

HLKA



Welcome to ... / Bem-vindo à...



HLKA



about me... / sobre mim...

Timo Schneider
Detective Sergeant
Hessisches Landeskriminalamt
HSG13 (HTCU)
Germany

Age: 41
working at Police since 1988
working in Computer Forensics since 2002

What am I talking about... /
O que eu estou falando...

- Problems of internet investigations
corresponding on
German (Hessen) Law
ISP/SP
Mobile Internet / HotSpots
- How to handle the mass of data
- Organisation

Law / Lei

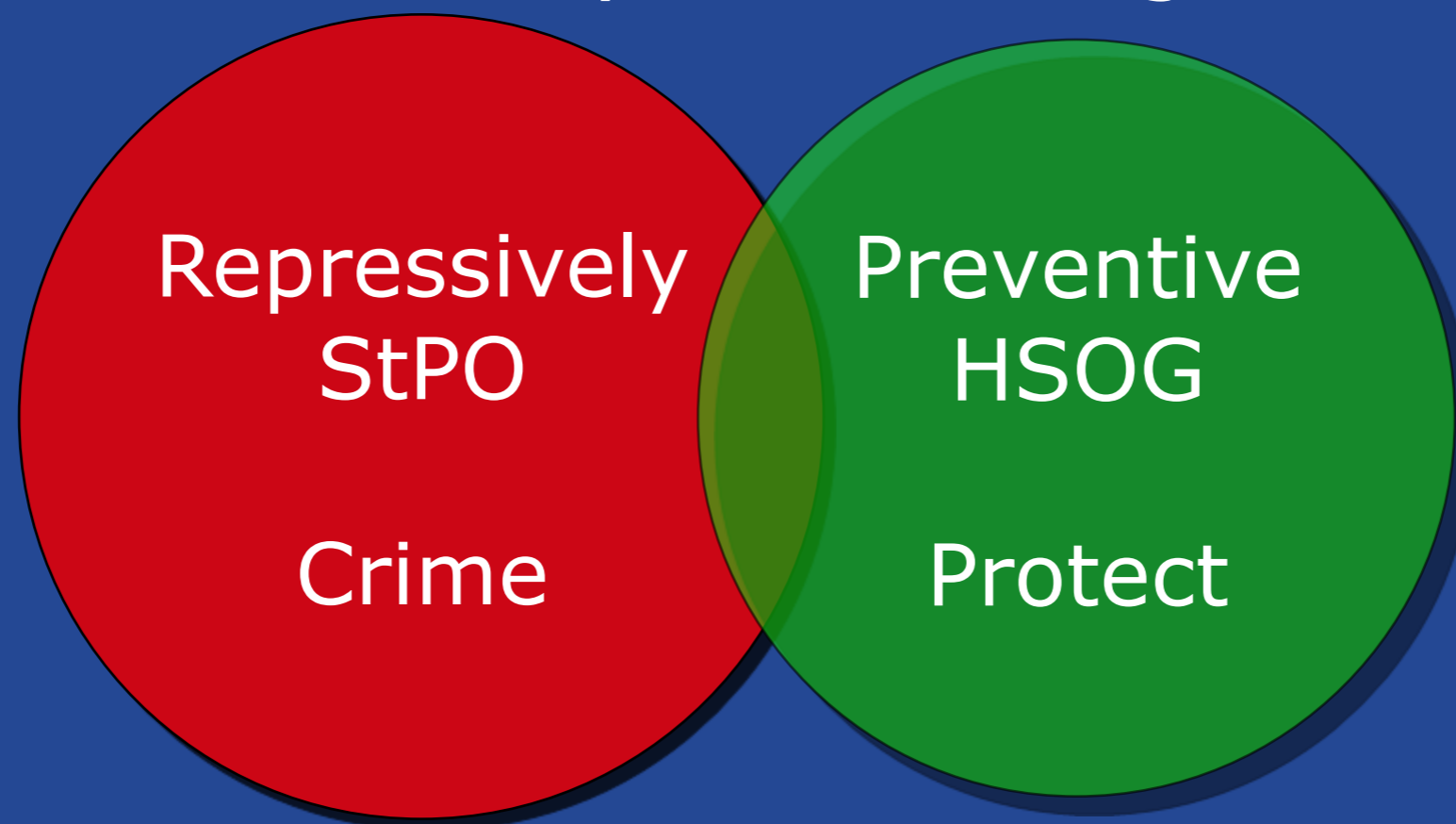
Law

in Germany, there is a general law for police to do all possible in investigating crime

BUT

when breaking into individual rights you need a specific law that allows you to do what you want to do!

Different ways of investigation



in many cases - MIXED

HLKA



Law / Lei

Special Units

own Accounts

provide Videos against
Scamming and mobbing

Preventive
HSOG

Protect

Problems in law

- getting Connection Infos

no special law for preventive
catalogue for repressive

„Problems“ ISP

generally good relation between Police and ISP
we get what they stored

by using general law for preventive

HLKA



Law / Lei

Policy of Privacy/Storing Data

different law for different providers

TMG

Service
Providers

TKG

Internet
Service
Providers

HLKA



Law / Lei

Policy of Privacy/Storing Data

ISP are in duty to store connection info

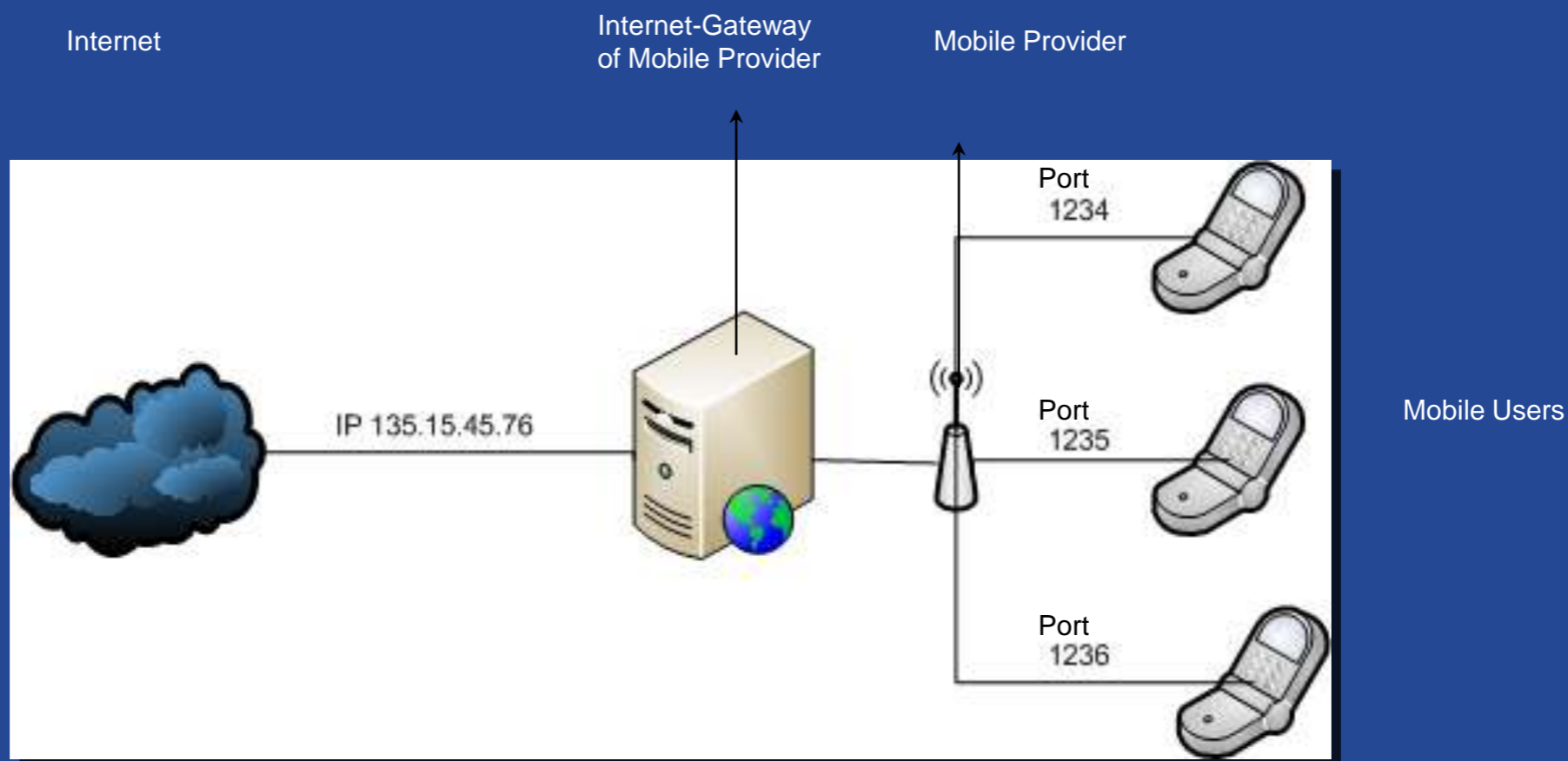
SP are not in duty

Problems Internet Investigations / Problemas nas investigações internet

How long have Providers to store data?

- changed in begin of 2009
- now 6 month

Problems Internet Investigations / Problemas nas investigações internet



Internet with Mobile Phones

Problems Internet Investigations / Problemas nas investigações internet

mobile Internet

- no back investigation to mobile phone
changes coming (hopefully) soon

Problems Internet Investigations / Problemas nas investigações internet

Letters of rogatory

- take a long time
- important data can be lost

Problems Internet Investigations / Problemas nas investigações internet

Alternatives

G8 24/7 contacts

How to manage Mass-Data / Como gerir Massdata

YOU CAN NOT HAVE A LOOK
AT EVERY BIT IN A CASE

How to manage Mass-Data / Como gerir Massdata

Target of investigation is to reduce the Massdata without loosing relevant data

How to manage Mass-Data / Como gerir Massdata

Target of investigation is to reduce the Massdata without loosing relevant data

by searchery
by selection/filtering
by hashing

How to manage Mass-Data / Como gerir Massdata

Searchery

- in cooperation with the investigator
(try to think about, what can be relevant)
- is it necessary to take everything

How to manage Mass-Data / Como gerir Massdata

Selection

- in cooperation with the investigator
- what kind of data is relevant
 - Docs, Spreadsheets, Pics etc.
(Categories)
 - keywords (Index)

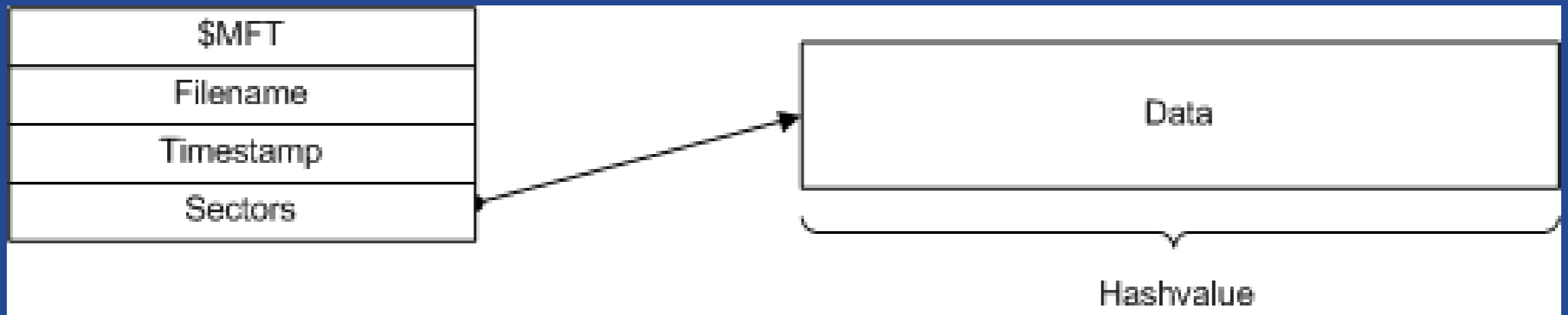
How to manage Mass-Data / Como gerir Massdata

Hashing

- to find relevant data fast
 - no duplicates
 - not looking twice at same file
- to reduce Data for the investigator

Hashing

How it works



HLKA



Hashing Databases

NIST/NSRL (OS, Software)

BKA-Perkeo (CP)

Interpol (CP)

HLKA

NR: 42.118.006

CP: 649.465

also

AP and

TP (since 2009)

How to manage Mass-Data / Como gerir Massdata

Integration of known File Filter
to filter out known non-relevant files

NIST,
own NR-Hashsets
and Duplicates

to bring out relevant Files with
own relevant Hashsets (CP, case specific)

How to manage Mass-Data / Como gerir Massdata

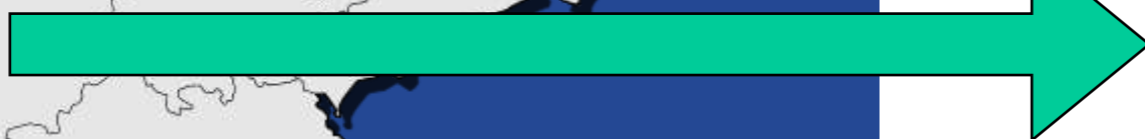
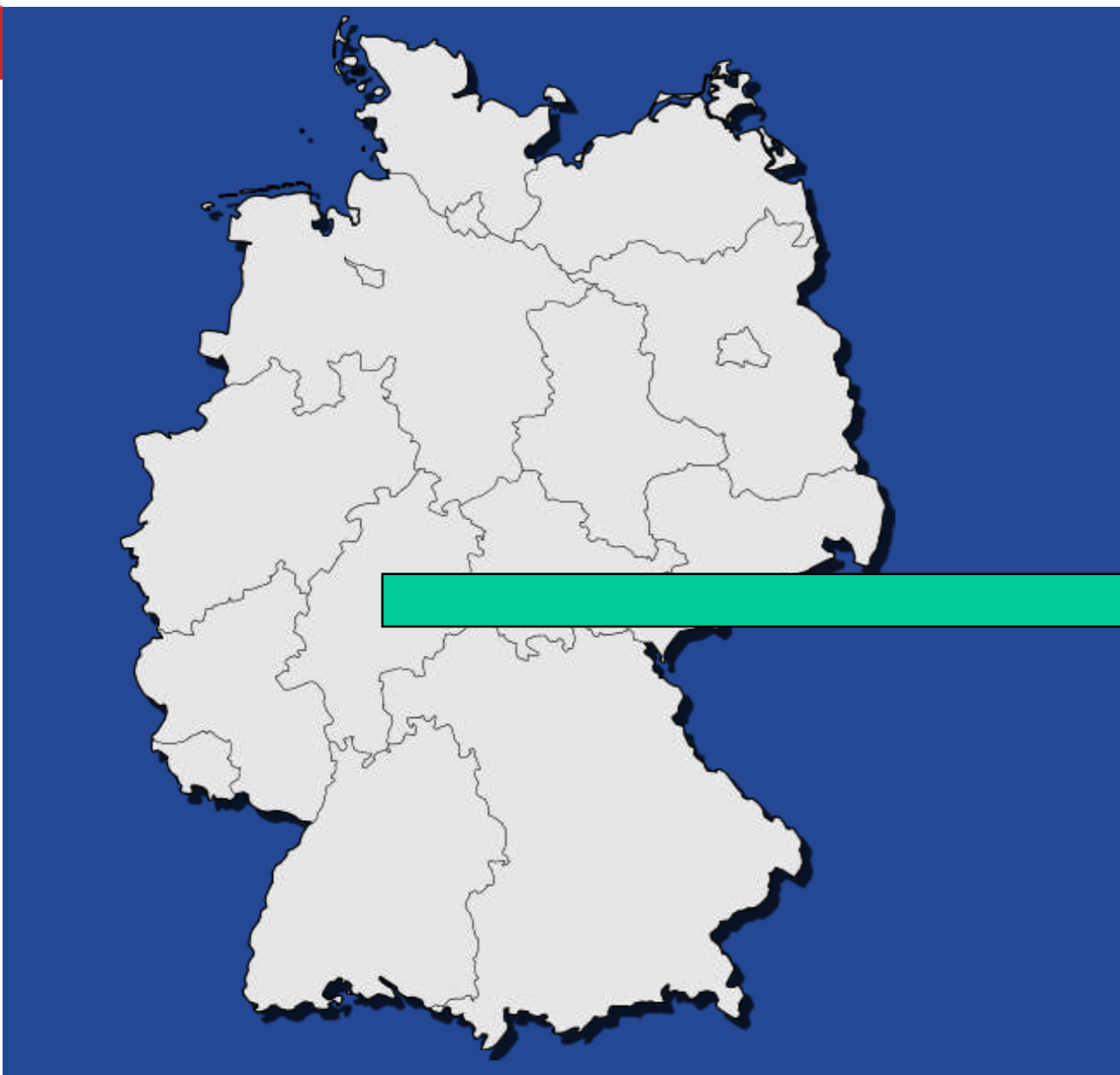
Case investigation

creating case specific Hash values
(alert, NR)

How to manage Mass-Data / Como gerir Massdata

let the investigators have a look directly

Organisation of Police in Hessen / Organização da Polícia



Organisation of Police in Hessen / Organização da Polícia Hessen

before 2002 only one unit for whole state

responsible for searchery and forensics

computer crime raises

2 years behind

Organisation of Police in Hessen / Organização da Polícia

in 2003 Re-Organisation HTCUC in Hessen

every Department get his own special unit
responsible for computer crime in cases of their
office

splitting Internet Investigation and Forensics

Organisation of Police in Hessen / Organização da Polícia

Forensic Units in Departments

HLKA
HSG13

PP NH
ZK50
RDVG

PP SOH
ZK50
RDVG

PP MH
ZK50
RDVG

PP WH
ZK50
RDVG

PP Ffm
K35
EG 1

PP SH
ZK50
RDVG

PP OH
ZK50
RDVG

Organisation of Police in Hessen / Organização da Polícia

forensic investigation decrease in most
departements down to 3 month behind

Organisation of Police in Hessen / Organização da Polícia Hessen

on time

- start thinking of reorganisation for computer crime
 - bringing Internet-Investigation, forensic examiners and technicians closer together

Organisation of Police in Hessen / Organização da Polícia Hessen

on time

- start of thinking about to renew
organisation at Prosecutors

specified units in Internet related crime

Statistics (State of Hesse) / Estadísticas



Thanks for your attention...
Obrigado pela sua atenção ...

Timo Schneider
HLKA- HSG13
Hölderlinstrasse 1-5
65185 Wiesbaden
Germany

Tel.: +49 611 831307
Fax: +49 611 831325
email: timo.schneider@sg613.de