

[DFRWS- 2021-Raspberry PI] Write-Up

작성자	TeamA
분석 일자	2024-06-08
작성 일자	2024-06-09
분석 대상	2-Raspberry_Pi_mSD.zip
문서 버전	1.0
작성자 E-mail	rlarudals877@gmail.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. Reference9

1. 문제

URL	-
문제 내용	1. Establishing whether the Raspberry Pi has been used to control the 3D printer. 2. Establishing whether objects of possible illicit use have been printed, when and which ones.
문제 파일	 2-Raspberry_Pi_mSD
문제 유형	System forensics
난이도	3/ 3

2. 분석 도구

도구명	다운로드 링크	Version
FTK Imager	FTK Imager Version 4.7.1 (exterro.com)	4.7

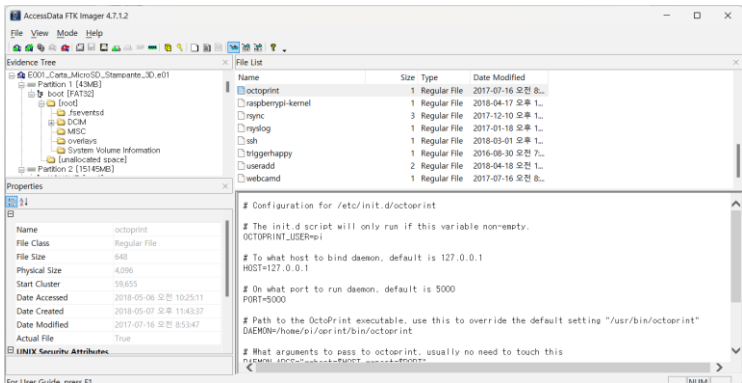
3. 환경

OS
Window 11 64 bit

4. Write-Up

파일명	E001_Carta_MicroSD_Stampante_3D.e01
용량	2.01GB
SHA256	1f6420581b901d647d98cb6fd1a4c6c8802f6a83a88ea4003405fa46b30e72a9
Timestamp	2021-07-29 2:33:00

[Establishing whether the Raspberry Pi has been used to control the 3D printer.]



[사진 1] ftk로 주어진 파일을 열어본 모습

먼저 주어진 파일을 FTK 로 열어보았다. 열어보면 파티션의 정보가 나와 있었다.

```
20:34:44.306 - octoprint.plugins.discovery - INFO - Registered 'OctoPrint instance "Cthulhuuuu's 3D Printer",_octoprint._tcp.local.' for _octoprint._tcp.local.
20:34:44.315 - octoprint.plugins.discovery - INFO - Registered OctoPrint instance "Cthulhuuuu's 3D Printer" for SSDP
20:34:44.372 - octoprint.server - INFO - Listening on http://127.0.0.1:5000
```

[사진 2] 3D print를 제어한 모습

주어진 파일을 탐색 중 파티션에 있는 home 파일을 발견했다. 해당 폴더를 살펴보면 print에 관련된 내용이 들어있었다. 폴더를 열어서 확인해보면 **octoprint.log** 파일이 나와있다. 내용을 보니 이 라즈베리 파이가 어떻게 쓰였는지가 나와있었다. 자세히 보니 3D 프린터로 사용된 기록이 있었다.

따라서 ./Partition 2/home/logs/ 디렉토리의 **octopint.log** 에 라즈베리 파이가 3D 프린터를 제어하는 데 사용되었다는 로그가 나와 있다.

[WHS-2] .iso














[Establishing whether objects of possible illicit use have been printed, when and which ones.]

위의 파일과 같은 디렉토리에 있는 octoprint_stats.json 파일을 열어보았다. 열어본 결과 PRINT_STARTED 라는 문구를 발견할 수 있었다. 따라서 무엇이 프린트가 시작되었는지 알면 프린트 결과물이 불법인지 아닌지 있을 것 같아 좀 더 살펴보았다.

```
"tool1_volume": 0, "tool2_length": 0, "tool2_actual": 0, "tool0_volume": 6.073179454425881,
"tool0_length": 859.1791381831281, "file": "VK_Spring.gcode", "tool0_actual": 187.0, "owner":
"arnimzola", "tool1_actual": 0, "size": 1157637, "tool2_volume": 0, "tool1_length": 0, "name":
"VK_Spring.gcode", "event_type": "PRINT_DONE", "418": {"data": {"origin": "local", "name":
"VK_frame(no_sn).gcode", "event_time": "2021-04-14 06:26:16.921332", "bed_target": 0.0,
"tool2_target": 0, "tool1_target": 0, "file": "VK_frame(no_sn).gcode", "owner": "arnimzola",
"size": 6747786, "tool0_target": 200.0, "user": "arnimzola", "event_type": "PRINT_STARTED",
"419": {"data": {"event_time": "2021-04-14 06:26:17.139730", "name": "VK_frame(no_sn).gcode",
"file": "VK_frame(no_sn).gcode", "target": "local", "event_type": "UPLOAD", "420": {"data":
{"origin": "local", "bed_actual": 0.0, "ptime": 28931.773657227, "event_time": "2021-04-14
14:28:29.087254", "tool1_volume": 0, "tool2_length": 0, "name": "VK_frame(no_sn).gcode",
"tool2_actual": 0, "tool0_volume": 199.53370683930143, "file": "VK_frame(no_sn).gcode",
"tool0_actual": 191.7, "owner": "arnimzola", "tool1_actual": 0, "size": 6747786, "tool2_volume":
0, "tool1_length": 0, "tool0_length": 28228.24511726573, "event_type": "PRINT_DONE", "421":
{"data": {"origin": "local", "name": "VK_Spring.gcode", "event_time": "2021-04-14
15:01:51.151617", "user": "arnimzola", "bed_target": 0.0, "tool2_target": 0, "tool1_target": 0,
"file": "VK_Spring.gcode", "owner": "arnimzola", "tool0_target": 0.0, "size": 1157637,
"event_type": "PRINT_STARTED", "422": {"data": {"origin": "local", "bed_actual": 0.0, "ptime":
1674.762556282003, "event_time": "2021-04-14 15:29:46.340420", "tool1_volume": 0, "tool2
_length": 0, "name": "VK_Spring.gcode", "tool2_actual": 0, "tool0_volume": 6.073179454425881
"file": "VK_Spring.gcode", "tool0_actual": 187.9, "owner": "arnimzola", "tool1_actual": 0, "size":
1157637, "tool2_volume": 0, "tool1_length": 0, "tool0_length": 859.1791381831281},
```

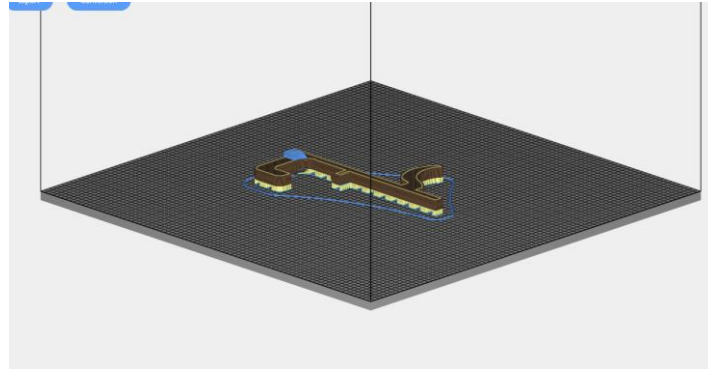
[사진 3] octoprint_stats.json 파일 내부 모습

위의 파일에서 name 옆에 있는 gcode가 무엇이 출력되었는지 나타낼 것 같아 gcode가 어디 있는지 살펴보았다. uploads라는 폴더에 있었다.

 .metadata.json	2C
 VK_20mm_cube_soft_edges.gcode	2C
 VK_380_barrel_(threaded).gcode	2C
 VK_2050938e-3012-4227-9a47-c4c4f5...	2C
 VK_Apple_Watch_Dock_shell_-_thingi...	2C
 VK_Bed_Levelling_0_3.gcode	2C
 VK_bottom_cover.gcode	2C
 VK_cb90900a-a426-44e8-a446-6dfa8f...	2C
 VK_frame(no_sn).gcode	2C
 VK_iphone_dock_customizer_2015011...	2C
 VK_Spring.gcode	2C
 VK_Switch.STLgcode	2C
 VK_trigger.gcode	2C

[사진 4] gcode가 모여 있는 폴더

gcode 파일 중 이름이 수상해 보이는 파일이 있었다.



[사진 5] 수상한 gcode 실행

. 바로 **VK_trigger.gcode** 인데 이를 시뮬레이션 할 수 있는 사이트에 (<https://www.3dpea.com/en/gcode-simulator>) 업로드 해서 확인해봤다. 그 결과 다음과 같이 나왔다. 바로 총이었다. 총은 3D 프린터로 출력하면 안 되는 불법적인 물건 중 하나이다.

```
"UPLOAD"), "406": {"data": {"origin": "local", "name": "VK_trigger.gcode", "event_time":
"2021-04-13 15:17:32.016423", "bed_target": 0.0, "tool2_target": 0, "tool1_target": 0, "file":
"VK_trigger.gcode", "owner": "arnimzola", "size": 320487, "tool0_target": 200.0, "user":
"arnimzola", "event_type": "PRINT_STARTED"}, "407": {"data": {"origin": "local", "bed_actual":
0.0, "ptime": 892.5423338669989, "event_time": "2021-04-13 15:32:24.911512", "tool1
_volume": 0, "tool2_length": 0, "tool2_actual": 0, "tool0_volume": 4.3423640522069, "tool0
_length": 614.31884765625, "file": "VK_trigger.gcode", "tool0_actual": 188.7, "owner":
"arnimzola", "tool1_actual": 0, "size": 320487, "tool2_volume": 0, "tool1_length": 0, "name":
"VK_trigger.gcode"}, "event_type": "PRINT_DONE"), "408": {"data": {"file":
"VK_bottom_cover.gcode", "name": "VK_bottom_cover.gcode", "event_time": "2021-04-13
```

[사진 6] 총이 출력된 시점

이번에는 이 총이 언제 출력되었는지 확인해야 한다. 앞서 살펴봤던 octoprint_stats.json 파일을 보면 계속 총 출력이 실패되다가 성공한다. 그 시점은 [사진 6]의 빨간색 부분이다.

5. Flag

- 1. ./Partition 2/home/logs/octopint.log
- 2. 2021-04-13 15:32:24.911512

6. 별도 첨부

7. Reference

-