1. **Explain in detail about the computer crime.**
    a. Computer crime is any criminal offense, activity or issue that involvescomputers
    b. Computer misuse tends to fall into two categories.
        i. Computer is used to commit a crime
        ii. Computer itself is a target of a crime. Computer is the victim. ComputerSecurity Incident.
    c. Computer Incident Response.
    d. **Computer Forensics** involves the preservation, identification, extraction,documentation and interpretation of computer data [1]
    e. **Computer Forensics** is the application of science and engineering to the legalproblem of digital evidence. It is a synthesis of science and law.
    f. **Computer forensics,** still a rather new discipline in computer security, focuseson finding digital evidence after a computer security incident has occurred .
    g. The goal of **computer forensics** is to do a structured investigation and find outexactly what happened on a digital system, and who was responsible for it.

Introduction

- The introduction of the **Internet** has created unparalleled opportunities for commerce, research, education, entertainment, and public discourse. A global marketplace has emerged, in which fresh ideas and increased appreciation for multiculturalism have flourished.
- The introduction of computerized encyclopedias, international consortia, worldwide connectivity, and communications has greatly enhanced quality of life for many individuals.
- Indeed, the Internet can be utilized as a window to the world, allowing individuals to satiate their curiosity and develop global consciousness. It allows individuals to experience those things that they have only dreamed about.
- Interested parties can visit the Louvre, devouring priceless artifacts at their leisure or take an African safari without the heat or mosquitoes. They can find answers to the most complex legal or medical questions or search for their soul mates.
- They can download coupons for their favorite restaurants or search for recipes to their favorite dishes.
- In addition, individuals, corporations, public organizations, and institutions can more effectively advertise their products or services, using graphically highlighted information and providing links to supplemental information or support.

- In fact, computerized access to unprecedented information has cut across traditional boundaries of communication.

Cyberspace and Criminal Behavior

- ✓ Cyberspace may be defined as the indefinite place where individuals transact and communicate. It is the place between places.
- ✓ Telephonic conversations, occurring across time and space, were pre-dated by wire exchanges. However, the new medium known as the Internet has monumentally increased the **physicality** of the virtual world, outpaced only by the exponential growth in the number of users.
- ✓ No other method of communication converges audio, video, and data entities so effectively.

✓ Unlike traditional methods, the Internet combines mail, telephone, and mass media. As stated previously, it exposes individuals to a myriad of new ideas and may serve as a social gathering place, a library, or a place to be alone.

- ✓ In fact, the two created the **Electronic Frontier Foundation** (EFF) offering to –fund**,** conduct**,** and support legal efforts to demonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive and unconstitutional.‖

✓ While early actions by the U.S. Secret Service may validate some of these early concerns, the efforts of the EFF have often overlooked the negative potentiality of this global marketplace that has reunited a society that had increasingly removed itself through suburbanization. Just as the Industrial Revolution enhanced threats to national security and created an environment conducive to street/predatory crime through the concentration of the urban population, the **Information** or **Digital Revolution** has created a new forum for both terrorist activity and criminal behavior. Indeed, this latest technological era has exacerbated the vulnerabilities of government institutions and personal residences alike. Critical infrastructures, increasingly characterized by tight couplings and interdependency of IT, emergency services, public utilities, banking sectors, food supplies, and transportation systems, have resulted in an interconnectivity inconsistent with traditional security strategies. Such myopia has similarly impacted private citizens who have failed to employ rudimentary measures of cyberprotection even as they add additional doorlocks and alarm systems to insulate themselves from physical attacks.

Clarification of Terms

- ✓ Just as debates rage over the appropriate codification of crime committed via electronic means, controversy surrounds the actual semantics associated with the phenomenon.
- ✓ For clarification purposes, then, it is necessary to define the historical usage of terms associated with technological or electronic crimes. **Computer crime** has been traditionally defined as any criminal act committed via computer. **Computer-related crime** has been defined as any criminal act in which a computer is involved, even peripherally.
- ✓ **Cybercrime** has traditionally encompassed abuses and misuses of computer systems or computers connected to the Internet which result in direct and/or concomitant losses. Finally, **digital crime,** a relatively new term, includes any criminal activity which involves the unauthorized access, dissemination, manipulation, destruction, or corruption of electronically stored data. As data may be accessed or stored in a variety of ways and in a variety of locations, *digital crime* may be characterized as any of the three depending on case characteristics.

- ✓ While *computer crime* and *computer related crime* will be used interchangeably throughout the text, *cybercrime* will only be used to describe that criminal activity which has been facilitated via the Internet.
- ✓ Just as confusion exists regarding the appropriate terminology for crimes involving computers, the nomenclature of the science developed to investigate such activity lacks universality.
- ✓ For clarification purposes in this text, **computer forensic science, computer forensics, and digital forensics** may be defined as the methodological, scientific, and legally sound process of examining computer media and networks for the identification, extraction, authentication, examination, interpretation, preservation, and analysis of evidence.

2. What is E-Cash in E-Commerce?

An anonymous e-cash system is equivalent to cash and private bank notes except that it is transferred through the network with bits of information. In essence, it is just another representation of monitory value.

How E-Cash is Used?

E-Cash is used over the internet, email, or personal computer to other workstations in the form of secured payments of cash that is virtually untraceable to the user. The way electronic cash works are similar to that of e-fund transfer done between banks.

The user first must have an electronic cash software program and an electronic cash bank account from which electronic cash can be withdrawn or deposited. The user withdraws the electronic cash from the account onto his/her computer and spends it on the internet without being placed or having personal information available to other parties that are involved in the process. The receipts of the e-cash send the money to their bank account similar to depositing real cash in the bank.

Properties of Electronic-Cash?

- Cash has a value it can be traded for goods or services.
- Previous owners of the cash are not known and in general it is not possible to keep track of by who and where the cash is spent that means it is annoymous.
- It is a secure cash currency is specifically designed to detect conter-filtering.

Requirenment of E-Cash?

- Privacy
- Security
- Hardware implementation
- Acceptability
- Transferbility
- Divisibility

E-Cash Advantages and Disadvantages

Advantages:

- It is easy to use
- Can we used for small payment
- Flexible
- Can be operate from anywhere with the help of online device

Disadvantages:

- Security Risk
- Not Accepted Everywhere

3. Explain in detail about the Traditional problems associated with Computer Crime.

8. Physicality and Jurisdictional Concerns
9. Perceived Insignificance, Stereotypes, and Incompetence
10. Prosecutorial Reluctance
11. Lack of Reporting
12. Lack of Resources
13. Jurisprudential Inconsistency
14. Jurisprudential Inconsistency

Physicality and Jurisdictional Concerns

- The physical environment that breeds computer crime is far different from traditional venues.
- In fact, the intangible nature of computer interaction and subsequent criminality poses significant questions for investigative agents.

- The lack of physical boundaries and the removal of traditional jurisdictional demarcations allow perpetrators to commit multinational crime with little fear (or potential) of judicial sanctions.
- For the first time, criminals can cross international boundaries without the use of passports or official documentation.
- Whereas traditional criminal activity required the physical presence of the perpetrators, cybercrime is facilitated by international connections that enable individuals to commit criminal activity in England while sitting in their offices in Alabama. In addition, electronic crime does not require an extensive array of equipment or tools.

Perceived Insignificance, Stereotypes, and Incompetence

- Investigators and administrators have displayed great reluctance to pursue computer criminals.
- A lack of knowledge coupled with general apathy toward cyber criminality has resulted in an atmosphere of indifference.
- Many stereotype computer criminals as nonthreatening, socially challenged individuals (i.e., nerds or geeks) and fail to see the insidious nature of computer crime;
- In addition, those administrators and investigators who grudgingly admit the presence and danger of electronic crime tend to concentrate exclusively on child pornography, overlooking motivations and criminal behaviors apart from sexual gratification.
- Even in situations where law enforcement authorities recognize the insidious nature of computer or cybercrime, many do not perceive themselves or others in their department to be competent to investigate such criminal activity.

Prosecutorial Reluctance

- As media focus has increasingly highlighted the dangers of cyberspace, including those involving cyber bullying and child exploitation, public awareness has heightened an urgency to protect children's virtual playgrounds.
- In response, federal and state resources have often been allocated to fund specialized units to investigate and prosecute those offenses which affect the safety of American children.
- For example, the Federal Bureau of Investigation maintains a partnership with the Child Exploitation and Obscenity Section of the Department of Justice.
- This organization is composed of attorneys and computer forensic specialists who provide expertise to U.S. Attorney's Offices on crimes against children cases.

Lack of Reporting

- The number of reported incidents handled by Carnegie-Mellon University's

Computer Emergency Response Team (CERT) has increased threefold, from 24,097 in 2006 to 72,065 in 2008.13 In their annual survey, *CSO Magazine* (in conjunction with the U.S. Secret Service; CERT, and Deloitte) reported that 58 percent of the organizations surveyed perceived themselves to be more prepared to prevent, detect, respond to, or recover from a cybercrime incident compared to the previous year.

- However, only 56 percent of respondents actually had a plan for reporting and responding to a crime.14 In 2011, it was reported that over 75 percent of all insider intrusions were handled internally without notification of authorities.
- Underreporting on the part of businesses and corporations may be attributed to a variety of reasons, but perhaps the most common are exposure to financial losses, data breach liabilities, damage to brand, regulatory issues, and loss of consumer confidence.
- Contemporary society, characterized by increased reliance on paperless transactions, demands assurances that the company's infrastructure is invulnerable and that confidential information remains inviolate.

Lack of Resources

- Computer intrusions have proven to be problematic within the corporate world, such institutions' unwillingness or inability to effectively communicate with judicial authorities has led to an increase in computer crime.
- Unfortunately, law enforcement and corporate entities desperately need to cooperate with one another.
- Unlike their civil service counterparts, the business communities have the resources (both financial and legal) necessary to effectively combat computer crimes.
- First, these companies, through their system administrators, have far more leeway in monitoring communications and system activities, and they have the ability to establish policies which enable wide-scale oversight.

Jurisprudential Inconsistency

- Unfortunately, the Supreme Court has remained resolutely averse to deciding matters of law in the newly emerging sphere of cyberspace.
- They have virtually denied cert on every computer privacy case to which individuals have appealed and have refused to determine appropriate levels of Fourth Amendment protections of individuals and computer equipment.
- This hesitation has become even more pronounced with the emergence of wireless communications, social networking sites, and smart phones.
- As such, obvious demarcations of perception, application, and enforcement of computer crime laws vary widely across the country, and

a standard of behavior in one jurisdiction may supersede or even negate legal standards in another.

- Traditionally, trial and appellate courts evaluated the constitutionality of computer crime statutes, searches, and investigations through the lens of the First and Fourth Amendment.
- Evaluating appropriate boundaries for free speech and establishing standards of reasonableness have varied across state and federal rulings, and an inconsistent patchwork of guidelines has resulted.

4. Explain in detail about the Identify theft and identify fraud.

- The generic term **identity theft** has been utilized to describe any use of stolen personal information. However, such characterization fails to provide a comprehensive picture of the totality of possibilities surrounding that construct known as *identity.*
- Identity fraud, which encompasses identity theft within its purview, may be defined as the use of a vast array of illegal activities based on fraudulent use of identifying information of a real or fictitious person.

Typologies of Identity Theft/Fraud

a. Assumption of Identity

b. Theft for Employment and/or Border Entry

c. Criminal Record Identity Theft/Fraud

d. Virtual Identity Theft/Fraud

e. Credit Identity Theft/Fraud

a. Assumption of Identity

- This is the rarest form of identity theft/fraud and occurs when an individual simply assumes the identity of his or her victim, including all aspects of the victim's lives.
- It must be noted that this type of activity is atypical as it is significantly more difficult to accomplish.
- Even if a thief could identically duplicate the physical characteristics and appearance of his intended target, the likelihood of mastering personal histories, intimate relationships, and communication nuances is extremely remote.
- However, it is important to note that this type of identity fraud has occurred even in cases where the plausibility of such assumption borders on the ridiculous.

b. Theft for Employment and/or Border Entry

- This type of identity theft/fraud is increasingly common due to the growth of illegal immigration and alien smuggling. It involves the fraudulent use of stolen or fictitious personal information to obtain employment or to gain entry into the United States.
- The documents most frequently intercepted by officials included alien

registration cards, nonimmigrant visas, passports and citizenship documents, and border crossing cards. These documents were presented by aliens who were attempting to enter the United States in search of employment or other immigration benefits, like naturalization or permanent residency status.

Here are some recent examples of identity theft for employment:

• **2008—Agriprocessors,** Inc.—CEO, company managers, and human resource employees were charged with multiple counts of federal immigration violations. Among other charges, the meat processing company was charged with harboring illegal aliens for profit, document fraud, bank fraud, and aggravated identity theft.

• **2009—George's Processing**, Inc.—Company paid nearly half a million dollars after 136 illegal aliens were found working at the Missouri plant.

• **2008—Columbia** Farms—Approximately 300 individuals, including eleven supervisors and one human resources manager, were arrested by federal authorities after a ten-month investigation revealed charges relating to identity theft for employment. The arrests in Greenville, South Carolina, followed earlier arrests of nearly two dozen plant managers.

Criminal Record Identity Theft/Fraud

- This type is often overlooked in discussions of identity theft, perhaps because it is not as common or because the immediate financial repercussions are not significant.
- It has been used historically by individuals attempting to evade capture or criminal prosecution.
- **Reverse criminal record identity theft** occurs when a criminal uses a victim's identity not to engage in criminal activity but to seek gainful employment. Unfortunately, criminal record identity theft/fraud is especially insidious as it often remains undiscovered until the victim is pulled over for a routine traffic violation. Unlike other types of identity fraud, in this case many victims are horrified to discover that they have been victimized by a friend or relative.

d. Virtual Identity Theft/Fraud

Virtual Identity Theft/Fraud

- A relatively new phenomenon, virtual identity theft/fraud involves the use of personal, professional, or other dimensions of identity toward the development of a fraudulent virtual personality.
- As in the previous types discussed, motivations range from the relatively innocuous to extreme malevolence.

- Unlike physical identities which are tied to social networks, legal documentation, and biological characteristics, virtual identities are largely personally constructed.
- Indeed, many individuals develop a virtual identity which is antithetical to their physical one—making themselves taller, richer, younger, more charismatic, and so on.
- In other words, virtual identities are often far removed from reality.
- As such, they are inherently less veracious and less trustworthy. They are often used for online dating, role-playing, and accessing deviant sites or locations containing questionable content.
- Although many individuals create virtual identities to explore forbidden areas or satisfy their curiosity behind a veil of anonymity, most do not cross the line between the legal and the illegal worlds.

Credit Identity Theft/Fraud

- It may be defined as the use of stolen personal and financial information to facilitate the creation of fraudulent accounts.
- This definition, specific by design, requires the affirmative act of securing additional credit.
- It does not include traditional activities like the illegal use of a stolen credit card, as that activity is more appropriately situated under statutes concerning credit card fraud.
- It is also not defined under identity theft, as the primary incentive is instant gratification.
- As credit cards are treated as cash by consumers and merchants alike, the use of a stolen one may be likened to purse snatching or pick-pocketing without physical contact.

Physical Methods of Identity Theft

a. Mail Theft
b. Dumpster Diving
c. Theft of Computers
d. Bag Operations
e. Child Identity Theft
f. Insiders
g. Fraudulent or Fictitious Companies

h. Card Skimming, ATM Manipulation, and Fraudulent Machines

a. Mail Theft

- Although it is hard to identify which method of identity theft/fraud is most commonly employed, the theft of information from physical mailboxes is certainly one of the most common.
- Unfortunately, numerous documents containing personal and financial information are deposited in unlocked containers on the side of the road until it is retrieved.
- Oftentimes, such retrieval is conducted by someone other than the intended recipient and is used to generate illicit profit or to facilitate criminal activities. Physical mailboxes can contain a plethora of valuable information.
- Even as the government cautions citizens to take measures to protect their personal and financial information, they themselves are delivering government identification documents through U.S. Mail. Many times, they even mail breeder documents.

Some Instances of Compromised Data

Date	Institution	Type of Breach	Number of Victims
2011	Sutter Physicians Services	Theft of computer	3.3 million
2011	NASDAQ	Hack (cyberattack)	10 thousand
2011	SONY	Hack (cyberattack)	100 million
2011	Epsilon	Hack (cyberattack)	50–60 million
2011	Tricare	Theft of tapes	4.9 million
2011	University of Hawaii	Hack (cyberattack)	98 thousand
2011	Yale University	Accidental Web disclosure	43 thousand
2011	Texas comptroller	Accidental Web disclosure	3.5 million
2011	Ohio State University	Hack (cyberattack)	760 thousand

Dumpster Diving

- As the name implies, dumpster diving is the practice of sifting through commercial or residential trash or waste for information deemed valuable. Such information ranges widely, but may include account numbers, social security or tax payer identification numbers, and passwords.
- It may be located on discarded computer media or in paper form, and may be housed in personnel records, accounting spreadsheets, receipts, invoices, or the like.

- Fortunately, both consumers and businesses have increasingly taken measures to prevent the misuse of discarded information. Many now employ paper shredders and disk-wiping software.
- Diving for information has been practiced by criminals and law enforcement alike. Early hackers found the trash to be especially helpful toward their exploitation of computer vulnerabilities. Passwords, computer systems, and software could be located there.

Theft of Computers

- Physical theft of computers is among the most common techniques employed by identity thieves, as it alleviates the need to analyze and organize voluminous paper documents.
- As the majority of individuals necessarily store personal information on their computer, identity fraudsters are all but guaranteed a score.
- Even those individuals without technical expertise recognize that the computer as a warehouse of information has significant value on the black market, even if they themselves are incapable of retrieving the data.
- Areas vulnerable to such activity are limited only by the criminal mind.

Bag Operations

- Another tactic historically utilized by intelligence agents which is currently used by identity thieves and fraudsters is known as a –bag operation,‖ and it involves the surreptitious entry into hotel rooms to steal, photograph, or photocopy documents; steal or copy magnetic media; or download information from laptop computers.
- Almost routine in many countries, bag operations are typically conducted by the host government's security or intelligence services, frequently with the cooperation of the hotel staff. They are most often committed when guests leave their room.

Child Identity Theft

- Increasingly, law enforcement authorities are reporting startling numbers of parents stealing their children's identities. According to the Federal Trade Commission, more than 140,000 children were victims of identity theft in 2011.28 This represented a marked increase in numbers released by the same group in 2003.

- Unfortunately, this type of identity theft or fraud is especially difficult to recognize and prosecute.
- The primary problem, of course, is the delayed identification of the victimization, as credit reports are usually not generated until the first application for credit, which usually occurs after the individual reaches the age of 18.
- Second, the theft itself is not characterized as either child abuse or exploitation, so the primary investigative agency for children

Insiders

- Many authorities suggest that corporate and government insiders pose the greatest risk to identity theft. As in other areas of computer crime, motivations vary and the facilitation of fraud is not always intentional.
- In fact, careless employees account for a large amount of the identity theft in the United States. Such negligence has been committed by both individual employees and corporate divisions.
- In 2005, for example, Bank of America reported that the personal information of 1.2 million U.S. government employees, including U.S. senators, had been compromised when tapes were lost during shipment. In the same year, CitiGroup reported that UPS had lost the personal financial information of nearly 4 million Citigroup customers.

Fraudulent or Fictitious Companies

- Recently, a more sophisticated method of identity theft/fraud involves the creation of shell companies.
- Almost always conducted by an organized ring of criminals, fake companies are established which are engaged in the processing or collection of personal financial information.
- These fictitious businesses range from debt collection to insurance agents. In a highly visible case, over 145,000 consumers were put at risk by Choice point, an Atlanta-based company, which is one of the largest data aggregators and resellers in the country.
- Among other things, it compiles, stores, and sells information on the vast majority of American adults with over 19 billion records.

Card Skimming, ATM Manipulation, and Fraudulent Machines

- A more sophisticated method of data theft involves the reading and recording of

Personal information encoded on the magnetic strip of an automated teller machine (ATM) or credit card.

- Once stored, the stolen data is re-coded onto the magnetic strip of a secondary or dummy card.
- This process, known as card skimming, results in a dummy card, which is a full-service credit or debit card indistinguishable from the original while purchasing.
- While card skimming was traditionally reserved to facilitate credit card fraud, it is increasingly being employed with the collection of other personal informationto create additional accounts.
- Card **skimmers** come in a variety of shapes and sizes (most often miniaturized cameras or copiers and can be mounted on retail and ATMs).
- In some cases, thieves have actually developed fraudulent ATMs. Thus, consumers are strongly encouraged to only use those machines that are maintained by financial institutions, and to be alert for any suspicious equipment or appendage.