

Forum:[Hack Forums](#)

Thread: [\[TuT\] Metadata - Gather Information & Improve PDF exploit success in Kali](#)

_Silky - April 20, 2013, 2:38 am

In this tutorial, I'm going to show you an easy and effective technique to extract metadata literally in seconds using exiftool. Metadata is nothing more than "data of data", which is actually a lot. They used metadata to catch McAfee when he went AWOL last year. Not many people knew of exiftool in the Backtrack 5 series and I was quite upset when it didn't come with Kali and I am not a fan of the current image forensics tools that came with Kali so I went and installed it. Exiftool goes way beyond this tutorial as you can read, write, and manipulate metadata in such files as photos, microsoft office documents, xml and more. This is VERY valuable information during any penetration test. I'm not going to show you how to manipulate metadata yet and this time I'm not going to assume you're new to Linux, but here is a [Cheat Sheet](#) if you need it.

Requirements

ExifTool [Install ExifTool for Kali, Windows, or OS X here.](#)

That website also comes with complete documentation of ExifTool and I highly recommend you to look it over.

For Backtrack users - Type "exiftool -ver", and if you have the default version 7.*, you'll need to upgrade it to 9.2 or higher to extract data from Microsoft Office documents.

Windows users, you're on your own as the only thing you have to do is drag and drop from now on, though you'll miss out.

1. Extract Metadata from JPG

Get a photo, any photo. My photo is called IMG_3881.JPG. You must be in the same directory as the file you want to extract, in my case it's on the desktop. We're going to do a painfully easy command. My photo is called IMG_3881.JPG, it's important to note that the file extensions are case sensitive.

Code exiftool IMG_3881.JPG

As you can see how much valuable information you will get. I couldn't even fit all the information in one picture, what doesn't show are the almost exact GPS location of where the photo was taken, along with the direction. Also note that you'll be able to see if the photo was edited or not and with what software, in this case it wasn't. Let's use some filters to only show interesting data...

Code exiftool -filename -gpsposition -exposureprogram -cameramodelname -createdate -flash -exif:fnumber -xmp: all IMG_3881.JPG

Let's take our information gathering even further and search that GPS Position on Google Maps. You'll have to take out the quotes and "deg" so it will look like 36 4 12.60 N, 115 2 42.00 W

And as you can see I come up just short of Paradise. Using this technique makes it very easy to create a nasty social engineering attack as some of you may notice.

2. Removing Metadata Anti-Forensics

Looking at the first photo, you can see it was taken with an iPhone 4S and we all know Apple is Notorious in not giving a shit about your privacy, so we're going to remove this metadata with one easy command.

Code exiftool -all= IMG_3881.JPG

Compare these results with the first photo. You'll have to delete the photo that is now tagged with "original" as that is the one with all the original metadata.

3. PDF Analyzing

Let's move on to something even more important, analyzing metadata from a PDF file. As every hacker knows, the more information you have, the more successful your exploit will be and good hackers are never lazy. PDF metadata is a vital piece of information if you can get it from your victim.

I just did a quick Google file:pdf search and downloaded the first result which was something from Ohio State University, called "lesson2.pdf". We're going to extract the metadata and save it to a text file, because you need to keep the information you gather about your target to be successful right? Yes!

```
Code exiftool -pdfversion -createdate -metadatadate -creatortool -xmptoolkit -documentid -hasxfa -producer -xmp: lesson2.pdf > pdf_info.txtCode cat pdf_info.txt
```

And as you can see, the results can be deadly. This was a quick tutorial and as always, I lay it out for you to play it out. I highly recommend you to play around with this tool and learn it well because there are many more things you can do with it. Hope this helped you, thanks for reading!

Rasen_Shurik3n - April 20, 2013, 11:34 am

Very usefull information for those interested in forensics.

One question though. Why do you prefer this exact tool? Are any cons with it that other tools doesn't have?

_Silky - April 20, 2013, 1:13 pm

(Apr 20, 2013 11:34 AM)Rasen_Shurik3n Wrote: [\[CITE\]](#) Very usefull information for those interested in forensics.

One question though. Why do you prefer this exact tool? Are any cons with it that other tools doesn't have?

Because ExifTool is fast, effective, and easy! And powerful. You can suck every ounce of raw information out of just about any file out there without messing around compared to the other tools, and best of all you can manipulate the data. It's just as much an information gathering technique as it is forensics.

falkonviper - April 28, 2013, 1:41 am

Very Good , keep it up ?

..
???????

Ancalagonn - April 28, 2013, 9:12 am

I was wondering what tool they used for this. Thanks, good tutorial.

?rew - April 29, 2013, 6:58 pm

Just a heads up there is a Gui version of this tool <http://u88.n24.queensu.ca/~bogdan/>

_Silky - April 29, 2013, 7:21 pm

(Apr 29, 2013 06:58 PM)?rew Wrote: [\[CITE\]](#) Just a heads up there is a Gui version of this tool <http://u88.n24.queensu.ca/~bogdan/>

I never use Windows and thought ExifTool automatically came with a GUI. Unfortunately, I can't reference this in the tutorial for another 1440 minutes >.< But hopefully Windows users won't pass

up your link. Thanks for sharing this krew!

DrDinosaur - April 29, 2013, 7:23 pm

This is a very interesting tool and tutorial.

bruce_jones - May 2, 2013, 12:39 am

Nice important tool and interesting share mate.

Goodies - July 19, 2013, 3:26 pm

This is neat but I do this with python (I think this is actually written in python)

MFFS - July 20, 2013, 1:50 am

Nice tutorial. Very helpful. Keep it up.

Shadow Walker - July 20, 2013, 8:14 am

this is a solid guide, will come back to it very soon indeed.

Regards,
Shadow Walker

Hermes00 - July 21, 2013, 4:40 pm

Very useful information! Thanks for sharing with us ;)

Goodies - August 15, 2013, 8:22 pm

I may POSSIBLY make a java GUI for this. That would be so fucking fun but I'm busy :/