

# Forum:[Hack Forums](#)

Thread: [GPS Meta data Recovery Photos \[TUT\]](#)

Culperring722 - August 2, 2015, 8:10 pm

## Forensics Metadata Photos

Meta data can be very dangerous. The FBI uses it to track down criminals and pedophiles who post images to the web. Criminals can use it to track your every movements. You may not know it but when you upload photos to the internet you may be uploading your Latitude and Longitude cords, Date picture was taken, Your Name, The brand used to take the picture, and possible even more.

Tooday ill show you guys how to extract some information. Ill be using random images from the web to see if I can extract some interesting information.

Tools:

Hex Edito

Hexidecimal to decimal converte

Now that we have our Hex Editor of choice im using HxD we can begin. Start by opening the file in your hex editor and look at the beginning. You will notice some interesting information at the beginning of the file.

In Red You will see the type of device that took the photo.

In Blue You will see the Date the photo was taken

In Black You will see the Time it was taken(Military Time)

The main purpose of this tutorial is how to find GPS location in photo. I just wanted to briefly show where the other information was located.

First we will look for some key identifiers ( N S W E) These are the directions you would see on a cumpous and they are going to help us locate the latitude and longitude cords.

Ok now I need to tell you something.

1. Keep an eye out for this pattern 00 00 xx xx 00 00 00 01 00 00 xx xx 00 00 00 01 00 00 00 xx xx 00 00 00 64 or 00 00 03 E8.

2. 00 00 00 00 64 = 100

3. 00 00 03 E8 = 1000

Note that the pattern may also look like this 00 00 xx xx 00 00 00 01 00 00 xx xx 00 00 00 64

Can You see the pattern ?

First we are going to count 4 bytes before the first 00 00 00 01. Which is 00 00 00 2A

Now convert those hexadecimal numbers to decimal.

00 00 00 01 = 1  
00 00 00 2A = 42  
 $42/1 = 42$   
Degrees = 42

Now count the next 4 bytes 00 00 07 E4(2020)  
The next for bytes is 00 00 00 64 (100)  
 $2020/100 = 20.2$   
Minutes = 20  
Now take off every thing after the decimal and times it by 60  
 $.2 \times 60 = 12$   
Seconds = 12

Latitude = 42:20:12 N

Normally the next 8 bytes we would do the same but for the seconds. But since the Minutes produced a decimal we just converted it right there. So skip the next 8 bytes 00 00 00 00 00 00 00 01

Now lets find the Longitude

Ok First take 00 00 00 47 and convert it to decimal like before  
00 00 00 47 = 71  
00 00 00 01 = 1  
 $71/1 = 71$   
Degree = 71

Now for the minutes.  
00 00 03 48 = 840  
00 00 00 64 = 100  
 $840 / 100 = 8.4$   
Minutes = 8

We can find the seconds by multiplying .4 by 60  
 $.4 \times 60 = 24$   
Seconds = 24.

Longitude = 71:8:24

Your Location is :  
Latitude = 42:20:12 N  
Longitude = 71:8:24 W  
Now i can stalk you?

We can check it by right click the pic going to properties and looking at the details tab.

Want to try it yourself???

Here is the photo that i used... I picked the first pick in google images and it looks like they didnt turn off their gps location with their iphone.

[https://mega.co.nz/#!akl1wDBA!E5Iib0l\\_CrsnlhKO4W5kgI33RAtx9oI0m3MDKt\\_hNSM](https://mega.co.nz/#!akl1wDBA!E5Iib0l_CrsnlhKO4W5kgI33RAtx9oI0m3MDKt_hNSM)

Now that you know where to find this information you can easily use your hex editor and write over that data with 000000s so that it erases it. Or better yet turn off that GPS location.

PS.

I never see forensics tutorials in this section im not sure if you guys like them or not. If so let me know cuz i know how to do some cool stuff. Like recovery deleted files manually not using automated tools, Hide files in slack space, ntfs file system forensics, fat32 file system forensics, Registry forensics, and some other stuff.

**DrDinosaur** - August 2, 2015, 9:12 pm

You should use exiftool, which is much easier and less prone to error.

**\_Silky** - August 3, 2015, 3:59 am

It's been in the graveyard for some time now but I made a tutorial on [Exiftool](#) a long ass time ago which is basically just a shortcut to what you're doing.

A better example would have been an exe or something but this tut is good for beginners, a lot don't know how to read that hex even though it's right in front of their face, in English!

**Culperring722** - August 3, 2015, 4:48 am

(Aug 2, 2015 09:12 PM)DrDinosaur Wrote: [\[CITE\]](#) You should use exiftool, which is much easier and less prone to error. Tools are nice and all but some times its nice to know whats happening under the hood and how to do stuff manually with out using automated tools. If you know how to do it manually you can make your own tools?. Also if you know where to find this data you can easily scrub it from your pictures or even put in misleading GPS coordinates to trick forensics.

If i was actually trying to get location data i would use a tool just for the speed. Exiftool is great especially when combined with kismet so you can plot the cords on a map.

**Josch** - August 3, 2015, 11:42 am

Great tutorial! Agree 100% that it's best to know how to do something manually before even considering using an automated tool just to cut time.

**hahdbwoannniabs** - August 3, 2015, 12:58 pm

This is a very old method and only plausible in cases where Location Services are enabled when the picture was taken.

**.GonZ0.** - August 3, 2015, 2:22 pm

Wow thanks for sharing this info with us!

**SIM-5561** - August 4, 2015, 12:46 pm

(Aug 2, 2015 09:12 PM)DrDinosaur Wrote: [\[CITE\]](#) You should use exiftool, which is much easier and less prone to error.

Yeah I agree with DrDinosaur. For digital forensics, you cannot afford to be a tiny, tiny, tiny bit wrong. If you're wrong about anything, even by a 0 or 1 in hex - your investigation was worth ZERO...

I would stick to the tools to pull this out. I can't say for sure, but I don't think this technique would work on newer iPhones (would it?) I notice the example was an iPhone 3GS which is ancient.

I'd just use exiftool. I actually created a free tool on github that would rip coordinates from

photographs and display them on google earth.

**Culperring722** - August 4, 2015, 8:41 pm

(Aug 4, 2015 12:46 PM)puzzle9 Wrote: [\[CITE\]](#) Yeah I agree with DrDinosaur. For digital forensics, you cannot afford to be a tiny, tiny, tiny bit wrong. If you're wrong about anything, even by a 0 or 1 in hex - your investigation was worth ZERO...

I would stick to the tools to pull this out. I can't say for sure, but I don't think this technique would work on newer iPhones (would it?) I notice the example was an iPhone 3GS which is ancient.

I'd just use exiftool. I actually created a free tool on github that would rip coordinates from photographs and display them on google earth.

Yup you should use verified tools for forensics. But for all my forensics classes they have made us learn how to do it manually before even touching automated tools. This works on all devices with GPS-location turned on... Only difference it that it can sometimes be located a little further down in the text, or maybe its reversed and you will have to do it backwards. But for the most part its the same with minor changes that are easy to detect and deal with according if you know what your doing.

**gizmodo** - August 5, 2015, 5:26 pm

(Aug 4, 2015 08:41 PM)Culperring722 Wrote: [\[CITE\]](#) Yup you should use verified tools for forensics. But for all my forensics classes they have made us learn how to do it manually before even touching automated tools. This works on all devices with GPS-location turned on... Only difference it that it can sometimes be located a little further down in the text, or maybe its reversed and you will have to do it backwards. But for the most part its the same with minor changes that are easy to detect and deal with according if you know what your doing.

I'd say good effort, I take it you are just learning Mobile forensics? Once they start you with Cellebrite or XRY those dates and time will be included in your report automatically. The reason why the school is teaching you the basic meta data recovery is because if you end up as an expert witness at least you would know how to explain it on how you managed to extract the data.

**Culperring722** - August 6, 2015, 6:33 pm

(Aug 5, 2015 05:26 PM)gizmodo Wrote: [\[CITE\]](#) I'd say good effort, I take it you are just learning Mobile forensics? Once they start you with Cellebrite or XRY those dates and time will be included in your report automatically. The reason why the school is teaching you the basic meta data recovery is because if you end up as an expert witness at least you would know how to explain it on how you managed to extract the data.

Learned this like a year ago in my beginning forensics class. We were actually learning forensics with NTLM and Fat32 systems. He just happen to throw that in there just to show us the dangers of gps location.