Cyber – Tinker

Drums Of Liberation

Index

Encryption Security Tool-kit V3

This will be acting as a template or guide

It is your choice how far down the Rabbit Hole you go

We will update the Kit to best suit the Times but it’s your responsibility to Check the Code of the Tools and Check Risks

If you don’t have the skills, Team up with a Spec Ops person / A Person who is Computer Literate

There is no One Shoe Fits All here

Smartphones

- F-Droid (App Store / Open-Source)

- Brave Private Browser (Internet Browser)

- DuckDuckGo Privacy (Internet Browser)

- Tor Browser (Internet Browser)

- Orbot Tor

- Edge (Crypto Wallet)

- Luno (Centralized Crypto Exchange / SA)

- Briar (Tor Messanger)

- Signal (Encryption Messenger)

- Jami (Peer2Peer Messanger / Free-Software)

- Linephone (Encryption Calls / ZRTP – Protocol)

- Jitsi (Encryption Video Calls / ZRTP – Protocol)

- Text Secure (Encryption SMS)

- GrapheneOS (Privacy / Security)

- LinageOS (Privacy)

Operating Systems

- Tails

- PureOS (Free-Software)

- Manjaro (Free-Software)

- Trisquel (Free-Software)

- Kali

- Ubuntu

-Debian

PC Software

- Icecat (Internet Browser / Free-Software)

Tor (Internet Browser)

- Exodus Wallet / Hardware Wallet (Open-Source Crypto Wallet)

- Ghost (Decentralized Crypto Exchange)

- bisq.network (Decentralized Crypto Exchange)

- Monero GUI (Crypto Wallet)

- Linephone (Encryption Calls / ZRTP – Protocol)

- Aether (Social Messenger)

- Jami (Peer2Peer Messenger)

- Mailpile (Email -Messenger)

- Pidgin (Encryption Messenger / Sever required for Host)

- Gajim (Encryption Messenger / Sever required for Host)

- Dino (Encryption Messenger / Sever required for Host)

- LibreOffice (Open-Source Office Suite)

- Ejabberd (Encryption Messenger Sever)

- Prosody (Encryption Messenger Server)

- Matrix (Encryption Messenger Server)

- iRedMail (Email Server)

- Emacs (Text – Editor)

- VLC (Video Player)

- OBS (Video Editor)

- GIMP (Alternative PhotoShop)
- GNU Taler (GNU Cash)
- GNUnet (Building the Internet from the ground up)
- KeePassXC (Password Database)
- WireShark (Monitor Device Electronic Signals)
- Veracrypt (Encrypt Drives)
- Coreboot (Bootloader)
- GRUB (Bootloader)
- Feather (Crypto Wallet Lightweight)
- Wasabi (Crypto Wallet / Shuffle)
- OnionShare (Tor File-Share/Web-Host)
- iRedMail (Email Server)
- Bleachbit (Drive Data Cleaner)
- Opencart (Ecommerce Open-Source)
- MixMaster (Email Messenger)

Cyber Security - SetUp Tool-Kit

Light Weight

USB / SD card - Tails OS

- Portable Computer / Stateless Traveler
- Install feather or Monero GUI for Crypto-Currency

USB / SD card

- Small portable Hard Drive = For Memory

** Software To Install On Drive **

KeyPassXC

- Password Database
- Password Generator
- Encrypted Database

VeraCrypt

- Encryption Software to Encrypt the Portable Drive / Memory for security

Smartphone

(Note : you can't make a smartphone 100% Secure, So use it wisely)

Messangers

- Briar = Tor Network / Bluetooth Compatible / Encrypted / None Portable Account
- Jami = No Server, No Middle Man / Encrypted / Portable Account

(Recommend Jami for Common Folk)

Caller

- Linphone = Encrypted Calls

(Note : Try to aim for forward secrecy encrypting protocols = Meaning in terms of encryption passwords - By never meeting in the same place twice, you secure the other ***Meeting Spots / Password / Encryption*** even if one is already compromised or in simple language wash your hands ever time before you eat - You Know what happens when you are lazy)

Video Caller

- Jitsi = Forward Secrecy Encryption

App Store

- F-Droid

Internet

- Tor Browser = Privacy Focus
- Orbot = Sends Network Traffic / Apps Over Tor Network

Crypto Banking

- Edge
- Exodus

(Note : Smartphone can not be 100% Secure, Always try to aim to move your Crypto-Currency to a Hardware Wallet Device for security, if you can afford to do so and always check the current up to date INFO on the crypt ecosystem / Economy as it is a quickly evolving BEAST / Technology)

This is a basic Lightweight SetUp for Common Folk, as we can't afford PC's and this is TRUTH and if you can get the Top Of The Line Smartphone, Change the OS to GrapheneOS

For those with a Budget you can add additional equipment like Hardware Tools / Lock-picks / Duplicate Device for BackUps and any other useful tools for a Lightweight SetUp - Remember to have FUN and think of it as playing with Patterns, as if you wanted to add Extra Flavor to Grannies Famous Baking Recipes and for all the Orphans this can be your Tech Grannies Recipe

Much Love / Love Thy Self / Love Thy Fellow Human & Make The World A Better Place

A Future We All Share

Middleweight

Portable PC

- Low Budget = Focus on the OS (Operating System) - So PureOS for security & Debian for testing the waters

(Note : Takes time to learn like Learning to Swim / Cook / Ride a Bike or Car)

- Have a Budget to afford secure Hardware - Go with Purism PC or Manjaro - Any Free Hardware Movement Focused PC Manufacture

Additional Software

- Jami = Messenger

- Pidgin = Messanger

- Monero GUI = Crypto-Currency Wallet

- Exodus = Crypto-Currency Wallet

- Bisq - Decentralized Crypto-Currency Exchange Over Tor Network

- Tor Network

- GNUnet

- Jitsi = Video Caller

- OnionShare = WebHosting / File Sharing / Messenger / Over Tor Network

(Note : it's easier and cheaper to re-engineer existing hardware than building from the Ground Up - Remember its a Multi-Generational process, So each plays their part)

If you still have a Budget you can get a Faraday Box of your choice - Faraday Box's can come in the Sizes, from phone bags to full Lounge Sized Room Box's, So you have variety to even Backpacks and any other spy Gadgets you can carry

Heavyweight

Stationary PC - Qubes OS

-Security Focus / High Budget

Server (Prosody / Software) - Communication (Pidgin / Software)

Server (iRedMail / Software) - Email (Mailpile / Software)

If your a Heavyweight Welcome to the Abyss at the bottom of the Rabbit Hole

Please don't forget to have fun or the darkness will consume you - Humanity is what keeps the Torch Of Free Will Lit down here

OK - Now Granny Throws You Into The Pool

SWIM COMRADE, SWIM

Bonus #01

Ubuntu

Website:

Kali

(USB)

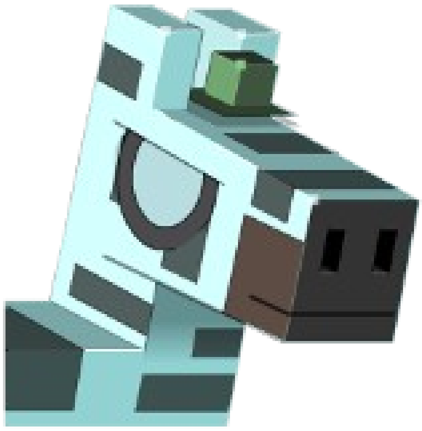
Website:

TailsOS

Website:

Deepin

Website:



SubgraphOS

Website:

Bonus #02

https://empirical4.github.io/

https://mydoge.com/Kyrillos

https://www.luno.com/invite/3AMKR

https://liberapay.com/Woodpecker/

https://deep.edge.app/pay/piratechain/
zs10fzvxfllw86t9aag0fcdhecxtljsxgpqtmrywhs4ed6lg97zs63uw5uz795yvw08202xqxdnglj

https://mad69hatter.github.io/Mercury%20Hgt/index.html

Automated License Plate Readers (ALPRs)

Automated license plate readers (ALPRs) are high-speed, computer-controlled camera systems that are typically mounted on street poles, streetlights, highway overpasses, mobile trailers, or attached to police squad cars. ALPRs automatically capture all license plate numbers that come into view, along with the location, date, and time. The data, which includes photographs of the vehicle and sometimes its driver and passengers, is then uploaded to a central server.

Vendors say that the information collected can be used by police to find out where a plate has been in the past, to determine whether a vehicle was at the scene of a crime, to identify travel patterns, and even to discover vehicles that may be associated with each other. Law enforcement agencies can choose to share their information with thousands of other agencies.

Taken in the aggregate, ALPR data can paint an intimate portrait of a driver’s life and even chill First Amendment protected activity. ALPR technology can be used to target drivers who visit sensitive places such as health centers, immigration clinics, gun shops, union halls, protests, or centers of religious worship.

Drivers have no control over whether their vehicle displays a license plate because the government requires all car, truck, and motorcycle drivers to display license plates in public view. So it’s particularly disturbing that automatic license plate readers are used to track and record the movements of millions of ordinary people, even though the overwhelming majority are not connected to a crime.

Body-Worn Cameras

Unlike many other forms of police technology, body-worn cameras can serve both a law enforcement and a public accountability function. Body cameras worn by police can be useful for documenting police misconduct and use of force, but footage can also be used to surveil both people that police interact with and third parties who might not even realize they are being filmed. If combined with facial recognition or other technologies, thousands of police officers wearing body-worn cameras could record the words, deeds, and locations of much of the population at a given time, raising serious First and Fourth Amendment concerns.

How Body-Worn Cameras Work

Body-worn cameras are small cameras which can be clipped onto a police officer's uniform or worn as a headset and turned on to record video and audio of law enforcement encounters with the public. The video is often saved with time and date stamps and GPS coordinates. Some body cameras offer real-time video streaming. Some cameras offer Bluetooth trigger options for automatic recording. Agencies can select input that triggers body-worn cameras to automatically turn on without manual activation, such as turning on a cruiser's lights or sirens, crash sensor activation, when the car reaches a certain speed, or when nearby dashboard cameras or body cameras are switched on. A new wireless holster sensor can alert body cameras when a gun is drawn. Some body-worn cameras provide 30 seconds of sound-free video footage from before the time the camera officially starts recording. Footage is uploaded to external databases maintained by police agencies or to third party vendors.

Cell-Site Simulators/IMSI Catchers

Cell-site simulators, also known as Stingrays or IMSI catchers, are devices that masquerade as legitimate cell-phone towers, tricking phones within a certain radius into connecting to the device rather than a tower.

Cell-site simulators operate by conducting a general search of all cell phones within the device's radius, in violation of basic constitutional protections. Law enforcement use cell-site simulators to pinpoint the location of phones with greater accuracy than phone companies. Cell-site simulators can also log IMSI numbers (unique identifying numbers) of all of the mobile devices within a given area. Some cell-site simulators may have advanced features allowing law enforcement to intercept communications or even alter the content of communications.

How Cell-Site Simulators Work

Generally, there are two types of device used by law enforcement that are often referred to interchangeably: passive devices (which we will call IMSI catchers), and active devices (which we will call cell-site simulators.) Passive devices, as a rule, do not transmit any signals. They work by plucking cellular transmissions out of the air, the same way an FM radio works. They then decode (and sometimes decrypt) those signals to find the IMSI of the mobile device and track it.

Active cell-site simulators work very differently from their passive cousins. Cellular devices are designed to connect to the cell site nearby with the strongest signal. To exploit this, cell-site simulators broadcast signals that are either stronger than the legitimate cell sites around them, or are made to appear stronger. This causes devices within range to disconnect from their service providers' legitimate cell sites and to instead establish a new connection with the cell-site simulator. Cell-site simulators also have passive capabilities, such as identifying legitimate cell sites and mapping out their coverage areas. For the purposes of this article we will primarily discuss active cell-site simulators.

It is difficult for most people to know whether or not their phone's signals have been accessed by an active cell-site simulator, and it is impossible for anyone to know if their phone's signals have been accessed by a passive IMSI catcher. Apps for identifying the use of cell-site simulators, such as SnoopSnitch, may not be verifiably accurate. Some more advanced tools have been built, which may be more accurate. For instance, security researchers at the University of Washington have designed a system to measure the use of cell-site simulators across Seattle. There are other researchers, including those at EFF, looking into this further.

Face Recognition

Face recognition is a method of identifying or verifying the identity of an individual using their face. Face recognition systems can be used to identify people in photos, video, or in real-time. Law enforcement may also use mobile devices to identify people during police stops.

But face recognition data can be prone to error, which can implicate people for crimes they haven't committed. Facial recognition software is particularly bad at recognizing African Americans and other ethnic minorities, women, and young people, often misidentifying or failing to identify them, disparately impacting certain groups.

Additionally, face recognition has been used to target people engaging in protected speech. In the near future, face recognition technology will likely become more ubiquitous. It may be used to track individuals' movements out in the world like automated license plate readers track vehicles by plate numbers. Real-time face recognition is already being used in other countries and even at sporting events in the United States.

How Face Recognition Works

Face recognition systems use computer algorithms to pick out specific, distinctive details about a person's face. These details, such as distance between the eyes or shape of the chin, are then converted into a mathematical representation and compared to data on other faces collected in a face recognition database. The data about a particular face is often called a face template and is distinct from a photograph because it's designed to only include certain details that can be used to distinguish one face from another.

Some face recognition systems, instead of positively identifying an unknown person, are designed to calculate a probability match score between the unknown person and specific face templates stored in the database. These systems will offer up several potential matches, ranked in order of likelihood of correct identification, instead of just returning a single result.

Face recognition systems vary in their ability to identify people under challenging conditions such as poor lighting, low quality image resolution, and suboptimal angle of view (such as in a photograph taken from above looking down on an unknown person).

When it comes to errors, there are two key concepts to understand:

A "false negative" is when the face recognition system fails to match a person's face to an image that is, in fact, contained in a database. In other words, the system will erroneously return zero results in response to a query.

A "false positive" is when the face recognition system does match a person's face to an image in a database, but that match is actually incorrect. This is when a police officer submits an image of "Joe," but the system erroneously tells the officer that the photo is of "Jack."

When researching a face recognition system, it is important to look closely at the “false positive” rate and the “false negative” rate, since there is almost always a trade-off. For example, if you are using face recognition to unlock your phone, it is better if the system fails to identify you a few times (false negative) than it is for the system to misidentify other people as you and lets those people unlock your phone (false positive). If the result of a misidentification is that an innocent person goes to jail (like a misidentification in a mugshot database), then the system should be designed to have as few false positives as possible.

Tattoo Recognition

Tattoo recognition technology uses images of people’s tattoos to identity them, reveal information about them such as their religion or political beliefs, and associate them with people with similar tattoos. While still in its infancy, the technology is being actively developed by private companies with the support of federal agencies, state law enforcement, and universities. Researchers test and train the technology using photographs of inmates or scraped off social media, raising critical issues of ethics, privacy, and our First Amendment rights. Tattoo recognition is a form of biometric technology in the same category as face recognition, fingerprinting, and iris scanning.

How Tattoo Recognition Works

Tattoo recognition functions in a similar manner as face recognition. Once an image of a tattoo is captured and submitted to the system, image recognition software creates a mathematical representation and analyzes it for specific details and matches those against images already in the database. Humans can also tag these images with metadata to further describe or categorize them.

What Kinds Of Data Are Collected for Tattoo Recognition

Tattoo recognition often captures multiple images of individual’s tattoos and may also capture people’s faces or their entire bodies.

The National Institute on Standards and Technology (NIST) has developed a series of “Best Practices” for capturing images of tattoos for use with tattoo recognition technology, including taking two photographs of each tattoo, one that narrows in on the tattoo itself and another that more clearly shows where tattoos are located on the body. For large tattoos, NIST encourages police to take a full photo of the tattoo in its entirety, followed by photos of particular areas of interest in the tattoo. It is important to note that in detention environments, images of tattoos may be collected from entire body, including areas that would not be publicly visible, such as upper legs, chests, and genital areas.

These tattoos are often tagged with metadata about the tattoo, including position on the body and ink color. The recommended tagging system (ANSI/NIST-ITL Standard) has dozens of codes to categorize the imagery of the tattoo, ranging from general categories such as political symbols and sports icons to very specific images such as a dragon or the American flag.

Law enforcement may also collect images in the field during routine police stops using regular cameras or mobile biometric devices. At least one application in use in Indiana also attaches GPS location data.

In addition, tattoo recognition software may ingest images found online on website or social media.

Iris Recognition

Iris recognition or iris scanning is the process of using visible and near-infrared light to take a high-contrast photograph of a person’s iris. It is a form of biometric technology in the same category as face recognition and fingerprinting.

Advocates of iris scanning technology claim it allows law enforcement officers to compare iris images of suspects with an existing database of images in order to determine or confirm the subject’s identity. They also state that iris scans are quicker and more reliable than fingerprint scans since it is easier for an individual to obscure or alter their fingers than it is to alter their eyes.

Iris scanning raises significant civil liberties and privacy concerns. It may be possible to scan irises from a distance or even on the move, which means that data could be collected surreptitiously, without individuals’ knowledge, let alone consent. There are security concerns as well: if a database of biometric information is stolen or compromised, it is not possible to get a new set of eyes like one would get a reissued credit card number. And iris biometrics are often collected and stored by third-party vendors, which greatly expands this security problem.

How Iris Recognition Works

Iris scanning measures the unique patterns in irises, the colored circles in people’s eyes. Biometric iris recognition scanners work by illuminating the iris with invisible infrared light to pick up unique patterns that are not visible to the naked eye. Iris scanners detect and exclude eyelashes, eyelids, and specular reflections that typically block parts of the iris. The final result is a set of pixels containing only the iris. Next, the pattern of the eye’s lines and colors are analyzed to extract a bit pattern that encodes the information in the iris. This bit pattern is digitized and compared to stored templates in a database for verification (one-to-one template matching) or identification (one-to-many template matching).

Iris scanning cameras may be mounted on a wall or other fixed location, or they may be handheld and portable. Researchers at Carnegie Mellon University are developing long-range scanners that could even be used to capture images surreptitiously from up to 40-feet away.

Surveillance Cameras

Surveillance cameras are one of the most ubiquitous and recognizable technologies used to watch us as we move about our daily lives. Networks of cameras are installed by government agencies and by local businesses, but the distinction blurs with the development of real-time crime centers that access both public and private video feeds. Camera technology is growing in sophistication: some cameras are capable of 360-degree video or infrared vision. Some models can be equipped with real-time face recognition or license plate recognition software. Since many are also being connected directly to the Internet, the camera networks have also proven easy targets for malicious attackers.

Data Sharing

Cameras often broadcast footage over the Internet, allowing operators to monitor security camera feeds remotely. In some cases, surveillance systems are paid for and operated by the cities themselves. But in other cases, residents and businesses share surveillance camera footage with police officers.

Many law enforcement agencies have begun private security camera registration programs (sometimes called "SafeCam"), whereby residents and business owners can provide basic information about the cameras they own and where they are located. Then, when a crime is reported, police may search their database of cameras and contact the owner directly to obtain the footage. Some examples of this program include the Philadelphia Police Department (PA), Fultondale Police Department (AL), and the San Francisco District Attorney's Office (CA). The Phoenix Police Department refers to its program as the "Virtual Block Watch."

In San Francisco, the Union Square Business Improvement District launched an outdoor security camera program in 2012 with just six privately owned cameras. Now it is a surveillance network of 350 cameras, all of which share footage with the police. According to news reports, grant money pays for around 90% of the cost for the cameras in Union Square, and business owners who wish to participate pay the remainder.

Drones/Unmanned Aerial Vehicles

Drones are unmanned aerial vehicles that can be equipped with high definition, live-feed video cameras, thermal infrared video cameras, heat sensors, and radar—all of which allow for sophisticated and persistent surveillance. Drones can record video or still images in daylight or infrared. They can also be equipped with other capabilities, such as cell-phone interception technology, as well as backend software tools like license plate readers, face recognition, and GPS trackers. There have been proposals for law enforcement to attach lethal and non-lethal weapons to drones.

How Drones Work

Drones vary in size, from tiny quadrotors to large fixed aircraft. They are harder to spot than airplane or helicopter surveillance and can sometimes stay in the sky for a longer duration. Some drones are tethered to the ground with a very thin wire so that they do not need to land to recharge their batteries.

Drones are different than manned aircraft because they are generally smaller, less expensive, faster to deploy, and are able to fly at low altitudes and, in some cases, indoors. Some drones are controlled manually through hand-held devices. These usually have a video camera attached to them, not just for surveillance, but for the operator to view through the camera to control the drone. Some drones may also be autonomous in the sense that they can fly and perform certain functions without continuous operator engagement.

Civil agencies often use drones to survey land and monitor animal populations. Many academic institutions acquire drones for educational purposes. Private parties often use drones for recreation, research, and journalism. On some occasions, private individuals have used drones to spy on people through windows.

The technology that can be equipped to a drone is disconcerting, as they are capable of highly advanced and near-constant surveillance.

What Kinds Of Data Drones Collect

Drones can be equipped with various types of surveillance equipment that can collect high definition video and still images day and night. Drones can be equipped with technology allowing them to intercept cell phone calls, determine GPS locations, and gather license plate information. Drones can be used to determine whether individuals are carrying guns. Synthetic-aperture radar can identify changes in the landscape, such as footprints and tire tracks. Some drones are even equipped with facial recognition.

Electronic Monitoring

Electronic monitoring is a form of digital incarceration, often in the form of a wrist bracelet or ankle "shackle" that can monitor a subject's location, and sometimes also their blood alcohol level or breath.

Monitors are commonly used as a condition of pretrial release, or post-conviction supervision, like probation or parole. They are sometimes used as a mechanism for reducing jail and prison populations. Electronic monitoring has also been used to track juveniles, immigrants awaiting legal proceedings, adults in drug rehabilitation programs, and individuals accused or convicted of DUIs or domestic violence.

Typically, people on monitors must charge their devices daily and can't leave their homes without permission, and/or have areas of the city, called exclusion zones, where they're not allowed to visit without triggering an alarm. Some counties require as much as a full week's notice for a schedule change, even in the event of an emergency. Some counties impose installation fees and daily fees for the devices and require users to own a landline phone. If the device disconnects, the monitored person may be incarcerated.

Electronic monitoring has seen a 140 percent increase in just over a decade. About 125,000 devices are in use, with up to 30,000 of them attached to immigrants on any given day. States with the most prolific use of electronic monitoring include Florida, Texas, California, Massachusetts, and Michigan.

Not only does electronic monitoring impose excessive surveillance on people coming home from prison, but it also hinders their ability to successfully transition back into the community. Additionally, there is no concrete evidence that electronic monitoring reduces crime rates or recidivism.

How Electronic Monitoring Works

Electronic monitoring devices typically use active or passive GPS tracking, radio frequency monitoring, secure continuous remote alcohol monitoring, or breathalyzer monitoring.

Active GPS tracking uses satellites to triangulate and transmit location information at set intervals.

Passive GPS tracking tracks and stores location information for download at a later time.

Radio frequency is used for curfew monitoring. A home monitoring unit detects the monitor within a specific range and sends confirmation back to a monitoring center.

Secure Continuous Remote Alcohol Monitoring, or SCRAM, analyzes perspiration to send a blood alcohol content report every hour.

A breathalyzer monitor usually has a camera. It tests a subject's breath at random to estimate their blood alcohol content.

Acoustic Gunshot Detection

Acoustic gunshot detection is a system designed to detect, record, and locate the sound of gun fire and alert law enforcement. The equipment usually takes the form of sensitive microphones and sensors, some of which must always be listening for the sound of gunshots. They are often accompanied by cameras. They are usually mounted on street lights, or other elevated structures, though some mobile and fixed systems operate in both indoor and outdoor settings.

Police and companies that manufacture and sell acoustic gunshot detection systems have claimed that the point of this technology is to inform police of the location of shots fired, more quickly and accurately than relying on witnesses who overheard gun fire and who may call the police. However, we now know that gunshot detection systems can also hear and record human voices¾and police have used these recordings as evidence in court. As is so often the case with police surveillance technologies, a device initially deployed for a less intrusive purpose (here, to report the sound and location of gunshots to police) is now being used for a far more intrusive purposes (to spy on people having conversations within the vicinity of their sensitive microphones).

How Acoustic Gunshot Detection Works

Acoustic gunshot detection relies on a series of sensors, often placed on lamp posts or buildings. If a gunshot is fired, the sensors detect the specific acoustic signature of a gunshot and send the exact time and location to the police. Location is determined by measuring the amount of time it takes for the sound to reach sensors in different locations.

According to ShotSpotter, the largest vendor of acoustic gunshot technology, this information is then verified by acoustic experts to confirm the sound is gunfire, and not a car backfire, fire crackers, or other sounds that could be mistaken for gun shots. The sensors themselves can only determine whether there is a loud noise that somewhat resembles a gunshot. It’s still up to people, sitting and listening on headphones, to say whether or not shots were fired.

With microphones running and recording during the moments that it captures any sounds resembling gunshots, acoustic gunshot detection also records other sounds, including human voices, that occur within the vicinity of its microphones during a suspected shooting incident.

XMR :

84oJbjf1VCCDGjXeHvrvLhhj94ji4TQNC1i7NQ2vn3yvHU5GkG4gw1cd4mwoJvo6wSJpmCGryvwYRVe3QsLcABjb15g93xW

Drums Of Liberation