VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur-603203

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Academic Year: 2016-17

QUESTION BANK - ODD SEMESTER

NAME OF THE SUBJECT	CYBER FORENSICS
SUBJECT CODE	CS 6004
SEMESTER	VII
YEAR	IV
DEPARTMENT	COMPUTER SCIENCE AND ENGINEERING
HANDLED & PREPARED BY	Mr. S.VENKATESH,AP(OG) Dr A.SAMYDURAI,ASSOC. PROF

UNIT -I

PART-A

Q.No	Question	Competence	Level
1	Distinguish between HMAC and MAC.	Understand	BTL2
2	List out the basic components of the IPsec architecture	Remember	BTL1
3	Identify Security Associations with the help of three parameters.	Remember	BTL1
4	Give some basic differences between encryption and decryption.	Understand	BTL 2
5	What do you know about Key Management for IPsec?	Remember	BTL 1
6	Classify Payload into different types.	Analyze	BTL 4
7	Differentiate between SSL Protocol and TSL protocol.	Understand	BTL 2
8	Design ISKMP in terms of its header format.	Create	BTL 6
9	Asses alternative operation of HMAC computation using MD5/SHA-1.	Evaluate	BTL 5
10	List the fields in AH Format . .	Remember	BTL 1

11	List the elements involved in the session states.	Analyze	BTL 4
12	Analyze the differences between SSL and IPsec.	Analyze	BTL4
13	Classify using some specifications of SSL related Alerts which are always fatal to be used.	Apply	BTL 3
14	Show how the TLS supports all of the error alerts defined in SSLv3..	Apply	BTL 3
15	State Compression and Decompression using SSL Reco Protocol.	Remember	BTL 1
16	Define a Pseudo-Random Function	Remember	BTL 1
17	Differentiate between SSL v3 and TLSMAC Schemes.	Understand	BTL 2
18	Decide when and under which circumstances “FINISHED MESSAGE” used?	Evaluate	BTL5
19	Show in points the three services for SSL connections between Server and Client.	Apply	BTL3
20	Develop the two ways for exchange of the premaster Secret .	Create	BTL6

PART-B

Q.No	Question	Competence	Level
1	(i) Explain in detail about IPSec Protocol Documents. (6) (ii) Explain in detail about HMAC with its Structure and suitable example. (10)	Analyze	BTL 4
2	Illustrate briefly about the computation of HMAC using the following methods:- (i) HMAC-MD5 computation using the RFC method. (8) (ii) HMAC-SHA 1 computation using Alternative method. (8)	Apply	BTL 3
3	Analyze how is the Security Association used in the following parameters:- (i) Security Policy Database (4) (ii) Security Association Database (4) (iii) Transport Mode SA (4) (iv) Tunnel Mode SA (4)	Analyze	BTL 4
4	Illustrate about:- (i) IPAuthentication Header (6) (ii) AH Format (6) (iii) AH Location (4)	Apply	BTL 3
5	Give a brief account of IP ESP with some suitable diagrams. (16)	Understand	BTL 2
6	Describe in detail about :- (i) Session and Connection State. (8) (ii) SSL Record Protocol. (8)	Remember	BTL 1
7	(i) Explain the SSL Change Cipher Spec Protocol. (8) (ii) Explain the SSL Alert Protocol. (8)	Analyze	BTL4
8	Explain in detail about SSL Handshaking Protocol between a Server and Client Connection with an appropriate diagram. (16)	Understand	BTL2
9	Examine the Cryptographic Computations while using the following scenario:- (i) Computing the Master Secret (10) (ii) Converting the Master Secret into Cryptographic Parameters (6)	Remember	BTL 1
10	Discuss about Key Management Protocol for IPSec. (16)	Understand	BTL 2
11	Describe TLS Protocol with suitable example. (16)	Remember	BTL 1

12	Examine a key Generation using Pseudo Random Function to expand secrets into blocks of data in TLS with a suitable example. (16)	Remember	BTL 1
13	Compose a short note on:- (i) Error Alerts (8) (ii) Certificate Verify Message (4) (iii) Finished Message (4)	Create	BTL 6
14	Design a Pseudo Random Function (PRF) generation scheme using the parameters :- Seed=Ox 80 af 12 5c 7e 36 f3 21 Label=rocky mountains= 0x 72 6f 63 6b 79 20 6d 6f 75 6e 74 61 69 6e 73 Secret=0x 35 79 af 12 c4 (i) Deduce Data Expansion by P_MD5 (8) (ii) Deduce Data Expansion by P_SHA-1 (8)	Evaluate	BTL 5

UNIT -II
PART-A

Q.No	Question	Competence	Level
1	Pointout the Digital Signature Service Provided by PGP.	Analyze	BTL 4
2	Differentiate between PGP and S/MIME.	Understand	BTL 2
3	List the algorithms used in PGP 5.X .	Understand	BTL 2
4	What do you mean by 'Inside Signature' in S/MIME ?	Remember	BTL 1
5	How will you assess 'Digital Envelope' in S/MIME ?	Evaluate	BTL 5
6	Generalize the types of 'Bastion Host' in Internet Firewall .	Create	BTL 6
7	Classify different types of firewalls available in Forensics.	Apply	BTL 3
8	Define Virtual Private Network (VPN).	Remember	BTL 1
9	Classify various types of Proxies.	Understand	BTL 2
10	Tabulate any example of SMTP Packet rule sets.	Remember	BTL 1
11	Define Logging.	Remember	BTL 1
12	Discriminate between circuit-level gateway and application-level gateway.	Evaluate	BTL5

13	Contrast choke point and audit log .	Analyze	BTL4
14	Formulate the important features of Firewalls.	Create	BTL 6
15	Demonstrate FTP Packet Filtering with an example.	Apply	BTL 3
16	Define SET for E-Commerce Transactions.	Understand	BTL 2
17	List the cryptographic principles used in SET.	Apply	BTL 3
18	Define Dual signature.	Remember	BTL 1
19	List some of the processes in merchant registration.	Remember	BTL 1
20	Pointout the business requirements for SET.	Analyze	BTL 4

PART-B

Q.No	Question	Competence	Level
1	Explain in detail the basic concepts of (i) Confidentiality via. Encryption (8) (ii) Authentication via. Digital Signature. (8)	Analyze	BTL 4
2	Formulate the idea behind using the following terms: (i) Compression (4) (ii) Radix-64 Conversion with an example. (12)	Create	BTL 6
3	Explain in detail about :- (i) Packet Header (8) (ii) Packet Structure (8) with suitable examples.	Analyze	BTL 4
4	Illustrate briefly about the Electronic mail security mechanisms: a) Enhanced Security Services for S/MIME b) MIME	Apply	BTL 3
5	Explain in detail about :- (i) Role of Firewalls. (4) (ii) Firewall Related Terminology (12)	Understand	BTL 2
6	Briefly explain the types of Firewalls with a neat diagram and examples (16)	Remember	BTL 1
7	Write a short note on (i) Firewall Designs (10) (ii) Examining the Packet Filtering gateway and Application Level Gateway dissimilarities. (6)	Analyze	BTL 4

8	Explain briefly about the following security mechanisms:- (i) Logging and Alarms , VPN (4) (ii) DMZ and Choke Point (4) (iii) Key material Packets in PGP (8)	Evaluate	BTL 5
9	Explain in detail about S/MIME and the general syntax it uses to support different content types. (16)	Remember	BTL 1
10	Explain in detail about :- (i) Single-Homed Bastion Host (5) (ii) Dual Homed Bastion Host (6) (iii) Screened Subnet Firewall (5)	Understand	BTL 2
11	Describe the transaction protocols required for secure Payment Processing in SET (16)	Understand	BTL2
12	(i) Describe Cryptographic principles incorporated in SET. (8) (ii) Examine Dual Signature and Signature Verification . (8)	Remember	BTL 1
13	Describe the following E-Commerce Transactions :- (i) Business Requirements for SET (8) (ii) Authentication and Message Integrity (8)	Remember	BTL 1
14	Demonstrate the SET system Participants with a diagram (16)	Apply	BTL 3

UNIT -III
PART-A

Q.No	Question	Competence	Level
1	Define Traditional Computer Crime.	Remember	BTL 1
2	What is meant by Identity theft?	Remember	BTL 1
3	What is 'Identity Fraud'?	Understand	BTL 2
4	Pointout which CF Techniques are being used for Investigations.	Analyze	BTL 4
5	Show what preparations are required for Incident Response Methodology?	Apply	BTL 3
6	Show the steps in Incident Response Methodology?	Apply	BTL 3
7	List some of the scopes of Foreign Investigations.	Understand	BTL 2
8	How will you specify the rules for computer Forensics in investigation ?	Understand	BTL 2

9	Classify different types of Computer Forensics Technology?	Apply	BTL 3
10	What are the types of Computer Foresics Systems?	Analyze	BTL 4
11	Decide the Criminal and civil proceedings which can be used as computer Forensics Evidence .	Evaluate	BTL 5
12	Define the term ' HACKING'	Remember	BTL 1
13	How will you find out the Hidden Data in Forensics Technology ?	Analyze	BTL 4
14	What are the hierarchy involved in internet security forensic system?	Remember	BTL 1
15	How can the Hackers gain advantage in stealing essentials of investigation in forensics?	Create	BTL 6
16	Express about why the evidence media be write Protected.	Understand	BTL 2
17	List the three items should be on an evidence custody form.	Remember	BTL 1
18	How will you plan the most critical aspects of computer Evidence?	Create	BTL 6
19	Define RAID Data Acquisition.	Remember	BTL 1
20	Assess the disadvantages of using the WINDOWS XP/VISTA USB write-protection Registry Method?	Evaluate	BTL 5

PART-B

Q.No	Question	Competence	Level
1.	Examine the traditional Computer crimes associated with Cyber Forensics. (16)	Analyze	BTL 4
2	Explain in detail about Identity Theft and Identity Fraud and mention the points of differences between them. (16)	Analyze	BTL 4
3	Explain in detail about Incident Response Methodology and the six steps associated with it (16)	Evaluate	BTL 5
4	Analyze briefly about the Forensic Duplication and Investigation (16)	Analyze	BTL 4
5	Examine in detail the roles of the following in detail:- (i) Forensics Technology (8) (ii) Forensics Systems (8)	Apply	BTL 3

6	Discuss in detail about the following:- (i) Systematic Approach in Computer Investigations. (10) (ii) Conducting an Investigation in Computer Investigations. (6)	Understand	BTL 2
7	Describe in detail about the following :- (i)Understanding Data Recovery Workstations and software (8) (ii) Preparing for a Computer Investigation. (8)	Understand	BTL 2
8	Examine the following terms in detail:- (i) Understanding Storage Formats for Digital Evidence (8) (ii) Using Acquisition Tools. (8)	Remember	BTL 1
9	Describe in detail about the following terms in detail:- (i) Validating Data Acquisition (8) (ii) Performing RAID Data Acquisitions (8)	Remember	BTL 1
10	Demonstrate how to use Remote Network Acquisition Tools in cyber Forensics. (16)	Apply	BTL 3
11	Examine the following cases in Cyber Forensics:- (i) Completing the case (6) (ii) Critiquing the case (2) (iii) Analysing the Digital Evidence. (8)	Remember	BTL 1
12	Describe the following Procedures for Corporate high tech investigation : (i) E-mail abuse Investigation (4) (ii) Media Leak Investigation (4) (iii) Industrial Espionage Investigation (4) (iv) Interviews and Interrogations in high-tech investigation. (4)	Remember	BTL 1
13	Discuss the investigation of Employee termination case , internet abuse investigation ,Attorney Client Privilege investigation in corporate high tech investigation.	Understand	BTL 2
14	Formulate a plan to determine the following points:- (i) The best acquisition method. (6) (ii) Contigency planning for image Acquisition. (4) (iii) Using other Forensics Acquisition Tools in Data. (6)	Create	BTL 6

UNIT -IV
PART-A

Q.No	Question	Competence	Level
1	Define the term “Digital Evidence”.	Remember	BTL 1
2	List the general tasks investigators perform while working with Digital Evidence.	Remember	BTL 1
3	Pointout the three types of field kit to be used in a crime scene.	Apply	BTL 4
4	List the set of feature applicable to computer forensics practice.	Remember	BTL 1
5	Assess what materials you would collect to complete your analysis and processing of a scene?	Evaluate	BTL 5
6	Define the tasks of using a Technical advisor for forensic purposes.	Remember	BTL 1
7	How will you identify the use case requirements for forensic purposes?	Apply	BTL 4
8	List some of the general tasks you perform in any computer Forensics.	Remember	BTL 1
9	Define Hashing algorithms commonly used for forensic purposes.	Remember	BTL 1
10	Differentiate between Master Boot Record(MBR) and Master File Table(MFT).	Understand	BTL 2
11	How will you create “New Technology File System”?	Create	BTL 6
12	Show the five major categories refining data analysis and recovery functions in computer forensic tools.	Apply	BTL 3
13	Give the meaning of the term “Virtual Cluster Number”.	Evaluate	BTL 5
14	Express the meaning of the term “Zoned Bit Recording(ZBR)”.	Understand	BTL 2
15	Distinguish between Trusted Computing Group and Trusted Platform Module.	Understand	BTL 2
16	Classify Hardware Forensic Tools with Software Forensic Tools.	Apply	BTL 3
17	Show how the reconstruction tool is useful in forensics?	Apply	BTL 3
18	Pointout the tools used in validation and discrimination in Forensics.	Analyze	BTL 4
19	Express the term ‘Computer Forensics Tool Testing’?	Understand	BTL 2
20	How will you generalize the utility of National Software Reference Library ?	Create	BTL 6

PART-B

Q.No	Question	Competence	Level
1	Illustrate how will the processing of an incident or a crime scene takes place in cyber forensics. (16)	Apply	BTL 3
2	Explain in detail about about how the understanding of File Systems plays a crucial role in cyber forensics. (16)	Analyze	BTL 4
3	Explain in detail about the following :- (i) Computer Forensics Software Tools (8) (ii) Computer Forensics Hardware Tools (8)	Evaluate	BTL 5
4	Explain in detail about the following terms:- (i) Disk Partitions (8) (ii) Master Boot Record (2) (iii) Examining FAT disks (6)	Analyze	BTL 4
5	Describe the following terms in detail:- (i) Examining NTFS Disks (6) (ii) NTFS System Files (6) (iii) NTFS Compressed Files (4)	Remember	BTL 1
6	Discuss in detail about the following terms with suitable examples:- (i) NTFS Data Streams (4) (ii) NTFS Compressed Files (4) (iii) EFS Recovery Key Agent (4) (iv) Deleting NTFS Files (4)	Understand	BTL 2
7	Describe about how the whole disk encryption is performed in Cyber forensics (16)	Remember	BTL 1
8	Formulate the idea behind using the following tools in forensics :- (i) Exploring Windows Registry (8) (ii) Examining the Windows Registry (8)	Create	BTL 6
9	Examine the MS-DOS Startup Tasks and about other Disk Operating Systems in Detail. (16)	Understand	BTL 2
10	Describe about the following mechanisms: (i) Understanding File Systems (6) (ii) Whole Disk Encryption (10)	Remember	BTL 1

11	Examine the following points used for preparation of search: (i) Identifying the nature of case (4) (ii) Identifying the type of computing system (4) (iii) Determining whether computer can be seized (4) (iv) Obtaining a detailed description of Location (4)	Remember	BTL-1
12	Discuss briefly about : (i) Determining the tools that are needed for Forensics (8) (ii) Storing a digital evidence (8)	Understand	BTL-2
13	Demonstrate the following :- (i) How will you obtain a Digital Hash ? (12) (ii) Conducting the investigation: Acquiring Evidence withAccessData FTK (4)	Apply	BTL-3
14	Analyze how the following techniques are used : (i) Processing Data Centers with RAID systems (8) (ii) Documenting Evidence in the Lab (4) (iii) Processing and Handling Digital Evidence (4)	Analyze	BTL-4

UNIT -V

PART-A

Q.No	Question	Competence	Level
1	Define how data discrimination is done by using Hash Values.	Remember	BTL 1
2	Give some legal and illegal purposes for using Steganography?	Understand	BTL 2
3	Pointout whether password recovery is included in all the Computer Forensic Tools is used or not.Why ?	Analyze	BTL 4
4	Show the guidelines for identifying stegnography files.	Apply	BTL 3
5	List the following general procedures used for most Computer Forensics Investigations.	Remember	BTL 1
6	Express the most critical aspects of Computer Forensics.	Understand	BTL 1
7	Classify the Compression techniques used in Computer Forensics..	Apply	BTL 3
8	Define Bit Shifting with an example.	Understand	BTL 1
9	Pointout the Shareware Programs for Remote Acquisitions.	Analyze	BTL 4
10	Define Network Forensics.	Remember	BTL 1
11	How will you generalize the three modes of Protection used ?	Create	BTL 6
12	Define any three standard procedures used in Network Forensics.	Remember	BTL 1

A

13	Examine whether all the e-mail headers contain the same type of information.	Apply	BTL 3
14	Decide the roles of Client and Servers in E-mail investigations.	Evaluate	BTL 5
15	Mention the e-mail storage format available in Novell Evolution.	Understand	BTL 2
16	How can the Router logs be used to verify the types of E-mail data?	Analyze	BTL 4
17	Decide whether you need a search warrant to retrieve information from a system server.	Evaluate	BTL 5
18	Mention the four places where mobile device information might be used.	Understand	BTL 2
19	What are the SIMCon's features ?	Understand	BTL 2
20	How will you isolate a mobile device from incoming signals ?	Create	BTL 6

PART-B

Q.No	Question	Competence	Level
1	Discuss how will you validate the forensic data using: (i) Validating the hexadecimal Editors (8) (ii) Validating with Computer Forensics Programs (8)	Understand	BTL 2
2	Examine in detail the techniques used for Addressing Data Hiding. (16)	Remember	BTL 1
3	Describe Remote Acquisitions when used with (i) Runtime Software (8) (ii) Preparing DiskExplorer and HDHOST (4) (iii) Remote Connection with DiskExplorer (4)	Remember	BTL 1
4	Explain the following terms in detail:- (i) Securing a Network (8) (ii) Performing Live Acquisitions (8)	Evaluate	BTL 4
5	Briefly generalize the roles of the following term in investigations:- (i) E-mail in investigations (4) (ii) E-mail in Client and Server (4)	Evaluate	BTL 6
6	Explain briefly about the following terms in detail:- (i) Examining E-mail Messages (2) (ii) Copying an E-mail Message (8) (iii) Viewing an E-mail Headers (6)	Analyze	BTL 4

7	Describe the following terms in detail :- (i) Examining Additional Files (4) (ii) Tracing an E-mail Message (4) (iii) Using Network E-mail Logs (4) (iv) Examining E-mail Headers (4)		Understand	BTL 2
8	Describe in detail about using specialized E-mail Forensics Tools	(16)	Remember	BTL 1
9	Describe in detail about Understanding E-mail Servers	(16)	Remember	BTL 1
10	Assess how mobile devices play a crucial role in forensics by : (i) Basics of mobile Forensics (8) (ii) Inside Mobile Devices (4) (iii) Inside PDAs (4)		Evaluate	BTL-5
11	How will examine the following e-mail server logs: (i) UNIX E-mail server Logs (8) (ii) Microsoft E-mail Server Logs (8)		Apply	BTL-3
12	Examine the following techniques used in Forensics : (i) Steganography to hide Data (4) (ii) Examining Encrypted Files (4) (iii) Recovering Passwords (4) (iv) AccessData Tools with Passworded and Encrypted Files (4)		Apply	BTL-3
13	Give a brief description of the following data-hiding techniques: (i) Hiding Partitions (8) (ii) Bit-Shifting (6) (iii) Marking Bad Clusters (2)		Understand	BTL-2
14	Explain in detail about validating and testing Forensics Software	(16)	Analyze	BTL-4

SUBJECT INCHARGE **HOD/CSE**