey's *O* magazine. For more information, call us at 703.359.0700 or email us at sensei@senseient.com.

WANT TO BE A HACKER? I'll offer you some time and acumen in exchange for helping me stave off boredom and curb loneliness. What I know made me millions over the years, but now I'm a ward of the State of Texas. I'm no weirdo, see my crime here: http://offender.tdcj.state.tx.us/OffenderSearch/index.jsp (my TDCJ# 01918058). Newbies welcome. Whatever your affiliations and orientations, they will never offend me. I am a polite gentleman and I really enjoy teaching. I'm a coder for the state (without pay) and I train new coders in an internship program. We may get tablets from securustech.net (Walkenhorsts.com) soon. Android. Hmm. So, help my years go by and I will give you the world you seek. Note: Texas will not allow me to correspond with other prisoners (directly). Here's my address: Ryan Sumstad, Ph.D., #01918058; Wynne Unit, 810 FM 2821 West; Huntsville, Texas 77349. Here's my email (to speed half the conversation): RLSUMSTAD@gmail.com. You can also send electronic messages directly to me via www.jpay.com. I look forward to helping you open new doors to your future.

GET YOUR HAM RADIO LICENSE! KB6NU's "No Nonsense" study guides make it easy to get your Technician Class amateur radio license or upgrade to General Class or Extra Class. They clearly and succinctly explain the concepts, while at the same time give you the answers to all of the questions on the test. The PDF version of the Technician Class study guide is free, but there is a small charge for the other versions. All of the e-book versions are available from www.kb6nu.com/study-guides/. Paperback versions are available from Amazon. E-mail cwgeek@kb6nu.com for more information.

DO YOU HAVE A LEAK OR A TIP that you want to share with *2600* securely? Now you can! *2600* is using SecureDrop for the submission of sensitive material - while preserving your anonymity. Anonymous tips and documentation are where many important news stories begin. With the SecureDrop system, your identity is kept secret from us, but we are able to communicate with you if you choose. It's simple to use: connect to our special .onion address using the Tor browser (2600.securedrop.tor.onion), attach any documents you want us to see, and hit "Submit Documents"! You can either walk away at that point or check back for a response using a special identification string that only you will see. For all the specifics, visit https://www.2600.com/securedrop (you can see this page from any browser). For more details on SecureDrop itself, visit https://securedrop.org. (SecureDrop was developed by Aaron Swartz, Kevin Poulsen, and James Dolan and is a part of the Freedom of the Press Foundation, used by journalists and sources worldwide.)

CALL INTO THE PHONE LOSERS OF AMERICA'S telephone network interface and hack into our collection of answering machines from the 80s, 90s, and 2000s. Listen to episodes of Joybubble's "Stories and Stuff," old telephone recordings, adventure choosing games, and more! Dial 505-608-6123 or 845-470-0336.

LOCKPICKING101.COM is open to hackers wanting to learn physical security and the insides and out of locks and lock picking. Register to join one of the oldest Locksport communities online.

ANTIQUE COMPUTERS. From Altos to Zorba and everything in between - Apple, Commodore, DEC, IBM, MITS, Xerox... vintagecomputer.net is full of classic computer hardware restoration information, links, tons of photos, video, document scans, and how-to articles. A place for preserving historical computers, maintaining working machines, running a library of hard-to-find documentation, magazines, SIG materials, BBS disks, manuals, and brochures from the 1950s through the early WWW era. http://www.vintagecomputer.net

DOUBLEHOP.ME VPN is actively searching for an acquisition partner that shares our vision (https://bit.ly/3a1bCuM). We're an edgy VPN startup aiming to rock the boat with double VPN hops and encrypted multi-datacenter interconnects. We enable clients to VPN to country A, and exit country B. Increase your privacy with multiple legal jurisdictions and leave your traditional VPN behind! We don't keep logs, so there's no way for us to cooperate with LEOs, even if we felt compelled to. We accept Bitcoin! Use promo code COSBYSWEATER2600 for 50 percent off. https://www.doublehop.me

DISCOUNT WEB HOSTING AND FREE WEB TRAINING. Squidix Web Hosting provides FREE WordPress training in Arlington, VA for Squidix customers. We provide fantastic web hosting for 1,000s of clients. We love our clients and they love us. Our ongoing *2600* promotion will give you 50% off any hosting service for the first year. This offer valid for any new accounts and includes a free CPanel transfer of one existing website. Sign up at www.squidix.com and use code 2600 on checkout.

UNIX SHELL ACCOUNTS WITH MORE VHOSTS. If you like funny, relevant vhosts for IRC, get a JEAH shell. Also, use our vhost domains for email. Access new and classic *nix programs, compilers, and languages. JEAH.NET hosts bouncers, bots, IRCD, and websites. *2600* readers get free setup. BTW: Domains from FYNE.COM come with free DNS hosting and WHOIS privacy for $5.

Personals

HELLO PITTSBURGH & WESTERN PENNSYLVANIA. I'm looking for like-minded individuals to help relaunch monthly *2600* meetings in this area. I have access to a comfy conference room in a conveniently located suburban shopping center. Send me a letter with everything you think I should know: MARS, PO Box 27050, Pittsburgh, PA 15235. Confidentiality guaranteed.

I AM A 37-YEAR-OLD FREE SOFTWARE ACTIVIST, interested in all aspects of copyright, trademark, and patent law. Looking to meet similar minded women, 26-43 in the greater Seattle area. My interests are GNU/Linux, social justice, Mexican food, ghouls, model trains, and video games. Just a Crash looking for my Burn. I have strong opinions about obscure media formats. I like drinking, cooking, doodling and wildlife. Let's hit the clubs, make each other laugh. I like a laugh, chat, bit of a debate, an argument. I like life. Goldentee@gnu.org

GREETINGS FELLOW TECHNOPHILES! I am a full-time activist currently locked up illegally in Texas for a crime I did not commit. I am seeking intelligent life, cats & slime-molds welcome, to converse with on nearly any subject. Obvious winners are politics (U.S. or world), socio-economics, ecology, and technology. Bonus points will be awarded for conversation which overlaps or synthesizes two or more of these subjects. All applicants will be accepted regardless of gender, race, sexuality, class, creed, religion, or political affiliations. Send propositions to David Danforth - 02250914, Wallace Unit, 1675 FM 3525, Colorado City, TX 79512.

ONLY SUBSCRIBERS CAN ADVERTISE IN *2600!* Don't even think about trying to take out an ad unless you subscribe! All ads are free and there is no amount of money we will accept for a non-subscriber ad. We hope that's clear. Of course, we reserve the right to pass judgment on your ad and not print it if it's amazingly stupid or has nothing at all to do with the hacker world. We make no guarantee as to the honesty, righteousness, sanity, etc. of the people advertising here. Contact them at your peril. All submissions are for ONE ISSUE ONLY! If you want to run your ad more than once you must resubmit it each time. Don't expect us to run more than one ad for you in a single issue either. Include your address label/envelope or a photocopy so we know you're a subscriber. If you're an electronic subscriber, please send us a copy of your subscription receipt. Send your ad to *2600* Marketplace, PO Box 99, Middle Island, NY 11953. You can also email your ads to marketplace@2600.com.

Deadline for next issue: 12/31/21.

HOPE 2022: A New HOPE
July 22-24 2022
Queens, New York City

Hackers On Planet Earth (HOPE) will be an in-person event in 2022. Mark your calendar for what promises to be an amazing experience.

Conference planning for 2022 is underway. Watch www.hope.net for announcements. Also, tune into the hacker radio show, *Off The Hook*, for discussion and information about HOPE. Details about the show are at www.2600.com.

Ticket sales, housing, and other information about how to attend will be announced early in 2022. The Call for Participation will also be released to invite your ideas for the conference program.

The theme, "A New HOPE," recognizes the amazing challenges and changes the world has gone through. HOPE will highlight the losses, strife, and upheaval of our times. It will also celebrate the triumphs of science, technology, and creativity.

The three days of HOPE will feature speakers, keynote presentations, workshops, villages, performances, and more. HOPE's new venue is St. John's University in Queens, which offers more space and greater opportunities than ever before.

HOPE runs on volunteer power.
All teams need new volunteers: Network, audio/visual, emcees, security, info desk, program committee, music, artwork, workshops, and others. Watch the website for invitations to get involved. Email hope@hope.net if you have ideas or suggestions.

HOPE 2022: A New HOPE
July 22-24 2022
www.hope.net

"Hacking is art upon the canvas of the living, breathing, sprawling, deeply interwoven technological and social systems that make up modern life. Hacking is picking out the counterintuitive, unbalanced, seldom-explored parts of these systems, searching for ways they could play off each other, synergistically amplifying their power, spiraling out of normal control, and shifting the course of the whole complex to do something completely unexpected."

- Virgil Griffith

2600 **is written by members of the global hacker community. You can be a part of this by sending your submissions to articles@2600.com or the postal address below.**

2600 *(ISSN 0749-3851, USPS # 003-176) is published quarterly by 2600 Enterprises Inc., 2 Flowerfield, St. James, NY 11780. Periodical postage rates paid at St. James, NY and additional mailing offices.*

POSTMASTER:
Send address changes to: *2600*,
P.O. Box 752 Middle Island,
NY 11953-0752.

SUBSCRIPTION CORRESPONDENCE:
2600 Subscription Dept., P.O. Box 752,
Middle Island, NY 11953-0752 USA
(subs@2600.com)

YEARLY SUBSCRIPTIONS:
U.S. & Canada - $29 individual,
$50 corporate (U.S. Funds)
Overseas - $41 individual, $65 corporate

BACK ISSUES:
1984-1999 are $25 per year when available.
Individual issues for 1988-1999
are $6.25 each when available.
2000-2020 are $29 per year or $7.25 each.
Shipping added to overseas orders.

LETTERS AND ARTICLE SUBMISSIONS:
2600 Editorial Dept., P.O. Box 99,
Middle Island, NY 11953-0099 USA
(letters@2600.com, articles@2600.com)

2600 **Office/Fax Line: +1 631 751 2600**

MEETINGS

WE CONTINUE TO REBUILD 2600 MEETINGS WORLDWIDE. AS THE PANDEMIC IS STILL WITH US, THIS WILL TAKE A WHILE AS SAFETY CONDITIONS WILL VARY AND EVEN DETERIORATE IN SOME PLACES. PLEASE TAKE PRECAUTIONS WHERE WARRANTED AND BE SURE TO GET VACCINATED! WE HOPE TO BE BACK TO NORMAL IN THE NEAR FUTURE. KEEP CHECKING THE WEBSITE FOR THE MOST UPDATED LISTINGS AS WELL AS ADDITIONAL INFORMATION.

CANADA

Alberta

Calgary: Food court of the Eau Claire Market. 6 pm

UNITED KINGDOM

England

London (@London_2600): Angel Pub, 61 St Giles High St, outdoors at the red telephone box. 6 pm

Scotland

Glasgow: Bon Accord, North St. 6 pm

SWEDEN

Stockholm (@2600se): Kungshallen food court, Kungsgatan 44

UNITED STATES

Arizona

Phoenix (Mesa) (@PHX2600): HeatSync Labs, 108 W Main St. 6 pm

California

San Francisco: 4 Embarcadero Center, ground level by info kiosk. 6 pm

Colorado

Denver (Lone Tree) (@denver2600): Park Meadows food court.

Connecticut

Farmington: Barnes and Noble cafe area, 1599 South East Rd.

Florida

Jacksonville (#Jax2600): Goozlepipe & Guttyworks, 910 King St.

Kansas

Kansas City (Overland Park): Barnes & Noble cafe, Oak Park Mall. 6 pm

Maine

Portland (@Maine2600): Maine Mall food court. 6 pm

Massachusetts

Boston (Cambridge) (@2600boston): The Garage, Harvard Square, food court area. 7 pm

Minnesota

Bloomington: Mall of America, north food court by Burger King. 6 pm

New Jersey

Somerville: Bliss Coffee Lounge, 14 E Main St.

New York

Albany: Starbucks, 1244 Western Ave. 6 pm

New York (@NYC2600): The Atrium at 875, 53rd St & 3rd Ave, lower level.

Rochester (@roc2600): Interlock Rochester, 1115 E Main St, Door #7, Suite 200. 7 pm

North Carolina

Raleigh (@rtp2600): Outside Morning Times, 10 E Hargett St. 7 pm

Pennsylvania

Philadelphia (@philly2600): 30th St Station, food court outside Taco Bell. 6 pm

Texas

Austin (@atx2600): Central Market mezzanine level, 4001 N Lamar Blvd. 7 pm

Houston (@houston2600): Ninfa's Express seating area, Galleria IV. 6 pm

Washington

Seattle: Cafe Allegro, 4214 University Way NE (alley entrance), upstairs. 6 pm

All meetings take place on the first Friday of the month. Unless otherwise noted, *2600* meetings begin at 5 pm local time. To start a meeting in your city, send email to meetings@2600.com.

NOTE: Please do not come to meetings if you're not vaccinated. This is for your own safety. Proof of vaccination is not required but we hope that common sense prevails.

WE ARE ONLY LISTING MEETINGS IN AREAS WHERE THE PERCENTAGE OF TOTALLY VACCINATED PEOPLE IS 40 PERCENT OR HIGHER.

Follow @2600Meetings on Twitter and let us know your meeting's Twitter handle or hashtag so we can stay in touch and share them here!

www.2600.com/meetings

Payphones With a View (U.S.)

Arizona. Found in the Petrified Forest National Park (that's petrified wood lining the parking lot). Frontier, incidentally, is part of Citizens Utilities Company, an independent phone company that's been around since 1935.

Photo by Marcus Watanabe

New Hampshire. Seen in North Conway, this phone has a lot going for it: plenty of artwork and a fantastic view. And did we mention that it works?

Photo by Jeff Hanson

California. Wandering around Yosemite National Park, one wouldn't expect to come upon a working payphone complete with a booth. The forest is full of surprises.

Photo by Ian French

California. In this case, maybe the phone itself doesn't have a view, but we can honestly say that the view here happens to be the phone itself. Discovered (somehow) in Forestville.

Photo by Kevin Strishock

Visit **www.2600.com/payphones** to see our foreign payphone photos!
(or turn to the inside front cover to see more right now)

The Back Cover Photos

Congratulations to **Joshua Pritt** for spotting this gasoline-powered Bayside 2600 bicycle (you can see the 2600 on the frame under the seat) in Melbourne, Florida. It's a bit ironic how this started out as the best form of transportation environmentally and wound up getting converted to the worst polluting option for pedal assistance. It's actually a bit of an insult to our name.

Now this is super cool. It's one thing to have an actual card puncher from the really old days of computing. But to have it be a Model 2600 on top of that is almost too much to believe. This was spotted by Jon Guidry at an Atlanta Historical Computing Society meeting, where apparently people sometimes bring in really awesome artifacts.

If you've spotted something that has "2600" in it or anything else of interest to the hacker world (such as funny uses of "hacker," "unix," "404," you get the idea...), take a picture and send it on in! Be sure to use the highest quality settings on your camera to increase the odds of it getting printed. Make sure and tell us where you spotted your subject along with any other info that makes it interesting - many photos are eliminated due to lack of detail.

Email your submissions to articles@2600.com or use snail mail to
2600 Editorial Dept., PO Box 99, Middle Island, NY 11953 USA.

If we use your picture, you'll get a free one-year subscription (or back issues)
and a *2600* t-shirt of your choice.