

# Caso 002: Operação Amigo

CET 8493 | UFCD 9196 - Cibersegurança Ativa | Formador: Paulo Vaz

Formando: João Rodrigo Mota da Costa

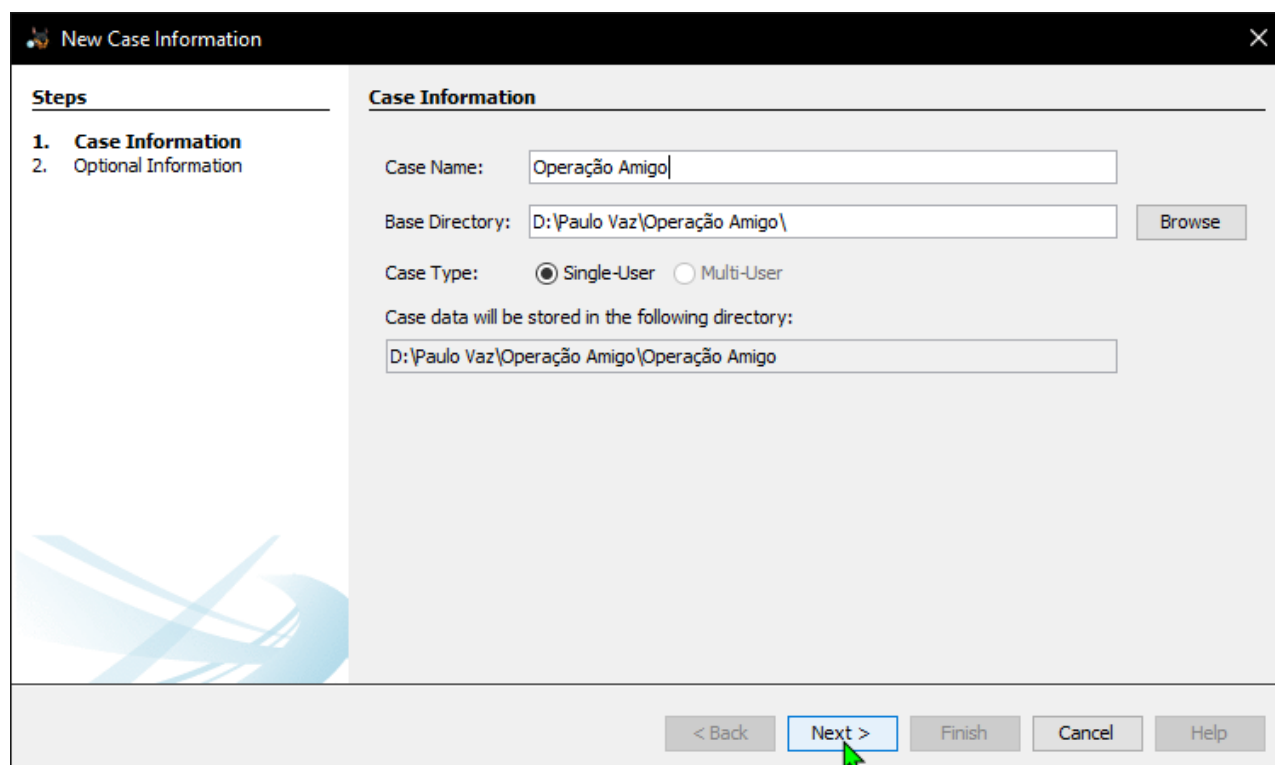
## Introdução

Neste documento, vou fazer a exposição de todas as provas e responder a algumas perguntas relacionadas com o caso 002, intitulado "Operação Amigo". A pedido do formador Paulo Vaz, foi pedido para tentar fazer uma análise de uma *pen* de um político que foi apreendida durante uma operação de investigação. Uma cópia binária da mesma é o apresentado para análise.

O objectivo desta análise é confirmar se há ligações entre este políticos e outros políticos, tal como pagamentos ilícitos e ligações internacionais e a figuras da sociedade portuguesa.

## Criação do caso

Para esta análise, utilizamos o *software* Autopsy. Foi criado então um caso para podermos analisar o conteúdo da *pen*.



The screenshot shows the 'New Case Information' dialog box in the Autopsy software. The dialog has a title bar with a close button (X) and a 'New Case Information' label. On the left, there is a 'Steps' panel with two steps: '1. Case Information' (selected) and '2. Optional Information'. The main area is titled 'Case Information' and contains the following fields and controls:

- Case Name:** A text box containing 'Operação Amigo'.
- Base Directory:** A text box containing 'D:\Paulo Vaz\Operação Amigo\' with a 'Browse' button to its right.
- Case Type:** Two radio buttons: 'Single-User' (selected) and 'Multi-User'.
- Case data will be stored in the following directory:** A text box containing 'D:\Paulo Vaz\Operação Amigo\Operação Amigo'.

At the bottom of the dialog, there are five buttons: '< Back', 'Next >' (highlighted with a green mouse cursor), 'Finish', 'Cancel', and 'Help'.

New Case Information

Steps

1. Case Information

2. **Optional Information**

Optional Information

Case

Number: 002

Examiner

Name: João Rodrigo Mota da Costa

Phone:

Email: joaomotacosta@tuta.io

Notes:

Organization

Organization analysis is being done for: Not Specified Manage Organizations

< Back

Next >

Finish

Cancel

Help

Em seguida, foi importado a nossa "fonte de dados", ou seja, a *pen* em si. Após o importe, vamos fazer uma primeira ingestão do conteúdo da nossa fonte.

Add Data Source

Steps

1. Select Host

2. Select Data Source Type

3. **Select Data Source**

4. Configure Ingest

5. Add Data Source

Select Data Source

Path: D:\Paulo Vaz\Operação Amigo\Evidence\OA\_Pen.E01 Browse

☐ Ignore orphan files in FAT file systems

Time zone: (GMT+0:00) Europe/London

Sector size: Auto Detect

Hash Values (optional):

MD5:

SHA-1:

SHA-256:

NOTE: These values will not be validated when the data source is added.

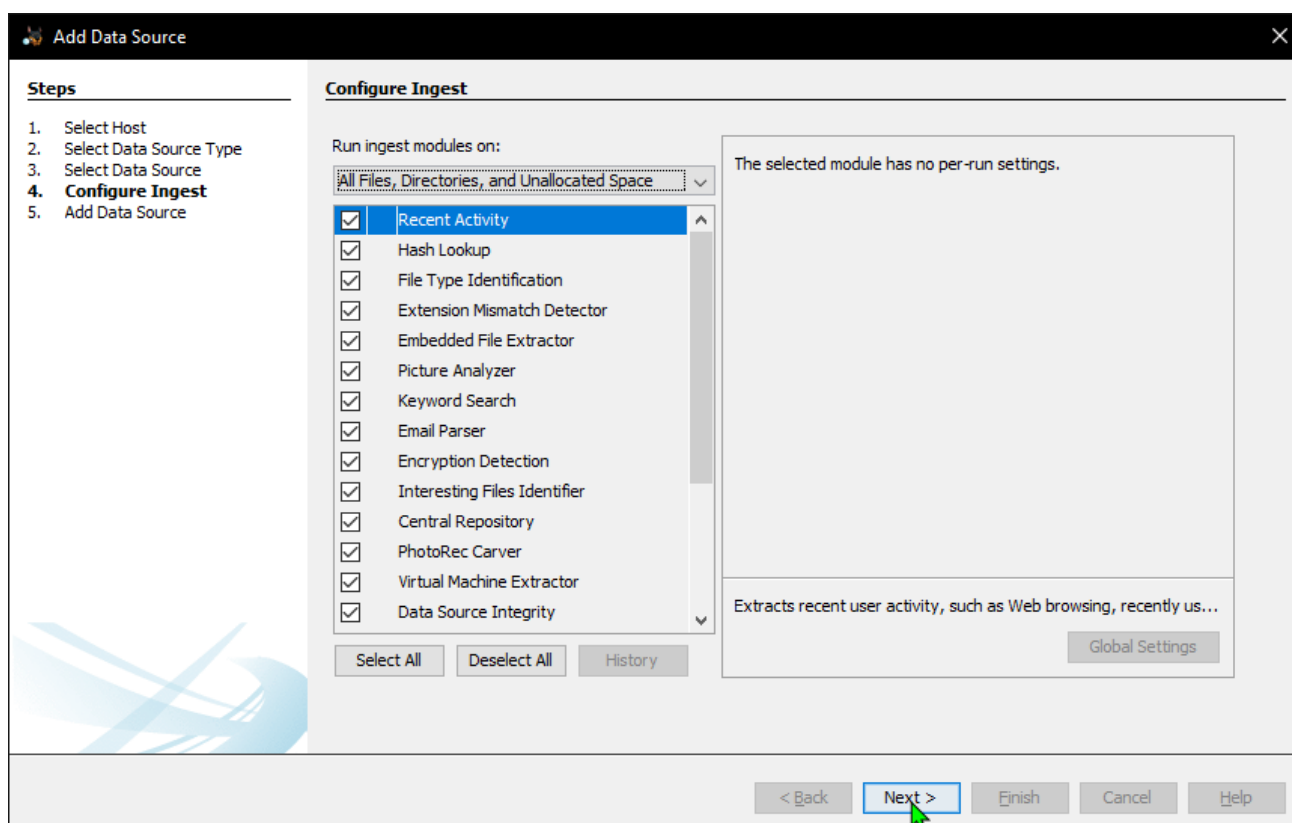
< Back

Next >

Finish

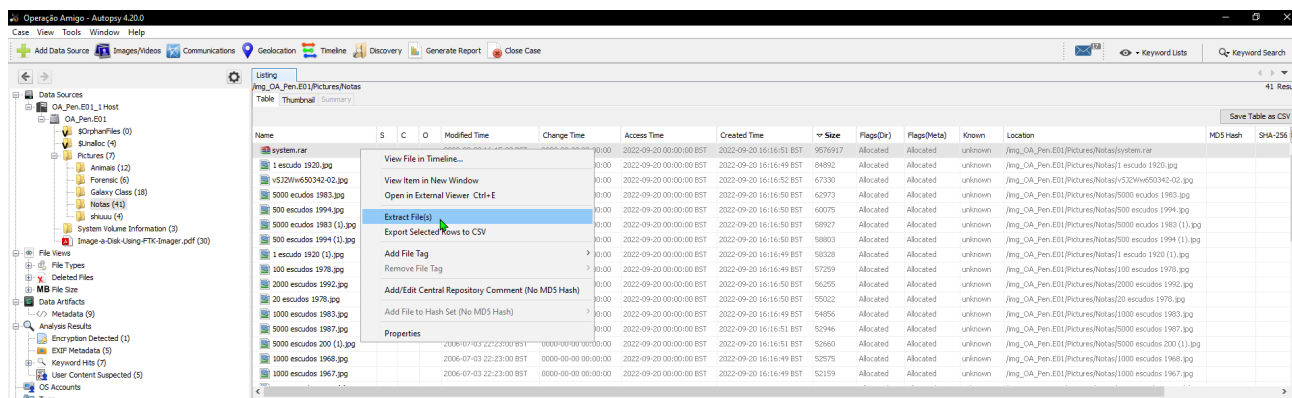
Cancel

Help

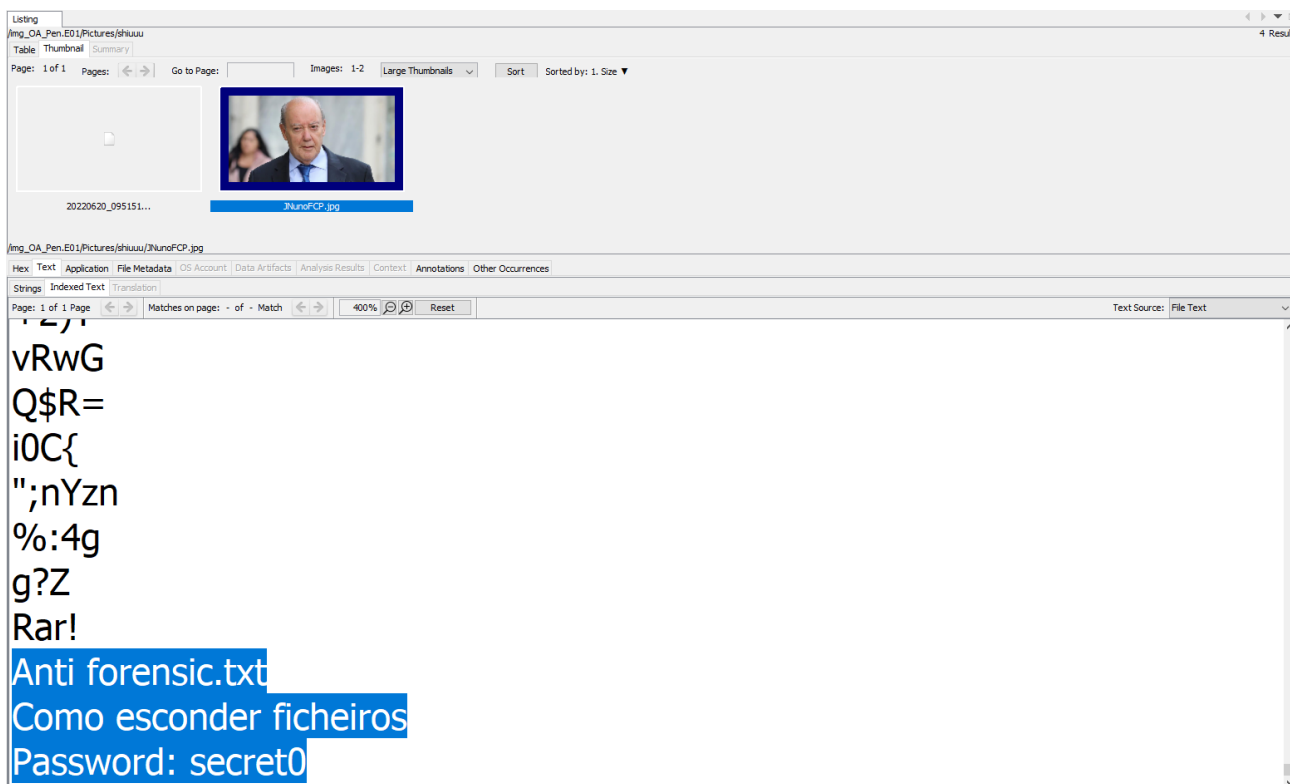


## Prova 001 - system.rar

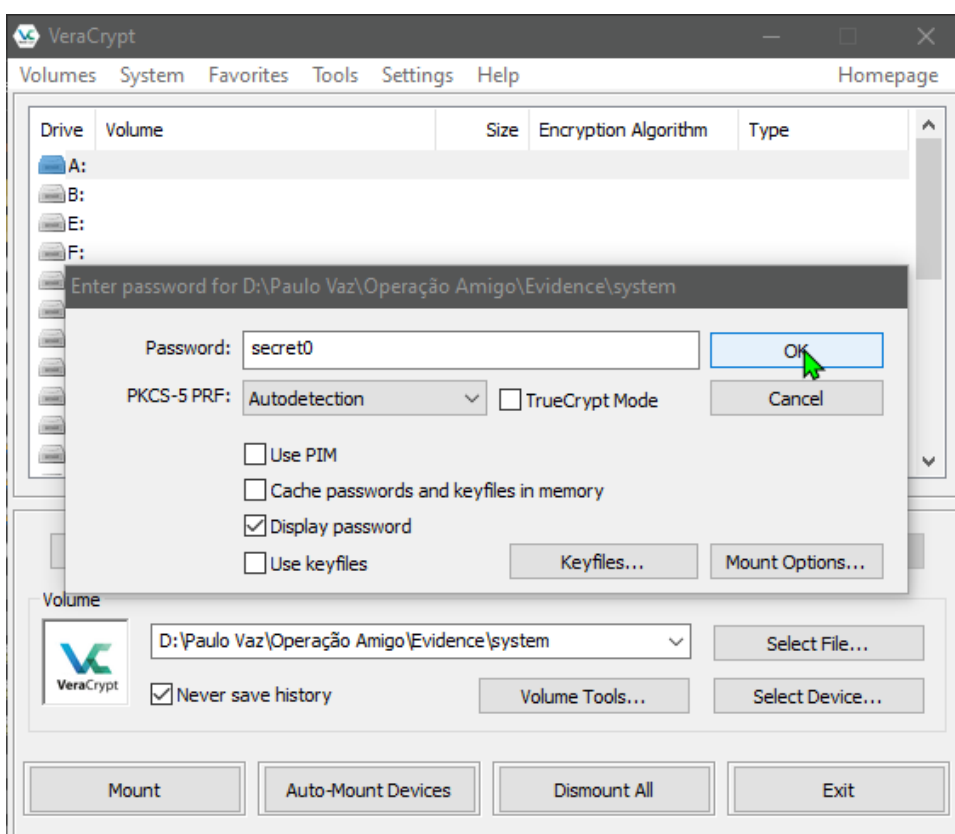
Escondida dentro da pasta "Pictures", encontramos uma pasta denominada "Notas", onde podemos encontrar fotografias de notas de escudo, a antiga moeda portuguesa utilizada antes de 2002. Mas entre as fotografias, encontramos o ficheiro `system.rar`. A extração do mesmo foi feito para análise mais aprofundada.



Ao exportar este ficheiro `rar`, temos um ficheiro escondido de sistema chamado `system`. Utilizando outro *software* chamado VeraCrypt, conseguimos "montar" este ficheiro como um disco virtual na nossa máquina de análise. Mas esta necessita de uma palavra-passe. Após uma investigação mais profunda, foi encontrada uma fotografia do presidente do Futebol Clube do Porto, Jorge Nuno Pinto da Costa, na qual podemos ver no separador "Text" que no final temos um pedaço de texto que nos indica que há uma palavra-passe `secret0`.



Ao utilizar esta palavra-passe no VeraCrypt, conseguimos montar o ficheiro `system` no sistema.



## Provas 002 e 003 - Diário de Notícias, Sócrates e Costa

No novo disco que importamos com o VeraCrypt, conseguimos verificar que existem dois ficheiros `.pdf` e uma pasta com o nome `Investigacao`. Um dos ficheiros `.pdf` é uma capa do jornal Diário de Notícias, datado ao dia 25 de novembro de 2014. Nesta edição, a capa é focada no aprisionamento de ex-primeiro ministro, José Sócrates. Um pedaço importante de informação nesta capa é a linha que diz:

**Reações.** Socialistas cumprem pedido de António Costa e mantêm-se em silêncio, tal como todos os partidos

# Diário de Notícias 150 ANOS

www.dn.pt

TERÇA-FEIRA, 25 de novembro de 2014, Ano 150.º, N.º 53 184, 1,10€  
Diretor ANDRÉ MACEDO Diretora adjunta MÓNICA BELLO Subdiretores ANA SOUSA DIAS, JOANA PETIZ E NUNO SARAIVA Diretor de arte PEDRO FERNANDES

## Juiz decreta prisão de Sócrates para não perturbar investigação

DECISÃO FOI APOIADA PELA PROCURADORA-GERAL

**Medidas de coação.** Empresário Carlos Santos Silva e motorista João Perna também ficam presos  
**Reações.** Socialistas cumprem pedido de António Costa e mantêm-se em silêncio, tal como todos os partidos  
**Vistos gold.** Interrogatório a José Sócrates atrasa prisão domiciliária de arguidos da Operação Labirinto

Com esta informação em mente, podemos começar a "ligar os pontos" entre os dois políticos e com a situação que temos entre mãos. Ao abrir a pasta Investigacao , podemos confirmar as nossas suspeitas ao ver um conjunto de fotografias de António Costa, algumas delas com José Sócrates. Com estas provas, podemos confirmar a suspeita de alguma ligação entre o actual e antigo primeiros-ministros portugueses e o presidente do FC Porto (que pode envolver pagamentos ilícitos).

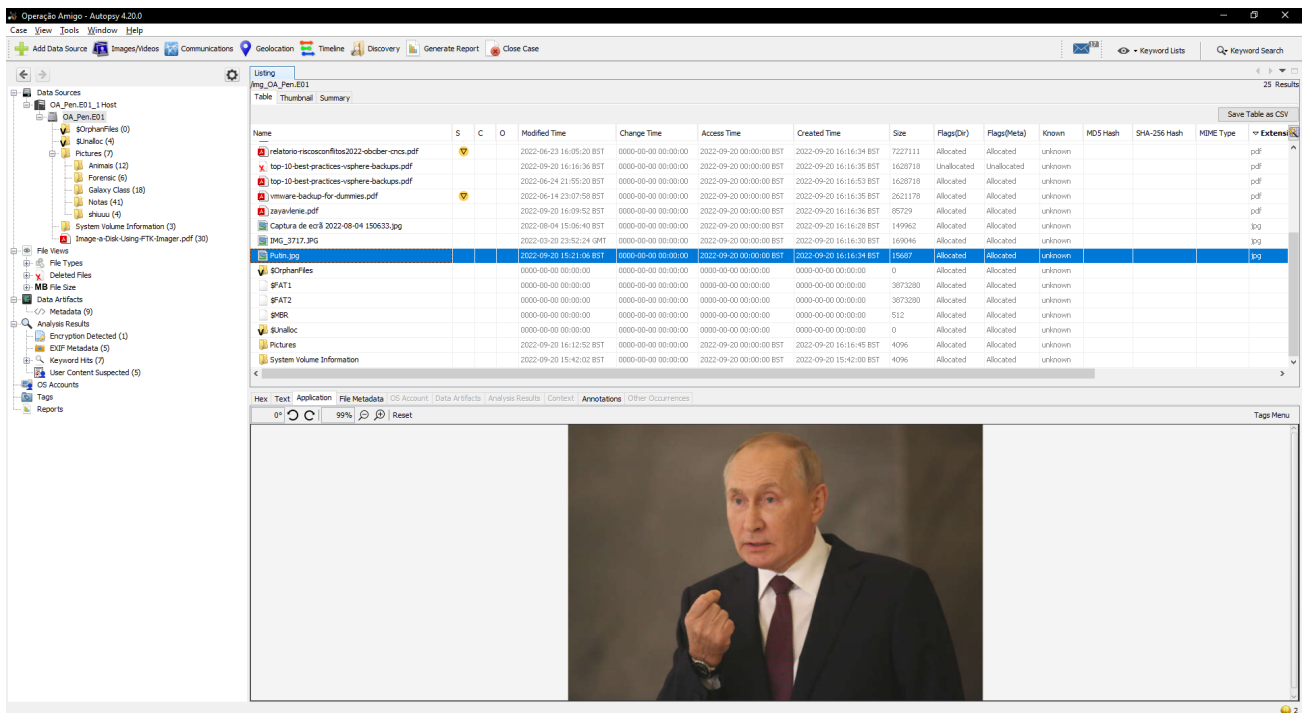
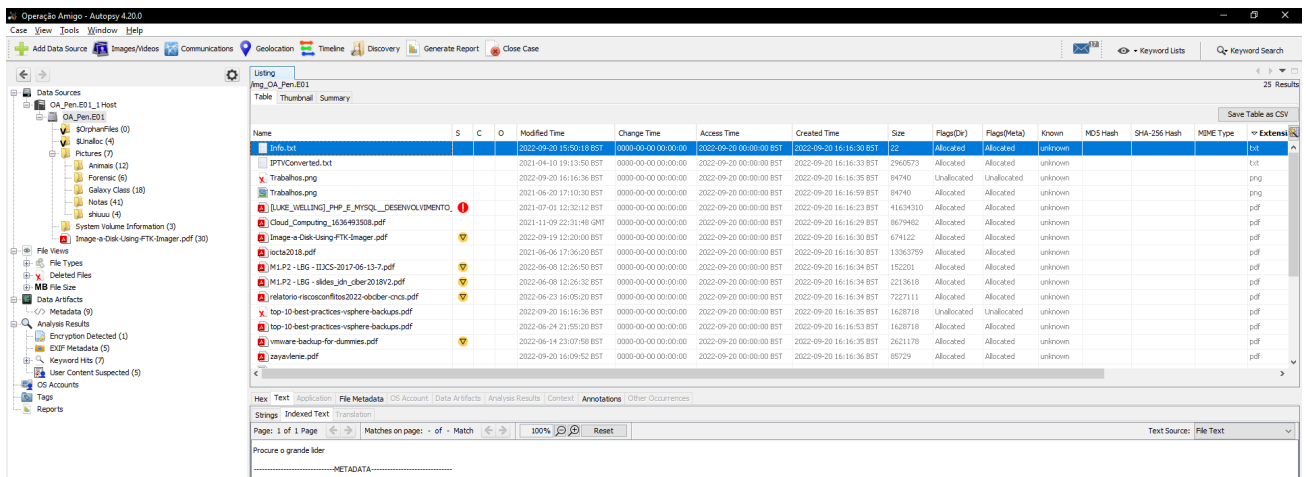


### Prova 004 - Vladimir Putin

Voltando ao Autopsy, podemos avistar mais um ficheiro suspeito com o nome de Info.txt , que cita:

Procura o grande lider

Ao procurar na mesma pasta onde o ficheiro estava guardado, podemos encontrar uma fotografia do presidente russo, Vladimir Putin. Com esta descoberta, podemos então confirmar as suspeitas de ligações internacionais e preparar a extração das provas para serem utilizadas na investigação da "Operação Amigo".



## Fecho do caso

Para sumariar os acontecimentos, temos confirmação de um conjunto de pagamentos ilícitos feitos entre:

- O político alvo da investigação
- Presidente do FC Porto, Jorge Nuno Pinto da Costa
- Ex-primeiro ministro, José Sócrates
- Actual primeiro ministro, António Costa
- E presidente russo, Vladimir Putin

Ao examinar a *pen* do político, temos algum tipo de confirmação das suspeitas levantadas, que podem ser úteis para o resto da investigação.

Caso encerrado.