CASECRACKER
by Cardinal Peak

CaseCracker Onyx Overview
Interview Recording Management System (IRMS)

Prepared for:

Prepared by:
Cardinal Peak Technologies

May 2017

This white paper contains confidential and proprietary information of Cardinal Peak Technologies.

Company Overview

Cardinal Peak Technologies is the developer of the CaseCracker Interview Management System, the industry-leading solution for recording of custodial interrogations for law enforcement. CaseCracker has been adopted by over 1300 agencies and locations worldwide, including local police and sheriff departments, state agencies, and several large Federal agencies such as US Naval Criminal Investigative Service, US Coast Guard Investigative Service, US Air Force Office of Special Investigations and the US Army Criminal Investigation Command.

Cardinal Peak is structured as two LLCs under common ownership, with combined gross revenue of over $17M in 2016. The sister company of Cardinal Peak Technologies, Cardinal Peak LLC, is a 65-person R&D engineering services company that develops video and "internet-of-things" products for customers such as Pelco/Schneider Electric, Ball Aerospace, the US Navy, VBrick, Samsung, Qualcomm, Echostar, DirecTV, Comcast, and Time Warner Cable.

Both Cardinal Peak companies have deep video engineering expertise. Cardinal Peak has designed numerous video products for security, military, and entertainment applications. Cardinal Peak's two founders, Mike Perkins, Ph.D., and Howdy Pierce, are well known in the video industry, with engineering experience dating back to the early 1990s. Dr. Perkins was a key member of the committee that drafted the MPEG-2 video compression standard, and Mr. Pierce did early work designing the digital video networks used by DISH Networks, DirecTV, and other digital cable operators.

Past Performance and Product History

Within a few years of its 2003 introduction, CaseCracker was granted sole source justification as the interview recording solution for Naval Criminal Investigative Service (NCIS) after an extensive pilot test of various solutions on the market. NCIS has been very pleased with the performance of the solution and is in the process of refreshing all aged systems. Shortly after the first unit shipped to an NCIS location, Army CID selected CaseCracker and just recently mandated that previously-purchased competitive products be replaced with CaseCracker as they age out of use. To date, Army CID is our largest agency, with over 460 CaseCracker systems in use.

The current CaseCracker solution was originally developed to support state and local law enforcement agencies that often operate in a cost-constrained budgetary environment with little to no IT support and a historically poor networking infrastructure. These criteria initially made CaseCracker a desirable choice: No network connection was required for operation, and each CaseCracker appliance would reliably and securely record and store sensitive interrogations. Over time, certain networking features were added to CaseCracker, including the ability to view and search both live interviews and stored recordings over the local area network, but the product is still fundamentally appliance-focused.

In recent years, the network infrastructure of law enforcement agencies has dramatically improved, making it possible to envision a central online repository for all interview recordings and thus eliminate the need for evidentiary DVDs. Simultaneously we see increasing demand for mobile recording solutions based on smartphones and tablets.

As a result of these trends, in late 2014 we began planning a next-generation, network-based offering: CaseCracker Onyx. Based on face-to-face feedback from our other large customers, CaseCracker Onyx is targeted squarely at enterprise law enforcement agencies, which have multiple locations, large numbers of users, and demanding requirements for security and reliability. The first release of CaseCracker Onyx is planned for release in the spring of 2017. The remainder of this document provides a product overview. We would welcome the opportunity to answer your questions or discuss the product in more detail interactively.

Solution Synopsis

CaseCracker Onyx is an enterprise-class, network-based interview management system designed for larger law enforcement agencies such as the FBI, the DEA, and larger state and metropolitan police departments. CaseCracker Onyx is:

- Network-based: The system is based around a "headless" server, which performs recording, secure hashing, indexing, storage, and streaming. All cameras, mics, switches, etc., connect to the server over a secure isolated network. In a

similar manner, the user interface into the system is from a client application over the network.

- Distributed: Multiple CaseCracker Onyx servers in different locations will eventually communicate with each other and perform distributed searching (if the system is network connected).

- Robust: The system is built with numerous redundancies throughout, so no single point of failure exists that could stop the ability to record new content or access previously stored content.

A conceptual view of the system for one site is shown in Figure 1, below:

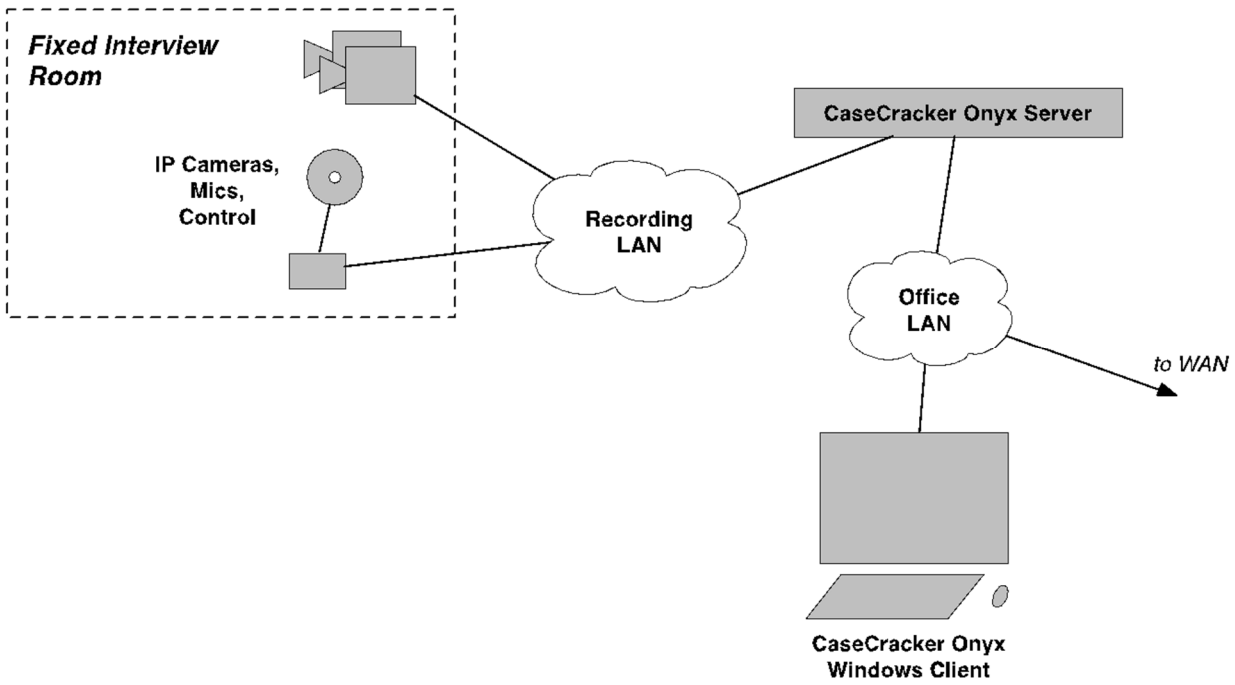

Fig. 1: Conceptual View of one station's interview room

Video recorded from a fixed interview room enters the system in the upper left corner. Although only one room is shown in the figure, up to 16 rooms can be supported based on the server size and configuration for each location. We will describe this room in greater detail below; for now, it is connected over a private LAN to a **CaseCracker Onyx Server**. This server forms the heart of the system, and performs recording, secure hashing, indexing, storage, and streaming.

Users interact with the system through the **CaseCracker Onyx Client**, shown in the lower right of Figure 1. This is a Windows application that allows users (based on authorization level) to view live video and audio, review recorded content, add and edit metadata, search, export, and import recordings.

The subsequent sections below give additional details on how the CaseCracker Onyx system works.

Fixed Interview Room Equipment

A fixed interview room is shown in the upper left corner of Fig. 1. Although there are many options for configuration of the interview room, a high redundancy configuration—which we recommend—is shown in greater detail in Fig. 2:

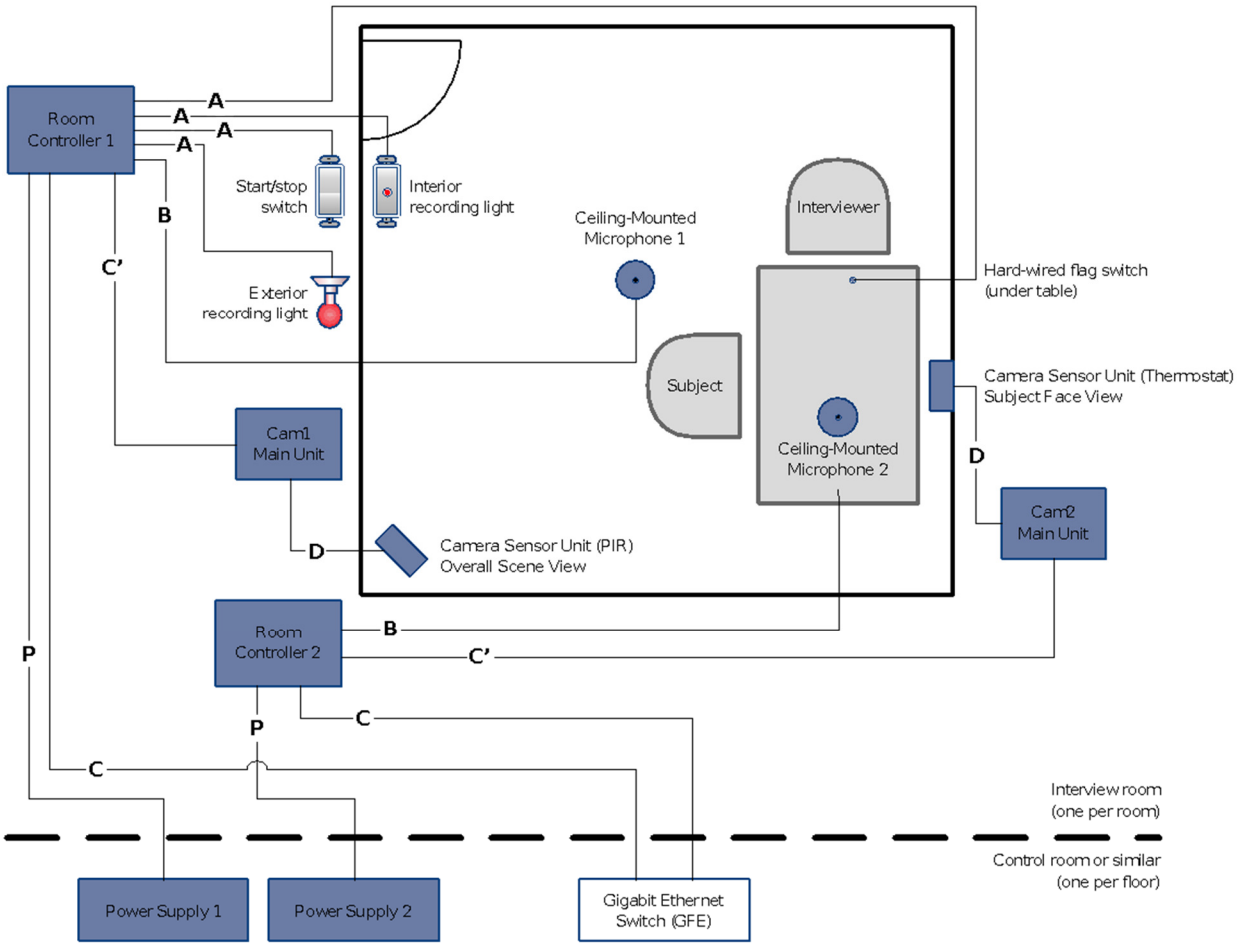

Fig. 2: Fixed Interview Room detail showing wiring detail

Each interview room contains:

- Two high definition **IP Cameras**. These are COTS products and can be covert (typical) or overt. The CaseCracker Onyx system supports most ONVIF-compliant cameras, so it is likely we can meet any particular camera requirement law enforcement agencies might have in the future by selecting an appropriate COTS option. Initially, we are providing Axis P1264 cameras for covert use and Axis F1015 cameras for overt use.

The Axis P1264 camera is ideal for covert use, as it has a small lens element that can be separated from the camera's CPU by up to 8 meters of cable. These units offer excellent concealment options with high video quality. We embed one camera in a thermostat housing situated on the wall opposite the interview subject, near seated eye height. The second camera is embedded in a PIR housing located just below ceiling level in an opposite corner of the interview room. The CPUs for both cameras are concealed above the ceiling of the interview room. The Axis P1264 offers up to 720p resolution and has a fixed lens.

The Axis F1015 is our recommendation for overt, but still discreet, use. This unit is similar to the P1264 but offers slightly better (and, alas, more visible) lenses. The Axis F1015 supports up to 1080p resolution and has a fixed-iris, varifocal lens.

Both cameras support h.264 encoding and are powered via power-over-Ethernet (IEEE 802.3af/802.3at). In our system

this power can be supplied from the Room Controller, or optionally by a separate 12 VDC connection.

Both cameras being proposed offer a wide range of configurable parameters, including frame rate, bit rate, etc. Additionally, it is possible to configure the cameras to superimpose the time onto the video when the video is originally encoded. This timestamp becomes a permanent part of the video and cannot be removed.

- Two digital **Microphones**. The CaseCracker Onyx system supports a range of choices for flexibility in interview room design. Initially we are providing one Louroe Verifact A USB microphone and one Louroe Verifact D microphone, which are both excellent covert microphones that can be mounted on on the ceiling (the Verifact A) or on a wall (Verifact D). The Verifact A unit is a half-space microphone that fully captures the voices of the people in the interview room, with a cylindrical housing 4" in diameter and 1.4" high. The unit has a frequency response from 20Hz - 5kHz (-6dB). The Verifact D housing is a simple 1-gang stainless steel face plate, 2.75"W × 4.5"H; it will perform similarly when placed on the wall (although with any wall-mounted unit, a loss of audio performance will result if the person speaking is facing away from the wall). Sampling for both mics is performed at 44.1 kHz, 16 bits per sample.

- A **Start/Stop Switch** combined with a discreet **Interior Recording Light**, mounted in a 1-gang electrical box inside or outside the interview room near the door. The switch can start or stop recording, and the light unobtrusively assures the interviewer that recording is in progress.

- An **Exterior Recording Light** is a bright LED mounted outside the interview room, with the words "In Use" to warn others that a recorded interview is in progress. Both exterior and interior lights are connected to a Room Controller and are turned on only if the RC is receiving positive confirmation of recording from the server.

- A **Wired Flag Switch** allows the interviewer to unobtrusively mark important parts of the interview. It is a small, wired, momentary contact switch that is mounted under a table near where the interviewer sits. Pressing it during the interview places an index point ("flag") in the video recording.

- Two **Room Controllers.** Each Room Controller (RC) is a metal enclosure measuring 10.4" × 7.3" × 2.0" with an off-white powder coat finish. It is plenum-rated and should be mounted above the ceiling tile, near the CPU units for the two cameras.

The RC performs the following functions: (a) It receives uncompressed audio from the microphones and formats that audio, still uncompressed, for streaming across the recording LAN; (b) it provides breakouts to the wall switch, the recording lights, and the flag switch; and (c) as an installation convenience, the RC contains a power-over-Ethernet switch, so that the IP cameras can be directly connected to the RC and thus only two Ethernet drops are required per room, one per RC. Although one RC is capable of connecting the entire interview room on its own, two are provided to eliminate a potential single point of failure. In the redundant configuration shown in Fig. 2, each microphone and each IP camera is wired to a different RC, with RC-1 also being wired to the recording lights, the start/stop switch, and the flag switch.

A note about administration: One problem with IP cameras, when deployed at scale, is the difficulty of managing the units. In the CaseCracker Onyx system, all cameras and RCs on the Recording LAN are auto-discovered and managed by the CaseCracker Onyx Server, so the system administrator need not worry about a number of the details that are often painful to manage with IP cameras, such as IP address discovery. When an administrator desires to change camera configuration settings, this can be done from the CaseCracker Onyx Client. The user simply clicks on a button that automatically launches their default browser (on the client computer). The CaseCracker Onyx Server dynamically creates a temporary web proxy to the camera's web interface, and this proxy serves to bridge traffic from the Office LAN to the Recording LAN in order to access the camera. The proxy URL on the server is unique to the client, and automatically times out after 5 minutes of inactivity.

Recording LAN

Returning to Fig. 1, the **Recording LAN** is a standard Gigabit Ethernet (GbE) network.

It is important that the Recording LAN be kept private to the CaseCracker Onyx system, for two reasons. Most importantly, in a network based system such as CaseCracker Onyx, video is not recorded until it reaches the server. Therefore, it is imperative that network traffic from other applications be segregated from the live video and audio being streamed from the interview room to the server, so that there is no opportunity for the other traffic to interrupt recording. As a second reason, COTS cameras typically do not encrypt video, and therefore the video and audio is streamed unencrypted to the CaseCracker Onyx Server; anyone with access to the Recording LAN would be able to view live video and audio while interviews are in session.

CaseCracker Onyx Server

During recording, the video and audio from the interview transits the Recording LAN to the **CaseCracker Onyx Server** (CCOS). The server records the video and audio internally in redundant fashion: The evidentiary copy is written to a read-only file on one filesystem, and the working copy is written to a read-write file on a second filesystem. Both filesystems are encrypted and are protected with RAID-1 (mirrored redundancy), so in fact four copies of the interview end up on physical disks within the CCOS.

While recording, the CCOS computes a cryptographic SHA 3-256 fingerprint to ensure later evidence integrity, which is written into each stored file. The hash is computed on each video and audio stream, and the hash values are updated in the file approximately every two seconds[1]. When the recording is complete, the system automatically runs the verification process on the file to ensure it was written to disk correctly, and alerts if any errors are detected. Additionally, an authorized user can manually re-verify the file to ensure integrity at a later date.

In the CaseCracker Onyx system, all cameras and microphones in a room are tightly time-synchronized together. Network Time Protocol (NTP) is used throughout the system to keep all clocks tightly in sync.

As shown in Fig. 1., the CCOS has two network interfaces. One connects to the Recording LAN and the other connects to the Office LAN. The CCOS provides only very limited and controlled routing between these two networks; in general, the Recording LAN is not reachable from the Office LAN. All network interfaces support both IPv4 and IPv6 addressing.

Physically, the CCOS is a standard 1 RU COTS server hardware with redundant power supplies and redundant fans, running CentOS Linux. The operating system and CaseCracker Onyx software are stored on a highly reliable solid-state disk (SSD) for booting, and all video and audio data are stored on mirrored RAID-1 disks. The CCOS can be located in in a secure data room or equipment closet; it should be physically secured and does not need to be accessed for normal operation.

Depending on hardware configuration, the CCOS can support up to 16 interview rooms, with two cameras and two microphones per room. We offer three different hardware configurations based on a Supermicro 5019S-MR 1U SuperServer unit, backed with a rack-mountable uninterruptible power supply suitable for very short power outages. These three configurations are appropriate to serve (a) one to two interview rooms, (b) three to eight rooms, or (c) nine to 16 rooms. Each configuration consumes two rack-units of space, one each for the server itself and for the UPS.

CaseCracker Onyx Client

Returning again to Fig. 1, the **CaseCracker Onyx Client** (CCOC) is shown in the lower right of the system diagram. This software runs on government-furnished Windows desktops or laptops. The CCOC is the main interface into the system. It allows authorized users to view and flag live interviews; search and play back stored interviews; redact interviews; and export content. The CCOC is a traditional Windows application, not a web client. Some screens are shown in the figures below.

[1] Although the server is internally redundant, this is done so that if recording were to stop suddenly due to catastrophic failure, it would be possible to verify the recording up to the last several seconds.

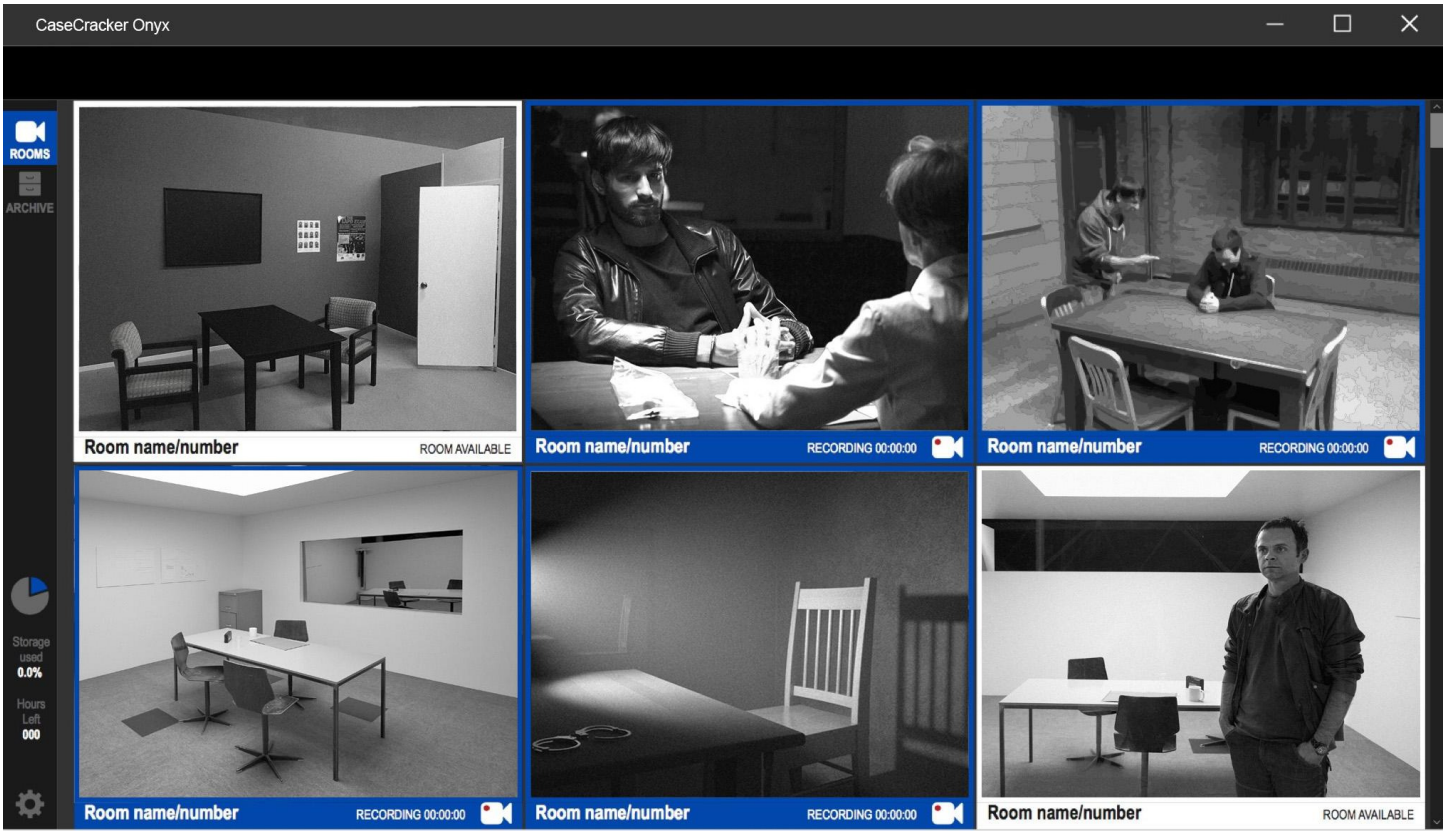

Fig. 3: CaseCracker Onyx Client, Rooms View

The **Rooms View** is typically the first view shown upon logging into the system. This screen shows live, thumbnail views of the interview rooms, without audio. This view can be used on its own to provide security for investigators conducting interviews—for instance, a desk officer working late at night can provide oversight to multiple investigators who are conducting interviews. In addition, this view shows which rooms are currently actively recording (blue border and pulsing red recording icon, four are shown) and which rooms are available (white border, two shown). Clicking on an interview in progress allows an authorized user to observe the interview, with full ability to hear audio, view both cameras, and view, add, and edit per-session metadata and flags. Clicking on an unused room allows a user to immediately start recording.

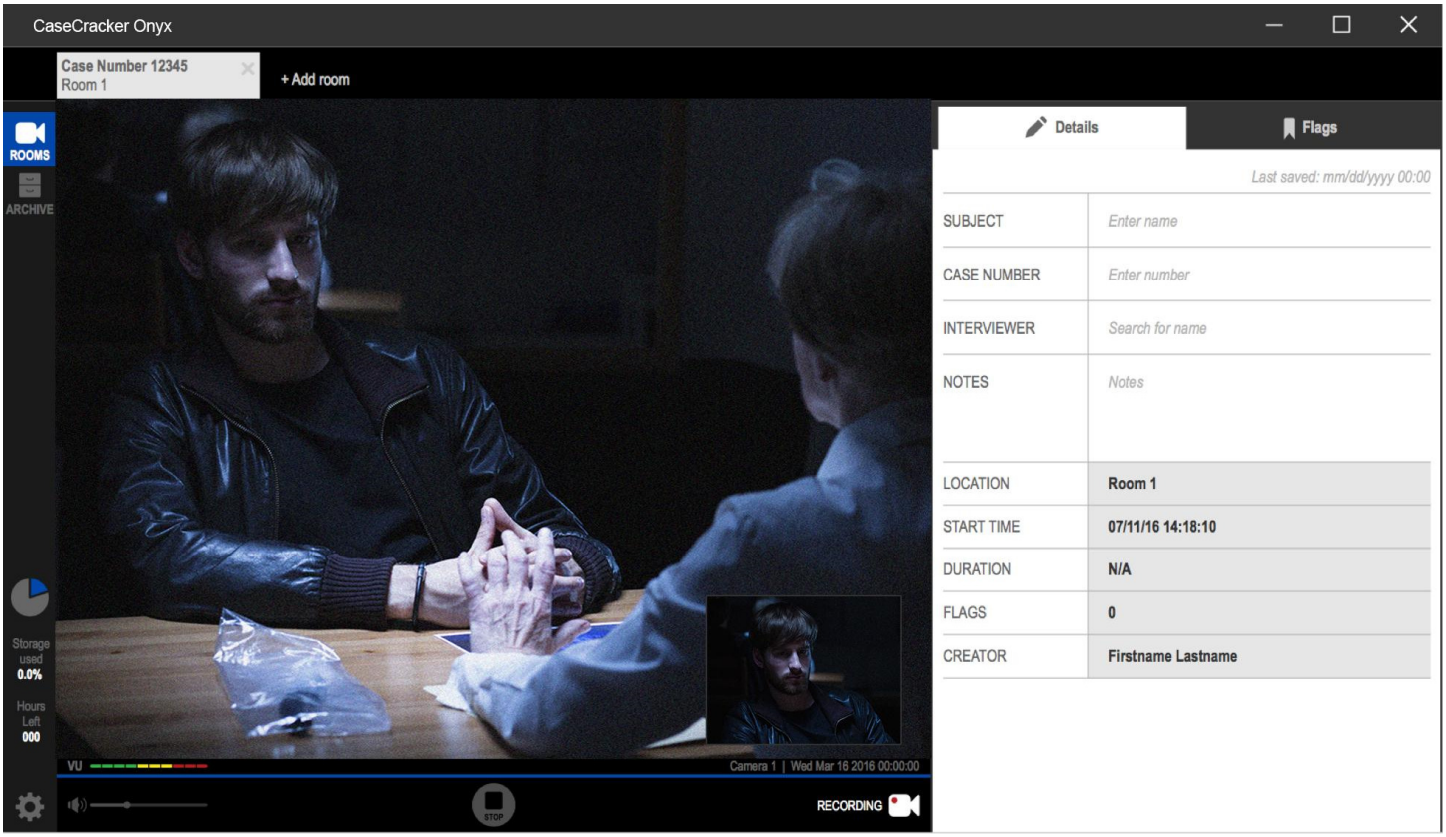

Fig. 4: CaseCracker Onyx Client, Interview View

The **Interview View** is the primary way users interact with video and audio in the CaseCracker Onyx system. It has slight variations between live recording (shown) and stored playback. From here, users can view both camera views and hear the audio. (The two cameras can be swapped by clicking on the picture-in-picture.) The wall-clock time that a particular frame was recorded is displayed in the lower right, directly below the video (and above the "RECORDING" icon). A VU meter in the lower left provides visual feedback that audio is being recorded.

On the right of the screen, an authorized user can fill out the metadata for the session. The default fields are shown but all system metadata is configurable if additional fields are desired. CaseCracker pre-populates the following per-session metadata fields: room/location, start time, duration (populated after the interview completes), number of flags, and the user who initiated recording (who may be different from the interviewer). The other metadata fields can be edited by authorized users.

Case notes can be stored in two ways in the system. One, there is a per-session Notes field (by default; please note that all per-session metadata fields can be customized, so more fields could be added or the defaults deleted). Two, case notes that are specific to points in the recording can be entered as flags, which allows quick access to the associated video. Both types of metadata entry are full-text searchable.

By clicking on the Flags tab in the upper right of the Interview View, the user can view, add, edit, and delete flags. Flags are always tied to a specific instant in the interview, and they can be added from the CCOC with or without descriptive text. In addition to free-form text entry, the CCOC allows users to fill in flags with pre-defined text selected from an administrator-configured list, which could contain commonly-used tags such as "Miranda" or "Confession". Finally, a flag (without descriptive text) is also added to the interview when the interviewer presses the flag switch in the interview room during recording.

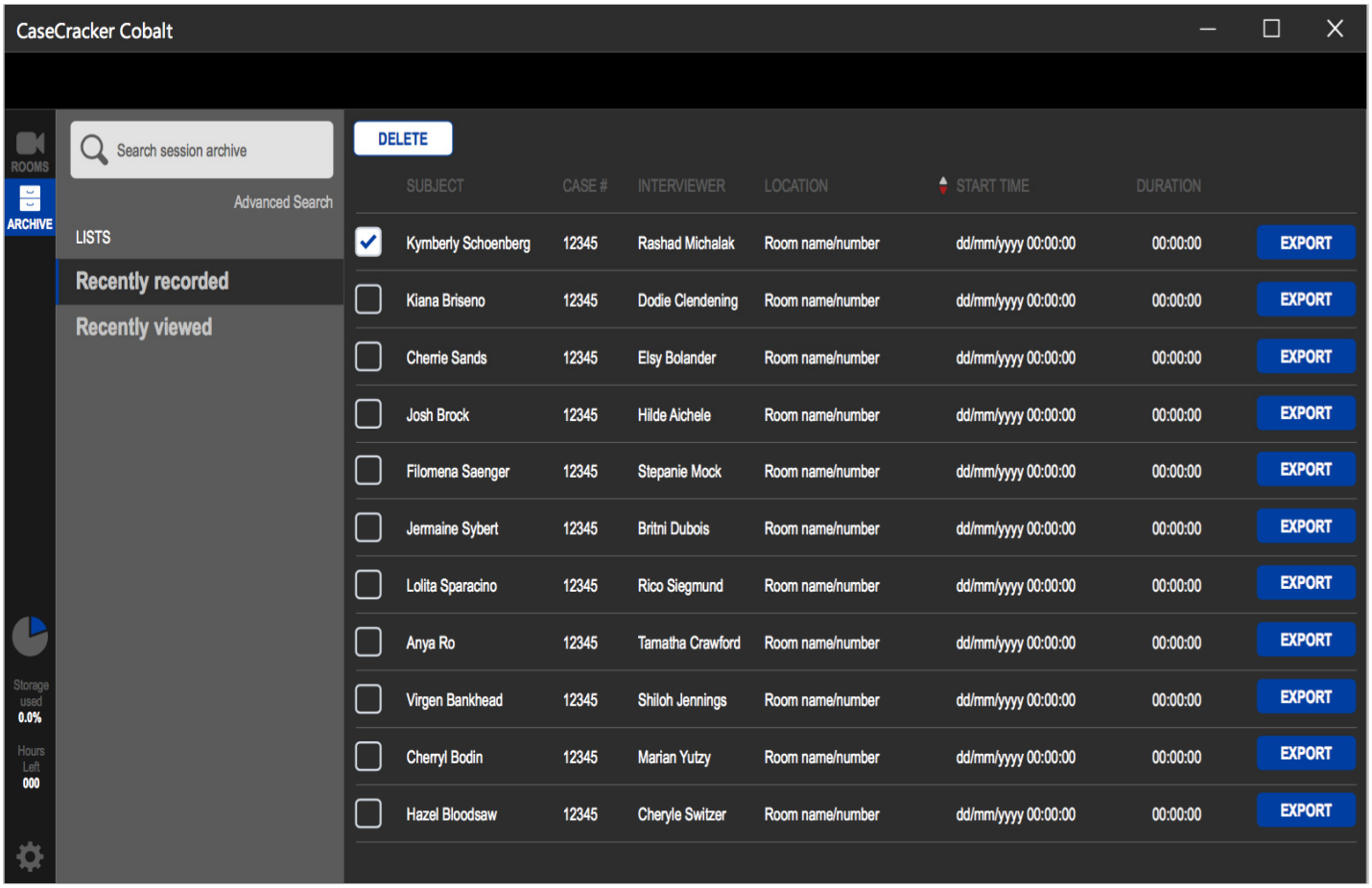

Fig. 5: CaseCracker Onyx Client, Archive View

The **Archive View** shows video stored on the system. Users can view Recently Recorded or Recently Viewed video, or they can search all stored video. Clicking on one of the sessions in the list view will bring up the Interview View for that recording.

Administration pages for all system functions (overall system configuration, policy definition, mapping of permissions to users and groups, etc.) are accessible to authorized users as well.

System Audit Log

The CCOS maintains a system audit log, which records virtually all activity of all users for audit purposes. The system audit log writes to standard syslog and to a flat file. The retention window is configurable but the default is 180 days.

The following events are logged:

- User logs in, user logs out
- Begin or end recording (either client-initiated or wall-switch-initiated)
- Pause or resume recording
- Delete recording
- View video/audio
- Export video, audio, or other data from the system
- Add/edit/delete metadata or flags
- Numerous system administration functions

Data Export and Import

The CCOC supports exporting a number of different file formats:

- An **MP4 file** containing both video streams and both audio streams. The user can choose to include all streams, or select any subset of streams for inclusion, so it is possible for instance to export an MP4 file containing just one video track and no audio. When present, video is encoded using h.264, and represents the exact encoded bits that were delivered from the IP camera(s) at the time of recording. When present, each track of audio will be included twice: Once using the Apple lossless ALAC codec, and again using the lossy AAC algorithm. In addition, the MP4 file contains secure hash information, so that it can later be validated, as well as the information needed to compute the wall-clock recording time of any point during the recording. At the user's option, it can either contain or not contain the per-session and flag-based metadata.

The MP4 file follows open standards, and can be played in readily-available commercial players such as Windows Media Player, Quicktime, and VLC. Note, however, that these players generally only display one of the two video streams and one of the two audio streams, and they cannot display metadata or flags.

- A **WAV or AAC file** containing only the audio from the interview. In the case of WAV format this audio will be the exact PCM samples recorded during the interview (generated from the lossless audio track). In the case of AAC format this audio will be compressed.

- A **PDF file** containing the per-session metadata from the interview.

All files (audio+video, audio-only, video-only, metadata) are exported on the CCOC and can be stored to any file system supported by the underlying hardware, so removable media and enterprise-wide file servers are both supported assuming they are available to the investigator's desktops.

User Management and Authentication

The CaseCracker Onyx Server requires an authenticated user for all actions performed on the system, with the exception of pressing the start/stop button located outside an interview room. Each user must log in to the CaseCracker Onyx Client when it is started, unless single sign on (SSO) is configured, in which case the credentials that logged the user onto the Windows desktop will also be used to log him or her into the CCOC. Permissions may be individually set on a per-group or per-recording basis (as appropriate) for a large number of actions on the system.

CaseCracker Onyx supports having Microsoft Active Directory (AD) groups as the core of its permissions system. Various privileges in CaseCracker can be mapped, using the CaseCracker Onyx admin interface, to different AD groups. We currently have a lightweight, stand-alone alternative for user and group privilege management until AD integration is enabled.

Hierarchical Storage; Synchronization to External Systems

In the future CaseCracker Onyx roadmap, individual Onyx servers can integrate in multiple ways with systems located elsewhere on the agency's network, as summarized below:

- First, in the future it will be possible to connect CaseCracker Onyx Servers together across a wide-area network. All searches are distributed amongst participating CCOS nodes using elastic search technology, so if all the CCOS units within an agency's network were so configured, a search performed on any server will result in searching the video across the entire enterprise. Once a user selects a particular interview, the corresponding video, audio, and metadata will be securely streamed to that user from the CCOS that hosted it, across the WAN if needed.

- Second, future CaseCracker Onyx Servers will support hierarchical storage, so it will be possible to configure recordings to be automatically transferred over the WAN to a master CaseCracker Onyx Server located at a central location. Only once the recording has been successfully transferred and validated will the source content be deleted from the origin CCOS server. In this manner, a federal agency could arrange to store all countrywide interview video

in a single location.

- Finally, today CaseCracker Onyx files are entirely open standards based and entirely self-contained, so it is possible to immediately export these files into any enterprise-wide storage system. These internal files are based on the open MP4 format and they will play without modification using QuickTime, Windows Media Player, and VLC.