Draft Scheme of Valuation/Answer Key

(Scheme of evaluation (marks in brackets) and answers of problems/key)

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

THIRD SEMESTER M.C.A. DEGREE EXAMINATION, DECEMBER 2022

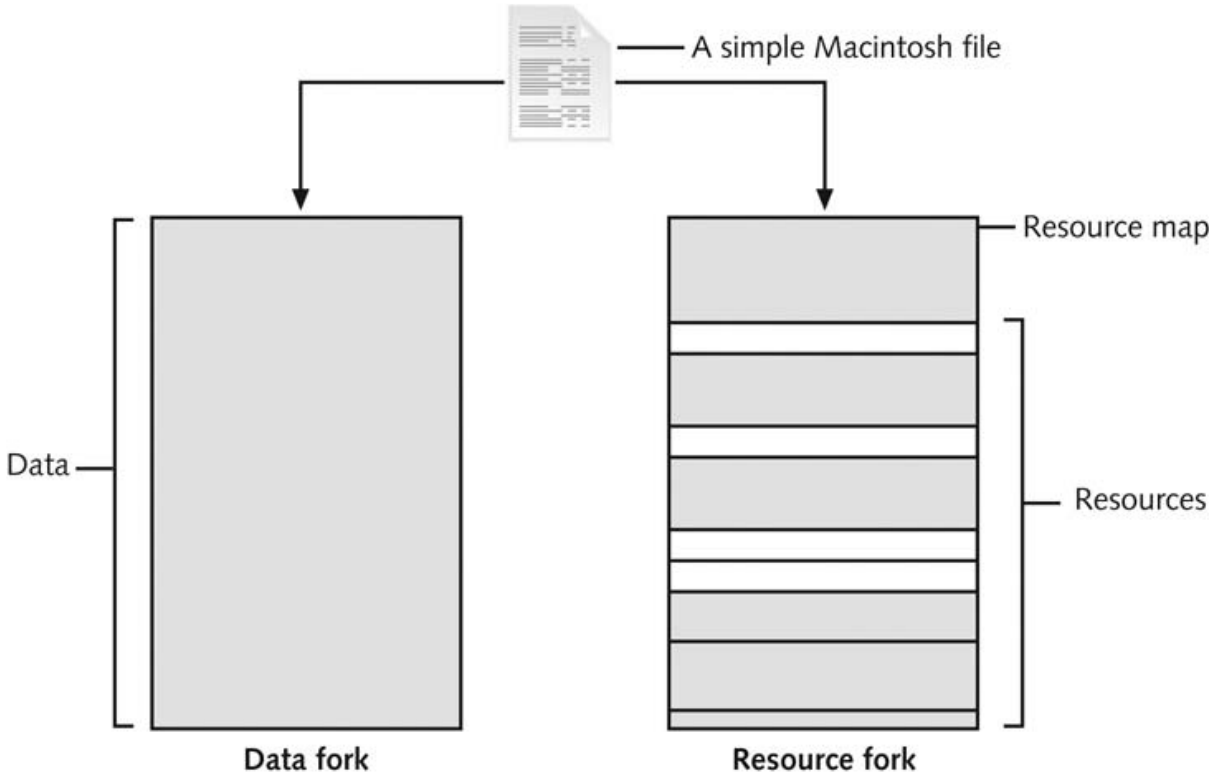
Course Code: 20MCA267

Course Name: CYBER FORENSICS

Max. Marks: 60		Duration: 3 Hours

PART A

		Answer all questions, each carries3 marks.	Marks
1		Corporate /private sector computer crimes can involve e-mail harassment, falsification of data, gender and age discrimination, embezzlement, sabotage, and industrial espionage. Any three with explanation - one mark each	(3)
2		Raw, Proprietary and AFF one mark each	(3)
3		Wear -levelling- if deleted data is not immediately, it might lost for ever. In solid state drive memory cells shifts data at physical level so as to acquire a uniform wearing. Also when the data is rotated to another memory cell, the old addresses are listed in the firmware file called garbage collector which will erase the data at some point overwriting the cells in the garbage collector file. Hence making a full forensic copy is necessary in the case of a solid state drive.	(3)
4		When a user empties the Recycle Bin.) The OS performs the following tasks: 1. The associated clusters are designated as free—that is, marked as available for new data. 2. The $Bitmap file attribute in the MFT is updated to reflect the file's deletion, showingthat this space is available. 3. The file's record in the MFT is marked as being available. 4. VCN/LCN cluster locations linked to deleted nonresident files are then removed from the original MFT record. 5. A run list is maintained in the MFT of all cluster locations on the disk for nonresident files. When the list of links is deleted, any reference to the links is lost. 0.5 marks each. 0.5 marks for when delete file move to recycle bin.	(3)
5		In older Mac OSs, a file consists of two parts: a data fork, where data is stored, and a resource fork, where file metadata and application information are stored Both forks contain the following essential information for each file: • Resource map • Resource header information for each file	(3)

		• Window locations • Icons fig 1 mark, explanation 1 mark each  	
6		Hard Links & Symbolic Links example comands usage 1 mark (ln and ln -s) explantion 1 mark each A hard link is a pointer that allows accessing the same file by different file names. The file name refer to the same inode and physical location of the on a drive. All files pointing to the same inode need to be on the same physical drive. (Eg. People with different logins can access the same physical file and change it. Need to reflect the change to others) Use ln command to create a hard link. Asymbolic link/ Softlink/Simlinks are pointers t their files . Not included in link count. Can point to items on other disk/network. Simlinks have a inode of its own. Existence as long as the destination file exists. Identify using a name and path ,Use ln –s command	(3)
7		investigating mobile devices is one of the most challenging tasks in digital forensics. 1. No single standard exists for how and where cell phones store messages, although many phones use similar storage schemes 2. new phones come out about every six months, and they're rarely compatible with previous mode , Biggest challenge is dealing with constantly changing phone models 3. Due to the growing problem of mobile devices being stolen, service providers have started using **remote wiping t**o remove a user's personal information stored on a stolen device 4. All mobile devices have volatile memory, Making sure they don't lose power before you can retrieve RAM data is critical	(3)

		5. Isolate the device from incoming signals (by puting in air plane mode ect) 6. Mobile device attached to a PC via a USB cable should be disconnected from the PC immediately, Helps to prevent synchronization that might occur automatically and overwrite data Any 4 points (.75 each)	
8		DiD- Each Component and explanation one mark each	(3)
9		Two Roles listing (Fact Witness and Expert Witness) 1 mark Exaplantio of each type 1 mark each	(3)
10		preliminary written or verbal report to your attorney, An examination plan for the attorney who has retained you. A verbal report is less structured than a written A written report is frequently an affidavit or a declaration. Each one mark	(3)
PART B			
Answer any one question from each module. Each question carries 6 marks.			
Module I			
11		Each point 2 marks each a. Internet Abuse Investigations b. E-mail Abuse Investigation c. Industrial espionage investigations	(6)
OR			
12		Contents: Single evidence, multi evidence form Case number—The number your organization assigns when an investigation is initiated. • Investigating organization—The name of your organization. In large corporations with global facilities, several organizations might be conducting investigations in different geographic areas. • Investigator—The name of the investigator assigned to the case. If many investigators are assigned, specify the lead investigator's name. • Nature of case—A short description of the case. For example, in the corporate environment • Location evidence was obtained—The exact location where the evidence was collected. If you're using multi-evidence forms, a new form should be created for each location. • Description of evidence—A list of the evidence items. On a multi-evidence form, write a description for each item of evidence you acquire. • Vendor name—The name of the manufacturer of the computer evidence. Model number or serial number—List the model number or serial number (if available) of the computer component. Many computer components, including hard drives, memory chips, and expansion slot cards, have model numbers but not serial numbers. • Evidence recovered by—The name of the investigator who recovered the evidence. • Date and time—The date and time the evidence was taken into custody. This information	(6)

		establishes exactly when the chain of custody starts. • Evidence placed in locker—Specifies which approved secure container is used to store evidence and when the evidence was placed in the container. • Item #/Evidence processed by/Disposition of evidence/Date/Time—When you or another authorized investigator retrieves evidence from the evidence locker forprocessing and analysis, list the item number and your name, and then describewhat was done to the evidence. • Page— The forms used to catalog all evidence for each location should have page numbers. Four or more - 4 marks Importance: 2 marks The first rule for all investigations is to preserve the evidence, which means it should not be tampered with or contaminated. When this happens, there's the possibility that the evidence has been compromised. To document the evidence, you record details about the media, including who recovered the evidence and when and who possessed it and when. Use an evidence custody form	
		Module II	
13		NTFS offers more information about a file, including security features, file ownership, and other file attributes. With NTFS,you also have more control over files and folders (directories) than with FAT file systems. NTFS was Microsoft's move toward a journaling file system. The system keeps track of transactions such as file deleting or saving. This journaling feature is helpful because it records a transaction before the system carries it out. That way, in a power failure or other interruption, the system can complete the transaction or go back to the last good setting. In NTFS, everything written to the disk is considered a file. On an NTFS disk, the first data set is the Partition Boot Sector, which starts at sector [0] of the disk and can expand to 16 sectors. Immediately after the Partition Boot Sector is the Master File Table (MFT). The MFT, similar to FAT in earlier Microsoft OSs, is the first file on the disk. An MFT file is created at the same time a disk partition is formatted as an NTFS volume and usually consumes about 12.5% of the disk when it's created. As data is added, the MFT can expand to take up 50 % of the disk. Another important advantage of NTFS over FAT is that it results in much less file slack space. Features Fat , NTFS two marks each	(6)
		OR	
14		Registry is a database that stores hardware and software configuration information, consolidates ini files, network connections, user preferences (including usernames and passwords), and setup information. Registry—A collection of files containing system and user information. – Importance 2 marks. Registry contents- 2 marks Registry HKEYs and their functions 2 marks HKEY_CLASS_ROOT A symbolic link to HKEY_LOCAL_MACHINE\SOFTWARE\Classes; provides file type and file extension information, URL protocol prefixes, and so forth	(6)

		HKEY_CURRENT_USER A symbolic link to HKEY_USERS; stores settings for the currently logged-on user HKEY_LOCAL_MACHINE Contains information about installed hardware and software HKEY_USERS Stores information for the currently logged-on user; only one key in this HKEY is linked to HKEY_CURRENT_USER HKEY_CURRENT_CONFIG A symbolic link to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profile\xxxx (with xxxx representing the current hardware profile); contains hardware configuration settings HKEY_DYN_DATA Used only in Windows 9x/Me systems; stores hardware configuration settings	
		Module III	
15		Everything is a file Including disks, monitors, NIC, RAM Files are objects with properties and methods (writing, deleting, adding).A block is the smallest Disk allocation unit. In Linux min is 512 bytes – 1 marks consists of four components defining File system Boot block ,Superblock ,inode block, Data block – 1 mark each. Figure 1 mark	(6)
		OR	
16		Acquiring data with dd and dcfldd in Linux: 2 marks each Validation tools – md5sum and sha1sum – 1 marks each each command explanation and various optiosn – 2 mark sample command usage 1 mark – dd (“data dump”) command • Can read and write from media device and data file,• Creates raw format file that most computer forensics analysis tools can read Shortcomings of dd command • Requires more advanced skills than average user,• Does not compress data Dcfldd-(DCFL dd) command is used for forensic acquisition. data dcfldd additional functions • Specify hex patterns or text for clearing disk space • Log errors to an output file for analysis and review • Use several hashing options • Refer to a status display indicating the progress of the acquisition in bytes • Split data acquisitions into segmented volumes with numeric extensions • Verify acquired data with original disk or media data	(6)

		• **md5sum** or **sha1sum** utilities should be run on all suspect disks and volumes or segmented volumes	
		Module IV	
17		Need for a standard procedure 2 marks- Any two There should be an established procedure in each organization on how the network data is being collected after an attack/intrusion incident. This will ensure you that all compromised systems are found, and able to ascertain attack methods so that able to prevent similar. The procedure should be based on organization's needs and should complement the network infrastructure. Network administrators should be able to stop the intruders, understand how they got in, what they copied/modified or still in the network. SOP: 4 marks A standard procedure used in network forensics is as follows: 1. Always use a standard installation image for systems on a network. This image isn't abit-stream image but an image containing all the standard applications used. You should also have the MD5 and SHA-1 hash values of all application and OS files. 2. When an intrusion incident happens, make sure the vulnerability has been fixed to prevent other attacks from taking advantage of the opening. 3. Attempt to retrieve all volatile data, such as RAM and running processes, by doing a live acquisition before turning the system off. 4. Acquire the compromised drive and make a forensic image of it. 5. Compare files on the forensic image to the original installation image. Compare hash values of common files, such as Win.exe and standard DLLs, and ascertain whether they have changed.	(6)
		OR	
18		Hardware parts: 3 marks The hardware consists of a microprocessor, ROM, RAM, a digital signal processor, a radio module, a microphone and speaker, hardware interfaces (, and an LCD display. Also have removable memory cards, and Bluetooth and Wi-Fi Information in SIM -3 marks • Service-related data, such as identifiers for the SIM card and subscriber • Call data, such as numbers dialed • Message information • Location information	(6)
		Module V	
19		• Abstract • Table of contents • Body of report • Conclusion • References, Glossary, Acknowledgments, Appendixes	(6)

		Explanation of each 1 mark. Each section should have a title indicating what you're discussing, If the report is long and complex, you should provide an abstract – 1 mark	
		OR	
20		Factors courts have used in determining whether to disqualify an expert include the following: Whether the attorney informed the expert that their discussions were confidential Whether the expert reviewed materials marked as confidential or attorney work product Whether the expert was asked to sign a confidentiality agreement Number of discussions held over a period of time The type of documents that were reviewed (publicly filed or confidential) The type of information conveyed to the expert—whether it included general or specific data or included confidential information, trial strategies, plans for method of proof. The amount of time involved in discussions or meetings between the expert and attorney Whether the expert provided the attorney with confidential information Whether the attorney formally retained the expert Whether the expert voiced concerns about being retained Whether the expert was requested to perform services for the attorney Whether the attorney compensated the expert. Each point 0.5 marks	(6)
		****	