1. **Introduction**
   * Essential to have a workspace for data extraction, analysis, and reporting.
   * Secure storage for gear and evidence.
2. **Basic Principles**
   * Responsibility for preserving and protecting evidence.
   * Maintaining professional standards:
     + Lab accreditation.
     + Education, experience, certifications.
     + Insurance and liability.
     + Lab equipment and software certifications.
3. **Setting Up Your Lab**
   * **Physical Controls:**
     + Fencing, Bollards, Locks.
     + HVAC, Fire detection, and suppression.
     + Power supply, Lighting.
     + Facility selection or construction.
   * **Administrative Controls:**
     + Facility management, Personnel controls.
     + Training, Auditing.
     + Emergency procedures.
     + Security policies and procedures.
   * **Technical Controls:**
     + Access controls, Intrusion detection.
     + Firewalls, Identify and access management.
     + Backups, File permissions, Monitoring (CCTV).
4. **Services Offered**
   * **Digital forensic services:**
     + Evidence retrieval.
     + Analysis.
     + Expert testimony.
     + Staffing.
5. **Physical Location Needs**
   * Location considerations: Access to emergency services, electrical power, Internet.
   * **Security:**
     + **Physical:** Gates, locks, cameras, dogs.
     + **Logical:** Passwords.
     + **Administrative:** Policies, background checks.
   * **Types of Security Controls:**
     + **Preventive**: Stops incidents from occurring.
     + **Detective**: Discovers ongoing or past incidents.
     + **Corrective**: Fixes root causes.
     + **Recovery**: Restores to a good state.
     + **Deterrent**: Creates obstacles for attackers.
     + **Compensating**: Fills gaps when permanent controls are lacking.
6. **Software**
   * **General Applications:**
     + Windows, Linux, UNIX, Mac OS, Commodore systems.
     + Graphical image display: QuickView, IrfanView.
     + Accounting software: Quicken, QuickBooks.
     + Databases: Microsoft Access, LibreOffice.
     + Video players: VLC, RealPlayer, Windows Media Player.
   * **Forensic Tools:**
     + Activities: Acquisition, Validation, Extraction, Reconstruction, Reporting.
     + Popular tools: EnCase, FTK, HashCalc, FeelTheBase, Process Explorer, Wireshark, NetStat, TCPView.
7. **Hardware**
   * **Write Blockers:** Prevent data alteration during access.
   * **Imaging Tools:** Create exact replicas of original data.
     + Examples: Ninja disk imager, Atola Insight.
8. **Mobile Forensic Tools**
   * **Devices**: Cell phones, tablets, GPS devices, MP3 players.
   * **Tools**: Magnet Axiom, Cellebrite, Micro Systemation, Oxygen.
9. **Secure Storage**
   * Preferred method: Pelican® cases.
   * Importance of maintaining chain of custody.
10. **Conclusion**
    * Awareness of tools and their integration into the investigative process.