UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER I
FINAL EXAMINATION SEMESTER I
SESI 2021/2022
SESSION 2021/2022

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD KURSUS ***COURSE CODE***	**: BITS 3453** ***BITS 3453***
KURSUS ***COURSE***	**: ANALISA MALWARE & PENYIASATAN DIGITAL** ***MALWARE ANALYSIS & DIGITAL INVESTIGATION***
PENYELARAS ***COORDINATOR***	**: MOHD ZAKI MAS'UD**
PROGRAM ***PROGRAMME***	**: 3 BITZ**
MASA ***TIME***	**: 9:00 a.m – 11:00 a.m**
TEMPOH ***DURATION***	**: 2 JAM** ***2 HOURS***
TARIKH ***DATE***	**: 31 JANUARI 2021** ***31 JANUARY 2021***
TEMPAT ***VENUE***	**: HALL 5**

ARAHAN KEPADA CALON:
INSTRUCTION TO CANDIDATES:

1. **Kertas soalan ini mengandungi DUA (2) Bahagian. Sila Jawab SEMUA Soalan di kedua-dua Bahagian**
   The exam paper consists of TWO (2) PARTS. Please ALL the questions in both part
2. **Kertas soalan ini mempunyai versi dwi-bahasa.**
   The exam paper consists of dual-language version.

KERTAS SOALAN INI TERDIRI DARIPADA (20) MUKA SURAT SAHAJA
(TERMASUK MUKA SURAT HADAPAN)
THIS QUESTION PAPER CONTAINS (20) PAGES INCLUSIVE OF FRONT PAGE

BAHAGIAN A: SOALAN BERSTRUKTUR (25 MARKAH)

ARAHAN: *Sila jawab* ***SEMUA*** *soalan*

(a) Terangkan persamaan yang ada pada kod hasad *REvil*, *Avaddon* dan *Conti*?

(2 markah)

(b) Komputer Azlin baru sahaja di diagnosis dengan kod hasad *Ransomeware* dan dipercayai mirip kod hasad *WannaCry*. Apakah jenis Sistem Pengoperasian yang digunakan oleh Azlin? Berikan justifikasi anda dan Apakah **TIGA (3)** kebarangkalian yang mungkin berlaku kepada komputer Azlin dan persekitaran sistem rangkaian organisasi Azlin?

(4 markah)

(c) Soh Hoon baru sahaja membeli sebuah tablet dan dia belum lagi membuat keputusan sama ada untuk memasang *antivirus* atau tidak ke dalam tablet beliau. Dalam usaha untuk memujuk beliau untuk membeli antivirus, anda yang merupakan jurujual tablet tersebut, perlu menjelaskan secara terperinci mengenai ancaman *malware* yang mungkin menjangkiti tablet beliau. Senarai dan terangkan **EMPAT (4)** sifat umum *malware* yang mungkin berlaku jika tablet tersebut dijangkiti *malware*.

(8 markah)

(d) Sebagai penganalisa kod hasad, Thanasilan telah diberikan sampel kod hasad Conficker. Apakah **TIGA (3)** simptom yang akan dilihat oleh Thanasilan semasa kod hasad ini dijalankan didalam komputer? Apakah **TIGA (3)** persoalan teknikal yang mungkin disoal oleh Thanasilan semasa menganalisa kod hasad ini dan nyatakan sumber-sumber maklumat dari komputer yang boleh membantu Ghazali dalam menjawab persoalan tenikal tersebut?

(9 markah)

BAHAGIAN B: SOALAN BERSTRUKTUR (75 MARKAH)

ARAHAN: *Sila jawab **SEMUA** soalan*

SOALAN 1 (25 MARKAH)

Kajian Kes 1:

Danial mempunyai Ijazah Sarjana Muda Sains Komputer (Keselamatan Komputer) dari Universiti Teknikal Malaysia Melaka (UTeM) dan telah menghadiri temuduga untuk jawatan penganalisa malware di R-Protect Sdn. Bhd. Soalan berikut merupakan soalan-soalan semasa temuduga tersebut.

Berdasarkan Kajian Kes 1 di atas, jawab soalan-soalan berikut.

(a) Terangkan kenapa penganalisa kod hasad perlu meyediakan persekitaran yang selamat sebelum mengalisa sampel kod hasad dan cadangkan **TIGA (3)** langkah pendekatan dan persediaan selamat yang perlu sebelum menyiasat sampel ko hasad.

(6 markah)

(b) Bincangkan kaedah yang boleh digunakan untuk menganalisa sampel kod hasad Android dan Terangkan secara ringkas kebaikan dan kelemahan setiap kaedah analisa kod hasad tersebut?

(8 marks)

(c) Cadangkan **DUA (2)** kaedah analisa secara Automatik dan berikan satu contoh perisian/ alatan yang boleh digunakan untuk setiap kaedah itu.

(4 markah)

(d) Senaraikan **LIMA (5)** kaedah yang digunakan oleh pengarang malware untuk mempertahankan diri mereka daripada penganalisa malware.

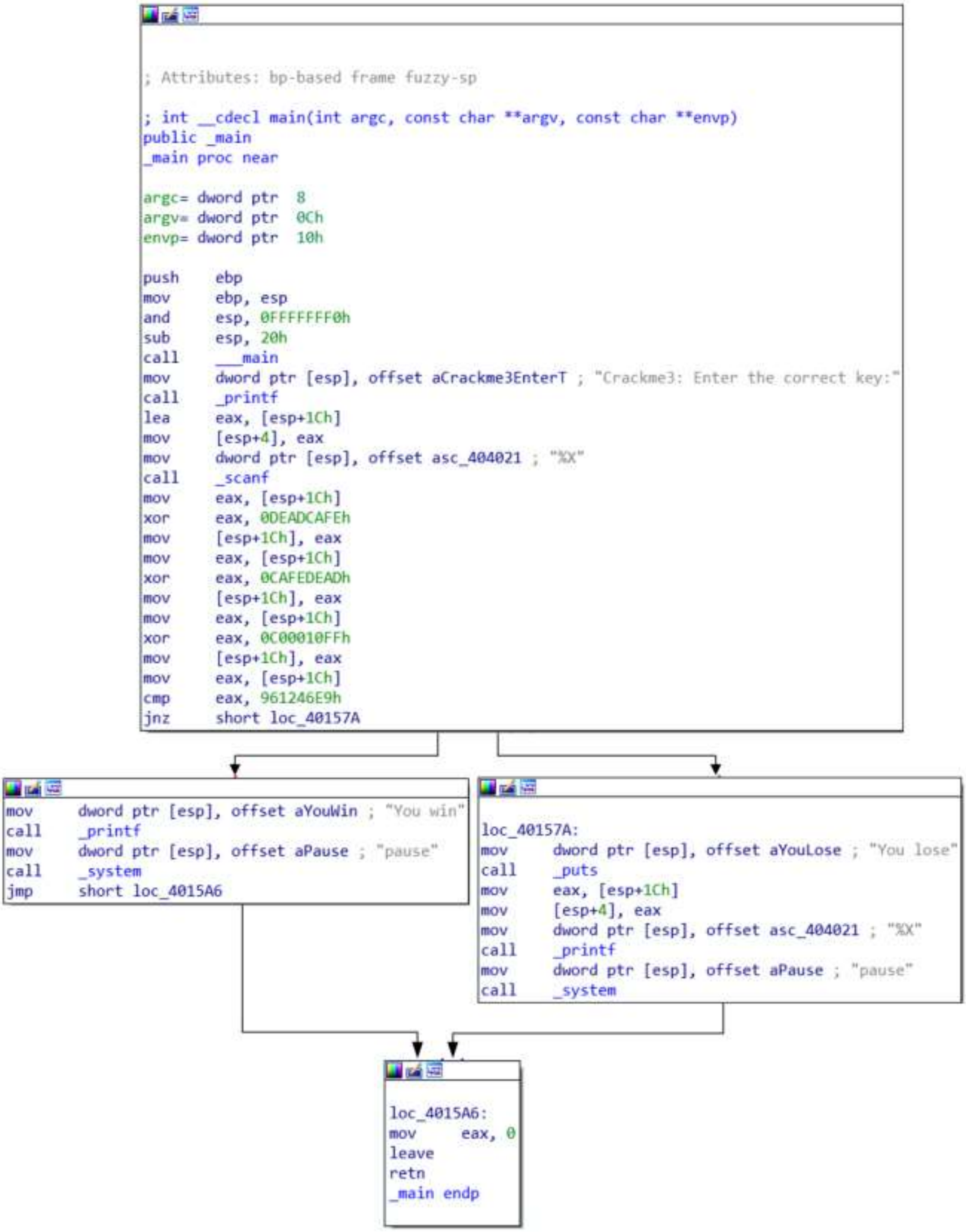
(5 markah)

(e) Berikan **DUA (2)** contoh perisian *Virtual Machine*.

(2 markah)

SOALAN 2 (25 MARKAH)

Soalan (a) hingga (e) berdasarkan Gambarajah 1



```
; Attributes: bp-based frame fuzzy-sp

; int __cdecl main(int argc, const char **argv, const char **envp)
public _main
_main proc near

argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF0h
sub     esp, 20h
call    ___main
mov     dword ptr [esp], offset aCrackme3EnterT ; "Crackme3: Enter the correct key:"
call    _printf
lea     eax, [esp+1Ch]
mov     [esp+4], eax
mov     dword ptr [esp], offset asc_404021 ; "%X"
call    _scanf
mov     eax, [esp+1Ch]
xor     eax, 0DEADCAFEh
mov     [esp+1Ch], eax
mov     eax, [esp+1Ch]
xor     eax, 0CAFEDEADh
mov     [esp+1Ch], eax
mov     eax, [esp+1Ch]
xor     eax, 0C00010FFh
mov     [esp+1Ch], eax
mov     eax, [esp+1Ch]
cmp     eax, 961246E9h
jnz     short loc_40157A
```

```
mov     dword ptr [esp], offset aYouWin ; "You win"
call    _printf
mov     dword ptr [esp], offset aPause ; "pause"
call    _system
jmp     short loc_4015A6
```

```
loc_40157A:
mov     dword ptr [esp], offset aYouLose ; "You lose"
call    _puts
mov     eax, [esp+1Ch]
mov     [esp+4], eax
mov     dword ptr [esp], offset asc_404021 ; "%X"
call    _printf
mov     dword ptr [esp], offset aPause ; "pause"
call    _system
```

```
loc_4015A6:
mov     eax, 0
leave
retn
_main endp
```

Gambarajah 1: Paparan Graf dari IDA PRO

Gambarajah 1 menunjukkan paparan graf dari IDA PRO, ia merupakan hasil dari analisa yang dibuat terhadap satu fail perisian. Berdasarkan paparan ini, sila jawab soalan-soalan berikut: -

(a) Apakah Bahasa pengatucaraan yang digunakan untuk menulis aturcara perisian ini? Sila kemukan bukti anda.

(2 markah)

(b) Lukiskan paparan konsol yang mungkin dipaparkan oleh perisian ini apabila pengguna memasukan 8ACF567 sebagai input.

(3 markah)

(c) Apakah yang akan membuatkan aplikasi ini memberikan pilihan yang benar? Berikan justifikasi.

(2 markah)

(d) Cari input rahsia yang boleh dimasukkan sebagai input perisian ini dan menyebabkan perisian ini boleh memaparkan *“You win”?* Tunjukan jalan kerja anda .

(6 markah)

(e) Berapa banyakkah Bytes yang digunakan untuk mewakili "UNITE" dalam format ASCII? Tunjukkan langkah anda (Sila rujuk jadual ASCII dalam Lampiran A)

(4 markah)

(f) Dengan merujuk kepada kod berikut, apakah yang disimpan dalam register EAX? Tunjukkan langkah anda

```
mov eax, 1Ah
sub eax, 11h
move edx, eax
shr edx, 3
```

(3 markah)

(g) Dengan merujuk kepada kod berikut, apakah yang disimpan dalam register EAX? Tunjukkan langkah anda

```
      PUSH 0AH
      POP eax
      PUSH 14h
      POP ebx
      SUB eax, 2
```

(5 markah)

SOALAN 3 (25 MARKAH)

Kajian Kes 2:

Dalam analisa dinamik, penganalisa malware perlu menyediakan persekitaran yang selamat sebelum mereka boleh menjalankan analisa malware. Sebagai penganalisa malware yang baru di Z Secure Sdn. Bhd., Anda telah ditugaskan untuk menganalisa kod hasad yang menyebabkan Router NetGear mempunyai simptom jangkitan kod hasad *Confickers.*

Berdasarkan Kajian Kes 2 di atas, jawab soalan-soalan berikut.

(a) Senaraikan alatan penganalisa perisian yang dikehendaki dalam

i. Penangkapan lalu lintas rangkaian

ii. Penangkapan aktiviti proses / *thread*

iii. Penangkapan *windows library* yang digunakan oleh sampel

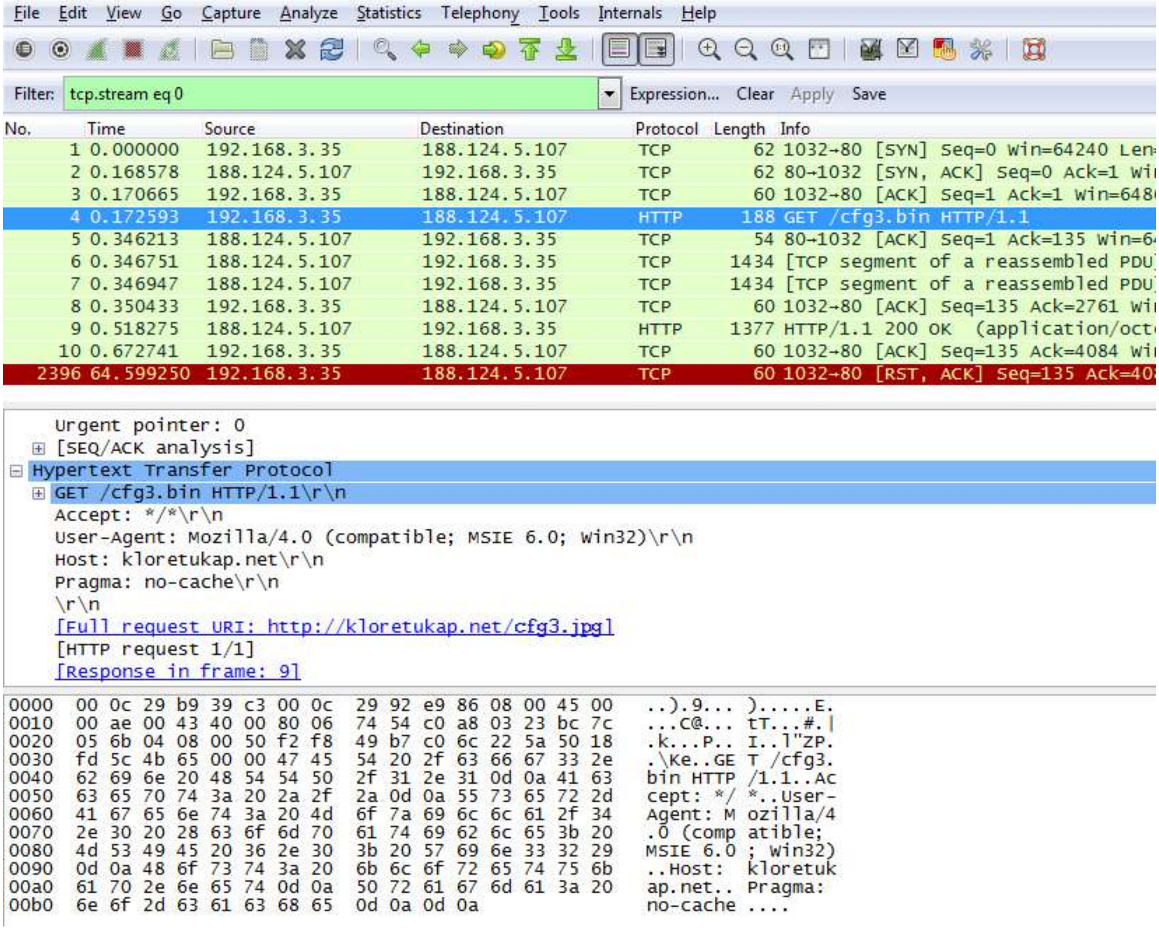
iv. Memeriksa samaada sampel kod telah di sembunyikan atau tidak

v. *Decompile* sampel binari

(5 markah)

(b) Rekabentuk dan lukiskan tapak kajian rangkaian yang boleh membantu anda dalam menyediakan persekitaran yang selamat untuk menganalisa botnet windows tersebut.

(5 markah)

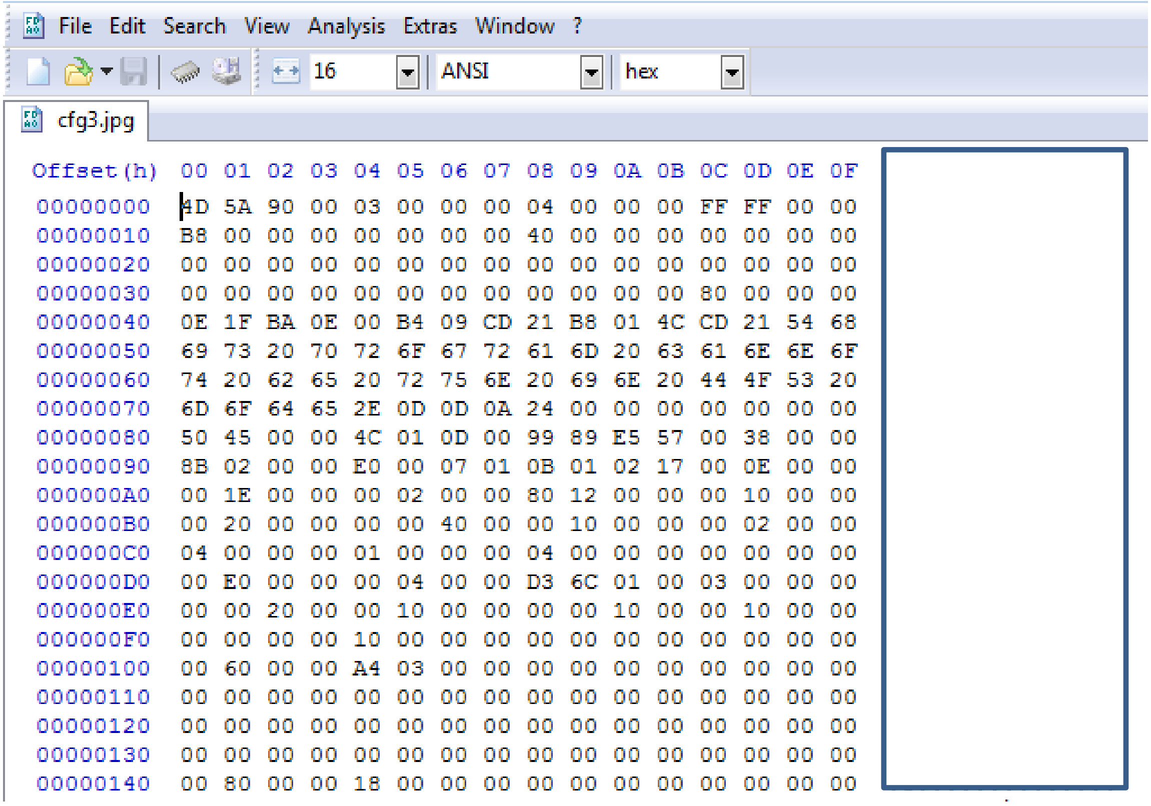

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

```
Filter: tcp.stream eq 0

No.   Time        Source          Destination     Protocol Length Info
    1 0.000000    192.168.3.35    188.124.5.107   TCP        62 1032→80 [SYN] Seq=0 Win=64240 Len
    2 0.168578    188.124.5.107   192.168.3.35    TCP        62 80→1032 [SYN, ACK] Seq=0 Ack=1 Wi
    3 0.170665    192.168.3.35    188.124.5.107   TCP        60 1032→80 [ACK] Seq=1 Ack=1 Win=648
    4 0.172593    192.168.3.35    188.124.5.107   HTTP      188 GET /cfg3.bin HTTP/1.1
    5 0.346213    188.124.5.107   192.168.3.35    TCP        54 80→1032 [ACK] Seq=1 Ack=135 Win=6
    6 0.346751    188.124.5.107   192.168.3.35    TCP      1434 [TCP segment of a reassembled PDU
    7 0.346947    188.124.5.107   192.168.3.35    TCP      1434 [TCP segment of a reassembled PDU
    8 0.350433    192.168.3.35    188.124.5.107   TCP        60 1032→80 [ACK] Seq=135 Ack=2761 Wi
    9 0.518275    188.124.5.107   192.168.3.35    HTTP     1377 HTTP/1.1 200 OK  (application/oct
   10 0.672741    192.168.3.35    188.124.5.107   TCP        60 1032→80 [ACK] Seq=135 Ack=4084 Wi
 2396 64.599250   192.168.3.35    188.124.5.107   TCP        60 1032→80 [RST, ACK] Seq=135 Ack=40

      Urgent pointer: 0
   ⊞ [SEQ/ACK analysis]
⊟ Hypertext Transfer Protocol
   ⊞ GET /cfg3.bin HTTP/1.1\r\n
      Accept: */*\r\n
      User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)\r\n
      Host: kloretukap.net\r\n
      Pragma: no-cache\r\n
      \r\n
      [Full request URI: http://kloretukap.net/cfg3.jpg]
      [HTTP request 1/1]
      [Response in frame: 9]

0000  00 0c 29 b9 39 c3 00 0c  29 92 e9 86 08 00 45 00   ..).9... ).....E.
0010  00 ae 00 43 40 00 80 06  74 54 c0 a8 03 23 bc 7c   ...C@... tT...#.|
0020  05 6b 04 08 00 50 f2 f8  49 b7 c0 6c 22 5a 50 18   .k...P.. I..l"ZP.
0030  fd 5c 4b 65 00 00 47 45  54 20 2f 63 66 67 33 2e   .\Ke..GE T /cfg3.
0040  62 69 6e 20 48 54 54 50  2f 31 2e 31 0d 0a 41 63   bin HTTP /1.1..Ac
0050  63 65 70 74 3a 20 2a 2f  2a 0d 0a 55 73 65 72 2d   cept: */ *..User-
0060  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 34   Agent: M ozilla/4
0070  2e 30 20 28 63 6f 6d 70  61 74 69 62 6c 65 3b 20   .0 (comp atible;
0080  4d 53 49 45 20 36 2e 30  3b 20 57 69 6e 33 32 29   MSIE 6.0 ; Win32)
0090  0d 0a 48 6f 73 74 3a 20  6b 6c 6f 72 65 74 75 6b   ..Host:  kloretuk
00a0  61 70 2e 6e 65 74 0d 0a  50 72 61 67 6d 61 3a 20   ap.net.. Pragma:
00b0  6e 6f 2d 63 61 63 68 65  0d 0a 0d 0a               no-cache ....
```

Gambarajah 2: Aktiviti lalu lintas rangkaian Botnet.

(c) Gambarajah 2 menunjukkan sebahagian daripada sampel aktiviti rangkaian botnet yang ditangkap oleh alat menangkap aktiviti rangkaian. Kenalpasti **ENAM (6)** maklumat penting yang anda boleh dapati dari sampel ini yang berkaitan dengan aktiviti botnet.

(6 markah)



```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000   4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
00000010   B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00000020   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030   00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00
00000040   0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
00000050   69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F
00000060   74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
00000070   6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00
00000080   50 45 00 00 4C 01 0D 00 99 89 E5 57 00 38 00 00
00000090   8B 02 00 00 E0 00 07 01 0B 01 02 17 00 0E 00 00
000000A0   00 1E 00 00 00 02 00 00 80 12 00 00 00 10 00 00
000000B0   00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00
000000C0   04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00
000000D0   00 E0 00 00 00 04 00 00 D3 6C 01 00 03 00 00 00
000000E0   00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00
000000F0   00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00
00000100   00 60 00 00 A4 03 00 00 00 00 00 00 00 00 00 00
00000110   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000120   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000130   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000140   00 80 00 00 18 00 00 00 00 00 00 00 00 00 00 00
```

Gambarajah 3: Fail Yang Dimuat Turun Oleh Aktiviti Botnet.

(d) Maklumat yang dikumpul dari gambarajah 2 telah membawa kepada fail yang dimuat turun ke komputer mangsa, fail yang dimuat turun kemudian terus dianalisa menggunakan perisian editor hex dan Gambarajah 3 menunjukkan paparan fail tersebut dalam paparan hex . Dengan merujuk kepada Lampiran B, berikan petunjuk penting yang menunjukkan keraguan fail ini. Sila terangkan jawapan anda.

(4 markah)

(e) Jika sampel yang diberikan adalah berasaskan botnet Android dan penganalisa *malware* perlu melakukan analisa malware meggunakan kaedah statik dan dinamik, apakah **LIMA (5)** alatan/persisian yang diperlukan untuk membuat analisa tersebut?

(5 markah)

-SOALAN TAMAT-

PART A: STRUCTURED QUESTIONS (25 MARKS)

INSTRUCTION: *Answer **ALL** questions.*

(a) Explain what do REvil, Avaddon and Conti Malicious software have in commons?

(2 marks)

(b) Azlin's Personal Computer has been diagnosed with *Ransomware* and believed to be Similar like *WannaCry*. What type of Operating System platform Azlin used in her computer? Justify your answer and what are the **THREE (3)** possibilities that could happen to Azlin's computer and her network environment?

(6 marks)

(c) Soh Hoon just bought a tablet, and she cannot decide whether to include an antivirus or not in his tablet. To persuade her to buy the antivirus, you as a salesperson need to explain in detail about the behaviour of malware and the effect that might happened in her tablet if infected by malware. List and explain **FOUR (4)** general behaviours of malware once it is infecting a tablet.

(8 marks)

(d) As a malware analyst, Thanasilan has been given a sample of Conficker malware. What are the **THREE (3)** symptoms Thanasilan might notice on a machine when running this malware? What are **THREE (3)** Technical questions Thanasilan might ask during the analysis of this malware and state which sources in the infected machine Thanasilan might use to get the answer to his Technical questions?

(9 marks)

PART B: STRUCTURED QUESTIONS (75 MARKS)

INSTRUCTION: *Answer **ALL** questions*

QUESTION 1 (25 MARKS)

Case Study 1:

Danial has obtained Bachelor Degree of Computer Science (Computer Security) from Universiti Teknikal Malaysia Melaka (UTeM). He is attending an interview for a junior malware analyst in R-Protect Sdn. Bhd. The following questions are asked during the interview. Based on this Case Study 1, answer the following questions.

(a) Explain why a malware analyst must create a safe environment before analysing a malware sample? And suggest **THREE (3)** precaution step a malware analyst should do and prepare before investigating a malware sample.

(6 marks)

(b) Discuss the methods that can be used to analyse an android malware sample and briefly discuss the benefits and drawbacks of each analysis method?

(8 marks)

(c) Suggest **TWO (2)** approaches for automated malware analysis and give an example of tools that can be used for each approach.

(4 marks)

(d) List **FIVE (5)** methods used by a malware author to avoid detection from a malware analyst.

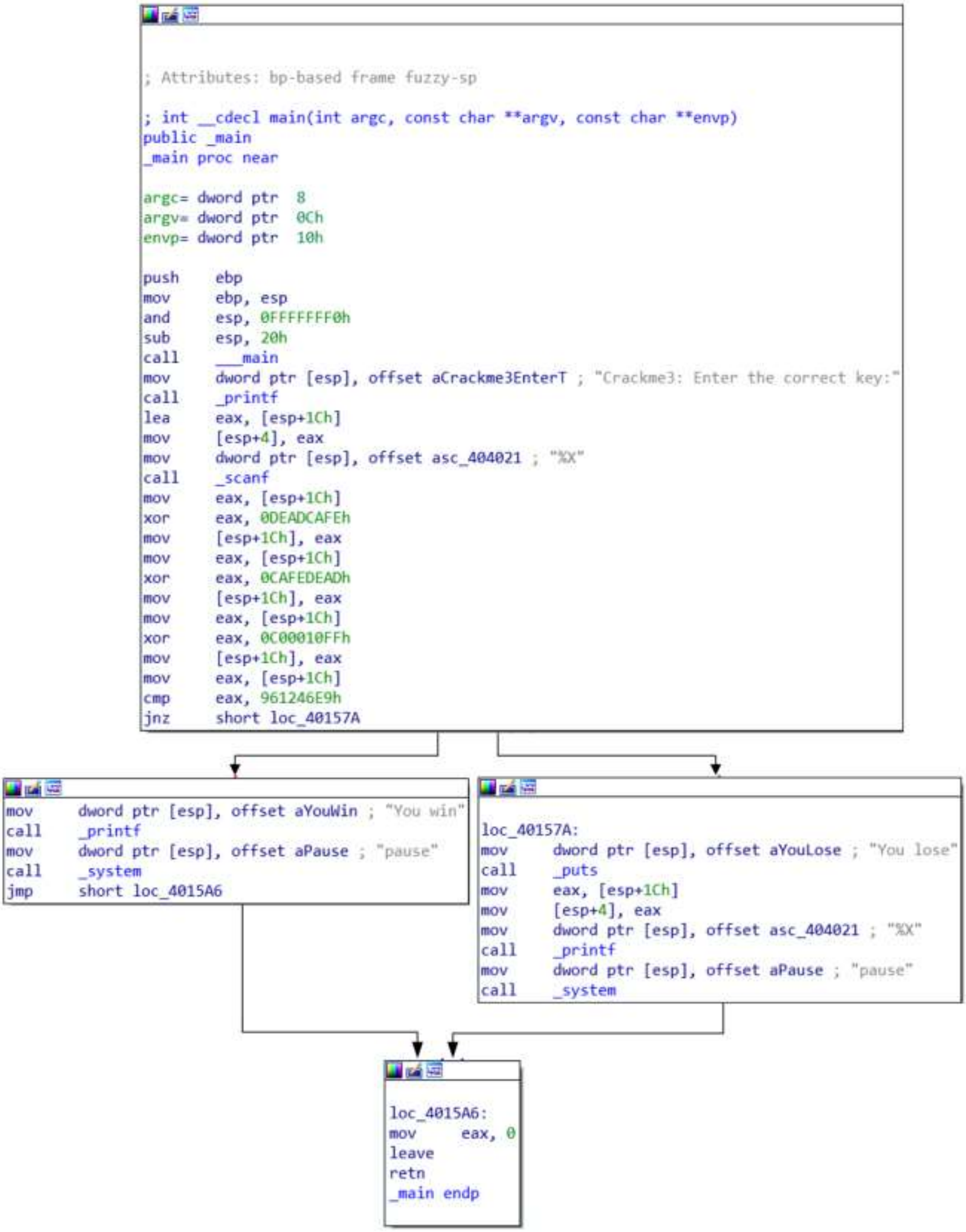
(5 marks)

(e) Give **TWO (2)** Virtual Machine tools that can be used for malware analysis.

(2 marks)

QUESTION 2 (25 MARKS)

Question (a) to (e) is based on Figure 1:



```
; Attributes: bp-based frame fuzzy-sp

; int __cdecl main(int argc, const char **argv, const char **envp)
public _main
_main proc near

argc= dword ptr  8
argv= dword ptr  0Ch
envp= dword ptr  10h

push    ebp
mov     ebp, esp
and     esp, 0FFFFFFF0h
sub     esp, 20h
call    ___main
mov     dword ptr [esp], offset aCrackme3EnterT ; "Crackme3: Enter the correct key:"
call    _printf
lea     eax, [esp+1Ch]
mov     [esp+4], eax
mov     dword ptr [esp], offset asc_404021 ; "%X"
call    _scanf
mov     eax, [esp+1Ch]
xor     eax, 0DEADCAFEh
mov     [esp+1Ch], eax
mov     eax, [esp+1Ch]
xor     eax, 0CAFEDEADh
mov     [esp+1Ch], eax
mov     eax, [esp+1Ch]
xor     eax, 0C00010FFh
mov     [esp+1Ch], eax
mov     eax, [esp+1Ch]
cmp     eax, 961246E9h
jnz     short loc_40157A
```

```
mov     dword ptr [esp], offset aYouWin ; "You win"
call    _printf
mov     dword ptr [esp], offset aPause ; "pause"
call    _system
jmp     short loc_4015A6
```

```
loc_40157A:
mov     dword ptr [esp], offset aYouLose ; "You lose"
call    _puts
mov     eax, [esp+1Ch]
mov     [esp+4], eax
mov     dword ptr [esp], offset asc_404021 ; "%X"
call    _printf
mov     dword ptr [esp], offset aPause ; "pause"
call    _system
```

```
loc_4015A6:
mov     eax, 0
leave
retn
_main endp
```

Figure 1: Graph View from an IDA PRO Output

Figure 1 shows a Graph View from an IDA PRO Output for an executable file. Based on Figure 1, answer the following questions:-

(a) What is the programming language being used to code this program? Why?

(2 marks)

(b) Draw a possible console output for this program when the user enters 8ACF567.

(3 marks)

(c) What makes the application to trigger a true condition in this program? Justify your answer.

(2 marks)

(d) Find the correct input to be entered into the program so that the user will be notified by “You win”? Show your steps.

(6 marks)

(e) How many bytes are used to represent “UNITE” in ASCII code? Show your step (You may refer to the ASCII to Hexadecimal Table in Appendix A)

(4 marks)

(f) By referring to the following code below, what will be stored in register `edx`? Show your steps in getting your answer.

```
mov eax, 1Ah
sub eax, 11h
move edx, eax
shr edx, 3
```

(3 marks)

(g) By referring to the following code, what will be stored in register `eax`? Show your steps in getting your answer.

```
      PUSH 0Ah
      POP eax
      PUSH 14h
      POP ebx
      SUB eax, 2
```

(5 marks)

QUESTION 3 (25 MARKS)

Case Study 2:

In dynamic analysis, malware analyst needs to prepare a safe environment before they can run a malware analysis. As a new malware analyst at Z Secure Sdn. Bhd., you have been assigned to analyse a malware that causes the NetGear router to have a symptom like Confikers infections.

Based on the Case Study 2, answer the following questions.

(a) List the tool a malware analyst required to

i. Capture the network traffic

ii. Capture the process/thread activity

iii. Capture all the windows library use by the sample

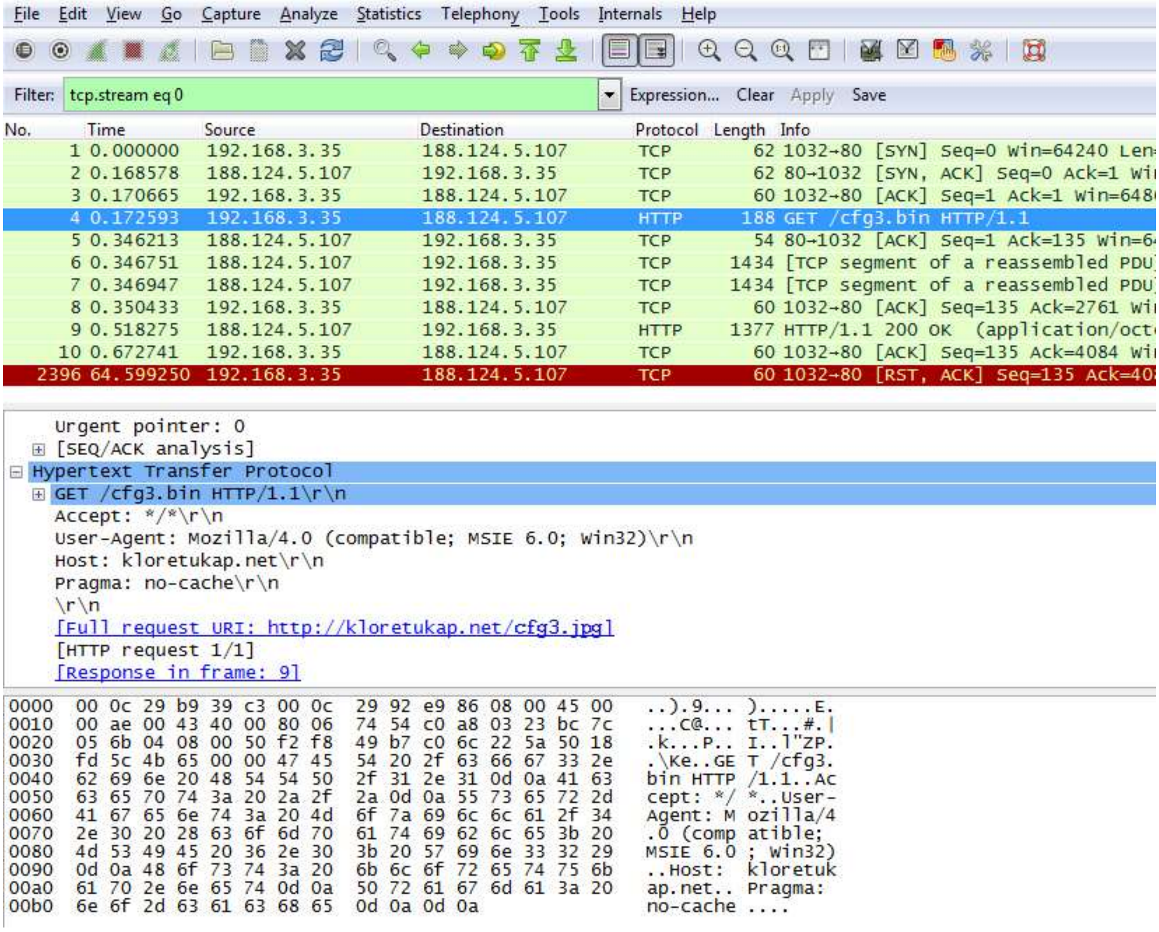
iv. Check whether the sample is obfuscated or not

v. Decompile the binary sample

(5 marks)

(b) Design and draw a network testbed that can help you in providing a safe environment for running a windows botnet.

(5 marks)


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: tcp.stream eq 0

```
No.   Time        Source          Destination     Protocol Length Info
    1 0.000000    192.168.3.35    188.124.5.107   TCP        62 1032→80 [SYN] Seq=0 Win=64240 Len
    2 0.168578    188.124.5.107   192.168.3.35    TCP        62 80→1032 [SYN, ACK] Seq=0 Ack=1 Wi
    3 0.170665    192.168.3.35    188.124.5.107   TCP        60 1032→80 [ACK] Seq=1 Ack=1 Win=648
    4 0.172593    192.168.3.35    188.124.5.107   HTTP      188 GET /cfg3.bin HTTP/1.1
    5 0.346213    188.124.5.107   192.168.3.35    TCP        54 80→1032 [ACK] Seq=1 Ack=135 Win=6
    6 0.346751    188.124.5.107   192.168.3.35    TCP      1434 [TCP segment of a reassembled PDU
    7 0.346947    188.124.5.107   192.168.3.35    TCP      1434 [TCP segment of a reassembled PDU
    8 0.350433    192.168.3.35    188.124.5.107   TCP        60 1032→80 [ACK] Seq=135 Ack=2761 Wi
    9 0.518275    188.124.5.107   192.168.3.35    HTTP     1377 HTTP/1.1 200 OK  (application/oct
   10 0.672741    192.168.3.35    188.124.5.107   TCP        60 1032→80 [ACK] Seq=135 Ack=4084 Wi
 2396 64.599250   192.168.3.35    188.124.5.107   TCP        60 1032→80 [RST, ACK] Seq=135 Ack=40
```

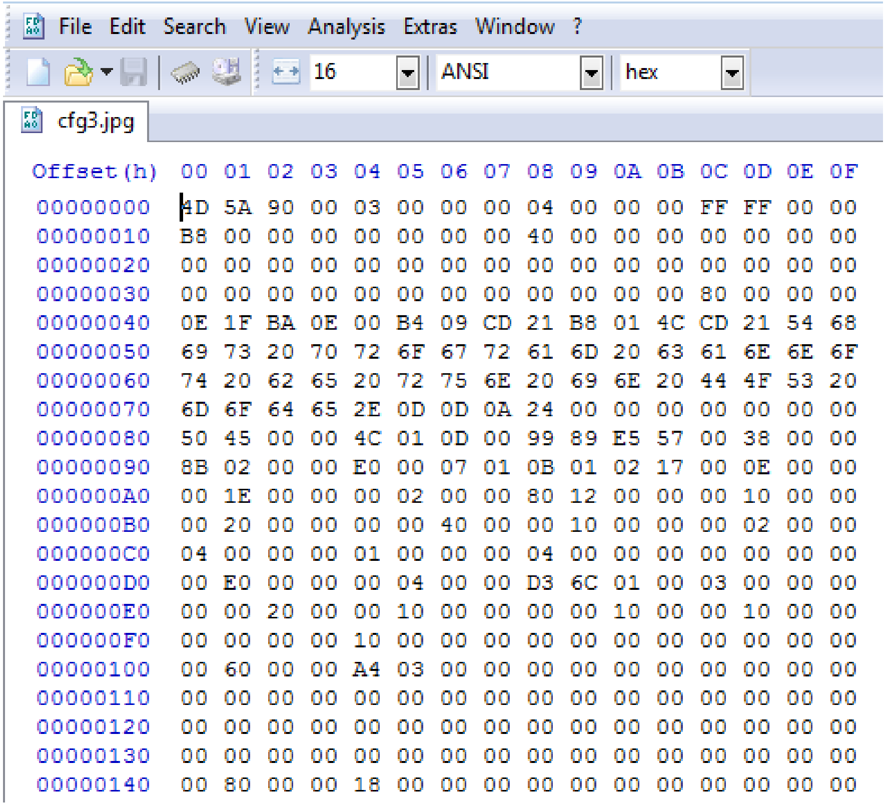
```
    Urgent pointer: 0
  ⊞ [SEQ/ACK analysis]
⊟ Hypertext Transfer Protocol
  ⊞ GET /cfg3.bin HTTP/1.1\r\n
    Accept: */*\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Win32)\r\n
    Host: kloretukap.net\r\n
    Pragma: no-cache\r\n
    \r\n
    [Full request URI: http://kloretukap.net/cfg3.jpg]
    [HTTP request 1/1]
    [Response in frame: 9]
```

```
0000  00 0c 29 b9 39 c3 00 0c  29 92 e9 86 08 00 45 00   ..).9... ).....E.
0010  00 ae 00 43 40 00 80 06  74 54 c0 a8 03 23 bc 7c   ...C@... tT...#.|
0020  05 6b 04 08 00 50 f2 f8  49 b7 c0 6c 22 5a 50 18   .k...P.. I..l"ZP.
0030  fd 5c 4b 65 00 00 47 45  54 20 2f 63 66 67 33 2e   .\Ke..GE T /cfg3.
0040  62 69 6e 20 48 54 54 50  2f 31 2e 31 0d 0a 41 63   bin HTTP /1.1..Ac
0050  63 65 70 74 3a 20 2a 2f  2a 0d 0a 55 73 65 72 2d   cept: */ *..User-
0060  41 67 65 6e 74 3a 20 4d  6f 7a 69 6c 6c 61 2f 34   Agent: M ozilla/4
0070  2e 30 20 28 63 6f 6d 70  61 74 69 62 6c 65 3b 20   .0 (comp atible;
0080  4d 53 49 45 20 36 2e 30  3b 20 57 69 6e 33 32 29   MSIE 6.0 ; Win32)
0090  0d 0a 48 6f 73 74 3a 20  6b 6c 6f 72 65 74 75 6b   ..Host:  kloretuk
00a0  61 70 2e 6e 65 74 0d 0a  50 72 61 67 6d 61 3a 20   ap.net.. Pragma:
00b0  6e 6f 2d 63 61 63 68 65  0d 0a 0d 0a              no-cache ....
```

Figure 2: Windows Botnet network traffic activity.

(c) Figure 2 shows part of botnet sample network activity captured by a network capturing tool. Identify **SIX (6)** important valuable information that you can observe from this botnet activity.

(6 marks)



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000030  00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00
00000080  50 45 00 00 4C 01 0D 00 99 89 E5 57 00 38 00 00
00000090  8B 02 00 00 E0 00 07 01 0B 01 02 17 00 0E 00 00
000000A0  00 1E 00 00 00 02 00 00 80 12 00 00 00 10 00 00
000000B0  00 20 00 00 00 00 40 00 00 10 00 00 00 02 00 00
000000C0  04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00
000000D0  00 E0 00 00 00 04 00 00 D3 6C 01 00 03 00 00 00
000000E0  00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00
000000F0  00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00
00000100  00 60 00 00 A4 03 00 00 00 00 00 00 00 00 00 00
00000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000140  00 80 00 00 18 00 00 00 00 00 00 00 00 00 00 00
```

Figure 3: Hex Value for the file downloaded from the botnet activity.

(d) The information gathered from Figure 2 has led to a file downloaded to the victim's computer. The downloaded file is then further analysed using a hex editor and Figure 3 shows the hex value of the file. By refering to Appendix B, give an important clue what is wrong with this file? Justify your answer.

(4 marks)

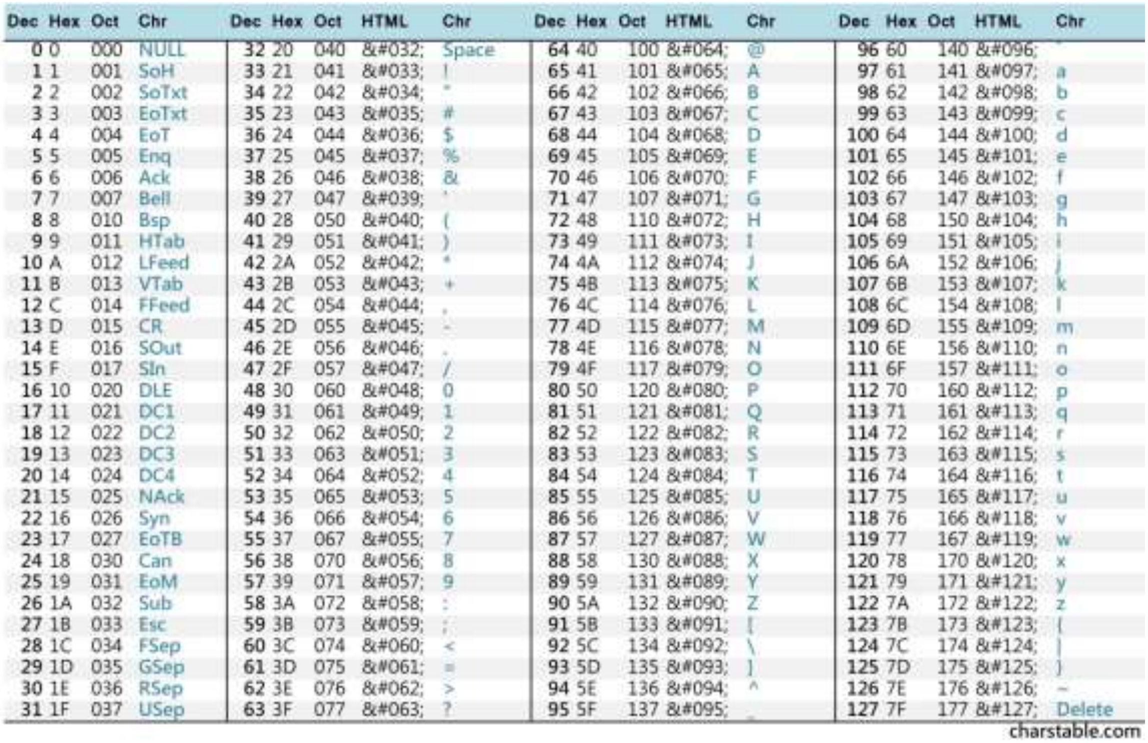
(e) If the given sample is an Android based botnet and the malware analyst needs to do a static and dynamic malware analysis approach on the botnet, give **FIVE (5)** tools needed to do the analysis ?

(5 marks)

- END OF QUESTIONS-

Appendix A /Lampiran A

ASCII Conversion Table/ Jadual Penukaran ASCII



Dec	Hex	Oct	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr	Dec	Hex	Oct	HTML	Chr
0	0	000	NULL	32	20	040	&#032;	Space	64	40	100	&#064;	@	96	60	140	&#096;	`
1	1	001	SoH	33	21	041	&#033;	!	65	41	101	&#065;	A	97	61	141	&#097;	a
2	2	002	SoTxt	34	22	042	&#034;	"	66	42	102	&#066;	B	98	62	142	&#098;	b
3	3	003	EoTxt	35	23	043	&#035;	#	67	43	103	&#067;	C	99	63	143	&#099;	c
4	4	004	EoT	36	24	044	&#036;	$	68	44	104	&#068;	D	100	64	144	&#100;	d
5	5	005	Enq	37	25	045	&#037;	%	69	45	105	&#069;	E	101	65	145	&#101;	e
6	6	006	Ack	38	26	046	&#038;	&	70	46	106	&#070;	F	102	66	146	&#102;	f
7	7	007	Bell	39	27	047	&#039;	'	71	47	107	&#071;	G	103	67	147	&#103;	g
8	8	010	Bsp	40	28	050	&#040;	(	72	48	110	&#072;	H	104	68	150	&#104;	h
9	9	011	HTab	41	29	051	&#041;	)	73	49	111	&#073;	I	105	69	151	&#105;	i
10	A	012	LFeed	42	2A	052	&#042;	*	74	4A	112	&#074;	J	106	6A	152	&#106;	j
11	B	013	VTab	43	2B	053	&#043;	+	75	4B	113	&#075;	K	107	6B	153	&#107;	k
12	C	014	FFeed	44	2C	054	&#044;	,	76	4C	114	&#076;	L	108	6C	154	&#108;	l
13	D	015	CR	45	2D	055	&#045;	-	77	4D	115	&#077;	M	109	6D	155	&#109;	m
14	E	016	SOut	46	2E	056	&#046;	.	78	4E	116	&#078;	N	110	6E	156	&#110;	n
15	F	017	SIn	47	2F	057	&#047;	/	79	4F	117	&#079;	O	111	6F	157	&#111;	o
16	10	020	DLE	48	30	060	&#048;	0	80	50	120	&#080;	P	112	70	160	&#112;	p
17	11	021	DC1	49	31	061	&#049;	1	81	51	121	&#081;	Q	113	71	161	&#113;	q
18	12	022	DC2	50	32	062	&#050;	2	82	52	122	&#082;	R	114	72	162	&#114;	r
19	13	023	DC3	51	33	063	&#051;	3	83	53	123	&#083;	S	115	73	163	&#115;	s
20	14	024	DC4	52	34	064	&#052;	4	84	54	124	&#084;	T	116	74	164	&#116;	t
21	15	025	NAck	53	35	065	&#053;	5	85	55	125	&#085;	U	117	75	165	&#117;	u
22	16	026	Syn	54	36	066	&#054;	6	86	56	126	&#086;	V	118	76	166	&#118;	v
23	17	027	EoTB	55	37	067	&#055;	7	87	57	127	&#087;	W	119	77	167	&#119;	w
24	18	030	Can	56	38	070	&#056;	8	88	58	130	&#088;	X	120	78	170	&#120;	x
25	19	031	EoM	57	39	071	&#057;	9	89	59	131	&#089;	Y	121	79	171	&#121;	y
26	1A	032	Sub	58	3A	072	&#058;	:	90	5A	132	&#090;	Z	122	7A	172	&#122;	z
27	1B	033	Esc	59	3B	073	&#059;	;	91	5B	133	&#091;	[	123	7B	173	&#123;	{
28	1C	034	FSep	60	3C	074	&#060;	<	92	5C	134	&#092;	\	124	7C	174	&#124;	|
29	1D	035	GSep	61	3D	075	&#061;	=	93	5D	135	&#093;	]	125	7D	175	&#125;	}
30	1E	036	RSep	62	3E	076	&#062;	>	94	5E	136	&#094;	^	126	7E	176	&#126;	~
31	1F	037	USep	63	3F	077	&#063;	?	95	5F	137	&#095;	_	127	7F	177	&#127;	Delete

charstable.com

APPENDIX B/ LAMPIRAN B

File Signatures Table/ Jadual *File Signature*

Hex signature	**ISO 8859-1**	**Offset**	**File extension**	**Description**
FF FE 00 00	....	0		Byte-order mark for text file encoded in little-endian 32-bit Unicode Transfer Format
FF FE	..	0		Byte-order mark for text file encoded in little-endian 16-bit Unicode Transfer Format
FF FB	˙ű	0	mp3	MPEG-1 Layer 3 file without an ID3 tag or with an ID3v1 tag (which's appended at the end of the file)
FF D8 FF E0 or FF D8 FF DB	ÿØÿà	0	jpg, jpeg	JPEG
4D 5A	....	0 or typically 0x1000		COM, DLL, DRV, EXE, PIF, QTS, QTX, SYS Windows/DOS executable file
FE ED FA CE	....	0 or typically 0x1000		Mach-O binary (32-bit)
EF BB BF	ï»¿	0		UTF-8 encoded Unicode byte order mark, commonly seen in text files.

Hex signature	ISO 8859-1	Offset	File extension	Description
49 44 33	ID3	0	mp3	MP3 file with an ID3v2 container
47 49 46 38 37 61 47 49 46 38 39 61	GIF87a GIF89a	0	gif	Image file encoded in the Graphics Interchange Format (GIF)[2] Graphics interchange format file Trailer: 00 3B (.;)
46 4F 52 4D nn nn nn nn 59 55 56 4E	FORM....YUVN	0, any	yuvn, yuv, iff	IFF YUV Image