Future Challenges in the Lawful Interception of IP based Telecommunication

Dipl.-Ing. Thomas Kröckel

DigiTask GmbH, Germany

DigiTask – Who we are and what we do

- *Special Telecommunication Systems for Law Enforcement Agencies (LEA)*
- *Development of special solutions for the needs of LI*
- *Located in the middle of Germany*
- *DigiTask has overall experience of many years in LI systems*
- *DigiTask is market leader for LI in Germany*
- *DigiTask is privately owned and independent*

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

DigiTask – Who we are and what we do

- *The LI systems cover the following input interfaces:*
  - ISDN - BRI and PRI, X.25, IP, FTP, ATM
- *with recording of*
  - Voice, Fax, Data
  - Modular and flexible in extensions
- *Implementation of European (ETSI) and National Regulations*
  - TS 101 671, TS 33.108, TS 102 232, TR TKÜ, …
- *DigiTask is full member of ETSI*

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

DigiTask – Who we are and what we do

- *Main Products*
  - Database supported Investigation System "DigiBase"
    - Automatic correlation of CC/IRI
    - User friendly and intuitive GUI
    - Wide functionality for investigation, combination and annotations for recorded data
  - Database supported Analysing System "DigiNet II"
    - Real time decoding of all standard internet traffic protocols

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

DigiTask – Who we are and what we do

- *Main Products (continued)*
  - Database supported Analysing System "DigiNet II"
    - Decoding of proprietary protocols
    - Special tools for presentation
  - Mass Storage solutions up to 1 PetaByte and more
  - Storage Management solutions
  - WiFi-Catcher
  - Support for core area of private life
  - Onsite training

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

DigiTask – Who we are and what we do

- *Main Products (continued)*
  - Own Mediation Device
    - Complete LI Data in one hand from ISP to LEA
    - Sniffer solution
  - Geo-Tracking
  - Geo-Region and Geo-Live
  - additional special solutions

The New Internet

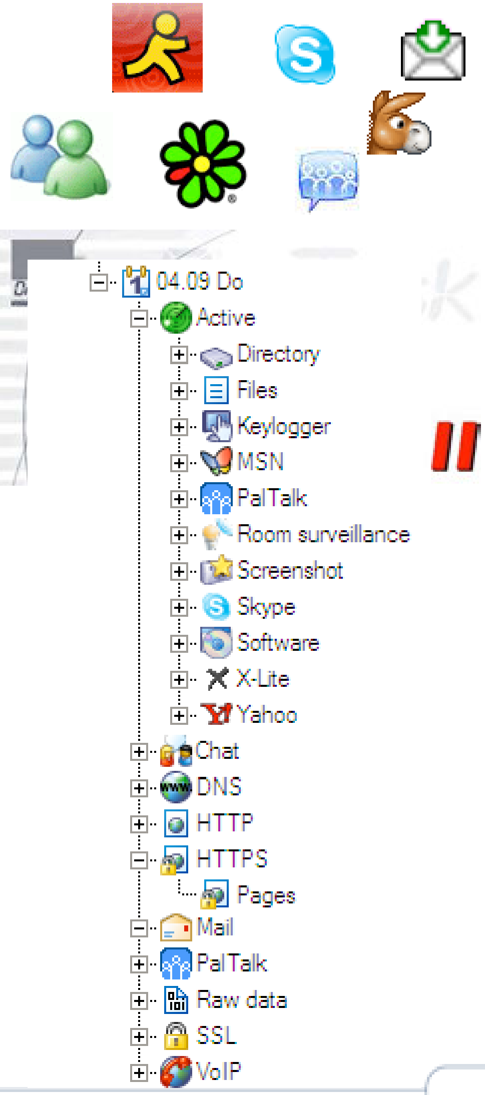
- *Yes, I know the internet!*
  A statement frequently heard.
- *Various new applications/services arise*
  - Second Life, World of Warcraft
  - Dynamic WebPages, RSS, …
- *New communication protocols appear daily without notice*
- *There are a lot of questions*
  - Who is able to review and investigate the new information?
  - What about the increasing encrypted communication?

DigiTask provides solutions and not additional problems and speculations!

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

DigiNet – Decoding of Internet Traffic Protocols

- *Live decoding and visualisation*
- *Modular decoder implementation*
- *Extensive data retrieval, investigation and different user defined filters*
- *Functions for annotation and marking*
- *Supported protocols*
  - HTTP, POP3, SMTP, IMAP, FTP, TELNET
  - VoIP (H.323, SIP), MMS, Webmail
  - IRC, AIM, ICQ, MSN, PalTalk, Yahoo
  - PeerToPeer – eMule/eDonkey, BitTorrent
  - SSL and Skype (only recognition) in conventional LI



This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

DigiNet – Decoding of Internet Traffic Protocols

- *The number of protocol decoders is continually expanded*
- *Storage on web server*
- *Secure Analysis*
- *Use of terminal server or virtualisation to prevent network from viral infection*
- *Search in decoded results*

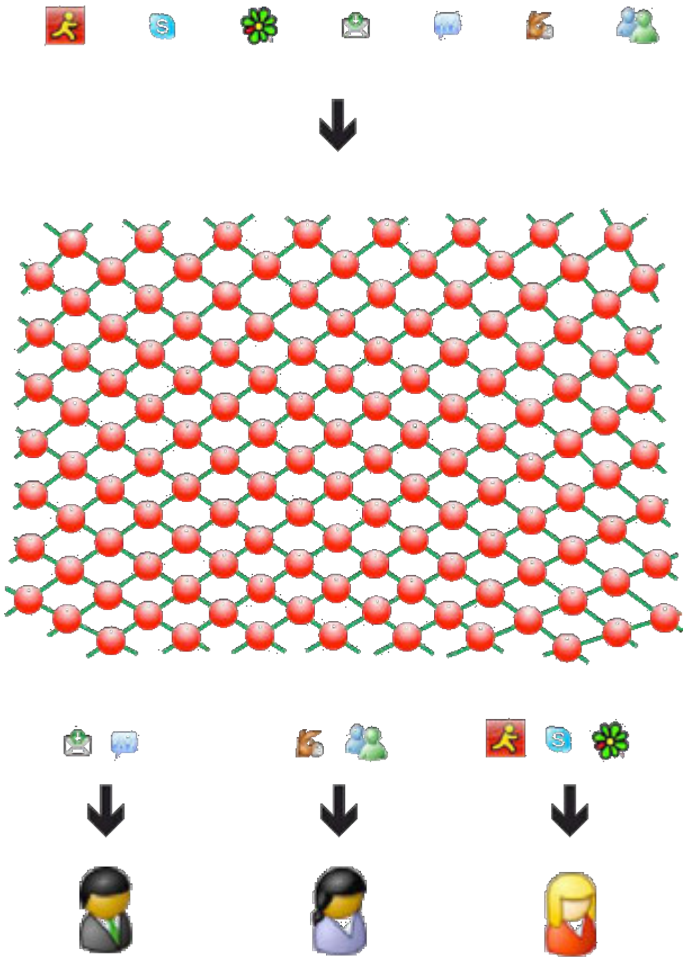
- *Processing possibilities*
  - Marking (colouring)
  - Text reports
  - Search tool for marks and text

Use of Smart Tools for Investigation

– *SPAM filter*
  - Decrease of data to investigate
  - User defined
  - More overview in analysing results
  - Focus on important data
  - Works on all protocols
  - Works immediately after definition and activation

Use of Smart Tools for Investigation

– *Neural network*
  - Statistical procedure
  - Based on input data
  - Automatic correlation between data and objects (target, person) after training
  - Different profiles multithreading
  - Self learning after new training
  - Result for each profile



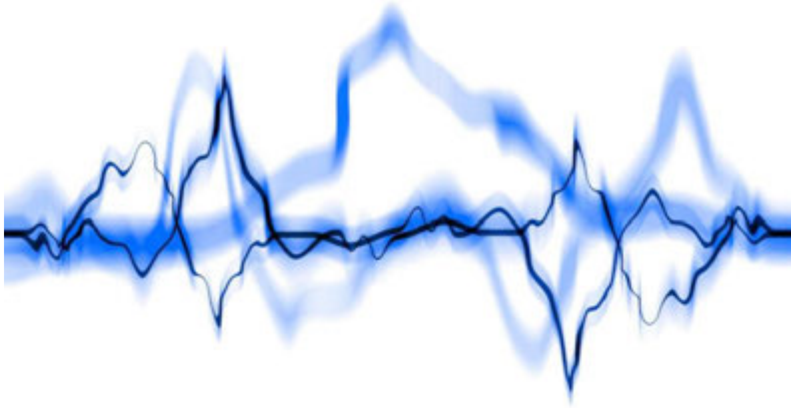
Use of Smart Tools for Investigation

- *Classification of decoded internet data*
  - Behaviour of target while surfing the web or using other services
  - Preferences in communication
  - Manual classification
    - ineffective
    - Time wasting
  - URL classification
    - Allocation into classes
    - Classes are measurements for importance

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

Use of Smart Tools for Investigation

- *Keyword Spotter*
  - Statistical procedure
  - Recognition of speaker
  - Topic spotter
    - Voice
      - » PSTN or IP
  - Live streaming
  - Results
    - Position within a file
    - Success probability
    - Storage in central database for further investigation
    - Supports more than 20 languages

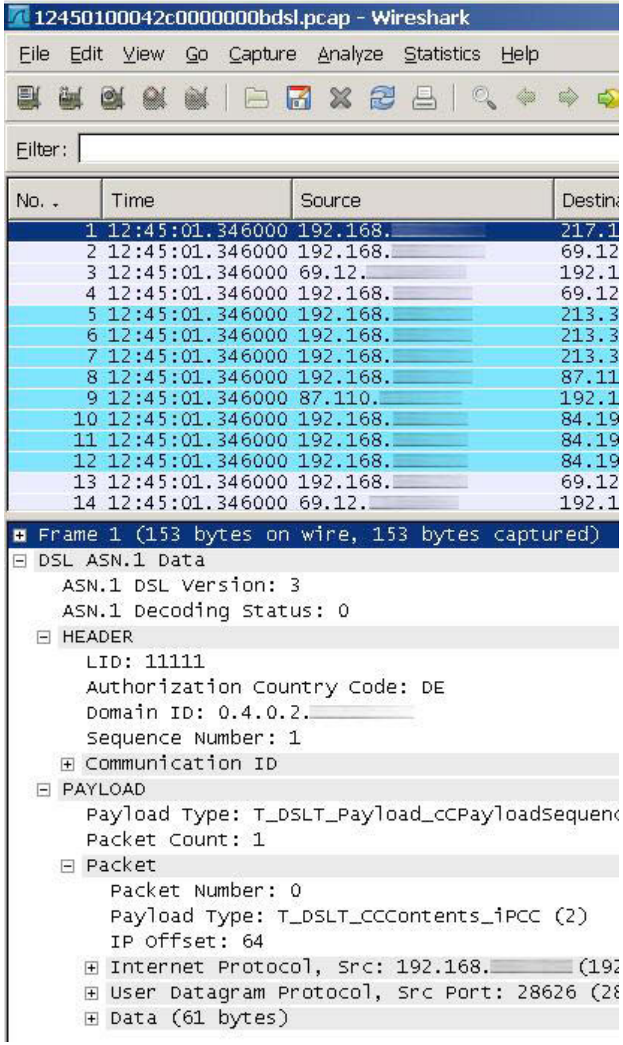


This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

Use of Smart Tools for Investigation

– *RAW Data Inspection*

- Interface for 3rd party tools
- 1st step analysis for newly released communication protocols
- Designed for specialists at LEA
- Deep view into packets of intercepted data
- Approved standard tool Wireshark with special LI Header Plugins
- Adjustable to additional needs



12450100042c0000000bdsl.pcap - Wireshark

```
No. .  Time             Source                Destina
     1 12:45:01.346000 192.168.[redacted]     217.1
     2 12:45:01.346000 192.168.[redacted]     69.12
     3 12:45:01.346000 69.12.[redacted]       192.1
     4 12:45:01.346000 192.168.[redacted]     69.12
     5 12:45:01.346000 192.168.[redacted]     213.3
     6 12:45:01.346000 192.168.[redacted]     213.3
     7 12:45:01.346000 192.168.[redacted]     213.3
     8 12:45:01.346000 192.168.[redacted]     87.11
     9 12:45:01.346000 87.110.[redacted]      192.1
    10 12:45:01.346000 192.168.[redacted]     84.19
    11 12:45:01.346000 192.168.[redacted]     84.19
    12 12:45:01.346000 192.168.[redacted]     84.19
    13 12:45:01.346000 192.168.[redacted]     69.12
    14 12:45:01.346000 69.12.[redacted]       192.1
```

```
⊞ Frame 1 (153 bytes on wire, 153 bytes captured)
⊟ DSL ASN.1 Data
    ASN.1 DSL Version: 3
    ASN.1 Decoding Status: 0
  ⊟ HEADER
      LID: 11111
      Authorization Country Code: DE
      Domain ID: 0.4.0.2.[redacted]
      Sequence Number: 1
    ⊞ Communication ID
  ⊟ PAYLOAD
      Payload Type: T_DSLT_Payload_cCPayloadSequen
      Packet Count: 1
    ⊟ Packet
        Packet Number: 0
        Payload Type: T_DSLT_CCContents_iPCC (2)
        IP Offset: 64
      ⊞ Internet Protocol, Src: 192.168.[redacted] (192
      ⊞ User Datagram Protocol, Src Port: 28626 (28
      ⊞ Data (61 bytes)
```

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

Use of Smart Tools for Investigation

- *WiFi-Catcher*
  - Modular unit for interception of WLAN traffic
  - Main features
    - Catching/Recording of data
    - Presentation of decoded data
    - Mobile usage
    - One channel interception
    - Multi channel interception (14 chann
  - Cracking of WEP encrypted traffic
  - Intersection of MAC address
  - Building of negative sessions
  - Supports standards 802.11a, 802.11b, 802.11g, 802.11n

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

Use of Smart Tools for Investigation

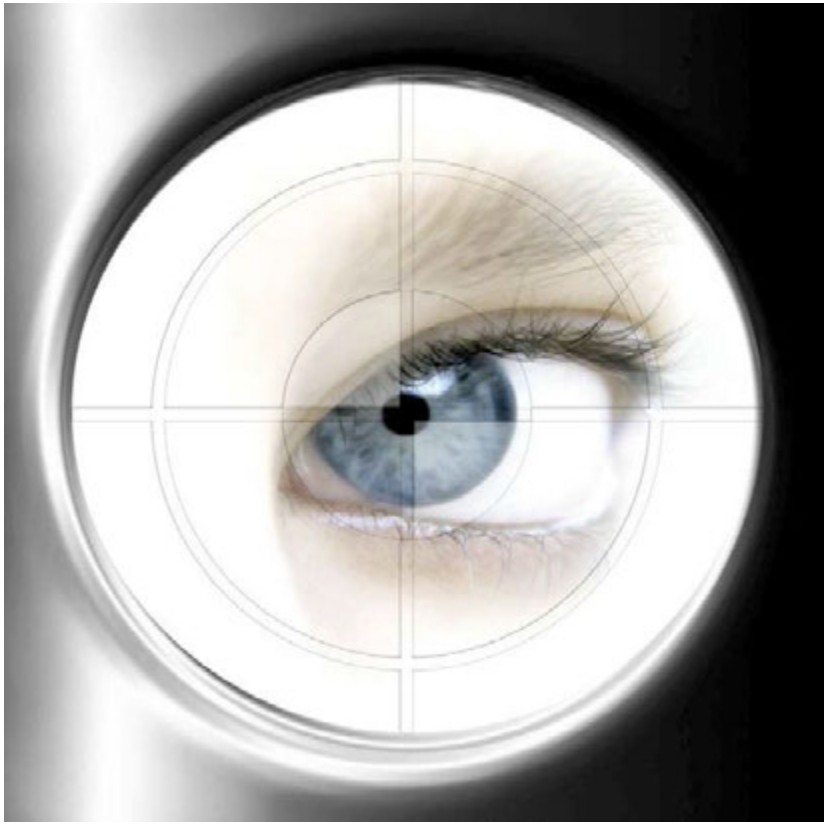
- *Core area of private life*
  - Law in Germany
  - Information in CC about private life has to be deleted
  - Two aspects
    - Recorded voice delivered via ISDN
      - Indication and deletion of raw data
    - Recorded Data delivered via ISDN or IP
      - Raw data has to be analysed by various decoders before presentation
      - Indication and deletion of decoded data
      - Raw data will be unaffected

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

Problems and Risks for Lawful Interception

– *Let us return to Web 2.0, Internet 3.0*

- Further development of security standards
- Secure communication between dedicated users
- Privacy protection
- Result and conclusion
  - » Communication which can be intercepted with LI is decreasing



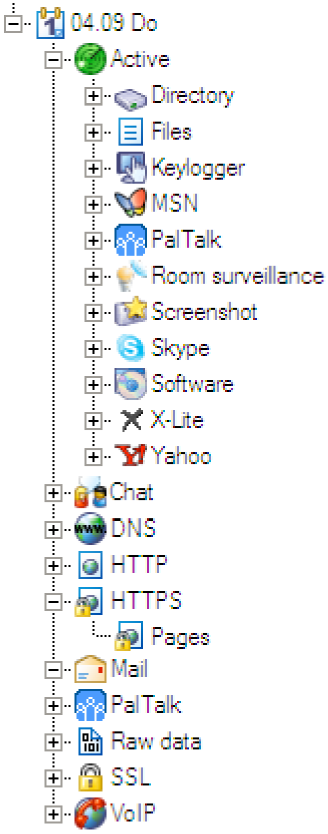
This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

– *Development of Remote Forensic Software*

- Encrypted communication like Skype or SSL can be made visible
- Please visit our demonstrations in track 5
- We like to meet you on
  - Thursday, October 2nd 2008
    - » **14:30h – 15:30h**
      Live demonstration: DigiNet II
    - » **16:00h – 17:00h**
      Live demonstration: Remote Forensic Software

Visit our booth in main exhibition hall

Arrange presentation at your location



```
04.09 Do
  Active
    Directory
    Files
    Keylogger
    MSN
    PalTalk
    Room surveillance
    Screenshot
    Skype
    Software
    X-Lite
    Yahoo
  Chat
  DNS
  HTTP
  HTTPS
    Pages
  Mail
  PalTalk
  Raw data
  SSL
  VoIP
```

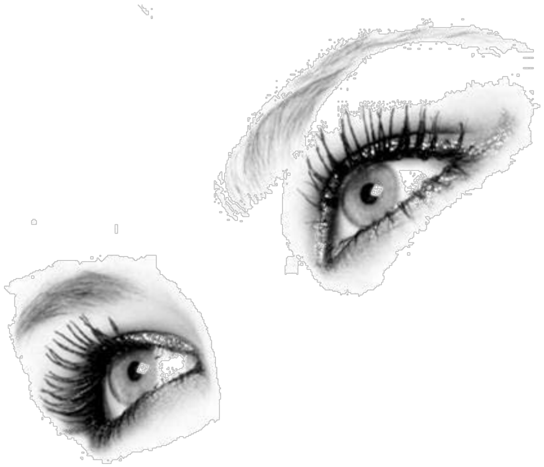
This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.

Perspective

- *Continuous further development to decode and present intercepted data*
- *Indication of contents concerning private life*
- *Inhouse demonstration at LEA*

➔ Complete LI from DigiTask

➔ Competence based on innovation



Thank you.

This material is proprietary of DigiTask GmbH. Any unauthorized reproduction, use or disclosure of this material, or any part thereof, is strictly prohibited.
This material is meant solely for the use by DigiTask employees and authorized DigiTask customers.