
	IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b>	Report written by: <b>Jesse Russell</b> Revision: 1
---	--	---

## 1 Contents

2	Executive Summary.....	2
3	Incident Discovery.....	3
3.1	Summary .....	3
3.2	Action Items – investigation artifacts .....	3
3.3	Description of system(s)- drive geometry.....	3
4	Forensics Process .....	3
4.1	Tools (list all tools used).....	3
4.2	Evidence to Analyze - Fill out data .....	4
5	Results and Findings.....	4
5.1	Analysis of Evidence.....	4
5.1.1	deathstar.jpg.....	4
5.1.2	notes.txt .....	5
5.1.3	xwing physics.png .....	5
5.1.4	xwing-cockpit1.jpg .....	6
5.1.5	x-wing-cockpit2.jpg.....	6
5.1.6	x-wing3.jpg.....	7
5.1.7	\$R810TZ.jpg.....	7
5.1.8	\$RU90TV.webp.....	8
5.1.9	\$RX4HKQJ.jpg.....	9
6.0	Conclusion.....	9


	IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b>	Report written by: <b>Jesse Russell</b> Revision: 1
---	--	---

## 2 Executive Summary

Forgive my Star Wars errors – the last movie I saw was the original release in 1977, at a theater 😊. Some of the information has been created by me, but I thought a Star Wars theme might be fun.

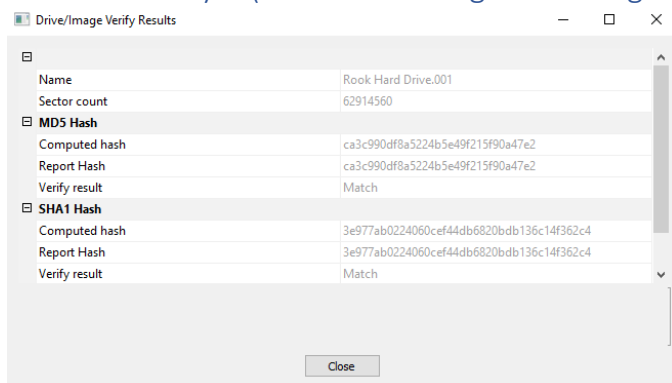
**Bodhi Rook**, is a former Imperial cargo pilot who, under the influence of Galen Erso, an Imperial scientist who worked on the Death Star project., Rook defected to the Rebel Alliance in an attempt to steal the plans to the Death Star. He fought alongside a group of rebels during the Battle of Scarif, where he was killed. After his death, Galen Erso, hear rumors that Rook may have been a double agent and was in fact passing information back to the Empire. In this scenario, you have been hired by the Rebel Alliance as forensic investigator set to clear Bodhi Rook's good name. You have been given access to Rook's computer, which no one has touched since his death, to form your report. It is expected, and normal, that Bodhi would have images and information on the x-wing, but not other alliance technology.

**Nature of the case:** **Investigation into the suspicions that Bodhi Rook is secretly transmitting confidential Rebel information to the Empire.**

	<p>IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b></p>	<p>Report written by: <b>Jesse Russell</b> Revision: 1</p>
---	---	--

### 3 Incident Discovery

#### 3.1 Summary - (include screen grab of image hash)



Galen Erso is suspicious that Bodhi Rook is treacherously transmitting confidential information to the enemy, The Galactic Empire. This report will look at the evidence and attempt to make a determination of guilt as to whether or not Bodhi committed this act.

#### 3.2 Action Items – investigation artifacts there are 9 evidence files in this case

Item to analyze	Assigned to	Status / Completion date
<b>deathstar.jpg</b>	<b>Jesse Russell</b>	<b>1/23/2021 10:47 AM</b>
<b>notes.txt</b>	<b>Jesse Russell</b>	<b>1/23/2021 11:00 AM</b>
<b>xwing physics.png</b>	<b>Jesse Russell</b>	<b>1/23/2021 11:05 AM</b>
<b>xwing-cockpit1.jpg</b>	<b>Jesse Russell</b>	<b>1/23/2021 11:20 AM</b>
<b>x-wing-cockpit2.jpg</b>	<b>Jesse Russell</b>	<b>1/23/2021 11:21 AM</b>
<b>xwing3.jpg</b>	<b>Jesse Russell</b>	<b>1/23/2021 11:29 AM</b>
<b>\$R810TZ.jpg</b>	<b>Jesse Russell</b>	<b>1/23/2021 11:42 AM</b>
<b>\$RU9OTSV.webp</b>	<b>Jesse Russell</b>	<b>1/23/2021 11:44 AM</b>
<b>\$RX4HKQJ.jpg</b>	<b>Jesse Russell</b>	<b>1/23/2021 11:49 AM</b>

#### 3.3 Description of system(s)- drive geometry

### 4 Forensics Process

#### 4.1 Tools (list all tools used)

##### 4.1.1 ProDiscover 8.2.0.2


This is a program used for finding and analyzing

##### 4.1.2 FTK Imager 4.5.0.3

This is a free program used to obtain the image form the VM OVA.

##### 4.1.3 WinMD5Free

This is a free program used to generate MD5 hashes for files.

	IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b>	Report written by: <b>Jesse Russell</b> Revision: 1
---	--	---

## 4.2 Evidence to Analyze - Fill out data

File name	MD5	Status
<b>deathstar.jpg</b>	e5f0b7e7dacc649933c4cbf539f23c9f	Completed
<b>notes.txt</b>	5c7cea9233192b061bb34a7dfdbf2ed8	Completed
<b>xwing physics.png</b>	09ce7d6c75f6a36ec0c1a757a68a56c6	Completed
<b>xwing-cockpit1.jpg</b>	f6ba746add858be3ca5648e75d4a2df9	Completed
<b>x-wing-cockpit2.jpg</b>	6020f4a687815c231a156b8358ca70a0	Completed
<b>xwing3.jpg</b>	74d86ea2e4699974cca45523fecc9f0b	Completed
<b>\$R810TZ.jpg</b>	151befd6bc85b659281fd54b5bef4a8f	Completed
<b>\$RU9OTSV.webp</b>	9f2cf83694bff39472316d9080338264	Completed
<b>\$RX4HKQJ.jpg</b>	13d41b39a7c31da14888e5b986eb56c8	Completed

## 5 Results and Findings

### 5.1 Analysis of Evidence


#### 5.1.1 deathstar.jpg

Image:



D:\Users\Bodhi Rook\Desktop

MD5: e5f0b7e7dacc649933c4cbf539f23c9f

	IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b>	Report written by: <b>Jesse Russell</b> Revision: 1
---	--	---

Comment: This appears to be an image of the Death Star that the rebels are trying to get the plans for.

#### 5.1.2 notes.txt

```

Leia,

If you're reading this it means I have failed my mission. My attempt to retrieve the death star plans has failed.

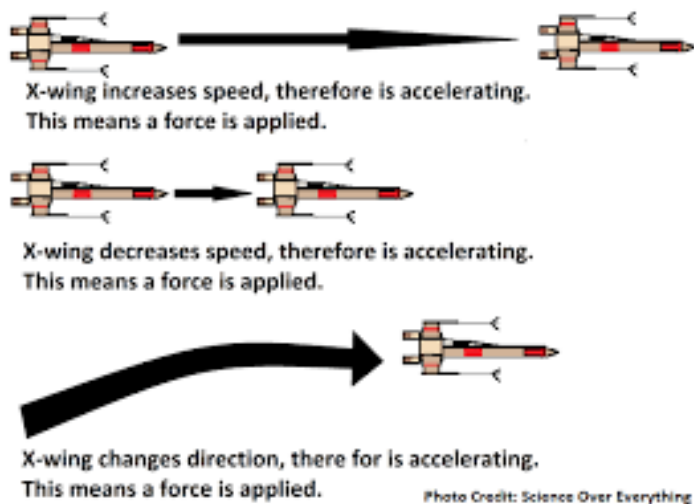
Bodhi Rook

```

D:\Users\Bodhi Rook\Documents  
 MD5: 5c7cea9233192b061bb34a7dfdbf2ed8


Comment: This appears to be a note from Bodhi Rook to Princess Leia, informing her of his death and failure.

#### 5.1.3 xwing physics.png



D:\Users\Bodhi Rook\Documents  
 MD5: 09ce7d6c75f6a36ec0c1a757a68a56c6

Comment: This appears to be diagram of the physics of an X-Wing fighter, which is normal for Bodhi to have access to.

	IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b>	Report written by: <b>Jesse Russell</b> Revision: 1
---	--	---

5.1.4 xwing-cockpit1.jpg



D:\Users\Bodhi Rook\Pictures

MD5: f6ba746add858be3ca5648e75d4a2df9

Comment: This appears to be an image of an X-Wing cockpit, which is normal for Bodhi to have.


5.1.5 x-wing-cockpit2.jpg



D:\Users\Bodhi Rook\Pictures

MD5: 6020f4a687815c231a156b8358ca70a0

Comment: This appears to be another image of an X-Wing cockpit, which is normal for Bodhi to have.

	<p>IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b></p>	<p>Report written by: <b>Jesse Russell</b> Revision: 1</p>
---	---	--

#### 5.1.6 x-wing3.jpg

D:\Users\Bodhi Rook\Pictures



MD5: 74d86ea2e4699974cca45523fecc9f0b


Comment: This appears to be an image of an X-Wing fighter, which is normal for Bodhi to have.

#### 5.1.7 \$R810TZ.jpg

D:\\$Recycle.Bin\S- 1-5-21-3517868603-3021280496-499751809—1002



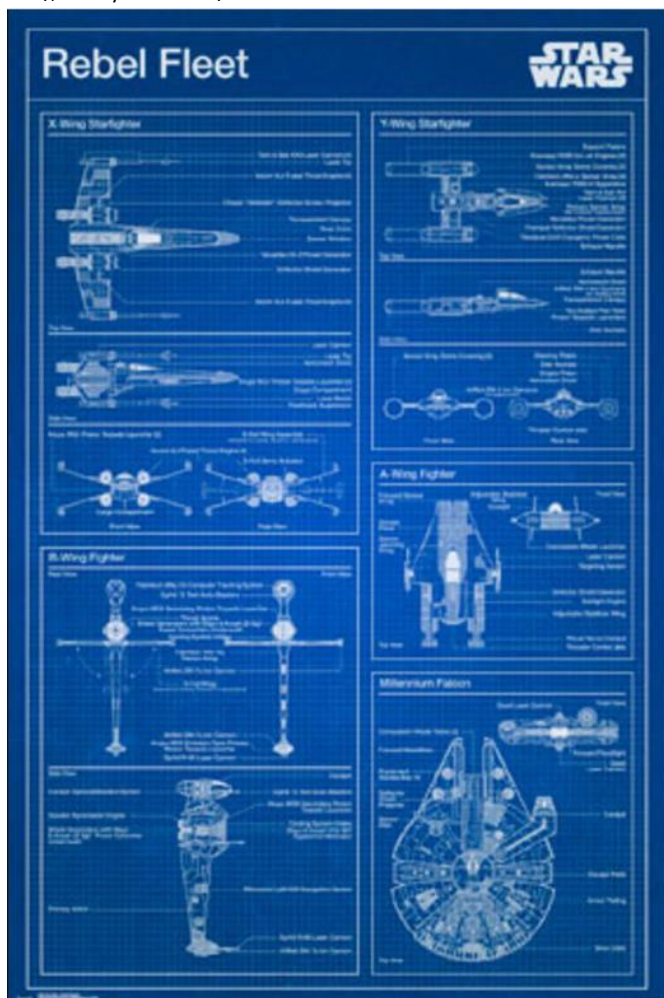
MD5: 151befd6bc85b659281fd54b5bef4a8f

	<p>IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b></p>	<p>Report written by: <b>Jesse Russell</b> Revision: 1</p>
---	---	--

Comment: This appears to be the rebel insignia, it was deleted and found in the recycle bin.

5.1.8 \$RU90TV.webp


D:\\$Recycle.Bin\S- 1-5-21-3517868603-3021280496-499751809—1003



MD5: 9f2cf83694bff39472316d9080338264

Comment: This appears to be some blueprints for rebel ships, including some that are not X-Wings, which Bodhi should not have access to. It was deleted and found in the recycle bin.



	<p>IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b></p>	<p>Report written by: <b>Jesse Russell</b> Revision: 1</p>
---	---	--

#### 5.1.9 \$RX4HKQJ.jpg

D:\\$Recycle.Bin\S- 1-5-21-3517868603-3021280496-499751809—1003



MD5: 13d41b39a7c31da14888e5b986eb56c8

Comment: This appears to be an image of Darth Vader, who is a top military leader for the Empire. It was deleted and found in the recycle bin.

#### 6.0 Conclusion

Given the evidence above, I determined that there is not sufficient evidence to determine if Bodhi Rook was, in fact, transmitting confidential information to the Empire. After this determination, however, I did notice some pieces of evidence that are suspicious and may warrant further investigation. I found multiple images regarding X-Wings, which is not suspicious because Bodhi should have access to these. What I found suspicious was the group of files that were deleted and found in the recycling bin folder. Bodhi had an image of other Rebel technologies that he should not have access to, as well as a picture of the Empire's leader, Darth Vader. The fact that these were deleted raises some suspicion, as this suggested he had a reason to hide them. My professional advice would be to investigate these pieces further to form a solid determination of guilt.


**Provide summary conclusion as instructed in class**

Delete your Rook files when you are satisfied with your report

=====

A peak ahead – **Steganography** - *the practice of concealing messages or information within other non-secret text or data. (Web Dictionary)*

1. Install WinRAR to your forensic desktop.

	IA-427 Forensics Report Internal Case <b>Bodhi Rook</b> Incident Status: <b>COMPLETE</b>	Report written by: <b>Jesse Russell</b> Revision: 1
---	--	---

2. Turn on “view file extensions” in your 4n6 OS
3. Copy the Deathstar.jpg image to another location on your desktop
4. Change the file extension to .zip
5. Open the zip
6. Aha-steganography was used- Hook his more data inside the deathstar.jpg image.
7. Did you find it??
8. More inside x-wing3.jpg