 <div> <div>ESCOLA</div> <div>SUPERIOR</div> <div>DE TECNOLOGIA</div> <div>E GESTÃO</div> </div>	Tipo de Prova: Exame Normal Curso: LSIRC U.C.: Análise Forense Digital	Ano Letivo 2022/2023	Data: 02/02/2023 Hora: 10:00 Duração: 2 horas
---	--	-------------------------	---

Observações: Com consulta de documentação própria.

O tempo previsto para responder a cada questão é apresentado entre parêntesis reto.

A cotação atribuída a cada pergunta é apresentada entre parêntesis curvo.

No final da prova, entregue o enunciado, as folhas de teste e de rascunho.

Grupo I

1. [10 min] (2,5 valores)
“Investigação digital a sistemas ligados tentar extrair informação não volátil.”
Comente a afirmação, indicando também se **concorda ou não** com a mesma. Fundamente a sua resposta com um **exemplo concreto**.
2. [10 min] (2,5 valores)
“O módulo de identificação de tipos de ficheiros do *Autopsy* gera *output* próprio.”
Comente a afirmação, indicando também se **concorda ou não** com a mesma. Fundamente a sua resposta com um **exemplo concreto**.
3. [10 min] (2,0 valores)
Distinga, **por palavras suas**, técnicas de investigação digital forense, de técnicas anti-forense. Apresente exemplos de ambas.
4. [10 min] (2,0 valores)
Desenhe um esquema gráfico de um disco particionado com MBR que contenha as partições seguintes, por ordem: duas partições estendidas FAT32 e uma partição primária NTFS. As partições devem ter um tamanho igual.
5. [10 min] (2,0 valores)
Enumere todos os comandos necessários para espelhar, num *switch* Cisco, todo o tráfego de entrada nas portas Gig0/23 e Gig0/24 para a porta Gig0/1.

Grupo II

6. [25 min] (3,0 valores)
Analise o resumo do pacote apresentado de seguida.


```

1 Ethernet II, Src: 5c:78:f8:8a:67:67, Dst: a8:6d:aa:70:76:6e
2 Address Resolution Protocol (request)
3   Hardware type: Ethernet (1)
4   Protocol type: IPv4 (0x0800)
5   Hardware size: 6
6   Protocol size: 4
7   Opcode: request (1)
8   Sender MAC address: 5c:78:f8:8a:67:67
9   Sender IP address: 192.168.3.1
10  Target MAC address: 00:00:00:00:00:00
11  Target IP address: 192.168.3.129

```

Responda a cada uma das seguintes questões. **Indique sempre a linha do resumo** que lhe permitiu chegar a cada resposta.

6.1) Que protocolos estão presentes no pacote?

 <div> <div>ESCOLA</div> <div>SUPERIOR</div> <div>DE TECNOLOGIA</div> <div>E GESTÃO</div> </div>	<div>Tipo de Prova: Exame Normal</div> <div>Curso: LSIRC</div> <div>U.C.: Análise Forense Digital</div>	<div>Ano Letivo</div> <div>2022/2023</div> <div>Data: 02/02/2023</div> <div>Hora: 10:00</div> <div>Duração: 2 horas</div>
---	---	---

- 6.2) Qual é o MAC do emissor?
- 6.3) Qual é o IP do destinatário?
- 6.4) Qual é a aplicação geradora do pacote? **Justifique.**
- 6.5) Qual é o propósito deste pacote? **Justifique.**
- 6.6) O pacote é confidencial? **Justifique.**

7. [20 min] (3,0 valores)

Apresente uma linha de comandos que lhe permita listar **as ligações TCP efetuadas pelo PC com o endereço IP 192.168.10.12**, bem assim como **todas as ligações seguras estabelecidas para o servidor web com o endereço IP 192.168.0.1**, constantes de uma captura de rede guardada no ficheiro **captura.pcap**. Recorra ao **tcpdump** e filtros do tipo **BPF**.

8. [25 min] (3,0 valores)

Analise a seguinte sessão de terminal de um analista forense digital. Note que o comando utilizado suprime sequências de linhas iguais, apresentando apenas um asterisco (*) no início da linha, aceita o parâmetro *-s* para especificar um *offset* inicial e o parâmetro *-n* para especificar o limite de bytes a mostrar.

```

1 aap@aap:$ hexdump -C -n 256 ficheiro
2 00000000 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 |.PNG.....IHDR|
3 00000010 00 00 05 b7 00 00 01 2c 08 02 00 00 00 7f 8d 19 |.....,.....|
4 00000020 be 00 01 9e 8a 49 44 41 54 78 9c ec bd 7b 7c 5d |.....IDATx...{|}
5 00000030 d5 75 2e 3a e7 5c 6b cb 96 fc d0 cb 8f d8 32 96 |.u...k.....2.|
6 00000040 5f 18 f0 db 80 4d 9a 80 65 93 07 24 6d c0 0e e9 |_....M...e...$m...|
7 00000050 69 68 13 c0 70 cf b9 bf 96 34 40 d2 de 7f 7a 00 |ih..p....4@...z.|
8 00000060 03 c9 b9 bf 7b db 03 84 24 b4 fd dd 82 31 6d d2 |....{...$....1m.|
9 00000070 f4 9c 04 6c c8 03 92 82 24 9b 3c b0 c1 6f f3 b2 |...l...$.<..o..|
10 00000080 2c 5b b6 64 e3 97 24 cb 96 64 6b af 35 e7 9d 63 |, [.d...$.dk.5..c|
11 00000090 8c 39 d7 96 41 7b 1b 89 2d 4b 96 c7 07 98 2d 79 |.9..A{...-K....-y|
12 000000a0 ef b5 d7 63 3e c6 f8 c6 18 df 08 8d 31 82 c1 60 |...c>.....1..'|
13 000000b0 30 18 0c 06 e3 42 87 b5 68 24 fd a9 85 51 fe f5 |0....B..h$....Q..|
14 000000c0 40 9f 15 83 c1 60 30 18 8c 0b 0a e1 40 9f 00 83 |@....'0.....@...|
15 000000d0 c1 60 30 18 0c c6 c7 85 |..'0.....|
16 000000d8

```

Que informação consegue extrair do extrato apresentado? Na sua resposta, seja tão exaustivo quanto possível.

Anexo 1: Estrutura

Offset	Length	Contents
0	8 bytes	Signature (0x89 50 4e 47 0d 0a 1a 0a)
8	4 bytes	Header size
12	4 bytes	Header ID (0x49 48 44 52)
16	4 bytes	Width (in pixels)
20	4 byte	Height (in pixels)
24	1 byte	Bits per sample (depth)
25	1 byte	Color
26	1 byte	Compression (0x00 Deflate)
27	1 byte	Filter
28	1 byte	Interlace
29	4 bytes	CRC32

Color Type	Allowed Bit Depths	Interpretation
0	1,2,4,8,16	Each pixel is a grayscale sample.
2	8,16	Each pixel is an R,G,B triple.
3	1,2,4,8	Each pixel is a palette index; a PLTE chunk must appear.
4	8,16	Each pixel is a grayscale sample, followed by an alpha sample.
6	8,16	Each pixel is an R,G,B triple, followed by an alpha sample.

Filter:

0	None
1	Sub
2	Up
3	Average
4	Paeth

Interlace:

0	No Interlace
1	Adam7 interlace