Configuration Manual

MSc Research Project
Programme Name

Ivan Ronald Dsouza
Student ID: X22189386

School of Computing
National College of Ireland

Supervisor: Eugene McLaughlin

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Ivan Ronald Dsouza
Student ID:	X22189386
Programme:	MSc Cyber Security **Year:** 2024
Module:	MSc Research Practicum
Lecturer:	Eugene McLaughlin
Submission Due Date:	12/12/2024
Project Title:	IOT Forensics: A Comprehensive Analysis of an IOT Device using Digital Forensic and Penetration Testing Tools and Methodologies

Word Count: 795 **Page Count: 10**

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Ivan Ronald Dsouza

Date: 12/12/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Ivan Dsouza
Student ID: X22189386

1 Introduction

This document is a configuration manual that comprises of the steps undertaken for successful execution of the project along with screenshots. In addition, details pertaining to system configurations, hardware/software requirements and other technicalities will also be addressed.

2 System Configuration

This section details information about the device used for the entire research project

Specifications	Description and Versions
Operating System	Windows 10 Home Version 22H2
Processor	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 2.42 GHz
System Type	64-bit operating system, x64-based processor
Memory	8 GB

3 Tools and Software Configuration and Requirements

This Section Highlights the external tools and software utilised for this project.

Software	Version	Use case
VMWare Workstation	Version 17.0 Player	Virtual environment creation for hosting Kali Linux
Kali Linux	Version 6.6.9 64 bit	Conduct Vulnerability Analysis and Penetration Testing on the Baby Monitor
Nmap	7.94 SVN	Scanning the IOT Device
Binwalk		Firmware analysis of IOT Device
JohnTheRipper	Open source	Brut forcing the password
FTK Imager	4.7.1.2	Creating Forensic Image for Digital Forensics
Autopsy	4.21.0	Analysis of Forensic Image to generate artefacts

4 Implementation

Static Analysis via USB

To execute static analysis via USB, connect the Baby Monitor to the laptop as shown in the Figure 1:

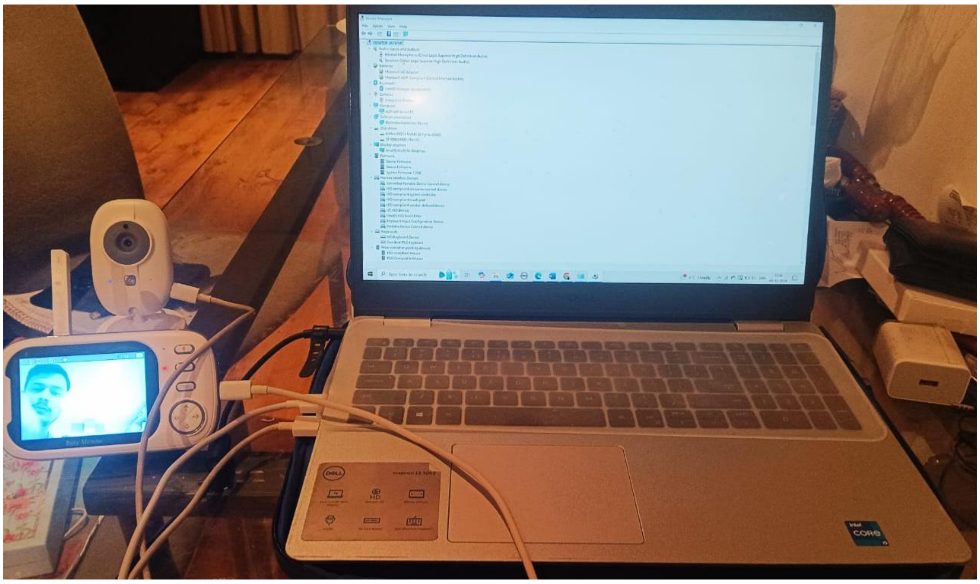
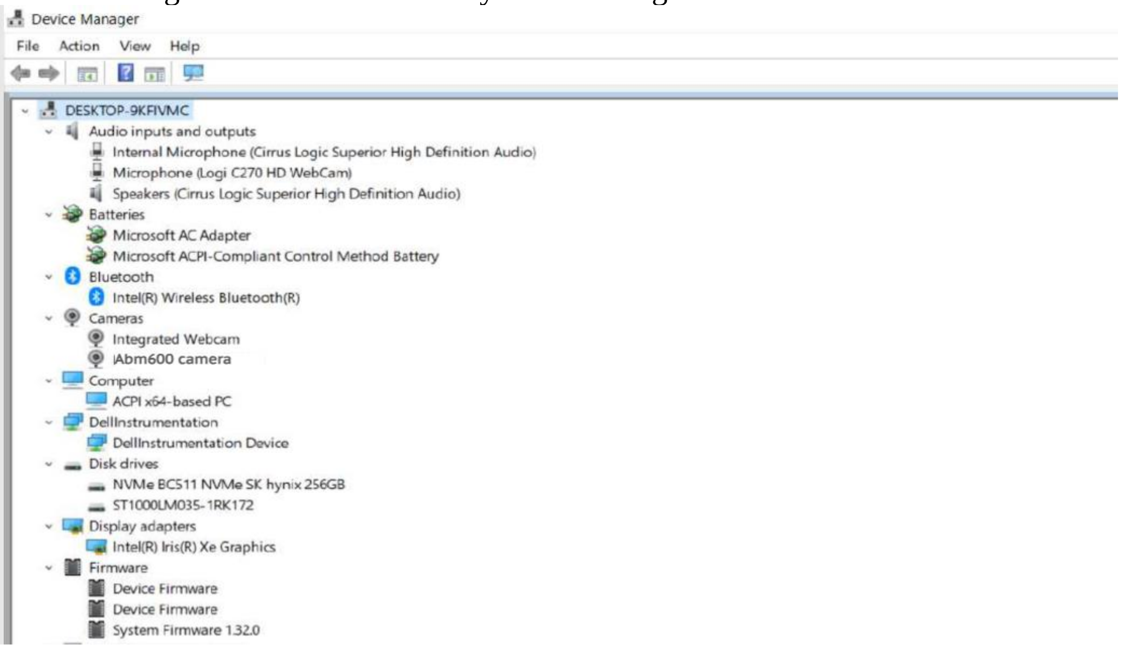


Figure 1: Connection of IOT Device to Laptop via USB

However, after connecting the baby monitor to the laptop through the USB port there is a possibility that the laptop might not detect the IOT Device. In this scenario, go to Control Panel => Device Manager => Cameras. If the device is not detected then reset your Drivers and repeat the process. The same error was faced in this research after which the drivers were reset resulting in detection of the Baby Monitor. Figure 2



```
DESKTOP-9KFIVMC
    Audio inputs and outputs
        Internal Microphone (Cirrus Logic Superior High Definition Audio)
        Microphone (Logi C270 HD WebCam)
        Speakers (Cirrus Logic Superior High Definition Audio)
    Batteries
        Microsoft AC Adapter
        Microsoft ACPI-Compliant Control Method Battery
    Bluetooth
        Intel(R) Wireless Bluetooth(R)
    Cameras
        Integrated Webcam
        iAbm600 camera
    Computer
        ACPI x64-based PC
    DellInstrumentation
        DellInstrumentation Device
    Disk drives
        NVMe BC511 NVMe SK hynix 256GB
        ST1000LM035-1RK172
    Display adapters
        Intel(R) Iris(R) Xe Graphics
    Firmware
        Device Firmware
        Device Firmware
        System Firmware 1.32.0
```

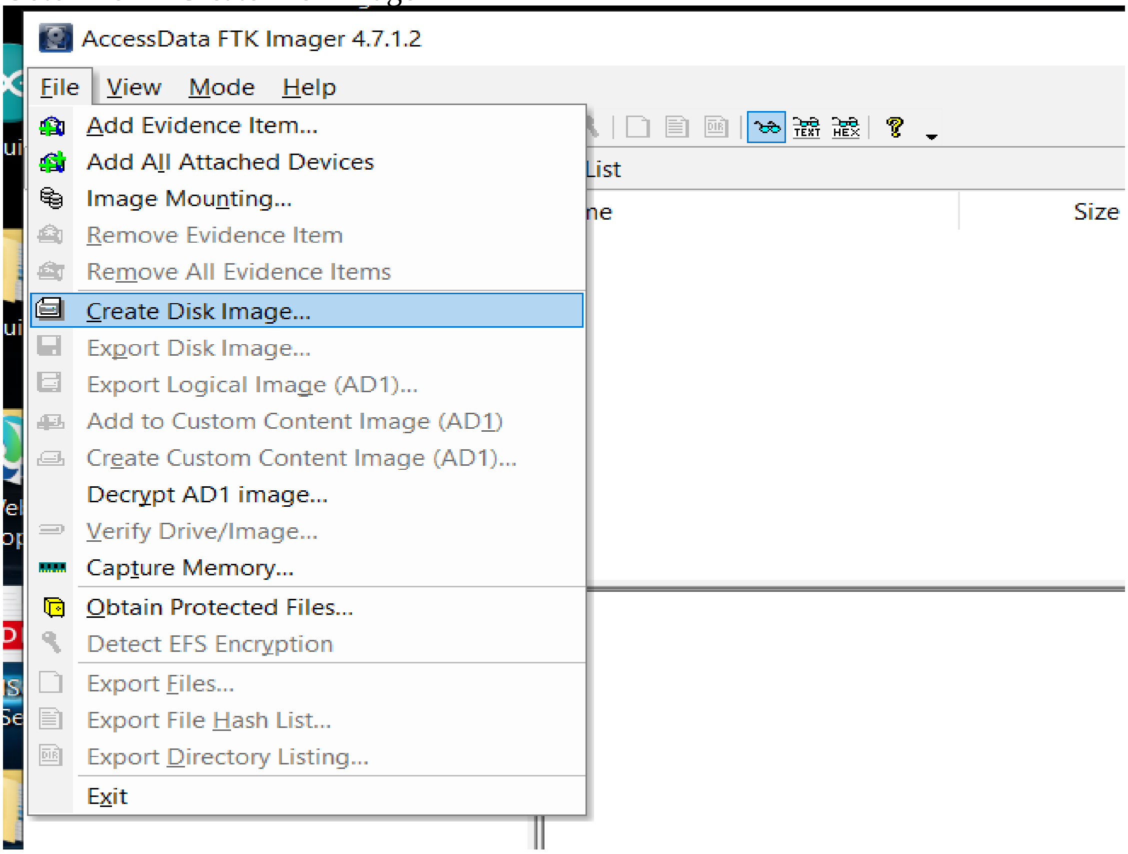
Figure 2: Device Driver

Digital Forensic Analysis

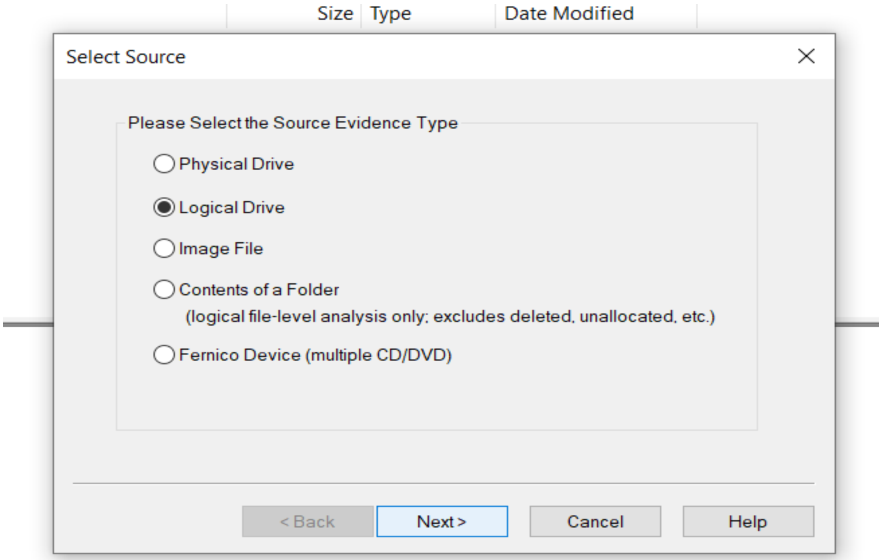
To carry out Digital Forensic Analysis FTK Imager is used to create a forensic image while Autopsy is used to analyse the forensic image. The steps taken can be given as follows

Creation of Forensic Image

Goto File => Create Disk Image

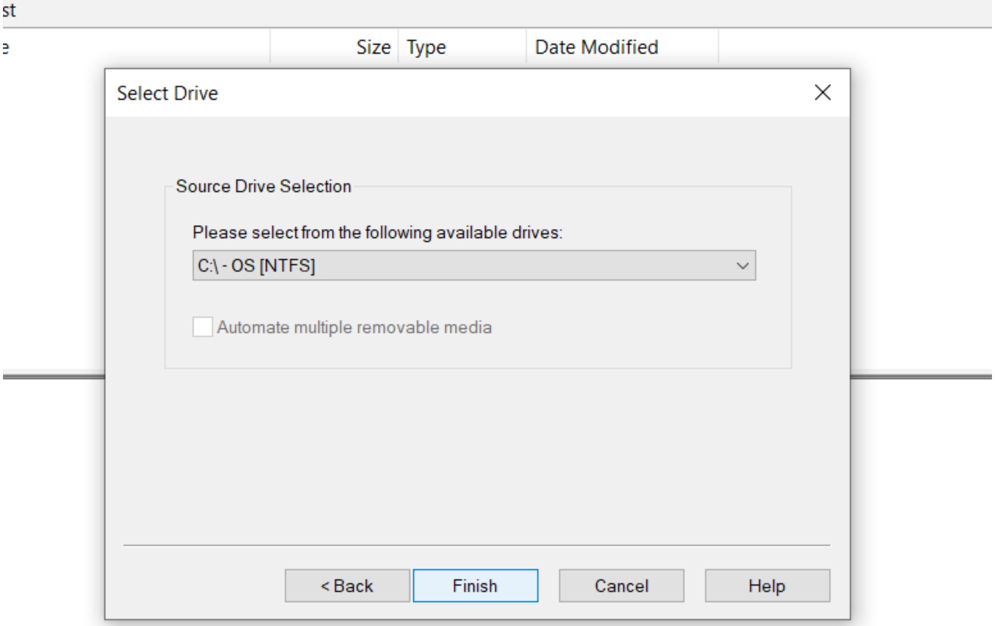


As the forensic image created is a logical image select Logical File



Size
Type
Date Modified
Select Source
Please Select the Source Evidence Type
○ Physical Drive
● Logical Drive
○ Image File
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)
○ Fernico Device (multiple CD/DVD)
< Back
Next >
Cancel
Help

Select C Drive as the source drive to create the forensic image and then select E drive as the destination drive to store the forensic image. The source and the destination drive cannot be same. Select and press Finish



Please select from the following available drives:

C:\ - OS [NTFS]

□ Automate multiple removable media

The Forensic Image has been created and verified successfully

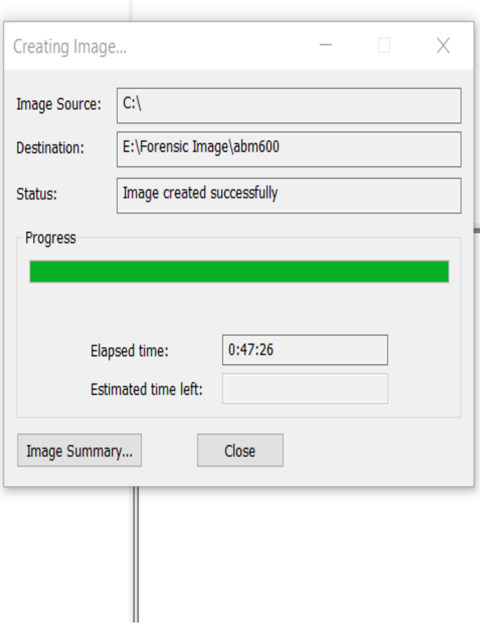


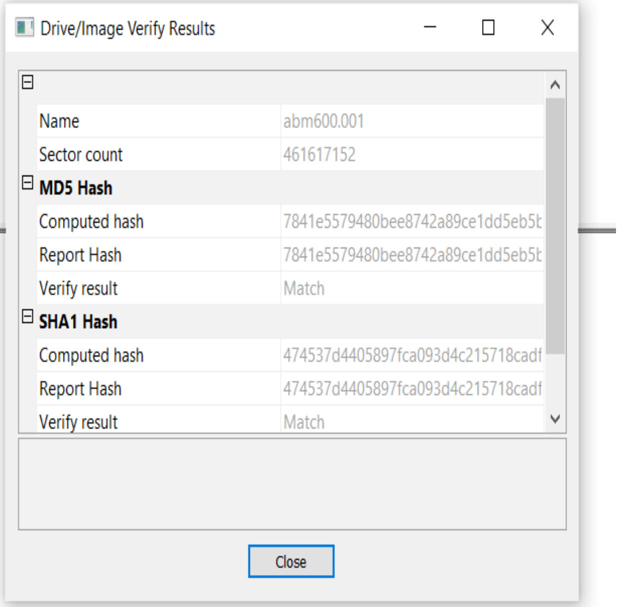
Image Source: C:\

Destination: E:\Forensic Image\abm600

Status: Image created successfully

Elapsed time: 0:47:26

Estimated time left:

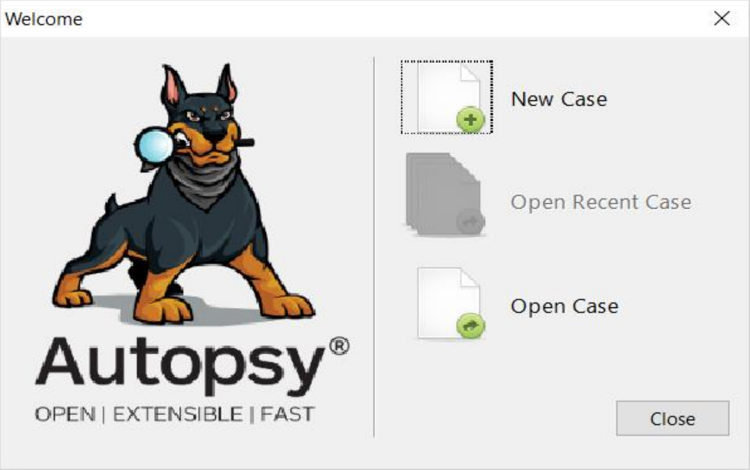


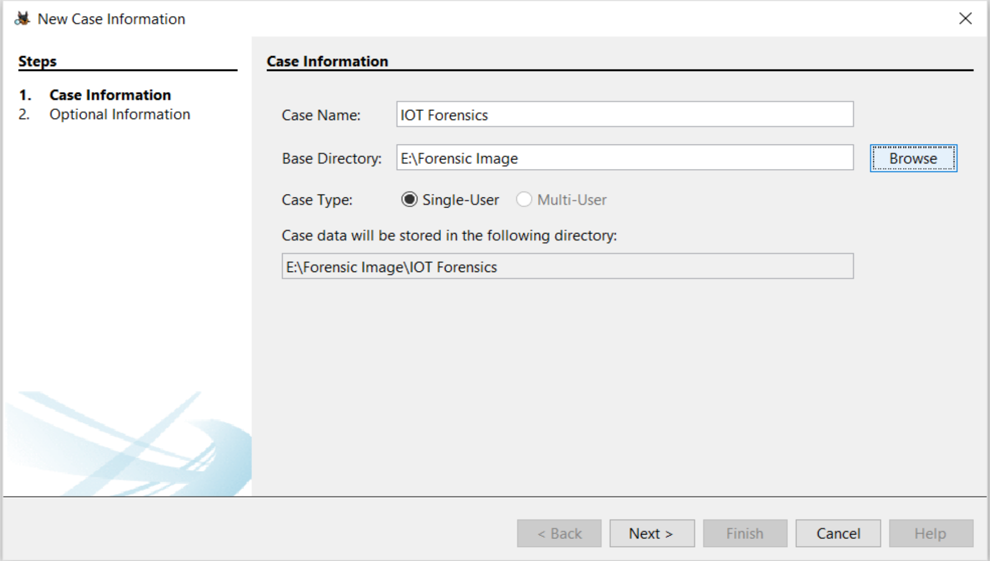
Name	abm600.001
Sector count	461617152
MD5 Hash	
Computed hash	7841e5579480bee8742a89ce1dd5eb5t
Report Hash	7841e5579480bee8742a89ce1dd5eb5t
Verify result	Match
SHA1 Hash	
Computed hash	474537d4405897fca093d4c215718cadf
Report Hash	474537d4405897fca093d4c215718cadf
Verify result	Match

Once the forensic image is created Autopsy is used to analyze and investigate the forensic image

Analysis of Forensic Image

Open Autopsy and Create a New Case. Then enter the Case Information selecting E drive as the base directory, as that is the destination of the Forensic Image. Then enter the optional information as well




New Case Information

Steps

1. **Case Information**
2. Optional Information

Case Information

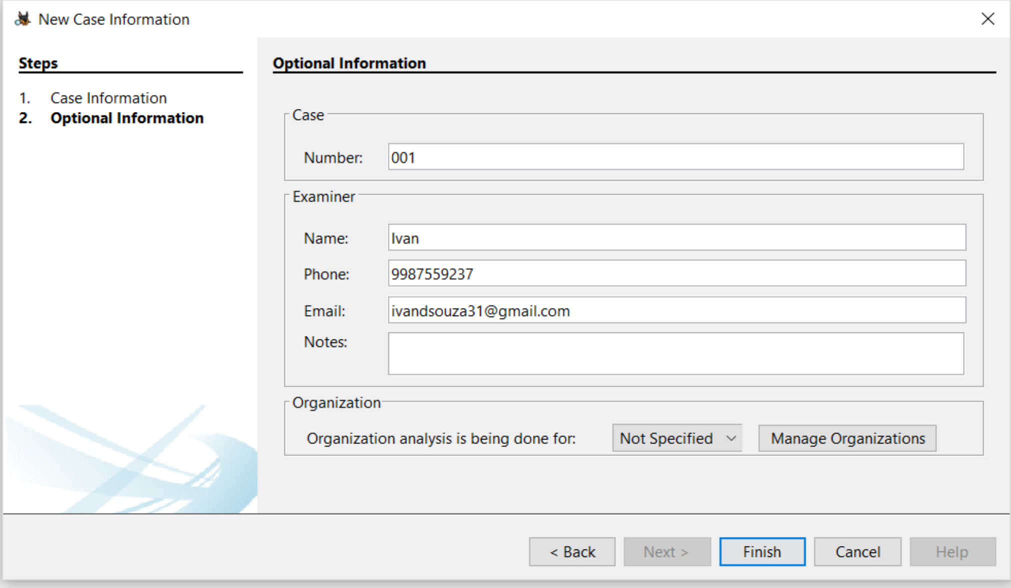
Case Name: IOT Forensics

Base Directory: E:\Forensic Image

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

E:\Forensic Image\IOT Forensics


New Case Information

Steps

1. Case Information
2. **Optional Information**

Optional Information

Case

Number: 001

Examiner

Name: Ivan

Phone: 9987559237

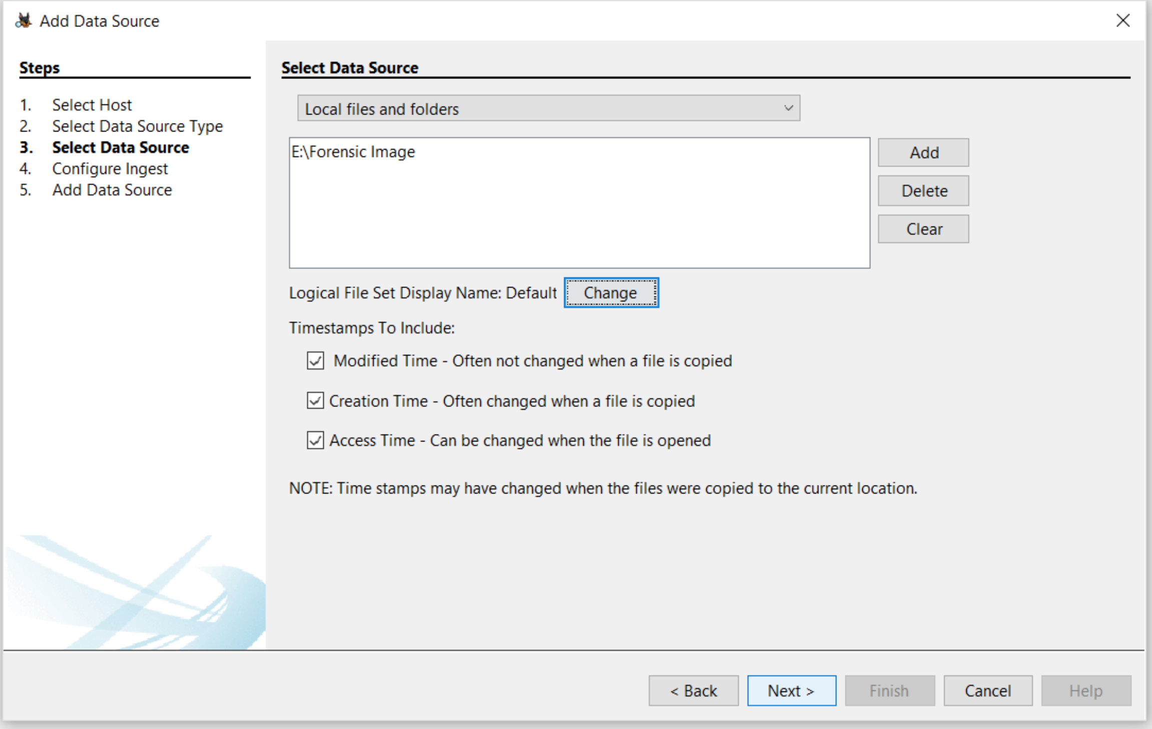
Email: ivandsouza31@gmail.com

Notes:

Organization

Organization analysis is being done for: Not Specified

Now Select and Add the Data Source which is the forensic image in E Drive


Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. **Select Data Source**
4. Configure Ingest
5. Add Data Source

Select Data Source

Local files and folders

E:\Forensic Image

Logical File Set Display Name: Default

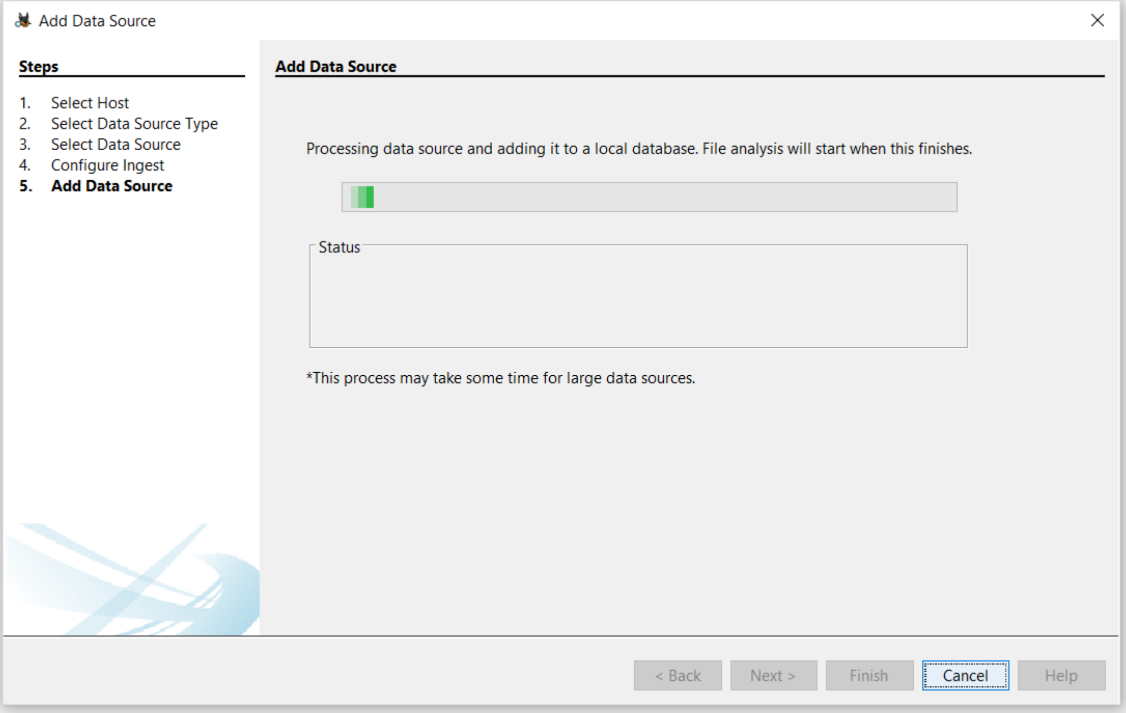
Timestamps To Include:

☑ Modified Time - Often not changed when a file is copied

☑ Creation Time - Often changed when a file is copied

☑ Access Time - Can be changed when the file is opened

NOTE: Time stamps may have changed when the files were copied to the current location.


Add Data Source

Steps

1. Select Host
2. Select Data Source Type
3. Select Data Source
4. Configure Ingest
5. **Add Data Source**

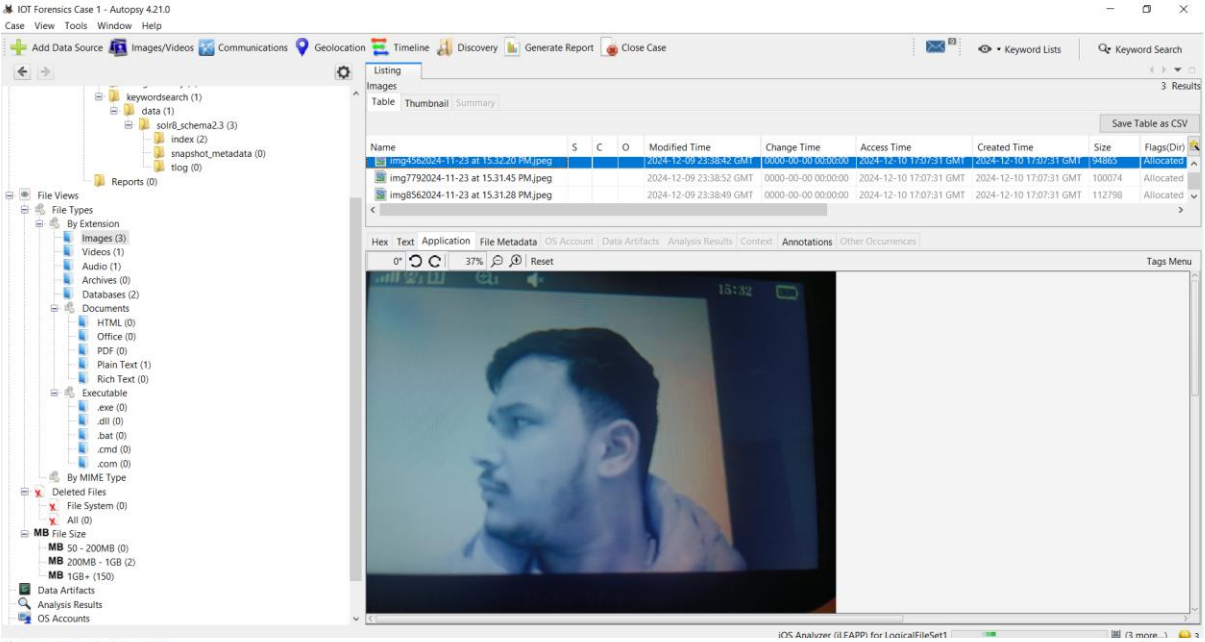
Add Data Source

Processing data source and adding it to a local database. File analysis will start when this finishes.

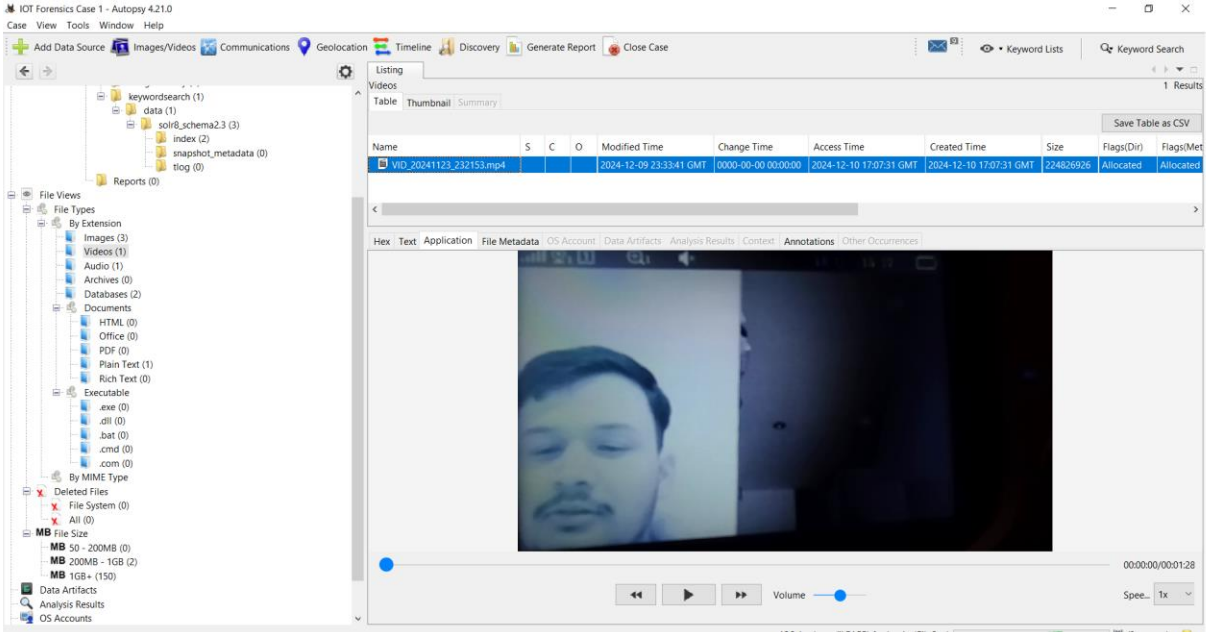
Status

*This process may take some time for large data sources.

The following Image Files and Video Files are retrieved upon forensic analysis



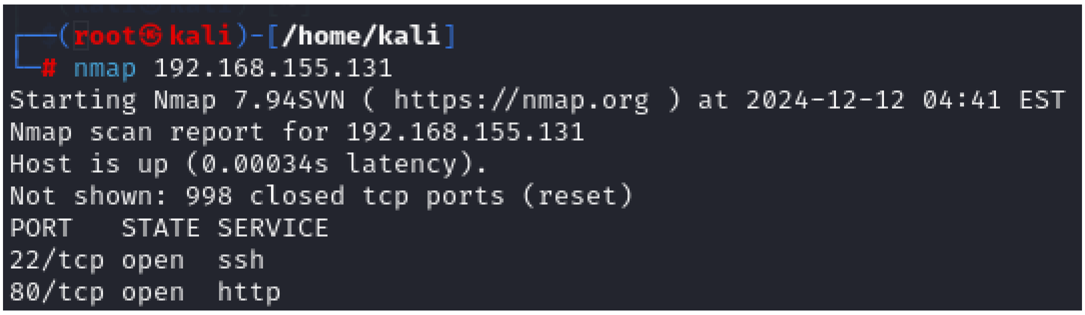
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
img4562024-11-23 at 15.32.20 PM.jpeg				2024-12-09 23:38:42 GMT	0000-00-00 00:00:00	2024-12-10 17:07:31 GMT	2024-12-10 17:07:31 GMT	94865	Allocated
img7792024-11-23 at 15.31.45 PM.jpeg				2024-12-09 23:38:52 GMT	0000-00-00 00:00:00	2024-12-10 17:07:31 GMT	2024-12-10 17:07:31 GMT	100074	Allocated
img8562024-11-23 at 15.31.28 PM.jpeg				2024-12-09 23:38:49 GMT	0000-00-00 00:00:00	2024-12-10 17:07:31 GMT	2024-12-10 17:07:31 GMT	112798	Allocated


IOT Forensics Case 1 - Autopsy 4.21.0
Case View Tools Window Help
Listing
Videos
1 Results
Table Thumbnail Summary
Save Table as CSV
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
00:00:00/00:01:28
Volume
Speed 1x

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Met
VID_20241123_232153.mp4				2024-12-09 23:33:41 GMT	0000-00-00 00:00:00	2024-12-10 17:07:31 GMT	2024-12-10 17:07:31 GMT	224826926	Allocated	Allocated

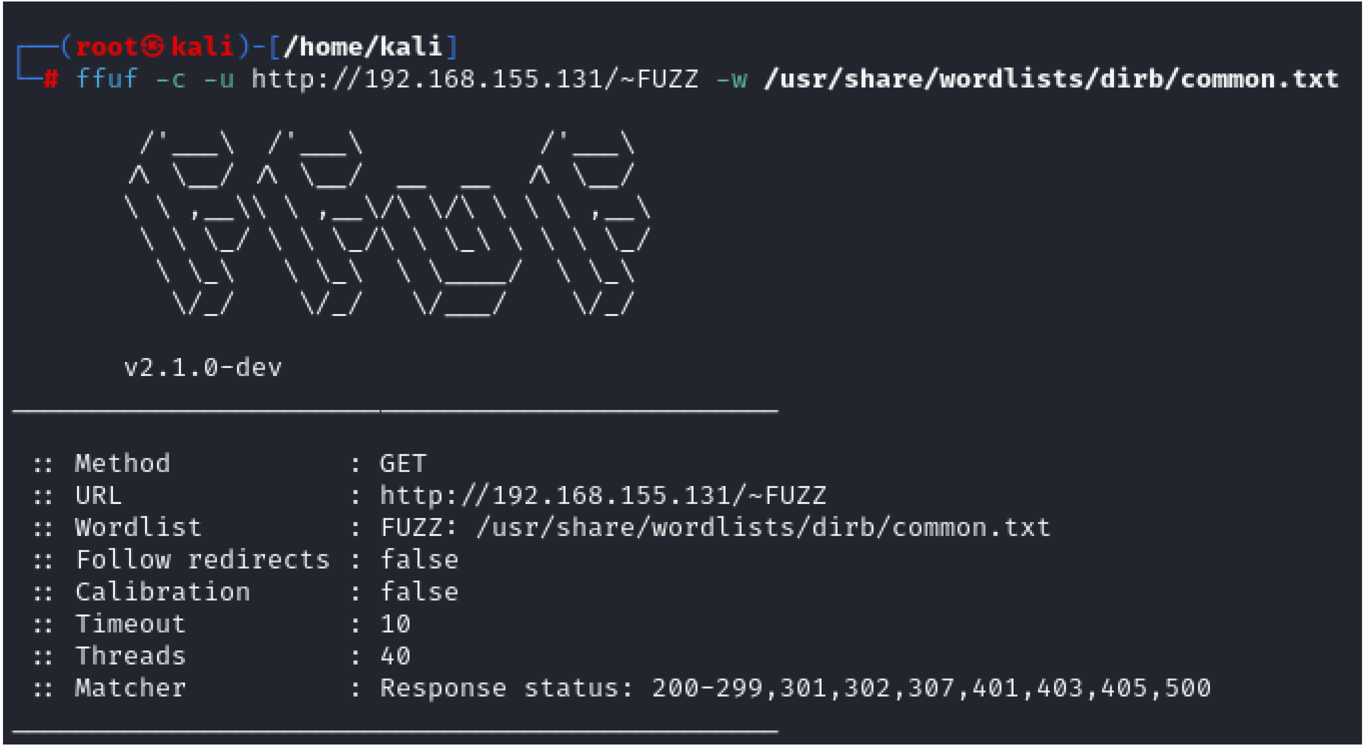
Vulnerability Analysis and Penetration Testing

Scanning Phase using Nmap ports 22/ tcp ssh and 80/tcp are open



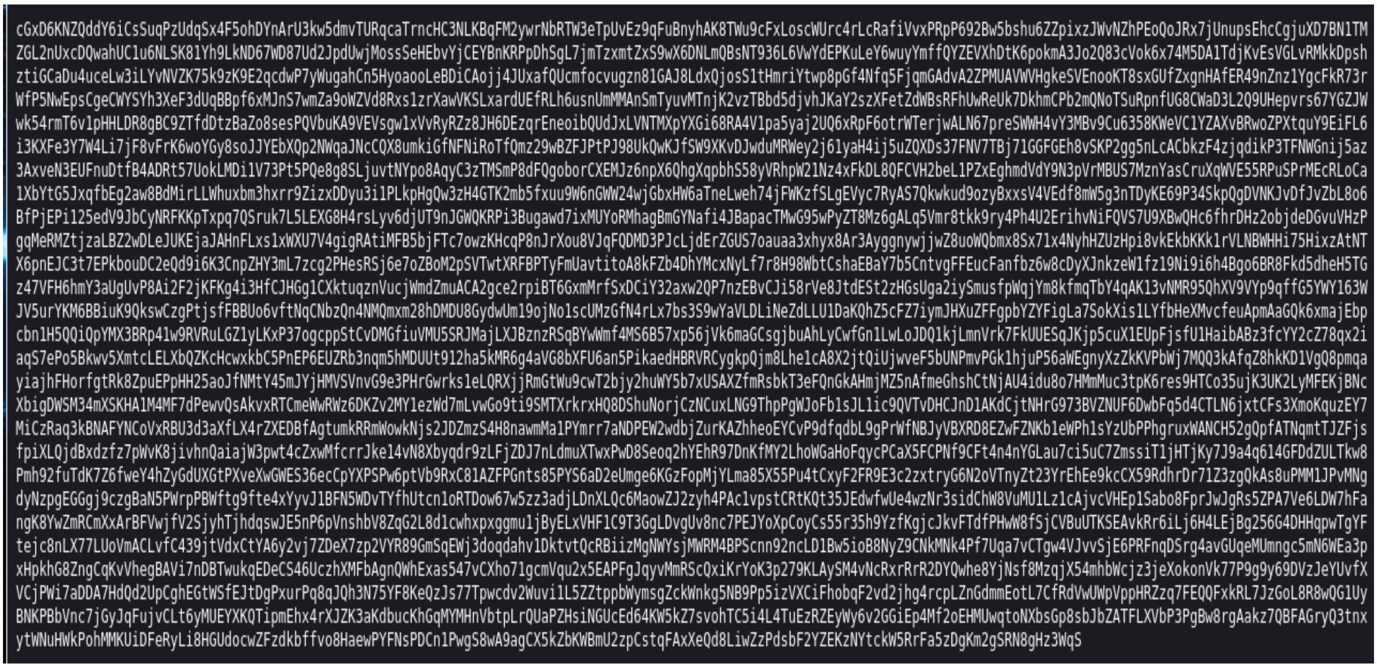
```
┌──(root㉿kali)-[/home/kali]
└─# nmap 192.168.155.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-12 04:41 EST
Nmap scan report for 192.168.155.131
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Fuzzing using FFUF Fuzzer and wordlist



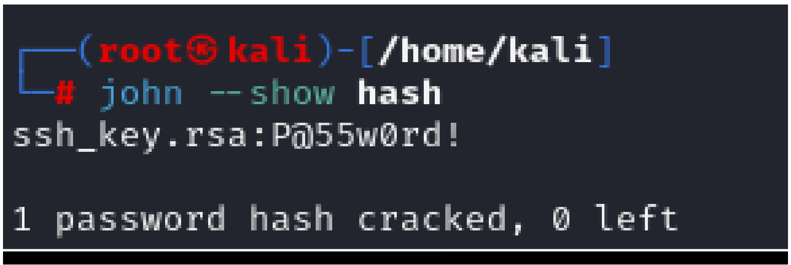
```
┌──(root㉿kali)-[/home/kali]
└─# ffuf -c -u http://192.168.155.131/~FUZZ -w /usr/share/wordlists/dirb/common.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.155.131/~FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________
```

Base 58 encoded file decoded using CyberChef



```
cGxD6KNZQddY6iCsSuqPzUdqSx4F5ohDYnArU3kw5dmvTURqcaTrncHC3NLKBqFM2ywrNbRTW3eTpUvEz9qFuBnyhAK8TWu9cFxLoscWUrc4rLcRafiVvxPRpP692Bw5bshu6ZZpixzJWvNZhPEoQoJRx7jUnupsEhcCgjuXD7BN1TM
ZGL2nUxcDQwahUC1u6NLSK81Yh9LkND67WD87Ud2JpdUwjMossSeHEbvYjCEYBnKRPpDhSgL7jmTzxmtZxS9wX6DNLmQBsNT936L6VwYdEPKuLeY6wuyYmffQYZEVXhDtK6pokmA3Jo2Q83cVok6x74M5DA1TdjKvEsVGLvRMkkDpsh
ztiGCaDu4uceLw3iLYvNVZK75k9zK9E2qcdwP7yWugahCn5HyoaooLeBDiCAojj4JUxafQUcmfocvugzn81GAJ8LdxQjosS1tHmriYtwp8pGf4Nfq5FjqmGAdvA2ZPMUAVWVHgkeSVEnooKT8sxGUfZxgnHAfER49nZnz1YgcFkR73r
WfP5NwEpsCgeCWYSYh3XeF3dUqBBpf6xMJnS7wmZa9oWZVd8Rxs1zrXawVKSLxardUEfRLh6usnUmMMAnSmTyuvMTnjK2vzTBbd5djvhJKaY2szXFetZdWBsRFhUwReUk7DkhmCPb2mQNoTSuRpnfUG8CWaD3L2Q9UHepvrs67YGZJW
wk54rmT6v1pHHLDR8gBC9ZTfdDtzBaZo8sesPQVbuKA9VEVsgw1xVvRyRZz8JH6DEzqrEneoibQUdJxLVNTMXpYXGi68RA4V1pa5yaj2UQ6xRpF6otrWTerjwALN67preSWWH4vY3MBv9Cu6358KWeVC1YZAXvBRwoZPXtquY9EiFL6
i3KXFe3Y7W4Li7jF8vFrK6woYGy8soJJYEbXQp2NWqaJNcCQX8umkiGfNFNiRoTfQmz29wBZFJPtPJ98UkQwKJfSW9XKvDJwduMRWey2j61yaH4ij5uZQXDs37FNV7TBj71GGFGEh8vSKP2gg5nLcACbkzF4zjqdikP3TFNWGnij5az
3AxveN3EUFnuDtfB4ADRt57UokLMDi1V73Pt5PQe8g8SLjuvtNYpo8AqyC3zTMSmP8dFQgoborCXEMJz6npX6QhgXqpbhS58yVRhpW21Nz4xFkDL8QFCVH2beL1PZxEghmdVdY9N3pVrMBUS7MznYasCruXqWVE55RPuSPrMEcRLoCa
1XbYtG5JxqfbEg2aw8BdMirLLWhuxbm3hxrr9ZizxDDyu3i1PLkpHgQw3zH4GTK2mb5fxuu9W6nGWW24wjGbxHW6aTneLweh74jFWKzfSLgEVyc7RyAS7Qkwkud9ozyBxxsV4VEdf8mW5g3nTDyKE69P34SkpQgDVNKJvDfJvZbL8o6
BfPjEPi125edV9JbCyNRFKKpTxpq7QSruk7L5LEXG8H4rsLyv6djUT9nJGWQKRPi3Bugawd7ixMUYoRMhagBmGYNafi4JBapacTMwG95wPyZT8Mz6gALq5Vmr8tkk9ry4Ph4U2ErihvNiFQVS7U9XBwQHc6fhrDHz2objdeDGvuVHzP
gqMeRMZtjzaLBZ2wDLeJUKEjaJAHnFLxs1xWXU7V4gigRAtiMFB5bjFTc7owzKHcqP8nJrXou8VJqFQDMD3PJcLjdErZGUS7oauaa3xhyx8Ar3AyggnywjjwZ8uoWQbmx8Sx71x4NyhHZUzHpi8vkEkbKKk1rVLNBWHHi75HixzAtNT
X6pnEJC3t7EPkbouDC2eQd9i6K3CnpZHY3mL7zcg2PHesRSj6e7oZBoM2pSVTwtXRFBPTyFmUavtitoA8kFZb4DhYMcxNyLf7r8H98WbtCshaEBaY7b5CntvgFFEucFanfbz6w8cDyXJnkzeW1fz19Ni9i6h4Bgo6BR8Fkd5dheH5TG
z47VFH6hmY3aUgUvP8Ai2F2jKFKg4i3HfCJHGg1CXktuqznVucjWmdZmuACA2gce2rpiBT6GxmMrfSxDCiY32axw2QP7nzEBvCJi58rVe8JtdESt2zHGsUga2iySmusfpWqjYm8kfmqTbY4qAK13vNMR95QhXV9VYp9qffG5YWY163W
JV5urYKM6BBiuK9QkswCzgPtjsfFBBUo6vftNqCNbzQn4NMQmxm28hDMDU8GydwUm19ojNo1scUMzGfN4rLx7bs3S9wYaVLDLiNeZdLLU1DaKQhZ5cFZ7iymJHXuZFFgpbYZYFigLa7SokXis1LYfbHeXMvcfeuApmAaGQk6xmajEbp
cbn1H5QQiQpYMX3BRp41w9RVRuLGZ1yLKxP37ogcppStCvDMGfiuVMU5SRJMajLXJBznzRSqBYwWmf4MS6B57xp56jVk6maGCsgjbuAhLyCwfGn1LwLoJDQ1kjLmnVrk7FkUUESqJKjp5cuX1EUpFjsfU1HaibABz3fcYY2cZ78qx2i
aqS7ePo5Bkwv5XmtcLELXbQZKcHcwxkbC5PnEP6EUZRb3nqm5hMDUUt912ha5kMR6g4aVG8bXFU6an5PikaedHBRVRCygkpQjm8Lhe1cA8X2jtQiUjwveF5bUNPmvPGk1hjuP56aWEgnyXzZkKVPbWj7MQQ3kAfqZ8hkKD1VgQ8pmqa
yiajhFHorfgtRk8ZpuEPpHH25aoJfNMtY45mJYjHMVSVnvG9e3PHrGwrks1eLQRXjjRmGtWu9cwT2bjy2huWY5b7xUSAXZfmRsbkT3eFQnGkAHmjMZ5nAfmeGhshCtNjAU4idu8o7HMmMuc3tpK6res9HTCo35ujK3UK2LyMFEKjBNc
XbigDWSM34mXSKHA1M4MF7dPewvQsAkvxRTCmeWwRWz6DKZv2MY1ezWd7mLvwGo9ti9SMTXrkrxHQ8DShuNorjCzNCuxLNG9ThpPgWJoFb1sJL1ic9QVTvDHCJnD1AKdCjtNHrG973BVZNUF6DwbFq5d4CTLN6jxtCFs3XmoKquzEY7
MiCzRaq3kBNAFYNCoVxRBU3d3aXfLX4rZXEDBfAgtumkRRmWowkNjs2JDZmzS4H8nawmMa1PYmrr7aNDPEW2wdbjZurKAZhheoEYCvP9dfqdbL9gPrWfNBJyVBXRD8EZwFZNKb1eWPh1sYzUbPPhgruxWANCH52gQpfATNqmtTJZFjs
fpiXLQjdBxdzfz7pWvK8jivhnQaiajW3pwt4cZxwMfcrrJke14vN8Xbyqdr9zLFjZDJ7nLdmuXTwxPwD8Seoq2hYEhR97DnKfMY2LhoWGaHoFqycPCaX5FCPNf9CFt4n4nYGLau7ci5uC7ZmssiT1jHTjKy7J9a4q614GFDdZULTkw8
Pmh92fuTdK7Z6fweY4hZyGdUXGtPXveXwGWES36ecCpYXPSPw6ptVb9RxC81AZFPGnts85PYS6aD2eUmge6KGzFopMjYLma85X55Pu4tCxyF2FR9E3c2zxtryG6N2oVTnyZt23YrEhEe9kcCX59RdhrDr71Z3zgQkAs8uPMM1JPvMNg
dyNzpgEGGgj9czgBaN5PWrpPBWftg9fte4xYyvJ1BFN5WDvTYfhUtcn1oRTDow67w5zz3adjLDnXLQc6MaowZJ2zyh4PAc1vpstCRtKQt35JEdwfwUe4wzNr3sidChW8VuMU1Lz1cAjvcVHEp1Sabo8FprJwJgRs5ZPA7Ve6LDW7hFa
ngK8YwZmRCmXxArBFVwjfV2SjyhTjhdqswJE5nP6pVnshbV8ZqG2L8d1cwhxpxggmu1jByELxVHF1C9T3GgLDvgUv8nc7PEJYoXpCoyCs55r35h9YzfKgjcJkvFTdfPHwW8fSjCVBuUTKSEAvkRr6iLj6H4LEjBg256G4DHHqpwTgYF
tejc8nLX77LUoVmACLvfC439jtVdxCtYA6y2vj7ZDeX7zp2VYR89GmSqEWj3doqdahv1DktvtQcRBiizMgNWYsjMWRM4BPScnn92ncLD1Bw5ioB8NyZ9CNkMNk4Pf7Uqa7vCTgw4VJvvSjE6PRFnqDSrg4avGUqeMUmngc5mN6WEa3p
xHpkhG8ZngCqKvVhegBAVi7nDBTwukqEDeCS46UczhXMFbAgnQWhExas547vCXho71gcmVqu2x5EAPFgJqyvMmRScQxiKrYoK3p279KLAySM4vNcRxrRrR2DYQwhe8YjNsf8MzqjX54mhbWcjz3jeXokonVk77P9g9y69DVzJeYUvfX
VCjPWi7aDDA7HdQd2UpCghEGtWSfEJtDgPxurPq8qJQh3N75YF8KeQzJs77Tpwcdv2Wuvi1L5ZZtppbWymsgZckWnkg5NB9Pp5izVXCiFhobqF2vd2jhg4rcpLZnGdmmEotL7CfRdVwUWpVppHRZzq7FEQQFxkRL7JzGoL8R8wQG1Uy
BNKPBbVnc7jGyJqFujvCLt6yMUEYXKQTipmEhx4rXJZK3aKdbucKhGqMYMHnVbtpLrQUaPZHsiNGUcEd64KW5kZ7svohTC5i4L4TuEzRZEyWy6v2GGiEp4Mf2oEHMUwqtoNXbsGp8sbJbZATFLXVbP3PgBw8rgAakz7QBFAGryQ3tnx
ytWNuHWkPohMMKUiDFeRyLi8HGUdocwZFzdkbffvo8HaewPYFNsPDCn1PwgS8wA9agCX5kZbKWBmU2zpCstqFAxXeQd8LiwZzPdsbF2YZEKzNYtckW5RrFa5zDgKm2gSRN8gHz3WqS
```

Retrieved P@55w0rd!



```
┌──(root㉿kali)-[/home/kali]
└─# john --show hash
ssh_key.rsa:P@55w0rd!

1 password hash cracked, 0 left
```