EXAMINATION SOLUTIONS

6G7Z1009 – Introduction to Computer Forensics and Security

SOLUTION Question 1 (Dr. Majdi Owda)

(a)

1 – Identification [1]
Identify electronic devices such as computers, mobiles, and mobile phones. Identification can also include electronic files and emails. [1]
2- Preservation [1]
Preservation of evidence including packaging and transporting the evidence [1] and producing a forensic copy. [1]
3- Analysis [1]
During the analysis stage we will be looking for digital forensic artifacts, in order to determine what evidence can be deduced to reconstruct what has happened. [1]
4- Documentation [1]
A report should be made describing the methodology used and the findings. The report should include all related evidence. [1]
5- Presentation [1]
The investigator might be asked to go to the court as an expert witness to present his or her findings. The investigator would then need to prepare an oral presentation and defend his or her findings. [1]

Total [11]

(b)

FAT1: The first file allocation table [1] responsible for tracking allocated and unallocated blocks/clusters [1]
DOS Boot Record: Contains the mounting/boot code, information (size, file system etc.) and error messages for the disk/volume. [2] Two out of three is enough for full mark.
Root Directory: Reserved area for the directory entries for files and folders created at the root level/top level [2]
Slack space is the bytes not used between the end of the logical file size and the end of the last block allocated to that file. Fore example: A deleted file used to occupy 1 block 512 Bytes and another file replaced that file but only occupied 300 Bytes only. File slack space: 212 bytes from the deleted file. [2]

Total [8]

(c)

MD5 Hash: Message Digest algorithm 5 [1], to maintain the evidence file integrity, any change in the file MD5 will change [1].
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] Question Total [25]

SOLUTION Question 2 (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]

SOLUTION Question 3 (Dr. Majdi Owda)
(a) Answer:
(i) The hard disk size = CHS (cylinders * heads * sectors) * 512
512 * 16 * 63 * 512 = 264241152 Bytes [2]

(ii) According to above which is each block = 2 sectors then minimum
physical size is 1024 Bytes [2]

(iii) The slack space from a file size 912, physical size is 1024 so
1024 – 912 = 112 Bytes slack [2]

Total [6]

(b) ***Answer:***
Answer: NTFS stores file meta data in the Master File Table $MFT [2], resident file/attribute means all attributes are stored in the MFT of the NTFS including the file data, nonresident data located outside the MFT [3]. NTFS uses Unicode – A 16-bit character code representation that is replacing ASCII [2]. $Bitmap which provide a map of the disk shows which blocks are used and which are free. [2]

Total ***[9]***

(c)
(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 [10]

Question Total [25]

Section B: Questions 4 -6

Question 4 (Dr. Liangxiu Han):

4a)
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)

2)
Computational security: which means that the best algorithm for breaking the cryptosystem requires a very large number of operations. e.g.AES. [3]

Provable security: which means that breaking the cryptosystem is at least as hard as solving some other difficult problem. e.g. RSA, Diffie-Hellman. [3]

Unconditional security: where the cryptosystem can never be broken even with infinite computational resources. e.g. One-time pad. [3]

Question 5 (Dr. Liangxiu Han):

5a) block cipher and stream cipher

Block ciphers [5]

- 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
- This transformation takes place under the action of a user provided secret key
- Decryption is performed by applying the reverse transformation to the ciphertext block using the same secret key
- The fixed length is called the block size, and for many block ciphers, the block size is 64 bits

Stream cipher [5]

- A stream cipher generates what is called a keystream (a sequence of bits used as a key)
- Encryption is accomplished by combining the keystream with the plaintext, usually with the bitwise XOR operation
- The generation of the keystream can be independent of the plaintext and ciphertext, yielding what is termed as synchronous
- Or it can depend on the data and its encryption, in which case the stream cipher is said to be self-synchronising.
- Most stream cipher designs are for synchronous stream ciphers.

5b)

If A can decrypt a message that has been encrypted with B's private key using B's public key it could be assumed that this authenticates B to A. This is only the case if the public key that A possess and believes is B's public key is in fact B's public key. This means that a secure means of distributing and binding identities to public keys is required and ultimately means that A has to trust some 'authority' to provide B's public key. [4]

5c)
i) 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. [3]

s- (18+10) mod26 = 28 mod 26 →2 - C ; e- (4+10)mod26->14-O; c-(2+10)mod26=20->U; u->(20+10) mod 26->4->E; r-(17+10)mod26->1->B; e-(4+10)mod26->14- O
Encrypted message: COUEBO [4]

Decryption: W-(22-10+26)mod26=12->m; A-(00-10+26)mod26=16->q; N-(13-10+26)mod26-> 3->d; T-(19-10+26)mod26->9->j;
Decrypted message: mqdj

[4]

Question 6 (Dr. Liangxiu Han):

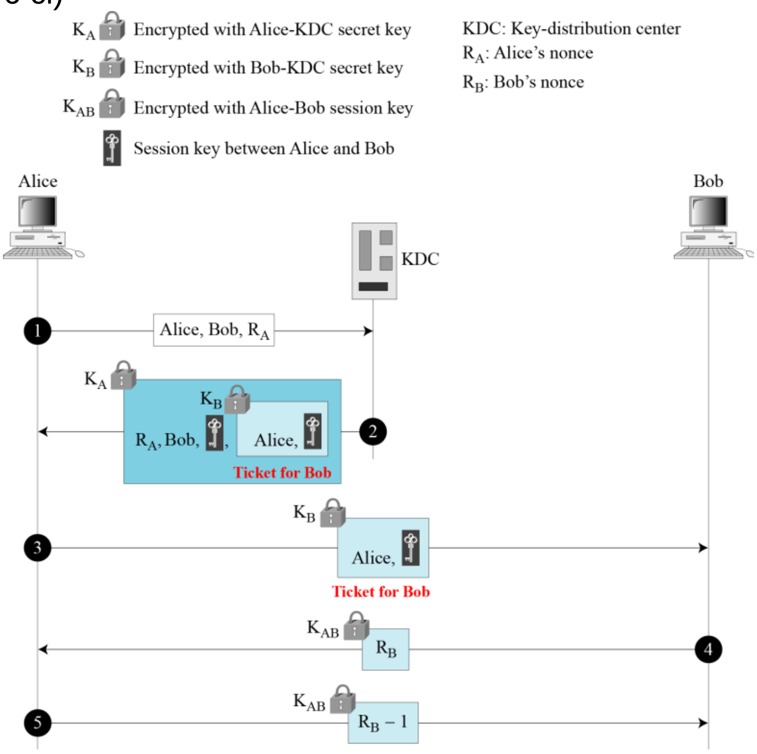
6a) Message Authentication Code [2]

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

[5]