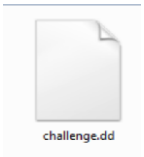
Análise Forense Digital e a Inteligência de Ameaças Cibernéticas

MÓDULO 3 | Forense em dispositivos móveis

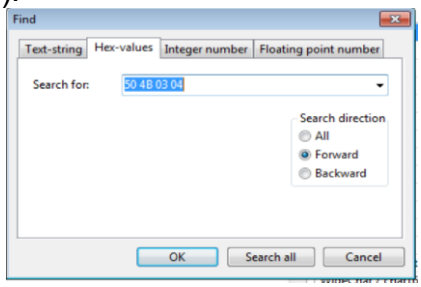
NOME: Gonçalo João Santos Silva
N.º DE ESTUDANTE: 2000499
DATA DE ENTREGA: 05/10/2025

Pergunta 1 – Realizar a extração de um ficheiro comprimido (ZIP) da imagem *challenge.dd*, documentando todos os passos e apresentando o *hash* MD5 do ficheiro extraído. (5 valores)

1- Abrir o ficheiro challenge.dd no HxD.



2- Usar Pesquisar → Procurar → Valores Hexadecimais e colocar 50 4B 03 04 (assinatura de ZIP).



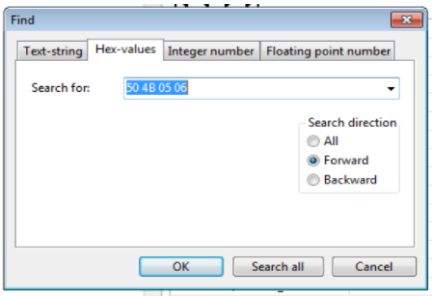
O primeiro 50 4B 03 04 encontrado corresponde ao início do ficheiro ZIP.

3- Quando encontrar, anotar o offset inicial.

```
03000000  50 4B 03 04  0A 00 00 00 00 00 84 60 75 5A 10 17  PK..........„`uZ..
```

Offset inicial encontrado: 3000000.

4- Após localizar a assinatura EOCD do ZIP (50 4B 05 06), verifiquei no próprio registo os 2 bytes “ZIP file comment length” que neste caso são 12 00 = 0x0012 = 18 bytes. Como o EOCD tem 22 bytes fixos + n bytes de comentário, o fim do ficheiro está em End = Start_EOCD + (22 + 18) − 1 = 0x3003B1E.

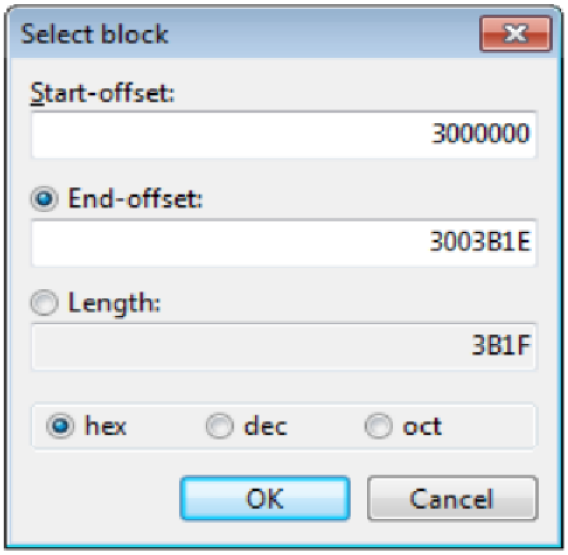


5- Anotar o offset final.

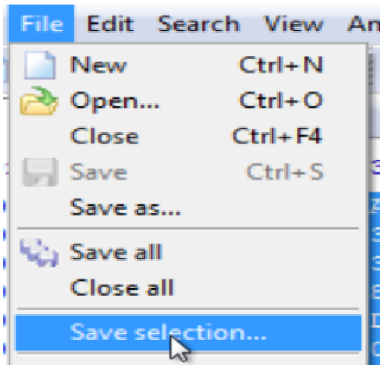
```
03003B00  00 00 00 00 00 00 00 00 00 50 4B 05 06 00 00 00
03003B10  00 01 00 01 00 5B 00 00 00 AE 3A 00 00 00 00 00
```

Offset final encontrado: 3003B1E.

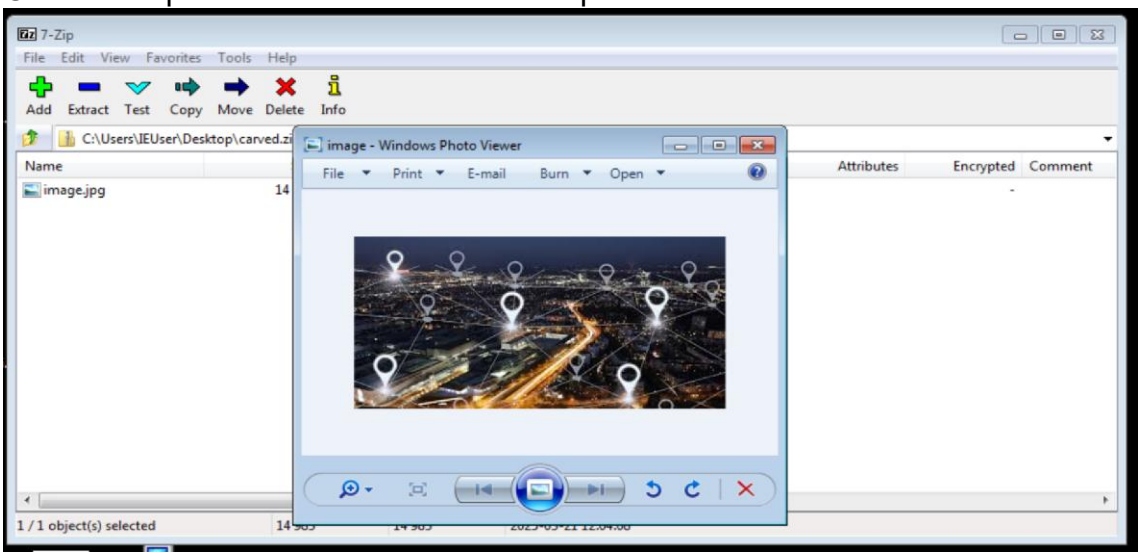
6- Selecionar todo o bloco entre estes offsets → Editar → Selecionar Bloco



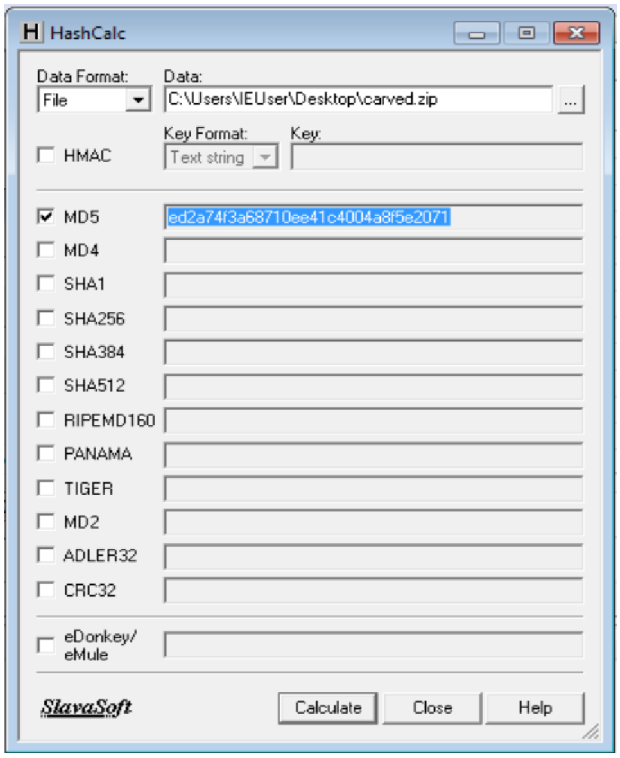
7- Guardar a seleção com Arquivo → Salvar seleção como… → carved.zip.



8- Confirmar que o ficheiro abre com o 7-zip.



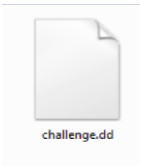
9- Calcular o hash MD5 do ficheiro extraído:



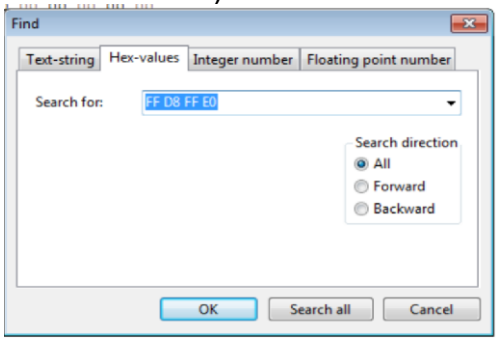
R: Hash obtido: ed2a74f3a68710ee41c4004a8f5e2071

Pergunta 2 - Extrair uma imagem JPEG da imagem *challenge.dd*, documentar o processo, calcular o *hash* MD5 e apresentar evidências adicionais, como metadados e localização GPS. (5 valores)

1- Abrir o ficheiro challenge.dd no HxD.



2- Usar Pesquisar → Procurar → Valores Hexadecimais e colocar FF D8 FF E0 (Assinatura de início de JPEG).



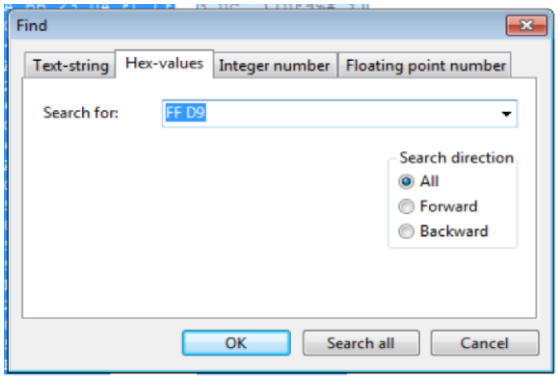
O primeiro FF D8 FF E0 encontrado corresponde ao início da assinatura de início de JPEG.

3- Quando encontrar, anotar o offset inicial.

```
03000020  61 67 65 2E 6A 70 67 FF D8 FF E0 00 10 4A 46 49  age.jpgÿØÿà..JFI
```

Offset inicial encontrado: 3000027

4- Continuar a procurar até encontrar FF D9 (fim do diretório central de um JPEG).

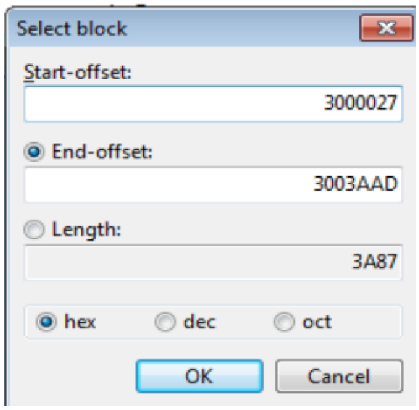


5- Anotar o offset final.

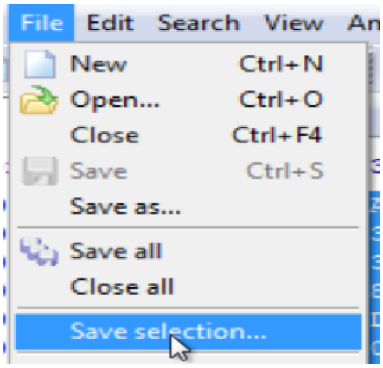
```
03003AA0  1C 40 AC BD 46 2D 45 72 66 E7 2E 19 FF D9 50 4B  .@¬½F-Erfç..ÿÙPK
```

Offset final encontrado: 3003AAD

6- Selecionar todo o bloco entre estes offsets → Editar → Selecionar Bloco

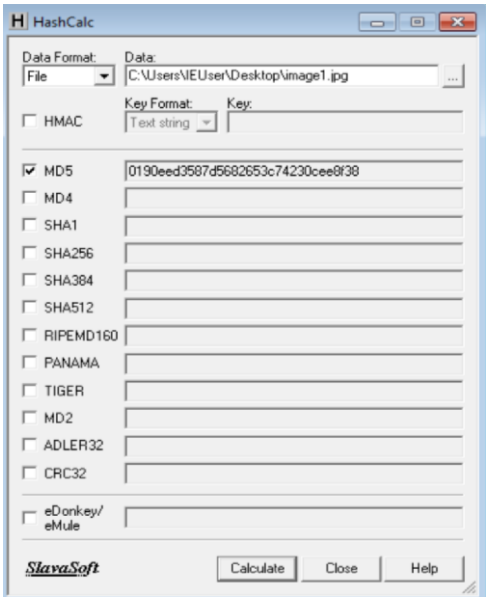


7- Guardar a seleção com Arquivo → Salvar seleção como… → image1.jpg



8- Abrir image1.jpg num visualizador de imagens

9- Calcular o hash MD5 do ficheiro extraído:



R: Hash obtido:0190eed3587d5682653c74230cee8f38

Extração de metadados

Copiei exiftool.exe para o Ambiente de Trabalho, na mesma pasta onde está a imagem image1.jpg:

Abri o CMD e naveguei até ao Desktop:

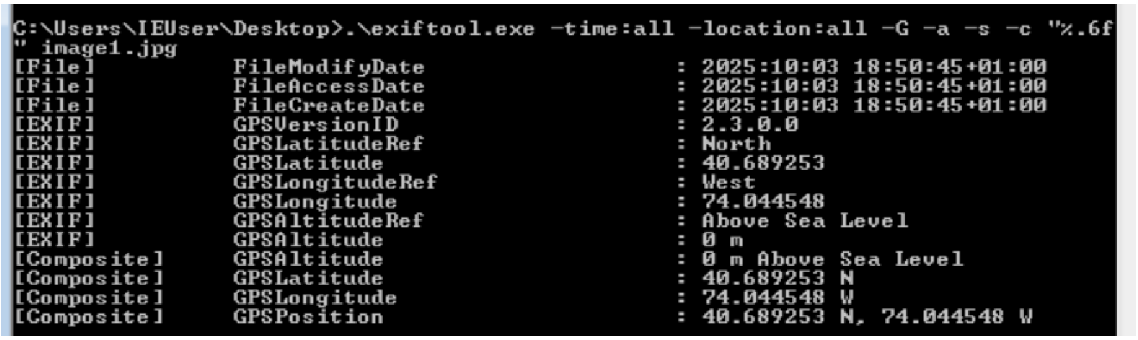
```
C:\Users\IEUser>cd %USERPROFILE%\Desktop
```

Executei o ExifTool com parâmetros para recolher todos os campos de tempo e localização, mostrando o grupo da tag, sem duplicados, e com coordenadas GPS em graus decimais.

```
C:\Users\IEUser\Desktop>.\exiftool.exe -time:all -location:all -G -a -s -c "%.6f
" image1.jpg
```

Registei os campos relevantes da saída:

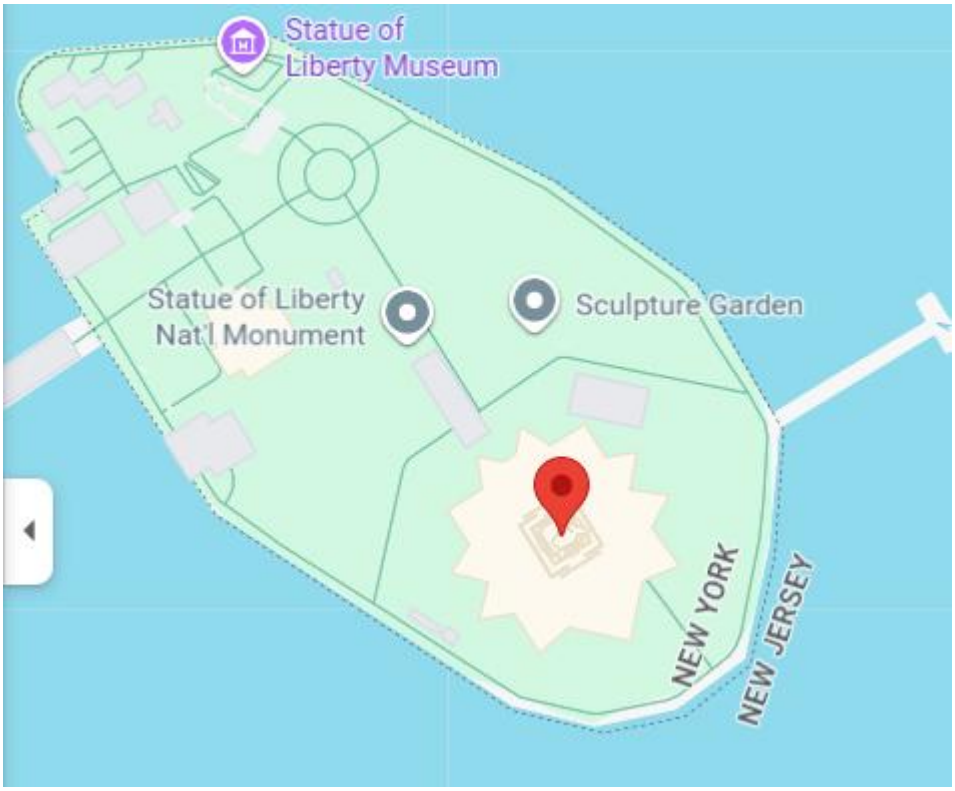
- CreateDate / DateTimeOriginal (timestamp da captura)
- Make / Model (dispositivo/câmara)
- GPSLatitude / GPSLongitude / GPSAltitude
- GPSPosition (resumo das coordenadas)



Resultados

- [File] FileModifyDate : **2025:10:03 18:50:45+01:00**
- [File] FileAccessDate : **2025:10:03 18:50:45+01:00**
- [File] FileCreateDate : **2025:10:03 18:50:45+01:00**
- [EXIF] GPSVersionID : **2.3.0**
- [EXIF] GPSLatitudeRef : **North**
- [EXIF] GPSLatitude : **40.689253**
- [EXIF] GPSLongitudeRef : **West**
- [EXIF] GPSLongitude : **74.044548**
- [EXIF] GPSAltitudeRef : **Above Sea Level**
- [EXIF] GPSAltitude : **0 m**
- [Composite] GPSLatitude : **40.689253 N**
- [Composite] GPSLongitude : **74.044548 W**
- [Composite] GPSAltitude : **0 m Above Sea Level**
- [Composite] GPSPosition : **40.689253 N, 74.044548 W**

As coordenadas GPS apontam para Estátua da Liberdade.



Pergunta 3 - Extrair uma imagem JPEG da imagem *challenge2.dd*, documentando os passos realizados, calcular o *hash* MD5 e apresentar o resultado da tentativa de visualização. (5 valores)

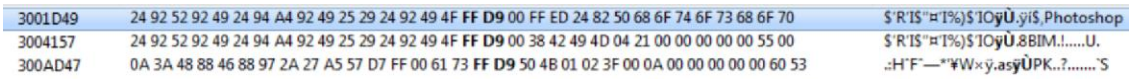
1- Abrir o ficheiro challenge2.dd no HxD.

2- Usar Pesquisar → Procurar → Valores Hexadecimais e colocar FF D8 FF (Assinatura de início de JPEG).

3- Quando encontrar, anotar o offset inicial.

4- Continuar a procurar até encontrar FF D9 (fim do diretório central de um JPEG).

5- Anotar o offset final.



6- Selecionar todo o bloco entre estes offsets → Editar → Selecionar Bloco

7- Guardar a seleção com Arquivo → Salvar seleção como… → image.jpg

Neste caso encontrei 3 JPEG (Procedimento igual para cada um deles)

JPEG #1

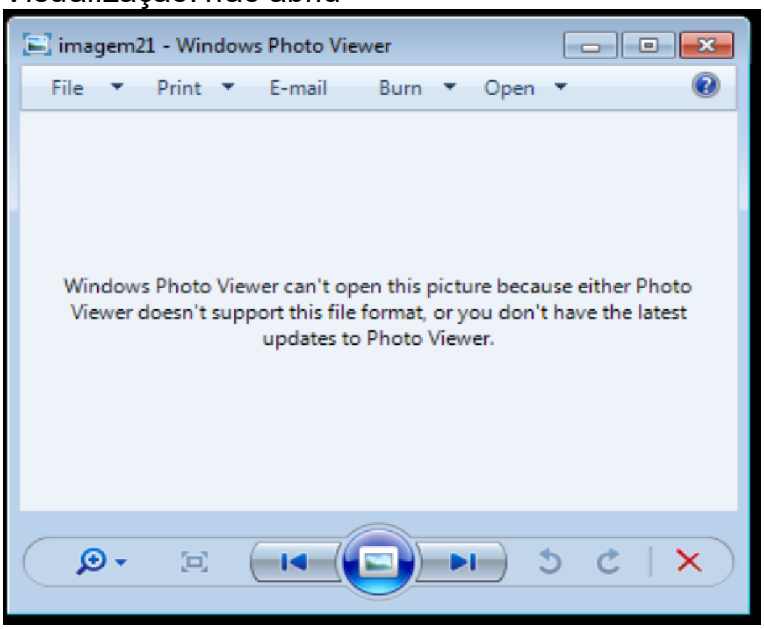
1. SOI localizado por pesquisa a FF D8 em 0x3000028.
2. EOI observado na linha iniciada em 0x3001D49 (sequência FF D9)

3. Seleção do bloco
    - Start-offset: 3000028
    - End-offset: 3001D4A

4. Exportado como imagem21.jpg.

5. MD5: 6f91f6e6197d8e5595f16af91795f1d6

6. Visualização: não abriu



JPEG #2

1. SOI em 0x30001FE.
2. EOI observado na linha iniciada em 0x3004157 (sequência FF D9)

3. Seleção do bloco
    - Start-offset: 30001FE
    - End-offset: 3004158

4. Exportado como imagem22.jpg.

5. MD5: 0431b49af2c76597410e481baba20e31

6. Visualização: abriu

JPEG #3

1. SOI em 0x300260C.

2. EOI observado na linha iniciada em 0x300AD47 (sequência FF D9)

3. Seleção do bloco
   - Start-offset: 300260C
   - End-offset: 300AD48

4. Exportado como imagem23.jpg.

5. MD5: e8be7c8a39f6e1a298c9318887fd7f1e

6. Visualização: abriu

Pergunta 4 - Extrair a miniatura (thumbnail) contida numa das imagens JPEG da imagem *challenge2.dd*, demonstrando os passos, calculando o *hash* MD5 e apresentando o resultado da visualização. (5 valores)

Para resolver este exercício fui por tentativas.

Tentativa A — ExifTool (falhou)

1. Ir para o Desktop no CMD

   cd %USERPROFILE%\Desktop

2. Procurar se existe uma *thumbnail* (ou pré-visualização) no EXIF

   exiftool.exe -a -G1 -s imagem21.jpg | findstr /i "Thumbnail Preview JpgFromRaw"

- exiftool.exe: utilitário para ler metadados EXIF.
- -a (*allow duplicates*): mostra tags mesmo que apareçam em grupos diferentes.
- -G1: mostra o grupo de cada tag a nível "G1" (ex.: IFD0, IFD1, Composite).
- -s (*short*): saída compacta (nome curto da tag = valor).
- imagem21.jpg: o ficheiro a analisar.
- | findstr /i …: filtra a saída do ExifTool para linhas que contenham, sem diferenciar maiúsc/minúsc (/i), uma destas palavras-chave:
- Thumbnail → tag típica ThumbnailImage (a miniatura EXIF na IFD1)
- Preview → PreviewImage (algumas câmaras usam esta)
- JpgFromRaw → JpgFromRaw (pré-visualização vinda de RAW)

3. Tentar extrair a miniatura

   exiftool.exe -b -ThumbnailImage imagem21.jpg > thumb_imagem21.jpg

- -b (*binary*): em vez de texto, devolve os bytes brutos da tag pedida.
- -ThumbnailImage: pede exatamente o conteúdo binário da tag ThumbnailImage.
- > thumb_imagem21.jpg: redireciona a saída binária para um novo ficheiro no disco.

O ExifTool não conseguiu devolver a miniatura

Motivo: Este JPEG não contém segmento APP1/EXIF (FF E1) com a estrutura TIFF/IFD1, onde normalmente estão as tags JPEGInterchangeFormat (0x0201) e JPEGInterchangeFormatLength (0x0202) que apontam para a thumbnail. Sem APP1/EXIF (ou com EXIF corrompido), não existe ThumbnailImage para o ExifTool extrair.

Tentativa B — Extração manual (funcionou)

Mesmo quando não há EXIF válido, a miniatura pode estar presente como um fluxo JPEG autónomo dentro do ficheiro (com os seus próprios marcadores SOI/EOI). Nesses casos, aplica-se file carving por assinaturas: selecionar do SOI FF D8 ao EOI FF D9 e guardar apenas esse bloco.

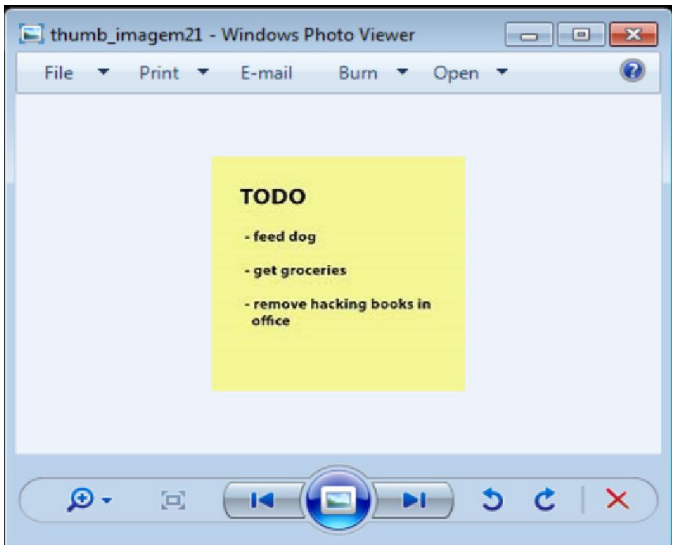
Passos executados no HxD:

1. Pesquisar → Valores Hexadecimais → FF D8 (SOI) dentro de imagem21.jpg.

   Havia dois FF D8 no ficheiro. Usei o segundo FF D8, porque a seguir apareciam marcadores típicos de um JPEG válido. O primeiro FF D8 vinha seguido de FF 01 + bytes soltos de EXIF e parecia corrompido.

   - Start-offset: 0x1D6.
2. Continuar a procurar até FF D9 (EOI).
   - End-offset: 0x1D22
3. Editar → Selecionar Bloco (modo *hex*):
   - Start: 1D6
   - End: 1D22
   - O HxD indicou Length = 0x1B4D (6 989 bytes).
4. Arquivo → Salvar seleção como… thumb_imagem21.jpg.

A miniatura abriu corretamente no visualizador.



MD5 da miniatura:

419f645a77575f30884a81c0f03764c8