INSTITUTO SUPERIOR TÉCNICO

Departamento de Engenharia Informática

Forensics Cyber Security

MEIC / METI 2021-2022 – 1st Period

# Digital Forensics Report

**Fátima Napoleão - 91605**

**Miguel Henriques - 102148**

**Ielga Oliveira - 92479**

## 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.

Analisando os ficheiros fornecidos encontrámos os cinco artefactos pedidos. Para os encontrar primeiramente, analisámos superficialmente todos os ficheiros no geral, em seguida passamos para uma análise mais profunda, para isso recorremos a várias ferramentas de steganography e outros comandos descritos nos pontos a seguir:

- ticket.jpg: executamos no terminal o comando **xxd ticket.jpg** e reparamos que no final havia um EOF o que significou a existência de um ficheiro PDF. Para extraí-lo recorremos ao binwalk e executamos o comando **binwalk –D=".*"ticket.jpg,** este gera uma pasta **_ticket.jpg.extracted,** no interior da mesma encontramos o primeiro artefacto **ticket.pdf** (135A0).
- daft_punk.gif: recorremos ao exiftool para obter informação sobre este ficheiro. Antes de tudo executamos o comando **exiftool -v daft_punk.gif,** que nos ajudou a identificar o ficheiro James_Santos_profile.pdfUT que estava inserido na tag comment (Comment=PK.....qu(SXm.. James_Santos_profile.pdfUT). Para conseguirmos extraí-lo utilizamos este comando: **exiftool -b comment daft_punk.gif > out,** que gera um zip **out** que descompactado contém o segundo artefacto **(James_Santos_profile.pdf)**.
- hbfs.wav: executamos no terminal o comando **xxd hbfs.wav** e analisando os dados encontramos um link (https://bit.ly/39jit4x ) que corresponde à tool. No terminal executamos o comando **file tool** para descobrir que tipo de ficheiro correspondia – phyton 3.8. Para descompilar alteramos o nome para tool.pyc e utilizamos o descompilador online Toolnb (https://www.toolnb.com/tools-lang-en/pyc.html). Após análise do código da tool desenvolvemos um script que extrai de um ficheiro wav os "Less Significant Bits". Sendo que os documentos que tínhamos encontrado até agora eram pdf, fizemos com que o script procurasse os bits correspondentes aos 3 caracteres iniciais da signature do PDF. O script**(lsb.py)** encontrou então um pdf e escreveu os bytes para um ficheiro**(result.bin).** Para remover tudo após o End of File fizemos análise binária do ficheiro, vimos o offset do %%EOF e por último executamos o comando **dd ibs=1 count=$((0x9609)) if=result.bin of=hbfs.pdf.** (hbfs.pdf) que é o terceiro artefacto.

Os ficheiros SNA_Footbal_Lyrics.mp4, Ram.jpg, Homework.jpg, Discover.jpg ajudaram-nos a descobrir a palavra-passe da pasta chant. Chegamos a conclusão de que a palavra-passe estava ligada a banda Daft Punk. No entanto,

recorremos a ferramenta cupp que gerou um dicionário com a letra da música Seven Nation Army -( https://www.letras.mus.br/the-white-stripes/67250/) e com os anos de lançamento dos álbuns. Tentamos as palavras-passes que o dicionário gerou por força bruta e descobrimos que a palavra-passe é **Wichita.**

Para ter acesso aos documentos da pasta chants utilizamos a palavra-passe Wichita, extraímos e analisámos os dois ficheiros que lá estavam:

- chant2 - executamos no terminal o comando **xxd chant2** e reparamos que no início tem uma parte da signature de PDF (%PDF-1.5, sendo que continha o 1.5) e no final tem um EOF. Usamos um comando para adicionar os bytes referentes à signature (**printf "\x25\x50\x44\x46\x2d" | cat - chant2 > chant2.pdf**) e verificamos que este ficheiro era um ficheiro PDF válido**(chant2.pdf)** quarto artefacto.
- chant.wav - o procedimento que utilizamos foi quase idêntico ao hbfs.wav exceto o último comando. Executando o **binwalk -D=" .* " result.bin**, que gera a pasta**(_result.bin.extracted)** que contém o Quinto artefacto 0 **(chant1.pdf).**

## 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?

No PDF extraído a partir do ficheiro Hbfs.wav **(hbfs.pdf)** conseguimos encontrar um extrato bancário relativo à conta de Mr. Velucci onde se pode ver que houve uma transferência para a sua conta de 3,000,000€, o valor que Mr. Daniels acusa de ter sido desviado.

## 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.

Depois de termos analisado todos os artefactos identificamos os potenciais envolvidos no caso, o presidente do clube - **Levy Fran Velucci**, analisando o extrato de sua conta**(hbfs.pdf)** confirma-se a entrada de um valor avultante sem justificativo, que Daniels afirmava Velucci ter desviado.

**George Sednem** é o outro potencial envolvido uma vez que recebeu 10% do valor da transferência do jogador James Santos, facto este exposto num dos artefactos**(ticket.pdf),** este valor excede normalmente o negociado, o que nos leva a suspeitar que este pode estar envolvido no caso.

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

Com base nos artefactos encontrados, um próximo passo seria verificar a autenticidade dos documentos, principalmente do extrato bancário. Em seguida identificar e analisar possíveis relações entre o Velucci e George, por final adquirir dados de George que possam comprovar o seu envolvimento no caso.