EXAMINATION SOLUTIONS

6G7Z1009 – Introduction to Computer Forensics and Security

Manchester Metropolitan University

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)

Raw format and EnCase .E0 or EnCase .Ex01 [2] MD5 and SHA-1 [2]

Total [4]

(c)

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] **Total [4]**

(d)

speed up the report creation as using the forensics tools reports are going to be created while the examiner is analysing the case [2] technical information such as file times and dates could be exported easily using forensic tools [2]

Total [6]

Question Total [25]

SOLUTION Question 2

In FAT file system; answer the following questions:

a.
File system type, volume label, serial, boot code, error messages, signature, etc [3]

b.
FAT 1 (File Allocation table) [1] is created by the file system during format and contains pointers to clusters located on a drive; its role is tracking allocated and unallocated clusters [1].

c. two [2]

d. 32 bytes [2]

e.
1- file name
2-Date/Time
3- File extension
4-starting cluster [4]

f.
1- a directory entry for the file is created,
2- the FAT assigns the necessary clusters to the file
3-the file's data is filled in to the assigned clusters. [6]

g.
the logical size is the file's actual number of bytes that the file contains [2]
the phyical size is the size in clusters used by the file i.e. logical size and bytes left to the end of the last cluster used by the file. [2]
slack space [2]

Total [25]

SOLUTION Question 3 (Dr. Majdi Owda)
(a)
(i) Contiguous allocation: 5 blocks[1], 2560/512 = five contiguous blocks [2]
(ii) Linked allocation: 6 blocks [1], 6 linked blocks since 2560/508 = 5.03 blocks [2]
(iii) Indexed allocation: 6 [2], 1 block for the index block and 5 for data blocks 2560/512 = 5 [2].

Total [10]

(b)
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]

Total [6]

Question Total [25]

Section B: Questions 4 -6

Question 4 (Dr. Liangxiu Han):

4a) Answer (20):

1) Deterrence: need to create and implement policies that allow the generation of a feasible and believable deterrence [4]

2) Detection: need to create and implement policies and procedures that allow the detection of how, when and where intrusion has taken place [4]

3) Protection: need to create and implement policies and procedures that allow the management of people and the IS in an effective manner so as to protect against unauthorised usage[4]

4)Reaction: [4]
need to create and implement policies and procedures which define how to react to an intrusion
need to ensure that penetration does not happen again
need to ensure that vulnerabilities are eliminated

Recovery: need to create and implement policies and procedures to recover all data and programs after a breach in security [4]

4b) [5]
Security attack: Any action that compromises the security of information owned by an organisation [1]

Type of attacks: [4]
Passive attack: a passive attack attempts to learn or make use of information from the system but does not affect system resources.
Active attack: an active attack attempts to alter system resources or affect their operation.

Question 5 (Dr. Liangxiu Han):

5a) [9]
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]

5b) [16]
Encryption: welcomtru, K=16
W (22) e (04) l (11) c (02) o(14) m(12) e(04)
W = (22+16) mod 26=12 ->m
E=(4+16) mod 26=20->u
l=(11+16) mod 26=1->b
c=(2+16) mod 26=18->s
o=(14+16) mod 26=4->e
m=(12+16) mod 26=2->c
t=(19+16)mod26=9->J
r=(17+16)mod26=7->H
u=(20+16)mod26=10->k

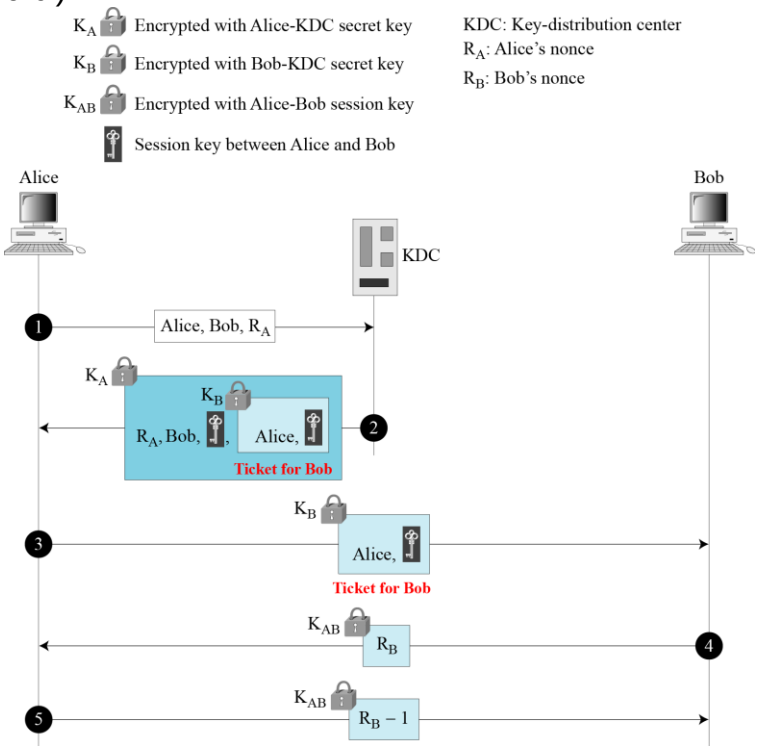
Decryption: XYZANBJ, k=16
X (23) = (23-16+26)mod 26 = 7-> H
Y (24)=(24-16+26) mod 26 = 8->I
Z(25)=(25-16+26)mod 26 = 9 ->J
A(00)=(00-16+26)mod 26 = 10->k
N(13)=(13-16+26)mod 26 = 23 ->X
B(01)=(1-16+26) mod 26 = 11-> L
J(09)=(9-16+26)mod 26=19 -> T

Question 6 (Dr. Liangxiu Han):

6a)
Zero-knowledge proof system only does authentication. It allows you to prove that you know a secret (something associated with your public key) without actually revealing the secret. A zero-knowledge proof is a proof of some statement which reveals nothing other than the truth of the statement.[4]

For example, RSA is a Zero-knowledge proof system. In the RSA algorithm, you can prove you know the secret associate with your public key without revealing your private key [6]

6 bi)



[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]