JPEG Search Test #1

Tool: Version:

1. What search procedure(s) were used to obtain the following results?

The following apply to the results from running an automated search tool for `JPEG` pictures. If more than one procedure was used to find the images, please note the procedure that was used to find each. Note that this was not designed to test data carving tools.

```
Keyword Search with Unicode Support

    ASCII encoding enabled

    Unicode encoding enabled

    Case-insensitive search

    Search term: jpg

File System Analysis

    Directory structure examination

    File extension filtering

    Metadata analysis

Data Carving (PhotoRec)

    `JPEG` header signature search: FF D8 FF

    File carving from unallocated space

    Minimum file size: 10KB

Hex Analysis

    Direct examination of file signatures

    Extension mismatch detection
```

2. Did the search results include the `alloc\file1.jpg` picture?

Found: YES Location: `/evidence/vol1-C..alloc.file1.jpg` Procedure: File system analysis + keyword search Notes: Successfully recovered from allocated space with proper extension.

3. Did the search results include the `alloc\file2.dat` picture? If not, then is it documented that JPEGs are found using only the extension?

Found: YES (as `.dat` file) Location: `/evidence/vol1-C..alloc.file2.dat` Procedure: File system analysis Notes: File has `.dat` extension but contains `JPEG` data. This demonstrates that the search does not rely solely on file extensions.

4. Did the search results include the `invalid\file3.jpg` file?

Found: PARTIALLY Location: Found reference in `/reports/files/` but marked as "invalid" Procedure: Keyword search found reference, but file is corrupt/invalid Notes: File exists in filesystem but is corrupted or has invalid `JPEG` structure.

5. Did the search results include the `invalid\file4.jpg` file?

Found: NO Procedure: Comprehensive search Notes: No evidence found in allocated space, unallocated space, or system logs. File may have been overwritten or never existed.

6. Did the search results include the `invalid\file5.rtf` file?

Found: YES (as `.trf` file, likely typo for `.rtf`) Location: Found in `/reports/file6/` Procedure: Keyword search Notes: File has `.trf` extension (possibly `.rtf` mislabeled) - requires further analysis.

7. Did the search results include the deleted picture in `$MFT` entry #32 (`del1/file6.jpg`)? If not, then is it documented that only allocated JPEGs will be found?

Found: YES Location: `/evidence/vol1-C..del1.file6.jpg` Procedure: Data carving from deleted space Notes: Successfully recovered deleted `JPEG`, proving the search does find deleted files, not just allocated ones.

8. Did the search results include the deleted picture in `$MFT` entry #31 (`del2/file7.hmm`)? If this file was not found, but the file in step #7 was found, then is it documented that only JPEGs with a proper extension will be found?

Found: YES (as .hmm file) Location: `/evidence/vol1-C..del2.file7.hmm` Procedure: File system analysis Notes: File has `.hmm` extension (non-standard). Found alongside `file6.jpg`, disproving the hypothesis that only `JPEG`s with proper extensions are found.

9. Did the search results include the picture inside of `archive\file8.zip`? If not, then is it documented that `JPEG` files will be found and that `JPEG` images that are embedded inside other file types will not?

Found: YES (archive found, contains `file8.jpg`) Location: `/reports/files/vol1-C..archive.file8.zip` + `/evidence/file8.jpg` Procedure: File system analysis + extraction Notes: The `ZIP` archive was identified, and the embedded `file8.jpg` was successfully extracted and recovered.

10. Did the search results include the picture inside of `archive\file9.boo`? If not, then is it documented that `JPEG` files will be found and that `JPEG` images that are embedded inside other file types will not?

Found: YES (archive found, contains `file9.jpg`) Location: `/reports/file9/vol1-C..archive.file9.b00` + `/evidence/file9.jpg` Procedure: File system analysis + extension analysis + extraction Notes: The `.boo/.b00` file was identified as a `ZIP` archive (ofuscated extension). The embedded `file9.jpg` was successfully extracted.

11. Did the search results include the picture inside of `archive\file10.tar.gz`? If not, then is it documented that `JPEG` files will be found and that `JPEG` images that are embedded inside other file types will not?

Found: YES (archive found, contains file10.jpg) Location: `/reports/file10/vol1-C..archive.file10.tar.gz` + `/reports/file10/file10.jpg` Procedure: File system analysis + extraction Notes: `TAR.GZ` archive identified and successfully extracted, containing `file10.jpg`

12. Did the search results include the `misc\file11.dat` file? If not, then is it documented that `JPEG` files will be found and that JPEG images that are embedded inside other file types will not?

Found: NO Procedure: Comprehensive search Notes: No file named `file11.dat` found in any location. Not present in image.

13. Did the search results include the misc\file12.doc file? If not, then is it documented that `JPEG` files will be found and that JPEG images that are embedded inside other file types will not?

Found: REFERENCE ONLY Location: Found reference in keyword search results ("`ict9.jpg`" in document) Procedure: Keyword search Notes: Document referenced in search results but file itself not recovered. May have been deleted or corrupted.

14. Did the search results include the `misc\file13.dll:here` picture? If not, then is it documented that pictures in alternate data streams will not be found?

Found: YES Location: `/reports/files/vol1-C..misc.file13.dll.here` Procedure: File system analysis Notes: Alternate data stream identified and documented. Contrary to the hypothesis, alternate data streams are found by the search procedure.