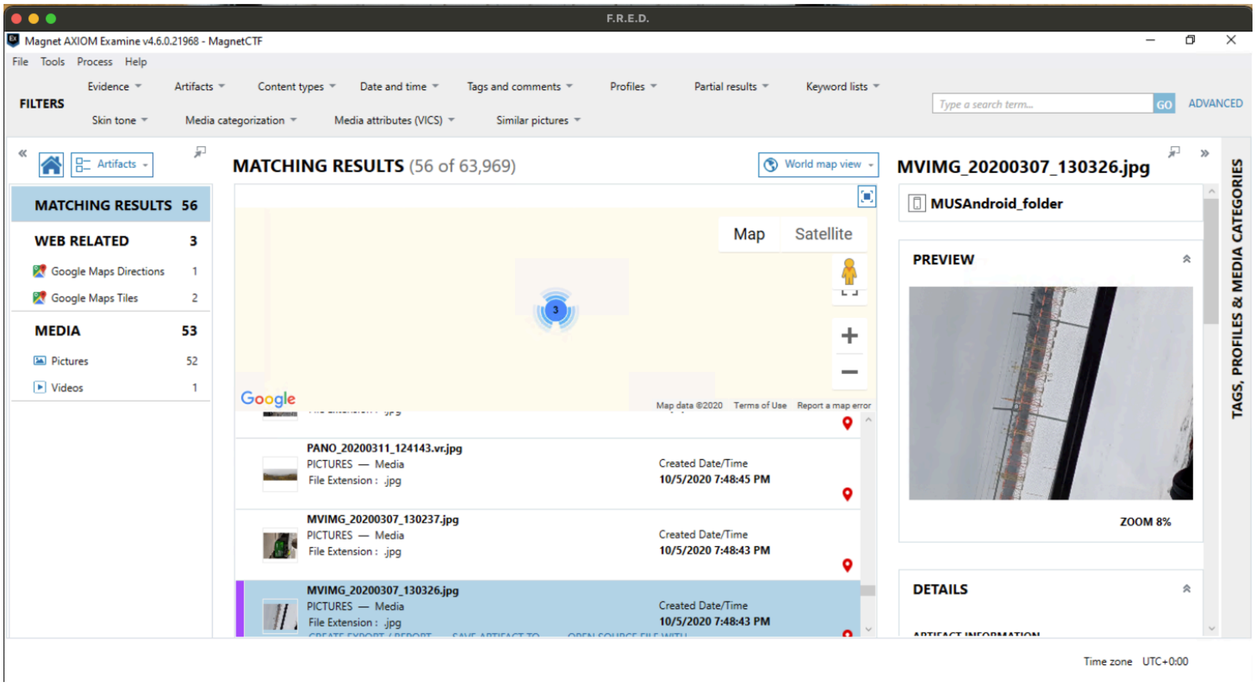
Magnet CTF:

Question 3 Solution Walk-Through

Challenge 3…Which exit did the device user pass by that could have been taken for Cargo?

In NJ it's common to inquire where someone resides with the question "What exit?" I found it interesting that some of the test data examined as part of the CTF included artifacts that *originated* in New Jersey. Yup. I hail from the land of Bruce Springsteen and Bon Jovi and if you even mention Jersey Shore in the context of a *reality* show, please just… quietly go away. Many types of forensic artifacts include metadata that ties that evidence to a particular location using GPS data. Maps and driving applications are among these, and commonly you can retrieve this data from photos and videos. (Note: a lot of services Facebook, Instagram, etc. – will have settings on whether or not they remove this data when media is shared.)
One of the really useful features of Magnet Axiom is that one of the selectable views is **World map view.**



MATCHING RESULTS (56 of 63,969)

MATCHING RESULTS	56
WEB RELATED	3
Google Maps Directions	1
Google Maps Tiles	2
MEDIA	53
Pictures	52
Videos	1

PANO_20200311_124143.vr.jpg
PICTURES — Media
File Extension : .jpg
Created Date/Time
10/5/2020 7:48:45 PM

MVIMG_20200307_130237.jpg
PICTURES — Media
File Extension : .jpg
Created Date/Time
10/5/2020 7:48:43 PM

MVIMG_20200307_130326.jpg
PICTURES — Media
File Extension : .jpg
Created Date/Time
10/5/2020 7:48:43 PM

MVIMG_20200307_130326.jpg
MUSAndroid_folder

Selecting this view limits the presentation of artifacts to just those that include GPS data. Reviewing the artifacts with GPS metadata there was nothing that immediately presented as a reference to *exit* or *cargo*.

However, just like Transformers, within these artifacts there is more than meets the eye. In the screenshot above you'll see that several files start with MVIMG_ . These files are Google Motion Photos, essentially the functional equivalent of Live Photos on iOS.

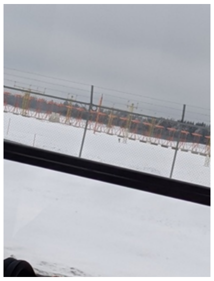
A few weeks back I saw a Magnet webinar: Mobile Artifact Comparison – Understanding the Similarities Between iOS and Android Data
https://www.magnetforensics.com/resources/mobile-artifact-comparison-webinar-recording-oct-7

Included in the comparison were both of these "live photo" types and B1n2h3x reference that previously she had carved out the MVIMG_ files and was able to isolate the key frame and the MP4 image (video) that comprised it.

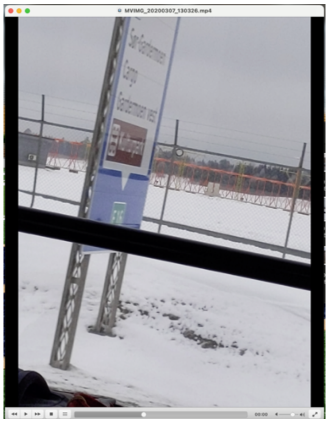
If you're not supplementing your Magnet course training with their free webinars you're really missing out.

- Using Axiom, I exported all the MVIMG_ files to a folder.
- Next I utilized GoMoPho - Google motion photos video extractor https://github.com/cliveontoast/GoMoPho and ran it against the directory which split the MVIMG_ files into .jpg and .mp4
- From there I loaded the videos into VLC. They were only a few seconds long and played very fast. This is where the playback speed settings in VLC come in handy. Drop it back to the slowest it will play.

When initially previewed, MVIMG_20200307_120326.jpg presented what appeared as a view from the highway in winter. There are no immediate discernable landmarks in the photo.



However, when the extracted video is played, we get a few seconds visibility from the car on the highway, including passing the following sign:



Among the words on the sign we can read “Cargo” and the exit show at the bottom of the sign, **F16**.