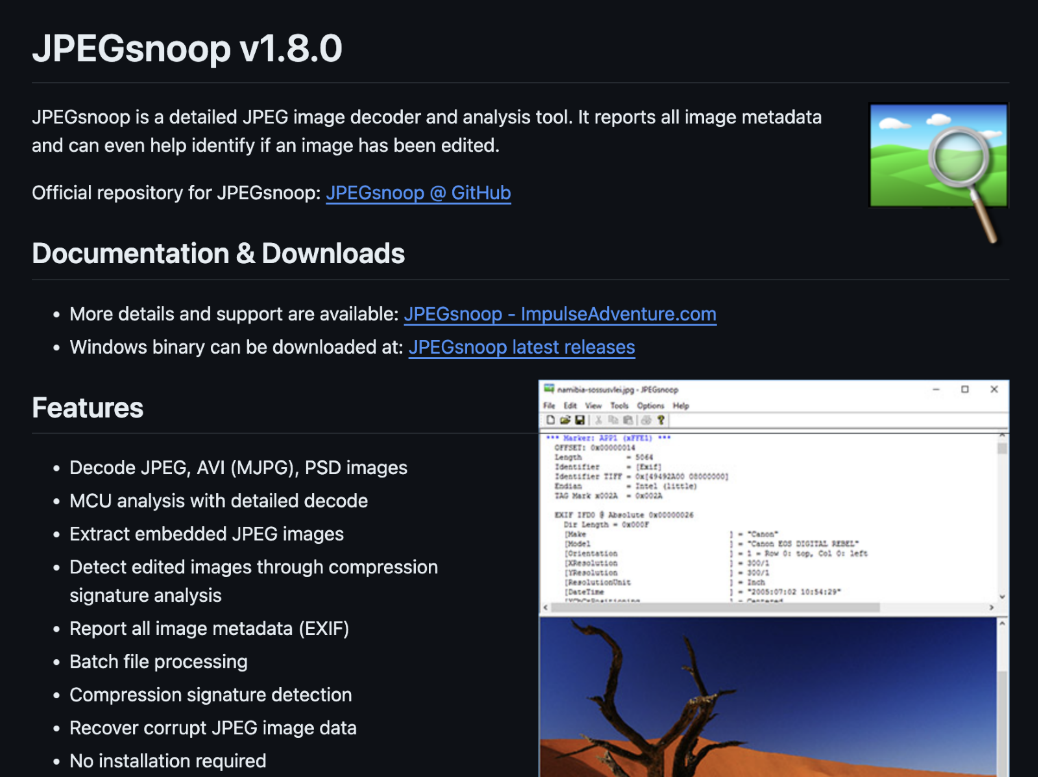
**5.3. Kasus: analisis gambar menggunakan JPEGsnoop**

JPEGsnoop adalah aplikasi alternatif yang dapat digunakan oleh ahli untuk dapat memberikan pengetahuan dalam mendeteksi keaslian dari suatu foto dan mendapatkan detail struktur dari suatu file gambar. Selain memiliki fitur deteksi manipulasi gambar, aplikasi ini juga mampua melakukan ekstraksi metadata yang tersimpan dalam suatu file dengan format JPEG seperti misalkan data Exchangeable Image File Format (EXIF). JPEGsnoop juga memiliki kemampuan untuk melakukan analisis dari algoritma kompresi yang diterapkan pada gambar, melakukan identifikasi kode spesifik dari penggunaan perangkat atau perangkat lunak penyuntingan gambar.

Gambar 5.7. JPEGSnoop

JPEGsnoop juga ditambahkan fitur untuk melakukan diagnosis serta analisis struktur untuk menemukan bagian dari file gambar yang rusak agar dapat diperbaiki atau dipulihkan kembali. Struktur internal dari file gambar juga dapat dikenali oleh perangkat lunak ini termasuk informasi mengenai tabel huffman yang digunakan dalam pengkodean entropi dalam pembentukan suatu gambar.

* File JPEGsnoop merupakan aplikasi portabel sehingga tidak perlu diinstall ke sistem Windows. Untuk aplikasi telah disediakan di lokasi direktori **\labs\bab5\tools\**
* Untuk contoh images dapat dilihat di lokasi direktori \labs\bab5\images\
* Untuk mengunduh aplikasi dari situs aslinya dapat dengan mengakses url:

<https://github.com/ImpulseAdventure/JPEGsnoop/releases/download/v1.8.0/JPEGsnoop_v1_8_0a.zip>

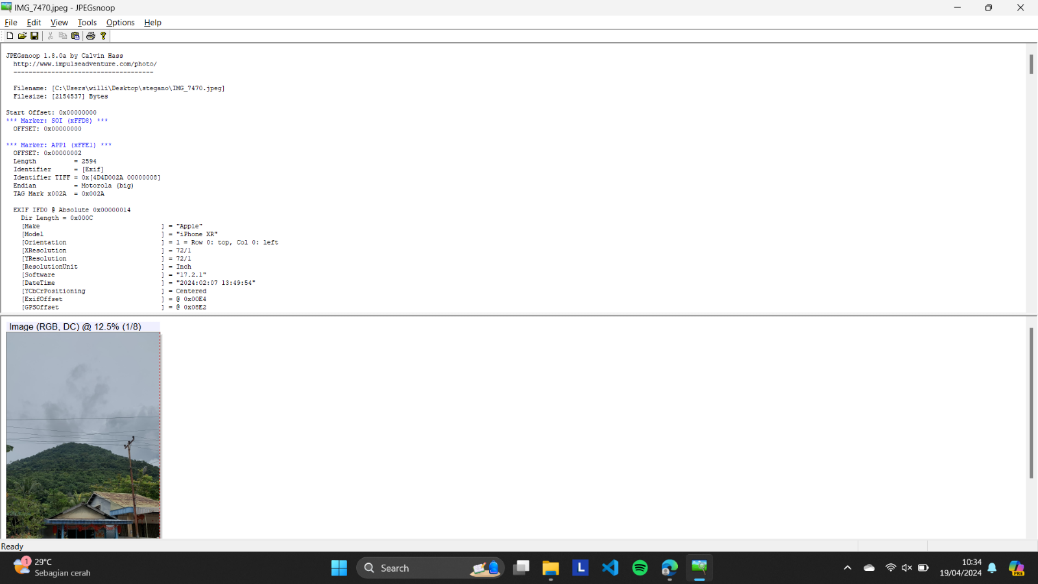
* Untuk melihat kode sumbernya dapat mengakses url:

<https://github.com/ImpulseAdventure/JPEGsnoop/archive/refs/tags/v1.8.0.zip>

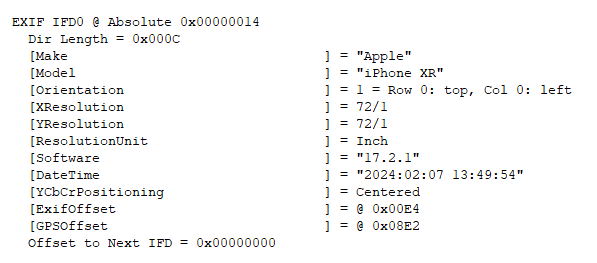
* Melihat dashboard dari alat JPEGsnoop. Dilanjutkan dengan mengakses menu untuk membuka file gambar yang sudah dipersiapkan sebelumnya, sebagai contoh dengan nama file dan ruang penyimpanan gambar sebagai berikut:

  
Gambar 5.8 Tampilan awal JPEGSnoop

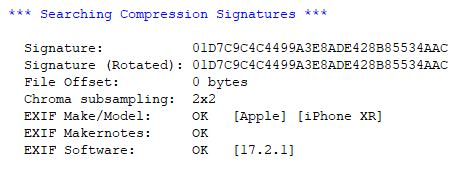
* Setelah gambar sampel dengan nama, Master.jpg berhasil dibuka, maka akan menampilkan informasi rinci metadata gambar.

Gambar 5.9 Tampilan informasi dari gambar

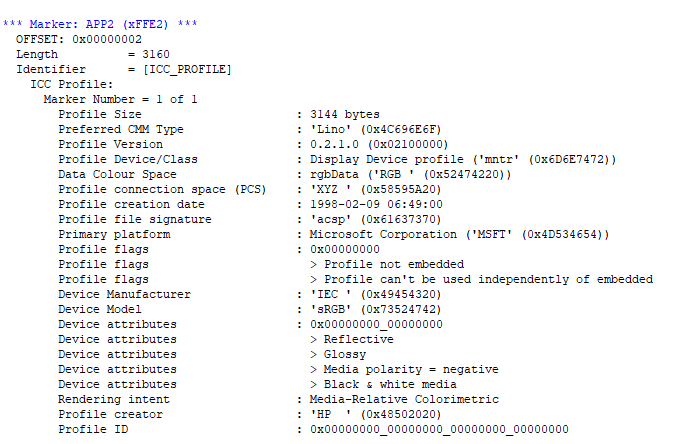
* + Contoh informasi yang dihasilkan dari alat ini adalah contoh jenis dan spesifikasi perangkat kamera yang menghasilkan gambar, perangkat lunak yang digunakan pada kamera, hingga menyertakan tanggal saat gambar tersebut dibuat.

Gambar 5.10 Informasi kamera yang didapatkan

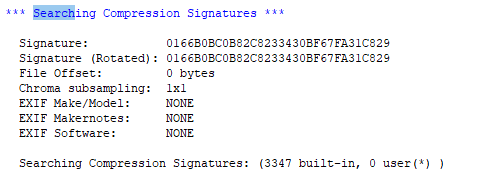
* + Contoh informasi lain yang berhasil dihapus dari file gambar adalah kompresi Signature yang digunakan oleh perangkat lunak yang disertakan dalam perangkat kamera.

  
Gambar 5.11. Informasi signature

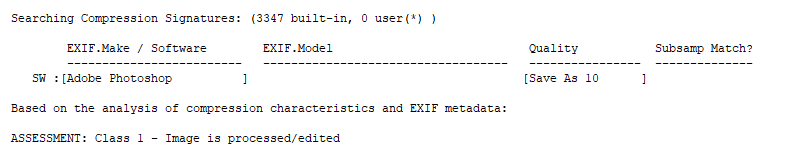
* Cobalah melakukan transmisi informasi dari gambar yang sudah berubah. Apakah alat JPEGsnoop memberikan hasil laporan yang sama? Nama dan jalur direktori dari contoh gambar yang telah dimodifikasi sebagai berikut: \labs\bab5\images\master2.JPG.

Gambar 5.12. Informasi gambar

Informasi yang diperoleh dari alat ini mengindikasikan bahwa gambar modifikasi ini tidak lagi menyimpan informasi spesifikasi perangkat kamera yang digunakan. Karena sudah diubah dengan menggunakan perangkat lunak khusus yang digunakan dalam penyuntingan gambar.

Gambar 5.13. Compression Signatures

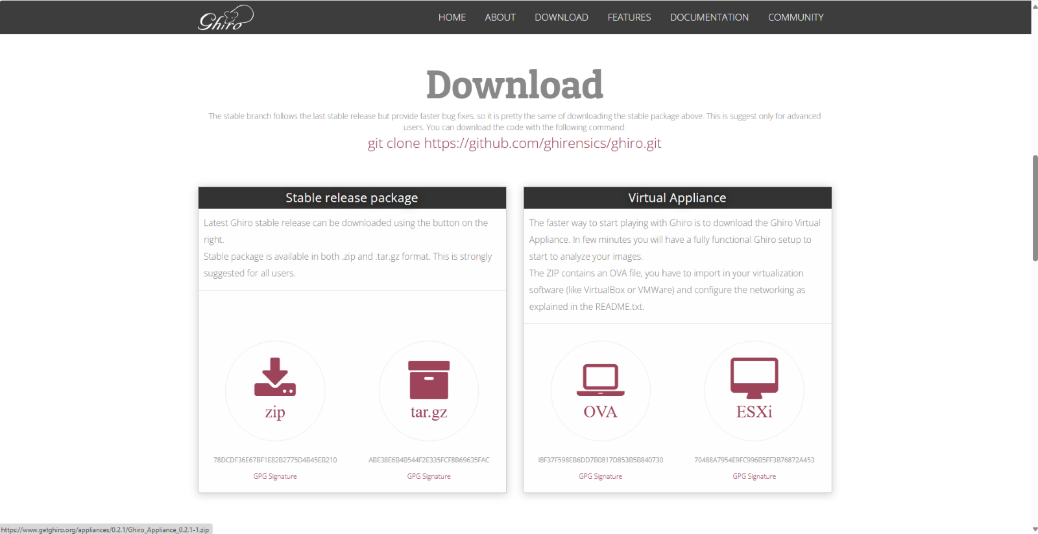
informasi detail mengenai nama perangkat lunak penyuntingan gambar yang dapat digunakan dalam melakukan modifikasi dan disimpulkan dari alat tersebut yang menyebutkan bahwa gambar adalah hasil modifikasi.

Gambar 5.14. Perangkat lunak penyunting

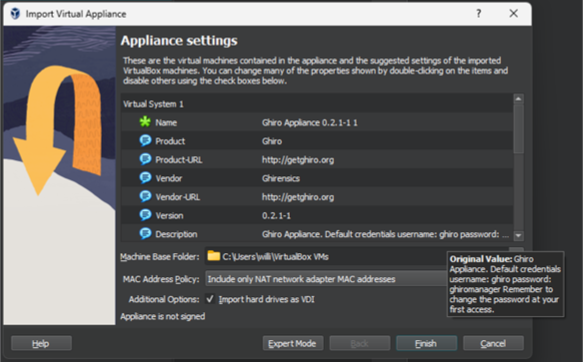
5.4 Kasus: analisis menggunakan Ghiro

Pada kasus kali ini, ahli sudah memiliki dua foto digital yang akan dianalisis menggunakan aplikasi Ghiro yang telah terpasang di mesin virtual.

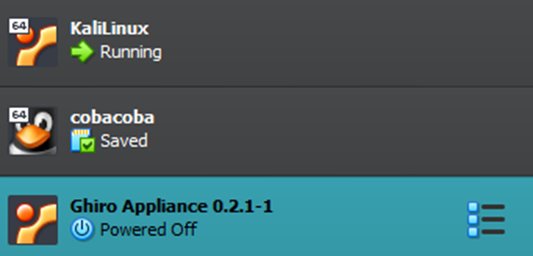
Download master file dengan ekstensi OVA di: <https://www.getghiro.org/>

Gambar 5.15. Situs Ghiro

Lakukan proses ekstraksi file master dan lanjutkan dengan memasukkan file berektensi .OVA menggunakan perangkat lunak virtualisasi seperti virtual box dengan memilih menu Import Virtual Appliance dari aplikasi.

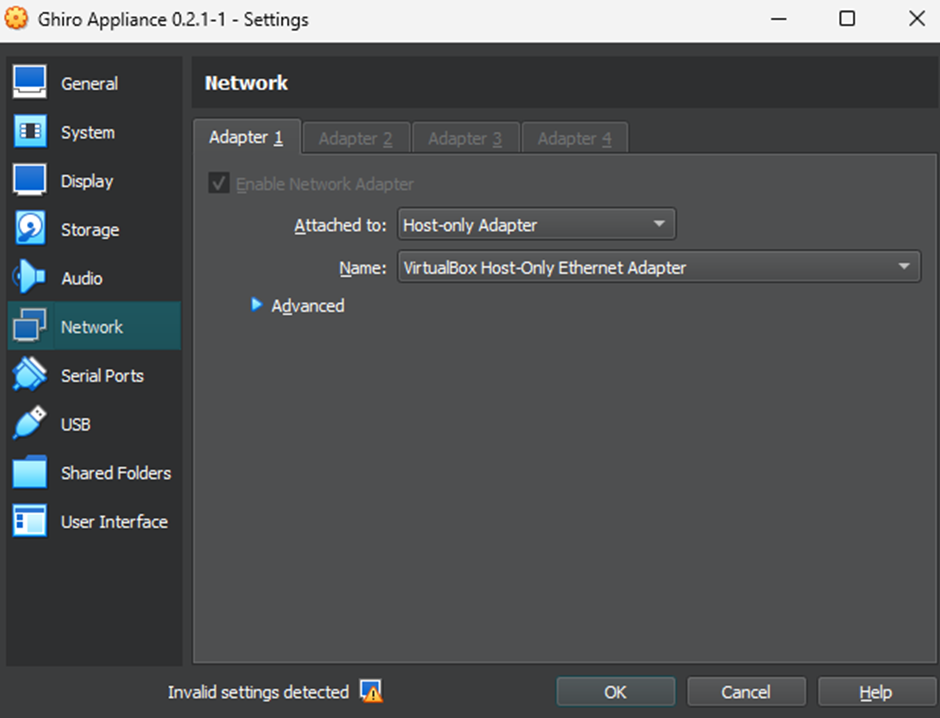
.

Gambar 5.16. Instalasi Ghiro pada Kali Linux

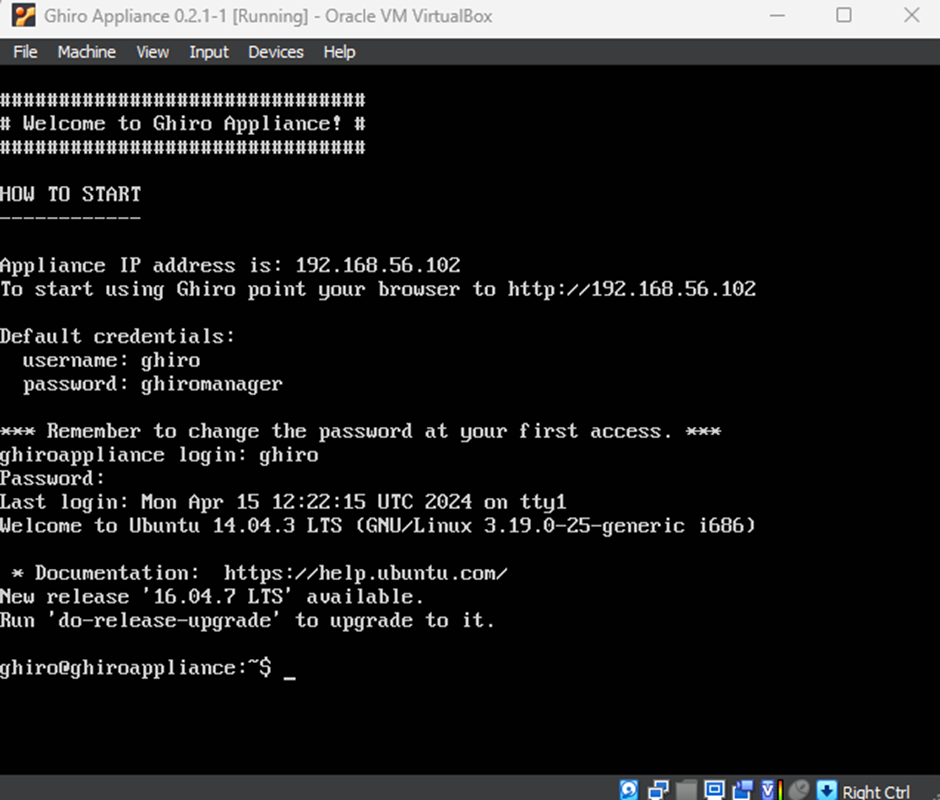


Gambar 5.17. Virtual Machine Ghiro

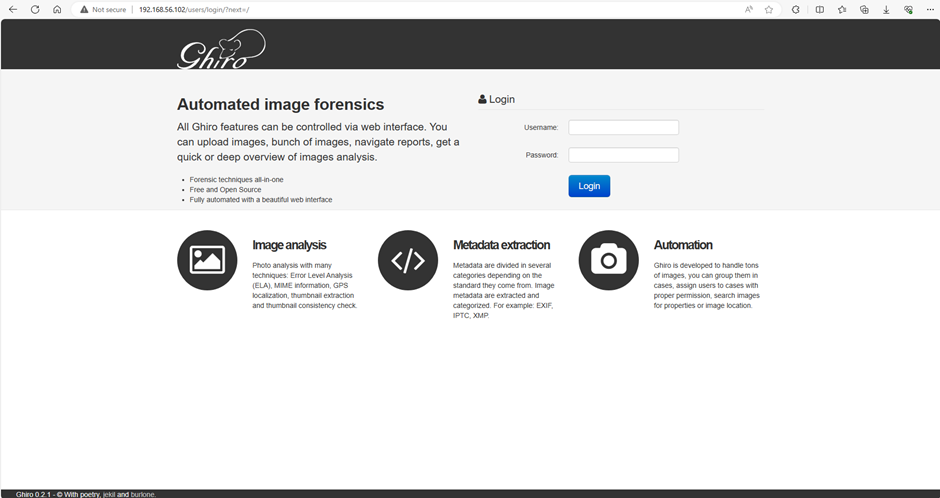
* Setelah itu masuk ke setting dan ubah network ke “host-only adapter”

Gambar 5.18. Pengaturan jaringan mesin virtual

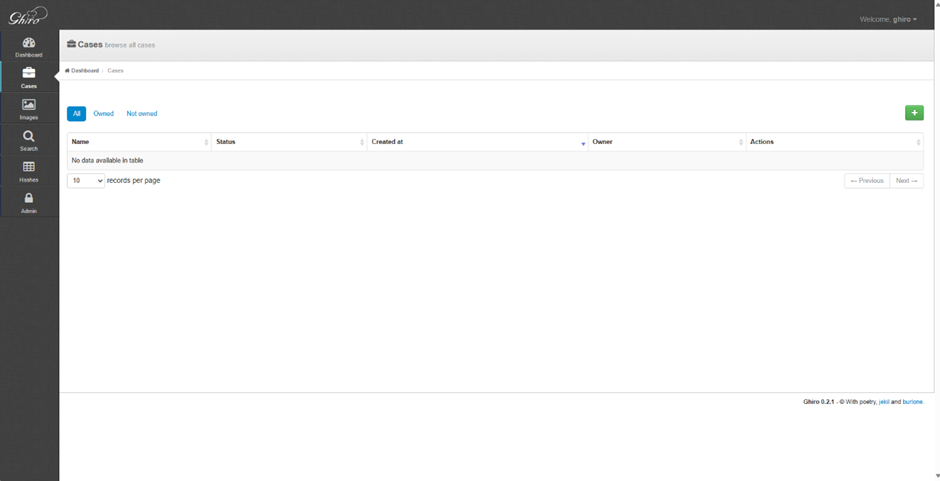
* Jalankan Ghiro dan login dengan username ghiro dan password ghiromanager

Gambar 5.19. Tampilan Aplikasi Ghiro saat dijalankan

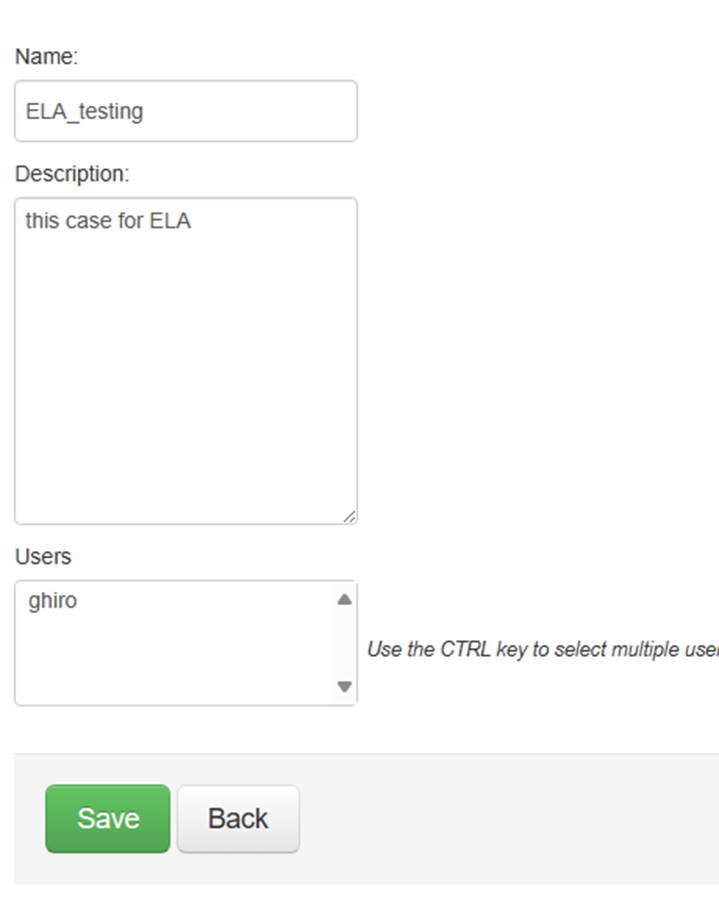
* Selanjutnya, ahli dapat berpindah ke browser dan mengakses antarmuka berbasis web melalui IP yang telah diberikan sebelumnya ketika aplikasi mulai dijalankan.

Gambar 5.20. Situs Ghiro

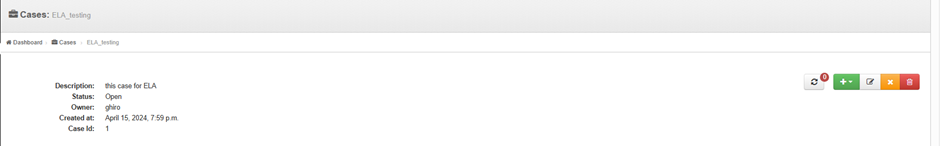
* Login dengan informasi username ghiro dan password ghiromanager.

Gambar 5.21. Tampilan Ghiro setelah login

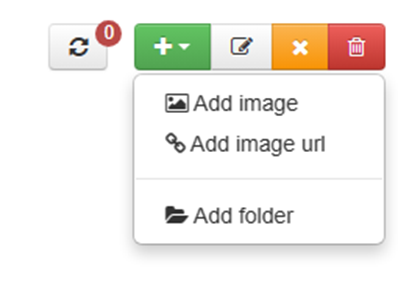
* Masuk ke tab case, dan buatlah case baru (nama dan deskripsi ditentukan oleh ahli). Lalu tekan save.



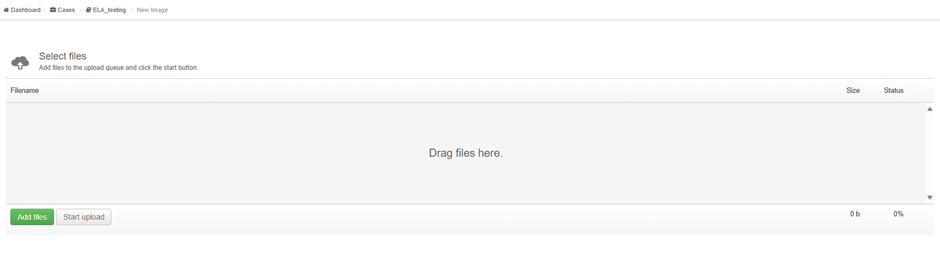
Gambar 5.22. Kasus baru pada Ghiro

Gambar 5.23. Setelah membuat kasus baru pada Ghiro

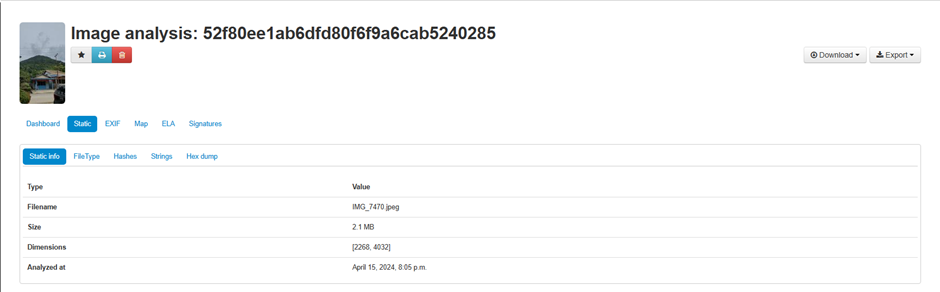
* Setelah itu, masukkan file images seperti pada gambar dibawah ini. File contoh yang akan dianalis terdapat di lokasi direktori \labs\bab5\images\

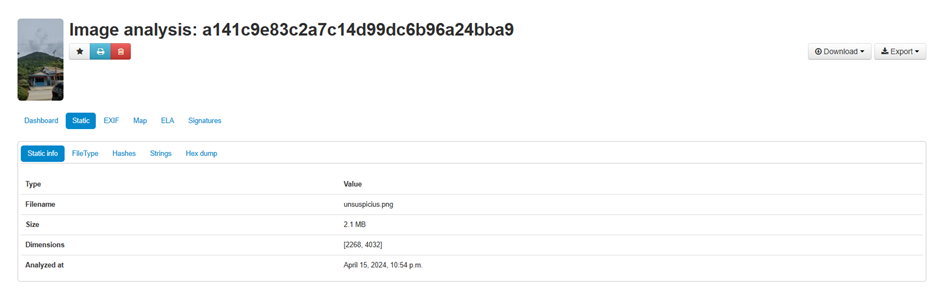


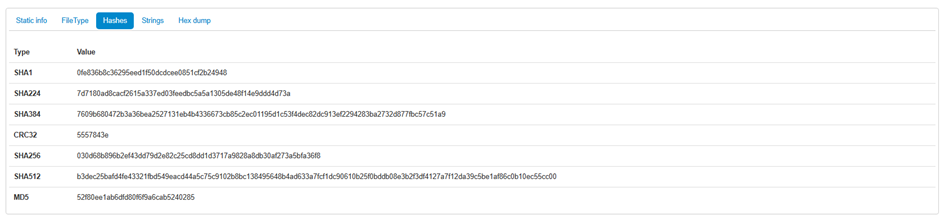
Gambar 5.24. Tambah file image

Gambar 5.25. Tampilan sisipan gambar

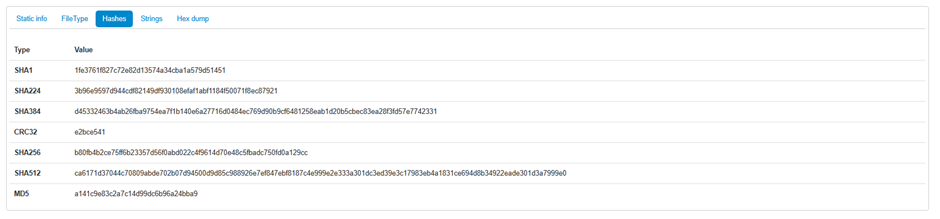
* Selanjutnya, ahli akan mulai menganalisis kedua gambar tersebut. Dapat dilihat sekilas kedua gambar tersebut adalah sama. Namun ketika ahli memasukannya ke dalam aplikasi ghiro, terdapat beberapa perbedaan signifikan misalnya pada informasi ekstensi, nilai hash dan hasil analisis ELA.
  + Static Info

Gambar 5.26. Foto asli

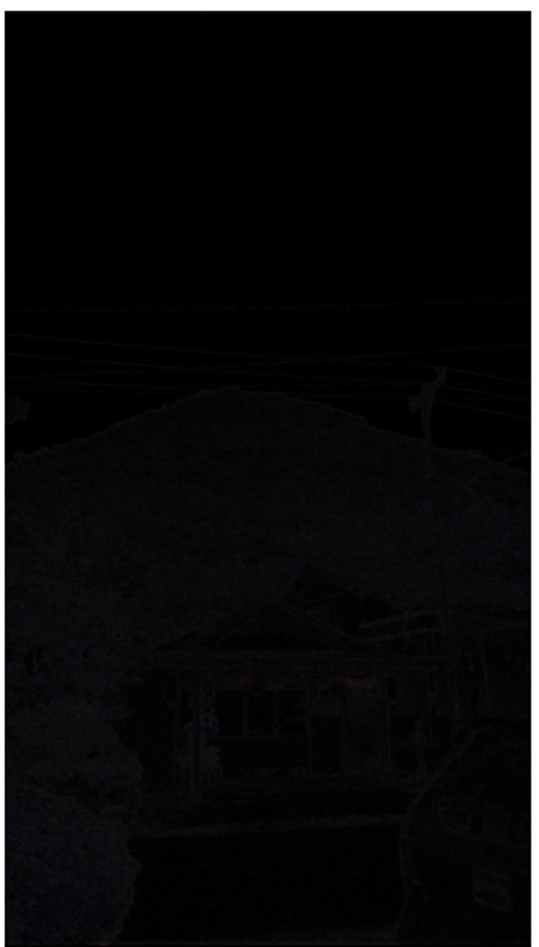
Gambar 5.27. Foto hasil steganografi

Gambar 5.28. Nilai hash dari foto asli

* + - Unsuspicius.png

Gambar 5.29. Nilai hash dari foto hasil steganografi

* + ELA
    - IMG\_7470.jpeg



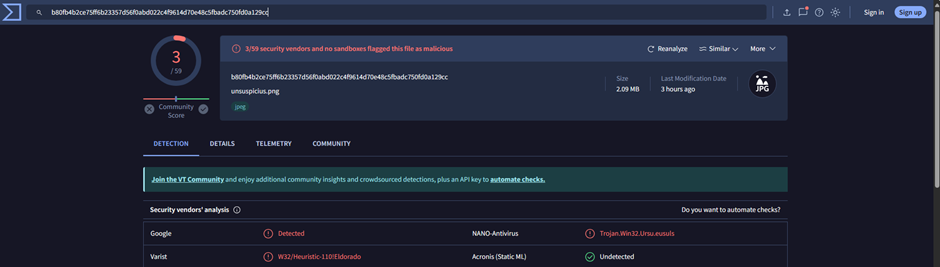
Gambar 5.30. ELA foto asli

* + - Unsuspicius.png



Gambar 5.31. ELA menggunakan foto hasil steganografi

* Ketika ahli mengetahui adanya perbedaan, ahli mencoba untuk memasukan hash value (SHA256) dari gambar Unsuspicius.png ke dalam situs virustotal. Dari hasil analisis aplikasi terlihat bahwa foto unsuspicius.png ternyata termasuk dalam kriteria malware.

Gambar 5.32. Hasil Virus Total