

# RELATÓRIO TÉCNICO

## INVESTIGAÇÃO CIBERNÉTICA PRELIMINAR

### SOLICITANTE

Prof. Dr. João Benedito dos Santos Junior

CPF:

### RELATÓRIO TÉCNICO DE INVESTIGAÇÃO CIBERNÉTICA PRELIMINAR

No dia 16 de abril de 2025, foram encaminhados para análise os seguintes códigos HASH:

b8137f941bed1f29f4bf00ef75c0128307b6e6e58616e6e700f76b7cd2cd4852  
ac8a9e876b6ccb76257cdeb4f6e81456056cfc34e11555e091112784a7449190  
6df5f3b05fc727413e134cff35a98a39e0092f009698c25d04d3d7d0d8e152c7  
d23f0aaf0a4044cdb6a0e0011fcf7381e90d07bc63aec68606db426511ef6179  
5a414f36b6a8f982f5d5c096ac7f4328178e354e2c7a430fd8f36d1916b2a76b  
7f2f561f0b5ae8f44a99bd5ffe321ed7c4ea6085cd3fde30b365aa1a2829cda1  
d6a32890de734cd6e109896ce8222f1db6797eb019604716e4edf2695fdfa70b  
6369568f26e218856b8af13f45017c0c79ae212d31e4c9db41af71ce1f022a22

No dia 14 de abril de 2025, às 23:59, em entrega via plataforma Canvas, o Prof. Dr. João Benedito dos Santos Junior, encaminhou um conjunto de 3 (três) arquivos, em formato TXT, 01 (um) contendo 8 (oito) códigos HASH, 01 (um) contendo um dicionário com nomes masculinos e 01 (um) contendo um dicionário com nomes femininos.

Na data de 16 de maio de 2025, em ambiente laboratorial, foi realizada uma análise preliminar dos códigos HASH para descobrir seu tipo e constatou-se:

1. Tamanho de 64 caracteres Hexadecimal, totalizando 256 Bits.
2. O formato da HASH sendo SHA-256.

No período de 16 a 17 de abril de 2025, este **Agente de Inteligência** elaborou o presente **Relatório Técnico de Investigação Cibernética Preliminar**, descrevendo com verdade e com todas as circunstâncias o conjunto completo de informações que possa interessar ao **Solicitante**,

tanto no contexto **extrajudicial** quanto em eventual(is) demanda(s) judicial(is). Todas as tarefas periciais foram realizadas em conformidade com o que preconiza a Lei No. 13.105, de 16 de março de 2015, em seu Artigo 473, do Código de Processo Civil, que, em suma, estabelece os parâmetros para elaboração de laudos periciais e pareceres técnicos periciais, que servem como diretrizes para o trabalho do **Agente de Inteligência**.

A **Computação Forense e a Perícia Forense Computacional** consistem, basicamente, no uso de métodos técnicos e científicos para preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidências digitais com validade probatória em juízo. Este **Agente de Inteligência** observou o que preconiza a Norma ABNT ISO/IEC 27037:2013, que apresenta as diretrizes para identificação, coleta, aquisição, extração e preservação de evidências digitais em todas as etapas de um processo judicial e/ou de investigação, preservando, assim, a **cadeia de custódia**.

No dia 18 de abril de 2025, às 16:40, este **Agente de Inteligência** enviou cópia eletrônica deste **Relatório Técnico de Investigação Cibernética Preliminar** para o Prof. Dr. João Benedito dos Santos Junior, via plataforma Canvas, conforme solicitado.

## **QUESITO ÚNICO**

O quesito básico estava centrado na identificação das senhas que deram origem aos códigos HASH, utilizando os dicionários de palavras (nomesfemininos.txt e nomesmasculinos.txt).

## **METODOLOGIA**

Na primeira etapa, este **Agente de Inteligência** realizou o Download dos arquivos que continham os dicionários e do arquivo que continha os códigos HASH que deveriam ser atacados.

Na segunda etapa, utilizando o sistema **Kali Linux**, juntamente com a ferramenta **HashCat**, foram submetidos, o arquivo que contém os resumos de HASH e os dicionários.

baseando-se no fato da HASH ser do tipo SHA-256, foi utilizado o seguinte comando para realizar um **Ataque de Dicionário**:

**(hashcat -m 1400 hashs.txt nomesfemininos.txt)**

A execução deste comando na ferramenta **HashCat** resultou num conjunto de 4 (quarto) resultados, que estão sendo exibidos na **Tabela 01** e **Captura de tela 01**.

**Tabela 01 – Resultado do Ataque de Dicionário utilizando o arquivo de códigos HASH  
SHA-256 “hash.txt” e dicionário “nomesfemininos.txt”**

HASH SHA-256	RESULTADO
ac8a9e876b6ccb76257cdeb4f6e81456056cfc34e11555e091112784a7449190	Beatriz
b8137f941bed1f29f4bf00ef75c0128307b6e6e58616e6e700f76b7cd2cd4852	Raquel
6df5f3b05fc727413e134cff35a98a39e0092f009698c25d04d3d7d0d8e152c7	Juliana
d23f0aaf0a4044cdb6a0e0011fcf7381e90d07bc63aec68606db426511ef6179	Zilda

**Captura de tela 01 – Resultado da execução da ferramenta HASHCAT para o arquivo de  
códigos HASH “hash.txt” e dicionário “nomesfemininos.txt”**

```

kali@kali: ~/Documentos/HASHCAT
Arquivo  Ações  Editar  Exibir  Ajuda
Approaching final keypace - workload adjusted.

ac8a9e876b6ccb76257cdeb4f6e81456056cfc34e11555e091112784a7449190:Beatriz
b8137f941bed1f29f4bf00ef75c0128307b6e6e58616e6e700f76b7cd2cd4852:Raquel
6df5f3b05fc727413e134cff35a98a39e0092f009698c25d04d3d7d0d8e152c7:Juliana
d23f0aaf0a4044cdb6a0e0011fcf7381e90d07bc63aec68606db426511ef6179:Zilda

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target.....: hashes.txt
Time.Started.....: Wed Apr 16 15:14:31 2025 (0 secs)
Time.Estimated...: Wed Apr 16 15:14:31 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (nomesfemininos.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 12342 H/s (0.25ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 4/8 (50.00%) Digests (total), 4/8 (50.00%) Digests (new)
Progress.....: 989/989 (100.00%)
Rejected.....: 0/989 (0.00%)
Restore.Point....: 989/989 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Ana → Zilda
Hardware.Mon.#1..: Temp: 42c Util: 23%

Started: Wed Apr 16 15:13:43 2025
Stopped: Wed Apr 16 15:14:33 2025

(kali@kali)~[~/Documentos/HASHCAT]
$

```

Após isto, para verificar possíveis associações dos códigos HASH com o dicionário “nomesmasculinos.txt” este Agente de Inteligência utilizou o comando:

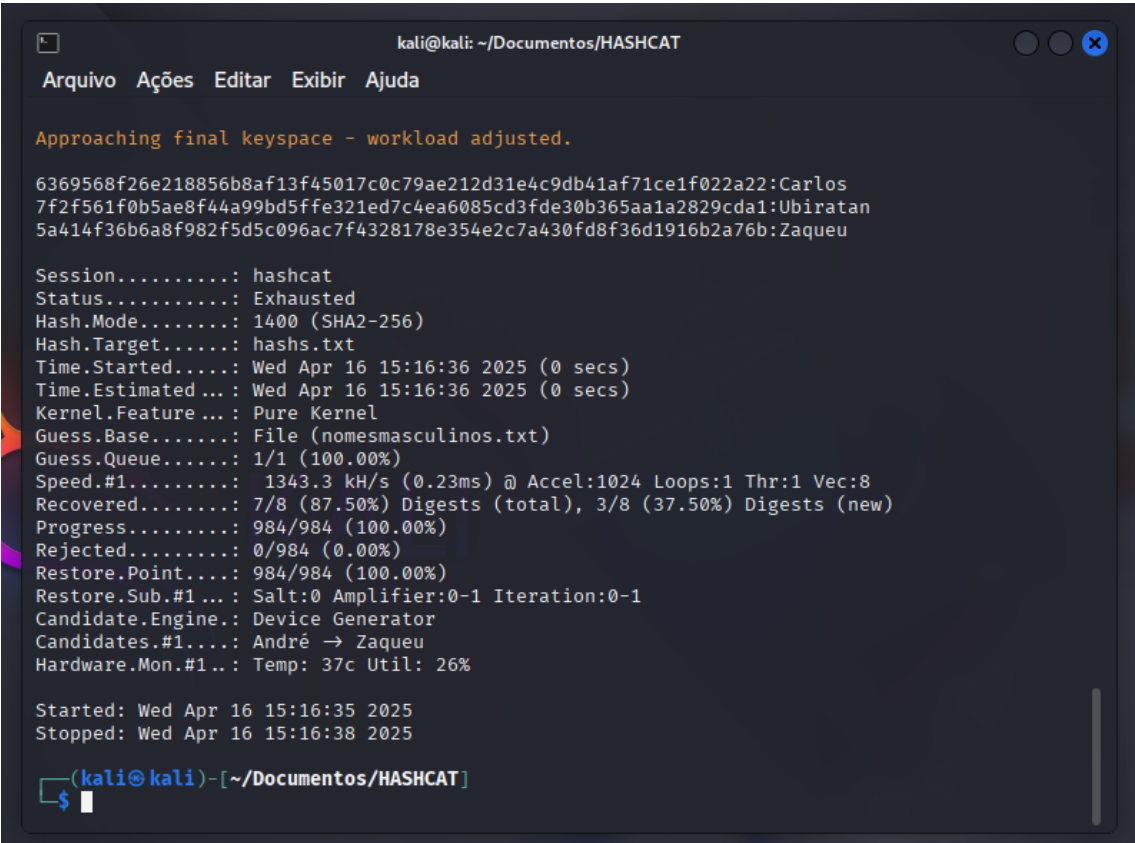
(hashcat -m 1400 hashes.txt nomesmasculinos.txt)

A execução deste comando na ferramenta HashCat resultou num conjunto de 3 (três) resultados, que estão sendo exibidos na Tabela 02 e Captura de tela 02.

Tabela 02 – Resultado do Ataque de Dicionário utilizando o arquivo de códigos HASH SHA-256 “hash.txt” e dicionário “nomesfemininos.txt”

HASH SHA-256	RESULTADO
6369568f26e218856b8af13f45017c0c79ae212d31e4c9db41af71ce1f022a22	Carlos
7f2f561f0b5ae8f44a99bd5ffe321ed7c4ea6085cd3fde30b365aa1a2829cda1	Ubiratan
5a414f36b6a8f982f5d5c096ac7f4328178e354e2c7a430fd8f36d1916b2a76b	Zaqueu

Captura de tela 02 – Resultado da execução da ferramenta HASHCAT para o arquivo de códigos HASH “hash.txt” e dicionário “nomesmasculinos.txt”



```
kali@kali: ~/Documentos/HASHCAT
Arquivo  Ações  Editar  Exibir  Ajuda

Approaching final key space - workload adjusted.

6369568f26e218856b8af13f45017c0c79ae212d31e4c9db41af71ce1f022a22:Carlos
7f2f561f0b5ae8f44a99bd5ffe321ed7c4ea6085cd3fde30b365aa1a2829cda1:Ubiratan
5a414f36b6a8f982f5d5c096ac7f4328178e354e2c7a430fd8f36d1916b2a76b:Zaqueu

Session.....: hashcat
Status.....: Exhausted
Hash.Mode.....: 1400 (SHA2-256)
Hash.Target.....: hashes.txt
Time.Started.....: Wed Apr 16 15:16:36 2025 (0 secs)
Time.Estimated...: Wed Apr 16 15:16:36 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (nomesmasculinos.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1343.3 kH/s (0.23ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered.....: 7/8 (87.50%) Digests (total), 3/8 (37.50%) Digests (new)
Progress.....: 984/984 (100.00%)
Rejected.....: 0/984 (0.00%)
Restore.Point....: 984/984 (100.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: André → Zaqueu
Hardware.Mon.#1..: Temp: 37c Util: 26%

Started: Wed Apr 16 15:16:35 2025
Stopped: Wed Apr 16 15:16:38 2025

(kali@kali)-[~/Documentos/HASHCAT]
```

Por fim, constatou-se a descoberta de **07 (sete) das 08 (oito)** senhas criptografadas via **HASH SHA-256**.

Apenas a HASH

**“d6a32890de734cd6e109896ce8222f1db6797eb019604716e4edf2695fdfa70b”**, não retornou resultado satisfatório ao realizar a associação com os dicionários de palavras recebidos pelo **Agente de Inteligência**

## RESPOSTA AO QUESITO

Realizadas todas as etapas do trabalho técnico e pericial, este **Agente de Inteligência** informa as seguintes respostas ao quesito:

1. Foi possível descobrir a palavra original de **07 (sete) dos 08 (oito)** resumos criptográficos contidos no arquivo **“hashs.txt”**, utilizando o **Ataque de Dicionário**;
2. A análise resultou nas senhas: **Raquel, Beatriz, Juliana, Zilda, Zaqueu, Ubiratan e Carlos**, respectivamente;
3. Apenas **01 (um) dos 08 (oito)** códigos HASH **não resultou em uma senha** baseada nos dicionários que foram fornecidos a este **Agente de Inteligência**.

## RECOMENDAÇÕES

Este **Agente de Inteligência** recomenda que um novo ataque seja realizado, utilizando outros dicionários, baseados em mais nomes masculinos e femininos, baseado na possibilidade de seguir o mesmo padrão, para verificar se é possível descobrir a palavra que gerou a HASH: **“d6a32890de734cd6e109896ce8222f1db6797eb019604716e4edf2695fdfa70b”**

## CONCLUSÃO

Foram estes os elementos analisados, periciados e passíveis de serem apresentados por este **Agente de Inteligência**. Nada mais havendo a constar, este **Agente de Inteligência** encerra o presente **Relatório Técnico de Investigação Cibernética Preliminar**, elaborado em 07 (sete) páginas.

Poços de Caldas – MG, 17 de abril de 2025.

## **Bruno Felipe Barretto de França**

Estudante do 4º Período de Ciência da Computação

### **SOBRE O AGENTE DE INTELIGÊNCIA**

**Conforme preconiza o inciso II, § 2º do artigo 465 do CPC**

**Bruno Felipe Barretto de França**, *estudante do curso de Ciência da Computação*

Em 2023 iniciou o Curso de Ciência da Computação da Pontifícia Universidade Católica de Minas Gerais – PUC Minas ([www.pucpcaldas.br](http://www.pucpcaldas.br)), *campus* de Poços de Caldas, e encontra-se no 4º período do curso.