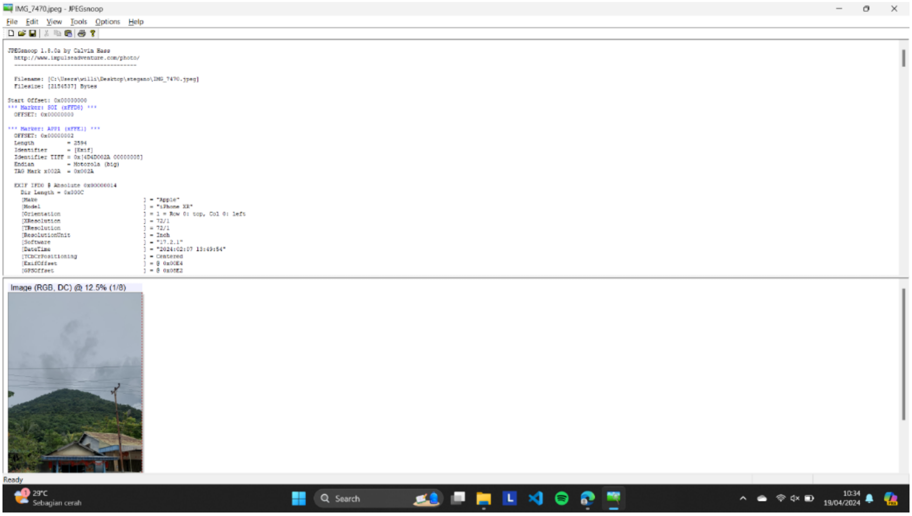
Pada Bagian photo and Video Forensics saya membantu dalam membuat dan menganlisis sebuah gambar. Gambar yang dibuat adalah gambar yang teridentifikasi sebagai file stegano dan analisisnya menggunakan JPEGsnoop dan Ghiro. Berikut beberapa dokumentasinya

JPEGSnoop:

Tampilan awal JPEGSnoop

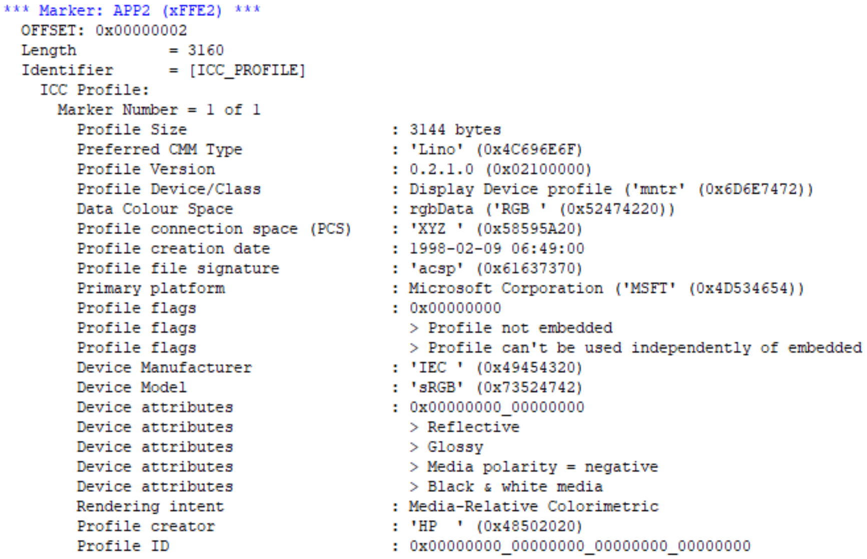

IMG_7470.jpeg - JPEGsnoop
File Edit View Tools Options Help
Image (RGB, DC) @ 12.5% (1/8)
Ready
29°C
Sebagian cerah
Search
10:34
19/04/2024

```
JPEGsnoop 1.8.0a by Calvin Hass
  http://www.impulseadventure.com/photo/
  ----------------------------------------

  Filename: [C:\Users\willi\Desktop\stegano\IMG_7470.jpeg]
  Filesize: [2154537] Bytes

Start Offset: 0x00000000
*** Marker: SOI (xFFD8) ***
  OFFSET: 0x00000000

*** Marker: APP1 (xFFE1) ***
  OFFSET: 0x00000002
  Length          = 2594
  Identifier      = [Exif]
  Identifier TIFF = 0x[4D4D002A 00000008]
  Endian          = Motorola (big)
  TAG Mark x002A  = 0x002A

  EXIF IFD0 @ Absolute 0x00000014
    Dir Length = 0x000C
    [Make                                 ] = "Apple"
    [Model                                ] = "iPhone XR"
    [Orientation                          ] = 1 = Row 0: top, Col 0: left
    [XResolution                          ] = 72/1
    [YResolution                          ] = 72/1
    [ResolutionUnit                       ] = Inch
    [Software                             ] = "17.2.1"
    [DateTime                             ] = "2024:02:07 13:49:54"
    [YCbCrPositioning                     ] = Centered
    [ExifOffset                           ] = @ 0x00E4
    [GPSOffset                            ] = @ 0x08E2
```

Tampilan informasi dari gambar

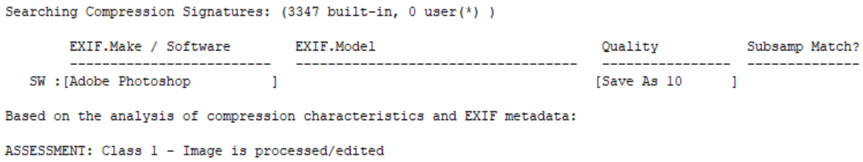
```
EXIF IFD0 @ Absolute 0x00000014
  Dir Length = 0x000C
  [Make                                 ] = "Apple"
  [Model                                ] = "iPhone XR"
  [Orientation                          ] = 1 = Row 0: top, Col 0: left
  [XResolution                          ] = 72/1
  [YResolution                          ] = 72/1
  [ResolutionUnit                       ] = Inch
  [Software                             ] = "17.2.1"
  [DateTime                             ] = "2024:02:07 13:49:54"
  [YCbCrPositioning                     ] = Centered
  [ExifOffset                           ] = @ 0x00E4
  [GPSOffset                            ] = @ 0x08E2
  Offset to Next IFD = 0x00000000
```

Informasi kamera yang didapatkan



```
*** Marker: APP2 (xFFE2) ***
  OFFSET: 0x00000002
  Length           = 3160
  Identifier       = [ICC_PROFILE]
    ICC Profile:
      Marker Number = 1 of 1
        Profile Size                        : 3144 bytes
        Preferred CMM Type                  : 'Lino' (0x4C696E6F)
        Profile Version                     : 0.2.1.0 (0x02100000)
        Profile Device/Class                : Display Device profile ('mntr' (0x6D6E7472))
        Data Colour Space                   : rgbData ('RGB ' (0x52474220))
        Profile connection space (PCS)      : 'XYZ ' (0x58595A20)
        Profile creation date               : 1998-02-09 06:49:00
        Profile file signature              : 'acsp' (0x61637370)
        Primary platform                    : Microsoft Corporation ('MSFT' (0x4D534654))
        Profile flags                       : 0x00000000
        Profile flags                         > Profile not embedded
        Profile flags                         > Profile can't be used independently of embedded
        Device Manufacturer                 : 'IEC ' (0x49454320)
        Device Model                        : 'sRGB' (0x73524742)
        Device attributes                   : 0x00000000_00000000
        Device attributes                     > Reflective
        Device attributes                     > Glossy
        Device attributes                     > Media polarity = negative
        Device attributes                     > Black & white media
        Rendering intent                    : Media-Relative Colorimetric
        Profile creator                     : 'HP  ' (0x48502020)
        Profile ID                          : 0x00000000_00000000_00000000_00000000
```

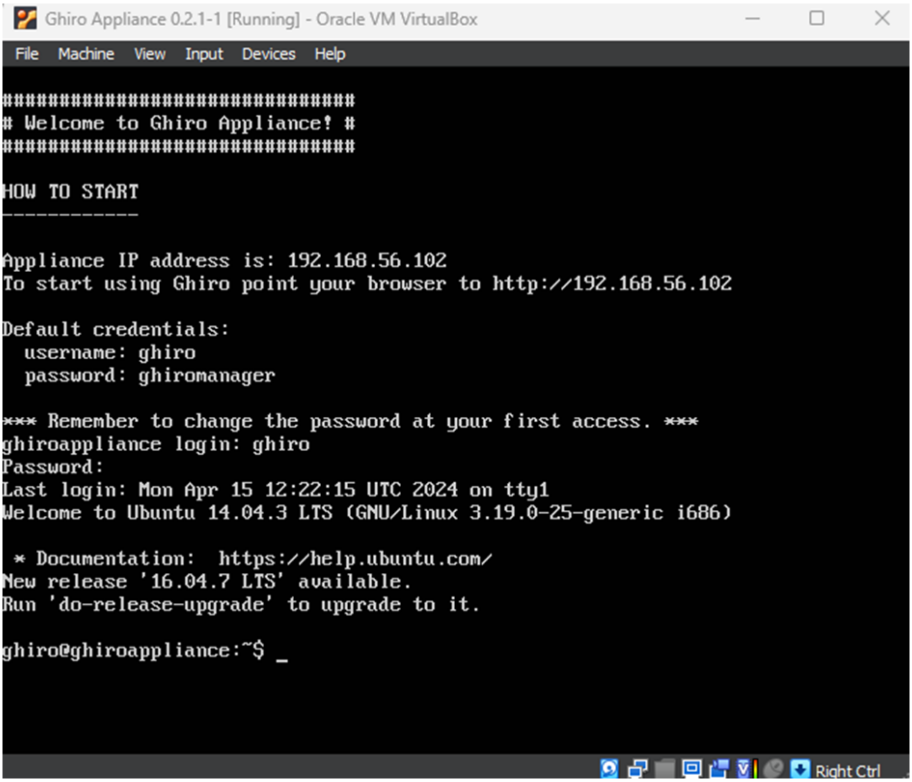
Informasi gambar



```
Searching Compression Signatures: (3347 built-in, 0 user(*) )

          EXIF.Make / Software        EXIF.Model                            Quality           Subsamp Match?
          -------------------------   -----------------------------------   ----------------  --------------
    SW :[Adobe Photoshop          ]                                        [Save As 10      ]

Based on the analysis of compression characteristics and EXIF metadata:

ASSESSMENT: Class 1 - Image is processed/edited
```

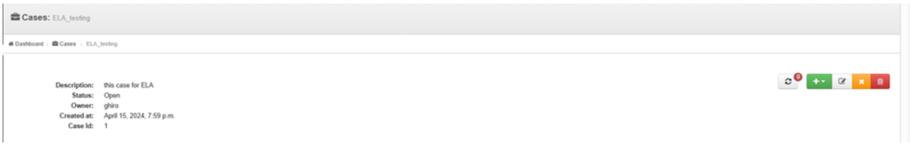
Perangkat lunak penyunting

Ghiro:



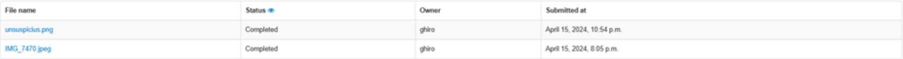
```
#################################
# Welcome to Ghiro Appliance! #
#################################

HOW TO START
------------

Appliance IP address is: 192.168.56.102
To start using Ghiro point your browser to http://192.168.56.102

Default credentials:
  username: ghiro
  password: ghiromanager

*** Remember to change the password at your first access. ***
ghiroappliance login: ghiro
Password:
Last login: Mon Apr 15 12:22:15 UTC 2024 on tty1
Welcome to Ubuntu 14.04.3 LTS (GNU/Linux 3.19.0-25-generic i686)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

ghiro@ghiroappliance:~$ _
```

Tampilan Aplikasi Ghiro saat dijalankan



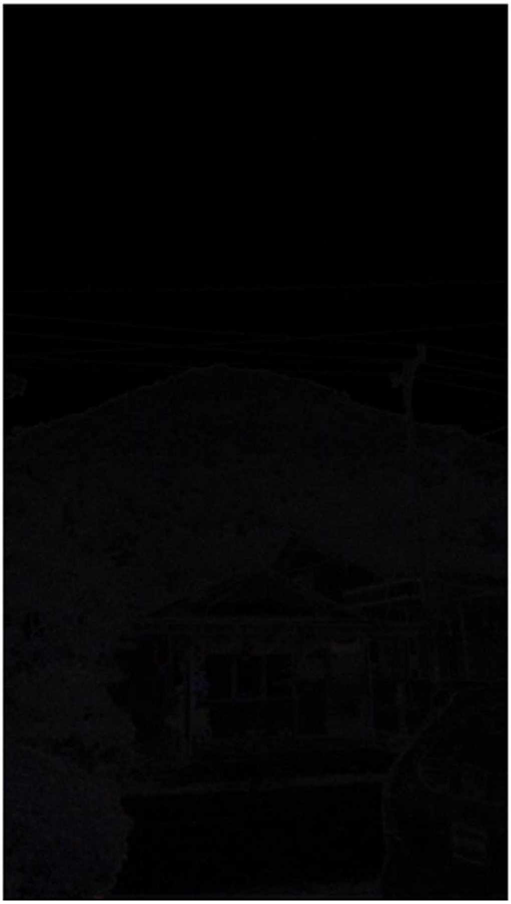
Description: this case for ELA
Status: Open
Owner: ghiro
Created at: April 15, 2024, 7:59 p.m.
Case Id: 1

Setelah membuat kasus baru pada Ghiro

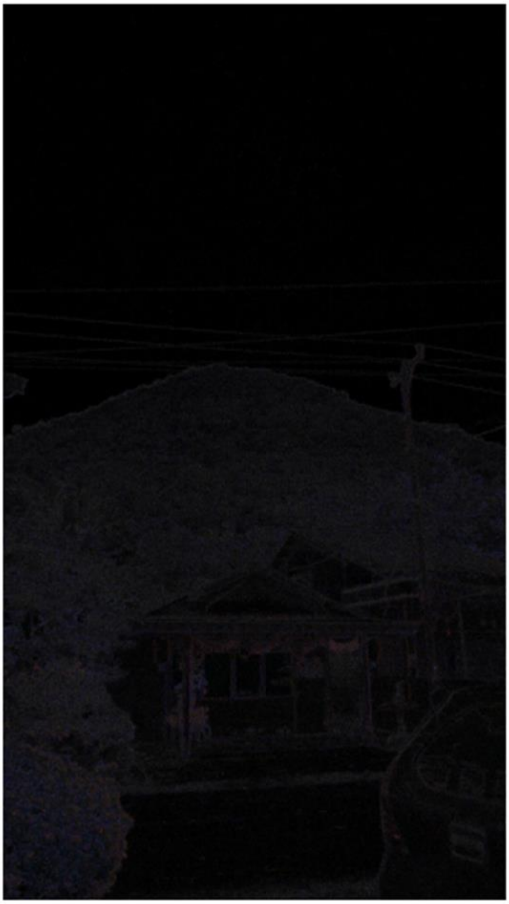


File name	Status	Owner	Submitted at
unsuspicius.png	Completed	ghiro	April 15, 2024, 10:54 p.m.
IMG_7470.jpeg	Completed	ghiro	April 15, 2024, 8:05 p.m.

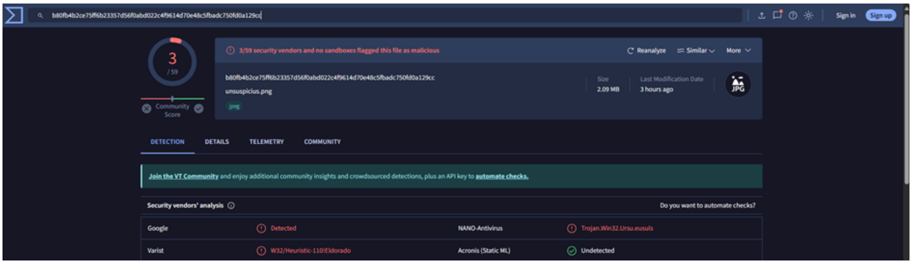
Tampilan sisipan gambar



ELA foto asli



ELA menggunakan foto hasil steganografi



3/59 security vendors and no sandboxes flagged this file as malicious

b80fb4b2ce75ff6b23357d56f0abd022c4f9614d70e48c5fbadc750fd0a129cc

unsuspicius.png

jpeg

Size 2.09 MB

Last Modification Date 3 hours ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Google	Detected	NANO-Antivirus	Trojan.Win32.Ursu.eusuls
Varist	W32/Heuristic-110!Eldorado	Acronis (Static ML)	Undetected

Hasil Virus Total