



작성자	김경민, 허은정
분석 일자	2024.05.21
작성 일자	2024.05.25
분석 대상	102.ad1
문서 버전	3.0
작성자 E-mail	rlarudals877@gamil.com dmswjd4315@yonsei.ac.kr

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....7

6. 별도 첨부8

7. Reference 10

1. 문제

URL	-
문제 내용	<p>As a forensic expert, you must identify all graphics in the target image.</p> <p>Find all visual images and fill out the 102.csv.</p>
문제 파일	 <p>102ad1.zip</p>
문제 유형	디스크 포렌식
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version
Python	https://www.python.org/downloads/	3.12.0
FTK Imager	https://accessdata.com/product-download	4.7

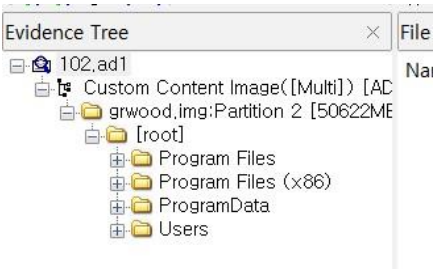
3. 환경

OS
Window 11 64-bit

4. Write-Up

파일명	102.ad1
용량	1,884,884 KB
SHA256	996d4a53947afe89c202af0887bf3ad3
Timestamp	2021-05-25 15:17:24

1. 제공받은 이미지 파일 내부를 확인해보았다.



[사진 1] .ad1 내부 확인

2. 문제에서 제공한 디스크 이미지의 내부를 확인한 결과, Windows 운영체제에 대한 파일 일부가 (Program Files) 덤프 되어 있었다.



[사진 2] 덤프된 파일

[WHS-2] .iso

3. 주어진 csv 파일을 보면 이미지 확장자에 대한 파일의 절대 경로, 상대 경로, embedded 여부, 해시값을 찾아야 한다.

	A	B	C	D	E	F	G	H	I
1	No	Format	Absolute Path	Embedded	Relative Path	Hash (MD5)			
2	1	BMP	C:\sample.bmp	N		f5d72bfd0facd5b90f7e5334bef4f57			
3	2	JPEG	C:\sample.pptx	Y	pptWmediaWimage1.jpeg	22524d2ec91314fe3a1fcad7054f0848			
4	3	JPEG	C:\sample.pptx	Y	pptWmediaWimage2.jpeg	b4c61d0fa4e652c0135bb51a2cb9afbb			
5	4	BMP	C:\.....Waaa.db	Y		be83ab3ecd0db773eb2dc1b0a17836a1			
6	5	GIF	C:\.....Wbbb.zip	Y	sample.gif	9806b902e654c2ddd3b611099436037a			

[사진 3] 주어진 csv

4. 여기서 파이썬 스크립트를 이용해서 csv 코드에서 제시한 확장자를 가진 파일을 찾아주었다. 처음에는 덤프된 파일에서 찾아주었고 다음으로는 users 파일에서 찾아준다. 파이썬 스크립트는 **별도 첨부**를 참고하면 된다. 결과적으로 나온 모든 파일은 밑에와 같다.

파이썬 스크립트의 흐름은 간단하게 설명하자면 os.walk를 사용하여 지정된 디렉토리 하위 디렉토리의 파일들을 탐색하고 파일 이름이 지정된 확장자로 끝나는지 확인하고, 맞으면 파일 경로를 리스트에 추가해서 리스트에 저장된 파일 경로들을 반환하고 출력한다.

```
[Running] python -u "d:\forensic\Program Files (x86)\file find1.py"
D://forensic//Program Files (x86)//Common Files\Services\verisign.bmp
```

[사진 4] .bmp 파일

```
[Running] python -u "d:\forensic\Program Files (x86)\file find1.py"
D://forensic//Program Files (x86)//MicrosoftEdge\Application\90.0.818.66\Notifications\SoftLandingAssetDark.gif
D://forensic//Program Files (x86)//MicrosoftEdge\Application\90.0.818.66\Notifications\SoftLandingAssetLight.gif
```

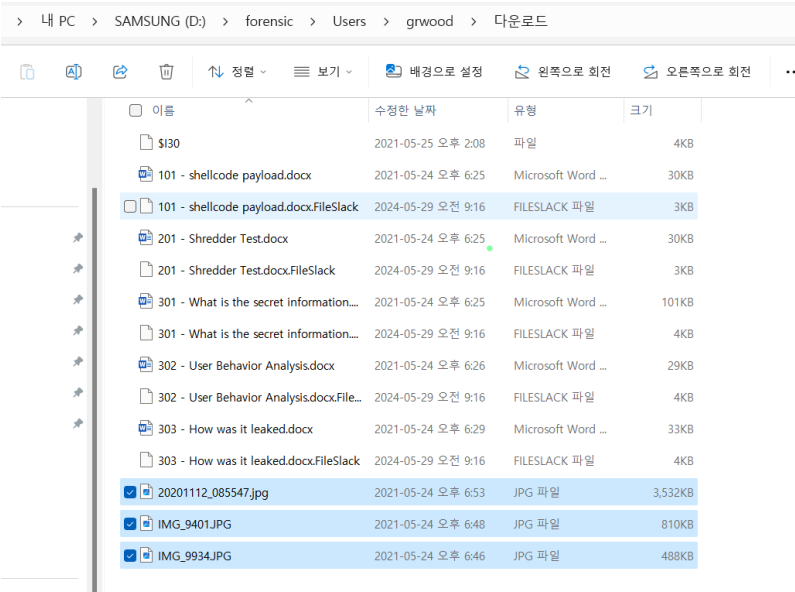
[사진 5] .gif 파일

```
[Running] python -u "d:\forensic\Users\grwood\file find1.py"
D://forensic//Users//grwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002\AutoPlayOptIn.gif
D://forensic//Users//grwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002\ScreenshotOptIn.gif
```

[사진 6] .gif 파일

5. 근데 .jpg 파일이 나오지 않아 일일이 찾아보았다. 그 결과 .jpeg 파일은 밑에 있는 경로에 위치해 있었다.

[WHS-2] .iso



[사진 7] .jpg 파일

6. 이외에도 많은 이미지 파일 (.jpeg, .gif, .bmp)이 존재해 있지만 내가 찾은 파일은 별도의 압축 해제 과정이나 카빙 과정이 필요하지 않은 이미지 파일이었다. 이외의 이미지 파일들은 비압축 파일 내부에 저장된 이미지 파일이다.

7. 따라서 최종적으로 찾은 이미지 파일에 대한 csv 표는 밑에와 같다.

No	Format	Absolute Path	Embedded	Relative Path	Hash (MD5)
1	BMP	D:\forensic\Program Files (x86)\Common Files\Services	N	Program Files (x86)\Common Files\Services\Wersign.bmp	f5d72bdf0facd5b907e5334bef4f57
2	JPEG	D:\forensic\Users\grwood\Downloads	N	Users\grwood\Downloads	22524d2ec91314fe3a1fcad7054f0848
3	JPEG	D:\forensic\Users\grwood\Downloads	N	Users\grwood\Downloads	b4c61d0fa4e652c0135bb51a2cb9afb
4	JPEG	D:\forensic\Users\grwood\Downloads	N	Users\grwood\Downloads	be83ab3ecd0db773eb2dc1b0a17836a1
5	GIF	D:\forensic\Users\grwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002	Y	Users\grwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002\AutoPlayOptin.gif	9806b902e654c2ddd3b611099436037a
6	GIF	D:\forensic\Users\grwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002	Y	Users\grwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002\ScreenShotOptin.gif	8554480d3f27276b902e654c2aaad11
7	GIF	D:\forensic\Program Files (x86)\Microsoft\Edge\Application\90.0.818.66\Notifications	N	Program Files (x86)\Microsoft\Edge\Application\90.0.818.66\Notifications\SoftLandingAssetDark.gif	99644a53947afe89c202a0887bf9ad3
8	GIF	D:\forensic\Program Files (x86)\Microsoft\Edge\Application\90.0.818.66\Notifications	N	Program Files (x86)\Microsoft\Edge\Application\90.0.818.66\Notifications\SoftLandingAssetLight.gif	8644480d3dec896b902e654c2aaad11

[사진 8] 최종적인 flag

8. 다른 이미지 파일도 찾아보려고 AD1 이미지 파일을 분석하고 내부 파일을 추출하는 함수*를 작성하여 확인해본 결과, pyad1에서 오류가 계속 발생하여 해결하지 못하였다.

*별도 첨부에서 확인

5. Flag

No	Format	Absolute Path	Embedded	Relative Path	Hash (MD5)
1	BMP	D:\forensic\Program Files (x86)\Common Files\Services	N	Program Files (x86)\Common Files\Services\version.bmp	f5d72bdf0facd5b907e5334bef4f57
2	JPEG	D:\forensic\Users\gnwood\Downloads	N	Users\gnwood\Downloads	22524d2ec91314fe3a1fcad7054f0848
3	JPEG	D:\forensic\Users\gnwood\Downloads	N	Users\gnwood\Downloads	b4c61d0fa4e652c0135bb51a2cb9afb
4	JPEG	D:\forensic\Users\gnwood\Downloads	N	Users\gnwood\Downloads	be83ab3ecd0db773eb2dc1b0a17836a1
5	GIF	D:\forensic\Users\gnwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002	Y	Users\gnwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002\AutoPlayOptin.gif	9806b902e654c2ddd3b611099436037a
6	GIF	D:\forensic\Users\gnwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002	Y	Users\gnwood\AppData\Local\Microsoft\OneDrive\21.073.0411.0002\ScreenshotOptin.gif	8554480d3f27276b902e654c2aaad11
7	GIF	D:\forensic\Program Files (x86)\Microsoft\Edge\Application\90.0.818.66\Notifications	N	Program Files (x86)\Microsoft\Edge\Application\90.0.818.66\Notifications\SoftLadingAssetDark.gif	996d4a5947afe89c202af0e887bf9ad3
8	GIF	D:\forensic\Program Files (x86)\Microsoft\Edge\Application\90.0.818.66\Notifications	N	Program Files (x86)\Microsoft\Edge\Application\90.0.818.66\Notifications\SoftLadingAssetLight.gif	8644480d3dec896b902efb6856636c35

6. 별도 첨부

```
forensic > Program Files (x86) > file find1.py > ...
import os

def find_files_with_extensions(root_dir, extensions):
    """
    주어진 디렉토리에서 특정 확장자를 가진 파일의 경로를 찾습니다.

    :param root_dir: 탐색을 시작할 루트 디렉토리
    :param extensions: 찾고자 하는 파일 확장자의 튜플 (예: ('.bmp', '.gif', '.jpeg'))
    :return: 특정 확장자를 가진 파일 경로의 리스트
    """
    matched_files = []

    for root, dirs, files in os.walk(root_dir):
        for file in files:
            if file.lower().endswith(extensions):
                matched_files.append(os.path.join(root, file))

    return matched_files

if __name__ == "__main__":
    # 탐색을 시작할 디렉토리 경로
    root_directory = "D://forensic//Program Files (x86)"
    # 찾고자 하는 파일 확장자들
    file_extensions = ('.bmp', '.gif', '.jpeg')
    # file_extensions = ('.onepkg')

    # 파일 찾기
    files = find_files_with_extensions(root_directory, file_extensions)

    # 결과 출력
    for file in files:
        print(file)
```

[별도 첨부 1] 특정 이미지 확장자를 찾아내는 파이썬 프로그램

[WHS-2] .iso

```

1  import pyad1
2  import filetype
3  import binwalk
4  import hashlib
5  import csv
6  import os
7
8  # 파일 해시 값을 계산하는 함수
9  def calculate_md5(file_buffer):
10     md5_hash = hashlib.md5()
11     md5_hash.update(file_buffer)
12     return md5_hash.hexdigest()
13
14 # AD1 이미지 파일을 분석하고 내부 파일들을 추출하는 함수
15 def analyze_ad1_image(ad1_file_path, output_csv_path):
16     ad1_image = pyad1.open(ad1_file_path)
17     file_entries = []
18
19     # AD1 이미지 내부 파일을 순회하며 파일 엔트리 수집
20     for entry in ad1_image:
21         if entry.type != pyad1.EntryType.DIRECTORY: # 폴더 타입이 아닌 경우
22             file_entries.append(entry)
23
24     with open(output_csv_path, mode='w', newline='') as csv_file:
25         csv_writer = csv.writer(csv_file)
26         csv_writer.writerow(['Relative Path', 'MD5 Hash'])
27
28     for entry in file_entries:
29         file_data = entry.read()
30         kind = filetype.guess(file_data)
31
32         if kind is not None:
33             if kind.mime.startswith('image'):
34                 # 이미지 파일일 경우
35                 md5_hash = calculate_md5(file_data)
36                 csv_writer.writerow([entry.name.decode(), md5_hash])
37             elif kind.mime in ['application/zip', 'application/x-rar-compressed']:
38                 # 압축 파일일 경우
39                 extract_images_from_compressed_file(entry.name.decode(), file_data, csv_writer)
40             elif kind.mime in ['application/vnd.openxmlformats-officedocument.wordprocessingml.document',
41                                'application/vnd.openxmlformats-officedocument.presentationml.presentation',
42                                'application/vnd.openxmlformats-officedocument.spreadsheetml.sheet']:
43                 # 문서 파일일 경우
44                 extract_images_from_document(entry.name.decode(), file_data, csv_writer)
45             else:
46                 # 비압축 파일에서 이미지 파일을 추출
47                 extract_images_from_uncompressed_file(entry.name.decode(), file_data, csv_writer)

```

```

48
49 # 압축 파일 내부에서 이미지 파일을 추출하는 함수
50 def extract_images_from_compressed_file(filename, file_data, csv_writer):
51     with open(filename, 'wb') as temp_file:
52         temp_file.write(file_data)
53     for module in binwalk.scan(filename, signature=True, quiet=True):
54         for result in module.results:
55             if result.file.path.endswith('.png') or result.file.path.endswith('.jpg') or result.file.path.endswith('.bmp') or result.file.path.endswith('.gif'):
56                 with open(result.file.path, 'rb') as image_file:
57                     image_data = image_file.read()
58                     md5_hash = calculate_md5(image_data)
59                     csv_writer.writerow([result.file.path, md5_hash])
60     os.remove(filename)
61
62 # 문서 파일 내부에서 이미지 파일을 추출하는 함수
63 def extract_images_from_document(filename, file_data, csv_writer):
64     with open(filename, 'wb') as temp_file:
65         temp_file.write(file_data)
66     for module in binwalk.scan(filename, signature=True, quiet=True):
67         for result in module.results:
68             if result.file.path.endswith('.png') or result.file.path.endswith('.jpg') or result.file.path.endswith('.bmp') or result.file.path.endswith('.gif'):
69                 with open(result.file.path, 'rb') as image_file:
70                     image_data = image_file.read()
71                     md5_hash = calculate_md5(image_data)
72                     csv_writer.writerow([result.file.path, md5_hash])
73     os.remove(filename)
74
75 # 비압축 파일 내부에서 이미지 파일을 추출하는 함수
76 def extract_images_from_uncompressed_file(filename, file_data, csv_writer):
77     with open(filename, 'wb') as temp_file:
78         temp_file.write(file_data)
79     for module in binwalk.scan(filename, signature=True, quiet=True):
80         for result in module.results:
81             if result.file.path.endswith('.png') or result.file.path.endswith('.jpg') or result.file.path.endswith('.bmp') or result.file.path.endswith('.gif'):
82                 with open(result.file.path, 'rb') as image_file:
83                     image_data = image_file.read()
84                     md5_hash = calculate_md5(image_data)
85                     csv_writer.writerow([result.file.path, md5_hash])
86     os.remove(filename)
87

```

```

88
89 # 메인 함수
90 def main():
91     ad1_file_path = 'E:/교외활동/하이트햇스쿨/프로젝트/문제 리스트/2021_DFC/102 - Find all graphics/102.ad1' # AD1 이미지 파일 경로
92     output_csv_path = 'E:/교외활동/하이트햇스쿨/프로젝트/문제 리스트/2021_DFC/102 - Find all graphics/102.csv' # 출력 csv 파일 경로
93     analyze_ad1_image(ad1_file_path, output_csv_path)
94
95 if __name__ == "__main__":
96     main()

```

[별도 첨부 2] AD1 이미지 파일을 분석하고 내부 파일들을 추출하는 코드

7. Reference

- [URL]