TYCS Semester VI

Subject: Cyber Forensics

Slno	Questions
1	There are three c's in computer forensics. Which is one of the three? A. Control B. Chance C. Chains D. Core
2	Process of cyber Forensics is A. Collection->Analysis->Reporting->Examination B. Collection->Examination->Analysis->Reporting C. Examination->Collection->Reporting->Analysis D. Collection->Reporting->Analysis->Examination
3	Which of the equipment don't you have to get ready for recording video? A. Use date/time B. Carry extra batteries C. Bring paper and an extra pencil D. Carry extra memory
4	You are a computer forensic examiner tasked with determining what evidence is on a seized computer. On what part of the computer system will you find data of evidentiary value? A. Microprocessor or CPU B. USB controller C. Hard drive D. PCI expansion slots
5	Who work in a team to make computers and networks secure in an organization. A. Cyber criminals B. Investigators C. Police officer D. None of the above
6	A program or hardware device that filters information coming through an internet connection to a network or computer system. A. Firewall B. Cookies C. Cyber security D. Anti virus
7	The smallest area on a drive that data can be written to is a _____, while the smallest area on a drive that a file can be written to is a _____. A. bit and byte B. sector and cluster C. volume and drive D. memory and disk
8	The NT File System (NTFS) file system does which of the following? A. Supports long file names B. Compresses individual files and directories C. Supports large file sizes in excess of 4GB D. All of the above

9	Which tool is needed for a computer forensics job? A. PenDrives B. Hard disks C. Backup computer D. Compact Disk
10	Which of the following principle is violated if computer system is not accessible? A. Confidentiality B. Availability C. Access control D. Authentication
11	_____ is a password recovery and auditing tool. A. LC3 B. LC4 C. Network Stumbler D. Maltego
12	_____ is a popular tool used for network analysis in multiprotocol diverse network. A. Snort B. SuperScan C. Burp Suit D. EtterPeak
13	Data__is used to ensure confidentiality. A. Encryption B. Locking C. Deleting D. Backup
14	When shutting down a computer, what information is typically lost? A. Data in RAM memory B. Running processes C. Current network connections D. All of the above
15	How can we maintain data availability to authenticated users---------- A. Data clustering B. Data backup C. Data recovery D. Data Altering
16	How is the chain of custody maintained? A. By documenting what, when, where, how, and by whom evidence was seized B. By documenting in a log the circumstances under which evidence was removed from the evidence control room C. By documenting the circumstances under which evidence was subjected to analysis D. All of the above
17	Which of the following is not a property of computer evidence? A. Authentic and Accurate. B. Complete and Convincing. C. Duplicated and Preserved. D. Conform and Human Readable.
18	As a good forensic practice, why would it be a good idea to wipe a forensic drive before reusing it? A. Chain-of-custody B. Cross-contamination C. Different file and operating systems D. No need to wipe

19	Where can you find evidence of web-based email such as from MSN Hotmail or Google Gmail on a Windows XP system? A. In Temporary Internet Files under Local Settings in the user's profile B. In Unallocated Clusters C. In the pagefile.sys folder D. All of the above
20	Breaking the computer system of other people to acquire confidential information or gain financial benefits A. Piracy B. Phishing C. Napster D. Hacking
21	When a forensic copy is made, in what format are the contents of the hard drive stored? A. As compressed images. B. As bootable files. C. As executable files. D. As operating system files.
22	Which of the following is a proper acquisition technique? A. Disk to Image B. Disk to Disk C. Sparse Acquisition D. All of the above
23	Wireshark is a _____ tool. A. network protocol analysis B. network connection security C. connection analysis D. defending malicious packet-filtering
24	Traditional crimes that became easier or more widespread because of telecommunication networks and powerful PCs include all of the following except A. Money laundering B. Illegal drug distribution C. DoS attacks D. Child pornography
25	Computer forensics involves all of the following stated activities except: A. Interpretation of computer data B. Preservation of computer data C. Extraction of computer data D. Manipulation of computer data
26	An evidence custody form is also known as_____. A. Chain of Custody B. Chain of evidence C. Evidence form D. None of the above
27	Which duplication method produces an exact replica of the original drive? A. Bit-Stream Copy B. Image Copy C. Mirror Copy D. Bit stream copy
28	The most popular software forensic tools include all of the following except: A. Forensic Autopsy B. Quicken C. SMART D. Forensic Toolkit

29	Areas of files and disks that are not apparent to the user, and sometimes not even to the operating system, is termed: A. Hidden Data. B. Exceptional Data. C. Latent Data. D. Missing Data.
30	A powerful search tool, used to perform keyword searches in Linux and in Encase software. A. grep B. grub C. gcc D. gnu
31	The ability to hide data in another file is called A. Encryption. B. Steganography. C. Data parsing. D. A and B.
32	In establishing what evidence is admissible, many rules of evidence concentrate first on the _____ of the offered evidence. A. Relevancy B. Search and Seizure C. Material D. Admissibility
33	Monitor network traffic and alerts on suspicious activities A. TCP B. Firewalls C. Switches D. NIDS/NIPS
34	Why would a hacker use a proxy server? A. To create a stronger connection with the target. B. To create a ghost server on the network. C. To obtain a remote access connection. D. To hide malicious activity on the network.
35	Which phase of hacking performs actual attack on a network or system? A. Reconnaissance B. Maintaining Access C. Scanning D. Gaining Access
36	A file header is which of the following? A. A unique set of characters at the beginning of a file that identifies the file type B. A unique set of characters following the file name that identifies the file type C. A 128-bit value that is unique to a specific file based on its data D. Synonymous with the file extension
37	What is the purpose of a Denial of Service attack? A. Exploit a weakness in the TCP/IP stack B. To execute a Trojan on a system C. To overload a system so it is no longer operational D. To shutdown services by turning them off
38	A network tool used to determine the path packets take from one IP address to another A. Traceroute B. Ping C. Route D. None of the above

39	The ability to recover and read deleted or damaged files from a criminals computer is an example of a law enforcement specialty called? A. Robotics B. Simulation C. Computer Forensics D. Animation
40	The science of hiding messages in messages is known as ___ A. Scanning B. Spoofing C. Steganography D. Steganalysis
41	The first phase of hacking an IT system is compromise of which foundation of security? A. Availability B. Confidentiality C. Integrity D. Authentication
42	Performing hacking activities with the intent on gaining visibility for an unfair situation is called _____. A. Cracking B. Analysis C. Hacktivism D. Exploitation
43	Sniffing is used to perform _____ fingerprinting. A. Passive stack B. Active stack C. Passive banner grabbing D. Scanned
44	What are hybrid attacks? A. An attempt to crack passwords using words that can be found in dictionary. B. An attempt to crack passwords by replacing characters of a dictionary word with numbers and symbols. C. An attempt to crack passwords using a combination of characters, numbers, and symbols. D. An attempt to crack passwords by replacing characters with numbers and symbols.
45	What is the full form of ITA-2000? A. Information Tech Act -2000 B. Indian Technology Act -2000 C. International Technology Act -2000 D. Information Technology Act -2000
46	Which of the following is not considered as direct evidence A. Fingerprint B. Confession C. Video recording D. Eyewitness statement
47	Which database allows a system administrator to associate a function with a relation. A. Virtual database B. Private database C. Custom database D. Virtual Private Database(VPD)
48	A crime is : A. illegal act only if observed by a police officer. B. Act forbidden by law C. Omission forbidden by law D. Both b and c

49	If a DNS server accepts and uses the wrong details from a host that has no authority giving that information, then this technique is called A. DNS hijacking B. DNS lookup C. DNS spoofing D. All of the above
50	Which of this is an example of physical hacking? A. Remote Unauthorised access B. Inserting malware loaded USB to a system C. SQL Injection on SQL vulnerable site D. DDoS (Distributed Denial of Service) attack