



Computer Forensics Project

IT 330

Tasin Naveed(Lead Investigator): 20%
Brandon Hunt: 20%
Philip Abedua: 20%
Mauricio Pereira: 20%
Dharmesh Patel: 20%

Executive Summary

Case: 20130406-19125

Nov 27, 2022

Location: Nuclear power plant in Lower Alloways Creek Township, New Jersey

Suspect: Mr. Alexander Makarov

400 Paramus Rd.

Paramus, NJ 07410

Details: Mr. Alexander Makarov was spotted with a quadcopter capable of video recording and trying to take pictures at the perimeter of the New Jersey nuclear generating stations in Salem County (the Salem and Hope Creek Generating Stations) where taking pictures is prohibited. When the guards confronted him, he sprayed a neuro-paralyzing agent. The police received information and took him to the custody. Police Primarily found he is involved with identity theft and was accused of being a Russian spy. A search warrant was issued and notified the forensics unit to search and analyze all the digital evidence found at his home for further investigation.

Objectives

- Determine possible reasons of violating “No Photos Allowed Zone”
- Obtain evidence demonstrating potential threats contained in the recording devices.

Case Correspondence

Nuclear power plant,
Lower Alloways Creek Township, New Jersey

Dear Forensic Investigator;

Recently we have encountered a man with a quadcopter(equipped with GoPro) and trying to take pictures at the perimeter of no photos allowed zone of our power plant station. He also sprayed a neuro-paralyzing agent to our security guard when they confronted him. Upon investigation by our security staff we found evidence of misuse and possible criminal activity. We have notified the police and they requested a forensic unit to take the digital devices as evidence. We would like you to advise us of your findings.

Attached is the police report regarding the suspect and the digital evidence seized. Please obtain copies of the evidence and evaluate them to determine if he involved in the arsons.

If you need any further information please contact our lead on this case, Richard Mendez, at rmendez@nppt.org or 360.555.2314.

Regards,

John Smith

Security Director

Case Correspondence

Lower Alloways Creek Police Department

From: Detective John Holmes, Counter-Espionage Unit

To: Computer Forensics Investigative Unit

Case: 20130406-19125

The Salem County Police Department is contacting you to request the assessment of digital evidence.

On November 27th, 2022, the Salem County Police Department conducted an investigation in the house of Mr. Alexander Makarov who is suspected of possible Russian spy conducting industrial espionage on US. Mr. Alexander Makarov was taken into custody after being questioned and is maintaining his innocence. Although some physical evidence was captured, the District Attorney does not feel that the evidence is strong enough to bring charges. Mr. Alexander Makarov is not providing any additional information on the advice of his attorney.

A quadcopter capable of video recording was seized at the spot. Further from his home a flash drive and hard drive also seized.

Please examine the provided forensic image of Mr. Alexander Makarov's hard drive and flash drive for evidence that could link him to industrial espionage against US.

Sincerely,

Detective John Holmes, Counter-Espionage Unit

Photography on Prohibited Property

- The foundation for prohibition of photography on private property is trespass.
- A photographer has the right to take photos of nearly anything. The only legal prohibitions relate to a few military installations and nuclear power facilities.
- After 9/11, it is illegal to photograph this building [or oil refinery, or dam, etc.]





Critical Infrastructure Security & Operations Officers

Tips in Responding to a UAS Incident



Direct attention outward and upward to attempt to locate individuals who are holding a controller or device (laptop, notebook, cell phone) and appears to be operating a UAS. Look at windows, balconies, rooftops, and open spaces. For special events, predetermine likely locations that would enable a person to control a UAS.

Report incident to state or local law enforcement immediately and request a response if necessary. Execute organization's emergency response action plan if appropriate.

Observe the UAS and maintain visibility of the device. Look for the direction of travel, damage to facilities, and individuals. NOTE: Battery life is typically 20-30 minutes.

Notice features and identify the type of device (i.e., Fixed-wing/Multi-rotor/Retail or Custom), size, shape, color, payload, video camera equipment, and activity.

Execute appropriate security/emergency response action by maintaining a safe environment for the public and first responders in accordance with Federal, State, and local laws and regulations. Document event details including photos if possible.

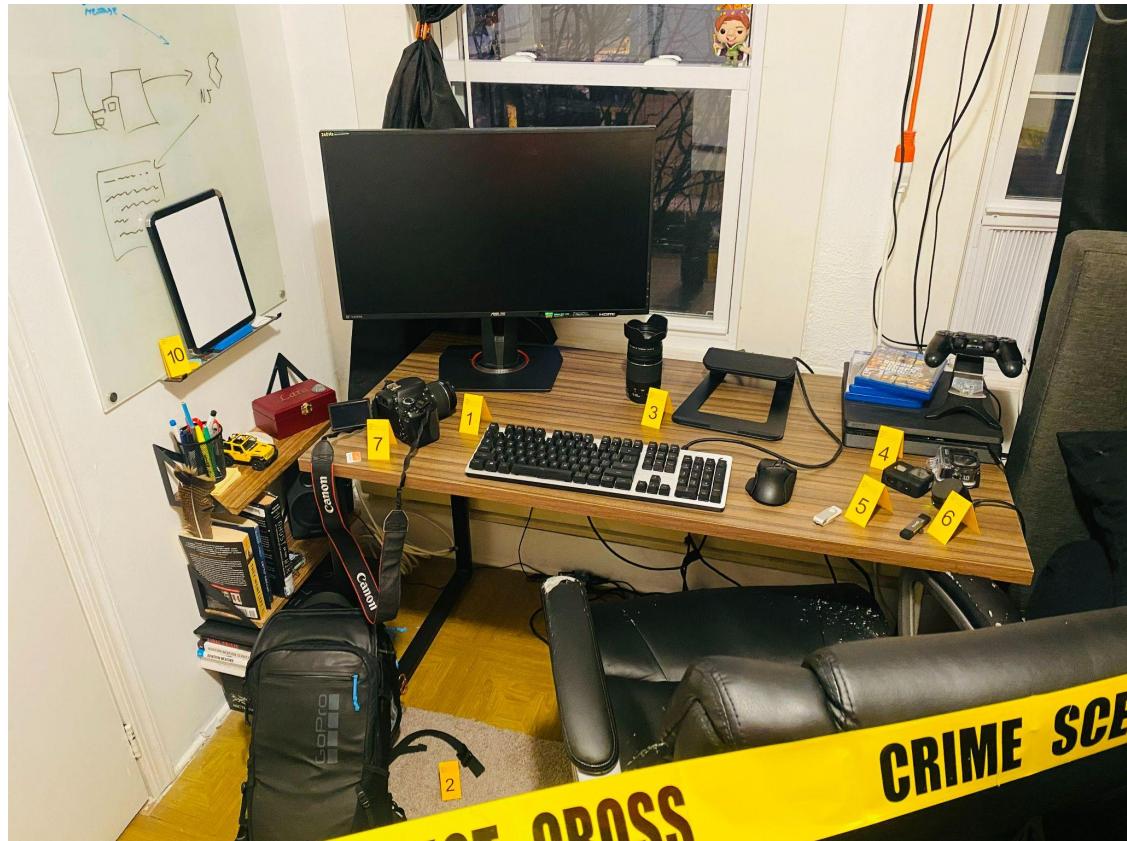
Seized Evidence (Mauricio Pereira)

Items that tell a story:

- No computer found on site
- **1 and 4** - Multiple cameras.
- **3** - DSLR advanced Zoom lens.
- **2 and 6** - Variety of camera accessories.
- **10** - Board notes and plans of Nuclear facility.

Evidence for digital investigation:

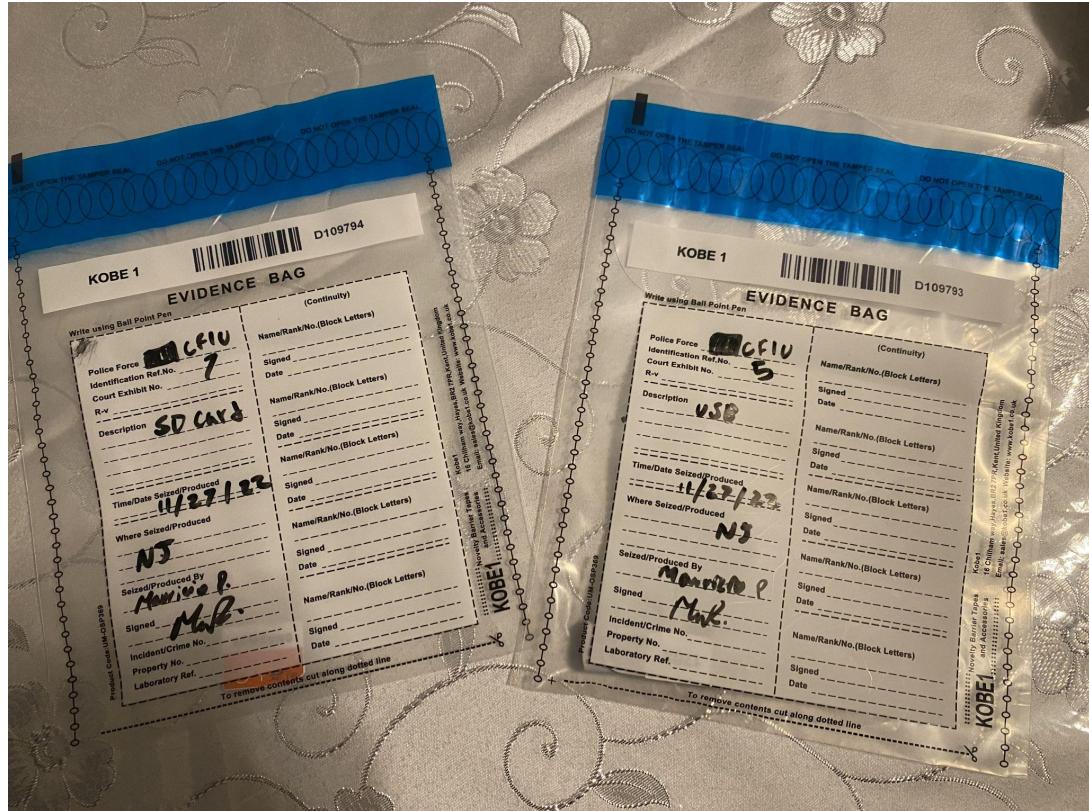
- **5** - USB Flash drive
- **7** - SD memory Card



Seized Evidence (Cont'd)

The evidence was placed in sealed bags along with their respective information:

- **Item 7**
 - **Description:** SD Card
 - **Date:** 11/27/22
 - **Department:** Computer Forensics Investigative Unit
 - **Location:** State of NJ
 - Officer signature
 - **Item 5**
 - **Description:** USB Drive
 - **Department:** Computer Forensics Investigative Unit
 - **Date:** 11/27/22
 - **Location:** State of NJ
 - Officer signature



Search Warrant

AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of New Jersey

In the Matter of the Search of _____
(Briefly describe the property to be searched
or identify the person by name and address)
Suspects residence and all digital devices _____
)

) Case No. 19125
)
)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
The residence of Mr. Alexander Makarov (400 Paramus RD Paramus, NJ 07410) who is suspected of possible Russian spy conducting industrial espionage on the US.

located in the Salem County District of New Jersey, there is now concealed (identify the person or describe the property to be seized):

Mr. Alexander Makarov lives in a gray fenced-off single-family house. All digital devices will be held to a search such as but not limited to, laptops, hard disks, SSDs, USBs, cameras, and phones.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
 contraband, fruits of crime, or other items illegally possessed;
 property designed for use, intended for use, or used in committing a crime;
 a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
18 USC §798.
18 USC §794.
18 USC §795.

Offense Description
Disclosure of classified information
Gathering or delivering defense information to aid foreign government
Photographing and sketching defense installations

The application is based on these facts:
The suspect was trying to take pictures at the perimeter of the no photos allowed zone of the power plant station.
The suspect sprayed a neuro-paralyzing agent.

- Continued on the attached sheet.
 Delayed notice of 5 days (give exact ending date if more than 30 days:) is requested
under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

TN

Applicant's signature
Tasin Naveed

Printed name and title

Sworn to before me and signed in my presence.

Date: 11/29/2022

JR

Judge's signature
John Robert

City and state: Paramus, New Jersey

Printed name and title

First Responder Seizure Record(Philip A)

First responder seizure record indicating the nature of the equipment taken from the suspect's location.

Case No.	22455988/00002		Case Name	Alexander Makarov	
Location of Seizure					
Full Address:	Room No Building Address Line 1 Address Line 2 Address Line 3 Address Line 4 Post code	400 Paramus Rd. Paramus, NJ 07410			
Details of Evidence Seized					
Type: (E.g. computer, disk, paper etc)	Quadcopter, USB Flash drive, SD Memory		Where Located	Perimeter of NJ nuclear generating facilities	
Make	DSLR Advanced		Model	Canon	
Serial No:	C619820		Evidence Bag No:	41912	
Acquisition Details					
Have you enquired of the owner any passwords used?				YES	NO
If yes to above please state passwords and how used.					
Was the equipment attached to a telephone line at the time of seizure?				YES	NO
Was the equipment switched on at the time of seizure?				YES	NO
If yes to above please state how equipment was switched off and secured.					
Has the equipment been switched on since being seized?				YES	NO
If yes to above please state the reason and the details of the person.					
Photos of exhibits taken (If so attach them)	YES	NO	Sketch produced (If so attach it)	YES	NO
Witness Signature (Forensic Analyst making seizure)					
Full Name:	Philip Abedua		Title:	Police Detective	
Phone:	(973)444-6666		Department	Forensics Unit	
Signature:	<i>Philip Abedua</i>		Date and time:	11/27/22 02:30pm	
Witness Signature (Second signature only if required)					
Full Name:	N/A		Title:	N/A	
Phone:	N/A		Department	N/A	
Signature:	N/A		Date and time:	N/A	

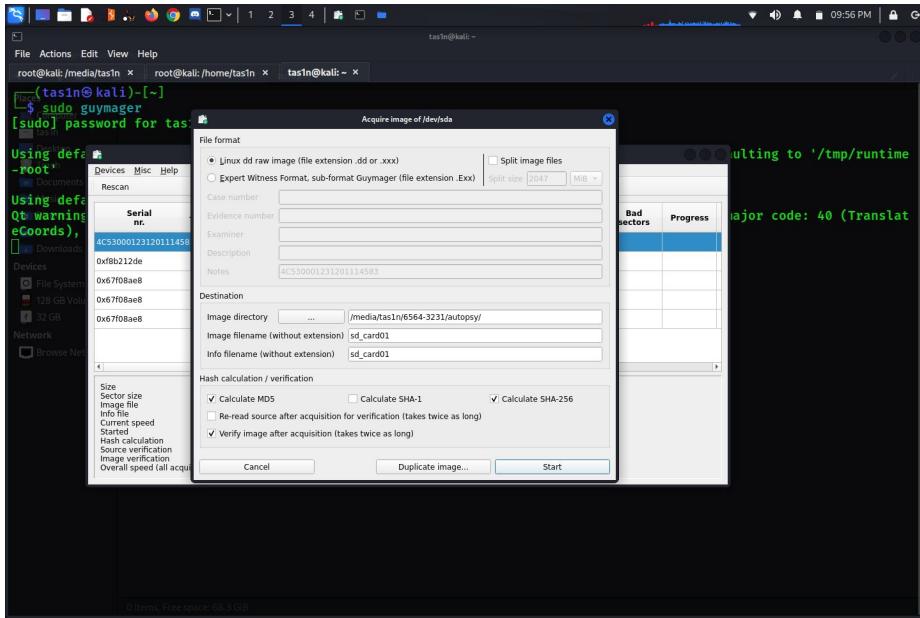
Chain of Custody Log(Dharmesh)

Incident Identification: 25437850-01035

Evidence Custodian: Brandon Hunt

Description of Item	Evidence ID:	Name for Logging Out & Signature	Date Item Received	Name of Person receiving Item back In	Date Item Received
Quadcopter	7425	David Anderson <i>D. Anderson</i>	Nov. 27, 2022	Brandon Hunt <i>Brandon H.</i>	Nov. 28, 2022
USB Flash Drive	6438	David Anderson <i>D. Anderson</i>	Nov. 27, 2022	Brandon Hunt <i>Brandon H.</i>	Nov. 28, 2022
SD Memory	5570	David Anderson <i>D. Anderson</i>	Nov. 27, 2022	Brandon Hunt <i>Brandon H.</i>	Nov. 28, 2022

Making dd image



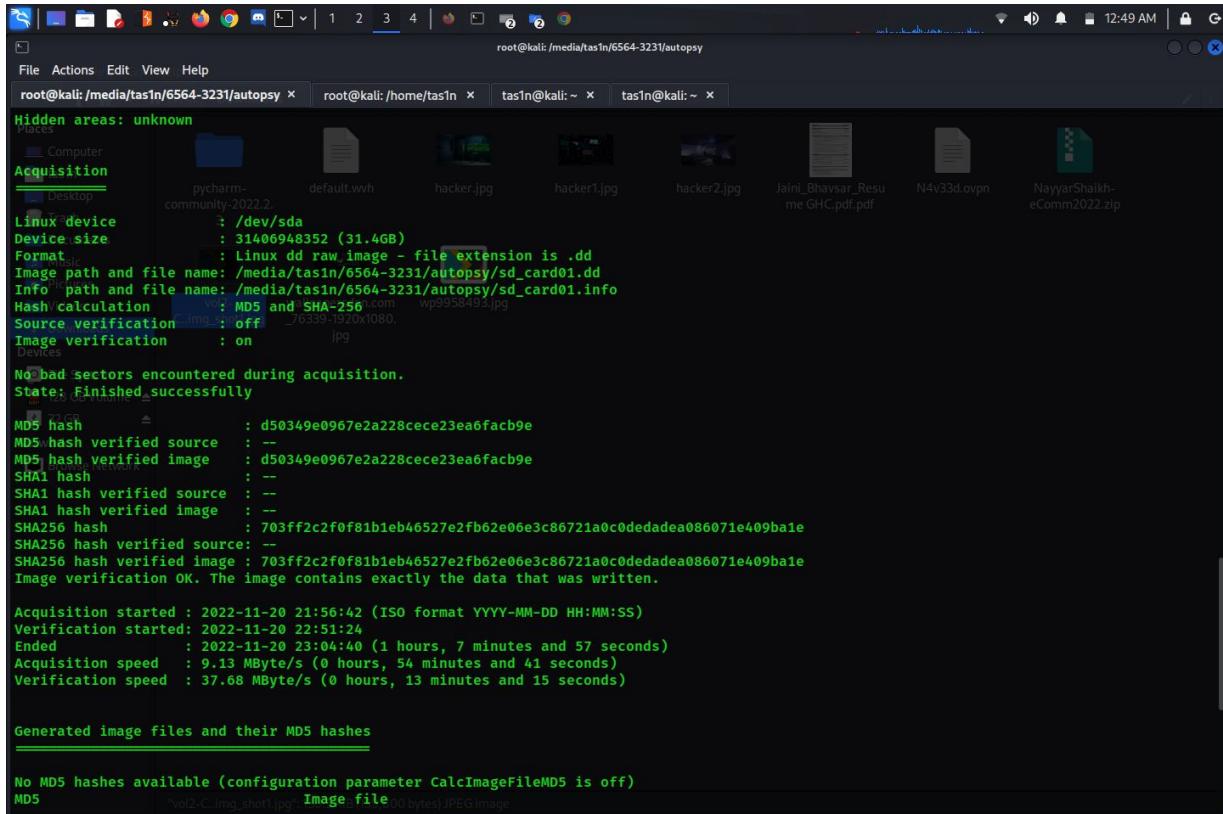
Used “guymager” for creating image

Size	31,406,948,352 bytes (29.3GiB / 31.4GB)
Sector size	512
Image file	/media/tas1n/6564-3231/autopsy/sd_card01.dd
Info file	/media/tas1n/6564-3231/autopsy/sd_card01.info
Current speed	
Started	20. November 21:56:42 (01:07:57)
Hash calculation	MD5 and SHA-256
Source verification	off
Image verification	on
Overall speed (all acquisitions)	

Enabled image verification to maintain the integrity

Hash Comparison

Verified MD5 and SHA256 hash prove that we have not compromised integrity of the evidence. It shows we have the same hash before and after of making dd image.



```
File Actions Edit View Help
root@kali: /media/tasIn/6564-3231/autopsy x root@kali: /home/tasIn x tasIn@kali: ~ x tasIn@kali: ~ x
Hidden areas: unknown
Places Computer pycharm-community-2022.2.desktop default.wvh hacker.jpg hacker1.jpg hacker2.jpg Jaini_Bhavsar_Resume GHC.pdf.pdf N4v33d.ovpn NayyarShaikh-eComm2022.zip
Acquisition
  Desktop : /dev/sda
  Device size : 31406948352 (31.4GB)
  Format : Linux dd raw, image - file extension is .dd
  Image path and file name: /media/tasIn/6564-3231/autopsy/sd_card01.dd
  Info path and file name: /media/tasIn/6564-3231/autopsy/sd_card01.info
  Hash calculation : MD5 and SHA-256
  Source verification : off
  Image verification : on
  Devices
    No bad sectors encountered during acquisition.
  State: Finished successfully
  MD5 hash : d50349e0967e2a228cece23ea6facb9e
  MD5 hash verified source : --
  MD5 hash verified image : d50349e0967e2a228cece23ea6facb9e
  SHA1 hash : --
  SHA1 hash verified source : --
  SHA1 hash verified image : --
  SHA256 hash : 703ff2c2f0f81b1eb46527e2fb62e06e3c86721a0c0dedadea086071e409ba1e
  SHA256 hash verified source: --
  SHA256 hash verified image : 703ff2c2f0f81b1eb46527e2fb62e06e3c86721a0c0dedadea086071e409ba1e
  Image verification OK. The image contains exactly the data that was written.

  Acquisition started : 2022-11-20 21:56:42 (ISO format YYYY-MM-DD HH:MM:SS)
  Verification started: 2022-11-20 22:51:24
  Ended : 2022-11-20 23:04:40 (1 hours, 7 minutes and 57 seconds)
  Acquisition speed : 9.13 MByte/s (0 hours, 54 minutes and 41 seconds)
  Verification speed : 37.68 MByte/s (0 hours, 13 minutes and 15 seconds)

  Generated image files and their MD5 hashes
  _____
  No MD5 hashes available (configuration parameter CalcImageFileMD5 is off)
  MD5      "vol2-C-Img_shott.jpg"  Image file
```

General Analysis

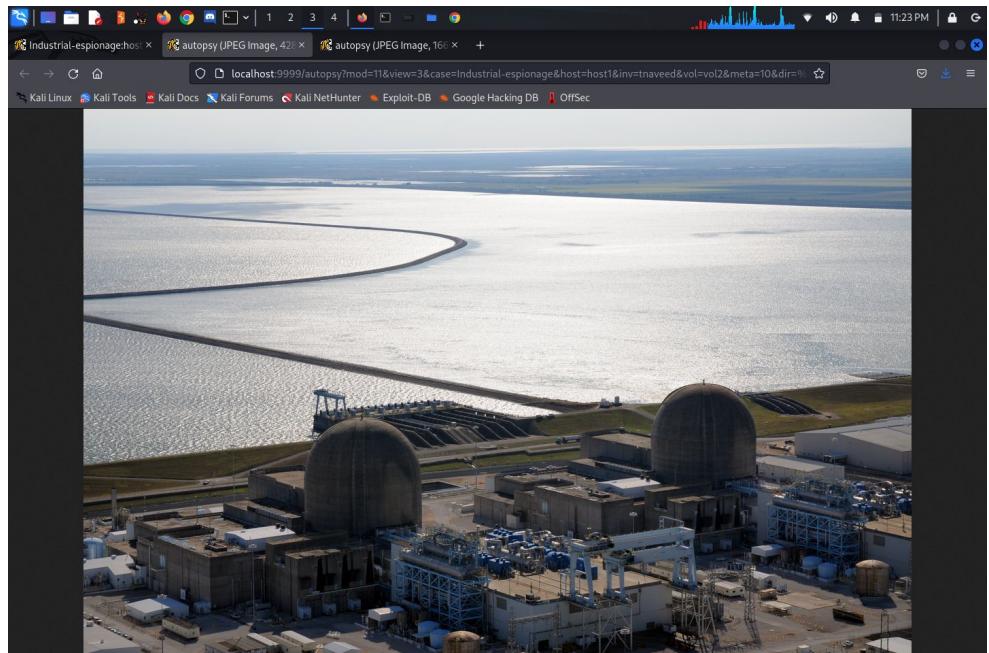
- At our first sight we have found some general footage of the plant. That gives an overview about the plant

The screenshot shows the Industrial-autopsy interface with two tabs open: 'autopsy (JPEG Image, 42)' and 'autopsy (JPEG Image, 16)'. The left pane contains a 'FILE ANALYSIS' section with tabs for KEYWORD SEARCH, FILETYPE, IMAGE DETAILS, META DATA, DATA UNIT, HELP, and CLOSE. Below it is a 'Directory Seek' section where the user has entered 'C:\'. A 'VIEW' button is present. The main area is a 'File Name Search' table:

		STAT1	STAT2	SNR				
v / v		0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	7663616	0	0	980910084
v / v		0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	7663616	0	0	980910085
v / v		0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	980910083
r / r	32 GB (Volume Label Entry)	2022-11-20 21:31:32 (EST)	00:00:00 (UTC)	00:00:00 (UTC)	0	0	0	3
r / r	img_shot1.jpg	2022-11-19 19:34:46 (EST)	00:00:00 (EST)	21:32:13 (EST)	139800	0	0	8
r / r	img_shot2.jpg	2022-11-19 19:34:46 (EST)	00:00:00 (EST)	21:32:13 (EST)	7817142	0	0	10
r / r	erofile.pic.jpg	2022-11-19 17:40:42 (EST)	00:00:00 (EST)	21:32:15 (EST)	183202	0	0	13
d / d	System Volume Information/	2022-11-20 21:31:32 (EST)	00:00:00 (EST)	21:31:30 (EST)	16384	0	0	6

Below the table, there is a 'SEARCH' section with a 'SEARCH' button, an 'ALL DELETED FILES' section, and an 'EXPAND DIRECTORIES' section. At the bottom, there is a 'Thumbnail:' section with a thumbnail image of a nuclear power plant and a 'View Full Size Image' link.

Thumbnail view in autopsy



Larger View of the image

Findings with Autopsy

- We have found some deleted images as well by using autopsy. Among them one of the images set the red flag.
- This image shows he and his wife wearing KGB's uniform which indicates they are possibly involved with spying and industrial espionage.

Screenshot of the Autopsy interface showing file analysis results for a deleted image.

FILE ANALYSIS **KEYWORD SEARCH** **FILE TYPE** **IMAGE DETAILS** **META DATA** **DATA UNIT** **HELP** **CLOSE**

Directory Seek
Enter the name of a directory that you want to view.
C:/

VIEW

File Name Search
Enter a Perl regular expression for the file names you want to find.

SEARCH

ALL DELETED FILES

EXPAND DIRECTORIES

v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	
r / r	32 GB (Volume Label Entry)	2022-11-20 21:31:32 (EST)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	
r / r	img_shot1.jpg	2022-11-19 19:34:46 (EST)	2022-11-21 00:00:00 (EST)	2022-11-20 21:32:13 (EST)	139800	0	0	
r / r	img_shot2.jpg	2022-11-19 19:36:48 (EST)	2022-11-21 00:00:00 (EST)	2022-11-20 21:32:13 (EST)	7817142	0	0	
✓ r / r	profile_pic.jpg	2022-11-19 17:40:42 (EST)	2022-11-20 00:00:00 (EST)	2022-11-20 21:32:15 (EST)	183202	0	0	
d / d	System Volume Information/	2022-11-20 21:31:32 (EST)	2022-11-20 00:00:00 (EST)	2022-11-20 21:31:30 (EST)	16384	0	0	

ASCII (display - report) * Hex (display - report) * ASCII Strings (display - report) * Export * View * Add Note
File Type: JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, progressive, precision 8, 1660x864, components 3

C:/profile_pic.jpg

Thumbnail: [View Full Size Image](#)

Thumbnail of deleted image

Screenshot of the Autopsy interface showing a full-size image of a person in a KGB uniform.

localhost:9999/autopsy?mod=11&view=3&case=Industrial-espionage&host=host1&inv=tnameved&vol=vol2&meta=13&dir=%

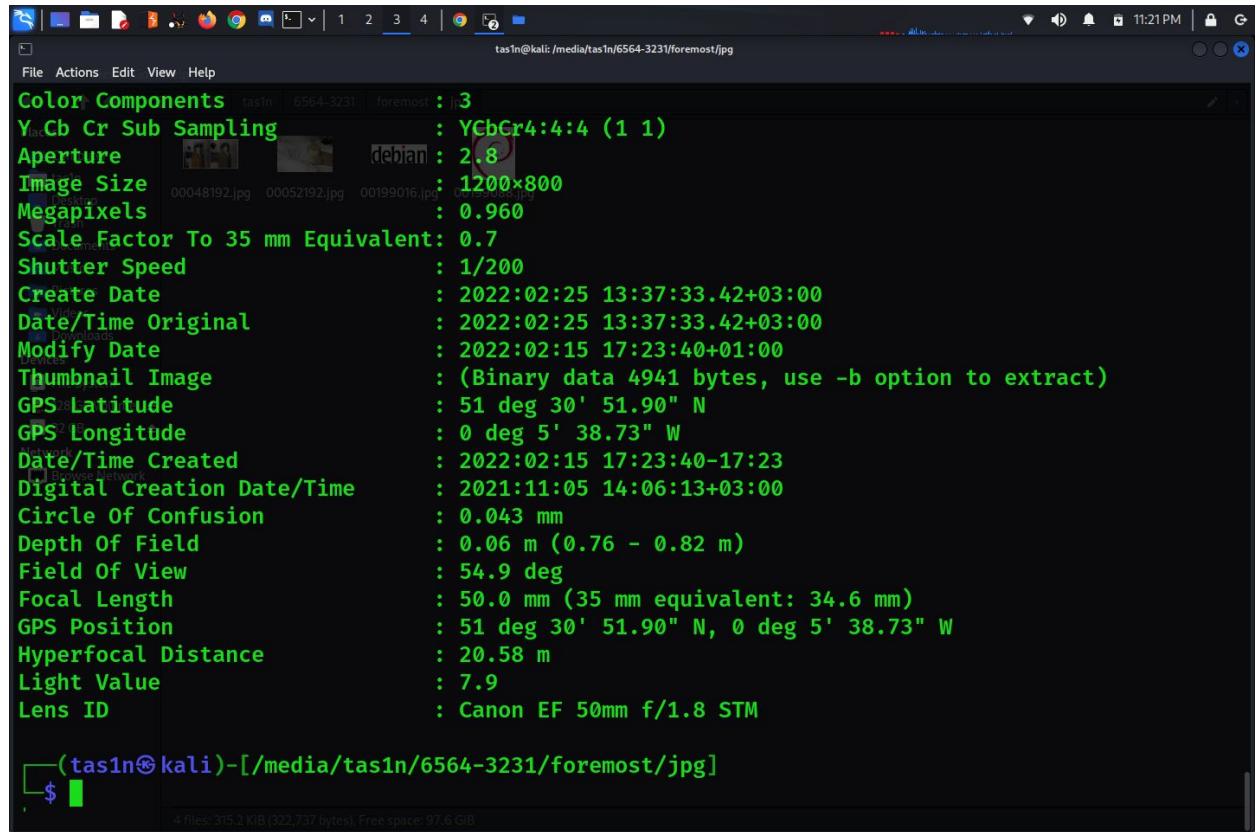
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Full size image

Detailed Analysis

Used **exiftool** and the image had GPS Latitude and Longitude. And the gps position indicates the picture was taken somewhere in Russia.



The screenshot shows a terminal window on a Kali Linux system. The title bar reads "tasIn@kali: /media/tasIn/6564-3231/foremost.jpg". The terminal displays the output of the exiftool command, listing various metadata fields and their values. Key information includes:

- Color Components: YCbCr 4:4:4 (1 1)
- Aperture: 2.8
- Image Size: 1200x800
- Megapixels: 0.960
- Scale Factor To 35 mm Equivalent: 0.7
- Shutter Speed: 1/200
- Create Date: 2022:02:25 13:37:33.42+03:00
- Date/Time Original: 2022:02:25 13:37:33.42+03:00
- Modify Date: 2022:02:15 17:23:40+01:00
- Thumbnail Image: (Binary data 4941 bytes, use -b option to extract)
- GPS Latitude: 51 deg 30' 51.90" N
- GPS Longitude: 0 deg 5' 38.73" W
- Date/Time Created: 2022:02:15 17:23:40-17:23
- Digital Creation Date/Time: 2021:11:05 14:06:13+03:00
- Circle Of Confusion: 0.043 mm
- Depth Of Field: 0.06 m (0.76 - 0.82 m)
- Field Of View: 54.9 deg
- Focal Length: 50.0 mm (35 mm equivalent: 34.6 mm)
- GPS Position: 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
- Hyperfocal Distance: 20.58 m
- Light Value: 7.9
- Lens ID: Canon EF 50mm f/1.8 STM

The terminal prompt at the bottom is "(tasIn㉿kali)-[/media/tasIn/6564-3231/foremost.jpg] \$".

Deleted Files

- Further we used Foremost tool for recovering specific types of files

```
(root㉿kali)-[~/home/tas1n]
root# foremost -v -q -t pdf,jpg,png,docx -i /dev/sda1 -o /media/tas1n/6564-3231/foremost
Foremost version 1.5.7 by Jesse Kornblum, Kris Kendall, and Nick Mikus
Audit File
File Actions Edit View Help
[root@kali ~]# foremost -v -q -t pdf,jpg,png,docx -i /dev/sda1 -o /media/tas1n/6564-3231/foremost
Foremost started at Mon Nov 21 22:30:00 2022
Invocation: foremost -v -q -t pdf,jpg,png,docx -i /dev/sda1 -o /media/tas1n/6564-3231/foremost
Output directory: /media/tas1n/6564-3231/foremost
Configuration file: /etc/foremost.conf
Processing: /dev/sda1
File: /dev/sda1
Start: Mon Nov 21 22:30:00 2022
Length: 29 GB (31405899776 bytes)

Num      Name (bs=512)    Size     File Offset   Comment
0: 00048864.pdf       629 KB    25018368   (PDF is Linearized)
1: 00050144.pdf       654 KB    25673728   (PDF is Linearized)
2: 00051456.pdf       184 KB    26345472   (PDF is Linearized)
3: 00051936.pdf       43 KB     26591232
4: 00052032.pdf       69 KB     26640384
5: 00048192.jpg        178 KB    24674304
6: 00052192.jpg        124 KB    26722304
7: 00199016.jpg         8 KB     101896192

2 folders, 5 files recovered, 35.7 GB.
```

Recovering deleted files with
foremost

File	Name	Size	Offset	Comment
19:	00199100.png	353 B	101939200	(16 x 16)
20:	00199104.png	299 B	101941248	(15 x 16)
21:	Computer00199108.png	321 B	101943296	(15 x 16)
22:	tas1n00199112.png	344 B	101945344	(16 x 16)
23:	Tresh00199116.png	16 KB	101947392	(640 x 480)
24:	09869992.png	1 KB	50534	
25:	09885892.png	209 B	5061576704	(36 x 108)
26:	10420248.png	1 KB	5335166976	(96 x 40)
27:	12198938.png	62 KB	6245856256	(256 x 256)
28:				

Finish: Mon Nov 21 22:52:18 2022

28 FILES EXTRACTED

pdf:= 5
jpg:= 4
png:= 19

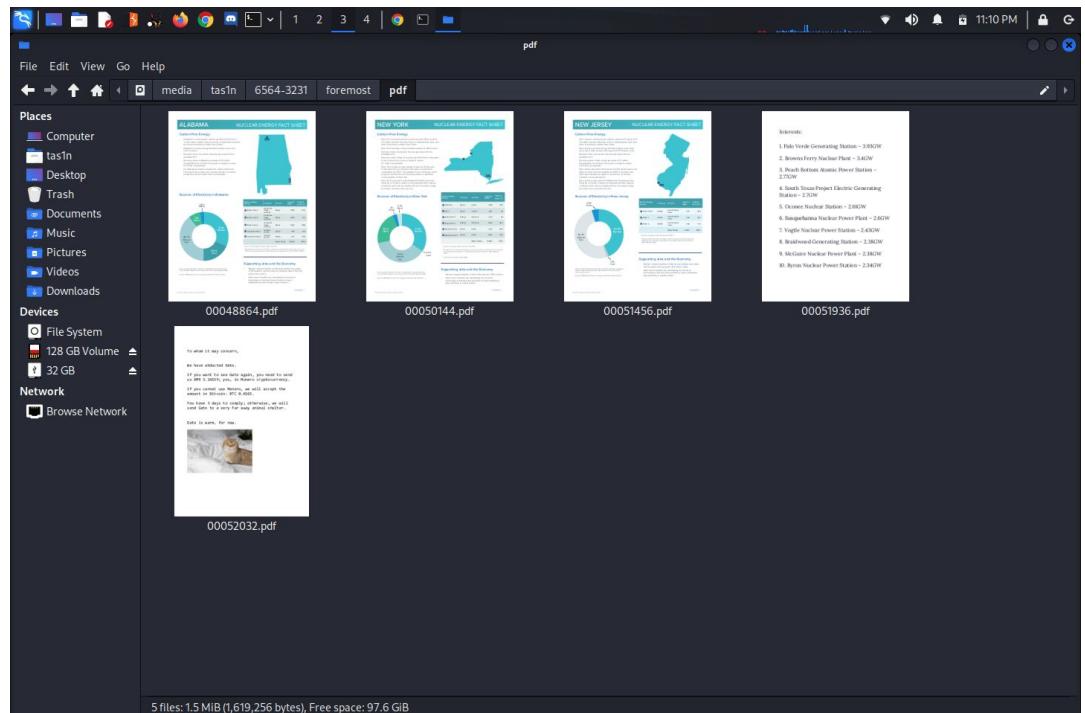
Foremost finished at Mon Nov 21 22:52:18 2022

```
[root@kali ~]#
```

Total 28 of files recovered

Relevant Findings Analysis

- We found pdf files contain names and information of employees.
- Found top 10 powerplant names listed as “interested”. Also some pdf had facts about different nuclear plants of different state.
- All these indicates the involvement of industrial espionage.



Analysis of Relevant Findings



One of the photos was tested for stenography.

StegoVeritas runs several tests on the file including application of filters to visualize stenography.

In this case, it was not visible but it did find something related to the StegHide tool as highlighted above.

```
root@test:/home/mauri/Desktop/forens# stegoveritas nuclear.JPG
Running Module: SVImage
+-----+
| Image Format | Mode |
+-----+
| JPEG (ISO 10918) | RGB |
+-----+
Found something with StegHide: /home/mauri/Desktop/forens/results/steghide_bb2a28385a4f424ae39ec68a50277310.bin
+-----+
| Offset | Carved/Extracted | Description
+-----+
| 0xe8738 | Carved | LZMA compressed data, properties
ry size: 0 bytes, uncompressed size: 128 bytes | E8738.7z |
| 0xe8738 | Extracted | LZMA compressed data, properties
ry size: 0 bytes, uncompressed size: 128 bytes | E8738 |
| 0xffffde7 | Carved | LZMA compressed data, properties
ry size: 0 bytes, uncompressed size: 64 bytes | FFDE7.7z |
| 0xffffde7 | Extracted | LZMA compressed data, properties
ry size: 0 bytes, uncompressed size: 64 bytes | FFDE7 |
+-----+
Running Module: MultiHandler
Exif
====
```

The screenshot shows a terminal window displaying the output of the `stegoveritas` command on a file named `nuclear.JPG`. The output indicates that the module `SVImage` was used and found something related to the `StegHide` tool, specifically a file at `/home/mauri/Desktop/forens/results/steghide_bb2a28385a4f424ae39ec68a50277310.bin`. Below this, the `MultiHandler` module was run, and the `Exif` section shows a series of equals signs (=). To the right of the terminal, a file viewer window titled "Image Viewer" is open, showing a grid of numerous files generated by the analysis process. One file, `nuclear.JPG_red_plane.png`, is selected and displayed in a preview window at the bottom left, showing a red-tinted version of the original nuclear power plant image. Other files in the grid include various enhanced versions of the image, such as `nuclear.JPG_enhance...`, `nuclear.JPG_Green_...`, and `nuclear.JPG_Mode...`.

Analysis of Relevant Findings (Cont'd)

After StegOveritas results, `stegHide` was ran in attempt to extract the hidden information.

It indeed found an embedded file called "Secret.txt"

The Text file turned out to have a message written in Russian!

When translating the Russian text, It appears to have been a secret communication to the recipient suggesting that there was low security in that particular area.

Firefox Web Browser Dec 1 02:50

G translate english to russi... https://www.google.com/search?q=translate+ 80%

About 1,030,000,000 results (0.43 seconds)

Russian English

Я добрался до ближайшей точки ко входу в ядерную базу в Салеме с востока. С этой стороны не хватает безопасности. - Александр Макаров

I got to the nearest point to the entrance to the nuclear base in Salem from the east. There is a lack of security on this side.
- Alexander Makarov

es Terminal Dec 1 02:46

root@test:/home/mauri/Desktop/forens

```
root@test:/home/mauri/Desktop/forens# steghide info nuclear.JPG
"nuclear.JPG":
  format: jpeg
  capacity: 49.5 KB
Try to get information about embedded data ? (y/n) y
Enter passphrase:
embedded file "secret.txt":
  size: 242.0 Byte
  encrypted: rijndael-128, cbc
  compressed: yes
root@test:/home/mauri/Desktop/forens# steghide extract -sf nuclear.JPG
Enter passphrase:
wrote extracted data to "secret.txt".
root@test:/home/mauri/Desktop/forens# cat secret.txt
Я добрался до ближайшей точки ко входу в ядерную базу в Салеме с востока. С этой стороны не хватает безопасности. - Александр Макаров
root@test:/home/mauri/Desktop/forens#
```

Supporting Details

- The combination of the intention to hide questionable photos and the gps location coordinates recovered with exiftool suggests possible identity fraud
- The combination of the violation of the “No Photography Rule” and spraying a neuro-paralyzing agent suggests possible espionage
- The combination of several power plants labels as interested and the collection of employee's and their information suggests possible industrial espionage

Investigative Leads

- Further investigation of digital storage mediums in possession of the suspect may be necessary to determine if there are photos of anything that is not allowed to be photographed
- Further investigation of digital storage mediums in possession of the suspect may be necessary to determine if the recovered photos were taken in Russia and how the suspect would've obtained these storage mediums
- Further investigation of digital storage mediums in possession of the suspect may be necessary to determine what the label "interested" means to the suspect
- Further investigation of the suspect's home may be necessary to determine if he/she had obtained the neuro-paralyzing spray legally

References

- <https://steghide.sourceforge.net/>
- <https://exiftool.org/>
- <https://www.uscourts.gov/sites/default/files/ao106.pdf>
- <https://foremost.sourceforge.net/>