Sr.No	Question	A	B	C	D	Answer
1	A valid definition of digital evidence is:	Data stored or transmitted using a computer	Information of probative value	Digital data of probative value	Any digital evidence on a computer	C
2	What are the three general categories of computer systems that can contain digital evidence?	Desktop, laptop, server	Personal computer, Internet, mobile telephone	Hardware, software, networks	Open computer systems, communication	D
3	In terms of digital evidence, a hard drive is an example of:	Open computer systems	Communication systems	Embedded computer systems	None of the above	A
4	In terms of digital evidence, a mobile telephone is an example of:	Open computer systems	Communication systems	Embedded computer systems	None of the above	C
5	In terms of digital evidence, a Smart Card is an example of:	Open computer systems	Communication systems	Embedded computer systems	None of the above	C
6	In terms of digital evidence, the Internet is an example of:	Open computer systems	Communication systems	Embedded computer systems	None of the above	B
7	Computers can be involved in which of the following types of crime?	Homicide and sexual assault	Computer intrusions and intellectual property theft	Civil disputes	All of the above	D
8	A logon record tells us that, at a specific time:	An unknown person logged into the system using the account	The owner of a specific account logged into the system	The account was used to log into the system	None of the above	C
9	Cybertrails are advantageous because:	They are not connected to the physical world	Nobody can be harmed by crime on the Internet.	They are easy to follow.	Offenders who are unaware of them leave behind more clues than they otherwise would have.	D

Sr.No	Question	A	B	C	D	Answer
10	Private networks can be a richer source of evidence than the Internet because:	They retain data for longer periods of time.	Owners of private networks are more cooperative with law enforcement.	Private networks contain a higher concentration of digital evidence.	All of the above.	C
11	Due to caseload and budget constraints, often computer security professionals attempt to limit the damage and close each investigation as quickly as possible. Which of the following is NOT a significant drawback to this approach?	Each unreported incident robs attorneys and law enforcement personnel of an opportunity to learn about the basics of computer-related crime.	Responsibility for incident resolution frequently does not reside with the security professional, but with management.	This approach results in under-reporting of criminal activity, deflating statistics that are used to allocate corporate and government spending on combating computer-related crime.	Computer security professionals develop loose evidence processing habits that can make it more difficult for law enforcement personnel and attorneys to prosecute an offender.	B
12	The criminological principle which states that, when anyone, or anything, enters a crime scene he/she takes something of the scene with him/her, and leaves something of himself/herself behind, is:	Locard's Exchange Principle	Differential Association Theory	Beccaria's Social Contract	None of the above	A
13	The author of a series of threatening e-mails consistently uses "im" instead of "I'm." This is an example of:	An individual characteristic	An incidental characteristic	A class characteristic	An indeterminate characteristic	A
14	Personal computers and networks are often a valuable source of evidence. Those involved with ______ should be comfortable with this technology.	Criminal investigation	Prosecution	Defense work	All of the above	D
15	An argument for including computer forensic training computer security specialists is:	It provides an additional credential.	It provides them with the tools to conduct their own investigations.	It teaches them when it is time to call in law enforcement.	None of the above.	C
16	Computers can play the following roles in a crime:	Target, object, and subject	Evidence, instrumentality, contraband, or fruit of crime	Object, evidence, and tool	Symbol, instrumentality, and source of evidence	B

17	The first US law to address computer crime was:	Computer Fraud and Abuse Act (CFAA)	Florida Computer Crime Act	Computer Abuse Act	None of the above	B
18	The following specializations exist in digital investigations:	First responder (a.k.a. digital crime scene technician)	Forensic examiner	Digital investigator	All of the above	D
19	The first tool for making forensic copies of computer storage media was:	EnCase	Expert Witness	dd	Safeback	C
20	One of the most common approaches to validating forensic software is to:	Examine the source code	Ask others if the software is reliable	Compare results of multiple tools for discrepancies	Computer forensic tool testing projects	C
21	An instrumentality of a crime is:	An instrument used to commit a crime	A weapon or tool designed to commit a crime	Anything that plays a significant role in a crime	All of the above	D
22	. Contraband can include:	Child pornography	Devices or programs for eavesdropping on communications	Encryption devices or applications	All of the above	D
23	A cloned mobile telephone is an example of:	Hardware as contraband or fruits of crime	Hardware as an instrumentality	Information as contraband or fruits of crime	Information as evidence	A
24	Digital photographs or videos of child exploitation is an example of:	Hardware as contraband or fruits of crime	Hardware as an instrumentality	Information as evidence	Information as contraband or fruits of crime	D
25	Stolen bank account information is an example of:	Hardware as contraband or fruits of crime	Information as contraband or fruits of crime	Information as an instrumentality	Information as evidence	B
26	A network sniffer program is an example of:	Hardware as contraband or fruits of crime	Hardware as an instrumentality	Information as contraband or fruits of crime	Information as evidence	C
27	Computer equipment purchased with stolen credit card information is an example of:	Hardware as contraband or fruits of crime	Hardware as an instrumentality	Hardware as evidence	Information as contraband or fruits of crime	A
28	A printer used for counterfeiting is an example of:	Hardware as contraband or fruits of crime	Hardware as an instrumentality	Hardware as evidence	Information as contraband or fruits of crime	B
29	Phone company records are an example of:	Hardware as contraband or fruits of crime	Information as contraband or fruits of crime	Information as an instrumentality	Information as evidence	D

30	In the course of conducting forensic analysis, which of the following actions are carried out?	Critical thinking	Fusion	Validation	All of the above	D
31	Having a member of the search team trained to handle digital evidence:	Can reduce the number of people who handle the evidence	Can serve to streamline the presentation of the case	Can reduce the opportunity for opposing counsel to impugn the integrity of the evidence	All of the above	D
32	An attorney asking a digital investigator to find evidence supporting a particular line of inquiry is an example of:	Influencing the examiner	Due diligence	Quid pro quo	Voir dire	A
33	A digital investigator pursuing a line of investigation in a case because that line of investigation proved successful in two previous cases is an example of:	Logical reasoning	Common sense	Preconceived theory	Investigator's intuition	C
34	A scientific truth attempts to identify roles that are universally true. Legal judgment, on the other hand, has a standard of proof in criminal prosecutions of:	Balance of probabilities	Beyond a reasonable doubt	Acquittal	None of the above	B
35	Regarding the admissibility of evidence, which of the following is not a consideration:	Relevance	Authenticity	Best evidence	Nominally prejudicial	D
36	According to the text, the most common mistake that prevents evidence seized from being admitted is:	Uninformed consent	Forcible entry	Obtained without authorization	None of the above	C
37	In obtaining a warrant, an investigator must convince the judge on all of the following points except:	Evidence of a crime is in existence	A crime has been committed	The owner or resident of the place to be searched is likely to have committed the crime	The evidence is likely to exist at the place to be searched	C
38	If, while searching a computer for evidence of a specific crime, evidence of a new, unrelated crime is discovered, the best course of action is:	Abandon the original search, and pursue the new line of investigation	Continue with the original search but also pursue the new inquiry	Stop the search and obtain a warrant that addresses the new inquiry	Continue with the original search, ignoring the new information	C
39	The process of documenting the seizure of digital evidence and, in particular, when that evidence changes hands, is known as:	Chain of custody	Field notes	Interim report	None of the above	A

40	When assessing the reliability of digital evidence, the investigator is concerned with whether the computer that generated the evidence was functioning normally, and:	Whether chain of custody was maintained	Whether there are indications that the actual digital evidence was tampered with	Whether the evidence was properly secured in transit	Whether the evidence media was compatible with forensic machines	B
41	The fact that with modern technology, a photocopy of a document has become acceptable in place of the original is known as:	Best evidence rule	Due diligence	Quid pro quo	Voir dire	A
42	Evidence contained in a document provided to prove that statements made in court are true is referred to as:	Inadmissible evidence	Illegally obtained evidence	Hearsay evidence	Direct evidence	C
43	Business records are considered to be an exception to:	Direct evidence	Inadmissible evidence	Illegally obtained evidence	Hearsay evidence	D
44	Which of the following is not one of the levels of certainty associated with a particular finding?	Probably	Maybe	Almost definitely	Possibly	B
45	Direct evidence establishes a:	Fact	Assumption	Error	Line of inquiry	A
46	What is one of the most complex aspects of jurisdiction when the Internet is involved?	Arranging to travel to remote locations to apprehend criminals	Determining which court can enforce a judgment over a defendant	Finding a court that is in two states	Finding a federal court that can hear a civil suit	B
47	In the US, to enforce a judgment over a defendant, a court must have which of the following?	Subject matter and personal jurisdiction	General and limited jurisdiction	Diversity and long arm jurisdiction	None of the above	A
48	The Miller test takes which of the following into account when determining if pornography is obscene?	It appeals to the public interest	It depicts sexual conduct in a patently offensive way	It lacks any monetary value	All of the above	B
49	Which of the following rights is not explicitly mentioned in the US Constitution?	Right of the people to keep and bear arms	Right of personal privacy	Right of the people peaceably to assemble	Right to a speedy and public trial	B

50	The definition of a “protected computer” is, according to the CFAA:	A computer that is used exclusively by a financial institution or the Federal government.	A computer that is used non-exclusively by a financial institution or the Federal government and the crime affects that use.	A computer that is used in state or foreign commerce or communication.	All of the above.	D
51	The legislation that made the theft of trade secrets a Federal crime was	The Lanham Act	The Economic Espionage Act	The Child Pornography Protection Act	None of the above	B
52	Which state does not have a law prohibiting simple hacking – gaining unauthorized access to a computer?	California	Texas	Washington	None of the above	D
53	The term “computer contaminant” refers to:	Excessive dust found inside the computer case	Viruses, worms, and other malware	Spam e-mails	Nigerian scam e-mails	B
54	In those states with legislation addressing computer forgery, contraband in the form of “forgery devices” may include:	Computers	Computer equipment	Specialized computer software	All of the above	D
55	Compelling a suspect to reveal passwords to provide access to encrypted media is considered to fall under the:	Second Amendment	Fourth Amendment	Fifth Amendment	Seventh Amendment	C
56	An example of a content-related crime would be:	Cyberstalking	Child pornography	Hacking	None of the above	B
57	Hacking is an example of:	Computer-assisted crime	Computer-related crime	Computer-integrity crime	Computer malfeasance crime	C
58	Forgery is an example of:	Computer assisted crime	Computer-related crime	Computer-integrity crime	Computer malfeasance crime	A
59	In Ireland, the Non-Fatal Offences Against the State Act of 1997 specifically addresses:	Computerized welfare fraud	Cyberbullying	Nigerian scams	Hacking	B
60	Jurisdiction claims may be based on:	Location of the perpetrator’s computer	Location of the victim’s computer	Location of intermediary computers	All of the above	D

61	Standard operating procedures (SOPs) are important because they:	Help individuals avoid common mistakes	Ensure that the best available methods are used	Increase the probability that two forensic examiners will reach the same conclusions when they examine the evidence	All of the above	D
62	The goal of an investigation is to:	Convict the suspect	Discover the truth	Find incriminating evidence	All of the above	B
63	An investigation can be hindered by the following:	Preconceived theories	Improperly handled evidence	Offender concealment behavior	All of the above	D
64	When you have developed a theory, what can you do to confirm that your hypothesis is correct?	Predict, based on your hypothesis, where artifacts should be located	Perform experiments to test results and rule out alternate explanations	Conclude, based on your findings, whether the evidence supports the hypothesis	All of the above	D
65	Which of the following would be considered an individual characteristic?	The originating IP address in a network packet or e-mail header	A scratch on the glass of a flatbed scanner or digital camera lens	Date-time stamps of files on a disk or entries in a database	All of the above	B
66	When digital photographs containing child pornography are found on a home computer, investigators can assert that: a	Someone in the house transferred the photographs onto the computer from a disk or the Internet	Someone in the house took the photographs with a digital camera and transferred them directly onto the computer.	Someone in the house took the photographs with a digital camera and transferred them directly onto the computer	None of the above.	D
67	Forensic examination involves which of the following:	Assessment, experimentation, fusion, correlation, and validation	Seizure and preservation	Recovery, harvesting, filtering, organization, and search	All of the above	C
68	Forensic analysis involves the following:	Assessment, experimentation, fusion, correlation, and validation	Seizure and preservation	Recovery, harvesting, filtering, organization, and search	All of the above	A

69	The first step in applying the scientific method to a digital investigation is to:	Form a theory on what may have occurred	Experiment or test the available evidence to confirm or refute your prediction	Make one or more observations based on events that occurred	Form a conclusion based on the results of your findings	C
70	Which of the following should the digital investigator consider when arranging for the transportation of evidence?	Should the evidence be physically in the possession of the investigator at all times?	Will the evidence copies be shared with other experts at other locations?	Will there be environmental factors associated with the digital media?	All of the above	D
71	In the Staircase Model, why is case management shown spanning across all of the steps in the process model?	Case documents are intangible objects that can be held.	Case management provides stability and enables investigators to tie all relevant information together.	Case management documents the process function.	None of the above.	B
72	Process models have their origins in the early theories of computer forensics which defined the field in terms of a _____ process	Complicated	Difficult	Linear	Polymorphic	C
73	Generating a plan of action and obtaining supporting resources and materials falls under which step in the digital investigation?	Preparation	Survey/identification	Preservation	Examination and analysis	A
74	The process model whose goal is to completely describe the flow of information in a digital investigation is known as:	The Physical Model	The Staircase Model	The Evidence Flow Model	The Subphase Model	C
75	The following organizations have published guidelines for handling digital crime scenes:	US Secret Service	Association of Chief Police Officers	US Department of Justice	All of the above	D
76	When a first responder encounters technology or equipment that he is not familiar with, the recommended course of action is to:	Seize the equipment as if it were a known device	Seek assistance from a more experienced digital investigator	Leave that particular piece of equipment at the crime scene	Ask the suspect for details on the equipment	B
77	When preparing a questionnaire for interviewing individuals of the crime scene which of the following should NOT be requested:	Passwords	Encryption keys	Admission of guilt	Details on removable storage	C

78	When entering a crime scene, the initial survey should:	Include user manuals	Involve tracing cables	Collect relevant data such as passwords and account details	All of the above	D
79	Examples of data that should be immediately preserved include:	USB drives	Digital picture frames	System and network information	USB bracelets	C
80	The crime scene preservation process includes all but which of the following:	Protecting against unauthorized alterations	Acquiring digital evidence	Confirming system date and time	Controlling access to the crime scene	C
81	A thorough crime scene survey should include:	Manuals for software applications	Removable media	Mobile devices	All of the above	D
82	The challenge to controlling access to a digital crime scene is that:	Information may be stored on Internet servers in different locations	The computer may be shared.	The computer case may be locked.	None of the above.	A
83	In the case where digital investigators dealing with distributed systems need to collect data from remote sites, the following procedure is recommended:	Notify personnel at the remote sites to leave everything as is, and arrange for travel to the remote locations	Notify personnel at the remote sites to shut down all systems and send the hard drives to the forensic lab	Utilize remote forensics tools to acquire data from the remote sites' RAM as well as the hard drives	None of the above	C
84	When presenting evidence on an organizational network, the digital investigator may require the assistance of:	System administrators	The CEO of the organization	The CSO (Chief Security Officer)	Additional forensic investigators	A
85	Which of the following is not a safety consideration for a first responder?	Additional personnel to control those present at the crime scene	Protection against ELF emanations from monitors	Proper tools for disassembling and reassembling computer cases	Protective gloves and eyewear	B
86	Digital investigators like to preserve every potential source of digital evidence; however, they are constrained by:	The law	Resources	The interests of business	All of the above	D

87	During the initial survey of a crime scene, why it is necessary to photograph or videotape the area and items of potential interest in their current state?	This simplifies inventorying the crime scene	Photographing items to be seized records their actual condition, and precludes damage claims when the items are returned to the offender.	To record the fact that a particular item was actually found at the crime scene.	None of the above.	C
88	Why is the first step to secure the physical crime scene by removing everyone from the immediate area?	To prevent them from contaminating evidence	To prevent them from asking questions about the case before they can be interviewed	To give them time to fill out a personal information survey	To keep them from blocking the view when photographs are being taken	A
89	When a piece of evidence has both a biological and a digital component, who should process it first?	The crime scene technician, because biological artifacts are much more fragile	The digital investigator, because processing the biological artifacts will destroy digital evidence	Neither; the evidence should be preserved and transported to the lab for processing	Both the crime scene technician and the digital investigator, in a cooperative effort, assuring that the biological evidence is collected in a way that does not damage the digital component	D
90	The process of evaluating available evidence objectively, independent of the interpretations of others, to determine its true meaning is referred to as:	Equivocal forensic analysis	Investigative reconstruction	Threshold assessment	Behavioral imprints	A
91	The words that an offender uses on the Internet, the tools that an offender uses online, and how an offender conceals his identity and criminal activity are referred to in the text as:	Investigation reconstruction	Threshold assessment	Behavioral imprints	Crime scene analysis	C
92	Investigative reconstruction is composed of three different forms	Which of the following is NOT one of those three forms?	Functional	Intentional	Relational	B

93	Creating a histogram of times to reveal periods of high activity is an example of which form of investigative reconstruction?	Functional	Intentional	Relational	Temporal	D
94	The investigation and study of victim characteristics is known as:	Criminal profiling	Behavioral imprints	Victimology	Crime scene analysis	C
95	Why should victimology include a thorough search of the Internet for cybertrails? a	Because the Internet can significantly increase the victims risk	Because it is well known that even traditional criminal offenses are documented on the Internet.	Because nearly everyone uses the Internet.	None of the above.	A
96	The type of report that is a preliminary summary of findings is known as:	SITREP	Threshold Assessment report	Full investigative report	Field notes	B
97	According to the text, the distinguishing features of a crime scene as evidenced by the offender's behavioral decisions regarding the victim and the offense location are known as:	Hard evidence	Fruit of the poison tree	Caveat emptor	Crime scene characteristics	D
98	In crimes against individuals the _____ period leading up to the crime often contains the most important clues regarding the relationship between the offender and the victim	24-hour	48- hour	60-minute	15-minute	A
99	One of the most important things to establish when a computer is directly involved in the commission of a crime is:	Where the computer was purchased	What operating system is in use	Who or what was the intended victim or target	None of the above	C
100	An example of online behavior that puts an individual at higher risk for cyberstalking is:	Using your real name online	Putting personal information in your profile	Posting photographs on a social networking page	All of the above	D
101	In the movie Home Alone one of the burglars would always turn the water on in the sinks so that the house would be flooded when the owners returned. In terms of crime scene characteristics, this is an example of:	Psychotic episode	Signature-oriented behavior	Modus operandi	Vandalism	B
102	The totality of choices an offender makes during the commission of a crime are referred to as:	The criminal's MO	Crime scene characteristics	Tangible evidence	None of the above	B

103	Because seemingly minor details regarding the offender can be important, investigators should get into the habit of contemplating which of the following:	What the offender brought to the crime scene	What the offender took from the crime scene	What the offender changed at the crime scene	All of the above	D
104	One reason digital investigators write threshold assessments more often than full reports is because:	They will be included in a final report, and so, distribute the time for final report preparation over the entire period of the investigation	They keep their supervisor aware of their productivity.	They take less time to prepare and may be sufficient to close out an investigation.	They serve as field notes for the investigator.	C
105	Every violent crime investigation should incorporate digital evidence because digital evidence may reveal:	Investigative leads	Likely suspects	Previously unknown crimes	All the above	D
106	How the offender approaches and obtains control of a victim or target is significant because it exposes the offender's:	Motives	Choice of weapons	Modus operandi	Signature behaviors	A
107	Crime scenes fall into two categories – primary and ___	Remote	Secondary	Ancillary	Theoretical	B
108	When reconstructing evidence surrounding a violent crime, it is generally helpful to:	Lay out all the evidence so it can be viewed in its entirety	Work with the crime scene technicians so that a better understanding of the crime is achieved	Construct a timeline of events from digital evidence	Begin the process of converting field notes to a final report	C
109	One reason not to put too much trust into those who run the company's computers is that:	There has always been an antagonism between system administrators and law enforcement	They are typically too busy to take the time to answer your questions	They are usually not authorized to answer questions.	They may be the offenders.	D

110	Although crime scenes are typically photographed, it is a good idea to create diagrams of the crime scene because:	Diagramming is a common crime scene technician's skill; however, it requires continual practice	The process of creating a diagram can result in a digital investigator noticing an important item of evidence that would otherwise have been missed	The quality of photographs taken at the crime scene is not known until the film is developed.	None of the above.	B
111	Given the scope and consequences of violent crimes, when collecting digital evidence it is advisable to:	Collect only that digital evidence that is clearly connected to the offense	Focus only on the primary crime scene, as searching the offender's home and workplace requires additional authorization	Seek out and preserve all available digital evidence	Focus only on the offender's digital evidence, as the victim's digital evidence is usually of little value	C
112	When swift action is needed, law enforcement personnel may be permitted to conduct searches without a warrant	Searches of this kind are permitted under:	Exigent circumstances	Eminent domain	Mens rea	A
113	When processing the digital crime scene in a violent crime investigation it is important to have _____ to ensure that all digital evidence and findings can hold up under close scrutiny	A good supply of electrostatic bags for holding sensitive electronic components	More than one reliable camera for photographing the crime scene	Standard operating procedures for processing a digital crime scene	A good supply of nitrile gloves	C
114	The Federal statute that has a provision allowing Internet service providers to disclose subscriber information to law enforcement in exigent circumstances is:	ECPA	CCPA	The Privacy Act	FCRA	A
115	When reconstructing evidence surrounding a violent crime, it is generally helpful to:	Diagram the crime scene	Create a timeline of events from digital evidence	Create a threat assessment report	None of the above	B
116	A thief who has programmed and released a virus to roam a network looking for victim passwords used for online banking is an example of what offense behavior?	Power assertive	Profit oriented	Power reassurance	Anger retaliatory	B

117	The case of a Michigan bank robber requiring tellers to undress so he could photograph them is an example of:	Deviant aberrant behavior	Criminal humor	Crime scene characteristics	Investigative reconstruction	C
118	The assessment of the victim as they relate to the offender, the crime scene, the incident, and the criminal justice system is known as:	Threat assessment methodology	Signature behaviors	Behavioral evidence analysis	Victimology	D
119	Computers and mobile devices are treated as _____ crime scenes in violent crime investigations	Temporary	Immediate	Remote	Secondary	D
120	During the commission of a crime, evidence is transferred between the offender's computer and the target This is an example of:	Locard's Exchange Principle	Sutherland's General Theory of Criminology	Martin's Rule d	Parkinson's Rule of Available Space	A
121	Intruders who have a preferred toolkit that they have pieced together over time, with distinctive features:	Usually have little experience and are relying on the kit	Show little initiative – letting the tool do the work	Are generally more experienced	Pose less of a threat	C
122	In the case of a computer intrusion, the target computer is:	The remote crime scene	The auxiliary crime scene	The virtual crime scen	The primary crime scene	D
123	A computer intruder's method of approach and attack can reveal significant amount about their:	Skill level	Knowledge of the target	Intent	All of the above	D
124	Determining skill level can lead to:	Determining the extent of the intrusion	Likely hiding places for rootkits and malware	Suspects	Offense behaviors	C
125	If digital investigators find an unauthorized file, they should:	Immediately move the file to removable media	Check for other suspicious files in the same directory	Execute the file to determine its purpose	Permanently delete the file	B
126	Remote forensic solutions can be used to access live systems, and include the ability to:	Acquire and, sometimes, analyze memory	Image systems without ever having to leave the lab	Conduct examination and analysis without the need to image	Image large systems across the Internet	A
127	A forensic analysis conducted on a forensic duplicate of the system in question is referred to as:	Virtual analysis	Clone analysis	Post-mortem analysis	Ex post facto analysis	C

128	Capturing all of the network traffic to and from the compromised system can:	Allow the network administrators to participate in the investigation, establishing rapport for later interviews	Reveal the source of the attack	Seriously slow down the network, affecting normal work	None of the above	B
129	A common technique that is highly useful and can be applied in a computer intrusion investigation is to simply focus on file system activities around the time of known events	This embodies a principle known as:	Temporal proximity	Timeline analysis	File system analysis	A
130	The registry key HKLM\Software\Microsoft\Windows\Current Version is one of the most common locations for:	New software entries	Time and date information	Trojans	A list of recently run programs	C
131	When collecting data from a compromised computer, consideration should be given to collecting the _____ data first.	CMOS	Most volatile	Magnetic	Optical	B
132	The forensic examiner needs to be aware that the process of collecting memory:	Is seldom useful and not often called for	Can take an extremely long period of time c	Is only needed for standalone systems d	Changes the contents of memory	D
133	A more thorough method of collecting specific volatile data from a computer is to:	Examine the specific memory addresses live	Collect the full contents of physical memory	Selectively collect contents of physical memory	Take screenshots	B
134	Why are “non-volatile” storage locations contained in the RFC 8227 “Order of Volatility”?	This is an old RFC and has not been updated	No form of data storage is permanent	An RFC is a Request for Comments – and corrections are expected.	None of the above.	B
135	The first state in the United States to enact a law to deal with cyberstalkers was: a	Texas b	Hawaii c	California d	New York	C
136	The first cyberstalking law in the US was passed in:	1985 b	1990 c	1995 d	2000	B
137	Stalkers want to exert power over their victims, primarily through:	Fear	Anxiety	Autosuggestion	Peer pressure	A

138	A stalker’s ability to frighten and control a victim increases with the amount of information that he can gather, such as:	Telephone numbers	Addresses	Personal preferences	All of the above	D
139	Stalkers have taken to the Internet because:	The cost of an Internet connection has dropped considerably	They depend heavily on information and the Internet contains vast amounts	They no longer have to go out to do their stalking	None of the above	B
140	An implication from studies indicating that many stalkers had prior acquaintance with their victims is that:	Part of the blame can be assigned to the victim	The offender is likely to be found in the same area as the victim	Investigators should pay particular attention to acquaintances of the victim	Investigators should always check the immediate family	C
141	An excellent set of guidelines developed specifically for victims of stalking is available from:	The National Center for Victims of Crime	The National White Collar Crime Center	The Department of Justice	The National Institute of Justice	A
142	When a cyberstalking case is stalled, it is a good idea to interview the victim again, because:	The victim might have been withholding information during the first interview	The information that investigators have gathered might help the victim recall additional details	The time between the first and second interviews has given the victim time to seek counseling	None of the above	B
143	In determining how and why the offender selected a specific victim, the investigator should determine whether the cyberstalker:	Knew the victim	Learned about the victim through a personal web page	Noticed the victim in a chat room	All of the above	D
144	A key aspect of developing victimology is determining victim and offender ____	Hobbies	Likes and dislikes	Risks	Roles	C
145	When searching for evidence of cyberstalking, it is useful to distinguish between an offender’s harassing behaviors and _____ behaviors	Grooming	Surreptitious monitoring	Initial contact	Congenial	B
146	That part of cyberstalking where the offender is using the Internet to find a victim is known as:	Profiling	Trolling	Surreptitious monitoring	None of the above.	C
147	When a cyberstalker chooses victims at random, he is said to be an:	Opportunistic stalker	Power assertive stalker	Profit-oriented stalker	None of the above	A

148	The initial stage in a cyberstalking investigation is to:	Search for additional digital evidence	Analyze crime scene characteristics	Conduct victimology and risk assessments	Interview the victim	D
149	It is extremely important for the investigator to be extremely cautious when dealing with a stalking case because:	If the victim becomes offended by the investigator's methods, she is likely to go file a complaint	If the investigation is conducted too openly, the offender may stop the harassment and move on to another victim	The victim must be protected, in case the offender decides to escalate to physical violence	The victims frequently become emotionally attached to the investigator	C
150	Which of the following is NOT part of the set of forensic methodologies referenced in this book?	Preparation	Interdiction	Documentation	Reconstruction	B
151	Preparation planning prior to processing a crime scene should include:	What computer equipment to expect at the site	What the systems are used for	Whether a network is involved	All of the above	D
152	The forensic crime scene processing kit should include all of the following, EXCEPT:	Evidence bags, tags, and other items to label and package evidence	Forensically sanitized hard drives to store acquired data	Compilers for developing forensic tools on site	Hardware write blockers	C
153	When processing the digital crime scene, one aspect of surveying for potential sources of digital evidence is:	Recognizing relevant hardware such as computers, removable media, etc	Determining if electrical wiring is capable of supporting forensic machines	Confirming that the operating environment is suitable for electronic equipment	Making sure there is sufficient space to set up the forensic crime scene processing kit	A
154	The _____ documentation specifies who handled the evidence, when, where, and for what purpose	Evidence inventory	Chain of custody	Evidence intake	Preservation notes	B
155	When documenting a crime scene, the computer and surrounding area should be photographed, detailed sketches should be made, and copious notes should be taken, because:	The more evidence collected, the stronger the case.	This provides a record for what to look for when you return for the second visit.	It is prudent to document the same evidence in several ways.	All of the above.	C
156	In regard to preservation, in a child pornography investigation, which of the following should be collected?	Photographs	Papers	Digital cameras	All of the above	D

157	If it is determined that some hardware should be collected, but there is no compelling need to collect everything, the most sensible approach is to employ:	Nearest reach doctrine	Direct connectivity doctrine	Independent component doctrine	Slice-the-pie doctrine	C
158	According to the us Federal guidelines for searching and seizing computers, safe temperature ranges for most magnetic media are:	60-80 degrees Fahrenheit	50-90 degrees centigrade	50-90 degrees Fahrenheit	60-80 degrees centigrade	C
159	Which of the following is NOT an artifact that will be irrevocably lost if the computer is shut down?	Running processes	Open network ports	Data stored in memory	System date and time	D
160	Which of the following is NOT one of the recommended approaches to preserving digital evidence?	Place the evidential computers and storage media in secure storage for later processing	Preview the evidential computer, taking appropriate notes	Extract just the information needed from evidential computers and storage media	Acquire everything from evidential computer and storage media	B
161	The reason UNIX "dd" is considered a de facto standard for making bitstream copies is:	The majority of tools for examining digital evidence can interpret bitstream copies	"dd" stands for "digital data" and was developed for making forensic copies.	"dd," although a UNIX tool, is universally able to traverse Windows file systems.	The developers of "dd" have made arrangements with other forensic software companies.	A
162	Regarding the examination of a piece of digital evidence, which of the following is NOT one of the fundamental questions that need to be answered?	What is it (identification)?	What classifications distinguish it?	Where did it come from?	What is its value?	D
163	Which of the following issues is NOT one that a forensic examiner faces when dealing with Windows-based media?	Invasive characteristics of the Windows environment	The facility in the standard Windows environment for mounting a hard drive as Read-Only	The location, organization, and content of Windows system log files	Available methods for recovering data from Windows media	B
164	Forensically acceptable alternatives to using a Windows Evidence Acquisition Boot Disk include all but which of the following?	Linux boot floppy	FIRE bootable CD-ROM	Booting into safe mode	Hardware write blockers	C
165	The standard Windows environment supports all of the following file systems EXCEPT _____	FAT16	ext2	FAT32	NTFS	B

166	Before evidentiary media is “acquired,” forensic examiners often _____ the media to make sure it contains data relevant to the investigation	Hash	Preview	Validate	Analyze	B
167	Log files are used by the forensic examiner to _____	Associate system events with specific user accounts b	Verify the integrity of the file system c	Confirm login passwords d	Determine if a specific individual is the guilty party	A
168	The Windows NT Event log Appevent	Contains a log of application usage	Records activities that have security implications, such as logins	Notes system events such as shutdowns	None of the above	A
169	When examining the Windows registry key, the “Last Write Time” indicates:	The last time RegEdit was run b	When a value in that Registry key was altered or added	The current system time	The number of allowable changes has been exceeded	B
170	File system traces include all of the following EXCEPT:	Metadata	CMOS settings	Swap file contents	Data object date-time stamps	B
171	When a file is moved within a volume, the Last Accessed Date Time:	Is unchanged	Changes if a file is moved to different directory	Changes if a file is moved to the root	Is unchanged; however, the Created Date-Time does change	A
172	Internet traces may be found in which of the following categories?	Web browser cache	Instant messenger cache	Cookies	All of the above	D
173	The Windows NT Event log Secevent evt:	Contains a log of application usage	Records activities that have security implications, such as logins	Notes system events such as shutdowns	None of the above	B
174	Which of the following is NOT one of the methods mobile devices use to communicate?	FDDI	Telecommunication networks	WiFi access points	Bluetooth piconets	A

175	One major advantage of mobile devices from a forensic perspective is that:	People very seldom delete information from mobile devices	The process for deleting information is much more complicated than for adding information, and users frequently don’t delete things correctly	Flash memory is deleted block-by-block and mobile devices generally wait for a block to be full before it is deleted	Manufacturers reserve a part of memory for storing deleted items	C
176	The reason that malware developers are beginning to target mobile devices is:	Because available memory is much smaller and the operating system is much less sophisticated on mobile devices, it is much easier to develop malicious code	The malware market has become very crowded and developers are looking for new avenues	Since the coding is much simpler on mobile devices, many new programmers are trying at this particular platform	Since mobile devices are used more and more for online banking and making purchases, they have become prime targets for computer criminals	D
177	Software designed to monitor activities on mobile devices has come to be called: a	Malware b	Spouseware c	Trojan defense d	None of the above	B
178	One of the dangers (from a forensic standpoint) of mobile devices is:	Connected networks can contain investigatively useful information	Network service providers may provide information for comparison with data extracted from a mobile device	Connected networks can enable offenders to delete data remotely	Network service providers may provide additional historical call records	C
179	One of the difficulties unique to forensic processing of mobile devices is:	MD five hashes must be calculated for data recovered from mobile devices	Documentation must show continuous possession and control	An investigator must make a calculated decision to either prevent or allow the device to receive new data over wireless networks	Any issues encountered with processing the device should be documented	C

180	Powering down a mobile device and removing the battery may cause problems in that: a	When the battery is removed from a mobile device, the information in memory is lost	Doing so may activate security measures such as lock codes and encryption	The process of removing the battering can cause a capacitive discharge, destroying the device	You now have two pieces of evidence, which have to be documented	B
181	Which of the following are methods for preserving mobile devices by isolating them from the networks?	Reconfigure the device to prevent communication from the network	Place the device in an RF-shielded pouch	Jam RF signaling in the immediate area	All of the above	D
182	Why is it important to collect charging cables when seizing mobile devices?	Mobile device batteries have a limited charge life span, and the device will need a charger to maintain the battery until the device can be processed	To reduce owner complaints about missing cables when, at some point, seized devices are returned	In those cases where evidence seized is forfeit, you want to make sure you have everything you need to operate the device	None of the above	A
183	Which of the following is NOT one of the currently available methods for extracting data from mobile devices?	Manual operation via user interface	Logical acquisition via communication port	Connecting the communication port directly to an output device such as a printer	Physical acquisition via the communication port	C
184	Forensic examiners should be aware that a mobile device with a blank or broken display:	May as well be thrown away, as no data will be recovered from it	May only indicate that the screen is damaged and it may still be possible to extract data	May require that the mobile device be sent out to the manufacturer for repairs	None of the above	B
185	A peculiarity of mobile devices is the format that they store SMS messages, which is: a	ASCII	Unicode	GSM 7-bit	Baudot	C
186	The primary reason that brute-force methods are not used when trying to access an SIM card with the PIN set is:	A four-digit PIN represents 10,000 possible combinations	After three failed attempts, the SIM card will become locked	PIN disclosure by the offender can be required by a court order	None of the above	B

187	An understanding of networks helps with which of the following:	Establishing continuity of offense	Tracking down offenders	Understanding traces of online activities left on a PC	All of the above	D
188	When a Windows system connects to a shared folder on another Windows machine on the Internet, which of the following protocols are used?	TCP/IP	SMB	NetBIOS	All of the above	D
189	Hosts that connect two or more networks are called:	Routers	Switches	Hubs	All of the above	A
190	Which of the following are Layer 7 protocols?	Ethernet	HTTP	TCP	All of the above	B
191	Ethernet uses which of the following technologies?	CDPD	CSMA/CD	CDMA	All of the above	B
192	Another name for a hub is:	Switch	Router	Concentrator	NIC	C
193	Currently, the most widely used Internet protocols are:	TCP	UDP	IP	All of the above	D
194	The OSI reference model divides Internets into seven layers Choose the correct order, by layer	Transport, Session, Network, Presentation, Data-link, Application, Physical	Presentation, Data-link, Application, Physical, Transport, Session, Network	Physical, Data-link, Network, Transport, Session, Presentation, Application	Data-link, Network, Session, Application, Physical, Network, Session	C
195	The layer that actually carries data via cables or radio signals is the:	Transport layer	Physical layer	Network layer	Data-link layer	B
196	A hub joins hosts at the physical level whereas a switch joins them at the ____ layer	Transport	Physical	Network	Data-link	D
197	The layer responsible for managing the delivery of data is the:	Application layer	Presentation layer	Transport layer	Session layer	C
198	Which of the following network technologies uses a fiber-optic medium?	Ethernet	FDDI	Asynchronous Transfer Mode	802.11	B
199	Preservation of digital evidence can involve which of the following?	Collecting computer hardware	Making a forensic image of storage media	Copying the files that are needed from storage media	All of the above	D
200	A forensic image of a drive preserves which of the following?	Memory contents	File slack and unallocated space	System date and time	Screen contents	B
201	Examination of digital evidence includes (but is not limited to) which of the following activities?	Seizure, preservation, and documentation	Recovery, harvesting, and reduction	Experimentation, fusion, and correlation	Arrest, interviewing, and trial	B

202	Analysis of digital evidence includes which of the following activities?	Seizure, preservation, and documentation	Recovery, harvesting, and reduction	Experimentation, fusion, and correlation	Arrest, interviewing, and trial	C
203	Evidence can be related to its source in which of the following ways?	Top, middle, bottom	IP address, MD5 value, filename, date-time stamps	Production, segment, alteration, location	Parent, uncle, orphan	C
204	When a website is under investigation, before obtaining authorization to seize the systems it is necessary to:	Determine where the web servers are located	Inform personnel at the web server location that you'll be coming to seize the systems	Conduct a reconnaissance probe of the target website	None of the above	A
205	Which of the following is NOT an information gathering process?	Scanning the system remotely	Studying security audit reports	Attempting to bypass logon security	Examining e-mail headers	C
206	Unlike law enforcement, system administrators are permitted to _____ on their network when it is necessary to protect the network and the data it contains	Open unread e-mails	Monitor network traffic	Modify system logs	Divulge user personal information	B
207	Although it was not designed with evidence collection in mind, _____can still be useful for examining network traffic	EnCase	FTK	Wireshark	CHKDSK	C
208	Issues to be aware of when connecting to a computer over a network and collecting information include:	Creating and following a set of standard operating procedures	Keeping a log of actions taken during the collection process	Documenting which server actually contains the data that's being collected	All of the above	D
209	Occasionally, an intrusion detection system may trigger an alarm caused by an innocent packet that coincidentally contains intrusion class characteristics This type of alert is called:	False warning	Failsafe	DEF con	False positive	D
210	Information security professionals submit samples of log files associated with certain intrusion tools to help others detect attacks on the mailing lists at:	Bugtraq	Sam Spade	CNET	Security Focus	A

211	Which of the following are situations where a bitstream copy may not be viable?	The hard drive is too large to copy	The system cannot be shut down	The digital investigator does not have authority to copy the entire drive	All of the above	D
212	Who is authorized to conduct online undercover investigations when child pornography is involved?	Anyone	Computer security professionals	Journalists	Law enforcement	D
213	Which of the following Internet services can be used to exchange illegal materials?	IRC	Usenet	KaZaa	All of the above	D
214	What are two of the most useful headers for determining the origination of Usenet messages?	From and Message-ID	NNTP-Posting-Host and X-Trace	Path and Subject	RFC1036 and RFC2980	B
215	What information should you document when searching for evidence on the Web?	Date/time of search, search engine and terms used, address of pertinent results	Screenshots of significant search results	Download copies of the webpages and calculate their MD5 value	All of the above	D
216	Why is it important to hide your identity when conducting an online investigation?	To reduce the risk of alerting the offender	To get yourself in the mindset of covert web investigating	To make it easier for you to determine the offender's location	All of the above	A
217	When it is not possible to determine the identity of the author of a Usenet message using IP addresses in the header, what else can you do to learn more about the author?	Look for unusual signature and use of language	Search the Web using distinctive aspects of posts	Look for similar Usenet messages posted using an alias	All of the above	D
218	What characteristics of IRC make it attractive to criminals?	IRC enables them to exchange illegal materials with other criminals	IRC provides them with some level of anonymity	IRC gives them direct, "live" access to a large pool of potential victims	All of the above	D
219	Which of the following enables a user to connect to IRC and run IRC fserves without disclosing their IP address?	Freenet	psybnc bot	Fserve	All of the above	B
220	Which of the following applications leave traces of Internet activities on a personal computer?	Internet Explorer	KaZaA	IRC	All of the above	D
221	Which of the following tools can reconstruct TCP streams?	Tcpdump	Wireshark	Snoop	EnCase	B

222	What peer-to-peer clients use the Fast Track network?	KaZaA	Grokster	iMesh	All of the above	D
223	Web Whacker and Httrack are examples of tools that:	Search the Web	Deface websites	Capture websites	Launch websites	C
224	Metaverseink is a:	Search tool (people or things) for virtual worlds	Newsgroup aggregator	Social networking meta-tool	A file-sharing peer-to-peer network	A
225	Second Life is one of the better known:	Research websites	Archive websites	Virtual worlds	Web-based game shows	C
226	Synchronous chat networks are particularly conducive to criminal activity because of their	Privacy	Immediacy	Impermanence	All of the above	D
227	What is the maximum cable length for a 10BaseT network?	10 feet	100 feet	10 meters	100 meters	D
228	What is the approximate theoretical maximum number of bytes that can be downloaded in one minute on a 10BaseT network?	10 Mb	75 Mb	100 Mb	175 Mb	B
229	Which of the following commands can be used to obtain the MAC address of a remote Windows computer?	Netstat	Ping	Nbtstat	Traceroute	C
230	What is the maximum cable length for a 10 base five segment?	100 feet	500 feet	100 m	500 m	D
231	ARP stands for:	Address Resource Protection	Advanced Retrieval Protocol	Address Resolution Protocol	Added Resource Processing	C
232	The best operating system for capturing network traffic on high-speed networks is:	Microsoft DOS/Windows	OpenBSD/FreeBSD	Linux	Solaris	B
233	Which of the following applications is used to capture network traffic?	Snort	Wireshark	Tcpdump	All of the above	D
234	How many bytes per packet does tcpdump capture by default?	10 bytes	68 bytes	128 bytes	1024 bytes	B
235	Which of the following tools can reconstruct TCP streams?	Tcpdump	Wireshark	Snoop	EnCase	B
236	The transition method in which only one computer can transmit while all the others listen is known as:	Baseband	Narrowband	Broadband	Sideband	A

237	Although ARP is part of TCP/IP, it is generally considered a part of the _____ layer	Physical	Data-link	Network	Transport	B
238	The form of ARP that ATM uses to discover MAC addresses is known as:	ARPATM	ATMARP	MACATM	ATMMAC	B
239	TCP is an abbreviation for:	Transit Communication Protocol	Transportation Cost Product	Transport Control Protocol	Time Communication Protocol	C
240	What system is used to convert IP addresses to their associated names?	TCP/IP	DNS	ARP	Routing	B
241	What protocol does the “ping” command use?	TCP	IP	ICMP	All of the above	C
242	Which of the following logs record the IP addresses of computers accessing an FTP server? a	Wtmp	Xferlog	Syslog	Access log	B
243	In addition to the IP address of the sender, SMTP e-mail server logs contain which of the following?	The Message ID	The time the message was received	The name of the sender	All of the above	D