From the News

January 17, myCentralJersey.com – (New Jersey) Chemist admits to stealing sanofi-aventis secrets. A former research chemist with global pharmaceutical company sanofi-aventis headquartered in Bridgewater, New Jersey, pleaded guilty January 17 to stealing trade secrets and making them available for sale through a U.S. subsidiary of a Chinese chemical company, authorities said. The 29-year-old Chinese national is a resident of Franklin, New Jersey, who worked for sanofi-aventis. The convict worked as a research scientist at the firm from August 2006 to June 2011, where she directly assisted in the development of many compounds sanofi-aventis viewed as building blocks for future drugs. The compounds were trade secrets and had not been disclosed outside in any manner, including by means of a patent application. While employed at the firm, the convict was a 50 percent partner in Abby Pharmatech Inc., a subsidiary of Chinese chemical products company Xiamon KAK Science and Technology Co. Ltd. Abby also is engaged in the sale and distribution of pharmaceuticals. The convict admitted that between October 2008 and June 2011, she accessed an internal sanofi-aventis database and downloaded data and chemical structures related to many compounds onto her company-issued laptop. She said she then transferred the data to her home computer via e-mail or a USB thumb drive. The convict further admitted she made the stolen compounds available for sale on the Abby Catalog on Abby Pharmatech Web sites, as well as through a well-known online database. The convict’s lawyer said she only listed the items for sale but never had the compounds. He said she did this to make the size of the Abby Catalog, which included legitimate compounds, look bigger. The charge to which the convict pleaded guilty carries a maximum potential penalty of 10 years in prison and a $250,000 fine. Source: http://www.mycentraljersey.com/article/20120117/NJNEWS/301170036/Chemistadmits-to-stealing-sanofi-aventis-secrets For another story, see item 32

From the News

Reuters – (International) U.S. authorities probe U.S.-China commission e-mail hack. U.S. authorities are investigating allegations an Indian government spy unit hacked into e-mails of an official U.S. commission that monitors economic and security relations between the United States and China, including cyber-security issues, Reuters reported January 10. The request for an investigation came after hackers posted on the Internet what purports to be an Indian military intelligence document on cyberspying, which discusses plans to target the commission — apparently using technical know-how provided by Western mobile phone manufacturers. Appended to the document are transcripts of what are said to be e-mail exchanges among commission members. "We are aware of these reports and have contacted relevant authorities to investigate the matter. We are unable to make further comments at this time," said a spokesman for the U.S.-China Economic and Security Review Commission. The document’s authenticity could not be independently verified. However, the U.S.-China commission is not denying the authenticity of the e-mails. Source: http://www.reuters.com/article/2012/01/10/us-usa-india-hackingidUSTRE80828N20120110
CHAPTER 3
THE INVESTIGATOR’S OFFICE AND LABORATORY

Modified from the slides accompanying Nelson et al “Computer Forensics and Investigations”. Original content © Richard Austin

Assigned Reading

 Posted on class web site as curiosity.pdf
 Outside readings material may be present on the exam
Objectives

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

Understanding Forensics Lab Certification Requirements

- **Computer forensics lab**
  - Where you conduct your investigation
  - Store evidence
  - House your equipment, hardware, and software

- **American Society of Crime Laboratory Directors (ASCLD)** offers guidelines for:
  - Managing a lab
  - Acquiring an official certification
  - Auditing lab functions and procedures
Identifying Duties of the Lab Manager and Staff

- Lab manager duties:
  - Set up processes for managing cases
  - Promote group consensus in decision making
  - Maintain fiscal responsibility for lab needs
  - Enforce ethical standards among lab staff members
  - Plan updates for the lab
  - Establish and promote quality-assurance processes
  - Set reasonable production schedules
  - Estimate how many cases an investigator can handle

- Staff member duties:
  - Knowledge and training:
    - Hardware and software
    - OS and file types
    - Deductive reasoning
Identifying Duties of the Lab Manager and Staff

- Staff member duties:
  - Knowledge and training:
    - Technical training
    - Investigative skills
    - Deductive reasoning
  - Work is reviewed regularly by the lab manager

Lab Budget Planning

- Break costs down into daily, quarterly, and annual expenses
- Use past investigation expenses to extrapolate expected future costs
- Expenses for a lab include:
  - Hardware
  - Software
  - Facility space
  - Trained personnel
Lab Budget Planning

- Estimate the number of computer cases your lab expects to examine
  - Identify types of computers you're likely to examine
- Take into account changes in technology
- Use statistics to determine what kind of computer crimes are more likely to occur
- Use this information to plan ahead your lab requirements and costs

Chapter 3

Lab Budget Planning

- Check statistics from the **Uniform Crime Report**
  - For federal reports, see [www.fbi.gov/ucr/ucr.htm](http://www.fbi.gov/ucr/ucr.htm)
- Identify crimes committed with specialized software
- When setting up a lab for a private company, check:
  - Hardware and software inventory
  - Problems reported last year
  - Future developments in computing technology
- Time management is a major issue when choosing software and hardware to purchase

Chapter 3
Lab Budget Planning

Chapter 3

Lab Budget Planning

Acquiring Certification and Training

- Update your skills through appropriate training
- International Association of Computer Investigative Specialists (IACIS)
  - Membership/Training Only Available to Law Enforcement
  - Created by police officers who wanted to formalize credentials in computing investigations
- Certified Electronic Evidence Collection Specialist (CEECS)
- Certified Forensic Computer Examiners (CFCEs)
Acquiring Certification and Training

- High-Tech Crime Network (HTCN)
  - Certified Computer Crime Investigator, Basic and Advanced Level
  - Certified Computer Forensic Technician, Basic and Advanced Level
- EnCase Certified Examiner (EnCE) Certification
- AccessData Certified Examiner (ACE) Certification
- Other Training and Certifications
  - High Technology Crime Investigation Association (HTCIA)

Acquiring Certification and Training

- Other training and certifications
  - SysAdmin, Audit, Network, Security (SANS) Institute -- GCFA
  - Computer Technology Investigators Network (CTIN)
  - NewTechnologies, Inc. (NTI)
  - Federal Law Enforcement Training Center (FLETC)
  - National White Collar Crime Center (NW3C)
Determining the Physical Requirements for a Computer Forensics Lab

- Most of your investigation is conducted in a lab
- Lab should be secure so evidence is not lost, corrupted, or destroyed
- Provide a safe and secure physical environment
- Keep inventory control of your assets
  - Know when to order more supplies

Identifying Lab Security Needs

- **Secure facility**
  - 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
Conducting High-Risk Investigations

- High-risk investigations demand more security than the minimum lab requirements
  - TEMPEST facilities
    - Electromagnetic Radiation (EMR) proofed
    - [http://nsi.org/Library/Govt/Nispom.html](http://nsi.org/Library/Govt/Nispom.html)
  - TEMPEST facilities are very expensive
    - You can use low-emanation workstations instead

Using Evidence Containers

- Known as evidence lockers
  - Must be secure so that no unauthorized person can easily access your evidence
- Recommendations for securing storage containers:
  - Locate them in a restricted area
  - Limited number of authorized people to access the container
  - Maintain records on who is authorized to access each container
  - Containers should remain locked when not in use
Media Protection

Computer Media is so easily damaged, manufacturers recommend computer media not be exposed to temperatures over 125°F or humidity over 85%. Even a hot mug of coffee represents a real hazard, so imagine what a small fire would do.
http://www.safetyfile.com

Using Evidence Containers

- If a combination locking system is used:
  - Provide the same level of security for the combination as for the container’s contents
  - Destroy any previous combinations after setting up a new combination
  - Allow only authorized personnel to change lock combinations
  - Change the combination every six months or when required
Using Evidence Containers

If you’re using a keyed padlock:
- Appoint a key custodian
- Develop procedure for loss/theft of key
- Stamp sequential numbers on each duplicate key
- Maintain a registry listing which key is assigned to which authorized person
- Conduct a monthly audit
- Take an inventory of all keys
- Place keys in a lockable container
- Maintain the same level of security for keys as for evidence containers
- Change locks and keys annually

Using Evidence Containers

- Container should be made of steel with an internal cabinet or external padlock
- If possible, acquire a media safe
  - 125°F, ≤ 80%RH
- When possible, build an evidence storage room in your lab
- Keep an evidence log
  - Update it every time an evidence container is opened and closed
Overseeing Facility Maintenance

- Immediately repair physical damages
- Escort cleaning crews as they work
- Minimize the risk of static electricity
  - Antistatic pads
  - Clean floor and carpets
- Maintain two separate trash containers
  - Materials unrelated to an investigation
  - Sensitive materials
- When possible, hire specialized companies for disposing sensitive materials

Considering Physical Security Needs

- Create a security policy
- Enforce your policy
  - 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 Computer Forensics Lab

- Auditing ensures proper enforcing of policies
- Audits should include:
  - 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 all evidence
    - Lock all “hot” workstations

Determining Floor Plans for Computer Forensics Labs

![Diagram of a small or home-based lab]

**Figure 3-2** Small or home-based lab
Determining Floor Plans for Computer Forensics Labs

**Figure 3-3** Mid-size computer forensics lab

**Figure 3-4** Regional computer forensics lab
Selecting a Forensic Workstation

- Depends on budget and needs
- Use less powerful workstations for mundane tasks
- Use multipurpose workstations for high-end analysis tasks

“Ultimate Forensics Machine” from Forensic Computers, Inc
$13,500.00

Selecting Workstations for Police Labs

- Police labs have the most diverse needs for computing investigation tools
  - Special-interest groups (SIG)
- General rule
  - One computer investigator for every 250,000 people in a region
  - One multipurpose forensic workstation and one general-purpose workstation
Selecting Workstations for Private and Corporate Labs

- Requirements are easier to determine
- Identify the environment you deal with
  - Hardware platform
  - Operating system
- Gather tools to work on the specified environment

Stocking Hardware Peripherals

- Any lab should have in stock:
  - Drive cables
  - Ribbon cables for floppy disks
  - Peripheral interface cards
  - Graphics cards
  - Power cords
  - Storage devices
  - Adapters (e.g., 2.5-inch Notebook IDE hard drives to standard IDE/ATA)
  - Hand tools
Maintaining Operating Systems and Software Inventories

- Maintain *licensed* copies of software like:
  - Microsoft Office
  - Specialized viewers
  - Common Applications
  - Etc

Using a Disaster Recovery Plan

- Restore your workstation and investigation files to their original condition
  - Recover from catastrophic situations, virus contamination, and reconfigurations
- Includes backup tools for single disks and RAID servers
- **Configuration management**
  - Keep track of software updates to your workstation
Planning for Equipment Upgrades

- **Risk management**
  - Involves determining how much risk is acceptable for any process or operation
  - Identify equipment your lab depends on so it can be periodically replaced
  - Identify equipment you can replace when it fails
- Computing components last 18 to 36 months under normal conditions
  - Schedule upgrades at least every 18 months
    - Preferably every 12 months

Using Mobile Forensic Workstations

- Create a lightweight, mobile forensic workstation
- $$ $$
Digital Intelligence Ultra Kit

- **UltraBlock Bridges**
  - UltraBlock-IDE (Write Blocked)
  - UltraBlock-IDE (Read-Write)
  - UltraBlock-SATA (Write Blocked)
  - UltraBlock-SCSI (Write Blocked)
- **Power Supplies**
  - Two UltraBlock Power Supplies
  - Two Power Cables
  - Two Drive Power Adapters
- **Drive Interface Cables**
  - Two IDE Interface Cables
  - One SATA Interface Cable
  - One SCSI Interface Cable
  - One 2.1/2’’ Hard Drive Adapter
- **Computer Interface Cables**
  - Two USB Cables
  - Two FireWire A (6 pin - 6 pin) Cables
  - Two FireWire A (6 pin - 4 pin) Cables
  - Two FireWire B Cables

Weibetech Forensic Field Kit

**Kit "A-3"** comes with a Forensic UltraDock and six v4 Combo Adapters -- everything you need to acquire data in the field from a large variety of hard drives, including 2.5 & 3.5-inch PATA or SATA drives, 1.0-inch MicroDrives, CompactFlash modules, SD cards, 1.8-inch drives, and ZIF drives.
Building a Business Case for Developing a Forensics Lab

- Can be a problem because of budget problems
- **Business case**
  - Plan you can use to sell your services to management or clients
- Demonstrate how the lab will help your organization to save money and increase profits
  - Compare cost of an investigation with cost of a lawsuit
  - Protect intellectual property, trade secrets, and future business plans
  - Insourcing vs Outsourcing Advantages
    - Prevent exposure of sensitive information to outside parties

Preparing a Business Case for a Computer Forensics Lab

- When preparing your case, follow these steps:
  - Justification
  - Budget development
    - Facility cost
    - Computer hardware requirements
    - Software requirements
    - Miscellaneous costs
  - Approval and acquisition
  - Implementation
Bootstrapping

- Start small with the bare minimum of investment
  - It's much easier to turn down a request for $100K than one for $100
- Demonstrate capability and build credibility
- Increase budget as organizational perception of advantages improves

Preparing a Business Case for a Computer Forensics Lab

- Steps:
  - Acceptance testing
  - Correction for acceptance
  - Production
Summary

- A computer forensics lab is where you conduct investigations, store evidence, and do most of your work
- Seek to upgrade your skills through training
- Lab facility must be physically secure so that evidence is not lost, corrupted, or destroyed
- Harder to plan a computer forensics lab for a police department than for a private organization or corporation

Summary

- A forensic workstation needs to have adequate memory, storage, and ports
- Prepare a business case to enlist the support of your managers and other team members when building a forensics lab