Week 7 – **Digital Forensics Lab**

Objectives:-

- Describe certification requirements for digital forensics labs
- **List physical requirements** for a digital forensics lab
- Explain the **criteria for selecting a basic forensic workstation**
- Describe **components used to build a business case for developing a forensics lab**

Digital Forensic lab

- Ideally…

- In real life…

Identifying Lab Security Needs

- **Secure facility**
  - Should preserve integrity of evidence data
- **Minimum requirements**
  - Small room with **true floor-to-ceiling walls**
  - Door access with a **locking mechanism**
  - **Secure container**
  - **Visitor's log**
- People working together should have same access level
- Brief your staff about **security policy**

Considering Physical Security Needs

- Enhance security by setting **security policies**
- **Enforce** your **policy**
  - Maintain a **sign-in log for visitors**
    - Anyone that is not assigned to the lab is a visitor
    - Escort all visitors all the time
  - Use **visible or audible indicators** that a visitor is inside your premises
    - Visitor badge
  - Install an **intrusion alarm system**
  - Hire a guard force for your lab

Auditing a Digital Forensics Lab

- **Auditing** ensures **proper enforcing of policies**

- Audits should include inspecting the following **facility components** and **practices**:
  - Ceiling, floor, roof, and exterior walls of the lab
  - Doors and doors locks
  - Visitor **logs**
  - Evidence container **logs**
  - At the end of every workday, secure any evidence that's not being processed in a forensic workstation

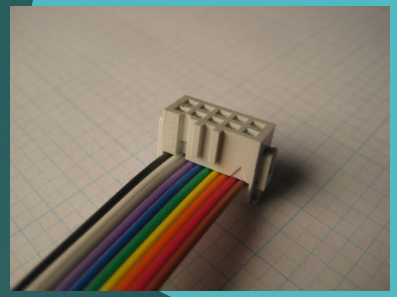
Selecting a Basic Forensic Workstation

- Depends on budget and needs
- Use **less powerful** workstations for mundane tasks
- Use **multipurpose workstations** for resource-heavy analysis tasks

Ref : http://verity.com.sg

Stocking **Hardware Peripherals**

- Any lab should have in stock:
  - IDE cables
  - Ribbon cables for floppy disks
  - Extra USB 3.0 or newer cables and SATA cards
  - SCSI cards, preferably ultrawide
  - Graphics cards, both PCI and AGP types
  - Assorted FireWire and USB adapters
  - Hard disk drives
  - At least two 2.5-inch Notebook IDE hard drives to standard IDE/ATA or SATA adapter
  - Computer hand tools



Quiz Time…

Q1. Lab costs can be broken down into monthly, ____, and annual expenses.

a. daily
b. weekly
c. bimonthly
d. quarterly

Q2. Which of the following is not a requirement to secure a Digital Forensic lab

a. Small room with true floor-to-ceiling walls
b. Data encryption and decryption
c. Secure container
d. Visitor's log

Quiz Time… (Cont)

Q3. Auditing ensures proper enforcing of policies. Which of the following is not a Forensics Lab facility that auditor will include:

a. Tables and chairs in the lab
b. Doors and doors locks
c. Evidence container logs
d. Ceiling, floor, roof and exterior walls of the lab

Q4. Any Forensic Lab should have in stock many useful tools except:

a. IDE cables
b. SCSI cards
c. Hard disk drives
d. Printer