Police Citizens Advisory Committee
Body Camera Ordinance Recommendation

After careful consideration and discussion, the Police Community Advisory Committee has drafted the following statements regarding the Fort Pierce Police Department (FPPD) and the policy for Body Worn Cameras (BWC)

1. Committee agreed that the policy for BWC's was comprehensive and included necessary disciplinary action for non-compliance.

2. Committee does not believe any further disciplinary action is necessary for non-compliance as it is already included in the policy.

3. Supervisors conduct monthly random audits of the footage on the BWC system to assure officers are acted properly and is following policy. On top of that, these audits are reviewed by a Quality Assurance Manager to confirm the actions of previous reviews.

4. Attached is the statement from Axon that the BWC cannot be compromised in any way by an officer. All information on the camera remains on the camera.

5. The passage of an ordinance to arrest officers for failure to download their BWC immediately after the end of shift will further erode morale amongst officers at this very difficult time. There is no other police agency in Florida that has this provision.

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

Axon Body Worn Video: Data Integrity and Authenticity

April 2020

Axon holds the integrity and authenticity of the data captured with its body worn cameras (BWCs) and transmitted to Axon Evidence as a high priority. Measures are in place at each stage of the process to ensure that the data recorded is the same data transmitted to Axon Evidence, and that same data is available for replay and/or download.

Axon BWCs – Data Integrity:
Axon BWCs are designed and built to meet the needs of the public safety community and undergo strict security analysis and assessments during the development process. In order to protect the integrity of the data on the camera, safeguards are in place to limit non-authorized access to the camera and its data. The BWC hardware is rugged, designed to meet the US Department of Defense environmental standard MIL-STD-810G, and are IEC 60529 rated for water and dust ingress. During production, they are configured in Axon facilities with up-to-date firmware and physical tampering protection. Data is stored on a solid-state, embedded MultiMediaCard (eMMC) integrated circuit, ball-grid-array (BGA) soldered onto the main circuit board – easily removable storage media is not used. Any firmware updates to the device in the field are done automatically during charging and data transfer via the Axon Dock; no human intervention is needed to ensure that the latest fixes and security updates are installed.

Wireless pairing (using Bluetooth or WiFi technology) requires simultaneous physical button presses. Due to known limitations in Bluetooth LE pairing security, Axon Cameras and Axon View (a client mobile application which does not allow modification of recorded data) contain additional application-level security pairing to protect against eavesdropping attacks. On initial connection over Bluetooth LE, the Axon Camera, Axon View or View XL apps exchange cryptographic keys using the Elliptic-curve Diffie-Hellman key exchange protocol. Axon Cameras use the Advanced Encryption Standard (AES), a standard adopted by the US government, to derive 256-bit session keys and establish an encrypted session for subsequent Bluetooth communication. WiFi connections create a secure network with a unique non-broadcasted services set identifier (SSID) secured via Wi-Fi Protected Access version 2 with a Pre-Shared Key (WPA2-PSK). A passphrase is generated on the camera to be entered on the paired device.

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

Data sent to Axon Evidence is encrypted during transfer using encryption that meets industry standards – Federal Information Processing Standard (FIPS 140-2), validated Transport Layer Security (TLS) 1.2 (256-bit AES, RSA 2048 bit key), and Perfect Forward Secrecy (PFS).

Axon Body 3 (AB3) Cameras - Enhanced Security:

Axon Body 3 cameras have additional protections that establish not only integrity of the data on the device, but also provide assurance that the data is from a verified and specific Axon device. Data on an AB3 device is encrypted using the XTS-AES mode of the Advanced Encryption Standard with a 128-bit key, a full disk encryption method which protects against unauthorized manipulation of the encrypted data. Encrypting the data on the device is an added layer or protection to minimize the possibility of data extraction or data manipulation before being transferred to Axon Evidence.

Each AB3 camera contains a cryptographic certificate for each individual device stored in a dedicated hardware 'trustzone' on the device. This certificate is generated inside the trustzone on the device, signed in the Axon factory premises during manufacturing, and chained to the Axon root certificate. Therefore, only Axon applications that are also chained to the Axon root can authenticate the individual identity of each Axon camera. This ensures that AB3 cameras boot securely from Axon-signed firmware, and critical incoming commands including evidence deletion are verified to be coming from a trusted Axon source.

During upload, video files are parsed and verified to be identical to the copy created on the camera. At the completion of the upload process, the digital signature is verified to ensure an exact copy of the file has been successfully transmitted and the camera is instructed to delete the successfully uploaded file through signed commands. In the event of a disconnect or interruption in transmission, uploads will resume where they last left off.

Axon Evidence: SHA-2 Usage

Axon Evidence uses Secure Hashing Algorithm 2 (SHA-2), created by the United States National Security Agency (NSA), as a tool to authenticate copies of specific digital evidence. Specifically, Axon uses SHA-256, which is calculated using the data within the file and outputs a 64-character string that is specific to that file. The SHA-2 value

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

is a "fingerprint" of the digital file. If any data within the file (not including the filename) were to change, then the SHA-2 value would also change. For example, if a single pixel of a single frame of a video file were to be changed and saved, the new file will have a different SHA-2 value than the original. And with that fact, we know that if 2 files have the same SHA-2 value, then we can guarantee the 2 files are identical, bit-for-bit (again, not including the filename).

When an Axon BWC recording is successfully uploaded to Axon Evidence, the system calculates and stores the SHA-2 value. This value is located on the Evidence Audit Trail for the video. Because the original file is always unchanged on Axon Evidence, all downloads of the file are simply identical copies. If the SHA-2 value of a copy of the file matches the original value on the Evidence Audit Trail, it is guaranteed that the copy is identical to the original. Audit trails are highly resistant to tampering and are stored in a secure database; they can be viewed, in a read-only format, by agency users with the appropriate permissions within Axon Evidence. Audit trails include system and user activity and interactions with the evidence file, and each log entry record is accompanied by a timestamp.

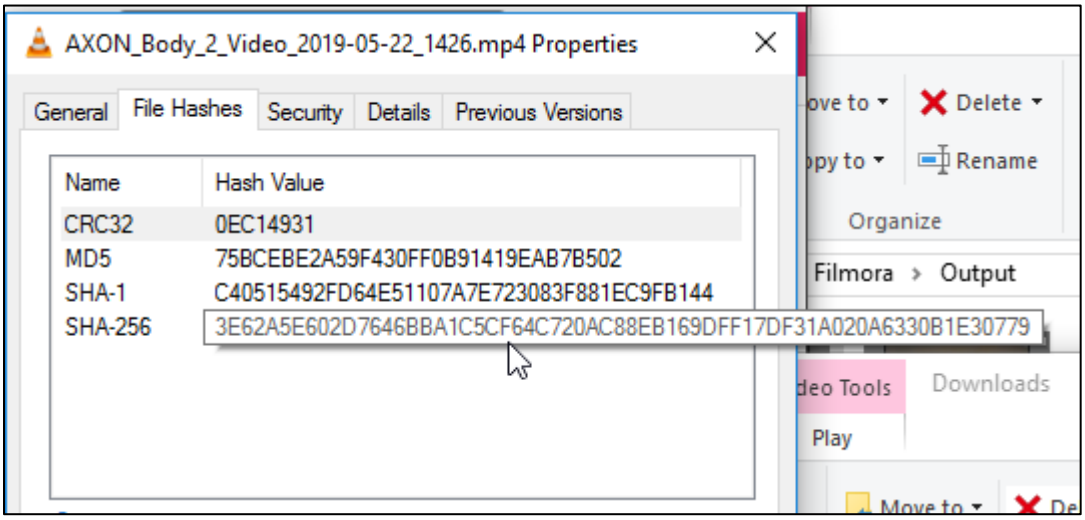
The video file contents of an Axon BWC configured for use with Axon Evidence cannot be accessed for editing, deletion, or any type of altering by the user. Users only have access to view the video or add annotation via app, neither of which changes any data contained within the file. For this reason, SHA-2 comparison is a preferred method to determine the authenticity of an Axon BWC video. When doing a comparison, there are multiple software solutions available that can calculate the SHA-2 hash of a file, but for this demonstration, we use Implbits® Hashtab™ (http://implbits.com/products/hashtab/).

There are 2 ways to compare using Hashtab:

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

METHOD 1: Open the properties of the file, select the “file hashes” tab, select the SHA-256 Hash, and visually compare it to the Audit Trail:



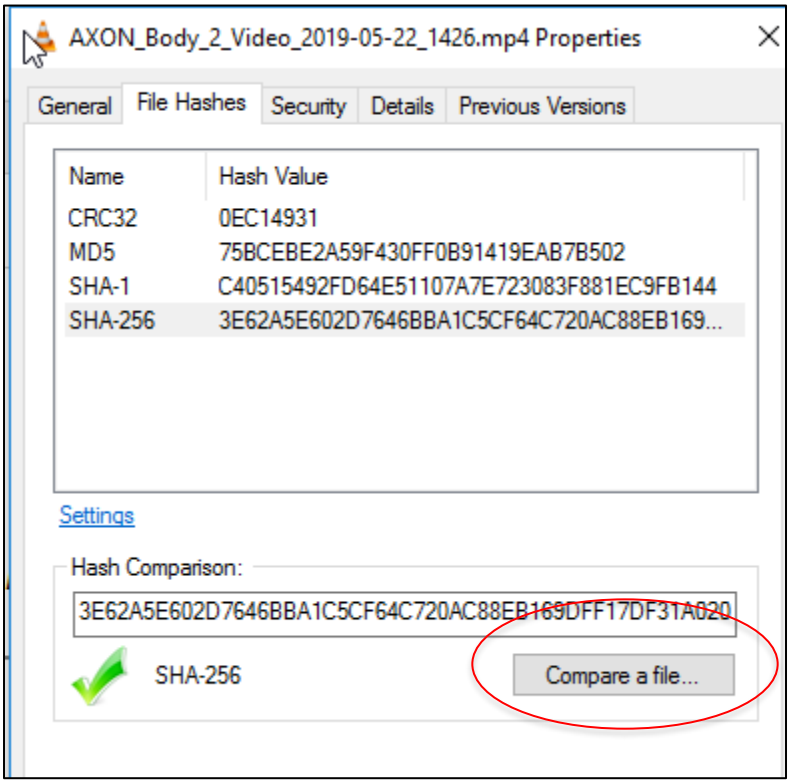
EVIDENCE AUDIT TRAIL

Evidence	
Evidence ID	
Categories	
Title	AXON Body 2 Video 2019-05-22 1426
CheckSum	Sha2-3e62a5e602d7646bba1c5cf64c720ac88eb169dff17df31a020a6330b1e30779

17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

METHOD 2: Compare the copy to the original file (if both files are available on the computer) using HashTab:



As mentioned above, when the SHA-256 value calculated by Hashtab matches exactly to the SHA-2 listed on the Audit Trail, this means they are identical, bit for bit. If the values do not match, it simply means that something in the file has changed. Investigation into what changed and why is then needed. Only a thorough investigation can conclude whether video content has been altered or not.