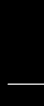


Snoop unto them
as they snoop unto us



Yo!

- Alan Meekins
 - nullagent
 - Aka: sevenbitbyte
 - <https://www.nullagent.com>
- Co-Speakers
 - [rekcahdam](#)
 - 5@V@g3



About - nullagent

- Robotics Clouds
- Embedded Systems
- Linux
- Digital Communications
- Previous Work:
 - Microsoft FTE
 - Disney
 - Walmart
 - European Space Agency
 - Oil & Gas
- Founder of Dataparty



<https://dataparty.xyz>

No Knock Raids



Jose Guerena
(2011)



Matthew
Stewart(2011)

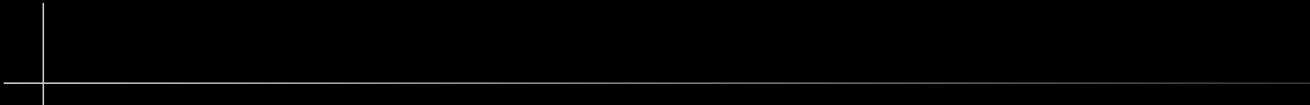


Breonna Taylor
(2017)



Jason Kloepper
(2022)

WWLND



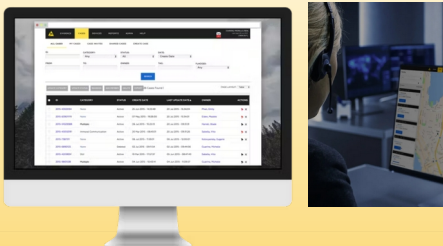


WWLND

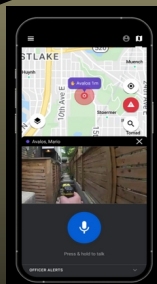
What Would Lord Nikon Do



The boys in blue?



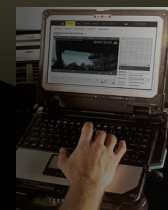
Evidence.com



"Drone as first responder"



**READ PLATES +
IDENTIFY VEHICLES**



"[Bi-directional communications] is a lot faster than to have to stop what I am doing, to key up on my radio."



- 5. Tap **Axon Signal Unit** in the device list.
- 6. Place the phone near an enabled Axon Signal Vehicle device and tap **Start Scan**. Select the device from the list of available devices and tap **Connect**. This will initiate the Bluetooth pairing of the device to the phone.
- 7. If the Axon Signal Vehicle device's firmware is out-of-date, an update will automatically begin after pairing. The update can be monitored by the progress bar at the top.

Axon Signal

Axon Signal technology is included with the Axon Fleet system. However, your agency's administrator must activate the Axon Signal capability for it to work. When it is active, Axon Signal technology can take your Axon Fleet system from BUFFERING to EVENT mode.

Emergency vehicles can be equipped with an Axon Signal Vehicle unit. With light bar activation, or other triggers, the Axon Signal Vehicle unit sends a signal to your Axon Fleet system. Upon receiving this signal, your Axon camera transitions from BUFFERING to EVENT mode. When your

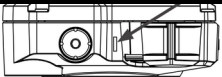
Chapter 3: Recording with the Axon Fleet System | 10

Axon Fleet Camera System User Manual

camera starts recording, you will hear 2 beeps.

The Axon Signal Vehicle unit has a range of approximately 30 feet (9.1 meters).

Cradlepoint and NetCloud are trademarks of Cradlepoint, Inc.



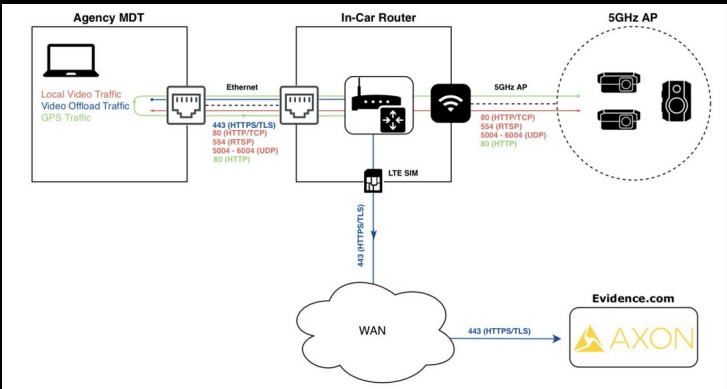
Function Enabled	Function LED
Mute	Blinking blue
Camera error*	Solid red
Bluetooth feature is booting up	Solid blue

* Use the ON/OFF switch to turn the camera OFF and ON.

Upload Status LED

Indicates when the camera is uploading data to the Evidence.com website wirelessly or via the Axon Dock.

Upload Status LED



RTFM

5. Tap **Axon Signal Unit** in the device list.

6. Network Requirements

When used in online mode, Evidence Sync requires that you have implemented network-based controls to restrict access to Axon Cloud Services unless specified domains listed below are accessible on Port 443. This is commonly called "whitelisting."

- *.evidence.com
- sync.evidence.com
- *.mixpanel.com
- mxpnl.com

Chapter 3: Recording with the Axon Signal Unit

Chapter 3: Recording with the

Tips when Signing In to Evidence Sync

- When asked to enter your agency to sign in, use the Evidence.com sub-domain as the agency name. When you go to Evidence.com for your agency, you can see the sub-domain in your web browser's address bar.

Example: If the Evidence.com URL for your agency is:

`https://youragencyname.evidence.com`, then your sub-domain is youragencyname.

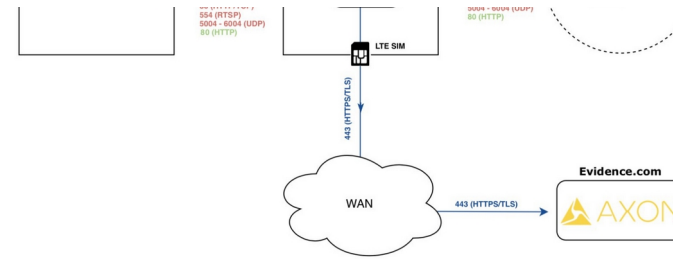


Page 9 of 81

Axon Fleet Camera System User Manual

camera starts recording, you will hear 2 beeps.

The Axon Signal Vehicle unit has a range of approximately 30 feet (9.1 meters).



RTFM

5. Tap **Axon Signal Unit** in the device list.

6. Network Requirements

When used in online mode, Evidence Sync require have implemented network-based controls to r connecting with Axon Cloud Services unless spe domains listed below are accessible on Port 44: Services. This is commonly called “whitelisting.”

- *.evidence.com
- sync.evidence.com
- *.mixpanel.com
- mxpnl.com

receiving the signal, your Axon camera transitions from DCH to ECH

Chapter 3: Recording with th

Axon Fleet Camer

camera starts recording, you will hear 2 beeps.

The Axon Signal Vehicle unit has a range of approximately 30 feet (9.1 meters).

7. Axon Interview Log4J Vulnerability

On December 9, 2021 there was a Remote Code Execution (RCE) vulnerability discovered in the Java logging library log4j given [CVE-2021-44228](#). The RCE is triggered by Java-based applications logging the exploit string and executing a remote payload that the string is pointing to. This vulnerability leaves any server hosting an unpatched java application vulnerable to exploitation.

On December 10, 2021 Axon identified that a service dependency utilized by Axon Interview for streaming services (Wowza) utilized a vulnerable version of the log4j library. This applies to all Axon Interview versions between 4.5.2 and 4.7.9.2 (Note: The affected versions information was updated, because v4.3.0 is not affected). Axon has worked with Wowza to create a batch file to update the affected Wowza components of Axon Interview to mitigate the disclosed vulnerabilities.

Axon recommends that you download the updatelog4j.bat-v1.3 batch file, from the link provided below, and run the batch file is through PowerShell (in admin mode), as shown in the image below, on all servers with Axon Interview version between 4.5.2 – 4.7.9.2. The batch file will perform prerequisite checks and replace the vulnerable log4j files as necessary. At this time, Axon does not anticipate recommending additional action.

Important: If you downloaded the batch file before January 12, 2022, you must download and apply the new updatelog4j.bat-v1.3 batch file.

Note: You will not be able to use Axon Interview during the update process. The update will stop all in-progress Axon Interview sessions. Ensure there are no ongoing sessions before running the batch file. During the update, the batch file will stop your Axon Interview service and then restart the service after the update is complete.

```
Administrator: Windows PowerShell
PS C:\Users\mjoshi\Downloads\updatelog4j-v1.3> .\updatelog4j.bat

Log4j Updater v1.3

Verifying running as administrative user
Administrative privileges were provided

Checking if Axon Interview Server service if running
Stopping Axon Interview Server service; this might take a while . . . Please wait
Axon Interview Server service is stopped

Checking if Wowza Streaming Engine Manager service if running
Service Name: WowzaStreamingEngineManager4816+1
```

NetCloud are trademarks of Cradlepoint, Inc.

-domain as
can see the

ub-domain

Page 9 of 81



RTFM

5. Tap **Axon Signal Unit** in the device list.

6. Network Requirements

When used in online mode, Evidence Sync requires have implemented network-based controls to r connecting with Axon Cloud Services unless spe domains listed below are accessible on Port 44: Services. This is commonly called “whitelisting.”

- *.evidence.com
- sync.evidence.com

Axon
istral
tech

7. Axon Interview Log4J Vulnerability

On December 9, 2021 there was a Remote Code Execution (RCE) vulnerability discovered in the Java logging library log4j given [CVE-2021-44228](#). The RCE is triggered by Java-based applications logging the exploit string and executing a remote payload that the string is pointing to. This vulnerability leaves any server hosting an unpatched java application vulnerable to exploitation.

On December 10, 2021 Axon identified that a service dependency utilized by Axon Interview for streaming services (Wowza) utilized a vulnerable version of the log4j library. This applies to all Axon Interview versions between 4.5.2 and 4.7.9.2 (Note: The affected versions information was updated, because v4.3.0 is not affected). Axon has worked with Wowza to create a batch file to update the affected Wowza components of Axon Interview to mitigate the disclosed vulnerabilities.

Axon recommends that you download the `updateLog4j.bat-v1.3` batch file, from the link provided below, and run the batch file is through PowerShell (in admin mode), as shown in the image below, on all servers with Axon Interview version between 4.5.2 – 4.7.9.2. The batch file will perform prerequisite checks and replace the vulnerable log4j files as necessary. At this time, Axon does not anticipate recommending additional action.

Important: If you downloaded the batch file before January 12, 2022, you must download and apply the new `updateLog4j.bat-v1.3` batch file.

NetCloud are trademarks of Cradlepoint, Inc.

-domain as
can see the

ub-domain

plan or prefer not to offload non-prioritized video via cellular data.

- SSID naming convention. Axon recommends using *VehicleNumber_5G* (for example: 535_5G)

}1

Axon Fleet Camer

camera starts recording, you will hear 2 beeps.

The Axon Signal Vehicle unit has a range of approximately 30 feet (9.1 meters).

```
Checking if Axon Interview Server service if running
Stopping Axon Interview Server service; this might take a while . . . Please wait
Axon Interview Server service is stopped
```

```
Checking if Wowza Streaming Engine Manager service if running
Service Name: WowzaStreamingEngineManager4816+1
```



RTFM

5. Tap **Axon Signal Unit** in the device list.

6. **Network Requirements**

When used in online mode, Evidence Sync requires the device to have implemented network-based controls to connect to the Axon Cloud Services platform.

7. **Axon Interview Log4J Vulnerability**

On December 9, 2021 there was a Remote Code Execution (RCE) vulnerability discovered in the Java logging library log4j given [CVE-2021-44228](#). The RCE is triggered by Java-based applications logging the exploit string and executing a remote payload that the string is pointing to. This vulnerability leaves any server or application using log4j vulnerable to RCE.

NetCloud are trademarks of Cradlepoint, Inc.

Axon Fleet 2 is a video solution that connects police vehicles to an intelligent, cloud-based evidence ecosystem. Axon Fleet 2 allows agencies to access and analyze in-car video. The cameras are mounted in the car, where they can be activated using Axon Signal technology, through the in-car computer using the Axon View XL application, or manually with the on-camera button. The cameras then communicate with the Axon View XL application and can offload video wirelessly through LTE or Wi-Fi technology to the Evidence.com website.

camera starts recording, you will hear 2 beeps.

The Axon Signal Vehicle unit has a range of approximately 30 feet (9.1 meters).

```
Stopping Axon Interview Server service; this might take a while . . . Please wait
Axon Interview Server service is stopped

Checking if Wowza Streaming Engine Manager service if running
Service Name: WowzaStreamingEngineManager4816+1
```



RTFM



PRODUCTS / CAMERAS

AXON SIGNAL SIDEARM

Capture vital footage without lifting a finger

[CONTACT US](#)

The boys in BLE

Hack the Planet

- "Basics of Breaking BLE"
 - Freqy (@FreqyXin, DC29)
- "Handoff All Your Privacy"
 - Jeremy Martin et al. (2019)
- "You better secure your BLE devices"
 - Damien Cauquil (@virtualabs, DC26)
- "I know what you did last summer"
 - Mike Spicer (@d4rkm4tter, DC27)



What's in a BLE broadcast?

- MAC Address
- Manufacturer Data
- Services
- Product
- Company
- Localname
- RSSI
- URI
- Additional GAP fields

Determining Fingerprint

- Custom GAP parsing
- Wigle'd
 - wigle.net
- Built rfparty.xyz
 - Open Source
- Decompiled Apps

5. Tap **Axon Signal Unit** in the device list.
6. Place the phone near an enabled Axon Signal Vehicle device and tap **Start Scan**. Select the device from the list of available devices and tap **Connect**. This will initiate the Bluetooth pairing of the device to the phone.
7. If the Axon Signal Vehicle device's firmware is out-of-date, an update will automatically begin after pairing. The update can be monitored by the progress bar at the top.

Axon Signal

...cluded with the Axon Fleet system. However, your agency's administrator must activate the Axon Signal capability for it to work. When it is active, Axon Signal technology can take your Axon Fleet system from BUFFERING to EVENT mode.

Emergency vehicles can be equipped with an Axon Signal Vehicle unit. With light bar activation, or other triggers, the Axon Signal Vehicle unit sends a signal to your Axon Fleet system. Upon receiving this signal, your Axon camera transitions from BUFFERING to EVENT mode. When your

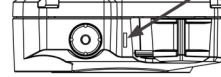
Chapter 3: Recording with the Axon Fleet System | 10

Axon Fleet Camera System User Manual

camera starts recording, you will hear 2 beeps.

The Axon Signal Vehicle unit has a range of approximately 30 feet (9.1 meters).

Cradlepoint and NetCloud are trademarks of Cradlepoint, Inc.



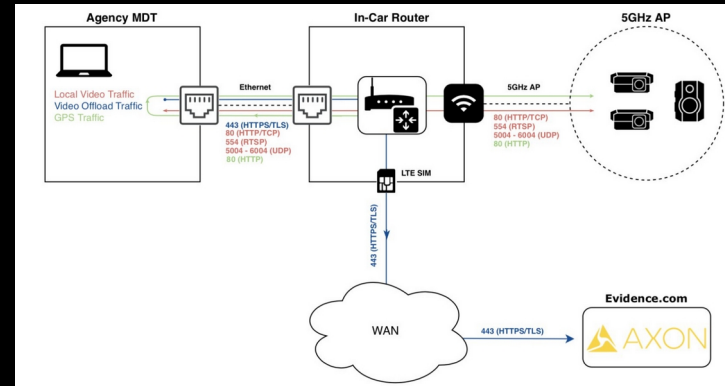
Function Enabled	Function LED
Mute	Blinking blue
Camera error*	Solid red
Bluetooth feature is booting up	Solid blue

* Use the ON/OFF switch to turn the camera OFF and ON.

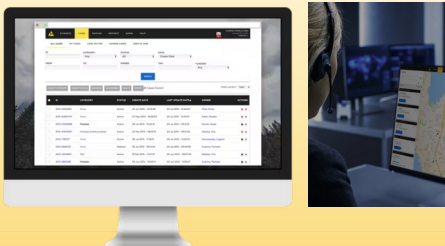
Upload Status LED

Indicates when the camera is uploading data to the Evidence.com website wirelessly or via the Axon Dock.

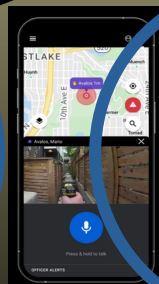
Upload Status LED



RTFM



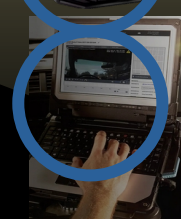
Evidence.com



"Drone as first responder"



**READ PLATES +
IDENTIFY VEHICLES**



"[Bi-directional communications] is a lot faster than to have to stop what I am doing, to key up on my radio."

What is Axon Signal?

- Architecture
- Devices it is deployed on
- How it works
- Where is it used?

RTFM - OUI

- 00:25:DF
- Registered 2010
- Taser International Inc.
- Block size 2^{24}
 - 16 Million

Taser International Inc.

VendorDetailsHistory 4

 OUI: 00:25:DF

 Vendor name: [Taser International Inc.](#) 

 Address:

17800 N 85th St.
Scottsdale AZ 85255
US.

 Assignment Type MA-L

Mac Address Block Large (previously named OUI). Number of address 2^{24} (~16 Million)

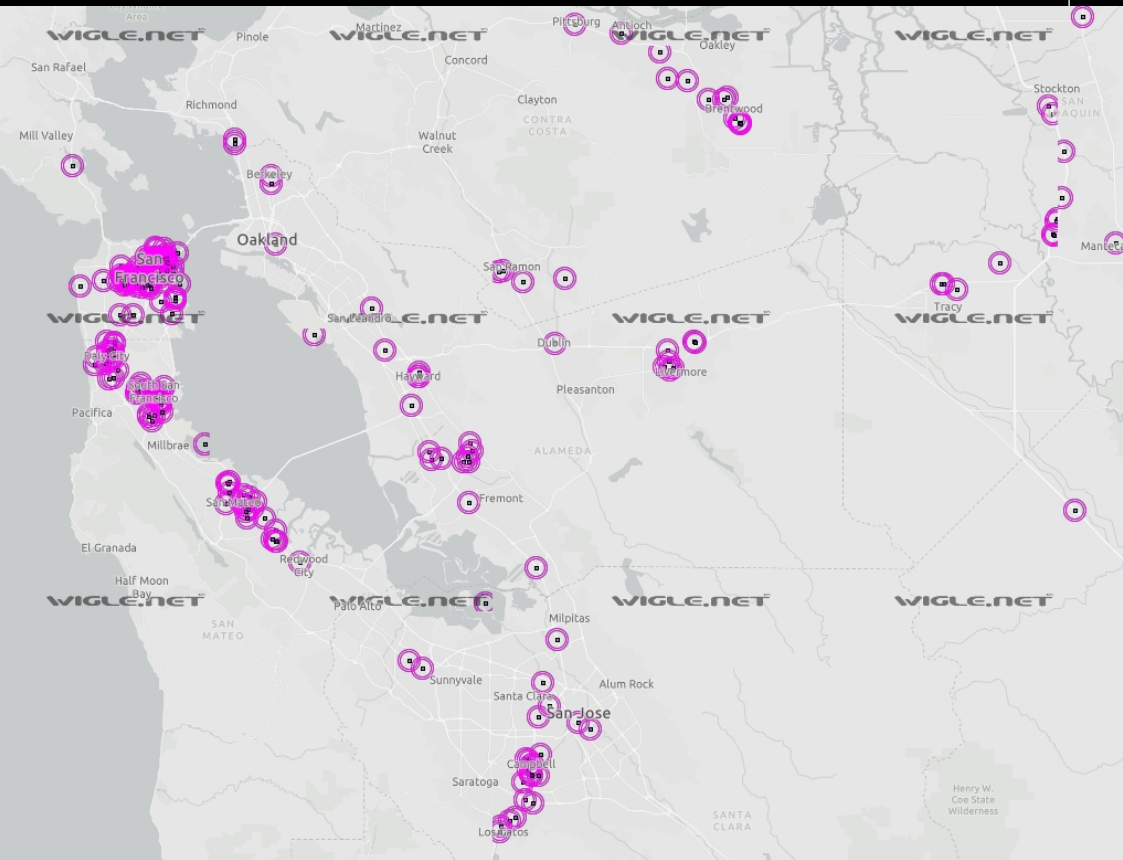
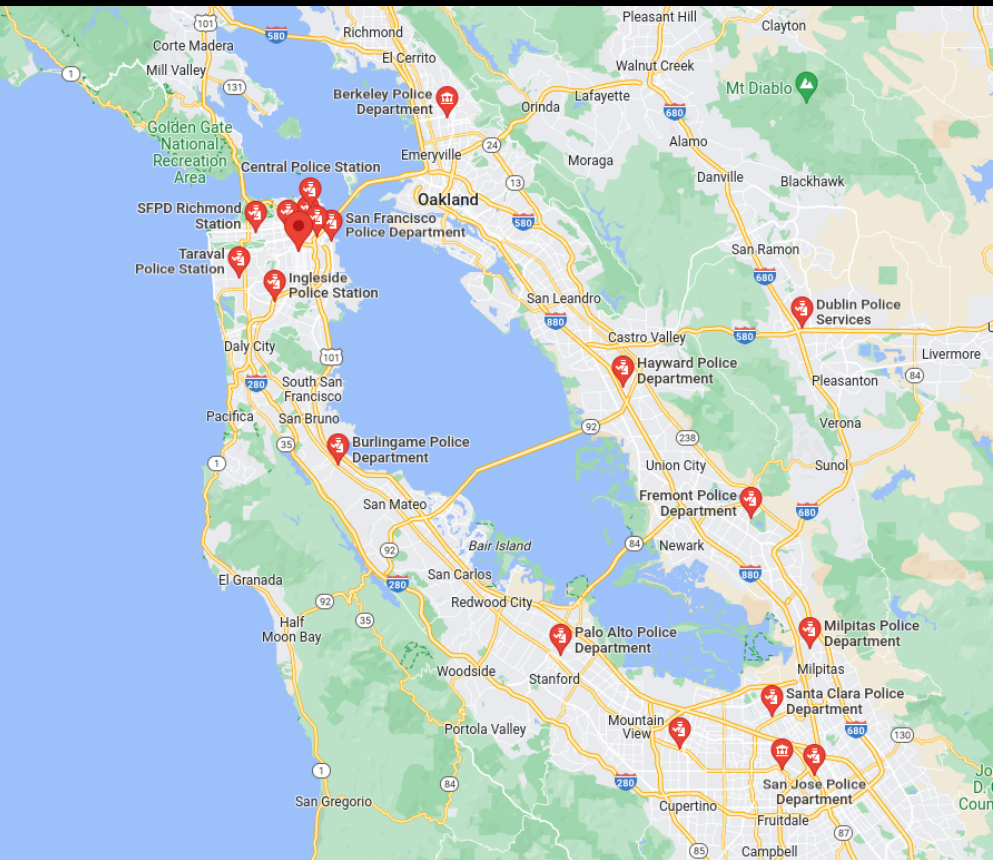
 Last updated: 14 May 2022

 Initial registration: 05 January 2010

Prevalent broadcast protocols

- COVID exposure tracking
- Apple continuity
- DroneID
- Axon Signal

Demo - Wigle



RFPARTY



What does this enable?

- Axon Signal
 - Proof of Body Cam
 - Cop Alert
 - Identify Specific Cops
 - Body Cam Prevalence
- rfparty
 - Product Market Research
 - BLE Vulnerability Alerts
 - Devices following you

Tools

- PDF Viewer
- OUI Database
 - maclookup.app
 - ouilookup.com
- Wigle.net
- nRF Connect
- rfparty.xyz
 - Android
 - Mac, Linux, Windows
 - Open Hardware coming soon!

Party On!

<https://blog.dataparty.xyz/snoop-onto-them>
