EXAMINATION SOLUTIONS

6G7Z1009 – Introduction to Computer Forensics and Security

Question 1 (Dr. Majdi Owda):

(a) ***Answer:***
admissible evidence: evidence allowed to be presented at trial [2]
Search warrant: is issued only if law enforcement provides sufficient proof to the judge that there is probable cause a crime has been committed, which allows the law enforcement officer to search and seize the evidence. The amount and type of material that can be seized differ from country to another.[2]
Hearsay evidence is second-hand evidence not admissible in court. [2]

Total [6]

(b) During the,
1) Identification [1]: make sure you don't damage the evidence while identifying it. [2]

2) Preservation [1]: package the evidence with care and lock it in a safe place [1], acquire a forensic image of the suspect machine/drive [1], and Keep the chain of custody maintained [1] [two points from the above three to take two marks]. [3 marks for this section]

3) Analysis [1]: make sure you are working on the forensic image and keep log file of all actions taken [mentioning one point is enough 1].

4) Documentation [1]: document all evidence found and all actions taken. Evidence should be preserved and documented to such an extent that a third party is able to repeat the same process and arrive at the same result. [1] [one point from the above related to documentation].

5) Presentation [1]: formulate a report with all evidence found with mentioning the report should display continuity, objectivity, and integrity. [1]

Total [11]

(c) (i) ***Answer:*** Case name, Case Number, Examiner Name, notes, file segment size, password, and compression information.
(4 points out of the previous points)

(c) (ii) ***Answer:*** *CRC Cyclic Redundancy Check [1], carry a calculated value based on the block of data, to make sure change in the data will be detected [1]*

(c) (iii) Answer: Message Digest algorithm 5 [1], to maintain the evidence file integrity, any change in the file MD5 will change [1].

Total [6]

Total [25]

SOLUTION Question 2 (Dr. Majdi Owda)

(a) Answer: FAT12 [1], Bytes 54-61 from the DOS boot record. [1]

(b) Answer: 9 sectors [1], bytes 22-23 [1] (09 00) to little endian 00 09 = 9 sectors [1]

(c) Answer: 224 [2], from bytes 17 and 18 [1] > E0 00 little endian 00 E0, converting E0 into decimal 14 * 16 + 0 * 1= 224 [2]
or looking at the size of the root directory of FAT12 contains (14 sectors * 512 each) / (32 bytes directory entry length) = 224. [5]

(d) Answer: passwords.txt [1.5], topsecretdata.doc [1.5], mytarget.jpg [1.5]
Looking at short file names and long file names. [1.5]

(e) Answer: moneyparts [1.5], identified by extracting the name from the long file name entry, and identified as directory by looking at entry file attributes value byte 11 saying it is a directory or by identifying from the basic entry that there is no extension and the size is zero. (One explanation point is enough) [1.5]

(**f) Answer:** ?ypic.jpg [1.5], identified by the directory entry 32 bytes. The first byte is E5 marking it as a deleted file [1.5].

(g) ***Answer:*** *bytes 28 to 31 [1], 00 01 00 00 to little endian 01 00 > 256 bytes[1] [1] for calculation.*

Total [25]

SOLUTION Question 3 (Dr. Majdi Owda)

(a) Answer: FAT12 or FAT16 or FAT32 **[2]**

(b) Answer: Contains the starting cluster address **[2]** FAT file system use 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 0111000010000010
  - The Next 6 Bits are Minutes 0111000010000010
  - The Last 5 Bits are Seconds 0111000010000010
    - 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 0010110110011111
      - Add 1980
    - The Next 4 Bits are the Month 0010110110011111
      - Value of 1-12
    - The Last 5 Bits are the Day 0010110110011111
      - Value of 1-31
        [2]

Total [25]

Section B: Questions 4 -6

Question 4 (Dr. Liangxiu Han):

4a)
Information security: Information Security is defined as as methods and technologies for deterrence (scaring away hackers), protection, detection, response, recovery and extended functionalities (e.g. while information in transmission over networks, storage, hardware, etc.) (2)
Any action that compromises the security of information owned by an organisation . Security attacks include passive and active attacks (2)
Security mechanism: A mechanism designed to detect, prevent, or recover from a security attack: (2)
Security service: Basic security service and additional security services
Confidentiality: Prevention of unauthorised disclosure of information (2)
Integrity: prevention of unauthorised modification of information (To make sure that a message has not been changed while on transfer, storage, etc.). (2)
Availability: Prevention of unauthorised with-holding of information or resources (to make sure that the services are available to users) (2)
Authentication: the process of verifying an identity claimed by or for a system entity (To verify the identity of the user / computer) (2)
Access control: protection of system resources against unauthorised access (To be able to tell who can do what with which resource) (2)
Non-repudiation service: a security service that provides protection against false denial of involvement in a communication (To make sure that a user/server can't deny later having participated in a transaction) (2)
4b)
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)

Question 5 (Dr. Liangxiu Han):

5a) Symmetric cipher:
Symmetric key cipher (also called a secret-key cipher, or a one-key cipher, or a private-key cipher, or a shared-key cipher) is one that uses the same (necessarily secret) key to encrypt messages as it does to decrypt messages.
(2)
Asymmetric cipher:
Also called public-key cryptography, is one that requires two separate keys, one of which is secret (or private) and one of which is public. (2)
5b)
h- (07+18) mod26 = 25 mod 26 →25-Z ; e- (4+18)mod26->22-W; l-(11+18)mod26=3->D; l->D; o-(14+18)mod26->G
Encrypted message: ZWDDG (4)

Decryption: D-(03-15+26)mod26=14->o; E-(04-15+26)mod26=15-p; F-(05-15+26)mod26->16-q; I-(08-15+26)mod26->19-t; N- (13-15+26)->24-y; E->p
Decrypted message: opqtyp
(4)
5c)
In cryptography, a Feistel cipher is a symmetric structure used in the construction of block ciphers, named after the German-born physicist and cryptographer Horst Feistel who did pioneering research while working for IBM. (1)
Partitions input block into two halves (2)

- process through multiple rounds which (2)
- perform a substitution on left data half (2)
- based on round function of right half & sub-key (2)
- then have permutation swapping halves (2)

5d) plaintext – DEFAC T OSTAN D,
encrypted message: DSC AO N F ATE T D

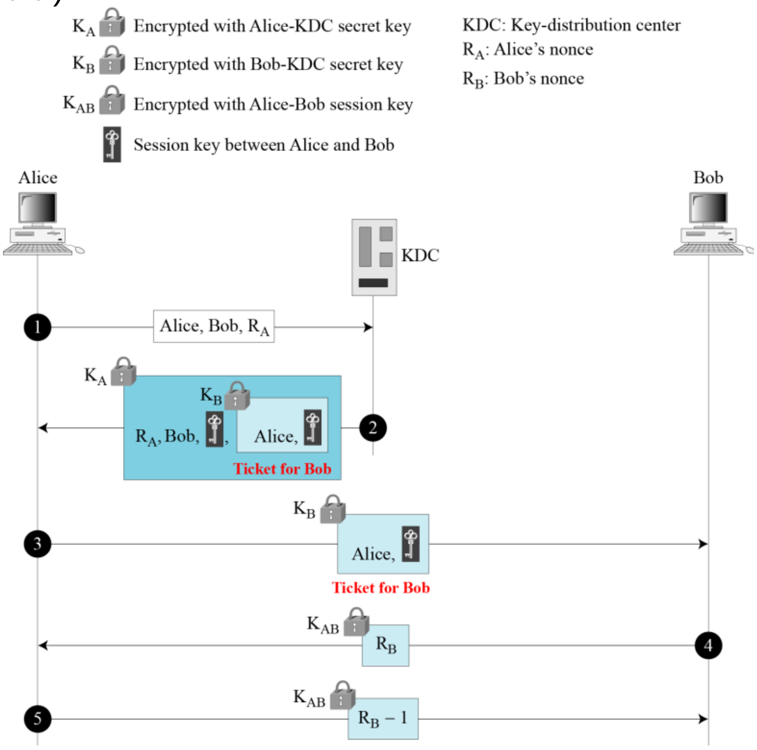
Question 6 (Dr. Liangxiu Han):

6a) Message Authentication Code

6b) In cryptography, a key distribution center (KDC) is part of a cryptosystem intended to reduce the risks inherent in exchanging keys. It consists of databases which hold every user's secret key. It involves users to request from a system to use services. (4)

The ways of key distribution: Flat Multiple KDCs, Hierarchical Multiple KDCs (4)

6 ci)


K_A Encrypted with Alice-KDC secret key
K_B Encrypted with Bob-KDC secret key
K_{AB} Encrypted with Alice-Bob session key
Session key between Alice and Bob
KDC: Key-distribution center
R_A: Alice's nonce
R_B: Bob's nonce
Alice
Bob
KDC
1
Alice, Bob, R_A
K_A
K_B
R_A, Bob,
Alice,
2
Ticket for Bob
K_B
3
Alice,
Ticket for Bob
K_{AB}
R_B
4
K_{AB}
5
$R_B - 1$

(2)

1). Alice sends a message to KDC that includes her nonce RA.
The KDC sends an encrypted message to Alice that includes Alice's nonce, the session key, and an encrypted ticket to B that includes the session key. The ticket is encrypted using Bob's key and the whole message is encrypted using Alice's key.
(2)

2): Alice sends the ticket to Bob. Bob decrypts the ticket and sends his challenge RB to Alice encrypted with the session key.
Alice responds by sending to Bob the encrypted value RB-1 (rather than RB to prevent replay attacks). (2)

3) Alice sends a message to Bob that includes a common nonce R and her challenge RA and a ticket to the KDC containing both R and RA.The ticket is encrypted with Alice's secret key.
Bob creates a similar ticket but with his own nonce RB. Bob sends both tickets to KDC.
(2)

4) The KDC creates a message that contains R, a ticket for Alice with nonce RA and a ticket for Bob with nonce RB. The tickets contain the session key.
The KDC sends the message to Bob.
Bob sends Alice her ticket.
Alice sends a short (hello) message encrypted with the session key to Bob.
(2)

cii) If session key between A and B is compromised and the ticket to B is recorded, an intruder can impersonate A by carrying out last 3 steps.
The weakness can be remedied by adding a timestamp to message 3, so that it becomes: A->B{A, t, KAB {N2 }}KB. B decrypts this message and checks that it is recent. This is the solution adopted in Kerberos