



---

## Digital Forensics Report

### Authors

### Group 12

89415 - António Lopes

90074 - Francisco Romão

92513 - Mafalda Ferreira

### 1 Do you find any traces of the documents that Mr. Daniels claims to have in his possession? Present your findings explaining the procedure you followed to retrieve these documents.

Charles Daniels claimed to have in his possession proof that Levy Fran Velucci, president of the Red Hawks Football Club, was involved in a fraudulent transaction of one of the club's stars by diverting 3 million euros into his bank account. After examining a copy of Mr. Daniels' files, extracted from his pen drive, we found 5 crucial hidden documents (5 PDFs):

- Artifact no. 1 - **Red Hawks Club Statement** (*red\_hawks\_club\_statement.pdf*)

The first document we found was hidden in the ticket.jpg file.

We started by creating a hex dump of the file by running the Linux command `xxd ($ xxd ticket.jpg | grep "%PDF")` and found a PDF signature (%PDF-).

We then ran the Linux command `xedit ($ xedit ticket.jpg)` to edit the file and formatted the text to include everything from the signature until the trailer (%%EOF).

The result was a club statement signed by Mr. Velucci, directly related to James Santos' transfer, including the amount of money involved.



### List of commands:

1. `$ xxd ticket.jpg | grep "%PDF"`
2. `$ xedit ticket.jpg` (from %PDF- until %%EOF)



### Club Statement

Red Hawks Football Club can confirm that it has formally come to an agreement with both Mattressmakers Football Club and James Santos for his transfer to the club.

The club has informed the Securities Market Commission that Mattressmakers Football Club will pay € 80,000,000 (eighty million euros) for the transfer of the player, from which € 8,000,000 (eight million euros) will be directly paid to George Sednem, James Santos' agent, who had a determinant role in closing the deal.

Therefore, Red Hawks Football Club will receive the total amount of € 72,000,000 (seventy-two million euros).

Moreover, Red Hawks are delighted to announce this important deal as it represents a significant amount of money to the club's balance sheet that will help us grow and become more competitive.

We would like to thank James Santos for his excellent contribution as a Red Hawk and wish him all the best for the future.

August 30, 2021

The President of Red Hawks Football Club,

*Levy Fran Velucci*

**Figure 1** - Hidden artifact no. 1, a club statement regarding James Santos' transfer

- Artifact no. 2 - **James Santos player profile** (*James\_Santos\_profile.pdf*)

Our next finding was "inside" the file daft\_punk.gif.

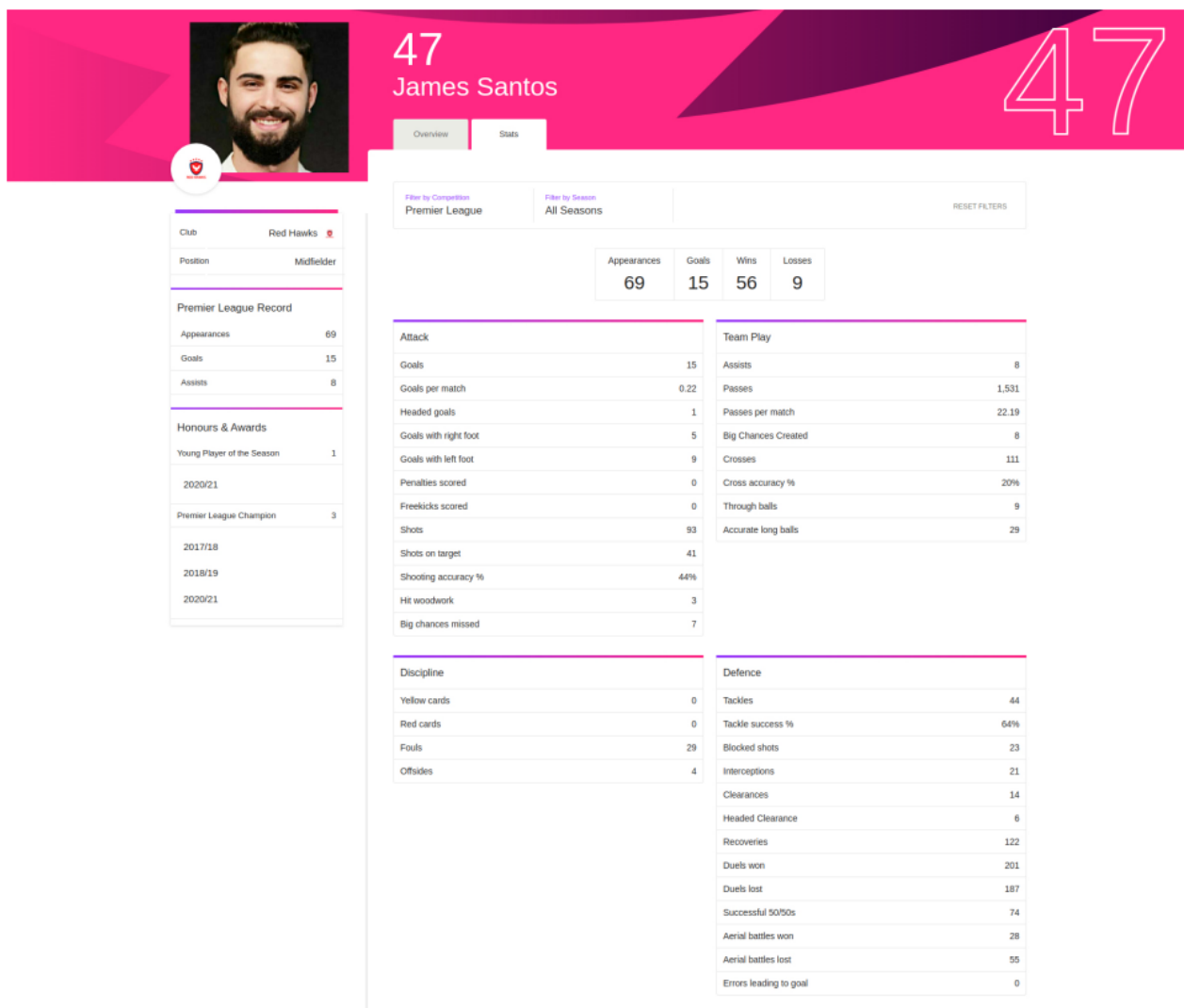


After reading its metadata, by running the exiftool Linux command (`$ exiftool daft_punk.gif`) we realised there was a *Comment* tag with a hidden file, in this case a ZIP file due to its signature (PK..).

After extracting the ZIP (`$ exiftool -Comment -b daft_punk.gif > secret.zip`), there was a file named James\_Santos\_profile.pdf inside it as shown below. As the file name indicates it's a profile from none other than the player in question.

### List of commands:

1. `$ exiftool daft_punk.gif`
2. `$ exiftool -Comment -b daft_punk.gif > secret.zip`
3. `$ unzip secret.zip`



**Figure 2** - Hidden artifact no. 2, James Santos' player profile with all his statistics

Our next step was to try and extract a password protected ZIP file with the name chants.zip. Our immediate thought was to run fcrackzip, a Kali Linux tool used as a fast password cracker specifically for ZIP files with brute force or dictionary based attacks.

We tried using a famous dictionary called RockYou (`$ fcrackzip -D -p rockyou.txt chants.zip`), which didn't work.

After that, we decided to gather every word we could find from all the files we had access to and built our custom dictionary. We then ran it through CUPP (Common User Passwords Profiler) using the -w option (`$ cupp -w custom_dict.txt`) to improve our wordlist (wasn't really necessary). When we ran fcrackzip again (`$ fcrackzip -D -p custom_dict.txt chants.zip`) it showed a list of possible passwords and running it with the -u option (`$ fcrackzip -D -u -p custom_dict.txt chants.zip`) listed the correct password - *Wichita* - from the file SNA\_Football\_Lyrics.mp4 which is a Seven Nation Army lyrics video.

Extracting chants.zip gave us two new files to analyze: chant1.wav and chant2, where artifacts no. 5 and no. 3 were hidden, respectively.

#### List of commands:

1. `$ fcrackzip -D -p rockyou.txt chants.zip` (didn't work)
2. `$ cupp -w custom_dict.txt` (unnecessary after building custom dictionary)
3. `$ fcrackzip -D -p custom_dict.txt chants.zip`
4. `$ fcrackzip -D -u -p custom_dict.txt chants.zip`
5. `$ unzip chants.zip`

- Artifact no. 3 - **Red Hawks FC Internal Communication** (*red\_hawks\_fc\_internal\_communication.pdf*)

As said before, artifact no. 3 was obtained through chant2.

Repeating the same process as artifact no. 1 (`$ xxd chant2`) we quickly noticed a PDF trailer (%%EOF) and scrolling to the top of the hex dump we detected that the signature was incorrect, it only showed 1.5.

After correcting it by adding %PDF- to the beginning of the file (`$ xedit chant2`) it revealed an internal communication from the club's board which seemed to be against the transfer as shown below.

#### List of commands:

1. `$ xxd chant2`
2. `$ xedit chant2` (add %PDF-)





## Internal Communication

To: Levy Fran Velucci  
From: Board of Directors  
CC: Ryan Coast  
Date: 08/23/2021

This is to express the Board's views on the ongoing negotiations for the transfer of the professional football player James Santos.

Although the Board believes that the value offered for the player may positively influence the Club's balance sheet, it is also expected that the value may double within 3 to 6 months, due to the player's performance over the first games of the ongoing season.

Furthermore, the Board believes that the value to be paid to the player's agent severely impacts the overall negotiation, as the margin being offered - 10% of the value - exceeds any previous margins negotiated by the Club, setting a precedent for the future.

**Figure 3** - Hidden artifact no. 3, board's opinion about James Santos' transfer

- Artifact no. 4 - **Holy Spirit Bank Statement of Account** (*holy\_spirit\_bank\_statement\_of\_account.pdf*)

The file *hbfs.wav* hadn't been examined at this time so it was our next focus.

We decided to take the first easy step and listen to the audio. We noticed the first seconds had only noise and the music only started after seven seconds. This seemed weird and we immediately thought something was hidden within the audio file. With this in mind, we decided to analyze the content of the file.

To begin, we decided to take a look at the metadata of the audio file using *exiftool* (`$ exiftool hbfs.wav`) confirming this was a WAVE audio file with 16-bit frames, one channel and 48000 Hz.

We then ran the *strings* command on Linux to look for recognizable sequences of characters (`$ strings hbfs.wav`). When scrolling down to the bottom of the output, we faced an interesting URL (<https://bit.ly/39jit4x>) that redirected us to download a file named tool.

Since we had no idea what the purpose of this tool was, we decided to take a look at its printable content (`$ strings tool`). We noticed some familiar sequences of characters and understood this tool was, in fact, a stenography tool to “hide files within least significant bits of mono (1 channel) wav sound files”, as written in the content of the file.

Since the extension of the tool was unknown, we ran the command `file` to determine the file type (`$ file tool`). This command immediately confirmed it was a Python 3.8 byte-compiled file. Knowing this, we added `pyc` to the extension of the file, which corresponds to a byte-compiled file.

After looking into it, we understood that it was possible to recover the original Python file using a decompiler, after a quick google search we found the following online website <https://www.toolnb.com/tools-lang-en/pyc.html> that uses the `uncompyle6` python library. The output of the conversion revealed the algorithm that was used to hide the file inside the WAV audio.

With the possession of the original code, we were now able to analyze it carefully and came to the following conclusions:

- This tool was able to hide files within the least significant bits of a mono channel wav sound file;
- The `password` defines the offset, from the beginning of the audio, where the payload starts to be injected into the audio file;
- The `payload_size` corresponded to the size of the file to be hidden;
- The `n_lsb` corresponded to the number of bits hidden within a single frame (16 bits) of the file.

Consequently, we assumed that it would be necessary to do reverse engineering of the original tool in order to extract the original file hidden in `hbfs.wav` so we created a Python tool named `reverse.py`. This tool used five parameters: `audio_path`, `n_lsb`, `password`, `payload_bits` and `output_path`.

Firstly, we set `payload_bits` to a reasonably high number, similar to the size of other documents that we had in possession, which would be 400000 in this case.

Then, we had to figure out the combination between the number of LSBs and the password. We tried the following combinations of `n_lsb` and `password`: (1, 0), (2, 0) (`./reverse.py hbfs.wav 1 0 400000 extracted_secret` and `./reverse.py hbfs.wav 2 0 400000 extracted_secret`) but we weren't successful since the content of the output file was considered random and didn't have any shreds of evidence of a valid file. We verified this by running `xxd` (`$ xxd extracted_secret`). Then, we decided to set both `n_lsb` and `password` to 2 and ran the reverse tool (`$ ./reverse.py hbfs.wav 2 2 400000 extracted_secret`). Now we were able to extract a pdf document regarding the statement of Velucci's bank account.


Although we already had the document in hand, we decided to verify its content using `xedit` (`$ xedit extracted_secret`) and removed any content before the signature (`%PDF-1.5`) and



after the trailer (%%EOF). We also renamed the file and added the missing extension (\$ `mv extracted_secret holy_spirit_bank_statement_of_account.pdf`).

#### List of commands:

1. \$ `exiftool hbfs.wav`
2. \$ `strings hbfs.wav` (copy link and download tool)
3. \$ `strings tool`
4. \$ `file tool` (add `pyc` as tool extension)
5. \$ `uncompyle6 tool.pyc tool.py`
6. \$ `./reverse.py hbfs.wav 1 0 400000 extracted_secret` (unsuccessful)
7. \$ `./reverse.py hbfs.wav 2 0 400000 extracted_secret` (unsuccessful)
8. \$ `./reverse.py hbfs.wav 2 2 400000 extracted_secret`
9. \$ `xedit extracted_secret` (remove "garbage" before %PDF and after %%EOF)
10. \$ `mv extracted_secret holy_spirit_bank_statement_of_account.pdf`



HOLY SPIRIT BANK

231 Valley Farms Street  
Saint Peter  
accounts@hsb.com

STATEMENT OF ACCOUNT

Account Number: 339-834-926-290

Statement Date: 09/13/2021

Period Covered: 08/06/2021 to 09/07/2021

Page 1 of 1

Levy Fran Velucci

2450 Courage St, STE 108

Brownsville

Girighet St. Branch

Opening Balance: 2,175,800.00

Total Credit Amount: 3,010,000.00

Total Debit Amount: 94,000.00

Closing Balance: 5,081,800.00

Account Type: Current Account

Number of Transactions: 8

Transactions

Date	Description	Credit	Debit	Balance
08/12/2021	Payment - Credit Card		5,400.00	2,170,400.00
08/17/2021	Payment - Insurance		3,000.00	2,167,400.00
08/31/2021	Payment - Fresh Scallop Ltd.		1,500.00	2,165,900.00
08/31/2021	Payment - Vine&Wine Co.		600.00	2,165,300.00
08/31/2021	Payment - Eden Hotel & Spa		13,500.00	2,151,800.00
08/31/2021	Account Transfer Out		80,000.00	2,071,800.00
09/06/2021	Account Transfer In	3,000,000.00		5,071,400.00
09/11/2021	Cheque Deposit	10,000.00		5,081,400.00
--- End of Transactions ---				

Figure 4 - Hidden artifact no. 4, Mr. Velucci's bank account statement

- Artifact no. 5 - **The Hawks Official Supporters Statement** (*the\_hawks\_official\_supporters\_statement.pdf*)

Finally, running the same command as we did in the previous artifact (`$ strings chant1.wav`), the same link to the previous tool was present, so we decided to try and use the same script as before.

Firstly, we decided to use the same parameters in order to extract the hidden file inside chant1.wav using the reverse tool (`$ ./reverse.py hbfs.wav 2 2 400000 extracted_secret2`) and we were immediately successful and able to get a valid PDF document pretty straight forward.

As we did previously regarding the 4th artifact, we decided to verify the document's content using xedit (`$ xedit extracted_secret2`) and removed any content before the signature (%PDF-1.5) and after the trailer (%%EOF). We also renamed the file and added the missing extension (`$ mv extracted_secret the_hawks_official_supporters_statement.pdf`)

The final artifact was a statement from the official supporters of the team directed to Mr. Velucci, also expressing their opinion towards James Santos' sale.

#### List of commands:

1. `$ strings chant1.wav`
2. `$ ./reverse.py hbfs.wav 2 2 400000 extracted_secret2`
3. `$ xedit extracted_secret2` (remove "garbage" before %PDF and after %%EOF)
4. `$ mv extracted_secret2 the_hawks_official_supporters_statement.pdf`





## The Hawks

---

### Official Supporters Statement

To the President of The Red Hawks FC:

As the oldest support group of The Red Hawks FC, we, The Hawks, hereby express our total disagreement with the ongoing negotiations for the transfer of The Red Hawks FC player James Santos.

The club's performance has been positively affected by James Santos, one of the best midfielders to ever play for The Red Hawks. The team's morale has improved enormously since James joined the team.

With this said, we believe that if the transfer is confirmed to happen, The Red Hawk FC will be severely damaged by those who are in charge.

We, The Hawks, will not let greed be the ruler of the club and will fight to defend The Red Hawks values no matter the cost.

August 27, 2021

- The Hawks

**Figure 5** - Hidden artifact no. 5, official supporters' opinion regarding James Santos' sale

All of the analysis was done on a forensically sound virtual machine, in this case, a Kali Linux VM and the names and MD5 values of the found artifacts and the used script are indicated in the following table.

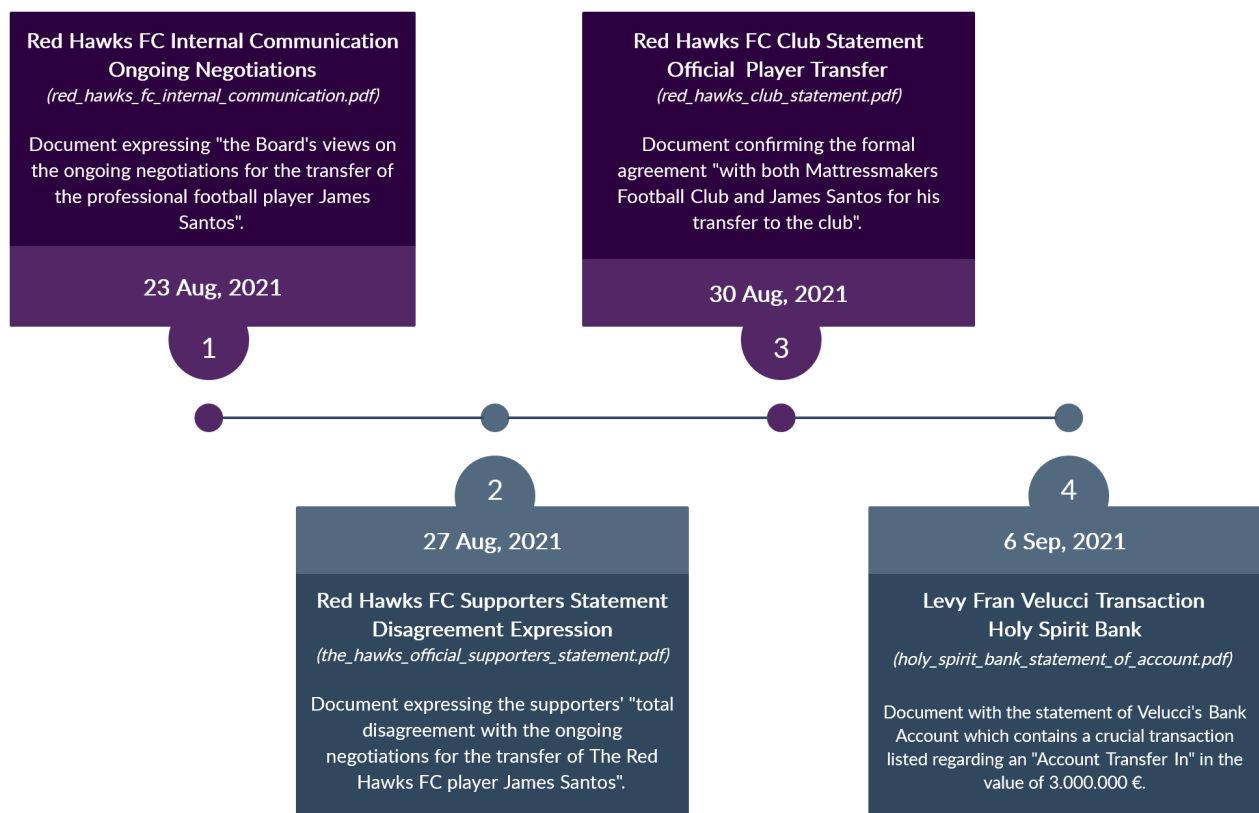
File	MD5 value
red_hawks_club_statement.pdf	e02839232a2283ac0843de8ecfc980a0
James_Santos_profile.pdf	44d015d11ecd0ec4ecaa6cb350032d17
red_hawks_fc_internal_communication.pdf	5756cd174e320710ec928f709a7ab743
holy_spirit_bank_statement_of_account.pdf	d566359b0a1f83ec3cc18bd9ffec7509
the_hawks_official_supporters_statement.pdf	dcc0b9a023db329076cec9e1f59a972a
reverse.py	d8a82a0180ae226248d51b01233633bc

**Table 1** - File names and respective MD5 values



## 2 In case you found any relevant documents, what can you learn from them at this point? Do they support the original hypothesis of Mr. Velucci's fraudulent actions put forth by Mr. Daniels?

After analyzing all the documents associated with this case, we managed to create a timeline related to all the relevant events that will be covered next (figure 7). This timeline includes all three statements and communications of Red Hawks FC and their supporters and one relevant transaction made into Velucci's bank account.



**Figure 7** - Timeline of events based on the artifacts' creation dates

After exploring in detail all the files inside Mr. Daniels' pen drive, we discovered five hidden documents. With this in mind, we suspected that two things could have happened. Either Mr. Velucci's was the real responsible for these crimes in Red Hawks FC or Mr. Velucci's was incriminated by someone that had access to his documents and, at this point, the only person who could be suspect for the incrimination would be Mr. Daniels. In fact, it is suspicious that Mr. Daniels would have hidden so many artifacts inside his pen-drive but, for now, we can't point a finger at him.

At the beginning of this investigation, we found a document from August 30, 2021 (artifact no. 1 - *red\_hawks\_club\_statement.pdf*) regarding the transfer of James Santos from the Red Hawks. This document reveals the total amount of 80,000,000 € (eighty million euros) involving the transfer from which 72,000,000 € (seventy-two million euros) were destined to the Red Hawks and the other 8,000,000 € (eight million euros) were given to James Santos' agent. At this point, we can confirm that there were some money transactions involved but we didn't find anything related to the diversion of 3,000,000 € (three million euros) to Mr. Velucci's bank account.

At the end of the investigation, we found a really suspicious document from September 6, 2021 (artifact no. 4 - *holy\_spirit\_bank\_statement\_of\_account.pdf*) regarding a statement of Velucci's bank account. After analyzing this document, we could verify several high valuable transactions from 2021:

Transactions				
Date	Description	Credit	Debit	Balance
08/12/2021	Payment - Credit Card		5,400.00	2,170,400.00
08/17/2021	Payment - Insurance		3,000.00	2,167,400.00
08/31/2021	Payment - Fresh Scallop Ltd.		1,500.00	2,165,900.00
08/31/2021	Payment - Vine&Wine Co.		600.00	2,165,300.00
08/31/2021	Payment - Eden Hotel & Spa		13,500.00	2,151,800.00
08/31/2021	Account Transfer Out		80,000.00	2,071,800.00
09/06/2021	Account Transfer In	3,000,000.00		5,071,400.00
09/11/2021	Cheque Deposit	10,000.00		5,081,400.00
--- End of Transactions ---				

**Figure 6** - Transactions from Mr. Velucci's bank account (artifact no. 4)

Among these eight transactions, we could easily see one with a certain amount that we had seen before and this would be the transaction from 09/06/2021 (September 9, 2021) where there was the accreditation of 3,000,000 € (three million euros) into the account, regarding an "Account Transfer".

Until then, we could prove three things:

- The amount of this transaction is exactly the same as the one from Mr. Daniels' accusations about Velucci's diversion.
- The transaction was described as an "Account Transfer In" which is the same method reported in the accusation.
- The bank transaction was recorded on the 9th of September, 2021 which was after the official transaction of James Santos done on the 30th of August, 2021.

Finally, with this analysis in mind and assuming that all these pieces of evidence are legit and were not modified by Mr. Daniels, we can easily infer that these two documents regarding the player transfer and the bank transactions are strong pieces of evidence that support the original hypothesis of Mr. Velucci's fraudulent actions.

### **3 From the analysis of all provided artifacts, what else have you learned? Present every interesting insight you may have gained, e.g., about the potential identity of involved stakeholders, sources of leakage, skill level of the individuals responsible for the leakage, etc.**

Firstly from the document where the transaction is settled (artifact no. 1), it is agreed that James Santos' manager is to receive 8 million dollars which is 10% of the total transaction price, however, the letter from the Board of Directors (artifact no. 3), on the 23rd of August, showed their disagreement about the price paid to the manager. Besides that, the team's support group, "The Hawks" expressed their total disagreement (artifact no. 5) on the deal that was being decided to buy the new player, stating that the ones who were in charge would severely damage the team.

Despite the clear opposition, the contract was signed on the 30th of August. This evidence and the fact that the contract was still signed may reveal that the director, who signed the contract, may have made a deal to pay such a high value to the player's manager with the objective of being compensated by him afterward. However, this is just an allegation without concrete evidence, for now.

Furthermore, we found odd the fact that the documents from August 23 and August 27 (artifacts no. 3 and no. 5), concerning, respectively a Red Hawks FC Internal Communication and an Official Supporters Statement, were in the possession of Mr. Daniels, since he, supposedly, does not have access to internal documents. These types of documents may contain confidential communication and should not be accessible from the club's exterior.

### **4 Based on your findings, suggest the next steps you would take to pursue this investigation.**

Although Mr. Daniels claims that Velucci was responsible for these fraudulent actions and the evidence found during the investigation supports this hypothesis, it is relevant to understand how Mr. Daniels got access to the documents inside the pen drive. Therefore, one next step in the investigation could be to trace the steps that lead him to the possession of the documents and possibly identify if these documents were actually modified in order to incriminate Velucci.

As stated in the last question it is known for a fact that the president received the amount of 3 million dollars, however, it is not known who made this transaction.

The next step, following this evidence, could be finding the origin of this capital and, perhaps, the owner of the original account who may have been involved in this fraudulent transaction.