CERIAS

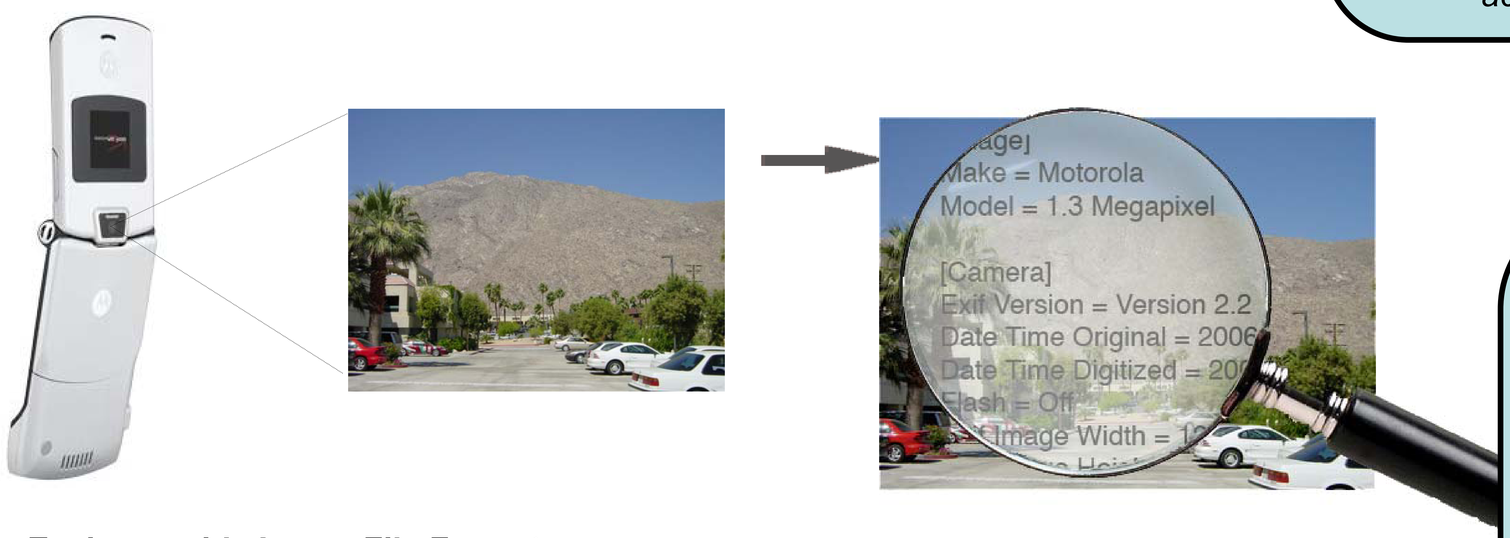
the center for education and research in information assurance and security

Mobile Phones: Digital Photo Metadata

Sean Sobieraj, Richard Mislan

Developing reliable methods of data recovery is critical for any forensic investigation, and current methods of mobile phone forensics leave much to be desired. There are many different software packages and utilities available today that attempt to forensically retrieve data from mobile phones; however the majority of them work selectively due to the lack of standards in the mobile phone market. This greatly limits their effectiveness and reliability. Due to their sometimes questionable performance, the validity of the forensic data will benefit from additional sources of information. This paper provides a brief introduction to a new source of potential forensic evidence from digital photographs in mobile camera phones. This data may have a wide range of applications and may provide new ways to definitively determine certain information in a forensic investigation.

Increased memory storage and high quality digital cameras are almost commonplace among mobile phones, making them capable of storing large quantities of images. These images may contain metadata, or additional embedded information, that describes critical details about the picture. This information may provide the time and date the picture was taken, the make and model of the camera that was used, and a large amount exposure information. This metadata was examined from pictures taken with seven different mobile phones in an attempt to determine its availability, accuracy and usability as forensic evidence.



Exif Data …
- *is independent of phone settings*
- *records time in UTC*
- *maintains its integrity through file transfer*
- *is part of the picture, not a file attribute*
- *applies to all digital photographs, not just from mobile phones*
- *may contain an unmodified version of an image itself*
- *may contain hidden strings of data*

and unfortunately it …
- *is easily modified*
- *is currently inconsistent*

Exchangeable Image File Format

Hundreds of possible Exif tags each store unique information. Some examples are:

- Exposure Time
- Image Resolution
- Image Height and Weight
- Shutter Speed
- Flash Usage
- Equipment Make and Model
- Timestamps
- Digital Zoom Ratio
- Location Information using GPS

The four Exif tags in the following table were the main focus of this research:

Tag ID	Tag Name	Field Name
010F	Manufacturer of image input equipment	Make
0110	Model of image input equipment	Model
9003	Date and time original image was generated	DateTimeOriginal
9004	Date and time image was made digital data	DateTimeDigitized

Results

- The table to the right shows the results from the seven camera phones.
- The only consistency was the format of the timestamps when they were available.
- Their availability, along with the other Exif data, was inconsistent and rather limited.
- The Make and Model tags contained different types of information depending on the phone.
- All available Exif information was 100% accurate.
- All Microsoft Windows file timestamps are reset when an image is copied from the phone.

					Exif Tags			
Phone	**Image Filename**	**Time Taken**	**Port Monitor Time**	**Windows Modified Timestamp**	**Make**	**Model**	**DateTimeOriginal**	**DateTimeDigitized**
Audiovox CDM-8910 (Verizon)	photo_0022.jpg	12:18 PM	NA	12:23:02 PM	NA	NA	NA	NA
LG Fusic LX-550 (Sprint)	P_00060.jpg	10:58 AM	15:58:53	11:32:59 AM	Sprint	Fusic	2006-11-07 15:58:53	2006-11-07 15:58:53
Motorola RAZR V3c (Verizon)	02-11-06_1310.jpg	1:09 PM	17:10:39	1:12:34 PM	Motorola	1.3 Megapixel	2006-11-02 17:10:39	2006-11-02 17:10:39
Motorola SLVR BC60 (Cingular)	11-07-06_1051.jpg	10:55 AM	NA	11:18:48 AM	NA	NA	NA	NA
Motorola V276 (Verizon)	10-17-06_1206.jpg	12:06 PM	16:06:57	12:12:24 PM	MOTO	1.2 MP	2006-10-17 16:06:57	2006-10-17 16:06:57
Motorola V551 (Cingular)	10-17-06_1228.jpg	12:26 PM	NA	12:31:56 PM	NA	NA	NA	NA
Nokia 6102b (Cingular)	Image009.jpg	11:38 AM	NA	11:42:38 AM	NA	NA	NA	NA

PURDUE UNIVERSITY

CERIAS

Discovery Park e-Enterprise Center