소프트웨어응용보안(F056-1)

Team # 2

201520890 박세환

201420948 김동현

201320878 박용채

201520892 이종인

201421273 이세린

**Term Project#2 – File system Dataset**

# **Dataset Constructor**

# 1. Dataset Structure

// 표로 dataset 1,2,3 별로 OS, Kernel verision, Partition size 정리

|  |  |  |  |
| --- | --- | --- | --- |
|  | **OS type** | **Kernel Version** | **Partition Size** |
| **Dataset #1** | ubuntu 16.04 | 4.15.0.70-generic | 10GB |
| **Dataset #2** | Debian GNU/Linux 9 | 4.9.0-6-amd64 | 15GB |
| **Dataset #3** | Linux Mint 19.2 Tina | 4.15.0-54 | 20GB |
| **Dataset #4** | ubuntu 18.04.3 LTS | 5.0.0-32-generic | 15GB |

# 2. Dataset Result

공통 수행과정

* 총 109개의 파일 중 33개를 삭제하였음.
* r-studio 및 UFS 복구툴을 이용한 파일 복구 진행
* 삭제한 파일 목록

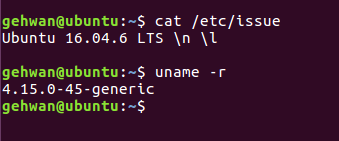
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 참가자정보.xlsx | 2.py | 3.py | 7.py | 201520890\_박세환.py | 개인 프로젝트.pptx | and\_ab\_xor\_c.bmp |
| 9조\_현성사\_혼전성관계에대한인식.pptx | Report2.pdf | Assignment3-MyLock-ko.pdf | 19.04.12\_보안프로젝트\_랜섬웨어\_성진.pdf | Report.pdf | Assignment-Mysh2.pdf | 20191124\_234139.jpg |
| 20190917\_105817.pdf | 20191111\_135421.jpg | 20191108\_111723.jpg | 20191124\_234145.jpg | ubuntu-18.04.1-desktop-amd64.iso | 공부 스터디 7-1주차.hwp | 공부 스터디 2주차.hwp |
| 공부 스터디 8주차-1.hwp | 공부 스터디 10주차-1-1.hwp | 공부 스터디 9주차-1.hwp | 5dbb99d534d4d.gif | 5dcb4ce53f3ea.gif | 5dc3bab4be08.gif | 보안프로젝트 2번째.docx |
| 랜섬웨어 구현 방향.docx | 링크 인턴 주간보고서.docx | 2019암호경진대회\_5번\_답안지\_홍길동\_OOO학교.docx | and\_bc\_and\_a.bmp | and\_bc\_or\_a.bmp |  |  |

위의 파일들은 지운 목록은 모두 동일하지만 지우고 복구하는 과정에서의 다양한 변수를 고려하기 위하여 다음과 같은 경우로 나누었다.

1. 쓰레기통을 비우고 img파일 추출
2. 쓰레기통을 비우지 않고 img 파일 추출
3. command rm으로 삭제한 후 img 파일 추출

## 2.1 Dataset #1

Ubuntu 16.04 사용. Ubuntu OS의 kernel version은 4.15.0.45-generic을 사용하였다.

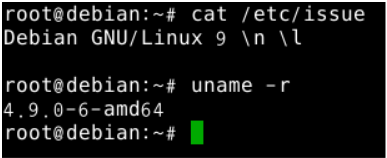


Partition Size는 10GB이며 다음과 같이 마운트 진행 이후,데이터 셋을 넣어 이미지를 추출하였다.



## 2.2 Dataset #2

Ubuntu 16.04 사용. Ubuntu OS의 kernel version은 4.15.0.45-generic을 사용하였다.



Partition Size는 15GB이며 이후의 과정은 Dataset #1과 동일하다.

## 2.3 Dataset #3

Mint OS 사용. Mint OS의 kernel version은 4.15.0-54를 사용하고 있다.

## 

1. 총 109개의 파일 중 33개를 삭제하였음.
2. Partition Size는 20GB이다.
3. 삭제한 파일 목록

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 참가자정보.xlsx | 2.py | 3.py | 7.py | 201520890\_박세환.py | 개인 프로젝트.pptx | and\_ab\_xor\_c.bmp |
| 9조\_현성사\_혼전성관계에대한인식.pptx | Report2.pdf | Assignment3-MyLock-ko.pdf | 19.04.12\_보안프로젝트\_랜섬웨어\_성진.pdf | Report.pdf | Assignment-Mysh2.pdf | 20191124\_234139.jpg |
| 20190917\_105817.pdf | 20191111\_135421.jpg | 20191108\_111723.jpg | 20191124\_234145.jpg | ubuntu-18.04.1-desktop-amd64.iso | 공부 스터디 7-1주차.hwp | 공부 스터디 2주차.hwp |
| 공부 스터디 8주차-1.hwp | 공부 스터디 10주차-1-1.hwp | 공부 스터디 9주차-1.hwp | 5dbb99d534d4d.gif | 5dcb4ce53f3ea.gif | 5dc3bab4be08.gif | 보안프로젝트 2번째.docx |
| 랜섬웨어 구현 방향.docx | 링크 인턴 주간보고서.docx | 2019암호경진대회\_5번\_답안지\_홍길동\_OOO학교.docx | and\_bc\_and\_a.bmp | and\_bc\_or\_a.bmp |  |  |

위의 파일들은 지운 목록은 모두 동일하지만 지우고 복구하는 과정에서의 다양한 변수를 고려하기 위하여 다음과 같은 경우로 나누었다.

1. 쓰레기통을 비우고 img파일 추출
2. 쓰레기통을 비우지 않고 img 파일 추출
3. command rm으로 삭제한 후 img 파일 추출

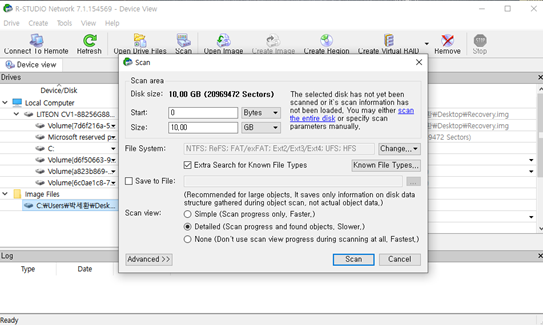
// 커널 버전을 포함한 이미지 추가 + 어떤 파일을 삭제했는지

# **Recovery Tool Test Analysis**

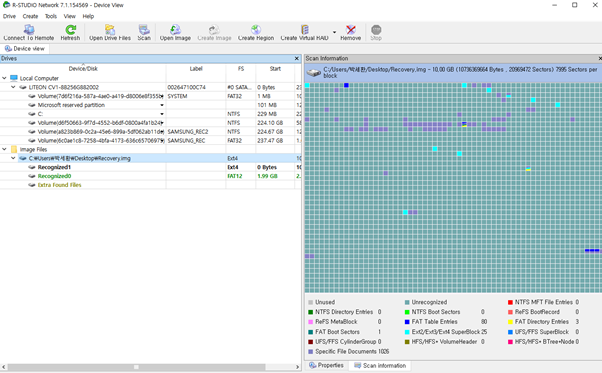
# 1. Dataset#1 Recovery Test

## 1.1 R-studio Test

* 이미지 오픈 및 파일 스캔



* 파일 스캔 결과



파일 스캔이후 다음과 같이 세 가지의 카테고리가 생성된다.

* Recognized1
* Recognized0
* Extra Found Files

이들 중 Recognized1 카테고리에서 전체스캔한 총괄적인 정보를 손쉽게 확인할 수 있으므로 Recognized1 카테고리를 확인하였다. Recognized1 카테고리에는 기존 데이터셋의 내용을 기본적으로 포함하였고 추가적으로 .Trash-1000과 Extra Found Files, Metafiles들이 생성되었다는 것을 알 수 있었다.

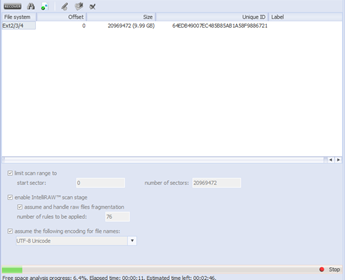
복구 여부

|  |  |  |  |
| --- | --- | --- | --- |
|  | 쓰레기통 비움 | 쓰레기통 안 비움 | rm으로 삭제 |
| 참가자정보.xlsx | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 2.py | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 3.py | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 7.py | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 201520890\_박세환.pptx | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 개인 프로젝트.pptx | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 9조\_현성사\_혼전성관계에대한인식.pptx | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| Report2.pdf | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| Assignment3-MyLock-ko.pdf | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 19.04.12\_보안프로젝트\_랜섬웨어\_성진.pdf | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| Report.pdf | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| Assignment-Mysh2.pdf | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 20191124\_234139.jpg | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 20190917\_105817.pdf | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 20191111\_135421.jpg | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 20191108\_111723.jpg | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 20191124\_234145.jpg | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| ubuntu-18.04.1-desktop-amd64.iso | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |

|  |  |  |  |
| --- | --- | --- | --- |
| 공부 스터디 7-1주차.hwp | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 공부 스터디 2주차.hwp | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 공부 스터디 8주차-1.hwp | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 공부 스터디 10주차-1-1.hwp | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 공부 스터디 9주차-1.hwp | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 5dbb99d534d4d.gif | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 5dcb4ce53f3ea.gif | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 5dc3bab4be08.gif | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 보안프로젝트 2번째.docx | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 랜섬웨어 구현 방향.docx | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 링크 인턴 주간보고서.docx | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 2019암호경진대회\_5번\_답안지\_홍길동\_OOO학교.docx | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| and\_bc\_and\_a.bmp | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| and\_bc\_or\_a.bmp | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| and\_ab\_xor\_c.bmp | Δ(0KB 로 복구) | ⚪ | Δ(0KB 로 복구) |
| 복구율 | 0% | 100% | 0% |

## 1.2 UFS explorer Test

UFS 도구를 이용하여 첫번째로 이미지를 넣어 복구를 위해 이미지를 스캔하였다.



스캔이 완료되면, 다음과 같이 확장자 별로 분류된 파일들과, 삭제되었던 파일들을 확인할 수 있으며, 해당 파일들을 복원할 수 있다.

복구 여부

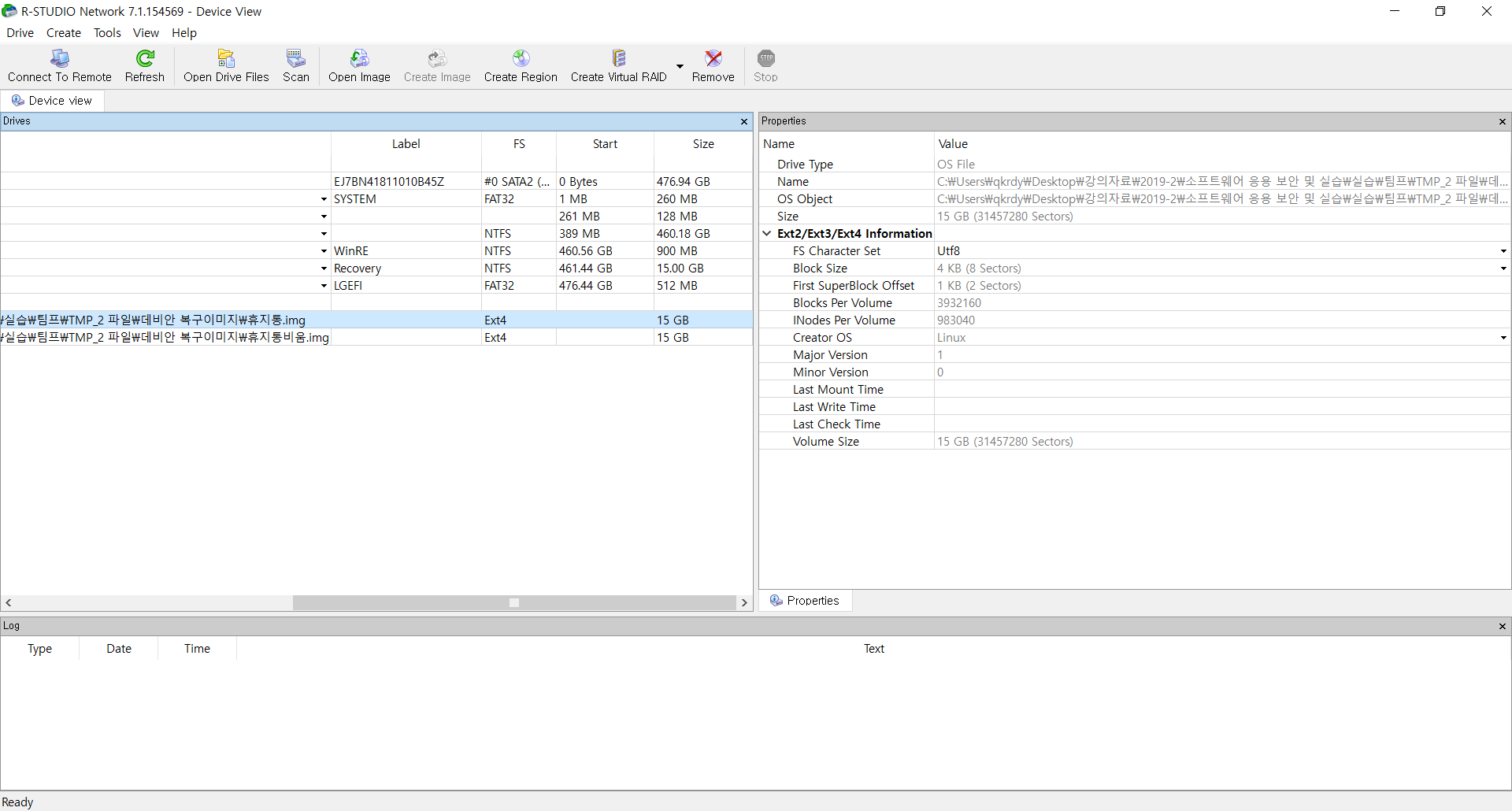
|  |  |  |  |
| --- | --- | --- | --- |
|  | 쓰레기통 비움 | 쓰레기통 안 비움 | rm으로 삭제 |
| 참가자정보.xlsx | ⚪ | ⚪ | Δ(파일 이름만 존재) |
| 2.py | ⚪ | ⚪ | ✖️ |
| 3.py | ⚪ | ⚪ | ✖️ |
| 7.py | ⚪ | ⚪ | ✖️ |
| 201520890\_박세환.pptx | ⚪ | ⚪ | ✖️ |
| 개인 프로젝트.pptx | ⚪ | ⚪ | ✖️ |
| 9조\_현성사\_혼전성관계에대한인식.pptx | ⚪ | ⚪ | ✖️ |
| Report2.pdf | ⚪ | ⚪ | ✖️ |
| Assignment3-MyLock-ko.pdf | ⚪ | ⚪ | ✖️ |
| 19.04.12\_보안프로젝트\_랜섬웨어\_성진.pdf | ⚪ | ⚪ | ✖️ |
| Report.pdf | ⚪ | ⚪ | ✖️ |
| Assignment-Mysh2.pdf | ⚪ | ⚪ | ✖️ |
| 20191124\_234139.jpg | ⚪ | ⚪ | ✖️ |
| 20190917\_105817.pdf | ⚪ | ⚪ | ✖️ |
| 20191111\_135421.jpg | ⚪ | ⚪ | ✖️ |
| 20191108\_111723.jpg | ⚪ | ⚪ | ✖️ |
| 20191124\_234145.jpg | ⚪ | ⚪ | ✖️ |
| ubuntu-18.04.1-desktop-amd64.iso | ✖️(정보에는 존재하나,용량이 커 복구 불가) | ✖️(정보에는 존재하나,용량이 커 복구 불가) | ✖️ |

|  |  |  |  |
| --- | --- | --- | --- |
| 공부 스터디 7-1주차.hwp | ⚪ | ⚪ | ✖️ |
| 공부 스터디 2주차.hwp | ⚪ | ⚪ | ✖️ |
| 공부 스터디 8주차-1.hwp | ⚪ | ⚪ | ✖️ |
| 공부 스터디 10주차-1-1.hwp | ⚪ | ⚪ | ✖️ |
| 공부 스터디 9주차-1.hwp | ⚪ | ⚪ | ✖️ |
| 5dbb99d534d4d.gif | ⚪ | ⚪ | ✖️ |
| 5dcb4ce53f3ea.gif | ⚪ | ⚪ | ✖️ |
| 5dc3bab4be08.gif | ⚪ | ⚪ | ✖️ |
| 보안프로젝트 2번째.docx | ⚪ | ⚪ | ✖️ |
| 랜섬웨어 구현 방향.docx | ⚪ | ⚪ | ✖️ |
| 링크 인턴 주간보고서.docx | ⚪ | ⚪ | ✖️ |
| 2019암호경진대회\_5번\_답안지\_홍길동\_OOO학교.docx | ⚪ | ⚪ | ✖️ |
| and\_bc\_and\_a.bmp | ⚪ | ⚪ | ✖️ |
| and\_bc\_or\_a.bmp | ⚪ | ⚪ | ✖️ |
| and\_ab\_xor\_c.bmp | ⚪ | ⚪ | ✖️ |
| 복구율 | 96.7% | 96.7% | 0% |

# 2. Dataset#2 Recovery Test

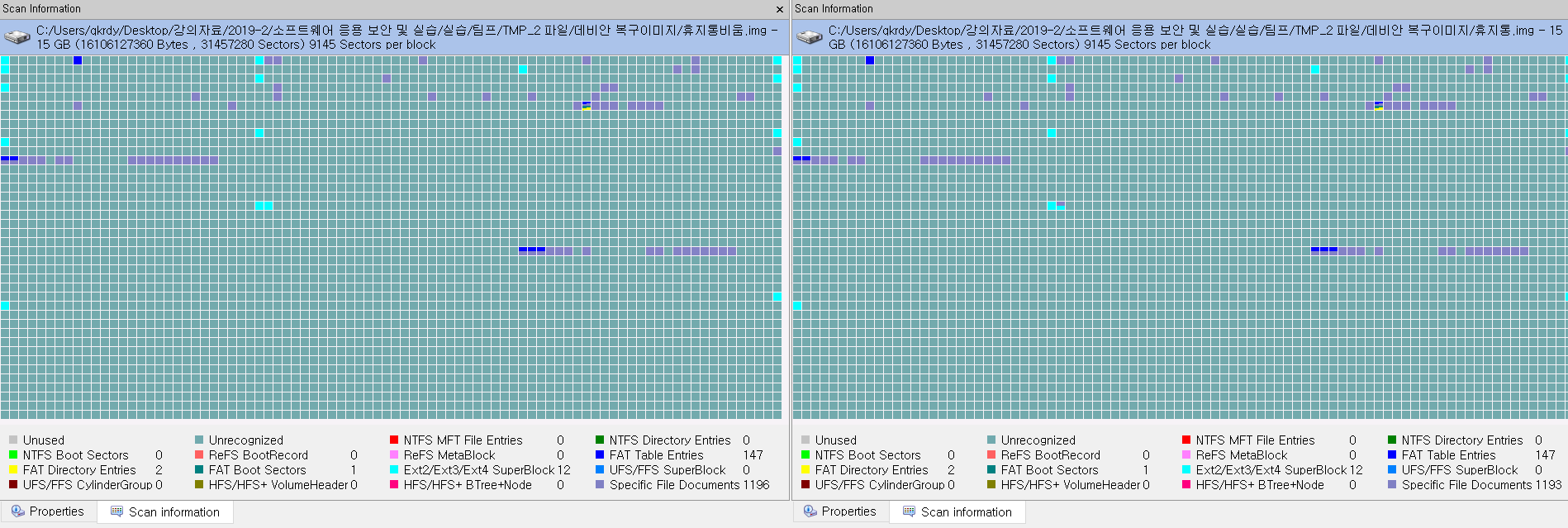
## 2.1 R-studio Test

* 이미지 오픈 및 파일 스캔

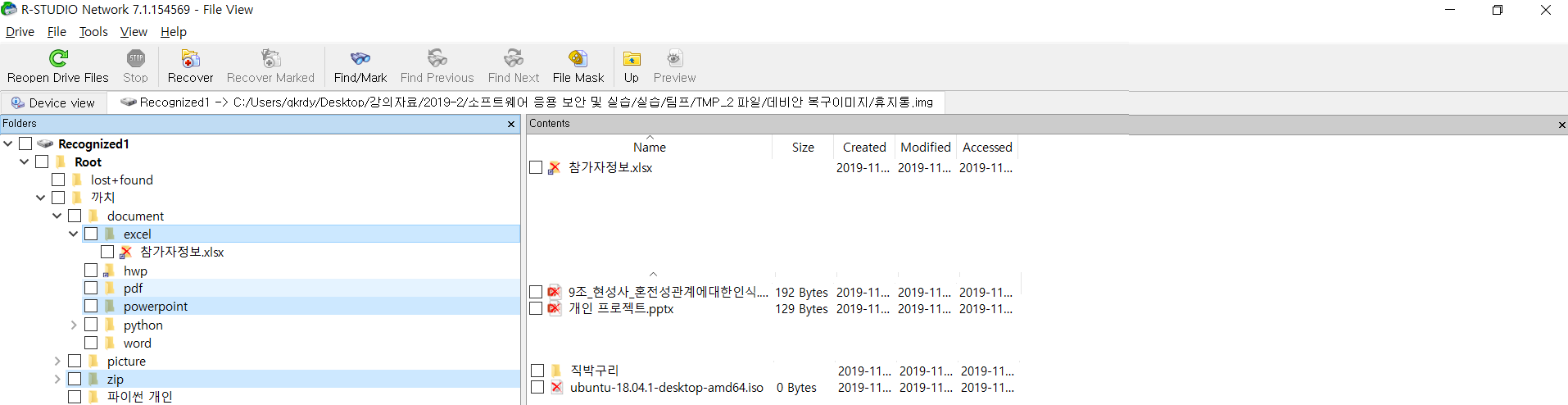


휴지통 비움의 경우와 rm 명령어로 삭제한 결과가 같게 나와 두가지 케이스만 비교한다.

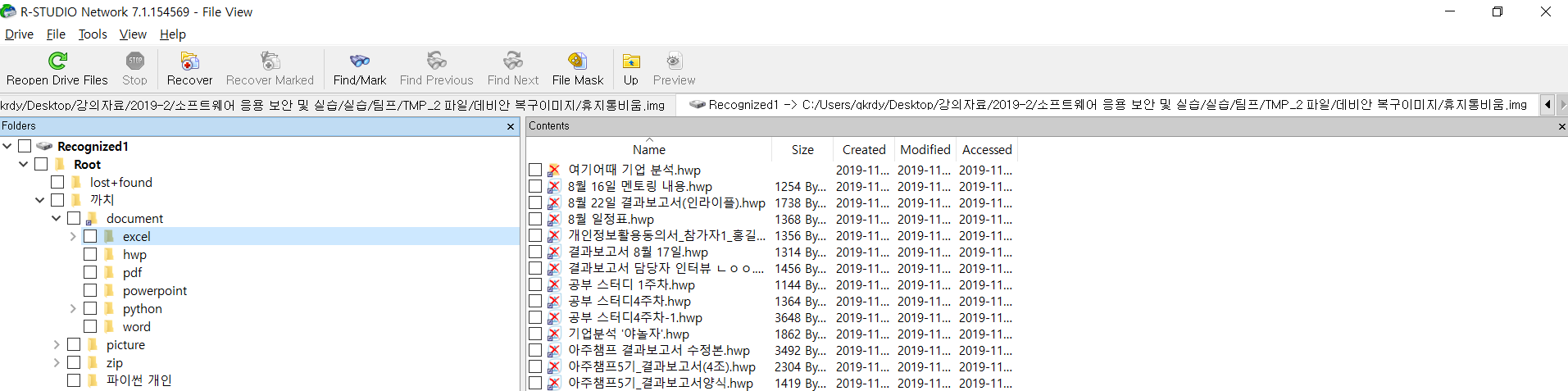
* 파일 스캔 결과

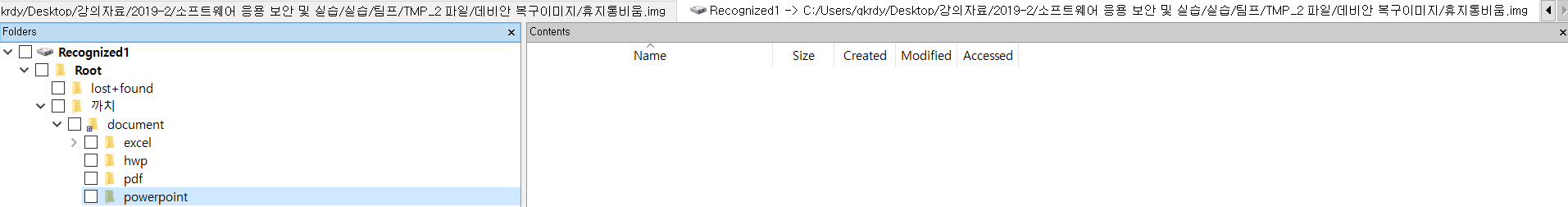


스캔 결과에서 오프셋12853306에서 할당된 차이가 있음을 볼 수 있다. 내부 복구 파일에서도 차이점을 볼 수 있는데 그 차이는 아래의 사진과 같다.



위 이미지는 휴지통에 남아 있는상태로 복구한 이미지이다. 파일이 원래 위치에 복구되진 않았지만 삭제된 일부 파일의 이름과 흔적을 찾을 수 있다.





하지만 휴지통 비움을 하고 덤프한 이미지에서는 엑셀 폴더에 hwp 파일이 삭제되었다는 흔적과 pptx, iso 파일의 흔적은 찾을 수 없었다.

파일 스캔이후 다음과 같이 세 가지의 카테고리가 생성된다.

* Recognized1
* Recognized0
* Extra Found Files

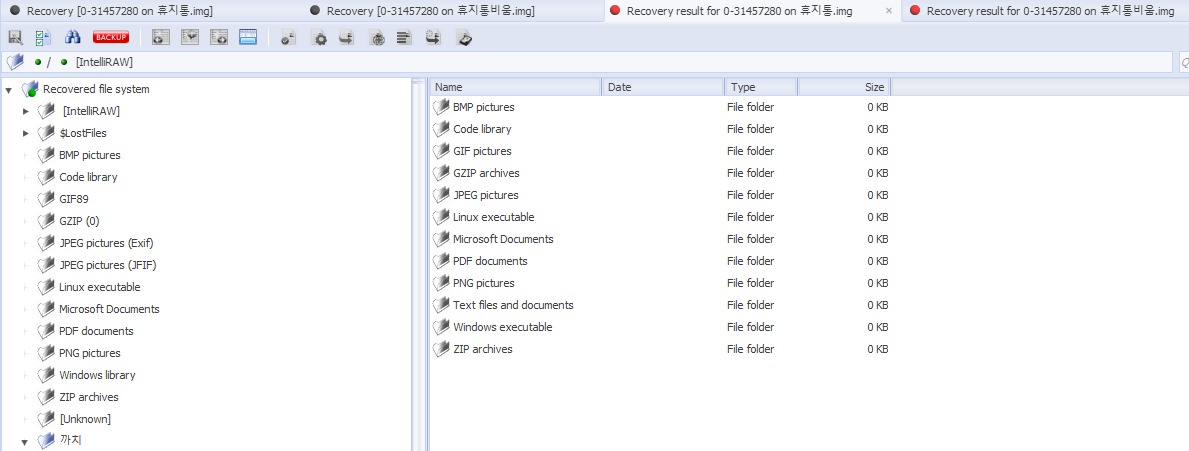
이들 중 Recognized1 카테고리에서 전체스캔한 총괄적인 정보를 손쉽게 확인할 수 있으므로 Recognized1 카테고리를 확인하였다. Recognized1 카테고리에는 기존 데이터셋의 내용을 기본적으로 포함하였고 추가적으로 . Extra Found Files, Metafiles들이 생성되었다는 것을 알 수 있었다. Extra Found Files에서는 휴지통, 삭제 방법에 따른 차이 없이 같은 결과를 도출했다.

복구 여부

|  |  |  |  |
| --- | --- | --- | --- |
|  | 복구 | 크기 | 해시값 |
| 참가자정보.xlsx | ⚪ | 일치 | ⚪ |
| 2.py | ⚪,txt 파일로 복구 | 일치 | x |
| 3.py | ⚪,txt 파일로 복구 | 일치 | x |
| 7.py | ⚪,txt 파일로 복구 | 일치 | x |
| 201520890\_박세환.py | ⚪,txt 파일로 복구 | 일치 | x |
| 개인 프로젝트.pptx | ⚪ | 일치 | ⚪ |
| 9조\_현성사\_혼전성관계에대한인식.pptx | ⚪ | 일치 | ⚪ |
| Report2.pdf | ⚪ | 디스크 할당 크기 | x |
| Assignment3-MyLock-ko.pdf | ⚪ | 디스크 할당 크기 | x |
| 19.04.12\_보안프로젝트\_랜섬웨어\_성진.pdf | ⚪ | 디스크 할당 크기 | x |
| Report.pdf | ⚪ | 디스크 할당 크기 | x |
| Assignment-Mysh2.pdf | ⚪ | 디스크 할당 크기 | x |
| 20191124\_234139.jpg | ⚪ | 일치 | ⚪ |
| 20190917\_105817.jpg | ⚪ | 일치 | ⚪ |
| 20191111\_135421.jpg | ⚪ | 일치 | ⚪ |
| 20191108\_111723.jpg | ⚪ | 일치 | ⚪ |
| 20191124\_234145.jpg | ⚪ | 일치 | ⚪ |
| ubuntu-18.04.1-desktop-amd64.iso | ⚪ | ⚪ | x |
| 공부 스터디 7-1주차.hwp | x |  |  |
| 공부 스터디 2주차.hwp | x |  |  |
| 공부 스터디 8주차-1.hwp | x |  |  |
| 공부 스터디 10주차-1-1.hwp | x |  |  |
| 공부 스터디 9주차-1.hwp | x |  |  |
| 5dbb99d534d4d.gif | x |  |  |
| 5dcb4ce53f3ea.gif | ⚪ | 디스크 할당 크기 | x |
| 5dc3bab4be08.gif | ⚪ | 디스크 할당 크기 | x |
| 보안프로젝트 2번째.docx | ⚪ | 일치 | ⚪ |
| 랜섬웨어 구현 방향.docx | ⚪ | 일치 | ⚪ |
| 링크 인턴 주간보고서.docx | ⚪ | 일치 | ⚪ |
| 2019암호경진대회\_5번\_답안지\_홍길동\_OOO학교.docx | ⚪ | 일치 | ⚪ |
| and\_bc\_and\_a.bmp | ⚪ | 디스크 할당 크기 | x |
| and\_bc\_or\_a.bmp | ⚪ | 디스크 할당 크기 | x |
| and\_ab\_xor\_c.bmp | ⚪ | 디스크 할당 크기 | x |
| 복구율 | 81.8% | 원본파일 크기 or 디스크 할당 크기 | MS파일에서 일치 |

## 2.2 UFS explorer Test

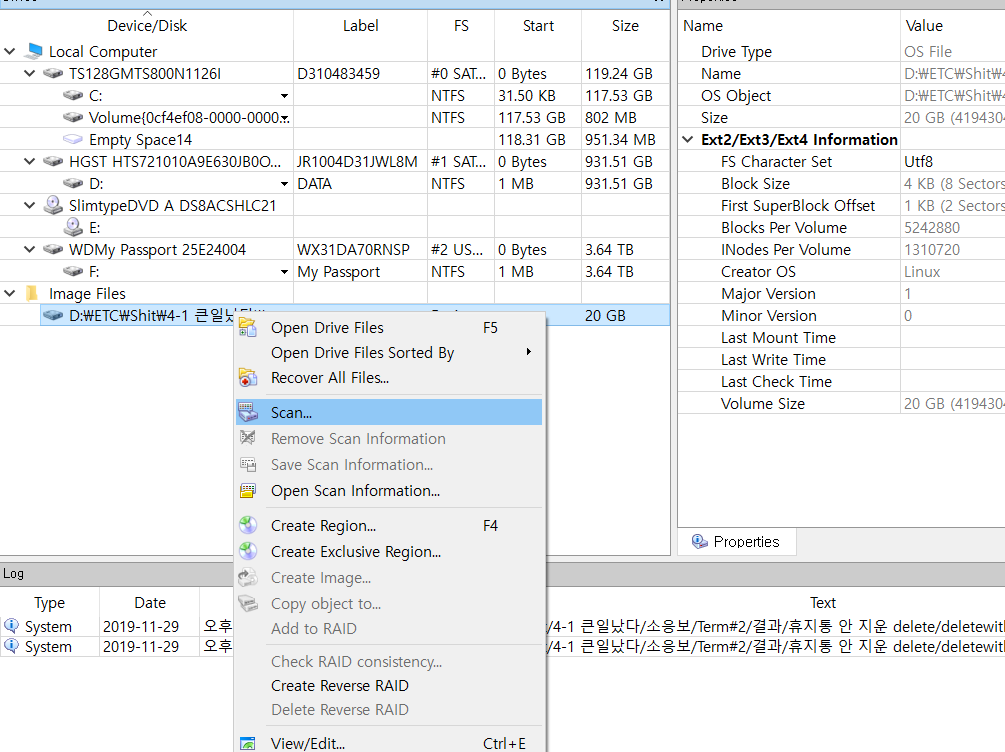
UFS 툴 역시 R-studio와 같은 이미지 파일을 스캔 후 복구한다. 휴지통, 비움, rm 명령어 조건의 차이는 확인 할 수 없었다. 원래 있던 위치에서의 흔적 또한 찾을 수 없었다. [IntelliRAW] 폴더내의 파일과 바깥의 파일 구성은 같은 것을 확인했다.



R-studio와는 다르게 MS파일을 확장자별로 복구하는 것이 아니라 msdoc확장자 명으로 복구한다. 파일 크기로 분석해 보았으니 디스크 할당크기와 같은 파일도 있었지만 크기가 같은 파일이 존재하지 않은 파일도 확인했다. pdf, gif, jpg, bmp 확장자를 갖고있는 파일은 복구했지만 모두 다 디스크 할당 크기로 복구되었고 해시값이 다름을 확인했다.

# 3. Dataset#3 Recovery Test

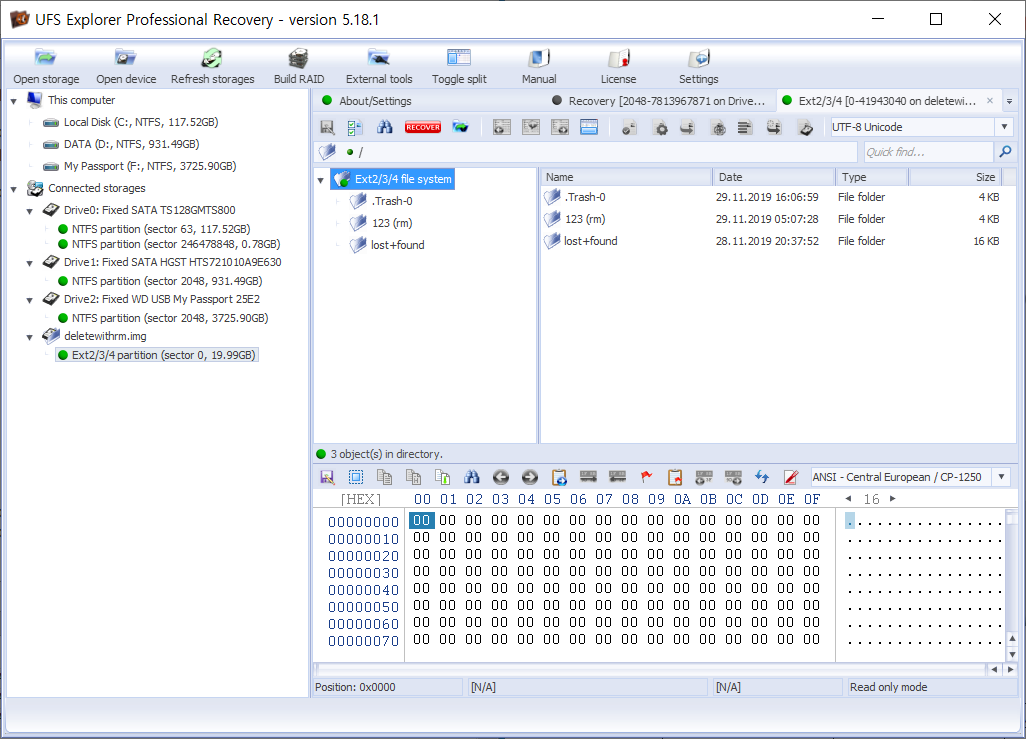
## 2.1 R-studio Test



* Scan을 한 후 모든 파일을 대상으로 복구를 시도하였음.
* 복구 여부(R-Studio)

|  |  |  |  |
| --- | --- | --- | --- |
|  | 쓰레기통 비움 | 쓰레기통 안 비움 | rm으로 삭제 |
| 참가자정보.xlsx | Δ(파일 이름만 존재) | Δ(파일 이름만 존재) | Δ(파일 이름만 존재) |
| 2.py | ✖️ | ⚪ | ✖️ |
| 3.py | ✖️ | ⚪ | ✖️ |
| 7.py | ✖️ | ⚪ | ✖️ |
| 201520890\_박세환.pptx | ✖️ | ⚪ | ✖️ |
| 개인 프로젝트.pptx | ⚪ | ⚪ | ⚪ |
| 9조\_현성사\_혼전성관계에대한인식.pptx | ⚪ | ⚪ | ⚪ |
| Report2.pdf | ✖️ | ✖️ | ✖️ |
| Assignment3-MyLock-ko.pdf | ✖️ | ✖️ | ✖️ |
| 19.04.12\_보안프로젝트\_랜섬웨어\_성진.pdf | ✖️ | ✖️ | ✖️ |
| Report.pdf | ✖️ | ✖️ | ✖️ |
| Assignment-Mysh2.pdf | ✖️ | ✖️ | ✖️ |
| 20191124\_234139.jpg | ✖️ | ✖️ | ✖️ |
| 20190917\_105817.pdf | ✖️ | ✖️ | ✖️ |
| 20191111\_135421.jpg | ✖️ | ✖️ | ✖️ |
| 20191108\_111723.jpg | ✖️ | ✖️ | ✖️ |
| 20191124\_234145.jpg | ✖️ | ✖️ | ✖️ |
| ubuntu-18.04.1-desktop-amd64.iso | ✖️ | ✖️ | ✖️ |
| 공부 스터디 7-1주차.hwp | ✖️ | ✖️ | ✖️ |
| 공부 스터디 2주차.hwp | ✖️ | ✖️ | ✖️ |
| 공부 스터디 8주차-1.hwp | ✖️ | ✖️ | ✖️ |
| 공부 스터디 10주차-1-1.hwp | ✖️ | ✖️ | ✖️ |
| 공부 스터디 9주차-1.hwp | ✖️ | ✖️ | ✖️ |
| 5dbb99d534d4d.gif | ✖️ | ✖️ | ✖️ |
| 5dcb4ce53f3ea.gif | ✖️ | ✖️ | ✖️ |
| 5dc3bab4be08.gif | ✖️ | ✖️ | ✖️ |
| 보안프로젝트 2번째.docx | ✖️ | ✖️ | ✖️ |
| 랜섬웨어 구현 방향.docx | ✖️ | ✖️ | ✖️ |
| 링크 인턴 주간보고서.docx | ✖️ | ✖️ | ✖️ |
| 2019암호경진대회\_5번\_답안지\_홍길동\_OOO학교.docx | ✖️ | ✖️ | ✖️ |
| and\_bc\_and\_a.bmp | ✖️ | ✖️ | ✖️ |
| and\_bc\_or\_a.bmp | ✖️ | ✖️ | ✖️ |
| and\_ab\_xor\_c.bmp | ✖️ | ✖️ | ✖️ |
| 복구율 | 6.1% | 18.2% | 6.1% |

## 2.2 UFS explorer Test

* 

|  |  |  |  |
| --- | --- | --- | --- |
|  | 쓰레기통 비움 | 쓰레기통 안 비움 | rm으로 삭제 |
| 참가자정보.xlsx | Δ(파일 이름만 존재) | Δ(파일 이름만 존재) | ✖️ |
| 2.py | ✖️ | ✖️ | ✖️ |
| 3.py | ✖️ | ✖️ | ✖️ |
| 7.py | ✖️ | ✖️ | ✖️ |
| 201520890\_박세환.pptx | ✖️ | ✖️ | ✖️ |
| 개인 프로젝트.pptx | ⚪ | ✖️ | ⚪ |
| 9조\_현성사\_혼전성관계에대한인식.pptx | ⚪ | ✖️ | ⚪ |
| Report2.pdf | ✖️ | ✖️ | ✖️ |
| Assignment3-MyLock-ko.pdf | ✖️ | ✖️ | ✖️ |
| 19.04.12\_보안프로젝트\_랜섬웨어\_성진.pdf | ✖️ | ✖️ | ✖️ |
| Report.pdf | ✖️ | ✖️ | ✖️ |
| Assignment-Mysh2.pdf | ✖️ | ✖️ | ✖️ |
| 20191124\_234139.jpg | ✖️ | ✖️ | ✖️ |
| 20190917\_105817.pdf | ✖️ | ✖️ | ✖️ |
| 20191111\_135421.jpg | ✖️ | ✖️ | ✖️ |
| 20191108\_111723.jpg | ✖️ | ✖️ | ✖️ |
| 20191124\_234145.jpg | ✖️ | ✖️ | ✖️ |
| ubuntu-18.04.1-desktop-amd64.iso | ✖️ | ✖️ | ✖️ |
| 공부 스터디 7-1주차.hwp | ✖️ | ✖️ | ✖️ |
| 공부 스터디 2주차.hwp | ✖️ | ✖️ | ✖️ |
| 공부 스터디 8주차-1.hwp | ✖️ | ✖️ | ✖️ |
| 공부 스터디 10주차-1-1.hwp | ✖️ | ✖️ | ✖️ |
| 공부 스터디 9주차-1.hwp | ✖️ | ✖️ | ✖️ |
| 5dbb99d534d4d.gif | ✖️ | ✖️ | ✖️ |
| 5dcb4ce53f3ea.gif | ✖️ | ✖️ | ✖️ |
| 5dc3bab4be08.gif | ✖️ | ✖️ | ✖️ |
| 보안프로젝트 2번째.docx | ✖️ | ✖️ | ✖️ |
| 랜섬웨어 구현 방향.docx | ✖️ | ✖️ | ✖️ |
| 링크 인턴 주간보고서.docx | ✖️ | ✖️ | ✖️ |
| 2019암호경진대회\_5번\_답안지\_홍길동\_OOO학교.docx | ✖️ | ✖️ | ✖️ |
| and\_bc\_and\_a.bmp | ✖️ | ✖️ | ✖️ |
| and\_bc\_or\_a.bmp | ✖️ | ✖️ | ✖️ |
| and\_ab\_xor\_c.bmp | ✖️ | ✖️ | ✖️ |
| 복구율 | 6.1% | 0% | 6.1% |

# **Result**

// 복구 결과 도구 비교 표(복구율, 복구 파일)

* 각 환경별 복구율 차이

(Recovery rate = 복구율 총합 / 전체 시도횟수)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **OS type** | **Kernel Version** | **Partition Size** | **Recovery rate** |
| **Dataset #1** | ubuntu 16.04 | 4.15.0.70-generic | 10GB |  |
| **Dataset #2** | ubuntu 18.04.3 LTS | 5.0.0-32-generic | 15GB |  |
| **Dataset #3** | Linux Mint 19.2 Tina | 4.15.0-54 | 20GB | 9.1% |
| **Dataset #4** | Debian GNU/Linux 9 | 4.9.0-6-amd64 | 15GB |  |

* 동 OS 환경 다른 kernel 밑 Partition Size에 따른 복구율 비교

(Recovery rate = 복구율 총합 / 전체 시도횟수)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **OS type** | **Kernel Version** | **Partition Size** | **Recovery rate** |
| **Dataset #1** | ubuntu 16.04 | 4.15.0.70-generic | 10GB |  |
| **Dataset #2** | ubuntu 18.04.3 LTS | 5.0.0-32-generic | 15GB |  |

* 각 환경별 복구한 파일 비교

//어떠한 파일을 복구해 냈는지.

* 각 Dataset 별 복구 tool에 따른 차이

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **R-studio** | | **UFS** | |
| **Dataset #1** |  |  |  |  |
| **Dataset #2** |  |  |  |  |
| **Dataset #3** | 11.1% |  | 6% | 개인 프로젝트.pptx |
| **Dataset #4** |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  | **R-studio** | 복원된 데이터 | **UFS** | **복원된 데이터** |
| **Dataset #1** | 휴지통 비우기 | 0% | 없음(0KB로 복원) | 96.7% | ubuntu-18.04.1-desktop-amd64.iso 제외 모든 데이터 |
| 비우기 x | 100% | 전체 | 96.7% | ubuntu-18.04.1-desktop-amd64.iso 제외 모든 데이터 |
| Rm | 0% | 없음(0KB로 복원) | 0% | 없음 |
| **Dataset #2** | 휴지통 비우기 | 81% | 전체 or 디스크 할당 크기 | 55% | 전체 or 디스크 할당 크기 |
| 비우기 x | 81% | 전체 or 디스크 할당 크기 | 55% | 전체 or 디스크 할당 크기 |
| Rm | 81% | 전체 or 디스크 할당 크기 | 55% | 전체 or 디스크 할당 크기 |
| **Dataset #3** | 휴지통 비우기 | 6.1% | 참가자정보.xlsx ,개인 프로젝트.pptx, 9조\_현성사\_혼전성관계에대한인식.pptx | 9.1% | 참가자정보.xlsx, 개인 프로젝트.pptx, 9조\_현성사\_혼전성관계에대한인식.pptx |
| 비우기 x | 18.2% | 참가자정보.xlsx, 2.py, 3.py, 7.py, 201520890\_박세환.pptx, 개인 프로젝트.pptx, 9조\_현성사\_혼전성관계에대한인식.pptx | 3% | 참가자정보.xlsx |
| Rm | 6.1% | 개인 프로젝트.pptx, 9조\_현성사\_혼전성관계에대한인식.pptx | 6.1% | 개인 프로젝트.pptx, 9조\_현성사\_혼전성관계에대한인식.pptx |
| **Dataset #4** | 휴지통 비우기 | 15% | jpg | 15% | jpg파일만 복구됨 |
| 비우기 x | 15% | jpg | 15% | jpg파일만 복구됨 |
| Rm | 15% | jpg | 15% | jpg파일만 복구됨 |

# 1. R-studio Testing Statistics

//R-studio 사용 결과 3개를 복구율, 복구 파일로 통계 내고 의미를 찾아낸다

# 2. UFS explorer Testing Statistics

//UFS explorer 사용 결과 3개를 복구율, 복구 파일로 통계 내고 의미를 찾아낸다

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **R-studio 7.1** | | | **UFS explorer 5.18.1** | | |
| 휴지통 | 휴지통비우기 | rm | 휴지통 | 휴지통비우기 | rm |
| **Dataset #1** | 100% | 0% | 0% | 96.7% | 96.7% | 6.6% |
| **Dataset #2** | 81.8% | 81.8% | 81.8% | 54.6% | 54.6% | 54.6% |
| **Dataset #3** | 19.8% | 6.6% | 6.6% | 3.3% | 9.9% | 6.6% |
| **Dataset #4** | 6.6% | 19.8% | 6.6% | 6.6% | 0% | 6.6% |

[표 3]복구 툴 별, 데이터 셋에서의 삭제 방식에 따른 복구율

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **R-studio 7.1** | | | **UFS explorer 5.18.1** | | |
| 휴지통 | 휴지통비우기 | rm | 휴지통 | 휴지통비우기 | rm |
| **Dataset #1** | 33개 | 0개 | 0개 | 32개 | 32개 | 2개 |
| **Dataset #2** | 27개 | 27개 | 27개 | 18개 | 18개 | 18개 |
| **Dataset #3** | 6개 | 2개 | 2개 | 1개 | 3개 | 2개 |
| **Dataset #4** | 2개 | 6개 | 2개 | 2개 | 0개 | 2개 |