

# Digital Forensic Report

**Investigator:** CyberCrow

**Report Written by:** CyberCrow

**Case:** Suspected Raspberry Pi found on 3D printer

**Case id:** 202517061430

# Table of Content

<b>1. Introduction</b>	<b>3</b>
1.1 Description of the case	3
1.2 Statement of compliance	3
1.4 Objectives	4
<b>2 Evidence Collection and Handling:</b>	<b>4</b>
2.1 Chain of Custody	4
2.3 Imaging/Duplication Procedures	6
2.4 Hash Values	6
<b>3. Examination Methodology and Tools</b>	<b>7</b>
3.1 Examination Environment	7
3.2 Analytical Procedures	8
<b>4. Findings and Analysis</b>	<b>10</b>
<b>5. Conclusion</b>	<b>12</b>

# 1. Introduction

## 1.1 Description of the case

On April 18th, 2021 Italian authorities were discovered a laboratory, but most of the devices and manufacturing equipment were destroyed. However, a specialist from the Reparto Investigazioni Scientifiche (RIS) of the Carabinieri identified a Raspberry Pi, connected to a 3D printer, seemingly forgotten in the destruction process. A forensic copy of the microSD card of the Raspberry Pi was acquired and is available for download [here](#).

- Filename : [2\\_Raspberry\\_Pi\\_mSD.zip](#)
- SHA2-256 :  
aabec0c1305e785d1ba5b4ba01c5dacd27cc128fdd32078758be826e75449953

No traces of 3D printed objects were found on site. Given the presence of the 3D printer connected to the Raspberry Pi, particular attention should be given to:

- Establishing whether the Raspberry Pi has been used to control the 3D printer.
- Establishing whether objects of possible illicit use have been printed, when and which ones.

## 1.2 Statement of compliance

All procedures followed during the forensic process—including imaging, hashing, evidence handling, and analysis—were conducted using validated tools and standard operating procedures approved by our ISO/IEC-accredited quality management system.

A full chain of custody was maintained throughout the process to preserve evidence integrity. All actions taken during the examination are fully documented and reproducible.

## 1.4 Objectives

### Objective of the Investigation

The primary objectives of this digital forensic investigation are as follows:

- Establishing whether the Raspberry Pi has been used to control the 3D printer.
- Establishing whether objects of possible illicit use have been printed, when and which ones.

## 2 Evidence Collection and Handling:

### 2.1 Chain of Custody

**CyberGrang Investigation Lab**  
**EVIDENCE CHAIN OF CUSTODY TRACKING FORM**

Case Number: 2 Offense: Suspected Manufacturing of Illicit Devices.

Submitting Officer: (Name/ID#) the Scientific Investigations Department (RIS) of the Carabinieri

Victim: \_\_\_\_\_

Suspect: Arnim Zola

Date/Time Seized: \_\_\_\_\_ Location of Seizure: Aosta, Italy.

Description of Evidence		
Item #	Quantity	Description of Item (Model, Serial #, Condition, Marks, Scratches)
1	1	Image of SD card is inside the Raspberry Pi


Chain of Custody				
Item #	Date/Time	Released by (Signature & ID#)	Received by (Signature & ID#)	Comments/Location
1	2025/05/26	<u>Specialist from</u> <u>Scientific</u> <u>Investigations</u> <u>Department (RIS) of</u> <u>the Carabinieri.</u>	CyberCrow	laboratory, Aosta, Italy.

Final Disposal Authority
<p><b>Authorization for Disposal</b></p> <p>Item(s) #: _____ on this document pertaining to (suspect): _____  is(are) no longer needed as evidence and is/are authorized for disposal by (check appropriate disposal method)</p> <p><input type="checkbox"/> Return to Owner      <input type="checkbox"/> Auction/Destroy/Divert</p> <p>Name &amp; ID# of Authorizing Officer: _____ Signature: _____ Date: _____  _____</p>
<p style="text-align: center;"><b>Witness to Destruction of Evidence</b></p> <p>Item(s) #: _____ on this document were destroyed by Evidence Custodian _____ ID#: _____  in my presence on (date) _____.</p> <p>Name &amp; ID# of Witness to destruction: _____ Signature: _____ Date: _____  _____</p>

<b>Release to Lawful Owner</b>	
Item(s) #: _____ on this document was/were released by Evidence Custodian	
_____ ID#: _____ to	
Name _____	
Address: _____ City: _____ State: _____ Zip Code: _____	
Telephone Number: (____) _____	
Under penalty of law, I certify that I am the lawful owner of the above item(s).	
Signature: _____ Date: _____	
Copy of Government-issued photo identification is attached. <input type="checkbox"/> Yes <input type="checkbox"/> No	
<b>This Evidence Chain-of-Custody form is to be retained as a permanent record by the Anywhere Police Department.</b>	

APD\_Form\_#PE003\_v.1 (12/2012)

## 2.3 Imaging/Duplication Procedures

On April 18th, 2021, during the search of a residence in Aosta by Italian authorities, a Raspberry Pi connected to a 3D printer was identified by a specialist from the Reparto Investigazioni Scientifiche (RIS) of the Carabinieri. To preserve the integrity of the digital evidence, a forensic copy of the microSD card from the seized Raspberry Pi was acquired.

The imaging process involved creating a bit-for-bit, forensically sound duplicate of the original microSD card. This was performed using industry-standard forensic tools and methodologies to ensure that no data on the original media was altered during the acquisition. A hash value (SHA2-256) was computed for the acquired image to verify its authenticity and integrity against the original media (if possible to hash the original in situ, or the derived hash from the copy process).

The forensic image was stored with the filename **2\_Raspberry\_Pi\_mSD.zip** and its integrity verified by the SHA2-256 hash value:

**aabec0c1305e785d1ba5b4ba01c5dacd27cc128fdd32078758be826e75449953**

This hash value serves as a digital fingerprint, allowing for future verification that the copy remains identical to the state it was in at the time of acquisition. The original microSD card was then secured according to standard evidence handling protocols.

## 2.4 Hash Values

To ensure the integrity and authenticity of the digital evidence, cryptographic hash values were utilized for verification.

The digital forensic unit of the police provided the following SHA2-256 hash value for the **2\_Raspberry\_Pi\_mSD.zip** image file upon its provision:

SHA2-256 (Provided by Italian Authorities ):

**aabec0c1305e785d1ba5b4ba01c5dacd27cc128fdd32078758be826e75449953**

Upon receipt of the **2\_Raspberry\_Pi\_mSD.zip** image file by our unit on 10th jun,2025 , a verification hash was independently calculated. The following PowerShell command was executed to obtain the hash value:

PowerShell

**Get-FileHash -Path ./2\_Raspberry\_Pi\_mSD.zip**

The SHA2-256 hash value calculated by our unit is as follows:

SHA2-256 (Calculated by Our Unit):

**AABEC0C1305E785D1BA5B4BA01C5DACD27CC128FDD32078758BE826E75449953**

A direct comparison of the provided and independently calculated SHA2-256 hash values confirmed they are identical. This verification confirms that the 2\_Raspberry\_Pi\_mSD.zip file has not been altered or corrupted during transfer and storage up to the point of our examination.

## 3. Examination Methodology and Tools

### 3.1 Examination Environment

The digital forensic examination of the evidence in this case was conducted in a controlled environment. Due to limited laboratory access and the requirements of a home lab setup, the examination was performed in my bedroom. The following measures were in place:

#### **Physical security:**

My bedroom was **locked** and nobody couldn't enter without **proper authorization** to ensure security and confidentiality of evidence.

The room was equipped with **air conditioner** to minimize potential environmental impact on digital media.

#### **Hardware and Software:**

All examination was conducted on dedicated VM. The specification for that VM are as follows:

- Processor: AMD Ryzen 7 5800 4 CPU
- RAM: 4GB
- OS: Windows10
- Storage: 150GB HDD

The following software were used during the examination:

- Oracle Virtualbox (Version 7.1.6 r167084 (Qt6.4.2))
- Autopsy(4.22.0)
- Chrome (136.0.7103.114 (Official Build) (64-bit))

- Winrar x64-711
- OpenJdk 25
- Ultimaker Cura 4.7.1

The following websites were used during the examination:

- <https://google.com>
- <https://docs.google.com/>
- 

## 3.2 Analytical Procedures

The primary objective of that examination is to identify and extract any record related to card data, specifically looking for patterns consistent with credit card numbers, and to understand functionalities of SD-card on “Skimming” device.

To preserve the integrity of the original evidence, the analysis was conducted on a verified working copy of the forensic image, utilizing Autopsy version 4.22.0 as the primary tool; prior to commencing analysis, the SHA256 hash values of both image files were meticulously compared to confirm their identical nature, and the working copy was accessed exclusively in a read-only mode.

Prior to unzipping 2\_Raspberry\_Pi\_mSD.zip we calculate file hash of that file and compare it with hash value provided by Italian Authorities. As documented in section 2.4 this confirmed integrity of the image file.

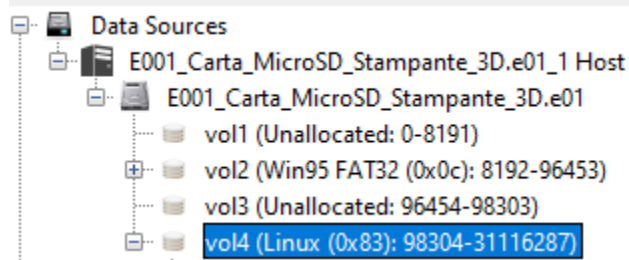
The 2\_Raspberry\_Pi\_mSD.zip file was first unzipped. Then the image file was then loaded into primary forensic software, Autopsy 4.22.0, according to publicly available information autopsy software will not modify original image file it writes everything made during analysis into its own database, thiagee.

As documented in section 1.4 our main objectives:

- Establishing whether the Raspberry Pi has been used to control the 3D printer.
- Establishing whether objects of possible illicit use have been printed, when and which ones.

### Examination of Raspberry Pi to identify if it was used to control 3D printer.

During the examination of ascuired evidence, a search for possible external device connection, we identified that disk devided into 4 volumes as shown in **Figures 1.0**





**Figure 1.0:** Volumes in disk image in autopsy 4.22.0.  
Only allocated volumes are Vol2 and Vol4.

**Vol2** contains a WIN95 FAT32 file system. Within this volume, an interesting file named **“octopi.txt”** was discovered. This file contains information about **Octoprint** software, including the following extracted URLs:

- <https://github.com/guysoft/OctoPi>
- <https://github.com/foosel/OctoPrint>

These URLs indicate that **OctoPi** and **OctoPrint** are publicly available software used to control 3D printers via a Graphical User Interface (GUI). Further research revealed that OctoPrint software logs are typically stored in the **.octoprint/logs** directory, which is located in the user's home directory.

### Analysis of Vol4

As depicted in Figure 1.0, **Vol4** is a Linux file system containing a Raspberry Pi Linux operating system. Our analysis identified that the Raspberry Pi is running under the user account **“pi.”** The home directory for this user is **/home/pi**, where the **.octoprint** folder is located.

Within that folder, a file named **octoprint\_stats.json** was found. The full path of this file is:

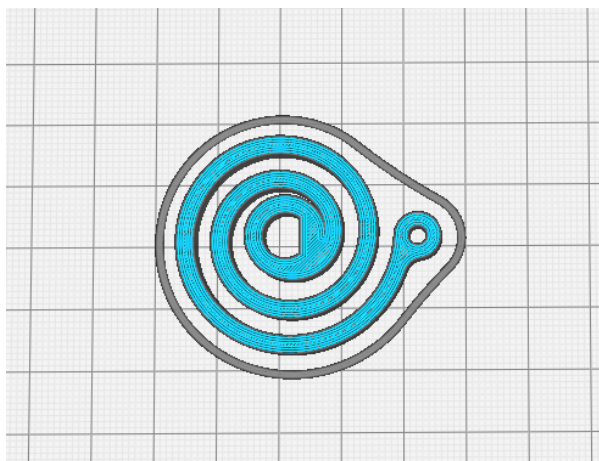
**/img\_E001\_Carta\_MicroSD\_Stampante\_3D.e01/vol\_vol4/home/pi/.octoprint/logs/octoprint\_stats.json.**

Examination of this file reveals that a printer was attached on port **/dev/ttyUSB0** in 2021-04-13, which is near the date when Italian Authorities identified this Raspberry Pi device. This file also contains printed objects history.

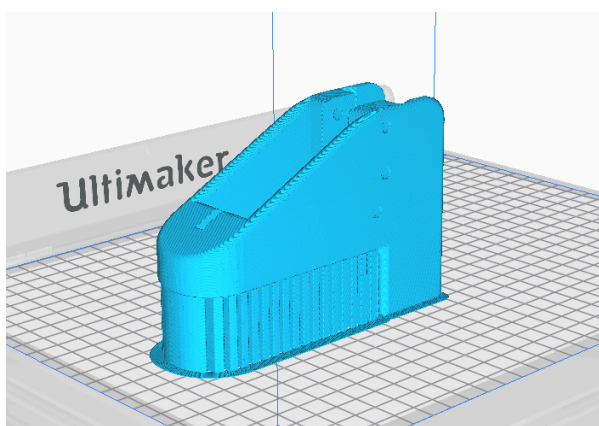
This Information is enough to say that this raspberry pi device was used to control 3D printer.

### Examination of printed objects of illicit use.

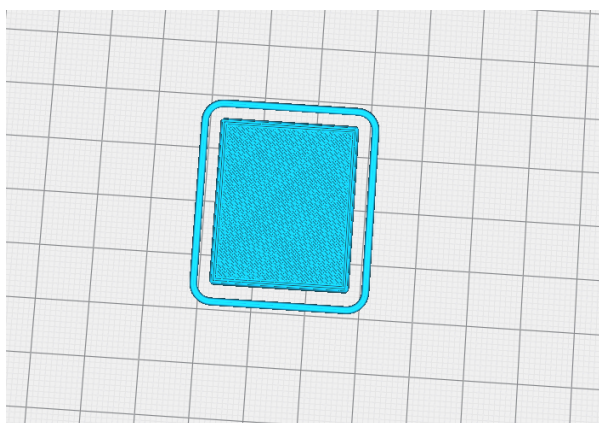
During the examination of **octoprint\_stats.json** file which contains lots of information about what objects were printed. Figure 2.0 shows our findings. All that logs contain printed object filename with **.gcode** file extension. A **.gcode** file is created by a slicing program, which turns a CAD drawing into a string of code that a 3D printer can understand. Figure 2.1 shows that these gcode files were created with **Cura\_SteamEngine 4.7.1**. That means this files made by using **Ultimaker Cura** to create 3d model of objects. Base



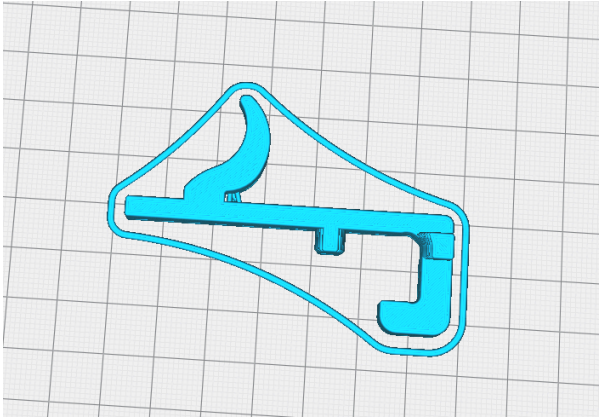
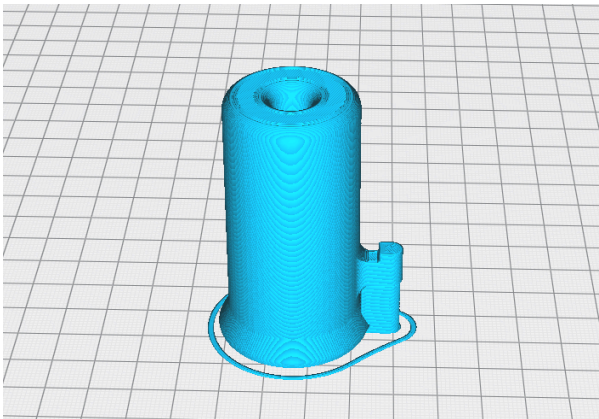
**Filepath:**  
/img\_E001\_Carta\_MicroSD\_Stampante\_3D.e  
01/vol\_vol4/home/pi/.octoprint/uploads/VK\_S  
pring.gcode  
**Printed Date:** 2021-04-14 15:29:46,  
2021-04-13 16:23:01  
**Owner:** animzola



**Filepath:**  
/img\_E001\_Carta\_MicroSD\_Stampante\_3D.e  
01/vol\_vol4/home/pi/.octoprint/uploads/VK\_fr  
ame\_(no\_sn).gcode  
**Printed Date:** 2021-04-14 14:28:29  
**Owner:** animzola



**Filepath:**  
/img\_E001\_Carta\_MicroSD\_Stampante\_3D.e  
01/vol\_vol4/home/pi/.octoprint/uploads/VK\_b  
ottom\_cover.gcode  
**Printed Date:** 2021-04-13 16:01:45  
**Owner:** animzola

	<p><b>Filepath:</b> /img_E001_Carta_MicroSD_Stampante_3D.e01/vol_vol4/home/pi/.octoprint/uploads/VK_trigger.gcode <b>Printed Date:</b> 2021-04-13 15:32:24 <b>Owner:</b> animzola</p>
	<p><b>Filepath:</b> /img_E001_Carta_MicroSD_Stampante_3D.e01/vol_vol4/home/pi/.octoprint/uploads/VK_380_barrel_(threaded).gcode <b>Printed Date(s):</b> 2021-04-13 13:53:00 <b>Owner:</b> animzola</p>

**Figure 2.0:** Printed object of possible illicit use.

Based on internet research all of above printed objects related to 3d printable gun parts, objects are publically available in "<https://github.com/jdneidig/Liberator>". Also another interesting file located in

"/img\_E001\_Carta\_MicroSD\_Stampante\_3D.e01/vol\_vol4/home/pi/.octoprint/printerProfiles/\_default.profile" this file shows us which printer model was used, as we find from that file Velleman Vertex K8400 3D printer model was used which is plugged into "**/dev/ttyUSB0**".

## 5. Conclusion

As we documented in section 1.1 our particular attension was given to followings:

- Establishing whether the Raspberry Pi has been used to control the 3D printer.
- Establishing whether objects of possible illicit use have been printed, when and which ones.

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

Based on our examination, Raspberry Pi has been used to control the 3D printer.

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

As shown in Figure 2.0 3D printer was used to print gun parts.