# *Information Security (CP3404)*

## Chapter 13 – Business Continuity

Based on the Fifth Edition of:

M. Ciampa:. *CompTIA® Security + Guide to Network Security Fundamentals*

Department of Information Technology, College of Business, Law & Governance

# Learning Objectives

- Define environmental controls
- Describe the features of a disaster recovery plan
- Explain different environmental controls
- Describe forensics and incident response procedures

# Outline

# Preface

- Earthquake, tsunamis, tornado, hurricanes, floods, and other natural disasters can have a major impact on business around the world
- In addition acts of nature, sabotage, acts of terrorism, and even acts on information technology can quickly bring a business to its knees or put it out of operation entirely
- Many organizations are completely unprotected
- Many organizations that do have plans on paper have never tested those plans to determine whether they would truly bring the business through an unforeseen event

# Business Continuity

## What is Business Continuity?

- Business Continuity – Ability of organization to maintain operations and services in face of disruptive event
- Business Continuity Planning and Testing – Process of identifying exposure to threats, creating preventive and recovery procedures, and testing to determine if sufficient
- Continuity of Operations – Ensuring an organization can continue to function in event of natural or human-made disaster

# Business Continuity

## Business Continuity Tools

- Succession Planning – Determining in advance who will be authorized to take over in the event of the incapacitation or death of key employees
- Business Impact Analysis (BIA) – Identifies mission-critical business functions and quantifies impact loss of functions may have on organization's operational and financial position
- Risk Assessment – Analyzing the risk in the context of business continuity

# Disaster Recovery

## Disaster Recovery

- Information Technology (IT) Contingency Planning – Developing outline of procedures to be followed in event of major IT incident (a denial-of-service attack) or incident that directly impacts IT (a building fire)
- Disaster Recovery Plan (DRP) – Restoring IT functions and services to former state
- Disaster recovery involves:
  - Disaster Recovery Plans
  - Redundancy and Fault Tolerance
  - Data Backups

# Disaster Recovery

## Disaster Recovery Plan (DRP)

- Disaster Recovery Plan (DRP) – Written document detailing process for restoring IT resources following a disruptive event
- Common features of most disaster recovery plans:
  1. Purpose and Scope
  2. Recovery Team
  3. Preparing for a Disaster
  4. Emergency Procedures
  5. Restoration Procedures
- A good DRP should contain sufficient details (see Figure 13-1)

# Disaster Recovery

**COMMUNICATIONS ROOM**

The purpose of a communications room is to provide a central point of contact and coordination. The telephone equipment in this room will include the following:

- Three wired telephones
- Four fully charged cellular telephones
- One satellite telephone

Media communications in this room will include the following:

- One television
- One standard radio
- One police radio
- One Citizens' Band radio
- One DVD player/recorder

This room should be isolated from other functional areas and only authorized personnel will be allowed to enter.

**Figure 13-1** Sample excerpt from a DRP

# Disaster Recovery

## Disaster Recovery Plan (DRP) — Exercises

- Disaster exercises designed to test effectiveness of DRP
- Objectives of disaster exercises:
  - Test efficiency of interdepartmental planning and coordination in managing a disaster
  - Test current procedures of DRP
  - Determine strengths and weaknesses in responses
- Tabletop exercises – Exercises simulate emergency situation but in informal and stress-free environment (see Table 13-1)

# Disaster Recovery

| Feature | Description |
|---|---|
| Participants | Individuals on a decision-making level |
| Focus | Training and familiarizing roles, procedures, and responsibilities |
| Setting | Informal |
| Format | Discussion guided by a facilitator |
| Purpose | Identify and solve problems as a group |
| Commitment | Only moderate amount of time, cost, and resources |
| Advantage | Can acquaint key personnel with emergency responsibilities, procedures, and other members |
| Disadvantage | Lack of realism; does not provide true test |

**Table 13-1** Features of tabletop exercises

# Disaster Recovery

## Redundancy and Fault Tolerance

- Single Point of Failure – Component or entity which will disable the entire system if it no longer functions
- Remove single point of failure results in high availability (system that can function for extended period of time with little downtime)
- Availability often expressed as percentage uptime in one year (see Table 13-2)

# Disaster Recovery

| Percentage | Name | Weekly downtime | Monthly downtime | Yearly downtime |
|---|---|---|---|---|
| 90 | One Nine | 16.8 hours | 72 hours | 36.5 days |
| 99 | Two Nines | 1.68 hours | 7.20 hours | 3.65 days |
| 99.9 | Three Nines | 10.1 minutes | 43.2 minutes | 8.76 hours |
| 99.99 | Four Nines | 1.01 minutes | 4.32 minutes | 52.56 minutes |
| 99.999 | Five Nines | 6.05 seconds | 25.9 seconds | 5.26 minutes |
| 99.9999 | Six Nines | 0.605 second | 2.59 seconds | 31.5 seconds |

**Table 13-2** Percentages and downtimes

# Disaster Recovery

## Redundancy and Fault Tolerance

- Mean time to recovery (MTTR) – Average amount of time takes device to recover from non-terminal failure
- Some systems designed to have MTTR of zero (redundant components that can take over the instant the primary component fails)
- Redundancy planning involves redundancy for:
  - Servers
  - Storage
  - Networks
  - Power and Sites

# Disaster Recovery

## Redundancy and Fault Tolerance — Servers

- Some organizations stockpile spare parts for servers or have redundant servers
- Clustering – Combining two or more devices to appear as one single unit
- Server cluster – Combination of two or more servers that are interconnected to appear as one
- Servers are connected through:
  - Public cluster connection – Clients see them as single unit
  - Private cluster connection – Servers can exchange data when necessary (see Figure 13-2)

# Disaster Recovery

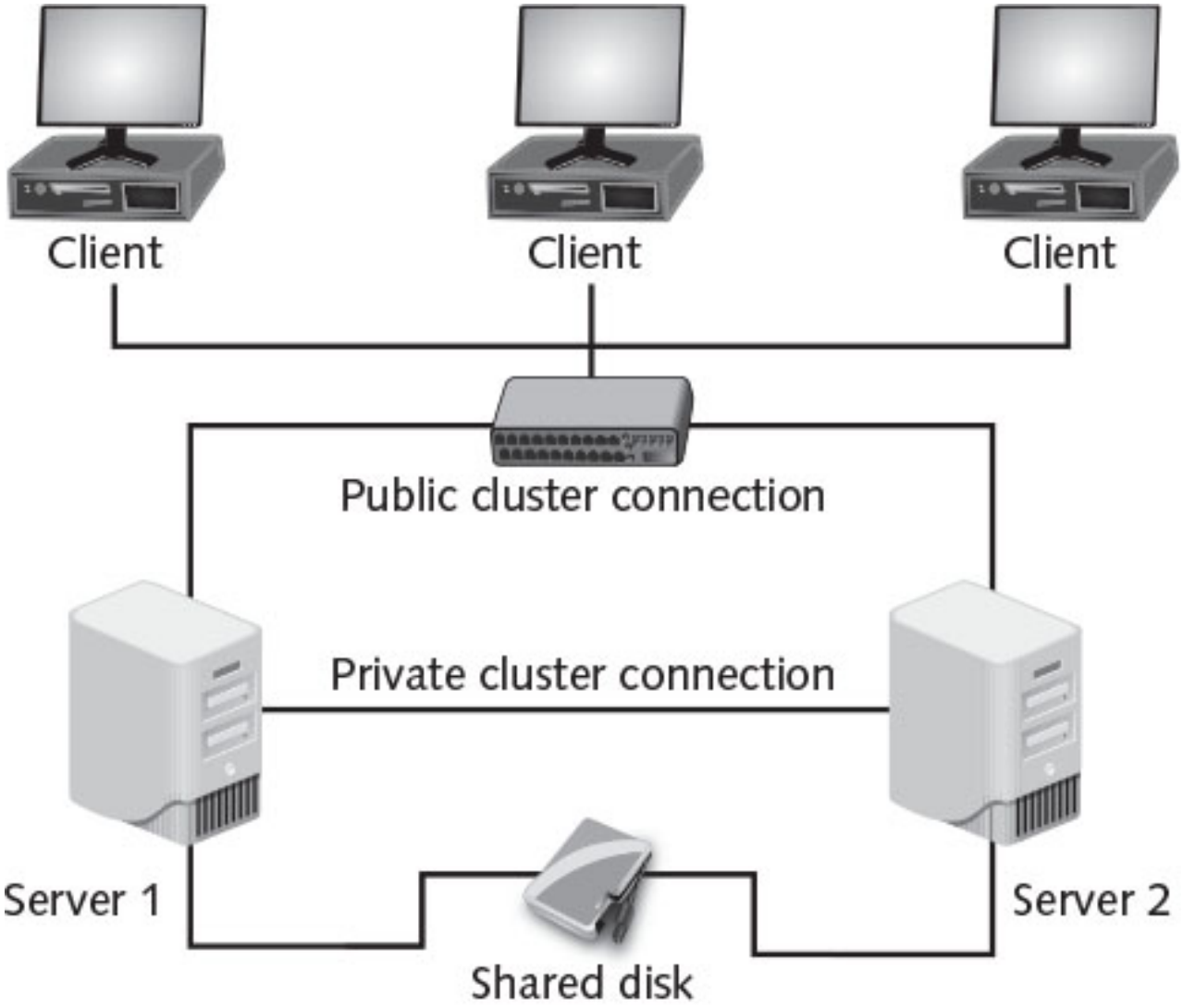


**Figure 13-2** Server cluster

# Disaster Recovery

## Redundancy and Fault Tolerance — Servers

- Asymmetric server cluster – Standby server exists only to take over for another server in event of failure; standby server performs no useful work other than to be ready if it is needed
- Symmetric server cluster – Every server in cluster performs useful work; if one server fails, remaining servers continue to perform their normal work as well as that of failed server

# Disaster Recovery

## Redundancy and Fault Tolerance — Storage

- Data storage technologies for computers today uses both solid-state drives (SSDs) and traditional Hard Disks Drives (HDDs)
- HDDs often first components to fail
- Some organizations keep spare hard drives on hand
- Mean time between failures (MTBF) – Measures average time until component fails and must be replaced
- Can be used to determine number of spare hard drives organization should keep

# Disaster Recovery

## Redundancy and Fault Tolerance — Storage

- Instead of waiting for hard drive to fail, more proactive approach can be used
- Redundant Array of Independent Devices (RAIDs) – Uses multiple hard disk drives to increase reliability and performance
- Can be implemented through software or hardware
- Several levels of RAID exist

# Disaster Recovery

## Redundancy and Fault Tolerance — Storage (RAID Level 0)

- RAID Level 0 (striped disk array without fault tolerance)
- Striping partitions hard drive into smaller sections
- Data written to the stripes is alternated across the drives
- If one drive fails, all data on that drive is lost (see Figure 13-3)

# Disaster Recovery

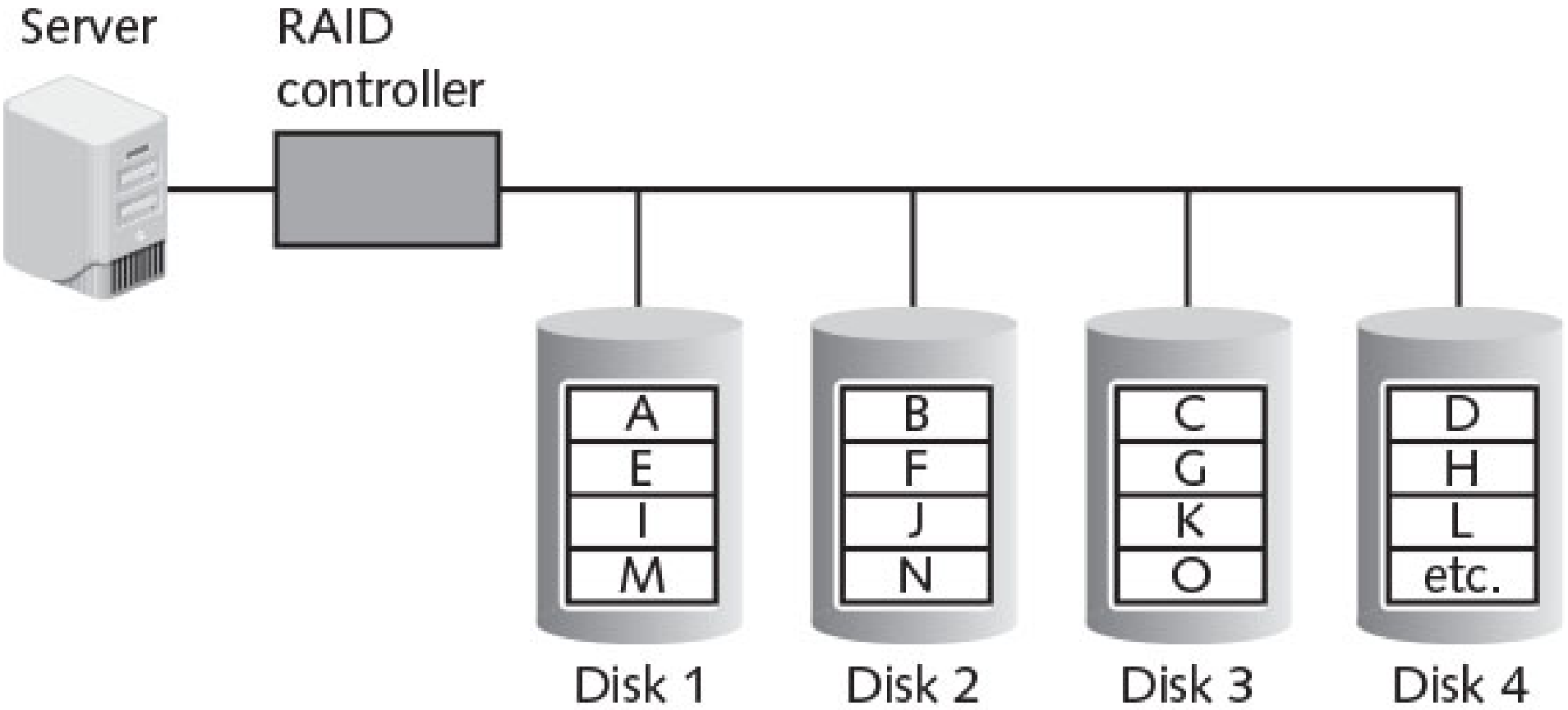


**Figure 13-3** RAID Level 0

# Disaster Recovery

## Redundancy and Fault Tolerance — Storage (RAID Level 1)

- RAID Level 1 (mirroring)
- Disk mirroring used to connect multiple drives to the same disk controller card
- Action on primary drive is duplicated on other drive
- Primary drive can fail and data will not be lost (see Figure 13-4)

# Disaster Recovery

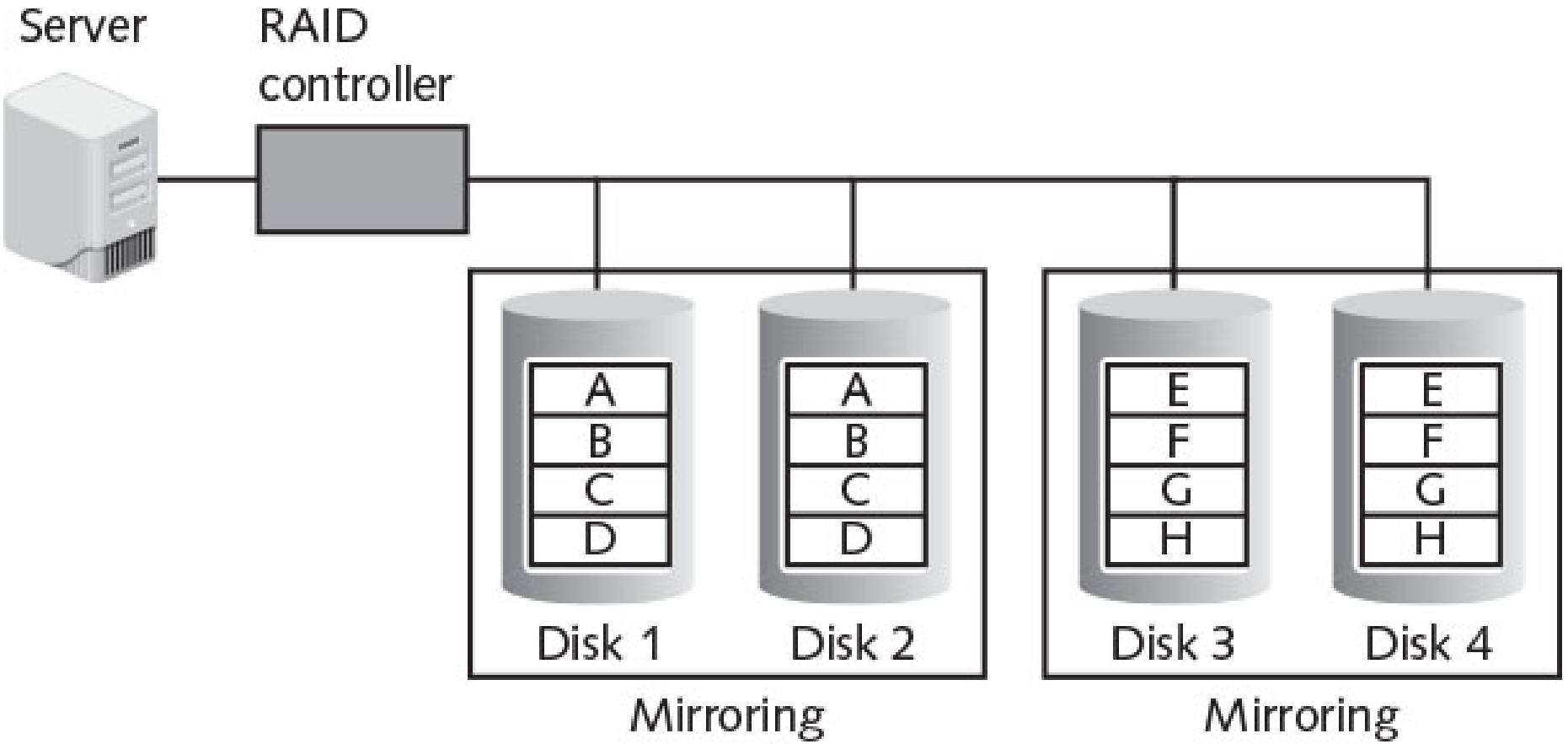


**Figure 13-4** RAID Level 1

# Disaster Recovery

## Redundancy and Fault Tolerance — Storage (RAID Level 5)

- RAID Level 5 (independent disks with distributed parity)
- Distributes parity (error checking) across all drives
- Data stored on one drive and its parity information stored on another drive (see Figure 13-5)

# Disaster Recovery

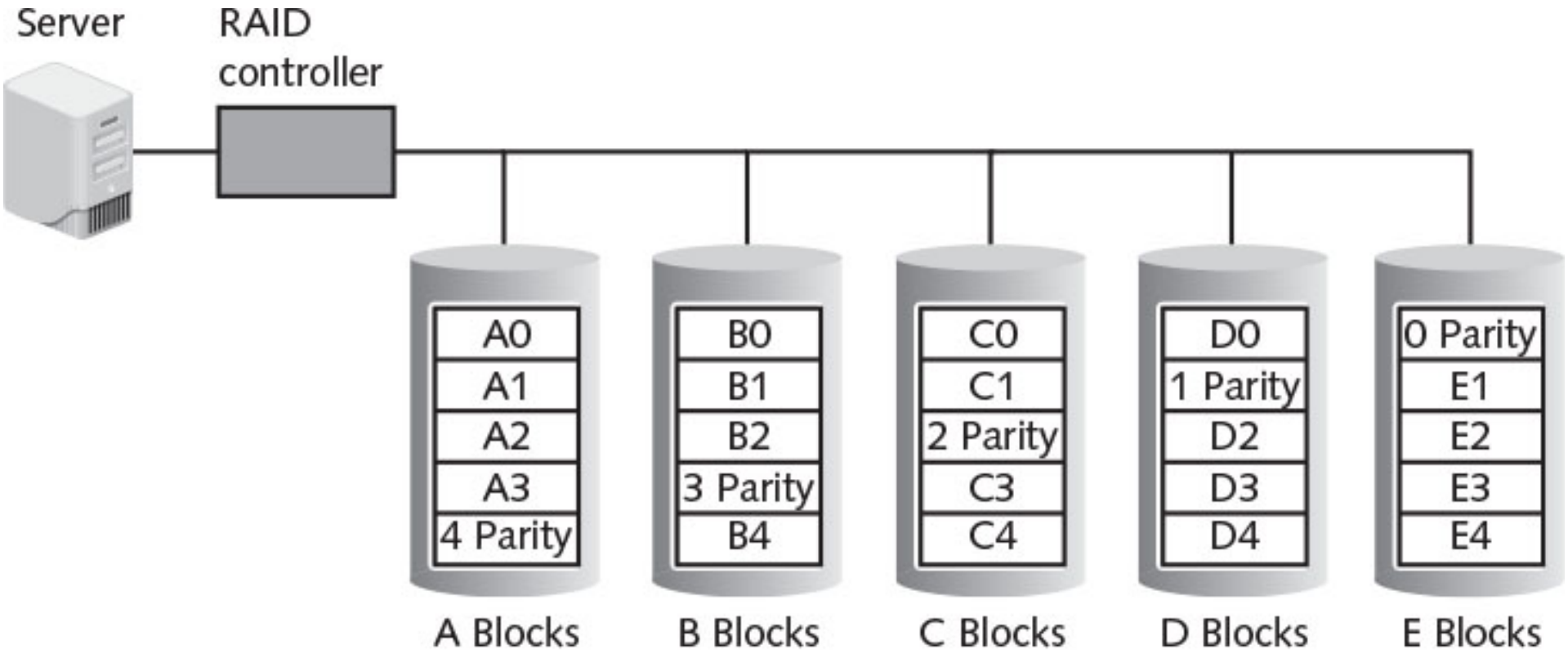


**Figure 13-5** RAID Level 5

# Disaster Recovery

## Redundancy and Fault Tolerance — Storage (RAID Level 0+1)

- RAID 0+1 (high data transfer)
- Nested-level RAID
- Mirrored array (i.e., RAID Level 1) whose segments are RAID 0 arrays
- Can achieve high data transfer rates (see Figure 13-6)

Table 13-3 summarizes the common levels of RAID

# Disaster Recovery

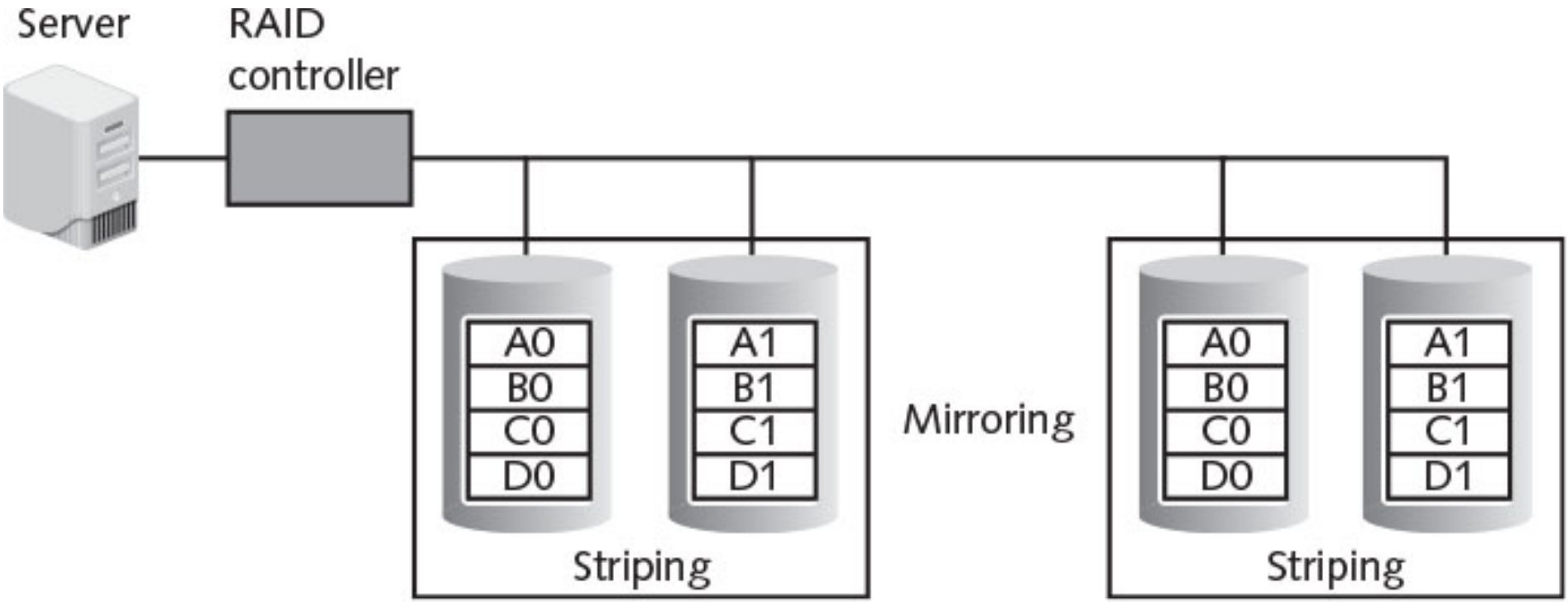


**Figure 13-6** RAID Level 0+1

# Disaster Recovery

| RAID level | Description | Minimum number of drives needed | Typical application | Advantages | Disadvantages |
|---|---|---|---|---|---|
| RAID Level 0 | Uses a striped disk array so that data is broken down into blocks and each block is written to a separate disk drive | 2 | Video production and editing | Simple design, easy to implement | Not fault-tolerant |
| RAID Level 1 | Data written twice to separate drives | 2 | Financial | Simplest RAID to implement | Can slow down system if RAID controlling software is used instead of hardware |
| RAID Level 5 | Each entire data block is written on a data disk and parity for blocks in the same rank is generated and recorded on a separate disk | 3 | Database | Most versatile RAID | Can be difficult to rebuild if a disk fails |
| RAID Level 0+1 | A mirrored array with segments that are RAID 0 arrays | 4 | Imaging applications | High input/ output rates | Expensive |

**Table 13-3** Common RAID levels

# Disaster Recovery

## Redundancy and Fault Tolerance — Network

- Redundant networks may be necessary due to critical nature of connectivity today
- Wait in the background during normal operations
- Use a replication scheme to keep live network information current
- Launches automatically in the event of a disaster
- Hardware components are duplicated
- Some organizations contract with a second Internet service provider (ISP) as a backup

# Disaster Recovery

## Redundancy and Fault Tolerance — Power

- Uninterruptible power supply (UPS) – Maintains power to equipment in the event of an interruption in primary electrical power source
- Offline UPS:
  - Least expensive, simplest solution
  - Charged by main power supply
  - Begins supplying power quickly when primary power is interrupted
  - Switches back to standby mode when primary power is restored

# Disaster Recovery

## Redundancy and Fault Tolerance — Power

- Online UPS:
  - Online UPS always running off its battery while main power runs battery charger
  - Not affected by dips or sags in voltage
  - Can serve as a surge protector
  - Can communicate with the network operating system to ensure orderly shutdown occurs
  - Can only supply power for a limited time

# Disaster Recovery

## Redundancy and Fault Tolerance — Sites

- Just as redundancy can be planned for servers, storage, networks, and power, it also can be planned for the entire site
- Backup sites may be necessary if flood, hurricane, or other major disaster damages buildings
- Three (3) basic types of redundant sites are used:
  1. Hot Site
  2. Cold Site
  3. Warm Site

# Disaster Recovery

## Redundancy and Fault Tolerance — Sites (Hot Site)

- Hot site – Run by a commercial disaster recovery service
- Duplicate of the production site
- Has all needed equipment
- Data backups can be moved quickly to the hot site

# Disaster Recovery

## Redundancy and Fault Tolerance — Sites (Cold Site)

- Cold site – Provides office space but customer must provide and install all equipment needed to continue operations
- No backups immediately available
- Less expensive than a hot site
- Takes longer to resume full operation

# Disaster Recovery

## Redundancy and Fault Tolerance — Sites (Warm Site)

- Warm site – All equipment is installed but no active Internet or telecommunications facilities
- No current data backups
- Less expensive than a hot site
- Time to turn on connections and install backups can be half a day or more

# Disaster Recovery

## Redundancy and Fault Tolerance — Sites (Cloud)

- Growing trend is use cloud computing in conjunction with sites
- Some organizations back up their applications and data to cloud and if disaster restore it to hardware in a hot, cold, or warm site
- Other organizations, instead of restoring to hardware at a site, restore to virtual machines in cloud, which then can be accessed from almost any location
- Reduces or even eliminates the need for maintaining sites

# Disaster Recovery

## Data Backups

- Data backup – Copying information to a different medium and storing offsite to be used in event of disaster
- Questions to ask when creating a data backup:
  1. What information should be backed up?
  2. How often should it be backed up?
  3. What media should be used?
  4. Where should the backup be stored?
  5. What hardware or software should be used?

# Disaster Recovery

## Data Backups — Files to Backup and Types of Backups

- Backup software can internally designate which files have already been backed up
- Archive bit set to 0 in file properties (see Figure 13-7)
- If file contents change, archive bit is changed to 1
- Three (3) basic types of backups:
  1. Full backup
  2. Differential backup
  3. Incremental backup
- Archive bit is not always cleared after each type of backup to provide additional flexibility (see Table 13-4)

# Disaster Recovery

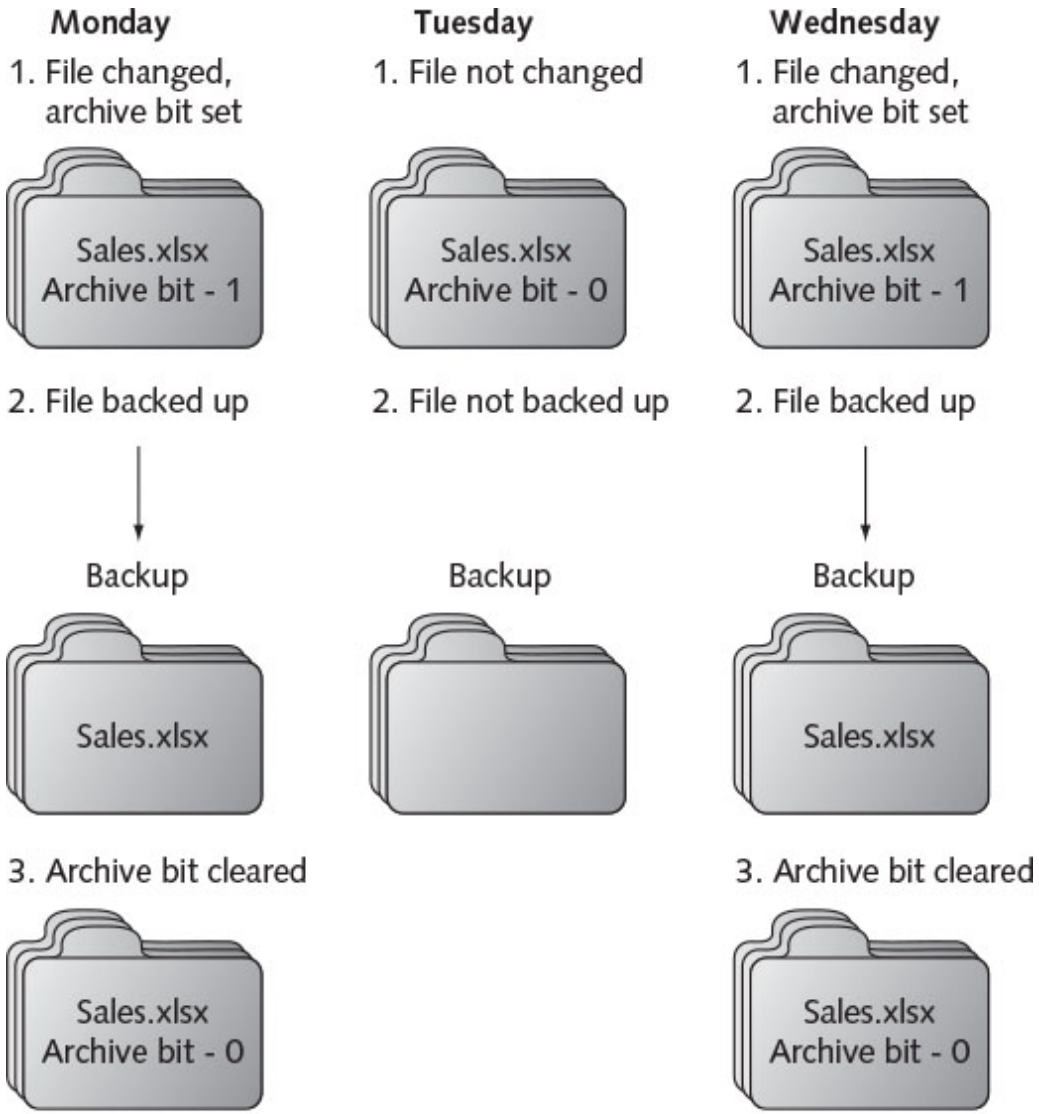


**Figure 13-7** Archive bit

# Disaster Recovery

| Type of backup | How used | Archive bit after backup | Files needed for recovery |
|---|---|---|---|
| Full backup | Starting point for all backups | Cleared (set to 0) | The full backup is needed |
| Differential backup | Backs up any data that has changed since last full backup | Not cleared (set to 1) | The full backup and only last differential backup are needed |
| Incremental backup | Backs up any data that has changed since last full backup or last incremental backup | Cleared (set to 0) | The full backup and all incremental backups are needed |

**Table 13-4** Types of data backups

# Disaster Recovery

## Data Backups — Calculations

- Two (2) elements are used in the calculation of when backups should be performed
  1. Recovery point objective (RPO) – Maximum length of time organization can tolerate between backups
  2. Recovery time objective (RTO) – Length of time it will take to recover backed up data

# Disaster Recovery

## Data Backups — Alternatives

- Disk to disk (D2D) – Offers better RPO than tape (because recording to hard disks is faster than recording to magnetic tape) and an excellent RTO
- Disk to disk to tape (D2D2T) – Uses magnetic disk as a temporary storage area so that server does not have to be off-line for an extended period of time (and thus D2D2T has an excellent RTO)
- Continuous data protection (CDP) – Performs continuous data backups that can be restored immediately for excellent RPO and RTO times —see Tables 13-5 and 13-6

# Disaster Recovery

| Name | Data protected | Comments |
|---|---|---|
| Block-level CDP | Entire volumes | All data in volume receives CDP protection, which may not always be necessary |
| File-level CDP | Individual files | Can select which files to include and exclude |
| Application-level CDP | Individual application changes | Protects changes to databases, email messages, etc. |

**Table 13-5** Continuous data protection types

# Disaster Recovery

| Backup technology | RPO | RTO | Cost | Comments |
|---|---|---|---|---|
| Magnetic tape | Poor | Poor | Low | Good for high-capacity backups |
| Disk to disk (D2D) | Good | Excellent | Moderate | Hard drive may be subject to failure |
| Disk to disk to tape (D2D2T) | Good | Excellent | Moderate | Good compromise of tape and D2D |
| Continuous data protection (CDP) | Excellent | Excellent | High | For organizations that cannot afford any downtime |

**Table 13-6** Data backup technologies

# Quick Quiz

1. Developing an outline of procedures that are to be followed in the event of a major IT incident is known as _____.
   Answer:

# Quick Quiz

1. Developing an outline of procedures that are to be followed in the event of a major IT incident is known as _____.
   Answer: IT contingency planning

# Quick Quiz

1. Developing an outline of procedures that are to be followed in the event of a major IT incident is known as _____.
   Answer: IT contingency planning
2. Which RAID (Redundant Array of Independent Drives) level acts as a mirrored array and can achieve high data transfer rates because there are multiple stripe segments?
   Answer:

# Quick Quiz

1. Developing an outline of procedures that are to be followed in the event of a major IT incident is known as _____.
   Answer: IT contingency planning
2. Which RAID (Redundant Array of Independent Drives) level acts as a mirrored array and can achieve high data transfer rates because there are multiple stripe segments?
   Answer: RAID 0+1 (high data transfer)

# Quick Quiz

1. Developing an outline of procedures that are to be followed in the event of a major IT incident is known as _____.
   Answer: IT contingency planning
2. Which RAID (Redundant Array of Independent Drives) level acts as a mirrored array and can achieve high data transfer rates because there are multiple stripe segments?
   Answer: RAID 0+1 (high data transfer)
3. A(n) _____ is always running off its battery while the main power runs the battery charger and is not affected by dips or sags in voltage.
   Answer:

# Quick Quiz

1. Developing an outline of procedures that are to be followed in the event of a major IT incident is known as _____.
   Answer: IT contingency planning
2. Which RAID (Redundant Array of Independent Drives) level acts as a mirrored array and can achieve high data transfer rates because there are multiple stripe segments?
   Answer: RAID 0+1 (high data transfer)
3. A(n) _____ is always running off its battery while the main power runs the battery charger and is not affected by dips or sags in voltage.
   Answer: on-line UPS

# Quick Quiz

1. Developing an outline of procedures that are to be followed in the event of a major IT incident is known as _____.
   Answer: IT contingency planning
2. Which RAID (Redundant Array of Independent Drives) level acts as a mirrored array and can achieve high data transfer rates because there are multiple stripe segments?
   Answer: RAID 0+1 (high data transfer)
3. A(n) _____ is always running off its battery while the main power runs the battery charger and is not affected by dips or sags in voltage.
   Answer: on-line UPS
4. The *age* of the data that an organization wants the ability to restore in the event of a disaster is known as _____.
   Answer:

# Quick Quiz

1. Developing an outline of procedures that are to be followed in the event of a major IT incident is known as _____.
   Answer: IT contingency planning
2. Which RAID (Redundant Array of Independent Drives) level acts as a mirrored array and can achieve high data transfer rates because there are multiple stripe segments?
   Answer: RAID 0+1 (high data transfer)
3. A(n) _____ is always running off its battery while the main power runs the battery charger and is not affected by dips or sags in voltage.
   Answer: on-line UPS
4. The *age* of the data that an organization wants the ability to restore in the event of a disaster is known as _____.
   Answer: recovery point objective (RPO)

# Environmental Control

## Environmental Control

- Better to take proactive steps to avoid disruptions rather than just trying to recover from them
- Preventing disruptions through environmental controls involves:
  - Fire Suppression
  - Electromagnetic Interference (EMI) Shielding
  - Configuring Heating, Ventilation, and Air Conditioning (HVAC)

# Environmental Control

## Environmental Control — Fire Suppression

- Fire is a constant threat to persons as well as property
- In order for a fire to occur, four (4) entities must be present at the same time (see Figure 13-8):
  1. Fuel or combustible material
  2. Oxygen to sustain combustion
  3. Heat to raise material to its ignition temperature
  4. Chemical reaction: fire itself

Table 13-7 lists the type of fires.

# Environmental Control

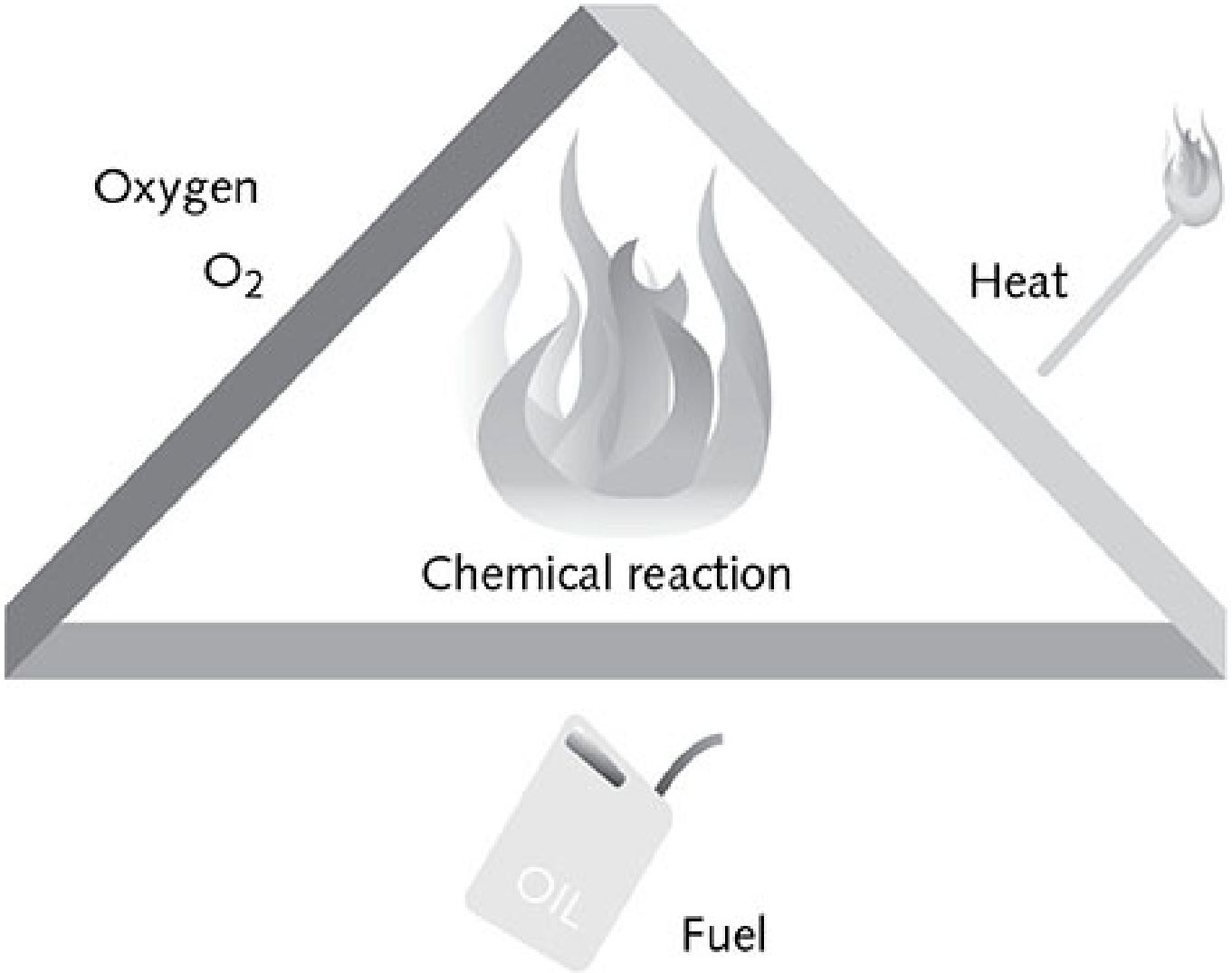


**Figure 13-8** Fire triangle

# Environmental Control

| Class of fire | Type of fire | Combustible materials | Methods to extinguish | Type of fire extinguisher needed |
|---|---|---|---|---|
| Class A | Common combustibles | Wood, paper, textiles, and other ordinary combustibles | Water, water-based chemical, foam, or multipurpose dry chemical | Class A or Class ABC extinguisher |
| Class B | Combustible liquids | Flammable liquids, oils, solvents, paint, and grease, for example | Foam, dry chemical, or carbon dioxide to put out the fire by smothering it or cutting off the oxygen | Class BC or Class ABC extinguisher |
| Class C | Electrical | Live or energized electric wires or equipment | Foam, dry chemical, or carbon dioxide to put out the fire by smothering it or cutting off the oxygen | Class BC or Class ABC extinguisher |
| Class D | Combustible metals | Magnesium, titanium, and potassium, for example | Dry powder or other special sodium extinguishing agents | Class D extinguisher |
| Class K | Cooking oils | Vegetable oils, animal oils, or fats in cooking appliances | Special extinguisher converts oils to noncombustible soaps | Wet chemical extinguisher |

**Table 13-7** Fire types

# Environmental Control

## Environmental Control — Fire Suppression

- Using handheld fire extinguisher not recommended because chemical contents can contaminate electrical equipment
- Stationary fire suppression systems integrated into building's infrastructure Systems classified as (see Table 13-8):
  - Water sprinkler systems – Spray area with pressurized water
  - Dry chemical systems – Disperse fine, dry powder over fire
  - Clean agent systems – Do not harm people, documents, or electrical equipment in the room

# Environmental Control

| Category | Name | Description | Comments |
|---|---|---|---|
| Water sprinkler system | Wet pipe | Water under pressure used in pipes in the ceiling | Used in buildings with no risk of freezing |
| | Alternate | Pipes filled with water or compressed air | Can be used when environmental conditions dictate |
| | Dry pipe | Pipes filled with pressurized water and water is held by control valve | Used when water stored in pipes overhead is a risk |
| | Pre-action | Like dry pipe but requires a preliminary action such as a smoke detector alarm before water is released into pipes | Used in areas that an accidental activation would be catastrophic, such as in a museum or storage area for rare books |
| Dry chemical system | Dry chemicals | Dry powder is sprayed onto the fire, inhibiting the chain reaction that causes combustion and putting the fire out | Used frequently in industrial settings and in some kitchens |
| Clean agent system | Low-pressure carbon dioxide ($CO_2$) systems | Chilled, liquid $CO_2$ is stored and becomes a vapor when used that displaces oxygen to suppress the fire | Used in areas of high voltage and electronic areas |
| | High-pressure carbon dioxide systems | Like the low-pressure $CO_2$ systems, but used for small and localized applications | Used in areas of high voltage and electronic areas |
| | FM 200 systems (Heptafluoropropane) | Absorbs the heat energy from the surface of the burning material, which lowers its temperature below the ignition point and extinguishes the fire | One of the least toxic vapor extinguishing agents currently used; can be used in computer rooms, vaults, phone rooms, mechanical rooms, museums, and other areas where people may be present |
| | Inergen systems | A mix of nitrogen, argon, and carbon dioxide | Used to suppress fires in sensitive areas such as telecommunications rooms, control rooms, and kitchens |
| | FE-13 systems | Developed initially as a chemical refrigerant, FE-13 works like FM 200 systems | Safer and more desirable if the area being protected has people in it |

**Table 13-8** Stationary fire suppression systems

# Environmental Control

## Environmental Control — Electromagnetic Interference (EMI) Shielding

- Computer systems, cathode ray tube monitors, printers, similar devices all emit electromagnetic fields that are produced by signals or movement of data
- Possible for attackers to pick up these electromagnetic fields and read the data that is producing them
- Faraday cage – Metal enclosure that prevents entry or escape of electromagnetic fields often used for testing in electronic labs (see Figure 13-9)

# Environmental Control

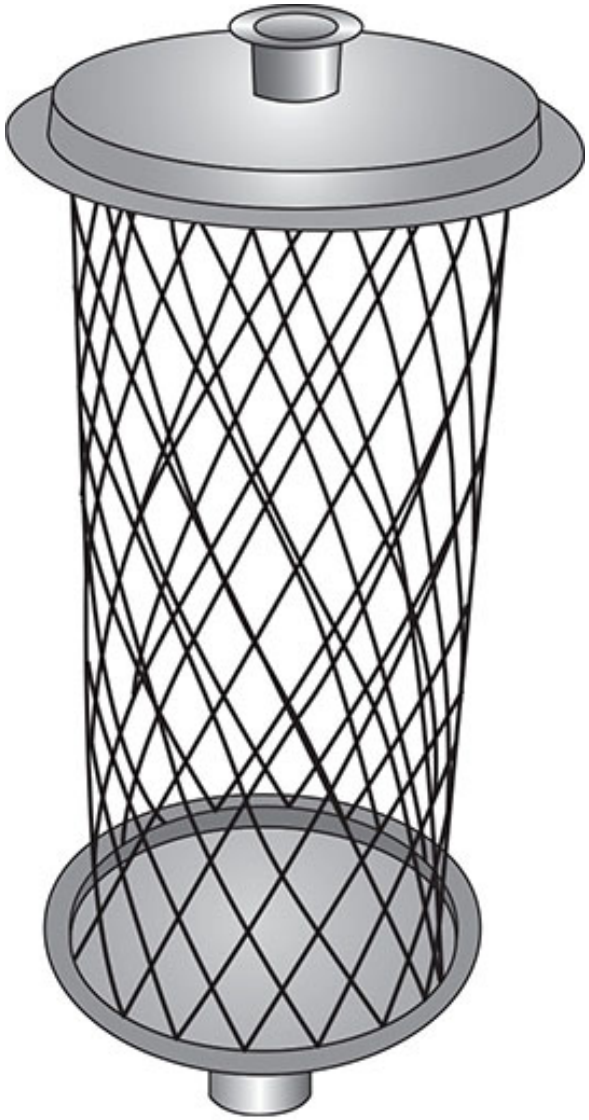

**Figure 13-9** Faraday cage

# Environmental Control

## Environmental Control — HVAC

- Data centers have special cooling requirements:
  - More cooling necessary due to large number of systems generating heat in confined area
  - Precise cooling needed
- Heating, ventilating, and air conditioning (HVAC) – Maintain temperature and relative humidity at required levels
- Controlling environmental factors can reduce electrostatic discharge
- Servers lined up in alternating rows with cold air intakes facing one direction and hot air exhausts facing other direction

# Incident Response

## Incident Response — Forensics

- Incident response procedures can include using basic forensics procedures
- Forensics – Applying science to legal questions for analyzing evidence
- Computer forensics – Uses technology to search for computer evidence of a crime
- Reasons for importance of computer forensics:
  - Amount of digital evidence
  - Increased scrutiny by the legal profession
  - Higher level of computer skill by criminals

# Incident Response

## Incident Response — Forensics

- When responding to a criminal event that requires an examination using computer forensics, four (4) basic steps are followed (similar to those of standard forensics):
  1. Secure the Crime Scene
  2. Preserve the Evidence
  3. Establish the Chain of Custody
  4. Examine for Evidence

# Incident Response

## Incident Response — Forensics (Secure the Crime Scene)

- First responders contacted
- Physical surroundings documented
- Photographs taken before anything is touched
- Computer cables labeled
- Team takes custody of entire computer
- Team interviews witnesses

# Incident Response

## Incident Response — Forensics (Preserve the Evidence)

- Digital evidence is very fragile
- Can be easily altered or destroyed
- Computer forensics team captures volatile data (e.g., contents of RAM, current network connections)
- Order of volatility must be followed to preserve most fragile data first (see Table 13-9)
- Capture entire system image
- Mirror image backup of the hard drive

# Incident Response

| Location of data | Sequence to be retrieved |
|---|---|
| Register, cache, peripheral memory | First |
| Random access memory (RAM) | Second |
| Network state | Third |
| Running processes | Fourth |

**Table 13-9 Order of volatility**

# Incident Response

## Incident Response — Forensics (Establish the Chain of Custody)

- Chain of custody – Documents that evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt evidence
- Chain of custody includes:
  - Documenting all of serial numbers of the systems involved
  - Who handled and had custody of the systems and for what length of time
  - How computer was shipped
  - Any other steps in the process

# Incident Response

## Incident Response — Forensics (Examine for Evidence)

- Examining for evidence includes searching word processing documents, email files, spreadsheets, and other documents for evidence
- Cache and cookies of the web browser can reveal websites that have been visited
- Frequency of emails to particular individuals may be useful
- All of exposed data is examined for clues

# Incident Response

## Incident Response — Forensics (Examine for Evidence)

- Hidden clues be mined and exposed
- One source of hidden data is slack
- Windows computers use two (2) types of slack:
  1. RAM slack – Windows pads the remaining cluster space with data that is currently stored in RAM (see Figure 13-10)
  2. Drive file slack (sometimes called drive slack) – Padded data that Windows uses comes from data stored on the hard drive (see Figure 13-11)

# Incident Response

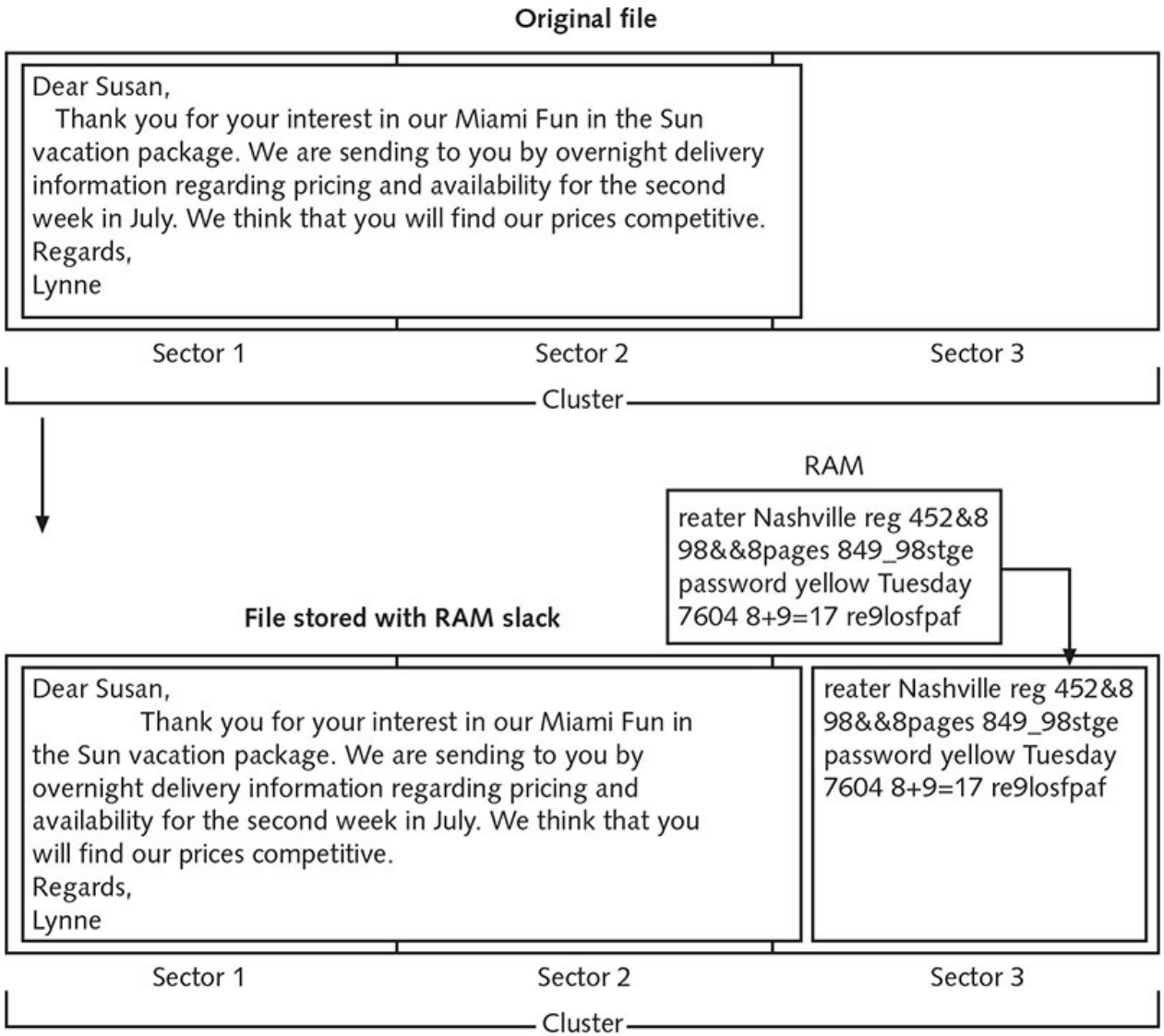


**Figure 13-10** RAM slack

# Incident Response

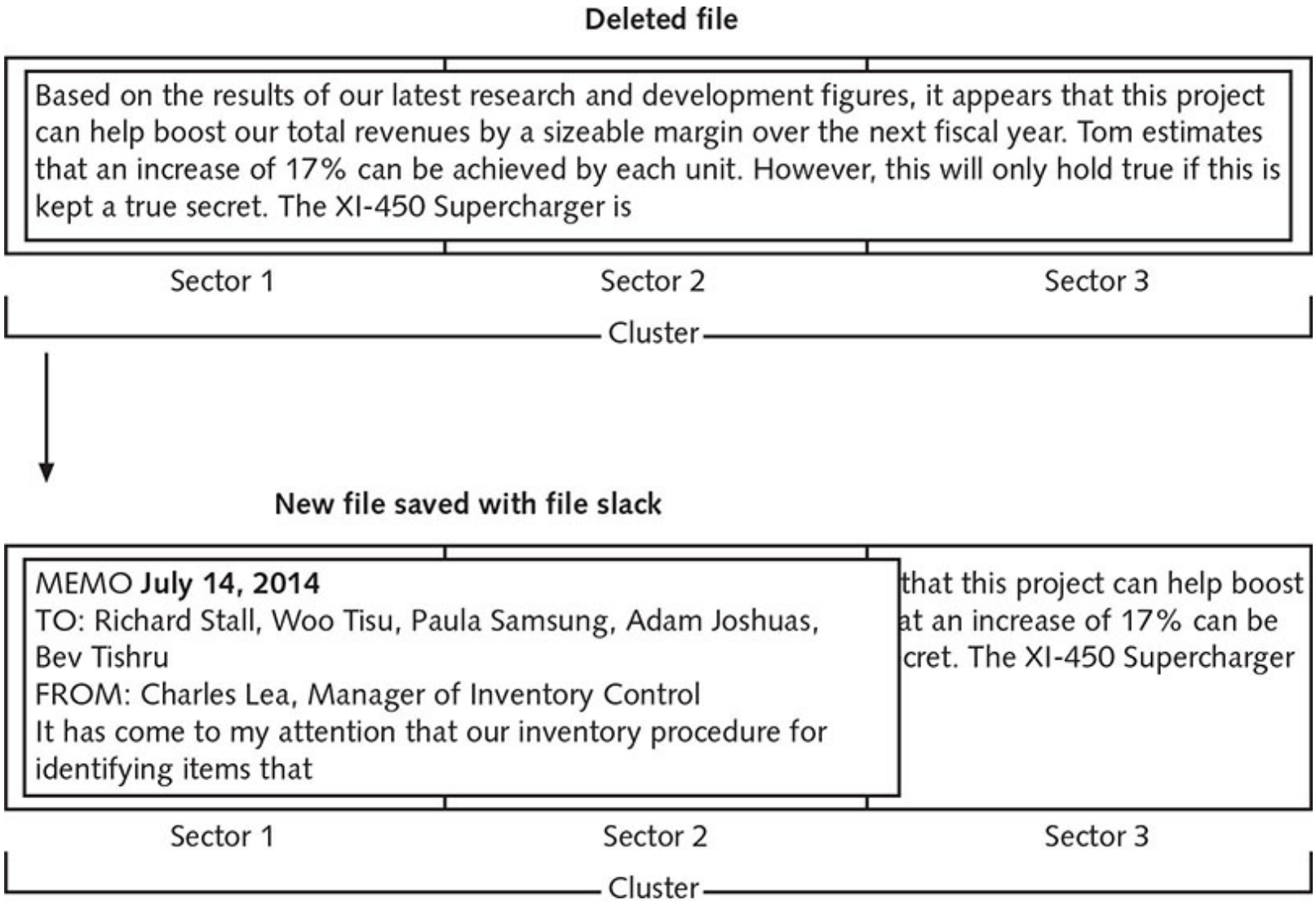


**Figure 13-11** Drive file slack

# Incident Response

## Incident Response Procedures

- Preparation – The key to properly handling event is be prepared in advance by establishing comprehensive policies and procedures
- Execution – Putting the policies and procedures in place involves several crucial steps
- Analysis – In aftermath, proper reporting should document how event occurred and what actions were taken; a *lessons learned* analysis should be conducted in order to use event to build stronger incident response policies and procedures in the future

# Quick Quiz

1. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a _____.
   Answer:

# Quick Quiz

1. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a _____.
   Answer: Faraday cage

# Quick Quiz

1. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a _____.
   Answer: Faraday cage

2. A new area known as _____ uses technology to search for computer evidence of a crime.
   Answer:

# Quick Quiz

1. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a _____.
   Answer: Faraday cage

2. A new area known as _____ uses technology to search for computer evidence of a crime.
   Answer: computer forensics

# Quick Quiz

1. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a _____.
   Answer: Faraday cage

2. A new area known as _____ uses technology to search for computer evidence of a crime.
   Answer: computer forensics

3. The _____ documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence.
   Answer:

# Quick Quiz

1. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a _____.
   Answer: Faraday cage

2. A new area known as _____ uses technology to search for computer evidence of a crime.
   Answer: computer forensics

3. The _____ documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence.
   Answer: chain of custody

# Quick Quiz

1. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a _____.
   Answer: Faraday cage

2. A new area known as _____ uses technology to search for computer evidence of a crime.
   Answer: computer forensics

3. The _____ documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence.
   Answer: chain of custody

4. _____ can contain any information that has been created, viewed, modified, downloaded, or copied since the computer was last booted.
   Answer:

# Quick Quiz

1. A metallic enclosure that prevents the entry or escape of an electromagnetic field is known as a _____.
   Answer: Faraday cage

2. A new area known as _____ uses technology to search for computer evidence of a crime.
   Answer: computer forensics

3. The _____ documents that the evidence was under strict control at all times and no unauthorized person was given the opportunity to corrupt the evidence.
   Answer: chain of custody

4. _____ can contain any information that has been created, viewed, modified, downloaded, or copied since the computer was last booted.
   Answer: RAM slack