FVU Request System - Introduction and Overview

Background

The Forensic Video Unit, embedded within the Homicide and Missing Persons Bureau, required an automated request form submission and ticketing system to enhance operational efficiency. While the system effectively tracks requests, keeps investigators informed of status updates, and provides management with progress metrics, the third-party ticketing provider could not accommodate the specialized field requirements unique to forensic video evidence handling.

The Challenge

The third-party ticketing system was designed for general use cases and lacked the flexibility to incorporate the specific data fields required by the Forensic Video Unit. With the provider unable to develop a custom solution, an innovative approach was necessary.

The Solution

A static HTML/JavaScript application was developed consisting of:

Landing Page

- Central hub where investigators select the appropriate request type
- Clear navigation to three specialized forms

Three Request Forms

1. **Analysis Request Form**

   - For in-office forensic analysis of previously recovered video evidence
   - Used when evidence is already in possession

2. **Upload Request Form**

   - For uploading video evidence to the secure server
   - The unit serves as the sole conduit between investigators and read-only server storage
   - Maintains evidence integrity through controlled access

3. **Recovery Request Form**

   - For on-scene CCTV recovery assistance
   - Investigators request Forensic Video Unit support for retrieving evidence from community DVR systems

Technical Implementation

Integration Architecture

The third-party developer provided an elegant integration solution:

- SFTP access to their system for file deployment
- Static application files uploaded via SFTP
- Forms served to end users through their existing system
- On submission:
    - Required form fields transmitted to ticketing system
    - PDF generated client-side for disclosure requirements
    - JSON document created for downstream efficiency applications

Client-Side Processing

- All data processing occurs in the user's browser
- No data storage within the application
- SFTP serves only static form files
- Complete security isolation from sensitive data

Deployment Considerations

Location Options for SFTP

1. **Standalone Internet Connection** (Ideal Solution)

    - **Advantage**: If server space available on the standalone network
    - **Benefit**: Complete isolation from corporate network
    - **Access**: Developer maintenance capability maintained

2. **Cloud Instance**

    - **Advantage**: Full developer control and maintenance access
    - **Consideration**: Additional integration complexity
    - **Benefit**: Professional hosting environment

Security Overview

The application presents no security concerns due to its architecture:

- Client-side processing only
- No data persistence
- Static file serving via SFTP
- Complete isolation from sensitive information

Documentation Scope

The following documentation provides:

- Comprehensive application details
- Security assessment of the SFTP solution
- Technical implementation specifications
- Integration requirements

Note: This documentation addresses security up to the point of third-party system integration. No affirmations are made regarding data security within the third-party system itself.