THE PROJECT

AGT Technology and Fox-IT vision on Forensic IT Laboratory

June 16, 2011
The Project

• Current lab has 30 workstations and handles 1,000 cases per year.

• The Project aim is to:
  – Increase the lab to 300 working experts
  – Equipped with the latest forensic tools
  – Training program, operations, processes
  – Working processes based on US and EU standards
Fox-IT and AGT

• Combining local presence with strong Forensic IT expertise

• Ambitious plan requires a strong
  – local partner that understands IT forensics and IT infrastructure
  – partner with a modern and clear vision on Forensic IT and international recognition
History on AGT and Fox-IT

• Road trip in 2007. Presentation to companies in the region.
• 2008 Joined Forensic IT training in Egypt
• 2009?? Visit to Netherlands Forensic Institute
Why Fox-IT?

• Forensic IT experts since 1999
• Founders of forensic computer science department at Netherlands Forensic Science Institute in 1992
• Senior forensic experts
• More than 100 cases per year
• SANS instructors
• Teaching at several Universities
• Portfolio of Forensic IT trainings
• International experience and recognition
Other Partners

• AccessData maker of Forensic Toolkit
• Guidance maker of Encase
• Dell leading in PC and Server market
• BlueArc maker of high end multi tier storage systems
NFI: Digital Forensics Lab
Vision Forensic IT department

• Services
• Organization
  – Staff
  – Infrastructure
  – Tools
• Training and development
• Quality Management
• 4 Year plan
Services

- Imaging disks
- File, database and mail server data collection
- Mobile phone imaging
- Analysis of user behavior on PC
- Data processing and filtering

- Document review
- Document production
- Database analysis
- Log file analysis
- Forensic reporting
- Expert witness testimony
- Decryption and password breaking.
- Internet interception?
Organisation

- Staff
- Infrastructure
- Tools
Staff

- Lab director
- Management team
- Office management
- Case management
- System administrators
- Senior forensic experts
- Forensic experts
- Assistants
- Reviewers
- Interns
- Security officer
- Communication and external relations
- Quality officer
- Procurement
- Front desk
- Finance
- Human resources
Infrastructure

- Forensic lab network and rooms
- Office network and office space
- Server room
- Evidence room
- Meeting rooms
- Review rooms
Software and hardware tools

- Forensic software and hardwired tools
- Forensic and Office pc and laptop
- Office documents, spreadsheets etc
- Case management solution
  - workflow, forms, documents, procedures ...
- Case based Time and expense accounting
- Financial accounting and reporting
- SAN fileservers
  - lab and office, multi-tier storage
- Email server
- Vmware ESX cluster
Training, research and development

- New hire training program
- Advanced trainings
- Conferences
- Certification programs
- Foreign exchange program
- Research program
Quality Management

- Client surveys
- Internal audits
- Procedures
- Benchmarking
4 Year Plan

• Year 1: 50 people, basic services, building, infrastructure, new hire training
• Year 2: depending on case load and required services grow further, work for other national agencies
• Year 3: consolidate growth, focus on external relations, attend international conferences
• Year 4: publications at conferences, procedures in place, senior experts