Blast from the past

saya diberikan sebuah file gambar yang dimana file gambar tersebut memiliki timestamp date

```
exiftool original.jpg | grep "Time"
File Modification Date/Time : 2026:01:28 12:04:32+07:00
File Access Date/Time : 2026:01:28 12:04:43+07:00
File Inode Change Date/Time : 2026:01:28 12:04:32+07:00
Exposure Time : 1/24
Date/Time Original : 2023:11:20 15:46:23
Sub Sec Time : 703
Sub Sec Time Original : 703
Sub Sec Time Digitized : 703
Time Stamp : 2023:11:21 03:46:21.420+07:00
Date/Time Original : 2023:11:20 15:46:23.703
```

sebagai berikut, yang saya perlukan adalah merubah timestamp ini menjadi lebih lawas

Deskripsi

Juri untuk gambar-gambar ini adalah penggemar sejati barang antik. Bisakah Anda menua foto ini sesuai spesifikasi?

bagaimana kita dapat melakukannya?

sebenarnya exiftool sendiri tak hanya dirancang untuk mengetahui metadata dari sebuah file, melainkkan juga untuk melakukan manipulasi pada metadata tersebut, salah satu contohnya adalah mengubah timestamp2 diatas sesuai dengan kemauan kita.

bagaimana commandnya?

sebelum itu ada 3 aspek yang perlu kita perhatikan, yaitu

```
Sub Sec Time : 703
```

`Sub Sec Time` (tanpa embel-embel) merepresentasikan **pecahan detik dari waktu terakhir metadata ditulis atau file difinalisasi**. Ini biasanya berpasangan dengan `DateTime`, yang sering diartikan sebagai “last modified time” di level EXIF, bukan filesystem. Ketika foto diedit, dikompresi ulang, atau disimpan ulang oleh software, field inilah yang paling sering berubah, sementara `SubSecTimeOriginal` tetap. Karena itu, dalam investigasi, perbedaan antara `Sub Sec Time` dan dua field lainnya sering menjadi indikator bahwa file telah diproses ulang setelah pengambilan gambar.

```
Sub Sec Time Original : 703
```

`Sub Sec Time Original` merepresentasikan **pecahan detik pada saat cahaya benar-benar ditangkap oleh sensor kamera**. Inilah momen paling “murni” dari sebuah foto, karena belum ada proses digital apa pun. Secara forensik, ini sering dianggap sebagai waktu kejadian paling dekat dengan realitas fisik. Jika seseorang memotret dua gambar dalam mode burst, perbedaan urutan biasanya paling jelas terlihat di field ini. Dalam kasus nyata, investigator sering menjadikan nilai ini sebagai referensi utama ketika ingin membuktikan urutan kejadian yang terjadi sangat berdekatan.

`Sub Sec Time Digitized : 703`

`Sub Sec Time Digitized` merepresentasikan **pecahan detik ketika sinyal analog dari sensor dikonversi menjadi data digital**. Setelah cahaya ditangkap, kamera melakukan analog-to-digital conversion (ADC). Proses ini terjadi sangat cepat, tetapi tetap membutuhkan waktu. Oleh karena itu, SubSecDigitized biasanya sama atau sedikit lebih besar dari SubSecOriginal. Dalam foto normal, selisihnya kecil sekali, sering kali identik karena resolusi jam internal kamera terbatas. Dalam konteks forensik, perbedaan yang aneh antara Original dan Digitized bisa mengindikasikan proses pasca-capture yang tidak wajar, seperti re-encoding atau manipulasi.

nah, bagaimana agar kita bisa melakukan manipulasi pada timestampnya, dengan command di bawah ketiga timestamp tadi bisa di manipulasi

```
exiftool
-SubSecCreateDate='1970:01:01 00:00:00.001' \
-SubSecDateTimeOriginal='1970:01:01 00:00:00.001' \
-SubSecModifyDate='1970:01:01 00:00:00.001' \
original_modified.jpg
```

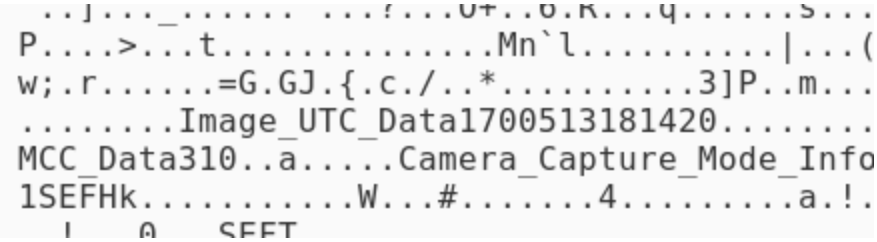
terdapat beberapa aspek yang ada pada command tersebut, antara lain

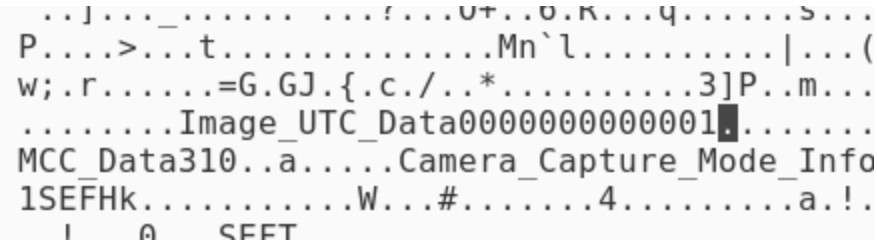
1. `-SubSecCreateDate='1970:01:01 00:00:00.001'` berarti kamu meminta `exiftool` untuk mengatur **waktu pembuatan metadata EXIF** ke epoch Unix dengan presisi satu milidetik. Field ini berpasangan dengan `CreateDate`, dan biasanya menunjukkan kapan file JPEG “dibuat” oleh kamera atau software pengolah. Dalam konteks forensik, ini sering dipakai untuk melihat apakah file pernah diproses ulang setelah pengambilan gambar.
2. `-SubSecDateTimeOriginal='1970:01:01 00:00:00.001'` menargetkan **waktu pengambilan gambar yang sebenarnya**, yaitu saat cahaya pertama kali mengenai sensor kamera. Ini adalah timestamp yang paling sering dianggap sebagai “waktu kejadian”. Dengan perintah ini, kamu memaksa `exiftool` untuk menulis ulang baik `DateTimeOriginal` maupun `SubSecTimeOriginal` agar menunjuk tepat ke 1 milidetik setelah Unix epoch.

3. `-SubSecModifyDate='1970:01:01 00:00:00.001'` mengatur **waktu modifikasi EXIF terakhir**, yang berpasangan dengan `ModifyDate`. Ini bukan waktu modifikasi filesystem, melainkan waktu modifikasi metadata di dalam file JPEG itu sendiri. Banyak orang keliru mengira keduanya sama, padahal sistem forensik membedakannya dengan jelas.

setekah memanipulasi ketiga bagian meta data tadi selanjutnya yang perlu kita lakukan adalah melakukan manipulasi pada raw data yang tertanam pada gambar dengan menggunakan hex editor, dengan ghex kita bisa memanipulasi variabel Image_UTC_Data menjadi yang kita inginkan misalnya

original file (yang akan kita ubah) menunjukan 1700513181420 (dalam milidetik)





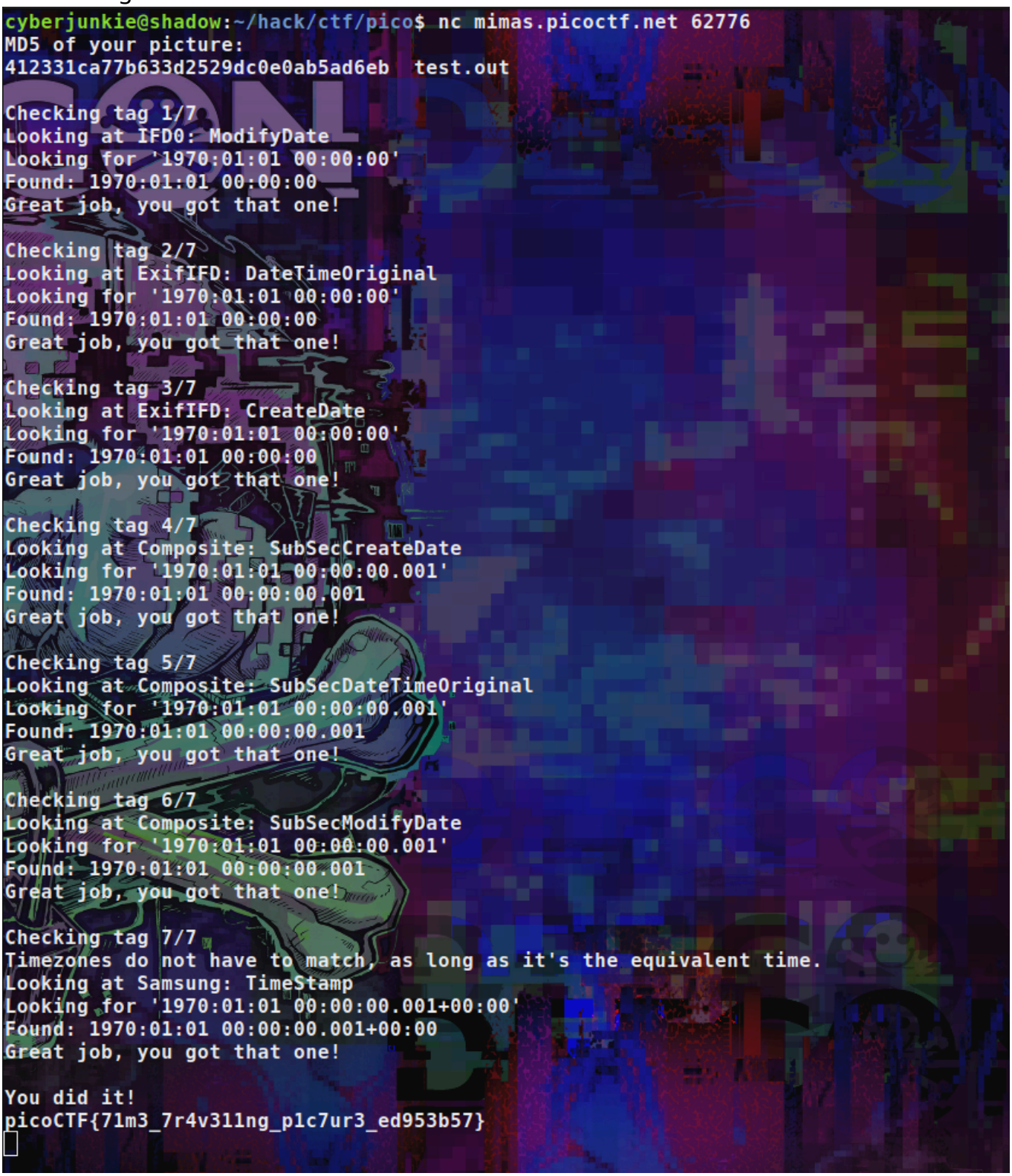
setelah di ubah maka file raw meta data akan terlihat seperti gambar di atas.
(**funfact:** *pengubahan metadata raw seperti ini bisa dilakukan dengan menggunakan hex editor*)

timestamp pada artefak digital tersebar di banyak layer (EXIF standar, sub-second, dan metadata vendor), dan semuanya harus konsisten karena satu residu waktu saja cukup untuk membongkar atau menggagalkan validasi dan kebohongan peretas.

kita akan mencoba melakukan verifikasi bahwa file dan metadatanya berhasil kita manipulasi

masukan file yang telah dimodifikasi ke server mimas, dan listen server di port 62776, server akan langsung mem-verifikasi file yang sudah kita modifikasi dan akan mendump

sebuah flag.


cyberjunkie@shadow:~/hack/ctf/pico$ nc mimas.picoctf.net 62776
MD5 of your picture:
412331ca77b633d2529dc0e0ab5ad6eb test.out
Checking tag 1/7
Looking at IFD0: ModifyDate
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!
Checking tag 2/7
Looking at ExifIFD: DateTimeOriginal
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!
Checking tag 3/7
Looking at ExifIFD: CreateDate
Looking for '1970:01:01 00:00:00'
Found: 1970:01:01 00:00:00
Great job, you got that one!
Checking tag 4/7
Looking at Composite: SubSecCreateDate
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!
Checking tag 5/7
Looking at Composite: SubSecDateTimeOriginal
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!
Checking tag 6/7
Looking at Composite: SubSecModifyDate
Looking for '1970:01:01 00:00:00.001'
Found: 1970:01:01 00:00:00.001
Great job, you got that one!
Checking tag 7/7
Timezones do not have to match, as long as it's the equivalent time.
Looking at Samsung: TimeStamp
Looking for '1970:01:01 00:00:00.001+00:00'
Found: 1970:01:01 00:00:00.001+00:00
Great job, you got that one!
You did it!
picoCTF{71m3_7r4v311ng_p1c7ur3_ed953b57}