UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA
PEPERIKSAAN AKHIR SEMESTER I
FINAL EXAMINATION SEMESTER I
SESI 2019/2020
SESSION 2019/2020

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI

KOD KURSUS ***COURSE CODE***	**: BITS 3453**
KURSUS ***COURSE***	**: ANALISA MALWARE & PENYIASATAN DIGITAL** ***MALWARE ANALYSIS & DIGITAL INVESTIGATION***
PENYELARAS ***COORDINATOR***	**: MOHD ZAKI MAS'UD**
PROGRAM ***PROGRAMME***	**: 3 BITZ**
MASA ***TIME***	**: 2.15 PTG** ***2.15 PM***
TEMPOH ***DURATION***	**: 2 JAM 30 MINIT** ***2 HOURS 30 MINUTES***
TARIKH ***DATE***	**: 30 DISEMBER 2019** ***30 DECEMBER 2019***
TEMPAT ***VENUE***	**: B. KULIAH 5 PBPI** ***PBPI LECTURE ROOM 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. Sila jawab di dalam buku jawapan yang disediakan.
   Please answer in the answer booklet provided.
3. Kertas soalan ini mempunyai versi dwi-bahasa.
   The exam paper consists of dual-language version.

KERTAS SOALAN INI TERDIRI DARIPADA DUA PULUH DUA (22) MUKA SURAT SAHAJA (TERMASUK MUKA SURAT HADAPAN)
THIS QUESTION PAPER CONTAINS TWENTY TWO (22) PAGES INCLUSIVE OF FRONT PAGE

PERINGATAN
REMINDER:

PELAJAR TIDAK DIBENARKAN SAMA SEKALI MEMBAWA APA-APA BUKU, KERTAS, SURATAN, GAMBAR, NOTA, SEBARANG ALAT YANG DI DALAM ATAU DI ATASNYA TERDAPAT CATATAN BERTULIS, 'PROGRAMMABLE CALCULATOR', TELEFON MUDAH ALIH ATAU SEBARANG ALAT KECUALI YANG DIBENARKAN OLEH PENGAWAS KE DALAM ATAU KELUAR DARI SESUATU DEWAN PEPERIKSAAN ATAU MENERIMA APA-APA BUKU, KERTAS, SURATAN, GAMBAR, NOTA, SEBARANG ALAT YANG DI DALAM ATAU DI ATASNYA TERDAPAT CATATAN BERTULIS, 'PROGRAMMABLE CALCULATOR', TELEFON MUDAH ALIH ATAU SEBARANG ALAT DARI MANA-MANA ORANG LAIN SEMASA DI DALAM DEWAN PEPERIKSAAN KECUALI SESEORANG PELAJAR SEMASA IA BERADA DI DALAM DEWAN PEPERIKSAAN ITU MENERIMA DARIPADA PENGAWAS APA-APA BUKU, KERTAS, DOKUMEN/GAMBAR ATAU LAIN-LAIN ALAT YANG DIBENARKAN OLEH NAIB CANSELOR ATAS SYOR PEMERIKSA ATAU FAKULTI.

STUDENTS ARE NOT ALLOWED TO BRING IN ANY BOOKS, PAPERS, DOCUMENTS, PHOTOGRAPHS, NOTES, ANY TOOLS WHICH THERE ARE WRITTEN RECORDS, MOBILE PHONES, OR ANY OTHER DEVICES WITHOUT THE PRIOR PERMISSION OF THE INVIGILATORS INTO OR OUT OF THE EXAMINATION HALL, OR RECEIVE ANY PAPERS, BOOKS, DOCUMENTS, PHOTOGRAPHS, NOTES, ANY DEVICES IN OR ON WHICH THERE ARE WRITTEN RECORDS, 'PROGRAMMABLE CALCULATORS', OR TOOLS FROM OTHER PERSON(S) PRESENT IN THE EXAMINATION HALL; EXCEPT MATERIALS OR DEVICES PROVIDED BY THE INVIGILATORS AND PERMITTED BY THE VICE CHANCELLOR ON THE RECOMMENDATIONS OF THE EXAMINERS OR FACULTIES.

PART A: STRUCTURED QUESTIONS (25 MARKS)

INSTRUCTION: *Answer ALL questions.*

(a) Explain what malicious software is and give one example of a malicious software?

(2 marks)

(b) Suriyanti's Personal Computer has been diagnosed with malware and it is believe to be a Botnet infection. List any **FOUR(4)** possibilities that might be a sign or symptom that can happen to her personal computer due to the Botnet infection.

(4 marks)

(c) Tan Loh Cheng just bought a tablet and he cannot decide whether to include an antivirus or not in his tablet. In order to persuade him to buy the antivirus, you as a salesperson need to explain in detail about the threats of malware that might infect his tablet. List and explain **FOUR (4)** types of malware that are possible to infect the tablet if an antivirus is not installed.

(8 marks)

(d) As a malware analyst, Khiran has been given a sample of a file that has been infected by malware. Give **TWO (2)** reasons why malware analysis must be done to the file. List **FOUR (4)** technical questions asked during malware analysis.

(6 marks)

(e) There are 5 general steps in digital investigation process that can be applied in investigating malware incident. List the **FIVE (5)** steps involve in digital investigation process.

(5 marks)

PART B: STRUCTURED QUESTIONS (75 MARKS)

INSTRUCTION: *Answer ALL questions*

QUESTION 1 (25 MARKS)

Case Study 1:

Haffez has a Bachelor Degree of Computer Science (Computer Security) from Universiti Teknikal Malaysia Melaka (UTeM). He attended an interview for a junior malware analyst in M-Secure Sdn. Bhd. The following questions are among the question asked during the interview.

Based on the case study 1, answer the following questions.

(a) Identify **FOUR (4)** approaches in creating virus signature.

(4 marks)

(b) Explain what is an automated malware analysis? And suggest **ONE (1)** tool that can be used to do an automated analysis on a malware sample.

(2 marks)

(c) Give a brief description on static and dynamic malware analysis?

(2 marks)

(d) Give **THREE (3)** benefits and drawbacks of each analysis.

(6 marks)

(e) List **FIVE (5)** methods used by a malware author to defence themselves from being detected by the malware analyst.

(5 marks)

(f) Briefly explain what Virtual Machine is and how it can help in providing a quick and safe malware analysis environment?

(4 marks)

(g) 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:

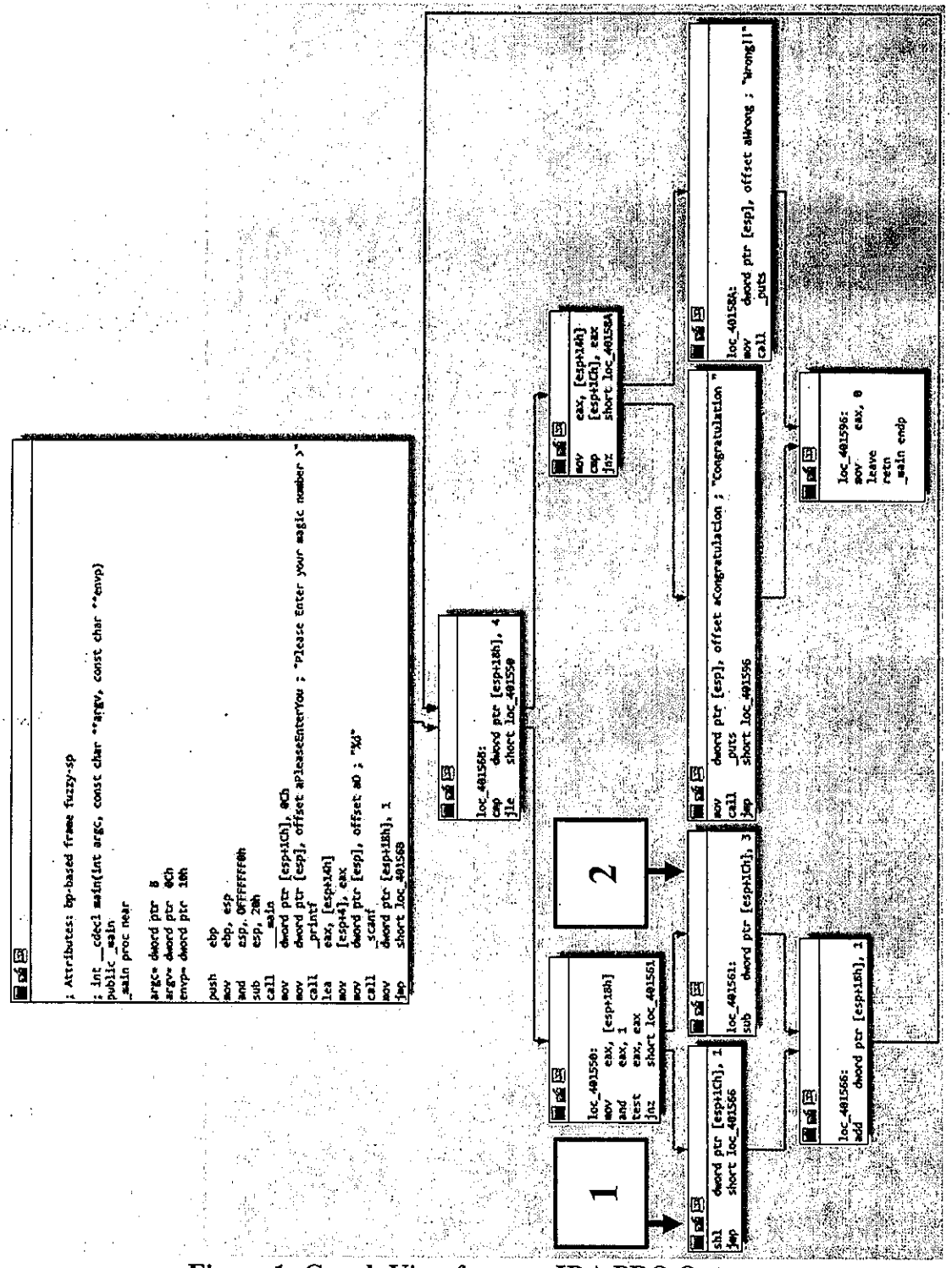


Figure 1: Graph View from an IDA PRO Output

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 used to code this program? Why?

(2 marks)

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

(3 marks)

(c) What is the two mathematical operation in the box 1 and 2 represent?

(2 marks)

(d) How many loop is being executed before the program compare the input keyed in and the magic number?

(1 mark)

(e) Find the correct secret number to be entered to the program so that the user will be notified by "Congratulation"? Show your steps.

(5 marks)

(f) How many Bytes are use to represent "UNITE" in Unicode? Show your step (Please refer to the ASCII to Hexadecimal Table in Appendix A)

(4 marks)

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

```
mov eax, 6
sub eax, 02h
move edx, eax
shr edx, 2
```

(3 marks)

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

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

(5 marks)

QUESTION 3 (25 MARKS)

Case Study 2:

There are two approaches in analysing malware, namely, static and dynamic analysis. In dynamic analysis, malware analyst needs to prepare a safe environment before they can run the malware analysis. As a new malware analyst at M Secure Sdn. Bhd., you have been assigned to analyse a new variant of windows based botnet that just hit the Internet. 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 wheather 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 the windows botnet.

(5 marks)

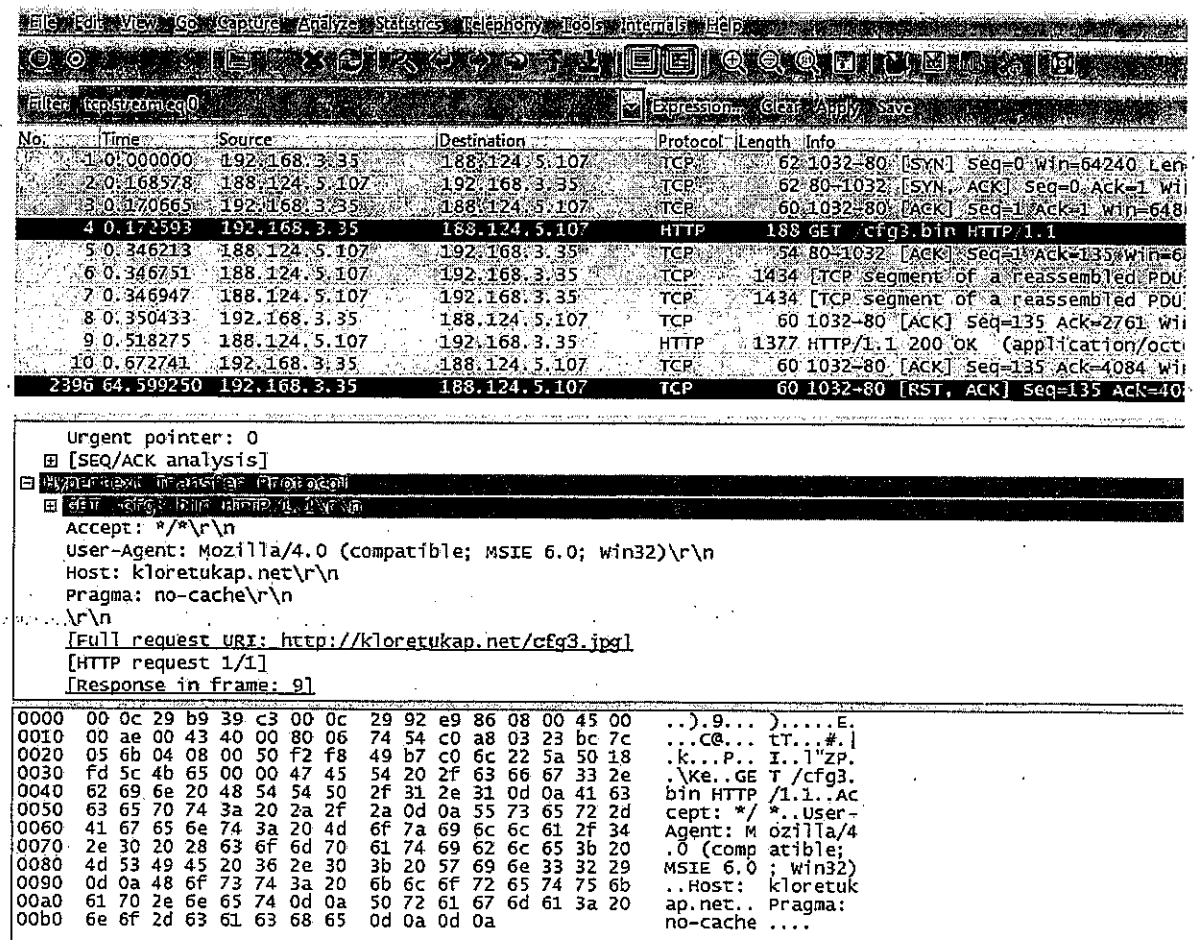
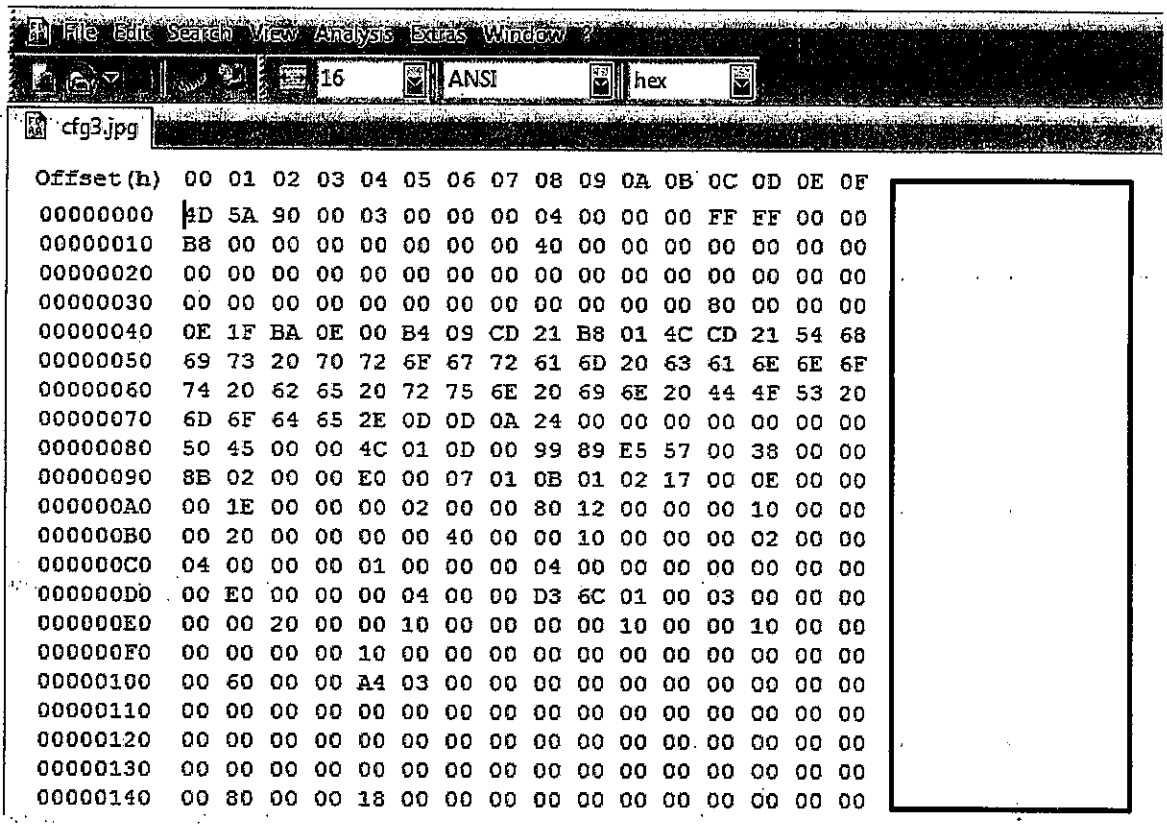


Figure 2: Windows Botnet network traffic activity.

(c) Figure 2 shows the part of botnet sample network activity captured by the network capturing tools. Identify **SIX (6)** important information that you can relate to the 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 gather 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 are android based botnet and the malware analyst needs to do a static and dynamic malware analysis approach on the botnet, what are the **FIVE (5)** tools needed to do the analysis ?

(5 marks)

- END OF QUESTIONS-

BAHAGIAN A: SOALAN BERSTRUKTUR (25 MARKAH)

ARAHAN: *Sila jawab SEMUA soalan*

(a) Apakah yang dikatakan sebagai perisian hasad dan berikan satu contoh perisian hasad?

(2 markah)

(b) Komputer Suriyanti baru sahaja dijangkiti oleh *malware* dan dipercayai *malware* itu adalah dari jenis *Botnet*. Senaraikan **EMPAT (4)** kemungkinan yang mungkin menjadi tanda atau gejala yang boleh berlaku kepada komputer riba beliau yang disebabkan oleh jangkitan *Botnet* itu.

(4 markah)

(c) Tan Loh Cheng baru sahaja membeli sebuah tablet dan dia belum lagi membuat keputusan sama ada untuk memasukkan *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)** jenis *malware* yang mungkin menjangkiti tablet Tan Loh Cheng jika tiada antivirus di masukkan kedalam telefon pintar tersebut.

(8 markah)

(d) Sebagai penyiasat *malware*, Khiran telah diberikan sampel fail yang telah dijangkiti oleh *malware*. Berikan **DUA (2)** sebab mengapa penganalisaan *malware* perlu dibuat ke atas fail tersebut? Dan senaraikan **EMPAT (4)** soalan teknikal yang akan ditanya semasa penganalisaan *malware* tersebut.

(6 markah)

(e) Terdapat 5 langkah umum dalam proses siasatan digital yang boleh digunakan dalam menyiasat kejadian malware. Senaraikan secara ringkas **LIMA (5)** langkah tersebut.

(5 markah)

BAHAGIAN B: SOALAN BERSTRUKTUR (75 MARKAH)

ARAHAN: *Sila jawab SEMUA soalan*

SOALAN 1 (25 MARKAH)

Kajian Kes 1:

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

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

(a) Kenal pasti **EMPAT (4)** pendekatan dalam membuat *virus signature.*

(4 markah)

(b) Terangkan apakah yang dimaksudkan dengan analisa *malware* secara automatik? Dan cadangkan **SATU (1)** peralatan yang boleh digunakan untuk menjalankan analisa malware secara automatik terhadap sampel malware.

(2 markah)

(c) Terangkan apakah yang di maksudkan sebagai penganalisian *malware* statik dan dinamik.

(2 markah)

(d) Berikan **TIGA (3)** kebaikan dan kelemahan setiap kaedah analisa *malware.*

(6 markah)

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

(5 markah)

(f) Terangkan secara ringkas apakah yang dimaksudkan dengan *Virtual Machine* dan bagaimana ia boleh membantu dalam menganalisa *malware* dengan cepat dan selamat.

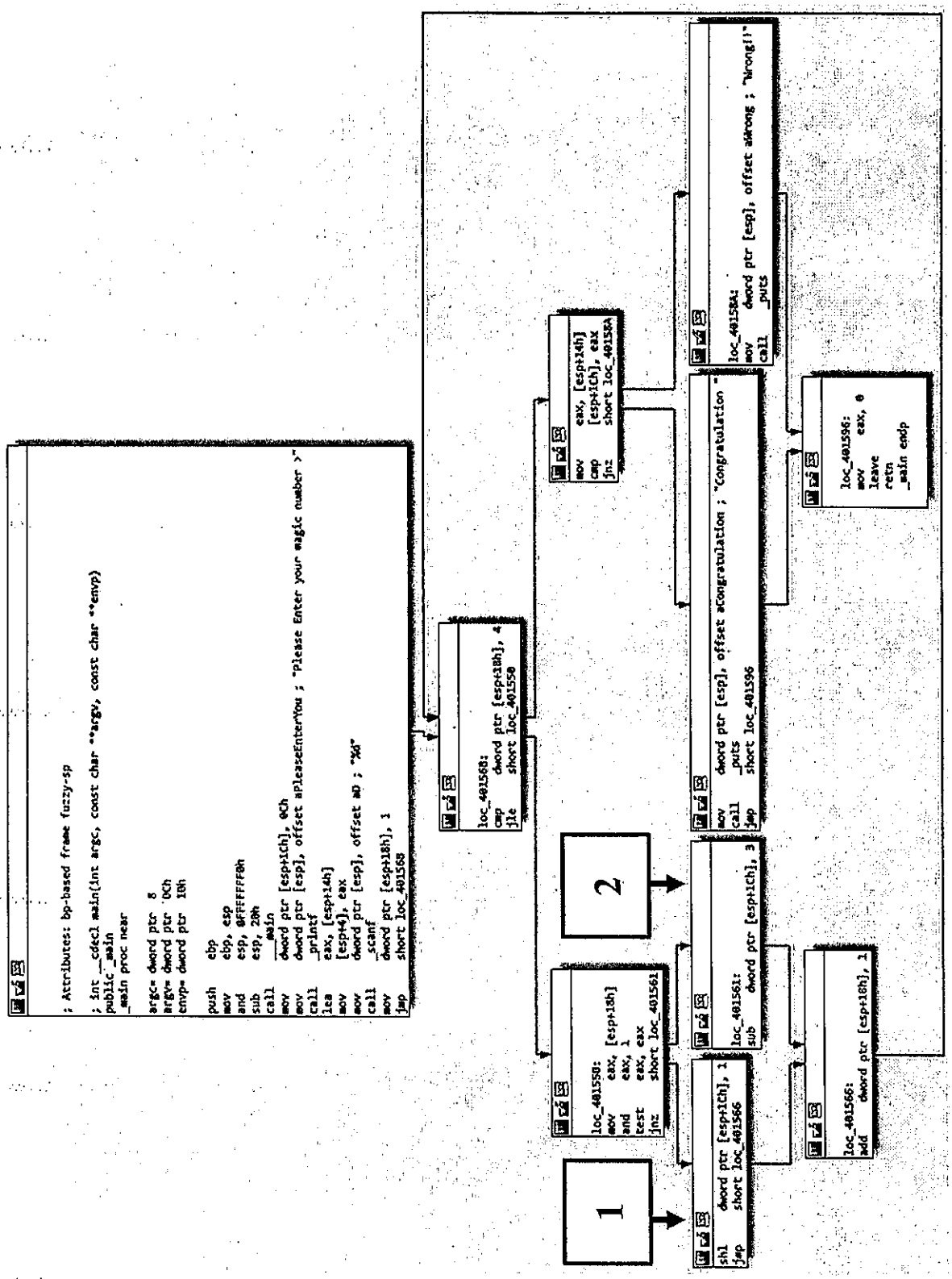
(4 markah)

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

(2 markah)

SOALAN 2 (25 MARKAH)

Soalan (a) hingga (e) berdasarkan Gambarajah 1



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 8 sebagai input.

(3 markah)

(c) Apakah dua operasi matematik yang digambarkan oleh kotak [1] dan kotak [2]?

(2 markah)

(d) Berapakah pusingan yang dibuat oleh atucara ini sebelum ia membandingkan data yang dimasukkan dengan nombor magik ?

(1 markah)

(e) Cari nombor rahsia yang boleh dimasukkan sebagai input perisian ini dan menyebabkan perisian ini boleh memaparkan *"Congratulation"?* Tunjukan jalan kerja anda .

(5 markah)

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

(4 markah)

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

```
mov eax, 6
sub eax, 02h
move eax, edx
shr edx, 2
```

(3 markah)

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

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

(5 markah)

SOALAN 3 (25 MARKAH)

Kajian Kes 2:

Terdapat dua pendekatan dalam menganalisa malware, iaitu analisa statik dan dinamik. Dalam analisa dinamik, penganalisa malware perlu menyediakan persekitaran yang selamat sebelum mereka boleh menjalankan analisa malware. Sebagai penganalisa malware yang baru di M Secure Sdn. Bhd., Anda telah ditugaskan untuk menganalisa varian baru botnet dalam platform Windows yang menyerang Internet. (Soalan-soalan berikut boleh membantu anda untuk menganalisa botnet baru ini)

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

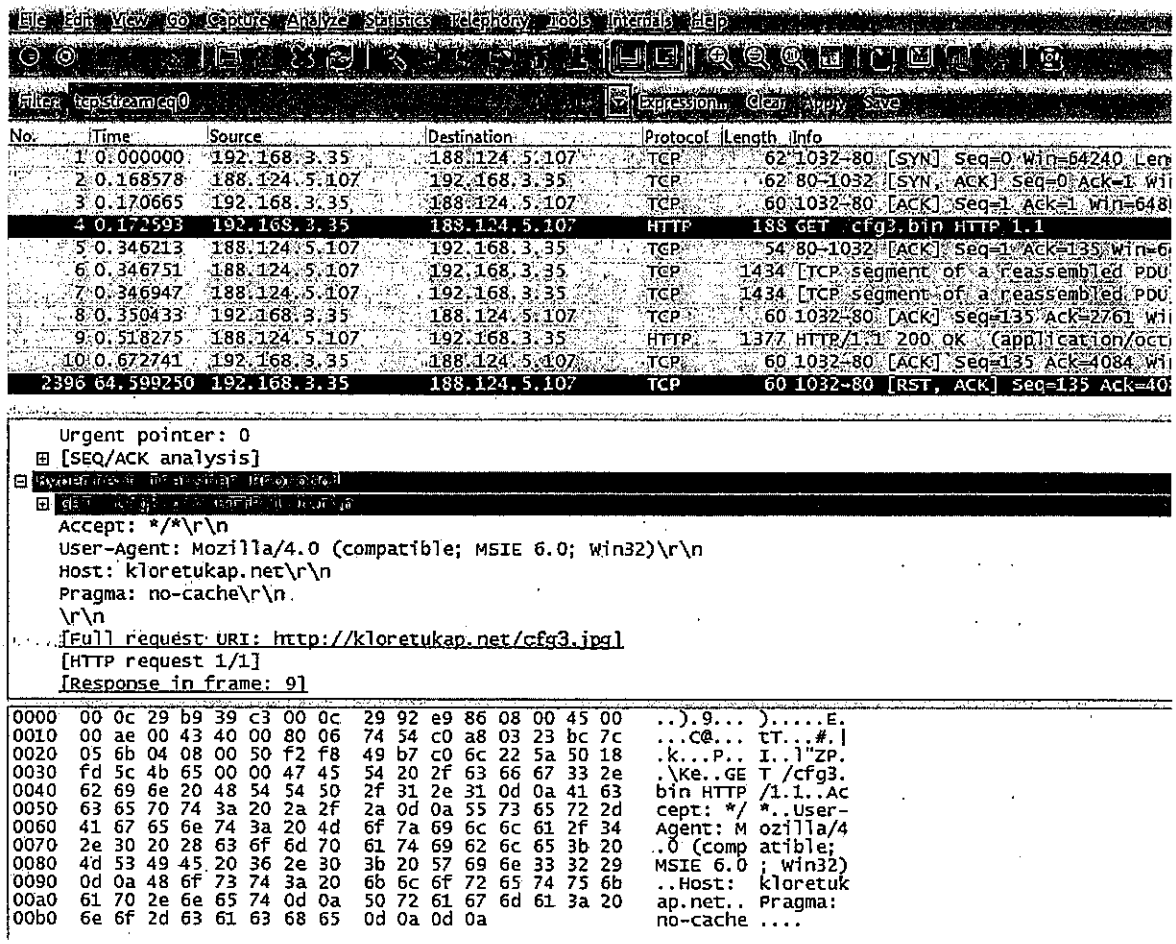
(a) Senaraikan alatan penganalisa perisian yang dikehendaki dalam

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.

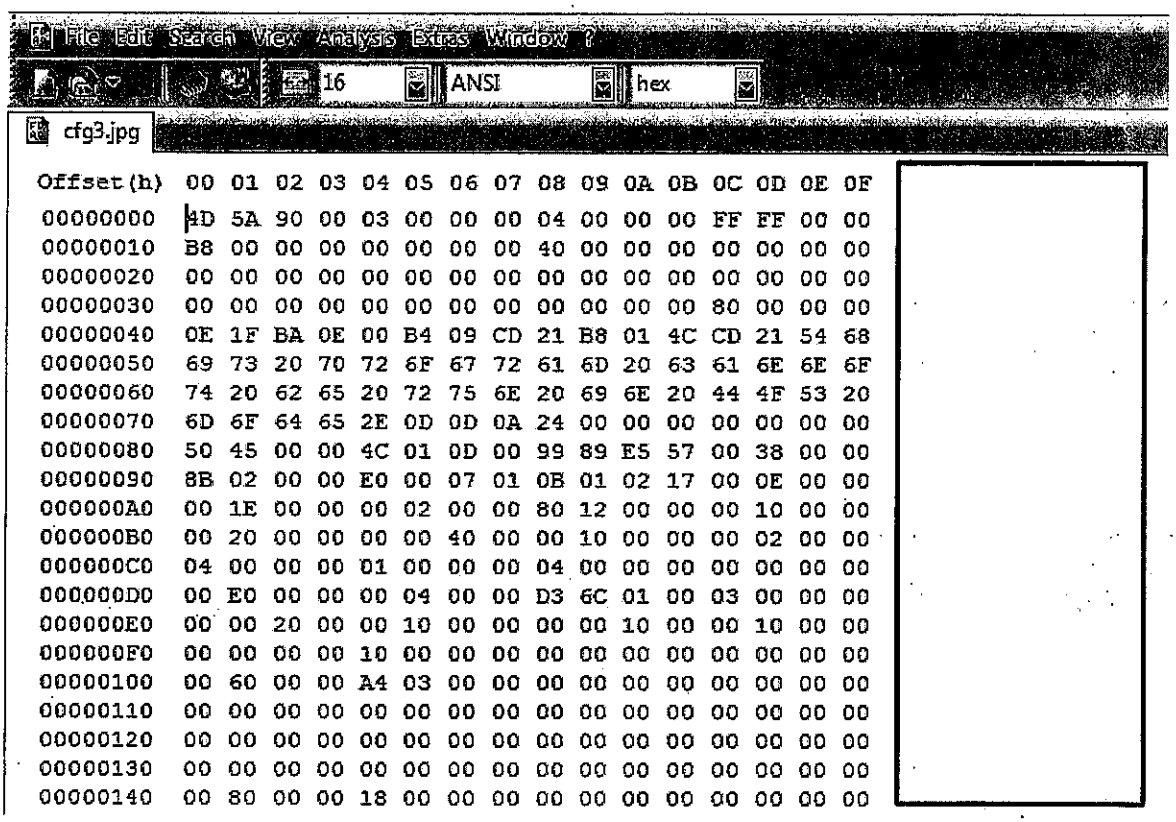
(5 markah)



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)** alat yang diperlukan untuk membuat analisa tersebut?

(5 markah)

-SOALAN TAMAT-

(BITS 3453)

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

(BITS 3453)

APPENDIX B/ LAMPIRAN B

File Signatures Table/ Jadual Signature Fail

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	˙ü	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)

Hex signature	ISO 8859-1	Offset	File extension	Description
EF BB BF	ï»¿	0		UTF-8 encoded Unicode byte order mark, commonly seen in text files.
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