BRNO UNIVERSITY OF TECHNOLOGY

FACULTY OF INFORMATION TECHNOLOGY

The General - Digital Investigation Case Report

Digital Forensics

Marián Kapišinský (xkapis00)

April 30, 2022

Contents

1 Introduction

After an extensive undercover operation, a known arms dealer named Monsieur Victor, commonly known as "The General," was lured out of hiding and apprehended in the Netherlands. He had expected a meeting to finalize a large sale of weapons, including tanks, missiles, attack helicopters, and assault rifles. Instead, he met with the police. When he realized the situation, he threw a mobile device in a nearby canal. The device was later retrieved by scuba divers and was found to be a Sony Ericsson K800i Cybershot.

Mr. Victor has been connected with several front companies, and a fleet of military cargo planes used to deliver weaponry. He has openly mocked arms embargoes and is suspected of selling arms to both sides in military conflicts around the globe. As a result of his brazen behavior of delivering large shipments to high-risk regions all over the world, he developed a reputation as the „UPS of arms dealers". In some situations, he traded weapons in exchange for oil, copper, cobalt, uranium 294, 298, 380, thorium, titanium and other materials he could resell. However, in the past, investigators could not find sufficient evidence to link him to any arms deals. Despite regular surveillance by authorities and efforts to the monitoring of his communications, he managed to slip through the net of several sting operations. One of his methods of operation is to use stolen and/or throw away cell phones, making it more difficult for investigators to track and monitor his activities.

In the current operation, undercover investigators arranged an arms deal through one of Mr. Victor's front companies, Smurf Celtic. To convince him that the deal was real, an initial down payment was made by electronic funds transfer to Smelt Bank in France into an account owned by another front company named RipTide Security. His meeting in Amsterdam was to finalize the full payment to a bank account in Dubai.

The goal is

- to prove connection of Monsieur Victor to the sale of arms through Smurf Celtic,
- to find evidence of the receipt of payment to RipTide Security,
- and to recover any leads that might connect Monsieur Victor to other individuals, companies, or bank accounts that are involved in his international arms business,

from the image of the device that was created and stored in XRY image format, and memory dumps of NAND and NOR flash memories.

2 Investigation

The investigation has been carried out in two steps. Firstly, the XRY image was examined using the XRY Reader 5.0 (see section 2.1). Several suspicious contacts, SMS messages, pictures, and a video were found. However, no undeniable evidence of connection between Monsieur Victor and Smurf Celtic or RipTide Security was found. All found items are listed in the section 2.2.

In the second step, hexdumps (see section 2.1) of the NAND and NOR flash memories were created and examined. Several emails were found on the NAND flash, and an address book was found on the NOR flash. All found items are listed in the section 2.2.

The section 2.1 provides a description of used tools. The section 2.2 provides a list of all evidence found on memory images.

2.1 Tools

XRY Reader 5.0 XRY Reader is an application for opening `.xry` image files. XRY files are used for mobile forensic purposes and may contain multiple types of data downloaded from a phone, including the phone book, call list, text messages, pictures, calendars, notes, audio, and video files.

hexdump 2.0.2 Hexdump is a utility that helps us to investigate the contents of a binary files. It can be used for data recovery, reverse engineering, and programming.

Scalpel 2.0 Scalpel performs file carving operations based on patterns that describe particular file. It was used to find XML files, HTML files, and pictures. However, nothing interesting was found.

2.2 Evidence

This section provides all relevant evidence found in each file. Table 2.1 contains suspicious contacts, table 2.2 contains suspicious SMS messages, and Figure 2.1 contains suspicious images found in the XRY file. There was also an video called MOV00002.3GP. Next, emails, an MMS, email settings, a recent list, and other texts that were recovered from the NAND flash are listed. Finally, there are two contacts listed that were found on the NOR flash.

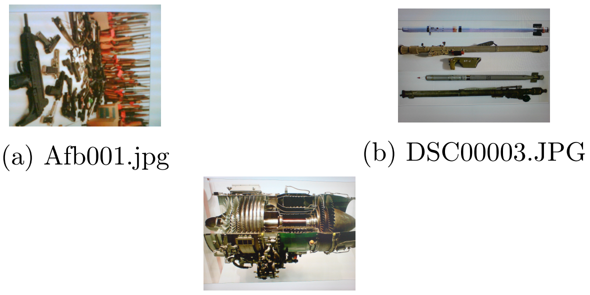
XRY

Table 2.1: Contacts

Name	Number	Email	Address
No Name	0628954735	Smurf_Celtic@live.com	Paddolaan 5, Meppel, Drenthe, 1245 TG, Netherlands
MV	0612803819	MVictor1956@gmail.com	-

Table 2.2: SMS

Number	Timestamp	Message	Status
+31628954735	3/30/2010 08:04:30	OK, will look after it	Read
+31631356695	3/30/2010 08:16:58	Can you deliver 100 J85-21 replacement engines in Irak in one week?	Read
+31633930545	4/1/2010 19:52:14	When shipped will arrive (translated)	Read
+31633930545	4/1/2010 19:58:17	Thanks for the quick response and we will wait for the shipment! Iraq (translated)	Read



(a) Afb001.jpg

(b) DSC00003.JPG

(c) DSC00004.JPG

Figure 2.1: Pictures found on the device

NAND

Emails recovered from the NAND flash:

- Email 1:
  - **Timestamp**: 2010-03-27 11:38:50
  - **From**: MVictor1956@gmail.com

  - **To**: Smurf_Celtic@live.com
  - **Subject**: Contact
  - **Attachment**: None
  - **Content**: None

- Email 2:
  - **Timestamp**: 2010-03-28 04:12:18
  - **From**: MVictor1956@gmail.com
  - **To**: grassyjansen@yahoo.com
  - **Subject**: Engine
  - **Attachment**: DSCOOOO4.JPG (see Figure 2.1c)
  - **Content**: „Dear mister Dutch, Is this what you mean? Kind regards, MV"

- Email 3:
  - **Timestamp**: 2010-03-29 04:39:30
  - **From**: MVictor1956@gmail.com
  - **To**: Smurf_Celtic@live.com
  - **Subject**: Buy
  - **Attachment**: None
  - **Content**: „Hi, Make sure replacement engines are bought. I will arrange further air deployment for customer. Best regards, MV"

- Email 4:
  - **Timestamp**: 2010-03-29 05:10:08
  - **From**: MVictor1956@gmail.com
  - **To**: Riptide101@rocketmail.com
  - **Subject**: Delivery
  - **Attachment**: None
  - **Content**: „Arrange for delivery of some stuff from Germany to iraq. Not via normal, MV"

- Email 5:
  - **Timestamp**: 2010-03-30 15:41:01
  - **From**: MVictor1956@gmail.com
  - **To**: Smurf_Celtic@live.com
  - **Subject**: Content
  - **Attachment**: None
  - **Content**: „Hi, Can you contact Iraquer? He wants to know when it arrives. MV"

- Email 6:

  - **Timestamp**: 2010-04-02 04:21:36
  - **From**: Riptide101@rocketmail.com
  - **To**: MVictor1956@gmail.com
  - **Subject**: payment
  - **Attachment**: None
  - **Content**: None

Suspicious MMS was found on the NAND flash, which was followed a call from in the call history in the XRY file. Details of the MMS:

- **Timestamp**: 2010-03-27 11:32:21
- **From**: - (supposedly this device)
- **To**: 0643926087
- **Subject**: For an example look at this short movie.
- **Attachment**: MOV00002.3GP (can be found in the XRY file)

Other suspicious texts found on the NAND flash or the XRY file:

- Sir is going to contact you about some rockets.
- Uranium 294, 298, 380
- Everything arranged! (Sent to 0615646978)

Email settings:

- **Account name**: Mv
- **Incoming mailbox**: MVictor1956@gmail.com
- **Incoming password**: Bollinger1975

A recent list was found on the offset 0x2d96aad on the NAND flash:

- 0650428000
- 0632082356
- 0615646978
- 0643926087
- 0620125081
- 0632122345
- Smurf_Celtic@live.com

- Riptide101@rocketmail.com
- grassyjansen@yahoo.com
- MuhammedAamina@hotmail.com
- DunkinBlue@hotmail.com
- 0631356695

NOR

Some names and addresses were found around the offset 0x3fc0ce0 on the NOR flash. Some correspond with the contacts found in the XRY file, but there are two new entries:

- Contact 1:
  - **Name**: Geen naam, RipTide Security
  - **Address**: Hekweg 5, Scheveningen, Zuid-Holland, 2495PG, Netherlands
  - **Contact**: Riptide101@rocketmail.com
- Contact 2:
  - **Name**: Fadhel Alhassouni
  - **Address**: Taylor street 5, Bagdad, FL 32530, Iraq

3 Conclusion

From the collected evidence, the connection of Monsieur Victor to Smurf Celtic is clearly shown from the email communication, namely emails 1, 3, and 5. The subject names and content of those emails clearly show intentions of making sale of an replacement engines.

Furthermore, the email named „payment" from „Riptide101@rocketmail.com", found on the NAND flash, suggests that a payment was mode. However, no detailed information about the transaction was found.

While browsing the hexdumps, many other contacts were found, namely in the recent list (see NAND in section 2.2) and one more contact on the NOR flash (see NOR in section 2.2).

Finally, the supposed timeline of the engine sale is shown in the Fig. 3.1.

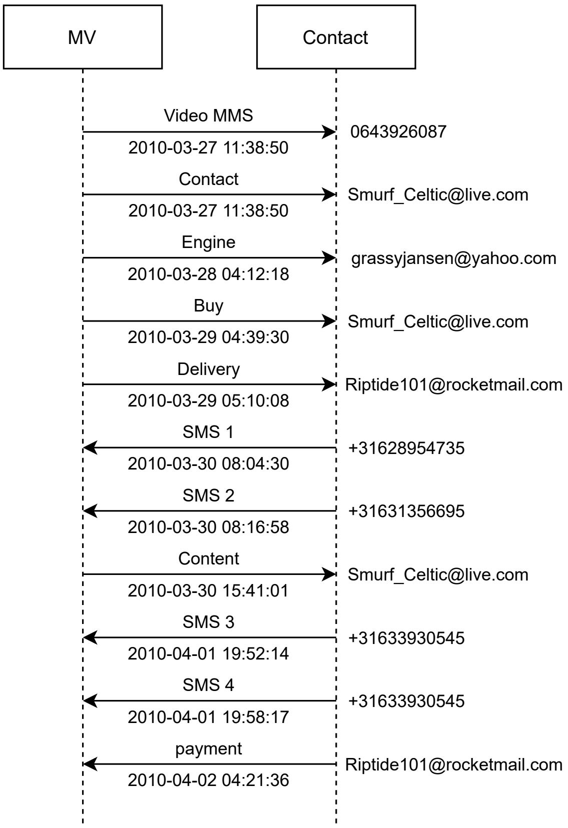


Figure 3.1: Timeline of the email and mobile communication