School of Computing
Digital Forensics and Investigation

Practical 3B: Media

Introduction

Forensic investigators can make use of digital photos, audio and video files found on a computer or electronic device. Thereby quickly help identify victims, suspects, or additional evidence that are relevant to the matter. Digital photos can be classified in the followings:

- savagely cruel or depraved behavior
- Child Abuse
- People
- Pornography
- Portrait
- Scanned Document
- Currencies
- Upskirting
- Vehicle
- Weapon
- Others (various not harmful or offensive class types)

Learning Objectives

In this lesson, students will take part in lectures, hands-on exercises, instructor-led exercises, and student practical exercises to gain an understanding of what types of media can be parsed by Magnet AXIOM and what views are available post-processing. Students will also learn how to view video artifacts. At the conclusion of this lesson, students will be able to identify, discuss, and utilize Magnet AXIOM to determine media that can be parsed and be able to view videos within Magnet AXIOM Process as well as be able to determine the best view available for the different artifact types.

Media Artifacts

Magnet AXIOM has the ability to both parse and carve for multiple media items during the processing phase. These artifacts include multiple types of images including, but not limited to, JPG, GIF, PNG, BMP, and many RAW image formats. Video formats include, but are not limited to, MPEG, AVI, MOV, and additional RAW video formats.

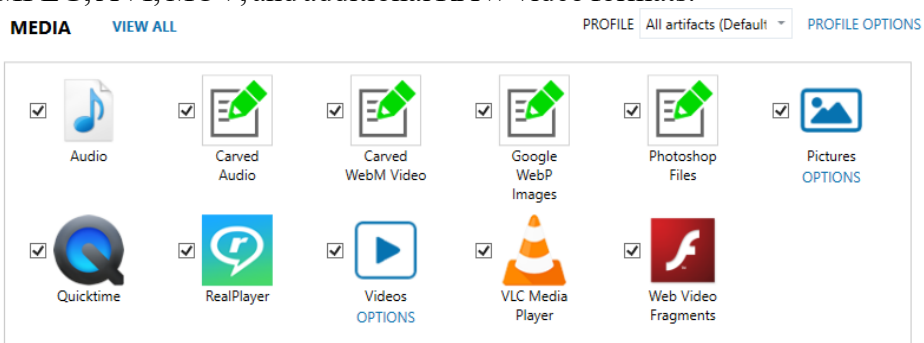


Figure 3-5-1: Media Artifacts And Options

Within AXIOM Examine, parsed media artifacts are displayed under the Media category. Examiners can review individual artifacts by selecting each listing, or review all artifacts matching the Media category by selecting the Media artifact header. Beside the artifact identifier, AXIOM will display how many of each artifact were recovered during the processing phase. For pictures, this will include carved photos, however, for videos, carved video is a separate artifact.

MEDIA	39,688
Carved Video	425
Pictures	39,201
Potential Facebook Pictures	1
Videos	61

Figure 3-5-2: Media Artifacts And Options

While Carved Video is a separate artifact category, Carved Pictures is not. In order to determine if a picture was carved or parsed from allocated space, consult the column heading Recovery Method:

EVIDENCE (39,201) Column view

Image	File Name	File...	Created Date/...	Recovery Method	Last Accessed...	L
	sliding_panel_a.png	.png		Parsing		
	tony_toast_a.png	.png		Parsing		
	sliding_panel_rgb.jpg	.jpg		Parsing		
	tony_toast_rgb.jpg	.jpg		Parsing		
	main_menu_hd_rgb.jpg	.jpg		Parsing		
	913ada711431fb8f3d54c68c72eb0d9c.jpg	.jpg	3/26/2019 3:47:12 PM	Parsing	3/27/2019 11:44:11 AM	3/
	grumpy-owl_c_2512435.jpg	.jpg	3/26/2019 3:47:31 PM	Parsing	3/27/2019 11:44:11 AM	3/
	resized owl moon.jpg	.jpg	3/26/2019 4:51:14 PM	Parsing	3/27/2019 11:44:11 AM	3/
	hqdefault.jpg	.jpg	3/26/2019 3:47:02 PM	Parsing	3/27/2019 11:44:11 AM	3/
				Carving		
				Carving		
				Carving		
				Carving		
				Carving		
				Carving		
				Carving		

Figure 3-5-3: Recovery Methods Of Carving And Parsing

Viewing Options

Magnet AXIOM offers several new views to review media artifacts. To change the view layout, select the view that you want from the dropdown menu. Depending on the type of review that you doing, you may review pictures and videos using more than one view.

Thumbnail View: Displays thumbnail images of all of the pictures and videos. This allows for a quick review of the artifacts. When selecting Thumbnail View, you are also presented with several other options to sort and filter your results. These include Filter by, Sort by, and Size of the thumbnails that you wish to view.

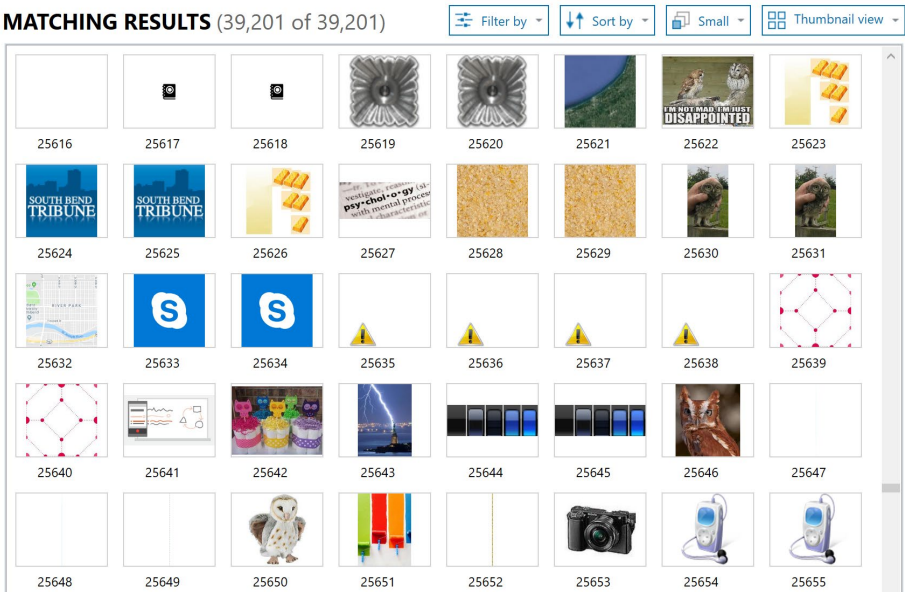


Figure 3-5-4: Thumbnail View

World Map View: Displays a map with drop pins for all of the pictures and videos that contain location metadata. Clicking on the drop pin will bring up details of the picture or video.

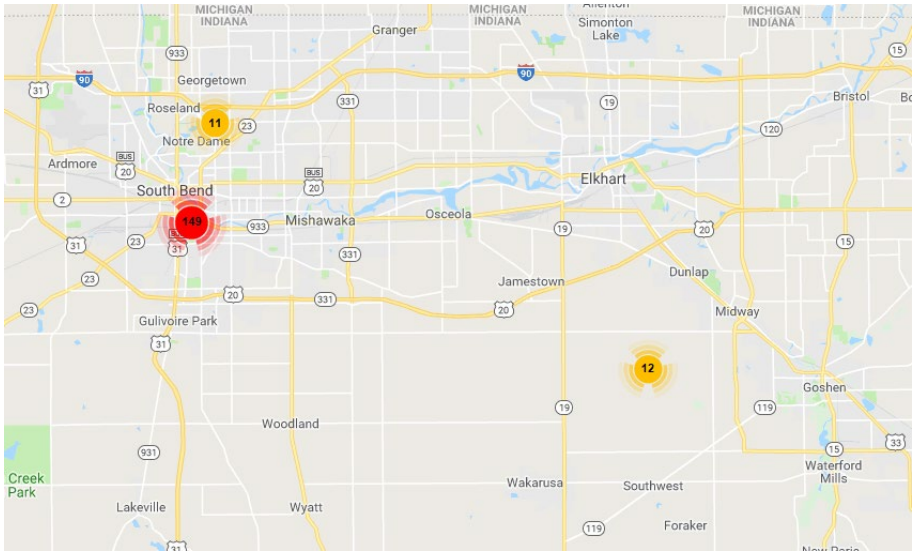


Figure 3-5-5: World Map View

Each view offers its own benefits for use. The standard views such as Column, Row, or Classic offer the ability to easily sort based off the metadata. This includes standard File System Metadata, such as File Name, Created Date, Last Accessed Date, and Last Modified Date.

EVIDENCE (21,992) Column view

File Name	Recovery M...	File E...	Created Date/Time	Last Accessed Date/Time	Last Modified Date/Time
logo.png	Parsing	.png	6/1/2017 2:21:56 AM	6/1/2017 2:21:56 AM	10/30/2015 8:51:00 PM
icon.png	Parsing	.png	6/1/2017 2:21:56 AM	6/1/2017 2:21:56 AM	10/30/2015 8:51:00 PM
StoreLogo.scale-10...	Parsing	.png	6/1/2017 2:21:56 AM	6/1/2017 2:21:56 AM	1/27/2017 12:01:05 AM
StoreLogo.scale-14...	Parsing	.png	6/1/2017 2:21:56 AM	6/1/2017 2:21:56 AM	1/27/2017 12:01:05 AM
StoreLogo.scale-18...	Parsing	.png	6/1/2017 2:21:56 AM	6/1/2017 2:21:56 AM	1/27/2017 12:01:05 AM

Figure 3-5-6: Column View Of Media Artifacts

In addition to these columns, columns are also generated for any Application Metadata. This includes information such as Make of the camera, Model of the camera, and GPS location.

EVIDENCE (39,201) Column view

Make	Model	Software	GPS Longitu...	GPS...	GPS Latitude	GPS...
Canon	Canon EOS-1D X Mark II	Adobe Photoshop CC 2018 (Macintosh)	117°50.5591'0.0000"	West	33°39.6513'0.0000"	North
Canon	Canon EOS 550D					
Canon	Canon EOS 5D Mark III	Adobe Photoshop CC 2017 (Macintosh)				
Canon	Canon EOS DIGITAL REBEL XTi	Adobe Photoshop CC 2019 (Macintosh)				
Canon	Canon EOS REBEL T5i	Adobe Photoshop CC 2019 (Macintosh)				
Canon	Canon EOS-1D X	Adobe Photoshop CS6 (Windows)				
Canon	Canon EOS REBEL T5i	Adobe Photoshop CC 2019 (Macintosh)				
Canon	Canon EOS 5D Mark III	Adobe Photoshop CC 2017 (Macintosh)				
NIKON CORPORATION	NIKON D60	Adobe Photoshop CC 2017 (Macintosh)				
NIKON CORPORATION	NIKON D700	Adobe Photoshop Lightroom 5.6 (Macintosh)				
OLYMPUS CORPORATION	C770UZ	paint.net 4.0.9				
OLYMPUS CORPORATION	C770UZ	v772-82				
OLYMPUS CORPORATION	C770UZ	paint.net 4.0.9				

Figure 3-5-7: Column View Of Media Artifacts

Videos

If, at the time of processing, 'Create a preview using still frames' was selected in the VIDEO options, the DETAILS pane for each video artifact will include a Preview card that is a filmstrip of the video content.

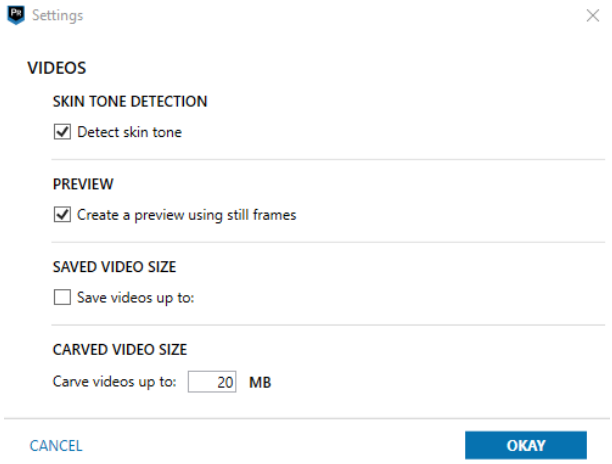


Figure 3-5-10: Video Options In Axiom Process

When reviewing Videos using Thumbnail view, the thumbnail of the video is displayed in Filmstrip View. During processing, whenever AXIOM encounters a video, it captures a screen shot of the video every 10%. This results in ten thumbnail images that are assembled into one filmstrip preview. This allows the examiner to quickly review the contents of a video file without having to watch the entire video.

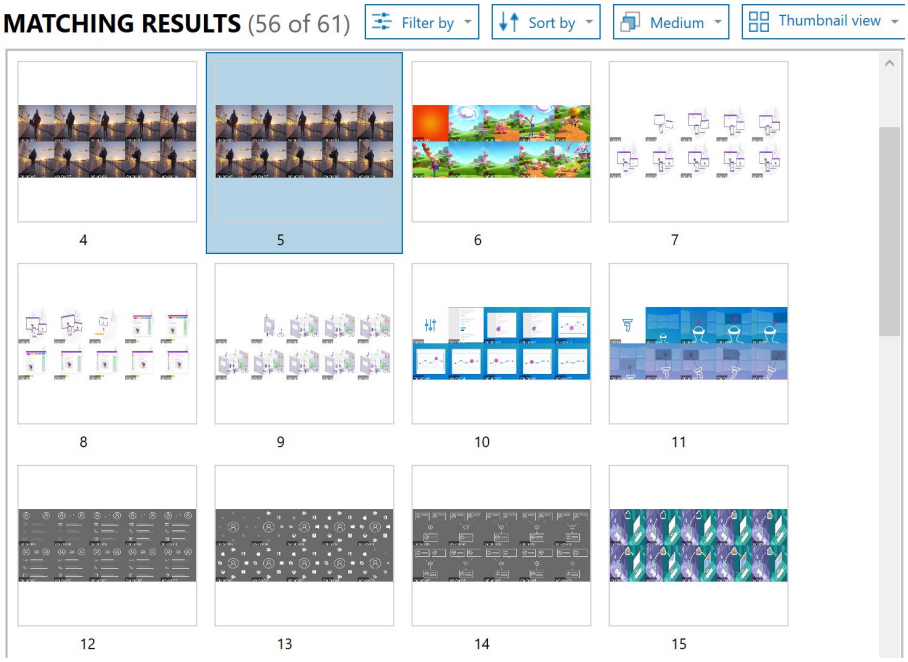


Figure 3-5-11: Filmstrip View

In addition, when selecting a video in the Evidence pane, two previews will be displayed in the Details pane. The first is the composite thumbnail, or filmstrip, consisting of the 10 thumbnail images. The second is an embedded player that allows the examiner to play the video.

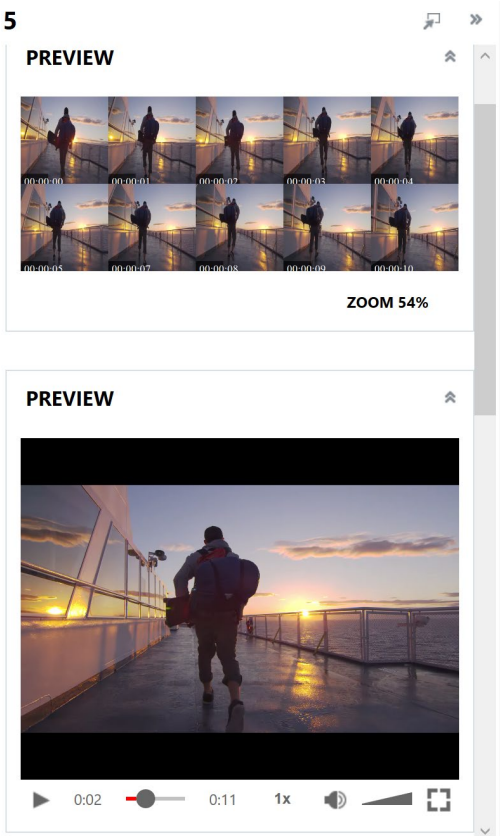


Figure 3-5-12: Filmstrip View And Integrated Preview Player

The standard detail review is also available for all pictures and videos under the Media categories. This viewer will allow the users to view metadata associated with the picture or video file including time/date values, size, make, model, software version, GPS coordinates, and associated hash values. Source Linking will allow the user to be directly linked to the file within the File System Explorer for further examination or exporting.

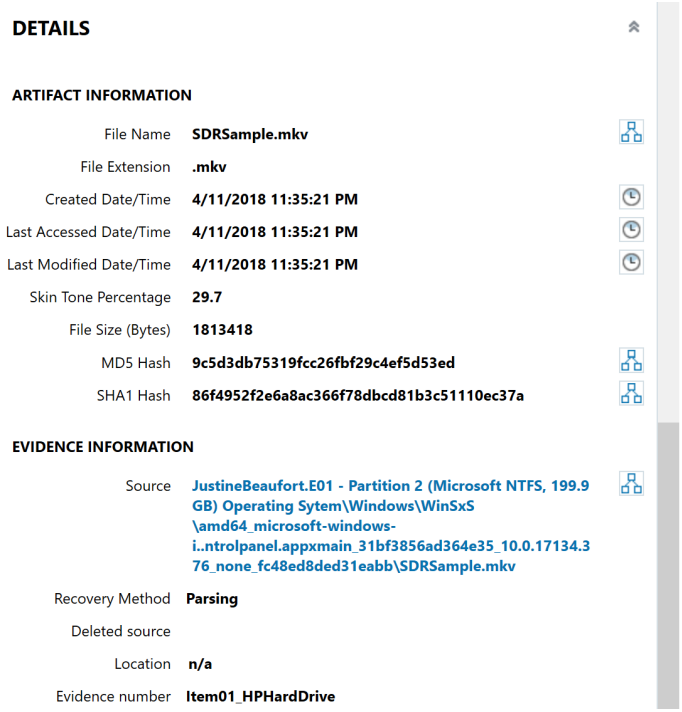


Figure 3-5-13: Details Card And Source Linking

Exercise 1. Carved Media

While Carved Video is a separate artifact category, Carved Pictures is not. In order to determine if a picture was carved or parsed from allocated space, consult the column heading "Recovery Method":

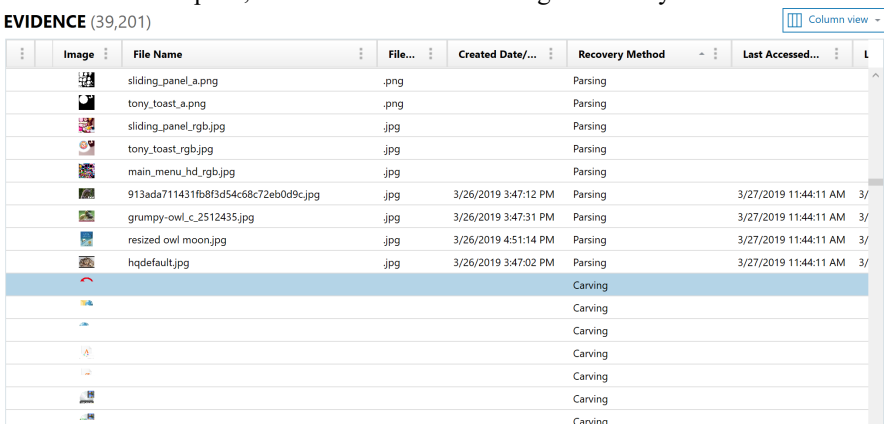


Figure 3-5-3: Recovery Methods Of Carving And Parsing

Exercise Question 1

Open case file "**DFI_Practical_1_Case**". Go to "**Artifacts**" then open "MEDIA/Pictures". As you can be seen in this screen shot (Figure 3-5-3), for pictures that were carved, there are no File Name or Date/Time stamps. Why there is no such information?

There is no information because the image is a carved image. This meant that it was a recovered image file from the unallocated space in the drive where it was either deleted or damaged. When the carving method is used, it only recovers files based merely on file structure and content, without any matching system meta-data, thus explaining why it did not have any file name or date/time stamps.

Exercise 2. Media Artifacts

We want to determine if there are any pictures on this hard drive that contain detailed application metadata, and if so, details about those pictures

Exercise Question 2

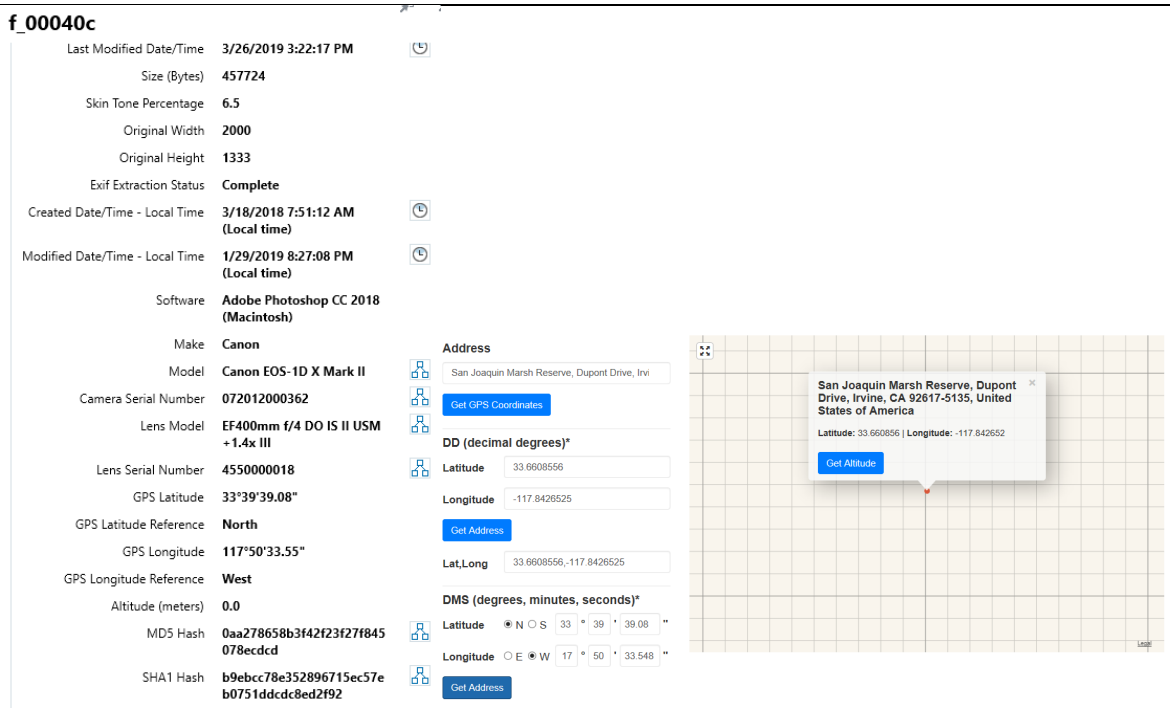
1. Go to the category "**Media**" –> "**Pictures**". How many total pictures (carved and parsed) are there on this drive?
   47,321.

2. While in "**Column View**", click on the column heading "**GPS Longitude**". This will sort the column and place all pictures containing GPS information together. How many pictures contain GPS information?
   1.

From the metadata, what device or software was used?
Software: Adobe Photoshop CC 2018 (Macintosh) Device: Canon EOS-1D X MARK II

What was the date/time picture was taken originally?
3/18/2018 7:51:12AM

Where was this picture taken?
San Joaquin Marsh Reserve, Dupont Drive, Irvine, CA 92617-5135, United states of America



-- End --