Manipulationen und Widersprüchlichkeiten gesammelt

→ **Übersicht**

A (A.1–A.7) Kopierter Header → Beweis, dass die E-Mail von 10.12.21 eine Fälschung ist

B (B.1–A.3) Widersprüche Anlage → Manipulationshinweise bei den Emails von 14.01.22

C (C.1–C.2) Aussagekraft Fotos → Fotos lassen sich weder einem Ort noch einem Zeitpunkt zuordnen

D Falsche Schreibweise Name → Angebliche Zeugin und Beschuldigende schreiben Vornamen des Beschuldigten auf gleiche Weise falsch

Hinweise:

- ■ Die schwarzen Anonymisierungen waren bereits im uns vorgelegten Material vorhanden
  ■ Die lila Anonymisierungen wurden zusätzlich von uns vorgenommen, um Persönlichkeitsrechte zu schützen
- Die Nummerierungen der Anlagen beziehen sich auf das durch die Beschuldigende vorgelegte Beweismaterial

A: Zusammenkopierter Header

Bei der ersten E-Mail (Anlage 2) wurde der Header der zweiten E-Mail (Anlage 3) kopiert und offenbar mit einem neuen, selbst verfassten Text versehen.

→ **Durch sieben verschiedene Merkmale ist diese Manipulation nachweisbar.**

1. **Die gleiche X-Sender-IP**
2. **Identischer Spam-Score-Header**
3. **Identische Received-Header**
4. **Manipulierte Message-ID**
5. **Gefälschte Zeiten**
6. **Fehler im E-Mail-Header**
7. **Fehlender X-UIDL-Header**

Übersicht Fehler Header gesamt

Anlage 2

Subject: update
From: "Jennifer Hills" <jennifer.hills@skymail.de>
5 **Date:** 10.12.21, 16:44
An: [redacted]
X-Mozilla-Status: 0001
6 **X-Mozilla-Status2:** 000000
6 **X-Mozilla-Keys:** Return-Path: <jennifer.hills@skymail.de>
7 **Delivered-To:** [redacted]
Received: (qmail 27533 invoked by uid 498); 10 Dec 2021 16:30:17 -0000
Received: from skymail.de (skymail.de [46.4.105.4]) by faye.uberspace.de (Haraka/2.8.28) with
3 ESMTPS id 194281A9-6D5F-461D-B399-CB0DFF7A98E0.1 envelope-from
<jennifer.hills@skymail.de> tls TLS_DHE_RSA_WITH_AES_256_GCM_SHA384; Fri, 10 Dec
5 2021 16:27:14 +0100
Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skymail.de with ESMTP id
03CA6BE9 for [redacted]; Fri, 10 Dec 2021 15:26:54 +0100 (CET)
MIME-Version: 1.0
4 **Message-ID:** <bbb970df1ad1e1e0bcc7667903b7c357@skymail.de>
4 **Message-ID:** <bbb124974c975f94zaa976eud8834027@skymail.de>
X-Mailer: b1gMail/7.4.0
1 **X-Sender-IP:** 185.117.215.9
Reply-To: Jennifer Hills <jennifer.hills@skymail.de>
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline
X-Abuse-Report: absuse@emailn.de
X-Rspamd-Bar: -
2 **X-Rspamd-Report:** R_SPF_ALLOW(-0.2) BAYES_HAM(-1.691486) MIME_HTML_ONLY(0.2)
R_MIXED_CHARSET(0.530303)
2 **X-Rspamd-Score:** -1.161183

Anlage 3

Betreff: Treffen
Von: "Jennifer Hills" <jennifer.hills@skymail.de>
Datum: 13.12.21, 06:44
An: [redacted]
X-Mozilla-Status: 0001
X-Mozilla-Status2: 00000000
X-Account-Key: account1
X-UIDL: 00000c9a5f9abe12
Return-Path: <jennifer.hills@skymail.de>
Delivered-To: [redacted]
Received: (qmail 27533 invoked by uid 498); 13 Dec 2021 05:44:34 -0000
Received: from skymail.de (skymail.de [46.4.105.4]) by faye.uberspace.de
(Haraka/2.8.28) with ESMTPS id 194281A9-6D5F-461D-B399-CB0DFF7A98E0.1
envelope-from <jennifer.hills@skymail.de> tls
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384; Mon, 13 Dec 2021 06:44:29 +0100
Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skymail.de with
ESMTP id 03CA6BE9 for [redacted]; Mon, 13 Dec 2021 06:44:24
+0100 (CET)
MIME-Version: 1.0
Nachricht-ID: <bbb970df1ad1e1e0bcc7667903b7c357@skymail.de>
X-Mailer: b1gMail/7.4.0
X-Sender-IP: 185.117.215.9
Antwort an: "Jennifer Hills" <jennifer.hills@skymail.de>
Content-Type: text/html; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline
X-Abuse-Report: absuse@emailn.de
X-Rspamd-Bar: -
X-Rspamd-Report: R_SPF_ALLOW(-0.2) BAYES_HAM(-1.691486)
MIME_HTML_ONLY(0.2) R_MIXED_CHARSET(0.530303)
X-Rspamd-Score: -1.161183

A1: Die gleiche X-Sender-IP

Beide E-Mails (Anlage 2 und 3) stammen von der selben IP-Adresse. Bei der sogenannten X-Sender-IP handelt es sich um sogenannte Tor-Exit-Knoten. Es wurde also die Anonymisierungssoftware Tor bzw. der sogenannte Tor-Browser zum Versenden der E-Mails verwendet. Aber: Tor ändert ca, alle zehn Minuten die IP-Adresse, um die Spuren der Nutzer:innen im Netz zu verwischen.

→ **Dass zwei E-Mails die mit drei Tagen Abstand verschickt worden sein sollen die gleiche X-Sender-IP haben, ist bei über 1000 verschiedenen Tor-Exit-Knoten nahezu unmöglich.**

X-Sender-IP Anlage 2

Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skyr
03CA6BE9 for [redacted]; Fri, 10 Dec 2021 15:26:54 +
MIME-Version: 1.0
Message-ID: <bbb970df1ad1e1e0bcc7667903b7c357@skymail.de>
Message-ID: <bbb124974c975f94zaa976eud8834027@skymail.de>
X-Mailer: b1gMail/7.4.0
X-Sender-IP: 185.117.215.9
Reply-To: Jennifer Hills <jennifer.hills@skymail.de>

X-Sender-IP Anlage 3

Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skyr
ESMTP id 03CA6BE9 for [redacted] Mon, 13 Dec 2021
+0100 (CET)
MIME-Version: 1.0
Nachricht-ID: <bbb970df1ad1e1e0bcc7667903b7c357@skymail.de>
X-Mailer: b1gMail/7.4.0
X-Sender-IP: 185.117.215.9
Antwort an: "Jennifer Hills" <jennifer.hills@skymail.de>

A2: Identischer Spam Score Header

Der X-Rspamd-Score Header der ersten beiden E-Mails ist gleich (-1.161183). Auch der gesamte X-Rspamd-Report Header ist exakt gleich, inkl. aller dort gelisteten Scores der Spam-Klassifizierer. Es ist auch ersichtlich, dass der Bayes-Ham Score gleich ist. Bei diesem Spam-Filter werden (Ketten von) Wörtern in E-Mails geprüft, um einen Score zu errechnen, der hier bis auf die sechste Nachkommastelle gleich sein soll.

→ **Dies ist bei zwei E-Mails mit komplett unterschiedlichem Inhalt schlichtweg unmöglich und für sich alleine ein hinreichender Beweis, dass einer diese E-Mails nicht in dieser Form versendet, also manipuliert, worden ist.**

Identischer Spam Score Header Anlage 2

X-Abuse-Report: absuse@emailn.de
X-Rspamd-Bar: -
X-Rspamd-Report: R_SPF_ALLOW(-0.2) BAYES_HAM(-1.691486) MIME_I
R_MIXED_CHARSET(0.530303)
X-Rspamd-Score: -1.161183

Identischer Spam Score Header Anlage 3

X-Abuse-Report: absuse@emailn.de
X-Rspamd-Bar: -
X-Rspamd-Report: R_SPF_ALLOW(-0.2) BAYES_HAM(-1.691486
MIME_HTML_ONLY(0.2) R_MIXED_CHARSET(0.530303)
X-Rspamd-Score: -1.161183

A3: Identische Received-Header

Die Received Header der ersten und zweiten Nachricht sind bis auf die Zeiten identisch. Darin enthalten sind ESMTP-IDs, die bei zwei verschiedenen E-Mails nicht identisch sein dürfen, es hier aber sind.

→ **Zwei verschiedenen E-Mails dürfen keine identischen ESMTP-IDs haben.**

Identische Received-Header Anlage 2

X-Mozilla-Keys: Return-Path: <jennifer.hills@skymail.de>
Delivered-To: [redacted]
Received: (qmail 27533 invoked by uid 498); 10 Dec 2021 16:30:17 -0000
Received: from skymail.de (skymail.de [46.4.105.4]) by faye.uberspace.de (Hara
ESMTPS id 194281A9-6D5F-461D-B399-CB0DFF7A98E0.1 envelope-from
<jennifer.hills@skymail.de> tls TLS_DHE_RSA_WITH_AES_256_GCM_SHA
2021 16:27:14 +0100
Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skymail.de wi

Identische Received Header Anlage 3

X-UIDL: 00000c9a5f9abe12
Return-Path: <jennifer.hills@skymail.de>
Delivered-To: [redacted]
Received: (qmail 27533 invoked by uid 498); 13 Dec 2021 05:44:34 -0000
Received: from skymail.de (skymail.de [46.4.105.4]) by faye.uberspace.de
(Haraka/2.8.28) with ESMTPS id 194281A9-6D5F-461D-B399-CB0DFF7A98E0.1
envelope-from <jennifer.hills@skymail.de> tls
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384; Mon, 13 Dec 2021 06:44:29 +0100
Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skymail.de with

A4: Manipulierte Message-ID

Die erste E-Mail hat zwei unterschiedliche Message-IDs (Message-ID ist in der Regel eine weltweit eindeutige Kennzeichnung einer E-Mail Nachricht). Das ist aber unmöglich, da eine E-Mail nur über eine Message-ID verfügen kann. Die erste der IDs ist darüber hinaus identisch mit der Message-ID der zweiten E-Mail. Ein weiterer Beleg, dass per Copy-Paste der Header der zweiten E-Mail als Vorlage für die erste E-Mail benutzt wurde.

→ **Jede E-Mail kann nur über eine einzige Message-ID verfügen.**

Manipulierte Message-ID Anlage 2

2021 16:27:14 +0100
Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skymail.de wi
03CA6BE9 for [redacted]; Fri, 10 Dec 2021 15:26:54 +0100 (CE
MIME-Version: 1.0
Message-ID: <bbb970df1ad1e1e0bcc7667903b7c357@skymail.de>
Message-ID: <bbb124974c975f94zaa976eud8834027@skymail.de>
X-Mailer: b1gMail/7.4.0
X-Sender-IP: 185.117.215.9

Manipulierte Message-ID Anlage 3

Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skymail.de
ESMTP id 03CA6BE9 for [redacted] Mon, 13 Dec 2021 06:44
+0100 (CET)
MIME-Version: 1.0
Nachricht-ID: <bbb970df1ad1e1e0bcc7667903b7c357@skymail.de>
X-Mailer: b1gMail/7.4.0
X-Sender-IP: 185.117.215.9
Antwort an: "Jennifer Hills" <jennifer.hills@skymail.de>

A5: Gefälschte Zeiten

Beim Manipulieren der Zeitstempel wurden offensichtliche Fehler gemacht: So sind die Zeiten, an denen E-Mails empfangen bzw. verschickt worden sind, nicht schlüssig. Diese betreffen die Umrechnung der Zeitzonen sowie eine unmögliche Senden/Empfangen-Zeitachse. Rechnet man die Zeiten alle in „unsere“ Zeit also CET/MEZ um, ergibt sich folgendes Bild:

→ Zeitpunkt 1: 16:44 CET die E-Mail wird von jennifer.hills@skymail.de abgeschicht
→ Zeitpunkt 2: 15:26:54 CET die E-Mail kommt beim Mailserver von Skymail an
→ Zeitpunkt 3: 16:27:14 CET der Empfänger Mailserver XXXX.de erhält die E-Mail
→ Zeitpunkt 4: 17:30:17 CET die E-Mail wird in die Mailbox von XXXX@XXXX.de zugestellt

Weder kann eine E-Mail durch die Zeit reisen und vor ihrem Versenden beim E-Mailserver ankommen, noch ist die Verzögerung von ca. einer Stunde beim Versenden an den E-Mailserver des Empfängers und eine weitere Verzögerung von über einer Stunde bis zur Zustellung der E-Mail zu erklären. Im Bereich der Zeitstempel sind also drei verschiedene Manipulationen sichtbar.

→ **Alleine aus technischen Gesichtspunkten ist es aufgrund der Zeitstempel unmöglich, dass diese E-Mails so verschickt wurden.**

A5: Gefälschte Zeiten

Date: 10.12.21, 16:44 1
An: [redacted]
X-Mozilla-Status: 0001
X-Mozilla-Status2: 000000
X-Mozilla-Keys: Return-Path: <jennifer.hills@skymail.de>
Delivered-To: [redacted]
Received: (qmail 27533 invoked by uid 498); 10 Dec 2021 16:30:17 -0000 4
Received: from skymail.de (skymail.de [46.4.105.4]) by faye.uberspace.de (Haraka/2.8.28) with ESMTPS id 194281A9-6D5F-461D-B399-CB0DFF7A98E0.1 envelope-from <jennifer.hills@skymail.de> tls TLS_DHE_RSA_WITH_AES_256_GCM_SHA384; Fri, 10 Dec 2021 16:27:14 +0100 3
Received: from skymail.de (localhost.localdomain [127.0.0.1]) by skymail.de with ESMTP id 03CA6BE9 for [redacted]; Fri, 10 Dec 2021 15:26:54 +0100 (CET) 2
MIME-Version: 1.0

A6: Fehler im E-Mail-Header

In der ersten E-Mail gibt es die Header-Zeile "X-Mozilla-Keys: Return-Path: <jennifer.hills@skymail.de>". Der Return-Path müsste aber eigentlich in einer eigenen Zeile stehen. Das ist ein Fehler, der nur durch nachträgliche Bearbeitung des Headers entstehen konnte.

A7: Fehlender X-UIDL Header

Bei der ersten E-Mail (Anlage 2) fehlt der X-UIDL Header der bei der zweiten E-Mail (Anlage 3) vorhanden ist. Das ist ein Fehler, der nur durch nachträgliche Bearbeitung des Headers entstehen konnte.

Anlage 2

X-Mozilla-Status2: 000000
X-Mozilla-Keys: Return-Path: <jennifer.hills@skymail.de>
Delivered-To: [redacted]
Received: (qmail 27533 invoked by uid 498); 10 Dec 2021 16:30:17 -0000
Received: from skymail.de (skymail.de [46.4.105.4]) by faye.uberspace.de (Hara
ESMTPS id 194281A9-6D5F-461D-B399-CB0DFF7A98E0.1 envelope-from
<jennifer.hills@skymail.de> tls TLS_DHE_RSA_WITH_AES_256_GCM_SHA
2021 16:27:14 +0100

Anlage 3

X-Mozilla-Status2: 00000000
X-Account-Key: account1
X-UIDL: 00000c9a5f9abe12
Return-Path: <jennifer.hills@skymail.de>
Delivered-To: [redacted]
Received: (qmail 27533 invoked by uid 498); 13 Dec 2021 05:44:34 -0000
Received: from skymail.de (skymail.de [46.4.105.4]) by faye.uberspace.de
(Haraka/2.8.28) with ESMTPS id 194281A9-6D5F-461D-B399-CB0DFF7A98E0.1

B1: Widersprüche Formatierung Anlage 7 (E-Mail vom 14.01., 11.52 Uhr)

Die E-Mail beeinhaltet im Header und Content-bereich zwei unterschiedliche Schriftgrößen und Schriftarten. Lässt man sich eine E-Mail im Original anzeigen, dann werden E-Mail-Header und E-Mail-Text mit der gleichen Schriftgröße und Schriftart dargestellt. Neben der geänderten Schriftgröße und -art ist auch die fehlende Signatur am Ende der E-Mail, die in allen anderen von dieser Adresse verschicken E-Mails enthalten ist, ein Hinweis auf eine mögliche Manipulation des Body.

Nachricht-ID: <d2ef6fcd625e6a547afbcad930b8f1a4@sky
X-Mailer: b1gMail/7.4.0
X-Sender-IP: 194.32.107.161
Antwort an: "Jennifer Hills" <jennifer.hills@skymail.de>
In-Reply-To: <5a9a891f-6d9e-6008-8e55-932091222bf0@
Referenzen: <6d61a2dd5226ba1f26aaee0a200a6656@sk
b198-75149e7a1521@gmail.com> <5a9a891f-6d9e-600
Content-Type: text/plain; charset="UTF-8"
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline
X-Abuse-Report: absuse@emailn.de

hallo [redacted]

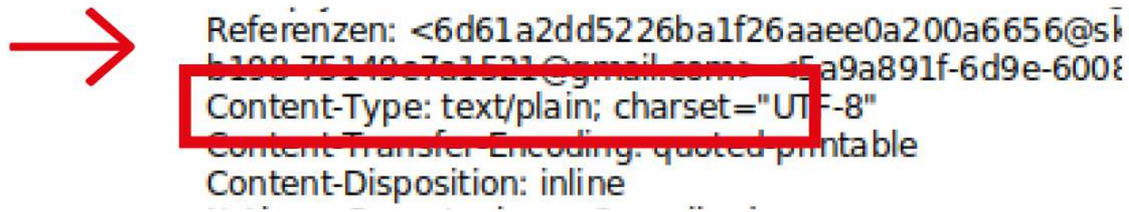
mir w[redacted]als zuverlässig beschrieben. es tut mir leid für d:
überbracht hat.

→ **Dies ist ein starker Hinweis, dass E-Mail-Header und E-Mail-Text nachträglich in einem Texteditor/Textverarbeitungs-programm zusammengefügt wurden.**

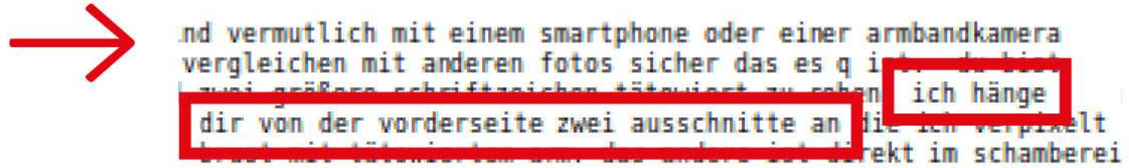
B2: Widersprüche Anhänge Anlage 7

(E-Mail vom 14.01., 11.52 Uhr)

Sowohl in der E-Mail als auch in der Parteivernehmung der Beklagten wird beschrieben, dass mit der E-Mail zwei Fotos verschickt wurden. Diese Anhänge fehlen jedoch. Auch wird die E-Mail als Content-Type: text/plain deklariert.



→ **Wären hier Anhänge/Fotos mitverschickt worden, hätte der Content-Type z.B. multipart/mixed lauten müssen.**



B3: Widersprüche Anlage 9

(E-Mail vom 14.01., 08.48 Uhr)

Formal: Die zwei Bilder wurden in einer ansonsten leeren E-Mail ebenfalls am 14.01. verschickt. Die Versende-Uhrzeit dieser E-Mail (08.48 Uhr) liegt mehr als drei Stunden vor der Versende-Uhrzeit (11.52 Uhr) der E-Mail in der die Versendung der Bilder überhaupt erste angekündigt wird. Das macht keinen Sinn.

Betreff: Re: ...
Von: "Jennifer Hills" <jennifer.hills@skymail.de>
Datum: 14.01.22, 11:52
An: [redacted]

Außerdem fehlt der Header, der in allen anderen E-Mails enthalten ist. Warum?

Inhaltlich: Die Fotos, auf denen sich die Beschuldigende erkannt haben will, entsprechen nicht den dazu verfassten Beschreibungen (eines der Bilder zeigt nicht wie beschrieben den Schambereich, sondern die verpixelte Nahaufnahme einer Tätowierung).

Betreff: nur fotos
Von: "Jennifer Hills" <jennifer.hills@skymail.de>
Datum: 14.01.22, 08:48
An: <[redacted]>

→ **Neben den inhaltlichen Widersprüchen sind aus IT-forensischer Sicht die formalen Fakten entscheidende Hinweise auf Manipulationen.**

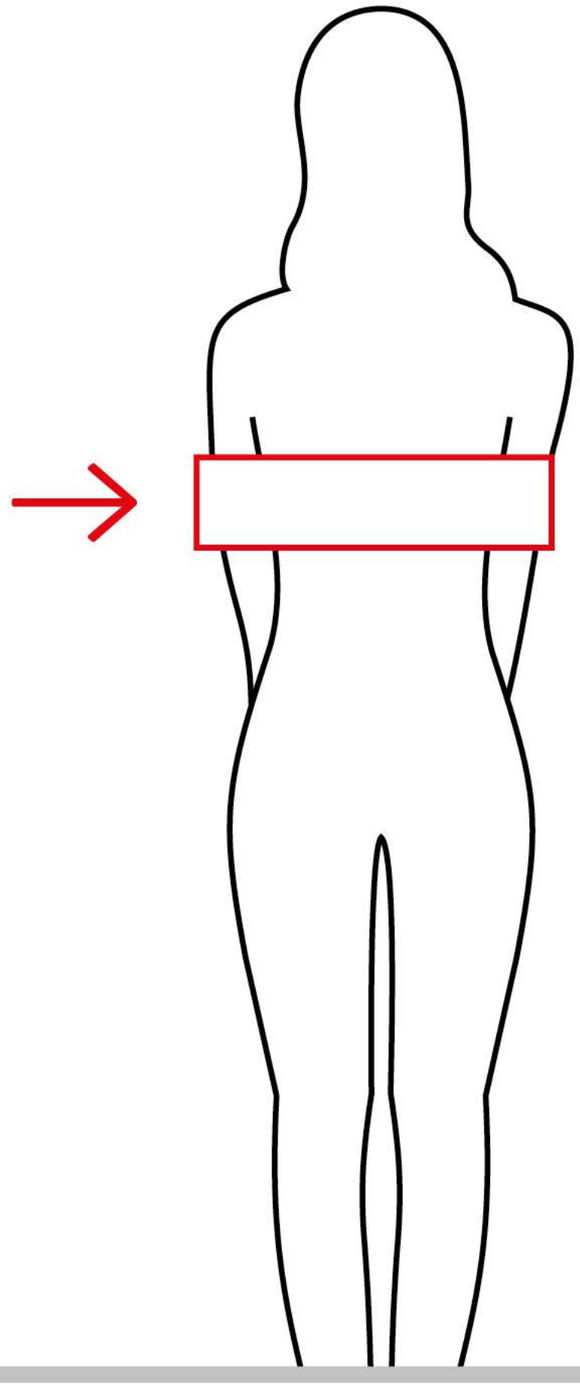
C1: Aussagekraft Foto 1

Statement IL im Juli 2022: "Es liegen u.a. Fotos vor, die vertrauenswürdige Personen gesehen haben und die eindeutig einem Treffen mit dem Täter zugerechnet werden."

Aussage der Beschuldigenden: Sie hat nur diese zwei Fotos von der anonymen Zeugin erhalten.

Das Foto 1 zeigt den Bildausschnitt einer Person die gerade und exakt mittig zur Kamera ausgerichtet mit anliegenden Armen steht. Das Fotos wurde zusätzlich verpixelt.

→ **Das Foto lässt sich keinem Ort oder Enstehungszeitpunkt zurechnen.**



Vollständiger Bildausschnitt, inklusive dem, was vom Hintergrund sichtbar ist.

C2: Aussagekraft Foto 2

Statement IL im Juli 2022: "Es liegen u.a. Fotos vor, die vertrauenswürdige Personen gesehen haben und die eindeutig einem Treffen mit dem Täter zugerechnet werden."

Aussage der Beschuldigenden: Sie hat nur diese zwei Fotos von der anonymen Zeugin erhalten.

Das Foto 2 zeigt die Nahaufnahme eines Tatoos (Asiatisches Schriftzeichen). Das Foto wurde stark verpixelt.

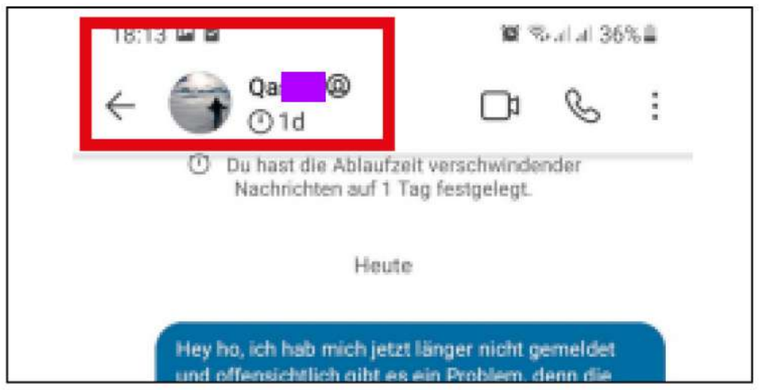
→ **Das Foto lässt sich keinem Ort oder Enstehungszeitpunkt zurechnen.**

Beispielbild. Entspricht dem Ausschnitt und Grad der Verpixelung des angeblich übersandten Fotos

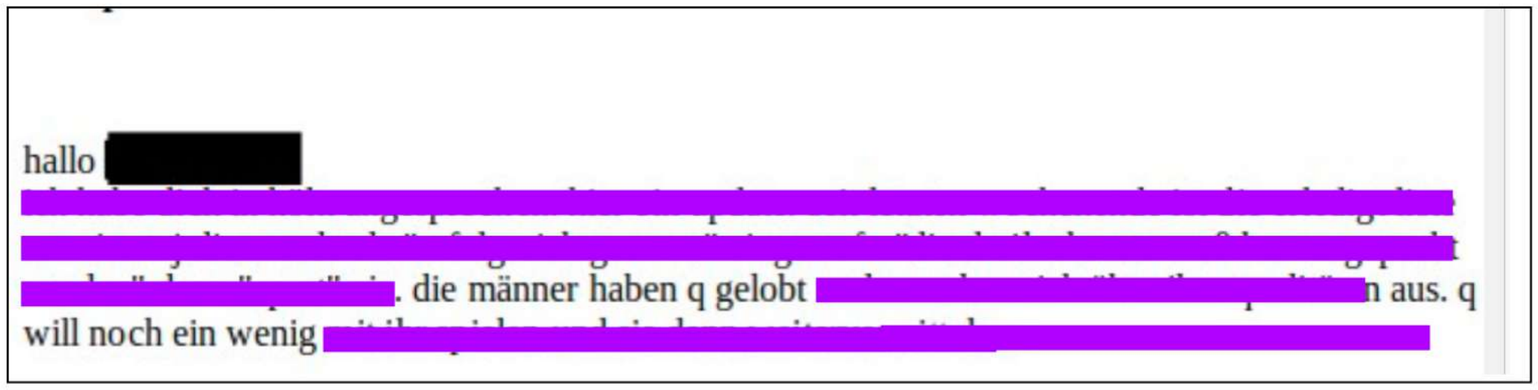
D: Falsche Schreibweise des Namens

Die Beschuldigende hat den als "Täter" Beschuldigten als „Qaxxx“ eingespeichert. Auch in den E-Mails von „Jennifer Hills“ wird der von ihr Beschuldigte stets als „Q“ bezeichnet. Da sich keinerlei weitere Ausführungen zu der Verwendung dieser Abkürzung in den E-Mails finden, muss davon ausgegangen werden, dass auch sie der Auffassung ist, der Name werde tatsächlich so geschrieben. Diese Schreibweise ist falsch.

→ **Sowohl die angebliche Zeugin als auch die Beschuldigende schreiben den Namen des von Ihnen Beschuldigten auf die gleiche weise falsch.**



Screenshot Chat Beschuldigende



Screenshot Mail von "Jennifer Hills"