Digital Forensics Analysis Report

Delivered to Alliance Defending Freedom

November 5, 2015

Prepared by Coalfire Systems, Inc.

Revision Summary

Date	Revision History	Comments
9/28/2015	1.0	Original final draft
11/5/2015	1.1	Corrected formatting issue on pages 10 and 11

Executive Summary

In September, 2015, CGS, the prime contractor on behalf of Alliance Defending Freedom, engaged Coalfire Systems, Inc., the sub-contractor (hereinafter "Coalfire") to conduct a computer forensics analysis of certain raw video and audio data files. Coalfire's objectives for this project are to:

- Forensically evaluate video and audio files provided by The Center for Medical Progress ("the Organization") through CGS ("raw" video and audio), and determine whether the raw video or audio content of the files have been edited or otherwise altered;
- Compare the raw video and audio to certain files posted to YouTube ("Full Footage" videos and a "Supplemental" video) for the purpose of determining inconsistencies between the files.

The scope of Coalfire's analysis did not cover or include:

- Validation of those individuals depicted in the video or audio, who recorded the video and audio files, the location where they were recorded, when they were recorded, or the purpose of the recordings;
- Providing an opinion on the chain of custody prior to receipt of source materials by Coalfire;
- Coalfire's analysis was limited to only the source materials received from the Organization and did not include interviews of participants in the videos or audio.

A flash drive containing recorded media was received via FedEx by Coalfire on September 17th, 2015, where it was examined using industry-standard forensic tools and techniques. The flash drive contained (i) a total of ten (10) videos with audio recorded on two (2) separate devices, and (ii) a total of eight (8) audio recordings made with two (2) audio-only devices.

Coalfire's analysis of the recorded media files contained on the flash drive indicates that the video recordings are authentic and show no evidence of manipulation or editing. This conclusion is supported by the consistency of the video file date and time stamps, the video timecode, as well as the folder and file naming scheme. The uniformity between the footage from the cameras from the two Investigators also support the evidence that the video recordings are authentic.

With regard to the "Full Footage" YouTube videos released by the Organization, edits made to these videos were applied to eliminate non-pertinent footage, including "commuting," "waiting," "adjusting recording equipment," "meals," or "restroom breaks," lacking pertinent conversation. Any discrepancies in the chronology of the timecodes are consistent with the intentional removal of this non-pertinent footage as described in this report.

Furthermore, four of the five raw video recordings, which also contained audio captured from the video recording device, are accompanied by a raw audio recording captured from a separate audio-only recording device. The raw audio-only recordings last for the duration of their associated raw videos. These raw audio recordings support the completeness and authenticity of the raw video recordings since they depict the same events within the same duration as captured from the two separate video recorders.

Evidence Acquisition Processing Procedures

Coalfire employed industry standard tools and techniques throughout handling, processing, and analysis of the evidence. A sealed FedEx Express envelope was received into Coalfire Labs via FedEx Overnight delivery on September 17, 2015 at 8:35 AM (MST). A Chain of Custody was established upon opening the package. The package contained one USB flash drive sealed in a FedEx label pouch. Details about the enclosed media are included below.

Device Make/Model	Device Serial Number	Description	Device Serial Number	Capacity
PNY “Turbo Plus” flash drive	2CE00713QB	USB flash drive (silver) USB 3.0	UID: 1C233FA33C1C2A38	128 GB

Coalfire used a Logicube Falcon to create a raw DD image of the evidence onto a previously wiped hard drive. The images were verified by their hash values. A working copy of the original image was created onto a previously wiped hard drive. All subsequent analysis was performed on the working copy forensic image, not on the original media or the original forensic image acquisition. The analysis was performed on a dedicated forensic workstation using AccessData’s Forensic Toolkit (FTK) version 5.6.3.16, VLC Player version 2.2.1, Apple QuickTime version 7.7.8, and iZotope RX Advanced.

Analysis

File and Folder Analysis

There were a total of 29 folders residing on the flash drive. Each of the folders shows a modified, accessed, and created date of 2015-09-13 UTC with the modified and created time stamps between 2015-09-13 03:36:03 UTC and 2015-09-13 04:57:35 UTC. Copying a folder from a source drive to a destination drive results in the creation of a new modified and created date and time stamp on the destination drive. The date and time stamp from the source drive directory does not carry over to the directory created on the destination drive. This suggests that the date and time stamps for the folders located on the flash drive are indicative of when the folders were copied from the original source drive to the flash drive.

The root consisted of 5 directories which are listed below with their creation time and date stamps.

Directory Name	Created
[root]\052215Dyer dinner	2015-09-13 03:36:47 UTC
[root]\072514DebNucatola	2015-09-13 03:36:03 UTC
[root]\PPGC040915	2015-09-13 03:36:32 UTC
[root]\PPPSGV020615	2015-09-13 03:36:15 UTC
[root]\PPRM040715	2015-09-13 03:36:26 UTC

Directories contained within the root of the flash drive

Within these directories were two subdirectories, each with the name of a male and a female. The male name will hereinafter be referred to as “Investigator 1” and the female name as “Investigator 2.” Within each of these folders were either a subdirectory named “MyRecord” or a folder named with a numeric date. Where there was a “MyRecord” folder present, the “MyRecord” folder contained a subdirectory named by numeric date. The folders named by numeric dates contained recorded video files corresponding to the numeric date of the folder. The five directories in the root listed above delineate five separate dates of video recordings which is explained in further detail below.

The folders named with numeric dates contained video files. In total, there were 86 AVI video files on the flash drive. The metadata for the AVI video files does not contain any metadata or unique file signatures to indicate the video recording device that was used to create the video. Review of the video content reveals that the video files were captured from two separate video recording devices which are separated into the Investigator 1 and Investigator 2

directories. The numeric dates within the video file names are consistent throughout all other folder names in the path to any given video file. Examples of the folder and file naming schemes are shown below.

- [root]\072514DebNucatola\[Investigator 1]\MyRecord\20140725\FNND0569_20140725114841.AVI

The example above shows a folder naming structure containing the "MyRecord" subdirectory. In the example above, the root directory name contains a numeric date of 7/25/2014, a subdirectory with a name containing the numeric date 7/25/2014, and containing a video file with a file name including the numeric date 7/25/2014. Another example of the folder and file naming structure is shown below.

- [root]\PPGC040915\[Investigator 2]\20150409\FNNI0773_20150409071900.AVI

In the example above, the root directory name contains the numeric date 4/9/2015, a subdirectory with a name containing the numeric date 4/9/2015, and containing a video file with a file name including the numeric date 4/9/2015.

Contrary to folders, the last modified and created date and time stamps of a file is preserved when the parent folder it resides in is copied from a source drive to a destination drive. Therefore, the last modified date and time stamps of the video files contained on the flash drive were preserved from the original source files. The video files residing on the flash drive show last modified and created time stamps between 2015-02-06 20:47:28 UTC to 2014-07-25 22:18:26 UTC. Review of the video file modified date stamps shows that they are consistent with the numeric dates reflected in the video file names as well as the folders in the path of those video files. Furthermore, the date stamps embedded within the videos themselves are consistent with the date stamps of the folders in the video file path.

An example of the relationship between the video file name and file created date stamp is shown below.

Video File Name	Created
FNNI0773_20150206130219.AVI	2015-02-06 22:02:18 UTC

Video file name and created date stamp relationship

The AVI file names also contain a number representing the timecode that is embedded in the first frame of that video file. An example of this is shown below.

- [root]\PPGC040915\[Investigator 1]\FNND0569_20150409081515.AVI

In this example (on the following page), the video file named FNND0569_20150409081515.AVI shows a date of 4/9/2015 and a first frame timecode of 08:15:15. Below is a screenshot of the first frame (frame 000000) of the 20150409081515.AVI video.

First frame from video file [root]\PPGC040915\[Investigator 1]\FNND0569_20150409081515.AVI

There were some videos, however, where the first frame does show a timecode that is one second behind the time shown in the video file name.

All of the AVI video files are 1011 MB in size or smaller. When the modified time stamps are in chronological order, it is evident that a new video file is created once the preceding video file size reaches 1011 MB during continuous recording. This is demonstrated by noting the final timecode embedded in the last frame of the video and comparing it to the timecode in the first frame of the next video in sequence (the first frame timecode number is also contained in the video file name). It is a common feature of video recording devices to capture continuous recording in numerous smaller separate files to avoid issues with file systems that cannot accommodate large file sizes and to minimize data loss in the case of file corruption as result of hardware failure (dead battery, malfunction, etc.). Review of the AVI files that were smaller than 1011 MB appears to be the result of a manual stop performed on the recording device by the camera operator.

Video File Recording Path	Continuous Video Recording Segments
052215Dyer dinner072514DebNucatola\[Investigator 1]\MyRecord\20140725	Continuous recording from 2014.07.25 11:48:41 to 2014.07.25 15:18:26 (frame 019233)
072514DebNucatola\[Investigator 2]\MyRecord\20130725	Continuous recording from 2013.07.25 11:41:24 to 2013.07.25 15:15:21 (frame 058664)
PPGC040915\[Investigator 1]\20150409	Continuous recording from 2015.04.09 07:18:22 to 2015.04.09 13:09:37 (frame 017915) Continuous recording from 2015.04.09 13:16:58 to 2015.04.09 14:56:40 (frame 025881)

PPGC040915\[Investigator 2]\20150409	Continuous recording from 2015.04.09 07:19:00 to 2015.04.09 13:20:01 (frame 062200)
PPPSGV020615\[Investigator 1]\20150206	Continuous recording from 2015.02.06 11:51:07 to 2015.02.06 13:34:49
PPPSGV020615\[Investigator 2]\20150206	Continuous recording from 2015.02.06 11:49:47 to 2015.02.06 13:36:05 (frame 060765)
PPRM040715\[Investigator 1]\MyRecord\20150407	Continuous recording from 2015.04.07 08:16:16 to 2015.04.07 13:04:06 (frame 006180) Continuous recording from 2015.04.07 13:05:19 to 2015.04.07 14:31:28 (frame 001483)
PPRM040715\[Investigator 2]\MyRecord\20150407	Continuous recording from 2015.04.07 08:16:08 to 2015.04.07 14:12:40 (frame 054178)

Continuous video recording segments

Based on this evidence presented in this section, Coalfire concludes that the video files located on the flash drive are accurate representations of the raw unedited footage captured by the original video camera with reliable and consistent timecodes.

Video Content Analysis and Comparison

The video recordings created by both Investigator 1 and Investigator 2 depict many of the same scenes from two different perspectives as captured by their individual cameras. The timecodes embedded in the video recordings are not synced to each other. Coalfire determined the approximate offsets of the two video cameras for each day of recording.

Video Recording Top Parent Directory	Offset of Investigator 2 Camera to Investigator 1 Camera
052215Dyer dinner	Approximately +00:00:32
072514DebNucatola	Approximately -00:04:03
PPGC040915	Approximately -00:00:50
PPPSGV020615	Approximately -00:00:29
PPRM040715	Approximately -00:00:50

Video Camera Timecode Offset

By establishing the offset in timecode, Coalfire was able to compare events from each of the cameras as they happened in real time. This was critical when comparing the raw footage videos contained on the flash drive to the Full Footage videos released by the Center for Medical Progress on YouTube. The Full Footage CMP YouTube videos are listed below and uploaded by the YouTube user “The Center for Medical Progress”.

Full Footage YouTube Video Name	YouTube Video URL
FULL FOOTAGE: Planned Parenthood VP Says Fetuses May Come Out Intact, Agrees Payments...	https://www.youtube.com/watch?v=wV2U9unI1NM

FULL FOOTAGE: Planned Parenthood Uses Partial-Birth Abortions to Sell Baby Parts	https://www.youtube.com/watch?v=H4UjIM9B9KQ
FULL FOOTAGE: Intact Fetuses "Just a Matter of Line Items" for Planned Parenthood TX Mega-Center	https://www.youtube.com/watch?v=MCiD9_ICt44
FULL FOOTAGE: Second Planned Parenthood Senior Executive Haggles Over Baby Parts Prices	https://www.youtube.com/watch?v=vwAGsjoorvk

Full Footage CMP YouTube videos

After these "FULL FOOTAGE" videos were posted, an additional video was posted by the Organization on August 30, 2015 (the "Supplemental Full Footage Video") that is of the same time duration as missing footage from the "FULL FOOTAGE: Intact Fetuses 'Just a Matter of Line Items' for Planned Parenthood TX Mega-Center".

Supplemental YouTube Video Name	YouTube Video URL
Part 2 Supplement TX FULL FOOTAGE: Intact Fetuses "Just a Matter of Line Items" for PP	https://www.youtube.com/watch?v=wV2U9unI1NM

Supplemental Full Footage CMP YouTube video

Coalfire reviewed any and all inconsistencies in timecode apparent in the Full Footage videos for comparison to the raw video footage corresponding to those videos. Notes were made upon review of the raw video content which described the events that took place during the missing footage that was edited from the Full Footage videos. Events that were left out of the Full Footage videos lacked pertinent conversation. The events depicted in the missing footage fell into five common categories: commuting, waiting, adjusting recording equipment, meals, and restroom breaks. "Commuting" footage consists of Investigator 1 and 2 driving in car to locations, or walking outside to locations outside or inside a building. "Waiting" footage consists of Investigator 1 and 2 waiting to engage with primary Planned Parenthood subject, or other personnel, usually in a lobby, office, or a restaurant table. "Adjusting recording equipment" footage consists of times when Investigator 1 and 2 are manually setting camera or audio recording device equipment, adjusting the equipment, or changing the batteries. "Meal" footage consists of Investigator 1 and 2 eating. "Restroom break" footage consists of Investigator 1 or 2 going to the restroom primarily to relieve themselves.

FULL FOOTAGE: Intact Fetuses "Just a Matter of Line Items" for Planned Parenthood TX Mega-Center

Begins 2015.04.09 07:37:48 (034977)

Ends 2015.04.09 14:50:13 (014278)

Corresponding raw video recordings: PPGC040915

Investigator 1 begins video recording at 07:18:23 and ends video recording at 14:56:40

Investigator 2 beings video recordings at 07:19:00 and ends video recording at 13:20:01

Gap from beginning of raw footage to beginning of Full Footage at 07:37:48

Adjusting recording equipment – Commuting – Waiting

Gap from 07:46:47 to 08:15:15

The 07:46:47 stop coincides with the end of the raw video file named FNND0569_20150409071822.AVI. The next file in the sequence (FNND0569_20150409074648.AVI) starts at 07:46:48 (frame 000000) and ends at 08:15:09 (frame 051046). The next video file in sequence (FNND0569_20150409081515.AVI) starts at 08:15:15 (frame 000000). The missing footage between in the Full Footage YouTube video between 7:46:47 and 8:15:15 matches the time duration of the raw video file FNND0569_20150409074648.AVI.

Coalfire reviewed the content of the Supplemental Full Footage video against the raw video and audio and determined that the supplemental video matches the timeframe, timecodes, and events depicted in the raw video file FNND0569_20150409074648.AVI.

Gap from 08:44:26 to 08:48:39

Restroom break – Waiting

Gap from 12:58:43 to 13:50:18

Commuting – Restroom break - Waiting

Raw video footage after end of Full Footage video at 14:50:13

Commuting (example follows)

Investigator 1 PPGC040915 “commuting” footage video frame

FULL FOOTAGE: Planned Parenthood VP Says Fetuses May Come Out Intact, Agrees Payments...

Being: 2015.04.07 09:10:10 (frame 045843)

End: 2015.04.07 14:17:27 (frame 027478)

Corresponding raw video recordings: PPRM040715

Investigator 1 begins video recording at 08:16:16 and ends video recording at 14:31:28

Investigator 2 begins video recordings at 08:16:08 and ends video recording at 14:12:40

Gap from beginning of raw footage to beginning of Full Footage at 09:10:10

Adjusting recording equipment – Commuting

Gap from 10:27:07 to 11:01:40

Meal – Waiting (example follows)

Investigator 1 PPRM040715 "meals" footage video frame

Gap from 11:24:49 to 11:27:37

Waiting

Gap from 11:36:47 to 11:39:25

Waiting

Gap from 11:41:43 to 11:43:54

Waiting

Gap from 12:35:50 to 13:43:46

Restroom break – Adjusting recording equipment – Waiting

Gap from 11:45:46 to 12:21:55

Waiting

Raw video footage after end of Full Footage video at 14:17:27

Commuting – Waiting – Restroom break

FULL FOOTAGE: Planned Parenthood Uses Partial-Birth Abortions to Sell Baby Parts

Begin: 2014.07.25 12:17:07

End: 2014.07.25 15:02:33

Corresponding raw video recordings: 072514DebNucatola

Investigator 1 begins video recording at 11:48:41 and ends video recording at 15:18:26

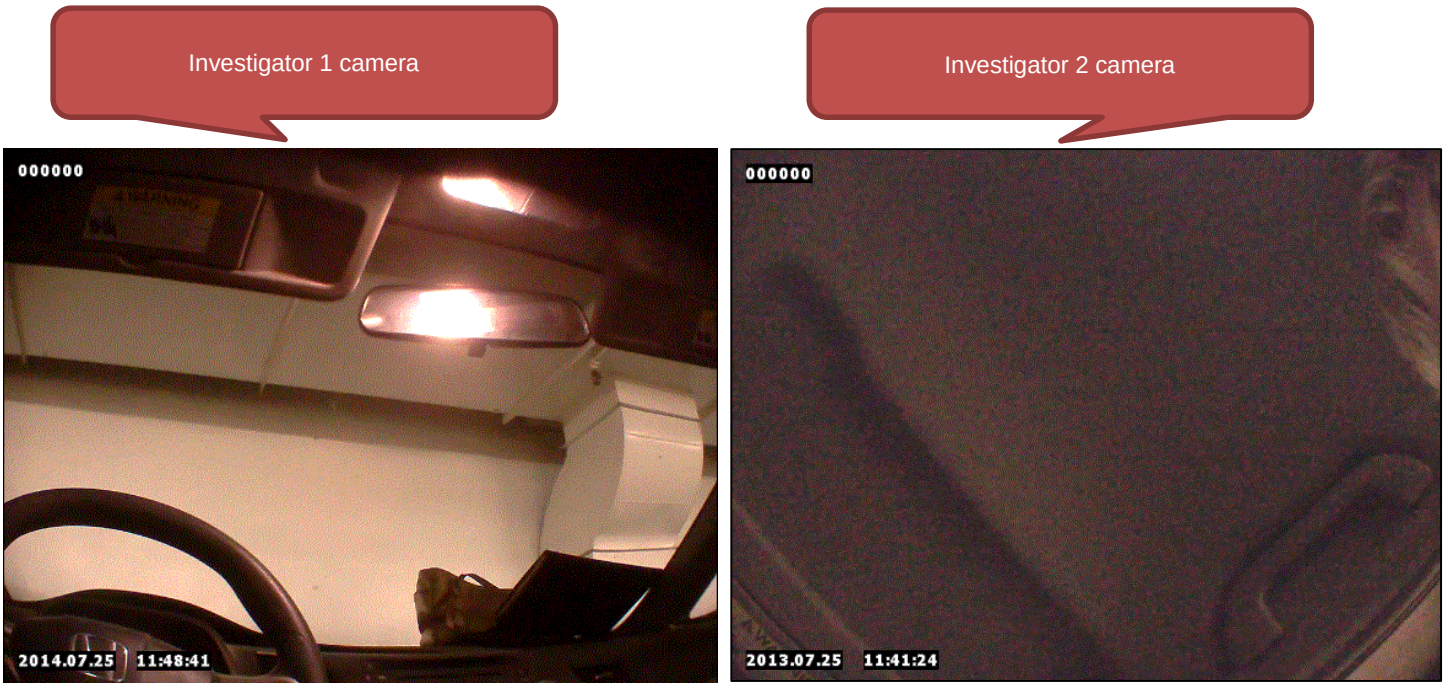
Investigator 2 begins video recordings at 11:41:24 and ends video recording at 15:15:21

Timecode and year change from 2014.07.25 14:32:07 to 2013.07.25 14:28:04

Restroom break

In the Full Footage video, the video recording starts from Investigator 1. When Investigator 1 excuses himself for the restroom, Investigator 2's camera is used to follow the conversation at the table. The -00:04:03 offset from Investigator 2's camera to Investigator 1's camera explains the jump in time.

The raw video shows that Investigator 1's camera shows the date stamp 2014.07.25 while Investigator 2's camera shows the date stamp 2013.07.25.



The first frame from the footage on 7/25 shows that the date stamps show a one year difference

Since the raw video recordings both depict the same events in real time, the discrepancy in the date stamp year is attributed to the two camera's date and time settings not being synced to each other.

Gap from 14:38:06 to 14:41:08

Restroom break (example follows)

Investigator 1 072514DebNucatola "restroom break" footage video frame

Raw video footage after end of Full Footage video (15:02:33)

Restroom break – Waiting – Commuting

FULL FOOTAGE: Second Planned Parenthood Senior Executive Haggles Over Baby Parts Prices

Begin: 2015.02.06 12:03:05

End: 2015.02.06 13:16:13

Corresponding raw video recordings: PPPSGV020615

Investigator 1 begins video recording at 11:51:07 and ends video recording at 13:34:49

Investigator 2 begins video recordings at 11:49:47 and ends video recording at 13:36:05

12:04:53 jumps back to 12:04:24

Restroom break (example follows)

Investigator 2 PPPSGV020615 “restroom break” footage video frame

The Full Footage video starts on Investigator 1's camera who is shown standing up from the table at 12:04:53. The video then switches to Investigator 2's camera at 12:04:24 which shows Investigator 1 walking from the table towards the restroom. The Full Footage video uses Investigator 2's camera for the remainder of the video. The time difference is attributed to the -00:00:29 offset of Investigator 2's camera to Investigator 1's camera.

Raw video footage after end of Full Footage video (13:16:13)

Waiting – Commuting

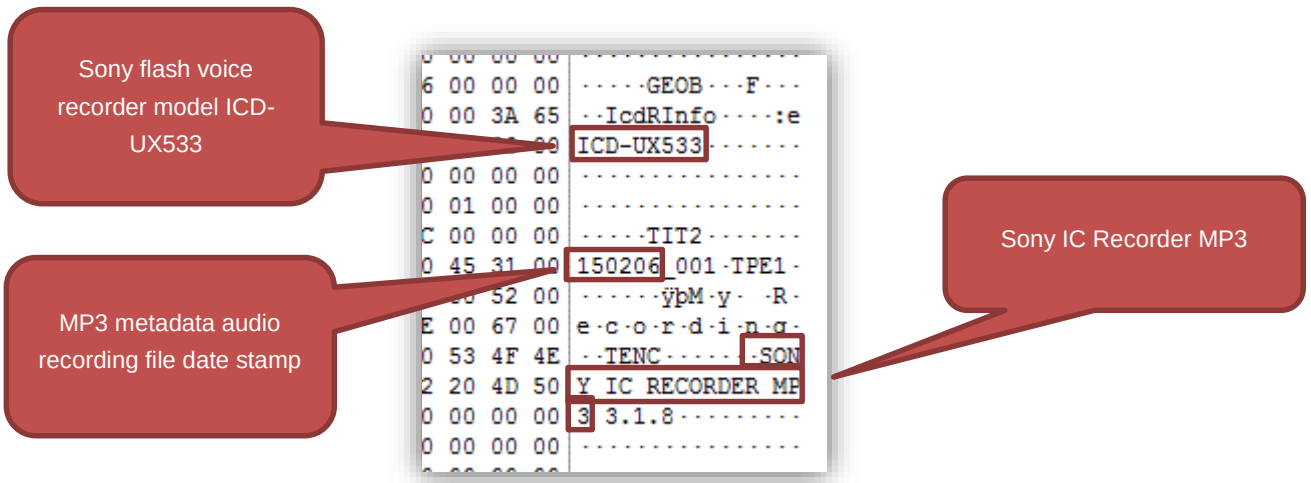
Audio Content Analysis

With the exception of the "052215Dyer dinner" directory, each day of video recording was accompanied by MP3 audio recordings within the Investigator 1 and Investigator 2 folders. This resulted in audio recordings from the point of view of both Investigator 1 and Investigator 2 that are separate from the audio captured by the video recording device. Like the video recordings, the audio files contained a numeric date in the file name. An example of one of the audio recording file paths is shown below.

Audio File with Path	Created
[root]\PPPSGV020615\[Investigator 1]\150206_001.MP3	2015-02-06 21:52:37 UTC

This MP3 audio recording exhibits a file name containing the date 2/6/2015 which is consistent with the numeric dates in the names of the other folders and files contained in the top level parent directory. The creation date of this file is also consistent with the date contained in the names of the files and folders contained within the top parent directory.

The metadata embedded in the header of the hexadecimal data reveals that this audio recording was captured with a Sony IC Recorder model ICD-UX-533. The metadata also reflects the date the recording was created which is consistent with the file date stamp.



Metadata from [root]\PPPSGV020615\[Investigator 1]\150206_001.MP3 Audio File

The audio recordings were started shortly before or after their corresponding video recordings and span the duration of the video recordings or more. Below is a chart with details about the audio recording.

Audio File with Path	Created	Duration
[root]\072514DebNucatola\[Investigator 1]\140725_002.MP3	2014-07-25 18:47:00 UTC	03:28:28
[root]\072514DebNucatola\[Investigator 2]\140725_001.MP3	2014-07-25 18:40:41 UTC	03:31:59
[root]\PPPSGV020615\[Investigator 1]\150206_001.MP3	2015-02-06 21:52:37 UTC	01:47:20
[root]\PPPSGV020615\[Investigator 2]\150206_001.MP3	2015-02-06 20:47:28 UTC	01:46:08
[root]\PPRM040715\[Investigator 1]\150407_001.MP3	2015-04-07 15:16:50 UTC	06:16:22
[root]\PPRM040715\[Investigator 2]\150407_001.MP3	2015-04-07 15:20:16 UTC	06:16:49
[root]\PPGC040915\[Investigator 1]\150409_001.MP3	2015-04-09 14:20:20 UTC	0:7:39:57
[root]\PPGC040915\[Investigator 2]\150409_001.MP3	2015-04-09 14:21:53 UTC	07:41:43

MP3 Audio Recording Files

Much like the footage from the two separate cameras, Coalfire was able to time align the audio recordings to the video footage to allow for review of any inconsistencies or anomalies in their content with both the video and audio recordings from the two video cameras.