Advanced German Technology
Forensic Lab
KSA
Content

• AGT-Company Brief
• overview Interception Solutions

• Digital Forensics Labs: way to prevent Terrorism
  • the Problem!
  • WHAT: What is it?
  • HOW: how should be done?
  • WHO: who?
  • WHY: Why this Team? Why AGT?

• Questions/ Open Discussion
Company Brief: What does AGT offer to you?

Consulting, System Integrations, Training outsourcing services

Encryption

Interception

Digital Forensics

Training Professional services

Data & Voice

Telecom & IP

Turn-key solutions

Security services

Know-How transfer & State-Of-The-Art Global Technologies
Company Brief: Our Service Approach

- Consulting
- System Integration
- Training
- Professional Services
- Technology

Global Market Leader

TECHNOLOGY TRANSFER

EMEA - East Asia

PARTNERS

CLIENTS

© 2011, Copyright AGT
Company Brief: Background Information

ADVANCED GERMAN TECHNOLOGY...

- Was founded more than decade ago
- Is a privately owned company
- European headquarter in Germany
- Provides localized operations with international expertise
- MENA Regional office in – Dubai
Company Brief: Our Added Value

• Cutting Edge Technology Provider
AGT does the job for its clients: we are close to the market in Europe and constantly build up the necessary know-how to deliver excellent (IT-)security solutions to our clients.

• Turn-Key Projects
We provide a full-service along the process chain. We analyze our clients’ needs, we provide robust concepts, we choose the right partners, we manage the implementation projects, train our customers, and maintain the solutions.

• System Integration House
We have in-house know-how to integrate the solutions provided by different suppliers in order to fulfill our clients’ requirements. We act as a catalyst and filter, hereby offering our customers a one-stop-shopping solution for all security related projects.
AGT : Projects and Clients

• 1999 AGT first project in ME.
• More than 22 satisfied Law enforcement Agencies
• Top 5 Central Banks around the Region
• Top 5 Telecom companies
• Top 3 Oil and Gas company in ME and GCC
• 3 from Big 4 Auditing Firms in the region
• 3 Lawful interceptions Projects MENA
• First Root CA based on German PKI in the Region 2007
• First Digital Forensic Lab 2005 in the ME
• First Digital Forensic Lab 2007 in the GCC
• Consulting on the First tier 4 Datacenter in GCC
AGT : Anas Chbib

Cologne Uni - Germany : Business admin and computer science

• LH consulting
• Deutsche Bank, Dresdner Bank
• Part of the team dev. First XML Browser for Defense company supplier in Germany
• German Railways (Deutsche Bahn) Systems
• PM of ROOT CA PKI in EYG First in the region.
• Security adviser to three MOI for Nat. Security projects.
• Set Strategy for the first Forensic Labs in the Region.
Lawful Interception Solutions
Overview: Areas of Application

- Gmail
- Facebook
- Skype
- Monitoring Centers
- IP Network
- Ethernet, OF, WiFi
- Radio
- H/V/UHF
- RADAR
- Satellite Air
- GSM Air
- Microwave Air
Cyber Forensics for …

Digital Forensic Labs: Tools to prevent Terrorism
Digital Forensics: Crucial to Homeland Security

Homeland Security

Law Enforcement (ex-post)

Military Operations (ex-ante)

Business (ex-post)

Critical Economic Infrastructure

Saudi Arabia

New York

Kenya

Madrid
Cyber Forensics for ...

- Terrorist Activities
- Child Pornography
- Arms Dealing
- Insurance Fraud
- Money Laundering
- Drug Trafficking
- Hijacking Kidnapping
- Human Trafficking
- White Collar Crime

Intelligence and Evidence Gathering

© 2011, Copyright AGT
What AGT can Offer in the Cyber Forensics?

Cyber Forensics

Legal Expertise

Investigative Expertise

Technical Expertise
Problem Statement

• Methods / methodologies of the past cannot cope

• Need to search more comprehensively for intelligence

• More powerful products are required

• Different intelligence processing methodologies

• Speed-up time to extract intelligence by using power of computers

• All investigators need basic skills, and Training.

• Lack of strategy, Planning, conceptional work, lack of proper Process.

• Focus on few Technologies and few commercial products.
Digital Forensics: Contents & Processes

Overview: DIGITAL FORENSIC

- Data Acquisition
- Computer Forensic Analysis
- E-mail Investigations
- Recovering Image Files
- Writing Investigation Reports
- Logfile Analysis
- Recovering Deleted Files
- Application Password Crackers
- Investigating E-Mail Crimes
- Investigating Web Attacks
- Investigating Network Traffic
- Data Duplication

Preservation → Collection → Analysis

Detailed Documentation & Reporting
How to win the **Champions League**?

**A.** Buy FC Barcelona 😁$$

**B.** Get FCB Player - 😧

**C.** Get the couch and the player 😆😆😆
**THE Project: The Champions League Winner**

**HOW?**

AGT: is your couch, which select the player for you to have the dream Team. BUT the the most important is not what are you doing? HOW you will do it?

**THE SUPER LAB**

1. **Strategy.**
2. Right **Planning.**
3. well define **organization, operations.**
4. Clear defined **process**
5. follow US/EU **Standard** and polices **STRICLY.** NIST USA and BSI GER
6. Select the right technologies suppliers and trainings partners
7. HR : TRAINING TRAINING and TRAINING.
What AGT can offer in the Cyber Forensics?

- Pre-Incident Preparation
  - Detection
    - Information Gathering
      - Analysis and Assessment
      - Incident Reconstruction
      - Isolate System(s)
        - Forensic Analysis of Live Systems
      - Monitor Activity
    - Contain Network
      - Forensic Investigation Process
      - Track & Trace External Links
    - Recover Strategy
      - Remediate
      - Confirm Recovery
      - Report
        - Legal Action
        - Lessons Learned
  - Response Strategy
    - Counter Measures
      - Legal Action
      - Lessons Learned

- Case Initiation
  - Case Feasibility
    - Planning of Operation
      - Legal Processes
        - Intelligence Gathering
      - Hot Acquisition
        - Search and Media Seizure
          - Debriefing/Lessons Learned
        - Transportation (Seizure, Storage and Return)
      - Safe Storage
      - Lab Acquisition
      - Evidence Analysis
        - Feedback and Reporting
          - Legal Action
        - Lessons Learned
      - Expert Witness
Forensic lab setup

- Lab room
  - Imager
  - Wiper
  - Analysts workstation
  - Analysts workstation

- Server room
  - Filer
  - Workhorse
  - Workhorse
  - Filer
  - SAN
  - Storage Network
  - VPN server

- LAB network
  - Connected via VPN

- Internet
  - Anonymous
    - Anonymous webserver
  - Anonymous internet system
  - Anonymous proxy

- Office network
  - Analysts workstation
  - Analysts workstation

- Corporate firewall

© 2011, Copyright AGT
THE PROJECT:
Steering committee from (TCC, MOI, founder of AD, CEO Guidance's, former Interpol Deputy, founder of the NFI, FBI Lab, former BKA Audio Forensic Lab)

- Project Leader: TCC AGT (Fox IT EU – SAIC USA)
- Technology Global leader: Guidance and AD USA, other non commercial SW JAP RUS HW UK and special forensic tools.
- System integrator: AGT & DELL inc USA.
- HW Lab and storage: DELL inc USA.
- Clean Room: TracIP FRA
- Audio Lab: Voice Recognitions, Global leader, Aginoito Spain, University of Seville
- Image Lab: Fraunhofer Inst. (THE GERMAN MIT) GER, cross match USA, Visage USA
- Mobile/ smart Phone unit: EU, USA, UK, UKR, RUS
- Training and professional service provider: AGT GER, Fox IT NL, Teel Tech USA, Traceip FRA X-team RUS
- Mobile forensic Lab: MH service FRA
WHY? AGT Forensic Investigators.

AGT is the only company who has wide spectrum of Know-how as provider of services in Interception Encryption and Forensics. AGT has deep local knowledge in most of the GCC and North Africa.

WHAT CAN AGT DO FOR THE PROJECT?
AGT has large network of partners in security & defense industry.
AGT has wide cooperation's with different large universities and leading scientific institutions.
AGT has excellent access to security experts network from around the world. With special security fields.
What can AGT do for the Project?

The steering committee is one of its kind ever set for a forensic LAB project world wide.

• There no other project done with many experts on board as this project, representing two schools EU and US
• All the companies selected, are leader in their fields
• The way how we do things is trend in the industry
• All employees are from international team (GER, UK, NL, US, CAN, FRA) have a security clearance for secret or higher (B and A) from one or more governmental bodies.
• A background check has been performed by the Local police
• All employees are a fully licensed Private Investigator
  - All employees have passed the required exam
• Bachelor and Master level education
• Expert witness experience.
15 March 2011

Aaron Barr, HBGary Federal CEO, resigns

The CEO of HBGary Federal, Aaron Barr, has stated that he is resigning his position. In a telephone interview with Threatpost, Barr said that “I need to focus on taking care of my family and rebuilding my reputation ... It's been a challenge to do that and run a company. And, given that I've been the focus of much of bad press, I hope that, by leaving, HBGary and HBGary Federal can get away from some of that. I'm confident they'll be able to weather this storm.”

15 June 2011

LulzSec takes down the CIA web site

Hacker group LulzSec, which already has more than 150,000 followers on Twitter, has claimed responsibility for taking down the United States Central Intelligence Agency (CIA) web site. In a post yesterday evening (15 June), the hackers said “Tango down – cia.gov – for the lulz.” It is not yet clear how LulzSec took down the site, however, the group likely used a distributed denial-of-service (DDoS) attack.

15 June 2011

Hackers breached Citibank security using simple URL manipulation – Update

The theft of approximately 200,000 Citibank customer accounts may have achieved by means of a simple manipulation of the Citibank URL. Security experts told the New York Times that the hackers were able to impersonate actual account holders by using a simple trick.

We are ready to help You?

Are You?
Thank you for your interest.

No System is 100 % secure...

... but it can come very close to it ...

with

CONTACT INFORMATION:

AGT FZ LLC Middle East office
P.O.Box: 502186
Bldg. 05 office 304
Dubai Media City
Dubai - UAE
Phone: +971 4 390 20 37
Fax: +971 4 390 47 57
Mail: achbib@agt-technology.com
Web: www.agt-technology.com