



AMPED AUTHENTICATE

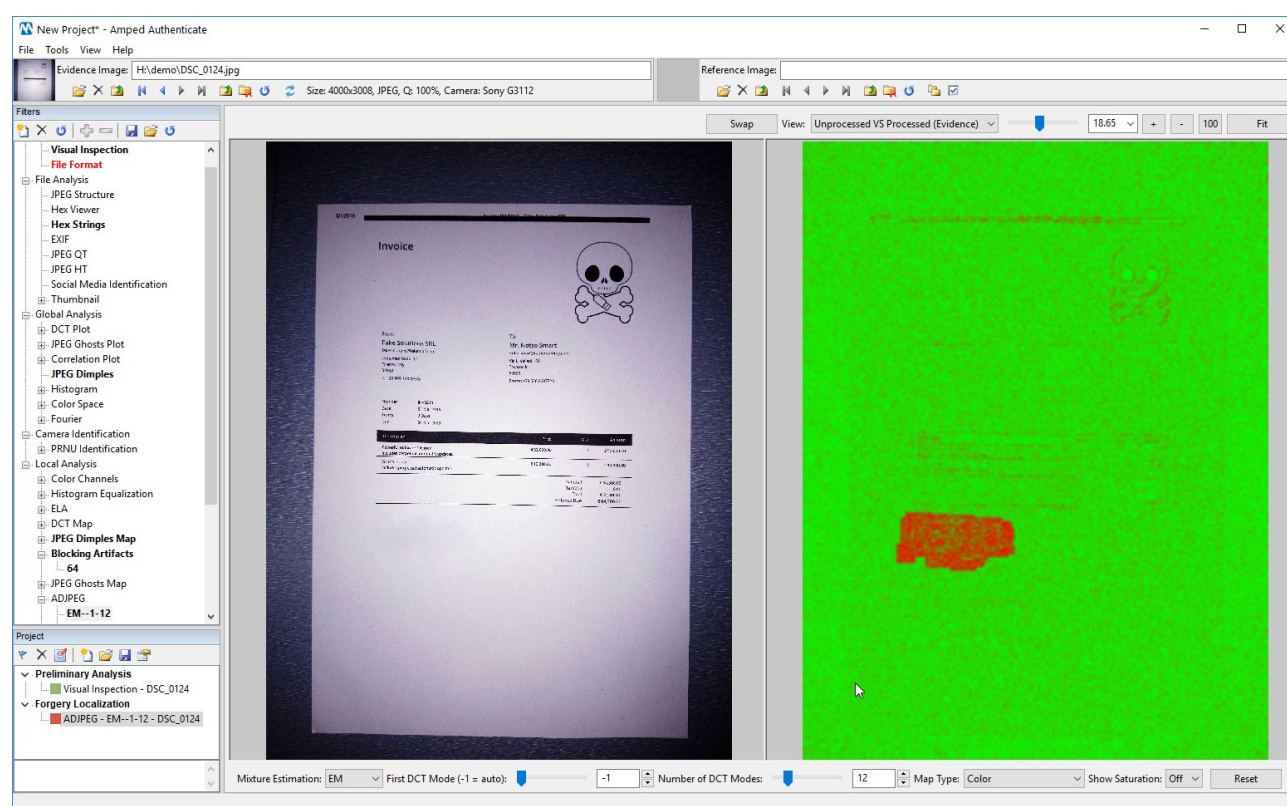
PHOTO ANALYSIS AND TAMPER DETECTION

- Detect tampered areas in images
- Determine the authenticity of images and documents
- Analyze multiple images with batch tools
- Identify the device used to take a photo or video
- Reveal whether an image or video has been recompressed
- A collection of the most powerful, real-world-application authentication filters and techniques based on science

WHAT IS AMPED AUTHENTICATE?

[Amped Authenticate](#) is the leading forensic software for unveiling the processing history of digital images and videos. It provides a suite of powerful tools to determine whether images are unaltered originals, originals generated by a specific device, or the result of manipulation using a photo editing software, making their admissibility as evidence questionable. Amped Authenticate is used by the world's top forensic labs, law enforcement agencies, government, military, and security organizations.

Authenticate is a collection of the most useful, real-world-application authentication filters and techniques identified by image analysts, based on hundreds of scientific papers and studies. These have been built into an easy-to-use, yet amazingly powerful interface to help investigators answer the many questions of authenticity and integrity surrounding today's digital images.



WHY AMPED AUTHENTICATE?

With the constant development and introduction of new digital technologies, digital images and videos are now key sources of evidence for investigations. And thanks to social media and the prevalence of high-quality mobile phone cameras, there is a dramatic increase of imagery submitted as evidence, by citizens and witnesses, to law enforcement agencies.

Modern digital images are mines of information: in addition to the visual content, metadata often contain precise information about when, where and who captured the image. But unfortunately, in just a few seconds, both visual content and metadata can now be easily manipulated to create credible fakes.

Without solid ways to validate that the information is accurate, these photographs could pose issues when they are presented as evidence in a case and in court. Therefore, thoroughly investigating an image and ensuring its trustworthiness and source is critical in today's investigations.

The courts and savvy defense attorneys and prosecutors have begun to understand how easy it is to manipulate a digital photo, so experts are often asked to analyze the authenticity and provenance of digital images.

A practical example of this is the Beckley case that the Second Appellate District Court (Los Angeles, CA) ruled:

...In this opinion we hold that the prosecution's failure to authenticate a photograph ...should have barred their admission... We also conclude there was insufficient evidence to support the street gang enhancement of each defendant's sentence."

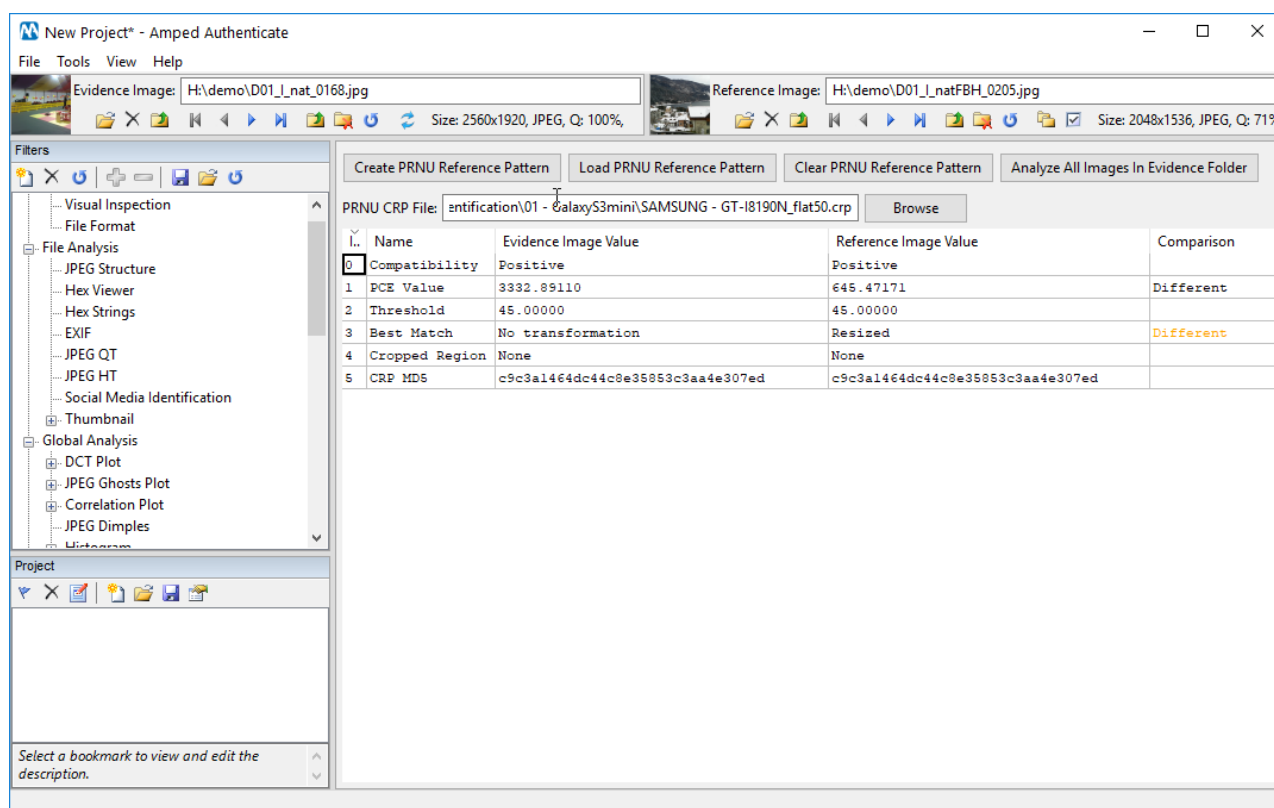
The court also decided that a photograph is a "writing" and stated:

...Authentication of a writing is required before it may be received in evidence. (Evid. Code, §§ 250, 1401, subd. (a)...) (People of CA vs. Beckley, Los Angeles County Superior Court Case Number: TA094886 6/9/10)

With this ruling, precedent is set in California for the challenge of any digital evidence on the grounds of authenticity or lack of scientific authentication.

As precedent is set by an appellate court, this doctrine may be applied elsewhere in the US where similar evidence rules exist.

It is also necessary to be able to link photographs to a specific camera and consequently to a suspect. Billions of images are uploaded to the internet and shared on social media platforms every day. Investigators are constantly faced with the task of trying to identify the person who posted the original photo on the internet. Linking a photo to a camera is now as important as linking a bullet to a gun.



THE DIFFICULT WAY OF WORKING

Understanding if an image is an original or the result of manipulation is not an easy task. Only a few world-recognized experts were able to determine if an image used as evidence in court was an original or if someone tampered with it, making the photo unacceptable as evidence or alibi. Experts previously had to do this with self-made tools, very specialized scientific techniques, or a cobbled-together set of very expensive mathematical/engineering tools.

THE EASY WAY OF WORKING

In order to permit more investigators and forensic labs to analyze the processing history of photos, Amped Software has integrated into one single software package, forensically accepted techniques that were previously only available to top-notch researchers.

Amped Authenticate empowers law enforcement agencies and forensic lab experts with very effective tools to identify tampering on an image and to verify if a digital photograph has been generated by a specific device. The camera ballistics feature in Amped Authenticate determines that a specific device - and not just the camera make or model – was used to generate a specific photo.

As opposed to other solutions that provide only one, or just a few, tools for authenticating images, Amped Authenticate puts the power of multiple scientific tools, procedures, and reporting, in one software package to improve the user's ability to detect tampered images or determine originality.

All tools available in Amped Authenticate are based on peer reviewed scientific papers, each performing a different test on the structure of an image and how it was created.

MAIN FEATURES

World Leader

Amped Authenticate is the leading software for forensic image authentication and tamper detection on digital images. Used by the world's top forensic labs, law enforcement, government, military, and security organizations, Amped Authenticate is the most complete image forensics suite. Amped partners with universities and research groups to remain constantly up to date with scientific achievements, in order to fill the gap, as quickly as possible, between the research lab and usage in real cases.

Powerful

Amped Authenticate provides more than 40 tools and filters with customizable configuration and optional post-processing parameters.

Portable

Works on a laptop in the field as easily as on a desktop in the lab.

Fast

Amped Authenticate's *Batch Processing* applies all filters to all images in a folder. *Smart Report* automatically selects the most appropriate subset of filters for each image, providing brief and readable reporting. Saved cache folders allow for speedy follow-up analysis.

Ballistics

Image ballistic tools allow you to verify which camera was used to shoot a specific photo, even if the photo has been scaled, cropped or re-saved. Experiments demonstrate that image ballistics can also work with images uploaded to social media platforms.

Comparison

Compare the results of two images side by side to understand where and how an image has been modified.

Integrations

Amped Authenticate is integrated with some of the leading tools used by many law enforcement organizations: Griffeye Analyze DI, CameraForensics, Microsoft Excel, Google Maps, Google Images, Flickr. Integrations increase speed and accuracy of your work. Thanks to Authenticate's command line interface, users are also free to write their own integrations to link Authenticate to other tools.

Certifies Evidence

Amped Authenticate automatically generates a report detailing all the bookmarked analyses, along with comments, settings and algorithms used, as well as their source information (including

publication date and page number), which makes it easy to present in court. The report layout and theme can be customized.



Flexible and Affordable

Since Amped Authenticate is compatible with standard PCs (Windows 7/8/10/11, 32 bit and 64 bit versions), the time and cost to deploy are minimal. As hardware standards change quickly, Amped Authenticate does not bind you to a platform that will soon be obsolete or cannot be upgraded without major expense (if at all). All required dependencies are installed during program setup, without any need for expensive external tools or environments.

UNDERSTANDING THE TERMS

In order to understand how Amped Authenticate works, we need to first understand what it means when an image is original or has been tampered with.

WHAT IS A CAMERA ORIGINAL IMAGE?

A camera original image is a picture taken by a camera device and never touched by any software after acquisition, not even within the device itself. Any manipulation introducing changes to pixels or metadata (including simple image rotation) breaks the integrity of the file, which is no longer considered original. Thus, a file which is not original can raise doubts about the authenticity of the image.

WHAT IS AN AUTHENTIC IMAGE?

An authentic image is an image which is an accurate representation of what it purports to be. An authentic image may have undergone some processing operations (e.g., scaling, minor cropping, recompression, uploading to a social media platform, ...) provided that such processing does not alter the meaning of the depicted scene. Therefore, an image which is not Camera Original may still be Authentic. Depending on the case, the authenticity of an image may also depend on the context in which it is published: for example, a truthful picture of an event could be deceptively used as proof for a different event, or a person's photo could be used to create a fake social media profile.

WHAT IS AN ALTERED IMAGE?

A photo that has undergone some kind of processing after acquisition (including simple rotation, resize, enlargement, cropping or other form of editing) is no longer an original, but is altered. It could also be a picture taken from a camera device (at this point it is an original) but uploaded to social networks, like Facebook. It is now no longer an original and is considered altered because the social network server recompresses and resizes the image. Any image processing software usually alters the file structure of the picture.

WHAT IS IMAGE TAMPERING?

Image tampering happens when an image has intentionally been modified to hide vital information by doing things like cut, paste, crop, delete and so on.

WHAT IS CAMERA IDENTIFICATION?

Camera ballistics is the task of linking a specific camera or smartphone to a specific photo captured by that device. Camera ballistics also makes it easy to differentiate between cameras and smartphones of the same make and model. Today, the main technology enabling camera ballistics is PRNU (Photo-Response Non-Uniformity) analysis: there are imperfections in each imaging sensor that are unique to that specific piece of silicon, although they cannot be seen with the naked eye. Identifying the pattern, and then comparing this with an image, is a reliable way of proving that the image was, or was not, taken by that specific camera.

It is also possible to carry out hybrid source identification for investigating the originating device of a digital video using images as reference (or vice-versa).

WHAT IS BATCH PROCESSING?

Batch Processing automatically applies all filters to one image or all images in a folder. This allows for quick automatic analysis and comparison of images. Authenticate also features the *Smart Report* tool, which applies a subset of automatically chosen filters to one or all images in a folder, producing an intuitive report which distinguishes camera original images from altered and tampered images.

HOW IT WORKS

Amped Authenticate provides numerous *Filters*, grouped into *Categories*, that help to determine if an image is an original, or has been altered or tampered with, by using photo editing software.

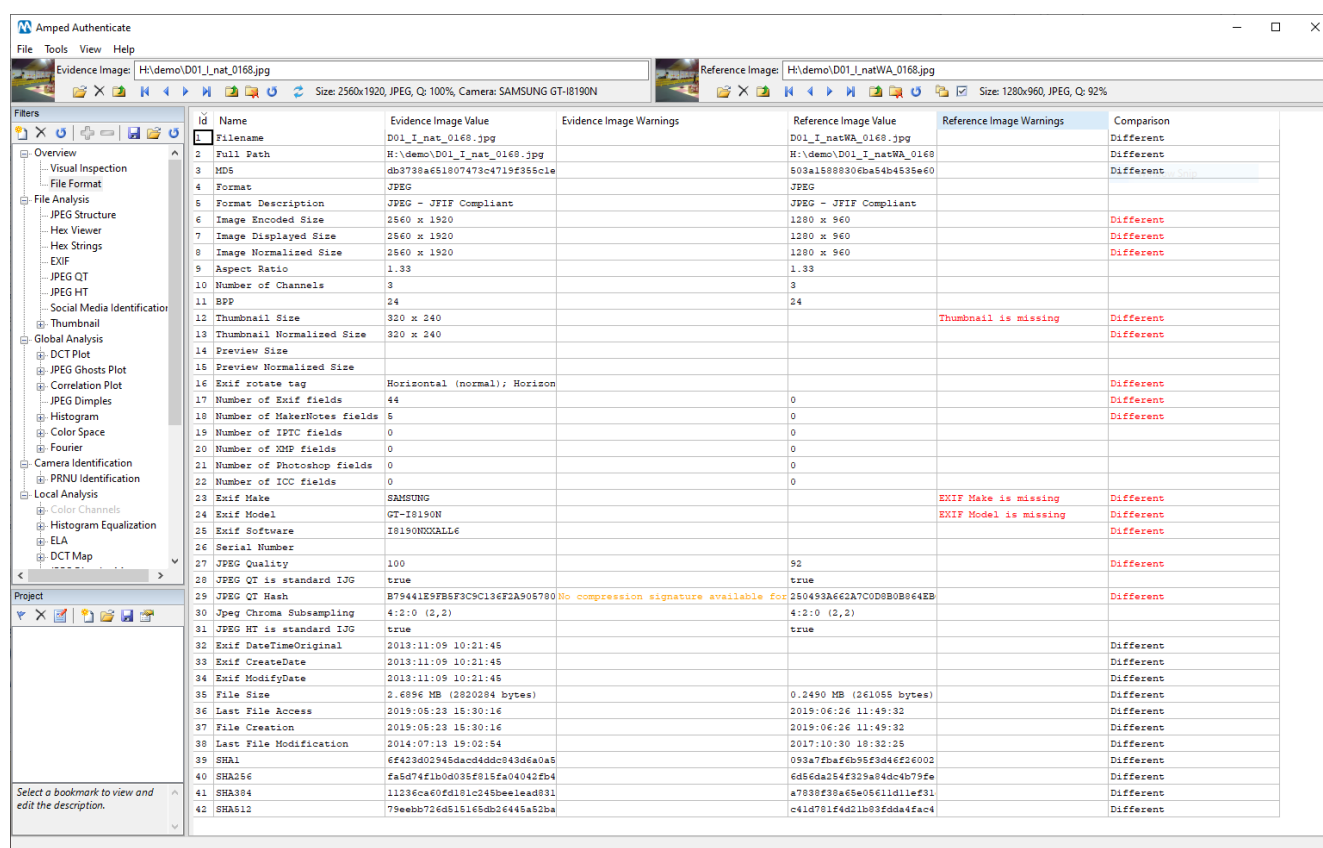
The tests provided in Amped Authenticate help call your attention to some details you may want to further examine to help you determine the authenticity of the image. Amped Authenticate can also determine if an image under investigation was actually taken by a specific camera. How does Amped Authenticate do all this?

HOW DOES AMPED AUTHENTICATE HELP IDENTIFY A CAMERA ORIGINAL OR AN AUTHENTIC IMAGE?

By using the filters in the *Overview* category, the analyst can visually inspect the image (taking advantage of zoom with no interpolation and level adjustment) and get a quick overview of the most important image file properties (such as image format, resolution, number of channels, aspect ratio, etc.) and metadata.

Authenticate does not just show data, it also helps interpret data: for example, the user is warned when some image characteristic or metadata that is not typical of camera original images is detected (see figure below). Furthermore, when a reference original image is available, Authenticate allows for a fast and intuitive comparison, highlighting elements having different values. Once again, not all differences weigh the same significance: it is normal to have different date of acquisition, while a different JPEG quantization table is more suspicious. Authenticate will warn the user only when problematic differences are found.

Batch comparison between evidence image file format against hundreds or thousands of reference images is also possible. While not being exhaustive by design, the *Overview* category frequently identifies, in just a few seconds, images whose integrity is broken.



	Evidence Image Value	Evidence Image Warnings	Reference Image Value	Reference Image Warnings	Comparison
Filename	D01_I_nat_0168.jpg		D01_I_natWA_0168.jpg		Different
Full Path	H:\demo\D01_I_nat_0168.jpg		H:\demo\D01_I_natWA_0168		Different
MD5	db3738a651807473c4719f355c1e		503a15888306ba54b4535e60		Different
Format	JPEG		JPEG		
Format Description	JPEG - JFIF Compliant		JPEG - JFIF Compliant		
Image Encoded Size	2560 x 1920		1280 x 960		Different
Image Displayed Size	2560 x 1920		1280 x 960		Different
Image Normalized Size	2560 x 1920		1280 x 960		Different
Aspect Ratio	1.33		1.33		
Number of Channels	3		3		
BPP	24		24		
Thumbnail Size	320 x 240			Thumbnail is missing	Different
Thumbnail Normalized Size	320 x 240				Different
Preview Size					
Preview Normalized Size					
Exif rotate tag	Horizontal (normal); Horizon				Different
Number of Exif fields	44		0		Different
Number of MakeNotes fields	5		0		Different
Number of IPTC fields	0		0		Different
Number of XMP fields	0		0		
Number of Photoshop fields	0		0		
Number of ICC fields	0		0		
Exif Make	SAMSUNG			EXIF Make is missing	Different
Exif Model	GT-I8190N			EXIF Model is missing	Different
Exif Software	I8190NOKIA6				Different
Serial Number					
JPEG Quality	100		92		Different
JPEG QT is standard IJG	true		true		
JPEG QT Hash	B79441E9FB5F3C9C136F2A905780	No compression signature available for	2504593A62A7C0D80B0864EB		Different
Jpeg Chroma Subsampling	4:2:0 (2,2)		4:2:0 (2,2)		
JPEG HT is standard IJG	true		true		
Exif DateTimeOriginal	2013:11:09 10:21:45				Different
Exif CreateDate	2013:11:09 10:21:45				Different
Exif ModifyDate	2013:11:09 10:21:45				Different
File Size	2.6896 MB (2820284 bytes)		0.2450 MB (261055 bytes)		Different
Last File Access	2019:06:23 18:30:16		2019:06:26 11:49:32		Different
File Creation	2019:06:23 18:30:16		2019:06:26 11:49:32		Different
Last File Modification	2014:07:13 19:02:54		2017:10:30 18:32:25		Different
SHA1	c6423d02945dacc4ddc843d6a0a5		093a7fbaf6b96f3d46cf26002		Different
SHA256	fa5d74f1b0d035f915fa04042fb4		6d56da254f329a84dc4b79fe		Different
SHA384	11236ca60fd181c245bbeelead931		a7838f38a65e05611d11ef31		Different
SHA512	79eebb726d516165db26445a52ba		c41d781f4d21b83fdda4fae4		Different

Figure 1: comparing a camera original image from an Apple iPhone 6 (left side) with its corresponding version sent via WhatsApp (right side). Note the image on the right shows three warnings, suggesting image integrity is broken. Moreover, several problematic differences between the two images are highlighted on the right column.

Filters in the *File Analysis* category allow users to look in depth at the details of image format and metadata. The user can compare the JPEG header of the image with reference material, check whether the image JPEG Quantization Table matches one of the 14.000+ stored in Authenticate's internal database, which can be integrated with user submitted images.

New Project* - Amped Authenticate

File Tools View Help

Evidence Image: H:\demo\D19_l_nat_0251.jpg Size: 3264x2448, JPEG, Q: 95%, Camera: Apple iPhone 6 Plus

Reference Image:

Filters

- Visual Inspection
- File Format
- File Analysis
 - JPEG Structure
 - Hex Viewer
 - Hex Strings
 - EXIF
 - JPEG QT**
 - JPEG HT
 - Social Media Identification
- Thumbnail
- Global Analysis
 - DCT Plot
 - JPEG Ghosts Plot
 - Correlation Plot
 - JPEG Dimples
 - Histogram
 - Color Space
 - Fourier
- Camera Identification
 - PRNU Identification
 - SAMSUNG__GT_I8190N_flat50
- Local Analysis
 - Color Channels
 - Histogram Equalization
 - ELA
 - DCT Map
 - JPEG Dimples Map
 - Blocking Artifacts
 - 64
 - JPEG Ghosts Map
 - ADJPEGL
 - EM--1-12
 - Iterative--1-48
 - NADJPEG

Project

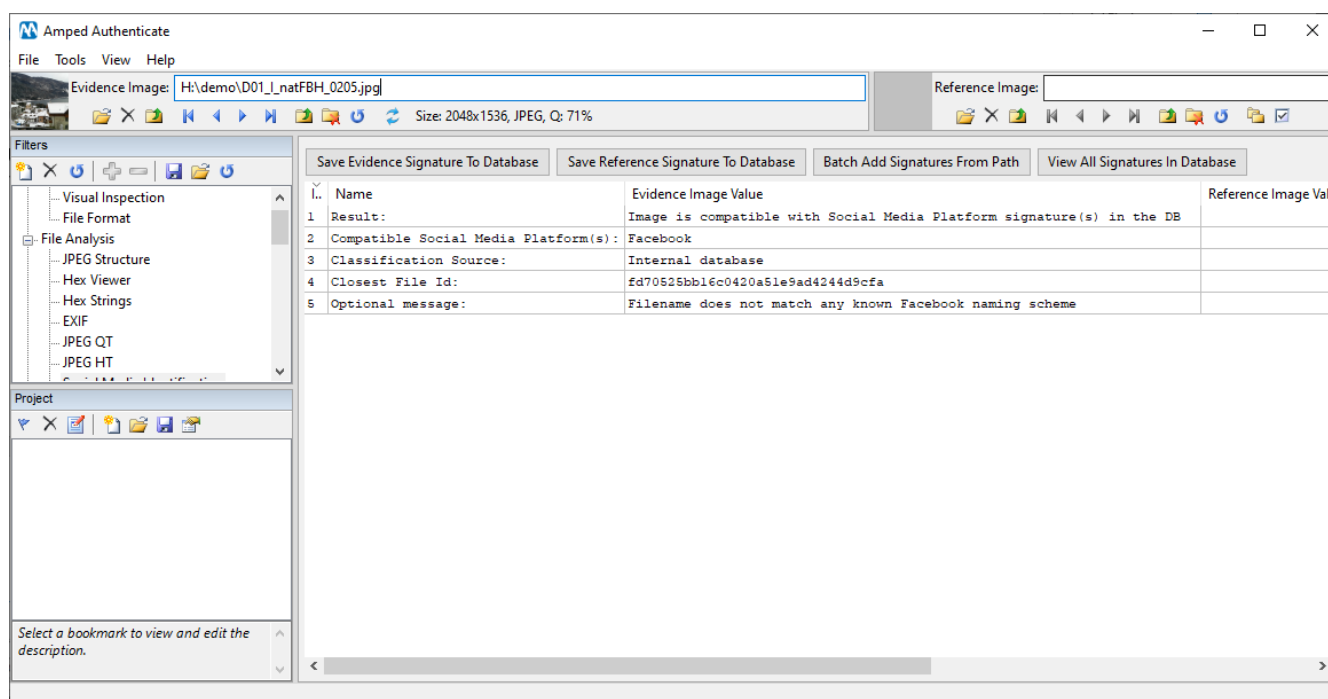
Select a bookmark to view and edit the description.

Save Evidence QTs To Database Save Reference QTs To Database Find Images With Same QTs View All QTs In Database

Id	Name	Evidence Image Value	Reference Image Value	Comparison
1	Compatible Cameras (Internal)	Apple,iPad Apple,iPhone 5 Apple,iPhone 6 Apple,iPhone 6 Plus Apple,iPhone 7 Plus Apple,iPhone XR Apple,iPhone XS Apple,iPhone XS Max		
2	Compatible Software (Internal)			
3	Compatible Cameras (User)			
4	Compatible Software (User)			
5	Image Quality	95		
6	Standard Table	false		
7	Color Space	YCbCr		
8	Chroma Subsampling	4:2:0 (2,2)		
9	QT Hash	9302D3AD39DC2BEADCF511EEE1E59DE		
10	QT 1 (Luma)	1 1 1 2 3 4 1 1 1 2 3 4 1 1 2 3 4 5 2 2 3 4 5 6 3 3 4 5 6 7 4 4 5 6 7 8 5 5 6 7 8 9 6 6 7 8 9 9		
11	QT 2 (Chroma)	1 1 2 4 9 9 1 2 2 6 9 9 2 2 5 9 9 9 4 6 9		
12	QT 3 (Chroma)			
13	Thumbnail Image Quality	95		
14	Thumbnail Standard Table	false		
15	Thumbnail Color Space	YCbCr		
16	Thumbnail Chroma Subsampling	4:2:0 (2,2)		
17	Thumbnail QT Hash	9302D3AD39DC2BEADCF511EEE1E59DE		
18	Thumbnail QT 1 (Luma)	1 1 1 2 3 4 1 1 1 2 3 4 1 1 2 3 4 5 2 2 3 4 5 6 3 3 4 5 6 7 4 4 5 6 7 8 5 5 6 7 8 9 6 6 7 8 9 9		

Figure 2: the JPEG QT filter shows that information about image make and model available in Exif metadata (Apple iPhone 6 Plus) are indeed confirmed by the fact that Quantization Tables of the image match those available in Authenticate's database for that model.

Since images uploaded to Social Media Platforms (SMPs) usually undergo several processing steps, which may invalidate some of the existing forensic analyses, Authenticate checks whether the image shows traces of processing from several well-known SMPs (such as Facebook, Twitter, Flickr, Instagram, and more).



HOW DOES AMPED AUTHENTICATE IDENTIFY AN ALTERED OR TAMPERED IMAGE?

A solid image forensic analysis requires revealing not only the presence of spliced regions, but also the global processing undergone by the image. An image with seemingly “innocent” metadata could still bear evident traces of processing in its pixels.

Filters in the Global Analysis category allows for the reconstruction of the digital processing history of the image: multiple JPEG compressions are exposed by the JPEG Ghosts and DCT Plot filters, while digital zoom or resizing becomes evident thanks to the Correlation Plot. The JPEG Dimples filter detects presence of compression artifacts that are left by some camera models, thus potentially strengthening the attribution of the image to a certain device.

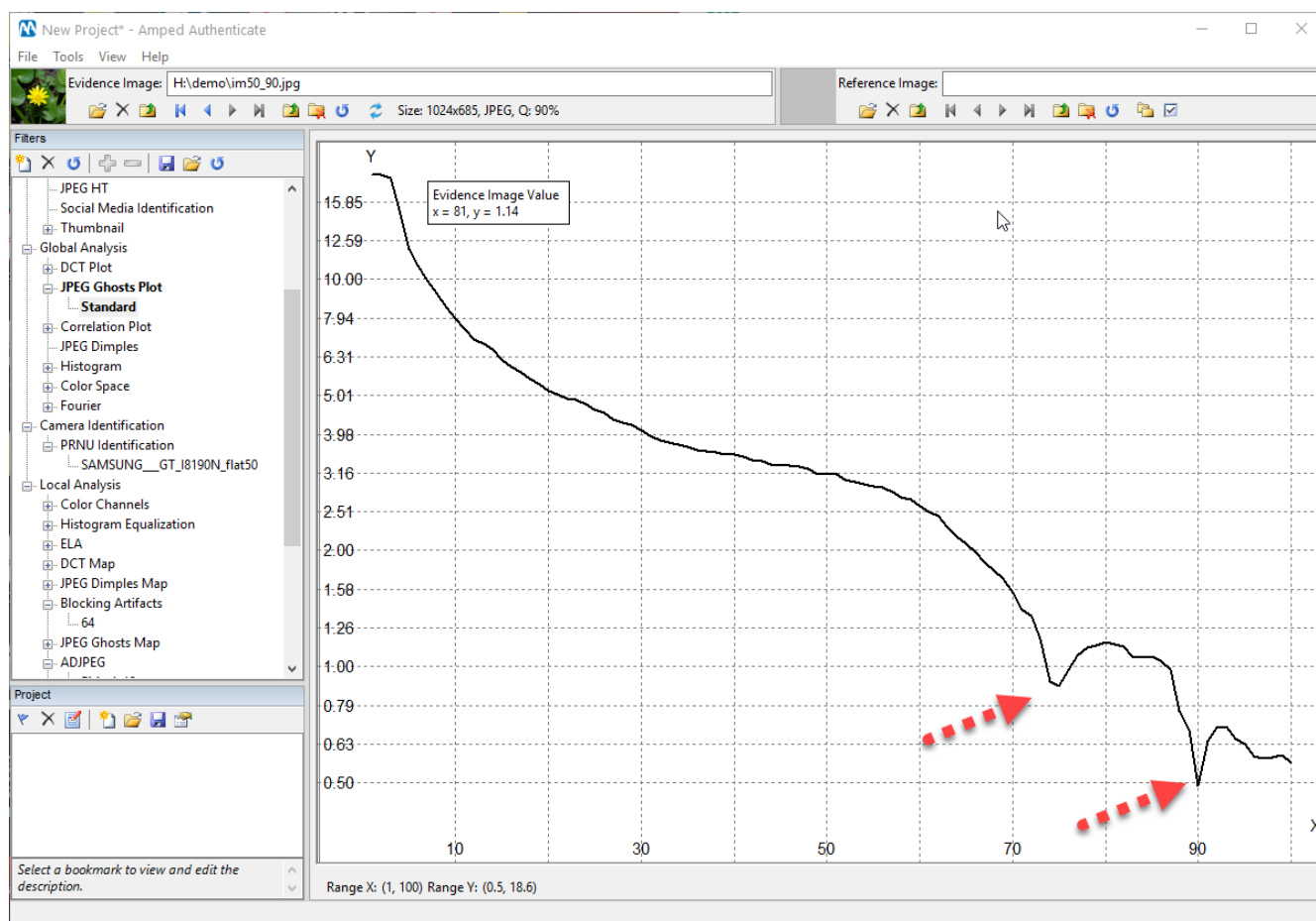


Figure 4: the two “valleys” in the JPEG Ghost plot reveal that the image has been JPEG compressed twice, once at quality 75 and once at quality 90.

Once the global processing history has been investigated, filters of the Local Analysis category will analyze image pixels to provide fine grained forgery maps, that is, maps indicating where alteration took place. Many of these filters are also capable of self-interpreting the map to raise a warning when something looks suspicious.

Authenticate features 17 different filters dedicated to forgery localization, in order to detect different kinds of splicing (erased regions, cloned objects, inserted objects, local smudging or recoloring, etc.), and the number of filters for this analysis keeps growing constantly.

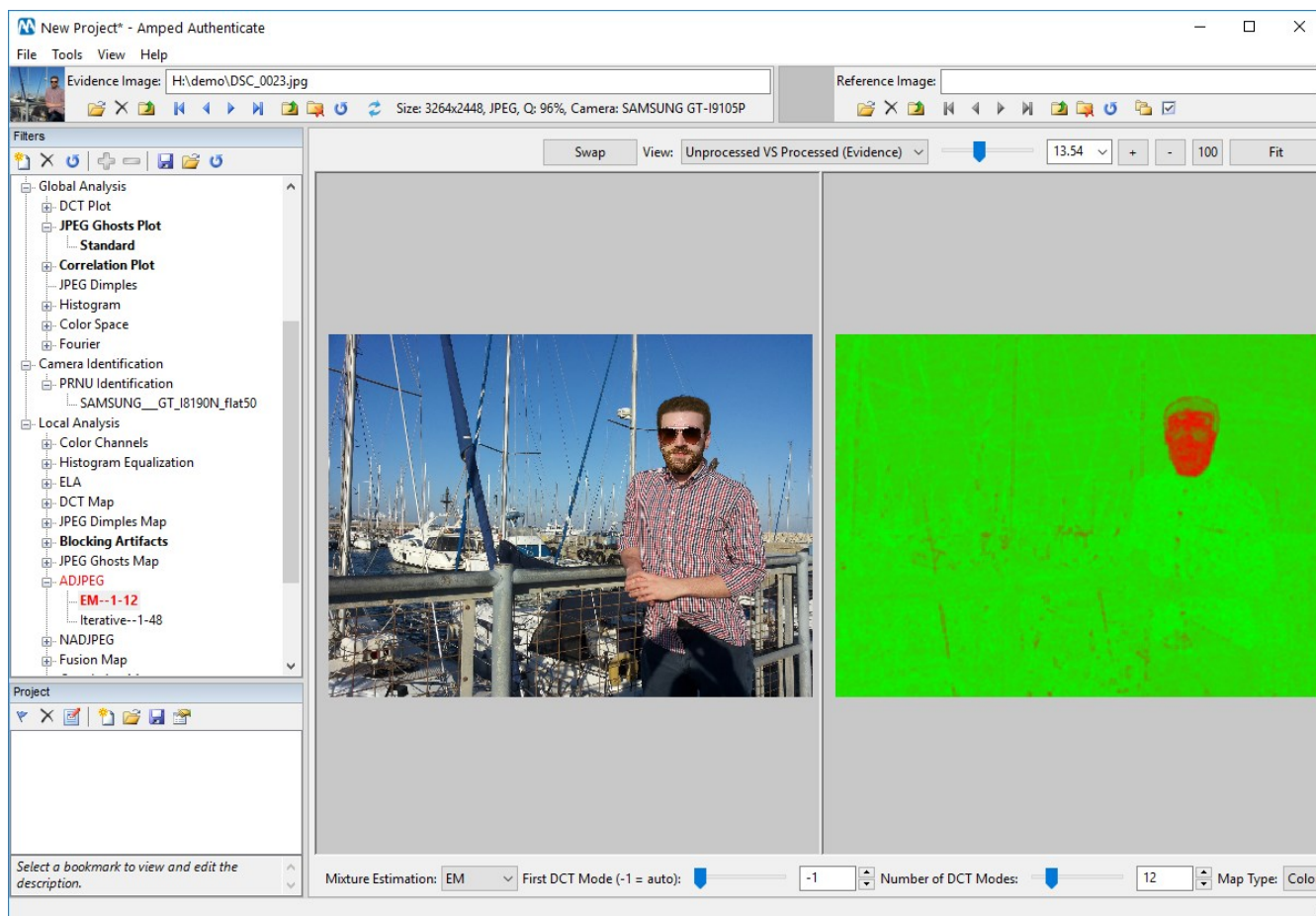


Figure 5: The Aligned Double JPEG (ADJPEG) filter clearly shows that the face of the subject has been tampered with.

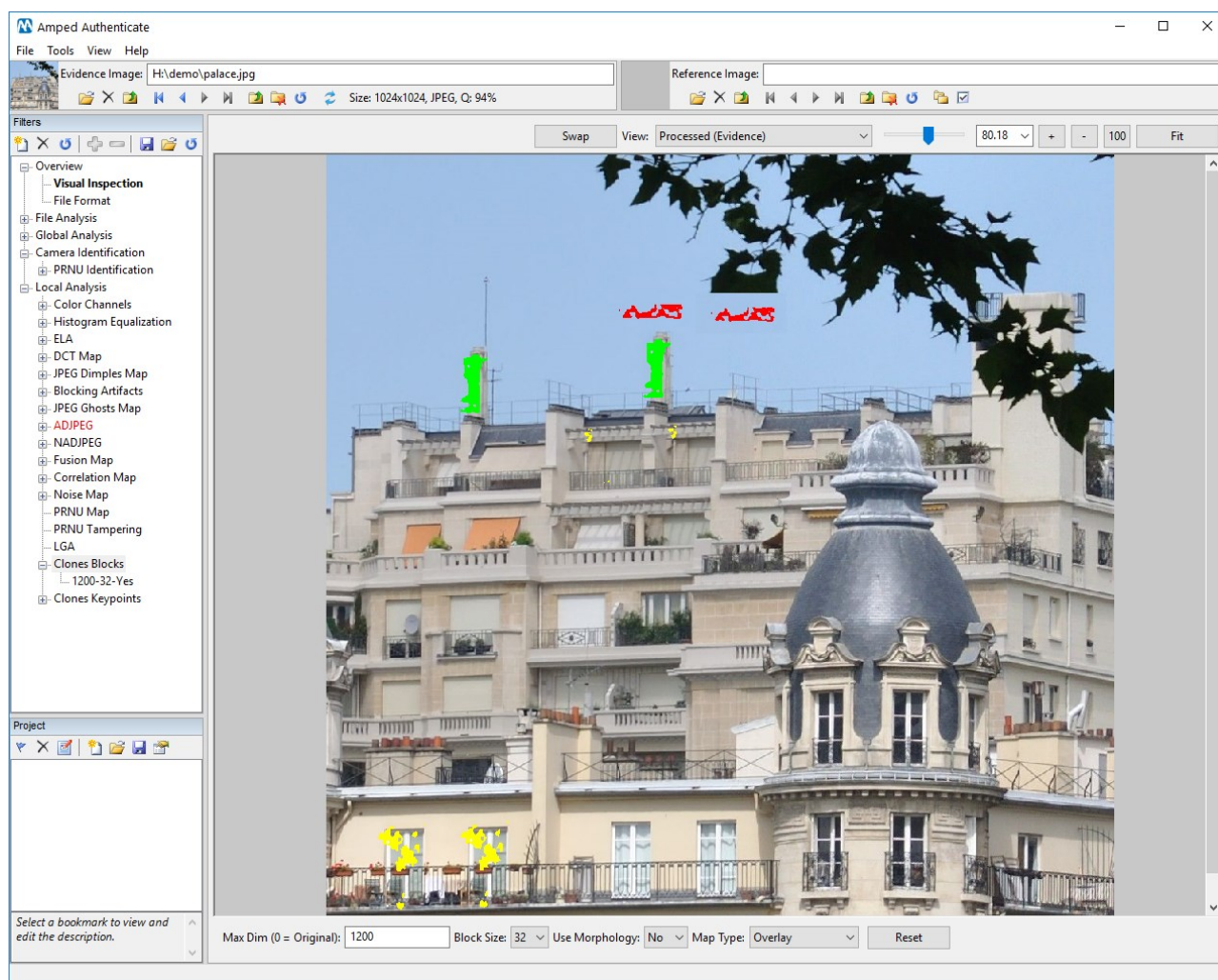


Figure 6: The Clones Blocks filter marks several regions as cloned. In an image like this one, localizing cloned regions by visual inspection alone would be very difficult.

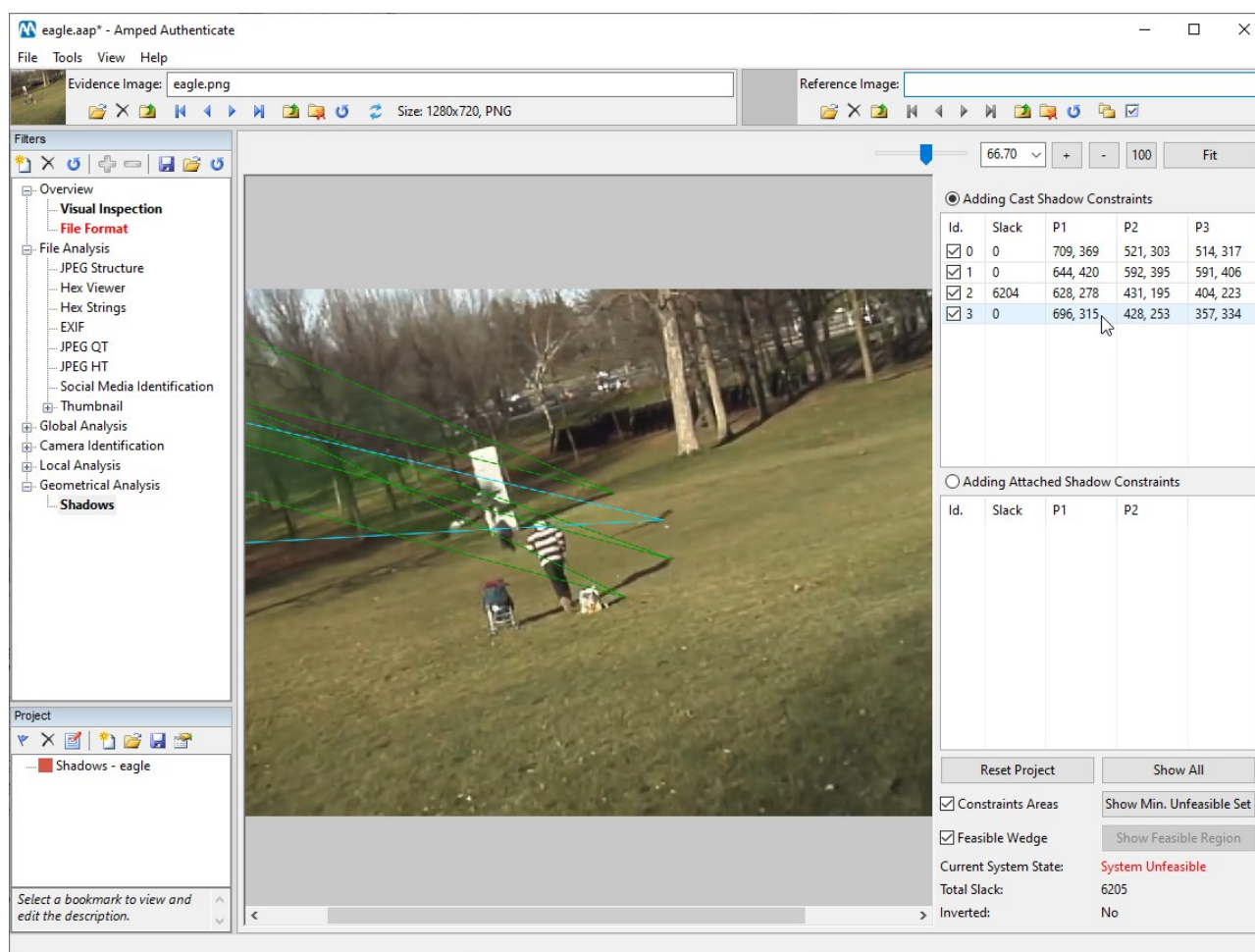


Figure 7: The Shadows filter reveals that the eagle's shadow is not consistent with other objects' shadows. This picture has been extracted from a viral video available on the web.

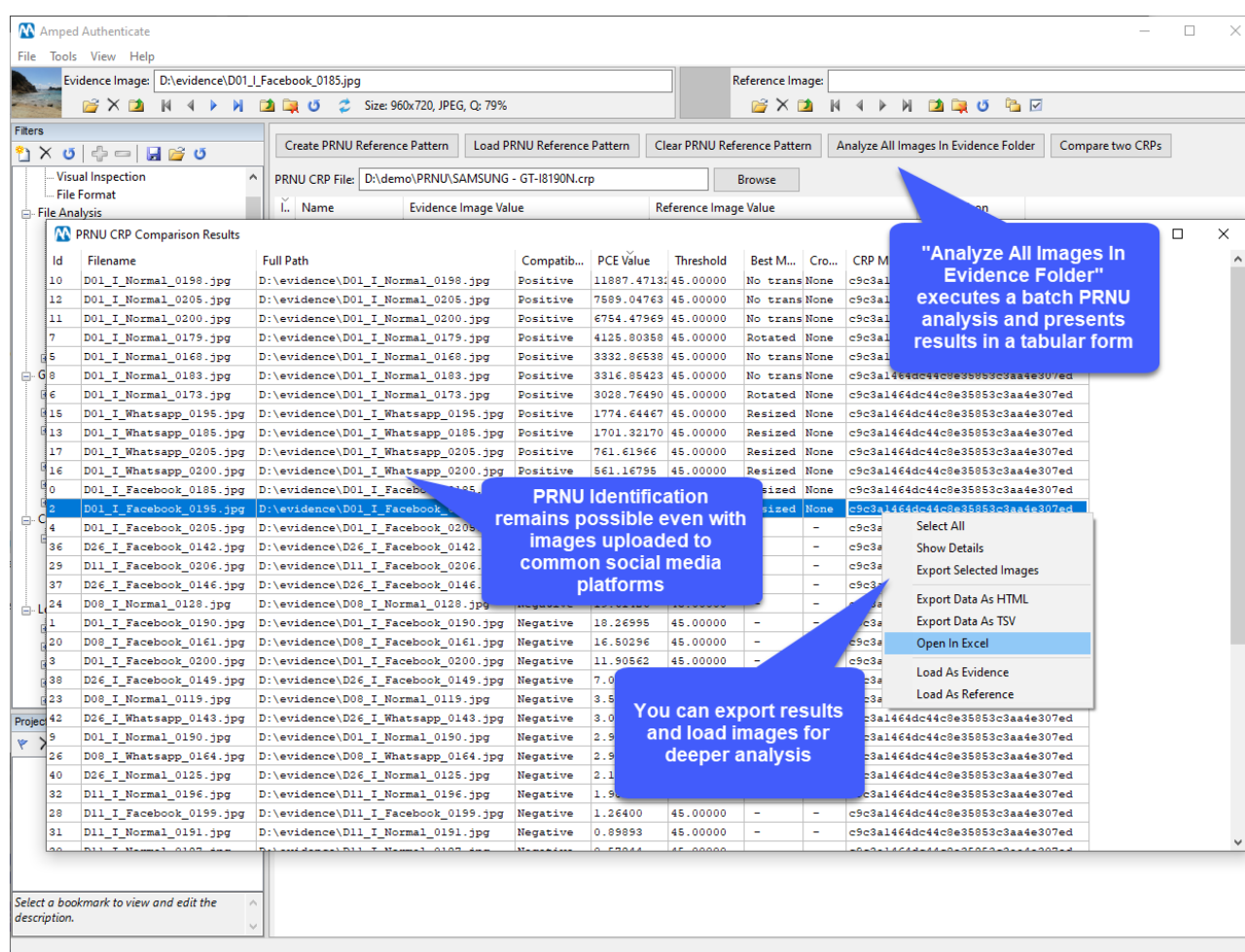
HOW DOES AMPED AUTHENTICATE IDENTIFY THE CAMERA THAT TOOK THE IMAGE?

All camera devices have a sensor that converts light into an electronic signal. These sensors consist of millions of tiny pixels. Variations in the size and properties of each pixel create a digital fingerprint of the sensor, that is unique to that specific exemplar (two devices, even of the same model, will have different fingerprints). These fingerprints can then be used to carry out "camera ballistic" tests to determine the source of the image.

Amped Authenticate has turned this complex process into an easy, 2 step process:

- 1) Take reference photos from the suspect's camera and train the Camera Reference Pattern (CRP) with them. When many images are available, Amped Authenticate automatically triages them to select the most appropriate for the fingerprint computation process.
- 2) Load evidence images to check whether they match the currently loaded reference pattern. Match will be detected even when the evidence image has been recompressed, cropped, scaled, or rotated. This means that you will often be able to link an image to its source even when the image comes from a social media platform like Facebook.

Step 2 can be run in batch mode to analyze all images in a folder, producing a tabular output that can be easily sorted and exported.



"Analyze All Images In Evidence Folder" executes a batch PRNU analysis and presents results in a tabular form

PRNU Identification remains possible even with images uploaded to common social media platforms

You can export results and load images for deeper analysis

Id	Filename	Full Path	Compatib...	PCE Value	Threshold	Best M...	Cro...	CRP M...
10	D01_I_Normal_0198.jpg	D:\evidence\D01_I_Normal_0198.jpg	Positive	11887.4713	45.00000	No trans	None	c9c3a1...
12	D01_I_Normal_0205.jpg	D:\evidence\D01_I_Normal_0205.jpg	Positive	7589.04763	45.00000	No trans	None	c9c3a1...
11	D01_I_Normal_0200.jpg	D:\evidence\D01_I_Normal_0200.jpg	Positive	6754.47969	45.00000	No trans	None	c9c3a1...
7	D01_I_Normal_0179.jpg	D:\evidence\D01_I_Normal_0179.jpg	Positive	4125.80358	45.00000	Rotated	None	c9c3a1...
6	D01_I_Normal_0168.jpg	D:\evidence\D01_I_Normal_0168.jpg	Positive	3332.86538	45.00000	No trans	None	c9c3a1...
8	D01_I_Normal_0183.jpg	D:\evidence\D01_I_Normal_0183.jpg	Positive	3316.85423	45.00000	No trans	None	c9c3a1...
6	D01_I_Normal_0173.jpg	D:\evidence\D01_I_Normal_0173.jpg	Positive	3028.76490	45.00000	Rotated	None	c9c3a1...
15	D01_I_Whatsapp_0195.jpg	D:\evidence\D01_I_Whatsapp_0195.jpg	Positive	1774.64467	45.00000	Resized	None	c9c3a1...
13	D01_I_Whatsapp_0185.jpg	D:\evidence\D01_I_Whatsapp_0185.jpg	Positive	1701.32170	45.00000	Resized	None	c9c3a1...
17	D01_I_Whatsapp_0205.jpg	D:\evidence\D01_I_Whatsapp_0205.jpg	Positive	761.61966	45.00000	Resized	None	c9c3a1...
16	D01_I_Whatsapp_0200.jpg	D:\evidence\D01_I_Whatsapp_0200.jpg	Positive	561.16795	45.00000	Resized	None	c9c3a1...
0	D01_I_Facebook_0185.jpg	D:\evidence\D01_I_Facebook_0185.jpg	Positive	561.16795	45.00000	Resized	None	c9c3a1...
2	D01_I_Facebook_0195.jpg	D:\evidence\D01_I_Facebook_0195.jpg	Positive	561.16795	45.00000	Resized	None	c9c3a1...
4	D01_I_Facebook_0205.jpg	D:\evidence\D01_I_Facebook_0205.jpg	Positive	561.16795	45.00000	Resized	None	c9c3a1...
36	D26_I_Facebook_0142.jpg	D:\evidence\D26_I_Facebook_0142.jpg	Negative	18.26995	45.00000	-	-	c9c3a1...
29	D11_I_Facebook_0206.jpg	D:\evidence\D11_I_Facebook_0206.jpg	Negative	16.50296	45.00000	-	-	c9c3a1...
37	D26_I_Facebook_0146.jpg	D:\evidence\D26_I_Facebook_0146.jpg	Negative	11.90562	45.00000	-	-	c9c3a1...
24	D08_I_Normal_0128.jpg	D:\evidence\D08_I_Normal_0128.jpg	Negative	3.5	45.00000	-	-	c9c3a1...
1	D01_I_Facebook_0190.jpg	D:\evidence\D01_I_Facebook_0190.jpg	Negative	3.0	45.00000	-	-	c9c3a1...
20	D08_I_Facebook_0161.jpg	D:\evidence\D08_I_Facebook_0161.jpg	Negative	2.9	45.00000	-	-	c9c3a1...
3	D01_I_Facebook_0200.jpg	D:\evidence\D01_I_Facebook_0200.jpg	Negative	2.9	45.00000	-	-	c9c3a1...
38	D26_I_Facebook_0149.jpg	D:\evidence\D26_I_Facebook_0149.jpg	Negative	2.1	45.00000	-	-	c9c3a1...
23	D08_I_Normal_0119.jpg	D:\evidence\D08_I_Normal_0119.jpg	Negative	2.1	45.00000	-	-	c9c3a1...
42	D26_I_Whatsapp_0143.jpg	D:\evidence\D26_I_Whatsapp_0143.jpg	Negative	1.9	45.00000	-	-	c9c3a1...
9	D01_I_Normal_0190.jpg	D:\evidence\D01_I_Normal_0190.jpg	Negative	1.26400	45.00000	-	-	c9c3a1...
26	D08_I_Whatsapp_0164.jpg	D:\evidence\D08_I_Whatsapp_0164.jpg	Negative	0.89893	45.00000	-	-	c9c3a1...
40	D26_I_Normal_0125.jpg	D:\evidence\D26_I_Normal_0125.jpg	Negative	0.89893	45.00000	-	-	c9c3a1...
32	D11_I_Facebook_0196.jpg	D:\evidence\D11_I_Facebook_0196.jpg	Negative	0.89893	45.00000	-	-	c9c3a1...
28	D11_I_Facebook_0199.jpg	D:\evidence\D11_I_Facebook_0199.jpg	Negative	0.89893	45.00000	-	-	c9c3a1...
31	D11_I_Normal_0191.jpg	D:\evidence\D11_I_Normal_0191.jpg	Negative	0.89893	45.00000	-	-	c9c3a1...

Figure 8: running a batch PRNU Identification on a set of images reveals that some of them were indeed captured by the Samsung Galaxy to which the employed CRP belongs to (these images have "D01" in their filename). You may also note that all images that read "Resized" in the Best Match column have "Facebook" or "Whatsapp" in their filename. These images were obtained from the Facebook and Whatsapp profile of the device owner: despite the aggressive resize and compression applied by these social media platforms, they still show Positive compatibility with the CRP. On the contrary, images coming from other devices (denoted by "D08", "D11", "D26" in the filename) have negative compatibility with the CRP, as expected.





HOW DOES AMPED AUTHENTICATE'S BATCH PROCESSING WORK?

Running the whole set of Authenticate filters on an image could take some time, especially when the image is at high resolution. However, Authenticate provides several solutions to optimize the time the user needs to be at the computer:

- 1) In running a Batch Processing, Authenticate will compute all filters' results and store them to a cache folder; when the user comes back to the computer, pre-computed outputs will be showed quickly. The set of filters and configurations that should be run by the Batch Processing is customizable by the user.

- 2) When the number of images to process is too huge even for Batch Processing, the Smart Report functionality comes in handy: it will first analyze each image metadata and file properties and pass to more detailed analysis only those images showing some suspicious value therein. Contrarily to Batch Processing, where the set of filters to be applied is statically configured, the Smart Report tool is able to automatically choose the most appropriate Local Analysis filters to be used for each image, aiming to provide the most meaningful results in limited time. The HTML Report shows a summary table where images are grouped by their integrity level, as in the example below.

Summary Table

Total number of processed images: 5			
			Images that are likely to be camera original: 4
			Images with suspicious metadata but no traces of forgery: 0
			Images with traces of possible forgery: 1

Images that are likely to be camera original



Images with traces of possible forgery



HOW DOES AMPED AUTHENTICATE INTERACT WITH THE INTERNET?

The internet often contains data that can help the analysis. The reverse image search feature provided by Google can locate images that are visually similar to your evidence file (provided you can upload the evidence to such services), making contextual analysis much easier. Moreover, the integration with Google Maps allows you to see where in the world the image was captured, thanks to GPS coordinates in image metadata left by modern devices.

When you don't have reference images to compare your evidence with, you can search and download images of the same camera make and model from Flickr, automatically filtering out images whose metadata suggest they are not camera original. Not only: you can use the integration with CameraForensics to perform an even faster and more accurate search, being able to locate and download dozens of reference images in seconds. Noticeably, when searching for reference images on the web, the image content is not uploaded (only minor metadata information is sent to the server). This means you can use these features even on classified evidence.

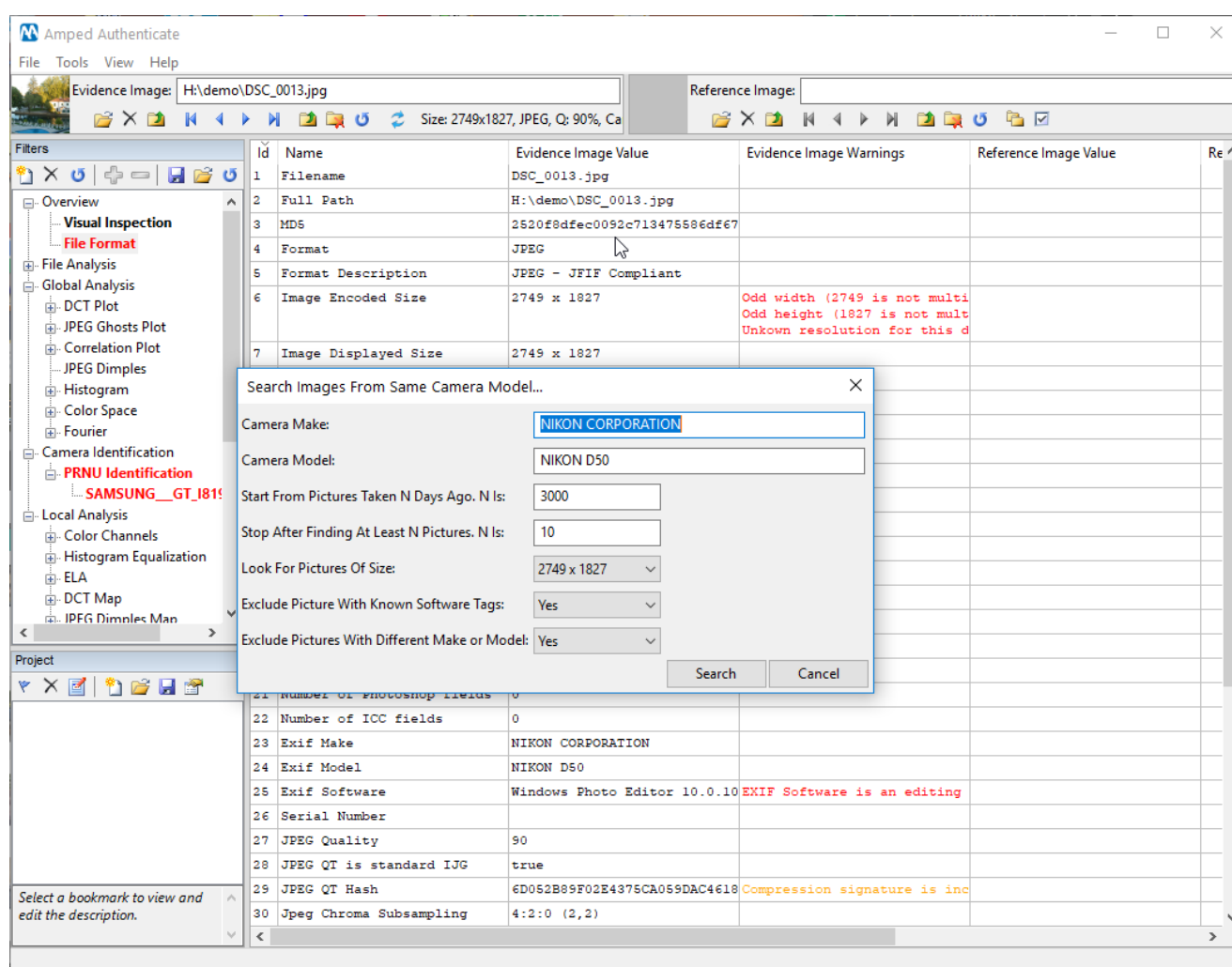


Figure 9: The "Search images from same camera model" tool lets you search the web for reference images of the same make and model as your evidence image.

Search Images From Same Camera Model...									
Id	Web Photo Id	Owner Id	Size	Make	Model	Software	Date Uploaded	Link	
0	44212191690	64237622@N05	3008x2000	NIKON CORPORATION	NIKON D50	Alien Skin	2018-11-24 15:47:30.000	https://farm5.staticflickr.com/4853/44212191690_12c77d10e1_o.jpg	
1	44874511384	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-28 15:48:25.000	https://farm2.staticflickr.com/1930/44874511384_7bedea2023_o.jpg	
2	43746430600	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-26 12:17:22.000	https://farm2.staticflickr.com/1904/43746430600_0906261808_o.jpg	
3	44788437634	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-23 11:02:15.000	https://farm2.staticflickr.com/1951/44788437634_ee7584b844_o.jpg	
4	30526912257	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-21 12:27:20.000	https://farm2.staticflickr.com/1906/30526912257_b4cd6e046d_o.jpg	
5	30526910217	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-21 12:27:20.000	https://farm2.staticflickr.com/1979/30526910217_af920a289d_o.jpg	
6	43627165370	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-20 11:06:24.000	https://farm2.staticflickr.com/1948/43627165370_09fce52e91_o.jpg	
7	44719894734	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-20 11:06:23.000	https://farm2.staticflickr.com/1980/44719894734_02ed7d7dd6_o.jpg	
8	43568093520	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-17 15:14:54.000	https://farm2.staticflickr.com/1977/43568093520_cbd2a2a20fc_o.jpg	
9	31458802458	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-15 10:17:43.000	https://farm2.staticflickr.com/1955/31458802458_4aef9f4708_o.jpg	
10	31411008908	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-13 10:12:47.000	https://farm2.staticflickr.com/1920/31411008908_55f514fb13_o.jpg	
11	45194585272	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-11 14:12:25.000	https://farm2.staticflickr.com/1914/45194585272_e7b922c3e6_o.jpg	
12	43384387430	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-09 10:52:59.000	https://farm2.staticflickr.com/1955/43384387430_934b427a3a_o.jpg	
13	30175657407	9701017@N08	3008x2000	NIKON CORPORATION	NIKON D50	Ver.1.00	2018-10-05 13:12:51.000	https://farm2.staticflickr.com/1906/30175657407_4fd2f47025_o.jpg	

Figure 10: results obtained by the search example shown above. All images in the list can be downloaded and used for comparison. The table can be exported to HTML or CSV to be included in the report for reproducibility.

CASE EXAMPLES

INTELLIGENCE AND COUNTERTERRORISM

During a terrorist attack to a country's embassy, one staff member is severely injured and kidnapped. A few weeks later an email is sent to the embassy claiming that a terrorist group is responsible for the attack and says the staff member is still alive and imprisoned. They attach a bitmap (.bmp) picture showing the person holding a newspaper dated the same day of the email. It is crucial to authenticate the attached image to evaluate chances that the staff member is currently alive.

Workflow

The image is scrutinized with Amped Authenticate. As expected, the bitmap picture does not have metadata providing indications about the camera model, acquisition date and place, etc.: conversion to bitmap is indeed in a frequently employed redaction method. However, filters in the Global Analysis category reveal that the image has traces of two previous JPEG compressions. These facts provide strong confidence against the integrity of the image, since camera original images are rarely in bitmap format, and do not show traces of double compression. Global Analysis also shows that the image contains the "JPEG Dimples" artifact (an imperceptible defect introduced throughout the image by many camera models). The JPEG Dimples Map filter is thus used to conduct a fine-grained forgery localization analysis, which reveals that the artifact is consistently present everywhere, including in the subject's body, but it is missing in the region containing the newspaper. The Correlation Map also reveals strong local correlation in the newspaper region, which is possibly a consequence of scaling/rotation applied to the newspaper to fit into the subject's hands.

Conclusion

The image is marked as non-authentic, but still conveys important information. Indeed, traces of modifications were found on the newspaper, while the region depicting the subject seems to be authentic, as supported by local presence of the JPEG Dimples artifact. This fact may suggest that the staff member was indeed kidnapped by the group and photographed by them but is no longer alive.

CSE CASES

Following a search in the home of a suspect, police seize several memory drives containing indecent images of children, together with two smartphones, one compact camera and one reflex camera. When the seized computer is investigated, it is revealed that the suspect regularly browses and downloads illicit child related content. It is of interest to the prosecutor to understand whether the suspect also produced some of the illicit material, besides downloading it.

Workflow

In less than an hour, sample images are taken with the seized smartphones and cameras, and Amped Authenticate generates a Camera Reference Pattern (CRP) for each device. Before investigating the illicit images, the user disables Authenticate's caching system, so that evidence images are not stored into their analysis workstation cache folder.

All the evidence images are then tested against the available CRPs to search for possible matches, revealing that several images have a strong compatibility with the reflex camera. Thankfully, there is no need to watch the content of images, since computation of the matching score is done by Authenticate in batch without even showing the images to the user.

Conclusion

The prosecutor is now able to charge the suspect with creation of child abuse material, making his case stronger.

CAR INSURANCE FRAUD

Every week, an insurance company receives thousands of damaged car images from its affiliated insurance experts spread around the territory. The company suspects that some of the experts are teaming up with customers to send fake images to the company, so they can ask for refunds.

Workflow

Due to the massive amount of data, analyzing one image at a time would take too long. The company decides to use Amped Authenticate's Smart Report tool, which scans all images in batch and separates images whose metadata and coding properties are compatible with native camera images from those images with problematic metadata and/or possible traces of local forgeries. The number of images to be investigated is now reduced by a factor of 95%, making single-image investigation feasible. Some of the images indeed contain traces of splicing; in particular, in several cases, damaged parts of the car are copied, scaled, rotated, and pasted again into the same image to increase the extent of the damage.

Conclusion

The company is able to sue the affiliated expert for fraud and ask for the funds to be returned.

JOURNALISM/PROPAGANDA

The editorial staff of a newspaper receives from an anonymous source a compromising picture of an important political figure. If published, the image would have dramatic consequences. However, the newspaper will face serious consequences if the image proves to be a hoax.

Workflow

The image is first scrutinized using File Format, and no warning appears. Searching the image on the web does not reveal any picture of similar content already published. Since information about camera make and model are available in the Exif metadata, Authenticate is able to find and download from the web, hundreds of images captured by the same camera model. After a batch file format comparison, every detail of the investigated image seems well compatible with reference material, including JPEG Quantization Tables, which are also confirmed to match the declared camera model by Authenticate's database. Filters in the Global Analysis category do not show any trace of recompression or resampling. JPEG Dimples are present, as expected for that specific camera model. Filters in the Local Analysis category do not reveal any suspicious region. Moreover, the JPEG Dimples Map filter detects presence of JPEG Dimples throughout the image, suggesting that no region has been tampered with.

Conclusion

Before the end of the day, the editorial team decides to publish the image. The decision remains courageous, but thanks to Amped Authenticate it is not a blind decision.

PARKING VIOLATION

Someone had their vehicle towed and incurred enormous fees. This person wants to dispute and has written a letter saying that he will pay for the parking ticket, but the red zone he was parked in is not a towing zone (as shown in an attached picture), so he is asking the city to refund the money that he had to pay for the impound of his car. The city needs to make a decision.

For towing to occur it is likely that the car was parked by a fire hydrant, or it was parked in an ambulance zone. But in the image, there is no fire hydrant nor any sign of an ambulance zone.

Workflow

Amped Authenticate inspects the format of the image and provides several warning signs: according to Exif metadata, the image comes from a Motorola Droid 4, but the Exif software tag reads "Photoshop CS4". This fact suggests that the image has been edited after acquisition. While this is enough to dispute the integrity of the evidence, Photoshop could have been used to simply increase the contrast, and that would not threaten image authenticity.

The analyst can do further analysis and discover that the image has been compressed at least two times (confirming an editing-and-resave chain) and, most noticeably, part of the sidewalk asphalt has been cloned. Incidentally, the cloned region has a shape and size compatible with those of a hydrant.

Conclusion

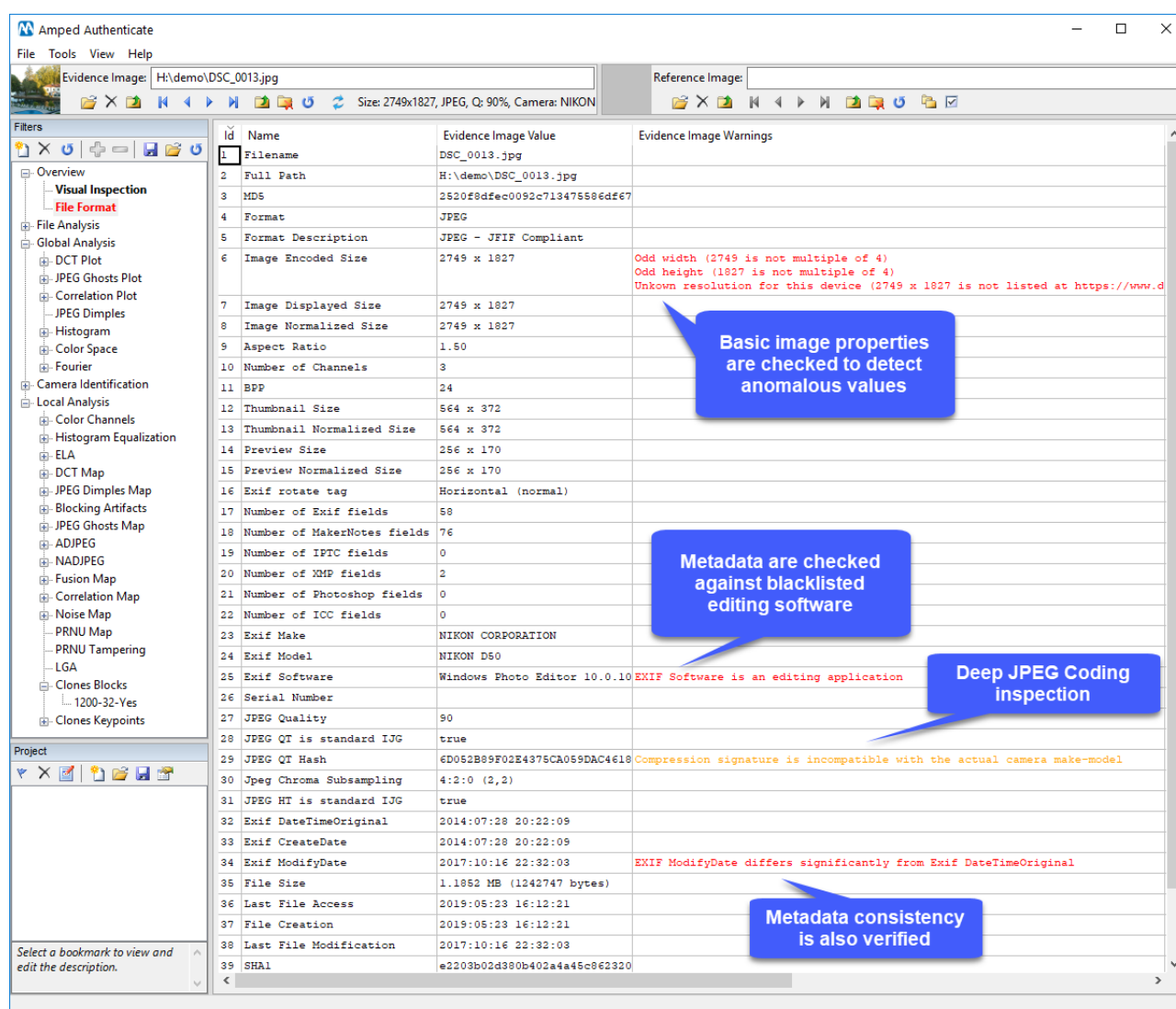
In less than 10 minutes the city is able to save themselves from refunding fees, but in addition, there is likely an additional penalty to the person who has introduced false evidence into a proceeding.

FILTER SAMPLES

Amped Authenticate provides a very user-friendly interface that allows to open an image in the most common formats (JPEG, PNG, TIFF, BMP, HEIF, etc.) and easily select several filters and tools to perform diverse tests on the image.

Amped Authenticate's features are all based on peer reviewed papers in the digital forensics field. Each feature allows the user to analyze the photo from many different perspectives using algorithms and techniques such as:

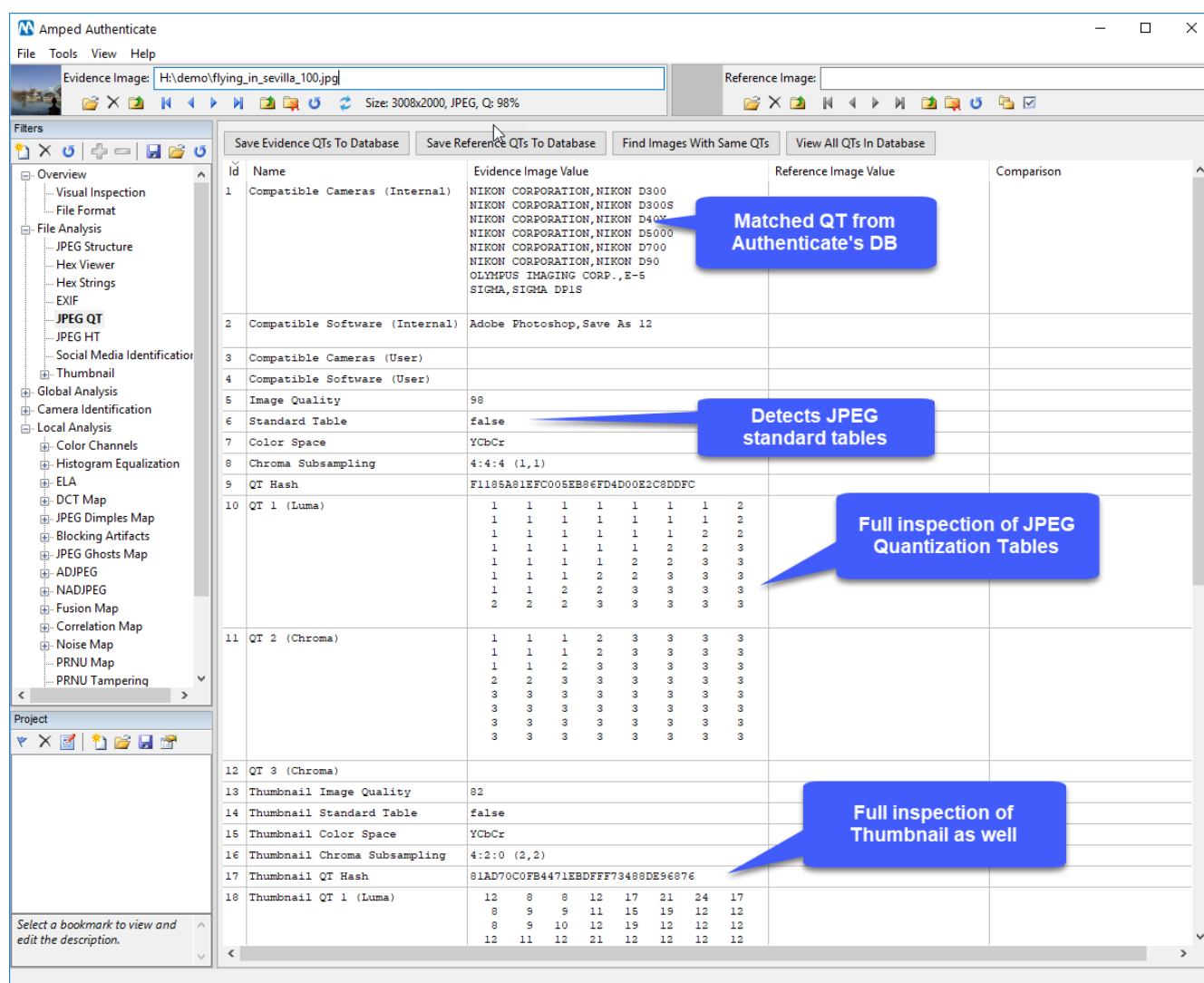
FILE FORMAT



Id	Name	Evidence Image Value	Evidence Image Warnings
1	Filename	DSC_0013.jpg	
2	Full Path	H:\demo\DSC_0013.jpg	
3	MD5	2520f8dfec0092c713475586df67	
4	Format	JPEG	
5	Format Description	JPEG - JFIF Compliant	
6	Image Encoded Size	2749 x 1827	Odd width (2749 is not multiple of 4) Odd height (1827 is not multiple of 4) Unknown resolution for this device (2749 x 1827 is not listed at https://www.d
7	Image Displayed Size	2749 x 1827	
8	Image Normalized Size	2749 x 1827	
9	Aspect Ratio	1.50	
10	Number of Channels	3	
11	BPP	24	
12	Thumbnail Size	564 x 372	
13	Thumbnail Normalized Size	564 x 372	
14	Preview Size	256 x 170	
15	Preview Normalized Size	256 x 170	
16	Exif rotate tag	Horizontal (normal)	
17	Number of Exif fields	58	
18	Number of MakerNotes fields	76	
19	Number of IPTC fields	0	
20	Number of XMP fields	2	
21	Number of Photoshop fields	0	
22	Number of IOC fields	0	
23	Exif Make	NIKON CORPORATION	
24	Exif Model	NIKON D50	
25	Exif Software	Windows Photo Editor 10.0.10	EXIF Software is an editing application
26	Serial Number		
27	JPEG Quality	90	
28	JPEG QT is standard IJG	true	
29	JPEG QT Hash	6D052B89F02E4375CA059DAC4618	Compression signature is incompatible with the actual camera make-model
30	Jpeg Chroma Subsampling	4:2:0 (2,2)	
31	JPEG HT is standard IJG	true	
32	Exif DateTimeOriginal	2014:07:28 20:22:05	
33	Exif CreateDate	2014:07:28 20:22:05	
34	Exif ModifyDate	2017:10:16 22:32:03	EXIF ModifyDate differs significantly from Exif DateTimeOriginal
35	File Size	1.1852 MB (1242747 bytes)	
36	Last File Access	2019:05:23 16:12:21	
37	File Creation	2019:05:23 16:12:21	
38	Last File Modification	2017:10:16 22:32:03	
39	SHA1	e2203b02d390b402a4a45c962320	

The File Format filter provides a quick overview of image properties, and highlights elements that are not common to camera original images. While not being exhaustive, this filter often allows users to rule out image integrity in a few seconds: in the example, presence of the “Adobe Photoshop CS4 Windows” metadata suffice to raise concerns on image trustworthiness, to be addressed in the rest of the analysis.

JPEG QUANTIZATION TABLE



The screenshot displays the Amped Authenticate interface with the 'File Format' filter selected. The 'Evidence Image' is 'H:\demo\flying_in_sevilla_100.jpg' (Size: 3008x2000, JPEG, Q: 98%). The 'Reference Image' is empty. The 'Filters' pane on the left shows the 'File Format' filter expanded, with 'JPEG QT' selected. The main window shows a table of analysis results with columns: Id, Name, Evidence Image Value, Reference Image Value, and Comparison.

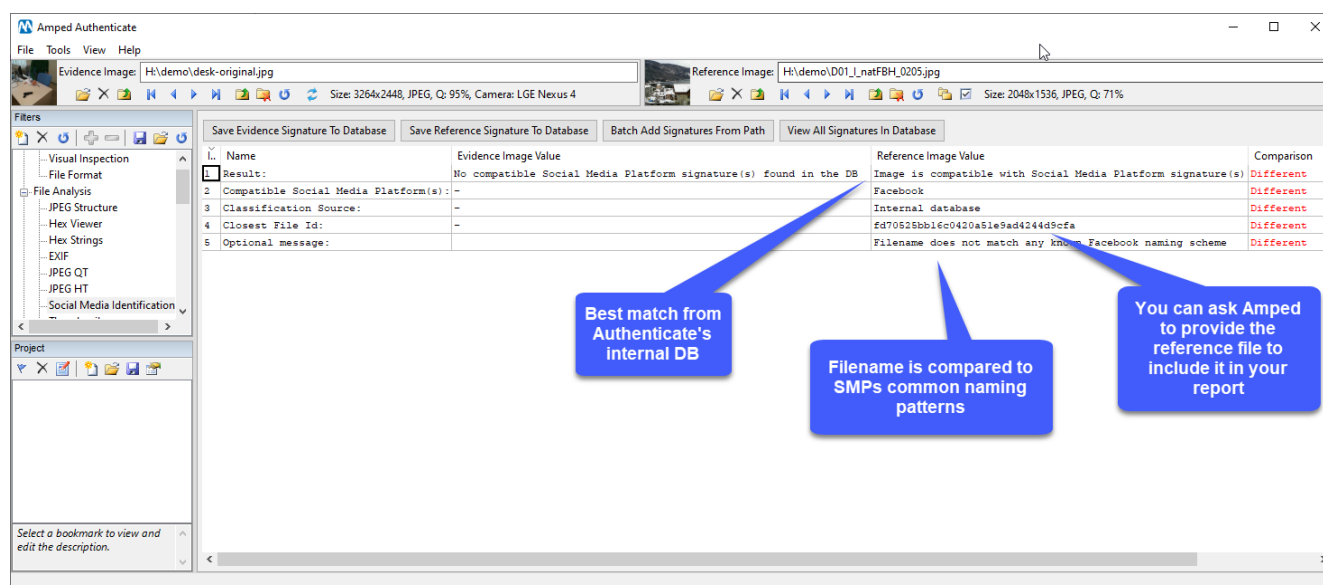
Id	Name	Evidence Image Value	Reference Image Value	Comparison																																																																
1	Compatible Cameras (Internal)	NIKON CORPORATION, NIKON D300 NIKON CORPORATION, NIKON D300S NIKON CORPORATION, NIKON D400 NIKON CORPORATION, NIKON D5000 NIKON CORPORATION, NIKON D700 NIKON CORPORATION, NIKON D90 OLYMPUS IMAGING CORP., E-S SIGMA, SIGMA DP1S																																																																		
2	Compatible Software (Internal)	Adobe Photoshop, Save As 12																																																																		
3	Compatible Cameras (User)																																																																			
4	Compatible Software (User)																																																																			
5	Image Quality	98																																																																		
6	Standard Table	false																																																																		
7	Color Space	YCbCr																																																																		
8	Chroma Subsampling	4:4:4 (1,1)																																																																		
9	QT Hash	F1195A81EFC005EB86FD4D00E2C9DDFC																																																																		
10	QT 1 (Luma)	<table border="1"> <tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td></tr> <tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td></tr> <tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td><td>2</td></tr> <tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td><td>2</td><td>3</td></tr> <tr><td>1</td><td>1</td><td>1</td><td>1</td><td>2</td><td>2</td><td>3</td><td>3</td></tr> <tr><td>1</td><td>1</td><td>1</td><td>2</td><td>2</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>1</td><td>1</td><td>2</td><td>2</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>2</td><td>2</td><td>2</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> </table>	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	2	1	1	1	1	1	2	2	3	1	1	1	1	2	2	3	3	1	1	1	2	2	3	3	3	1	1	2	2	3	3	3	3	2	2	2	3	3	3	3	3		
1	1	1	1	1	1	1	2																																																													
1	1	1	1	1	1	1	2																																																													
1	1	1	1	1	1	2	2																																																													
1	1	1	1	1	2	2	3																																																													
1	1	1	1	2	2	3	3																																																													
1	1	1	2	2	3	3	3																																																													
1	1	2	2	3	3	3	3																																																													
2	2	2	3	3	3	3	3																																																													
11	QT 2 (Chroma)	<table border="1"> <tr><td>1</td><td>1</td><td>1</td><td>2</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>1</td><td>1</td><td>1</td><td>2</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>1</td><td>1</td><td>2</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>2</td><td>2</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> <tr><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td><td>3</td></tr> </table>	1	1	1	2	3	3	3	3	1	1	1	2	3	3	3	3	1	1	2	3	3	3	3	3	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3		
1	1	1	2	3	3	3	3																																																													
1	1	1	2	3	3	3	3																																																													
1	1	2	3	3	3	3	3																																																													
2	2	3	3	3	3	3	3																																																													
3	3	3	3	3	3	3	3																																																													
3	3	3	3	3	3	3	3																																																													
3	3	3	3	3	3	3	3																																																													
3	3	3	3	3	3	3	3																																																													
12	QT 3 (Chroma)																																																																			
13	Thumbnail Image Quality	82																																																																		
14	Thumbnail Standard Table	false																																																																		
15	Thumbnail Color Space	YCbCr																																																																		
16	Thumbnail Chroma Subsampling	4:2:0 (2,2)																																																																		
17	Thumbnail QT Hash	81AD70C0FB4471EBDFFF73488DE96876																																																																		
18	Thumbnail QT 1 (Luma)	<table border="1"> <tr><td>12</td><td>8</td><td>8</td><td>12</td><td>17</td><td>21</td><td>24</td><td>17</td></tr> <tr><td>8</td><td>9</td><td>9</td><td>11</td><td>15</td><td>19</td><td>12</td><td>12</td></tr> <tr><td>8</td><td>9</td><td>10</td><td>12</td><td>19</td><td>12</td><td>12</td><td>12</td></tr> <tr><td>12</td><td>11</td><td>12</td><td>21</td><td>12</td><td>12</td><td>12</td><td>12</td></tr> </table>	12	8	8	12	17	21	24	17	8	9	9	11	15	19	12	12	8	9	10	12	19	12	12	12	12	11	12	21	12	12	12	12																																		
12	8	8	12	17	21	24	17																																																													
8	9	9	11	15	19	12	12																																																													
8	9	10	12	19	12	12	12																																																													
12	11	12	21	12	12	12	12																																																													

Annotations in the image highlight specific findings:

- Matched QT from Authenticate's DB**: Points to the list of camera models in row 1.
- Detects JPEG standard tables**: Points to the 'Standard Table' result (false) in row 6.
- Full inspection of JPEG Quantization Tables**: Points to the Luma and Chroma quantization tables in rows 10 and 11.
- Full inspection of Thumbnail as well**: Points to the thumbnail quantization table in row 18.

This allows for a deep analysis of the JPEG coding properties of the image: the quantization tables (QTs) of the JPEG file are shown and compared against a vast database of known QTs from thousands of different cameras and many softwares. The user can also add tables to the database from his own images, and search images based on their QT (for example for fast triage). In the example above, image QTs are found to be compatible with a few camera models and with Adobe Photoshop when set to save at maximum quality (12). The 4:4:4 Chroma Subsampling lends support to the hypothesis that the image is not camera native (4:2:2 and 4:2:0 subsampling is much more common in such cases).

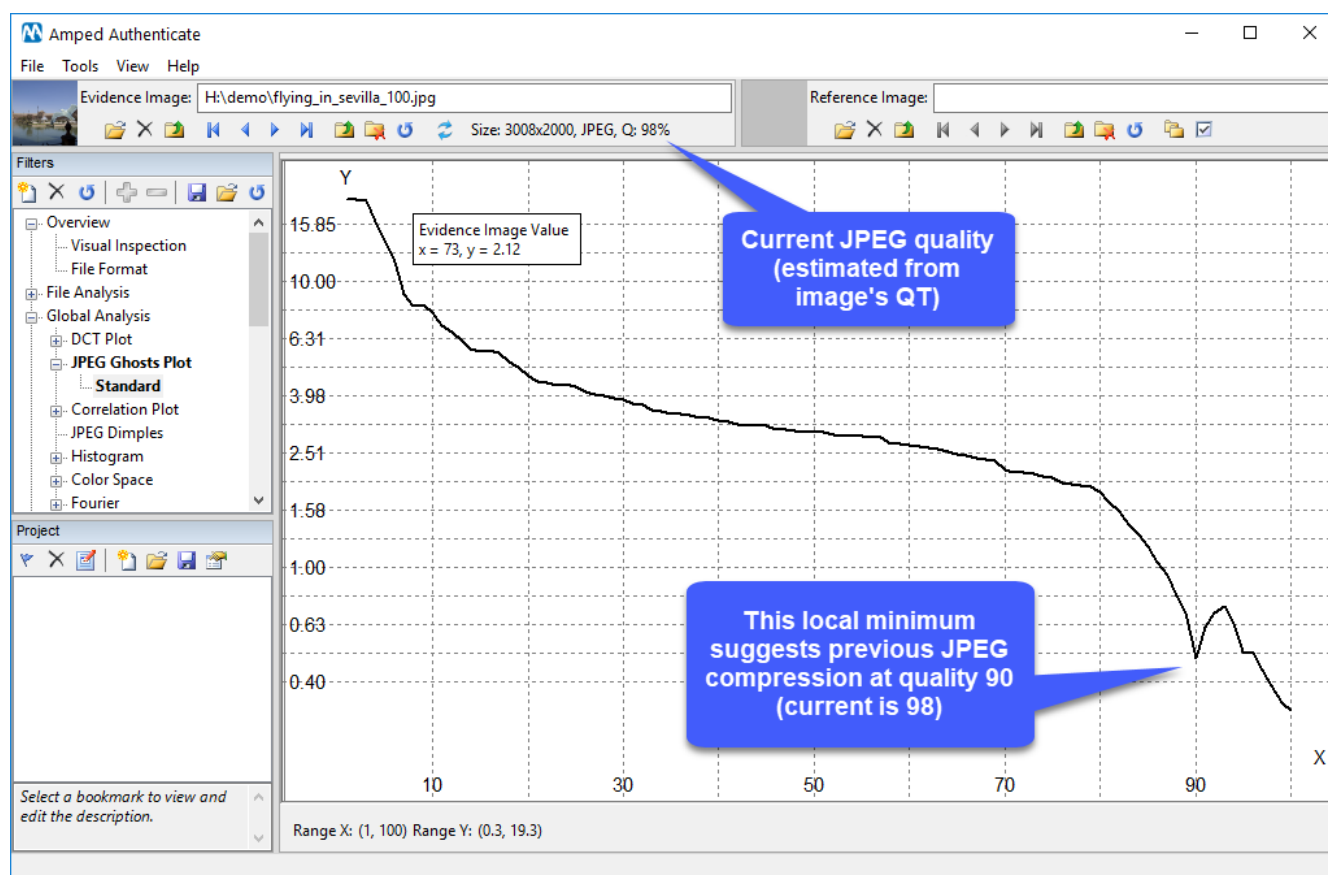
SOCIAL MEDIA IDENTIFICATION



This filter helps you detect images that come from social media. Authenticate comes with a rich database of images from Facebook, Flickr, Tumblr, Imgur, Whatsapp, Instagram, Tinypic, and Telegram. The user can enrich the database adding signatures from his own images (even in batch mode). The filename of the image is also compared to several naming patterns that are typical of some social media platforms: this may allow you to understand that an image has been downloaded from a social media platform even when the file has not been changed at all but just renamed during the process.

In the example above, the Evidence Image (left) seems to not be compatible with any known social media platform, while the Reference Image (right) is compatible with Facebook, although the name has likely been changed after download (since it does not match any known Facebook naming scheme).

JPEG GHOSTS PLOT



The JPEG Ghosts Plot is a simple yet brilliant way of detecting multiple JPEG compressions. Most camera original images are compressed only once by the acquisition device; presence of multiple compressions could indicate that the image has been re-processed out of the camera, or that the acquisition device performed an elaborated processing on the picture that required saving twice.

In the example above, while the current image quality is 98 (as estimated from the known JPEG quantization tables), the JPEG Ghosts Plot shows a local minimum at quality 90, suggesting that the image was JPEG compressed at such quality at some point in its life cycle.

PRNU IDENTIFICATION

Create Model PRNU

PRNU CRP Filename:

\\Amped Authenticate\prnu\models\SAMSUNG - GT-I8190N.crp

Browse

Reference images (all landscape and same size):

C:\Users\Dev\Dropbox (Amped Software)\new training authentic

Browse

Maximum number of reference images (0 = all found):

50

OK

Cancel

The PRNU Identification filter allows users to perform camera ballistics with Amped Authenticate, which means tracing an image back to the exact device that captured it. Given a set of reference images from a device, Authenticate trains a Camera Reference Pattern that models the PRNU noise, that is, a fingerprint that is unique to that specific device (the very intuitive dialog for creating the PRNU model is shown above).

Amped Authenticate

File Tools View Help

Evidence Image: D:\demo\PRNU\evidence\D01_nat_0168.jpg

Reference Image: D:\demo\PRNU\evidence\D11_nat_0191.jpg

Size: 2560x1920, JPEG, Q: 100%, Camera: SAMSUNG

Size: 3264x2448, JPEG, Q: 96%

Create PRNU Reference Pattern

Load PRNU Reference Pattern

Clear PRNU Reference Pattern

Analyze All Images In Evidence Folder

Compare two CRPs

PRNU CRP File: D:\demo\PRNU\SAMSUNG - GT-I8190N.crp

Browse

	Name	Evidence Image Value	Reference Image Value	Comparison
1	Compatibility	Positive	Negative	Different
2	PCE Value	3332.89110	0.89893	Different
3	Threshold	45.00000	45.00000	
4	Best Match	No transformation	-	Different
5	Cropped Region	None	-	Different
6	CRP MD5	c9c3f464dc44c8e35853c3aa4e307ed	c9c3a1464dc44c8e35853c3aa4e307ed	

Visual Inspection

File Format

File Analysis

JPEG Structure

Hex Viewer

Hex Strings

EXIF

JPEG QT

JPEG HT

Social Media Identification

Thumbnail

Global Analysis

DCT Plot

JPEG Ghosts Plot

Correlation Plot

JPEG Dimples

Histogram

Color Space

Fourier

Camera Identification

PRNU Identification

SAMSUNG__GT_I8190N

APPLE__IPHONE_4S

HUAWEI__HUAWEI_VNS_L31

Local Analysis

Color Channels

Histogram Equalization

ELA

DCT Map

JPEG Dimples Map

Project

Select a bookmark to view and edit the description.

Very high PCE Value indicates strong compatibility of this image with the selected camera reference pattern (CRP)

You can load multiple CRPs and run a batch comparison against all of them

PRNU Identification allows linking an image to the specific camera exemplar that captured it! It's also known as *camera ballistics*.

This other image was captured with a different exemplar of the same camera model. The PCE Value is close to zero, denoting negative compatibility

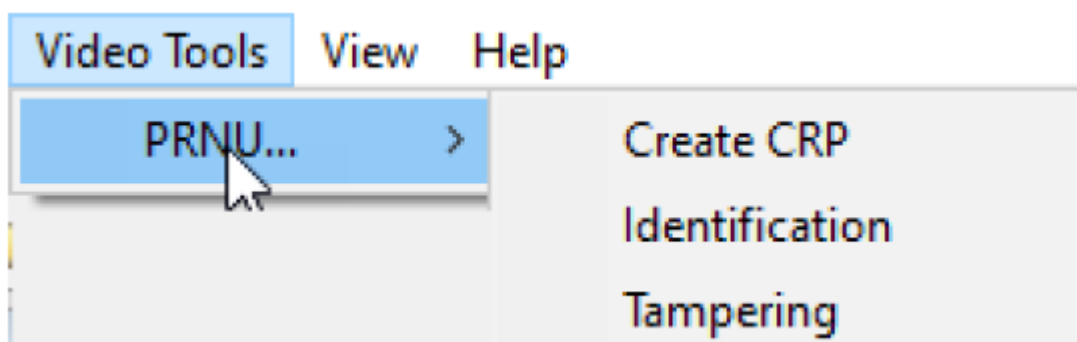
You can compare two CRPs

Using the computed CRP, you can then check whether evidence images have been captured by the device. Amped Authenticate's Camera Identification filter can resist to crop, resize, rigid rotation,

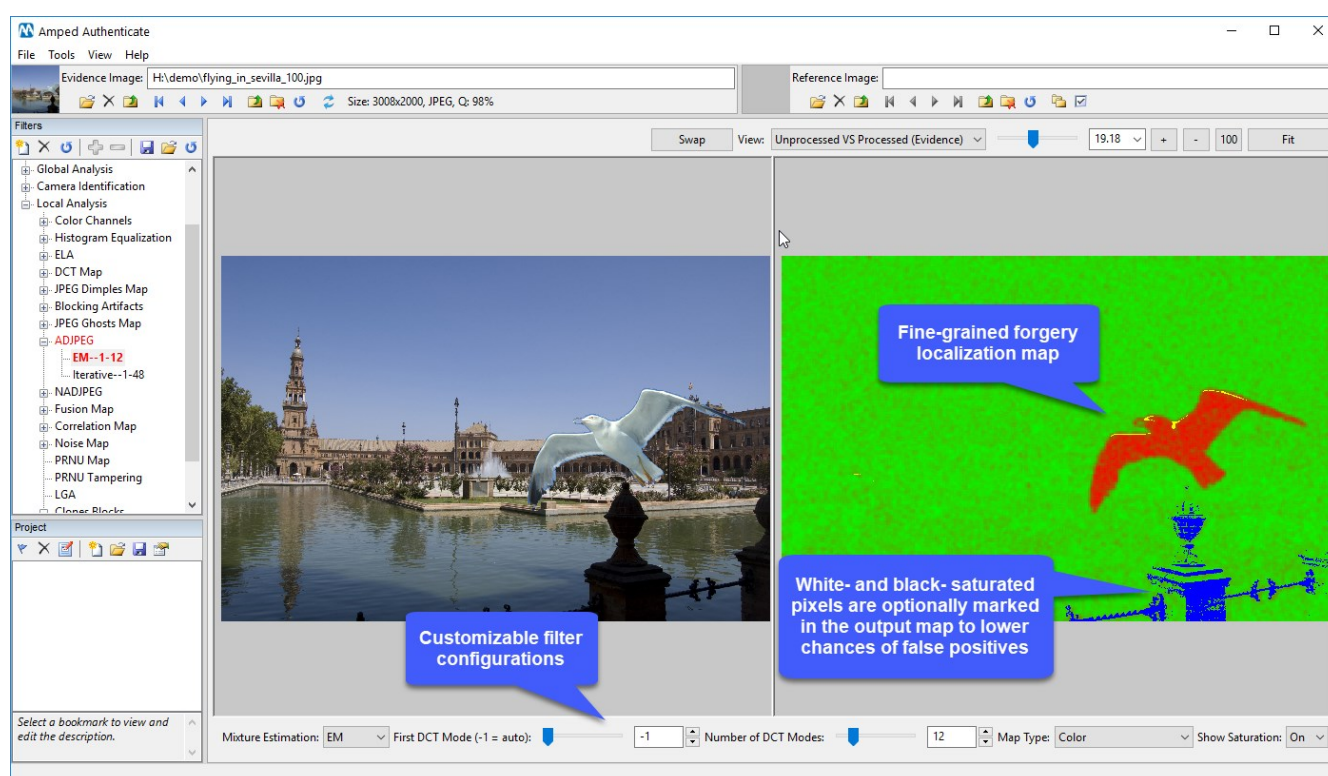
recompression. When one of the mentioned geometric transformations is detected, the user is advised.

In the example above, a good match is found for the evidence image with the reference CRP file, and a considerable crop is detected and reported. You can also compare two different CRP files to check whether two groups of images are coming from the same source device.

Amped Authenticate also includes a Video Tools menu for exploiting PRNU using videos. For more information, please see “Video Tools” in the table below (section “Amped Authenticate Technical Specification”).



ALIGNED DOUBLE JPEG

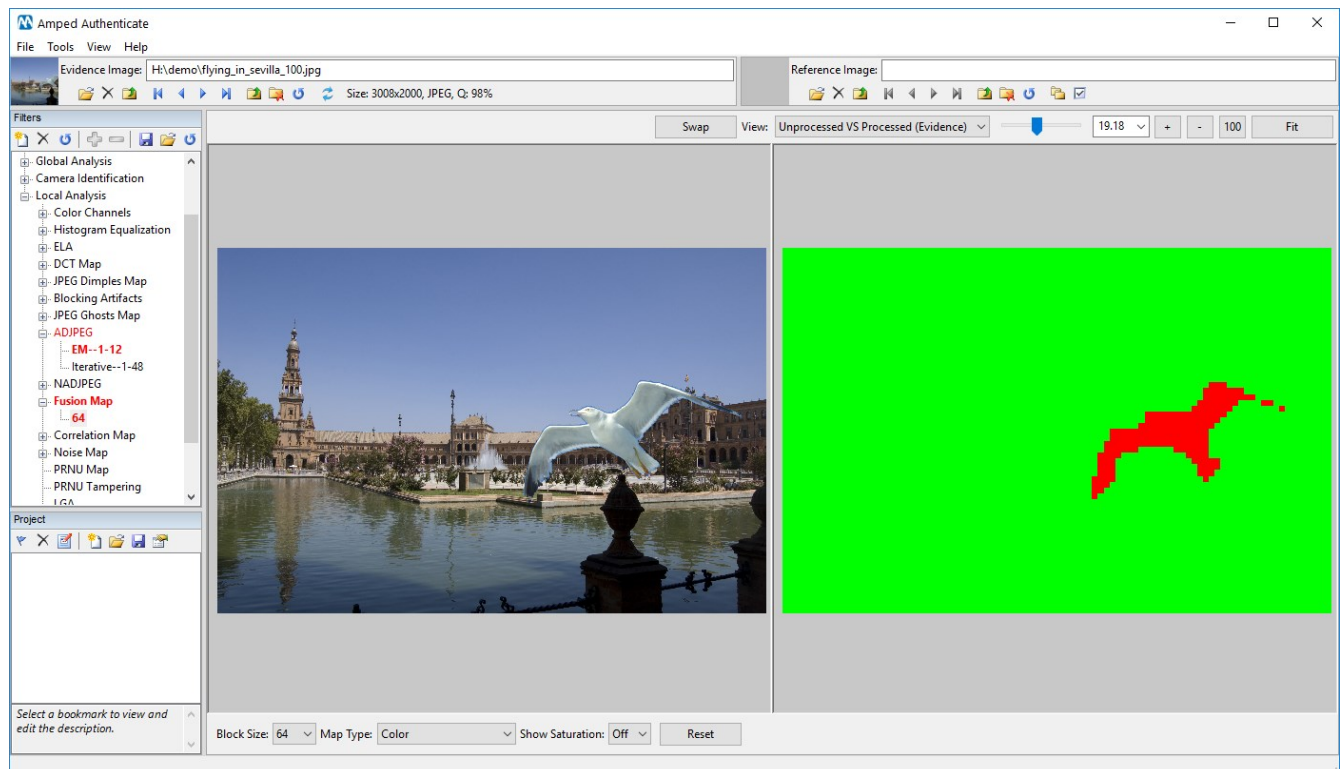


The aligned-double JPEG (ADJPEG) filter provides fast, clear and reliable forgery maps highlighting regions that have been tampered with. The core idea of the algorithm is that, since most images are stored as JPEG during acquisition, a forger has to decode the image (by opening it in some image

processing software) tamper with pixels, and then save it again, commonly in JPEG. Thus, authentic regions go through two JPEG compressions, while forged regions only show traces of the last compression. This dual nature of pixels is statistically examined to obtain the output forgery localization map.

In the example above, it can be confidently said that the seagull is detected to be fake.

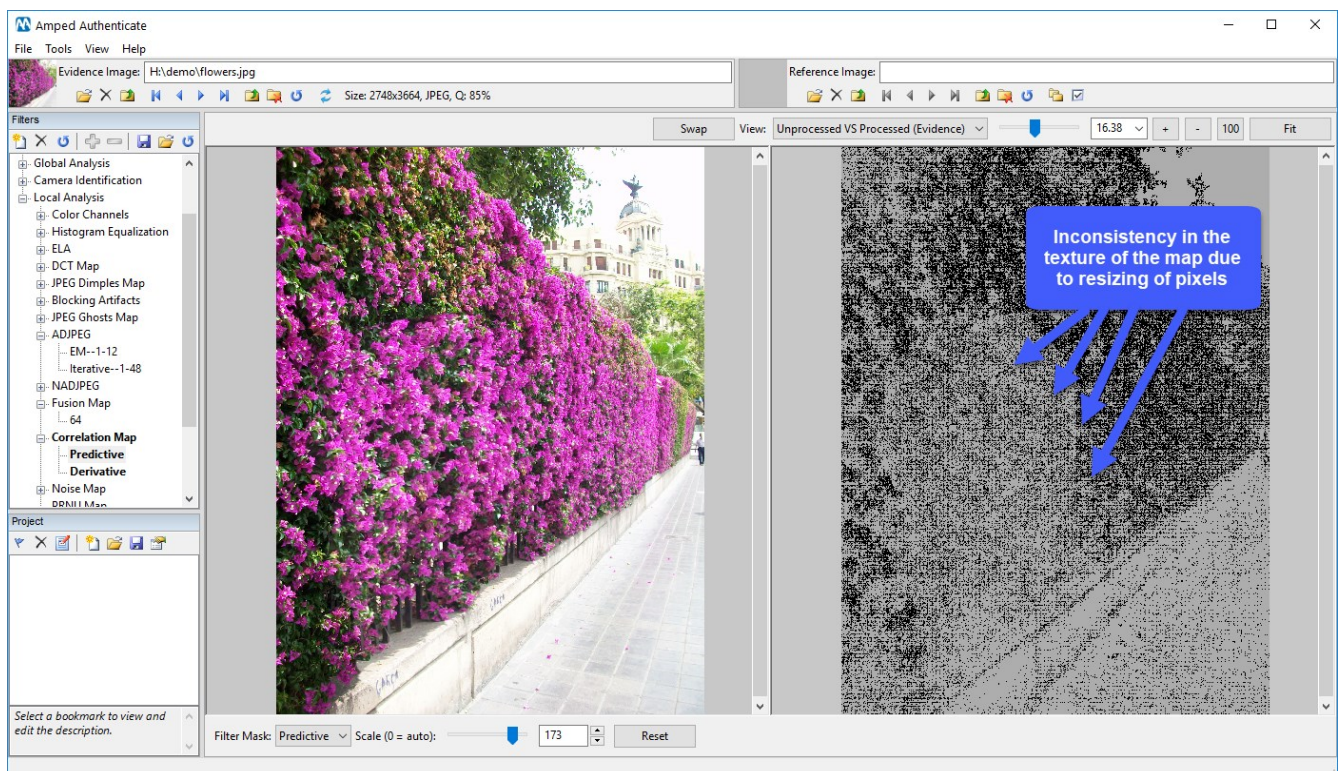
FUSION MAP



Sometimes the forgery localization maps produced by Local Analysis filters are noisy or disturbed by the image content. The Fusion Map filter combines the output from Blocking Artifacts, ADJPEG, NADJPEG and JPEG Ghosts Map into a single, fused map. It also takes into account local image properties (texture, saturation, etc.) in order to discard false positives and produce a “clean” forgery localization map.

In the example above, the seagull is clearly marked as spliced.

CORRELATION MAP

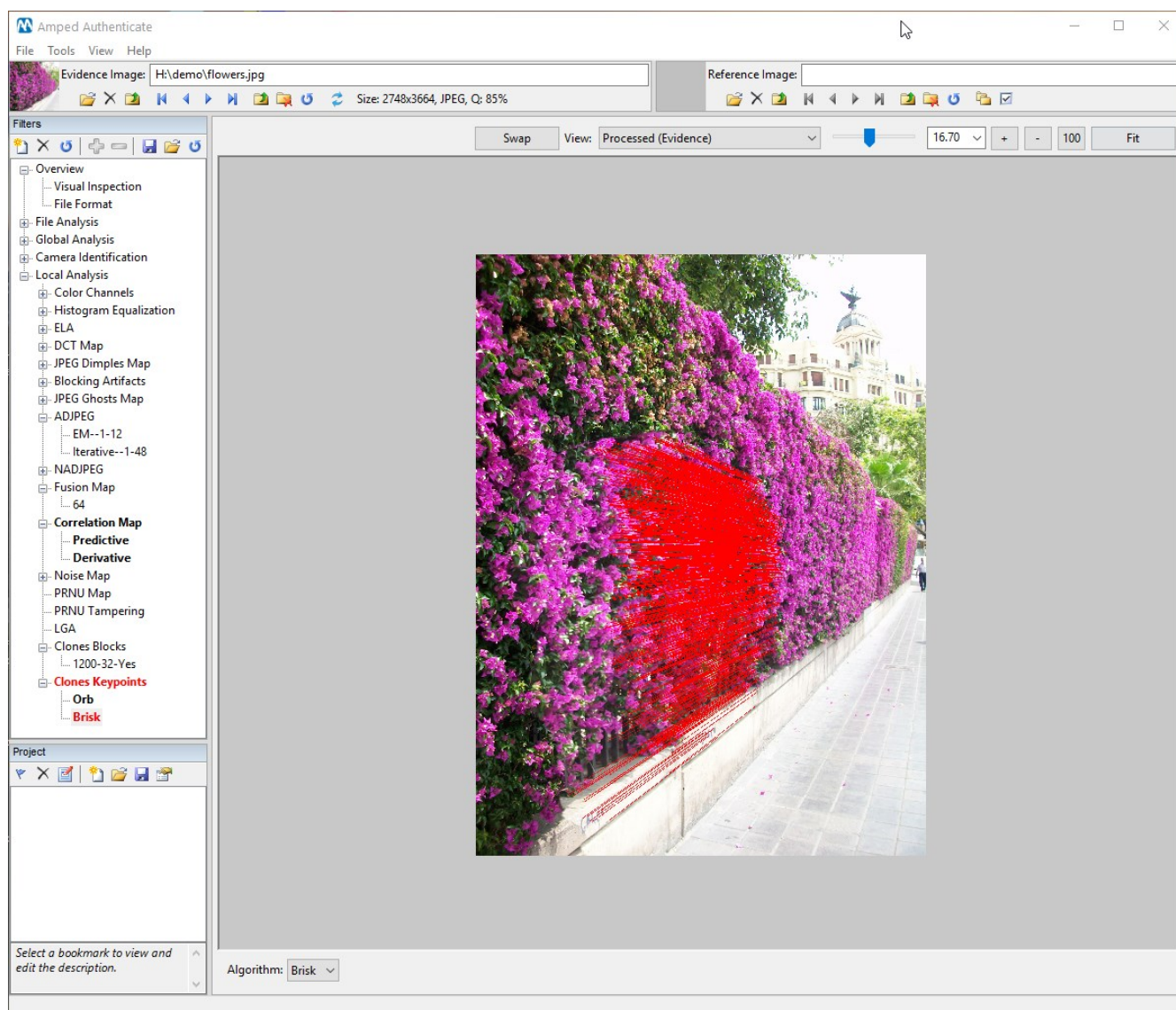


Analyzing the local correlation of pixels is an effective way to expose inconsistencies. The Correlation Map filter highlights local correlation by using predictive or derivative filters: sometimes the spliced region shows less local correlation than the original pixels (e.g., when the image background maintained traces of interpolation due to color filter array demosaicking algorithm), in some other cases it shows stronger local correlation (e.g. when the inserted object had to be resized/rotated, causing interpolation of pixels, which makes pixels correlated with each other).

In the example above, part of the hedge has a much brighter correlation map than the rest (the border of the brighter region is quite evident). Brighter regions of the map indicate stronger correlation between neighboring pixels, suggesting that part of the hedge has been obtained through pixel interpolation, for example as a consequence of scaling/rotation; these are processing operations that are necessary when pasting an object/region inside an image to make it fit into the target location.

CLONES BLOCKS AND CLONES KEYPOINTS

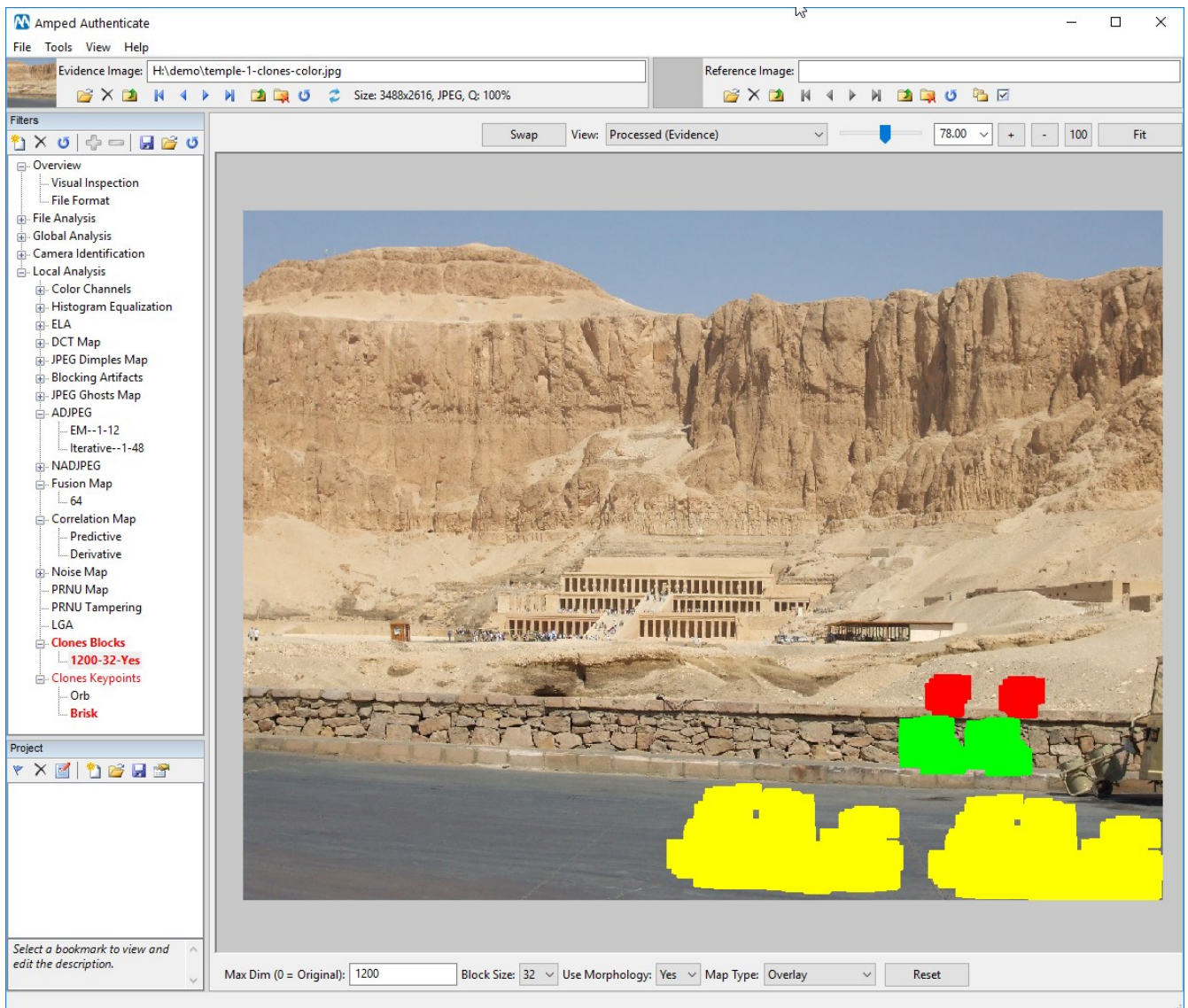
Copy-move is a specific type of forgery where part of an image is cloned and pasted into the image itself (possibly after geometric transformations). Compared to other kinds of manipulations, copy-move is usually simpler to carry out and it deserves particular attention when investigating the authenticity of an image.



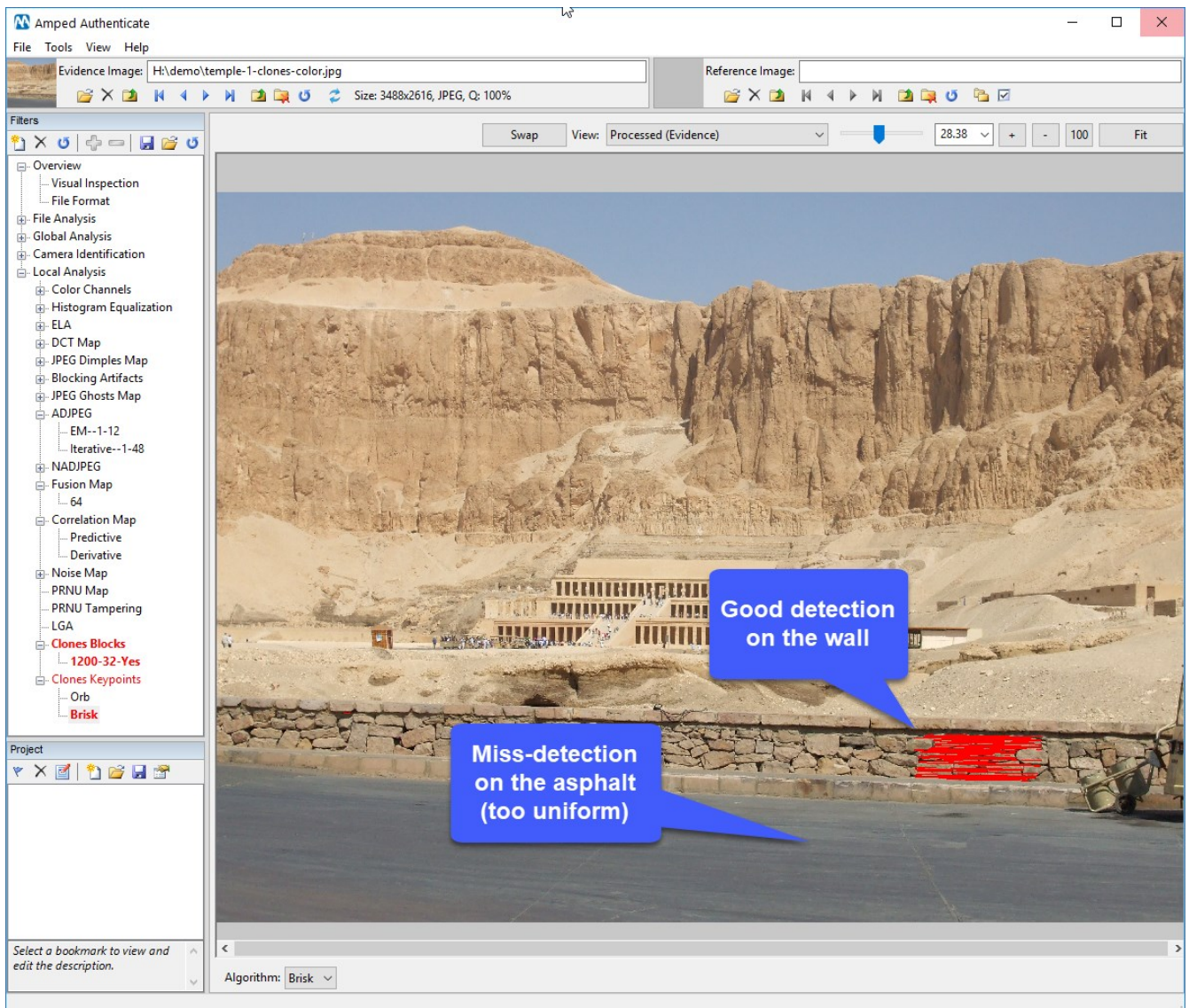
Authenticate features two different and complementary tools for clone detection: Clones Blocks and Clones Keypoints.

Clones Keypoints works by extracting local image descriptors from the image and looking for sets of matching descriptors. The strength of this filter is its robustness to geometric transformations: even if the cloned object has been severely scaled and/or rotated, there are good chances to detect it, as shown in the example above. This is important because, when replicating an object in the image, it is often necessary to adjust its geometry to preserve physical and perspective coherence.

Unfortunately, when the cloned region is very flat, keypoints are usually not present, so detection fails.



This is where the Clones Blocks comes in handy: it performs a dense matching between all regions of the image, so even the flattest clones can be detected. Contrary to the Clones Keypoints filter, Clones Blocks works best when the cloned region has not been rotated/scaled significantly. This commonly happens when the clone operation aims to hide something that was in the original image, as in the example above: the attacker cloned part of the asphalt to cover something that was on the street (part of the wall was cloned as well). Since the asphalt has a uniform representation in the image, the Clones Keypoints would have missed this clone, as shown below.

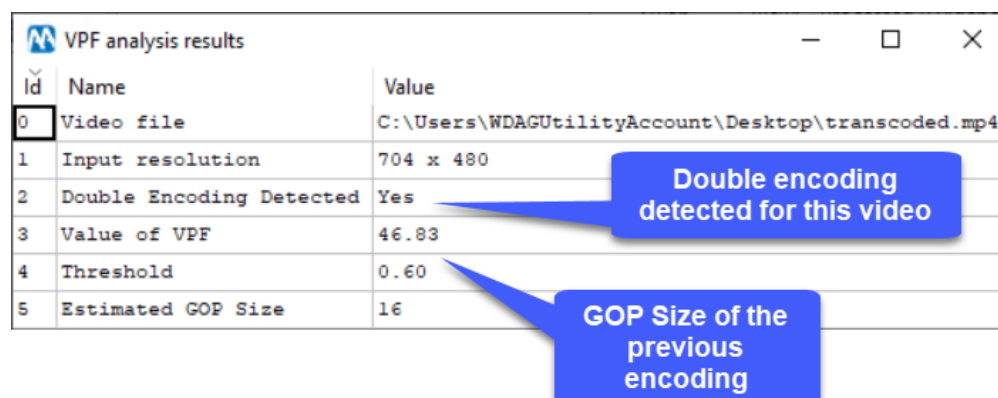


This example stresses the importance of a synergistic analysis: image integrity and authenticity verification need a comprehensive suite of reliable and documented tools: this is what Amped Authenticate provides.

VIDEO INTEGRITY VERIFICATION

Detecting double encoding is an important step towards integrity verification: indeed, virtually all videos are encoded during acquisition, and if integrity is preserved, that should be the only encoding step. Instead, whenever a video is processed in any way, including simple recompression or conversion to a different codec, that normally implies one more encoding step at the end of the processing.

The VPF Analysis aims at revealing whether a video shows traces of double compression, and when this is the case, it provides an estimate of the Group of Picture (GOP) size of the previous encoding.



VPF analysis results

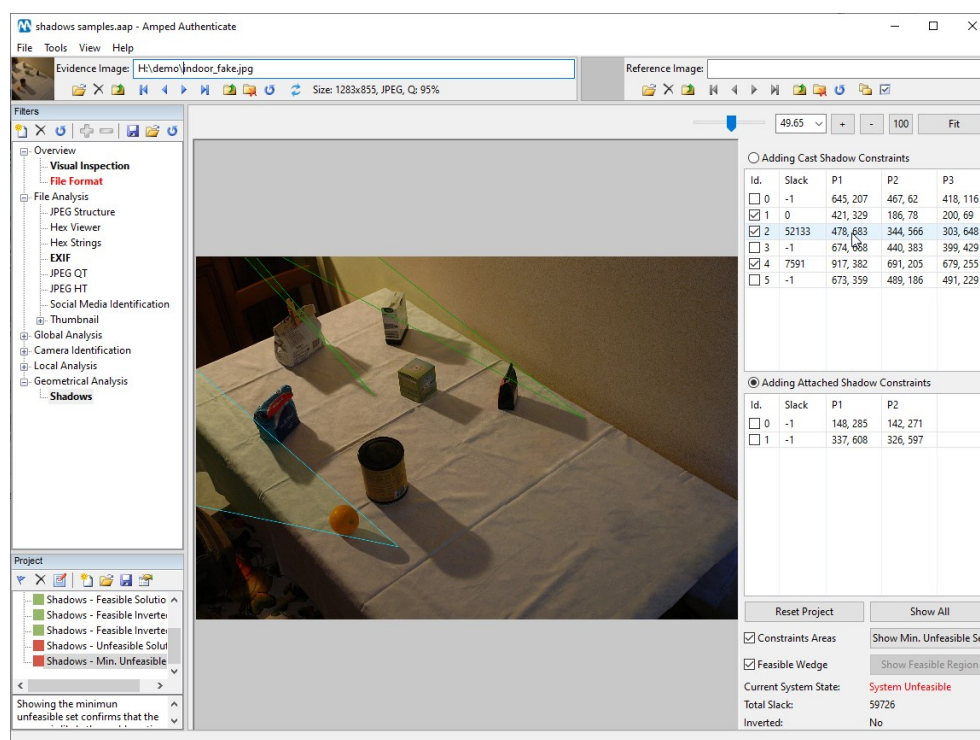
Id	Name	Value
0	Video file	C:\Users\WDAGUtilityAccount\Desktop\transcoded.mp4
1	Input resolution	704 x 480
2	Double Encoding Detected	Yes
3	Value of VPF	46.83
4	Threshold	0.60
5	Estimated GOP Size	16

Double encoding detected for this video

GOP Size of the previous encoding

SHADOWS

One of the hardest parts of forging an image is to keep lights, shadows, and perspective consistent. The Shadows filter, under the Geometrical Analysis category, help the analyst check the technical consistency of cast and attached shadows in an image. Since they don't depend on compression or acquisition traces, Geometrical Analysis filters are very robust to post-processing and are suitable for low-quality images such as those from social media platforms. They can also be used on scanned images or frames extracted from a video.



shadows.samples.aap - Amped Authenticate

File Tools View Help

Evidence Image: H:\demo\indoor_fake.jpg Size: 1283x855, JPEG, Q: 95%

Reference Image:

Filters

- Overview
- Visual Inspection
- File Analysis
 - JPEG Structure
 - Hex Viewer
 - Hex Strings
 - EXIF
 - JPEG QT
 - JPEG HT
 - Social Media Identification
 - Thumbnail
- Global Analysis
- Camera Identification
- Local Analysis
- Geometrical Analysis
 - Shadows

Project

- Shadows - Feasible Solution
- Shadows - Feasible Invert
- Shadows - Feasible Invert
- Shadows - Unfeasible Solution
- Shadows - Min. Unfeasible

Showing the minimum unfeasible set confirms that the

Adding Cast Shadow Constraints

Id.	Slack	P1	P2	P3
0	-1	645, 207	467, 62	418, 116
1	0	421, 329	186, 78	200, 69
2	52133	478, 683	344, 566	303, 648
3	-1	674, 988	440, 383	399, 429
4	7591	917, 382	691, 205	679, 255
5	-1	673, 359	489, 186	491, 229

Adding Attached Shadow Constraints

Id.	Slack	P1	P2
0	-1	148, 285	142, 271
1	-1	337, 608	326, 597

Reset Project Show All

Constraints Areas Show Min. Unfeasible Set

Feasible Wedge Show Feasible Region

Current System State: System Unfeasible

Total Slack: 59726

Inverted: No

SMART REPORT

The Smart Report is designed for fast screening of many images. It automatically processes multiple files with a self-tuning set of filters, including metadata analysis and forgery localization. Images are then grouped in the output report based on their “integrity level”, represented as a traffic light icon:

- 1) Green is shown when all metadata are consistent with those of a camera original image (in this case, forgery localization filter are not executed to speed up processing).
- 2) Yellow is presented when at least one metadata raised a warning, but forgery localization did not reveal any tampering.
- 3) Red is used when at least one forgery localization tool raised a warning.

Amped Authenticate Smart Report

Report Generation: 2019-05-24 09:08:07
 Program Version Info:
 Build date: 20190523
 Revision: 13332
 Platform: Microsoft Windows, 64 bit

Summary Table

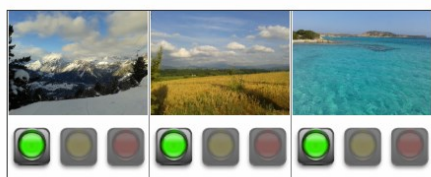
Total number of processed images: 5

   Images that are likely to be camera original: 3

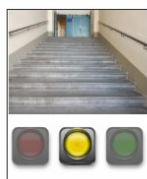
  Images with suspicious metadata but no traces of forgery: 1

  Images with traces of possible forgery: 1

Images that are likely to be camera original



Images with suspicious metadata but no traces of forgery



Images with traces of possible forgery



File 4: pier.jpg



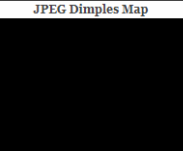
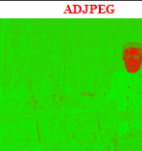
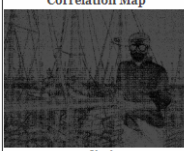



Visual inspecting the image may reveal inconsistencies in lights, shadows, proportions. Also consider possible inconsistencies at the context level (object that could not be there, image content inconsistent with information available in metadata, etc.). Click on the image to view it in a separate tab.

Brief File Format Analysis - WARNING! -

Image Properties			
Id	Name	Value	Warning message
0	Format	JPEG	
1	Image Encoded Size	[3264,2448]	
2	Aspect Ratio	1.33	
3	Thumbnail Size	[160,120]	
4	MD5	eb690c0395f0742ed0b7a092de8b611f	
Image Metadata			
Id	Name	Value	Warning message
5	Exif Make	SAMSUNG	
6	Exif Model	GT-I9105P	
7	Exif Software	Adobe Photoshop CS4 Windows	EXIF Software is an editing application
8	Exif ModifyDate	2018:10:10 12:34:34	EXIF ModifyDate differs significantly from Exif DateTimeOriginal
9	Number of Exif fields	48	
10	Number of Photoshop fields	21	
11	Number of XMP fields	62	
JPEG Info			
Id	Name	Value	Warning message
12	JPEG Quality	96	
13	JPEG QT Hash	863DA02155829A5B46C85B789F2982F8	Compression signature is incompatible with the actual camera make-model
14	JPEG HT is standard LJG	false	Huffman tables are not LJG standard

Brief Local Analysis-WARNING!-

ELA	ELA	JPEG Dimples Map	ADJPEG
			
MSE-75	MSE-90	Auto	EM-1-12
Correlation Map	Clones Keypoints		
			
Predictive	Brisk		

TRAINING

Amped Software [training](#) courses provide hands-on training on the use of Amped Software products as well as provide insight into the challenges users face in forensic video and digital multimedia evidence processing. Our courses are delivered worldwide, in large groups or private sessions, by experienced trainers.

The purpose of the Amped Software training is to:

- Provide students with the theory and the basics of image processing
- Understand the issues affecting images and videos in an investigative context
- Acquire in-depth knowledge of all software features to solve those issues, including the technical and scientific background behind the implemented techniques
- Learn the workflow that is compatible with forensic needs and constraints to take the proper steps to obtain better results
- Work on real cases and learn to testify on the results

FORENSIC IMAGE ANALYSIS WITH AMPED AUTHENTICATE

This course is recommended for users who recently purchased Amped Authenticate and for those who want to acquire training in the techniques necessary to perform authentication analysis on digital images in a forensic science setting as well as to package, deliver, and present those findings in court. The course is a mixture of lecture and hands-on. Students will obtain the knowledge and skills required to properly analyze digital images with a workflow compatible with forensic needs and constraints.

PURCHASE INFORMATION

APPLICATIONS

Amped Authenticate can be used to analyze digital images from many different sources of data that may be of interest to many different types of users.

Sources of Data	Types of End Users
<ul style="list-style-type: none"> • Crime scene • Car/House Insurance Claims / Accident Reconstruction • Child Pornography/Pedophile • Internet Search / Open-Source Intelligence • Media/Journalism • Propaganda • Documents • Social Media 	<ul style="list-style-type: none"> • Law Enforcement • Courts and judicial proceedings • District attorney / Prosecutor • City / Town halls • Protection Services • Intelligence / Secret Services • Military • Insurance companies • Private Forensics (companies / private experts)

<ul style="list-style-type: none"> • Parking/Traffic Infractions 	<ul style="list-style-type: none"> • Enterprise: Risk Management (internal company security) / corporate site security (video surveillance) • Media / News Outlets • Education / Research
---	--

MATERIAL AND LICENSING

Amped Authenticate is provided as a perpetual or subscription license, delivered electronically. For each license seat purchased the software can be installed on a single machine but used by multiple users. You can easily move the license to another machine by uninstalling it and deactivating the license on one machine before activating it on another. Alternative licensing methods can be evaluated upon request. The perpetual license guarantees that, once purchased, the software will keep working even if the Software Maintenance and Support (SMS) is expired (in that case, the user will lose access to new versions and technical support). On the other hand, the subscription license requires the user to renew the subscription to keep using the product, which is always made available in its most recent version. More information on the license terms and conditions can be found [here](#).

SOFTWARE MAINTENANCE AND SUPPORT (SMS)

Software Maintenance and Support (SMS) subscription allows you to always work with the latest version of Amped Authenticate. And if you run into any issues using Amped Authenticate, an active SMS subscription will provide you with access to technical support.

Software upgrades and unlimited technical support via email is always included with the subscription license. For the perpetual license, it is included for one year from the date of purchase. You may purchase additional years of SMS at any time.

For the perpetual license, renewal of SMS is not mandatory, so the license purchased is still valid and can be used even without an active SMS plan. Continued software upgrades and technical support however require the purchase of an SMS subscription plan. The SMS can be recovered even after its expiration, compensating for the missing years.

WHERE TO BUY

Amped Authenticate can be purchased directly from Amped Software or through one of our authorized worldwide distributors.

AMPED AUTHENTICATE TECHNICAL SPECIFICATIONS

GENERAL FEATURES

Feature	Description
	Overview
Supported Formats	Support for any standard image format (JPEG, TIFF, BMP, PNG, HEIF...) as well as RAW formats from many digital cameras.
Available Tools and Filters	40 different analysis filters and tools with user customizable configuration and optional post processing parameters (levels, scale to enhance the displayed image, highlighting of saturated regions).
Different Categories of Filters	Discriminate between camera original files, authentic images that have been modified without changing context, or non-authentic manipulated images. Perform camera identification (camera ballistics).
	User Interface
Image Display	Embedded viewer with multiple image comparison and synchronization.
Comparison Support	Most of the filters allow the comparison of results between two images, with automatic highlighting of different values or the possibility to see the difference image.
Output Image	Export options offer support for any standard image format (JPEG, TIFF, BMP, PNG...).
Output Data	Export options support export of analysis output as plain text, HTML, or TSV.
Cached Processing	Filter results are saved in a cache folder for speedy subsequent analysis.
Batch Processing	Automatically apply all filters to one image or all images in a folder. Includes support for nested folders.
Report Generation	Automatic output image and report generation with all processing results on one or more images (the user can fully customize the report layout). The following formats are available for the report generation: HTML, PDF (optionally protected) or DOC.

Batch File Format Analysis	Quick automatic analysis of the format of all images in a folder to find suspicious files (triage).
Batch File Format Comparison	Quick automatic comparison of the format of all files in a folder with the analyzed image (OR image under analysis).
Batch JPEG Comparison	Quick automatic comparison of the quantization tables of all files in a folder vs. a known reference image.
Smart Report	Designed for fast screening of many images, it automatically selects the most appropriate subset of filters for each image, providing brief and organized reporting.
Excel Integration	Export a multiple file analysis results table directly to Microsoft Excel for further processing.
Google Maps Integration	Display image location in Google Maps.
Google Images Integration	Search for images with similar content on Google Images.
Suncalc Integration	Shows the Sun position over a map for the date and time available in the metadata.
Flickr Integration	Search for images from a specific camera model on Flickr. Supports advanced filtering based on image features.
CameraForensics Integration	Search for images from a specific camera model, even specifying the JPEG Quantization Tables, on billions of images crawled by CameraForensics on the web (requires subscription to that service).
Extraction of Embedded JPEGs	Extract JPEG images embedded in any file type (images files, PDF, PPT, DOC, disk image...) for questioned document authentication support.
File Formats Warning Customization	Customization of all the criteria for evaluating the camera original files.
Used Filters and Configurations Customization	The user can add, remove, change, delete, enable or disable filter configurations (or even filter groups) to use for analysis. Different configurations and workspaces can be saved and reloaded when needed.

Automatic Warnings	If analysis of an image detects signs of manipulation, the filter's label appears in red (not available on all filters).
Log	All actions performed by the user are saved onto a log text file. Features can optionally be disabled by the user.
Command Line API	A simple but powerful command line API provides unsupervised operation and easy integration with third party tools.
	Video Tools
PRNU	<ul style="list-style-type: none"> - Create CRP: This tool computes a Camera Reference Pattern from a single digital video, provided it is not affected by digital stabilization. - Identification: After the CRP creation with the Create CRP tool, the Identification tool can be used to check whether an evidence video is compatible with such CRP in terms of sensor noise. - Tampering: After the CRP creation with the Create CRP tool, the Tampering tool will check which parts of an evidence video were acquired with the reference device.
Variation of Prediction Footprint (VPF)	VPF analysis allows video double encoding detection and estimating the Group of Pictures (GOP) size of the previous encoding. Detecting video recompression is an important step towards video integrity verification.
	System and Documentation
Compatibility	Compatibility. Runs on any standard PC, with Windows 7, 8, 10, 11 both 32 bits and 64 bits. Windows 10 or 11, 64 bits is suggested. Supports all major virtualization platforms. Macs are also supported via Bootcamp or virtual machines.
Available in 32 and 64 bits	The standard installer includes both the 32- and 64-bits version of the program and the user can switch freely between the two.
High Resolution Support	Support for HiDPI (Retina) screens keeping the proper layout of text and panels.
Licensing Mode	Standalone software provided as subscription or perpetual license, delivered electronically. Alternative licensing methods can be evaluated upon request. Once activated, the software can operate completely offline with no Internet or other network connection. The software installer is provided on the Amped Support Portal as a downloadable file.

Updates	All software updates, both minor and major, are guaranteed when the SMS (software maintenance and support) is active. The SMS is always included with the subscription license. For the perpetual license, the first year of SMS is included with the initial purchase, additional years can be purchased together with the license or at a later time.
Supported Languages	Available in English, Chinese, Italian, Japanese, Russian. All languages are installed and can be freely switched by the user with a simple restart. Additional languages can be added upon request. Localization includes the user interface, manuals, and generated reports.
Documentation and Tutorials	Complete and in-depth documentation which includes references to the scientific paper related to the algorithms used.
Samples	Rich collection of sample projects to help acquaint users with the filters and tools.
Training	In-depth training on the use of the software available worldwide (to be purchased separately, not available for all countries).

AVAILABLE FILTERS

Filter	Description
	Overview
Visual Inspection	Visual analysis of the image and comparison with a reference image.
File Format	Automatic inspection of most common parameters that could indicate non-originality of the image.
	File Analysis
JPEG Structure	Display / comparison of main JPEG markers.
Hex Viewer	Integrated hexadecimal viewer with search and comparison capabilities.
Hex Strings	Extraction of all textual information embedded into an image file.

EXIF	Display / comparison of EXIF information and other embedded metadata.
JPEG QT	Display / comparison of JPEG quantization tables and other compression parameters of the main image, embedded thumbnail, and preview. Internal camera and software database with thousands of configurations and support for user generated databases. New QTs are added periodically with new software updates.
JPEG HT	Display / comparison of JPEG Huffman Tables of the main image, embedded thumbnail, and preview.
Social Media Identification	Checks whether the image likely comes from a Social Media Platform (the available database covers Facebook, Flickr, Tumblr, Imgur, Whatsapp, Instagram, Tinypic, and Telegram)
Thumbnail	Display of embedded thumbnail and preview images and their difference with the main image.
Global Analysis	
DCT Plot	Analysis and comparison of the histogram of the DCT coefficients and its Fourier transform for detecting multiple re-saves of the image.
JPEG Ghosts Plot	Plot of the image with its recompressed version to identify signs of multiple compressions.
Correlation Plot	Analysis / comparison of correlation periodicities in the image pixels to analyze the presence and consistency of demosaicing or interpolation effects. Guidelines can assess the cause of different peaks in the plot.
JPEG Dimples	Measures the strength of the JPEG Dimples compression artifact in image pixels. JPEG Dimples are expected to be present for some camera models and not for others.
Histogram	Analysis of the histogram of the image to help spot excessive intensity adjustment.
Color Space	Analysis of the color space usage of the image in the HSV and Lab coordinates to help spot excessive color adjustment.
Fourier	Analysis of the image in the frequency domain to identity traces of screen recapture.
Camera Identification	

PRNU Identification	Creation of a PRNU (sensor noise) reference pattern from a user supplied set of pictures and identification of the device that generated the image by comparison with the reference pattern. Ability to distinguish pictures coming from different exemplars of cameras, even if of the same make and model. By enabling the “Advanced Research”, the algorithm works even if the image underwent both resize and crop (e.g. Digital Zoom), which makes it possible to carry out the source identification of digital videos when only images are available as reference and vice-versa. The comparison of two different reference patterns is also available.
	Local Analysis
Color Channels	Analysis of single image channels in different color spaces (RGB, YCbCr, YUV, HSV, HLS, XYZ, Lab, Luv, CMYK).
Histogram Equalization	Contrast enhancement that permits user to spot traces of manipulation.
ELA	Identification of manipulated areas of the image that have a different compression history (error level analysis).
DCT Map	Display image DCT values to help spot tampered uniform areas of the image.
JPEG Dimples Map	Identification of manipulated areas of the image based on the local absence of JPEG Dimples artifacts (works when the image is affected by the JPEG Dimples globally).
Blocking Artifacts	Detection of inconsistencies of compression blocking artifacts of the image due to image manipulation.
JPEG Ghosts Map	Identification of manipulated areas of the image based on pixel-domain analysis of multiple JPEG compression.
ADJPEG	Identification of manipulated areas of the image based on DCT-domain analysis of aligned double JPEG quantization artifacts (ADJPEG). Useful when a JPEG image is opened, locally changed (tampering with pixel, or pasting content from other image) and finally re-saved as JPEG without any global post-processing.
NADJPEG	Identification of manipulated areas of the image based on DCT-domain analysis of non-aligned double JPEG quantization artifacts (NADJPEG). Useful when a large patch of pixels was pasted from a JPEG image into the suspect image followed by JPEG compression without any global post-processing.

Fusion Map	Identification of manipulated areas of the image based on the joint analysis of JPEG Ghosts Map, ADJPEG and NADJPEG. Takes into account the local properties of the image to improve output map.
Correlation Map	Identification of discontinuities in the correlation between pixels of the image. Useful when part of the image contains interpolated pixels (e.g., due to resizing or rotation), or when the image is globally resized/rotated and then local tampering takes place.
Noise Map	Display of inconsistencies in the noise level of the image.
PRNU Map	Identification of inconsistencies in the PRNU noise of the image.
PRNU Tampering	Automatic identification of tampered areas of the image by comparison with the PRNU reference pattern of the image.
LGA	Identification of luminance discontinuities (luminance gradient analysis).
Clones Blocks	Identification of similar areas of the image that can be the result of cloning. Also works on uniform areas, but not if the clones have been modified.
Clones Keypoints	Identification of groups of similar points in the image that can be the result of cloning. Also works if the clones have been modified, but not on uniform areas.
	Geometrical Analysis
Shadows	Allows checking the inconsistency of cast and attached shadows in an image





HARDWARE REQUIREMENTS

	Minimum requirements	Suggested requirements
CPU	Intel Core i3	Intel Core i5 or faster
RAM	4 GB	8 GB or more
Hard drive space	1 GB free for program files	1 GB free for program files, 10 GB or more for casework files
Screen	13", 1024x768	24" or bigger, 2560x1440 or bigger
Graphic card	No specific requirement	No specific requirement

	Minimum requirements	Suggested requirements
OS	Windows 7 (32/64 bits) Windows 8 (32/64 bits) Windows 10 (32/64 bits) Windows 11 (32/64 bits)	Windows 10 or 11, 64 bits

THE AMPED ECOSYSTEM FOR FORENSIC IMAGE AND VIDEO ANALYSIS

Learn about the full line of solutions that have been developed to assist an entire organization with all investigations, starting from the field, up to the forensic lab, and then to the courtroom.

	<p>For investigators and frontline officers to conduct a first level analysis of their video evidence, with quick and easy conversion, enhancement and annotation functions.</p>
	<p>For technicians tasked with converting a great number of surveillance videos in various proprietary formats, speeding up the triage in cases such as major investigations.</p>
	<p>For forensic lab experts to manage the complete image and video analysis workflow, with advanced and fully customizable processes for conversion, restoration, enhancement, measurement, presentation, and reporting, all in a single tool.</p>
	<p>For digital forensic experts to exploit the data behind digital images. Allowing analysis of image integrity, authenticity, metadata, source and history, and detection of tampering prior to its use as intelligence and evidence.</p>

ABOUT US

SETTING THE STANDARD FOR IMAGE AND VIDEO FORENSICS



OUR STORY

Amped Software was founded in Trieste, Italy, in 2008 by Martino Jerian. While working on his master thesis in Digital Image Processing at the University of Trieste, in collaboration with the Scientific Investigation Department of Carabinieri (Italian Military Police), Martino realized that video processing solutions for forensic applications were poor or non-existent, and not one single product could be found that met all of the needs of a forensic analyst. Products offered at the time were a compromise of features or were incomplete and required other products to accomplish common tasks. This is why Martino decided to develop Amped FIVE, the company's flagship product.

Amped Software has thus been recognized as an innovator in the national and international arena. In 2008, barely a year from its founding, Amped Software was awarded as the best Italian start-up at the Tech Garage business competition, held during SMAU tradeshow. In 2010, Amped Software was presented in the book "Winning Italy: Almanac of Italian Excellence" by the Ministry of Foreign Affairs, which highlights significant innovation and achievements by Italian companies and individuals. Amped Software was also highlighted as a leader in scientific accomplishments in a world class group which featured prominent companies such as Ferrari, senior "Big Bang" CERN researcher Lucio Rossi, and Lorenzo Thione, the developer of the technology used by Microsoft in the Bing search engine. In 2017, Amped Software was ranked on the Deloitte Technology Fast 500 EMEA, that recognizes companies that have achieved the fastest rates of revenue growth in Europe, the Middle East, and Africa (EMEA).

OUR FOCUS: JUSTICE THROUGH SCIENCE

Amped Software is committed to help fight crime to keep communities safe, by offering innovative solutions to help convict criminals and protect the innocent.

We are setting the standard for image and video forensics. We focus on developing the most advanced and complete, yet simple and easy-to-use technologies for all image and video processing needs related to forensics, public security, and investigations. With an emphasis on the transparency of the methodologies used, our solutions empower our customers with the three main principles of the scientific method: accuracy, repeatability, and reproducibility. We also invest in research and in the development of best practices to make image and video forensics evolve faster.

Our customers are our number one priority. We continually listen to our customers and adapt and update our solutions on a monthly basis, in order to meet their evolving needs in digital image and video forensics.

OUR TEAM

Amped Software is made of a team of highly experienced digital forensic experts that used our own software to work on numerous real cases, in which many are of national and international importance. Some team members have also previously served in law enforcement and military. Because of our diverse experience we have a rare insight into how our tools work in practice and are able to emphasize any limitations or missing features for us to improve.

OUR CUSTOMERS

Important forensic labs, law enforcement, government, military, and security organizations worldwide use our solutions. Our products have been sold in close to 90 countries.

OUR PARTNERS

Amped Software has a large worldwide network of distributors. We also have several strategic and technological partnerships with some of the best companies in the law enforcement and video surveillance fields.

GLOBAL HEADQUARTERS

Amped SRL

Loc. Padriciano, 99

34149 Trieste, Italy

P: +39 040 3755333

info@ampedsoftware.com

NORTH AMERICAN SALES

Amped Software USA Inc.

18 Bridge Street, Unit 2A

Brooklyn, NY 11201, USA

P: + 1 (718) 395-9736

info@ampedsoftware.com

