

UNREDACTED

MY DIGITAL DETOX

Benefits of reducing exposure to technology

SOFTWARE DEFINED RADIOS

Will computer-powered devices replace our traditional receivers?

USB MULTI-BOOT OPTIONS

Boot unlimited Linux Operating Systems from one drive

BITCOIN SPECIAL

Privacy tools, anonymous tactics, and OSINT tips



UNREDACTED ISSUE 004

Image: Jeremy Bezanger

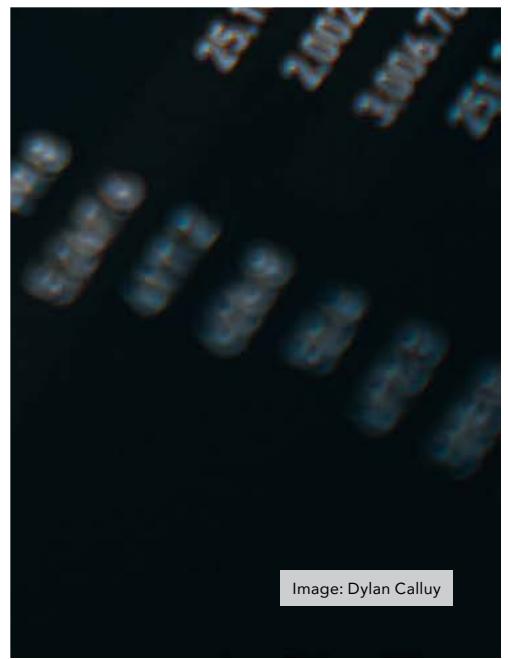
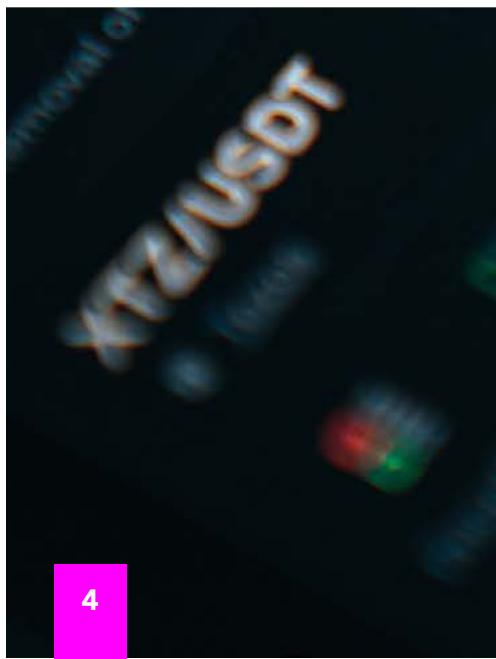
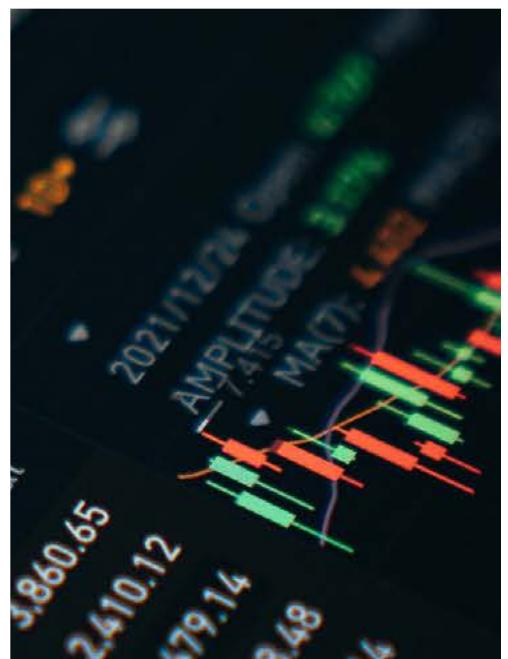
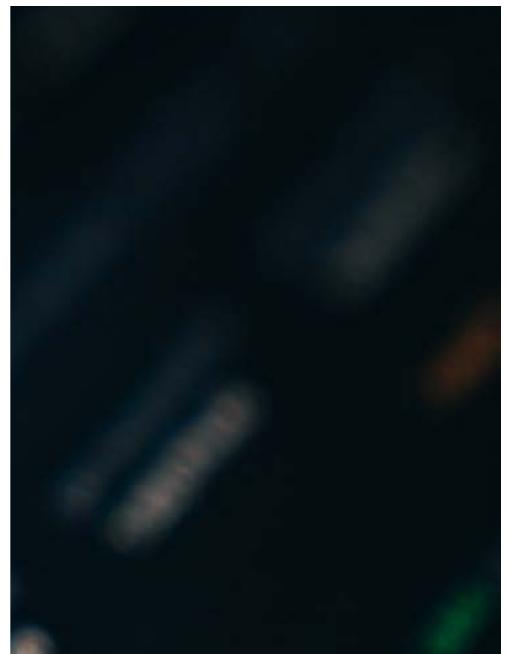
IN THIS ISSUE

- 5 From the Editor**
- 6 The Linux Lifestyle: USB Multi-Boot Options**
- 9 Random Mosaic: Detecting Access with Beans & Rice**
- 12 The Radio Receiver: Software Defined Radios**
- 17 Bitcoin Privacy Tools & Tactics**
- 19 Tracking Bitcoin: Tools for OSINT**
- 22 My Digital Detox**
- 25 The OSINT Corner Learning the Linux Command Line**
- 29 Mobile OSINT Mastery: Utilizing iOS Shortcuts and Telegram**
- 32 Archive Site Removal Guide**
- 36 When Stuff Gets Stuck: How search engines fail to provide reliable tools for cleaning up deleted content**
- 39 How Do Blockchains Provide the Trust Foundation for Decentralized Identity-Based Apps?**
- 42 Paranoid Seller's Guide to Secondhand Marketplaces**
- 44 How (not) to Fly Anonymously**
- 46 More Android Sanitization**
- 48 Using a Travel Router for Privacy on Public Wi-Fi**
- 49 Is Revolut a viable alternative for people outside of the USA?**
- 50 Encryption in the Age of Quantum Computing**
- 52 Reader Q&A**
- 55 Updates**
- 56 Letters**
- 58 Privacy-themed Puzzles**
- 59 Chuckles**
- 60 Final Thoughts**
- 60 Affiliate links**

UNREDACTED is published free of any charge to the reader, and this file may be publicly shared in its entirety. All issues are available for free download at UNREDACTEDmagazine.com. Contact details are also available at this site.

The contents of this publication are copyright © 2022 by UNREDACTEDmagazine.com, and are published via a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International license. You may share it for free as long as you keep the entire file intact. Commercial use is prohibited.

Cover Design by Anonymous Reader. Layout by [Astropost](#). Special thanks to everyone who helped make this happen. You know who you are.



FROM THE EDITOR

By Michael Bazzell

Welcome to the fourth issue of UNREDACTED Magazine. Now that we have multiple issues available, we can analyze the downloads better. Based on temporary server access logs, we estimate that each issue has been downloaded over 60,000 times, and at least 1,000 people currently download previous issues every day. I know nothing about sales or marketing, so I don't know if these numbers are good or bad. I only know that interest still seems to be growing, so we will keep publishing new issues.

When we announced the switch to a quarterly issue, we saw community contributions decline. This was expected, as there was no longer a monthly issue to serve as a reminder for contributions. We cleaned out our inbox on August 29, 2022 and are eagerly awaiting new submissions for the next issue (shortly after locking in the articles for this issue, we received several quality submissions which will be carried over into the next issue). Please send your best submission before November 15, 2022 for consideration for issue 005 (January 2023).

This seems like a good opportunity to further clarify how we handle all incoming email. We currently receive

over 500 emails from readers weekly, for which we are very grateful. If the message contains an article, reader question, letter, or other submission, it gets placed into a folder for that purpose, and is analyzed later by the staff. We basically pluck out anything which could be used in the next issue before purging all messages before publication.

This is where our privacy policy comes in. Once we have finalized all content for an issue, we permanently delete all email messages received up to that date. This way, we could never be forced to hand over details about a submission. We can't disclose what we no longer have. Since we host this email on Proton Mail, they have no ability to get into our account and see any content. It is not a perfect system, but is designed to minimize the data available for abuse.

Unfortunately, we can no longer directly respond to messages sent to the magazine, especially those asking for technical support or confirmation that a submission was read. When we did, it always began a never-ending back-and-forth conversation which ate up even more time while new messages piled up. This is the reality of limited staff hours for a free publication. I wish we had the resources to respond to

every email, but we do not. If you sent an email to the appropriate address and did not receive an automated bounce, be assured it was received, read, and considered.

Many people have asked for clarification of which topics are of most interest to the magazine. We really do not have an answer for that. The topics we find most interesting are those which we would have never known about prior to receiving the submission. We are always looking for new discussions which are otherwise off of our radar.

As I write this, the magazine email inbox, archive, sent, and trash folders are empty (with the exception of the articles mentioned previously carried over for the next issue). Please fill them up with your article submissions, questions, letters, or anything else which you believe fits this publication. It is YOUR magazine. YOU control what is seen here. We look forward to wherever you take it next.

MB



Image: Lasse Jensen

THE LINUX LIFESTYLE: USB MULTI-BOOT OPTIONS

By Michael Bazzell

The Linux Lifestyle is a quarterly column all about Linux. From new useful apps to working through Linux frustrations, this section aims to introduce others to a more secure operating system.

I have possessed numerous USB boot devices over the years. As I write this, I see my bin of small USB drives ready to boot Ubuntu, POP!_OS, TAILS, pfSense, and others. At one time, I carried a USB case with at least 10 drives everywhere I went. You know, just in case. Today I carry one drive which can boot any operating system I would ever need. Before we get to that, let's discuss the reasons why this is so important.

Boot drives are amazing. They allow us to boot a full operating system to practically any physical machine without modifying the host system. This allows us to test a new OS, install a full OS, or repair the current system. I typically boot to a USB drive at least once per week.

In the past, that meant a separate drive for each potential operating system. I would have one drive to boot TAILS and another which booted into Ubuntu. We have always had manual options which would make a drive capable of booting a selection of multiple operating systems, but the process was usually cumbersome with high chance of failure. Today we have an easy solution called Ventoy (ventoy.net).

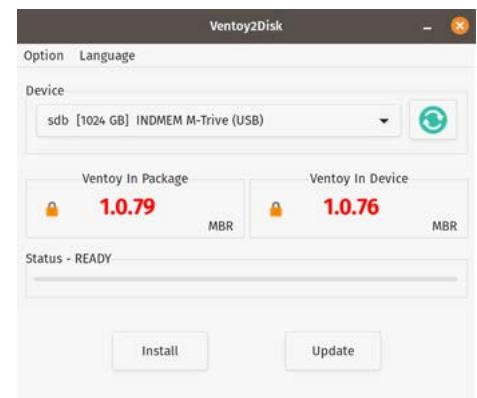
The Ventoy downloads page presents options for Windows, Linux, or a live ISO. These likely still forward to their GitHub page located at <https://github.com/ventoy/Ventoy/releases>. For the purposes of this article, I will use the Linux option within my Pop!_OS machine. The Windows executable is just as easy.

- Download the Linux version, titled similarly to "ventoy-1.0.79-linux.tar.gz".
- Decompress this file, which should

present a folder titled similarly to "ventoy-1.0.79".

- Open Terminal and navigate to the directory (my command was "cd Downloads/ventoy-1.0.79/").
- Execute "./VentoyGUI.x86_64" in Terminal.

This should present the Ventoy installation application which appears as follows. Choose the desired USB device and click "Install". Note that this will overwrite all data on the device.



Your Ventoy boot device is now ready for use, but it does not contain any bootable operating systems. This is where Ventoy excels. Instead of manually configuring multiple systems for boot, you only need to possess the bootable ISO files for any systems desired. The drive has an ExFat-formatted partition which can hold any type of data. This means we can use it as a storage drive and multi-boot drive.

I downloaded all of the ISO files for the various systems which I may need, and then re-titled the files to match my desired display. I added "V" for Ventoy before each to place them toward the bottom of the list within the Files viewer. I then placed each file at the root of the Ventoy USB drive. My files are as follows.

V-CloneZilla-20220522.iso
V-Hiren's Boot CD.iso
V-Knoppix-2021-01-25.iso
V-pfSense-CE-2.6.0.img
V-Pop!_OS-22.04.iso
V-Tails-5.1.img
V-Ubuntu-22.04.iso
V-Ubuntu-T2-22.04.iso
V-Windows.7.iso
V-Windows.10.LTSC.iso
V-Windows.11.iso

I then inserted this new drive within my computer and rebooted. I was sure to select the proper USB boot option within the BIOS, and the following screen appeared. I could then select any of these operating systems and each would boot as if I had inserted a dedicated USB boot device.



The files will appear exactly as the file names on the drive. The remainder of the drive can be used to store any data desired. Only available bootable Linux and Windows systems will display within the Ventoy boot screen. Let's discuss the benefits of this, and I will use my choices as examples.

CloneZilla: This is a bootable operating system which allows one to create true clones or images of hard drives or partitions. I use this to create a true clone of my host Linux drive, which could then be used for booting my entire system if my drive should ever crash or become corrupt. I can also use it to clone replacement hard drives.

Hiren's Boot CD: This is an old staple. It boots a minimal Windows 10 OS with many tools for repairing Windows systems. It has saved me many hours of headaches when helping family with computer woes.

Knoppix: This is a minimal Debian-based Linux boot CD which can be useful if you do not want to boot to an Ubuntu-flavored variant. I have used this to access Windows files when Ubuntu was not the best choice. I confess I don't use this often.

pfSense: This option has saved me many times. I have witnessed power failures which corrupted my pfSense firewall and prevented it from functioning. Booting to this option allowed me to repair or completely rebuild the firewall. I also keep a configuration file on this drive which allows me to completely restore my firewall within a few minutes if ever needed.

Pop!_OS: This is my primary operating system. Having a bootable live version allows me to repair or restore the system. I can also quickly install the OS to any other computer.

Tails: This bootable OS (tails.boum.org) allows me to launch an entire OS which is protected by the Tor network. It is beneficial for sensitive investigations which must possess a private connection and leave no trace behind.

Ubuntu: Much like Pop!_OS, a standard Ubuntu ISO allows me to run Ubuntu live or as an installation. It can also help diagnose and repair unhappy Ubuntu systems.

Ubuntu-T2: This custom build of Ubuntu 22.04 (t2linux.org) allows me to boot into a live Ubuntu system within T2-based MacBook computers. It includes all Wi-Fi, video, and even touch bar drivers.

Windows.7: This allows installation of Windows 7 if ever needed. Legal ISO files can be found on Microsoft's website or Archive.org.

Windows.10: This allows installation of Windows 10 if ever needed. Legal ISO files can be found on Microsoft's website or Archive.org

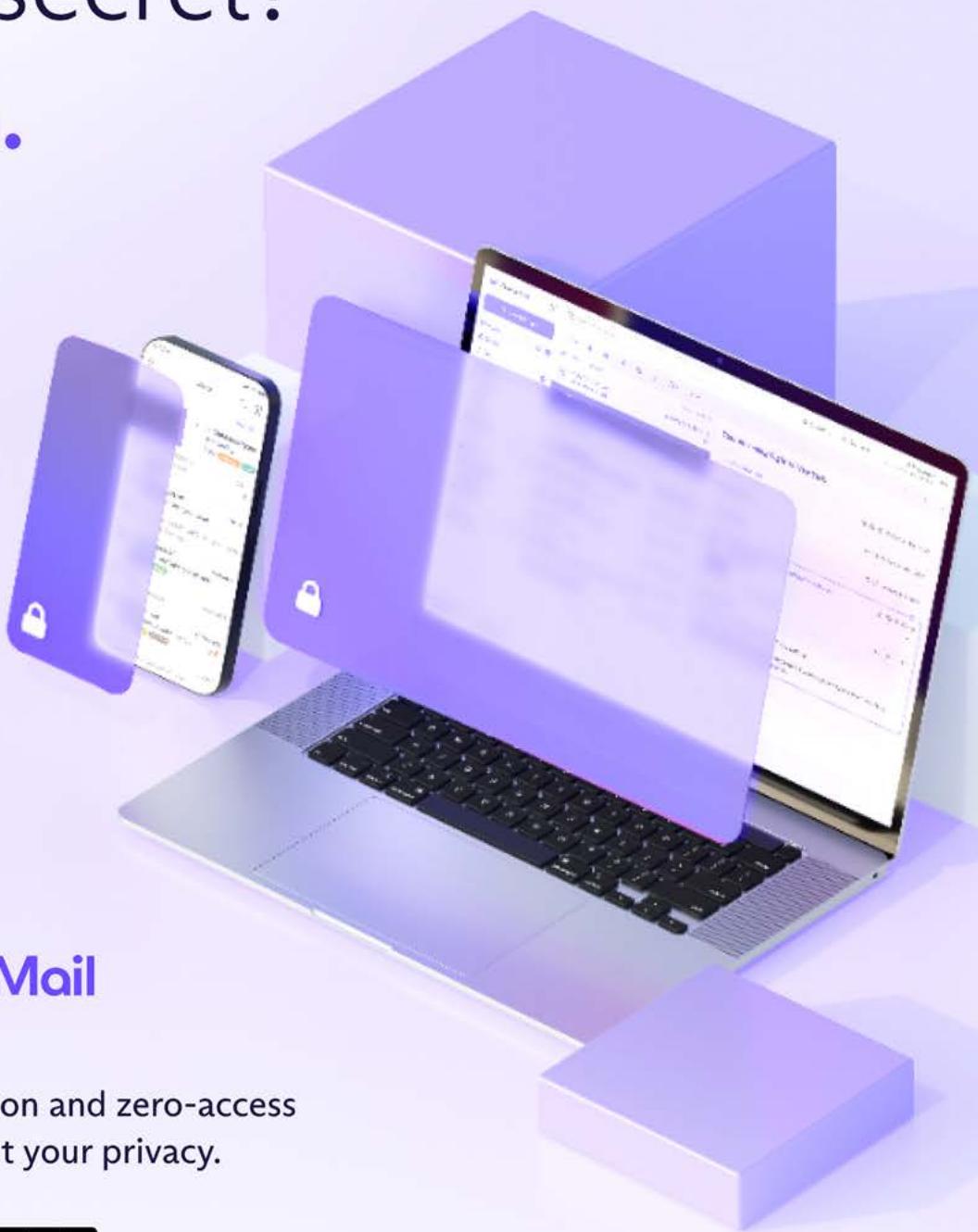
Windows.11: This allows installation of Windows 11 if ever needed. Legal ISO files can be found on Microsoft's website or Archive.org

Drive Selection

Technically, any decent USB drive should work for this. However, I recommend a fast drive with plenty of storage. I use a SanDisk Extreme Portable 1TB USB SSD (<https://amzn.to/3BLIHwd>). It loads live systems without any delay or stuttering, and installs new systems in a flash. It also allows me to use the remaining 95% of the drive for fast file transfer. One could even use it to query large breach data files quickly. Once you are accustomed to the speed of a fast USB SSD for booting and installation of Linux systems, you can never go back to slow flash drives.

Today, I keep my multi-boot with me at all times. Often, I forget that booting is the main purpose since I also use it to transfer large files. The best-case scenario is that you will never need it. If you do, you will be glad you made these efforts. ■

Can you keep a secret? **We can.**



Proton Mail

End-to-end encryption and zero-access
encryption to protect your privacy.



Join us for free at go.getproton.me/SHXg

We can't read your emails and neither can anyone else.

RANDOM MOSAIC: DETECTING ACCESS WITH BEANS & RICE

By b068931cc450442b63f5b3d276ea4297

The history of mankind is also a history of secrets, attacks and defense of the confidential. Steganography, cryptography and technical tools support us in protecting the private. The antagonists of confidentiality operate - depending on the actor - outside or inside legal frameworks, often adapting them with bogus arguments.

If we have objects or devices outside our view, we cannot rule out that there was unwanted/unauthorized access to them and the confidentiality and integrity possibly no longer exists. If there has been an unauthorized access (attempt), it is in the interest of the affected parties (owner/proprietor/transmitter/receiver) to know about it in order to initiate any follow-up measures and not to think themselves in a false sense of security.

For thousands of years, seals have been used in various forms with the goal of certifying the confidentiality and integrity of letters, for example. Attacks on these protective measures are similarly old. This continues to this day, but these attacks are now taking place on a very different level. A lot has changed since then, especially due to digital communication and the widespread presence of technical devices, as well as the accumulation and

automated analysis of data. Modern communication tools reach very deeply into our lives, so their confidentiality and integrity should also be a very high priority. Below we show a few examples of these attacks, summarize known countermeasures, and introduce a new method.

Tampering in transit (supply chain interdiction)

While the U.S. government has claimed for years that Chinese companies are building surveillance technology into devices exported to the U.S. (such as networking equipment), it was revealed in 2014 in the book "No Place to Hide" that the NSA's "TAO" (Tailored Access Operations) unit has been intercepting and tampering with technical devices in transit since at least 2010. Netzpolitik.org summarizes:

According to them, it is common practice to, among other things, prepare servers, routers, and other network technology with eavesdropping technology before exporting them to third countries. The equipment is then repackaged and shipped as planned. It is likely that such attacks are taking place in other states as well - whether against individuals or on a larger scale. The Intercept published a good article on supply chain attacks in 2019,

Microsoft started its own series of articles that same year.

Evil Maid attacks

If somebody has hardware access, an Evil Maid attack can be carried out within a few minutes. Whoever has access to the hardware can not only manipulate firmware and possibly software, but also replace or manipulate hardware and create images of storage media.

Protection methods

There are special screws, seals, "tamper-proof" labels and tape, "tamper-proof" bags, and much more to detect unauthorized access to items or to the contents of shipments, for example. We assume that most of the methods can be broken and are not a problem for talented and resourceful attackers. If you want to get an insight, you can have a look at presentations like the one from DEFCON 19: Introduction to Tamper Evident Devices. You can also learn more about this in the work of Sergei Skorobogatov (Physical Attacks and Tamper Resistance) and Elena Dubrova. There are also competitions to get around as many of these protections as possible. For example, Mos & Boo give us insights from the OzSecCon 2018 Tamper Evident Challenge.

Some companies deliberately avoid certain tamper-evident procedures. For example, Ledger, the manufacturer of the eponymous hardware wallet for cryptocurrencies, refers to the forgeability of seals and limits itself to hardware-side protection measures.

Anti-tamper seals: Ledger deliberately chooses not to use anti-tamper seals on its packaging. These seals are easy to counterfeit and can, therefore, be misleading. Rather, genuine Ledger devices contain a secure chip that prevents physical tampering: This provides stronger security than any sticker possibly could. After a leak in 2020, several Ledger customers received purportedly tampered replacement devices by mail in spring 2021.

Glitter Nail Polish

A relatively widespread method to seal screws on devices, for example, so that unauthorized access is more likely to be detected, is the use of nail polish with varicolored and differently-sized elements. To our knowledge, this technique was first presented at 30C3 by Eric Michaud and Ryan Lackey and is recommended and used by several companies and individuals, including journalists evaluating the Panama Papers. We have done a few experiments on our own to test the effectiveness of this process. Our conclusion so far is that depending on the method, it is sometimes very difficult or even impossible to detect manipulations.

Beans & Rice

An alternative to sealing is embedding the whole object in a substance whose surface forms a mosaic that is difficult to reproduce and changes when manipulated. It should be as easy as possible to check the mosaic manually or by technical means. The goal is to protect written documents, data carriers, communication devices, hardware wallets and other sensitive objects in such a way that unauthorized access can be detected with greater probability. We distinguish between two use cases: short-term storage and

longer-term storage or shipping. The sought mixture should:

- not be too fine-grained, so that the individual elements can be easily identified
- not be too coarse, so that it is as difficult as possible to reproduce the mosaic
- be composed of elements of different colors and/or sizes, in order to obtain a mosaic as rich in contrast as possible
- consist of elements that are as round as possible in order not to jam
- be as dry as possible and not tend to form lumps or stick together
- be simple and inexpensive to obtain
- be solid so as not to cause damage in the event of leakage
- have no sharp edges or pointed corners that could cause damage
- not be too heavy, e.g. to save shipping costs

To test the mixing behavior, the first three points in particular were relevant for us. We examined several substances, limiting ourselves to those that met the last three points of our requirements. Our favorites so far are: Red lentils & Beluga lentils, yellow and green peas and white beans, and colored rice.

Short-term storage

Following the history of its development, let's start with the first application, short-term storage. When we need to leave a place and leave items or equipment behind, we can store them in a box that is transparent from all sides. Then we fill the box with our colorful mixture so that our devices are covered. The box should be stored in such a way that shocks or other factors do not change the mosaic. For example, the box can be positioned on a towel or piece of clothing on an object in such a way that this attenuates minor

vibrations of the environment, but the box cannot slide off it.

For an overall comparison, we can photograph the box from all visible sides and store these photos on a device that is as secure as possible, send it to a trusted person via an encrypted and verified channel, or send it to another device of our own. The next step is to compare the found mosaic with the original one. The app Blink Comparison, which we will discuss below, is ideal for this purpose. To protect an object from damage, e.g., by staining or by the substance leaking into, say, the ports of a laptop, it can be wrapped in cling film, a bag, or otherwise. A combination with Haven as an additional security layer may be recommended at this point.

Long-term storage or shipping

Especially when shipping sensitive items, we see the need to be able to detect unauthorized access. Almost every shipping method involves people and locations unknown to us. Since the colored elements in the above proposal would not hold their position during transport, we change the procedure. Our object now goes into an air-impermeable wrapping. This is filled with our colored substance so that the object is covered from all sides as far as possible, and is then vacuumed. This holds the colored substance in place. If the wrapping is damaged and pressure equalization takes place, but at the latest when the enclosed object is accessed, the elements change their position.

Vacuuming

Since many people own vacuum cleaners and there are also public vacuum cleaners at gas stations, this method is our first priority. There are special reusable vacuum bags to store e.g. clothes and blankets in a space-saving and protected way. The air from the bag is removed with a vacuum cleaner or a hand pump through a valve. Commercially available bags are quite large, so they are well suited for laptops, for example, but less suited for small objects.



There are many different vacuum sealer machines, which differ in quality and size. They are used, for example, to keep food fresh for longer. Suitable bags are available in many sizes, but they cannot be reused easily or only with loss of material.



In both methods, the bags containing the elements can also be cascaded. To do this, after photographing the result of the first process, it is placed in another bag with additional substance and vacuumed again.



If one or more elements within the mosaic are modified, unauthorized access or compromise can be assumed. The assessment should be made depending on the situation and the individual need for protection. It may just be that one's pet or family member was a bit curious about what the colorful mixture was all about, or a bag was leaking.

Blink Comparison

With apps like Blink Comparison, it is easy to compare an original photo, which has been taken for example, by a manufacturer, signed and transmitted to a customer via an encrypted communication channel, with a photo of the current state. The app helps one take the comparison photo from the same angle and distance as the original photo. Blink Comparison then switches between the two images when the screen is touched, making direct comparison much easier.

If you have any further ideas, hints or suggestions for improvement, please feel free to write us or collaborate with us at <https://github.com/dys2p>.



INDUSTRY LEADING TECHNOLOGY AND A 24X7 SOC WORKING FOR YOU

Cyber threats are evolving rapidly. SMBs and Enterprise businesses are looking to their Managed Service Providers to provide them with cybersecurity solutions. Our managed SOC is highly-skilled in the constantly evolving threat landscape and will provide absolute security for you and your clients.



FORTIFY24X7.COM | (800) 989-2647 | INFO@FORTIFY24X7.COM

THE RADIO RECEIVER: SOFTWARE DEFINED RADIOS

By Michael Bazzell

I typically prefer knobs and buttons over keyboards and mice, but to each their own. In previous issues, I have begun the conversation about radio monitoring, and we have discussed a lot about frequencies and strategies. Until now, I have focused on traditional radios which allow a listener to manually tune past frequencies waiting to hear a transmission. That may seem very dated to many readers.

Within this issue, I want to begin the conversation about Software Defined Radios (SDRs). These have been around many years, but things have finally become interesting enough for me to consider making the switch. First, let's define the SDR.

In basic terms, a SDR is a piece of hardware which contains the required components to receive a specific range of radio frequencies, but does not possess the software required to actually monitor any audio. There are countless online documents which can take over from there. This typically makes the hardware quite small and easy to power, and allows listeners to customize software on their computers to make the hardware functional. This also usually offers a smaller price tag for the hardware. The chosen SDR connects to a computer via USB cable and the software on the computer makes the magic happen. I have played with numerous SDRs over the years,

and I place all hardware options into four categories.

Tier 1 (Toys): This is where I began over a decade ago. These are cheap USB dongles with labeling such as "RTL-SDR" which can be found priced as low as \$10. They work, but not well. You will pick up some frequencies, but they might "drift". These are fun, hence the term toys, but any long-term listening will be frustrating.

Tier 2 (Hobbyists): This is where I landed a couple of years ago. These devices cost approximately \$50 and are better built than the previous tier. I include the Nooelec NESDR in this category, which was much more stable than any knock-off RTL-SDR devices. These are very listenable with less interference than the cheap sticks.

Tier 3 (Enthusiasts): This is where I am today. These devices are made of better quality, have less interference, and are more listenable long-term. I include the \$160 Airspy HF+ Discovery in this category, which is my daily SDR unit. I explain more about this device in a moment. This is the tier where I believe any SDR enthusiast should be.

Tier 4 (Cutting-Edge Explorers): I have dabbled in this area, but always regretted it. I have purchased both the \$350 HackRF One and \$340 KiwiSDR only to realize that my Airspy worked the same, if not better, and focused on the frequency ranges most appropriate for radio monitoring. These are both

fine units, but the expense did not justify the actual usage for me.

That brings us back to the Airspy. I believe it offers the most bang for your SDR buck. Let's play with one.

The unit itself is tiny at 2" x 1.5". A micro USB port is at one end while an SMA antenna adapter is at the other. Inside is the hardware required to receive HF coverage between 0.5 kHz and 31 MHz (AM/SW) and VHF coverage between 60 and 260 MHz (HAM/FM/Air/Marine). This is all of the bandwidth I am interested in with regard to traditional radio monitoring.



The hardware is not very exciting. There are no moving parts or screens. It simply exists to receive radio frequencies. The software has all the power. This is the main benefit of SDRs. The hardware doesn't change. The frequencies will not need updated. However, the software can be tweaked, customized, and updated as often as desired without purchasing new hardware. That brings us to the choice of software options.

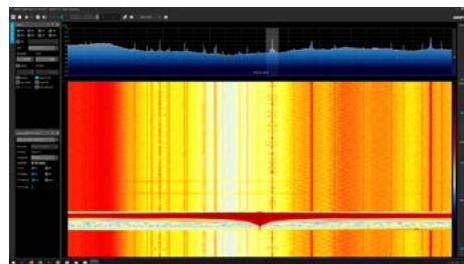
For Windows users, I believe the Airspy custom version of SDR# (SDRSharp), available for free at airspy.com/download, is the absolute best option. It was made for this hardware, and it just works. It is also updated often. Unfortunately, they only offer a Windows package.

For Mac users, I also recommend the Windows Airspy version of SDR# if one is willing to run a virtual machine while using the product. Some have had success using WINE or Mono instead of a full VM, but I never cared for it. If I were still using a Mac today, I would probably experiment with GQRX (gqrxdk.com), SmartSDR (roskosch.de/smartsdr-for-mac), SdrDx (fyngyrz.com), or CubicSDR (cubicsdr.com), to see if they could replicate the features of SDR#. All are compatible with Airspy and most other units.

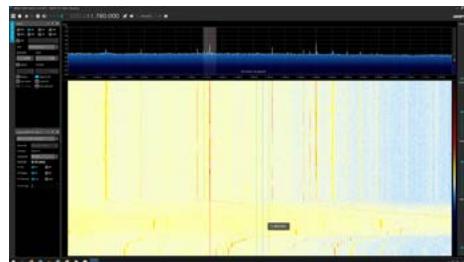
For Linux users, I recommend either a minimal Windows VM with the official version of SDR# for Airspy or GQRX (gqrxdk.com). There are many other options, and I encourage users to try them all.

Overall, I always prefer the official Airspy software releases because they are updated often and work best without any tweaks. I am currently using a Windows 10 VM on my Linux machine to display the native SDR# software option.

Once you have your software installed, the interface can seem overwhelming. I recommend "The Big Book of SDRsharp and its Whole Universe", available for free at <https://airspy.com/downloads/>. I read it thoroughly as I was waiting for my unit to arrive. The following is the SDR# dashboard while focused on traditional local AM coverage. I only clicked the "start" arrow in the upper left to detect my device and start monitoring. I clicked the upper and lower portions of each number in the upper left to tune my device. Note that I redacted all frequencies from this image because of, you know, privacy. The following non-local screen captures display more data.



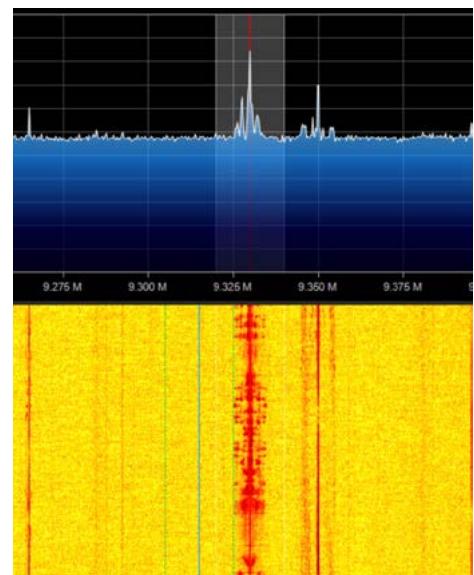
In this image, you can see the peaks of active AM transmissions in the top section. I can easily click on each to start monitoring that frequency. This may not seem too valuable as the AM band is quite small and already easy to navigate. Let's take another look at the 11 MHz area in the following screen.



I typically avoid this range because I rarely pick anything up. I would need to manually tune into each frequency with my traditional radio. However, my Airspy visually shows me the seven transmissions which I can receive in this range. I can click on each without wasting time tuning individual frequencies. If I were writing this in the evening, these peaks would be much more powerful. I am writing this during the day with weak reception, but it still shows me where I should focus my attention. I can scroll my mouse wheel to navigate to lower or higher frequencies, or click the numbers to raise/lower them.

This is the true power of a SDR. I can visually view all of the frequencies by navigating to my desired ranges and see right away if I should tune into something. More important, I can see right away when there is nothing going on of any interest. The following screen shows an otherwise unknown strong transmission at 9330 KHz. The waterfall below the chart displays a historical view of the audio transmission. This portion helps me visually identify voice transmissions versus music. Music is more compressed and "full" while

voice transmissions are visually broken into segments. The following is a voice transmission.

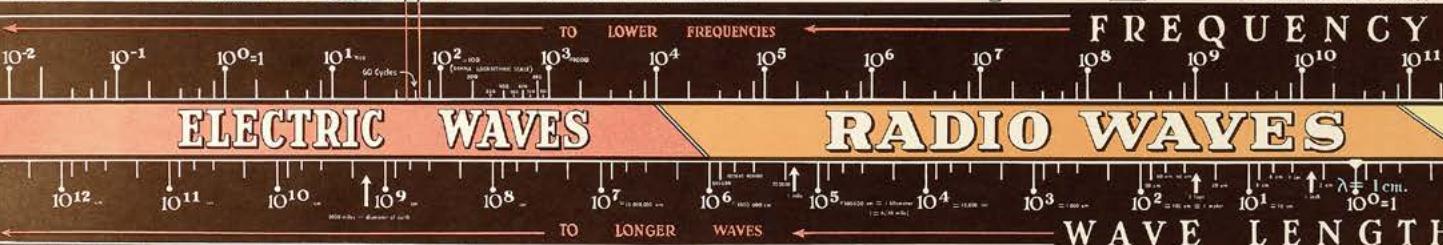
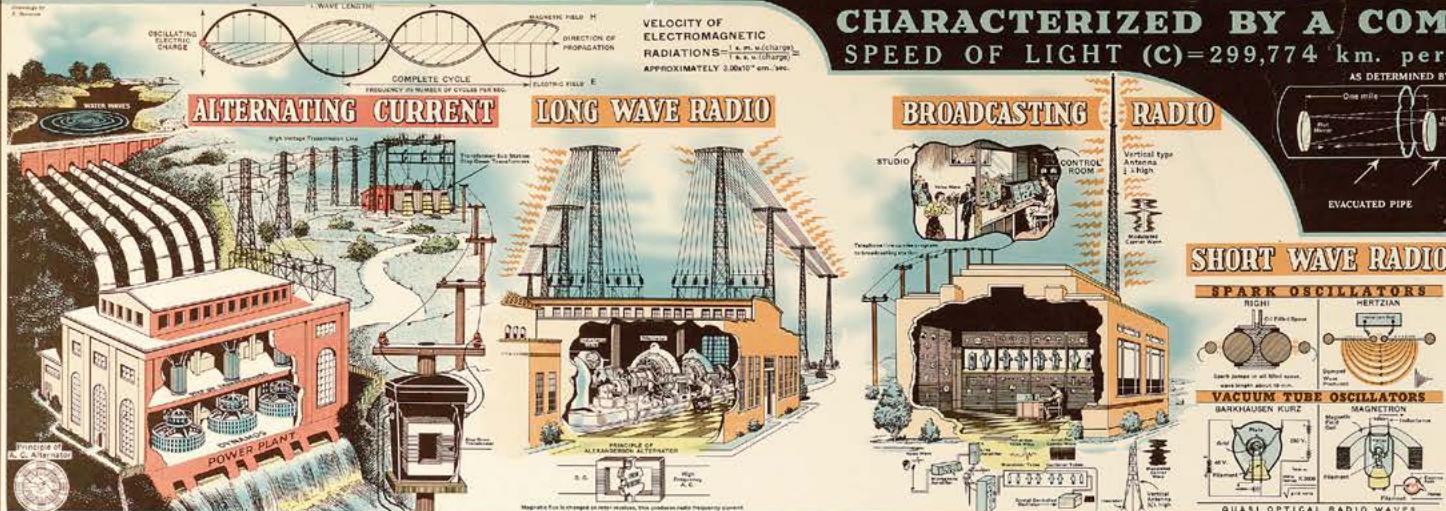


Before using SDRs, it could take me hours to manually navigate various bands and frequencies, and there was a good chance I would miss something. With SDRs, I can visually inspect the entire spectrum of frequencies within a few minutes. This identifies the current strongest bands and frequencies in use.

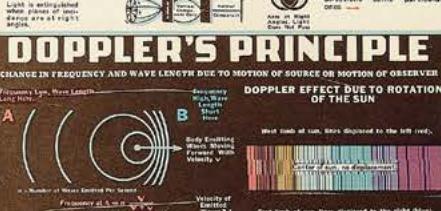
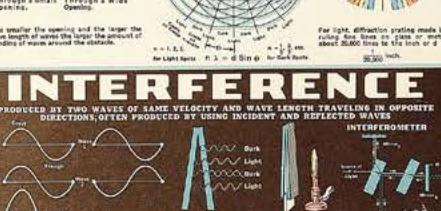
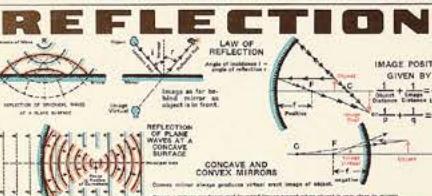
Your experience will only be as good as your antenna. I strongly recommend an outdoor antenna for best reception. I have both a sloper to the ground and a whip above my roof. Each have coax running into the house, terminating at a male BNC plug. Therefore, I make sure to always have a female BNC to male SMA adapter for the Airspy.

I hope this article serves as an introduction to SDRs. We still have a lot to talk about. Get your feet wet and see if a SDR provides any advantages for you. I admit this takes some of the old-school charm out of things. I no longer stumble upon a transmission by blindly turning a knob. However, we must take advantage of the latest technologies. I still use my traditional portable short wave device with its knobs and buttons. It scratches an itch I get on occasion. However, it will never be as robust as my Airspy. The visual representations of transmissions is something I can never permanently eliminate from my hobby. ■

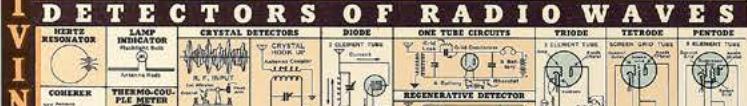
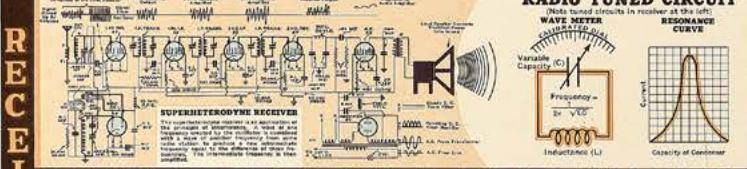
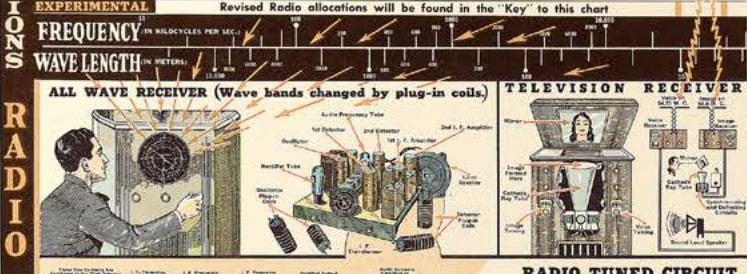
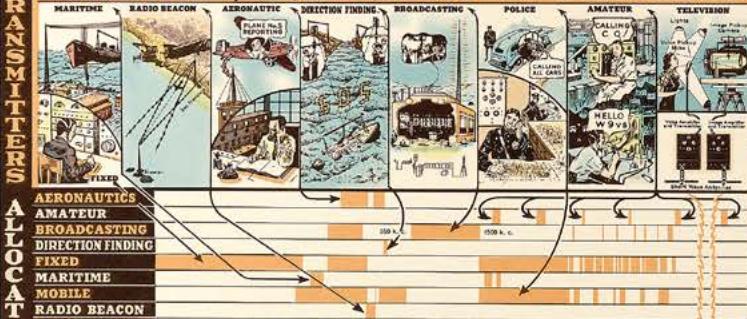
EMITTERS



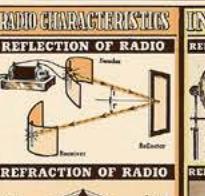
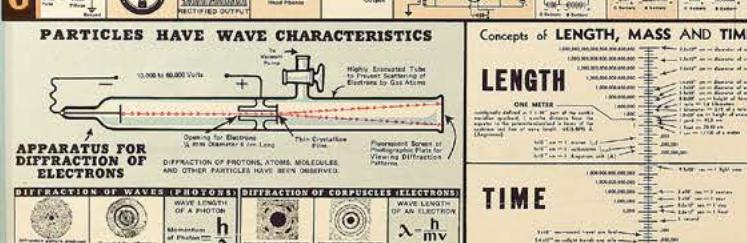
METHOD OF MEASURING THE WAVE LENGTH



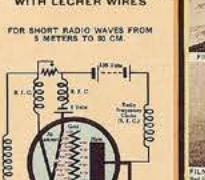
RADIO SPECTRUM: FREQUENCY and WAVE LENGTH ALLOCATIONS



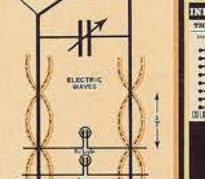
PARTICLES HAVE WAVE CHARACTERISTICS



POLARIZATION OF RADIO



INTERFERENCE OF RADIO

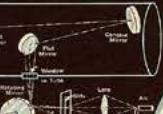


MAGNETIC RADIATIONS

MON SPEED IN A VACUUM

sec. = (Approximately) 186,000 Miles per sec.

A. A. MICHELSON



LONG WAVE
HEAT
(Radiation)

SHORT WAVE
HEAT
(Radiation)



RANGE (WAVES PER SECOND)

10^{12}

10^{13}

10^{14}

INFRARED

RANGE (IN CENTIMETERS)

10^{-1}

10^{-2}

10^{-3}

10^{-4}

10^{-5}

10^{-6}

10^{-7}

10^{-8}

10^{-9}

10^{-10}

10^{-11}

10^{-12}

10^{-13}

10^{-14}

10^{-15}

10^{-16}

10^{-17}

10^{-18}

10^{-19}

10^{-20}

10^{-21}

10^{-22}

10^{-23}

10^{-24}

10^{-25}

10^{-26}

10^{-27}

10^{-28}

10^{-29}

10^{-30}

10^{-31}

10^{-32}

10^{-33}

10^{-34}

10^{-35}

10^{-36}

10^{-37}

10^{-38}

10^{-39}

10^{-40}

10^{-41}

10^{-42}

10^{-43}

10^{-44}

10^{-45}

10^{-46}

10^{-47}

10^{-48}

10^{-49}

10^{-50}

10^{-51}

10^{-52}

10^{-53}

10^{-54}

10^{-55}

10^{-56}

10^{-57}

10^{-58}

10^{-59}

10^{-60}

10^{-61}

10^{-62}

10^{-63}

10^{-64}

10^{-65}

10^{-66}

10^{-67}

10^{-68}

10^{-69}

10^{-70}

10^{-71}

10^{-72}

10^{-73}

10^{-74}

10^{-75}

10^{-76}

10^{-77}

10^{-78}

10^{-79}

10^{-80}

10^{-81}

10^{-82}

10^{-83}

10^{-84}

10^{-85}

10^{-86}

10^{-87}

10^{-88}

10^{-89}

10^{-90}

10^{-91}

10^{-92}

10^{-93}

10^{-94}

10^{-95}

10^{-96}

10^{-97}

10^{-98}

10^{-99}

10^{-100}

10^{-101}

10^{-102}

10^{-103}

10^{-104}

10^{-105}

10^{-106}

10^{-107}

10^{-108}

10^{-109}

10^{-110}

10^{-111}

10^{-112}

10^{-113}

10^{-114}

10^{-115}

10^{-116}

10^{-117}

10^{-118}

10^{-119}

10^{-120}

10^{-121}

10^{-122}

10^{-123}

10^{-124}

10^{-125}

10^{-126}

10^{-127}

10^{-128}

10^{-129}

10^{-130}

10^{-131}

10^{-132}

10^{-133}

10^{-134}

10^{-135}

10^{-136}

10^{-137}

10^{-138}

10^{-139}

10^{-140}

10^{-141}

10^{-142}

10^{-143}

10^{-144}

10^{-145}

10^{-146}

10^{-147}

10^{-148}

10^{-149}

10^{-150}

10^{-151}

10^{-152}

10^{-153}

10^{-154}

10^{-155}

10^{-156}

10^{-157}

10^{-158}

10^{-159}

10^{-160}

10^{-161}

10^{-162}

10^{-163}

10^{-164}

10^{-165}

10^{-166}

10^{-167}

10^{-168}

10^{-169}

10^{-170}

10^{-171}

10^{-172}

10^{-173}

10^{-174}

10^{-175}

10^{-176}

10^{-177}

10^{-178}

10^{-179}

10^{-180}

10^{-181}

10^{-182}

10^{-183}

10^{-184}

10^{-185}

10^{-186}

10^{-187}

10^{-188}

10^{-189}

10^{-190}

10^{-191}

10^{-192}

10^{-193}

10^{-194}

10^{-195}

10^{-196}

10^{-197}

10^{-198}

10^{-199}

10^{-200}

10^{-201}

10^{-202}

10^{-203}

10^{-204}

10^{-205}

10^{-206}

10^{-207}

10^{-208}

10^{-209}

10^{-210}

10^{-211}

10^{-212}

10^{-213}

10^{-214}

10^{-215}

10^{-216}

10^{-217}

10^{-218}

10^{-219}

10^{-220}

10^{-221}

10^{-222}

10^{-223}

10^{-224}

10^{-225}

10^{-226}

10^{-227}

10^{-228}

10^{-229}

10^{-230}

10^{-231}

10^{-232}

10^{-233}

10^{-234}

10^{-235}

10^{-236}

10^{-237}

10^{-238}

10^{-239}

10^{-240}

10^{-241}

10^{-242}

10^{-243}



The World's Only All-in-One Privacy App



Sudos act as digital firewalls to eliminate data trails.

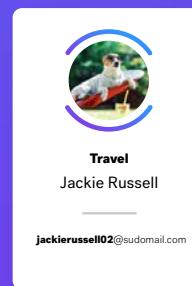
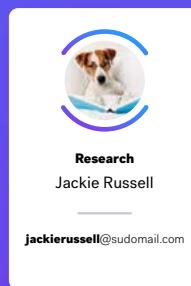


Call, Text, Email, Browse, Shop and Pay

Privately and Securely



Create digital identities, or **Sudos**, for different situations.



Sign up without an email, phone number or password | MySudo.com/bazzell





Image: André François McKenzie

BITCOIN PRIVACY TOOLS & TACTICS

By Ergo

Bitcoin: A Peer to Peer Electronic Cash System...

The title of the bitcoin whitepaper alludes to imagery of untraceable private transactions. A digital cash may have been the objective of cypherpunks and early bitcoin developers, but over the last 12 years development focus has shifted to "programmable sound money" or "digital property". The default privacy provided by the bitcoin protocol has not seen meaningful change since its creation.

Backwards compatible softforks have unlocked additional privacy tooling at the application layer at the cost of increased accuracy of change detection heuristics for "normal spending".

The result is a stagnant default protocol that is easily tracked as we had presented in our previous article. This article aims to introduce some key concepts about BTC's functions, steps, and tooling for transacting privately.

By understanding the fundamental steps to tracking, users can deploy the appropriate countermeasures.

To review, the fundamental steps to effective BTC tracking are as follows:

1. Establish a starting point: Blockchain analysis needs a blockchain starting point usually an address or transaction ID associated with a target.
2. Financial flow analysis: Identifying change outputs allows for tracking an entity's future spending over multiple transactions.
3. Evaluate flow intersection with known or custodial entities: When

a financial flows analysis intersects with a known custodial entity that collects user information (KYC/AML data) a target may be identified.

While private cryptocurrencies such as Monero aim to protect against the blockchain surveillance by sound protocol defaults, BTC users are forced to protect their privacy by using tools at the application layer. Thwarting any one of the steps above can stop an effective analysis in its tracks. The basic building blocks to thwarting effective bitcoin tracking are discussed below.

Coin Control – Managing TXOs: Most bitcoin wallets display a single wallet balance for an improved user experience. But that single balance is made up of one or more transaction outputs (TXOs). To maintain privacy understanding TXOs and managing TXO spending is critical. This process is usually referred to as “coin control”. A TXO can be thought of as a single physical cash bill. An address provided for receiving payment can be thought of as a container for TXOs. A total wallet balance is the sum of all TXOs in each address contained in the overall wallet. A single address can send and receive unlimited TXOs, which degrades privacy by automatically linking all sent and received transactions to the same user. TXOs can also be received to unique addresses, but these otherwise separate TXOs can be linked to a single user by future spending. Typically the coin control process includes labeling incoming TXOs including source and reason for payment, as well as deliberate selection of TXOs for spending based on their history.

Stealth Addresses–Denying a Starting Point: Receiving a bitcoin payment is easy, just post or share an address and anyone can send you a transaction. However, if this address is posted in a public online profile, all past and future spending associated with the profile can be evaluated by third parties. To prevent address reuse and help deny

analysts a starting point for evaluating transactions, a BIP47 payment code can be posted for receiving BTC in a more private manner. A BIP47 payment code is a stealth address, the code does not show up on the bitcoin blockchain while still allowing users to generate an infinite amount of unique addresses for receiving payment. These are particularly useful for recurring payments and eliminate address reuse, a significant benefit for privacy.

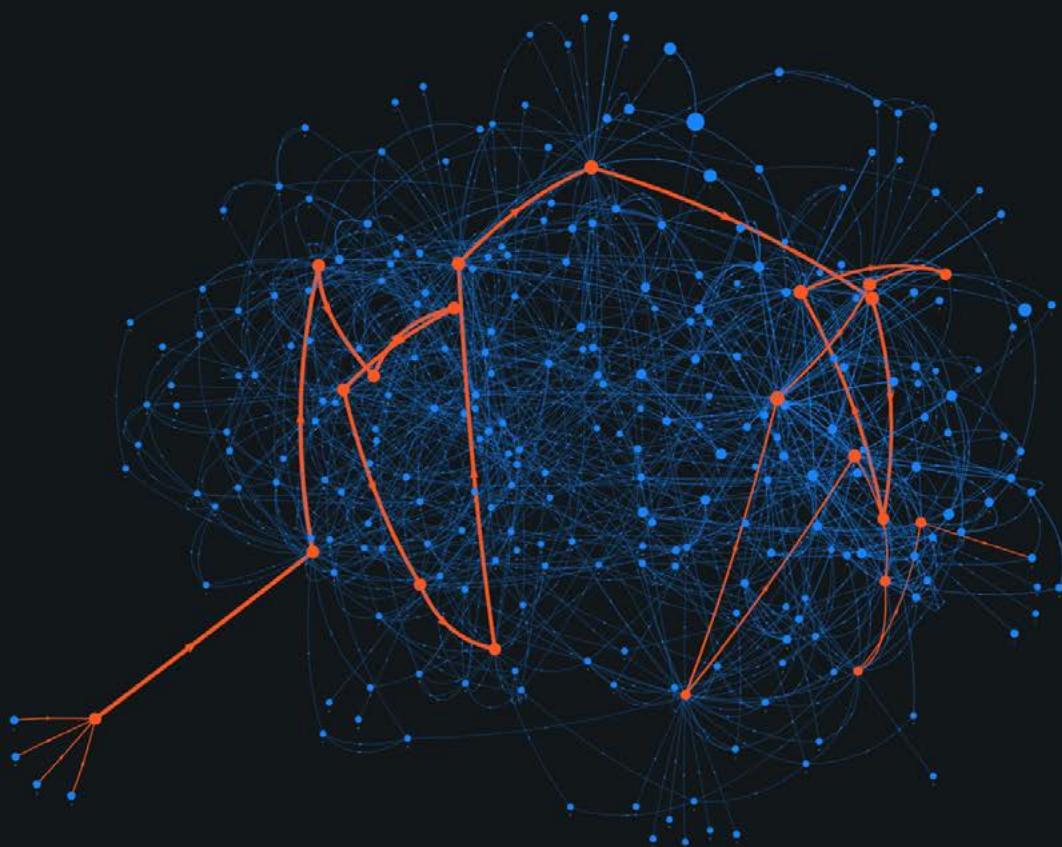
Defeating Change Detection – By identifying change outputs, analysts can track users over multiple transactions. Change is detected with multiple heuristics that can be extremely accurate when used in combination. Two of the most common heuristics are the different script heuristic and static change position heuristic. These heuristics can be broken by wallets with defaults that create like-type script outputs and randomize the static change position. Busting these heuristics makes tracking and automated surveillance more difficult.

Breaking Links with Whirlpool Coinjoin: Even with like-type scripts and randomized static change positioning, the relationship between inputs and outputs of simple spend transactions are deterministic. In a simple spend (1 input and 2 outputs) an analyst knows the single input TXO was used to transfer funds to both outputs. These are called deterministic links. Coinjoins are used to replace deterministic links with probabilistic links and establish forward privacy. A coinjoin is a collaborative transaction where users pool their funds into a single transaction and pay themselves as outputs to the same transaction. In contrast to the old school custodial bitcoin tumblers, coinjoin users remain in full custody of their private keys throughout the process and there is no risk of loss of funds. A small flat fee is paid to the coinjoin coordinator to maintain the service and mitigate sybil attacks.

Each of these features and more, are available on Android via Samourai Wallet and desktop via Sparrow Wallet. Both Samourai and Sparrow can be used with default nodes that require a level of trust in the node provider to serve the wallet client with accurate data and to maintain data security. For power users, each wallet can be supported by your own full node to minimize trust.

Unfortunately bitcoin's defaults disclose TXO composition to counterparties. TXO disclosure allows senders of transactions to evaluate a counterparty's future spending of their payment, effectively allowing tracking of merchants. Likewise, a payment recipient may be able to evaluate a spender's past transactions and future spending by tracking change outputs. This harsh reality is unlike anything available to participants in the traditional banking system and makes application level privacy add-ons, such as coinjoin for establishing forward privacy, critical for maintaining a basic level of privacy when using bitcoin for sending and receiving payments.

Many of these concepts may be completely new to readers who are just learning of bitcoin's privacy issues and trackability. While it's a somewhat steep learning curve for those unfamiliar with these concepts, the journey to competence is a short one that can be mastered with a bit of knowledge and the right tooling. Even if a reader chooses not to use these wallets or additional privacy features, they can get an appreciation for bitcoin privacy weaknesses by auditing their transactions with oxt.me. Stay safe out there. ■



TRACKING BITCOIN: TOOLS FOR OSINT

By Ergo

One definition for anonymity is indistinguishability from a set. Unfortunately bitcoin's default transactions fall well short of this definition. Its basic protection comes from the use of pseudonymous addresses instead of "true names".

Each bitcoin transaction includes a record of sender and receiver addresses and the amounts sent. A copy of each transaction is permanently recorded on the bitcoin blockchain. Thousands of copies of the bitcoin blockchain exist on node hard drives distributed across the globe. Services called block explorers process the blockchain and make it easily searchable for the general public through a web browser.

OSINT practitioners should immediately understand the implications of bitcoin's default privacy and the ease with which the permanent ledger can be searched by anyone.

In the traditional banking system, investigations can be slowed to a crawl by subpoena requests across multiple accounts, institutions, and jurisdictions. With the bitcoin blockchain, investigations can progress as quickly as a target spends funds. Accurate blockchain analysis can often lead to rapid identification of high profile attackers (see the case of the 2020 Twitter hacker).

With a basic toolset and understanding of bitcoin wallet software, OSINT practitioners can

incorporate bitcoin tracking and information into their investigations. Effective bitcoin tracking includes the following steps:

1. Establishing a blockchain starting point.
2. Financial flow analysis also known as a transaction graph analysis.
3. Evaluating flow intersection with known or custodial entities.

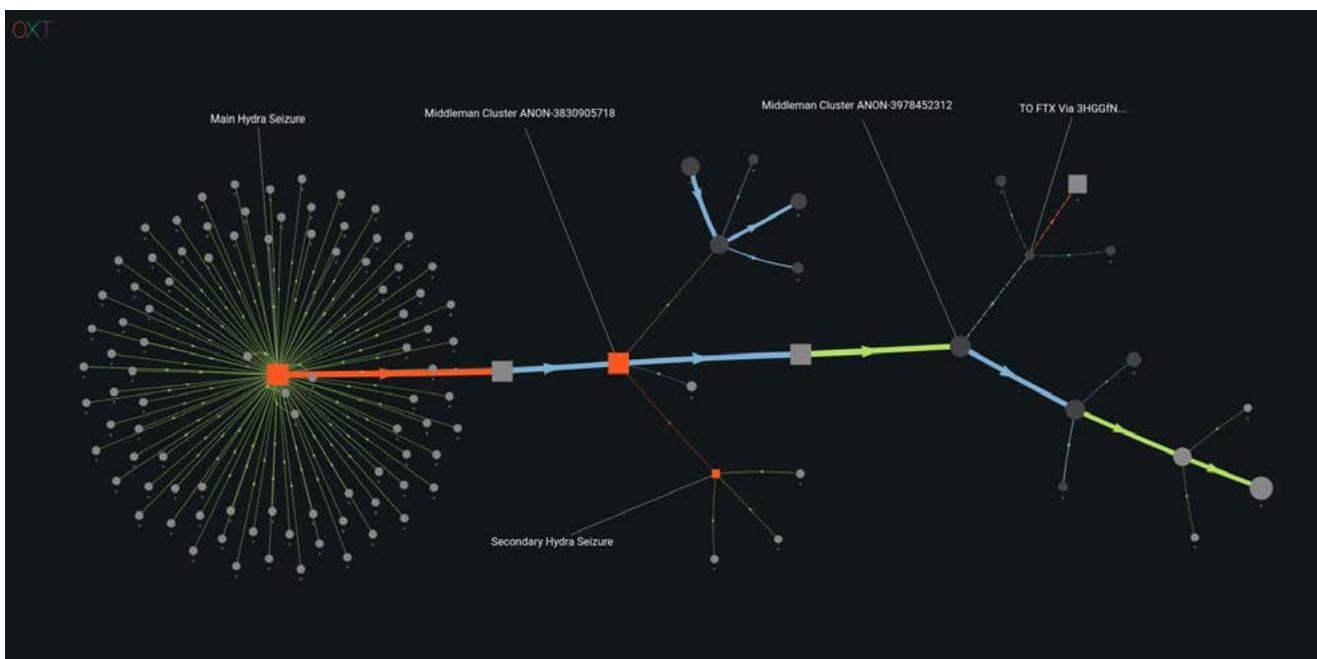
Establishing a starting point: A financial flow analysis needs a reference starting point on the bitcoin blockchain. OSINT practitioners are no doubt familiar with methods for obtaining this information. It is common for bitcoin users to include transaction and

address information in forum posts, social media profiles, and YouTube tutorials.

Financial flow analysis: The relationship and flow of bitcoins can be mapped over a series of transactions. Bitcoin transactions typically include one (or more) payment outputs and a

change output returning the surplus amount back to the spender. Change detection is accomplished with several heuristics about wallet software and normal user behavior. In a financial flow analysis, an investigator attempts to identify these change outputs so that a target entity can be tracked

over multiple transactions. This can be performed by manually mapping transaction details, or the process can be streamlined with a transaction graph tool that visually illustrates the relationship between transaction inputs and outputs. The following is an example Transaction Graph Analysis.



Flow intersection with known or custodial entities: The common input ownership heuristic (CIOH) is used by blockchain analysts to aggregate unique bitcoin addresses into a single "wallet cluster". The CIOH assumes that all transaction inputs are controlled by the same private key or user. Advanced block explorers will automatically evaluate transactions using the CIOH and assign reference IDs to wallet clusters.

Through OSINT techniques or direct interaction with clusters, analysts can add an entity label (exchange, payment processor, etc.) to a wallet cluster. If a financial flow analysis indicates coins have been sent to a custodial entity, the entity may freeze or otherwise help return stolen funds if a subpoena or sufficient information linking illicit activities is provided. Custodial entities, particularly cryptocurrency exchanges, are often required by

regulators to collect know-your-customer/anti-money laundering (KYC/AML) information on user accounts. If this information is provided to an exchange, the pseudonymity of blockchain activity can be broken and a user easily identified. The following is an example Wallet Cluster and Tagged Entity.



Readers of this magazine looking for access to transaction graph tooling and entity labeling may wish to avoid costly subscriptions to the software of surveillance firms that actively collaborate with governments and advocated for privacy destroying KYC/AML policies.

One such community driven alternative is available at oxt.me. OXT, or the Open Explorer Tool, is supported by the developers of Samourai Wallet and bitcoin users. OXT's tooling is normally reserved for surveillance firm subscribers but has been made freely available to bitcoin users so that they may audit their transaction and improve their privacy.

For OSINT practitioners, OXT's public directory of wallet cluster labels includes most of the largest bitcoin exchanges. Like any OSINT practitioners, most of our cluster labeling is obtained through

OSINT techniques and thoroughly documented. To protect the privacy of innocent users, we typically refrain from posting the source of these labels publicly. However, the source of a label can be provided upon request if the label accuracy is in question.

Most surveillance firm transaction graph software is dedicated to oversimplification for naive investigators. OXT's graph includes extremely accurate and detailed information that can be used to eliminate false positives and recognize when coins change hands, a process called wallet fingerprinting.

Additional features can be unlocked by registering for a free account. Registration only requires a pseudonym and password. Providing an email address is opt-in for users wishing to unlock password recovery and additional features such as:

- Details about wallet clusters and address activity are available.
- OXT transaction graph details can be exported to a CSV file.
- Graphs can be commented and bookmarked for sharing in reports.

Bitcoin's pseudonymous default and permanent record of transactions provides an extremely fragile privacy. For many readers, learning of this may be a wakeup call, and the first step to addressing a problem is awareness that it exists. ■

WORRY-FREE CRYPTO LOCKDOWN

At Cryo Security, we offer a full suite of state-of-the-art cryptocurrency and digital asset protection and consulting services for businesses and high-net-worth individuals. Secure your crypto with tailor-made operational security protocols.

FREE OPSEC CONSULTATION

CRYO SECURITY

cryosecurity.io

contact@cryosecurity.io





MY DIGITAL DETOX

By Michael Bazzell

In the early 90's, I bought my first computer. I had no internet access. I spent a few hours every night playing a few games, managing my RAM, and ending with a full disk defrag. It was a simple time. Today, all of our devices are connected to the internet at all times. We are constantly bombarded with notifications, communications, news feeds, social network posts, and everything in between. This is not only distracting to our real lives, but I believe our constant connection takes a toll on our bodies, minds, and sanity.

Over the past few years, I have made a strong effort to minimize my usage of technology. It has not been easy, but I have seen great benefit from my actions. Minimizing eye strain alone eliminates my evening headache and

greatly improves sleep.

This article is not a tutorial or guide. It is not to encourage you to replicate my actions. It is simply a summary of the things which have worked well for me. It is documentation of my digital detox experience.

Searching "Digital Detox" will provide endless tips about how to minimize your own exposure to technology. Unfortunately, most of it tells us to avoid technology for part of the day and go outside. I find this to be an over-simplification of the matter. Most people reading this magazine have a strong connection to technology for both work and pleasure. Telling me to "go outside" or "limit time in front of the screen" is

not enough. I needed more rules. The following strategies greatly reduced my constant connection to my devices and generated a lot of free time which was otherwise wasted.

Desktop vs. Laptop: I have discussed this on the show, but I will repeat it here. At home, I have transitioned away from a portable laptop and rely on a dedicated Linux desktop (System76 Thelio). This makes my time on the computer much more intentional. I boot it in the morning and shut it down when I am done working for the day. When I was using a laptop, it went everywhere with me. I found myself on it when I was supposed to be watching a movie or spending time with my family. There was always one more email to read, one more message to respond to,

or a desire to refresh my RSS feed to see what I had missed in the last hour. There are many nights when I realized I had wasted the entire evening within various online rabbit-holes. Now, when I walk away from my office, I am forced to leave the computer behind. Spoiler alert: all messages and feeds are there when I return the next day.

Home Mobile Usage: I possess a home Wi-Fi mobile device which I use for all communications within the home. The only apps present are for secure comms and email. I never use it to browse the internet or stream media. It allows me to leave my computer behind every night, but also allows me to be available to my family, friends, and staff if needed. It helps me stay away from the computer, and minimize the time checking the status of my communications.

Internet Restrictions: This option will not be popular. Every night around 9pm, I shut off the internet. All of it. The incoming modem, my firewall, and the Wi-Fi. This eliminates any possible connection since all cellular is prohibited in the house. This forces me to detach for the rest of the evening and prevents me from getting sucked into the next message or crisis. There have been too many times when I checked on something at 10pm, then worked on it for hours, when it could have waited until the next morning. I respect that many people cannot do this due to family or employer outrage. Consider your own modifications.

Site Restrictions: This was a huge step for me. I found myself wasting a lot of time on Reddit, Twitter, YouTube, and other outlets until a year ago. In 2021, I configured my firewall to completely block multiple social network and media domains. This prevents me from accessing the sites which had wasted too much of my time. Once a week, I disable this to post the podcast to Twitter, but it gets re-enabled quickly. This helps me focus on my work and

typically shaves off a few hours of the day.

Analog Re-Introduction: This is where my digital detox steers away from standard digital recommendations. This will require some background, so please hang in there with me. In the early 90's I became a teenager obsessed with music. I had a great home stereo system with a huge collection of rare vinyl records. I will spare you the genre or any name-dropping. Along the way, I became an adult, moved many times all over the country, and my prized stereo system was sold in pieces during various stops. Most of my albums were sold on eBay or given to friends. I miss them (the albums and those friends).

When I worked throughout the day, I would have music playing at all times. If I was not lazy, I would create a playlist in Kodi from my digital MP3 collection. However, I would usually throw on SiriusXM, a live radio feed, or another streaming service. These endless audio transmissions encouraged me to sit non-stop in front of my computer while listening to digitally-compressed versions of my favorite songs. I found this mentally and physically unhealthy.

This year, I decided to replicate my teenage analog stereo setup in my office. I needed a decent receiver, speakers, and record player (turntable). I began shopping online and discovered that things have changed. Receivers now rely on Bluetooth and speakers are "iPhone ready". There are plenty of high-end providers which still value the analog experience, but this comes at a cost. I abandoned my online search and went to a thrift store.

I was pleasantly surprised to see an abundance of stereo receivers from the past few decades. I picked up a Sony STR-DE605 100-watt per channel receiver with a dedicated Phono input for \$25. I found some nice older Klipsch floor speakers for \$50 (marked down from \$100, but originally retailed at

over \$700). Thrift stores are often eager to get rid of large floor speakers. Now, I just needed a turntable.

Vinyl records have made a huge resurgence, which has made record players more popular than ever. The thrift store had some, but they were way overpriced. A generic used turntable ranged from \$85-\$100. Most were extremely scuffed, and some were missing needles. No thanks. I wanted a new player with a fresh needle.

I returned to online shopping and discovered that a few companies were making affordable standalone players priced from \$100-\$200 for basic models. I read the reviews and jumped in. I chose the Crosley C100 turntable (crosleyradio.com). The retail price is \$169 but there are often discounts online. This was a step up from the introductory \$100 Crosley T400. Both have a similar needle, but the C100 has an adjustable tone arm (to help preserve my new upcoming record collection) and better pitch control. That was important to me and was missing from other affordable models.

Crosley is known for all-in-one units that have an embedded amplifier and speaker which can often be found in retail stores such as Target. I don't like those because they typically have low-powered amplification and don't provide the sound I am looking for. I wanted a standalone unit which I could connect to my own receiver via analog RCA connections. The C100 was just what I needed, and sounded great through the phono preamp. It is the unit in the header image of this article (by the way, the first reader to identify the album visible within the image receives a free hardcover copy of *Extreme Privacy*). My friends who still own \$3,000 turntables will scold me for this choice, but I just wanted an old-school analog experience. I no longer wanted to vacuum my records before I played them. I wanted a workhorse, not a show pony. I am also not confident

they could tell the difference between the two in a blind test. That statement will trigger a few readers.

You are likely wondering why I am going on about a record player. This is not just a nostalgic self-indulgence. Today, when I am at my home office, I play vinyl records while I work. Sure, I get that warm sound and crackle of the records, but there is a reason more relative to this article. Every 20-25 minutes, the record reaches the end and I am forced to stand up, stretch my legs, flip the record over, and begin the other side. When I do this, I force myself to look out the window and gaze at a distance for a few minutes. This is a huge relief from computer eye strain. Without this required music break, I would often sit in front of the screen for hours uninterrupted. The inconvenience of records helps my eyes, back, legs, and blood flow. As I write this, a record just ended. Up I go.

Instead of live radio feeds or music streams, I have re-embraced terrestrial radio. I attached a decent FM Dipole

antenna to the Sony receiver and located a community music station matching my preference. It is truly live and does not require my desktop computer to function.

Paper: Next, I have a new fondness for paper. I am an avid reader, and I now try to consume a traditional paperback book at least once a month. My e-reader is better on my eyes than a screen, but a paperback book gives me a better sense of leaving the digital world for a while. I understand the irony of this statement within a digital PDF.

This also applies to notes. Whenever I shut down for the day, there is always a collection of topics on my mind for the next day. I no longer track them in a digital form, I now take some time to write down my thoughts and tasks on paper with a pencil. This has taught me two things. First, writing things down helps me eliminate them from my mind, which helps me detach for the evening. Second, my handwriting is awful. I have no idea when that happened.

Fluids: My last modification is to drink much more water. I always have liquids by my side now. This is not necessarily due to the health benefits of high water intake (there are many), but it forces me to get up from the computer more often to find a toilet. I also find caring for my dog can be a great distraction from screens. The theme here is to keep moving throughout the day.

Every day, I believe I now eliminate at least two hours of time wasted in front of a screen. Again, I don't write this to tell you what you should do. I write this only to share what has helped me ditch technology on occasion in order to reclaim a balance of life versus work. I hope you find your own techniques which help you recover some personal time, health, and enjoyment. ■

Is privacy and security overwhelming? We can help.

Whether you are ready for a complete anonymous relocation with a full privacy reboot or simply need a one-hour call directly with Michael Bazzell, we can eliminate the frustrations encountered when trying to be invisible.





Image: Dan Dimmock

THE OSINT CORNER ↗ RESEARCHING EMAIL ADDRESSES: 15-MINUTE THREAT ASSESSMENT

By Jason Edison

Jason instructs live and online open source intelligence courses for IntelTechniques in addition to working as a cyber-crime detective for a large U.S. police department. Each issue will feature an OSINT tactic from the IntelTechniques online training.

Recently in class we were discussing the various approaches we might take when investigating an email address and how our workflow varies depending on the mission and any associated constraints. A common mission type in my world (US Law Enforcement) is a quick threat assessment. This typically involves investigating a potential threat to an individual, group, or event where the only leads to work from are the sender's email address and the message content. With that context in mind, let us look at my standard workflow for a 15-minute email investigation.

We always start a new mission by clarifying our primary goals as well as any constraints, such as the deadline for delivering our findings. In this type of scenario, we often have a very short

window to assess the seriousness of the threat and so I tend to refer to these as 15-minute threat assessments. Our interest is in answering the following questions as quickly as possible.

- Is the threat credible?
- Does the suspect have the intention to carry it out and do they have the means?
- Who is the real person(s) responsible for the threatening email?

The affirmation of our mission goals can be as simple as a quick mental acknowledgement or a short notation at the top of a notepad. Remember, the mission constraints for this type of threat scenario dictate

a quick assessment rather than a long investigation, so every step of our workflow is condensed. With our concise goals in mind, we move on to the following four primary investigative steps.

Content Analysis: We review the body of the email first because this may provide us with contextual intelligence that will benefit us during the later phases of the investigation. What motivates the sender? Do they use any unique language that might be worth searching for? For example, we sometimes review threatening emails which contain language from manifestos and extremist blogs. A quick Google search with the unique phrase in quotes is a long shot but can sometimes be fruitful in generating new

leads. Do they use any unique jargon or slang?

Header Analysis: Next, we should attempt to rule out that the “from” email address was spoofed. We do not want to spend time investigating an email address that isn’t correct, so reviewing the email header may reveal indications of address spoofing. Alternatively, it may increase our level of confidence that the email address of the sender is valid. The exact steps for accessing the email header will vary depending on your operating system and the client you use to view it. For our purposes, the following uses the Outlook application on Windows as an example.

- Double click the message in Outlook to open it in its own window.
- With the message open in Outlook, click on “File” in the upper left-hand corner.
- Now select “Properties” towards the bottom middle of the window.
- The bottom of the screen will have a box titled “Internet headers”.
- Click your mouse pointer anywhere in the box and then hit ctrl-A to select all text in the box.
- Hit ctrl-C to copy the highlighted header text.
- (Optional) If you are not experienced reading headers, you may want to paste the header data into a header analyzer such as <https://mxtoolbox.com>EmailHeaders.aspx> or <https://dnschecker.org/email-header-analyzer.php>.
- MxToolbox has an extensive list of instructions for pulling header data from various email clients at <https://mxtoolbox.com/Public/Content/EmailHeaders/>. Even within the Microsoft ecosystem your steps may vary depending on your operating-system and method of viewing the email file in question.

If you are new to header analysis it can be quite confusing, but some key data fields to review include the following.

- **Received From:** This lists the hostname of the sending server. If it does not match with the purported sender that may be an indication of illegitimacy.
- **Return-Path:** This shows the address the message was sent from. Some spoofed emails will fake the “From” field of the email itself but not the Return-Path in the header data. Compare this data field to the “From” field of the email message.
- **X-Originating IP:** This field may contain the originating IP address for the sender’s mail server. Use the IP queries in the IntelTechniques custom OSINT tools to research this IP address at <https://inteltechniques.com/tools/IP.html>.
- **Received-SPF:** This indicates if the sender has a valid SPF record and if they do the purported sender address is more likely to be true.
- **DKIM & DMARC:** These fields may also provide a higher level of confidence as to the legitimacy of the email’s sender. Even a legitimate email may not pass each of these validation tests, but each “PASS” increases the likelihood that the sender was not spoofed.

Email Address Research: This is your traditional OSINT phase of investigation.

- Start by querying the sender’s email address through the custom OSINT toolset at <https://inteltechniques.com/tools/Email.html>.
- Assess the “reputation” of the address. How old does it appear to be? Do we see associated accounts such as social media? For example, <https://emailrep.io/> can be valuable in showing if the email address has a history of use.
- The context of the email content may be important when analyzing

your query results. For example, if the demeanor of the email narrative is threatening and we start to see a lack of any history associated with the email address, the odds increase that it was a burner email account set up specifically to send the threat. Even the type of email service used may be an indicator. For example, a threat sent from a Protonmail address may indicate technical sophistication and/or an intention to obfuscate the sender’s identity.

If you exhaust the queries included in the online toolset and find no results, our next steps will vary based on your policies and authority.

- **Breach Data:** If you have access to breach data and are allowed to use it on your investigations, then querying breach data for the sender email address is the next step I recommend. Be certain of your agency’s policies and any legal constraints in your jurisdiction pertaining to the use of breach data.
- **Legal Requests:** If you have legal authority or subpoena power and there is probable cause of a crime, you may wish to submit a legal request to the email provider. For example, if we verify that the sender has an outlook.com domain, we will then look up the appropriate contact for outlook.com (Microsoft) at <https://www.search.org/resources/isp-list/>.

Trackers: This option is not part of a typical 15-minute assessment, but we do get questions about the use of trackers from time to time. If we exhaust all other methods of identifying the true sender of the email in question, we might consider utilizing a more offensive tactic such as trackers or loggers. Before utilizing any type of tracking code, you must be certain that doing so is within agency policy and is legal in your jurisdiction. This tactic is much more aggressive and privacy invasive so it will be beyond the acceptable scope of most investigations/operations.

- Tracking Token:** This involves sending an email containing tracking code to the target address. A very simple version of this would be creating a document with embedded tracking code on <https://canarytokens.org> and then sending that document to your target in hopes that they will open the attachment and activate the embedded code. These tokens can be hit and miss since they are often blocked by security software and network security appliances. This is a low success rate, last resort, measure as there is always a chance that your target will detect the attempt. Most government and law enforcement agencies will need a court order to deploy these types of trackers.

- Tracking Site:** A slightly less aggressive approach would be to bait our target into visiting a site that contains code to log the IP address and browser fingerprint of any visitors. This is typically viewed as less invasive than a token because we are not sending malicious code to our target. We would set up a web site with a

page like <https://inteltechniques.com/logger/> and then send the target an email coaxing them to visit the site. This can be any type of ruse as long as it is within agency policy. If we are successful and they visit our site, we have a chance to collect their session data. Keep in mind that even if you successfully get their IP address using this technique, they may be using a VPN or a proxy to hide their true internet address. (The logger example provided here is a page we have set up purely for defensive and demonstration purposes.)

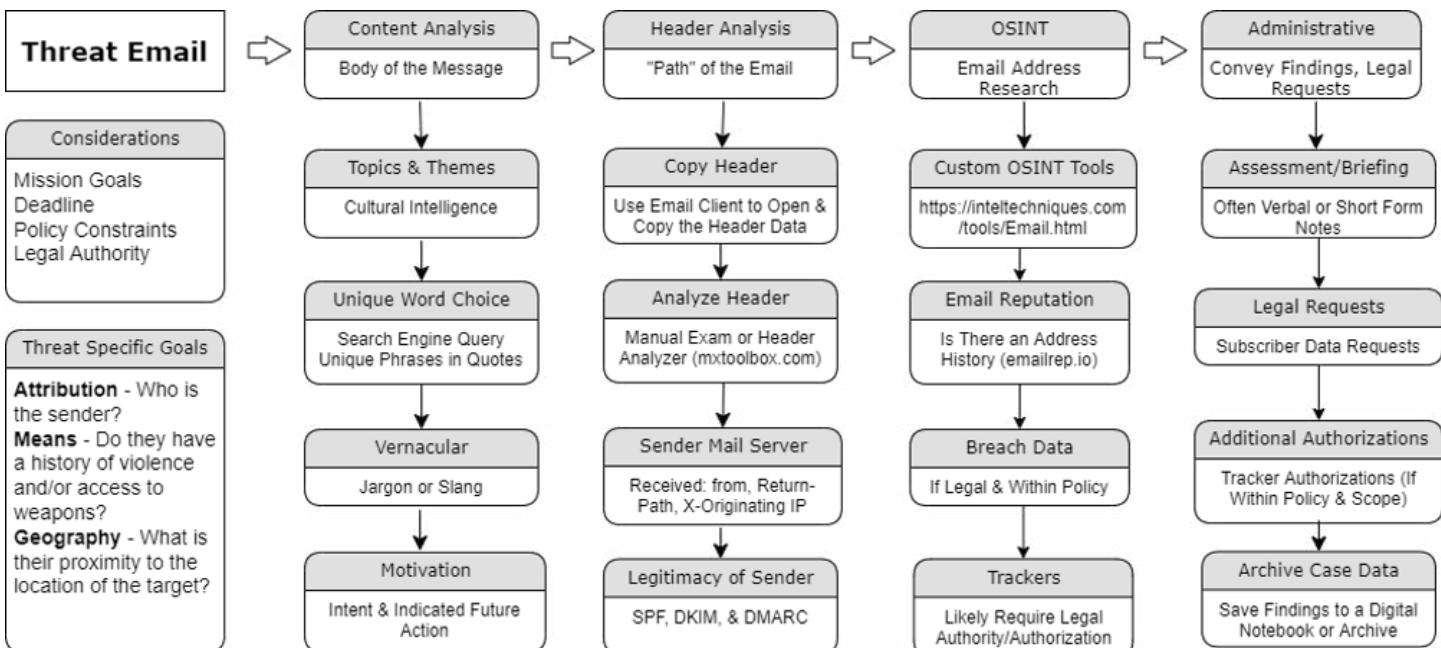
Assessment/Briefing: In shorter engagements we often will not have the time to write up a full investigative report, so we will provide a quick verbal assessment. Whether you are providing a written or verbal briefing, break your intelligence down into the following key findings which should reflect the previously established mission goals.

- Is the threat credible and why do we believe so? This portion may contain details such as verification that the sender of the email lives in the same geographical area of

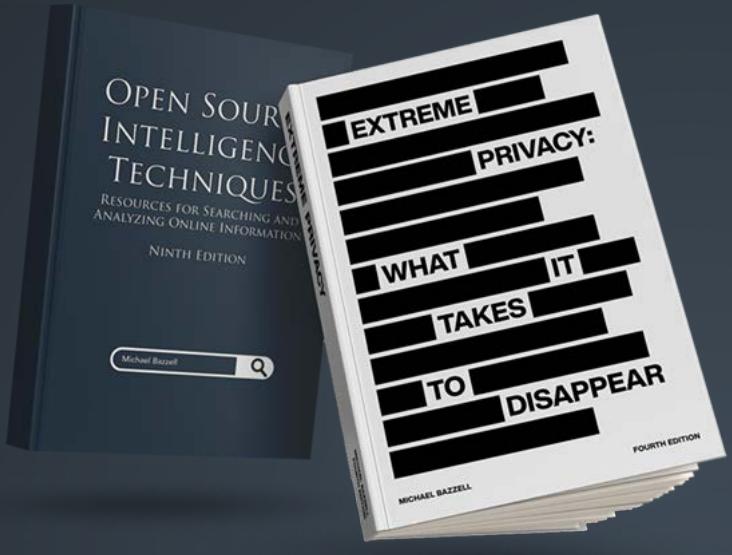
the target or intelligence from their social media indicates likely access to weapons.

- Attribution:** Were we able to identify the real person or group behind the threatening email? Do we know where they live, sleep, work, etc.? If appropriate we can deploy a team for either apprehension or field surveillance.
- Did we locate any other actionable intelligence pertinent to the mission?

At this point we have likely exhausted our limited window of time for gathering intelligence based on our threatening email. Hopefully, these steps provide a framework and some ideas on how to proceed for anyone new to short, high pressure OSINT missions such as threat investigations. If our investigation timeline expands, we will transition to a deep dive and utilize further queries and tools to hopefully uncover further intelligence on our target. Your own workflow may vary, and always be certain of the policies and laws where you work and stay well within those boundaries. ■



New 2022 Privacy & OSINT Books



- ✓ Hardcover & Paperback
- ✓ New & Updated Content
- ✓ 500+ Pages Each @ 8.5 x 11
- ✓ Our Full Playbooks
- ✓ Supports This Free Magazine

Order at IntelTechniques.com

OSINT & Privacy Video Training

90+ Hours of Video Training | Optional OSIP Certification

Register at IntelTechniques.net

Open Source Intelligence
Video Training + Certification

\$899.00

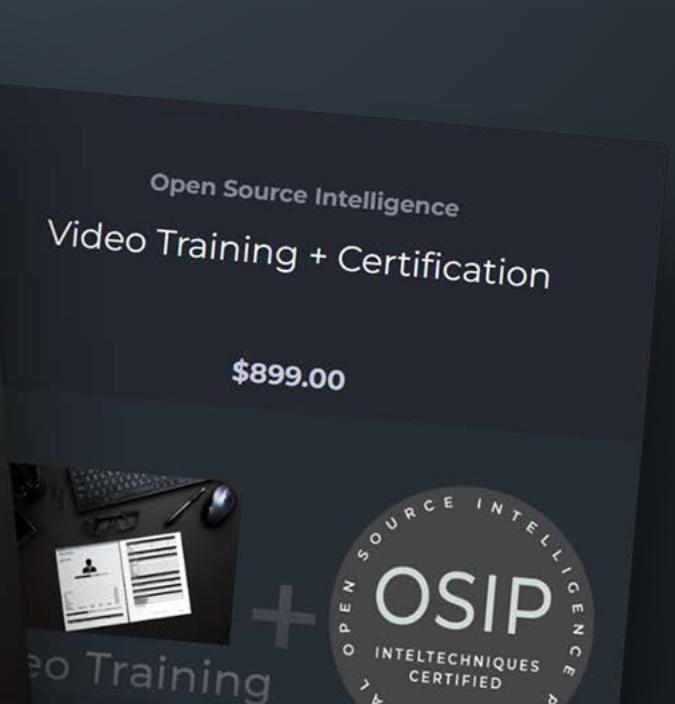




Image: Dima Solomin

MOBILE OSINT MASTERY: UTILIZING IOS SHORTCUTS AND TELEGRAM

By Anonymous

Let's be honest, mobile OSINT work is terrible. I've spent the last couple of years trying to figure out the best possible way to execute tasks on the run. And no matter how good I get on mobile, a desktop environment is always more efficient. But since I spend most of my day on the go, I have to rely heavily on mobile. Aside from using pre-made online tools, I usually end up snapping screenshots, manually archiving, sending myself links into a note application, and marking videos to "watch later". At the end of the day, what I've done on mobile is to decrease my efficiency.

I needed a way to make the workflow actually flow. Having online tools and sites in my bookmarks is great. But I wanted to get as close as possible to automating the tasks involved in my research. My goal was to make mobile as smooth as working on my desktop. I'm not there yet, but I've gotten pretty darn close. By utilizing iOS Shortcuts and Telegram bots, many of my tasks done on mobile are nearly painless.

I rely heavily on [Archive.org](#) and Archive Today. Most of my subjects are heavy social media users. So archiving their posts immediately is absolutely imperative. While Archive.

org does have a decent mobile app, I prefer Archive Today for its ease of use, especially for the less tech-savvy people that I will pass the information onto. But Archive Today does not have a mobile app. And if you've ever tried to submit an archive to that site on mobile it's not fun. Let's list the actions so you can appreciate the headache. First, open a new tab, then navigate to the web page. Return back to the page you need archived, copy the link, return to the Archive tab, paste it, and click "Submit". That's seven actions. Do that 20 times in a row on mobile and you'll want to throw your phone into the nearest sewer.

With iOS Shortcuts I was able to write a simple search for Archive Today that is a single button in my share sheet. It will query Archive Today with the page link. If the page is not already archived, it's now two clicks. "Archive this page" (which brings the URL over to the next page) and then click "Submit". I've trimmed 70% of my time when compared to doing it the original way. Not bad, right? It's fairly simple to write these shortcuts if you choose. I can already hear the tech novices sucking their teeth. Don't worry, we're on the same team. I don't know how to code at all. That's why it's easier to utilize pre-made Shortcuts from the sizable enthusiast community. My Archive

Today shortcut is the result of viewing someone else's automated search query and just plugging the Archive Today URL in its proper place.

Having a handful of options available right in your share sheet really speeds up many tasks. So if you have to conduct your research on the go let's make it as painless as possible. You'll notice a theme here: most of these revolve around search queries. And since a lot of OSINT research is made up of search queries, we are effectively doing what we would normally do on desktop. If you don't like the idea of having a long list of Shortcuts in your share sheet, you can also make these into standalone apps on your home screen. Here are my most used shortcuts on iOS. Most are easily found on [RoutineHub.co](#) and the r/Shortcuts sub reddit.

Archive.today Search (<https://www.icloud.com/shortcuts/be19f16d6ac7485bbe7c0adcc1db793a>): As mentioned above, this reduces the actions to archive a page on mobile by 65-70%. It works with any URL. By copying to the clipboard and inserting it into the search URL for the site, it makes an automated query. The good news is that if you're archiving social media posts, many times I get a positive search and it shows me an archive already exists. Task complete.

Twitter to Nitter (<https://www.icloud.com/shortcuts/c790a0f72c314e4ab8b65bfba09dcfad>): We all know that the Twitter can be a pain to view. If you're on Safari mobile, after a short scroll it will put a huge pop-up over the screen rendering it useless if you're not signed in. You can't close it out either. But Nitter is a front end for Twitter that displays all of the content on Twitter without tracking you and doesn't use a pop-up to block you from scrolling. The problem is that opening a tweet in Nitter is tedious. You have to copy the Twitter URL, edit the URL to add in the Nitter instance website, then hit enter. Now, I can view tweets and thread on Nitter with the click of a button. The "View on Nitter" shortcut I created, does all of that work with one click.

Search On (<https://www.icloud.com/shortcuts/654c5fc552244c439ff52ec5e16b7594>): this tool became one of my favorites. In the early stages of an investigation this shortcut acts much like the prefabricated set of tools from Intel Techniques. You can highlight any text, click the share button, and search your selection on a variety of websites. Naturally all of the search engines are there, and much more. The shortcut is written to search everything from IMDB, Wikipedia, Maps, Twitter, Reddit, and it can even conduct image searches on all of the major search engines. Want to add sites? No problem. Just add the query into the shortcut. It is your own custom search pages rolled into a single button. I keep Search On as a dedicated App on my phone's home screen along with a variation for just Twitter user mentions. This way I don't even have to go to Twitter or a search engine first. I simply click the icon, follow the prompts, and get taken to my results.

Open Link without Tracking (<https://www.icloud.com/shortcuts/91f4cdf5abf54a629a6054979c67fdb6>): While this is geared towards the privacy side of being a digital ninja, I use it often while conducting research because it's always good practice to avoid tracking. This shortcut will remove all tracking and share ID's

from popular sites. Since I sometimes do research with others, and we share links to groups, I think its best practice to not contaminate the group. And a trimmed URL with all tracking removed is a great first step.

Phone Number Lookup (<https://www.icloud.com/shortcuts/07777ab5d9bb4a02bfc95d80bc4dd597>): This option allows you to look up a phone number on Smart Background Checks. If you have a site you prefer over this one, just change it in your shortcuts. Want to search multiple background check sites? Copy the "Search On" shortcut above and remove the sites you don't want, and add in the ones that you do want.

DorkCutz (<https://www.icloud.com/shortcuts/d21ea7ebff0e4b4fbc541c250bb10d8d>): This shortcut uses Google Dorks to find files. Its modified from a useful custom Google Search engine focused on finding "direct download links for almost anything".

ExtractPDF (<https://www.icloud.com/shortcuts/72fa43eb8f2f4fcc8df0d9c2c831e3f5>): Have you ever gotten to a web page and seen an embedded PDF that seems impossible to download? I have. And we can avoid that now with this shortcut. The web page loads, recognizes the PDF that is there, and then extracts it and saves to your files.

We've barely cracked the surface. If you're eager to try this out I'll give you the best starting point. Routine Hub is a site where Shortcuts authors post their creations. Many are updated regularly and there is a steady stream of new and useful tools available on that site. Like anything related to OSINT, things will change. Tricks will stop working and some functionality may be completely lost in the future. But I encourage people to embrace the Shortcut. It's your first step to making mobile OSINT virtually painless. Step two? Obviously automated archiving for later retrieval. For that I utilize Telegram. The functionality and features of Telegram is unmatched right now. While I know that many have problems with the privacy issues that come with using it, I'm confident that limited use with

a VOIP number can be safe enough. The benefits outweigh the risks for me. Even if you decide that Telegram isn't going to be in your toolbox, just using Shortcuts has gotten you most of the way towards the goal of fast, painless mobile OSINT.

If you choose to utilize Telegram, here are a few bots and tools that I use to ensure I have cloud-stored backups. The app allows for up to 2.5gb per file. That's massive and it will handle nearly everything that requires archiving while I am stuck on mobile. My workflow on mobile starts like this: something happens, a subject (people, place, thing, or event) is identified, and I immediately make a channel for this topic. I then add bots to the channel so that every link I send from the share sheet is retained, and when applicable, media is automatically extracted, downloaded, and uploaded into the channel. This isn't pass-through or embedding of media. It is a legitimate separate copy. That way if the source vanishes, I'm in good shape. I now have my own copies and I haven't eaten up any of my own storage. I've never given Telegram my phone number because it accepts MySudo VOIP numbers and I can stay sandboxed.

YouTubeDL (@YtbDownBot): That's right, one my most heavily relied upon tools has an automated bot on Telegram. It's packed with many of the same features that are available in the desktop client. You can download the entire video, entire playlists, create clips with time stamps, extract just the audio, take a screenshot at a specific time, download the thumbnail, or change video quality. YouTubeDL bot grabs video from a large selection of sites so don't limit your archiving to just YouTube videos. If this bot won't do it, Video Download Bot will.

InstaSave(@Instasave_bot): Download Instagram videos, posts, and Reels with this bot. A few of these exist on Telegram and there is one downside to this bot: every 24 hours you have to subscribe and like a post in their main channel. It's a small price to pay for such a useful bot.

Twitter Media Downloader (@[twittervid_bot](#)): This bot will download both media and the original tweet text with a link to the original tweet and embed into one post. Twitter is notorious for deleting content and suspending users so I've found this bot to be one of the most helpful on the platform.

PDF Bot (@pdfbot): Send any web page to this bot and it will turn that page into a pdf. And its hosted for free on Telegram. I've run into sites that would not archive correctly and this was the only recourse. It's much easier than trying to screenshot a full page on mobile.

TT Save (@ttsavebot): A Tik Tok save bot similar to the Twitter media downloader. Keep in mind that while using the app, Tik Tok creates a unique share ID that links directly to your profile.

Those are just the pre-configured bots. Many more exist and are just waiting to be discovered. I have everything

from video archiving, Temporary Email, additional VOIP numbers, transcribing service, and Translation bots. Nearly anything I could do fast on desktop is now available on mobile via Shortcuts and Telegram. Just recently I was asked to research and monitor a subject that utilized Substack and YouTube multiple times per day. The person was known for deleting or editing content frequently. So how can I go about my day while ensuring that I don't miss anything important and store everything? Simple, I created my own bot on Telegram to grab the RSS feed of both YouTube and Substack. I then created a channel and added the bots I created; they will now post directly to this channel.

Next, I added the YouTubeDL bot to the same channel. If the subject makes ten posts per day and uploads 5 videos per day, I automatically have separate archival copies being hosted online for free. While the Substack post will only show a preview, I can use my Shortcut to send to Archive Today and share directly to the channel. Later, I can

peruse them at my leisure and I didn't have to be tied to a desktop or spend all day fooling around on my phone. When the investigation ends, or a party needs the content and won't use Telegram, I can just export the entire channel. If the channel can be public, then no one needs to install or use Telegram. They can view all of the content right in a web browser without an account.

I've only just touched the surface here. More tech-savvy users can get much more efficiency and functionality out of these two sets of tools. Both Telegram and Shortcuts provides endless opportunity for investigators to retain their edge even when removed from their desktop environment. No longer do I dread having to start an investigation while being away from my desktop. My cleanup and organizing later is not a complete mess of bookmarks and links sent to a Note-like application. I've successfully mastered mobile OSINT without needing to learn to code. This means that with a little practice, you can too. ■



**MDR | XDR | INCIDENT RESPONSE | PEN TESTING
VCISO | WEB3 & BLOCKCHAIN | MANAGED SIEM
HELPDESK | IDENTITY MANAGEMENT
DISINFO MANAGEMENT**



**REAL-TIME THREAT
DETECTION**



**REAL-TIME THREAT
RESPONSE**



**PROTECT YOUR ENTIRE
NETWORK**



**PEN TESTING AND
VULNERABILITY SCANNING**



**REDUCE YOUR IT/SECURITY
WORKLOAD**



**AFFORDABLE
PRICING**

FORTIFY24X7.COM | (800) 989-2647 | INFO@FORTIFY24X7.COM



ARCHIVE SITE REMOVAL GUIDE

By Michael Bazzell

Anything posted to the internet stays online forever. Well, sort of. Services such as [Archive.org](#) and [Archive.Today](#) aim to preserve all websites, which can be an unwelcome feature for those who wish to erase their past. Fortunately we still have some privacy powers which can be executed to remove undesired content associated with the domains which we own.

Archive.org Removal

If your website(s) appear on Archive.org, you may want to eliminate any sensitive historical details. This could include an old family photos site or a self-hosted blog which has not aged well. Archive.org now ignores robots.txt and "NOARCHIVE" tags. Conduct ALL of the following for best removal results and consider the option which follows to prevent new exposure.

- Search your domain at <https://archive.org/>

- Document any domains which display sensitive content.
- Add the following to a robots.txt file on your site.
- (Create a new file if one is not already present.)

User-agent: archive.org_bot

Disallow: /

- Create a file called verify.txt at the root of your site.
- Add the following text and save.
`please remove from archive.org`
- Generate an email from an address at the target domain.
- Direct the email to info@archive.org.
- Create a Subject of "Domain Removal".

- Insert the following text, modifying for your needs.

I am NAME owner of DOMAIN. I'm officially requesting the immediate removal of my site from all archive.org products. The "User-agent: archive.org_bot Disallow: /" code present in our robots.txt file is not being honored. It can be seen at:

<https://DOMAIN/robots.txt>

I am requesting removal of DOMAIN from all stored dates, including today, and all days going forward. I have been the sole owner of this domain since inception. I have sent this message from an address hosted at the domain which should be removed. I have also placed a confirmation message at the following link:

<https://DOMAIN/verify.txt>

Thank you for your prompt attention.

DMCA Notice:

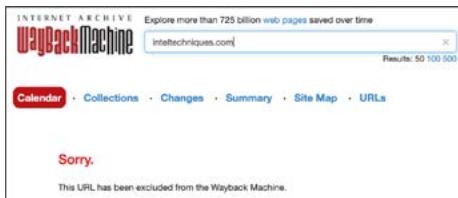
I am the site owner and sole copyright holder for each of the domains cited above. This letter is official notification under Section 512(c) of the Digital Millennium Copyright Act ("DMCA"), and I seek the removal of the aforementioned infringing material from your servers. Archive.org does not have any right or permission to reproduce, sell or display my websites in any way, shape or form. I am providing this notice in good faith and with the reasonable belief that rights I own are being infringed. Under penalty of perjury I certify that the information contained in the notification is both true and accurate, and I am the copyright owner and therefore have the authority to act on behalf of the owner of the copyright(s) involved. Thank you for your prompt assistance with this matter.

NAME

DOMAIN

- Wait 24-48 hours for a response.
- If challenged, provide receipt of domain purchase.
- If required, provide receipt of domain renewal(s).
- Send PDFs, never screen captures.
- After removal confirmation, search to confirm.

The following is the desired result.



Archive.org Prevention

- Add a robots.txt file on your site with the following.

```
User-agent: archive.org_bot
Disallow: /
```
- Modify your .htaccess file to include the following.

```
RewriteEngine On
RewriteCond %{HTTP_USER_AGENT} (archive.org_bot) [NC]
RewriteRule .* - [R=403,L]
```
- If using Cloudflare, add the following to a WAF rule.

```
(lower(http.user_agent) contains "archive")
```

While the robots.txt will be ignored, it can be cited later if the site is published again. The .htaccess modification prevents the Archive.org crawler from accessing any pages stored on your server at that domain. The Cloudflare option prevents any agent including "archive" within the string.

Archive.Today Removal

- Search your domain at <https://archive.ph/>
- Document any captures which display sensitive content.
- Some URLs may appear as "<https://archive.ph/jCqte>".
- Click any capture of concern.
- Click "report bug or abuse" in the upper-right.
- Insert your name.
- Insert an email associated with the domain.
- Insert any burner VOIP or generic number.
- Select an "Abuse Type" of "Copyright".
- Send the following message.

I am the owner of DOMAIN and

respectfully request removal of this capture and all other captures from DOMAIN.

DMCA Notice:

I am the site owner and sole copyright holder for each of the domains cited above. This letter is official notification under Section 512(c) of the Digital Millennium Copyright Act ("DMCA"), and I seek the removal of the aforementioned infringing material from your servers. Archive. Today does not have any right or permission to reproduce, sell or display my websites in any way, shape or form. I am providing this notice in good faith and with the reasonable belief that rights I own are being infringed. Under penalty of perjury I certify that the information contained in the notification is both true and accurate, and I am the copyright owner and therefore have the authority to act on behalf of the owner of the copyright(s) involved. Thank you for your prompt assistance with this matter. Thank you.

- Complete Captchas until "Message Sent" appears.
- After removal confirmation, search to confirm.
- If ignored, submit DMCA to webmaster@archive.today.

Archive.Today Prevention

[Archive.Today](#) does not honor robots.txt or meta tags within HTML. They also do not specify any unique User Agent when cloning a page. The only way to block them is to block their server IP addresses completely. Add the following to your .htaccess file at the root of your domain.

order allow,deny

Deny from 198.245.53.182

Deny from 37.1.213.27

Deny from 5.188.0.77

Deny from 37.1.213.27

| allow from all

If using Cloudflare, add the following to a WAF rule.

| (ip.src eq 198.245.53.182)

or

| (ip.src eq 37.1.213.27)

or

| (ip.src eq 5.188.0.77)

or

| (ip.src eq 37.1.213.27)

This prevents their current servers from accessing your pages. However, if new servers are added, this could fail. Attempt to capture a non-existing page, such as inteltechniques.com/fakepage.html, but from your own domain, on archive.ph. If you receive an error from Archive.Today, you are protected. If the page is captured (even with a 404 error), analyze your web server logs for the IP which accessed the page, then block it.

Google/Bing Cache Removal & Prevention

If you do not want your site to be historically collected as a "Cache" file and presented within every Google or Bing search, add the following line within the "head" section of every HTML page on your site. If using WordPress, copy it to the header.php file within your theme.

```
<meta name="robots" content="-noarchive">
```

The next time Google or Bing indexes your pages, they should remove any cached copies.

Archive Content DMCA

You may find content within Archive.org or Archive.Today which violates your copyright. This could be a PDF of your work, photograph taken and owned by you, or a video which was pirated. If you do not own the domain which hosted this content, then you must rely on a traditional DMCA takedown request. This will be more likely to exist

on Archive.org, as Archive.Today does not capture PDFs, videos, and other media. The following email to info@archive.org should assist.

The following content, to which I hold copyright, has been illegally uploaded to your service, please remove it immediately:

[link to Archive.org page]

The following confirms my claim of copyright

[link to external proof of ownership page]

Please consider these overall strategies when you encounter additional caches of your content on the internet. This article has been posted to my site at <https://inteltechniques.com/archive.html> and any updates will be posted there. ■

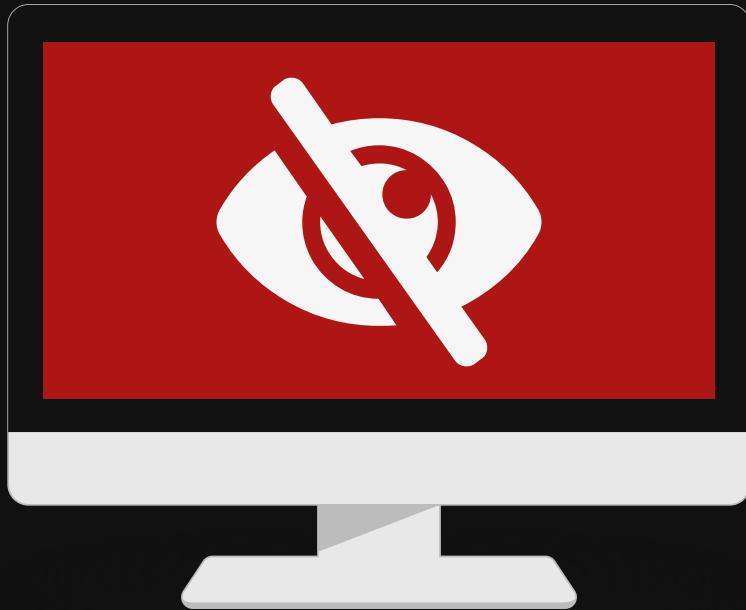
Are Trusts and LLCs overwhelming? We can help.

We believe all large assets should be titled to a Trust or LLC for privacy protection. Doing this correctly requires a lot of experience. We make sure your homes, vehicles, and any other assets which require titling stay out of your name. Contact us to reserve a consultation.



COOKIES BLOCKED. TO THE MOON.

Privacy-focused websites that sell.



Astropost

Astropost is the official design partner for this issue of UNREDACTED MAGAZINE. Need an ad designed for the magazine? We'll help you out!

WHEN STUFF GETS STUCK: HOW SEARCH ENGINES FAIL TO PROVIDE RELIABLE TOOLS FOR CLEANING UP DELETED CONTENT

By RedactedForPrivacy

If this headline caught your attention then I will go ahead and assume that you already in some capacity have dealt with removing your personal information from the internet. Regardless, if you decided to finally ditch your social media or managed to have your residential address taken down from shady data broker websites – you're on the right path and I commend you. It's never too late to make yourself less visible online. Even if you're yet to get started, I hope this piece of advice will make your journey towards online anonymity faster and more pleasant. It is a truly rewarding feeling to gradually see less and less results pop up when doing a self-search. So let's dive into it.

There's three possible initial outcomes when removing your information at its respective source website. Say you've deleted your Facebook. The link to your former profile will now return a 404/410 – page not found. Moving forward this will be the easiest one to also clean up from search engines. Now imagine there's a digital version of your old high school yearbook out there, with your name in it. You ask for it to be redacted and they do it, it's no big

deal. They take your information down but of course the page itself remains online. Your name is also still visible in the snippet and within the cached version of the site, so you will have to do something about it. Then there's a third, kind of special case. They might not error it out with a 404 but instead your old profile link from that moment on would forward to their main page. I've seen a few other websites handle things in a similar way, and it is indeed your worst possible option for the subsequent cleanup of deleted info.

As a general rule, search results do not disappear right away just because the original content is no longer there. You're dealing with the search index here which doesn't automatically update the second something is removed from the internet. For outdated information to completely stop showing up in a search, the page in question needs to be recrawled, a process which overwrites the snippet, updates the website cache and in case a keyword is no longer present drops the page from the search index in regards to that particular keyword. For 404 deleted pages – and for those only – this process can be sped up. Everything else might take weeks or even months.

Recrawl and the subsequent removal happen eventually, but until then traces of your old, deleted information will stick around on the internet. Now let's take a look at how major search engine providers handle each of the three types of deleted content which I described earlier – and how they sometimes fail at this task.

Google: First of all, you will need to create a burner Gmail account. This is mandatory if you want to use Google Removal, but you can also continue using this same Gmail when dealing with all the other relevant search engines. Just make sure to delete it when you're all done. On Google, use <https://www.google.com/webmasters/tools/removals>

Our deleted Facebook profile should stop popping up in the search within 24 hours of submitting the link. I've never experienced Google struggle with 404/410 pages so this one is simple. The high school yearbook will be processed in a different way. In addition to the link itself, you will need to input the keyword which has been deleted from the original source, in this case your name. Provided the tool picks up the link correctly, the page cache will be purged and where the snippet used

to be, you'll see an empty space below the search result.

The link itself will show up for the search keyword in question until Google actually recrawls the page. Which means in the meantime the search result will stick around in connection with your name, despite the name itself no longer being on the live page, in the cache or in the snippet. How frequently Google recrawls a particular page is something organic to its algorithm that you cannot influence from the outside. Worst case, if a professional investigator is really going after you, they will be able to easily connect the dots and determine you went to that high school. Longest I've seen it take for such a "stripped" search result to finally disappear was four months.

Here's also the point where things sometimes go wrong with Google's tool. In some cases, and from my experience this is random, it won't pick up that the original source had information deleted from it. Therefore it will reject your removal request, usually within seconds. You can submit your link then refresh a few times, and in case it still says "processing", you're good. If instead it says "rejected" then there's not much you can do. I found one workaround for this, but it applies to only a fraction of websites, and also it does not always work. You will need to go back to your search results page on Google then switch to picture search and see if there's any photos connected to your particular site that you had information deleted from. You then can try and submit each respective picture URL for removal. If one of those requests sticks, Google will also purge both cache and snippet of the link itself.

If not, the only option you have is to wait until the next recrawl makes all of it go away. The same applies for the special case of removal-by-forwarding. Google struggles with those type of links, actually all search engines do. I'd say two in three of these cases, the tool will not recognize content which has been deleted from a page and will spit out a rejection. Sadly you're in a bad position here if this is a website owner's modus operandi as far as removals go.

You can always try and specifically ask for your data to be errored out so it returns a 404, but there's no obligation for the other party to comply. You will have to wait. The link will eventually disappear from the search when Google recrawls it.

In case you're in the European Union, you can submit a GDPR removal request in the meantime. Always go for it if that's what makes you feel better about your online privacy. Google's processing time for GDPR went down from up to several months back in 2018 to same business day as of recently. If your request is successful, the link in question will be hidden from the index for all searches from EU IPs. Other than that, Google's customer service will not bother. There are many documented cases of the removal tool not working when it should have, for one reason or another, and users asking for help in Google communities. I myself tried their email support several times – at least, so I can tell you now that you can save yourself that experience altogether. None of my complaints have been resolved in a satisfactory manner. At least with Google, sooner or later all of your deleted content will disappear. Wish I could say the same about Bing.

Bing: Bing's content removal tool is terrible. It does not work at all, it hasn't for years. Just in case you want to find it out for yourself, go to <https://www.bing.com/webmaster/tools/content-removal>. It fails at tasks such as purging 404/410 links from the index. While they initially disappear within 24 hours after you submit your request, those links will almost certainly pop up in the search again some two or three weeks later. Wash, rinse and repeat.

I remember my own experience with them several years ago when I was in the process of deleting my own information from the internet. Microsoft and their search engine were by far the hardest obstacle on my way to privacy. I've had countless run-ins with their customer service and they either did not respond at all or replied with a generic message which had nothing to do with the nature of my respective request.

When looking up my name, Bing still casually spits out a link to a public Facebook group I used to be in. Well, I deleted my Facebook account in 2017 and there never was another person by my same name in that group. My name is not in the snippet or in the cache. That's already a win I guess. But why is that link still there? I ran it through the tool countless times over the years, then at some point I just gave up.

As of recently Microsoft at least seems to be addressing the issue more directly, so there's hope things will get better for the recent generation of internet users seeking privacy. Sometime in mid-late 2021, a new option was introduced in Microsoft's online support section which you can find at <https://www.microsoft.com/en-us/concern/bing>.

This is currently your safest bet to finally get Bing to let go of your deleted information. Fill out the form and make sure you attach a screenshot to reduce the chance of miscommunication. Whenever I took this route I always made sure to let them know "YOUR CONTENT REMOVAL TOOL IS NOT WORKING, AT ALL!", just like this, in caps. Even though they have you provide an email address, you won't receive a reply or any feedback. Nevertheless your requested content will actually disappear from Bing a few weeks after filing a claim.

Yandex: While it still mainly is the go-to search engine for Russia and ex-Soviet countries, you don't want to skip Yandex on your internet privacy mission. They index plenty of content in English, Spanish, German and pretty much every other European language, and then it stays on there. For a long time. I've seen Yandex cached pages as old as two years (picture titled Yandex goes here). You will need to actively do something about your deleted content on Yandex because otherwise chances are it might not get recrawled at all. Thankfully, the process is straightforward. Like with all the previous search engine providers, you will need to create an account. You can do so by simply logging in with the same burner Gmail you're already

using for Google and Bing. You then have two options:

For pages from where you had your info taken down but which other than that are still online, use the form at <https://yandex.com/support/abuse/troubleshooting/search/default.html>. It should kick off a targeted recrawl outside the usual schedule (which is a huge operational difference between Yandex and Bing/Google).

For completely deleted 404/410 pages, you can use the fast track tool at <https://webmaster.yandex.com/tools/del-url/>.

The fast track tool usually removes search results within a day. The outdated cache recrawl for still existing websites typically takes anywhere between one and four weeks. First, the cached version of the page will update. Then within a few days afterwards the result will no longer pop up in connection with your specific search term. You can check it off your to-do list. So far I've never seen anything reappear on

Yandex after it had been recrawled and dropped from the index. Should either tool ever struggle with a site - I had this happen with a deleted IG profile and some Reddit content - then your next step is to contact support at <https://yandex.com/support/search/troubleshooting/bug/mistake.html>.

They should respond within the same business day. The initial reply you receive may or may not be in Russian but they all speak decent English if they need to. Yandex support is generally pleasant to deal with given you have a comprehensible case of outdated content that their tool failed to take down. Screenshots always help. You will have to head straight to support with any removal-by-forwarding pages. The Yandex tool does not recognize this type of content as deleted. Customer service has to set it straight from their end.

Yahoo, DuckDuckGo, etc.: If you manage to have everything removed from the Big 3, the rest should not be a problem. Yahoo pulls their search results

exclusively from Bing. Both engines update simultaneously. DuckDuckGo is a compilation of Google, Bing and Yandex results with a few days of delay when it comes to updating their index. They do not have their own removal tool for this very reason. They also won't block or remove anything from their results while you're still dealing with the search engine where it originally comes from. Exalead can be contacted at <http://www.exalead.com/search/web/contact/>.

Conclusion: For an inexperienced user there is still no easy and straightforward resolution available when their stuff gets stuck on the internet due to no fault of their own. An individual wanting to be forgotten typically wants all of their online past gone and has already done everything in their power by having information deleted from the respective original sources. When things go wrong, in the end it's you against a corporation which doesn't care about your privacy despite laws being in place that are supposed to make them care. ■

A FACE WITH NO FACE.

**Complete brand identities.
For businesses that respect
privacy.**



Astropost

HOW DO BLOCKCHAINS PROVIDE THE TRUST FOUNDATION FOR DECENTRALIZED IDENTITY-BASED APPS?

By Paul Ashley

My first article, in the June 2022 issue of Unredacted, introduced some initial concepts around decentralized identity—the new technology that's giving users greater control over their personal data and identity. Here, I'll expand on those initial concepts and focus on decentralized identity blockchains—the trust foundation for decentralized identity-based applications and an essential part of the decentralized identity story.

Blockchain = verifiable data registry

The technical term for the decentralized identity component that provides the trust foundation for

the whole system is a verifiable data registry (VDR). Similar in its application to centralized public key infrastructure (PKI), the VDR allows users and services to verify their authenticity by proving they hold the private key corresponding to the public key written to the VDR. It is often called a decentralized PKI.

Most people don't use the term VDR, but rather the more widely known terms distributed ledger or blockchain, to describe how the component is implemented in the system. In reality, there are over 100 distinct VDRs available, built using well-known technologies such as Hyperledger Indy, Ethereum, Bitcoin, Interplanetary File System (IPFS), Hyperledger Fabric, Cosmos, and so on.

Hyperledger Indy

The most successful VDR is Hyperledger Indy. Created within the Linux Foundation, Indy is a public ledger designed specifically and only for privacy-preserving decentralized identity (also called self-sovereign identity). The Hyperledger Indy ledger is for credential issuers to publish data necessary for issuing verifiable credentials, and for holders to construct presentations based on those verifiable credentials.

Anonyme Labs supports and maintains validator nodes for both the Sovrin and Indicio Hyperledger Indy networks. Let's look at Hyperledger Indy's characteristics:

Public ledger	Anyone can read the data on the ledger.
Permissioned network	This statement has two different aspects: <ol style="list-style-type: none">1. The Hyperledger Indy network comprises a set of validators that have been approved (permissioned) to run the network. For example, the Sovrin Foundation approves validators to run on its three networks (Dev, Staging, and MainNet).2. The ability/permission to write data to the Hyperledger network, which allows for writing decentralized identifiers (DIDs), schemas, credential definitions and other decentralized identity-related items. To write to the ledger, an organization must have endorser permissions (which includes paying the appropriate fee to become an endorser).
Consensus algorithm	Just like Bitcoin, validator nodes must come to agreement (consensus) before anything is written to the Hyperledger Indy network. Indy uses the Redundant Byzantine Fault Tolerance (RBFT) consensus algorithm. Indy networks typically have 24 validator nodes.
Governance	Hyperledger Indy uses an offline and centralized governance model. In practice, that means people work together to create the network's governance policy, write policy documents and have validators and Endorsers sign the agreements. These governance activities happen in the physical world.
Economic model	Application developers pay the organizing company or foundation (e.g. Sovrin) for permission to write to the network.

Cosmos

Anonyme Labs runs a Cosmos validator node on the cheqd network. For comparison with Hyperledger Indy, here are some characteristics of a Cosmos-based VDR network:

Public ledger	Anyone can read the data on the ledger.
Permissioned network	This statement has two different aspects: <ol style="list-style-type: none">1. Any organization can join the network as a validator.2. Any organization can write to the network.
Consensus algorithm	Cosmos uses Tendermint Byzantine Consensus Algorithm (BCA) to establish a consensus between validator nodes.
Governance	Cosmos uses an online and decentralized governance model. In practice, that means that any validator can submit a governance proposal to the network, which validators will vote on and either approve, decline, abstain, or veto. All this happens online.
Economic model	Cosmos has a very well-defined crypto-economic model: <ul style="list-style-type: none">• Validators earn tokens through commissions to help run the network.• Writers to the network spend tokens. Cosmos also has an economic model for verifiable credentials .

DID methods

DID methods define how to interact with decentralized identity networks. Since Hyperledger Indy networks are so popular, I'll focus on the Indy DID method.

Written as did:Indy this DID method describes how to interact with a Hyperledger Indy network, including creating decentralized identifiers and issuing, verifying, and revoking verifiable credentials. It is proposed that in the future there could be hundreds of separately run Hyperledger Indy networks. The purpose of the did:indy method is to facilitate full interoperability between each of these networks.

The Indy DID method defines methods for writing the following data:

Decentralized identifier (DID)

A DID is the fundamental identifier of a decentralized identity in the network.

It may be the identifier for a user, a verifiable credential issuer, a service, an IoT device, etc. The DID structure is similar to a web URL.

The DID has four components, which are concatenated:

- DID: The hardcoded string did: indicating that the identifier is a DID
- DID Indy method: The hardcoded string indy: indicating that the identifier uses the Indy DID method specification
- DID Indy namespace: A string that identifies the name of the primary Indy ledger, followed by a colon. The namespace string may optionally have a secondary ledger name prefixed by another colon following the primary name.
- Namespace identifier: An identifier unique to the given DID Indy namespace.

The components are assembled as follows:

did:indy:<namespace>:<name-space identifier>

Some examples of did:indy DID method identifiers are:

- A DID written to the Sovrin MainNet ledger:
did:indy:sovrin:7Tqg6BwSSWapxgUDm9KKgg
- A DID written to the Sovrin StagingNet ledger:
did:indy:sovrin:staging:6cg-bu8ZPoWTnR5Rv5JcSMB
- A DID on the IDUnion Test ledger:
did:indy:idunion:test:2MZYuPv2Km7Q1eD4GCsSb6

DID documents (DIDDocs)

DIDDocs contains two primary data elements:

- Cryptographic material the DID owner can use to prove control over the associated DID (i.e., public keys and digital signatures).
- Routing endpoints for locations where one may be able to contact or exchange data with the DID owner.

DID resolution is the process of obtaining a DID document for a given DID.

Verifiable credential schema

A schema object is a template defining a set of attributes (names). A schema is bound to verifiable credential definitions in a Hyperledger Indy network. The bound schema restricts which claims an issuer can include in the credential. Schemas have a name and

version, and an issuer or authoritative organization (e.g. government authorities defining drivers license schemas) normally writes them to the ledger. Any client can read schemas from a Hyperledger Indy node.

Verifiable credential definition

A credential definition contains data required for both credential issuance and credential validation. Any Hyperledger Indy client can read it. A credential definition references a schema and the issuer's DID. The issuer's public key is included within the credential definition in order to enable validation of the credentials, which are signed by the issuer's private key. When credentials are issued using the issuer's credential definition, the attributes (names) of the schema must be used.

Revocation registry definition

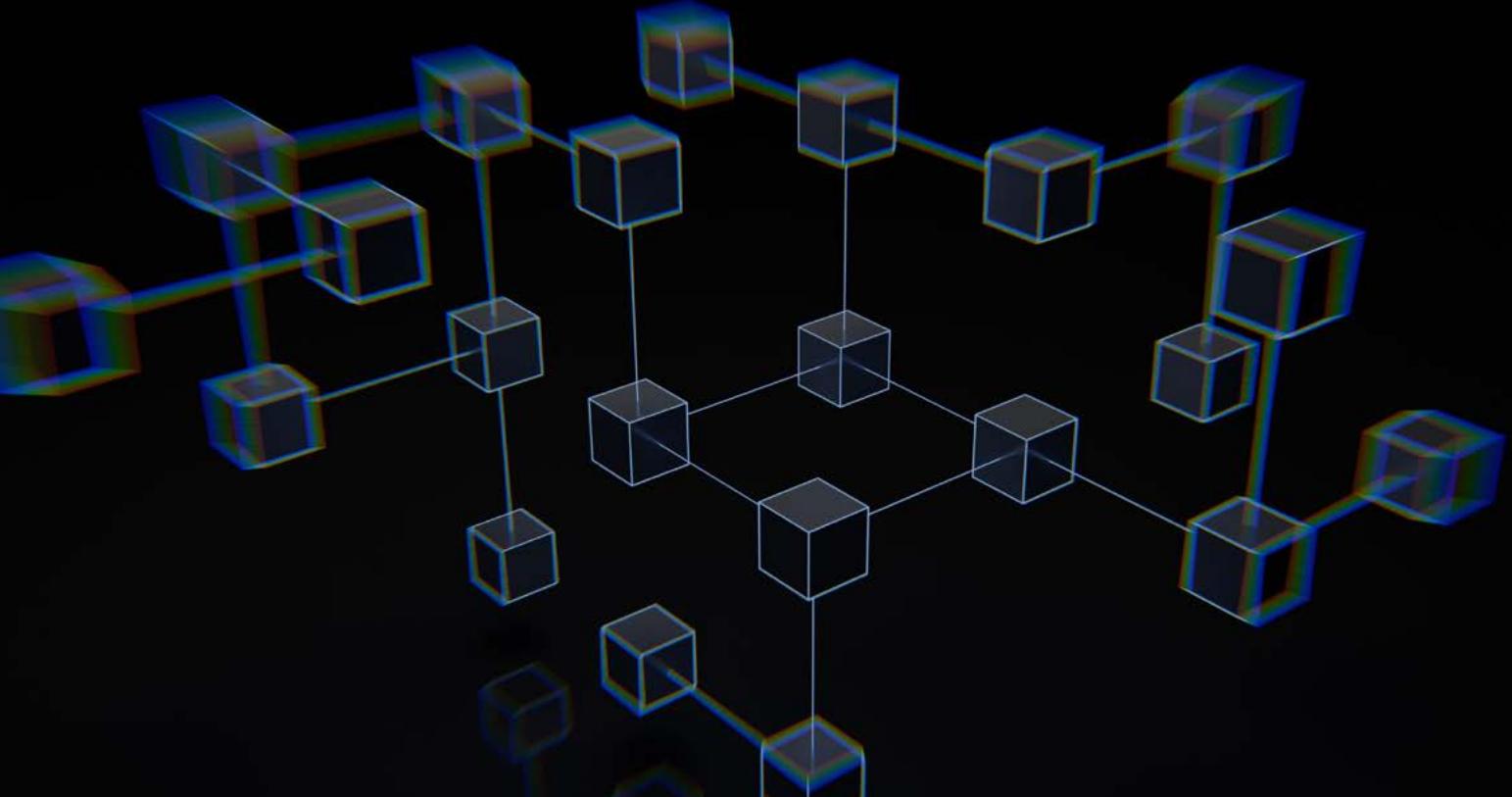
A revocation registry definition contains information required for

verifiers to determine whether the issuer has revoked a (revokable) verifiable credential. Revocation registry definitions are required for revokable verifiable credentials and are written to the ledger during creation of the credential definition. Any client can read them from a Hyperledger Indy node.

Revocation registry entry

A revocation registry entry marks the current status of one or more revokable verifiable credentials (i.e., "revoked" or "not revoked") in the ledger in a privacy-preserving manner. The owner of a revocation registry definition writes a revocation registry entry whenever they wish to make a batch (possibly only one) of revocations public and detectable. Any Hyperledger Indy client can read any revocation registry entry. ■■■

Image: GuerrillaBuzz Crypto PR



PARANOID SELLER'S GUIDE TO SECONDHAND MARKETPLACES

By **SneakerGust1999**

We all accumulate stuff and at times we choose to get rid of it in a safe fashion. Perhaps you don't want to take a drill to your old kitchen mixer or you want to realize some value from it. But how can you do it in a way that doesn't compromise your privacy? Read on to find out.

This article references North America specific sites and services, such as Craigslist. However, you can adjust it to your locale as the general principles will still apply. We will assume that in performing your transactions you want to keep the following aspects anonymous:

- Your name
- Your address
- Your phone
- Your email
- Your IP

We will present ideas based on our experience on how to achieve the above using two of the most popular secondhand markets at the time of this article: Craigslist and Facebook Marketplace.

We will assume you are familiar with basics of online/digital privacy. This is not an article on how to use VPNs, anonymous emails, VOIP numbers, and social media accounts. If you are unfamiliar with these concepts, we suggest Michael Bazzell's Extreme Privacy book. However, we will point out a few important aspects that will make your life easier as you sell your stuff online via the above-mentioned channels.

Online Stage

You are ready to sell your item. You write up a text, set the price, and snap some pictures. Consider the following basics and then you are ready to post.

- Most marketplaces will strip EXIF metadata from your photos, but why chance it? Run `mat2` tool against all images and clean them up, just to be sure.
- While you are at it, have a quick look at any reflections, identifying numbers/names, and so on in the image and blur them as needed.
- If you can avoid it, do not post your email and/or phone number in the body of the message. It may open it up to being more searchable and relatable to other posts over time.

Now that you have your message content and media, let's move on to the actual services. Here, we will examine Craigslist and Facebook Marketplace.

Craigslist

Despite the low tech appearance and the hippie vibe, Craigslist is rather unforgiving of people attempting to remain anonymous, as it has to weed through a lot of scammers. When establishing your account, you will almost certainly need a reputable looking email address (popular anon email domains will be rejected outright) and at some point you will also be asked to verify it via phone/SMS. VOIP numbers seem to work fine here, and we successfully tested a few of these using MySudo service. Craigslist does not seem to care what area code your number has, so you are fine to use out of state numbers.

Seems easy enough so far, right? Well, it is until it isn't. As of late, we have noticed that Craigslist may suddenly reject your sales post because of some unknown violation. You won't get an email about this - it will just appear as auto-deleted in My Account. Following the help link on that page will lead you to a list of vague rules (e.g. don't use VPN, don't steal other's photos, don't post in cities other than your own, etc.) and a forum with people giving all sorts of conflicting advice. The short of it is just like Amazon, Craigslist seems to have an algorithm for evaluating your trustworthiness. Here are some factors that will decrease that score:

- Using a VPN (likely checked via Cloudflare or similar)
- Posting in a city/area that does not match to your IP
- Using a stock photo (or any image that can be found via reverse image search)
- Copy and pasting a text from another ad (including your own, if it was previously rejected)
- Falling vastly out of line of expected value for an item (this seems to be triggered both on high and low end, i.e. charging way too much or too little)

Given the above, here is what we suggest. First, use a private/dedicated IP address from your VPN provider or use a mobile hotspot. Second, make sure it matches geographically to the place where you are selling. Third, do not use any existing online photos - your crummy 10-years-old-phone blurry photos will be rated higher than a clean professional photo off some public

website. Fourth, if your ad goes into auto-deleted mode, do not be tempted to re-post using just a different IP and/or set of photos. The text similarity will trigger another flag and your entire account will be degraded for some time. Consider that first warning seriously and see if you can wait several days/weeks, re-word your message, or post elsewhere.

Some people mention that posting as a dealer and paying some money for the privilege may reduce the scrutiny, but we found that not to be the case. Further, it adds financial details and ties your real identity closer to your account.

Facebook Marketplace

We will assume you have a Facebook account that is not using your real name, email, or phone number. When creating and using a Facebook account, we highly recommend the following steps:

- Register using a custom domain or popular service like Gmail, as it will face less scrutiny in any review
- If you have a face in your profile image, make sure you keep an original or generated photo that is just of that face and it looks like a normal mug shot. Should your Facebook account be flagged, you will need to provide this and it's much easier to have it on hand from the start. If you are using a GAN image, make sure to tweak it a bit in an image editor until it looks a bit less standard.
- Reserve a phone number that you may need for the eventual verification and/or provide it at account creation. That goes even if you enabled software 2FA. If you get flagged (and you likely will at some point), it's convenient to have a number to confirm your 'real' identity. VOIP numbers, such as those provided by MySudo seem to work fine.
- Train Facebook to be familiar with your VPN IP. Log into it from that one server consistently if you can.

It will be used to geolocate you so it makes sense to align it with the area you wish to sell in.

Understand that at some point your account will get flagged. A combination of VPN, low account activity (we presume you are not using this account actively for purposes other than selling), and engaging on Marketplace will raise flags of Facebook algorithms. Be ready with your verifiable phone number and that profile photo. When your account gets flagged, submit those two pieces of info and request re-consideration. We found that in most cases, you will get your account back within 1-2 days and after that it will not be considered suspicious any more.

Beyond the above, we also suggest you make an occasional post or interact with some groups every now and then to maintain your account. This could also be done by contacting other people on Marketplace (e.g. the usual pattern of asking whether some item is still available and then never following up).

Meeting Arrangement Stage

You posted your ad, someone wants your item, and now you are ready to arrange a meeting. We offer the following tips to make this stage safe.

- When asked where you are located, give a general area. It will be enough to let people make a decision if it's worth the effort to go out to get the item but will not reveal your actual address.
- When asked for a specific location, offer to exchange details over text. Here you can provide your VOIP number that you used to verify your account. Facebook already knows this so it reveals nothing new. As always, consider using this number for *only* marketplace transactions.
- Over text, provide a safe meeting area away from your actual location. Where is up to you. Consider your threat model. We suggest large apartment buildings rather than houses, but choose what works best for you.

Meeting Stage

You arranged the place, time, and all other details. You are almost ready to go. Consider a few last tips before you head out:

- The buyer does not know you. They will not care if you do not look like your profile image on Facebook or what you sound like on the phone (if you exchanged a call). In case they wonder why you are not the man/woman they expected, it's easy enough to say "that's my spouse/partner/roommate/family member/etc."
- For extra points, wear boring regular clothes and some manner of face obscuring fashion (sunglasses, hat, mask).
- Keep your wits about you. Bring nothing but your phone (if that) but pay attention. As much as you want to protect your anonymity, make sure to protect your physical safety too. If you have to drive to the meeting place, park a few blocks away.
- Don't fall for last minute changes (e.g. I'll wire you the money, and so on) and be ready to walk away if anything seems odd.
- And speaking of walking away, take an uncommon route back home.

Summary

Let's recap. If you followed the above steps, you have successfully posted an ad and transacted with a stranger using: an alias, an IP behind a VPN, an anonymous email address, an unconnected/alias social network account, a VOIP number not tied to your physical device, and met them at a place that is nor your home/business while wearing some manner of disguise.

Congratulations! Now keep it up and remember to change up your patterns over time, so that you do not develop something repeatable and identifiable. Good luck with your sales! ■



Image: Leio McLaren

HOW (NOT) TO FLY ANONYMOUSLY

By Anon E. Mouse

Editor's Note: Our legal division forced us to add "(not)" to the title of this entry and to state that the following might be illegal. We never condone breaking any laws. Getting arrested is the opposite of being private. The following submission is presented as an experience of the author and is not recommended by the magazine staff.

As you know, the TSA requires a photo identification in order to travel by plane (but not, to my knowledge, by bus, train or basically any other mode of transportation). Although I am a privacy enthusiast, I like the frequent flier miles so I always travel under my actual name; however, there are many scenarios where you might prefer to use a different name. I am going to explain how I stumbled upon a solution to this and how it might apply to you.

A few years back, but long after the updated security protocols

implemented in the wake of 9/11, I booked a family vacation, which included a flight for the nanny. I booked the flight far in advance in order to secure the best seats and prices. Of course, like most people, I booked a non-refundable ticket for the best price.

During the time between the booking of the ticket and the actual flight, I wound up changing nannies, so I called the airline to change the name on the ticket. Alas, the non-refundable ticket was in the name of the first nanny and could not be changed. A new ticket would be available for the second nanny, but at a higher fare, and, naturally, I would forfeit the fare of the original ticket. Rather than be irked and complain fruitlessly to the airline, I got creative.

For illustration purposes and to protect the guilty, let's say that I live in

Denver (I don't) and the vacation was to Orlando, and that the original non-refundable ticket was under the name of Nanny 1, to leave on January 1 at 10 a.m. and return on January 8 at 5 p.m. In this scenario, I separately bought a second refundable ticket under the name of Nanny 2 from Denver to, for example, Dallas, to leave on January 1 at around 10 a.m.

January 1 rolls around and I check Nanny 1 in for the flight to Orlando and print out the boarding pass and hand it to Nanny 2, which she keeps in her pocket for the time being. Nanny 2 separately checks in for the flight to Dallas under her own name, prints out the boarding pass, goes to the Denver airport and clears security using her actual government-issued photo ID as if she is going to Dallas. This is the only point at which Nanny 2 needs to show an ID. Upon Nanny 2 clearing security, I immediately call the airline and cancel

the flight to Dallas, getting a full refund. Nanny 2 then reaches into her pocket, grabs the boarding pass for Nanny 1 and boards the flight to Orlando.

I repeated this process for the return flight. I bought a refundable ticket for Nanny 2 to fly from Orlando to Newark on January 8 at around 5 p.m., on a different airline. Nanny 2 cleared security at the Orlando airport as herself, then I called the airline and canceled that ticket. She then flew from Orlando to Denver using the original ticket issued under the name of Nanny 1.

Did you see what happened there? Nanny 2 flew completely anonymously, under the name of a different person. In this case, Nanny 1 didn't even have to be an actual person; it could have been a fictitious name. Also, at no point in this process did Nanny 2 use fake identification or lie to a governmental agency.

Let's say that your name is Robert Jones and you live in San Diego and

wish to fly anonymously to Charlotte. You book a ticket from San Diego to Charlotte on whatever terms are comfortable to you using the name of, for example, John Williams. You separately book a second refundable ticket from San Diego to, for example, Phoenix under your actual name of Robert Jones to leave from San Diego at around the same time. You check in for both flights, go to the San Diego airport, clear security as Robert Jones, call the airline and cancel the ticket to Phoenix, then board the flight to Charlotte that was booked under the name of John Williams. Replicate this process for the return flight, perhaps using a different airline.

True, there will be records of your presence in San Diego and Charlotte in this example, but those records will be difficult to locate and realistically available only after you are no longer in either city. For added confusion to thwart a savvy stalker, if you are particularly paranoid, perhaps you buy a third refundable ticket involving two cities far from your actual location or

destination (e.g., from Minneapolis to Salt Lake City) in your real name and then cancel it at the last minute (obviously no need to check in).

In my actual case, I used my own credit card for both the original non-refundable ticket and the second ticket that I was to cancel, since my goal was not privacy per se, but for a higher level of anonymity I might have used a prepaid Visa, or I might have had a friend buy the ticket using their credit card.

Ethically, since I tied up a seat that the airline could have sold to someone else, I chose to purchase the second refundable ticket (which I knew I would cancel) last-minute (to keep the amount of time that the seat was tied up to a minimum), in a middle seat and on a flight with many empty seats.

Please note that this technique works only if you are flying within the United States, since you must also clear immigration (under your actual name) if you are flying internationally. ■





Image: Tim Mossholder

MORE ANDROID SANITIZATION

By Reginald

The Android Debug Bridge (ADB) commands allowing us to list, install, and uninstall Android Package Kits (APK) have been covered by MB (<https://inteltechniques.com/blog/2022/01/14/the-privacy-security-osint-show-episode-246/>) and several others sources, with some enrichment here in issue 002 (Android Sanitization Package Names, pp36). Now, let's explore ADB a bit more and delve very briefly into Package Manager (PM) to interact with Android applications.

Installing ADB on Windows, Linux, and macOS is covered in detail all over the web, as are the steps to allowing USB debugging on your device. As always, be very careful using ADB on your daily driver/production devices. A great practice is having a test Android phone to play with, and learning the correct way to interact in a safe environment, where executing the wrong command can cost you a lot. Follow along with the following instructions at your own risk.

ADB with shell

When connect to your device, you have options to interact either through the ADB interface, or in a shell, allowing you to interact directly with the Android system - both methods will achieve the same result.

Use the shell:

```
user:~$ adb shell  
shell:/# pm list packages
```

Use the ADB interface:

```
user:~$ adb shell pm list  
packages
```

Both methods give the same results. Using the adb shell command however saves having to type adb prior to every command. We'll stay with ADB's interface.

ADB with PM

The PM is used to interact with applications through ADB. This is our powerhouse to install, uninstall, clear

memory, and mess with permissions in a clean command line environment.

The following commands will perform straightforward actions to seek and destroy unwanted apps:

```
user:~$ adb shell pm list  
packages  
  
user:~$ adb shell pm list  
packages | grep -i <app name>  
  
user:~$ adb shell pm uninstall  
<app package name>
```

TIP: For those planning to go deep with ADB on a mainstream Android release running Google Play, you can find APK names by entering the Play Store -> Manage apps & device -> "manage" tab up top ->select the app you want to find, then in the 3-dot stack in the upper right, select it and tap the "share" symbol - the APK name will appear as the last portion of the sharable link. The equivalent path for Aurora store was given in issue 002.

ADB to clear memory

Using the clear command will do the same thing as clearing cache and storage for an app's settings page, but through the command line:

```
user:~$ adb shell pm clear <app package name>
```

This command will only clear the data for the app. Using uninstall is still required to ditch the app. The advantages here are obvious; you have the option of scripting the clear command for every APK you want, which saves a lot of time versus using the graphic interface on the device itself. Make a text file with each APK on a line once, and future you will be very grateful.

ADB to affect app permissions

Later versions of Android allow more granular control of app permissions. As with the clear command, having to go through each one in the handset graphic interface is tedious, but figuring out the syntax for the permissions, and knowing which APKs should be denied permissions, borders on more advanced usage. You'll spend more time in ADB, but be better for it. To get a full list of permissions in ADB, type:

```
user:~$ adb shell pm list permissions
```

The format for changing permissions is:

```
user:~$ adb shell pm [grant | <or> revoke] <app package name> <permission>
```

The following is one example of revoking an app's permissions. Here we specify "Fine Location", but some simple research will help generate syntax for any permission desired. Much of this is trial and error unless you are an app developer, since some apps may not have access to certain permissions, or others may not permit revocation of access. Be mindful of those apps that need specific permissions for basic functions. If your phone dialer app loses permission for RECORD_AUDIO, making phone calls with it could prove problematic.

```
user:~$ adb shell pm revoke com.example.myapp android.permission.ACCESS_FINE_LOCATION
```

Other notable options are:

```
android.permission.READ_CALENDAR
```

```
android.permission.READ_CALL_LOG
```

```
android.permission.RECORD_AUDIO
```

```
android.permission.READ_CONTACTS
```

```
android.permission.CAMERA
```

ADB to audit logs

Some of us would like to get a bit deeper checking out what our apps are doing when active on our phones. In ADB, we can scan an app's activity via the shell, which reveals a good bit of useful information. The tool used is logcat:

```
user:~$ adb logcat -d
```

This command and the -d switch will load all recorded logs collected by the Android system. To clear the logs for a fresh log pull, use:

```
user:~$ adb logcat -c
```

The example below is an instance of Telegram executed, but not used to send or receive messages. Notice the IP addresses called, which point to Telegram's data centers (dc1, dc2, etc.). At the bottom, we can see tgnet.dat, one of the files where Android stores the app's information. This is useful for building access control for a firewall, or just to see how chatty your apps are to their development servers. It's not as advanced as sniffing and examining packets using a Machine-in-the-Middle with a protocol analyzer in a lab, but it's a start.

```
07-12 12:59:50.311 8900 8961 I ... app=org.telegram.messenger
```

```
07-12 12:59:50.415 8900 8961 D tgnet : connection(0x-75cf47000, account0, dc2, type 1) received message len
```

```
552 equal to packet size
```

```
07-12 12:59:50.415 8900 8961 D tgnet : connection(0x-75cf47000, account0, dc2, type 1) received object 13TL_rpc_result
```

```
07-12 12:59:50.415 8900 8961 D tgnet : process server response 0x75fcfc5ac70 - 13TL_rpc_result
```

```
07-12 12:59:50.415 8900 8961 D tgnet : connection(0x-75cf47000, account0, dc2, type 1) received rpc_result with 14TL_gzip_packed
```

```
07-12 12:59:50.415 8900 8961 D tgnet : got response for request 0x75cf56500 - 17TL_help_getConfig
```

```
07-12 12:59:50.415 8900 8961 D tgnet : getConfig add 149.154.175.56:443 to dc1, flags 0, has secret = 0[0]
```

```
07-12 12:59:50.415 8900 8961 D tgnet : getConfig add 149.154.175.50:443 to dc1, flags 16, has secret = 0[0]
```

```
07-12 12:59:50.415 8900 8961 D tgnet : Config(0x757b8ad-dc0, /data/user/0/org.telegram.messenger/files/tgnet.dat) start write config
```

```
07-12 12:59:50.415 8900 8961 D tgnet : Config(0x757b8ad-dc0, /data/user/0/org.telegram.messenger/files/tgnet.dat) fileno = 112
```

```
07-12 12:59:50.417 8900 8961 D tgnet : Config(0x757b8ad-dc0, /data/user/0/org.telegram.messenger/files/tgnet.dat) config write ok
```

We covered just some very basic uses of ADB to list apps, clear app data, list permissions, revoke permissions, and view some logs. Build on this and learn more of the features offered by ADB. If any of the commands or details here are incorrect, please find the fix and submit it. Remember, be very cautious about using your main phone before testing. ■

USING A TRAVEL ROUTER FOR PRIVACY ON PUBLIC WI-FI

By Anonymous

Introduction: Normally, when I am at home, all of my devices have their traffic routed through a VPN that runs on my firewall. However, I recently went on a business trip that had me living out of a hotel for a couple of weeks, which left me without this protection. While out and about, or for a trip lasting only a few days, VPN clients running on devices are fine, but these clients tax the device and sometimes drop unexpectedly. For an extended trip I wanted to find a better solution.

Travel Routers: Travel routers are small pieces of dedicated hardware with a pair of wireless NICs that can connect to a public Wi-Fi (including networks with authentication) on one interface, and broadcast a custom SSID on the other. Throw in an onboard VPN client, and you have everything I am looking for. Once set up, my devices will be able to connect to my router with WPA3 protected 802.11, and then from there the router will wrap the traffic in a VPN, and forward it through the hotel Wi-Fi to the open web.

Several different brands make dedicated travel routers, and some people even make their own with Raspberry Pis, but if you are looking for something small and easy to setup, I recommend the GL.iNet GL-MT300N Mango (<https://amzn.to/3SHjJnG>). This model costs ~\$30, has a tiny form factor, an easy setup (OpenWRT), and enough hardware to max out your hotel Wi-Fi connection.

Configure Router: Once your Mango has power, it will begin to broadcast its default SSID (something like GL.iNet). Connect a device, and navigate to the admin page at 192.168.8.1 (why they use .8.1 and don't just use .0.1 or .1.1 I am not sure, but you can change it if you want). From there you can use the default password to get in, change

the admin password, and begin setup. There are four ways that you can connect the device to the internet, and we will go through each of them below.

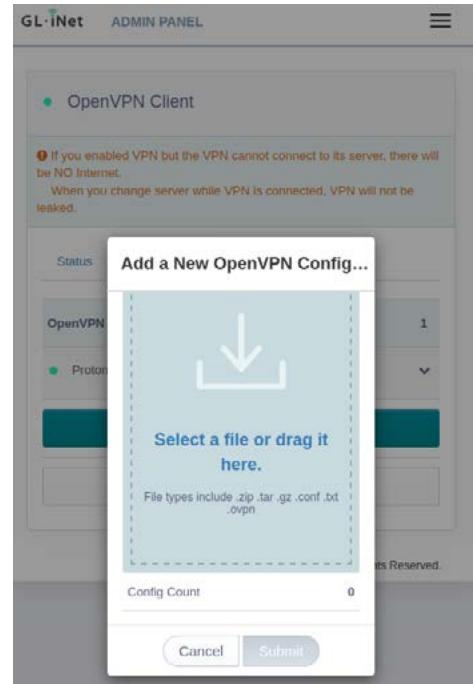
WAN: If you can hardline an ethernet cable from your Mango's WAN port to an open LAN port on one of the hotel's switches or access points, you can get online that way. This would be the best case scenario, since you won't have to worry about wireless interference or problems, but it's probably unlikely that you will be able to plug anything into the hotel network.

Repeater: This is probably the most likely scenario: your Mango will authenticate with the hotel Wi-Fi and act as a client on that interface. You can just click 'Scan' and the router will present you with a list of nearby networks that you can try to connect to.

Tether: Another option for connecting your Mango to the web is via your cellphone's network tethering option. This will obviously eat through data on your cellular connection, and most phones that allow hot-spotting can create their own SSID, but the capability is there. Just plug in your phone to the Mango's USB slot, and turn on the 'hotspot' option and the Mango should detect the connection.

Cellular Dongle: The last option is to use a Cellular USB Modem. I have not looked into this but may explore the idea in the future. You will obviously need to purchase a cellular data connection, and be subject to whatever speeds the network allows.

Add VPN: Once your router is online, you can add a VPN. The setup is straightforward, you just need a .ovpn file or WireGuard configuration file from your VPN provider and the accompanying credentials. The following displays the ability to drop this file into the settings.



You get a tiny window of the last few lines of cli messages for the connections, so you can try to diagnose problems there. There is also a handy color coded dot next to the VPN option (Green = Good, Yellow = Configured But not Connected, Red = Something Wrong) to quickly show the status.

Configure Wi-Fi: Last, you can setup your own private Wi-Fi SSID. This is straightforward, you can mirror your home settings so that all devices can automatically connect if desired.

Conclusion: Adding a travel router to my mobile kit was extremely easy and provides a layer of convenience and protection. Now when visiting new places, I do not have to configure multiple devices to authenticate to a public network, turn on individual VPN clients, and then worry about forgetting the network or disconnecting once I leave. With my Mango I can simply use it to scan for the public Wi-Fi, connect, and hide behind it and the onboard VPN. ■

IS REVOLUT A VIABLE ALTERNATIVE FOR PEOPLE OUTSIDE OF THE USA?

By SWhopper

[Privacy.com](#) is very often mentioned as a useful tool in the privacy toolkit both online and in Michael's Extreme Privacy book, and for good reason. It's a USA-based service which offers masked debit cards for online purchases allowing its users to protect their true name and address. I, like most of society these days, buy the majority of my goods online and so would benefit greatly from a service like Privacy.com. The only issue is I do not live in the USA and therefore cannot sign up. So what is my alternative?

Revolut is a relatively well known app-based bank operating mainly in Europe which does offer some of the same features as Privacy.com. I personally have been a Revolut customer for many months now and long enough to nail down my thoughts and feelings. I'll be sharing them here under the lens of a possible Privacy.com alternative for non-USA citizens.

The killer feature of Revolut and the reason it's a possible alternative to Privacy.com is the 'virtual cards'. These are VISA debit cards which can be created from within the app on demand and come in either a one-time disposable variety or for long-term use e.g. dedicated to a particular merchant, alias, or category of spending (subscriptions, bills, Amazon, eBay, etc.). There is seemingly no limit on the number of new cards that can be generated, however there is a limit on the total number of cards that can be held in the 'wallet' simultaneously - 6 physical cards, 5 virtual cards, and 1 disposable card at a time. There are handy features such as the ability to easily freeze a card, create a defined spending limit, or to add them to

Google Pay should you want to use them in physical shops. And Revolut's app is smart enough not to destroy a disposable card if a merchant is just doing a simple active card check rather than taking payment. As with Privacy.com, using unique card numbers for every transaction will greatly reduce the possibility of a leaked card number being used maliciously by an attacker and may even eliminate the risk entirely if just a disposable card or a card with a spending limit was leaked.

So what of Privacy.com's ability to hide your real name and address? In my experience, the success of hiding my real name and address while using Revolut virtual cards varies greatly depending on the merchant. My default position is to supply my initials (it's technically my name but just a shortened version) and the address of the hotel I'm staying in at the time, and this is accepted 9 times out of 10. However I've faced rejection anytime the merchant might be wary of fraud or abuse. For example when making a large purchase or when attempting to pay for a cloud VPS hosting provider. The merchants are able to tell the billing address I've provided is not matching the address held by Revolut and they reject my purchase. But whether this would be the same experience with Privacy.com I do not know.

This brings me nicely to the sign up process and requirements. It is all done through the app and unfortunately you will be required to provide your real name and address, plus a valid mobile number that can receive SMS (i.e. a real-SIM number and not VOIP as Revolut uses short-code messaging for their one-time passcodes). Also Revolut will demand a picture of a real ID document and of your face to verify your identity.

This is all mandatory as part of the know-your-customer laws in my country and I suspect Revolut would keep the requirements consistent across all the territories they operate in.

In terms of a general review of the app, it's relatively easy to navigate when focusing on the virtual card features I've discussed. It is quite cluttered with other features consummate with a 'fintech' app such as investments in stocks and cryptocurrency, offers on savings accounts, intelligent budgeting based on your spending habits, and discount vouchers for online shops. These can all be ignored easily without any interruption however I do note I keep Revolut frozen inside of an Android work-profile until it's launched so I'm never bothered by any excess notifications. Your mileage may vary. Also of note is that Revolut offers a number of 'premium' tiers that get you some additional perks for a fee which might be of interest to some. However virtual cards are all available on the free tier.

Finally I should say Revolut as a company is no stranger to controversy. Most significantly there have been reports of customer accounts being frozen when they've been incorrectly detected as fraudulent by Revolut's algorithms. This coupled with Revolut's customer service generally being regarded as poor might give pause for thought to anyone intending to use this account as their 'main' bank. Personally I haven't encountered these issues but I do only use Revolut for its virtual cards and only as additional to my other main banks accounts. I just transfer in enough money to pay for a transaction exactly as I am about to do it so no money sits there for long. ■

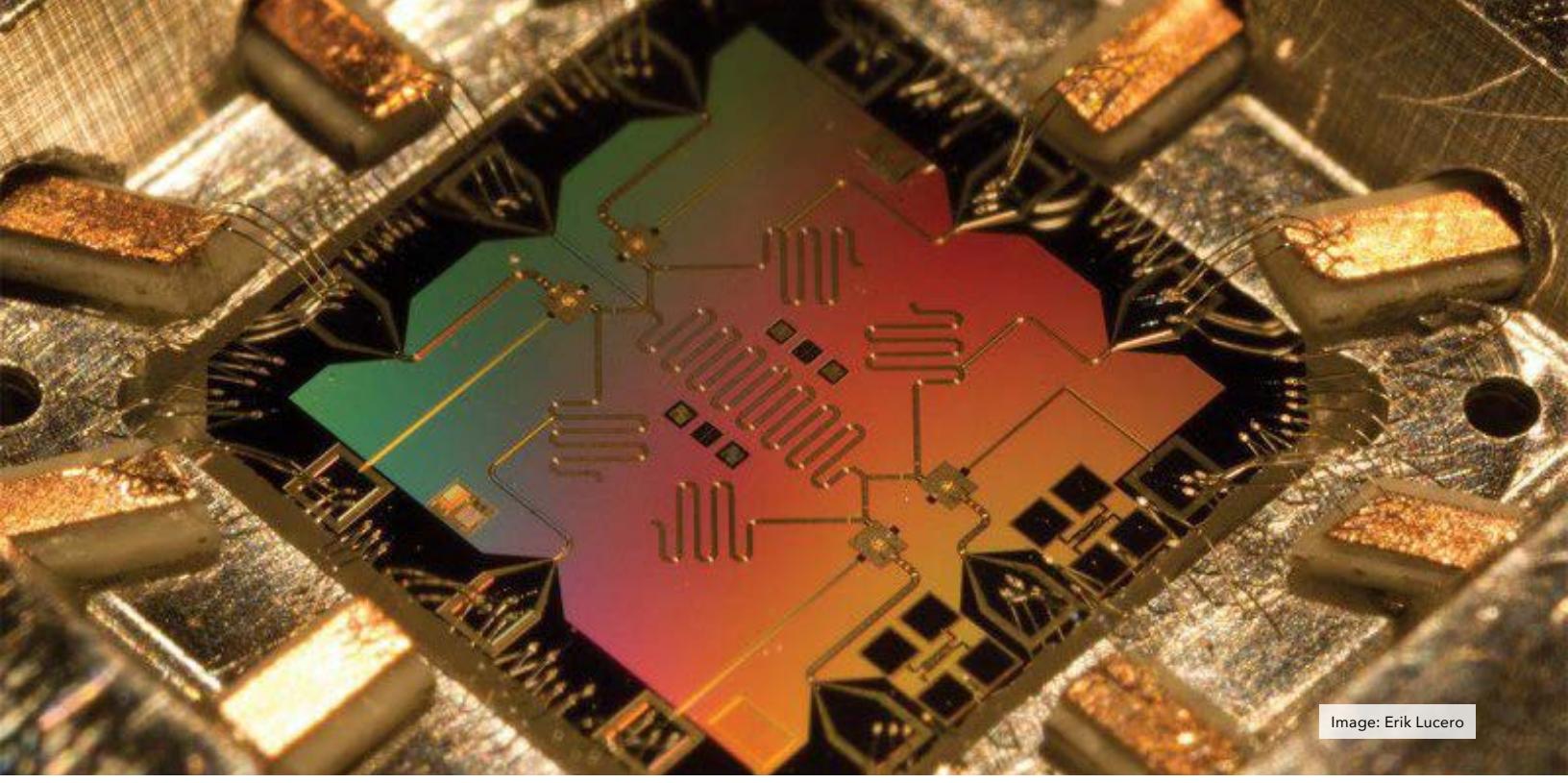


Image: Erik Lucero

ENCRYPTION IN THE AGE OF QUANTUM COMPUTING

By Jessie Misico

Encryption plays a key role in keeping our personal data protected. Without it, our bank accounts, cloud storage, messages, and other sensitive parts of our digital lives would be freely available to anyone who cared to access it. But with a strong password and our best encryption protocols, we could feel reasonably confident that a random malicious actor wouldn't go through the time and trouble it takes to brute force their way in.

That's right, encryption is completely breakable. It's basically a series of math problems designed to take a very long time for a computer to solve without the right key. However, quantum computers run on a fundamentally different technology. By harnessing quantum principles, these machines can solve calculations 150 million times faster than a supercomputer.

A password that would've taken a supercomputer thousands of years to crack could be deciphered in hours.

So what happens when such a critical element of our security infrastructure is rendered completely obsolete? The good news is the situation is a lot less bleak than it sounds. For starters, quantum computers have a long way to go before they become commercially available. The mechanics of this technology is highly sensitive and must be run in a controlled lab environment. We have plenty of time to prepare, and more sophisticated technology paves the way for encryption protocols that are even more secure than the ones we use every day.

Before we get into that, I'd like to acknowledge the tremendous leap in progress quantum researchers have made here. Not only are these computers incredibly fast, but they also offer security enthusiasts levels of

protection that aren't available under traditional computing. For example, quantum bits, or qubits, naturally come with tamper detection benefits. Without getting too technical, traditional bits can only hold a value of 1 or 0. Qubits have a probabilistic tendency to be 1, 0, or a combination of the two, and the simple act of observing a qubit will change its value.

So, let's say you want to get a top secret message to your friend. The computer will send off your message and a key in the form of qubits, and your friend's computer uses the key to translate it into a form your friend can read. If a third party intercepted your message before it got to your friend, the act of them reading or copying your message would change the value of the qubits. They would then have to send the changed qubits on to your friend, thereby notifying them that your exchange has been compromised.

Additionally, quantum computers can generate keys that are far more unique than any traditional computer could make. It sends your key over a fiber optic cable, and voila! You've just sent your friend a unique, untampered-with decryption key. Of course, your friend can only be as far away as the cable allows, which is another drawback researchers are working on.

To make matters better, the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) recently announced four different encryption algorithms they believe can stand up to a quantum attack. They explained in their press release, "The algorithms are designed for two main tasks for which encryption is typically used: general encryption, used to protect information exchanged across a public network; and digital signatures, used for identity authentication." NIST aims to release their full post-quantum cryptographic standard in the next two years.

In the meantime, there are a couple different things to think about when considering the best ways to future-proof our personal security. For starters, NIST's algorithms are still under development, so they may change. In fact, researchers at Ku Leuven have already published a paper calling into question the effectiveness of one of the four algorithms. Developers are encouraged to look into how they could be used in current systems, but it's not time to implement anything yet. It would be wise to keep that in mind when new services come out claiming to be "quantum-proof". Take it with the amount of salt you deem it worthy of.

This might also be a good time to take inventory of our services that rely on public-key encryption. Those include email and messaging services, cloud storage, and online accounts to name a few. While all that encrypted data might be useless now, the possibility exists that it could be collected to read later on when quantum computers become more widely available.

For sensitive data you'd like to protect long-term, consider cold storage options that cannot be accessed by the internet, such as a physical hard drive. Be sure to make multiple copies of these before deleting anything off the cloud, just in case something happens to one of them.

For anyone concerned about the long-term privacy of their communications, it might be worth considering messaging services that don't store your messages. Instead, look for services that will either destroy your conversations on a timer or allow you to store them locally on your computer.

For those of us with social media accounts, even the ones set to private, it's always a good idea to go way back into the depths of our activity and purge. The fact is, even without quantum computers, our thoughts and ideas don't always age well. Times change, and so do we. Let's keep up. ■

Is privacy and security overwhelming? We can help.

Whether you are ready for a complete anonymous relocation with a full privacy reboot or simply need a one-hour call directly with Michael Bazzell, we can eliminate the frustrations encountered when trying to be invisible.





Image: Ludovic Migneault

READER Q&A

By UNREDACTED Staff

Do you have a question or need clarification about a privacy-related topic? Submit it to us for publication consideration at UNREDACTEDmagazine.com. If you have questions, other people are wondering the same thing! Please make sure your submissions are actual questions, and not vague statements with a "?" at the end. Here are questions from last month.

Q: A lot of the websites provided in the look-up tools in the book "Open Source Intelligent Techniques" require payment for information. Which people search websites do you pay for? Do you have subscription to any of the websites that provide information regarding usernames, phone number owners, etc.? Any

recommendation on which service is worth getting a subscription for?

A: We believe that none of the services are worth any payment. The details available on premium services are almost always replicated on free options. Take advantage of the free OSINT search tools at IntelTechniques.com to conduct URL manipulation on most sites.

Q: My family recently started using WhatsApp, despite my request for everyone to join Signal instead. I am uncomfortable with the idea of Facebook collecting metadata on me even if I use an alias name and phone number. However, I also feel like it is foolish to choose SMS over an encrypted option even if suboptimal.

Does the magazine staff have any thoughts on whether WhatsApp is a tolerable alternative to SMS in the worst case scenario?

A: Everyone has a unique situation, and only you can make the best decision for yourself. However, an encrypted conversation on WhatsApp is much more secure than over SMS. Both collect some type of metadata. If you want to hide your conversation, WhatsApp is better. If you want to hide the fact that a conversation took place, neither help you.

Q: Your podcasts and Unredacted state that you use MySudo as a reliable VOIP service. I am confused as I believe you stated that you are not using Apple, Microsoft or Google

products. I am switching over to GrapheneOS, which you said you use now. So how exactly are you still using MySudo since they currently don't work on GrapheneOS?

A: I first must correct your inaccurate statement which exists as part of your question. MySudo DOES work on GrapheneOS. I use it every day. You only need to install the Android version using any of the options explained in the book. Incoming calls never work for me since I have no push services, but everything else works great.

Q: I just bought Extreme Privacy. So much to learn and do. I was wondering if it is possible to automate these processes. There are a lot of configurations to do and running again and again it becomes tedious process. Any thoughts?

A: We believe automation of privacy strategies is a bad idea. Things will get skipped, missed, and avoided. The manual process forces us to understand the steps we are taking and replicate them in the future if needed. Convenience is not always a good thing.

Q: Where do you draw the line between investigations and the territory of PI (Private Investigator)? There are licenses to consider and wondering where the line is.

A: Typically, physical surveillance. If I need to stake-out a house to get photos of my target, that might require a PI. If I can use the internet to find information, that is "research". Many PI's will disagree.

Q: Is there an alternative to Amazon fire stick? Even if is offline, I can't consume local media (plex, jellyfin, etc). A nuc or similar sffpc is doable but for wife and kids, Navigating the TV optimized UI is more intuitive. Do I have options ? Or is hardening at the network level my only choice?

A: We like the Kodi media server and Handbrake to rip physical discs.

Q: I am preparing to purchase a new home as anonymously as possible.

I am working with an attorney, but while knowledgeable, the process MB prescribes is very uncommon and attorneys have little experience with it. A few attorneys would not even respond when I told them what I wanted to do and the current attorney was referred from another. Is there a way to search for an attorney familiar with these privacy issues? MB states it is preferred NOT to get an EIN for the home trust. How do you put funds in and pay bills monthly without an EIN?

A: Your struggle is common. Most attorneys know very little about trust laws. We focus on "Estate" attorneys when needed, which is rare. Trusts can be executed without an attorney. We never recommend an EIN for a trust. If a utility demands an EIN, we will consider an LLC or Sole Proprietorship.

Q: I live in Canada where there are no LLCs. I have listened to the benefits you ascribe LLCs in keeping anonymous. How could someone in a country with no LLC get the Same benefits?

A: Research your version of sole proprietorships and trusts. We use those way more than LLCs lately.

Q: It has been recommended to use YubiKey or Authy for multifactor authentication. So far I have yet to see a Bank Portal that allows anything other than a phone number. Most if not all banks mandate this. What do you recommend using? VOIP Number? Or a real phone number on a phone set aside purely for online banking?

A: We see the same thing. We always recommend, in order, hardware key (Yubikey), software key (token), VOIP SMS, then traditional SMS. Any 2FA is better than none, but true SMS is last on the list.

Q: Will it be possible to have a text only printable version of UNREDACTED available for those of us that would like to read a hard copy of it? Printing the PDF version is becoming costly as it contains

numerous, beautiful, almost solid, colored pages.

A: Absolutely, someone just needs to create it. Our staff is committed to creating a quarterly high-quality PDF. If someone wants to make a print-friendly version with all content, we would be happy to host it. Like other community projects, any future products rely on you. If you want to see something be created, consider joining the process.

Q: I understood we can have a smooth experience with a Linux preinstalled. When you buy such native models for yourself or your clients, do you wipe out the preinstalled OS and reinstall it as you've been preaching? Doesn't that break any kind of delicate balance between the hardware and the software, which is the unique strong point of such native machines?

A: I typically wipe out any machine and install my desired (verified) OS. With most Linux machines, this is quite easy and you maintain all benefits between the OS and hardware. If I cannot replicate the OS on any Linux machine, I am not interested in using it.

Q: How does one start learning about cleaning breached data to the point where it is searchable?

A: Shameless self-promotion: The 9th edition of the OSINT book has an entire chapter dedicated to this. If you prefer to forgo the book, master the "sed" and "cut" commands within Terminal.

Q: I'm thinking about buying some Bitcoin as an investment. Any tips for buying and selling with more privacy?

A: I never advise people to enter the cryptocurrency game as an investment. I use it only as a tool to make private purchases. That said, I prefer to host my own wallet through Electrum.

Q: Do you have recommendations for privacy with an FCC Amateur Radio License? The callsign database is public and provides an operator's name and address. Also a note to any other ham operator: be aware that

if you have your callsign as a license plate, a simple Google search can give that person you accidentally cut-off your home address.

A: The FCC allows usage of a CMRA for your address, so that is covered. It could even be out of state. I agree with your advice on vehicle plates.

Q: Michael mentioned in the second edition of Unredacted Magazine that he has a laptop and desktop that are clones of each other and synchronize on a weekly basis. I find this a very interesting concept, and wonder if Michael could share more about this specific setup.

A: Please see The Linux Lifestyle articles in issues 002 and 003.

Q: Because of inflation, Series I Bonds, issued the U.S. Treasury, are hugely popular right because their unrivaled (and guaranteed) interest rates. While other types of Treasury

Bonds can be purchased through online brokerages, Series I Bonds can only be purchased directly, through treasurydirect.gov. They ask for a "street address." Driver's license information is optional, but that helps them verify you. If they can't verify you right away, you have to fill out their Form 5444 by going to a bank (who will surely ask for address documentation). While "street address" makes me want to use the street address version of my P.O. Box, or a PMB/CMRA address, this is likely to be flagged somewhere in the process. Also, it is a government agency, so one has to be careful. It seems like the only option here is to use my real home address in order to get a 9.6% interest rate on my money. Has anyone had experience with Treasury Direct?

A: The Treasury Direct website and overall service is very frustrating. Our experiences vary. I had no issues

adding my CMRA, but it was already on file with other government services. One of our staff was refused a new account completely. Fortunately, the bank stamp (seal) is easy to obtain. Much like a Notary, the bank is not confirming the content of any form, they are confirming the identity of the person signing it. The staff member completed the form, which included the PMB present on their license, had it signed and stamped at the bank, and submitted via postal mail. The account was activated in 20 days. Your results may vary. Note that you can also obtain I Bonds as part of a tax refund. I might know someone who intentionally overpays \$10,000 annually to the IRS, then accepts the refund in I Bonds with the high interest rate. ■

Are Trusts and LLCs overwhelming? We can help.

We believe all large assets should be titled to a Trust or LLC for privacy protection. Doing this correctly requires a lot of experience. We make sure your homes, vehicles, and any other assets which require titling stay out of your name. Contact us to reserve a consultation.



UPDATES

By Michael Bazzell

This quarter, I announced three big updates to the free resources available at [IntelTechniques.com](https://inteltechniques.com).

OSINT Tools

Three years ago, we were bullied into taking our search tools offline, threatened with lawsuits, and suspended by our web host. Now, the tools return with updates, free for everyone. New features are being added weekly. The latest version of all tools can be found at the following URL.

<https://inteltechniques.com/tools/>

Credential Exposure Removal Guide

We all have credential exposure. Within thousands of database breaches, our email addresses, usernames, passwords, and other sensitive details are being shared across the internet. Numerous websites allow anyone to search your email address and see the breach in which it was associated, often along with a partial password. For a few bucks, many sites will show anyone the full password. Let's do something about that. The following site explains how to remove your email address and exposed credentials from these services.

<https://inteltechniques.com/exposure.html>

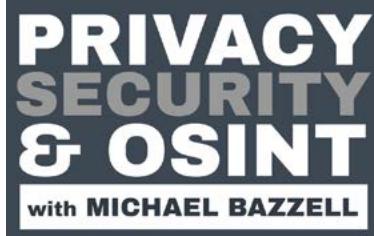
Proton VPN pfSense Config Files

The custom Proton VPN firewall import files have been updated to take advantage of the latest pfSense settings which help with overall stability.

<https://inteltechniques.com/firewall/>

As you can see, we are always busy updating the free resources on our site. Subscribe to our Blog to be notified of all changes, posts, podcasts, and magazine issues.

<https://inteltechniques.com/blog/>. ■



This magazine serves as a compliment to the podcast, which can be found at [IntelTechniques.com](https://inteltechniques.com). Below are summaries of the episodes from last month.

267-macOS Privacy & Security Revisited: After a lot of talk about Linux, I revisit privacy and security considerations for macOS machines.

268-CCW Permits, UNREDACTED 003, & Linux Questions: I discuss the California CCW leak, release the latest issue of UNREDACTED Magazine, and answer several listeners' Linux questions.

269-New OSINT Tools & Breach Data Lessons: I release the new online OSINT tools, offer three lessons from new breach data, and address several updates from past shows.

270-OSINT Tool Updates I: I explain numerous updates to the online OSINT search tools and offer some general usage tips.

271-OSINT Tool Updates II: I provide another substantial list of updates to the new OSINT tools, explain all usage, and offer numerous housekeeping changes. Yes, it is another OSINT episode.

272-Processor Attacks Explained: Paul Asadourian joins me to explain vulnerabilities within our computer processors and current solutions.

273-Credential Exposure Removal: I offer our new Credential Exposure Removal Guide and tackle the latest news and updates.

274-Firewall Stability Modifications: I explain some vital pfSense firewall modifications and offer a tip to prevent website chat apps from launching.

275-Archive Site Removal: I offer my new Archive Site Removal Guide and explain its usage.

276-When Google Attacks: I break down a recent report of Google terminating services of users who photographed their toddlers nude, the impact of their account loss, and solutions to prevent your own issues.

277-Burner Backfires & VoIP Updates: I explain how a recent client became exposed via temporary "burner" numbers and email, revisit VoIP solutions with a fresh look, offer a scripted way to directly access your Twilio calls, messages, and account details, and present an OSINT tip to passively collect content URLs within a site.

278-The Future Of Extreme Privacy: I offer a glimpse into the major projects we are wrapping up for the next level of Extreme Privacy.

LETTERS

By Michael Bazzell & UNREDACTED Staff

"Feedback on Radaris data removal process" by Long-time listener

I am proceeding through the workbook behind a VPN and using a new, anonymous email address, and encountered trouble with Radaris (<https://radaris.com/>). The link provided in your workbook to request removal (<https://radaris.com/control/privacy>) is a webform with entries for profile URL, user name, and email address, and only after completing a Captcha does it allow you to click "Send request". However, it fails with the error:

"We are unable to send a message to <email address>. Please email us directly to complete this request at, removals@radaris.com"

I followed this direction using my new Proton address and sent the following boilerplate message:

I have been unsuccessful in removing my personal information from your website. Per the information provided from your legal privacy policy, please remove the following details from your service.

Radaris profile url

Full Name

Physical Address

Telephone Number

Email Address

This was unsuccessful. As I refuse to make an account to remove my information, I replied using the same

boilerplate text but added an explicit mention of the CCPA and Radaris' "California Privacy Notice" (<https://radaris.com/page/ccpa>). This received a prompt response of "Your information removal request has been completed." Hopefully this is helpful.

"UK VoIP" by Niko

Firstly thank you for all your hard work, the magazine is brilliant! In regards to issue 003, I live in the UK so was particularly interested in the piece "Maintaining privacy in the United Kingdom". It's great to see someone else going through the same specific issues I have had in my privacy journey. I am particularly interested in VoIP and spent a lot of time looking into it, I originally followed MB's guide on creating a Twilio number and it all worked perfectly. However, to purchase a UK VoIP number from any provider you have to add a UK home address (I assume this is for emergency services but I never managed to confirm). Also, their servers were mainly in the US and I believe one was in Germany (if I remember correctly).

I wasn't sure if legally I would be ok to put any random UK address, and as there was no UK based server I felt it may become problematic in terms of latency for calls, with the server being at quite a distance. So I eventually scrapped that idea and looked around for other options, I ended up at MySudo being the best option in terms of ease of use. My main goal being to not have the number tied to my home address, and to have a few numbers to

segregate things. I haven't paid for the full version of MySudo that includes the VoIP numbers yet, as I still have some admin to do with my current number, but I had planned on purchasing the SudoPro plan in the very near future. At £10 a month it's certainly more expensive than it is in the US, but for 3 VoIP numbers and hassle free set up, it would be worth it personally.

Anyway; in the article it mentions MySudo being US/Canada usage only, which looking at their website is correct. However, within the app it gives me UK pricing for the sudo plans with VoIP numbers which indicates it will work, and also it states it's available in the UK. I assume you would probably still have to put a UK home address too but maybe there is a way around this that doesn't involve setting up a Limited Company or similar. And I'd love to know if there is a UK server, as I want minimal latency to minimise bad quality/dropped calls.

Editor's Note: I reached out to my contacts at MySudo, and received the following response: "MySudo plan pricing is based on the app store country to which a user's Google or Apple ID is configured. MySudo offers a UK plan and UK phone numbers. MySudo currently offers UK numbers with the same user account requirements as those associated with US and CA phone numbers. Regarding server location, MySudo's telephony services are provided using an intelligent routing network of points of presence in a number of countries, including across Europe."

"Anbox DNS Configuration" by Anonymous

I installed Anbox and had issues with Internet access. I found out it's because by default, Anbox points to Google DNS servers, which I block on the network. It doesn't appear to piggy back on the host system DNS. I may have missed you already doing this, but just in case, I thought I would mention that it would be good to tell the audience to run the following command:

```
snap set anbox container.network.dns=<DNS_IP>
```

Editor's Note: This is a big benefit from a community magazine. I was not aware of this and included the update on a previous podcast episode, and now include it here for coverage.

Gmail Script Update by Bill B.

I was implementing the Gmail auto-delete script you put out in Issue No. 3 of Unredacted and kept getting errors stating that the "requested entity could not be found." Turns out the script needed to be calling for deletion of threads, not messages. I also added a second round to delete spam emails as they're not automatically moved to the trash like inbox emails are using Gmail's forward and delete setting. This ensures that any emails hitting the account are deleted, including spam. Updated script below.

```
function deleteForever() {  
  var threads = GmailApp.  
    search("in:trash");  
  
  for (var i = 0; i <  
    threads.length; i++) {  
  
    Gmail.Users.Threads.re-  
      move("me", threads[i].  
        getId());}  
  
  var threads = GmailApp.  
    search("in:spam");  
  
  for (var i = 0; i <  
    threads.length; i++) {  
  
    Gmail.Users.Threads.re-  
      move("me", threads[i].get-  
        Id());}}
```

"Discover Credit Card Online Privacy Protection" by Frank

Long time listener, first time writer. I received an interesting email from Discover Credit Card offering me "Online Privacy Protection". Screenshot on the right.

Editor's Note: I have seen this, and I am torn. On one hand, it is providing a free service to remove personal information from a few sources. On the other, it is creating a false sense of security. Customers will assume that they are now anonymous, when the other 200 people search sites still display their information.

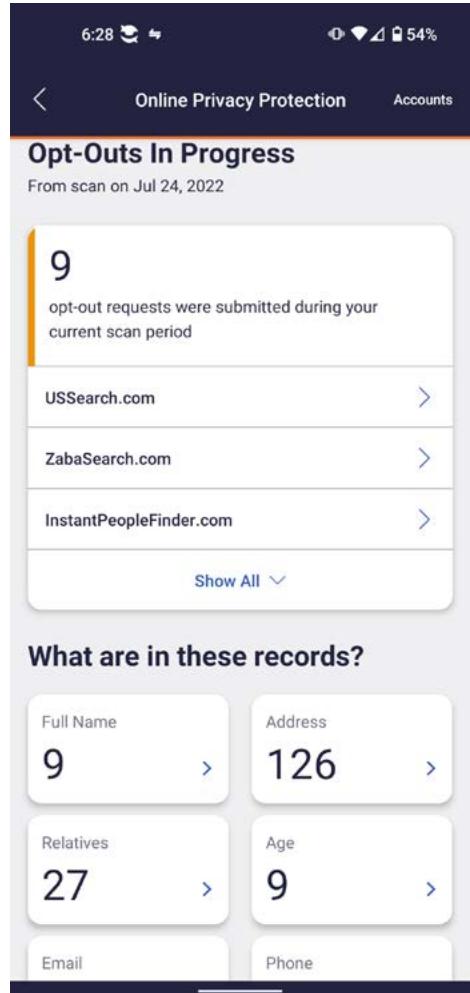


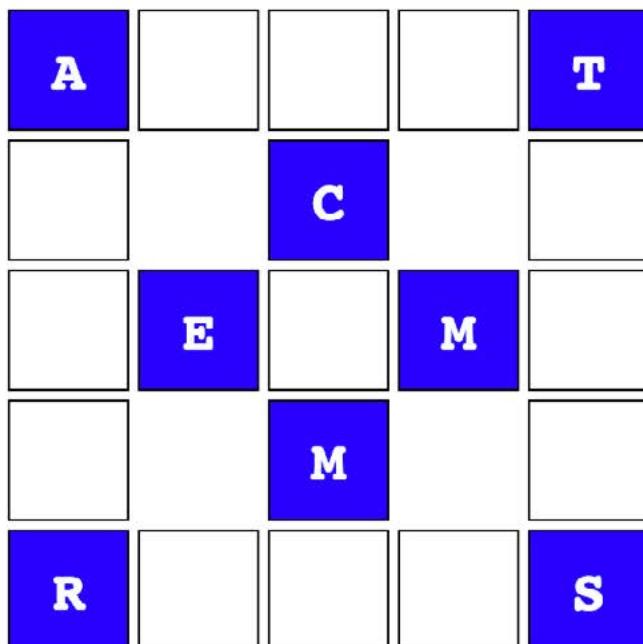
Image: Thom Milkovic



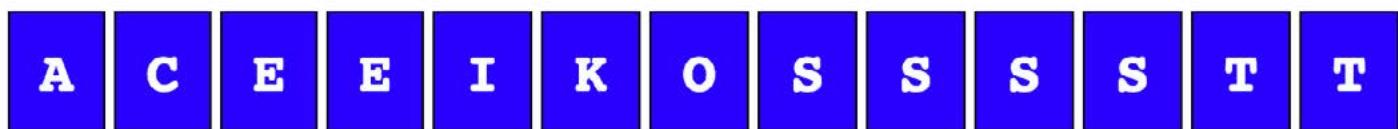
PRIVACY-THEMED PUZZLES

Security Word Puzzle #2

Michael J. Ross



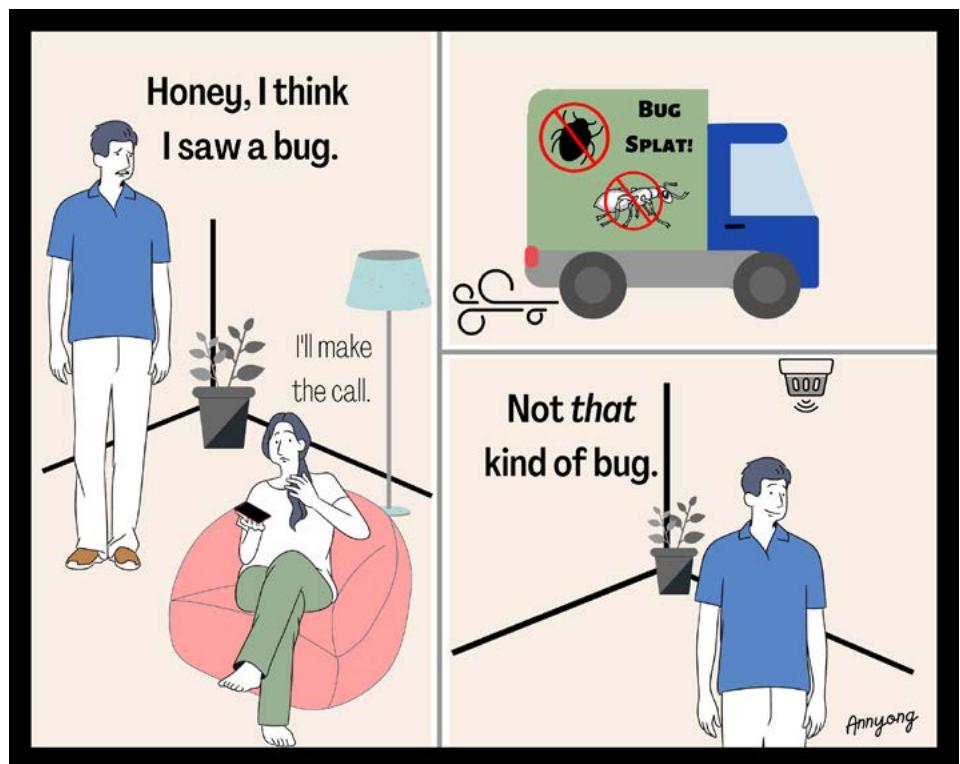
The objective of this puzzle is to discover the six words — all related to computer and network security — that fit in the above puzzle. Three of the words are horizontal and the other three are vertical, with overlap of some shared letters. Several of those letters have already been added to the puzzle to get you started. Here are the remaining letters to complete the puzzle:



The solution to the previous security word puzzle consists of the following six words (three horizontal and three vertical): OPSEC, IMAGE, THEFT, OSINT, SHARE, CHEAT.

CHUCKLES

By Annyong



FINAL THOUGHTS

By Michael Bazzell

Thanks for reading the final issue of UNEDACTED Magazine for 2022. I will meet you back here in January for issue 005 for Q1 of 2023. Please submit potential articles by November 15, 2022 for consideration within issue 005.

MB

AFFILIATE LINKS

If you would like to support this free publication, please consider using the following affiliate links. If you plan to purchase any of the items below, or other items from the vendor (such as Amazon), the following links provide a small financial contribution to us without costing you anything extra. We see nothing about you or your order.

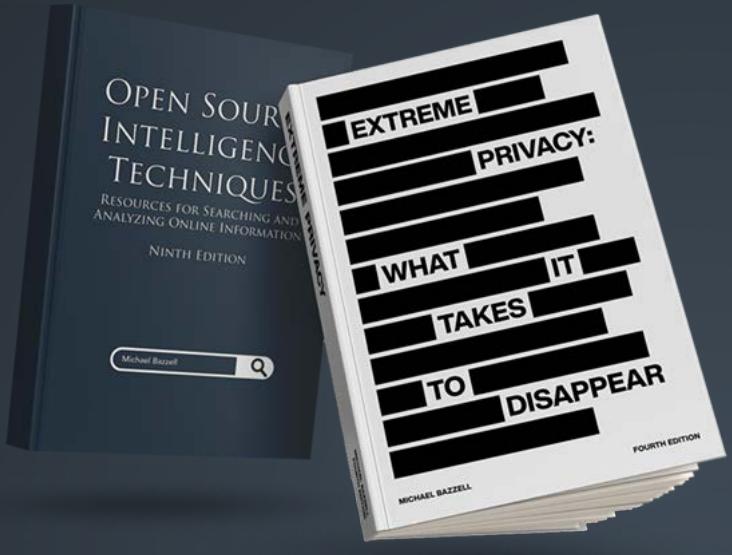
Extreme Privacy Book (Amazon): <https://amzn.to/3D6aiXp>

OSINT Book (Amazon): <https://amzn.to/3zoMZpZ>

ProtonVPN VPN Service: https://go.getproton.me/aff_c?offer_id=26&aff_id=1519

ProtonMail Encrypted Email: https://go.getproton.me/aff_c?offer_id=7&aff_id=1519

New 2022 Privacy & OSINT Books



- ✓ Hardcover & Paperback
- ✓ New & Updated Content
- ✓ 500+ Pages Each @ 8.5 x 11
- ✓ Our Full Playbooks
- ✓ Supports This Free Magazine

Order at IntelTechniques.com

OSINT & Privacy Video Training

90+ Hours of Video Training | Optional OSIP Certification

Register at IntelTechniques.net

Open Source Intelligence
Video Training + Certification

\$899.00

