ESTGF POLITÉCNICO DO PORTO	Tipo de Prova Exame Época Recurso	Ano lectivo 2014/2015	Data 15-07-2015
	Curso Mestrado em Engenharia Informática		Hora 19:00
	Unidade Curricular Informática Forense e Cibercrime		Duração 2 horas

Observações
Com consulta de documentação própria.
O tempo previsto para responder a cada questão é apresentado entre parêntesis recto.
A cotação atribuída a cada pergunta é apresentada entre parêntesis curvo.

Grupo I

1) [10 min] **(2,5 valores)**
"Um disco formado com FAT32 usa um protective MBR". Comente a afirmação, indicando também se concorda ou não com a mesma. Use exemplos concretos.

2) [10 min] **(2,5 valores)**
"A segmentação é uma característica intrínseca à análise forense em redes de computadores que facilita a vida do analista forense.". Comente a afirmação, indicando também se concorda ou não com a mesma. Use exemplos concretos.

Grupo II

3) [10 min] **(2,0 valores)**
Distinga a recolha de dados intrusiva da não intrusiva, dando exemplos concretos de duas situações onde se tenha de recorrer a cada uma destas.

4) [10 min] **(2,0 valores)**
Desenhe um esquema gráfico de um disco com uma partição primária NTFS, outra partição primária FAT32 e uma partição estendida EXT3. Todas as partições tem um tamanho igual. O disco serve de disco de arranque do PC.

5) [10 min] **(2,0 valores)**
Enumere os comandos necessários para espelhar, num switch Cisco, todo o tráfego de entrada na VLAN 10 para a porta Fa0/10, e o de saída da VLAN 10 para a porta Fa0/11.

Grupo III

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

```
     1 Ethernet II, Src: 00:25:90:d6:fe:98, Dst: d8:9d:67:95:52:b5
     2 Internet Protocol Version 4, Src: 132.245.213.50 , Dst: 172.20.100.154
     3 Transmission Control Protocol, Src Port: 993, Dst Port: 45772, Seq: 309, Ack:
245, Len: 85
     4 Secure Sockets Layer
     5     TLSv1.2 Record Layer: Application Data Protocol: imap
     6         Content Type: Application Data (23)
     7         Version: TLS 1.2 (0x0303)
     8         Length: 80
     9         Encrypted Application Data: 0c4b6efd02dd742179dd47d889623...
```

Responda a cada uma das seguintes questões. **Justifique** as suas respostas e **indique sempre a linha** do resumo que lhe permitiu chegar a cada resposta.

6.a) Que protocolos estão presentes no pacote?
6.b) Qual é o endereço MAC do equipamento emissor? E do destinatário?
6.c) Qual é o endereço IP do equipamento emissor? E do destinatário?
6.d) Qual é a aplicação geradora do pacote ?
6.e) Qual é o propósito deste pacote?

7) [20 min] **(3,0 valores)**
Apresente uma linha de comandos que lhe permita listar **todos os acessos a servidores de email (POP, IMAP, SMTP, cifrados ou não)**, bem como o **todos os pedidos de resolução de nomes efetuados pelo PC com o endereço IP 172.20.20.15** 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 inicio da linha. As linhas foram ainda numeradas recorrendo ao comando nl.

```
[aap@eb-aap ~] $ hexdump -C -n 1536 hdd.img | nl
     1 00000000  eb 3c 90 6d 6b 66 73 2e  66 61 74 00 02 08 01 00  |.<.mkfs.fat.....|
     2 00000010  02 00 02 00 00 f8 00 01  20 00 40 00 00 00 00 00  |........ .@.....|
     3 00000020  00 00 08 00 80 00 29 80  32 ea 33 42 41 44 4d 42  |......).2.3BADMB|
     4 00000030  52 20 20 20 20 20 46 41  54 31 36 20 20 20 0e 1f  |R     FAT16   ..|
     5 00000040  be 5b 7c ac 22 c0 74 0b  56 b4 0e bb 07 00 cd 10  |.[|."·t·V·......|
     6 00000050  5e eb f0 32 e4 cd 16 cd  19 eb fe 54 68 69 73 20  |^..2.......This |
     7 00000060  69 73 20 6e 6f 74 20 61  20 62 6f 6f 74 61 62 6c  |is not a bootabl|
     8 00000070  65 20 64 69 73 6b 2e 20  20 50 6c 65 61 73 65 20  |e disk.  Please |
     9 00000080  69 6e 73 65 72 74 20 61  20 62 6f 6f 74 61 62 6c  |insert a bootabl|
    10 00000090  65 20 66 6c 6f 70 70 79  20 61 6e 64 0d 0a 70 72  |e floppy and..pr|
    11 000000a0  65 73 73 20 61 6e 79 20  6b 65 79 20 74 6f 20 74  |ess any key to t|
    12 000000b0  72 79 20 61 67 61 69 6e  20 2e 2e 2e 20 0d 0a 00  |ry again ... ...|
    13 000000c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
    14 *
    15 000001f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 55 aa  |..............U.|
    16 00000200  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
    17 *
    18 00000400  00 00 01 00 00 00 04 00  33 33 00 00 3a b6 03 00  |........33..:...|
    19 00000410  ef ff 00 00 01 00 00 00  00 00 00 00 00 00 00 00  |................|
    20 00000420  00 20 00 00 00 20 00 00  00 08 00 00 69 b1 9a 55  |. ... ......i..U|
    21 00000430  b8 b1 9a 55 02 00 ff ff  53 ef 01 00 01 00 00 00  |...U....S.......|
    22 00000440  a0 af 9a 55 00 00 00 00  00 00 00 00 01 00 00 00  |...U............|
    23 00000450  00 00 00 00 0b 00 00 00  80 00 00 00 3c 00 00 00  |............<...|
    24 00000460  02 00 00 00 01 00 00 00  39 aa 5b 8a 5e ce 45 55  |........9.[.^.EU|
    25 00000470  bb 9f b4 67 46 ec e2 f9  00 00 00 00 00 00 00 00  |...gF...........|
    26 00000480  00 00 00 00 00 00 00 00  2f 74 6d 70 2f 65 6e 65  |......../tmp/ene|
    27 00000490  72 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |r...............|
    28 000004a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
    29 *
    30 000004c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01  |................|
    31 000004d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
    32 000004e0  08 00 00 00 00 00 00 00  00 00 00 00 06 8d 89 81  |................|
    33 000004f0  73 a9 4b ae 81 36 11 5a  b3 3d 3d 06 01 01 00 00  |s.K..6.Z.==.....|
    34 00000500  0c 00 00 00 00 00 00 00  a0 af 9a 55 03 c1 01 00  |...........U....|
    35 00000510  04 c1 01 00 05 c1 01 00  06 c1 01 00 07 c1 01 00  |................|
    36 00000520  08 c1 01 00 09 c1 01 00  0a c1 01 00 0b c1 01 00  |................|
    37 00000530  0c c1 01 00 0d c1 01 00  0e c1 01 00 0f c1 01 00  |................|
    38 00000540  10 c2 01 00 00 00 00 00  00 00 00 00 00 00 80 00  |................|
    39 00000550  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
    40 00000560  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
    41 00000570  00 00 00 00 00 00 00 00  8e 01 00 00 00 00 00 00  |................|
    42 00000580  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
    43 *
    44 00000600
```

Que informação consegue extrair do ficheiro **hdd.img**? Na sua resposta, seja tão exaustivo quanto possível.