

UNREDACTED

TRAVEL DISINFORMATION

Can we skew databases when we travel?

ORION VS SAFARI FOR IOS

A new mobile browser is offering
real value for iPhones

WHAT'S IN YOUR WALLET?


Three things we should all carry,
but most do not

LESSONS LEARNED FROM COLDPLAY



**UNREDACTED
ISSUE 008**

IN THIS ISSUE

- | | | | |
|----|--|----|---|
| 5 | From the Editor | 30 | Apple Updates |
| 6 | Lessons Learned from Coldplay | 31 | macOS Malware Monitoring |
| 7 | Revisiting the Prop Phone | 33 | ID Scanning is Getting Worse |
| 9 | What's In Your Wallet? | 34 | Another Home Address Exposure Concern |
| 12 | Self-Hosted SearXNG Guide | 35 | STR Wi-Fi Monitoring Concerns (& Solutions) |
| 14 | macOS VM on a Linux Host | 36 | E2EE Email Guide |
| 16 | Leaving Google Voice | 38 | Reader Q & A |
| 19 | Orion vs Safari for iOS | 41 | Windows 10 EOL |
| 21 | Testing the Cosmic Store | 42 | Take Me Out To The Reverse ATM |
| 22 | Testing Proton's Lumo AI | 44 | 911 What is your emergency? |
| 24 | Offline AI on Mobile | 48 | Final Thoughts |
| 26 | Detecting AI Text and Images | 48 | Affiliate links |
| 28 | Travel  information | | |

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 [IntelTechniques.com](https://inteltechniques.com). Contact details are also available at this site.

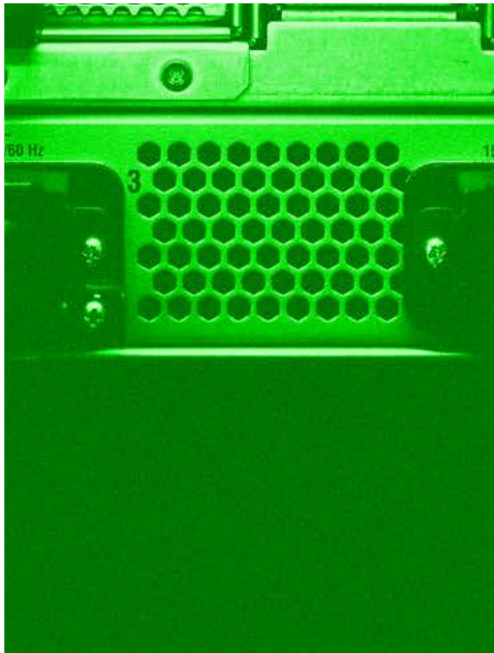
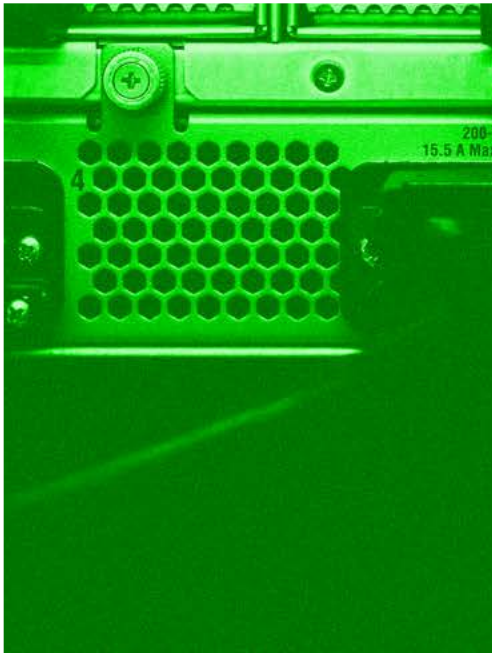
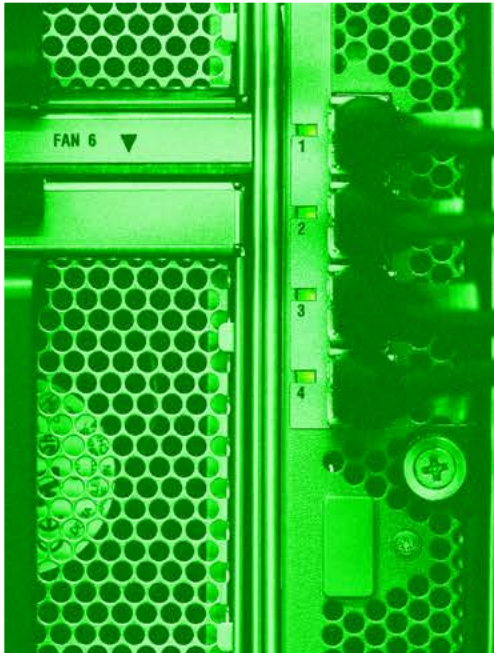
Copyright © of all articles belong to the original authors. The remaining contents of this publication are copyright © 2025 by UNREDACTED Magazine, and are published via a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International license. You may share it for free as long as you keep the entire file intact. Commercial use is prohibited.

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

Absolutely NO Artificial Intelligence (AI) was used to generate, review, or modify any content within this issue. We are embarrassed that we have to declare this now.

Editorial Image Policy

All images in this publication are presented for editorial, news, or commentary purposes. Some images may be modified for clarity, emphasis, or creative expression. Their appearance does not imply endorsement, approval, or affiliation by any individuals, companies, or organizations depicted. Copyright remains with the original rights holders.



FROM THE EDITOR

By Michael Bazzell

After publication of the previous issue, I had thought that this magazine might be finished. While downloads and overall interest were at an all-time high, article submissions were low. Not just low, practically non-existent. My goal for the magazine was always to combine three of my favorite things from the past: Bulletin Board System (BBS) text files, photo-copied hacker 'zines', and old-school 2600 quarterly issues. Each of those merged various views from the communities which they served into a long-form outlet, encouraging the reader to devour the content unavailable anywhere else. Times have changed.

The internet has spoiled us. We have overwhelming unlimited access to immediate information. Click bait titles draw us in while our attention spans, or lack of, become victim to the next juicy thing. When we do find something online of interest, the information is limited to a bite-sized chunk which we can handle while we check our messages and scroll our feeds. We get sucked into a video when the thumbnail shows the "influencer's" shocked face or they promise to tell us the one thing we need to know to solve all of our problems (but never seem to disclose the secret). OK, OK, I sound like Andy Rooney now... and I just lost half of the remaining readers as they go search to see who that is. I think we all need Andy today more than ever. We also need more long-form written content.

With this issue, I am trying something new. In April, we announced that our digital book provider was terminating our legacy account and eliminating the ability to send free updates to those who had purchased books. This was devastating, because they were the only provider who offered the specific services we needed. In order to keep our promises of free book updates, we decided to post any new content to our Blog, free for the world to see.

This was met with both praise and criticism. The majority preferred these online updates which were released as they were written, instead of waiting for a combined update within a PDF. They also preferred the ability to immediately see the new details instead of skimming through the entire book to find the modified content. However, many readers wanted a PDF which they could download and add to their files for future offline reference. Some felt it was unfair that the updates were free for everyone and not just those who bought the books. We respect both camps, but ultimately found it more important to do SOMETHING instead of NOTHING.

Recently, we decided to do both. We will continue to post updates to our Blog as needed over at <https://inteltechniques.com/blog/>. With this magazine issue, we are combining all of those recent update posts, plus many new articles with expanded content, within a single PDF which can be preserved and digested as desired. No

cost and no registration. Simply grab a copy from our site the same way as all previous issues.

While this issue is not much of a community effort, it allows us to use the existing avenue to deliver raw content which we feel is important. Most articles are simply attributed to "The IntelTechniques Team" since an internal group of us worked on them collectively. Any reference to "I" in those is a group effort "we". Two articles near the end were contributed by readers.

With this issue, we also eliminated any advertisements or paid endorsements. I am extremely thankful for our previous sponsors, as they made the past issues possible. This time around, we wanted to just focus on the content and not sales or ads. If you find value within these pages and have a strong desire to donate to the cause, please consider purchasing one of our digital books on our site. Give one as a gift to someone who needs it more than you. We also offer ways to donate virtual currency or smaller amounts at the end of this magazine. However, there is no pressure to donate, **we want to do this work.**

We now respectfully present issue 008 of UNREDACTED Magazine. No fluff. No filler. No agenda. Just free information.

MB



Image: Grace Springer via Storyful

LESSONS LEARNED FROM COLDPLAY

By The IntelTechniques Team

We suspect that every reader has witnessed the Coldplay exposure of a couple having an affair at one of their concerts. It began as an opportunity to connect with the attendees of their concert as the singer made up little songs about random people in the crowd. When the couple appeared on the jumbo screen, they panicked, ducked, and hid their faces hoping not to be exposed to their spouses. Of course, this blew up on the internet and led to the resignation of both people, who happened to be executives at the same company.

This started a slew of ridicule, mocking, and re-enactments. It also started a conversation about privacy, accountability, and lawsuits. We have no connection to any of it, but we wanted to discuss some lessons which can be learned from this incident.

First, they were in public, and there is no expectation of privacy in public. Some will say they were at a ticketed event and had some right to privacy, but we disagree. When you are at an event with thousands of other people,

you are in the public. You should expect that you are being recorded at all times.

Next, you give up many rights when you purchase a ticket for an event. We never read the full terms and conditions which are tucked away on a website hard to find. The terms change more often than we can digest. There is probably some lingo which explains that you can be recorded and possibly even made part of the show. In this case, the singer of the band announced what they were about to do before actually doing it. The speculation of lawsuits is ridiculous. Even if an attorney took the bait, the suit would quickly be thrown out.

Finally, the big lesson in all of this. **Abnormal behavior brings attention!** If the couple would have just smiled and froze, we would have never known about any of this. The video might have been posted online, but there would be nothing interesting to see. We would all move on to the next thing. When they panicked and embarrassingly hid from the cameras, they brought attention onto themselves and the world wanted to know why.

When you crave privacy in public, the best thing you can do is to blend in and go with the flow. I have seen people make a scene when a self-checkout register at Walmart displays a video of them, even though they were just captured by over 100 cameras throughout the store, only to become more scrutinized than those who slipped under the radar. I have also witnessed people hiding their faces from all security cameras, attracting the attention of security officers who would have otherwise not noticed their presence. In both cases their footage is likely stored longer in case of a future incident, which is the opposite of what we want.

When in public, we should prefer to never make a scene. The footage will drop off much quicker than if attention were focused on us. Everyone has a video recording device and an internet connection. If you give them the slightest reason to think you are doing something outside of the ordinary, they will record you and shame you on the internet. We hate that this is the case, but it is our new reality. ■



REVISITING THE PROP PHONE

By The IntelTechniques Team

In the Extreme Privacy series, we discussed the benefits of a prop phone. Specifically, we explained how a dead mobile device with a cracked screen can bypass the everyday demands to access things on your phone which would previously be done in person. During the pandemic, we were forced to download restaurant apps to order food. Showing a cracked phone magically allowed humans to talk to other humans and get things done without technology. Showing a

recently-cracked phone to a hotel clerk might bypass their demands to use their app to check in and unlock doors. The cracked screen trick still works, but we have a new preferred solution. The dumb phone.

Only a few years ago, you would receive looks of confusion if you were seen with an old-school flip phone. Today, they are making a comeback. As we all realize our addictions to screens are causing damage to our minds and bodies, many people are ditching the smart phone in favor of something less

technical. We now issue a generic flip phone to every client with high risk, especially domestic abuse victims. Consider the following.

- A flip phone typically possesses a longer battery life than a smart phone with a high-resolution screen. Tucking it away for a week while it is turned off should present a full battery upon boot.
- Any cellular telephone can make emergency calls without a SIM card or cellular plan. Having this phone in your car ensures you have a way

to contact 911 without disclosing your true cellular number. See the article near the end of this issue for more details.

Flip phones can't do all of the things a smart phone can. Most cannot store apps, scan QR codes, or browse the internet. This can be a real issue when you need the technology ... or it can be a great excuse when you don't want the fuss. I have witnessed all of the following scenarios play out in the past three months.

I attempted to buy tickets for an MLB Baseball game. The stadium requires usage of apps such as MLB Ballpark or Seat Geek to gain entry. You must display your smart phone at the gate and allow the QR code in the app to be scanned, which changes every 30 seconds, preventing screen captures or printed codes. I went to the stadium store and asked to buy tickets there. They happily agreed to sell them, but then demanded a cellular number to text a link which would again require their app to be downloaded.

I explained that I only had a flip phone due to social media addiction. They called my bluff and asked "Do you have it on you now?". I did not expect that but replied "Yes! I will go grab it!". I went to the car, grabbed the flip phone from the console and proudly displayed it to the sales person. Again, magically, they were able to print two tickets. The workers further explained that they do not advertise the ability to do that because everyone will just lie about their phones to get printed tickets. Apparently, this is an issue of

scalped tickets, but the extra effort to see a game is frustrating.

I once decided to visit a local water park with family members. We assumed we could just show up and pay the entry fee. Nope. You must purchase tickets through the website, which will automatically create an account through their portal. A phone number is required in order to send a URL via SMS text which opens the app store on the device to download the county parks app. Only there will you be presented with the numeric barcode allowing entry.

For this one, I called ahead and explained I did not have a smart phone. The worker was not sympathetic and only told me to find a family member who had one. I was explicitly told it would be impossible to enter the park without the app. I turned up the heat. I explained that my lack of smart phone was due to a vision impairment, and I was surprised that the facility did not accommodate those with disabilities (I wear glasses sometimes, technically this was all true). It should be no surprise, they told me that I actually could purchase the tickets at the gate with cash, but they just don't want everyone doing that because of the "hassle".

I encountered only one instance where none of my tactics seemed to work. At a local lake within a state park, there were kayaks which could be rented. The booth was well-staffed, but all of the kayaks were secured with smart locks which could only be opened within an app assisted by Bluetooth. I tried everything. The smug employees

would not budge. At one point they just said "No app, no boat, deal with it". They joked that I was a "loser" who could not afford a "real" phone.

I stared into their eyes, and explained with a dead face, "I have a pornography addiction. If I touch a smart phone, I will do things you do not want to see". Once again, magically, I was allowed to proceed with the transaction using cash without an app. The avenue exists. It should not be this difficult to get people to do their jobs.

Some will read this and think I am being foolish. Some may not like my lies to push the limits. I see things differently. If we all just accept the new ways which technology is invading our lives, nothing will change. Things will get worse. If we resist and push back, we may have a chance. It may remind them that we don't all want to live our lives through apps. We don't all want to get rid of cash. We don't all want to eliminate human communication as part of our daily tasks.

I ask you to consider how you will react the next time a one-off transaction demands that you download yet another invasive app. Will you give in, download the poorly-designed software, allow it rights to your data, complete the account creation, add another credential which will eventually get breached, enable your location services, and grant exclusive rights to sell anything it learns about you? Or, will you resist and identify the existing policies which likely grant the ability to hand over some cash to get what you need? ■



WHAT'S IN YOUR WALLET?

By The IntelTechniques Team

Readers of Extreme Privacy already know that I pay a lot of attention to my wallets. I always know which one has all of my real IDs and which have "employee" IDs in fake names, "secondary" name credit cards, and various filler cards to round them out. However, I have rarely spoken about three items which I now carry everywhere, which most people have probably never considered. This article might make me sound like an old man, but please consider how it may have an immediate impact on you.

Emergency Contact Card: Assume for a moment that you have played along with my books and executed everything perfectly. Your home,

vehicle, and assets are private and you may barely exist within consumer databases. You may be living in an area with no record of your existence. What happens after a catastrophe? If you overturned your vehicle and were unconscious, could authorities find your family or friends? How would they know where to start? If you were in a coma for three days, would anyone know how to access and care for your animals?

We spend a lot of time keeping people out of our business, but there are circumstances where we may want them to push through our privacy barriers. This is why I encourage all of my clients to possess a list of emergency contacts wherever they keep their driver's license. It could be a folded

piece of paper tucked behind your ID. Mine has my true home address, home pet information, and the telephone numbers (VoIP) of two emergency contacts. If a true emergency occurs, and my details are exposed, I would rather give up all of my privacy and move than to risk my health or the health of my pets.

This may seem invasive to you, but consider the following. When I was a street cop, I responded to a serious vehicle crash where the driver was flown to a trauma center with life-threatening injuries. While in his hospital room, a nurse gave me his wallet. He was from another state and only had a hotel key card as a lead to his temporary residence. He would likely be unconscious for several days and

we had no way to contact any relatives. We had no records of him in our system and the address on his license was now occupied by a different family. The hospital was concerned about end-of-life decisions and knew very little about their patient. I responded to the hotel to see what I could find out and let them know about the situation. They confirmed he was scheduled to check out at the end of the week and offered to let me in his room (while escorted) in an attempt to locate any documents which may help us find his family. Upon entering, a small dog within a kennel was whining, likely hungry and thirsty. The dog was taken by animal control, but we found no information which helped us.

The man died later that day. The dog was held at animal control. We still had no one to contact. The man's phone was destroyed in the crash and digital leads were thin (this was before every American was in hundreds of databases). The next day, a woman contacted the hotel stating that she was family and had not heard from the man. The hotel gave me her number and I broke the news. She arrived the next day to claim the body and take the dog. What if we would not have known about the hotel? What if we had not found the dog? While modern phones have an emergency contact option which can be accessed without unlocking the screen, I do not use this option. Phones break or get lost. A piece of paper can withstand more, it is easily discarded, and it shares no details with any third parties.

I believe every person who has taken extreme steps to protect their privacy should keep a list of emergency contacts in their wallet. This is especially true if you have pets. Many of us do not display our true home address on our driver's license or vehicle registration. This is a basic step for privacy, but

can be concerning if you are severely injured in an accident. My house is not in my name. If I die in an accident, law enforcement would have nothing to help them find a relative. If my dog is home alone, no one would know. This is why I keep a card in my wallet with the following information.

- Primary Emergency Contact Number
- Secondary Emergency Contact Number
- Pet Location
- Reward Details

My primary contact is the VoIP number of a relative and the secondary is the VoIP/Signal number of a close friend. Both know where I truly live. Both would know to go and take care of my dog. What if one or both of them was with me in a horrific accident? While far-fetched, it is possible. This is why I also keep my true home address and pet's name on this card. No one will see it unless my wallet is stolen or I am unconscious. If I am injured, privacy is secondary. I don't want to risk my pet dying alone in my home for weeks while strangers try to learn more about me.

I also believe reward information is warranted here. My card reads as follows:

"Reward if Found-All cash within wallet plus \$200-Contact 212-555-1212"

If my wallet is lost or stolen, recovering my IDs, credit cards, and other sensitive documents is worth the money.

I simply print all desired details on a piece of paper and then laminate it into the size of a credit card. I typically hide this card in the back of everything since I should never need to access it. If I am dead in a ditch, law enforcement will go through everything and find it.

Business Cards: This is another item which I always like to have immediately accessible. I have no desire to hand them out to gain new business, but they serve a much different purpose for me. They help me SELL the information and help me quickly KNOW the details.

Anyone who plays the privacy game has experienced the awkward moments when we try to remember which burner number we used or the appropriate email address to give. When I check into a health clinic for any reason, the questions start coming. What is your cell? What is your email? What is your address? Some of us may have memorized all of the details we prefer for every need. Some of us get confused. I like to take out my business card and just hand it to the receptionist. I let them read and type in my VoIP number, dedicated health email, and full PMB information. It is simply much easier than reciting everything and getting tripped up when they ask to repeat something.

I have also seen the business card bypass ID checks. When I roll in with the business card out and seem "helpful", there seems to be less overall scrutiny of my true identity. Anyone can have business cards made, or print their own, but for some strange reason these silly pieces of paper add realism to anything we do.

I prefer to order professional cards, but homemade jobs also do the trick. You can purchase breakaway cards in a standard sheet size and print them yourself. I keep mine fairly simple. They include my name, phone number, email address, CMRA address, and a very generic company name. I never get fancy or claim to be a pilot. Keep it boring.

I also keep an alias business card in my wallet. It can be used when there

is no need to give out a real name, cell, and email, but pressure from employees can be a burden. I may not want to make the privacy fight when I could just hand over a card with non-invasive details. I have done this when shopping for high-end items which often require a customer profile in some insecure database. We have all witnessed the sales person who must know if we are in their system before we can be shown a watch, piece of jewelry, or vehicle. I always frustratingly say "If you really need all that before I can see an item you want to sell me, copy it from here and let's move on". They think they are getting what they want for sales leads, and you are not giving out anything real.

Another person, even a cop, finding an alias business card is no big deal. One would assume your alias is someone you know. After all, who would actually carry a fake business card? Well, we would.

microSD Card: I always possess a 1 TB microSD card within my wallet. It stores a full backup of all personal documents and files primarily kept on my laptop. This encrypted drive is updated monthly. If my house explodes while I am away, I have all vital data with me to restore it to a new machine until I can access my out-of-state offsite archive. The full-disk encryption protects the contents.

Signal Protection: The image at the beginning of this article displays two RFID-blocking wallets from SLNT. I rely heavily on their thin wallets, but might consider a bi-fold when traveling long-term. The thin wallets allow me to discretely carry only the basics and limited cash, and easily fits in a front pocket for security. The Bi-fold allows more cash and more cards, but also adds more bulk. As stated in the book, I prefer to carry two slim wallets when traveling to shady areas. If robbed, I can easily throw them the wallet with

less-sensitive items in alias names and a little cash while preserving the wallet way more important to me. Fortunately, I have only needed this once.

Some will question the need for signal-blocking wallets. Cloning the chip from a credit card is quite difficult and using it for a purchase even more unlikely. However, I care more about my passport card and any access cards. I often find myself working in areas which require a contactless card for entry into a secured office, gate, or garage. Those can be trivial to clone, and I do not want to explain why my access card was used without authorization. Therefore, I always have a signal-blocking wallet with me. SLNT offers discounts to readers at <https://slnt.com/discount/IntelTechniques> if you prefer not to make your own with foil.

What is in your wallet? Don't let this be an afterthought. Prepare for emergencies and awkward situations now. ■

SELF-HOSTED SEARXNG GUIDE

By The IntelTechniques Team

In my books [Extreme Privacy](#) and [OSINT Techniques](#), I discuss the SearXNG as an option to access search engine results. SearXNG is not a search engine itself. It is a metasearch engine which aggregates the results of multiple search engines, such as Google, Bing, and others, but does not share information about users to the engines queried. It is also open source and can be self-hosted. The easiest way to get started is to visit <https://searx.space/> and test a few public instances.

After you have played with any of the public instances of SearXNG, you may now see the benefits of an aggregated search service. You may also be considering the risks associated with this behavior. Let's start with the benefits of a public instance which is not self-hosted.

- All queries are submitted to search engines from a third-party server.
- The IP addresses collected from engines are those of the server, not yours.
- Your queries cannot easily be associated to one user by the engines.

That may sound great, but there are risks with public instances. Consider the following.

- The host of the instance could monitor your queries.
- If the host is popular, some engines may block access.
- If the host has an outage, you are without service.

Overall, I believe it would be very unusual for a SearXNG host to monitor queries. This cannot be done with the stock SearXNG software, and hosts

would have to go out of their way to collect data about users. I just do not see the motive of that. However, anything is possible. Personally, I prefer to self-host my own instance of SearXNG. Consider the following benefits.

- All queries are submitted from your machine directly to the engines.
- The tracking code on engine websites is removed from the SearXNG pages.
- Minimal usage ensures that all options function reliably.
- Does not rely on the uptime of an online instance for my queries.

As always, there are also risks. My IP address is submitted with every query I make, but I am always behind a VPN so I am not bothered by that. The ability to host my own code and know that no one else is intercepting that data is more important to me. You can never hide the queries from the search engines themselves, but you can limit the information loaded into your browser by not visiting their sites directly. Receiving results from multiple search engines simultaneously is very advantageous. Take some time to determine whether you are better served with a public instance or your own. I took the following steps on my Linux machine to configure my own host locally. If you decide to replicate these steps, you should copy and paste the in its entirety directly into Terminal. Note that these steps deviate from the official installation guides which are mostly outdated.

All commands in this issue are on our website at <https://inteltechniques.com/data/008.txt> for easy copy and paste.

```
sudo -H apt-get install -y
python3-pip python3-dev py-
thon3-babel \

python3-venv uwsgi uws-
```

```
gi-plugin-python3 \

git build-essential libx-
slt-dev zlib1g-dev \

libffi-dev libssl-dev

mkdir ~/Documents/searxng &&
cd ~/Documents/searxng

git clone "https://github.com/
searxng/searxng"

python3 -m venv searxngEnvi-
ronment

source searxngEnvironment/bin/
activate

pip install -U pip

pip install -U setuptools

pip install -U wheel

pip install -U pyyaml

cd searxng && pip install
--use-pep517 --no-build-isola-
tion -e .

sudo -H mkdir -p "/etc/searx-
ng"

sed -i "s|ultrasecret-
key|$(openssl rand -hex 32)|g"
searx/settings.yml

sudo -H cp searx/settings.yml
/etc/searxng/settings.yml

export SEARXNG_SETTINGS_
PATH="/etc/searxng/settings.
yml"

deactivate
```

My machine is now configured to run the SearXNG software. The following commands execute the program.

```
cd ~/Documents/searxng

source searxngEnvironment/bin/
activate

cd searxng
```

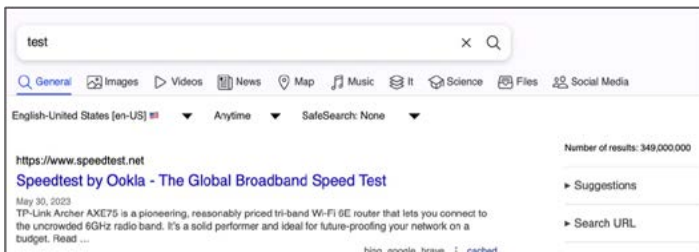


```
python searx/webapp.py
```

The software is now running in the background. You can minimize this Terminal window. As long as it is not closed completely, the service is running. You can launch Firefox and navigate to <http://127.0.0.1:8888> to load your own instance. Similar to public instances, any modifications you make to SearXNG will be erased when you close Firefox, unless you add <http://127.0.0.1> to your stored cookies (or modify the `settings.yml` file directly). You can execute the following commands to fetch any updates.

```
cd ~/Documents/venv/searxng/searxng
git pull "https://github.com/searxng/searxng"
```

If desired, you can add these two commands to the Linux update script presented in Extreme Privacy. You could also add the launch commands to the maintenance scripts within the book. The image below displays an example query. Notice that I receive results from Google, Bing, Brave, and DuckDuckGo simultaneously.



From any search result, I prefer to click the “Preferences” option on the far right and make a few modifications. I disable any auto-complete options; disable SafeSearch; switch to a light theme; enable results in new tabs; and enable preferred search engines throughout all topics. You can even modify the way URLs will be presented. This allows you to remove embedded URL tracking codes, force older or mobile versions of websites, or even remove affiliate tracking links. Your options are unlimited when you control the code. If you want to store these changes so they will be preserved after you restart Firefox, you must conduct the following.

- Navigate to Firefox’s Settings menu and click the “Privacy & Security” option.
- Click “Manage Exceptions” next to “Delete cookies...”.
- Enter the URL of your SearXNG instance, such as “<https://127.0.0.1>”.
- Click “Allow” and “Save Changes”.

I currently have a self-hosted SearXNG instance running on my laptop, which allows me to query dozens of search engines simultaneously from my browser without trusting any third-party middle man. Since I rarely search or browse websites from my mobile device, I simply rely on a public SearXNG instance on it.

Let’s repeat the process for those on macOS who want to self-host SearXNG. Make sure you have Homebrew

configured as explained in the book.

```
brew install python git
mkdir ~/Documents/venv && cd ~/Documents/venv
python3 -m venv searxng
source searxng/bin/activate
cd searxng
git clone "https://github.com/searxng/searxng"
pip3 install -U pip
pip3 install -U setuptools
pip3 install -U wheel
pip3 install -U pyyaml
cd searxng && pip install --use-pep517
--no-build-isolation -e .
cd searx && sed -i '' "s/ultrasecret-
key/00ef3039748274b4f2b93d16fb9695de00a4b-
b35e4c02b7704a167c7aeb274bd/g" settings.yml
sudo mkdir "/etc/searxng"
sudo cp settings.yml /etc/searxng/settings.yml
deactivate
```

My machine is now configured to run the SearXNG software. The following commands execute the program.

```
cd ~/Documents/venv
source searxng/bin/activate
cd searxng/searxng
python3 searx/webapp.py
```

The software is now running in the background. You can minimize this Terminal window. As long as it is not closed completely, the service is running. You can launch Firefox and navigate to <http://127.0.0.1:8888> to load your own instance. Similar to public instances, any modifications you make to SearXNG will be erased when you close Firefox, unless you add <http://127.0.0.1> to your stored cookies (or modify the `settings.yml` file directly). You can execute the following commands to fetch any updates.

```
cd ~/Documents/venv/searxng/searxng
git pull "https://github.com/searxng/searxng"
```

If desired, you can add these two commands to the macOS update script explained in the book. You could also add the launch commands to the maintenance scripts presented there. If there is enough interest in self-hosting in Windows, I will ask Jason to work out the steps on his Windows machine. ■



MACOS VM ON A LINUX HOST

By The IntelTechniques Team

In our book OSINT Techniques, we explain the importance of using virtual machines (VMs) for online investigations. In the book Extreme Privacy, we focus on the power of VMs when you need a private environment. In both books, we explain how VMs can be helpful when transitioning from Windows to Linux. You could run a Linux VM on Windows to become familiar with the OS or a Windows VM on Linux to access any apps which are only available within a Microsoft environment.

One thing we have not covered is the ability to run a macOS VM on a Linux host. This could be to access apps only available within Apple systems or to test macOS software. Accessing a macOS installation on a Linux host has never been easier. First, let's download and install the software needed with the following Terminal commands. These were tested on Pop!_OS, but should work on any Debian-based system, including Ubuntu.

```
sudo apt-add-repository ppa:-  
flexiondotorg/quickemu
```

```
sudo apt update
```

```
sudo apt install quickemu  
sudo apt install quickgui  
quickget macos sonoma
```

This will download an official base system installation file from Apple's servers. Note that at the time of this writing, the latest macOS operating system supported by Quickemu was Sonoma, even though the latest system available from Apple is Sequoia. However, choosing the Sonoma option actually downloaded the latest Sequoia file. Always choose the latest version of macOS offered by Quickemu.

This will create a file in the Home directory called `macos-sonoma.conf`. I opened this file and added the following two lines at the end. This increased my CPU cores from 2 to 16 and my RAM from 4 to 24. Change these based on your own resources.

```
cpu_cores="16"
```

```
ram="24G"
```

The following command launches Quickemu and boots to our Apple installation image.

```
quickemu --vm macos-sonoma.conf
```

Use the keyboard arrow keys to select 'macOS Base system' and strike Enter or Return, then allow the process to complete. Then conduct the following.

- Select "Disk Utility" and click Continue.
- Select the drive labeled "Apple Inc." and click "Erase".
- Rename to "macOS", select "APFS" and click "Erase".
- After completion, click "Done" then close Disk Utility.
- Click "Reinstall macOS..." and click Continue twice.
- Read and agree to any license terms.
- Select the "macOS" drive and click "Continue".
- Allow the installation configuration to complete.

This can take a long time, and pay no attention to the estimated completion clock. Mine took 30 minutes. Before I modified the settings within the configuration file, it took 60 minutes. Be patient and allow it to do what it wants to do. If a reboot presents a black screen, close the window and re-launch the VM. If a reboot prompts a disk selection, always choose the "macOS Installation" option until that option is no longer present. You may need to do this a few times and allow more long processes to complete. Hang in there.

Then choose the "macOS" disk once the "Installation" option is gone. You may need to allow a few reboots.

Your VM likely opened in a window in low resolution. I like to make modifications to the launch command which upgrades the display to my host resolution and opens the VM within its own full screen view. Modify the following command as desired for your own system.

```
quickemu --vm macos-sonoma.conf --fullscreen --width 1920 --height 1200
```

Upon boot, modify the resolution in macOS as desired. I modified the following.

- Settings > Display > Advanced > Show Resolutions as List > Done > Show all resolutions > 1920x1200

Next, we need to install software to the Linux host in order to allow file sharing and copy/paste capabilities between the Linux host and some VMs.

```
sudo apt install spice-vdagent -y
```

```
sudo apt install --no-install-recommends samba -y
```

We can now re-launch our VM with the following command.

```
quickemu --vm macos-sonoma.conf --fullscreen --width 1920 --height 1200 --display spice
```

Upon boot, go to Finder > Go > Connect to server and add the Samba server listed in Terminal when you boot the VM. You may need to change workspaces and click the Terminal icon to see the window. Mine was `smb://10.0.2.4/qemu`. This presented a new folder which shares data from my host machine in the Public folder under Home.

This is all great, but I do not want to type that entire command into Terminal every time I want to launch macOS. Therefore, the following command creates a shortcut for our needs.

```
quickemu --vm macos-sonoma.conf --fullscreen --width 1920 --height 1200 --display spice --shortcut
```

This will create a shortcut within your Applications list, but it will likely not launch with your settings unless you add "bash" and quotation marks around the entry within the desktop shortcut. My configuration file was at:

```
~/ .local/share/applications/macOS-sonoma.desktop
```

I changed the line to:

```
Exec=bash -xc "quickemu --vm macos-sonoma.conf --fullscreen --width 1920 --height 1200 --display spice"
```

I then launched the program from the new shortcut in my Applications list and all appeared as desired. This is optional. You could also use the Quickgui option to launch VMs, but I find it limiting.

You can now use the steps in Extreme Privacy to configure your new macOS VM any way desired. You can duplicate the folder and conf file to create other VMs. I keep both a full-functioning macOS VM and a limited duplication. I added `network="none"` within the restricted VM conf file to eliminate any internet to the VM. I can now use this for a completely offline option when I want to use Microsoft or Adobe products without interruption or sending data to their servers. I can also use a restricted VM for breach work if desired. Consider how these could help you. ■

LEAVING GOOGLE VOICE

By The IntelTechniques Team

Readers of my books know that I have relied on Google Voice heavily over the past twenty years. I created an account at GrandCentral in time to be grandfathered in to the first iteration of what became Google Voice. Having a free second phone number seemed magical at the time. I canceled my landline and began making calls from my computer. The early 2000's were amazing.

Eventually, my Google Voice number became a way to stop exposing my true cellular number. For a while, anyone could create unlimited accounts to obtain free phone numbers. I created way more than I should. Over the years, I allowed several of them to drop off, but kept about twelve actively-used numbers.

Over the past decade, I began to rely more on other VoIP providers such as MySudo, Voip.ms, Twilio, Telnyx, Cloaked, and others. I kept my Google Voice numbers active, but tried not to use them. They were treated as a way to receive incoming text messages and voicemails, but I almost never logged into a Google account in order to return any communication. When needed, I would respond from "better" numbers and have the other person update their contact information for me.

My concerns around Google Voice numbers are two-fold. First, they are not private. Google can see anything they want. While other VoIP providers are technically no more private either, Google runs a search monopoly and uses a lot of data to train their AI. While I would hope that my communications would never be used for that type of activity, I have no control over their data. Second, I worry about account suspension or mandatory ID verification.. I have had Google accounts terminated in the past over TOS violations. My account in my real name is banned from YouTube. I simply do not trust that Google will not cancel one or more of my numbers on a whim. Below is the message I receive when accessing YouTube from my original Google Account. The suspension occurred after I released a podcast critical of Google's services.

Unable to access a Google product

If you've been redirected to this page from a particular product, it means that your access to this product has been suspended. Read on for more information.

Your access to this Google product has been suspended because of a perceived violation of either the [Google Terms of Service](#) or product-specific Terms of Service. For specific product guidelines, please visit the homepage of each Google product you're interested in for a link to its Terms of Service.

Google reserves the right to:

- Disable an account for investigation.
- Suspend a Google Account user from accessing a particular product or the entire Google Accounts system, if the Terms of Service or [product-specific policies](#) are violated.
- Terminate an account at any time, for any reason, with or without notice.

I have finally decided to pull the plug. I am porting out all of my Google Voice numbers into better platforms. I will keep the numbers I need, allow unused numbers to expire, and document the entire process. I have been procrastinating this decision for years. I have explained port forwarding in the book, but I suspect there will be minor changes to the process since publication.

First, let's talk about unused accounts. Google Voice is constantly monitoring number usage with the intent of closing dormant accounts. Incoming calls and messages do not matter. If you have not logged into your Google Voice account and sent an outgoing message or placed an outgoing call within the past 30 days, you will receive a warning from Google. I received the following today.

We noticed that you haven't used your Google Voice number in a while. Because phone numbers are a limited resource, it is our policy to reclaim unused numbers so they can be made available to new users. If you'd like to keep your Google Voice number, you will need to make calls or send text messages by September 10, 2025 by logging in to your account or using the Google Voice app. Please remember that your current number will be reclaimed in 30 days unless you start using it. If the number is reclaimed, your existing messages will remain available in your account, but you will no longer be able to receive calls or text messages.

In the past, this was the only warning you received. Today, you also receive a 7-day warning before the number is

reclaimed. I received the following last week after I intentionally allowed a number to expire,

This is to confirm that your Google Voice number has expired. All of your existing messages remain available in your account, but you are no longer able to receive calls or text messages.

For most people, I never recommend allowing a number to expire. It will go dormant for a while, but will eventually be re-issued to a stranger. Anyone calling that number looking for you will be forwarded to someone else. I have way more numbers than I would ever need, and many were never used. Therefore, I have a process I go through whenever I receive a 30-day warning.

First, I search the number within my email. I have always had all incoming Google Voice SMS messages and voicemails set up to forward to a dedicated Proton email address, as explained in Extreme Privacy. I never delete any of these messages. If I have ever received any communication to this number, there should be an email message documenting the activity. In one recent case, I had no messages.

Next, I search the number within my password manager. Any time I use a VoIP number as part of any account creation or usage, I add that number to the entry for the credentials within the password manager. In this same recent case, I had two hits. I had provided this number to two utility services several years ago in connection to a home which I no longer occupy. There was no need to keep this number any longer, so I took no action and let it expire. If I had wanted to keep the number active within Google Voice, I could simply log in and send a few text messages to other numbers.

The email I received today was about a number I actually needed. I had used this number in connection to an LLC

which I use for asset management. The bank for this LLC uses this number for communications, and insists that I call them from this number for any inquiries about my account. I need to port this number out of Google Voice into another provider.

I decided to port this number into Voip.ms. I can follow the guide within Extreme Privacy to forward all incoming text messages to email and I can make (or receive) calls through my laptop or mobile device. I can also send SMS messages from mobile as explained in the book.

I logged into the Google Voice account and navigated to <https://voice.google.com/u/0/settings>. I then clicked the “Unlock” button which prompted me to provide a credit card to pay the \$3.00 unlock and transfer fee. I provided a Privacy.com card number without issue. Once the number was unlocked, I created a screen capture showing this change. I scribbled a signature onto this screen capture and added the date for later use. Next, I enabled the feature to “Call to listen”. This prompted me to assign a PIN to this number, which I did.

I logged into my Voip.ms account and navigated to <https://voip.ms/m/didporting.php>. I chose the “Start procedure” process for my country and entered my Google Voice number and PIN. I proceeded and provided the business name associated with the Google account and a CMRA address. Google never had any address, so it should not have an issue with this. I uploaded the screen capture and added my PIN to the comments section. I submitted the request and waited.

Within a few minutes, I received an email from Voip.ms that the number was added to my account in order to configure it before porting. This is very helpful so that the moment the number is ported, it will function as desired within Voip.ms and any incoming calls

will go through. I configured all call routing as explained in Extreme Privacy. Messaging will have to wait until the number is ported. I then received an email from Voip.ms anticipating the port to complete within 48 hours.

Two days later, I received a notice from Google Voice that my number had been ported away. Voip.ms still showed the transition as “Pending”, but also that it was set to be added to my account on that date. Later that same day, Voip.ms confirmed the porting and I had full access to the number. I followed the steps within Extreme Privacy to configure calls, voicemail, and text through both my laptop and mobile device. I activate encrypted SIP calling on all accounts. I then replicated the entire process again and ported numerous Google Voice numbers into Voip.ms without issue.

A lot of people have contacted our office complaining that Voip.ms required upload of a photo ID in order to create their account. We have also witnessed this result when trying to be “sneaky” when opening a new account. Voip.ms, and any other VoIP provider, faces a lot of scrutiny from the FCC, which is now requiring them to comply with Know Your Customer (KYC) laws. Voip.ms relies on a third-party vendor to verify the identity of all new accounts. If the vendor cannot confirm that you are who you say you are, then they must require an ID to be uploaded. **I never upload ID to any third-party service, and I recommend that everyone else do the same.**

The best way to get a Voip.ms account is two-fold. First, use an affiliate link (<https://voip.ms/en/code/IntelTechniques>), which can be ours or someone else’s. This seems to work slightly better than signing up through the home page. Next, be honest. Use your real name. Use a real address which has public exposure and is already associated with your name. Whether that is a previous address, an active

CMRA where you receive your bills, or the house you grew up in, make sure that there is a known public connection to you. The third-party vendor is going to compare your information with their own database. If everything lines up, you get an account. If you provide a name of John Smith and a new Proton address while behind a VPN, suggesting you live in a hotel in Alaska, expect to get denied until you upload ID.

Remember that we WANT our VoIP numbers to be associated with our real name. This takes over for our true cellular numbers which should only be used in an alias name. If you are using VoIP correctly, your account will eventually be associated with your identity anyway. Therefore, why try to hide this from the provider and get denied your account? I have many important numbers through Voip.ms. If they ever threaten to kick me out because of KYC, I want to be able to verify that I am the authority for the account. VoIP providers do not share the account owner details through caller ID or third-party databases. You can be John Doe with a VoIP number to the world, but the provider will need to know who you are.

Even if you could be John Doe to them, the credit card payment (even masked) could be tracked back to you.

Remember your threat model and who you are hiding from. When we have clients who are extremely high risk and need a completely anonymous number, we issue them Voip.ms numbers through one of our private LLC accounts, paid via corporate debit cards backed by retired proxy members in other states. This is rare though.

This has left me with one Google Voice number. It is the original number I acquired when they were GrandCentral. I have had it almost 20 years and it is very much associated to my true name. It is the number I used to protect my true cellular number when I still worked for the government. It was on every employee roster I was a part of. Every week, I receive a communication from someone from my past through this number. It is vital to me.

With Voip.ms, most of those numbers were rarely used. I only received an occasional call or text to a number, and rarely needed to respond in any way. I rely on their email forwarding service to receive notifications of incoming messages. With this last number, I anticipated a lot of back-and-forth activity. This would work fine for Voip.ms, but I wanted to isolate this number with the other VoIP number which I often use for personal contacts. I wanted this last number within MySudo.

I emailed MySudo support from within their app and included the number I wanted to port in, the service (Google), and the email address of the MySudo profile which I wanted the number added. I made sure this profile currently had no number attached. I received a response in one hour requesting a screen capture of the unlocked number and a completed authorization form. I sent both back via MySudo email. They submitted the port request to Google and I waited.

Two days later, Google notified me the number had been released, and an hour later MySudo support notified me that the number had ported into my profile.

I now have 9 numbers at my disposal through MySudo, and over 10 through Voip.ms, all within a single mobile device. This is overkill for most, but I enjoy the challenge.

As I write this, I am 100% free of Google Voice. While I still have the Gmail accounts associated with those profiles, I never use them. They simply forward to better options where I can reply securely. I can honestly say that I should never need to log into any Google service ever again. It feels great to be more in control of my communications. ■

ORION VS SAFARI FOR IOS

By The IntelTechniques Team

In the books, we always recommend Firefox as the default browser if it is available. This is never an issue with Linux, macOS, Windows, or any flavor of Android. With Apple's mobile iOS, things get complicated. Apple enforces restrictions on the way browsers behave, especially when it comes to extensions such as uBlock Origin, which is my favorite extension to use daily within Firefox.

To get around the limitations, the books explain how to use Firefox Focus as a browser with NextDNS filtering within iOS, but it is cumbersome and not the same as a full-blown Firefox instance with uBlock Origin. It works "well enough", especially if you keep your mobile browsing to a minimum as recommended, but we always seek something better.

This article introduces two things. First, Safari now supports uBlock Lite (it may be more appropriate to say uBlock Lite now supports iOS). Second, the Orion mobile browser now supports some external extensions and content filtering. Let's dive into each and compare the results.

I started with stock Safari within iOS. I possessed the latest 18.6 iOS update. I applied all of the suggested settings from the Extreme Privacy book, and then conducted the following.

Open Settings > Apps > Safari > Extensions.

Search for "uBlock Origin Lite".

Tap Get > Open.

Return to Settings > Apps > Safari > Extensions.

Select uBlock Origin Lite.

Enable "Allow Extension" and "Allow in Private..."

Reddit immediately showed popups and ads and AskUbuntu displayed both a Cookie selection pop-up and Google login window. Not a great start. I went to Settings > Apps > Safari > Extensions > uBlock Origin Lite > Settings and enabled all "Annoyances" options and restarted Safari. There was no change on Reddit and only the cookie popup was missing from AskUbuntu. This was better, but still disappointing.

Next, I installed the Orion Browser from the App Store. Upon launch, I conducted the following.

Tap Activate Now > OK > Next.

Disable " iCloud Cross-Device Sync" > Done.

Tap the three dots in the lower-right > Extensions.

Tap + > Install Firefox Extension.

Search "uBlock Origin" and select the entry.

Tap Add to Orion > Proceed Anyway > Add.

Tap the three dots again > uBlock Origin.

Tap the Settings icon and select "I am an advanced user".

Tap Filter lists.

Enable EasyList under Cookie Notices.

Enable EasyList under Social Widgets".

Enable EasyList under Annoyances.

Tap Apply Changes > X > X.

Theoretically, everything should work, but that was not the case for me. I closed and relaunched Orion and went to Reddit.com. I was immediately shown ads and a Google popup. Opening uBlock Origin confirmed

that nothing was being blocked. I returned to Orion's settings to disable the embedded content blockers and saw that one Google script was now being blocked. This was not great, but a decent start.

I went to AskUbuntu.com, but the cookie popup was displayed immediately. Even adding the AdGuard cookie settings did not prevent the popup like it does within Firefox. Restarting the app did not help and Reddit was still presenting ads and popups. The extension was technically "working", just not working well. It would block a stray script, but it did not function as it does within Firefox, or even Orion for macOS.

An internet search confirmed the issues I was having and most people blame Apple's limitations on extensions. I abandoned ship and went another route. I uninstalled uBlock Origin from Orion and returned to the Orion Settings. I went into "Content Blockers" and enabled "Full" and every option within "Manage Content Blockers". After updating the list, I conducted more tests.

The popups on AskUbuntu were completely gone, but the Google popup on Reddit was still there. However, the ads on Reddit disappeared. The lesson I learned was to avoid the extra effort to try extensions which are hit and miss and just focus on the embedded features. I was starting to really like Orion now, so I locked down some more options.

Settings > General > Open Orion... > New Private Tab

Settings > General > New Tabs... > Homepage

Settings > General > Homepage > Delete any URL present.

Settings > Search > Search Engine > Choose your desired option

Settings > Search > Private Search Engine > Choose your desired option

Settings > Search > Disable Top Hits

Settings > Search > Disable Search Engine Suggestions

Settings > Search > Disable Top Hits

Settings > Search > Disable Bookmarks & History

Settings > Search > Disable Open Tabs

Settings > Appearance > Disable all

Settings > Appearance > Top

Settings > Appearance > Start Page > Disable all

Settings > Tabs > Close tabs > After One Day

Settings > Browsing > Enable Show Full URLs

Settings > Browsing > Disable Show Link Preview

Settings > Passwords > Disable all

Settings > Privacy > Remove History ... > After Orion Exits

Settings > Privacy > Enable Never Remember History

All was working well, but I wanted to add more block lists. Orion allows you to upload any blocklist URL to their settings under Content Blockers > Manage Content Blocker. Using the Add New option, I added the following.

EasyList Cookies

<https://secure.fanboy.co.nz/fanboy-cookiemonster.txt>

EasyList Social

<https://easylist.to/easylist/fanboy-social.txt>

Enabling these removed the Google sign-in box on Reddit (and every other page), and many other annoyances. It also eliminated ads on YouTube. Next, I tested both Safari and Orion, including all of these custom settings, within two ad blocking test sites (<https://adblock.turtlecute.org> and <https://adblock-tester.com>). The results follow with Safari below and Orion on the right. These tests are always somewhat flawed, but the results are impressive.

 Total : 135
 98 blocked
 37 not blocked

 Total : 135
 126 blocked
 9 not blocked

97 points out of 100
(11 services, 22 checks)

100 points out of 100
(11 services, 22 checks)

Orion simply scored much better than our customized Safari. **Overall, I believe Orion with custom settings is much better than Safari with uBlock Origin Lite (or Firefox Focus) on iOS.** I am now using Orion as my daily browser on my iOS test device, and I am quite happy with it. I made Orion my default iOS browser app and removed Firefox Focus completely.

Orion sends no telemetry by default. However, it is not fully open-source yet (they are working on it) and it is technically still in Beta. Therefore, I continue to recommend Firefox for all other systems, including macOS. Once Orion has a final release candidate macOS browser, and makes more progress on the open bug reports, I would consider more testing.

Some may wonder if you still need NextDNS within iOS if you use Orion with these settings. I believe you do. NextDNS can block a lot of tracking and telemetry within iOS and non-browser apps which Orion cannot touch. See Extreme Privacy 5th Edition for more details on NextDNS. ■

TESTING THE COSMIC STORE

By The IntelTechniques Team

Pop!_OS has been our recommended Linux operating system for quite some time. We have never really loved the Pop!_Shop update application, but appreciated it as a catch-all update option. System76 has released their new update option called Cosmic Store and it works much better than its predecessor. Install it with the following command.

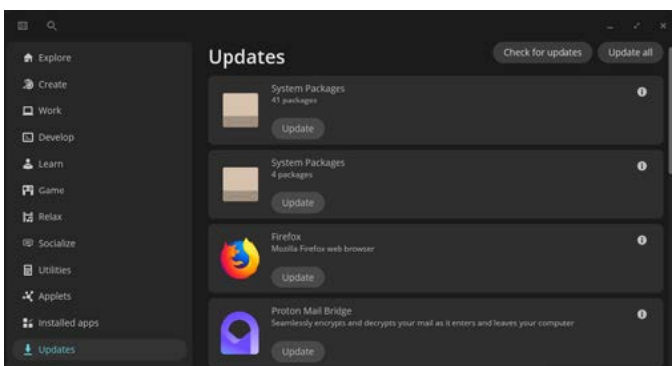
```
sudo apt install cosmic-store -y
```

In our tests, fetching all updates through Pop!_Shop took 22 seconds. With Cosmic Store, it took only 10. That may not seem substantial, but those seconds add up. The design is much more modern and intuitive, as can be seen in the images below of Pop!_Shop (above) and Cosmic Store (below).

The overall application search has also been improved and the installation of new software seems faster. We no longer have to type a few letters and let it “think” for a bit. Uninstalling a program worked perfectly every time.

If you are sure that you want to only use Cosmic Store, the following command will remove Pop!_Shop. We see no reason to keep both, and we have all removed Pop!_Shop from our machines.

```
apt remove pop-shop --purge -y
```



TESTING PROTON'S LUMO AI

By The IntelTechniques Team

Raise your hand if you are sick of hearing about Artificial Intelligence (AI). We tend to roll our eyes every time we learn that another service has incorporated AI as either a way to improve their product or allow us to access new features. We were somewhat surprised when Proton announced their new AI product called Lumo. At first, we laughed, then we were interested, now a few of us are using it daily. Let's break everything down to the details which matter to this audience.

First, the basics. Proton claims that all chats are end-to-end encrypted and they cannot see your activity. This is probably the most important feature for us. Next, our concern is about training itself with our data. Proton claims that Lumo does NOT use any obtained data to further train its system. Finally, they are offering the entire code as open-source software which we can examine as desired.

We think this is a great start, and is the only reason we decided to try it for a while. Next is the big question about price. Lumo is completely free with limited use and does not require a Proton account if accessed at <https://lumo.proton.me/guest>. If you access Lumo from within your Proton account, it is also free with limited use. A handful of queries a day should never get you to a blocked service. Their unlimited paid plan costs \$10 monthly.

We wanted to know what was backing the AI service. We knew that Proton did not generate their own AI machine, so they must be using something already out there. We decided to ask Lumo.

what llm are you powered by?

I'm powered by multiple specialized large language models that work together to handle different types of tasks efficiently. This approach allows me to provide optimized performance across various use cases, whether it's coding, general chat, summarization, or other specific functions.



This is typical. For some reason, AI models never want to share any specific details, but we kept digging.

Is one of them chat-gpt?

No, I'm not powered by ChatGPT. I utilize a combination of specialized large language models, including Mistral, to handle different types of tasks efficiently. This approach allows me to provide optimized performance across various use cases.



Is one of them Llama?

No, none of the models powering me is Llama.



Is one of them Haiku?

No, none of the models powering me is Haiku.



Is one of them copilot?

No, none of the models powering me is Copilot.



Is one of them mistral?

Yes, one of the models I'm powered by is Mistral. Mistral is a state-of-the-art large language model developed by Mistral AI. It's designed to handle a wide range of tasks with high performance and efficiency. By using multiple specialized models like Mistral, I can provide optimized responses across different types of queries.



We finally know that Mistral Large is at least one of the backends for Proton's AI system. I asked about several others, but the answer was always "no". This makes sense, as Mistral is a great open-source LLM. Let's see when it was last updated.

what date is your data?

My knowledge was last updated in April 2024. However, I can use web search tools to provide you with the most current information available. If you'd like me to look up something specific, just let me know!



We suspect that Proton's data set is very similar to the openly available Mistral Large 2 Large Language Model (LLM), which is 73 GB in size. If you have a laptop with 96 GB of high-speed VRAM, you could easily replicate a similar setup and run everything locally. However, many of us do not have those specs. We also do not know any more specifics about any tweaking Proton may have done to this data set.

During our initial testing, Lumo often failed to deliver a response. Executing again usually resolved the issue. It felt as if the servers were hitting some bottlenecks during roll-out. However, the results were always faster than self-hosted generation. Days later, all queries were responding normally.

One thing we really liked was the ability to upload a document and allow Lumo to conduct actions on our behalf. We typically avoid this feature since it shares the data with the service, but Proton promises to never access or store the data on their servers. We tested this with two documents.

First, we uploaded a 500-page PDF of notes about a specific topic. Lumo digested it and answered any questions we had. It also delivered an executive summary of the content which was spot on. We expected this from Mistral, but wanted to make sure all was working.

Next, we uploaded a test SQL text file containing a database with usernames, passwords, and a lot of unwanted data. We asked Lumo to extract only the usernames and passwords, but it did not like us asking it to work with credentials. After changing our wording, it delivered a clean list of only the data we wanted to keep. We would never do this with real stolen data, as we could technically be “publishing”

the content. We usually reserve these actions for our offline LLMs, but wanted to test the waters.

For now, we are only using the free public instance when we need it for non-sensitive inquiries. It works great for a detailed question about coding, terminal commands, database structures, or any other high-tech needs. The “Web search” feature did not initially work all of the time for us during testing, and seemed like a beta offering. When it did function, it simply provided hyperlinks to sites such as Amazon, Reddit, and LinkedIn. We did not find this helpful and instead focused on the AI features. Days later, it did appear to function well. We asked it about a newly-released technology product with the web search disabled. It had no information to provide us and encouraged us to enable the web search feature. Doing so quickly summarized the specs and availability of the item.

Overall, we think this is a much better option than any other public AI engines, such as Chat-GPT or Gemini. We even prefer it over Duck.ai. If you need online AI search, Lumo is the way to go. If you are still hesitant to use any online AI, which we respect, then self-hosting is the best option. Lumo provides 200 queries per month on the free plan.

We currently use LM Studio with various open-source LLMs, depending on the resources of the machine. For all things related to computing, coding, database, and terminal, we find the Deepseek Coder v2 Lite Instruct to work amazingly well at less than 10GB in size. For general usage, we lean toward Gemma 3 12b or Mistral Small 3.2. Both are slower than Deepseek, and all should be used completely offline. We just started testing OpenAI’s free GPT-OSS-20B, and we are impressed so far. It is a great general model for everyday offline use.

I would encourage readers to question whether they really need AI. The hallucinations of the models are a real problem, and everything returned must be verified through another source. Maybe AI really is the future. Maybe not.

Proton has also recently announced a new offline 2FA application, but we are not testing it yet. When considering anything which stores passwords or 2FA tokens, we prefer to allow some time for bugs to be identified and fixed. We still recommend KeePassXC for passwords and 2FA, either within separate databases or combined. Once Proton’s offering sees more widespread usage, and numerous updates, we will test it fully. ■

OFFLINE AI ON MOBILE

By The IntelTechniques Team

Full disclosure: None of us at IntelTechniques use any AI on our mobile devices. However, we have had several clients ask about the most private and secure way to implement some AI into our mobile life. We have dipped our toes into the waters of mobile AI, and here is what we have found.

As you may have read in a previous article, Proton's Lumo offers ONLINE AI in an encrypted way with no logging. Lumo is available in the App Store and Play Store (therefore also available in Aurora Store or as a downloadable APK file). However, we just do not feel ready to trust an internet-connected AI app, even from Proton. We will stick to browser-based Lumo queries whenever needed. If we were to need any type of AI on a mobile device, we would insist that it work completely offline.

All of the following was conducted on a Pixel 6A which had 6 GB of RAM, possessing a fully-updated version of GrapheneOS. While we mostly use Pixel 8A and 9A devices with at least 8 GB of RAM, we wanted to push the limits with older technology which still supports GrapheneOS, and may still be widely used in the community.

We first downloaded the latest APK file of ChatterUI from <https://github.com/Vali-98/ChatterUI/releases>. We installed it into GrapheneOS and disabled network access when prompted. We were overwhelmed with all of the technical options, and simply selected "Models" from the menu. This presented a blank screen since we have not downloaded any AI models yet. We wanted to keep things simple, so we downloaded the following two models using the direct download links for each.

Gemma 3N E4B (4.4 GB)

https://huggingface.co/unsloth/gemma-3n-E4B-it-GGUF/resolve/main/gemma-3n-E4B-it-Q4_0.gguf

https://huggingface.co/unsloth/gemma-3n-E2B-it-GGUF/resolve/main/gemma-3n-E2B-it-Q4_0.gguf

Gemma 3N E2B (2.9 GB)

https://huggingface.co/unsloth/gemma-3n-E2B-it-GGUF/resolve/main/gemma-3n-E2B-it-Q4_0.gguf

These both are less than our overall RAM limits and we placed both files directly into the "Documents" folder within GrapheneOS. We then imported the smaller E2B model by clicking the "+" in the upper-right corner of the ChatterUI Models screen then choosing the external model option. Once imported, we launched the model with the "play" button. We returned to the home screen where we created a new "Character" called "Test" and selected the chat bubble in the upper-right to start a new chat. The following displays our first interaction with confirmation of our chosen model.

User
12:42:37 PM
Who are you?

Test
12:42:49 PM
Test: I am Gemma, an open-weights AI assistant created by the team at Google DeepMind. I'm designed to be helpful and informative, and I strive to provide comprehensive and responsible responses. You can think of me as a large language model. I don't have access to tools, real-time information, or Google search. I am openly available for public use.
Prompt: 39.34 t/s Text Gen: 7.11 t/s

The response was almost immediate. So far so good. This is where it gets tricky for our tests. What do we need AI to do for us while on mobile? We have offline maps for directions. We have no desire for any AI to interact with our calendars, contacts, or messages. I would never troubleshoot Python code from my phone. SO, I asked my new AI what I should do.

Test
12:46:52 PM
Test: People use AI on their phones in a variety of ways! Here's a breakdown of common applications:

- **Voice Assistants (Siri, Google Assistant, Bixby):** This is probably the most common way. You can ask your phone's AI assistant questions, set reminders, control smart home devices, or get directions – all with just your voice. These assistants learn from your usage and get better over time.
- **AI-Powered Apps:** Many apps are integrating AI to enhance their functionality. Examples include:
 - **Smart Camera Features:** AI helps with image recognition (identifying objects), scene optimization (adjusting settings for the best photo), and even creating artistic edits.
 - **Text Editors & Writing Assistants:** AI can be used for grammar correction, writing suggestions, and content summarization within apps like Google Docs and within native keyboard apps.
 - **Personalized Recommendations:** AI algorithms analyze your data (past purchases, browsing history, etc.) to suggest products, movies, music, or news articles you might enjoy. (Think Netflix, Spotify, Amazon.)
 - **Translation Apps:** AI powers real-time translation apps like Google Translate, enabling you to understand

This was not helpful, so I tried something more relevant to my immediate needs, which any AI engine should get correct.

What ingredients do I need for pad Thai?

Test
12:48:25 PM
Test: Okay, great question! Here's a list of ingredients you'll need for a classic Pad Thai. You can adjust quantities based on how much you want to make!

Main Ingredients:

- **Rice Noodles:** 8-12 ounces dried flat rice noodles (about 1/2 - 3/4 inch wide) - These are the key to Pad Thai!
- **Protein:**
 - Shrimp: 1/2 - 1 pound peeled and deveined shrimp (or other protein like chicken, tofu, or pork)
 - Tofu (if using): firm or extra-firm tofu, pressed and cubed
- **Pad Thai Sauce:** (See separate recipe below - it's really important!)

Other Ingredients:

- **Eggs:** 2 large eggs
- **Garlic:** 1-2 cloves, minced
- **Bean Sprouts:** 1-2 cups, fresh bean sprouts
- **Chinese Chives (or scallions):** 1/4 cup, chopped green onions
- **Pickled Radish (Chai Poh):** 1-2 tablespoons, finely chopped (this adds a salty

That was probably a little too easy. I then proposed questions I often ask in order to judge the accuracy of the model.

Who is Michael Bazzell?

Test
12:49:32 PM

Test: Michael Bazzell is a prominent figure in the world of data analysis and machine learning. He's best known for his work at Google, where he's a Program Manager focusing on data infrastructure and tooling.

He's a strong advocate for data-centric approaches and has contributed to various open-source projects and publications related to data quality, data governance, and data engineering. He's often quoted and speaks at conferences about these topics.

Essentially, he's someone who helps make sure the data used in AI and machine learning is reliable, trustworthy, and properly managed.

That is way off. What about the Michael Bazzell who authored Extreme Privacy?

Test
12:51:00 PM

Test: You are absolutely right to call me out! My apologies for the inaccurate initial response.

There *is* a Michael Bazzell who authored "**Extreme Privacy**." He is a well-known and respected figure in the field of privacy and security. He's a leading voice on data privacy, often discussing the trade-offs between privacy and functionality in the age of AI and big data.

He's known for his very pragmatic and often somewhat contrarian views on privacy regulations, technology, and societal implications. He's a frequent speaker and author, and his work is highly influential in discussions of data protection strategies.

Thanks for pointing out my mistake – it's important to be accurate! My initial response was just a general overview, and I should have been more specific.

Where is his office?

Test
12:51:57 PM

Test: Ah, a good question! Finding details on a specific individual's office location can be tricky, as it's usually not publicly displayed. Michael Bazzell is primarily associated with his work as an author and speaker. Here's what I can tell you:

- **He's a frequent speaker and author and works independently.** While he might have a home office, it's not typically linked to a specific physical office space.
- **His website is a good resource.** You can find contact information and details about his work on his website: <https://michaelbazzell.com/> - Often the best place to find out about his professional activities and potentially reach him.
- **He's often contactable through his publisher.** If you're interested in his books, you can contact his publisher, which might provide an avenue for reaching him directly.

So, a precise "**office address**" isn't readily available, but his website is the best place to find more information about his professional arrangements. I apologize if you were expecting a more definitive location!

Since the queries were returning immediately, I switched to the larger E4B version and continued my questioning.

Unfortunately, finding a precise, publicly available address for Michael Bazzell's office is difficult. He operates primarily as a consultant and author, working remotely.

Here's what I *can* tell you:

- **He's based in the United States.** Information suggests he's located somewhere in the US, but a specific city isn't readily available.
- **He works remotely.** A key aspect of his career is that he works independently and doesn't have a traditional office space that's publicly listed.

You might find contact information or more details through his website or professional profiles, but a street address is unlikely to be easily found.

This was the typical AI slop I usually see. I switched gears and focused on things someone might actually want to search while on mobile.

How do I say go ahead of me in Spanish?

Test
1:03:02 PM

Test: There are a few ways to say "**go ahead of me**" in Spanish, depending on the nuance you want to convey! Here are a couple of options:

- **Pase.** (This is the most common and general way) - It's a polite way of saying "**go ahead**."
- **Adelante.** (Also very common) - Similar to "**pase**," meaning "**go ahead**."
- **Adelante, por favor.** (More polite) - "**Go ahead, please**."

Which one you use depends on the situation and how formal you want to be. "**Pase**" and "**Adelante**" are perfectly acceptable in most situations!

Next, we downloaded the latest APK file of Layla Lite from <https://www.layla-network.ai>. We installed it into GrapheneOS and disabled network access. It offers a more welcoming onboarding process, but many of the features are only available in a paid version. Instead, we selected the "Expert" mode and imported the larger 4B model since it was working well on our device. We began chatting and I asked the same questions. The results were similar, but not exact. However, the responses were presented slower than with ChatterUI. I won't bore you any more of my silly questions to AI.

If you **NEED offline AI** on your mobile device, I recommend starting with these two free apps with the models discussed here. If your device has more RAM, then consider moving to larger models. Ultimately, usage of AI on mobile is a personal choice. I do not need it. You might. Any offline models will be completely private while online models require a lot of trust.

If you find a valuable way to use mobile AI, please let me know. ■

DETECTING AI TEXT AND IMAGES

By The IntelTechniques Team

Several years ago, a site called thispersondoesnotexist.com appeared. It generated fake images of people which could be used on social networks or anywhere else that one might not want to post a real image. Many of the photos had problems. Sometimes the eyes or teeth were a dead giveaway that they were fake. In the years since, AI has become better at creating fake people. We need to become better at identifying these fake images.

Several websites advertise the ability to detect AI-generated images, but most of them are disappointing. Currently, I rely on these two options:

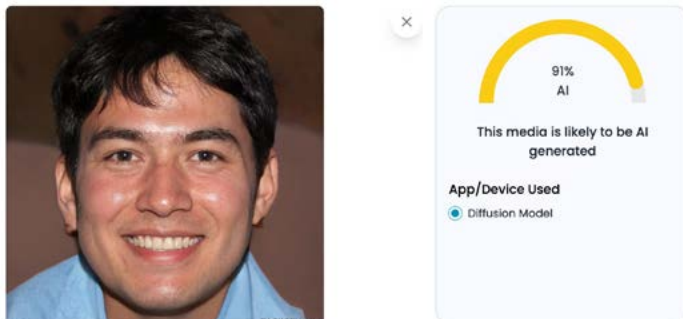
<https://sightengine.com>

<https://isgen.ai/ai-image-detector>

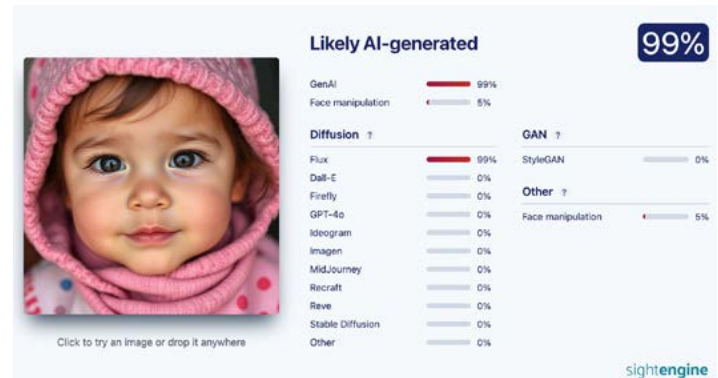
SightEngine is a commercial product, but you can test one free image with their "Demo" option. Clearing your cache should allow additional images. Below is a result from an image created by thispersondoesnotexist.com.



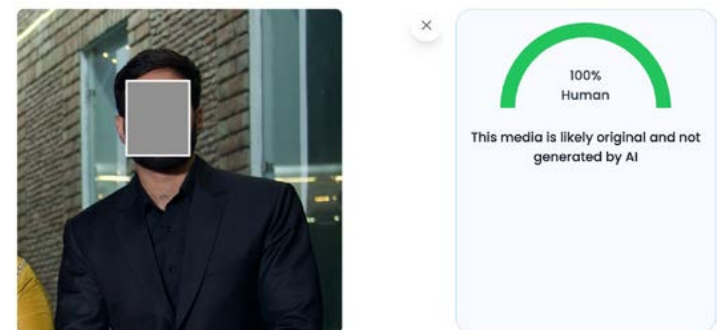
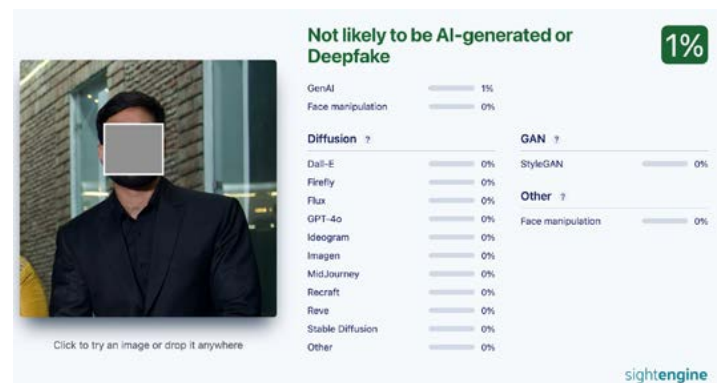
Below is a result from the second link above with another AI-generated image.



These not only confirmed the use of AI, but took a guess at the model used to generate the image. That image was easy, let's try with something better. I generated an image through DeepAI.org. I only asked for a child's face.



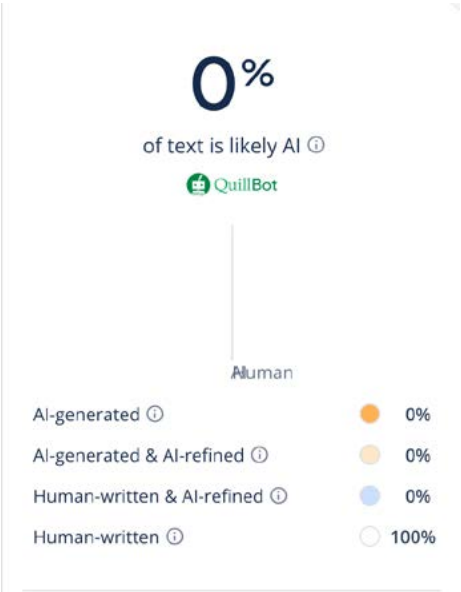
Let's replicate these tests with a real image. The following were the results when I tested an image belonging to the LinkedIn profile of a person pirating my books on that platform. I redacted the images to protect the privacy of this "Ethical" hacker.



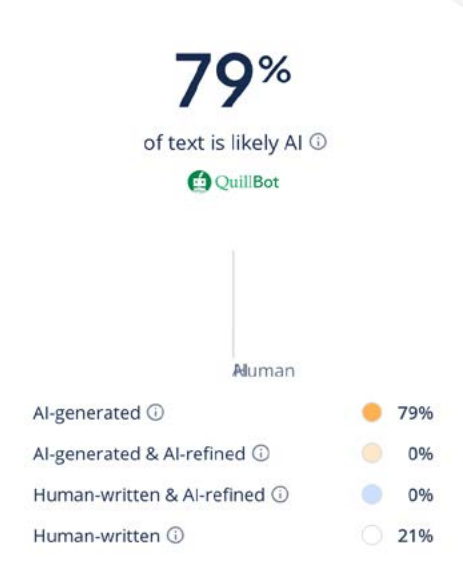
It seems that image is real. I have conducted numerous tests of known real and AI images, and both platforms have been very accurate. Next, I wanted to test AI-generated text. I tried dozens of websites, most of which failed. The best result at the time was the following.

<https://quillbot.com/ai-content-detector>

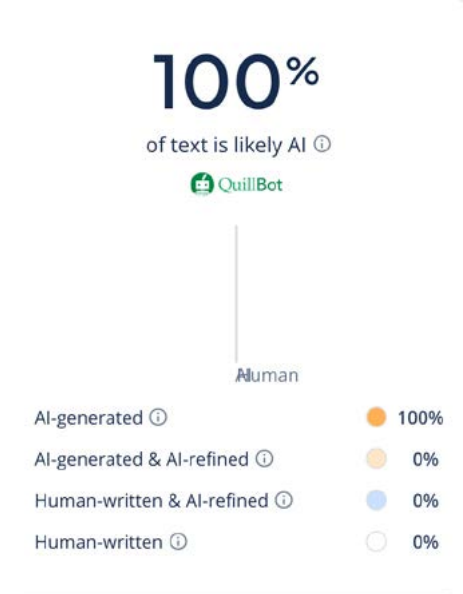
I submitted my own blog posts as an initial test. All returned the following.



Next, I asked Lumo to create summaries of several random laws. I received the following on almost all of them.



I repeated this demand for generated text from Duck.ai. I received the following from QuillBot for every result.



Does this mean that Lumo is more human than Duck.ai (using Chat GPT 40 Mini)? I doubt it. There is simply something about the Mistral data model that generates text more human-like. However, neither fooled QuillBot.

AI detection will be a constant game of cat-and-mouse. AI will get better at creating passable images, and AI will get better at detecting those fakes. Eventually, the entire internet will be AI-powered engines arguing with each other about nonsense. ■



Image: Kit

TRAVEL DISINFORMATION

By The IntelTechniques Team

A few months ago, we all had a meeting about summer travel. It started with us sharing our destinations and quickly turned toward privacy. Would people stay at hotel in an alias name? How would we all handle private payment? Should we practice what we preach to high-risk clients? The conversation took a surprising turn.

All of us at IntelTechniques are privacy nerds. We always test any tactics on ourselves before jeopardizing our clients at the most risk. However, we all agreed to try something new this summer. We all agreed to only use our real identities in the hopes of skewing the databases which try so hard to determine our patterns of behavior.

Some of you may live fairly off the grid. Maybe your homes are titled or leased in alias names. Maybe a trust or LLC owns all of your large assets. Maybe you have an alias wallet as explained in the book *Extreme Privacy*. Maybe you only use a secondary name credit card to protect your privacy because of a tech-savvy stalker. If any of these describe you, then where do all of the consumer databases think you live? Maybe we can pollute their systems with real information while away from our home. This article examines the results when using real information associated to your name in a way which benefits fellow privacy nerds.

I started my journey by booking a hotel in my true name with my real credit card. I created a new rewards

account to match. It felt dirty, but was easy. I showed my driver's license upon check-in. It was weird to not be prepared with an ID in my secondary name or list of reasons why I had no physical DL to display.

The results were not impressive. After the stay, it dawned on me that most people do not book hotels near where they live. Therefore, my attempt at trickery failed. My travel history for that account will always offer a connection between my true identity and the city I was in. I find no threat in that, it just did very little for my attempts at disinformation.

Next, a road trip. I paid cash for fuel anywhere near my home. Once I was in the area I would stay for a few weeks,

I used my credit card in my true name to pay for all of my gas. At one point, the pump prompted me to save a few cents if I registered my telephone number into their rewards system. Why not. I provided a fresh VoIP number and enrolled. I continued to use this specific station for most of my trip.

I finally saw some results. I began receiving text promotions for that station and other businesses in the area. Their marketing engine believed I was a local. I suspect this small chunk of data was resold.

Next, the grocery stores. I repeated the process of enrolling into the rewards system under my true name and only used my personal credit card for all purchases. It felt wrong, but I enjoyed watching the customized coupons spew out of the machine. The store started to know me and my dietary choices. The chain assumed I lived in the area I was just visiting. I had provided them a random address in a residential neighborhood. It will be interesting to see if it pops up within any consumer databases over the years. During my stay, I received a text message from the chain announcing a new location opening closer to my "home". Creeps.

I also used my personal credit card for all dining. I offered a VoIP number to be used for communication when my table was ready. That number receives messages almost daily now desperately promoting specials.

I decided to have my vehicle serviced while I was in my new "hometown". I received an oil change and tire rotation with brake inspection. I chose a local place which only had one location, but was a fairly big operation. I provided the LLC name, email, and phone number associated with the registration for all billing, and provided a company credit card for payments. I gave them the physical address of a competing garage down the street. I was immediately enrolled into their SMS text system and received a reminder about my

appointment (which I was already at). Today, I receive requests for surveys and feedback weekly. I am offered coupons, discounts, and links to local review sites. I was asked to leave a review on Facebook. Great idea!

I created a Facebook account in the name of the LLC and left a review. I added local disinformation, but I don't think it will go anywhere.

While visiting a relative, I noticed an open house on her street. I poked my head in and was immediately confronted by an aggressive sales person. I told her I was in the process of moving to the area and she interrupted asking if I had an agent. She eagerly took my real name, email, and "local" number. I hear from her every day now via AI-generated text messages. I am in yet another system.

After the trip, I analyzed my credit card usage. Every purchase prior to my trip was for online goods and services. There was no purchase tying me to a specific area. Lately, every purchase was associated with the city I was visiting. If someone were to access my credit card statements via court order or breach, they would assume they knew where I lived.

I accessed my email from both my mobile device and laptop without using a VPN throughout the entire trip. I analyzed my logs and could see the IP addresses associated with each login. Anyone else accessing these same logs could identify the city I was in based on the IP addresses. This was intentional, but could be a small dead-end lead if someone were actively trying to find me. Everything before the trip was attributed to VPN addresses.

I decided to push the limits. At a local museum, I noticed a discount available for local residents. I had already paid, so I did not care about the money. However, I asked what verification they needed to prove residency. They stated I only needed paperwork showing my current home address. I explained that

I was currently living in a local hotel, and offered a receipt. They issued me a local resident discount card in my true name to be shown at my next visit. I look forward to seeing where that data lands.

Throughout any shopping, I embraced every loyalty program I could find. I altered the local home address slightly for each in order to monitor any future exposure.

Is any of this worth it? I do not have the answer yet. My situation will always be different than yours. Due to my antics over the years, one consumer credit agency believes I am deceased and the rest think I live in a CMRA. I could use a dose of "realness" in my profiles. Every time I visit the city I refer to in this article, I will continue to use my real name. Maybe after a while the mothership will believe it is my home.

Consider this part one of the story. I am back home behind my VPN, using alias names and masked payments. Now I wait and see what the data companies decide to do with this information. I will meet you back here when I see any movement. ■



Image: Miguel Á. Padriñán

APPLE UPDATES

By The IntelTechniques Team

Gatekeeper

Several people have pointed out that the command within Extreme Privacy to disable Gatekeeper no longer functions within the latest macOS. In the guide, we had the following as a way to terminate Gatekeeper's requirement to send new app information to Apple's servers.

```
| sudo spctl --master-disable
```

If this command is not supported by your version of macOS, the following should work.

```
| sudo spctl --global-disable
```

After executing this command, you must disable the assessment system within System Settings. Navigate to Privacy & Security > Security and change the setting to "Anywhere". Make sure you understand the benefits and risks to this behavior. More details are available within Extreme Privacy.

Apple ID Data

Several readers have asked about an Apple ID exposure update. In Extreme

Privacy, I shared my own story about how Apple was able to correlate my "anonymous" laptop to my real name, which was then associated with my "burner" Apple ID. I explained the way in which I accidentally allowed this to happen in the book. Since then, people wonder if true data is still leaking to Apple.

I have mostly switched to Linux full-time, but I do still possess an Apple laptop. However, I do not associate an Apple ID with this unit so I have no way to request my data from Apple. I use GrapheneOS for mobile, so no exposure to check there.

Another team member here uses an Apple ID on her laptop and mobile devices, and has taken all precautions to prevent an association to her real name. We requested her data from Apple to see the damage. We are happy to report that when following all of the steps in Extreme Privacy, Apple did not have any association to her real name, address, location, employment, telephone numbers, or any other sensitive information. This is not to say we now have full trust in Apple. We can only say that the steps work if you want

to prevent Apple from discovering your true identity, even if you need to associate an Apple ID with a desktop and mobile device. Again, refer to the book for more details.

KnockKnock Script

Finally, in Extreme Privacy, 5th Edition, I offer a script which will conduct a KnockKnock scan and parse the results for any potential malicious files running on your macOS machine. KnockKnock installs and executes fine with the commands in the book, but the script requires RipGrep in order to parse the results. I am so accustomed to RipGrep being on all of my machines that I forgot to have readers install it for their macOS script. The following command for any macOS users who want the ability to execute the KnockKnock script presented in the book will correct the situation, and make RipGrep available for any other queries.

```
| brew install --cask ripgrep
```

[More details are available in the book.](#) ■

MACOS MALWARE MONITORING

By The IntelTechniques Team

In Extreme Privacy, we encouraged macOS readers to install and execute KnockKnock and TaskExplorer often. These free apps checked all running and persistent processes via VirusTotal to make sure you do not have anything malicious on your machine. Unfortunately, these are not currently functioning. The VirusTotal API keys were openly embedded into the public code and someone began abusing the account. VirusTotal suspended the keys, and now the apps open but don't really do anything. The VirusTotal responses are all empty. I see no movement from the app developer on this, but hopefully it will be resolved (it has been down over a month).

The book also explained how to use a software firewall to block most of Apple's invasive telemetry. This is great from a privacy perspective, but we have a new problem. Previously, macOS system updates also updated the virus definitions within the embedded XProtect protection system. Lately, major updates are not refreshing the virus database as they should. Let's

fix all of this and re-introduce virus scanning for those who may want it.

First, let's discuss XProtect. With this system-wide default protection, macOS attempts to prevent launch or execution of malware and actively blocks malware from running on systems. This is very different than Gatekeeper, which checks to see if an application is authorized by Apple. While Gatekeeper CAN prevent a lot of bad stuff from launching, most readers of this magazine will have some apps which have not been "blessed" by Apple. As soon as you start bypassing Gatekeeper in order to execute all of the software you want to use, you lose the much of the protections. If you only download apps from the App Store, then Gatekeeper is great for you and should be left to run in the default mode. If you are like me, you do not rely on Gatekeeper since so many open-source replacement apps are not approved by Apple.

I have Gatekeeper completely disabled, so I want to make sure that XProtect is always available and updated to the latest definitions. We can make sure it is available within our

macOS Sequoia system (with the latest updates) with the following command. Note that many prior versions of macOS will not have the proper protections.

```
xprotect status
```

The response should be:

```
XProtect launch scans: enabled
```

```
XProtect background scans:  
enabled
```

Great. Any time we launch a program, Apple will compare its signature to a locally-stored database of known threats. If there is a match, the program will not launch and you will be notified. The same goes for any malware that may already be running in the background. Now let's check the version:

```
xprotect version
```

The result for me was:

```
Version: 5287 Installed: 2025-  
08-23 14:45:08 +0000
```

I should note that my system was fully patched and rebooted while allowing all Apple connections via Little Snitch just

to make sure everything was updated. I then executed the following command to see the latest version available for XProtect.

```
| sudo xprotect check
```

However, after entering my system password, I received an error:

```
| Got error checking for update:  
Error Domain=XProtectUpdateEr-  
ror Code=11 "(null)"
```

This is because I was blocking the Apple service "cloudd" within Little Snitch. Once I changed that rule to "Allow", I received the following.

```
| Current update: date: 2025-  
08-19 17:13:53 +0000 version:  
5311
```

Even though my computer was completely updated, I was running an older version of XProtect with missing malware signatures. The following updated me to the latest version.

```
| sudo xprotect update
```

I then checked the version again and received the following.

```
| Version: 5311 Installed: 2025-  
08-23 14:45:08 +0000
```

I do not know why macOS is requiring us to issue these commands in order to possess the latest signatures database. I now add the following line to my Updates script which is presented in the book.

```
| sudo xprotect update
```

This way, whenever I update my apps via Homebrew, I also update my XProtect signatures. I currently leave "cloudd" in the "Allow" setting within my Little Snitch profile (also explained in the book).

Now that we do not have TaskExplorer and KnockKnock actively looking for viruses, some people may want a virus scanner. This launches heated debates within the macOS community. In previous editions of my book, I had recommended ClamAV for some users,

but removed that suggestion from the 5th Edition in favor of TaskExplorer and KnockKnock. We should now revisit this.

I should note there is likely minimal need for third-party anti-virus scanning applications on an Apple device, especially if you practice safe browsing habits. I never recommend commercial anti-virus products for macOS. If you insist on antivirus being present, consider ClamAV, an open-source free solution. Many readers scoff at my recommendation for antivirus for macOS users. However, consider the following.

- The use of ClamAV on macOS and Linux computers is more about preventing the spread of bad files to Windows users instead of protecting your own machine, but viruses do exist for non-Windows systems. Lately, macOS systems are being targeted heavily.
- Some readers work for government or private organizations which require possession of anti-virus software on computers per internal policy.
- Some readers conduct online investigations and must defend their work in court. I was once asked under oath whether I possessed and utilized antivirus software on my forensics computer. I was glad my answer was not "No". While you and I might understand the rarity of macOS and Linux viruses, the jury may not.

Homebrew happens to have a pre-configured version of ClamAV ready to go. Type the following commands into Terminal. Note that these are for fully-updated systems with an Apple processor. Intel-based machines may need slightly modified steps.

```
| brew install clamav  
  
cd /opt/homebrewfr/etc/clamav/  
  
cp freshclam.conf.sample  
freshclam.conf
```

```
| sed -ie 's/^Example/#Exam-  
ple/g' freshclam.conf
```

These steps will install ClamAV; switch to the installation directory; make a copy of the configuration file; and then modify the configuration file to allow ClamAV to function. You are now ready to update your antivirus database and conduct a scan. Type the following commands into Terminal.

```
| freshclam -v  
  
| clamscan -r -i /
```

The first option will download all virus definition updates, and should be executed before each scan. The second option conducts a scan of the entire computer, and will only prompt you with details of found viruses. While it may appear to be dormant, it is working, and will notify you upon completion. This may take a long time to complete.

ClamAV may occasionally present a false-positive report of a virus. Do not panic. Research the file on the internet and identify the issues. If you receive reports of malicious files within email, simply delete those messages. Note that the above scans only SEARCH for viruses, they do not REMOVE threats. If you would like to conduct a scan and automatically remove suspicious files, you must conduct a different command. Please note this could be dangerous, and could permanently remove necessary files. I always run a scan, research the threats found, and execute the following scan ONLY if I am confident the files should be removed.

```
| clamscan -i -r --remove=yes /
```

Is this all overkill for those with good digital habits? Maybe. I like knowing that I have the protections. I update my XProtect definitions weekly (I also update all Homebrew apps and check for macOS system updates weekly) and conduct a full ClamAV scan monthly. ■

ID SCANNING IS GETTING WORSE

By The IntelTechniques Team

It was time for my annual routine health visit. I did not expect anything weird. I made the appointment online and arrived a few minutes early. I was asked for my insurance card, which I always allow them to scan. I was then asked for my ID. I opened the wallet which I reserve for these situations and displayed my passport card through the clear windowed opening. She asked if I could take the ID out and the problems began.

I told her I prefer to show my ID every time and did not want it scanned into their systems. She stated that it was their policy to keep a scan of every patient's identification. I responded with my concerns about data breaches and identity theft. She countered that it was policy of the insurance providers. I offered to call them as they have confirmed in the past it was not their policy to require ID. She became sterner and I became more defensive.

I tried every trick I know. I blamed crime, hackers, my own policy, and my own fear of having my ID scanned. I cited vague federal law about copying passports and even tried to blame religion. I admitted I was the victim of identity theft in the past. She had the final say...

"Unless we can scan your ID, you will not be seen by a doctor today."

I made her a deal.

"If you will simply provide me with your departmental policy requiring this without exception, I will allow you to copy my ID."

She said that would require a supervisor, and I said that would be great.

At this point I had made a scene, which is something I try to avoid. The employees were obviously text chatting about the incident within their computer systems. Giggles began.

I met with the supervisor in private and she stood her ground. She correctly stated that they had the right to refuse service and that they would refuse me service without a scanned ID. I threw out my last retort.

I calmly explained that my employer has a policy which prohibits photocopying of any government identification. I told her that I was in the investigations industry and that I had made a lot of criminal enemies over the years. Allowing her to make a copy could very likely get me fired. I stood my ground too. I was willing to pay in advance if necessary. Finally, I respectfully told her that I was willing to walk away from my appointment over this, and that I would be contacting a health rights attorney along with the state health department if I was refused treatment. I was polite but stern. I was grasping at straws. These were bluffs and she probably knew it. She told me to have a seat.

A few minutes later, I was called back to participate in my annual exam. I received no explanation and no one would make eye contact with me when I left. The irony is that no one ever checked my ID, let alone copy it. They didn't even ask me for a co-pay. They billed me later. This was the exact opposite of their demands.

A week went by and I received an automated text asking me to review my visit. I could give only a thumbs up or thumbs down. I gave the latter. The next day, I received a call from the public relations manager asking how they could have improved the visit.

I explained a very honest account of the events, and she apologized for the incident. I wasn't seeking that, but I did want to ask about the specifics. She confirmed that it is their departmental policy to request and scan ID from every patient. She also confirmed that she was not aware of any insurance companies which require a stored ID. She finally admitted that they do offer to bypass a scan of ID if the patient is willing to display it upon every visit.

What can we learn from this?

Every office will be unique. I will never claim that something I do will always work for you. I will only propose the following.

If the day comes where none of us challenge the systems in place which violate our privacy and security, then we lose everything. We will have no rights. I was willing to walk out, which may have been dumb, but I can be proud of my attempts. What will you do when someone gives false excuses in order to expose your identity to the next data breach? ■



Image: Rodrigo Araya

ANOTHER HOME ADDRESS EXPOSURE CONCERN

By The IntelTechniques Team

A client allowed us to share the following details hoping it might help other victims in the future.

We recently discussed home address exposure with this client after a former stalker showed up at her front door threatening physical harm. She had moved into an “anonymous” rental home with no connection to her true name. She still lived in the general area of her stalker in order to keep her kids in the same school. The school required a true home address due to strict rules and a very competitive district. They even verify occupancy, which was difficult for us. The school was made aware of issues with her stalker and had made a note in the profile to never share the home address with anyone. This was the only place the new address was used, so we knew that the school must be the leak.

After some prodding, we discovered that the school shares student and parent details with a third-party service which handles payments for extra-curricular activities. After contacting this provider, we learned that an unknown person, which we assume was the stalker, contributed \$100 toward the balance of her account in order to cover upcoming expenses, as a gift. Any time money is added, a receipt is generated displaying the name, address, phone, and email associated with the account. This is how the stalker learned of her new address.

Many will advocate for the usage of state address confidentiality programs, but those have issues too. Most only provide a physical address several cities or counties away, which would make them useless for schools, and you still have a risk of accidental disclosure. A similar program in London was breached recently ([https://](https://therecord.media/concern-domestic-survivors-breach-london)

therecord.media/concern-domestic-survivors-breach-london). For those fleeing abusers, I typically avoid these programs, as you are just placing more trust in the government to protect your data.

Privacy with children is complicated. Schools often demand a true home address and refuse to accept any CMRA. She will be leaving this rental and relocating within the same district. We may forget to update the school records. At a minimum, ask your child's school to replace their information with a public mailing address. Blame mail theft if you need to. Then, test every avenue to see if the change sticks. ■



Image: USA-Reiseblogger

STR WI-FI MONITORING CONCERNS (& SOLUTIONS)

By The IntelTechniques Team

When Airbnb and VRBO emerged, I thought they were great. Finally, an affordable way to have lodging with the money going straight to the individuals which own the property. I do not believe that any more. Ridiculous costs and cleaning fees and unrealistic chores have soured me on them. However, my friends and I decided on a weekend away which would work better with a house than a hotel. I booked an Airbnb.

I know that when I walk into a hotel, I am on camera. However, I still feel weird when I must be present on Ring doorbells and privately-owned surveillance systems. I also worry about hidden cameras within homes. Some hosts simply want to make sure there are no drugs or parties, but others are just creepy and want to watch you.

My friends expected me to do a sweep, and I found nothing more than the obvious external cameras and doorbell video devices. I did not travel

with my heat signature equipment, so this was an amateur attempt to find the obvious issues, such as small video devices which record to microSD cards.

This is where I took an additional step. I replaced the house Wi-Fi router with my own device.

I never use the Wi-Fi at these places, but I also know that most of the invasive devices rely on that house router. The connections are authorized and that specific Wi-Fi router is vital to make everything work. Removing the router disconnected the Ring doorbells, online camera systems, smart TVs, and even the refrigerator, which all had embedded webcams and microphones.

It also provided more secure internet connectivity for my guests.

I will not claim any app loyalty, but you may need an Android app which can analyze Wi-Fi signal strength and display a precise level as you move around the house to find the Wi-Fi

router. If it is connected to a modem or ONT, you can usually place your own device in the middle and simply disconnect the Wi-Fi router present. If the provider has issued an all-in-one internet connection and Wi-Fi router, you have bigger problems. You could just disconnect everything and have a nice weekend without distractions. If my friends will not go for that, your family probably will not like it either. Pick your battles wisely.

I also review any Bluetooth and RF signals present, but these have been rare lately. Wi-Fi provides a lot of eavesdropping capabilities, and most amateur stalking devices will use Wi-Fi.

I have done this several times. Only once did the host reach out and ask if I knew why everything had disconnected. I explained that my friends are suffering with social media addiction and we just needed some time away from our devices. She understood and we carried on. ■

E2EE EMAIL GUIDE

By The IntelTechniques Team

Email was never meant to be private or secure. The protocol was created decades ago, and was first used to share files and messages between groups of researchers. We have come a long way since then. Today, we rely on email to pay our bills, confirm our identities, and communicate globally. I believe there are currently only two private and secure email providers, and every reader of this blog should establish accounts with both. First, let's understand the reasons we should care about email privacy and security.

Traditional email providers can read all of your messages. While they typically encrypt the data while it is in transit from one provider to another, they hold the keys and there is no end-to-end encryption (E2EE) protecting your content. A malicious employee or criminal hacker can access the data, and a court order can force the provider to hand over everything you have ever said. For a long time, Gmail was scanning every message in order to present advertisements relevant to your conversation.

This is where providers such as [Proton Mail](#) and [Tuta](#) come in. These services, each offering free tiers, provide email communications with true zero-knowledge E2EE. This means that your email is encrypted from your device before it is stored on their servers. Even with a court order, an employee of Proton Mail or Tuta would be unable to view any message content. If an email is sent from one Proton Mail user to another Proton Mail user (or one Tuta user to another Tuta user), it is never exposed to interception from a third party. Is this bulletproof? No, nothing is. There will always be some slight chance that an adversary could compromise your communications. However, it is extremely unlikely.

On the other side, a court order to Google, Yahoo, Microsoft, or any other traditional provider will hand over all of your account details and email communications stored with them without any resistance.

While I am not very concerned about court orders being executed on my accounts, I am extremely bothered by data breaches and internal abuses. If a breach occurs at [Proton Mail](#) or [Tuta](#), the thief gets a bunch of encrypted data that is of no use. In 2016, a large breach at Yahoo handed over access to over 500 million accounts to unknown criminal culprits. In 2021, Yandex caught an employee selling access to entire inboxes of targeted users. These scenarios are no longer theoretical. Verified threats toward your sensitive email content exist. A big part of being private is simply making better choices, even if they are not fool-proof.

I have a few opinions on email which may not be accepted by the security community. First, email is broken and outdated. I assume every email I write could be seen by someone else. I trust services such as [Proton Mail](#) and [Tuta](#) over any other mainstream provider because of the zero-knowledge environment. Even if they secretly had bad intentions, they could not access my data. Multiple independent third-party audits verify this protection. These audits carry more weight than online promises by the companies.

The bigger problem is on the other side of your messages. If you send a message from your Proton or Tuta account to a non-encrypted provider, then you lose most of the protection. Proton Mail and Tuta can only safeguard your information on their servers. They cannot control what happens when you leave their ecosystem. However, you can have comfort knowing that your historical email archive is protected

from prying eyes.

In the most recent edition of [Extreme Privacy](#), I recommended both [Proton Mail](#) and [Tuta](#), but displayed slight favor for Proton Mail due to wider adoption. I still see more Proton Mail users contacting me than Tuta fans, but the numbers are closing in. Also, both companies have made several improvements to their platforms. Let's dive into the latest comparisons for a full picture of each provider, sorted by the features I find most vital.

Email Security: This is a tie. Both services still provide industry standard E2EE and possess proper password and 2FA protocols.

Custom Domains: This is also a tie. I explain in the book the importance of owning your own domains for email communication. I place custom domains within each provider. If one service were to fail, shut down, kick me out, or become compromised, I can simply forward my DNS records to the other provider with almost no downtime. I am in true control of my addresses.

Adoption: This will vary, but Proton generally wins. Only a year ago, 99% of my contacts using secure email were Proton Mail users. Therefore, it simply made more sense to primarily use Proton Mail for communications. As I write this, 29% of the people who have emailed me from a secure provider in the past year are using Tuta. The other 71% are using Proton. That is quite a jump. When I have a contact using Tuta, whether a Tuta address or a custom domain on Tuta, I always communicate with that person via my own Tuta account. This protects the entire conversation, and is the right thing to do. This is why I believe we should all have accounts at each provider, even if only on the free tier.

Contacts: Tuta has a slight edge on this one. Both Proton Mail and Tuta do NOT fully encrypt the email addresses of incoming and outgoing mail. They must see the addresses to be able to facilitate the communications. However, Tuta encrypts the subject line while Proton does not. Is this a huge deal? Not to me, but it may be to you. Both providers encrypt everything else stored within a contact on their service. Personally, I do not store my sensitive contacts within any online service. I keep them in my offline desktop and mobile applications.

Calendars: This is a tie. Both providers offer a true E2EE calendar experience, and both now offer the ability to share a calendar between multiple users.

Offline Email Clients: The winner on this one will depend on how you want to store your email. I believe everyone should have an offline backup of every email communication. What if your email provider gets hacked or disappears? What if you logged in one day and all of your email was gone? An offline copy prevents this concern. Proton Mail offers a bridge application which allows you to use any traditional email desktop application to synchronize your emails to your computer. If you want to use Thunderbird or any other IMAP option, then Proton is the winner. Tuta allows you to export messages in bulk, which could then be imported into your email program, but that is an ongoing hassle. However, Tuta users can download their desktop application and synchronize all email for offline use. Make sure you select "Email" and change the "local data" to "999999 days" to get everything. Relaunch the program, disable internet, and scroll to your email archive to make sure all messages were synchronized. I am split on this. I like the ability to use my own application, but that means that I have to store all of my email twice on my machine (once encrypted via Proton's bridge application and once decrypted within my email program). Tuta's application is clean and just works.

Mobile Apps: I think Tuta gets a very slight win from me. Both providers offer great mobile apps, but Tuta's seems a bit cleaner, brighter, and faster to me. However, this should never be a reason to select a provider.

Multi-user Login: Tie. Both providers allow multiple paid and a single free account within the same mobile app. Proton is a bit easier to switch between users, but only because I am used to it.

Drive Access: Proton wins here. They provide a Drive service which allows you to store and share files securely. Tuta is working on their own version.

Audits: Slight advantage Proton. Both providers have had external audits of their services, but only [Proton's can be seen HERE](#). Tuta's plans to release theirs, but has not as of this post.

Open Source Apps: Tie. Both providers have open-source apps available through their Github pages [HERE](#) and [HERE](#).

Location: This is a tie for me. Proton is a Swiss company while Tuta is in Germany. I only prefer a non-U.S. provider, so I am happy either way. Only you can decide if either is a risk. Proton will obey Swiss court orders while Tuta will require a German court order. However, neither provider can give out any content since they cannot see through the encryption. They could only provide non-encrypted metadata.

Pricing: This is a loaded topic. While we should never choose providers based on costs, we should make sure we are receiving a fair deal. Again, both offer a free tier to try the services. Paid plans vary. Proton also offers a VPN service, so some users may prefer to bundle that in. Some may prefer it separate. Do your homework. Competition between the two should keep prices affordable, which is a good thing.

Payment: Proton has the slight advantage. They accept cash and

Bitcoin directly. Tuta can accept Bitcoin, Monero, and cash, but you must go through a third-party service called Proxystore. This works fine, but does introduce an additional hurdle. I would never send cash overseas, but I have used Bitcoin for both services without issue.

Disclosures: While I am an affiliate of both [Proton Mail](#) and [Tuta](#), I receive absolutely no information about you or your order. I was a user of (and recommended) both services before I became an affiliate. If you would like to support these guides, please consider registering with my custom links, even for a free trial, at https://go.getproton.me/aff_c?offer_id=7&aff_id=1519 and <https://tuta.com/?t-src=inteltechniques>. I was not asked to write this update and I provided no editorial control.

Which do I choose? Both. I possess paid accounts through each service and use them both daily. I possess custom domains on each service which can be changed to the other at any time. I am thrilled to have options. Which will you choose?

For much more information about secure email, and many other topics, please check out my book [Extreme Privacy](#). ■



Image: Ludovic Migneault

READER Q & A

By The IntelTechniques Team

Q: I followed your advice when I was at a hotel and put a sign on my door that said "Recording in progress, do not enter". It didn't work. The cleaners could not read English and came in while I was gone. What else can I do to keep hotel staff out of my room when I am away?

A: We have heard of this one other time, but never experienced it ourselves. One thing we have done when traveling with pets is to obtain a pet tag from the front desk. This alerts staff that an animal is present and they should not enter. We have been told by numerous hotels that the staff would never jeopardize a bite or escape and know to avoid rooms with this tag. We keep one from every hotel on hand whenever needed, even when we do not have a pet with us. This has never failed.

Q: I see you only offer your two main books now. Have you thought about offering every book you have ever made on privacy as one big digital archive?

A: We discussed it. However, there are a lot of redundancies and outdated information within all of the guides previously available. We really have not seen much interest in an "archive" but we can see the allure. If you truly want this, email us at staff@unredactedmagazine.com and we will see if it is something we can do.

Q: How to keep your XMR safe, any strategy?

A: My strategy is simple. I only use the official Monero applications offered directly from getmonero.org. Next, I always verify the hashes of the downloads and never use third-

party package managers to facilitate updates. Finally, I backup by wallets to encrypted offline and offsite local drives.

Q: Aside from Privacy.com and MySudo, have there been any notable developments in virtual privacy payment card solutions?

A: Somewhat. Privacy.com connects to your bank account and allows you to make private transactions in any name via virtual card numbers. MySudo is very similar but is linked to your debit or credit card. Cloaked requires you to purchase a virtual card with a set limit which can be used however you like. Those are the three which allow you to easily use alias names. Many traditional credit card companies, such as Capital One and Amex, are rolling out their own virtual card programs. With most

of these, you can easily get a “burner” card number, but they typically require you to use your real name. The benefits are more security than privacy. Many people online tout Revolut or Wise as the answer, but I find them no better than Capital One or Amex. You still have to disclose your true name and billing address for purchases.

Q: Suggestions in light of current wave of age verification laws being enacted across the world?

A: The internet has seemed to blow up over this. Based on the headlines, humans can no longer access any website without uploading our ID (which is not true). The UK Recently announced new laws which require all websites and online apps which display adult content must ensure their users are over 18 via age-verification checks. This includes several gaming, social media, and dating apps. Some US states require this for porn sites. The current solutions are either to avoid these services, identify alternative services not cooperating with the laws, or use a VPN. Will this get worse? Probably. Will we always find a way to circumvent the invasion? Definitely. YouTube is doing their own age-verification AI gimmick, but I don't care much about that either. I rarely go to YouTube.com, and I can't think of the last time I needed to watch an “adult” video on their service. If you do get flagged as a minor on YouTube, they will stop all targeted advertising, which could be a win itself. My concerns are the next phase. I believe we will all see a time in the near future where we will be required to verify confirmed identity through a third-party service in order to have any technical connection to the outside world, including internet, telephony, shopping, utilities, and text communication. We will be issued an identity wallet with unique hash values, similar to Bitcoin addresses, which will be required for daily activities. Services will see the hash but not necessarily our details. Apple and Google will offer digital transmissions through their devices. The third-party mothership will know all. Governments will get in on the game. We will rely on this system for voting, taxation, and payments. It will

be abused. We will find ways around it.

Q: For those who don't want to match their SIM card to their phone cell, can you give your recommendation for a good privacy SIM router?

A: I have no brand loyalty, but I would only consider routers which support flashing OpenWRT. I would also encourage you to identify your threat model. Carrying around a cell router is not much different than having data access on your mobile device if you have taken steps to make it private and secure (GrapheneOS). Also, a data-only plan on a phone would eliminate the need for an additional device without attaching a telephone number to your activity (if that is your concern). I don't think anyone in our office carries portable cellular routers any more.

Q: What are some ways users can evaluate the privacy-friendliness (or not) of LLMs? Are any recommended more than others from a privacy perspective, and if so, why?

A: Start with the articles in this issue about Proton Lumo and mobile AI. Overall, any locally-stored offline LLM will be private, especially if you run Little Snitch or Open Snitch to make sure your app is not calling home. It is more about finding the LLM best for your daily needs.

Q: In 2025, which methods of browser fingerprinting are the hardest to spoof, and why?

A: I don't think there is a single method which could not theoretically be spoofed. Instead, the danger is the totality of all fingerprinting. When we access a website, we are almost always unique (unless you only access the internet from a TAILS boot USB, which is not advised for daily usage). When we try to get sneaky and spoof details, we stick out even more. At the best-case scenario, we might share a fingerprint with a handful of privacy geeks, but now we all look suspicious. I accept that going online means that we can be identified as a unique visitor. As long as I am behind a proper VPN with proper

DNS and a hardened browser, I don't worry about everything else. Instead, I place my effort is segmenting personal and alias access. My laptop (and VPN) used for email, banking, and other things in my name is never used for breach work, covert activities, or shady stuff. To me, THAT is more important than tweaking obscure configurations hoping to “blend in”.

Q: You only focus on pfSense in your guides. Why not OpenSense?

A: OPNense is great. I focus on pfSense for three reasons: Familiarity, reliability, and history. I know pfSense better, it has never failed me, and I have many years of uptime under my belt. I would never recommend people switch to OPNsense until I can say the same about them. We are currently testing a OPNsense firewall with a OpenWrt router, both behind open-source coreboot firmware for a truly clean experience. Once we know this is sustainable long-term, we may consider a full guide. That just takes time.

Q: In your books you mention an unofficial Voip.ms app but not their official app. Will you be recommending the official app moving forward?

A: Possibly. We have been testing the official Voip.ms app on both Android and iOS. It is simply not ready yet, which the CEO acknowledges is a “Work in Progress”. On iOS, there is an issue preventing calls through encrypted SIP. On both versions, you can only use one account, and cannot switch between different numbers. I am told both of these issues will be resolved. UPDATE: As of this publication date, we see that Voip.ms has recently updated their mobile apps. We will test soon and report our findings on our website.

Q: Today, I was looking at a very nondescript photo on Instagram and decided to play with the Google Lens tool. Google's AI Feature was able to bring back (the full address of the image of a house) for me. I have not seen this discussed in any OSINT class that I have taken recently. From an EP perspective, this is a bit concerning.

It used to take additional steps and almost specialized knowledge to identify a home from an image like this, and now I'm not so sure. I'm trying to figure out what is the best proactive and defensive stance to take in light of this.

A: I have seen this behavior often, and every time I investigated the address, it was never accurate. I even gave Google screen captures from houses on Google Street View and it could not identify them. It is always worth checking Google Lens for a location, but then paste that address into Google Maps for a Street View. I believe you will find that the AI feature of Google Lens is rarely, if ever, accurate. That could change tomorrow though.

Q: I have been on your standby list for a consultation for over a year. What gives? When will you be able to help me?

A: I understand your frustration. I have not taken on any new clients in a long time. We finally reached the limits of our availability to serve our active clients and do not want to oversell our ability to help potential new clients. I know that the business playbook says to hire more staff, open more offices, and bring in a sales division to promote, but I have no interest in any of that. I like our small crew. I like the workload we have. I like the work-life balance this creates for all of us. We know this upsets people. Some even leave us bad reviews on Trust Pilot because we politely and clearly explained that we

were not accepting new clients right now and unfortunately could not help them (<https://www.trustpilot.com/review/inteltechniques.com>). What we can do is release products like our books and this magazine. I suspect over 50% of the people on our waitlist could resolve their own issues with the books. I know that is not always easy and that some things are more time-sensitive. However, I always encourage people to take the knowledge and do anything they can themselves before hiring someone to do it on their behalf. If we find ourselves with extra time, we will absolutely begin greeting new clients again.

Q: I want to write an article for UNREDACTED but do not know what to write. What are you looking for?

A: Whatever you are passionate about. Don't try to submit something you think people will want to read, tell us what YOU want to write. What is that one thing you know really well that others probably do not know anything about? Being related to privacy, security, OSINT is great, but anything technical is well-received too. Feel free to break through that barrier as well. I have thought about writing my own articles about physical and mental health tactics which I find valuable or interesting (and affordable) travel experiences I have had. There are no rules.

Q: I created a firewall per your guide. It seems like pfSense sends data to Google every time I reboot

it. What is this and how can I stop it (if I can)?

A: This is time synchronization. I don't love that pfSense chose to sync to Google's servers instead of something like NIST, but that is what it is. I don't think that is too concerning, as Google only knows that a firewall at your IP address asked to sync the time. It checks by IP address, so your ISP DNS is not involved. It shares nothing about you or your internet activity. A few minutes online within any browser probably shares more about you with Google. However, you can control this. In pfSense, go to Diagnostics > Command Prompt and enter the following in the first field one at a time, clicking Execute after each.

```
touch /conf/ntp-boot-time-servers

echo 129.6.15.28 > /conf/ntp-boot-time-servers

echo 132.163.96.1 >> /conf/ntp-boot-time-servers

download /conf/ntp-boot-time-servers
```

These create a configuration file to store alternative time server details, adds a primary IP address for a NIST time server, adds a secondary IP address for a NIST time server, and downloads the file you created so you can confirm the changes. Reboot pfSense and confirm it no longer connects to Google. If you want to undo these changes, enter "rm -f /conf/ntp-boot-time-servers" into the same field and execute. ■

WINDOWS 10 EOL

By The IntelTechniques Team

We are now approaching the October 2025 sun-setting of support for Windows 10. As a follow up to their previous announcements regarding post 2025 support, Microsoft recently announced additional options for those who wish to stay with Windows 10. I will not bury the lead: all of the options provided by Microsoft are bad for any privacy-minded users unless they want to shell out additional money for paid support. Let's first look at the pitch and then at the end of this article I will share my own strategy. The following graphic is the summary of options posted on Windows.com:

Extended Security Updates for Windows 10:

- **For individuals:** An enrollment wizard will be available through notifications and in Settings, making it easy to enroll in ESU directly from your personal Windows 10 PC. Through the enrollment wizard, you'll be able to choose from three options:
 - Use Windows Backup to sync your settings to the cloud—at no additional cost..
 - Redeem 1,000 Microsoft Rewards points—at no additional cost..
 - Pay \$30 USD (local pricing may vary).

Source: <https://blogs.windows.com/windowsexperience/2025/06/24/stay-secure-with-windows-11-copilot-pcs-and-windows-365-before-support-ends-for-windows-10/>

You might think, okay, I'll just buy myself out of this problem by paying the \$30 extension fee. This is a yearly fee so essentially they are pushing you back into a subscription to receive proper support for a product that you already own. Using Microsoft points does not change the fact that it is a subscription fee. The only difference is that you are using their proprietary "currency" which for most people is an even worse option.

As is common in these modern times, they are happy to provide a new alternative where you can trade your data for the right to continue using the software you already own. If you are already deep into the Microsoft cloud storage and services, you may not take issue with this, but the fact that you are reading this blog infers that you value your privacy and security. Having to store your workstation settings in Microsoft's cloud seems like a horrible idea. It means giving up even more control of your sensitive data.

The final option is to do what Microsoft really wants us to do, which is to comply and accept being forced into using Windows 11. First of all, not all hardware supports Windows 11, so this may require a significant hardware upgrade. Secondly, Windows 11 has even worse privacy implications than Windows 10 as well as being a far more "locked down" operating system. Anyone who has put effort into customizing their Windows 11 installation knows the pain of trying to remove the various unwanted "features" which harvest your personal data while also limiting your ability to customize your user experience. Then there is the Copilot (Microsoft's AI assistant) integration which they seem intent on forcing upon all of us.

You might be wondering at this point if I am just a Microsoft hater. Actually, Windows has been my primary operating system my entire adult life. Although Windows continues to offer some of the best broad application compatibility, each new version has been less privacy-respecting while also offering less control to users over their own systems. I would not tell anyone what choice they should make but I decided earlier this year to migrate to Linux as my primary daily operating system. This journey is not complete, but I will be posting a follow up article sharing some of my experiences as well as some tips and resources for others who may choose to head down the Linux rabbit hole as an alternative to submitting to Microsoft's non-privacy respecting business practices. ■

TAKE ME OUT TO THE REVERSE ATM

By heyczerny

I have been a fan of Visa Vanilla cards ever since my first read-through of Extreme Privacy, and over the years they have served me well. Recently, however, I have noticed a steep increase in “draining attacks” with these cards, including an alarming trend of cards hitting store shelves with the security code already scratched off and/or mag-stripe already demagnetized.

These attacks are a stark departure from one seen in years past, where criminals steal an inactivated card from a store and create a sticker matching its loading/activation barcode. In this attack they then return to the store and place this sticker over the same barcode of unsold cards still on the shelf. When a victim pays for and activates a card that contains this fraudulent bar code sticker, the money is instead deposited on the original stolen card. Checking for this by inspecting the packaging and looking for stickers is simple enough, but newer attacks involve stealing the card numbers and then scratching them off, and then demagnetizing it so that the person who actually buys it is unable to use the card.

Sometimes, incredibly, the packaging is still pristine, with no sign of tampering. At one store last year I explained the situation and asked a manager if he would let me open up the packaging at the register before deciding whether to load it with cash. I brought up a perfectly sealed Visa Vanilla card and we opened it at the register to discover the security code was scratched off. He couldn't believe it. I walked out without a card. Too risky.



Apparently, I am not alone. In the last year, at least two separate lawsuits against various companies involved in the sale of Visa Vanilla cards have been filed. While privacy.com had me set for online purchases, it was time to look for a better in-person solution.

In a seemingly unrelated story, I have watched with much sadness over the years as the ability to anonymously attend a staple of American culture, the Major League Baseball game, has all but disappeared. Not long ago you could pay cash for a physical ticket at the box office. But as ticket fraud rose and COVID-19 made businesses re-evaluate technical solutions, the MLB has locked tickets down hard. Today, to get past the gates and into the ballpark near me, the MLB app is required, and its ticket is both animated and incorporates a rolling code. No more print-at-home. No more screenshots. And once you're inside, it's 100% cashless. But if you were to look closely at the amenities, you might notice another new addition to game day: the Reverse ATM.

It works exactly as it sounds. To quote one article, “You insert cash into the machine and it uploads the amount onto a prepaid Mastercard... If you do not use all of the funds during your time at the stadium, the card can be used at your local gas station or anywhere Mastercard is accepted.”

This sounded perfect. But I had questions. Was some sort of account required? Would I be asked to scan an ID? To answer these questions and hopefully end up with such a card that suited my purposes, I would need to embark on a mission: Go to an MLB game anonymously, and find the reverse ATM.

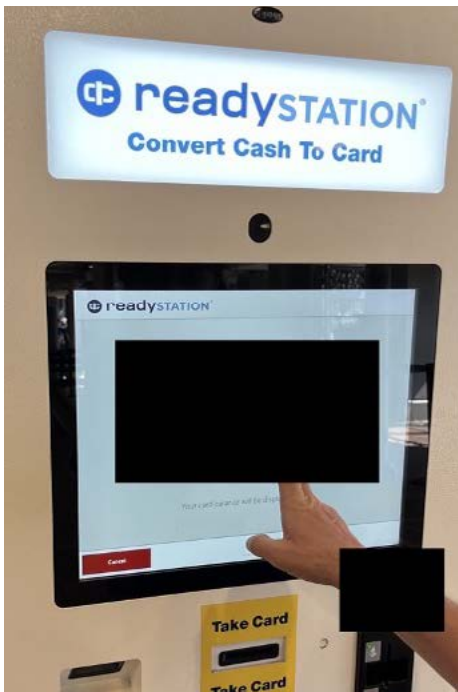
Creating an MLB account was easier than I expected. I provided a masked

email address for this specific task, and password. A birthday was also asked for. I gave the birthday of a famous retired MLB player. Interestingly, a name was not asked for. This signup was done in a privacy-hardened browser over a public VPN. So far so good.

At this point it was time to find a ticket. Unfortunately, the stadium seat picker would not load in the browser. Maybe it was the VPN, maybe my extensions or settings, who knows? But I would need to move to the MLB app earlier than expected.

I have an old Pixel 3a with GrapheneOS for these sorts of things. It has an anonymous Mint Mobile sim and Wi-Fi and Bluetooth are always off. Because it is so old, it no longer receives any updates. I was worried this might cause an issue but luckily it did not. I installed the MLB Ballpark app and logged in. Browsing for tickets worked fine on the app. I picked a game for the middle of the day in the middle of the week. This way I expected there to be fewer attendees and thus I could fuzz my actual seating a bit. There's good plausible deniability here – a seat is located by 3 distinct numbers! Maybe I just got confused.

Paying with a masked card and billing address was accepted, and I had my ticket. It was only viewable in the app, and contained an animation to defeat screenshots as well as a barcode which changes every few seconds. This phone was coming with me to the game.



On game day I put on the team colors to blend in, grabbed my Pixel 3a and hat and sunglasses, and headed out. I noticed a "Will Call" window near the gate which caught my attention since its existence suggested the ability to purchase a ticket app-free. But I was told that while they could maybe assist with a purchase, any ticket would eventually need to be sent to the app. Next it was time to head inside. I was a bit worried that my fake famous MLBer birthday might come back to haunt me as I passed through security, but it was completely uneventful. I was in, the Pixel 3a got turned off, and I grabbed a seat near my ticket. I decided I would wait until after the first inning to find the Reverse ATM and during that time I learned a few interesting privacy-related things.

The first is that at a game there is a very slim chance you win one of the random prizes selected for various seats and rows throughout the stadium. I saw free seat upgrades, free food, etc. handed out to various lucky fans as the camera zoomed in on them on the Jumbotron. The second is that if you happen to catch a ball at your seat, security might come have a chat with you. This is almost certainly a congratulatory thing, but they might also want some of your information in

exchange for that ball. Luckily, I was unlucky in both of these scenarios.

After the first inning I went and found the Reverse ATM. Interestingly, despite this being a cashless stadium, it was directly next to a regular ATM. The Reverse ATM dispenses Visa debit cards and loading a new card is as simple as pressing a few buttons on the touch screen, none of which require any data or ID scans. When prompted you simply insert cash bills up to a limit of \$500. I decided to put \$60 on the card which I thought should cover a beer and a couple of hotdogs. Unlike Visa Vanilla, there was no activation fee. This appears to go against some documentation I found on this card's website which states potential activation fees up to \$6.00. Perhaps they have a special deal with this ballpark. There is however a dormancy fee. The card was printed immediately, and dispensed. I was able to choose a paper receipt as well. I was surprised to see that the card had an expiration date of only 9 months from now. I'm not sure if this is by design, but it is something to keep in mind.

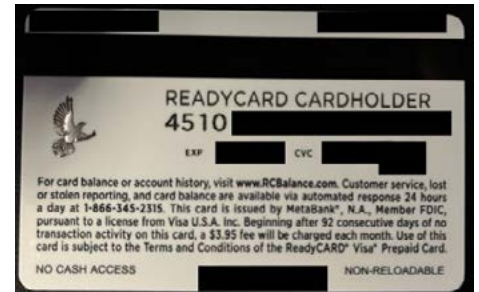
Immediately after the card was dispensed, I took it to go purchase a \$20 beer (I wasn't kidding) and it was accepted without issue. Back in some new seat, I decided to also test it with one of the vendors walking up and down the aisles selling hotdogs. It was accepted here too with no issue after being swiped on his mobile point-of-sale system.

This was mission accomplished. I had come to this game with an anonymous ticket and was now enjoying a beer and a hotdog courtesy of this new prepaid debit card with no activation fee. I stayed for more of the game, and then headed home. But there were still a few more tests to run.

You may recall that this card is supposed to work both inside and outside the ballpark. So the next day I made a small purchase at a convenience store and it worked fine. It did however ring up as a credit card transaction which was interesting (but a welcome sign in that it was accepted) and cost

me 38 cents. I think this charge came from the convenience store end and not Visa but I'm not sure.

The final test was an online purchase. Again, using a hardened browser and a public VPN, I am happy to report that the remaining funds on the card were able to be charged successfully in an anonymous donation to the EFF.



Some final notes: Like Visa Vanilla, there is a free website which lets you check the balance of the card at any time. Unlike Visa Vanilla, this website is much friendlier to VPNs. Be aware of short expiration timeframes and any dormancy fees. Also, your experience on activation fees may vary if this was a special agreement between the ballpark and the Reverse ATM company. Finally, be aware that the Reverse ATM does have a front facing camera similar to that on an Amazon Locker kiosk. However, it is high enough that a hat brim could likely shield your face.

Hopefully these Reverse ATMs show up in more locations over time. I would certainly use them again. They appear to be a nice alternative to Visa Vanilla and potentially cheaper as well. Finally, like other privacy tools that grant some level of anonymity, use them responsibly or we all run the risk of them either disappearing or being made ineffective through future identity verification requirements. ■

911 WHAT IS YOUR EMERGENCY?

By: UP

IntelTechniques training member "Up" recently shared a long write-up with our private group. He had a unique opportunity to connect with a person who operates a 911 Dispatch Center willing to answer all of his privacy-related questions about 911 calls. I believe some of these details have never been published before, and we should all understand how 911 works in the background. He gave permission to share the following partial excerpt publicly.

I wanted to test the 911 system because this is a tool we often hear myths about, but are not able to test first hand. I caution all readers to NOT attempt tests with the 911 system. This is NOT a toy and is ONLY to be used in emergency situations. In my test I was in the presence of a 911 Dispatch Center Operator, and we could in real time monitor the call volume to the center. I wanted to use the tools that I typically have at my disposal. This was not an exhaustive test, rather intended to reflect what would be used by Privacy Advocates. I wanted to see what would happen when those tools 'called' 911. My main interest was logging and location information. What exactly happens on both ends of the communication and what is ultimately captured by the 911 Dispatch Center?

True SIM: For this test, 24 hours prior to my visit I activated a Mint Mobile trial SIM card. During the activation process I used a zip code near by the 911 Dispatch Center to ensure I would be assigned an Area Code which is in the city which this center covers. I also provided an alias name of Bruce Wayne during the registration process to see if there would be any association when the test was performed. This shouldn't

have any effect on our test, but in the name of consistency I wanted to be precise. This test is significant as it represents how most people would contact 911, using the phone number associated with the SIM card in their phone. First, I noticed that a real time chat log was present on one monitor of the Dispatcher's screen. This was transcribing spoken word into text by both the caller and Dispatcher in real time. Next, I noticed the "Call Information Display" which provides some details related to the phone number calling 911. This displayed Phone Number, Date & Time, Carrier (T-Mobile) and Mapping Coordinates (Lat & Long). There was some other information related to the Dispatch Center, but this was all that was visible. I want to discuss a few things here.

Remember, I used a Mint Mobile trial SIM card for this test. The system identified T-Mobile as the carrier. While this is true it did not specify our MVNO of Mint Mobile with whom the account was registered. Yes, Mint is technically owned by T-Mobile now, but in all the logs I saw no specific MVNOs were identified. Next there was no name associated with the number on the Dispatcher's screen. I registered the name of Bruce Wayne with the phone number, but this was not present. I later pulled the CNAM (caller ID) information of this number after my visit and that produced yet another name (not Bruce Wayne) being associated with the number. Neither were present in the 911 log since no name was present in this case. This indicates that if the details of a phone number need to be determined, likely a legal process involving the carrier will need to be initiated.

Next is the location information. On the Dispatcher's screen there was a

visible map scaled to display about 3-4 neighborhood streets, but could be scaled as needed. Physical addresses are visible as text overlayed on each lot, home or structure. The software solution was using Open Street Maps for this mapping feature, but a proprietary solution over-laying the map. Anyone reading this could easily navigate the map. The difference is when a call is placed to 911, the combination of software used as a whole does it's best to provide a 'pin' of the location the phone is making a call from. This is visible on the screen, and can move as the system updates its information should a caller be in transit. Since this is likely the most sensitive feature to the privacy community I am going to convey as much as I can about this from what I witnessed.

When the call was placed the Android phone being used displayed a snippet on screen of a map (accurate location), Precise Lat & Long (accurate location), Plus Code (accurate location) and a physical address (not accurate but was a nearby home). This is likely displayed on screen to assist a caller who may not be familiar with an area they are calling from. But does this information also make its way to the 911 Dispatcher?

Back to the 911 Dispatcher's screen, the map did indicate an approximate location of the phone with a red 'pin' on the map. However, we were literally inside of the Dispatch Center and that was not the location indicated on the map. If more precise information is not able to be communicated to the technology stack the map will display a pin at the location of the cell tower which is involved with the 911 call. That is what happened with our test. If the only information available to the Dispatcher was the pin on the map, they would not have been able to

accurately locate the position of the phone making the call in this particular test.

Now I want to cover what was NOT present. No IMEI information was present. Even though a generalized location is being determined based upon the position of a nearby cell tower, that cell tower is not transmitting the IMEI of the phone to 911. I later confirmed this by selecting several calls at random from logs using the dispatch operator's privileged access and there is not even a field to enter IMEI information into the logs. It's not a data point of interest to them.

Interestingly, once the call was completed, the record of the call was not present in the call log of the dialer used on this Android phone. This behavior was the same for every smart phone I tested, but using a dumb phone did leave a record of the call history to 911 in the phone's log. This may vary by device, but I found it interesting and my view is that 911 is less of a phone call and more of a special mode the phone enters when those digits are 'dialed'.

No SIM: The final test I wanted to perform was using a phone with no SIM card present. 911 technology is one of the reasons older, less secure cellular standards remain functional and supported. The logic here being that anyone should be able to access 911 services no matter how out dated their phone may be. I have a very simple phone which has a removable battery. I can charge the battery and remove it from the phone. The battery will hold a reasonable level of charge for about 1 year outside of the phone. Leaving this in a car exposed to temperature fluctuations will likely reduce this ability over time, but I don't need to worry about it weekly.

I powered on the device and dialed 911. Same routine as before but the phone itself did not provide any mapping information on screen as the previous Android True SIM phone did. It only showed a call in progress to 911, with no SIM inserted.

On the Dispatcher's screen, we noticed something very interesting. A phone number did populate the screen. Remember this phone has no SIM card, thus no service attached to a cellular provider, thus no attached phone number to the device. However, on the Dispatcher's screen the area code of this phone number was "911-XXX-XXXX". This phone also indicated a carrier of AT&T, even though this phone has never had a SIM card inserted into it, and was carrier unlocked at the time of purchase. Phones which call with no SIM inserted are assigned a number with an area code of 911 since that is not an area code which will ever be used by carriers. We ended this call, and after a few minutes repeated the test. On the repeat test, the same number popped up on screen associated with this device. We are unclear on why this occurred, but assume it's the only way for a cellular tower to process a call in this situation. We assume that the IMEI is linked to a phone number at the cell tower for this purpose. The IMEI never populated the screen at the Dispatch Center.

I then decided to test a GrapheneOS (GOS) device which also has never used a SIM card to repeat the test with a different device. GrapheneOS is a security focused Android Mobile OS which is favored by Privacy Advocates. Again, a number with an area code of "911-YYY-YYYY" populated the screen but was a different phone number than our dumb phone. Oddly this phone displayed a carrier of Verizon, not AT&T like the dumb phone on the Dispatcher's screen. This device is carrier unlocked as well.

Both the dumb phone and GOS phone provided location information as well. The dumb phone pinged a location within a few hundred feet of the Dispatch Center (very accurate) and the GOS phone pinged at the location of the cell tower it was connected to (not as accurate). The GOS phone has many privacy-oriented settings including location services being off.

With the testing completed, the 911 operator agreed to be interviewed for the benefit of YOU the reader.

They have taken the time to answer a number of questions that you may have pondered when thinking about the implications of technology in relation to privacy.

Can you explain the basic process of what happens when someone dials 911 on their phone to report an emergency?

This process may vary slightly for each jurisdiction, but here is how it works for my region:

- a. Phone connects to OSP (Originating Service Provider), such as Verizon, AT&T, T-Mobile etc.
- b. OSP routes the 911 call to a 911 call aggregator. This aggregator collects 911 calls from all OSPs operating in the specific jurisdiction
- c. Aggregator routes the 911 call to the 911 authority call handling equipment for the jurisdiction.
- d. 911 authority routes the 911 call to the relevant PSAP (Public Safety Answering Point) depending on location of call and other criteria.
- e. PSAP either handles that 911 call entirely, or routes the 911 call to an sPSAP (Secondary Public Safety Answering Point) for further processing and handling
- f. Once call is completely handled by a PSAP, sPSAP, or both, call is completed and terminated

Can the public contact 911 services in any other way than by phone call at your location?

911 services can be contacted the following ways:

- a. Dialing 9-1-1
- b. Sending an SMS message to 9-1-1 (Jurisdiction dependent)
- c. Calling the PSAP/sPSAP non-emergency line (Jurisdiction dependent)
- d. Utilizing emergency call boxes (Jurisdiction dependent, such as in Boston, MA.)

Have you experienced Swatting attempts or something similar for Fire or EMS services by people calling in? If yes, can you explain what happens during or after an event like that at your center?

Yes, swatting happens at our facility. We do answer every 911 call and take them seriously. For suspected swatting incidents, we still process them as normal incidents and dispatch resources to the reported address and notify law enforcement. For repeated incidents, we do notify law enforcement of potential swatting calls and let them handle it. We do not reject 911 calls or refuse services to suspected swatting calls.

Do you process FOIA (Freedom of Information Act) request on a regular basis? If yes, are there any trends or obvious attempts to exploit/abuse that legal mechanism?

Yes absolutely. The only trends we see are when we process calls that are of high publicity. We are required by law to respond to all FOIA requests within 10 business days.

Can you explain what information is visible on a Dispatcher's screen when someone calls in for emergency services?

The following information is visible when someone calls 911:

- Call Type (Wired, Wireless, VOIP, Business, etc)
- OSP (Originating Service Provider)
- ALI Caller ID (Phone number)
- ANI Name (Business name or name of carrier)
- Call date and time stamps
- Address (Address registered for the phone number or of the cell tower)
- Location Coordinates (Lat/Long of the approximate caller's location)
- Live map of location, continuously updating if live location is received
- Live transcription of the phone conversation

Do you use any sort of speech recognition software or AI to transcribe a callers voice into text or perhaps interpret a caller's tone during a call?

Our facility utilizes a relatively new feature that provides live transcriptions of both side of the conversation for any incoming 911 calls. No plans for AI at this time.

Can you explain what information is stored after someone calls for emergency services, how long those records are stored and where they are stored?

All information is stored, including:

- ANI/ALI information from the 911 call
- Location updates
- Call nature
- Full phone call recordings
- Any dispatcher specific notes
- Radio traffic related to the incident

Retention various per agency. For our agency, we store data for 2 years and it is all stored onsite with encrypted backups offsite.

Who can obtain access to historical information related to 911 calls and are there controls in place to limit a rogue employee's attempts to access what would be deemed sensitive information stored by your systems?

Fire and EMS agencies we dispatch for can pull historical information for their agency only. Our facilities employees can pull all historical data with the exception of audio and screen recordings. Only supervisors can pull those. All data access is logged and can be audited.

Given your close relationship with Law Enforcement, does this also mean that any Law Enforcement entity can freely access any information from your systems at their will or must they follow legal processes to obtain that information?

Law enforcement agencies still need to go through the legal process

to obtain data from our facility. We have had incidents where we have denied request without pursuing the proper legal channels. Facilities which dispatch police may have the ability to access that call information without the need for a legal process.

Being in the unique position of a 911 Dispatch Center Operator, do you have any relationship with any cell tower companies or other entities that may allow you to locate individuals as you please using historical 911 data? For example, someone who called 911 in the past but for some reason there is a need to locate them currently.

No. We have no relationship with any telecom or cell tower companies. If we did, access to any non-public data would not be in scope of the agreement on either side.

If someone calls 911, does a dispatcher see any historical record of previous calls or historic information about a caller? If yes, can they access additional information about a caller at their discretion?

Partially; if a 911 call comes in for a specific address, our facility can see historical calls that our facility has processed for that same address. We are unable to see historical calls that any other agency may have handled. Dispatchers will refer to historical data to assist with dispatching and managing the current 911 incident. For example, if it's a gated community and the 911 caller is unable to provide a gate code to access the apartment complex, the dispatcher may reference previous incidents to search for a known good gate code.

Privacy advocates often avoid using the phone number which is assigned to a physical SIM card or more modern eSIM, and instead prefer to use VOIP phone numbers. This prevents location tracking by cellular towers. Unfortunately, we are often told 911 service is not available to VOIP users. Do 911 centers actively block VoIP numbers or is there more to this? Please elaborate on your experience with VoIP and 911 services.

911 centers do not actively block VoIP services. We often get 911 calls from different VoIP providers. I suspect the issue is with the VoIP provider. If they do not give you the option (or requirement) of supplying your address to use for emergency calls, the VoIP provider may not know who to redirect the 911 call to.

In the event a Privacy Advocate encounters an emergency situation and needs to use 911 services, can they simply call their local law enforcement agencies non-emergency number to bypass using the 911 system? Any additional thoughts or concerns using this method by someone in your role?

Using a local law enforcement (or even fire department) agency non-emergency number may not work as those agencies may not actually be the one dispatching the calls. They may only be able to tell you to hang up and dial 911. However, if you found the PSAP/sPSAP non-emergency number, that should work. The 911 center can process 911 emergency calls just the same, without all the additional information they get when using the 911 system. Keep in mind though that a non-emergency line will NOT have the

same reliability, resiliency, and priority that the 911 phone system has. Any desire to use non-official channels for emergency service should be tested in advance and over time as it could be dependent upon the person who happens to answer the phone at the time of your call.

Can a caller to 911 request to remain anonymous by saying anything specific, or will the call be logged no matter what a caller says?

Everything in a 911 call is logged and recorded. The caller is not legally required to provide their real name, phone number, or address during the 911 call. However, fabricated or missing information may hamper the ability for emergency services to appropriately respond to the incident.

As far as you are aware, is it a crime to provide an alias name to a dispatcher when calling 911? An Alias name being anything other than the name present on one's Birth Certificate or Government issued ID such as a Driver License.

It is not a crime to refuse to provide your legal name when calling 911, to

the best of my knowledge.

Are cellular devices tracked for any duration after a 911 call is ended by your systems?

No, tracking is halted as soon as the 911 call is terminated.

Visiting a 911 Dispatch Center was an eye-opening experience. Knowing the level of effort that has gone into providing reliability for a system that is in place to save lives was an impactful realization for me. I will be blunt, using 911 would not be considered a privacy friendly process. That being said we who adopt privacy strategies are accustomed to managing the hurdles technology presents us. The best way to develop an effective strategy is to have the most information possible, which I hope I provided you with today. I urge you to take a moment and determine a process you are comfortable with should an emergency arise. Practice your process with a clear mind so when the time comes you can execute it under stress. This includes knowing what you will say and not say on a recorded line. I hope you never need this information but if you do best wishes. ■

FINAL THOUGHTS

By Michael Bazzell

Well, here we are again. The end of another issue. What is next?

Content: Please consider contributing an interesting original article for the next issue. The entire team is waiting to read your submission at staff@unredactedmagazine.com. While the emphasis will always be privacy, security, OSINT, and technology, there is room for more. Maybe you would like to review past or upcoming shows or movies of interest to this community. Maybe you have tips starting a business, filing taxes, carrying tech gear, or frugal living. In the 90's and 2000's, there were

many "lifestyle" magazines for almost every community. We should have one now.

Support: If you found value in this issue, please consider telling a friend. If you want to see this continue, please consider financially supporting this work. Our team is small, but the effort to make this all happen is huge. From content, to editing, to layout, to cover design, there are many people involved. There are several ways to financially support this work, and any donations go directly to those who volunteer their time to make this happen.

Credit Card:

We have set up a link where you can buy this exact same PDF and pay whatever price you deem fair (minimum \$5) at <https://payhip.com/b/AheMw>.

We also accept Bitcoin and Monero donations on our website at <https://unredactedmagazine.com>.

As always, my thanks to the anonymous cover designer and Nick over at Astropost for all layout. If you have any website or design needs, reach out to him. ■

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/4fFC2Ft>

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

Proton VPN Service: <https://go.getproton.me/SH16Y>

Proton Mail Encrypted Email: <https://go.getproton.me/SH16Q>

Tuta Encrypted Email: <https://tuta.com/?t-src=inteltechniques>

Silent Pocket: <https://slnt.com/discount/IntelTechniques>

Standard Notes: Coupon Code IntelTechniques20

VoIP.ms: <https://voip.ms/en/code/IntelTechniques>

NOW AVAILABLE

Extreme Privacy (5th Edition)

OSINT Techniques (11th Edition)



WEBSITES AND CONTENT.

For businesses who respect privacy.



Astropost

Astropost is the official design partner for this issue of **UNREDACTED MAGAZINE**. Need an ad designed for the magazine? Or a website that gives you results? We'll help you out!