EXAMINATION SOLUTIONS

6G7Z1009 – Introduction to Computer Forensics and Security

Manchester Metropolitan University

SOLUTION Question 1 (Dr. Majdi Owda)

(a) The total size of all the clusters used by the file. **Or** The number of bytes in the logical file plus all slack space from the end of the logical file to the end of the last cluster [2]

(b) Slack space [2]

(c) Two [2]

(d) By means of an MD5 hash of the suspect hard drive compared to an MD5 hash of the data stored in the evidence file [2]

(e) hardware write blockers a hardware kits have write blocking software installed on a controller chip inside a portable physical device. [2]
It is used to make sure the suspect drive being image is not going to be altered, changed [2]

(f) Unicode uses TWO (2) bytes for each character [2], allowing the representation of characters [1] (65,536 or 2 to the power 16 exact number is not needed) [3]

(g) It simply compares the displayed file extension with the file's header/signature. [2]

(h) Thumbs.db, registry files such as netuser.dat, word documents .doc [3] students can list others as well.

(i) Case name, Case Number, Examiner Name, notes, file segment size, password, and compression information.
(3 points out of the previous points) [3]

(j) EnCase marks the deleted file as being overwritten. [2]

Question Total [25]

SOLUTION Question 2

(a) Answer: ?idden12.txt, the first character can't be recovered **[2]**

(b) Answer: Contains the starting cluster address **[2]** FAT file system uses it to find the first data cluster/block for this file in order to load it. **[2]**

(c) Answer: Deleted **[1]** given E5 at the beginning of the entry**[1]**

(d)*Answer:* *bytes 28 to 31* ***[1]*** *80 00 00 00 to little endian 80 > 128 bytes* ***[2]*** *for calculation.****[2]***

(e) ***Answer:*** File Created Time of 14:04:04 **[2]** would display as 82 70 in Hex

- This must be converted into binary as Little Endian
  - Input 70 82 into Base Converter – Little Endian
  - The binary result is 0111000010000010 **[2]**
  - The First 5 Bits are Hours 01110<u>00</u>010000010
  - The Next 6 Bits are Minutes 01110<u>00010</u>00010
  - The Last 5 Bits are Seconds 0111000010<u>00010</u>
    - Seconds are Multiplied by 2 **[2]**

- File Created Date of 31/12/2002 **[2]** in Hex would display as 9F 2D
  - 9F 2D > 2D 9F
    - The binary result is 0010110110011111 **[2]**
    - The First 7 Bits are the Year <u>0010110</u>10011111
      - Add 1980
    - The Next 4 Bits are the Month 0010110<u>1100</u>11111
      - Value of 1-12
    - The Last 5 Bits are the Day 001011011001<u>1111</u>
      - Value of 1-31

      [2]

Total [25]

SOLUTION Question 3 (Dr. Majdi Owda)

(a)
Contiguous allocation performance: better performance than linked allocation since it requires less disk seeks, since the blocks allocated next to each other. In the other hand linked allocation requires more disk seeks since blocks are distributed all over the disk and reading a block requires reading all the past blocks to arrive to it. [2]

Contiguous allocation disk space management which is wasteful of space. Linked allocation better managing of space, since data chunked into smaller pieces. [2]

Contiguous allocation files can't grow if another file started directly the block last block of the first file.
Linked allocation can grow easily. [2]

Contiguous allocation support random access of blocks since we know the start block address and block are contiguous.
Linked allocation does not efficiently support random access since we have to read each previous block in order to arrive to the destination block through reading the links bytes associated between them. [2]

Total [8]

(b)
ASCII (American Standard Code for Information Interchange) ANSI (American National Standards Institute) [2]

27 = 128 different codes [1]

Two general types of codes:
95 are "Printing" codes (displayable on a console)
32 are "Control" codes (control features of the console or communications channel) [2]

Represents
Latin alphabet, Arabic numerals, standard punctuation characters.
Plus small set of accents and other European special characters (Latin-I ASCII) [4] **Total [9]**

(c) Four out of the following, but could talk about others as well,

(i) FileName.LNK
Answer: .LNK files are link files (shortcut files) can provide details about the original file, can prove that the original file has been opened by the user on the machine. [2]

(ii) FileName.SPL
Answer: FileName*.SPL file contains the data to be printed* [2]

(iii) Thumbs.DB
Answer: Thumbs.DB contains a cache of thumbnails of photos and sub folders located in the same folder. [2]

(iv) NTUSER.DAT
This is the user registry file and forensic investigators could view most recently used files [2]

(v) PAGEFILE.SYS
Answer: PAGEFILE.SYS is a swap file that supplements the memory when needed; forensic examiners can recover usernames and passwords etc. from this file since it has traces of volatile memory that show what the operating system was most recently processing [2]

Total [8]

Question Total [25]

Section B: Questions 4 -6

Question 4 (Dr. Liangxiu Han):

4. a)

Answer:
A public key algorithm is asymmetric and uses two keys one of which is made publicly available. (1). The other “private key" is required to decrypt messages encrypted with the corresponding public key in the case of RSA or to generate a shared secret key in the case of Diffie-Hellman. (3)
RSA is used for encryption and for digital signatures. Diffie-Hellman is used for generating shared secret keys (3)

Total [7]

b)

Answer:

Confidentiality - Prevention of unauthorised disclosure of information (prevention of unauthorised reading). Privacy: protection of personal data. Secrecy: protection of data belonging to an organisation. (2)
Integrity - Prevention of unauthorised modification of information (prevention of unauthorised writing). (2)
Availability - Prevention of unauthorised with-holding of information or resources. (2)
Three additional services:
Access control - Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy (2)
Authentication - The process of verifying an identity claimed by or for a system entity. (2)
Non-repudiation service - A security service that provides protection against false denial of involvement in a communication (2)

Suitable examples of implementation of confidentiality, integrity and availability plus three of the above 3 services (6)

Total [18]

Question Total [25]

Question 5 (Dr. Liangxiu Han):

5 (a)

Answer:
The block cipher is a type of symmetric-key encryption:
•Transforms a fixed-length block of plaintext data into a block of ciphertext data of the same length (2)
•The fixed length is called the block size, and for many block ciphers, the block size is 64 bits (1)
•This transformation takes place under the action of a user provided secret key (2)

A typical example is Feistel Cipher Structure (2)

Total [7]

2b).

Answer:
In cryptography, a one-time pad (OTP) is an encryption technique that cannot be cracked if used correctly (1)
In this technique, a plaintext is paired with random, secret key (or pad). Then, each bit or character of the plaintext is encrypted by combining it with the corresponding bit or character from the pad using modular addition. (2)

If the key is truly random, and at least as long as the plaintext, and never reused in whole or in part, and kept completely secret, then the resulting ciphertext will be impossible to decrypt or break. It has also been proven that any cipher with the perfect secrecy property must use keys with effectively the same requirements as OTP keys. However, practical problems have prevented one-time pads from being widely used. (4)

Total [7]

2c)

Answer:

Encryption: JLIMCME
p—15+20=35mod 26=9 –J; r—17+20 = 37 mod 26 = 11-L
o—14+20=34 mod 26 =8 – I; m—12+26=38mod26 =12 –M; i—8+20=28mod26=2—C; s—18+20=38mod26=12—M; e—4+26=30mod26=4 –E

Decryption: lum
F—5-20= -15+26=11mod26=11—l ; O—14-20=-6+26=20mod26=20—u; G-6-20=-14+26=12mod26=12-m

Total [11]

Question Total [25]

Question 6 (Dr. Liangxiu Han):

6. a)
Answer:
Certificate Authority (CA): is trusted authority for certifying individuals and creating an electronic document. (1)
The basic tasks (3 marks in total --each 0.5)
•Key generation
•Digital certificate generation
•Certificate issuance and distribution
•Revocation
•Key backup and recovery system
•Cross certification

Total [4]

b)
Answer:
Digital Signature: ensure the origin and the integrity of a message via hashing.

Digital Certificate: a binding between an entity's public key and one or more attributes relating to its identity (1)

Issues with Digital signature: 1) Trust issue on the real identity of the signer;
2) Forging signatures when attackers intercepts message and private key; 3) Digital signature only ties a message to a person to a private key, not to a person (2)

Total [4]

c)
Answer:
Message authentication is a procedure that allows communicating parties to verify that received messages are authentic. (2)
Message authentication code: A function of the message and a secret key that produces a fixed-length value that serves as the authenticator (2)

Why it is needed:
•protecting the integrity of a message (1)
•validating identity of originator (1)

Total [6]

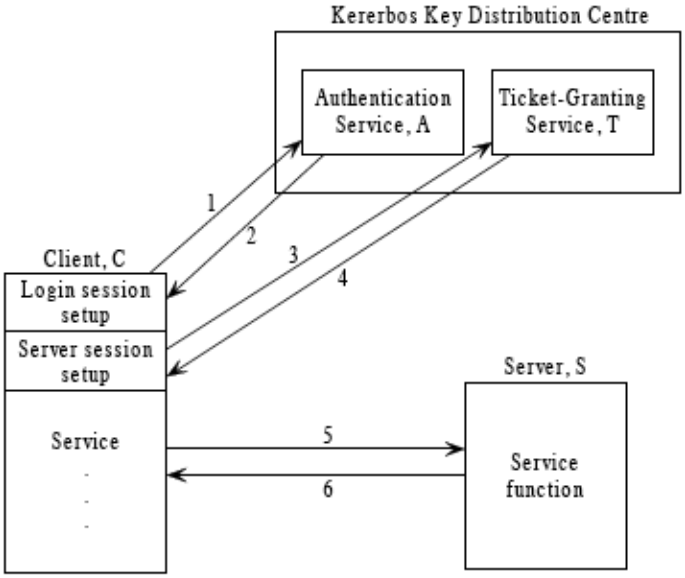
d)

Answer:

Kerberos is cryptographic based network authentication protocol. It uses symmetric cryptography and on-line authentication servers. It provides a centralised authentication server to authenticate users to servers and servers to users in a secure manner. (2)

The working mechanism for Kerberos (3)
1) The kerberos Client to authentication server: the client requests service on host and receives a ticket granting ticket (TGT). All tickets are timestamped;
2) It then contacts the ticket granting service and uses the ticket to prove his/her identity and ask for a service. If the client is eligible for the service, then the TGS sends another ticket to the client
3) The client contacts the service server and uses the ticket to demonstrate he/or she can use services on the server

With a figure explanation (2)



The pros and cons of Kerberos (4)
Pros: 1) User's passwords are never transferred across the network, encrypted or in plain text; 2) Secret keys are only passed across the network Client and Server mutually authenticate; 3) It limits the duration of the users'authentication; 4) Authentications are reusable and durable; (2)
The Cons of Kerberos: 1) Single point of failure: due to centralised model, if the kerberos server is down, no one can log on; 2) Once an attack obtains information from KDC, there is a risk that the attacker can impersonate any user; 3) Time of the hosts involved in the network must be synchronised since tickets has a time availability period. 4)Kerberos does not protect against Trojan horses, virus and worms. (2)

Total [11]

Question Total [25]