HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

Digitale Forensik im Strafverfahren

Nacht der Wissenschaft – Hochschule Mittweida

Freitag, 13. Juni 2014

Michael Spranger

Prof. Dr. rer. nat. Dirk Labudde

Prof. Dr. iur. Frank Czerner

Erpresseranruf –

- eingespielt nach der Erpressermail -

„Hier spricht XXY:

Der hochwürdigste Herr Abt zu Altzelle soll 250.000 Euro heute, am Freitag dem 13. Juni Zweitausend-undvierzehn, nach dem Ballspiel der Spanier mit den Niederländern, zwischen den Teufelssteinen auf dem Galgenberg zu Mittweide, wo jetzt die Hochschule ihren Sitz gefunden, hinterlegen. Keine Polizei! Sonst wird die Stadtkirche zu Mittweide ihrer neuen Technik beraubt. Tempus fugit - carpe diem!“

Geplanter Übergabeort des Geldes: Teufelssteine auf dem Galgenberg

Informierung der Polizei: Strafverfahren beginnt

§ 253 StGB: Erpressung

(1) Wer einen Menschen rechtswidrig mit Gewalt oder durch Drohung mit einem empfindlichen Übel zu einer Handlung, Duldung oder Unterlassung nötigt und *dadurch* dem Vermögen des Genötigten oder eines anderen Nachteil zufügt, um sich oder einen Dritten zu Unrecht zu bereichern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Rechtswidrig ist die Tat, wenn die Anwendung der Gewalt oder die Androhung des Übels zu dem angestrebten Zweck als verwerflich anzusehen ist.

(3) Der *Versuch* ist strafbar. [hier [+]]

(4) In besonders schweren Fällen ist die Strafe Freiheitsstrafe nicht unter einem Jahr. Ein besonders schwerer Fall liegt *in der Regel* vor, wenn der Täter gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung einer Erpressung verbunden hat.

Art und Ausmaß der Kriminalität: Polizeiliche Kriminalstatistik (PKS)

Bundesministerium des Innern

Polizeiliche Kriminal-statistik 2012

Erfasste Fälle für **2012**:

5.997.040 *darunter:*

Erpressung: 9.920 Fälle (= 0,17%)

hiervon 6.263 Versuche (= 63%) – Versuchsstrafbarkeit (!)

5.929 Tatverdächtige

> für 2013 (noch unvollständig):

insges. 5.961.662 Fälle, darunter 12.496 Erpressungen

(gegenüber 2012 = + 26%)

Art und Ausmaß der Kriminalität: PKS > nur Hellfeldbereich

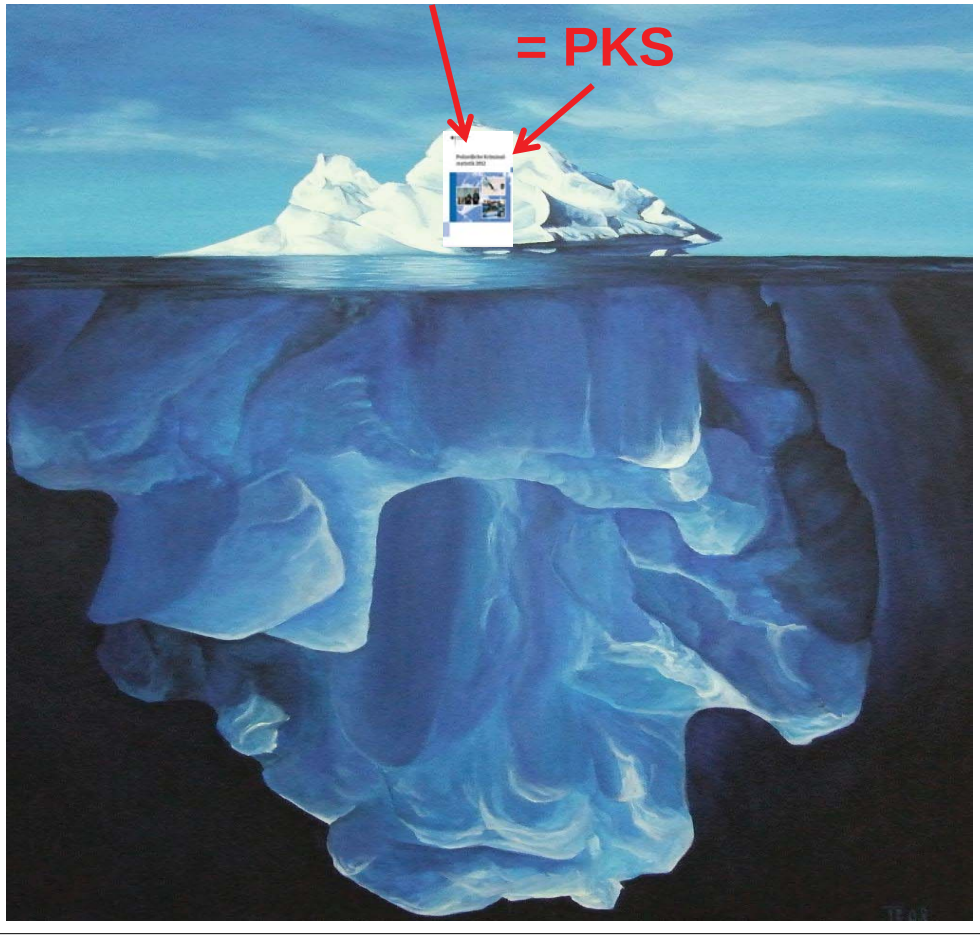
Hellfeld-/Dunkelfeld-Problematik

> darunter auch *Anzeigeverhalten* des Opfers, das für Hellfeld-/Dunkelfeldverschiebung verantwortlich ist

Opfer = informeller Agent der Sozialkontrolle / „Selektionsmacht des Opfers“

http://www.saz-aktuell.com/gallery/cache/689517dc38532d4155e32f91e3e6749b-360x276-1.jpg

...deshalb: Die offiziell registrierte Kriminalität (= Hellfeld) ist nur die Spitze..



Beginn des strafrechtlichen Ermittlungsverfahrens (§ 158 StPO)

http://www.booklooker.de/images/cover/user/0313/0810/Y2QwMjUw.jpg

Anfangsverdacht?

§ 152 II StPO

(1) Zur Erhebung der öffentlichen Klage ist die **Staatsanwaltschaft** berufen.

(2) **Sie** ist, soweit nicht gesetzlich ein anderes bestimmt ist, verpflichtet, wegen aller verfolgbaren Straftaten einzuschreiten, sofern *zureichende tatsächliche Anhaltspunkte* vorliegen.

Ermittlungsverfahren:

Vom Anfangs- zum hinreichenden Tatverdacht?

Prüfung der Staatsanwaltschaft, ob hinreichender Tatverdacht besteht

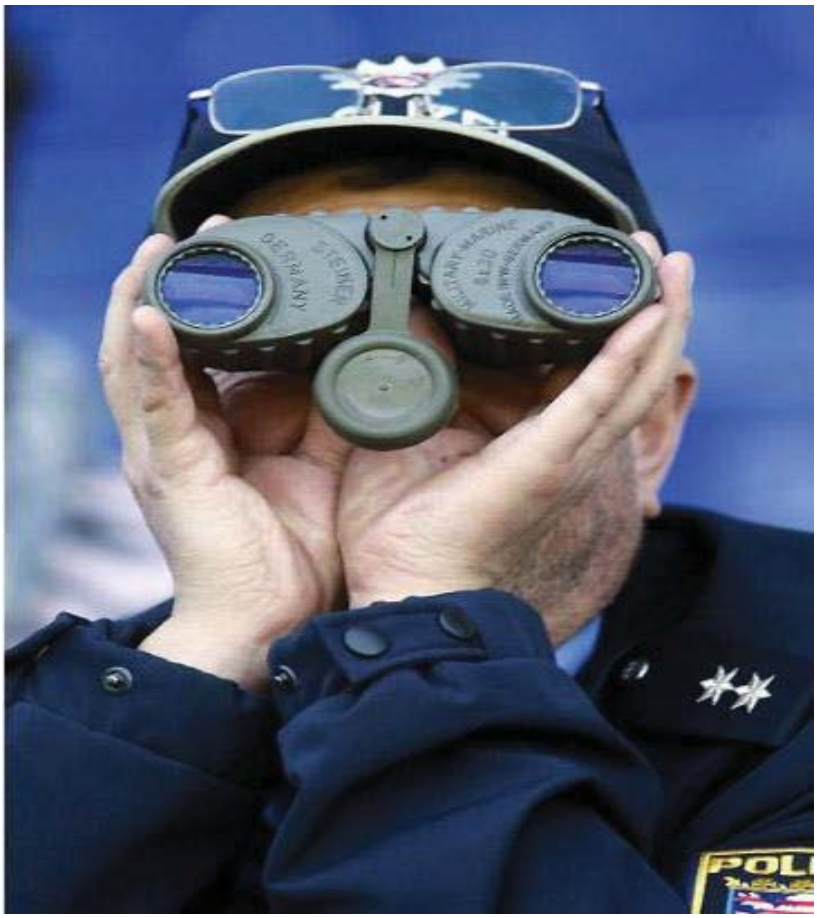
Beweiserhebung durch Polizei/StA

Falls TV (-): Einstellung

Falls TV (+): Anklage/Antrag auf Strafbefehl

ggf.: Einstellung/ Geldauflage (§ 153 a StPO)

Legalitätsprinzip - Verfolgungszwang



http://media1.faz.net/ppmedia/aktuell/sport/3886100968/1.563463/default/fans-im-fanblock-unter-ganz-genauer-beobachtung-der-polizei.jpg

• welches **Delikt**?

> § 253 StGB: Erpressung

• welche Ermittlungsmaßnahmen nach Strafverfahrensrecht (StPO) sind möglich bzw. zulässig?

Ermittlungsverfahren

- Ausgangspunkt: ***Anfangs***verdacht einer Straftat: Versuchsstadium einer Erpressung

„zureichende tatsächliche Anhaltspunkte“

> nicht lediglich vage Vermutungen

= Erpresser*mail* und Erpresser*anruf*

- Beweiserhebung durch StA/Polizei „in alle Richtungen“

> StA = „*objektivste Behörde der Welt*“: § 160 II StPO

Ermittlungsverfahren

Staatsanwaltschaftliche Ermittlungsmaßnahmen,

z.B.:
- Vernehmungen
- Haftbefehl
- Durchsuchung; Beschlagnahme
- Überwachung der Telekommunikation

Zwar grds.: „Ermittlungs-Generalklausel“ für Polizei/ Staatsanwaltschaft für *allgemeine, unspezifische* Maßnahmen, aber:

> Grundsätzliches Problem bei diesen Maß-nahmen: **Grundrechtseingriffe**!

Ermittlungsverfahren

§ 100a StPO: [Telekommunikationsüberwachung]

(1) Auch ohne Wissen der Betroffenen darf die Telekommuni-kation überwacht und aufgezeichnet werden, wenn

1. *bestimmte Tatsachen* den *Verdacht* begründen, dass jemand als Täter oder Teilnehmer eine in Absatz 2 bezeichnete *schwere Straftat* begangen, in Fällen, in denen der *Versuch strafbar* ist [[+], § 253 III StGB], zu begehen versucht, oder durch eine Straftat vorbereitet hat,

2. die Tat *auch im Einzelfall schwer wiegt* **und**

3. die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten *auf andere Weise wesentlich erschwert oder aussichtslos* wäre. [>>>]

Ermittlungsverfahren

(2) **Schwere Straftaten im Sinne des § 100 a Absatz 1 Nr. 1 StPO sind**: (= *numerus clausus!!!)*

1. aus dem Strafgesetzbuch:

a) Straftaten des Friedensverrats, des Hochverrats und der Gefährdung des demokratischen Rechtsstaates sowie des Landesverrats und der Gefährdung der äußeren Sicherheit nach den §§ 80 bis 82 […]

e) Geld- und Wertzeichenfälschung nach den §§ 146 und 151, […]

f) Straftaten gegen die sexuelle Selbstbestimmung in den Fällen der §§ 176a, 176b, 177 Abs. 2 Nr. 2 [….]

g) Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften nach § 184b Abs. 1 bis 3 […]

h) Mord und Totschlag nach den §§ 211 und 212,

i) Straftaten gegen die persönliche Freiheit nach den §§ 232 bis 233a, 234, 234a, 239a und 239b,

j) Bandendiebstahl nach § 244 Abs. 1 Nr. 2 und schwerer Bandendiebstahl nach § 244a,

k) Straftaten des Raubes und der Erpressung nach den §§ 249 bis 255,

l) gewerbsmäßige Hehlerei, Bandenhehlerei und gewerbsmäßige Bandenhehlerei nach den §§ 260 und 260a,

m) Geldwäsche und Verschleierung unrechtmäßig erlangter Vermögenswerte nach § 261 Abs. 1, 2 und 4,

n) Betrug und Computerbetrug […]

s) gemeingefährliche Straftaten in den Fällen der §§ 306 bis 306c, 307 Abs. 1 bis 3, des § 308 Abs. 1 bis 3, des § 309 […], des § 310 Abs. 1, der §§ 313, 314, 315 Abs. 3, des § 315b Abs. 3 sowie der §§ 316a und 316c […]

2. aus der Abgabenordnung [= Steuerhinterziehung]

3. aus dem Arzneimittelgesetz […]; 4. aus dem Asylverfahrensgesetz […] 7. aus dem Betäubungsmittelgesetz […]

9. aus dem Kriegswaffenkontrollgesetz […]; 11. aus dem Waffengesetz […]

10. aus dem Völkerstrafgesetzbuch (Völkermord, Verbrechen gegen die Menschlichkeit, Kriegsverbrechen)

Ermittlungsverfahren

Telekommunikation:

„Technischer Vorgang des Aussendens, Übermittelns und Empfangens von Nachrichten jeglicher Art in der Form von Zeichen, Sprache, Bildern oder Tönen mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können.“

(Anlehnung an § 3 Nr. 22, 23 TKG)

Quelle: Meyer-Goßner, StPO, 54. Aufl. 2014, § 100a Rdz. 6

http://content.stuttgarter-nachrichten.de/media_fast/626/Polizeianruf_1557260.JPG

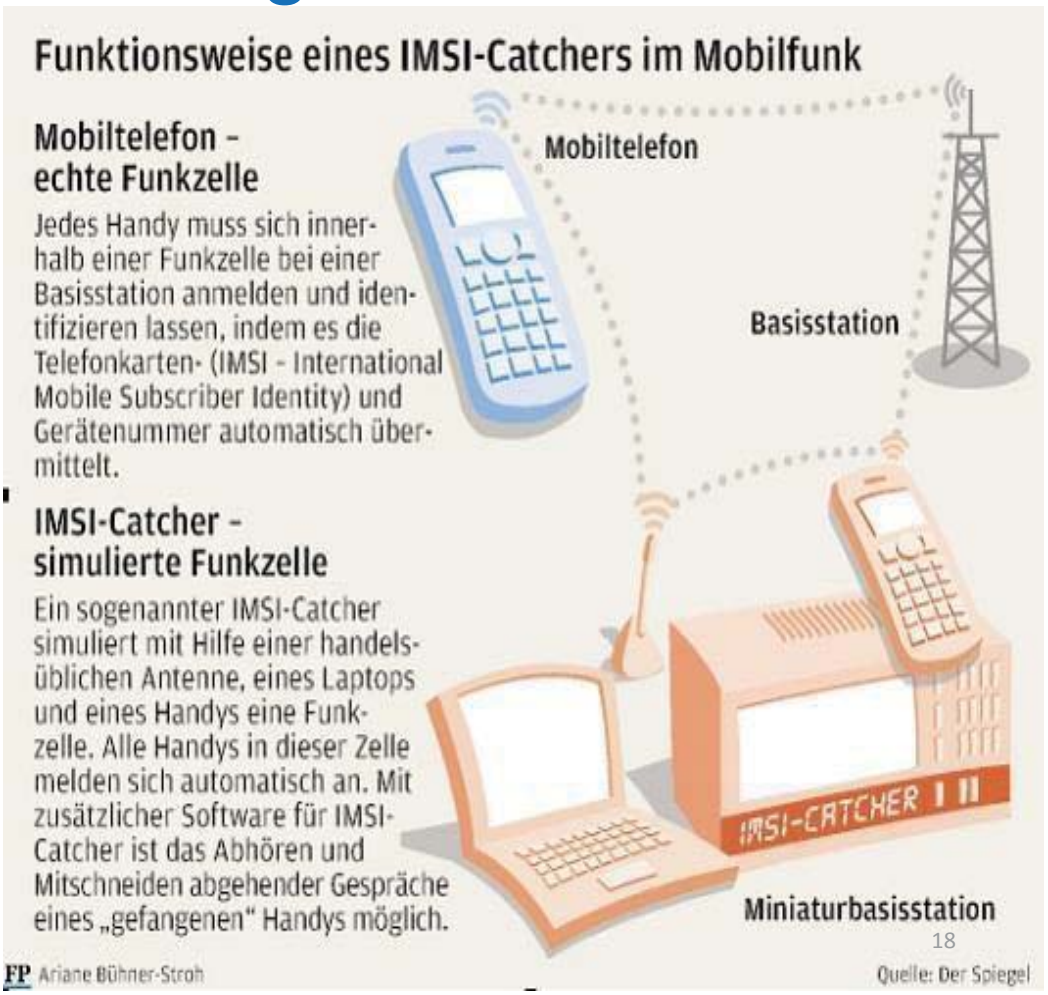
Absenden der Mail > Ankommen der Mail im Speicher des Providers und Abrufen der Mail durch den Empfänger: durch § 100a StPO erfasst

Ermittlungsverfahren

Technische Voraussetzungen für Handy-Ortung gem. § 100 i I 1 StPO:

BVerfG (2BvR 1345/03)

> ungefähre Kenntnis des Aufenthaltsorts eines Mobiltelefons des Tatverdächtigen



http://www.freiepresse.de/DYNIMG/21/58/3852158_W620.jpg

Ermittlungsverfahren

§ 94 StPO: Beschlagnahme

[Sicherstellung und **Beschlagnahme** von Gegenständen zu **Beweiszwecken**]

(1) Gegenstände, die als Beweismittel für die Untersuchung von Bedeutung sein *können*, sind in Verwahrung zu nehmen oder in anderer Weise sicherzustellen.

(2) Befinden sich die Gegenstände in dem Gewahrsam einer Person und werden sie nicht freiwillig herausgegeben, so bedarf es der **Beschlagnahme**.

http://img.mittelbayerische.de/bdb/2108900/2108901/300x.jpg

Digitale Forensik im Sachverständigengutachten:

- Pflicht zur umfassenden Aufklärung des Sachverhalts
- Wie weit reicht die eigene (persönliche) Sachkunde des Gerichts?
- Kompetenz-Kompetenz
- Auswahl und Bestellung der jeweils erforderlichen Sachverständigen – schon zu Beginn des Ermittlungsverfahrens möglich: > z.B. einen Sachverständigen auf dem Gebiet der **digitalen Forensik** zur Untersuchung der als Beweismittel sichergestellten/beschlagnahmten digitalen Medien (Handy > Erpresseranruf und Computer > Erpressermail)

Nach: http://www.christian-gabel.de/images/page32_pic001.jpg

FORENSISCHE UNTERSUCHUNG

Ausführende Stelle: FoSIL Mittweida

Einführung

Kriminalistische Ermittlungen erfordern häufig die Sicherstellung von Computern, mobilen Kommunikationsgeräten oder Datenträgern.

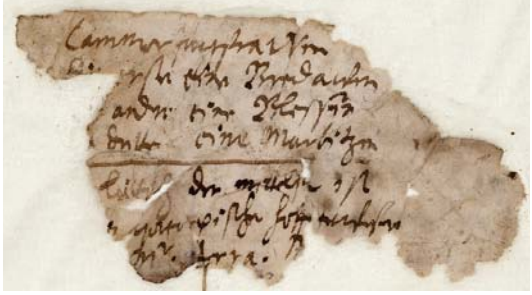
Ziel: Separierung und Extraktion fallrelevanter Informationen

Einführung

- Textkategorisierung und Relevanz-Clustering
- Suche nach Entitäten und Relationen
- Exploration von Personennetzwerken und Aufdeckung geplanter Aktivitäten
- Erkennen und Verstehen von *Versteckter Semantik*
- Suche und Sicherung beweiserheblicher Informationen

Eigenschaften forensischer Texte

Eigenschaften forensischer Texte



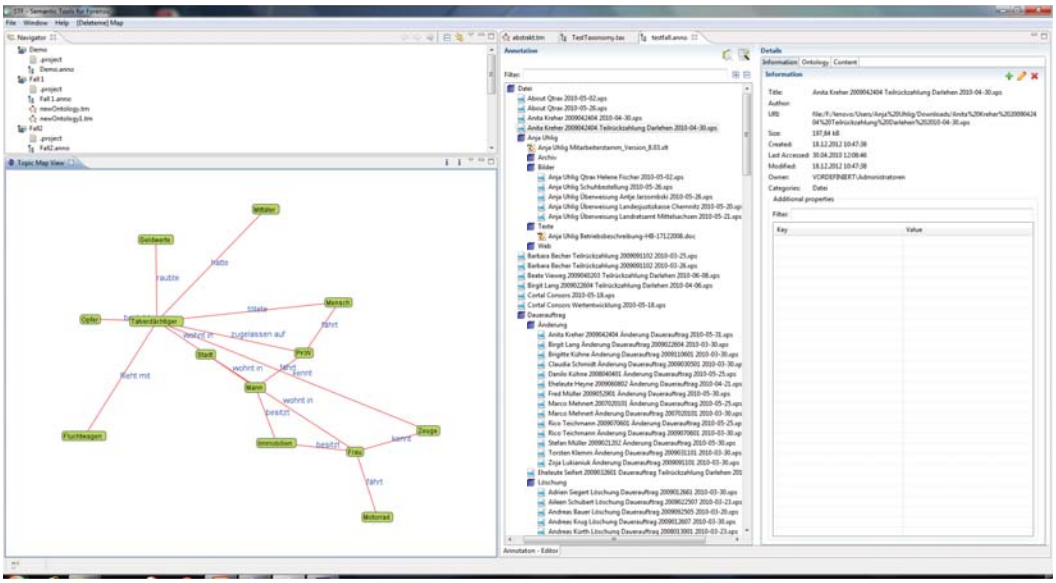
Michael Spranger Semantic Tools for Forensics 3 / 25

Untersuchungsauftrag

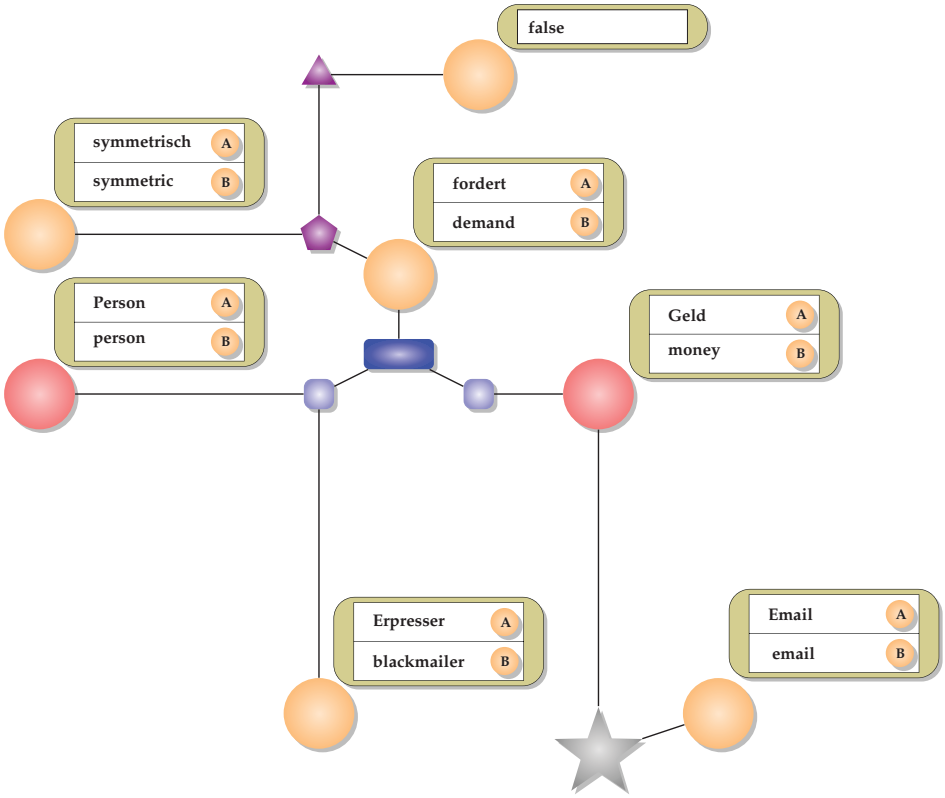
Staatsanwaltschaft
Chemnitz

1. Ist der Tatverdächtige *Eduard der Entschlossene* alias *XXX* der Verfasser des aktuellen Erpresserschreibens?
2. Besteht Identität zwischen dem Anrufer und dem Verfasser des Erpresserschreibens?
3. Gibt es weitere Geschädigte/Opfer?

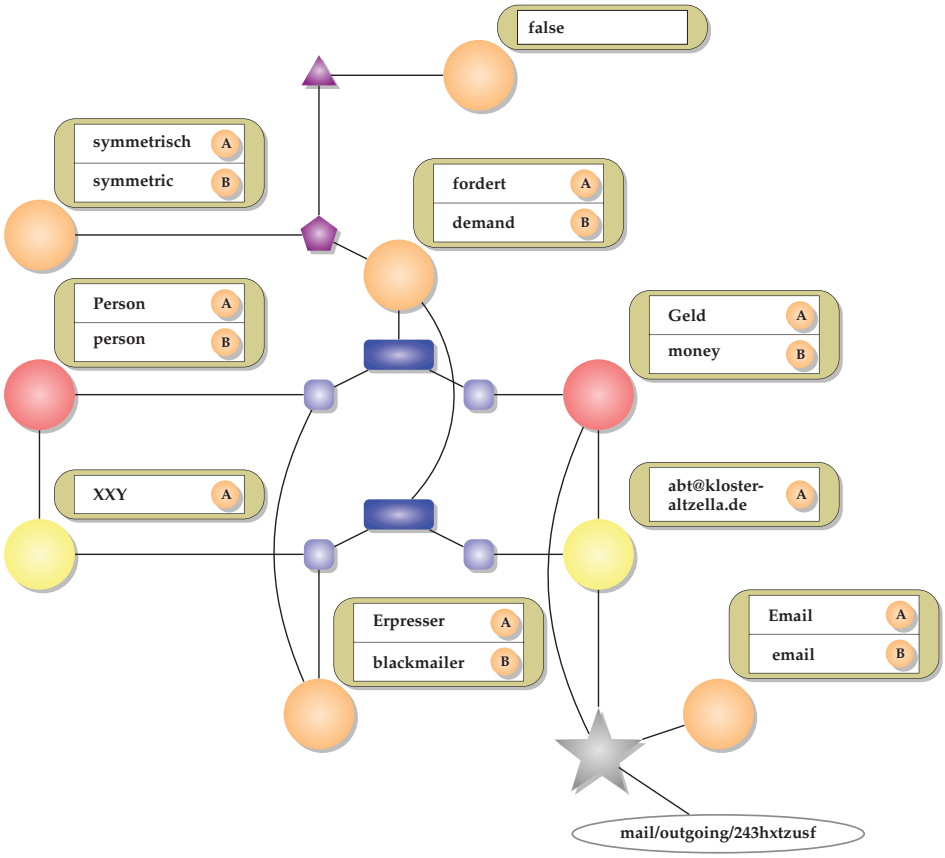
Semantic Text Analyzer



Forensische Topic Map



Forensische Topic Map - instantiiert



Prozess der forensischen Textanalyse

Präprozess

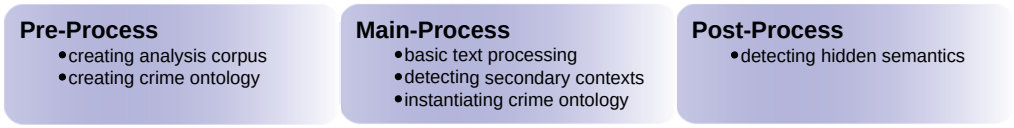
- **Textkategorisierung**, Separierung fallrelevanter Daten
- Textextraktion/OCR
- Erstellung der forensischen Ontologie

Hauptprozess

- syntaktische und semantische Annotation
- Instantiierung der forensischen Ontologie

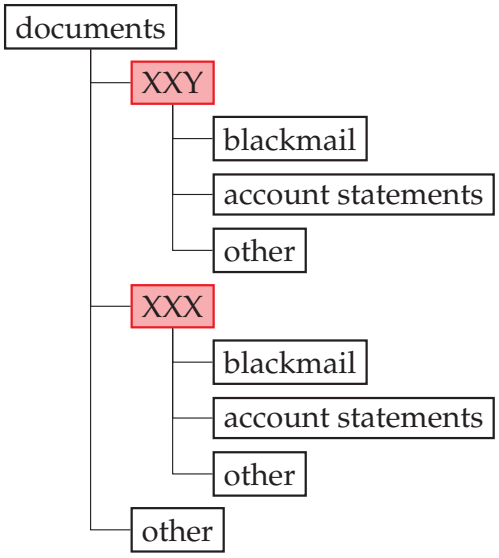
Postprozess

- **Zuweisung forensischer Rollen**
- Erkennung versteckter Semantik



Textkategorisierung — Schritt 1

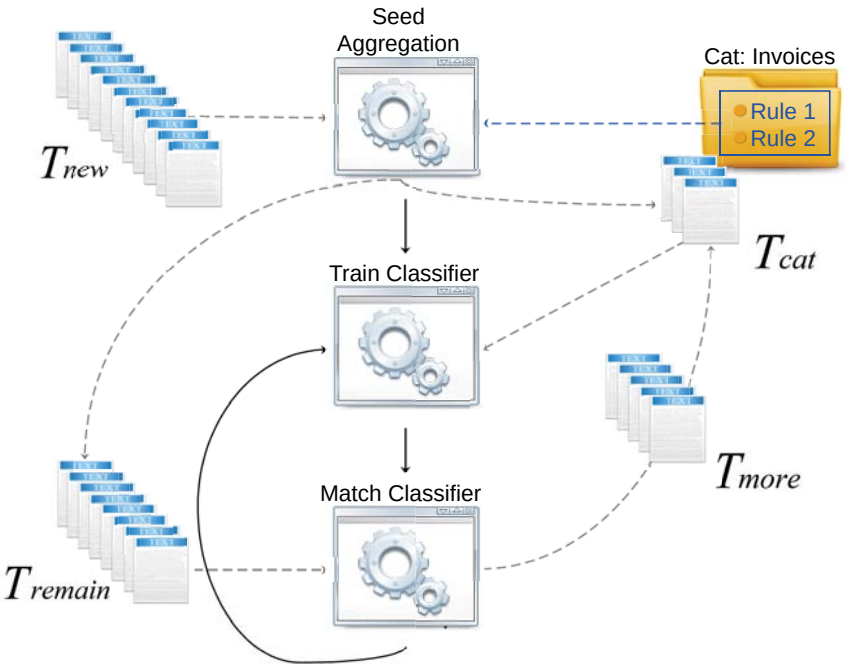
Kategoriedefinition



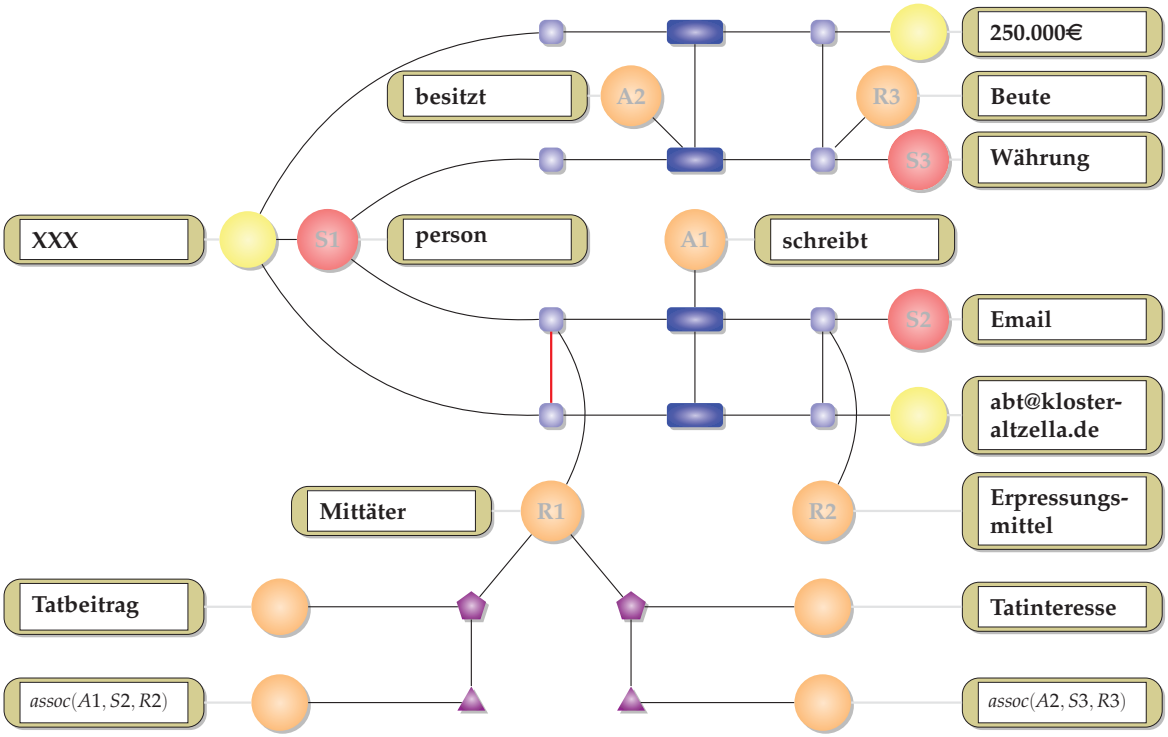
Regeldefinition

- Muster, Zeiträume, MIME, etc.
- angewandt auf Dateiname, Metadaten, Inhalt
- ODER-verknüpft innerhalb einer Kategorie
- UND-verknüpft zwischen Kategorien eines Zweiges

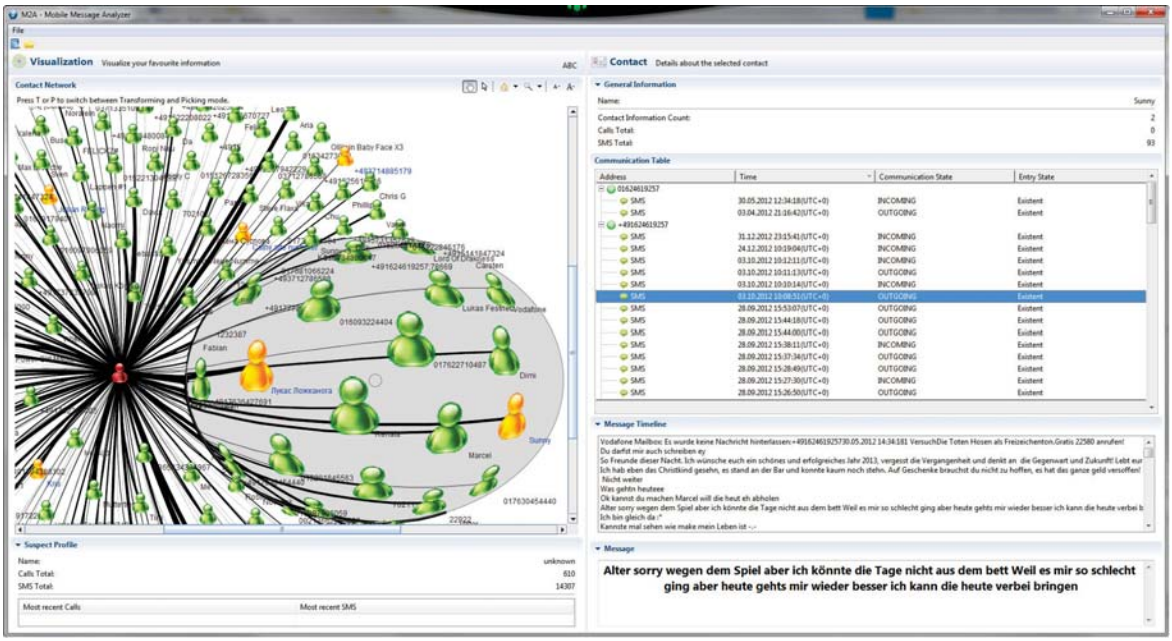
Textkategorisierung — Schritt 2



Zuweisung forensischer Rollen



Mobile Message Analyzer (M2A)

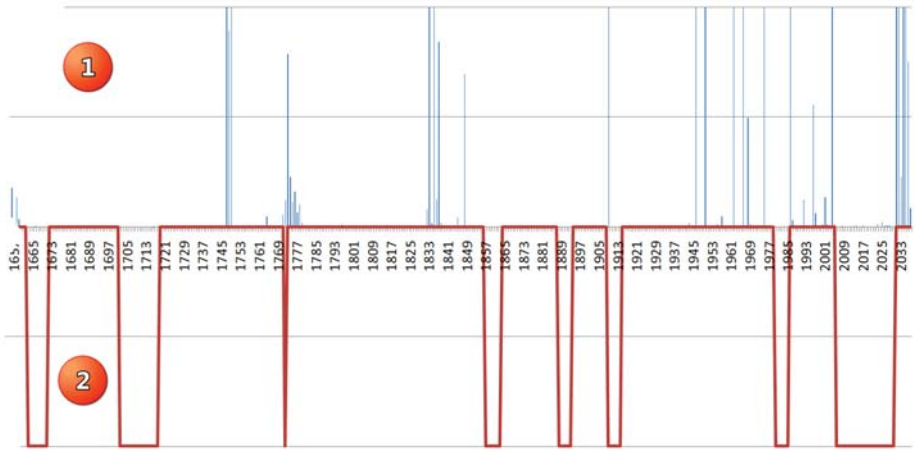


Charakteristik von Kurznachrichten

Low.du.sein, .gramatig.gelehrnt.bei.meister.yoda.ich.haben!!!!XDDD.
Yeaaaaaah.ich.bin.jetzt.so.krank.wieDu.xD
Jetzt kann ich mir keine drehen Weil Meine papers bei dir liegen
Wirklich?
Ja.xddd
Naja ich zock rauch und schreib mit dia
Ich.glaube.Du.haste.gerade.genauso.wenig.zutun.wie.ich.xd
Und ich rauch meine schon!!!jaa!!^_^
Ich dreh mir gerade eineeeeeeeeee
Ey willst Du am 1.2 mit nach berlin? Emily und Cathy gehen auf ein konzert und wir können ja bissl in Berlin chilln mit bissl was zum smoken und ja xD
Kp.wesch.itze.noch.nii!!!:D

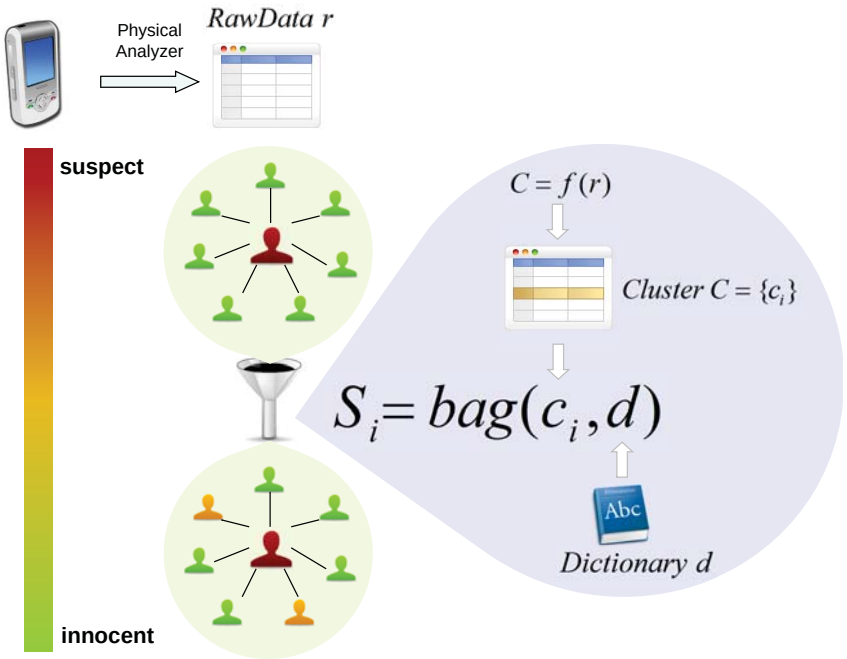
- keine konsistenten Satzstrukturen
- Tippfehler/T9-Fehler
- Affinität zu Subsprachen
- emotionsbedingt veränderte Schreibweisen
- situationsbedingtes Fehlen des Kontextes

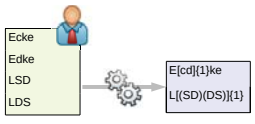
Separierung von Gesprächen

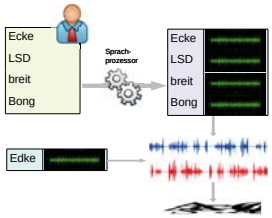


- lange Pausen fast nie im Bereich von relevanten Textabschnitten
- $\Rightarrow$ Pausenlänge als Basis zur Separierung von Dokumenten
- Problem: abhängig vom individuellen Kommunikationsverhalten

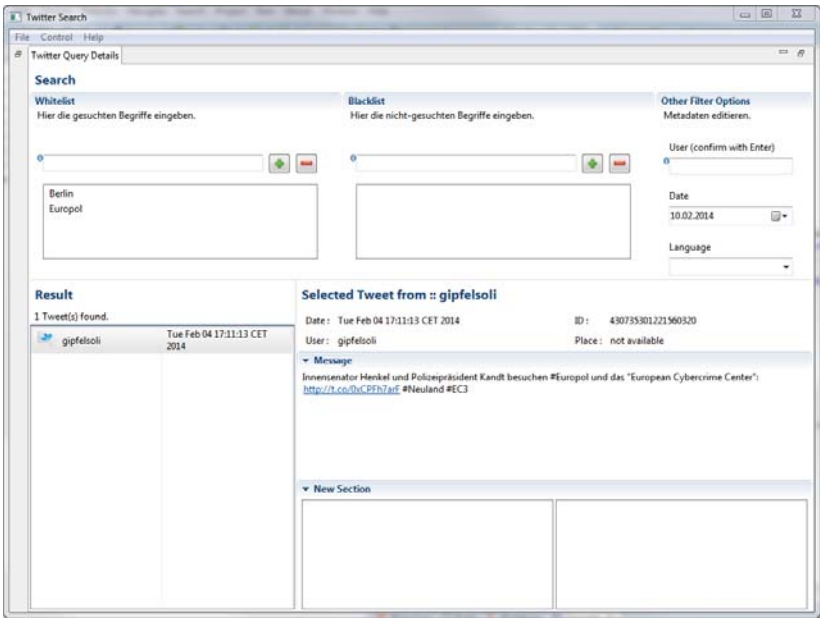
Analyse von Kurznachrichten







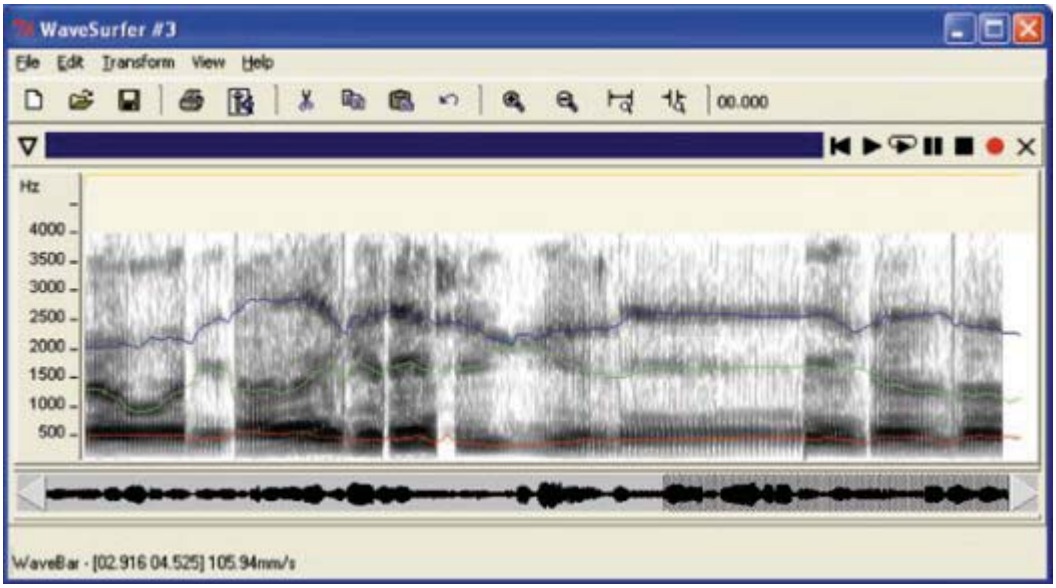
Social Search



Erzeugung von Zielgruppenprofilen

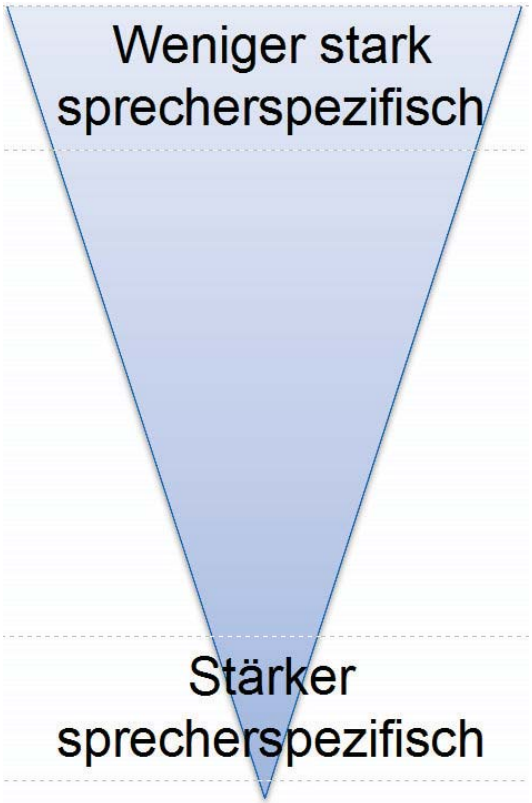
- Lernen von zielgruppenspezifischen Gemeinsamkeiten
- profilbasierte, verdachtsunabhängige Suche/Überwachung von Online-Aktivitäten
- Unterstützung der Instantiierung einer forensischen Topic Map

Phonetische Analyse



Phonetische Merkmale/ Voiceprint

- Geschlecht
- Alter
- Gewicht und Größe?
- Dialekt, Soziolekt, Idiolekt
- mittlerer F0
- Alkohol, Nikotin ?
- Stimmumfang
- Häsitationen
- nonverbal, z.B. schnalzen, räuspern
- pathologische Auffälligkeiten



Sprecheridentifikation durch Zeugen

Sprechererkennung durch Laien sinnvoll, wenn große Vertrautheit mit der Stimme oder besonders auffallende Stimme vorliegt

Erinnerungsvermögen an einer Stimme

- 2 Tage später 83 % korrekte Identifizierung
- 2 Wochen später 68 %
- nach 5 Monaten 13 %

Sprecheridentifikation durch Experten

Einzelstimmenanalyse

- erstellt Täterprofil
- biologische, soziale oder regionale Zuordnung

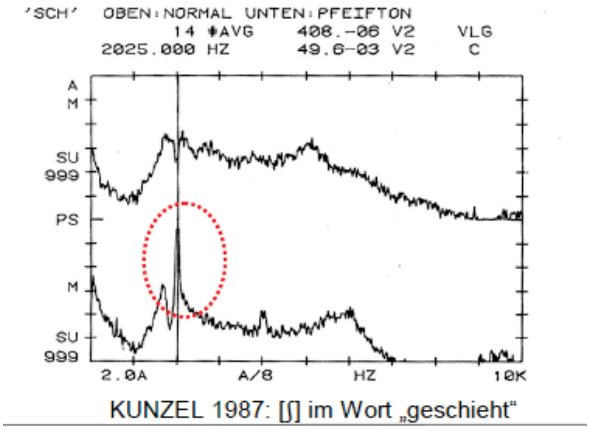
Stimmenvergleich

- mind. 2 Sprechproben (Tat- / Vergleichsaufnahme)
- basiert auf Einzelstimmenanalysen, die systematisch verglichen werden

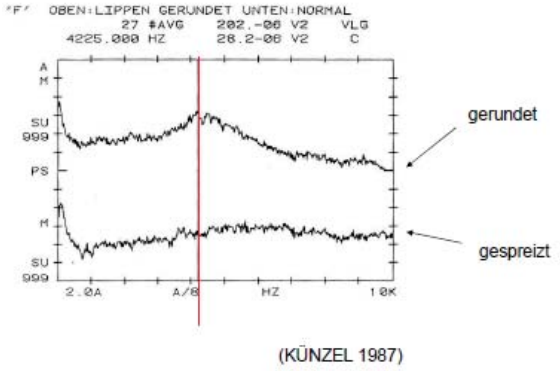
Verfahren

- Analyse der Laufgeschwindigkeit
- Überprüfung der Authentizität
- Auditive Analyse (Wahrnehmung durch den Hörer)
- Akustische Analyse (Charakteristik im normalen Sprechzustand/Grenzen, Umgebungsgeräusche)

Besonderheiten



KUNZEL 1987: [ʃ] im Wort „geschieht"



(KÜNZEL 1987)

Leistungsfähigkeit

- Problem: **menschliche Stimme ist variabel**
- **Stimmabdruck ist nicht so sicher** wie der Fingerabdruck
- **Variabilität von Sprechproben** einer Person ist u.a. abhängig von Faktoren:
  - Innere (psychische) und äußere Sprechsituation
  - Körperlichen Zustand des Sprechers (Erkältung oder Alkohol)
  - Absichtliche Veränderung der Sprechweise
- **Aussagen** können **nie** über die **Identität von Sprechern** gemacht werden
  - Aussagen nur möglich über eine hinreichende Ähnlichkeit von Sprechproben

Günstige Bedingungen

- Ausreichende technische Qualität der Tonaufnahme
- Ausreichende Zeitdauer der Aufnahme
- Möglichst geringe emotional oder durch eine Verstellungsabsicht bedingte Differenz zwischen den zu vergleichenden Aufnahmen
- Vorhandensein einer auffälligen Sprechweise aufgrund individueller Gewohnheiten oder Anomalien (Zahnschäden)

Gutachten

Frage 1:

Ist der Tatverdächtige *Eduard der Entschlossene* alias *XXX* der Verfasser des aktuellen Erpresserschreibens?

Ergebnis:

Eduard der Entschlossene ist mit an Sicherheit grenzender Wahrscheinlichkeit der Verfasser des aktuellen Erpresserschreibens.

Gründe:

1. Email mit dem Erpresserschreiben wurde als gesendete Nachricht im Postfach des TV festgestellt
2. TV ist einzig Zugangsberechtigter für den sichergestellten Computer
3. Fingerabdrücke des TV wurden auf der zugehörigen Tastatur festgestellt

GUTACHTEN

Frage 2:

Besteht Identität zwischen dem Anrufer und dem Verfasser des Erpresserschreibens?

Ergebnis:

Mit an Sicherheit grenzender Wahrscheinlichkeit ist Identität anzunehmen.

Gründe:

1. phonetische Stimmidentität nach Aufnahme eines Vergleichsmusters
2. Übereinstimmung in allen feststellbaren phonetischen Merkmalen
3. es liegt zusätzlich ein besonders auffälliges Merkmal vor (Zahnlücke)

GUTACHTEN

Frage 3:

Gibt es weitere Geschädigte/Opfer?

Ergebnis:

Folgende Gründe rechtfertigen die Annahme, dass auch Kloster Buch erpresst wurde.

Gründe:

1. Erpresserschreiben an Abt Kloster Buch im Dokumente-Ordner

Fall aufgeklärt