



# Remote Forensic Software

Dr. Michael Thomas  
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*

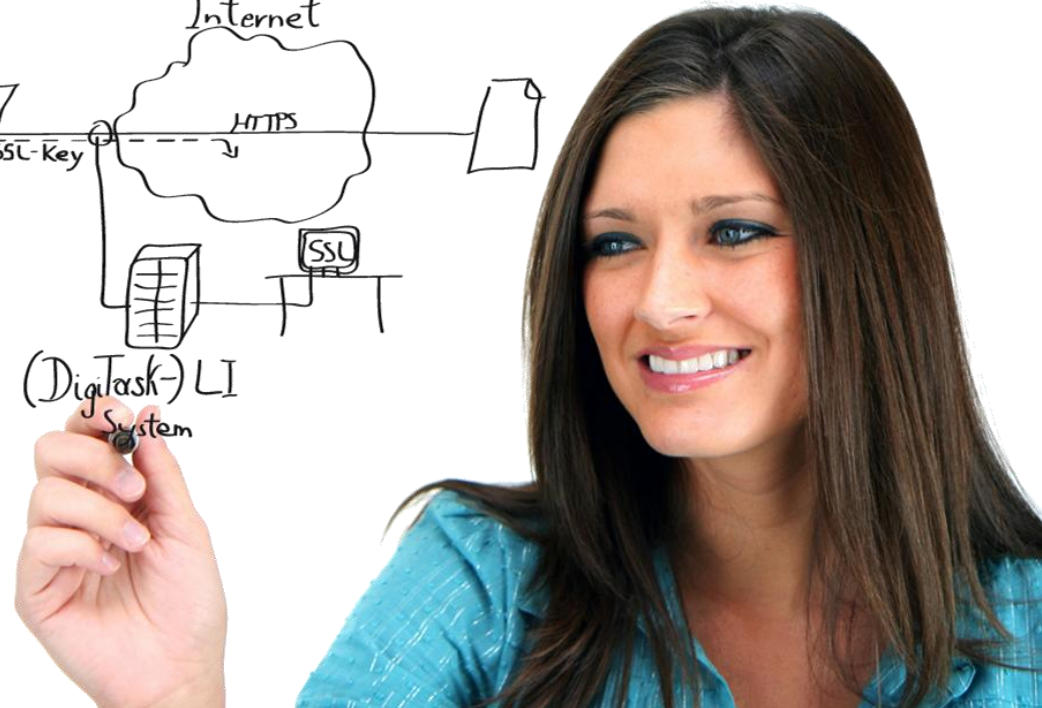
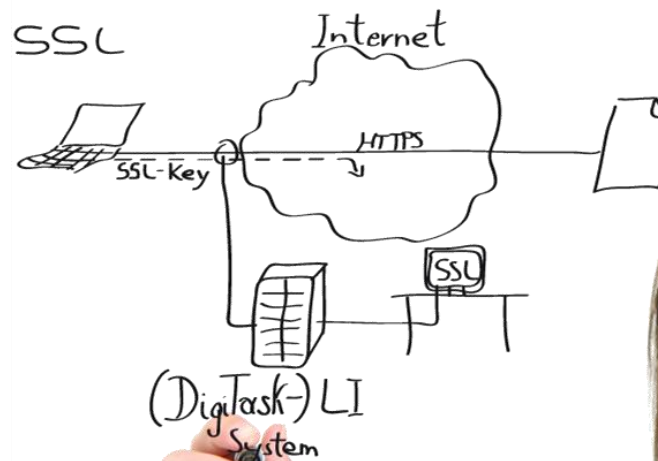


## DigiTask – Main Products

- *Complete LI systems*
  - Database supported analysis for
    - telephony
    - real time IP decoding and visualization
  - Integrating multimedia player
  - Supporting ETSI standards
  - Mediation Devices
  - 24/7 support
  - Onsite training
  
- *WiFi-Catcher*
- *Remote Forensic Software*

## Content

1. What intelligence may be lost with today's LI systems?
2. What is Remote Forensic Software?
3. What is provided by the DigiTask solution?



## 1. What intelligence is lost?

### 1. What intelligence may be lost with today's LI systems?

Information that

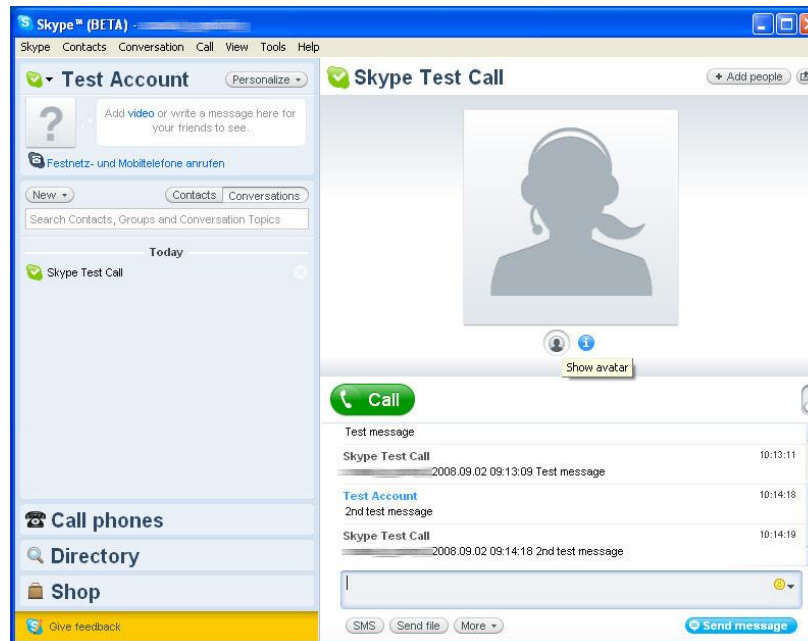
- can be gathered but not decoded
- might be decoded but cannot be gathered
- is not available even after seizure of equipment

# Remote Forensic Software

## 1. What intelligence is lost?

### – Instant Messaging Clients

- encrypted by default:
  - Wikipedia overview of IM lists 55 clients, 34 with out of the box encryption
  - Skype



	Toolkits or SDKs	Encryption
Adium	Cocoa	Yes <sup>11</sup>
AIM	W32	Yes
aMSN	Tcl/Tk	?
BitBee	n/a	No
BitWise IM	W32, GTK2, Carbon	Yes <sup>7</sup>
Centericq	ncurses	Partial <sup>9</sup>
climm	line based	Yes <sup>5,11</sup>
Coccinella	Tcl/Tk	Yes
Ebuddy	?	Yes
EQO	n/a	Yes
Exodus	W32	No
Fire	Cocoa	Yes <sup>6</sup>
Gadu-Gadu	W32	?
Gajim	GTK2	Yes <sup>9</sup>
GCN	W32	Yes <sup>4</sup>
GOIM	Java/SWT	Yes

Source: Wikipedia

## 1. What intelligence is lost?

- External tools for encryption:
  - e.g. SimpLite/SimpPro targets
    - Windows Live Messenger
    - ICQ/AIM
    - Yahoo

No.	Time	Source	Destination	Protocol	Info
78	10:54:57.999150	192.168.	205.188.	AIM Me	AIM Messaging, outgoing to: 3779
86	10:54:58.216001	192.168.	205.188.	AIM Me	AIM Messaging, outgoing to: 3779
94	10:54:58.370084	205.188.	192.168.	AIM Me	AIM Messaging, Acknowledge
95	10:54:58.469924	205.188.	192.168.	AIM Me	[TCP Retransmission] AIM Messaging, Acknow

0190	30	54	45	7a	07	05	05	77	05	79	53	4c	0d	50	72	0d	v4CzgeCW	eyJlcm0m
01a0	42	73	50	74	76	34	34	54	59	5a	33	64	4c	77	4b	66	BsPtv44T	YZ3dLwkf
01b0	69	31	6e	6a	48	6b	48	73	55	48	75	4a	32	2f	47	52	i1njHkHs	UHUJ2/GR
01c0	54	32	74	55	52	2f	79	32	6d	39	78	35	6d	44	56	64	T2tUR/y2	m9x5mDvd
01d0	75	68	69	56	31	73	62	48	53	6b	52	67	4d	2f	37	39	uhiv1sbH	SkRgM/79
01e0	4d	4f	52	42	74	67	72	35	32	54	37	61	4a	56	49	6f	MORbtgr5	2T7aJVio
01f0	74	71	5a	78	43	53	56	58	59	74	72	5a	49	38	6c	77	tqZxC5Vx	YtrZI8lw
0200	62	78	57	73	35	46	67	69	2b	47	62	57	48	30	6c	39	bxws5Fgi	+GbWH019
0210	4a	65	67	38	31	77	41	30	64	64	78	64	38	48	6d	73	Jeg81wA0	ddxd8Hms
0220	75	52	71	72	32	36	53	42	56	57	55	56	32	75	34	53	uRqr26SB	vWUV2u4S
0230	48	75	72	4d	6c	6d	4d	39	6e	78	36	44	72	39	30	4d	HurMlmm9	nx6Dr9OM
0240	77	37	71	41	63	70	4d	30	57	73	61	66	30	72	32	39	w7qAcpi0	wsaf0r29
0250	4d	61	35	57	36	71	68	78	6d	65	65	6d	66	7a	34	53	Ma5w6qhx	meemfz4S
0260	2b	54	38	59	36	2f	6d	61	34	38	71	7a	6d	67	7a	59	+T8Y6/ma	48qzmgzY
0270	7a	33	55	61	52	63	62	32	67	4a	4e	66	50	43	51	67	z3UaRcb2	gJNFPCqg
0280	58	6e	4a	71	38	74	79	76	63	35	4f	66	38	6f	52	36	Xnjq8tyv	c5of8oR6
0290	37	31	46	32	64	44	7a	66	67	0d	0a	56	69	61	3a	20	71F2dDzf	g..Via:
02a0	53	69	6d	70	20	4c	69	74	65	2d	49	43	51	2d	41	49	Simp Lit	e-ICQ-AI
02b0	4d	20	32	2e	32	2e	32	2e	31	32	0d	0a	0d	0a			M 2.2.2.	12....

Frame (702 bytes) | Reassembled TCP (654 bytes)

# Remote Forensic Software

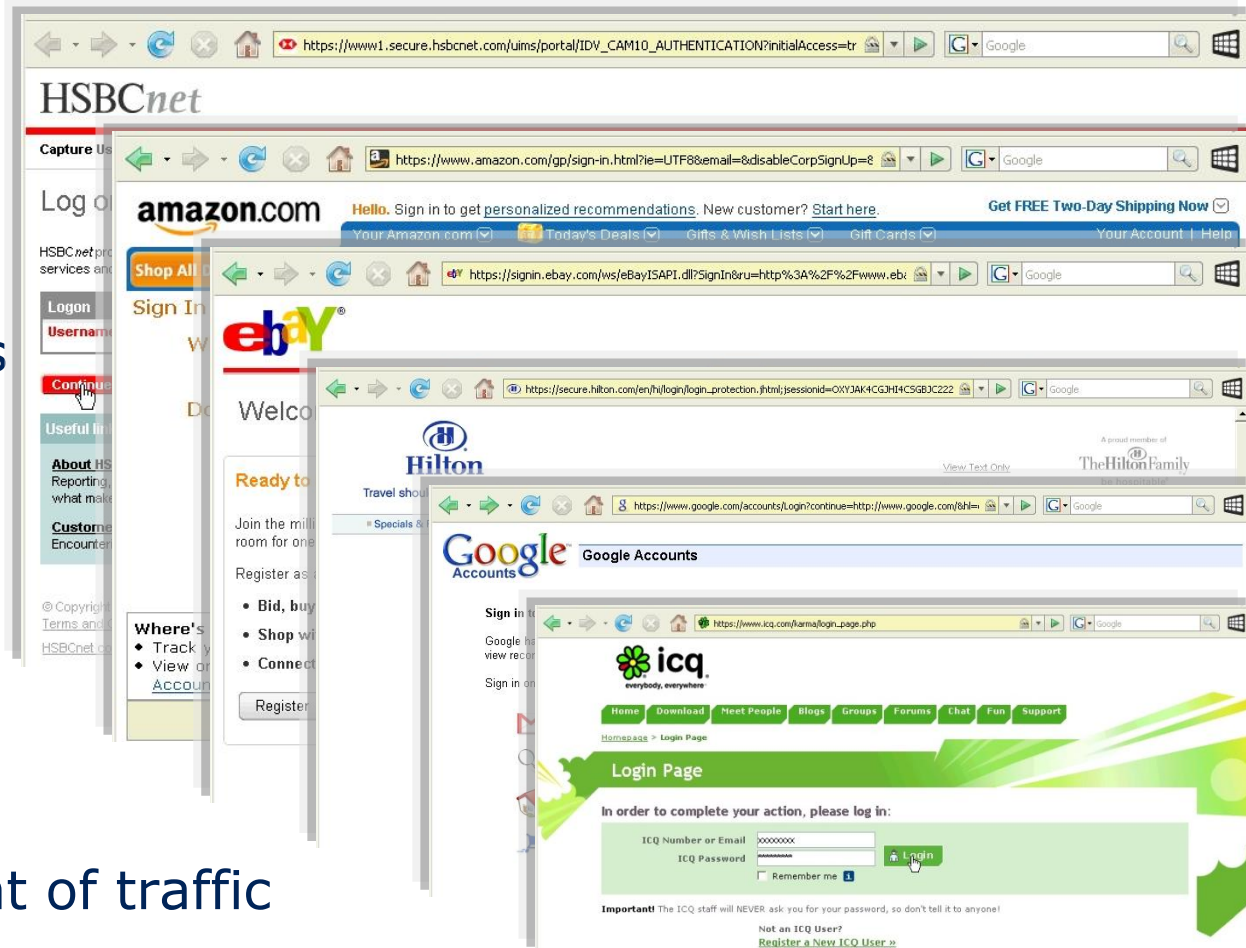
## 1. What intelligence is lost?

– *WWW: sensitive data uses HTTPS*

- Online banking
- E commerce
- Booking systems
- Webmail
- Chat

– *Observable data*

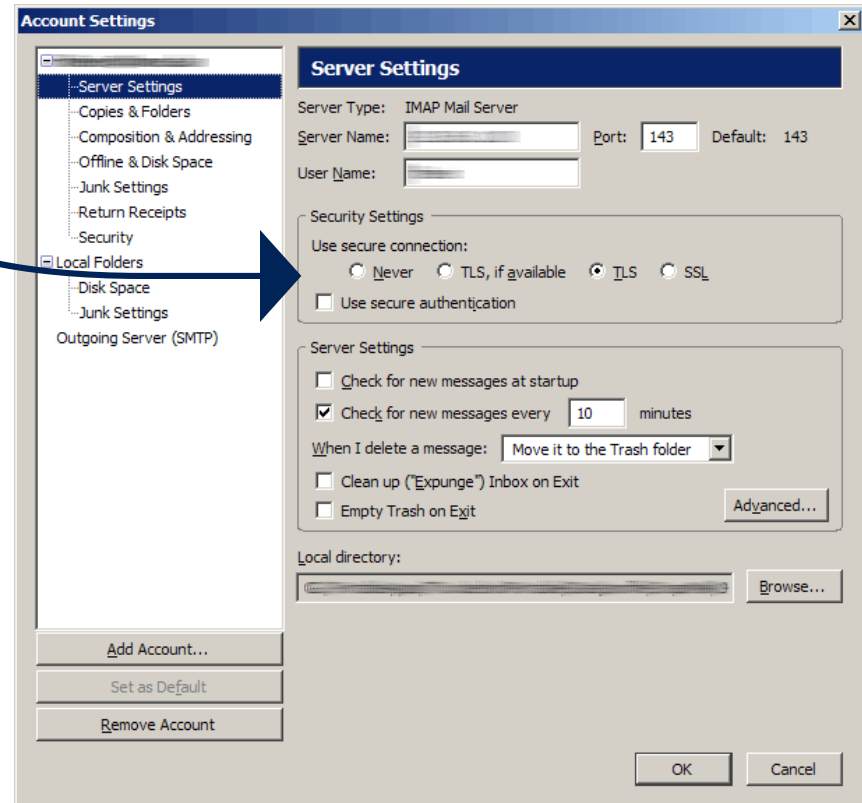
- Remote IP
- Time and amount of traffic





## 1. What intelligence is lost?

- *E-Mail*
  - POP/SMTP use TSL/SSL
- *Local encryption with PGP, GnuPG*



## 1. What intelligence is lost?

- *VPN connections*
  - between endpoints
  - commercial anonymising VPN e.g.
    - Relakks (Sweden, € 5/month)
    - Swissvpn (Switzerland, US\$ 5/month)
- *Tor/JAP*
  - encrypted traffic
  - changing endpoints



The screenshot shows the RELAKKS website with a green header and a dark red background. A white arrow points from the text 'Other organizations or individuals can't intercept or track your applications or communication.' in the screenshot to the corresponding text in the list on the left.

RELAKKS

HOME NEWS SIGN UP

### Security issues

Service Description - RELAKKS Safe Surf  
The Service consists of an encrypted VPN tunnel between your computer and RELAKKS. The IP-number you receive from your existing ISP is used to connect your computer to RELAKKS, from there on RELAKKS substitute your existing IP-number with a new IP-number from RELAKKS. This gives you a number of advantages:

- Your existing ISP will not be able to intercept and track your applications or communication.
- Your existing ISP can not limit what you can do nor limit what information you can access.
- Other organizations or individuals can't intercept or track your applications or communication.

Similar services have been available on the Internet for some time, this is the first time you can get all the advantages without any drawbacks.

## 1. What intelligence is lost?

- *Nomadic targets*
  - travellers
  - suspects seeking open WLANs
- *Tapping internet connections of targets useless*
- *Disk encryption software*
  - Seizure of equipment useless if password is unknown



## 1. What intelligence is lost?

### – *Availability*

- Most of this software is
  - easily available
    - » computer magazines
    - » internet
  - free of cost
  - easy to use

### – *Answer to question:*

- Everything may be lost
- With a few hours effort, today's LI systems can be turned blind and deaf.



## 2. What is Remote Forensic Software?

- *Stealth software installed on computer of target to*
  - overcome encryption
  - handle nomadic targets
  - monitor activity
  
- for
  - criminal investigations
  - intelligence gathering



## 3. What is provided by the DigiTask solution?

### 3.1. Additional intelligence

- *Audio data, e.g. from messengers*
- *Screenshots*
- *Keylogs*
- *File search*
- *Registry settings*
- *Remote shell*
- *... (more in track 5)*



## 3. What is provided by the DigiTask solution?

- *SSL decryption*
  - Keys intercepted in application
  - Keys and encrypted traffic tapped
  - Decoding possible
  - Requires DigiTask LI system



## 3. What is provided by the DigiTask solution?

### 3.2. Data Analysis

- *Standalone system*
  - Immediately deployable
  - Backward channel to target
- *Optional seamless integration in DigiTask LI system*
  - No new user interface for operators
  - Correlation of RFS data with conventional LI
  - Interactions with target become impossible
- *Core area of private life*



## 3. What is provided by the DigiTask solution?

### 3.3. Security

#### – *Protection of data stream*

- Data is AES encrypted
- Proxies between target and recording server
- Connection cannot be traced

#### – *Authenticity of data*

- File transfers are signed
- Safeguards against manipulations
- Important for criminal investigation

## 3. What is provided by the DigiTask solution?

### 3.4. Customization

- *Software may be built according to court order*
- *"Forbidden" features*
  - removed from software
  - cannot be activated
- *After installation:*
  - online update possible
- *Source code of customization*
  - archived
  - verifiable by expert witness



## Conclusion

- *Encryption for every kind of communication easily available*
- *Circumvention by means of Remote Forensic Software*
- *Standalone operation*
- *Integration in LI system*
- *Authenticity of data for criminal investigations*



**Presentation in track 2 today:**

**13:30** DigiTask LI system

**Life demonstration in track 5 today:**

**14:30** DigiTask LI system

**16:00** Remote Forensic Software

Visit our booth in main exhibition hall  
Arrange presentation at your location

Thank you.