

Plain Sight

Challenge

Challenge

1273 Solves



Hidden in Plain Sight

75

Analysts recovered a suspicious image from a threat actor's social media account. At first glance, it looks like an innocent selfie - but insider reports suggest that a flag might be hiding in the image metadata. Can you extract it?

View Hint



selfie.png

Flag

Submit

Workflow

1. Downloaded the image and reviewed the challenge description for hints.

2. Used `exiftool` to extract detailed metadata from the PNG image.
3. Located the flag within the metadata under the "Image Source" field.

Flag:

C1{smile_youre_flagged}

```
Actions Digital Source Type : http://cv.iptc.org/newscodes/digitalsourcetype/trainedAlgorithmicMedia
Exclusions Start : 33
Exclusions Length : 14149
Name : jumbf manifest
Alg : sha256
Hash : (Binary data 32 bytes, use -b option to extract)
Pad : (Binary data 8 bytes, use -b option to extract)
Instance ID : xmp:iid:4ab9f752-5816-4a57-bd02-22f6dde290f3
Claim Generator Info Name : ChatGPT
Claim Generator Info Org Cai C2 Pa Rs: 0.51.1
Signature : self#jumbf=/c2pa/urn:c2pa:a85273ea-e1fd-4098-b3a8-4439a2f3d746/c2pa.signature
Created Assertions Url : self#jumbf=c2pa.assertions/c2pa.actions.v2, self#jumbf=c2pa.assertions/c2pa.hash.data
Created Assertions Hash : (Binary data 32 bytes, use -b option to extract), (Binary data 32 bytes, use -b option to extract)
Title : image.png
Item 0 : (Binary data 1985 bytes, use -b option to extract)
Item 1 Pad : (Binary data 10932 bytes, use -b option to extract)
Item 2 : null
Item 3 : (Binary data 64 bytes, use -b option to extract)
C2PA Thumbnail Ingredient Jpeg Type: image/jpeg
C2PA Thumbnail Ingredient Jpeg Data: (Binary data 32785 bytes, use -b option to extract)
Relationship : componentOf
Format : png
Validation Results Active Manifest Success Code: claimSignature.insideValidity, claimSignature.validated, assertion.hashedURI.match, assertion.hashedURI.match, assertion.dataHash.match
Validation Results Active Manifest Success Url: self#jumbf=/c2pa/urn:c2pa:a85273ea-e1fd-4098-b3a8-4439a2f3d746/c2pa.signature, self#jumbf=/c2pa/urn:c2pa:a85273ea-e1fd-4098-b3a8-4439a2f3d746/c2pa.signature, self#jumbf=/c2pa/urn:c2pa:a85273ea-e1fd-4098-b3a8-4439a2f3d746/c2pa.assertions/c2pa.actions.v2, self#jumbf=/c2pa/urn:c2pa:a85273ea-e1fd-4098-b3a8-4439a2f3d746/c2pa.assertions/c2pa.hash.data, self#jumbf=/c2pa/urn:c2pa:a85273ea-e1fd-4098-b3a8-4439a2f3d746/c2pa.assertions/c2pa.hash.data
Validation Results Active Manifest Success Explanation: claim signature valid, claim signature valid, hashed uri matched: self#jumbf=c2pa.assertions/c2pa.actions.v2, hashed uri matched: self#jumbf=c2pa.assertions/c2pa.hash.data, data hash valid
Active Manifest Url : self#jumbf=/c2pa/urn:c2pa:a85273ea-e1fd-4098-b3a8-4439a2f3d746
Active Manifest Alg : sha256
Active Manifest Hash : (Binary data 32 bytes, use -b option to extract)
Claim Signature Url : self#jumbf=/c2pa/urn:c2pa:a85273ea-e1fd-4098-b3a8-4439a2f3d746/c2pa.signature
Claim Signature Alg : sha256
Claim Signature Hash : (Binary data 32 bytes, use -b option to extract)
Thumbnail URL : self#jumbf=c2pa.assertions/c2pa.thumbnail.ingredient.jpeg
Thumbnail Hash : (Binary data 32 bytes, use -b option to extract)
Comment : C1{smile_youre_flagged}
Image Size : 1024x1536
Megapixels : 1.6
```