OPERATING SYSTEMS

DIRECTORY MONITORING PROJECT TESTING & OUTCOMES

BENIAMIN-EMANUEL IMBRESCU

Overview

- Directories used for testing

TEST1

```
├── Beniamin-Imbrescu-CV.pdf
├── Carnet Student.pdf
├── Competențe Digitale.pdf
├── COMPETENȚE LINGVISTICE.pdf
├── semnatura.png
├── SV00086933600_2023_10.pdf
├── WhatsApp Image 2023-12-27 at 19.00.02.jpeg
└── _.zip

1 directory, 8 files
```

TEST2

```
├── (1) Computer Programming
│   ├── CP - Arrays.pdf
│   ├── CP - BItwise operations.pdf
│   ├── CP - Characters.pdf
│   ├── CP  - Conditional execution.pdf
│   ├── CP - DynamicAllocation.pdf
│   ├── CP - Files.pdf
│   ├── CP - Introduction.pdf
│   ├── CP - IO.pdf
│   ├── CP - Iterations.pdf
│   ├── CP - Pointers.pdf
│   ├── CP - Recursion.pdf
│   ├── CP - Strings.pdf
│   ├── CP - Structures.pdf
│   ├── EXAM MODELS
│   │   ├── ilovepdf_merged (4).pdf
│   │   ├── midterm2024-pb2.c
│   │   ├── p1.c
│   │   └── p2.c
│   ├── LAB MATERIALS
│   │   ├── LAB11-12CPEXTRA.png
│   │   ├── LAB11-12CPP1.png
│   │   ├── LAB11-12CPP2.png
│   │   ├── LAB2CP.png
│   │   ├── LAB3CP.png
│   │   ├── LAB4CP.png
│   │   ├── LAB6CP.png
│   │   ├── LAB8CPEXTRA.png
│   │   ├── LAB8CPP1.png
│   │   ├── LAB8CPP2.png
│   │   ├── LAB9CPP1.png
│   │   └── LAB9CPP2.png
│   └── LABURI CP - ROMANA
│       ├── Laborator 02 - Programarea calculatoarelor.pdf
│       ├── Laborator 03 - Programarea calculatoarelor.pdf
│       ├── Laborator 04 - Programarea calculatoarelor.pdf
│       ├── Laborator 05 - Programarea calculatoarelor.pdf
│       ├── Laborator 06 - Programarea calculatoarelor.pdf
│       ├── Laborator 07 - Programarea calculatoarelor.pdf
│       ├── Laborator 08 - Programarea calculatoarelor.pdf
│       ├── Laborator 09 - Programarea calculatoarelor.pdf
│       └── Laborator 10 - Programarea calculatoarelor.pdf
├── (2) Databases
│   ├── AirportData.txt
│   ├── AirportSchema.txt
│   ├── apex-overview-otn-4491378.pdf
│   ├── DB2_C10_DataOrg.pdf
│   ├── DB2_C1_RelationalModel.pdf
│   ├── DB2_C2_SQL_DDL.pdf
│   ├── DB2_C3_BasicSQL.pdf
│   ├── DB2_C4_Subqueries.pdf
│   ├── DB2_C5_Aggregation.pdf
│   ├── DB2_C6_APEX.pdf
│   ├── DB2_C7_PHP.pdf
│   ├── DB2_C8_DataModeling.pdf
│   ├── DB2_C9_RelAlgebra.pdf
│   ├── DB_Harbour-20231026.zip
│   ├── DB PROJECT.pdf
│   ├── LABS
│   │   ├── aggregation.pdf
│   │   ├── db_labs.txt
│   │   ├── L2.DDL.pdf
│   │   ├── L3.SELECT.pdf
│   │   ├── L4.Joins.pdf
│   │   ├── L5.Subqueries.pdf
│   │   ├── L6.SetOps.pdf
│   │   ├── L7.Aggregation.pdf
│   │   ├── L8.AppBuilder.pdf
│   │   └── L9.DB_Projects.pdf
│   └── UNIVERSITY database (create, populate, drop)-20231030
│       ├── db_university_data.sql
│       ├── db_university_drop.sql
│       └── db_university_schema_complete.sql
├── AC.LM6.04.2.LM613767-anexa-semnata.pdf
├── Computer Networks - Homework 2.pdf
├── Control System of a Car.pdf
└── homework_addressing.pdf

8 directories, 70 files
```

TEST3

```
├── BTree.java
└── test3

1 directory, 2 files
```

- Snapshot Creation

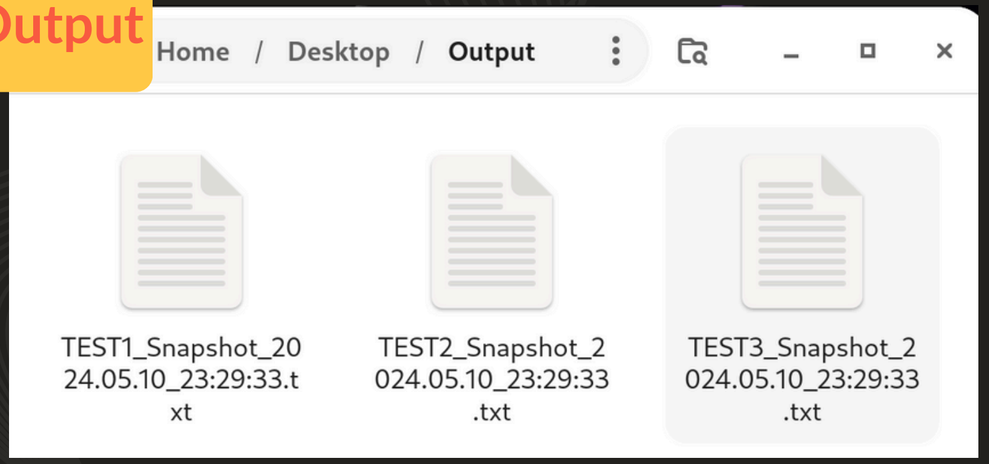
```
sh-5.2$ ./run_final_build -o /home/stikeez_/Desktop/Output -s /home/stikeez_/Desktop/Isola
ted /home/stikeez_/Desktop/TEST1 /home/stikeez_/Desktop/TEST2 /home/stikeez_/Desktop/TEST3


(Creating) Snapshot created successfully for  "TEST1"  in 0.00038 (s)
(Creating) Snapshot created successfully for  "TEST3"  in 0.00016 (s)
(Comparing) No snapshots were previously created for  "TEST1"
Child Process 1 terminated with PID 5630 and 0 files with potential danger for  "TEST1"
(Comparing) No snapshots were previously created for  "TEST3"
Child Process 3 terminated with PID 5632 and 0 files with potential danger for  "TEST3"


(Creating) Snapshot created successfully for  "TEST2"  in 0.002996 (s)
(Comparing) No snapshots were previously created for  "TEST2"
Child Process 2 terminated with PID 5631 and 0 files with potential danger for  "TEST2"
```

All the snapshot are created in the Output Directory.

If the Output Directory, given as argument in the terminal, does not exist, it will be created automatically (The same functionality is applied to the Isolated Directory).

• Snapshot Creation

Output



A snapshot contains information regarding all files and sub-directories within the monitored directory.

Open

TEST2_Snapshot_2024.05.10_23:29:33.txt
~/Desktop/Output

```
Path: /home/stikeez_/Desktop/TEST2/(1) Computer Programming
Size: 590 bytes
Access Rights: rwx rwx rwx
Hard Links: 1

Path: /home/stikeez_/Desktop/TEST2/(1) Computer Programming/LABURI CP - ROMANA
Size: 828 bytes
Access Rights: rwx r-x r-x
Hard Links: 1

Path: /home/stikeez_/Desktop/TEST2/(1) Computer Programming/LABURI CP - ROMANA/Laborator 09 - Programarea calculatoarelor.pdf
Size: 173132 bytes
Access Rights: rw- r-- r--
Hard Links: 1

Path: /home/stikeez_/Desktop/TEST2/(1) Computer Programming/LABURI CP - ROMANA/Laborator 07 - Programarea calculatoarelor.pdf
Size: 205492 bytes
Access Rights: rw- r-- r--
Hard Links: 1

Path: /home/stikeez_/Desktop/TEST2/(1) Computer Programming/LABURI CP - ROMANA/Laborator 04 - Programarea calculatoarelor.pdf
Size: 164243 bytes
Access Rights: rw- r-- r--
Hard Links: 1

Path: /home/stikeez_/Desktop/TEST2/(1) Computer Programming/LABURI CP - ROMANA/Laborator 10 - Programarea calculatoarelor.pdf
Size: 193427 bytes
Access Rights: rw- r-- r--
Hard Links: 1

Path: /home/stikeez_/Desktop/TEST2/(1) Computer Programming/LABURI CP - ROMANA/Laborator 02 - Programarea calculatoarelor.pdf
Size: 339690 bytes
Access Rights: rw- r-- r--
Hard Links: 1
```

• Snapshot Comparation

```
sh-5.2$ ./run_final_build -o /home/stikeez_/Desktop/Output -s /home/stikeez_/Desktop/Isola
ted /home/stikeez_/Desktop/TEST1 /home/stikeez_/Desktop/TEST2 /home/stikeez_/Desktop/TEST3


(Creating) Snapshot created successfully for  "TEST1"  in 0.00038 (s)
(Creating) Snapshot created successfully for  "TEST3"  in 0.00016 (s)
(Comparing) No snapshots were previously created for  "TEST1"
Child Process 1 terminated with PID 5630 and 0 files with potential danger for  "TEST1"
(Comparing) No snapshots were previously created for  "TEST3"
Child Process 3 terminated with PID 5632 and 0 files with potential danger for  "TEST3"


(Creating) Snapshot created successfully for  "TEST2"  in 0.002996 (s)
(Comparing) No snapshots were previously created for  "TEST2"
Child Process 2 terminated with PID 5631 and 0 files with potential danger for  "TEST2"
```

If the Output Directory was empty or non-existent no comparation will be made. Only a message will be printed

```
sh-5.2$ ./run_final_build -o /home/stikeez_/Desktop/Output -s /home/stikeez_/Desktop/Isolate
d /home/stikeez_/Desktop/TEST1 /home/stikeez_/Desktop/TEST2 /home/stikeez_/Desktop/TEST3


(Creating) Snapshot created successfully for  "TEST1"  in 0.000427 (s)
(Comparing) No differences found between the current and the previous snapshot for  "TEST1"
(Creating) Snapshot created successfully for  "TEST3"  in 0.000219 (s)
Child Process 1 terminated with PID 5789 and 0 files with potential danger for  "TEST1"
(Comparing) No differences found between the current and the previous snapshot for  "TEST3"
Child Process 3 terminated with PID 5791 and 0 files with potential danger for  "TEST3"


(Creating) Snapshot created successfully for  "TEST2"  in 0.003354 (s)
(Comparing) No differences found between the current and the previous snapshot for  "TEST2"
Child Process 2 terminated with PID 5790 and 0 files with potential danger for  "TEST2"
```

If the Output Directory contains a previous snapshot, then a comparation is made between the previous and the current. If the snapshots are identical, the previous one is deleted and a message is printed

• Snapshot Comparation


```
├── Beniamin-Imbrescu-CV.pdf
├── Carnet Student.pdf
├── Competențe Digitale.pdf
├── COMPETENTE LINGVISTICE.pdf
├── semnatura.png
├── SV00086933600_2023_10.pdf
├── WhatsApp Image 2023-12-27 at 19.00.02.jpeg
└── _.zip

1 directory, 8 files
```

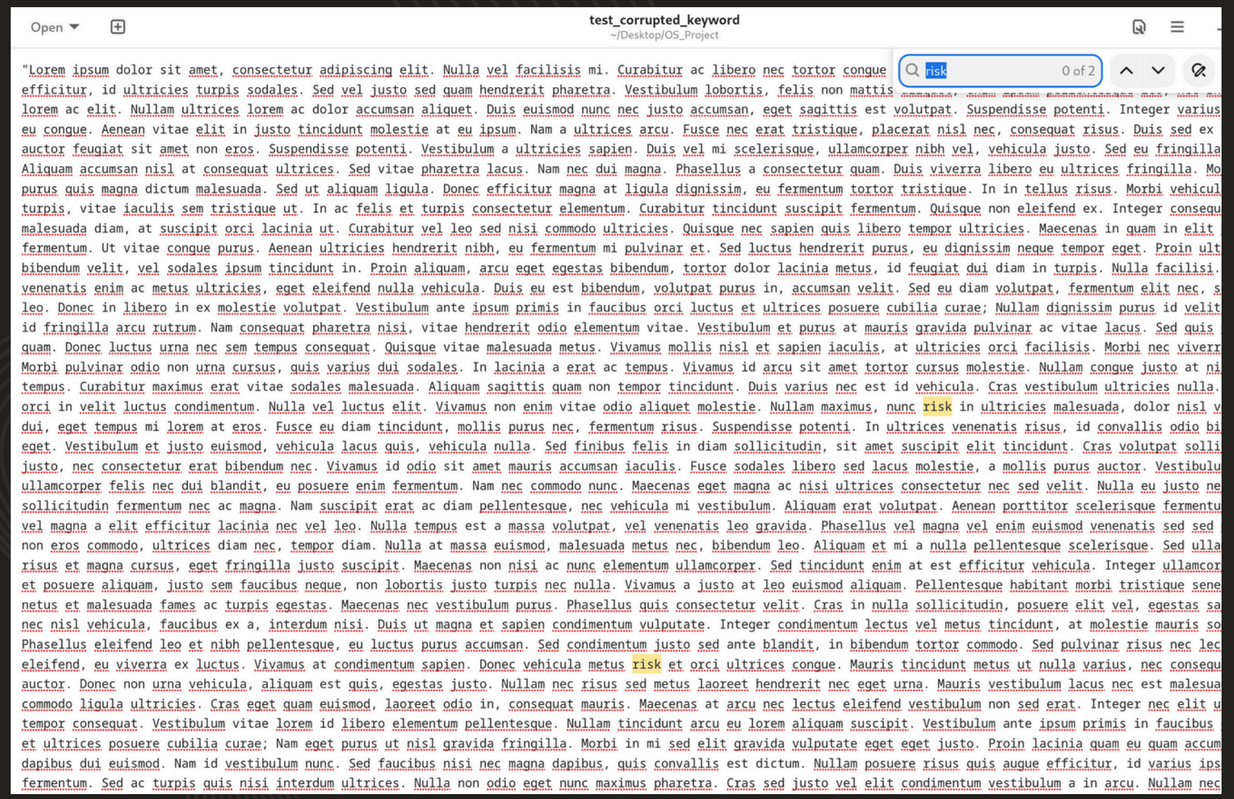
```
├── Beniamin-Imbrescu-CV.pdf
├── Carnet Student.pdf
├── Competențe Digitale.pdf
├── COMPETENȚE LINGVISTICE.pdf
├── SV00086933600_2023_10.pdf
├── WhatsApp Image 2023-12-27 at 19.00.02.jpeg
└── _.zip

1 directory, 7 files
```

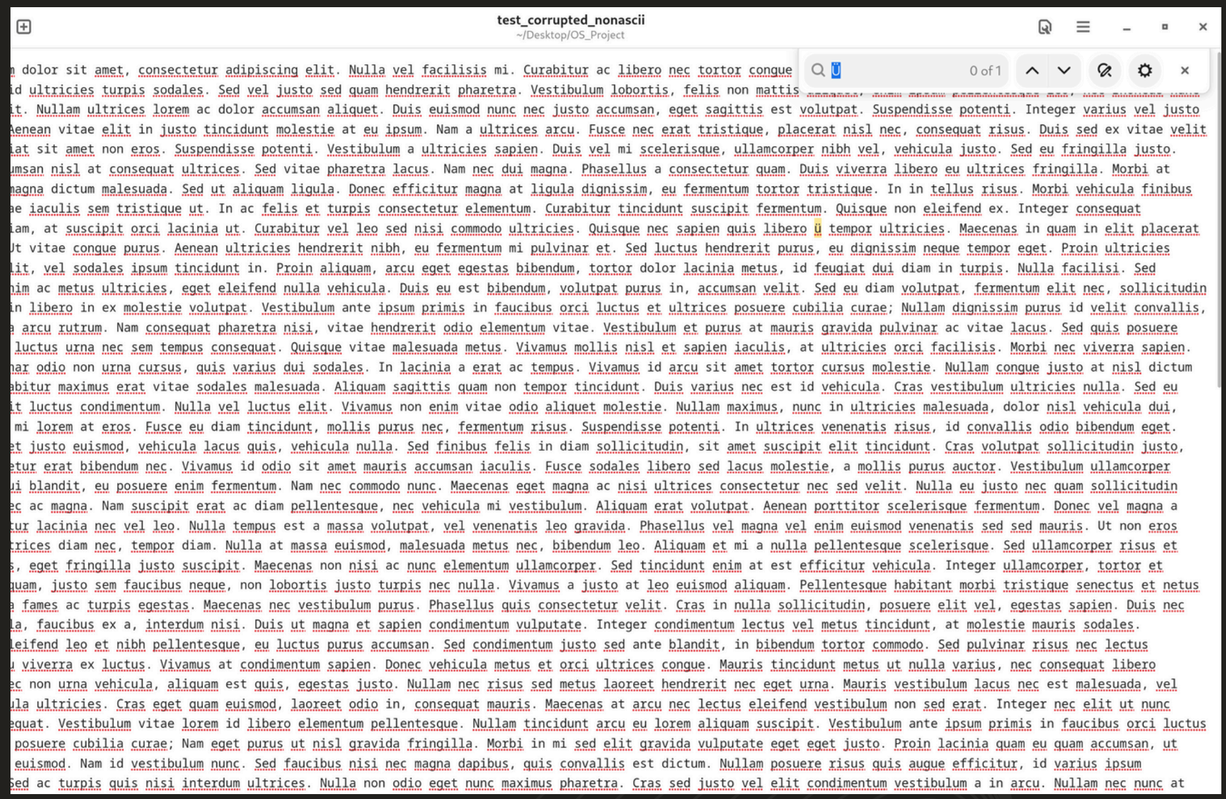
Let's delete an element from TEST1 directory and see the results

```
sh-5.2$ ./run_final_build -o /home/stikeez_/Desktop/Output -s /home/stikeez_/Desktop/Isolated /home/
stikeez_/Desktop/TEST1 /home/stikeez_/Desktop/TEST2 /home/stikeez_/Desktop/TEST3


(Creating) Snapshot created successfully for  "TEST1"  in 0.000378 (s)
(Creating) Snapshot created successfully for  "TEST3"  in 0.00014 (s)
(Comparing) Difference found between the current and the previous snapshot => Overriding the previou
s snapshot for  "TEST1"
(Comparing) No differences found between the current and the previous snapshot for  "TEST3"
Child Process 3 terminated with PID 5880 and 0 files with potential danger for  "TEST3"
Child Process 1 terminated with PID 5878 and 0 files with potential danger for  "TEST1"


(Creating) Snapshot created successfully for  "TEST2"  in 0.002997 (s)
(Comparing) No differences found between the current and the previous snapshot for  "TEST2"
Child Process 2 terminated with PID 5879 and 0 files with potential danger for  "TEST2"
```

When the snapshots are compared the program behaves differently. Now the previous snapshot is overriden and a different message is printed

- Introducing corrupted files

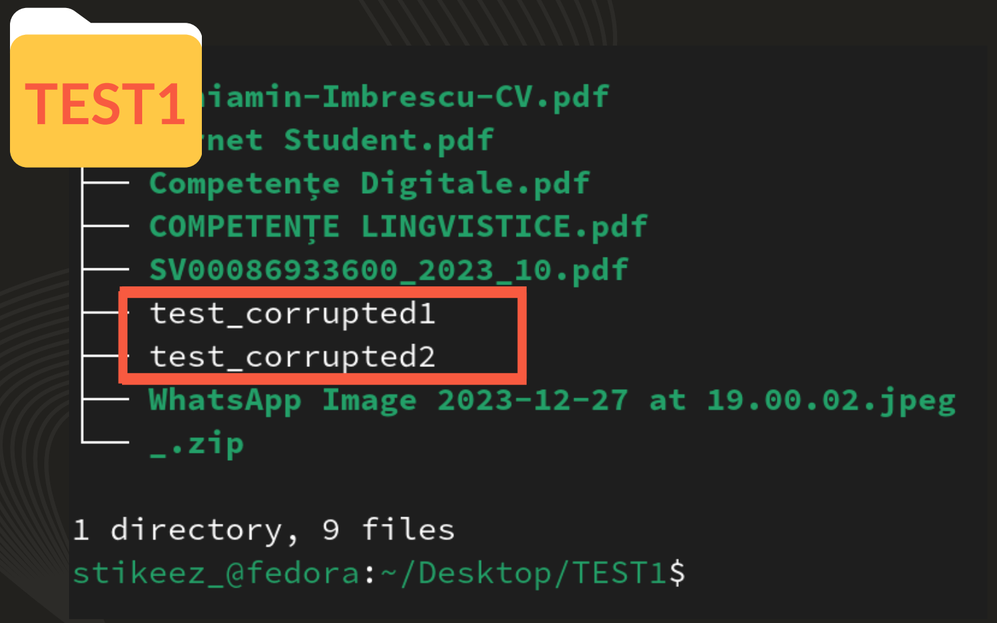


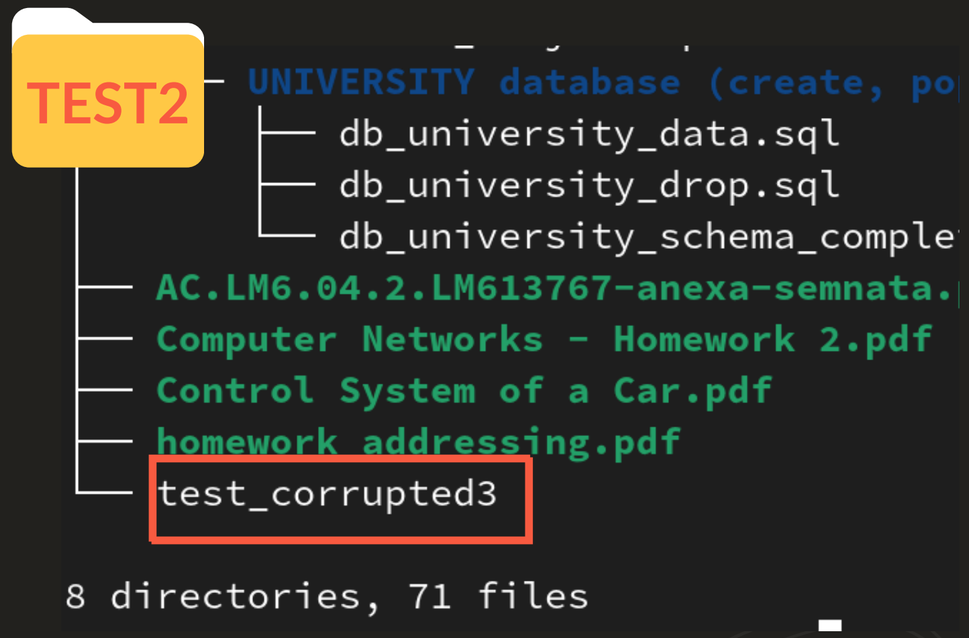


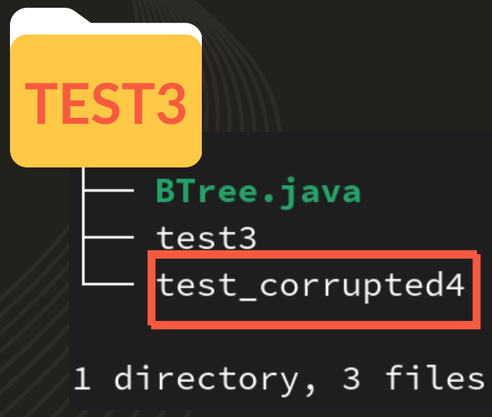
The files above meet the requirements to be considered suspicious (< 3 && > 999 words && > 1999 characters)

The first file contains the keyword “risk” and the second file the non-ascii character “Ü” => Both files would be considered corrupted when testing

- Introducing corrupted files







In every directory, a file with no access rights was added

test_corrupted1 - corrupted (contains keyword)

test_corrupted2 - regular file without acces rights

test_corrupted3 - corrupted (contains non-ascii characted)

test_corrupted4 - suspicius but not corrupted

- Syntactic Analysis

```
(Checking Permissions) "test_corrupted4" from "TEST3" has no access rights => Performing Syntactic Anaysis!
(Checking Permissions) "test_corrupted2" from "TEST1" has no access rights => Performing Syntactic Anaysis!
(Checking Permissions) "test_corrupted3" from "TEST2" has no access rights => Performing Syntactic Anaysis!
(Syntactic Analysis) "test_corrupted2" from "TEST1" is SAFE!
Grandchild Process 3.1 terminated with PID 3286 and exit code 3289 for file  "test_corrupted2"  from  "TEST1"

(Checking Permissions) "test_corrupted1" from "TEST1" has no access rights => Performing Syntactic Anaysis!
(Syntactic Analysis) "test_corrupted4" is suspicious after analyzing the number of lines, words, and characters.
(Syntactic Analysis) "test_corrupted3" is suspicious after analyzing the number of lines, words, and characters.
(Syntactic Analysis) "test_corrupted3" contains keyword: risk
(Syntactic Analysis) "test_corrupted3" from "TEST2" is malicious or corrupted => Moving it to the isolated directory!
Grandchild Process 2.1 terminated with PID 3285 and exit code 3291 for file  "test_corrupted3"  from  "TEST2"

(Syntactic Analysis) "test_corrupted1" is suspicious after analyzing the number of lines, words, and characters.
(Creating) Snapshot created successfully for  "TEST2"  in 0.004646 (s)
(Comparing) Difference found between the current and the previous snapshot => Overriding the previous snapshot for  "TEST2"
Child Process 2 terminated with PID 3285 and 1 files with potential danger for  "TEST2"

(Syntactic Analysis) "test_corrupted4" from "TEST3" is SAFE!
Grandchild Process 1.1 terminated with PID 3284 and exit code 3287 for file  "test_corrupted4"  from  "TEST3"

(Creating) Snapshot created successfully for  "TEST3"  in 0.000773 (s)
(Comparing) Difference found between the current and the previous snapshot => Overriding the previous snapshot for  "TEST3"
Child Process 1 terminated with PID 3284 and 0 files with potential danger for  "TEST3"

(Syntactic Analysis) "test_corrupted1" contains non-ASCII characters.
(Syntactic Analysis) "test_corrupted1" from "TEST1" is malicious or corrupted => Moving it to the isolated directory!
Grandchild Process 3.2 terminated with PID 3286 and exit code 3312 for file  "test_corrupted1"  from  "TEST1"

(Creating) Snapshot created successfully for  "TEST1"  in 0.001566 (s)
(Comparing) Difference found between the current and the previous snapshot => Overriding the previous snapshot for  "TEST1"
Child Process 3 terminated with PID 3286 and 1 files with potential danger for  "TEST1"
```

- Syntactic Analysis

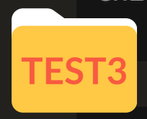
Running again the program and we can see that the malicious files were moved (only the safe ones remained in the directories

```
(Checking Permissions) "test_corrupted4" from "TEST3" has no access rights => Performing Syntactic Anaysis!
(Checking Permissions) "test_corrupted2" from "TEST1" has no access rights => Performing Syntactic Anaysis!
(Creating) Snapshot created successfully for  "TEST2"  in 0.003675 (s)
(Comparing) Difference found between the current and the previous snapshot => Overriding the previous snapshot for  "TEST2"
Child Process 2 terminated with PID 3394 and 0 files with potential danger for  "TEST2"

(Syntactic Analysis) "test_corrupted2" from "TEST1" is SAFE!
Grandchild Process 3.1 terminated with PID 3395 and exit code 3398 for file  "test_corrupted2"  from  "TEST1"

(Creating) Snapshot created successfully for  "TEST1"  in 0.001056 (s)
(Comparing) Difference found between the current and the previous snapshot => Overriding the previous snapshot for  "TEST1"
Child Process 3 terminated with PID 3395 and 0 files with potential danger for  "TEST1"

(Syntactic Analysis) "test_corrupted4" is suspicious after analyzing the number of lines, words, and characters.
(Syntactic Analysis) "test_corrupted4" from "TEST3" is SAFE!
Grandchild Process 1.1 terminated with PID 3393 and exit code 3396 for file  "test_corrupted4"  from  "TEST3"

(Creating) Snapshot created successfully for  "TEST3"  in 0.00076 (s)
(Comparing) Difference found between the current and the previous snapshot => Overriding the previous snapshot for  "TEST3"
Child Process 1 terminated with PID 3393 and 0 files with potential danger for  "TEST3"
```

- Errors

If a directory is monitored at runtime more than once, there is a chance of error. Because the processess are running in parallel, in one process, the previous snapshot is deleted from the output directory and exactly at that time the other process is trying searching for it

```
(Checking Permissions) "test_corrupted4" from "TEST3" has no access rights => Performing Syntactic Anaysis!
(Checking Permissions) "test_corrupted4" from "TEST3" has no access rights => Performing Syntactic Anaysis!
(Syntactic Analysis) "test_corrupted4" is suspicious after analyzing the number of lines, words, and characters.
(Syntactic Analysis) "test_corrupted4" is suspicious after analyzing the number of lines, words, and characters.
(Syntactic Analysis) "test_corrupted4" from "TEST3" is SAFE!
(Syntactic Analysis) "test_corrupted4" from "TEST3" is SAFE!
Grandchild Process 1.1 terminated with PID 3947 and exit code 3950 for file  "test_corrupted4"  from  "TEST3"

Grandchild Process 2.1 terminated with PID 3948 and exit code 3949 for file  "test_corrupted4"  from  "TEST3"

(Creating) Snapshot created successfully for  "TEST3"  in 0.000955 (s)
(Creating) Snapshot created successfully for  "TEST3"  in 0.000832 (s)
(Comparing) No differences found between the current and the previous snapshot for  "TEST3"
(Comparing) No differences found between the current and the previous snapshot for  "TEST3"
Child Process 2 terminated with PID 3948 and 0 files with potential danger for  "TEST3"
Child Process 1 terminated with PID 3947 and 0 files with potential danger for  "TEST3"
```




```
(Checking Permissions) "test_corrupted4" from "TEST3" has no access rights => Performing Syntactic Anaysis!
(Checking Permissions) "test_corrupted4" from "TEST3" has no access rights => Performing Syntactic Anaysis!
(Syntactic Analysis) "test_corrupted4" is suspicious after analyzing the number of lines, words, and characters.
(Syntactic Analysis) "test_corrupted4" is suspicious after analyzing the number of lines, words, and characters.
(Syntactic Analysis) "test_corrupted4" from "TEST3" is SAFE!
Grandchild Process 1.1 terminated with PID 4025 and exit code 4027 for file  "test_corrupted4"  from  "TEST3"

(Creating) Snapshot created successfully for  "TEST3"  in 0.000733 (s)
(Comparing) No differences found between the current and the previous snapshot for  "TEST3"
(Syntactic Analysis) "test_corrupted4" from "TEST3" is SAFE!
Child Process 1 terminated with PID 4025 and 0 files with potential danger for  "TEST3"
Grandchild Process 2.1 terminated with PID 4026 and exit code 4028 for file  "test_corrupted4"  from  "TEST3"


(Creating) Snapshot created successfully for  "TEST3"  in 0.00064 (s)
(Comparing) No snapshots were previously created for  "TEST3"
Child Process 2 terminated with PID 4026 and 0 files with potential danger for  "TEST3"
```

Wrong!