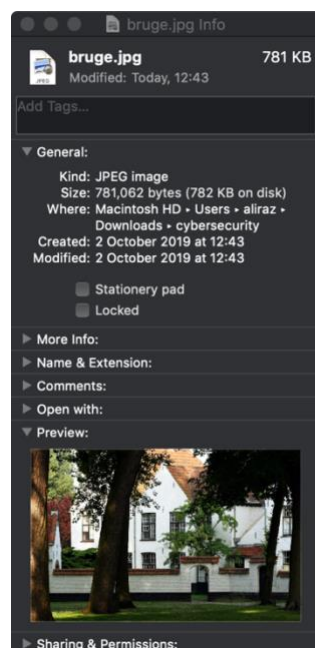


Task 1 Questions What are the filenames and file sizes for each of the *.jpg pictures discovered in image_01.dd?

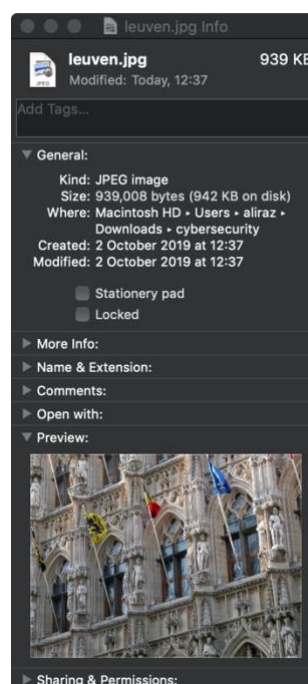
```
cybersecurity — -bash — 80x24
r/r 1-128-1:      $MFTMirr
r/r 9-128-8:      $Secure:$SDS
r/r 9-144-11:     $Secure:$SDH
r/r 9-144-5:      $Secure:$SII
r/r 10-128-1:     $UpCase
r/r 3-128-3:      $Volume
d/d 35-144-1:     private
+ r/r 40-128-1:   doel.exe
+ r/r 48-128-3:   key.txt
+ r/r 46-128-1:   mynotes
+ -/r * 47-128-1: key.txt
d/d 36-144-1:     public
+ d/d 37-144-1:   documents
++ r/r 45-128-1:  evidence.pdf
+ d/d 38-144-1:   pictures
++ r/r 41-128-1:  joyce.jpg
++ r/r 42-128-1:  leuven.jpg
++ r/r 42-128-3:  leuven.jpg:extra.txt
++ r/r 43-128-1:  lyon.jpg
++ r/r 43-128-3:  lyon.jpg:Zone.Identifier
++ -/r * 39-128-1:  brute.jpg
++ -/r * 44-128-1:  trees.jpg
d/d 256:          $OrphanFiles
dhcp-892b1c52:cybersecurity aliraz$
```

By using the `fls -o 61 -r image_01.dd` command we can find all of the file names including the jpg files

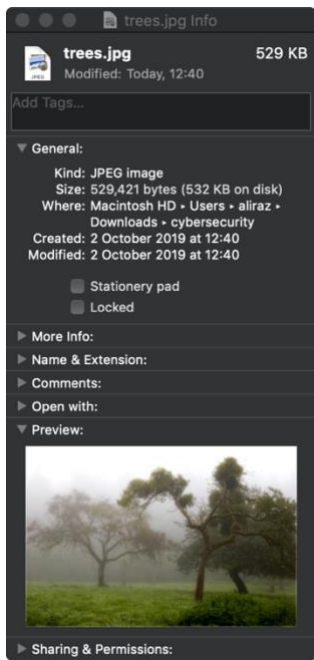
For finding the file size I extracted each one individually by `icat` command using the names found above.
E.g. `icat -o 61 image_01.dd 39 > brute.jpg`



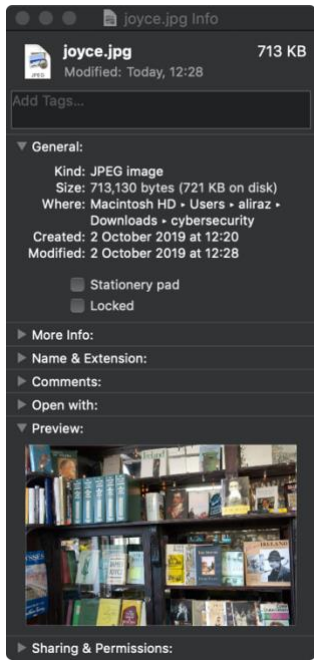
brute.jpg has file size of 781 KB



leuven.jpg has a file size of 939 KB



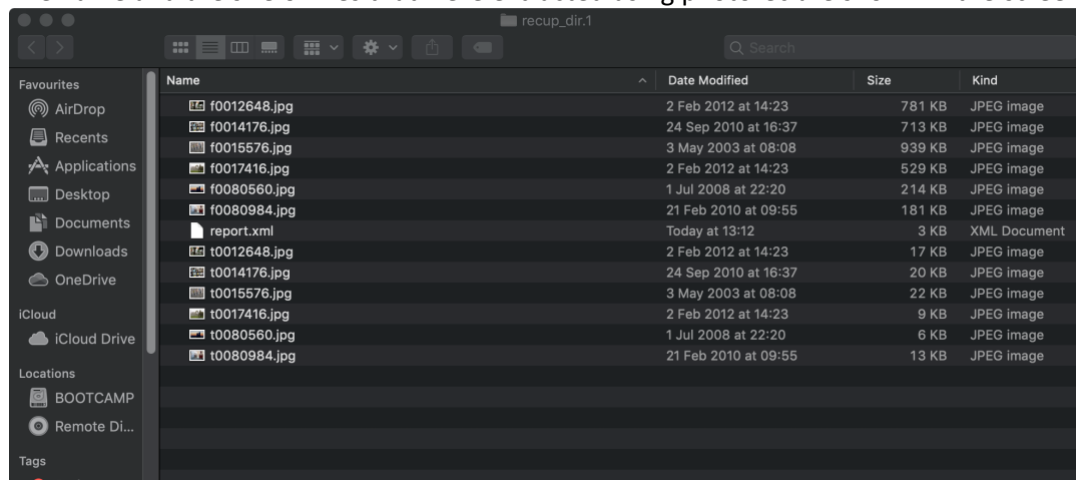
trees.jpg has file size of 529 KB



joyce.jpg has a file size of 713 KB

Task 2 Questions What are the filenames and file sizes for each of the *.jpg photos discovered in image_01.dd using Photorec?

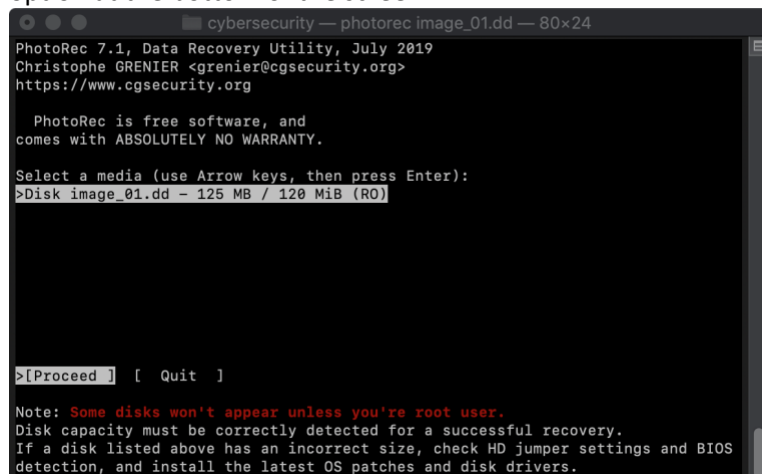
The name and the size of files that were extracted using photorec are shown in the screenshot below.



Name	Date Modified	Size	Kind
f0012648.jpg	2 Feb 2012 at 14:23	781 KB	JPEG image
f0014176.jpg	24 Sep 2010 at 16:37	713 KB	JPEG image
f0015576.jpg	3 May 2003 at 08:08	939 KB	JPEG image
f0017416.jpg	2 Feb 2012 at 14:23	529 KB	JPEG image
f0080560.jpg	1 Jul 2008 at 22:20	214 KB	JPEG image
f0080984.jpg	21 Feb 2010 at 09:55	181 KB	JPEG image
report.xml	Today at 13:12	3 KB	XML Document
t0012648.jpg	2 Feb 2012 at 14:23	17 KB	JPEG image
t0014176.jpg	24 Sep 2010 at 16:37	20 KB	JPEG image
t0015576.jpg	3 May 2003 at 08:08	22 KB	JPEG image
t0017416.jpg	2 Feb 2012 at 14:23	9 KB	JPEG image
t0080560.jpg	1 Jul 2008 at 22:20	6 KB	JPEG image
t0080984.jpg	21 Feb 2010 at 09:55	13 KB	JPEG image

To extract photos automatically using Photorec. We first need to run the program.

For running the program, we have to write **photorec image_01.dd** in a terminal. Then we choose the proceed option at the bottom of the screen.



```
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec is free software, and
comes with ABSOLUTELY NO WARRANTY.

Select a media (use Arrow keys, then press Enter):
>Disk image_01.dd - 125 MB / 120 MiB (R0)

>[Proceed] [Quit]
```

Then we have to deselect the type of files that we do not need. For that we choose file

>[File Opt]

opt

Then by pressing the 's' we deselect all of the options and by going on jpg and pressing 'x' we select it and that is our desired file type. After we chose our options, we press b to save the new instructions.

```
cybersecurity — photorec image_01.dd — 80x24
PhotoRec 7.1, Data Recovery Utility, July 2019
Christophe GRENIER <grenier@cgsecurity.org>
https://www.cgsecurity.org

PhotoRec will try to locate the following files

>[ ] custom Own custom signatures
[ ] 1cd Russian Finance 1C:Enterprise 8
[ ] 3dm Rhino / openNURBS
[ ] 7z 7zip archive file
[ ] DB
[ ] a Unix Archive/Debian package
[ ] abr Adobe Brush
[ ] acb Adobe Color Book
[ ] accdb Access Data Base
[ ] ace ACE archive
[ ] ab MAC Address Book
[ ] ado Adobe Duotone Options
[ ] afdesign afdesign
[ ] ahn Ahnenblatt
Next
Press s for default selection, b to save the settings
>[ Quit ]
Return to main menu
```

Afterwards we choose a location to extract the file to by pressing 'c' to confirm our location.

Include a full resolution copy of the extra photo discovered using Photorec in your Word Document (i.e. not recovered using sleuthkit)

