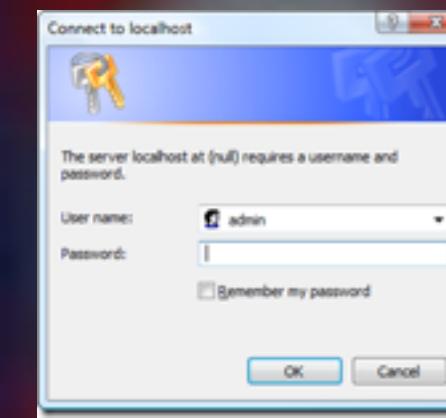
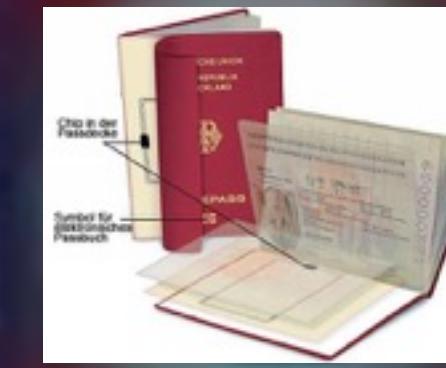


Zur Unsicherheit moderner Authentifizierungsverfahren



Passwort

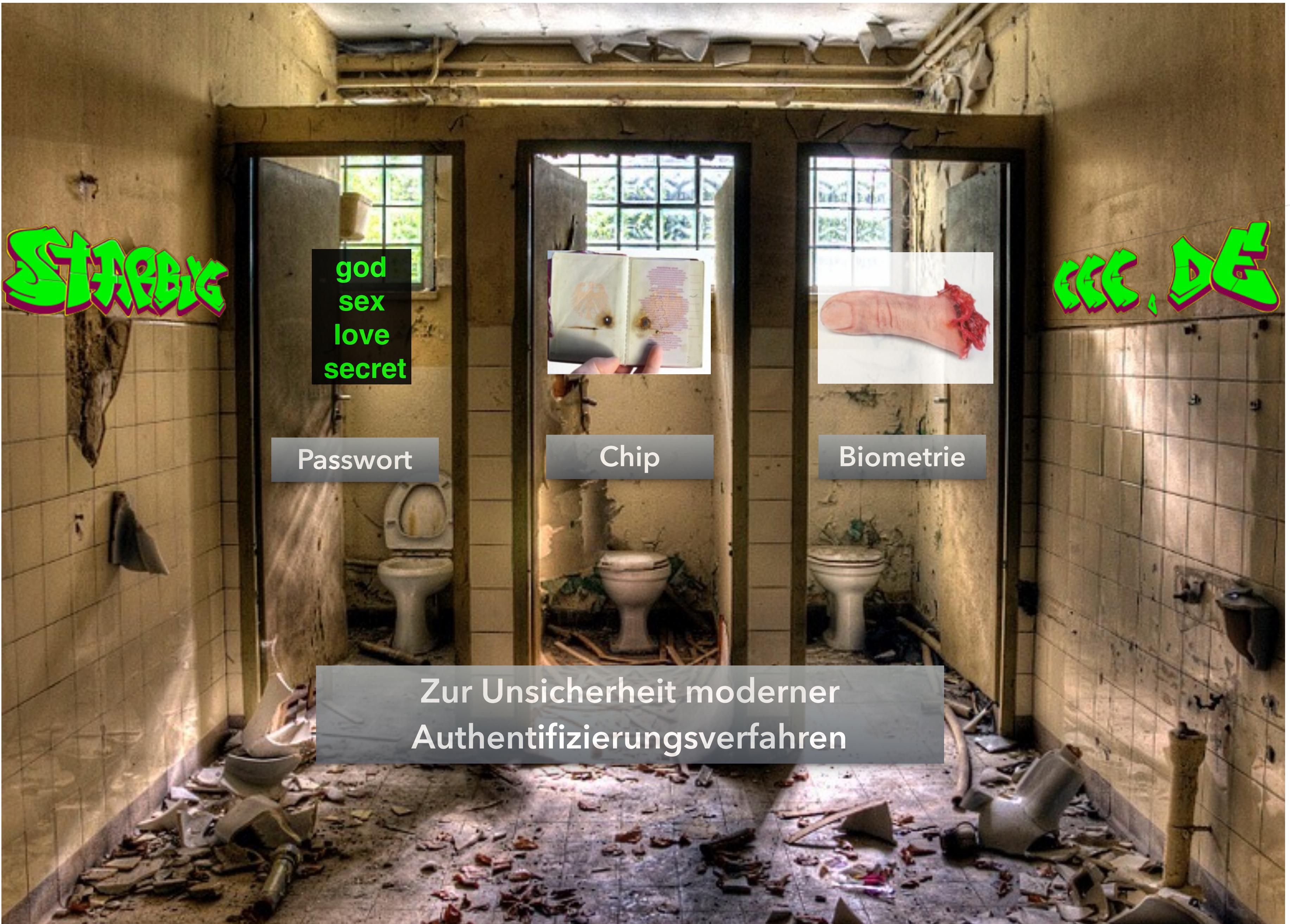


Chip



Biometrie





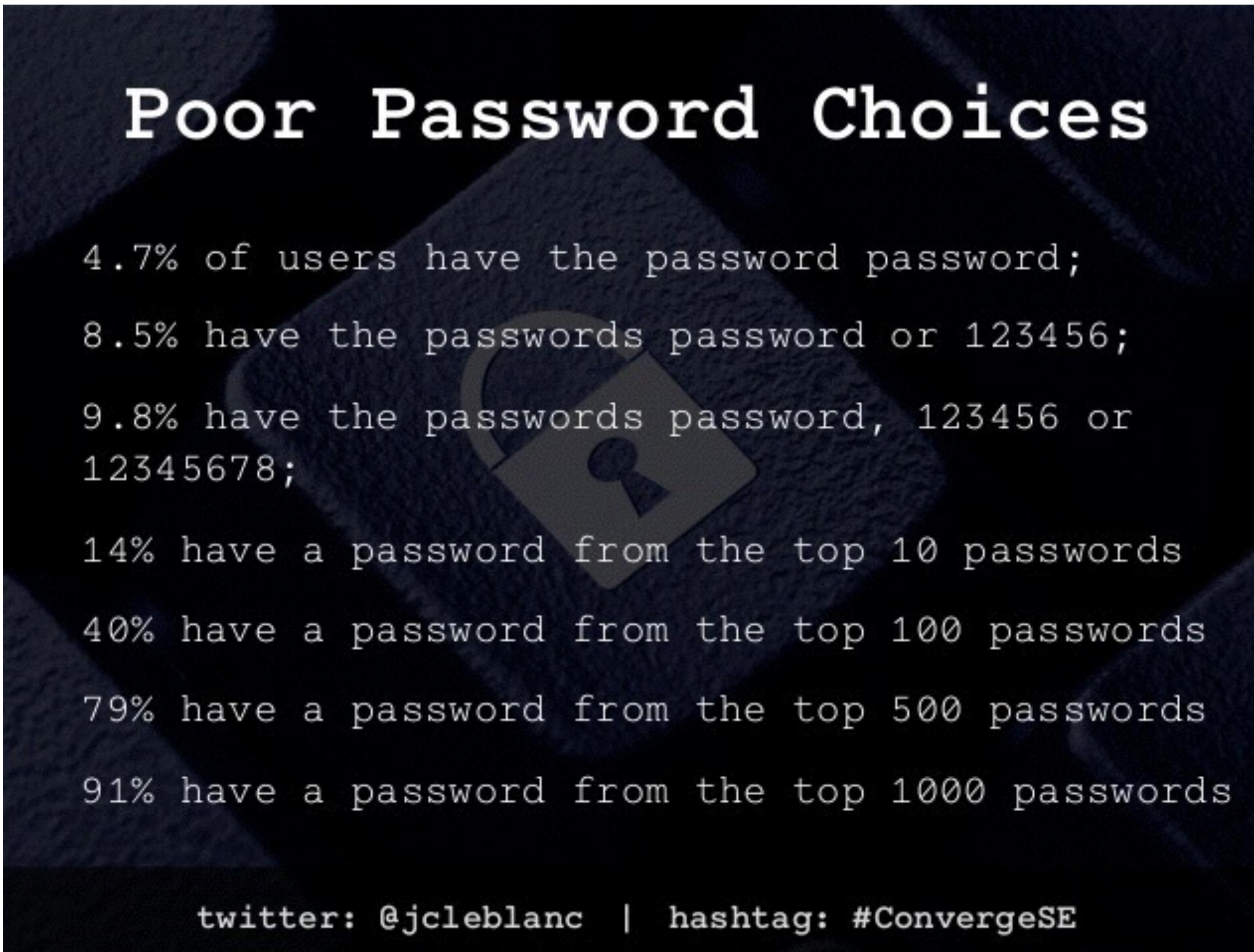
Post-it am Monitor



<http://microsoftmercenary.com/wp/wp-content/uploads/2015/02/image9.png>
<http://cdn1.spiegel.de/images/image-834158-galleryV9-gbup-834158.jpg>

schlechte Passworte

Poor Password Choices



4.7% of users have the password password;

8.5% have the passwords password or 123456;

9.8% have the passwords password, 123456 or 12345678;

14% have a password from the top 10 passwords

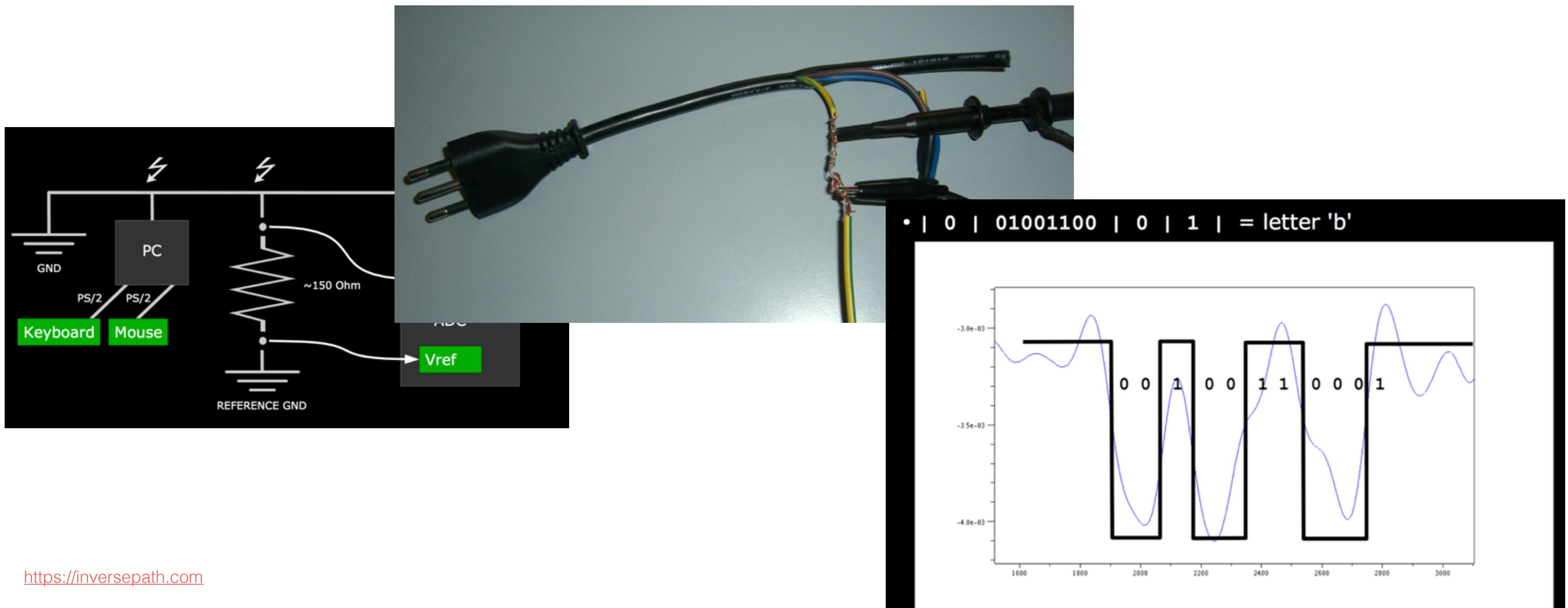
40% have a password from the top 100 passwords

79% have a password from the top 500 passwords

91% have a password from the top 1000 passwords

twitter: @jcleblanc | hashtag: #ConvergeSE

Seitenkanäle



Keylogger



<https://www.keelog.com/>

Funkttastaturen

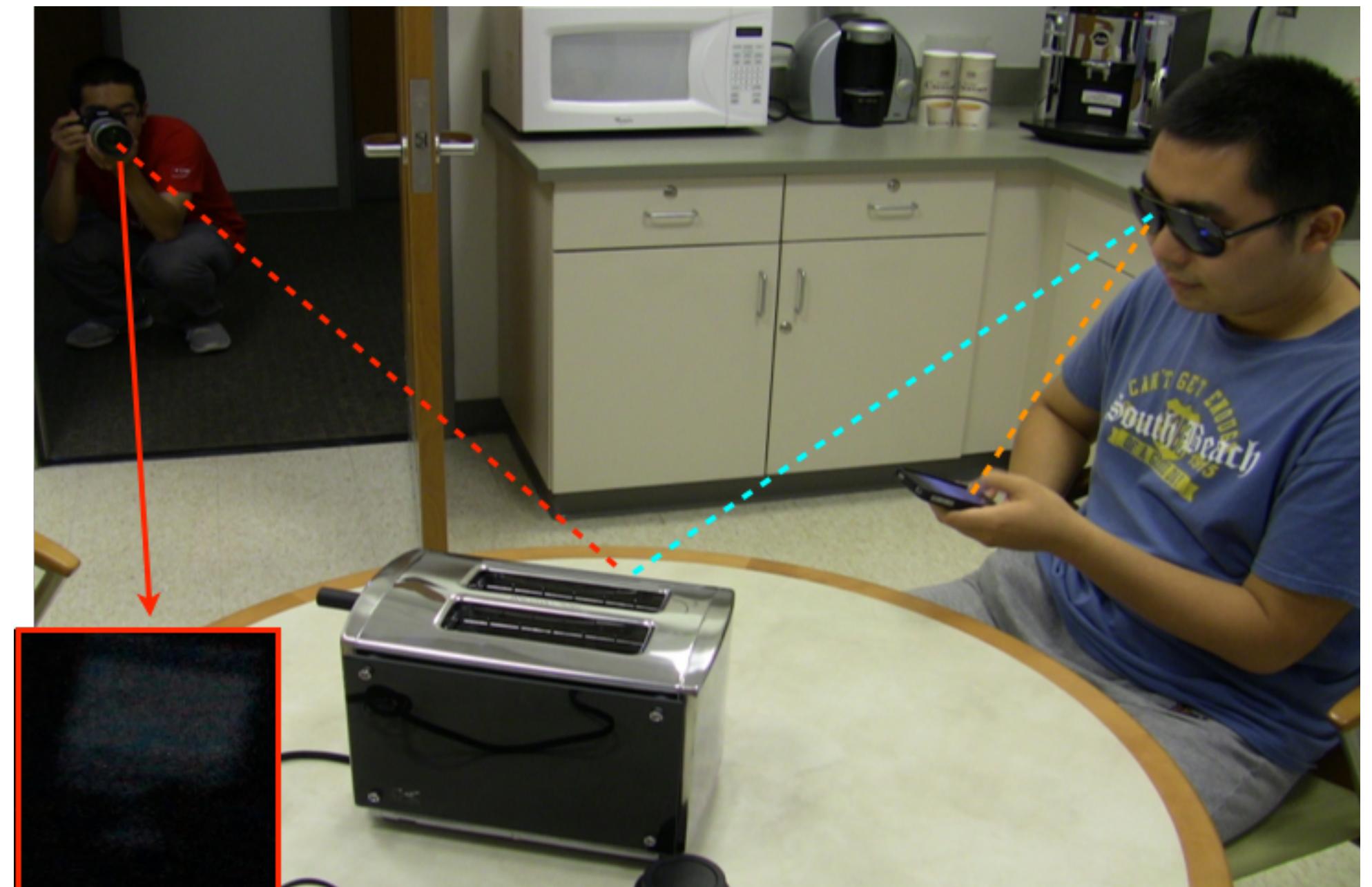


- KeyKeriki v1.0 – 27MHz
- KeyKeriki v2.0 – 2,4GHz
- KeySweeper

aus der Ferne



direkt oder ueber Eck

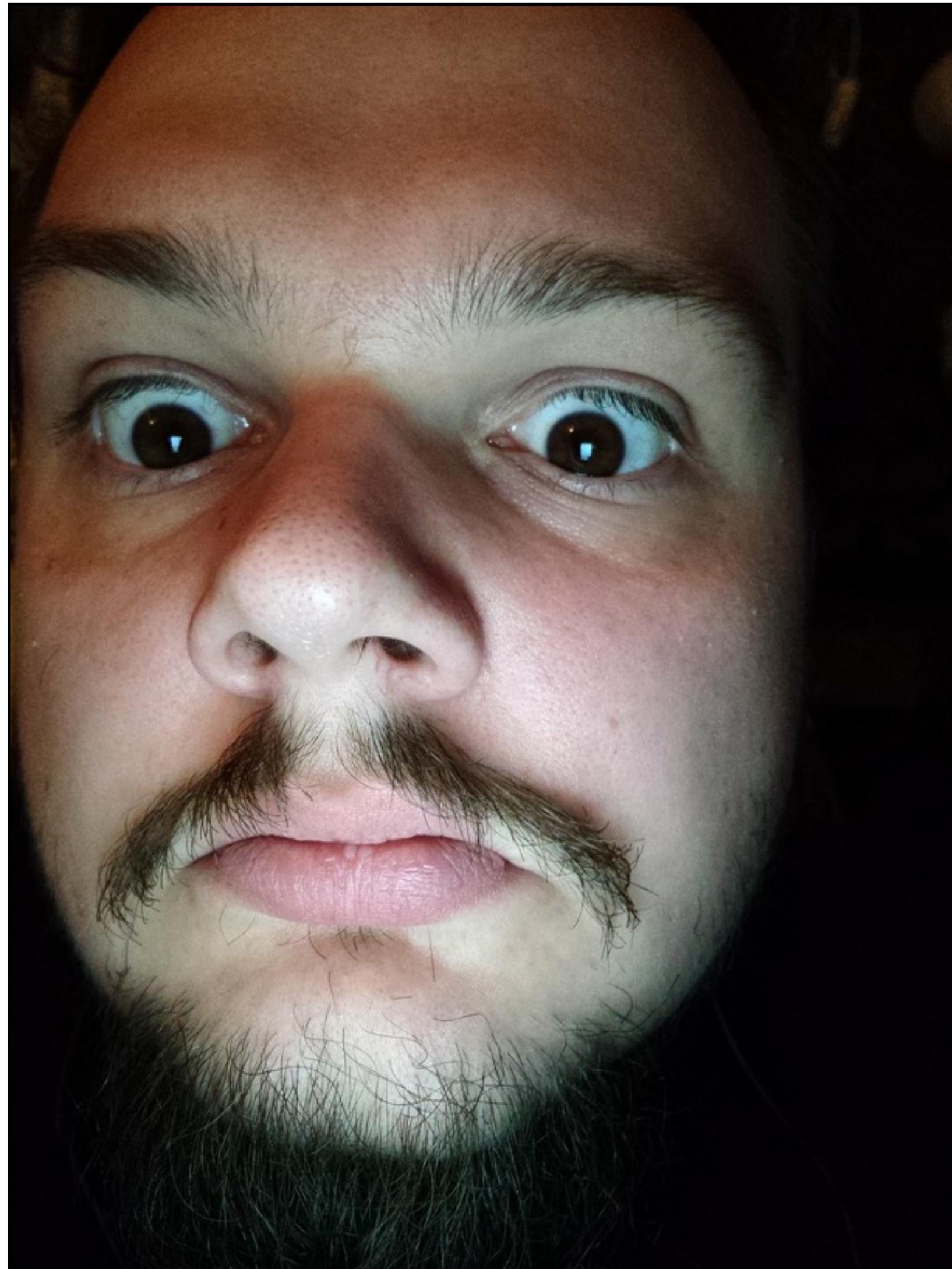


http://jacobsschool.ucsd.edu/news/news_releases/release.sfe?id=791

<http://cs.unc.edu/~yix/SeeingDouble/images/2.png>

Generation Selfie





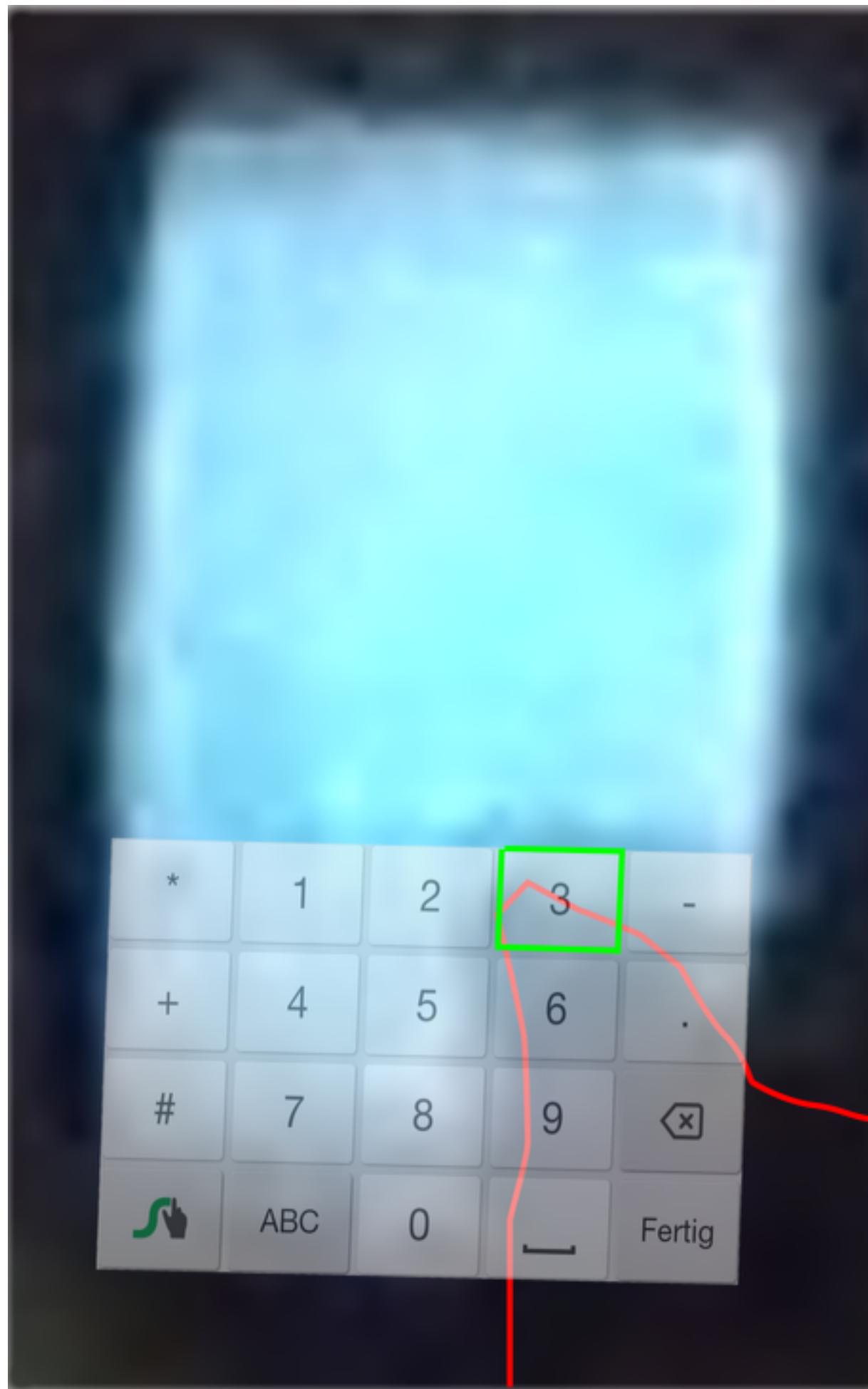




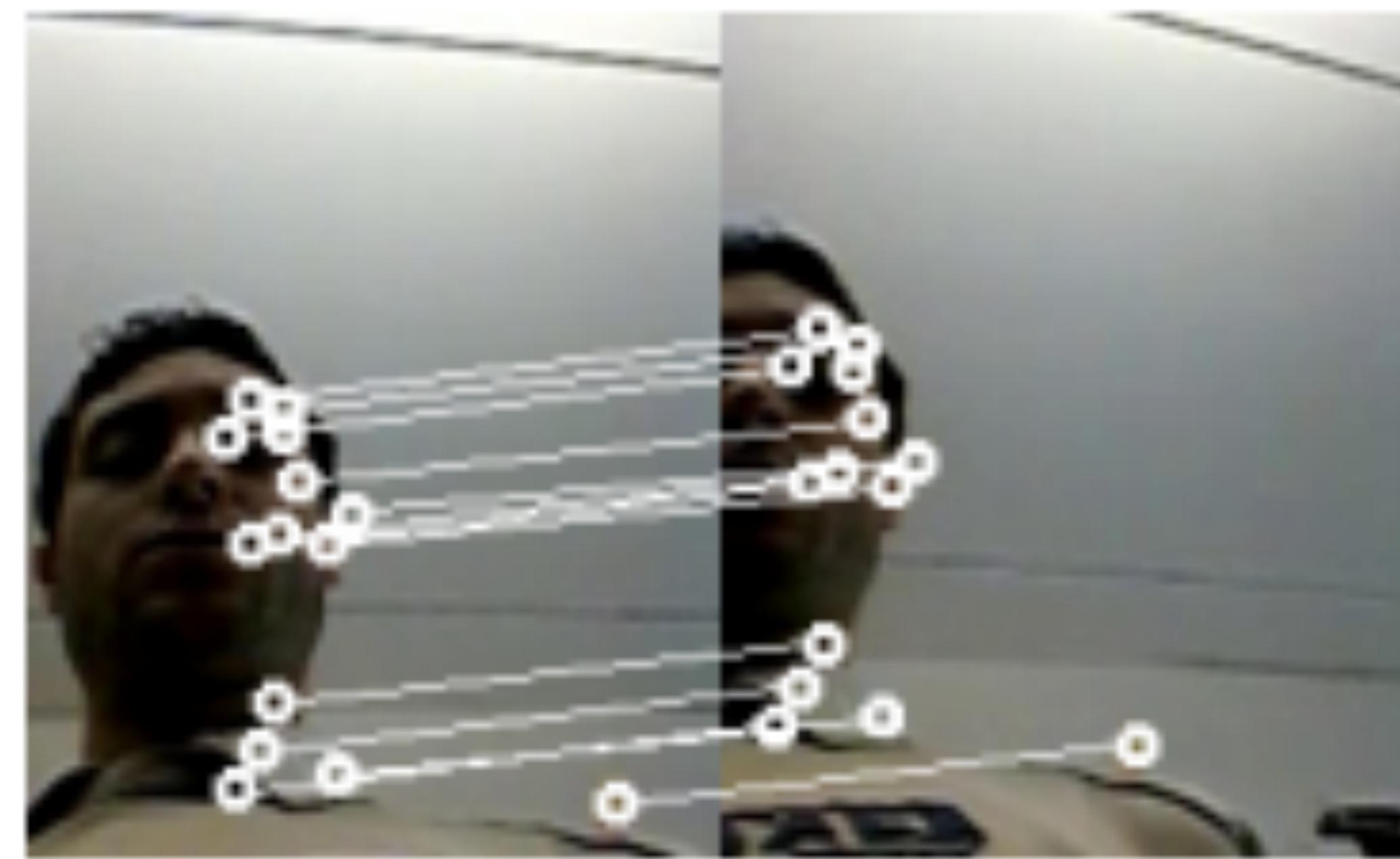




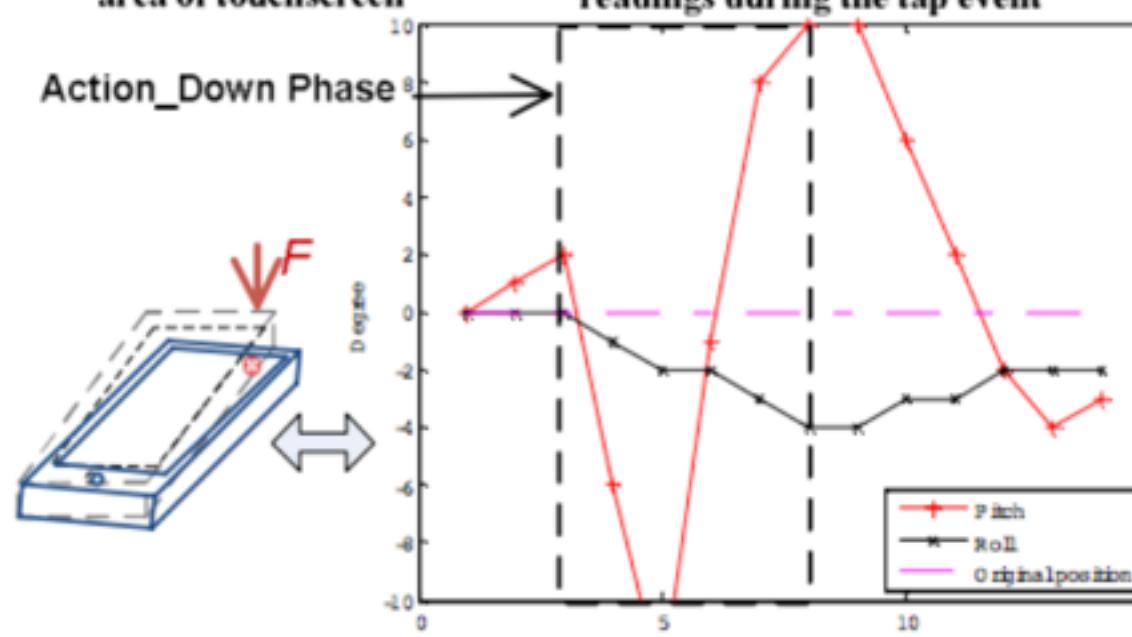
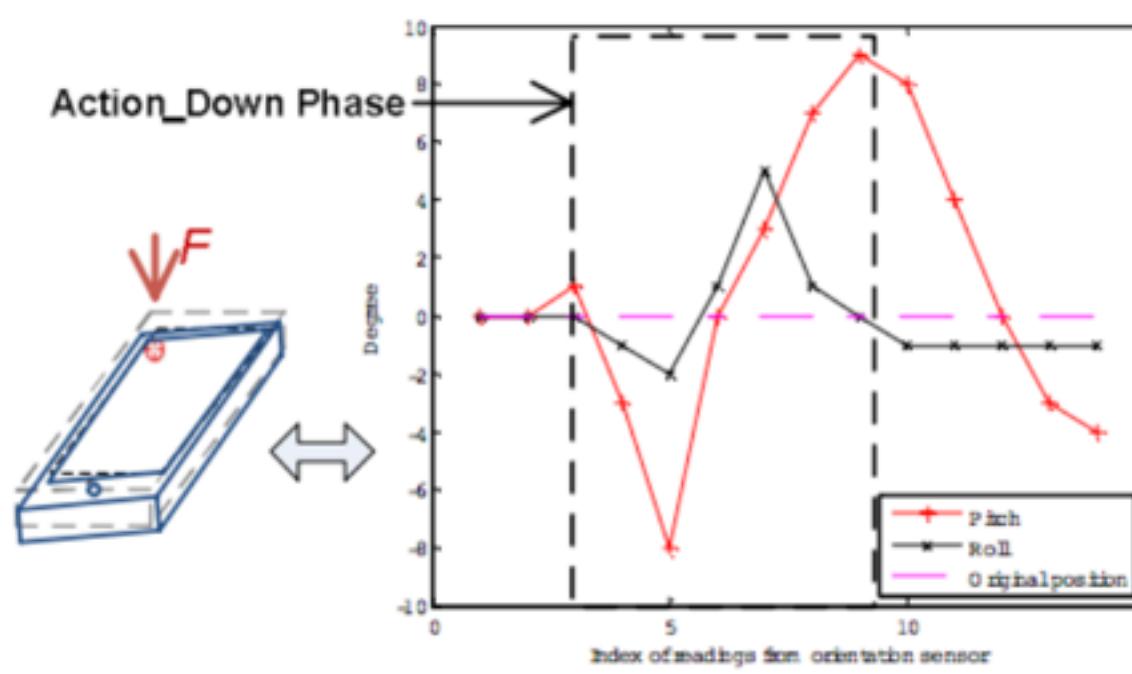
corneal key logger



motion detection



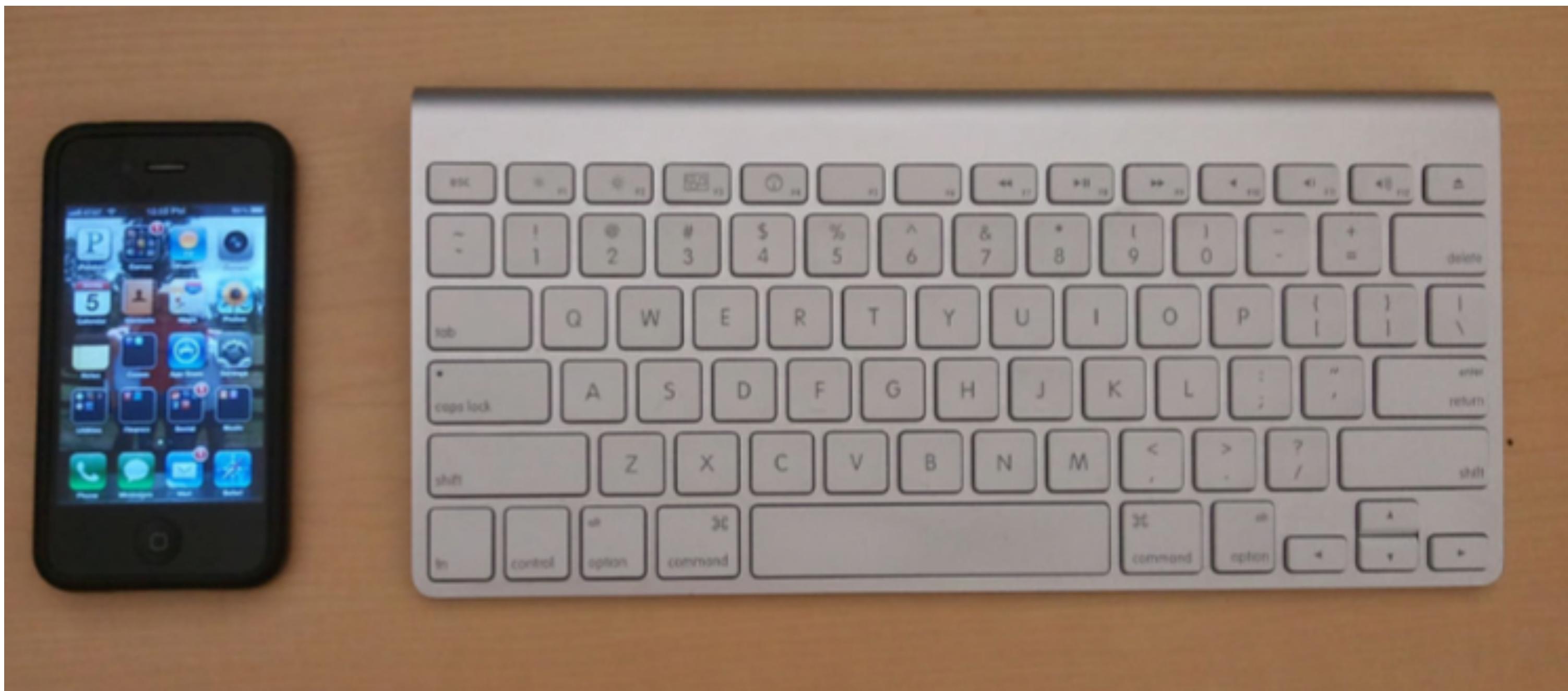
motion detection 2



Distribution of inferred labels after entering the passwords “5 7 6 0” for 32 rounds

Input#1: button 5	Input#2: button 7	Screen Lock Layout
Top-1 Inf.: 0 4 3 Top-2 Inf.: 0 7 3 Top-3 Inf.: Button {5} Button {5 or 9} Button {5 or 9 or 8}	1 0 0 9 0 0 13 0 1 7 1 0	1 2 3 4 5 6 7 8 9 OK 0 Del
Input#3: button 6	Input#4: button 0	
Top-1 Inf.: 0 0 1 Top-2 Inf.: 0 0 14 Top-3 Inf.: Button {6} Button {6 or Del} Button {6 or Del or 9}	0 0 0 0 0 2 0 2 5 0 10 13	Coverage: 75% Coverage: 100% Coverage: 100%

motion detection 3



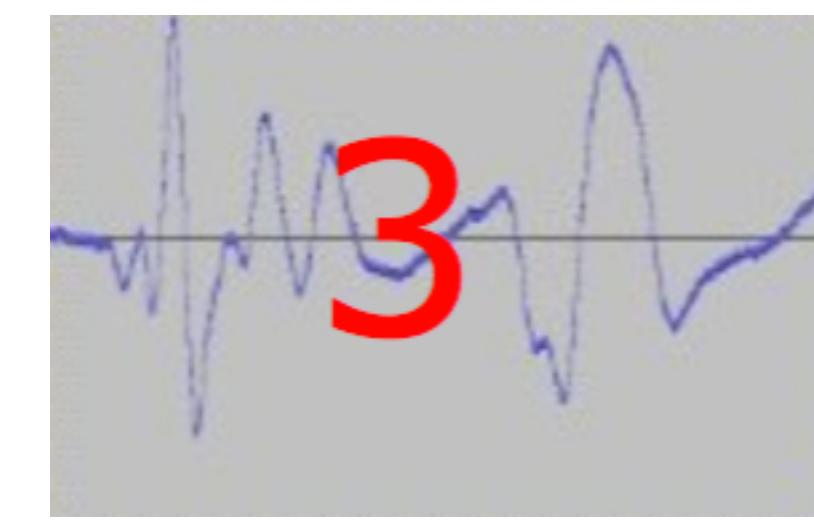
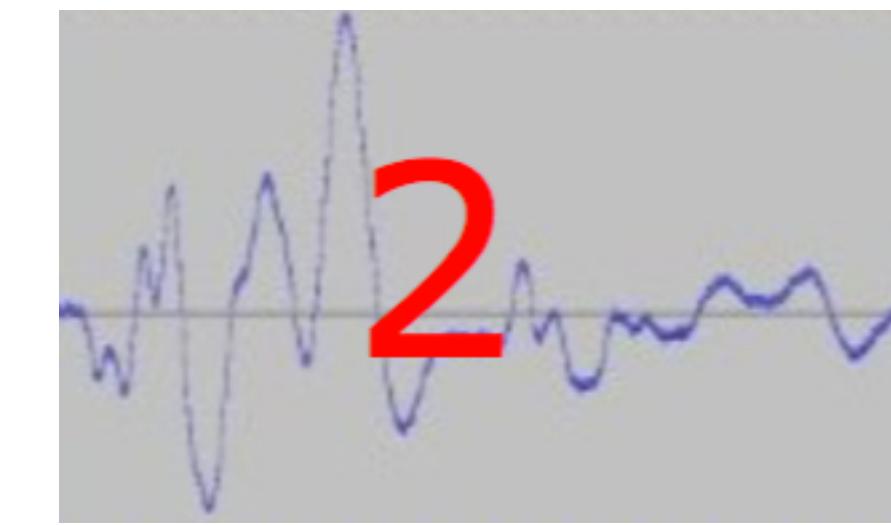
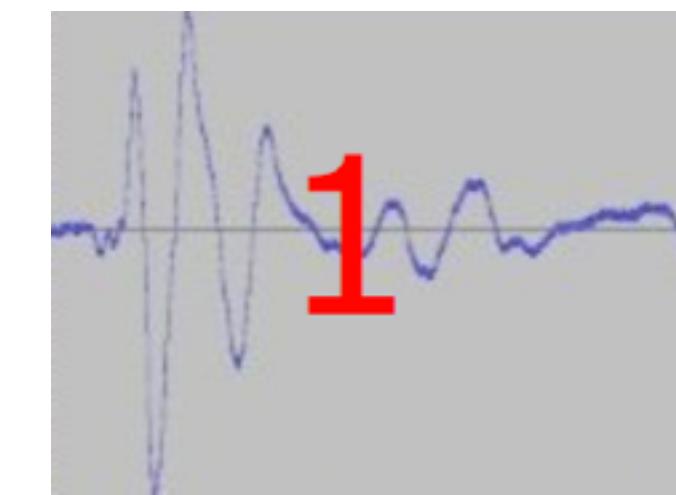
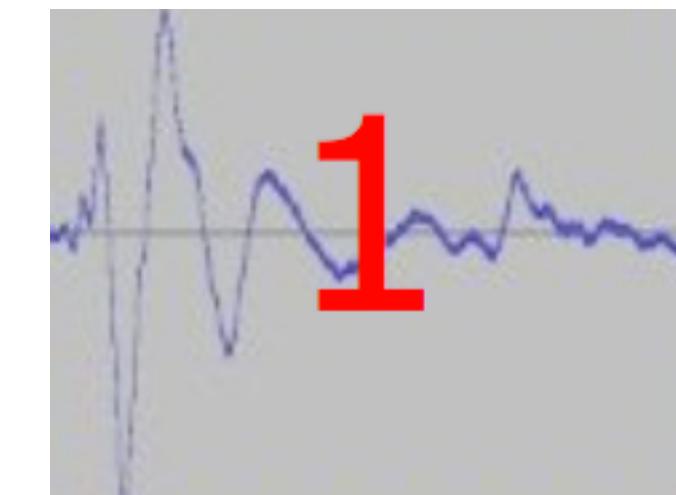
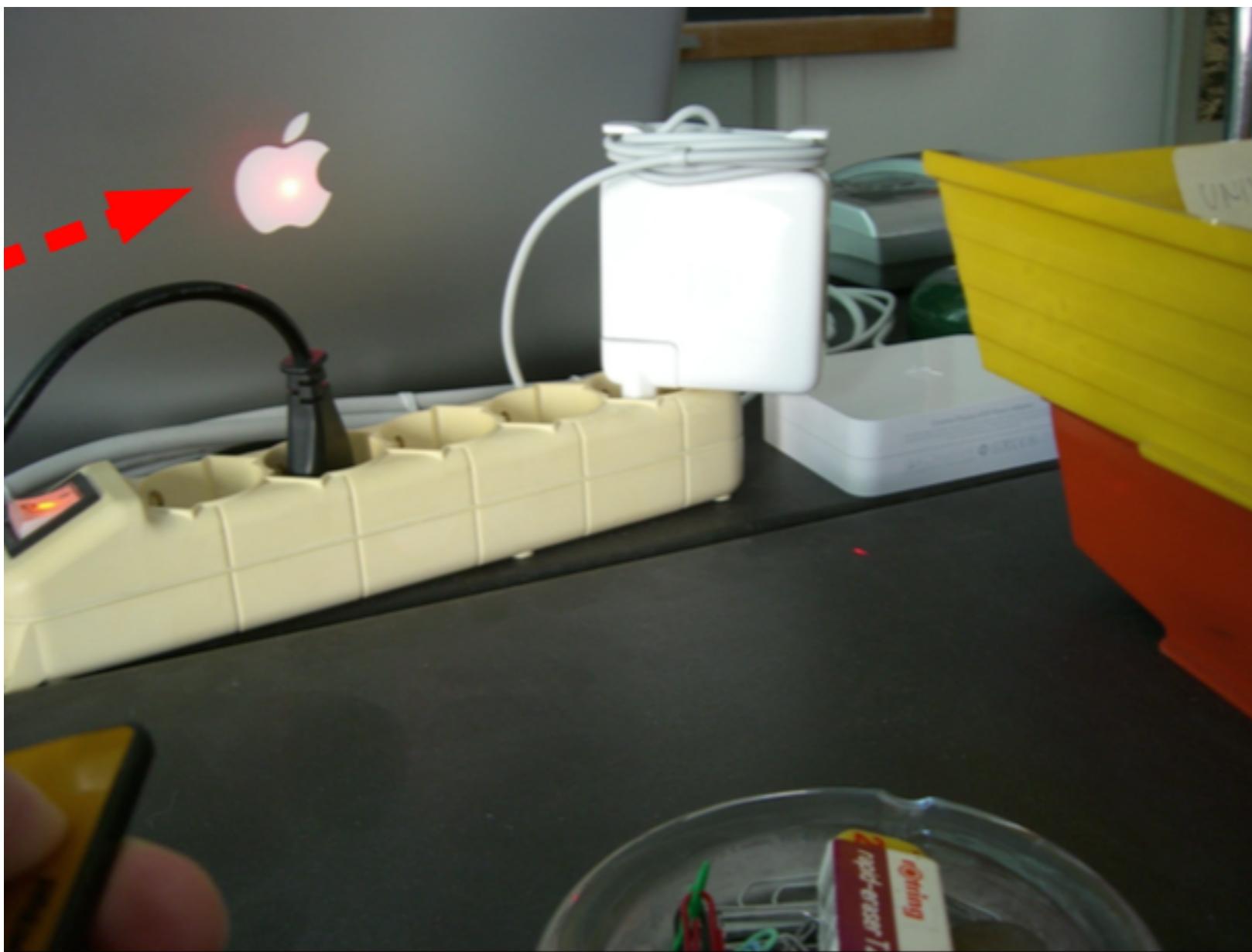
(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers

CCS2011

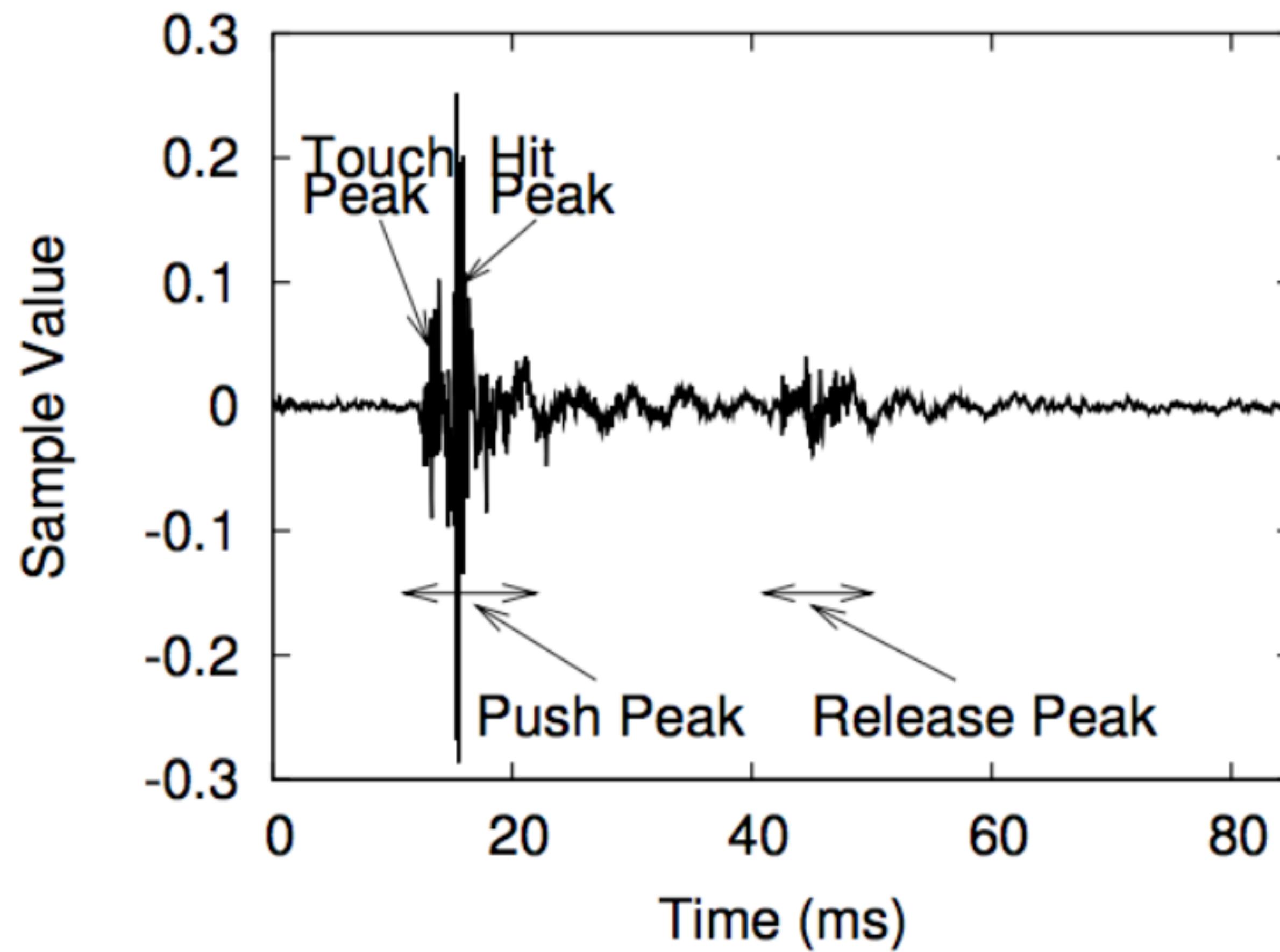
Smartwatch und Fitbit



motion detection 5



Tastaturgeräusche



visual microphone



High speed video
(actual video playing here)

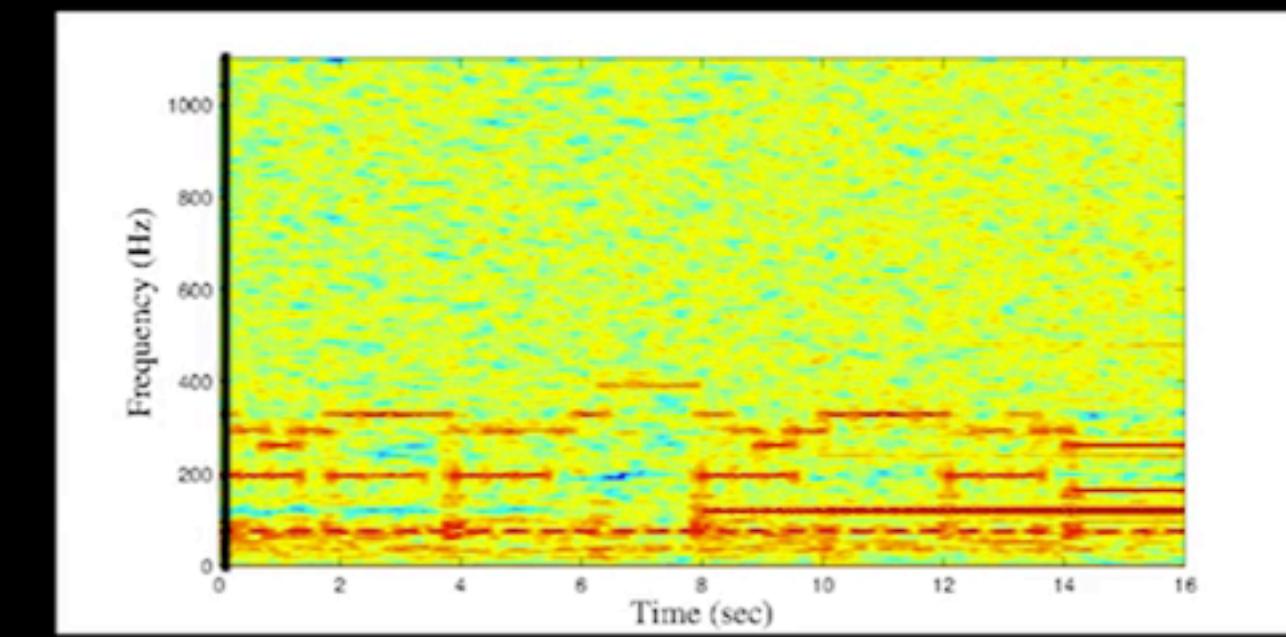


Object

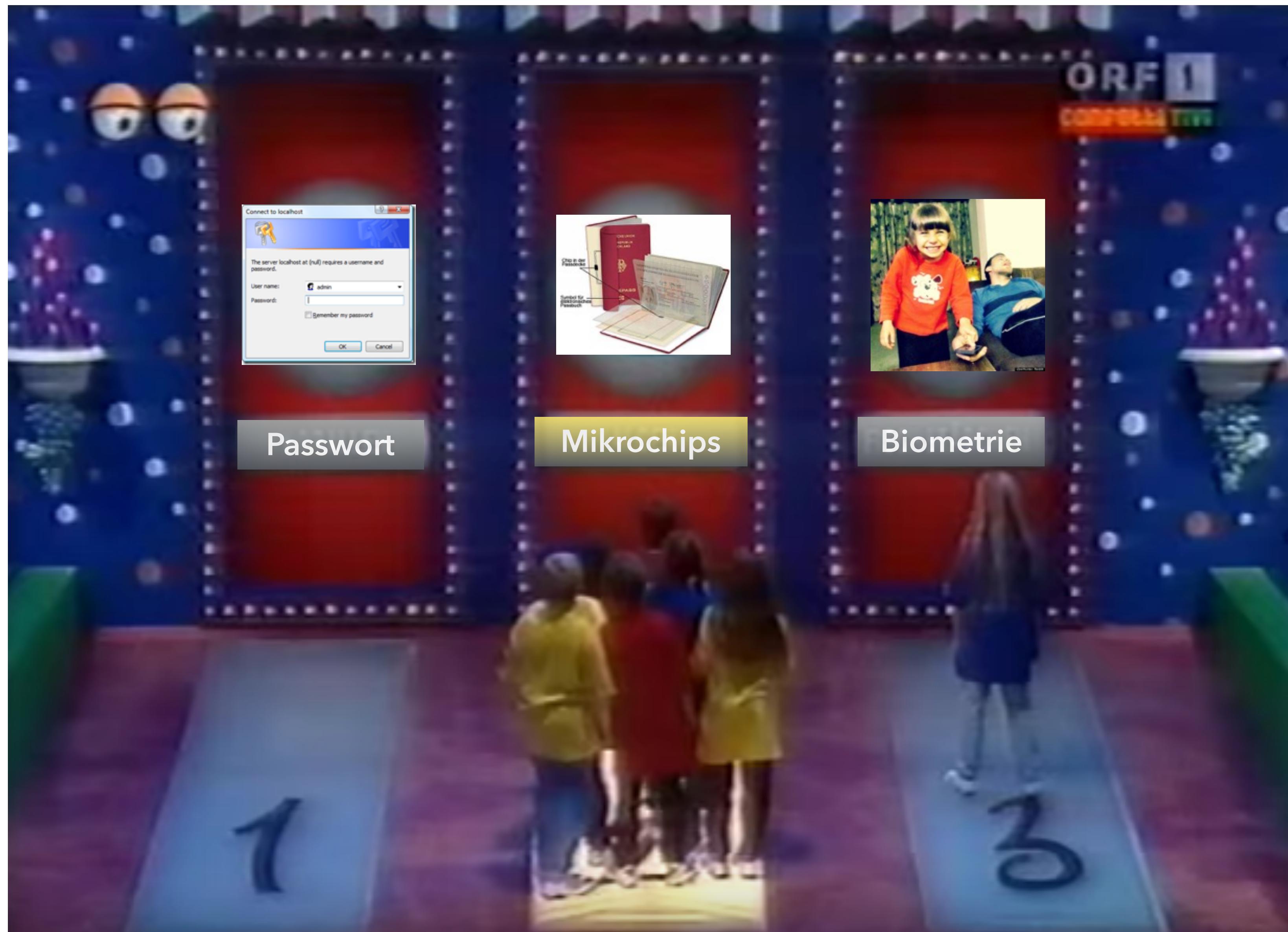
visual microphone



High speed video
(actual video playing here)



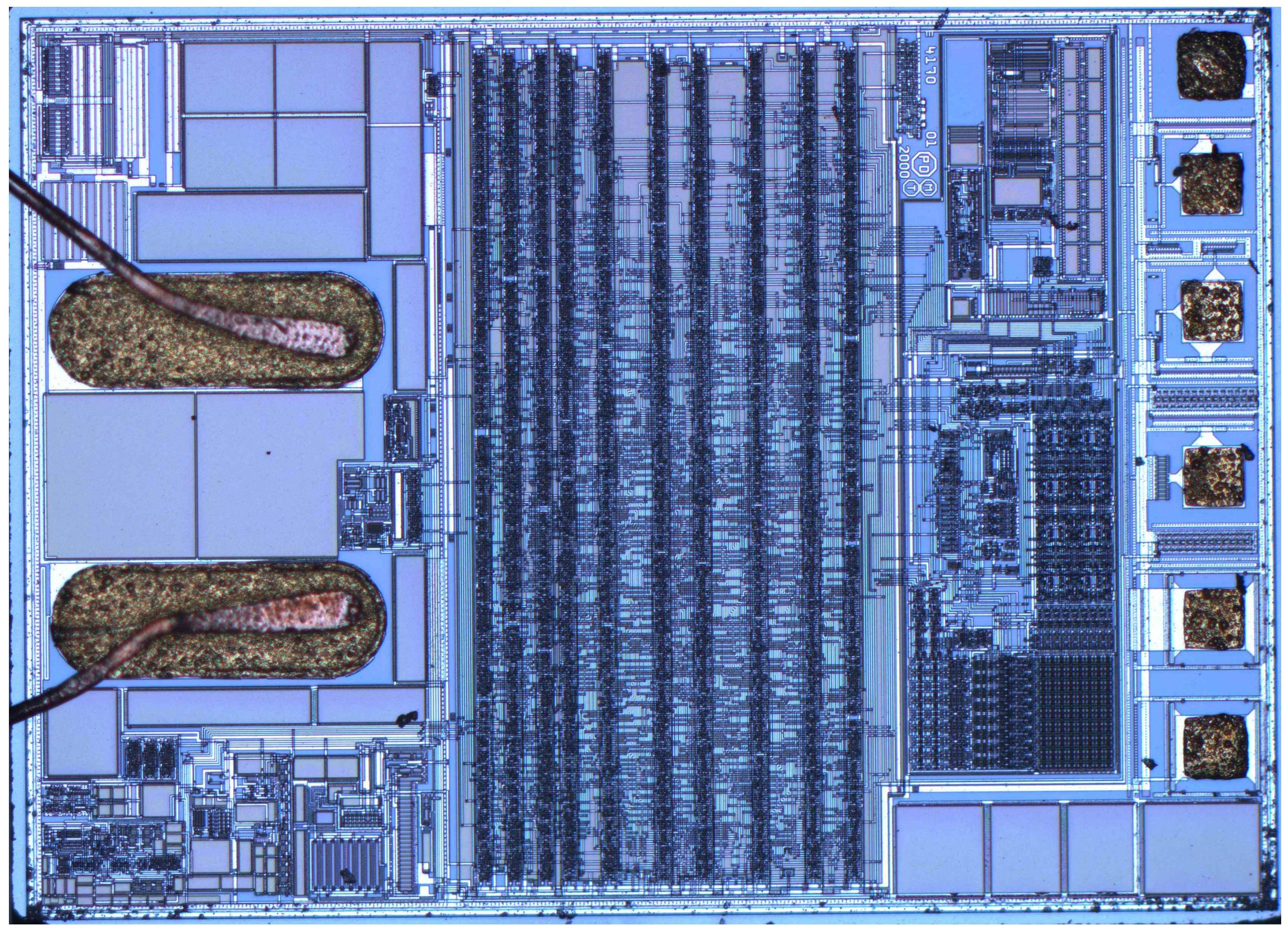
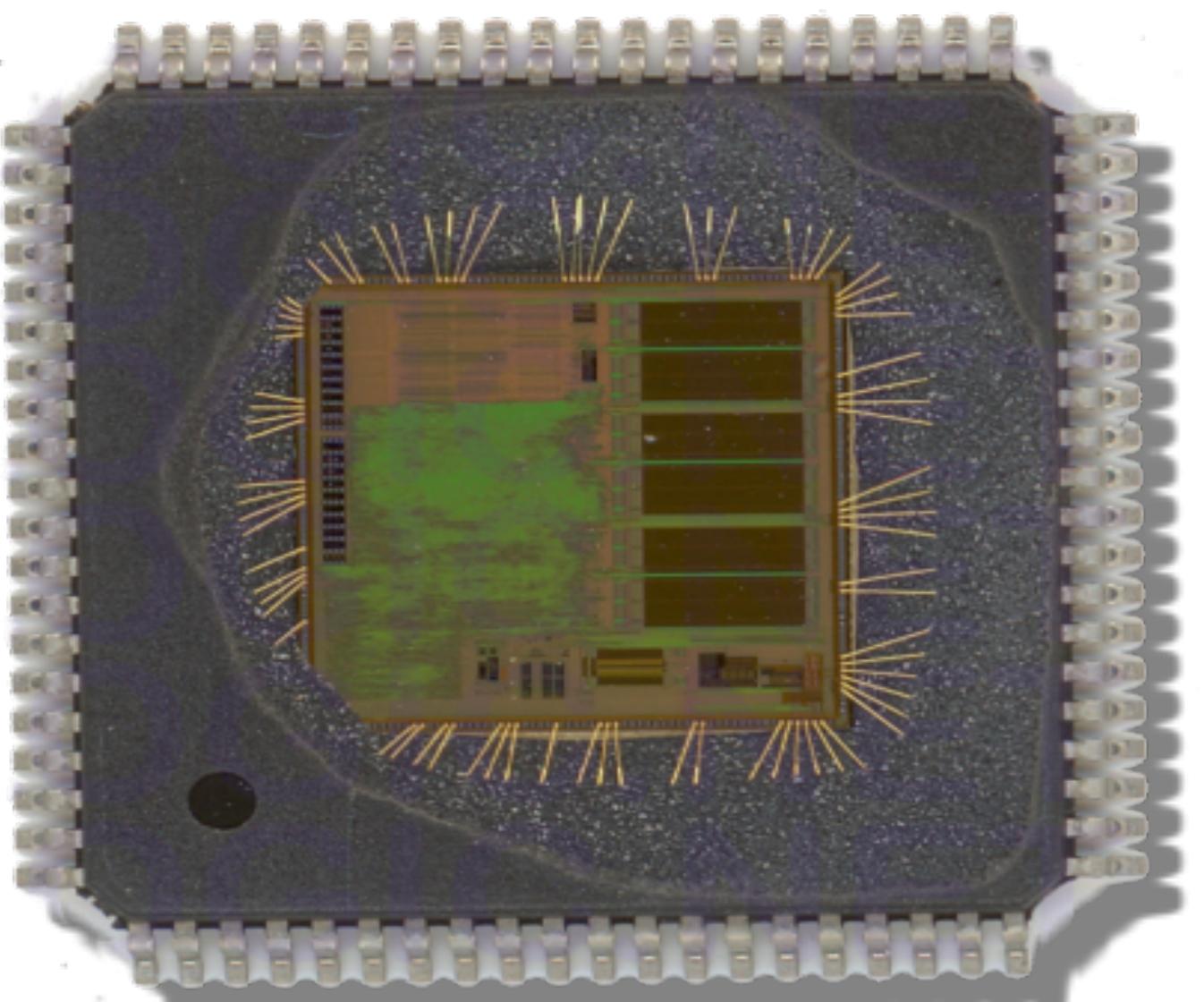
Sound Recovered
From Video



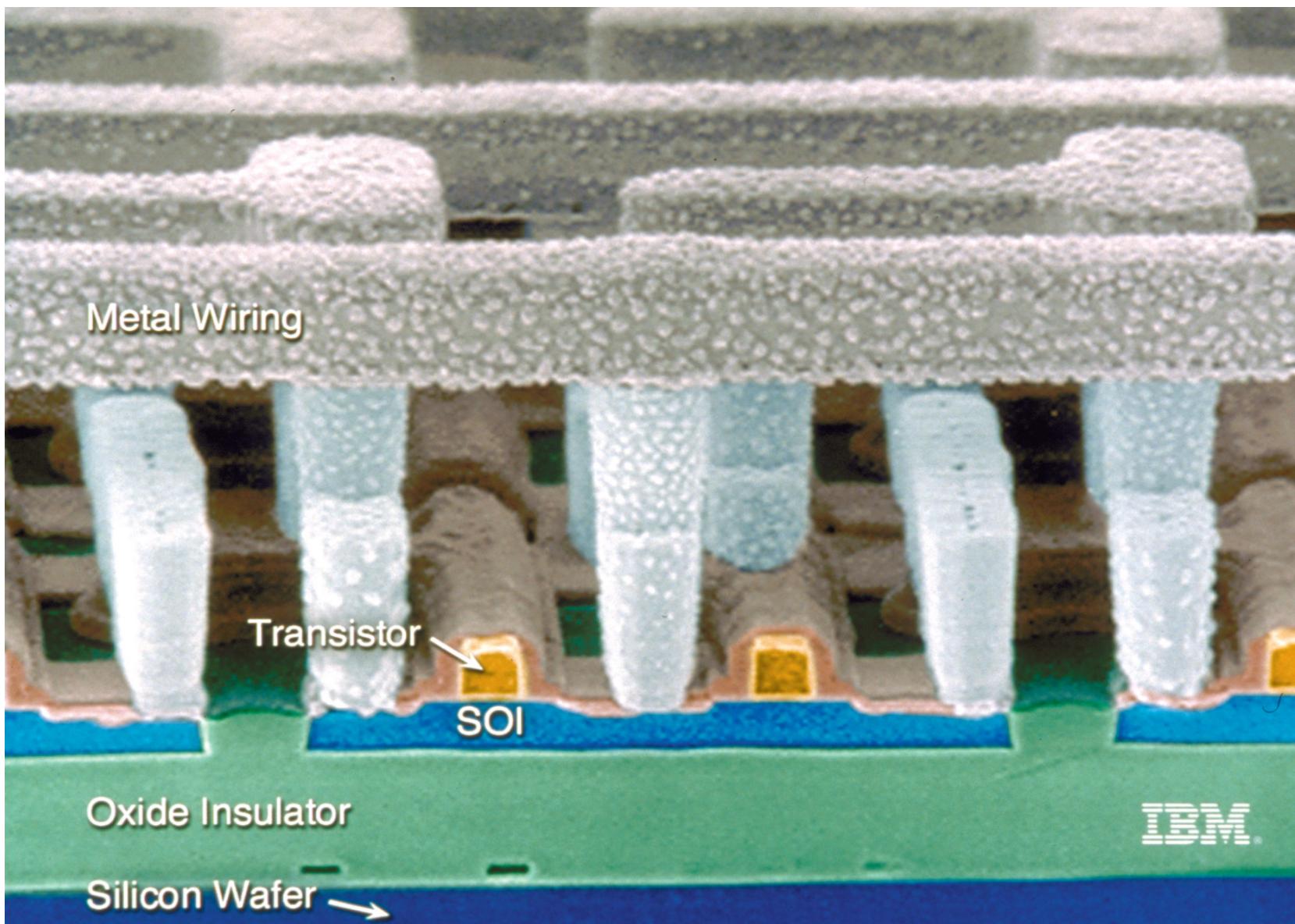
Chip extrahieren



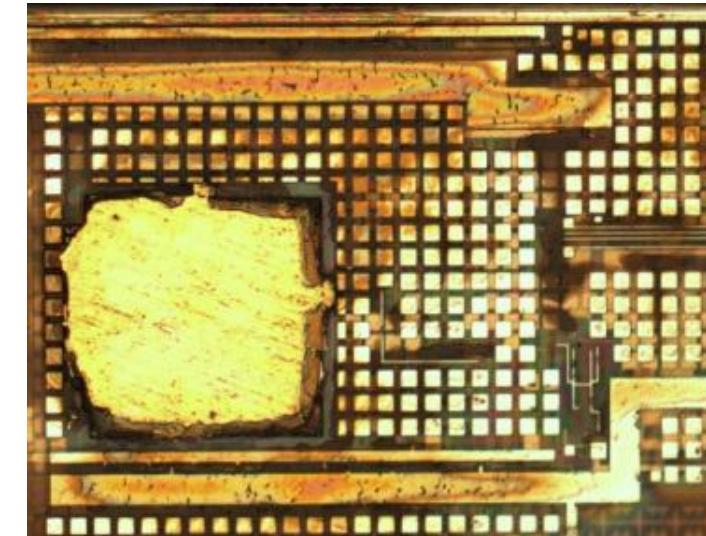
chip extrahieren



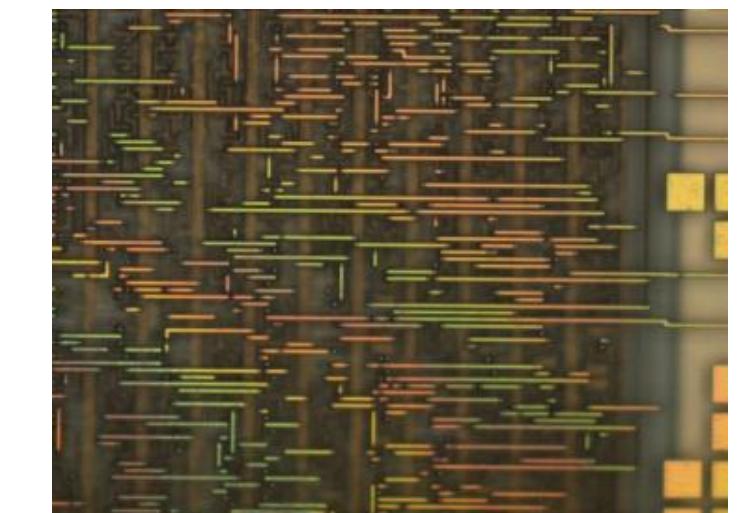
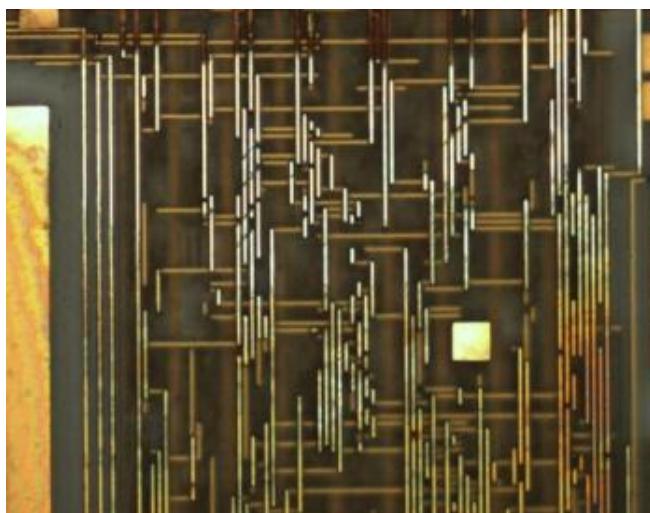
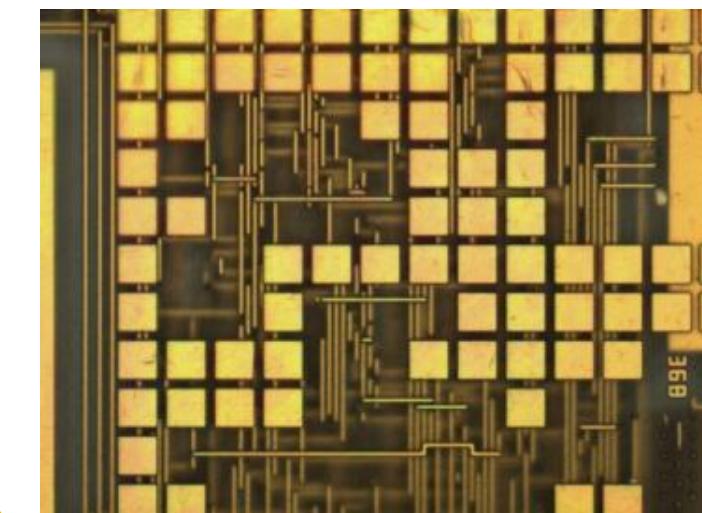
Aufbau eines Chips



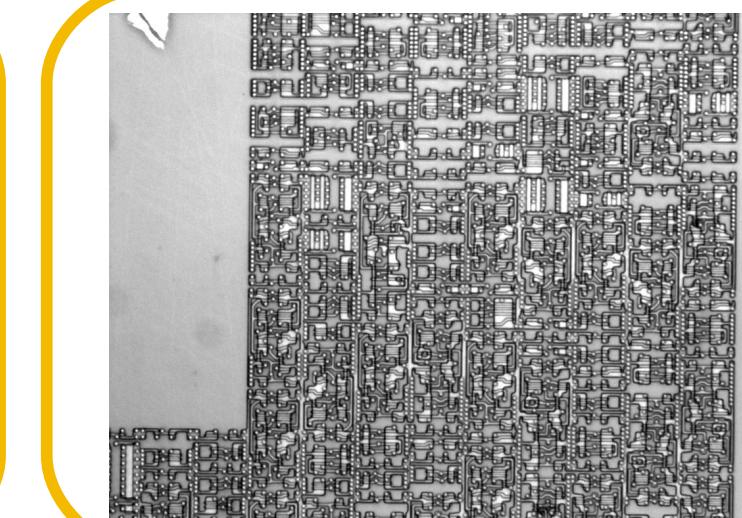
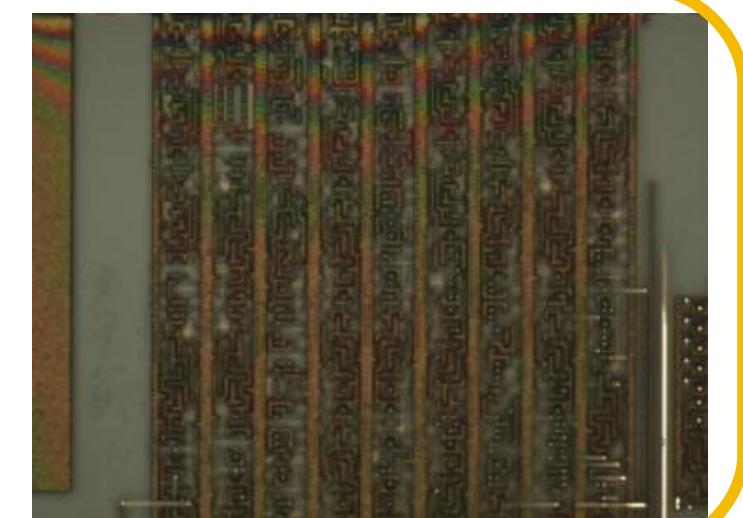
http://www.ece.utep.edu/courses/web5392/Notes_files/mos_fabrication.ppt.pdf



3 Interconnection layer

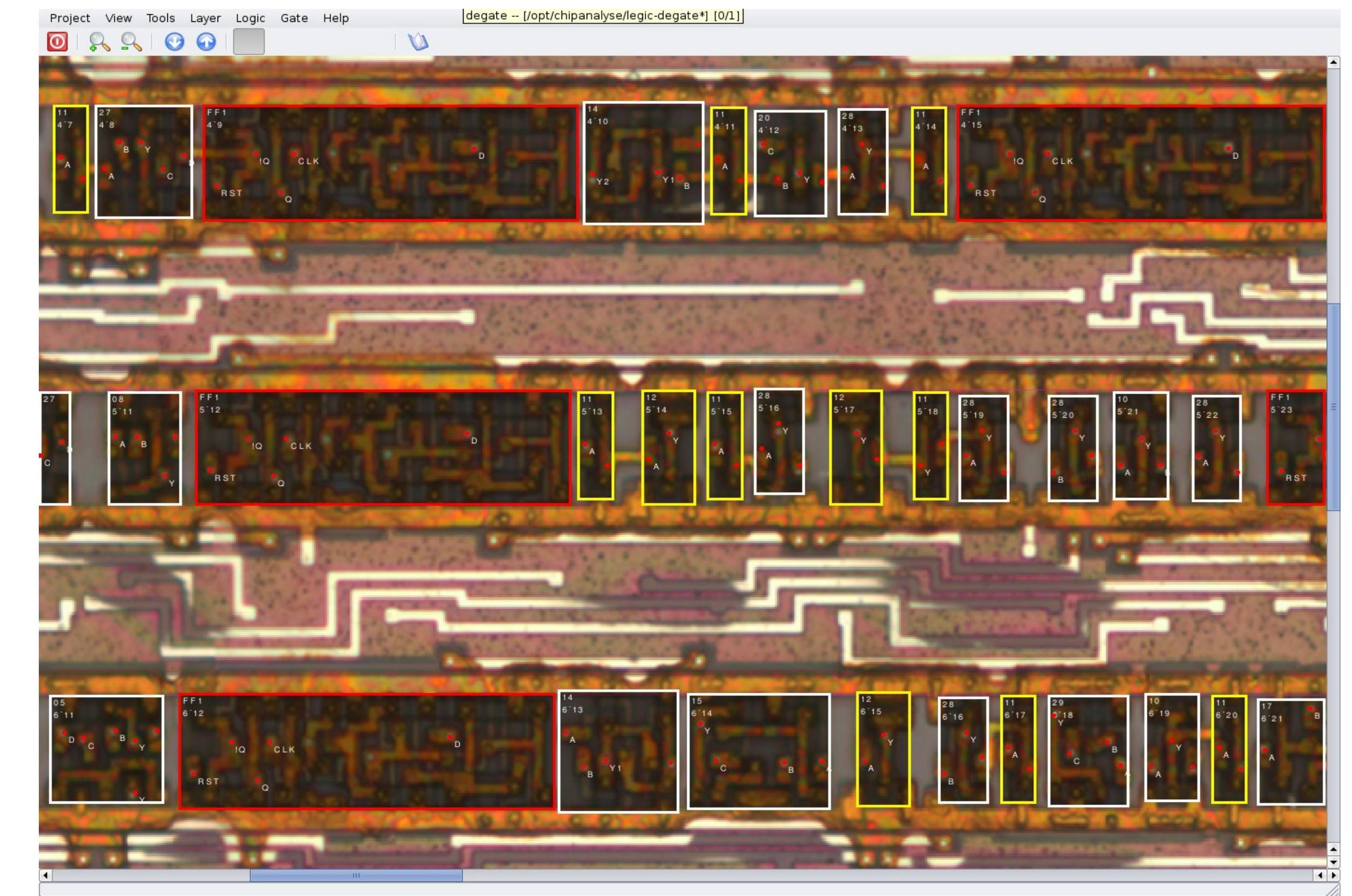
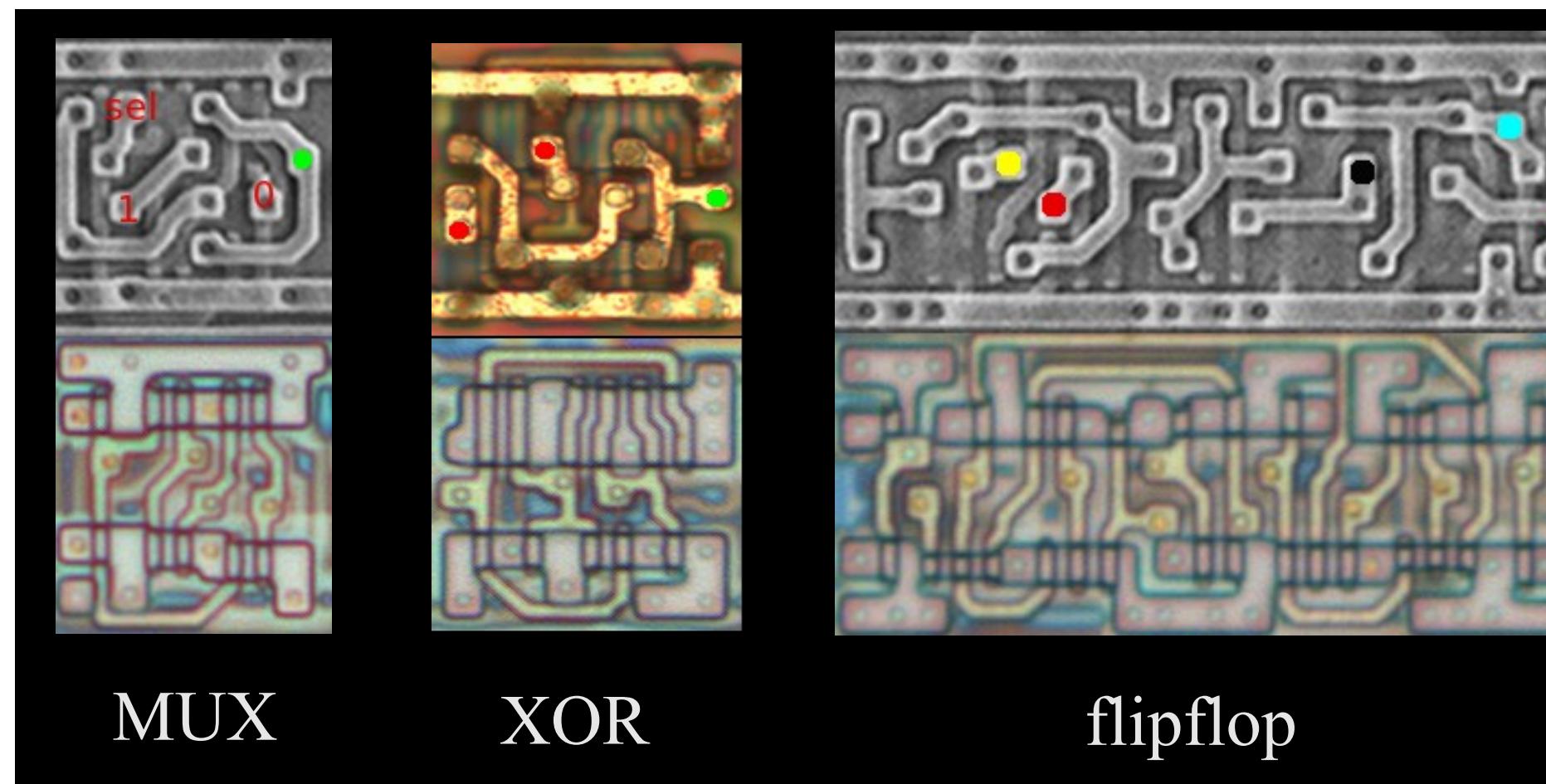


Logic
layer

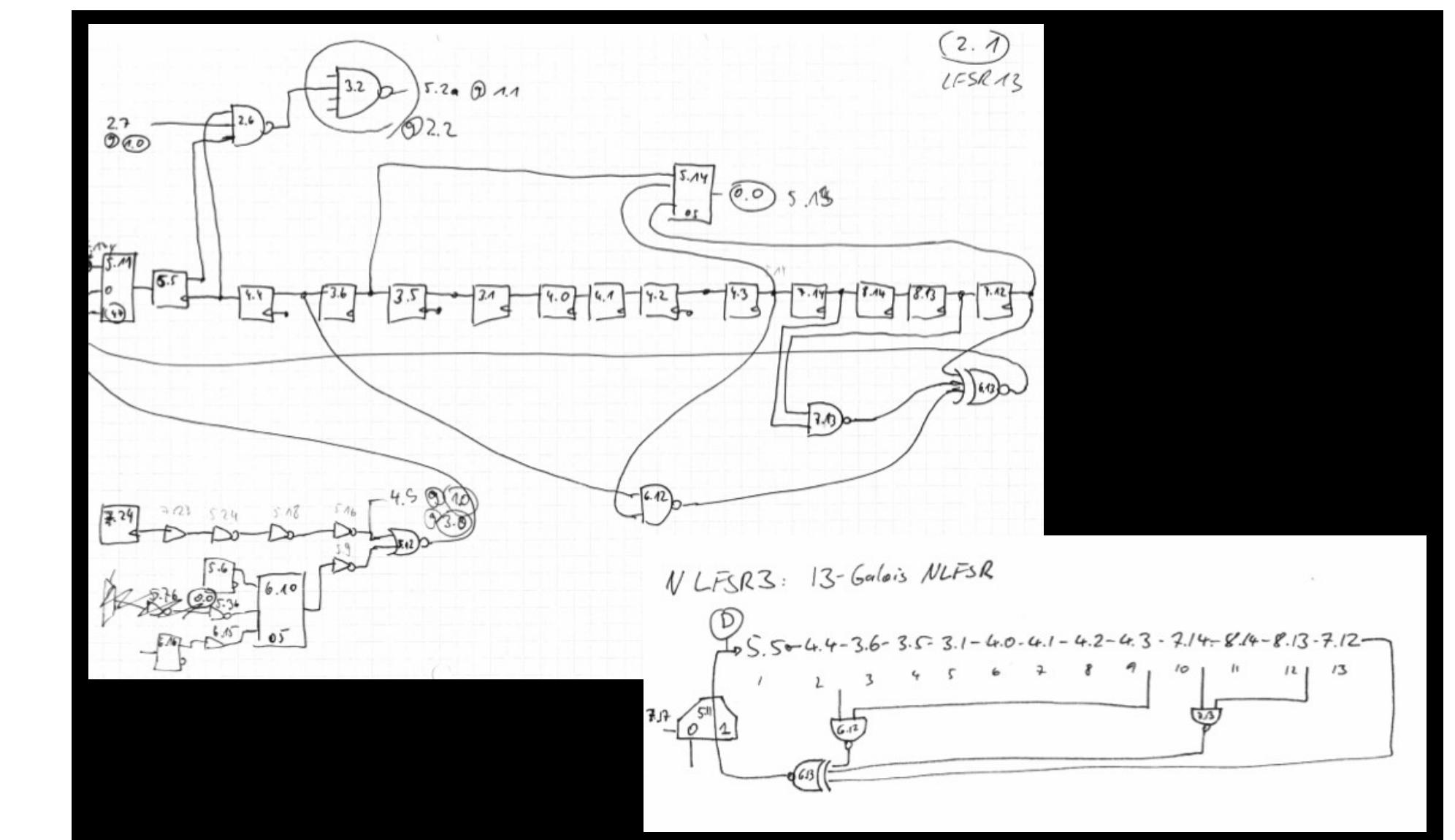
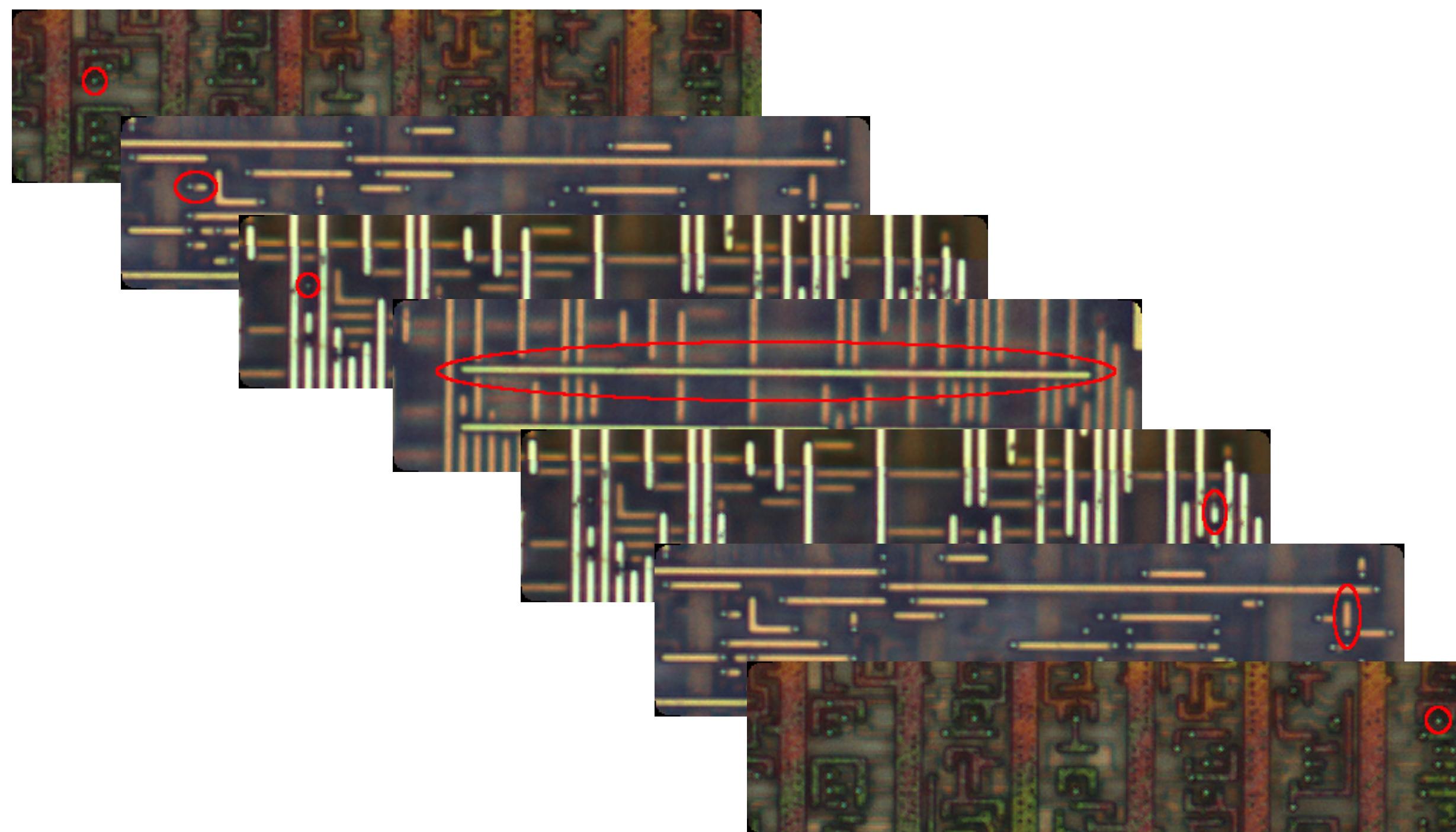


Transistor
layer

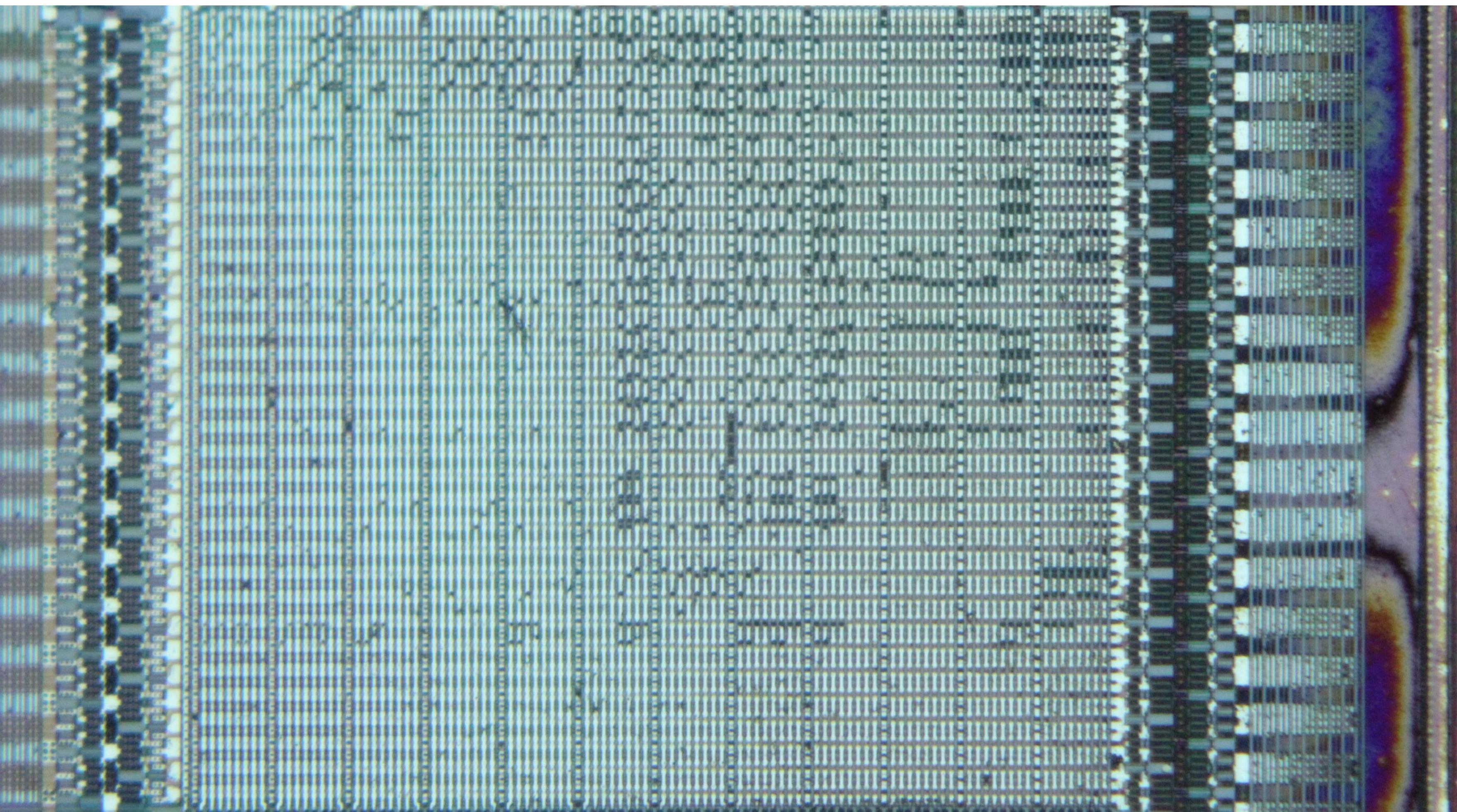
Gatter



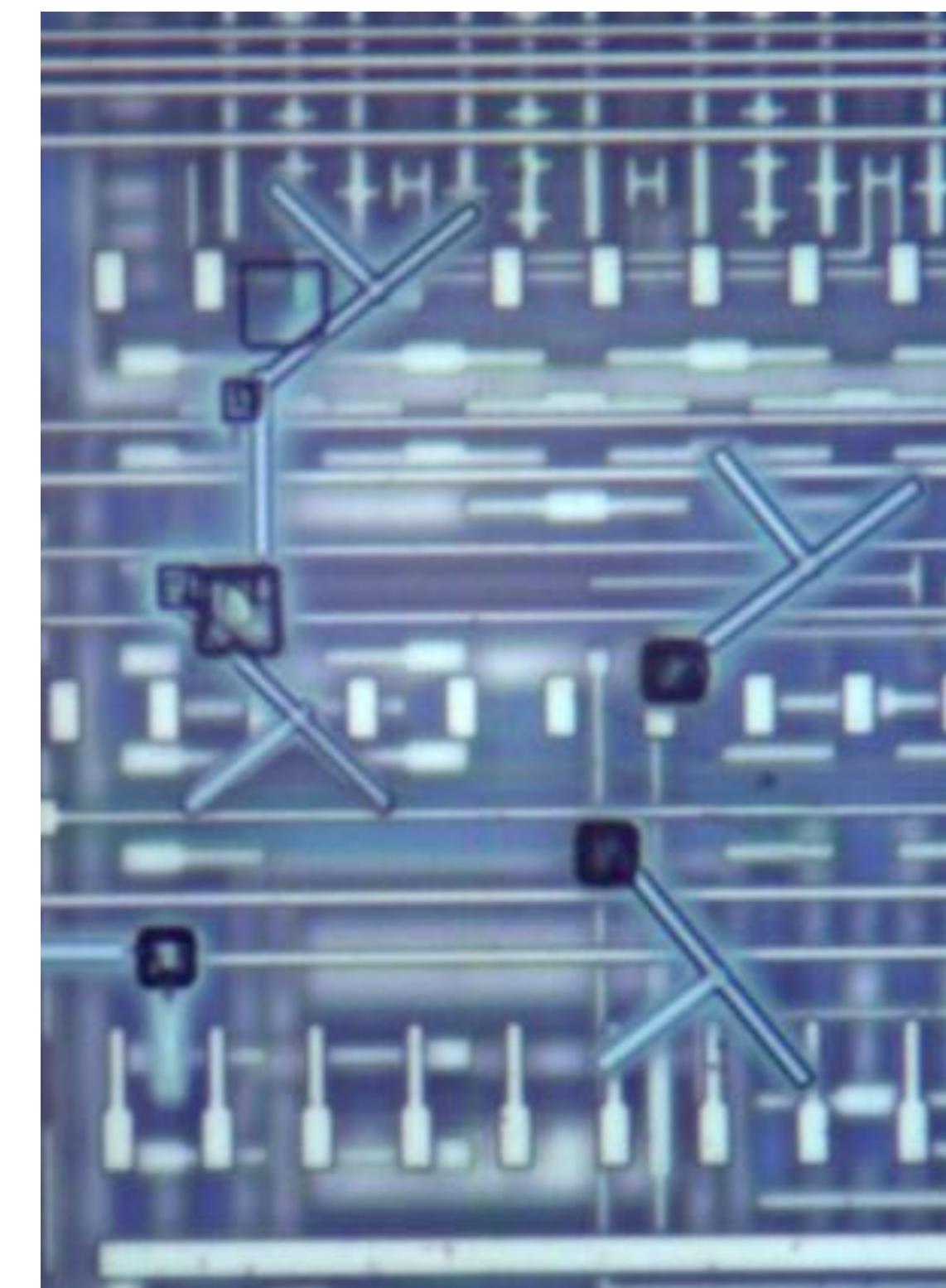
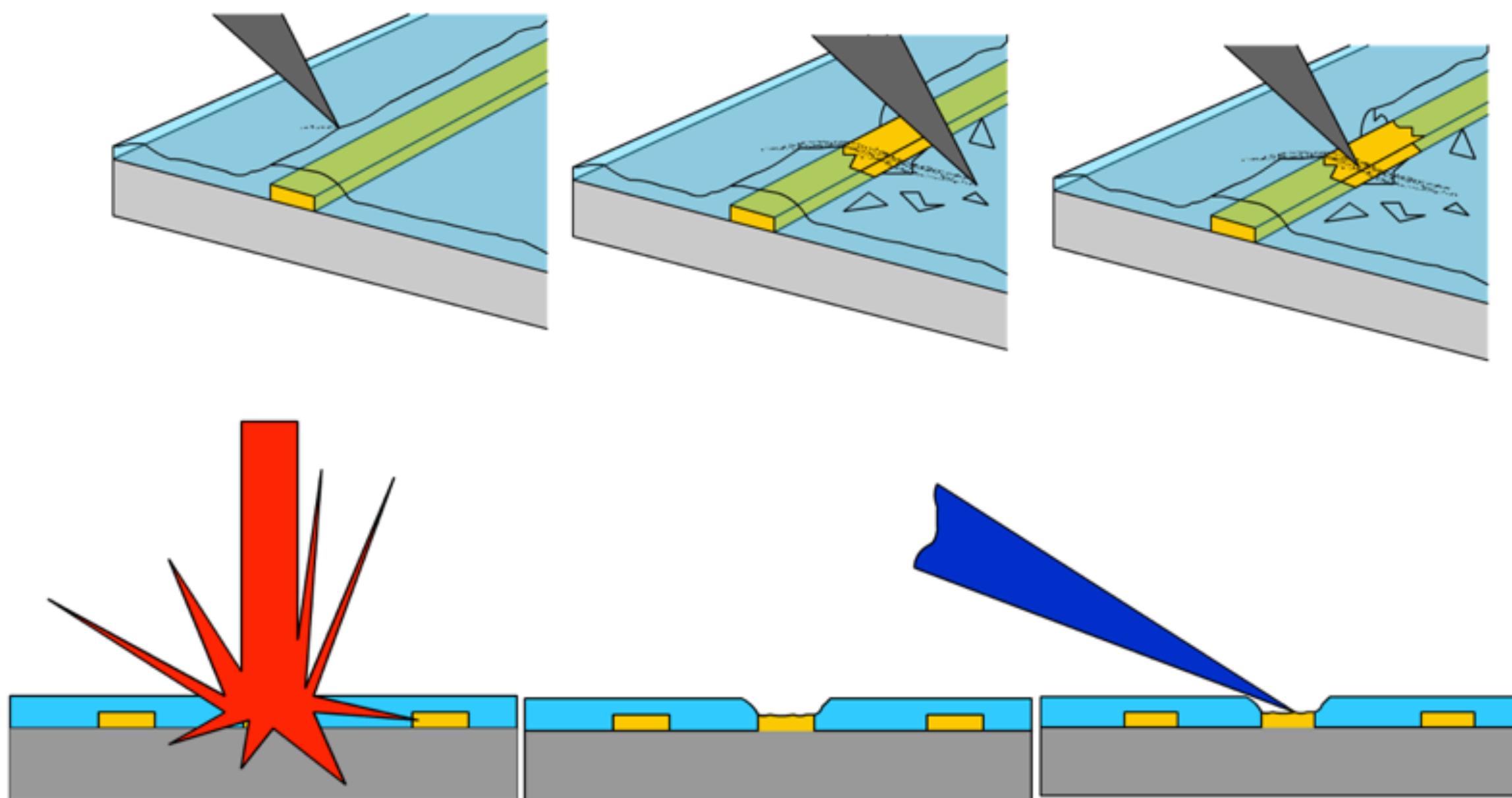
Tracing



ROM readout

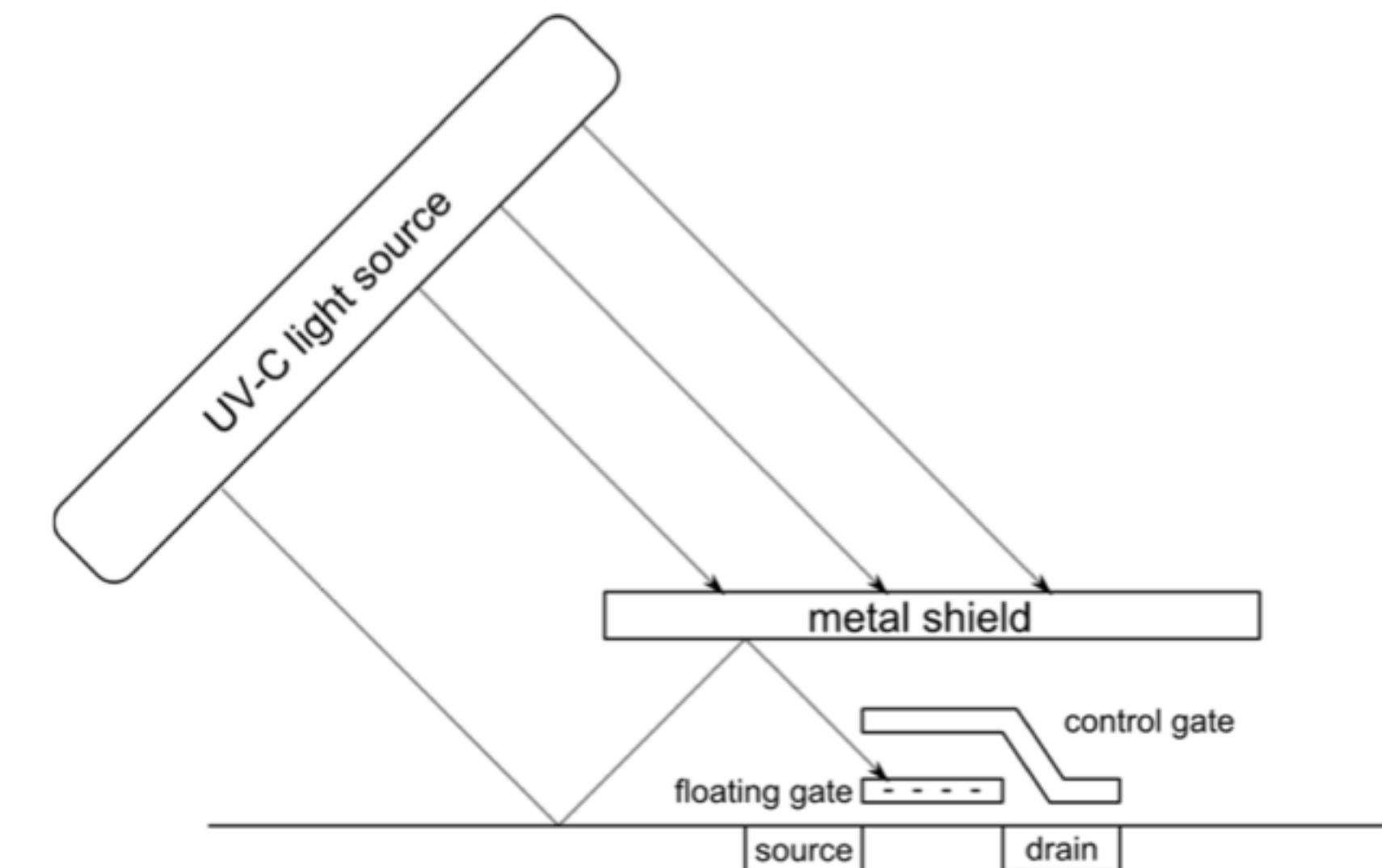
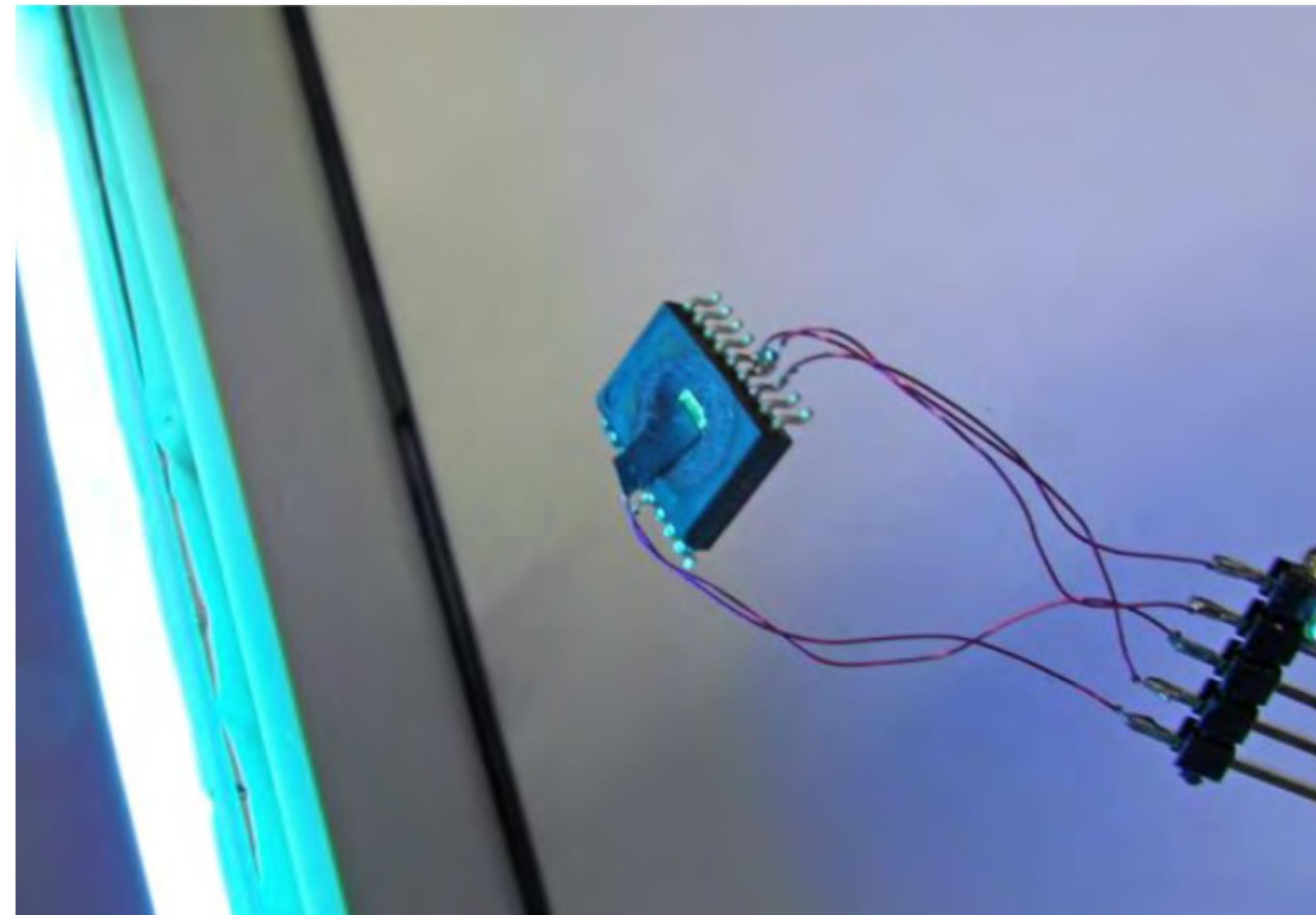


probing



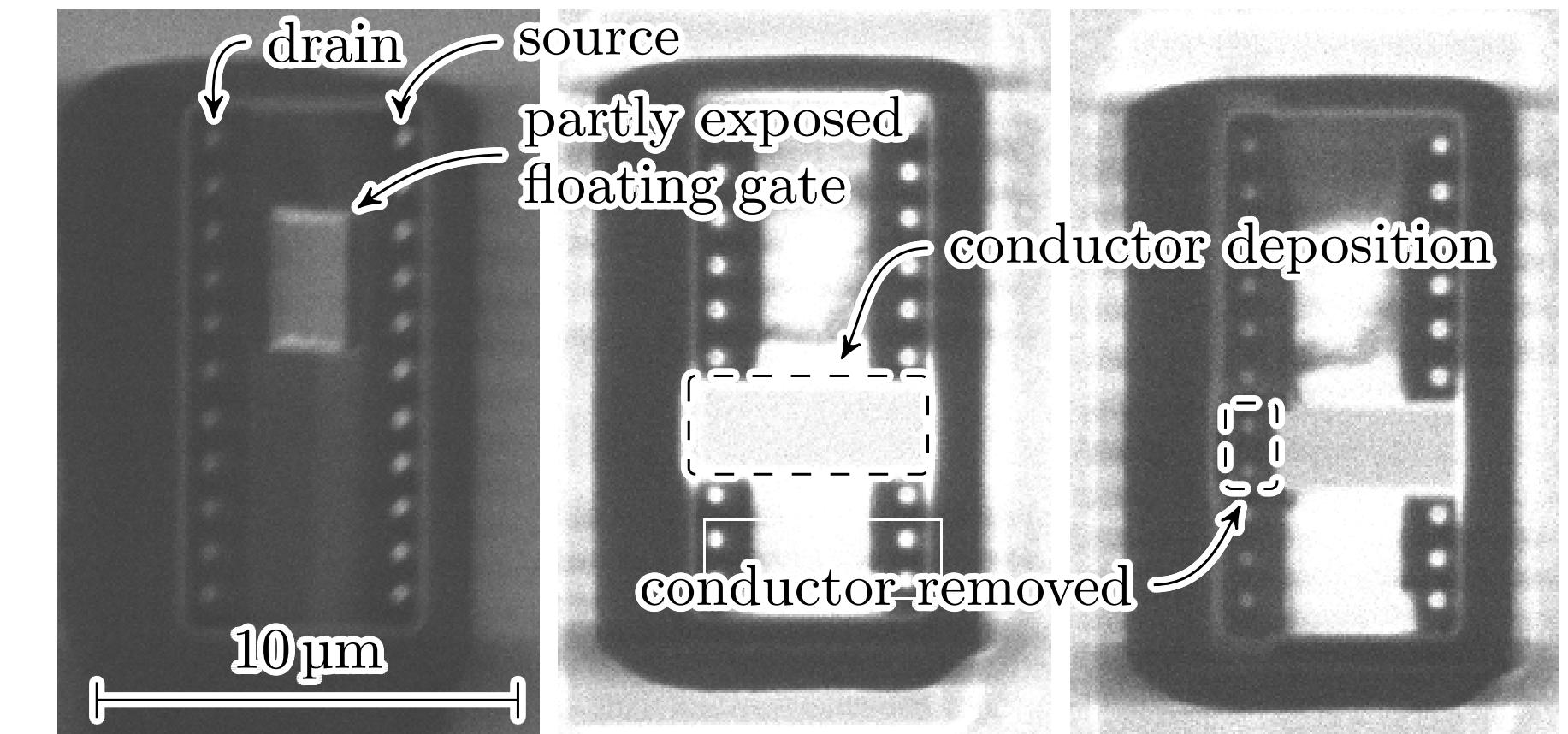
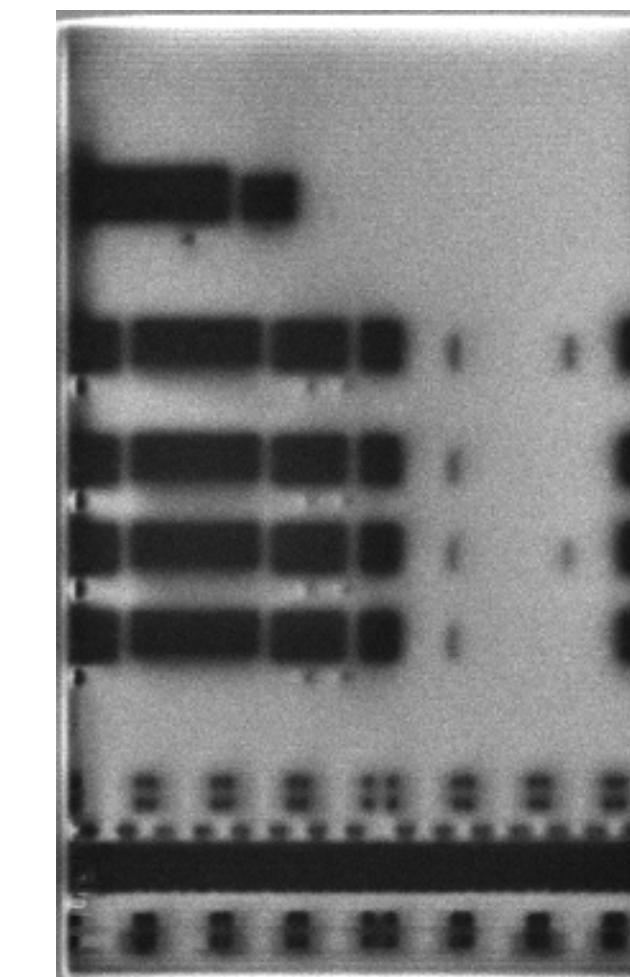
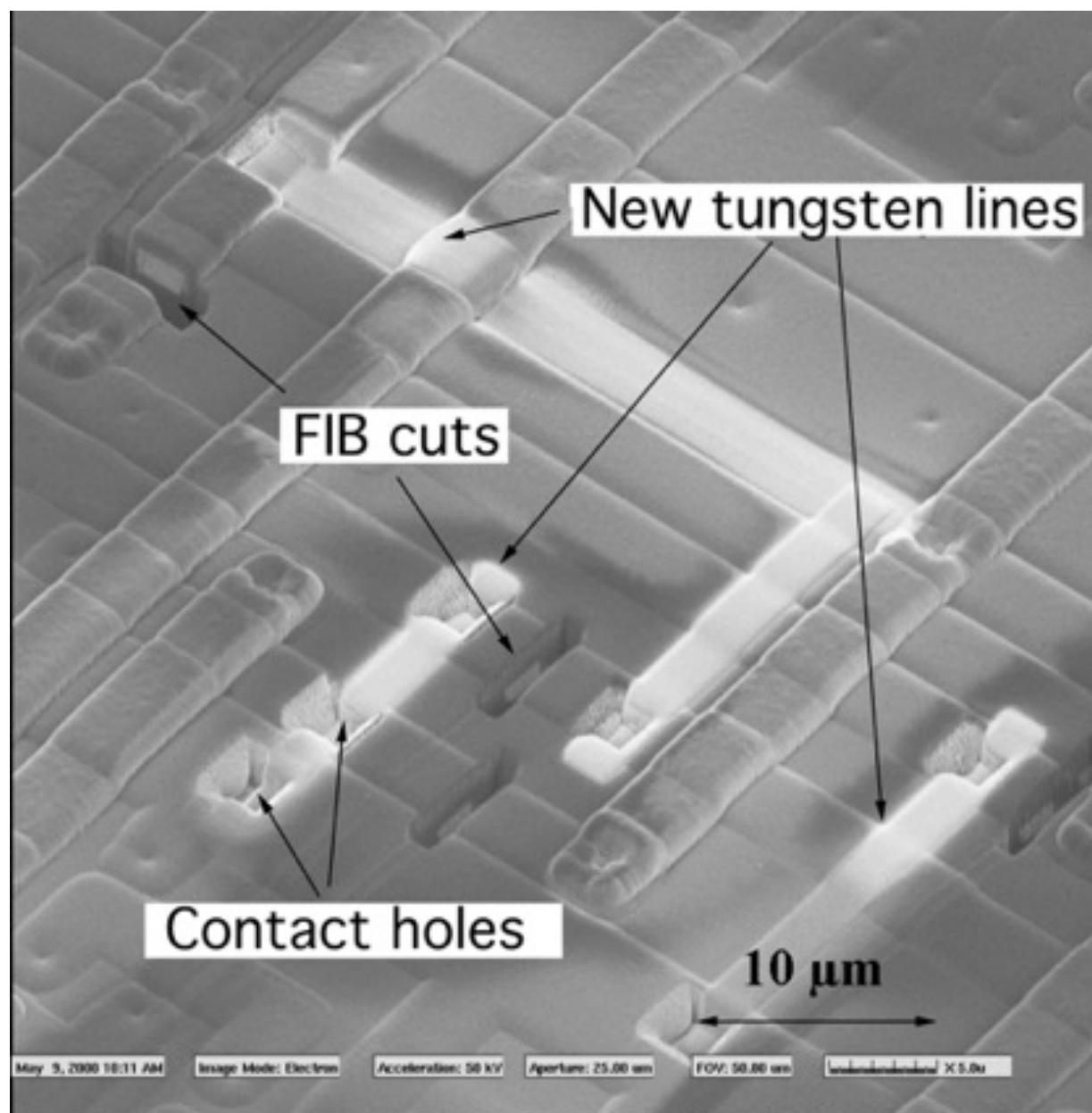
<http://prioritylabs.com/media/1085/optical-image-of-deposited-fib-probe-pads.jpg>

Fuses

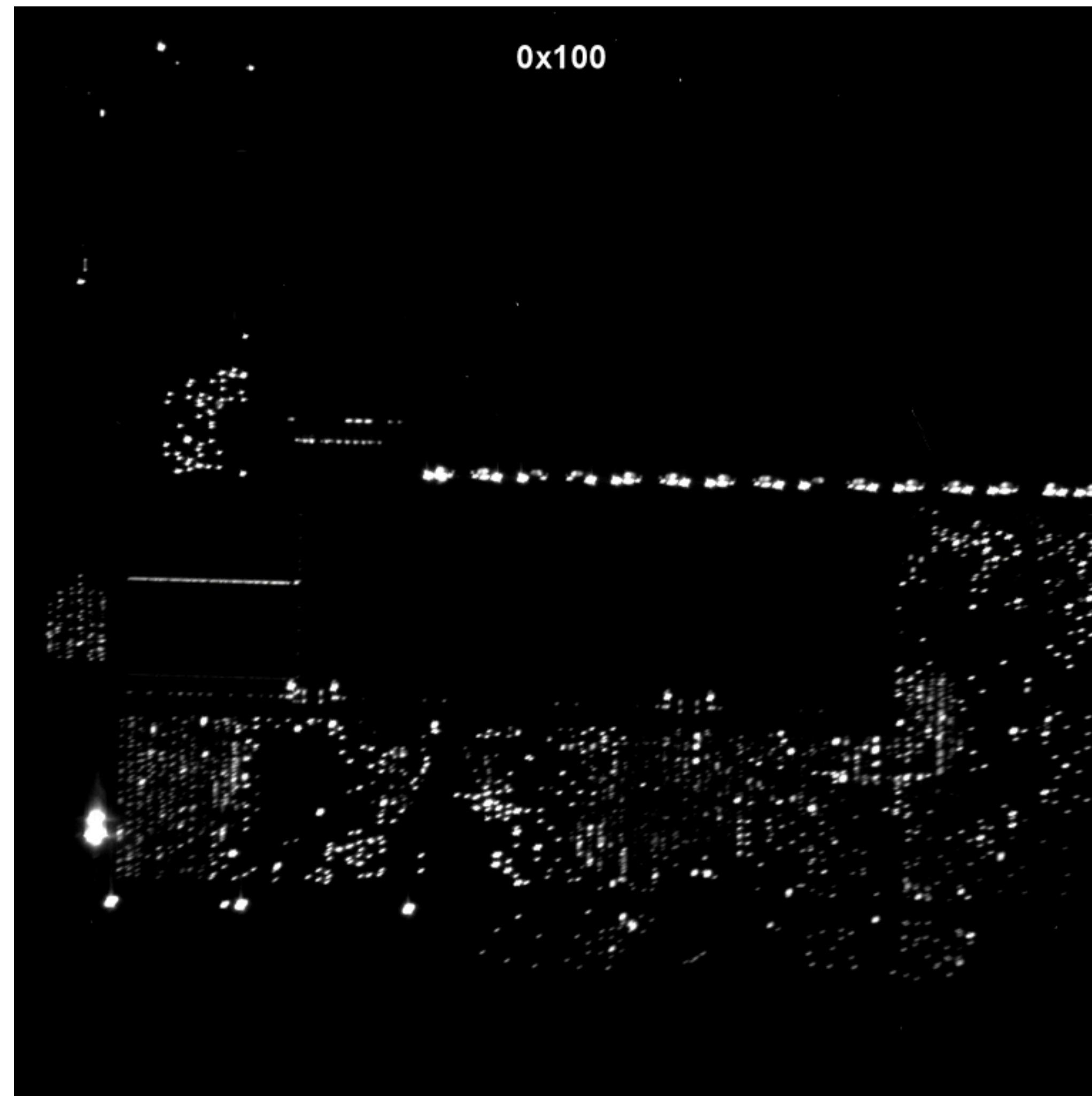


Quelle: Timo Kasper

FIB: kein Chip ist sicher



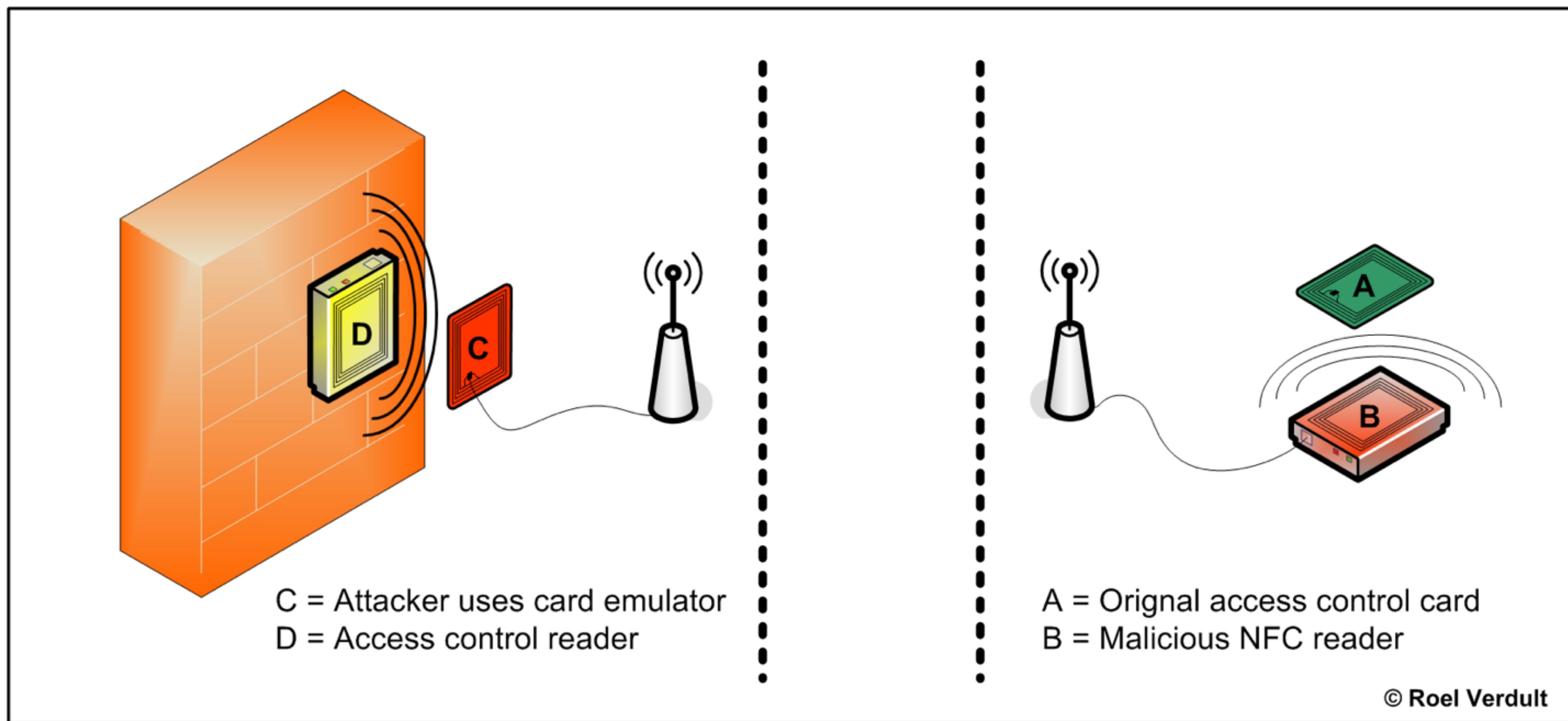
optical side channel

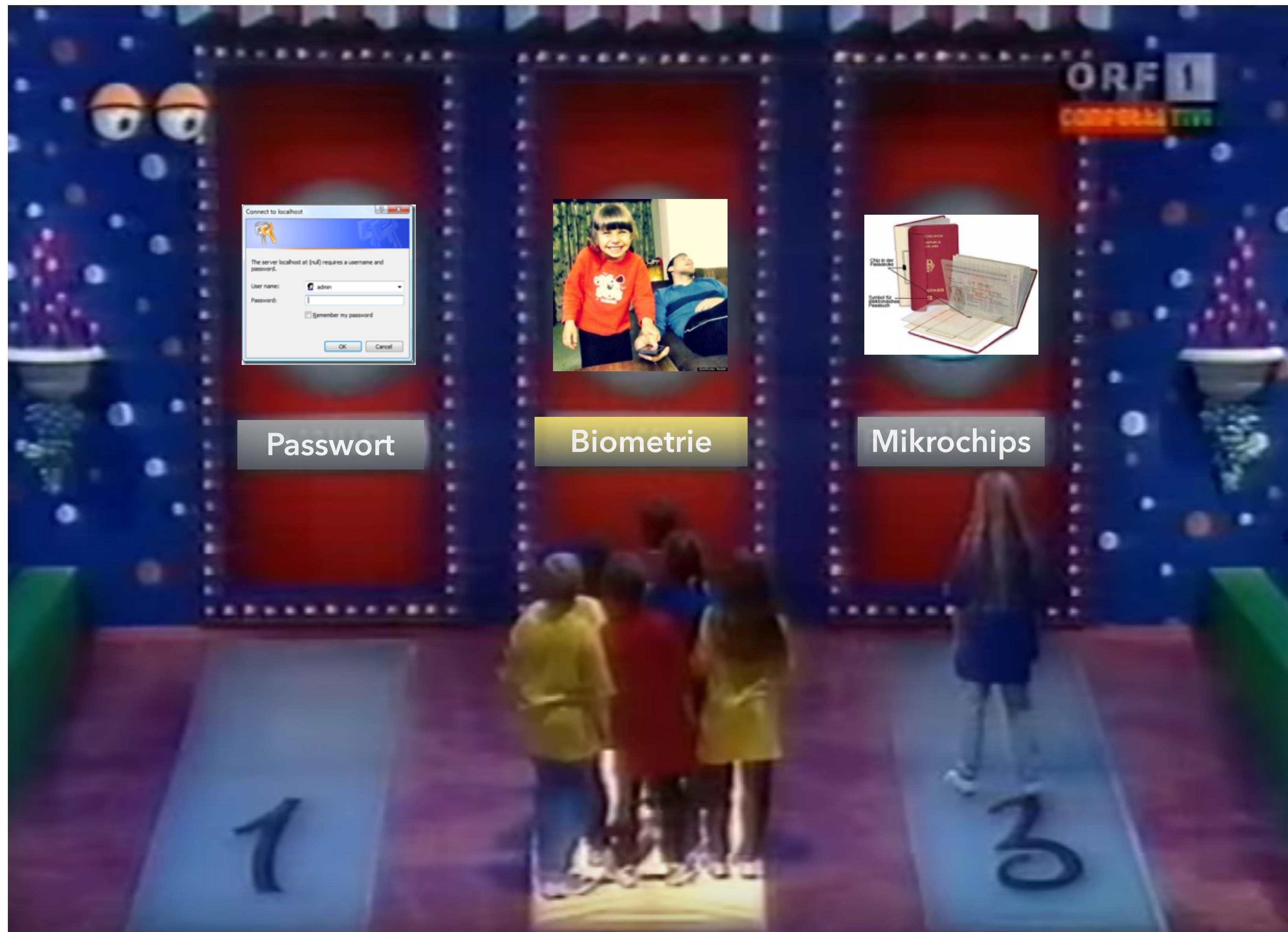


replay attack



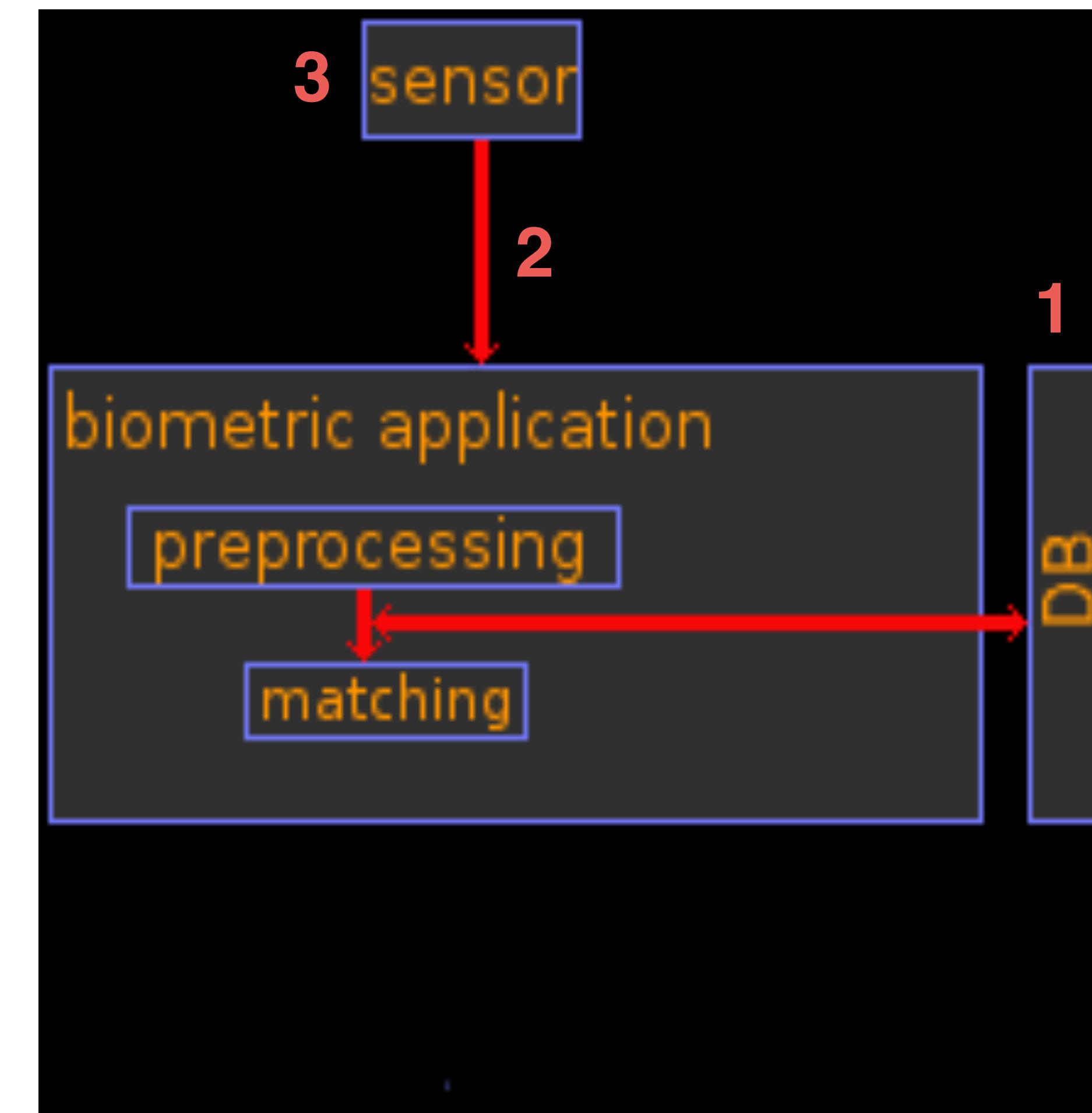
relay attack



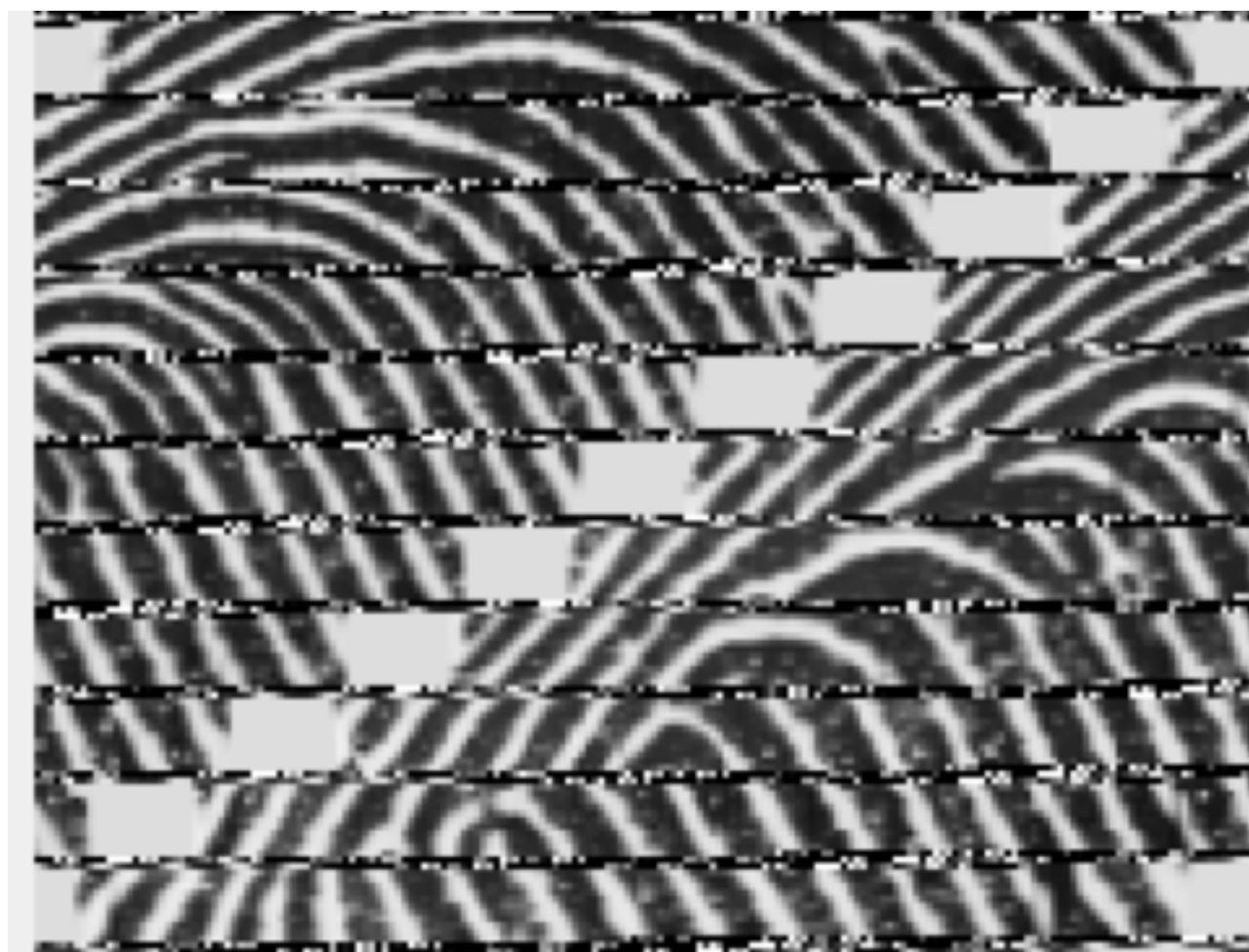


Biometrische Systeme

- Angriffspunkte
 - Datenbank
 - Kommunikation
 - Sensor

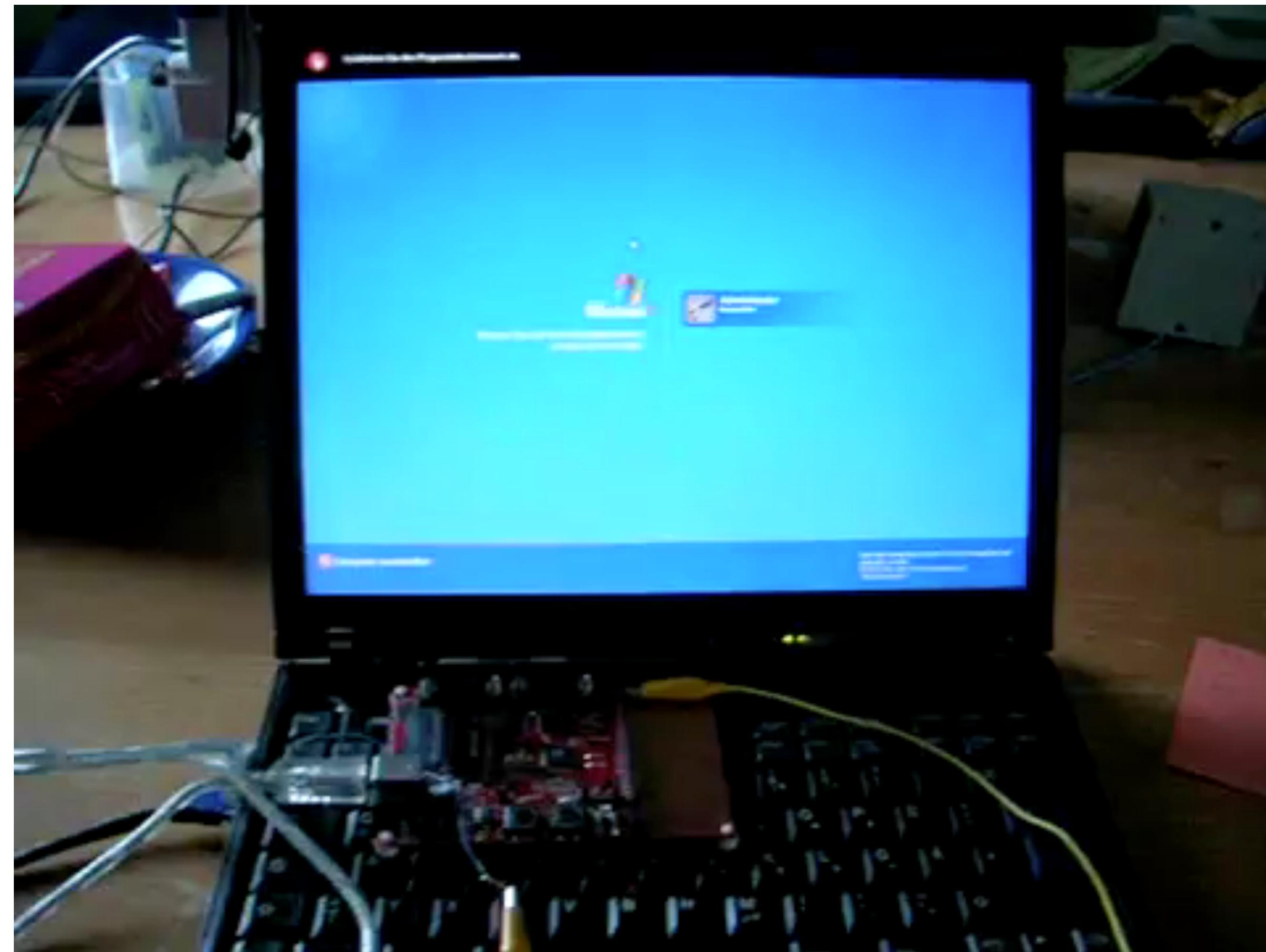


sniffing

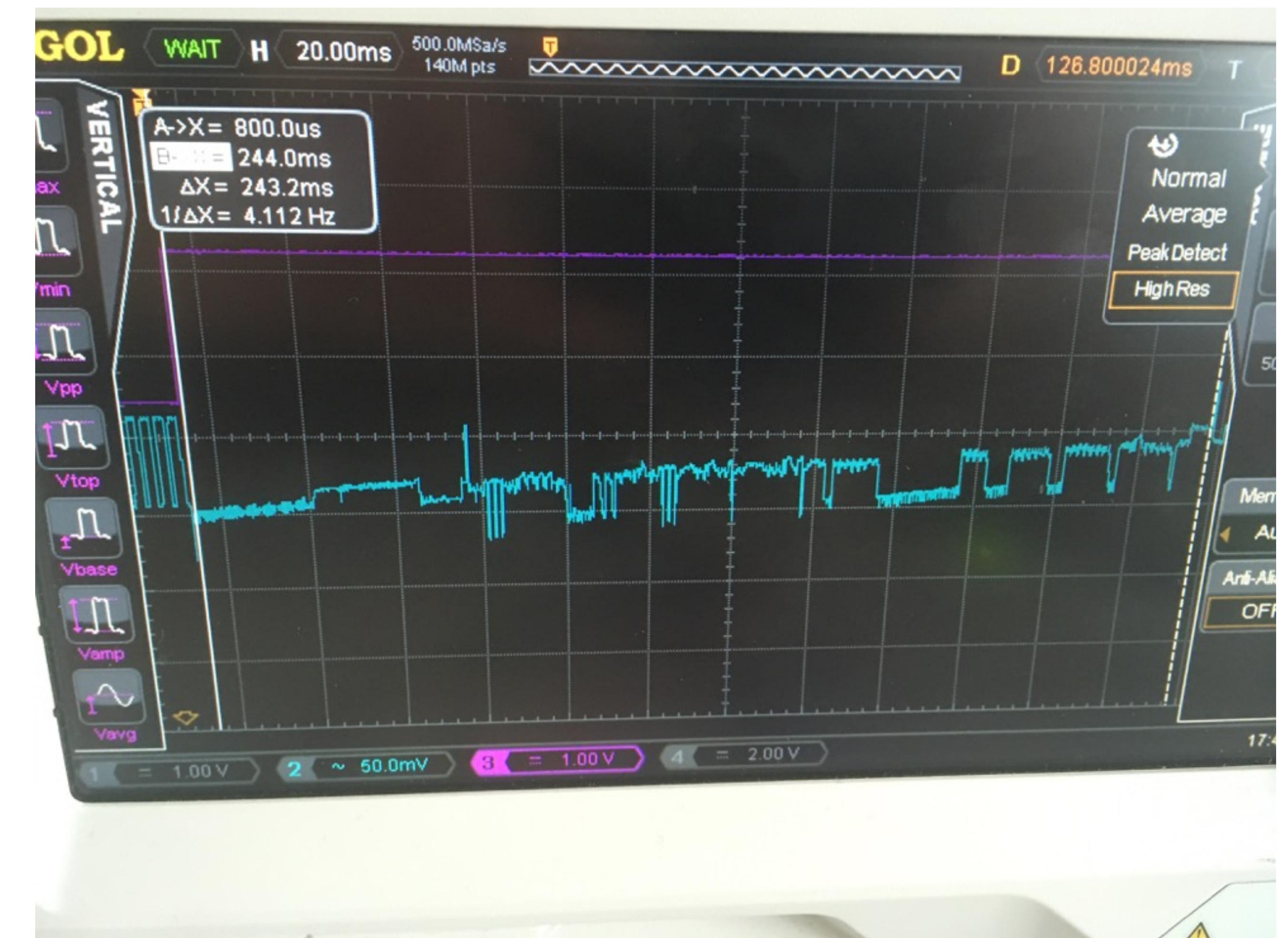
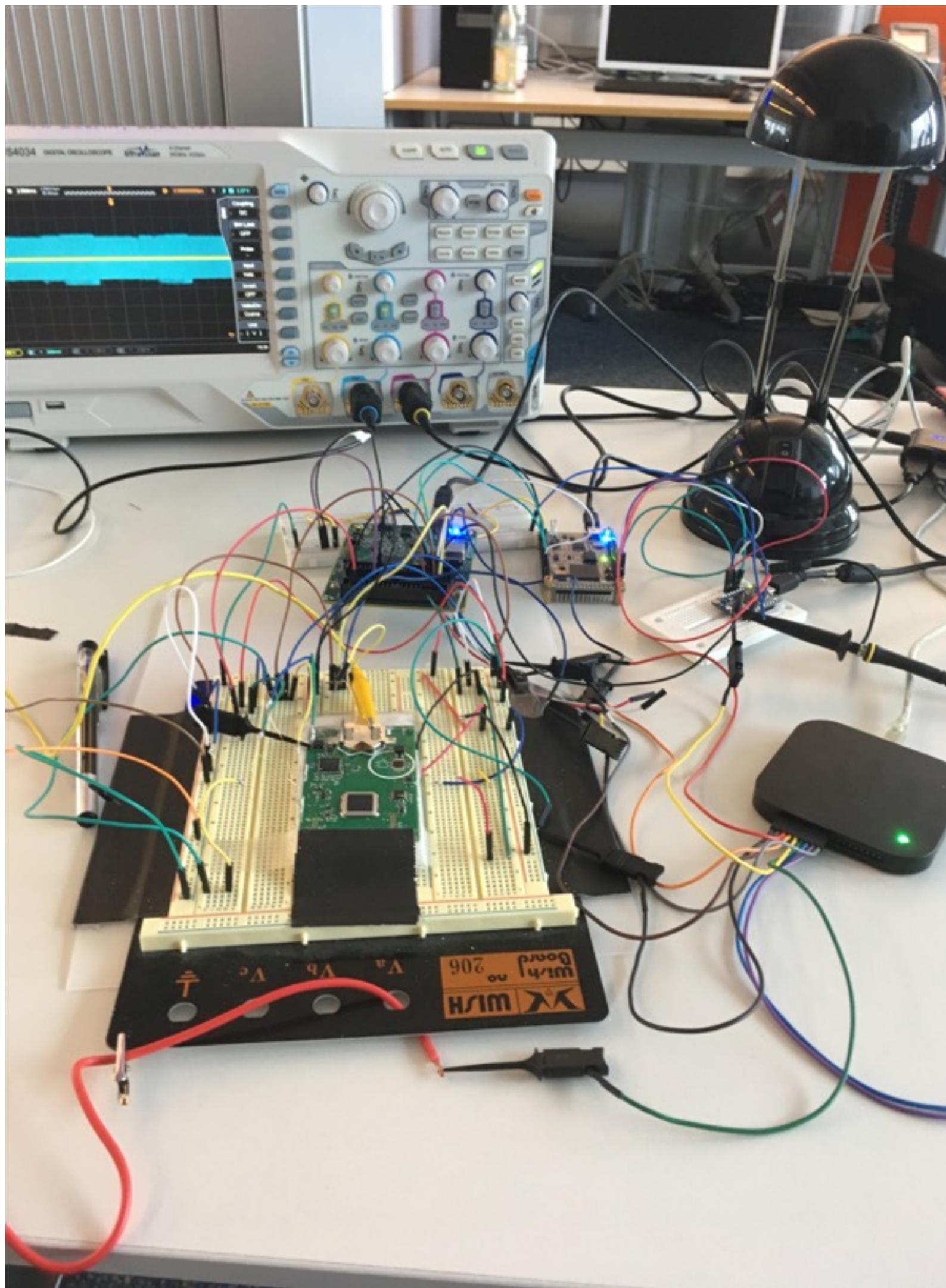


<http://images10.newegg.com/NeweggImage/ProductImage/34-995-074-02.jpg>

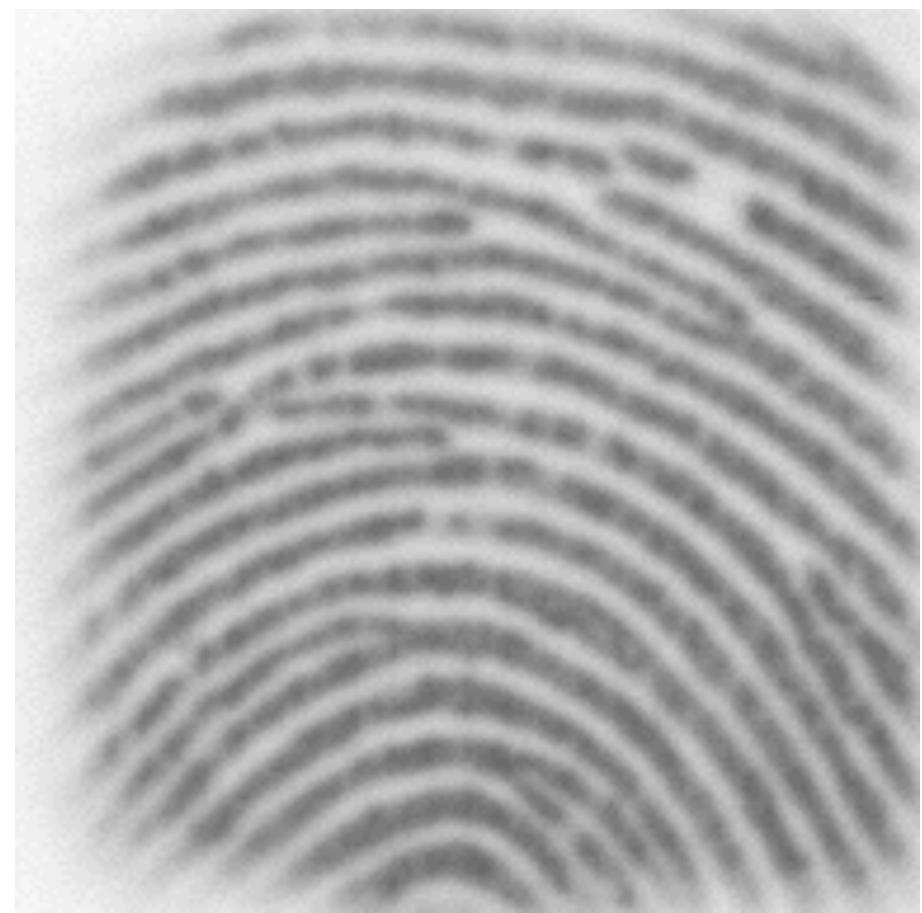
replay attack



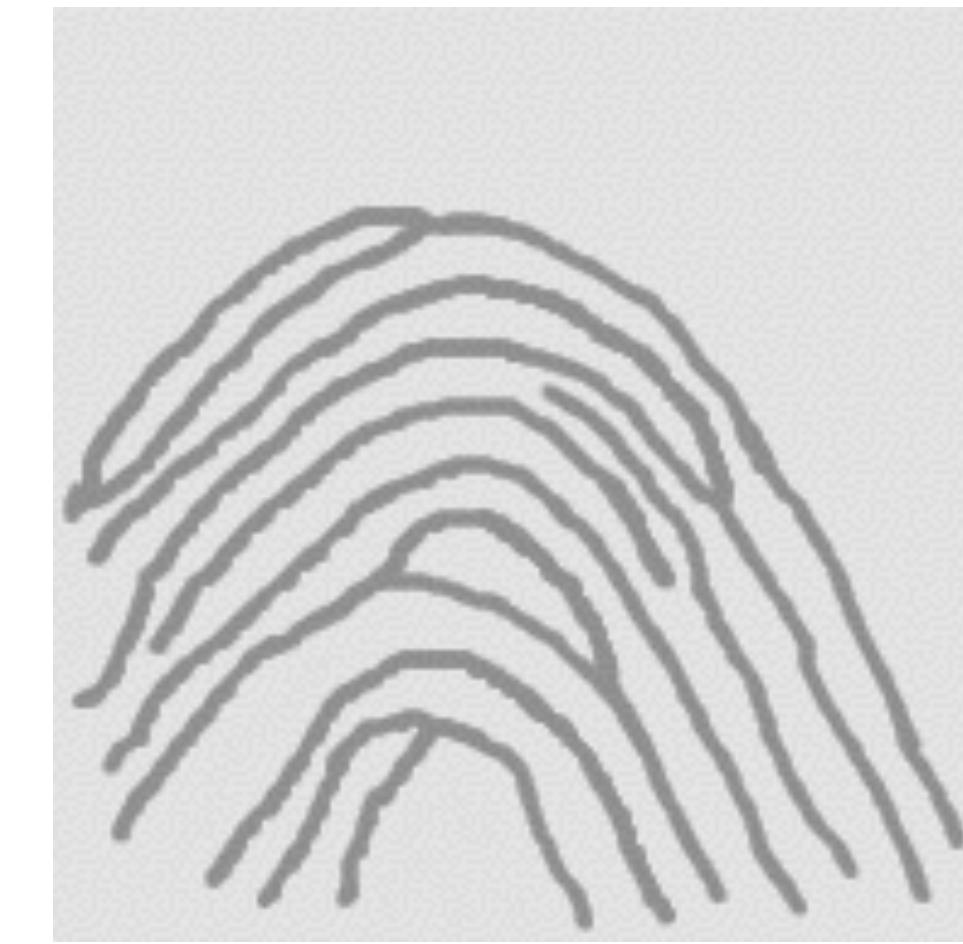
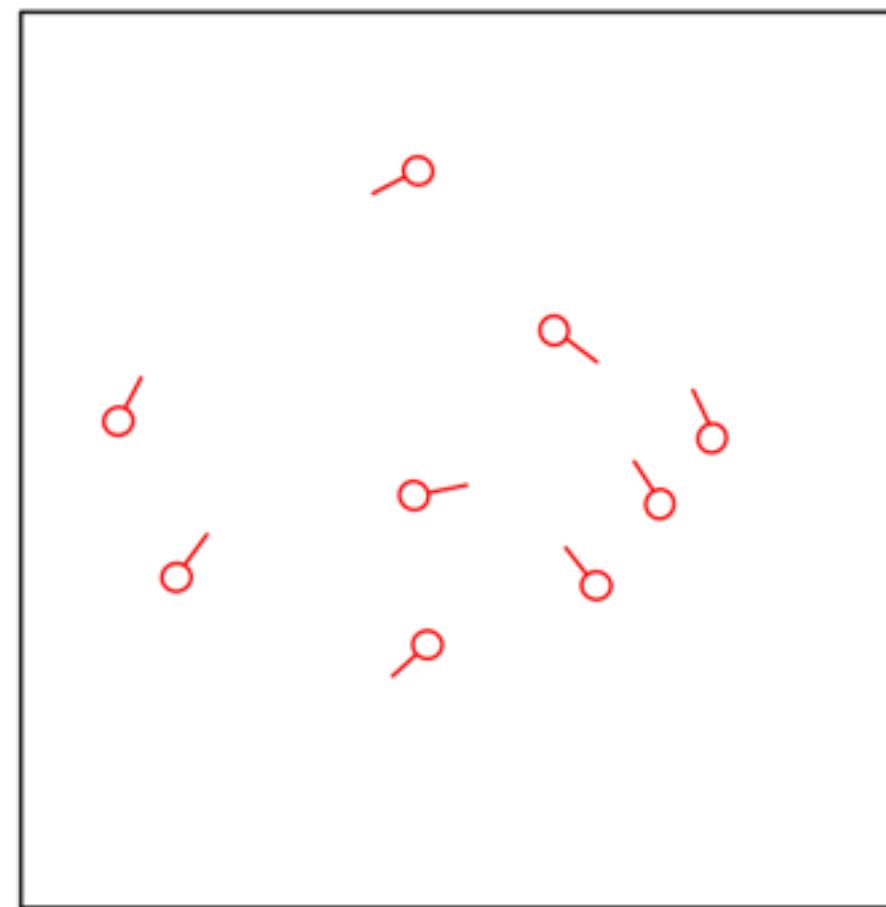
side channel



from template to image



```
00000000 46 4d 52 00 20 32 30 00 00 00 00 3c 00 00 00 c0  
00000010 00 c0 00 c5 00 c5 01 00 00 00 3c 05 80 8a 00 99  
00000020 c8 54 40 9e 00 99 ce 52 80 84 00 a5 a3 51 40 6f  
00000030 00 51 c0 49 80 88 00 b1 b8 3e 00 00
```



Hacker klauen Fingerabdruck

Bild HANNOVER
UNABHÄNGIG · ÜBERPARTEILICH
www.bild.de

Mallorca ab 49€
One-Way-Komplettreise inkl. Service und Meisen
airberlin.com Your Airline.

Irak-Rebellen ziehen sich nach Blutbad zurück
Bagdad - Feuerpause im Irak! Fünf Tage nach Ausbruch der blutigen Kämpfe im Südirak hat der schiitische Islamistenführer Muqtada al-Sadr seine Miliz-Soldaten an gewiesen, die Waffen niederzulegen und sich zurückzuziehen.
"Die In-

Nazi-Sex-Party!
Eine Szene aus dem Skandal-Video
Von PHILIPP HEDEMANN, GEORG NOLTE und FRANK SCHNEIDER Ein Sex-Video schockt die Motor- Sportwelt. Die Sonntagszeitung "Sportwelt. Die Sonntagszeitung World" berichtet

Löwe attackiert Mädechen in Zoo
Nizza - Ein Mädchen (4) wurde angegriffen und verletzt. Ein Onkel, der durch den Zoo von Nizza (Frankreich) ging, rettete das Kind am Löwen.

Keine Marken mehr auf Ebay?
Mannheim - Ein Hersteller von Markenartikeln darf den Verkauf seiner Produkte bei Ebay verbieten. Das entschied das Landgericht Mannheim.

Hacker klauen Fingerabdruck von Schäuble!
Innenminister Wolfgang Schäuble

96 0:0 - aber neuer Vertrag für Stajner
Der Kult-Stürmer soll diese Woche verlängern - SPORT

Montag, 31. März 2008 0,50 €

Reporterauf!
Von W.M. STRATEN Nachts um 1 Uhr griff No-namedator Jen Leb...
moen (38) in London Fotografen an. Was er sagt - SPORT.

GOLD-BINGO 5. Spiel GLÜCKS-CODE 50024050
141 184 208 211 224 326 430 437 513 538

CAROLINE Auftritt im Skandal-Kleid
Prinzessin Caroline (51) schockte beim Rosenball in Monaco mit einem durchsichtigen Chanel-Kleid - Seite 12.

NACHRICHTEN
Jet stürzt in Wohngebiet
London - Ein Kleinflugzeug ist am Sonntag im Süden von London abgestürzt. Die Maschine explodierte beim Auftaun auf zwei Einfamilienhäuser. Eines der Häuser brannte ab. (Foto). An Bord befanden sich fünf Insassen. Alle kamen ums Leben.

Bald unter 4 % arbeitslos?
Berlin - Wirtschaftsminister Rüdiger Rüttgers rechnet damit, dass die Arbeitslosigkeit sich mittelfristig auf „drei bis vier Prozent“ halbieren könnte.

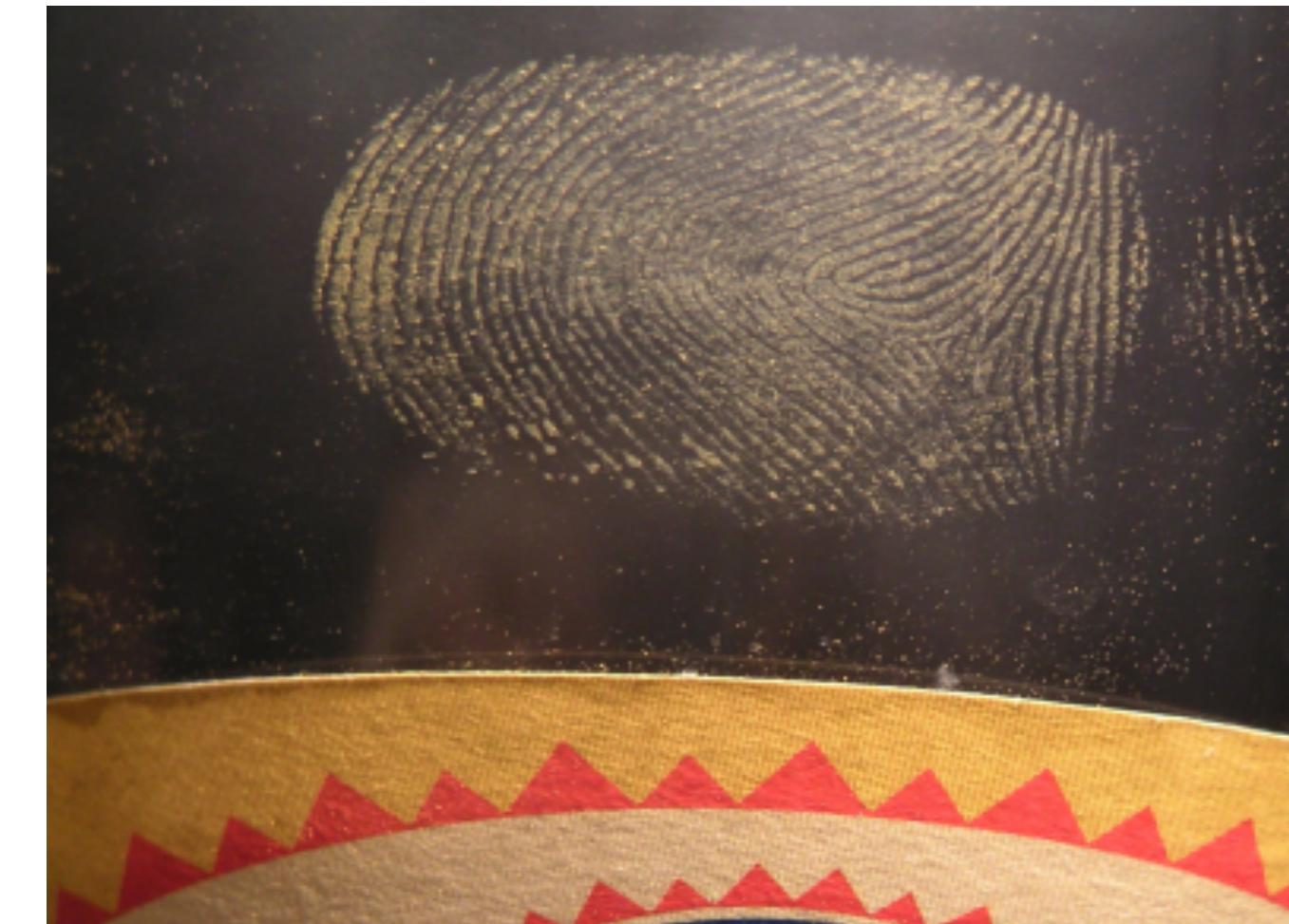
Deutsche Geiseln befreit
Santiago de Chile - Neun Ausbilder der Bundeswehr wurden in Chile von einer kriminellen Bande als Geiseln genommen. Einige wurden leicht verletzt. Die Polizei befreite die Soldaten, verhaftete die Täter.

Mehr Muslime als Katholiken
Vatikanstadt - Die Zahl der Muslime übersteigt mit weltweit 1,3 Milliarden die der Katholiken (1,1 Mrd.), meldet die Vatikan-Zeitung „Osservatore Romano“.

Bahn-Streik kostet 500 Mio.
Düsseldorf - Die Lokführersstreiks bei den Deutschen Bahn haben Kosten in Höhe von rund 500 Millionen Euro verursacht. Das errechnete der Vorsitzende des Vereins für Sozialpolitik, Friedrich



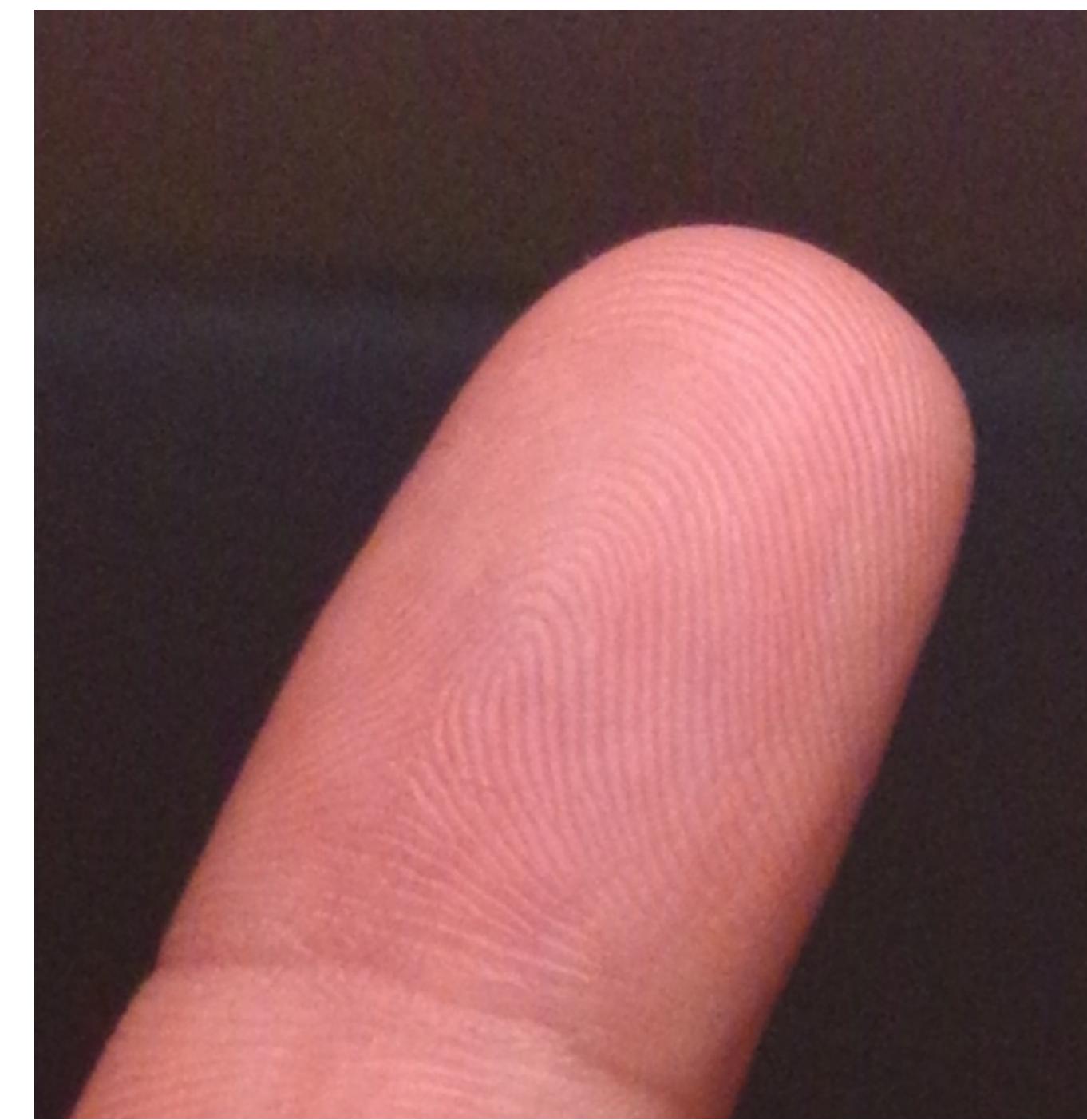
was die Polizei kann...



anonyme Erpresserbriefe

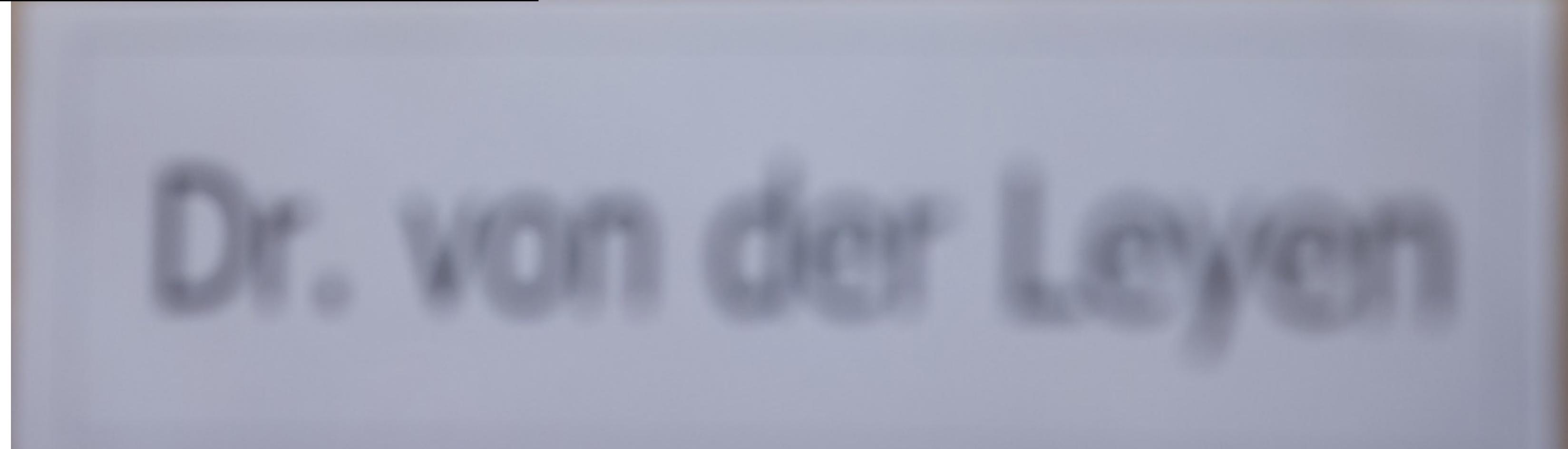


Fingerabdrücke fürs Fotoalbum



Zeig mir deine Hand . . .

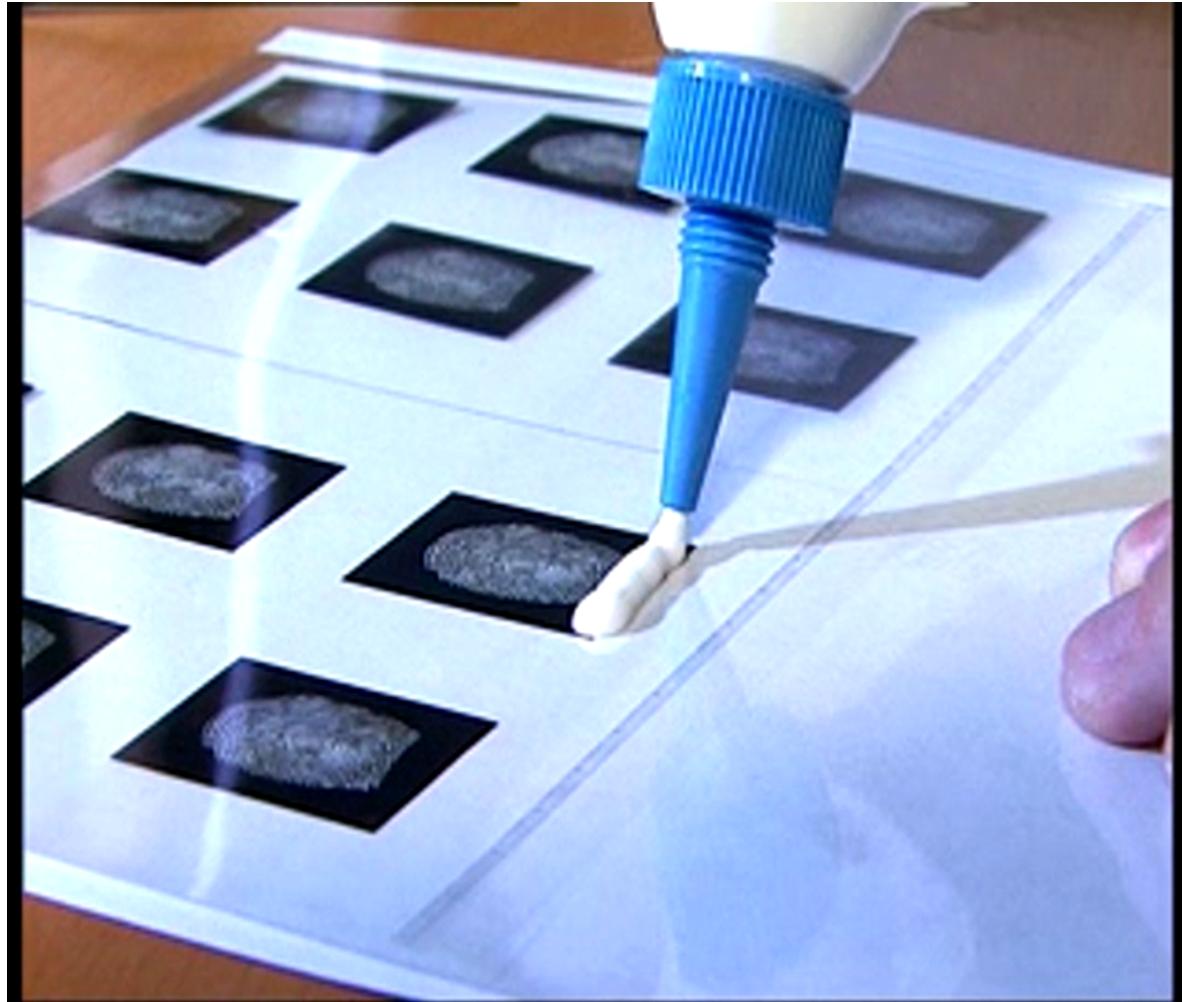




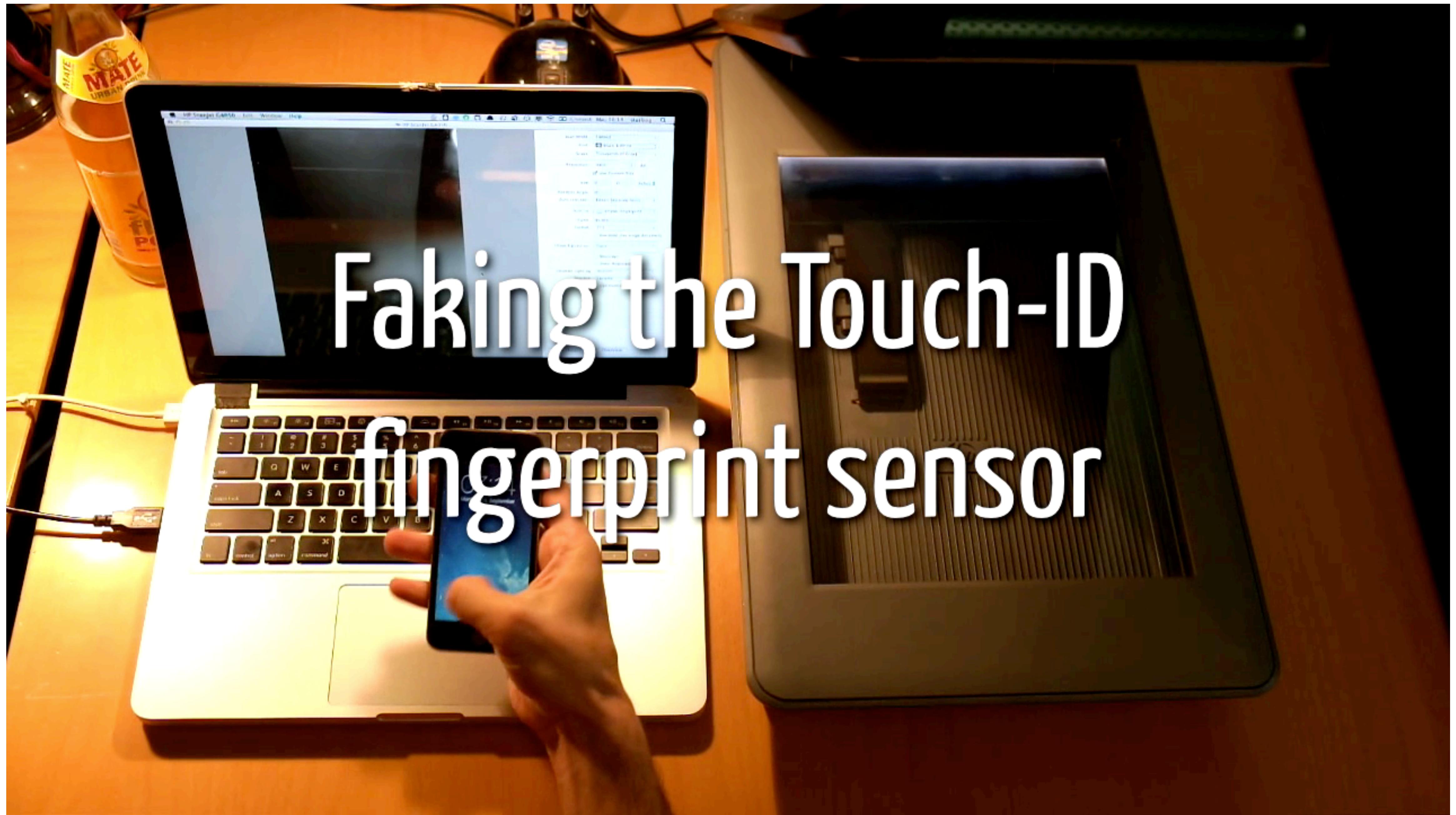
im Internet



Attrappenbau



Faking the Touch-ID fingerprint sensor

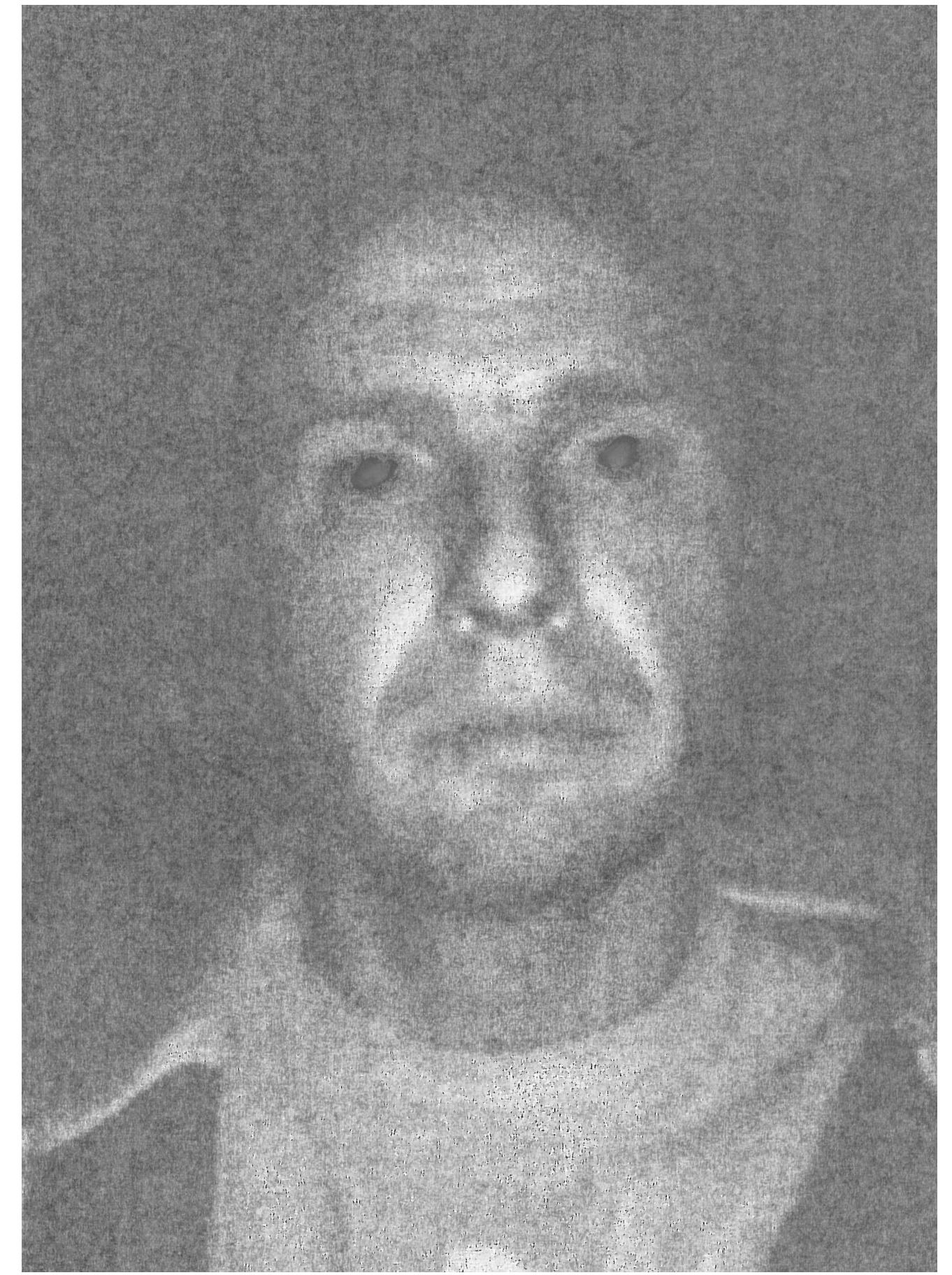
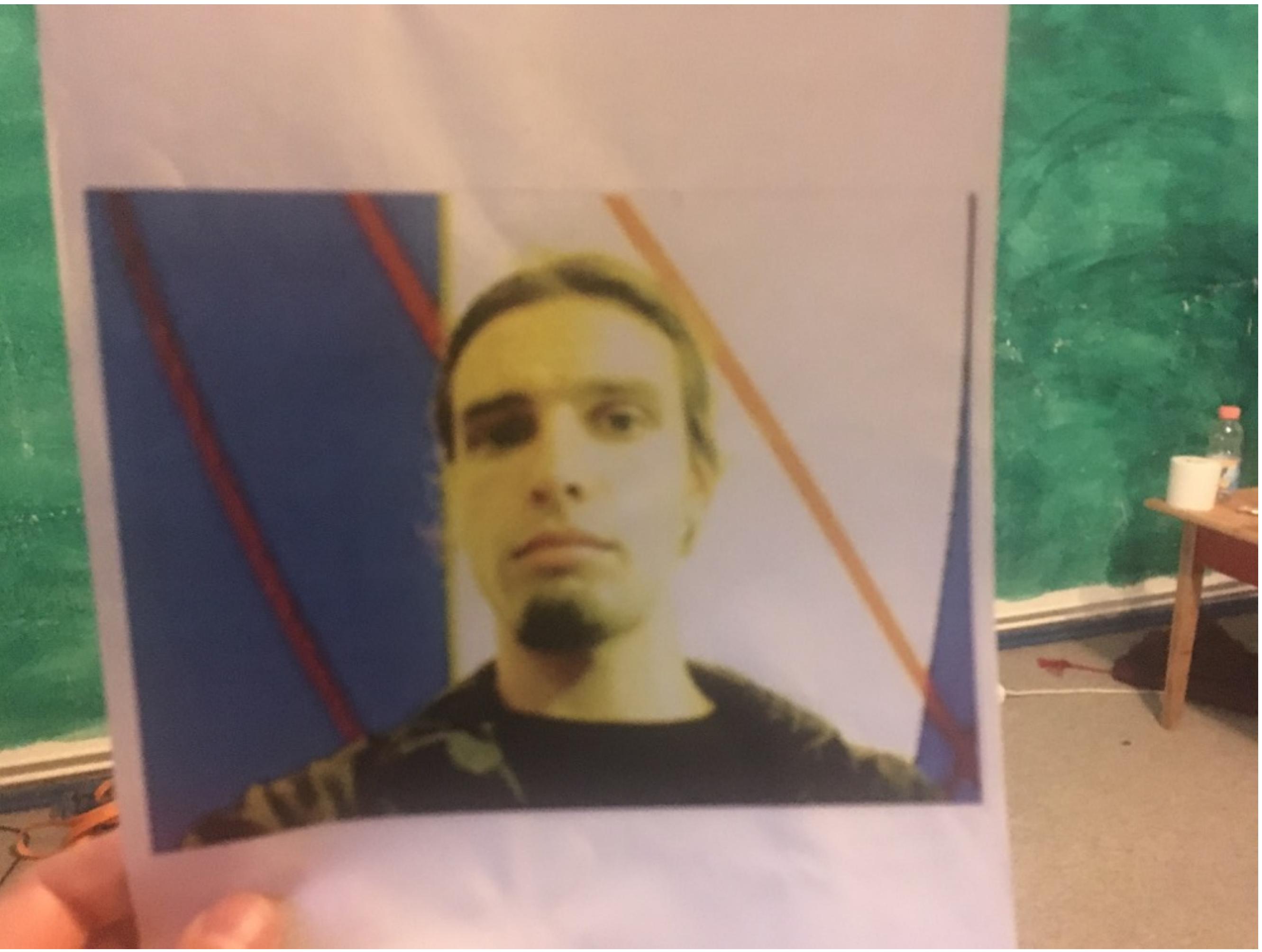


Finger aus dem Drucker

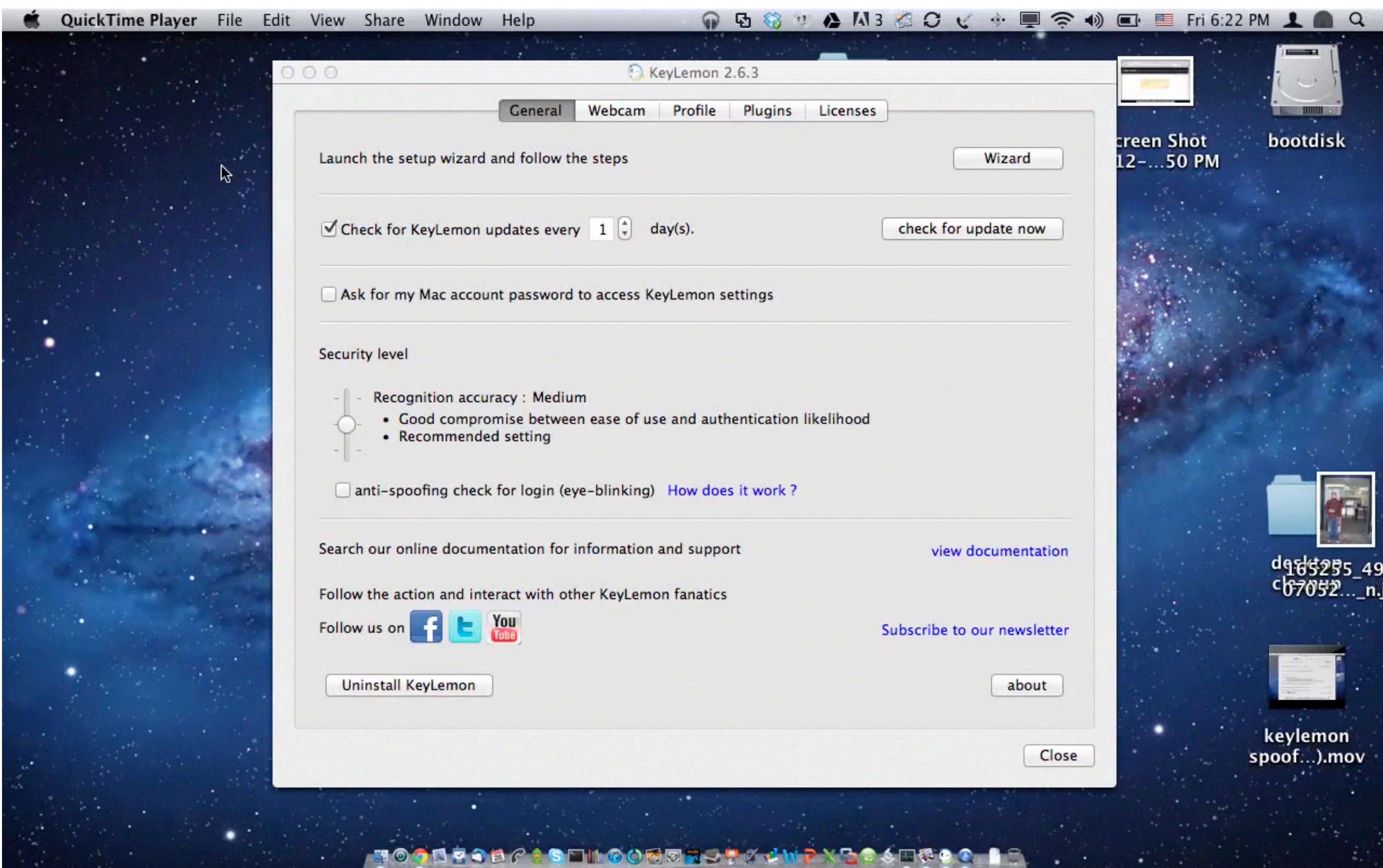


could
use similar methods to steal
personal identities and
other vital information.

I see faces



Gesichtserkennung *gähn*



Bewegtbilder



mastercard



<http://www.sharinpix.com/blog/take-a-selfie-and-pay-your-coffee>

face manipulation

Comparison to Previous Work



Input Video

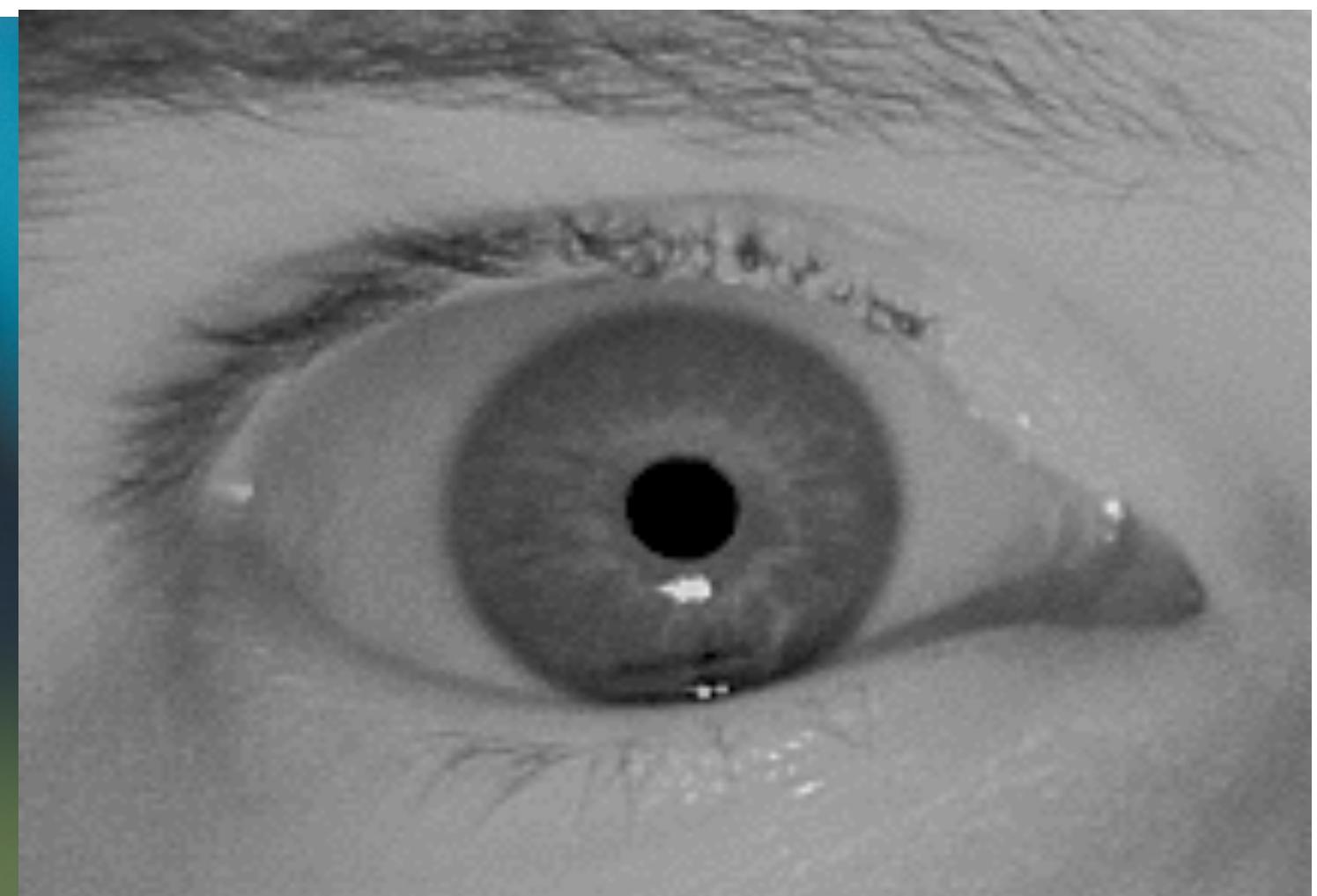
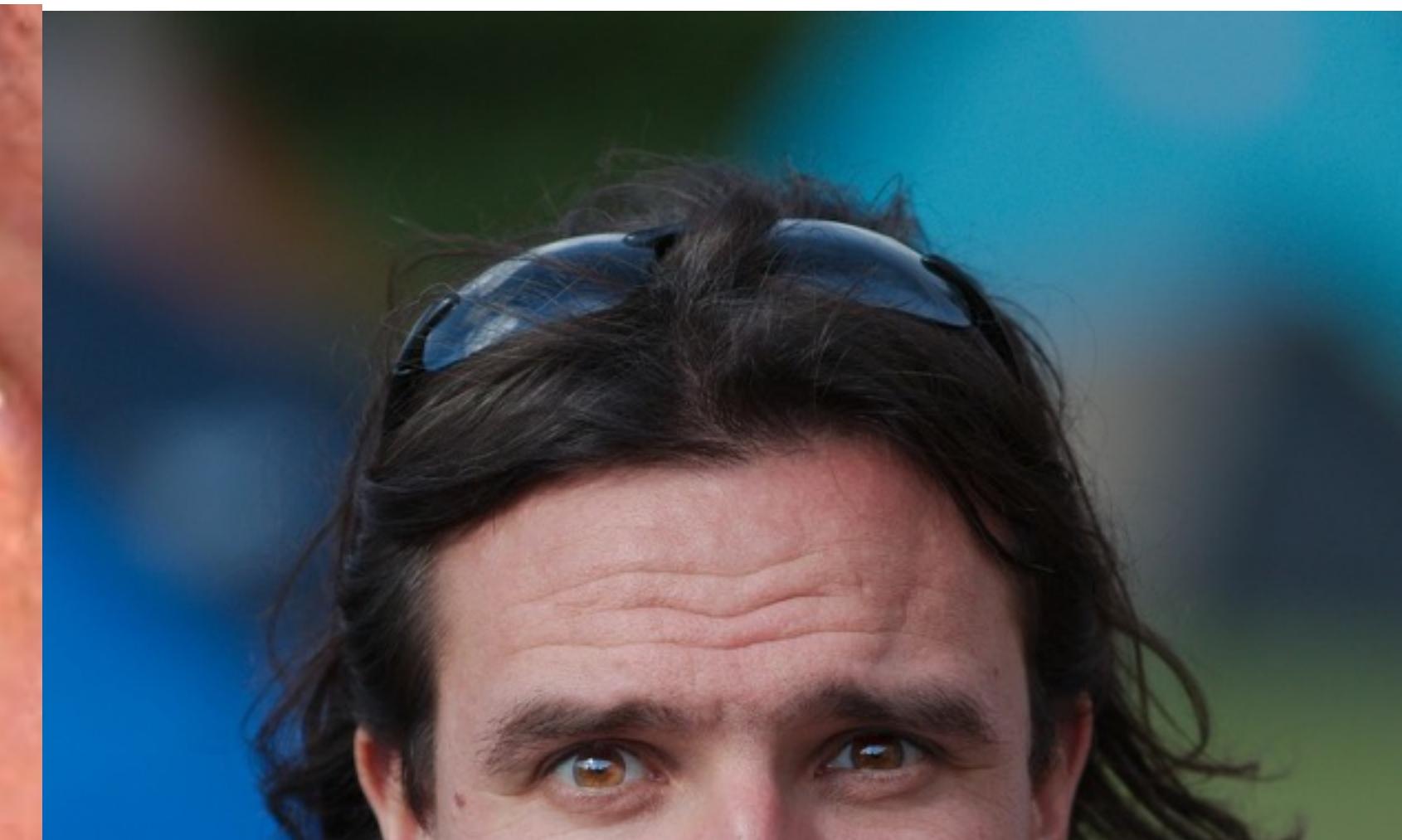
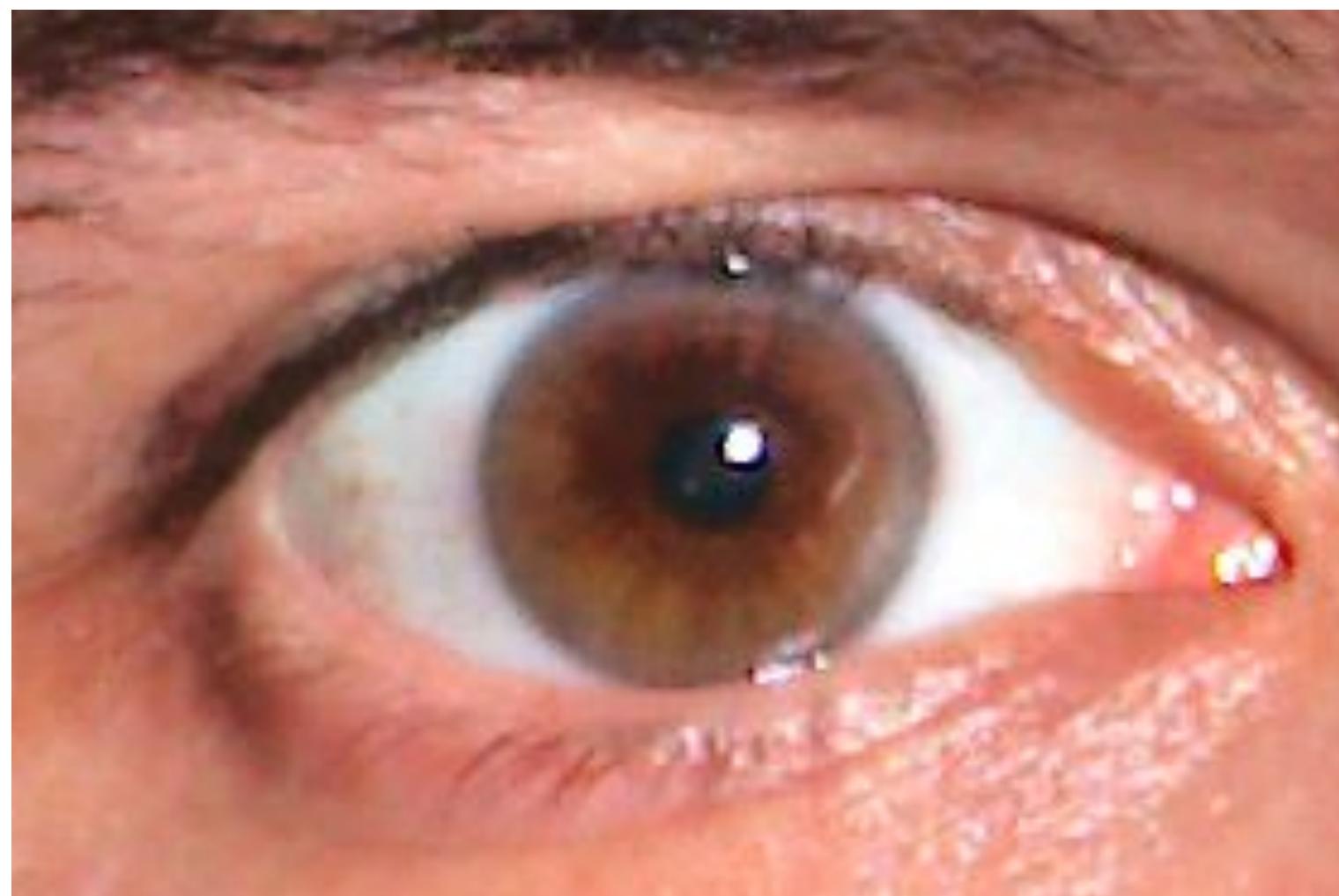


[Cao et al. 14] [Thies et al. 15] Ours
(RGB only) (RGB-D) (RGB only)

die dritte Dimension



schau mir in die Augen



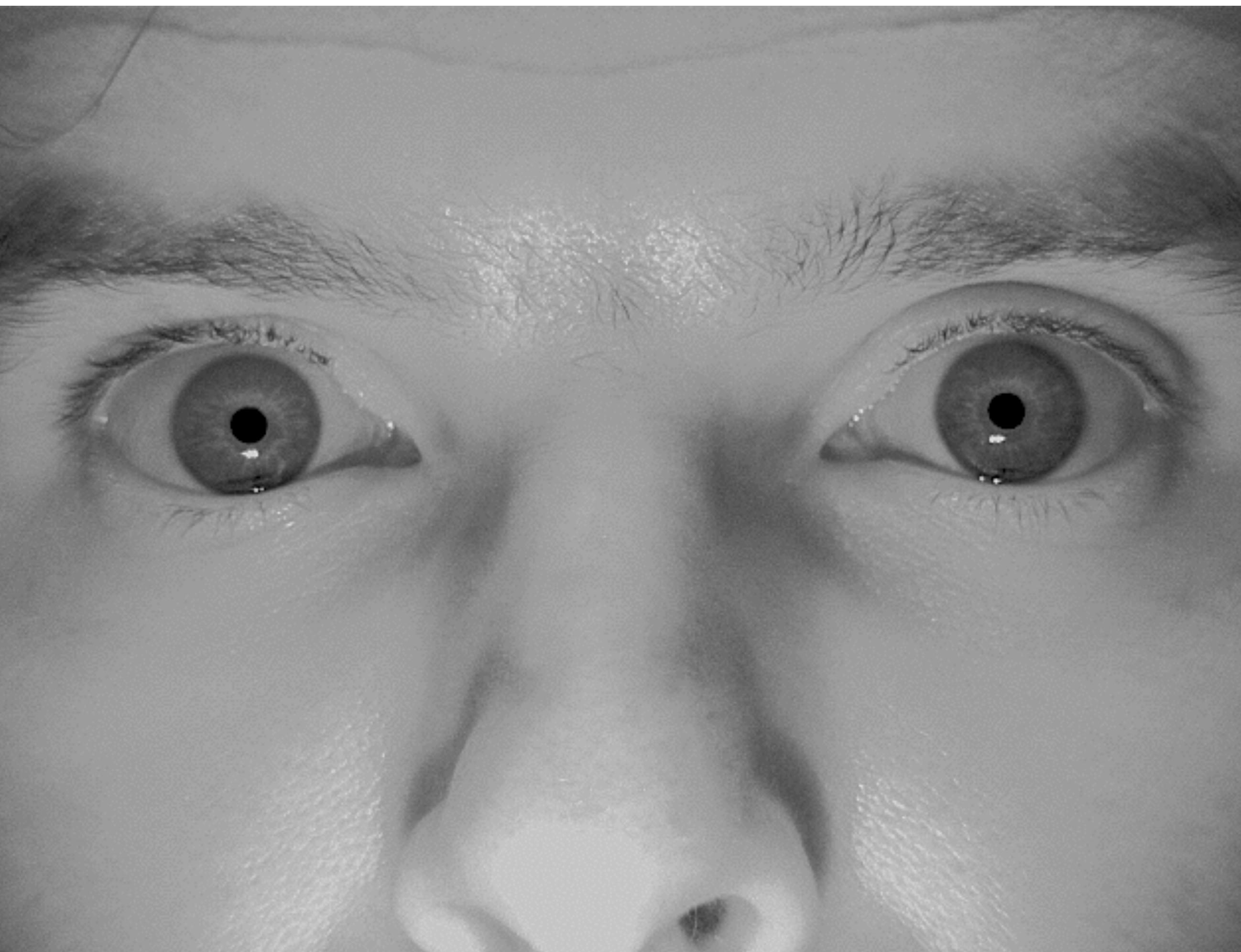
sooooo einfach



schau mir in die Augen



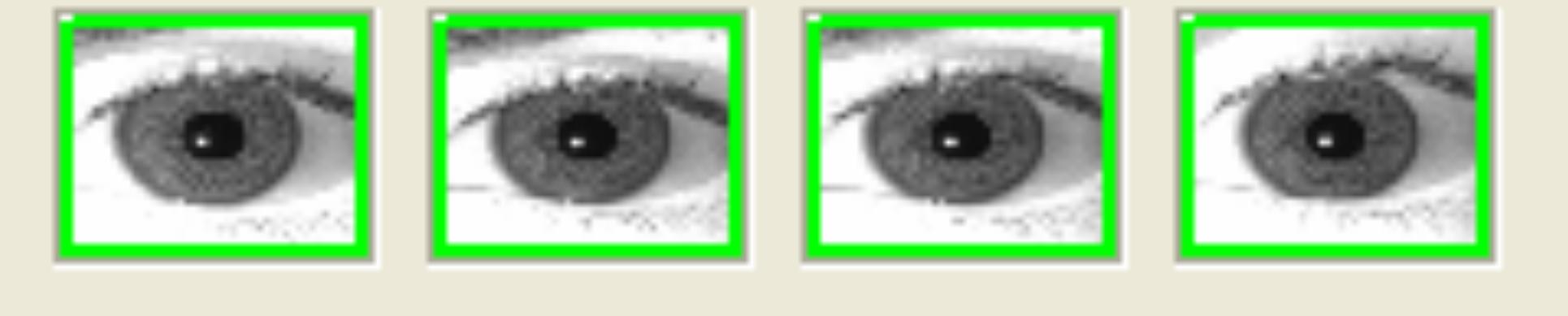
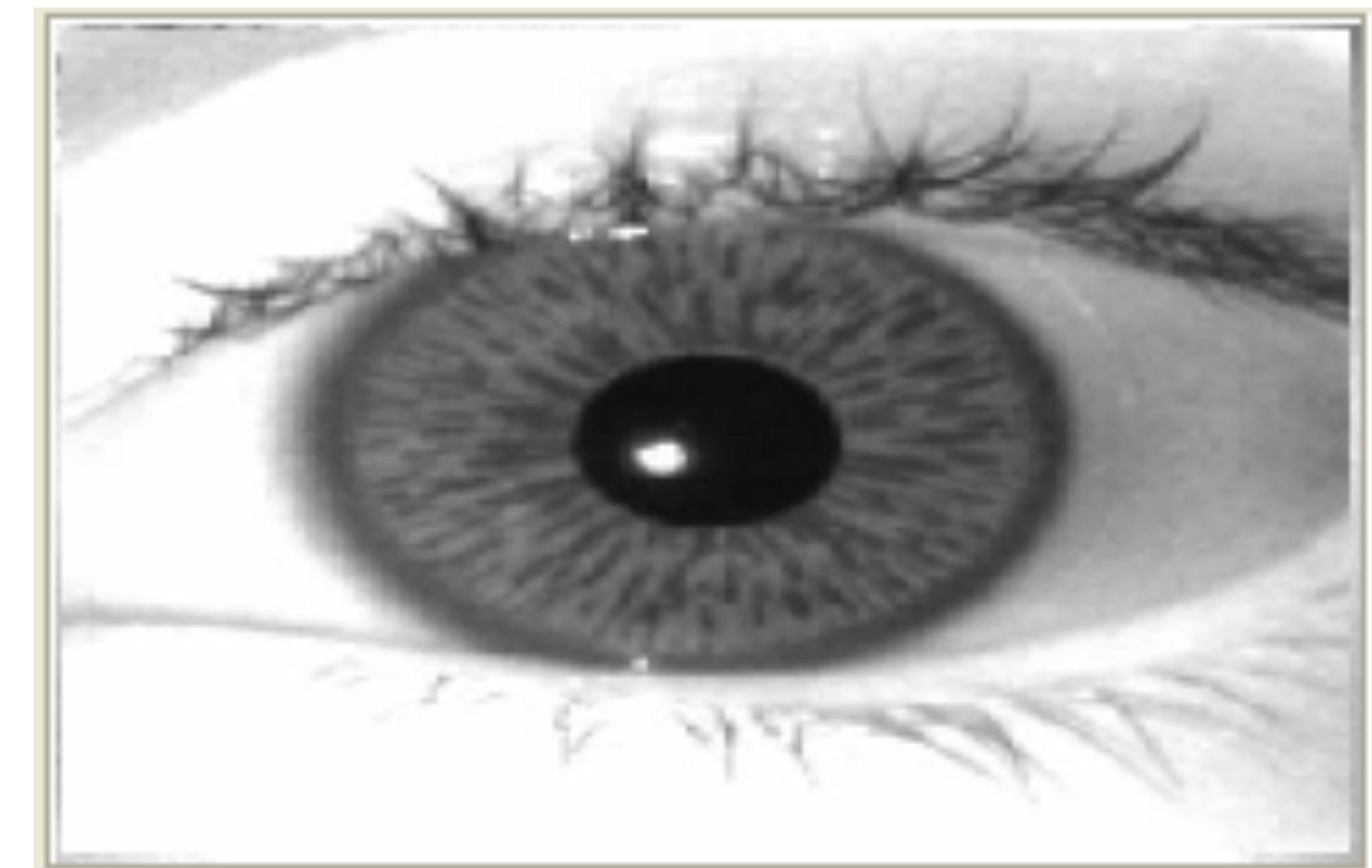
... und ich sage dir, wer du bist



distance [m]	diameter [pxl]
3	153
4	131
5	100
6	80
7	67



unsichtbare Identität



AI(b|p)träume?

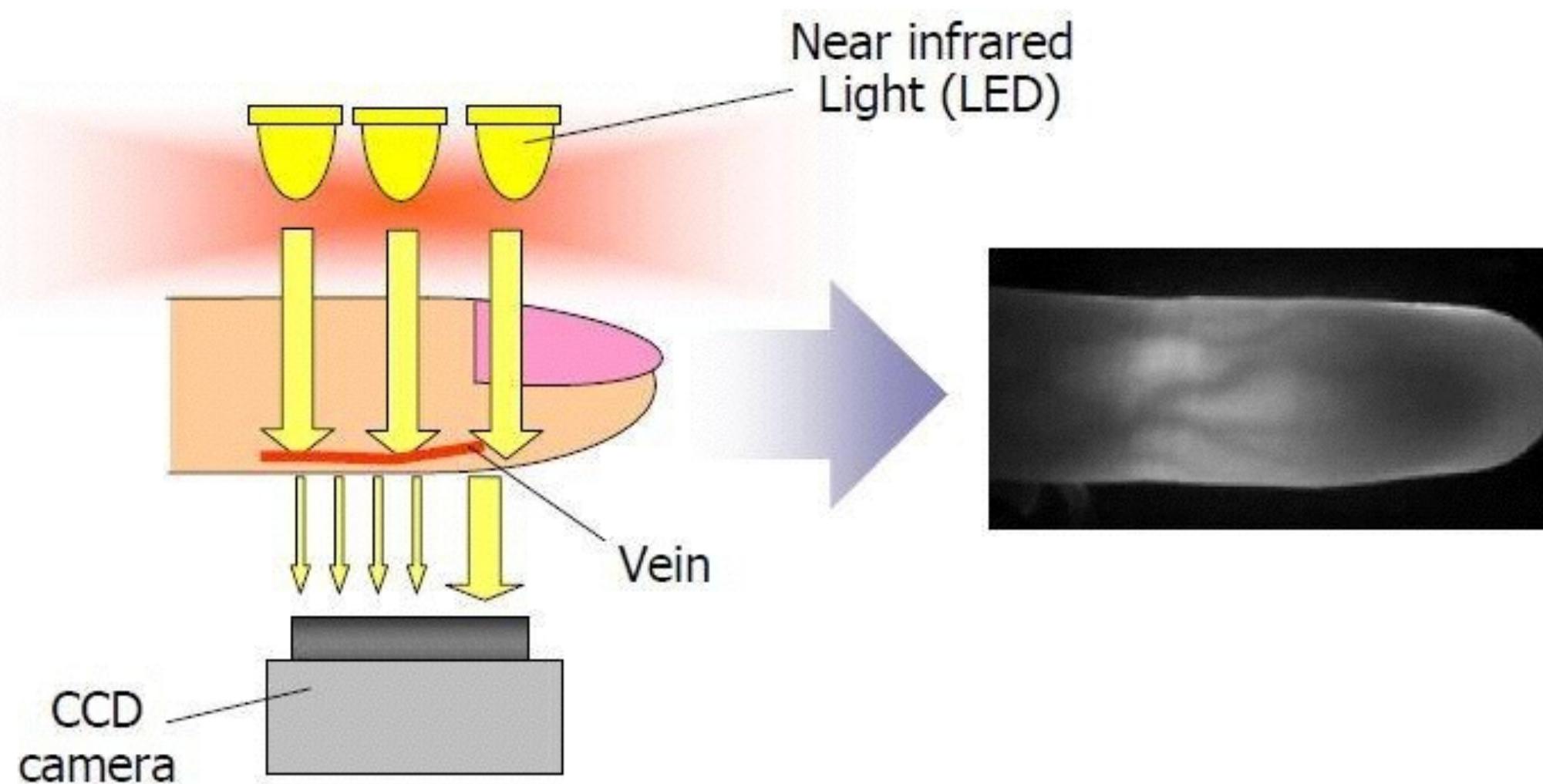


die Partei liefert

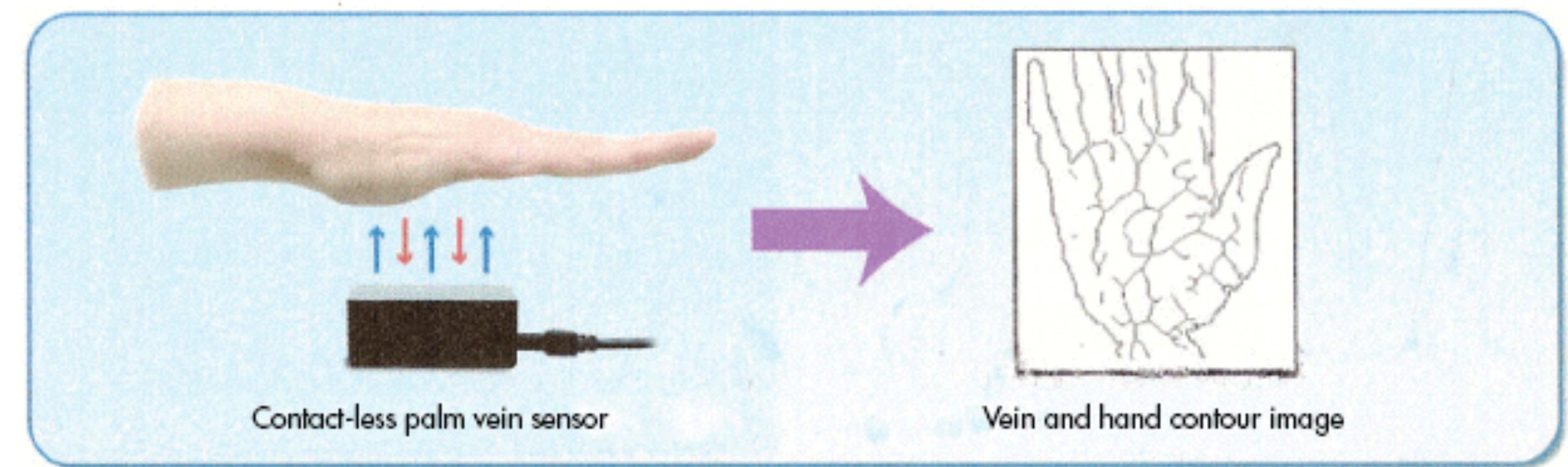




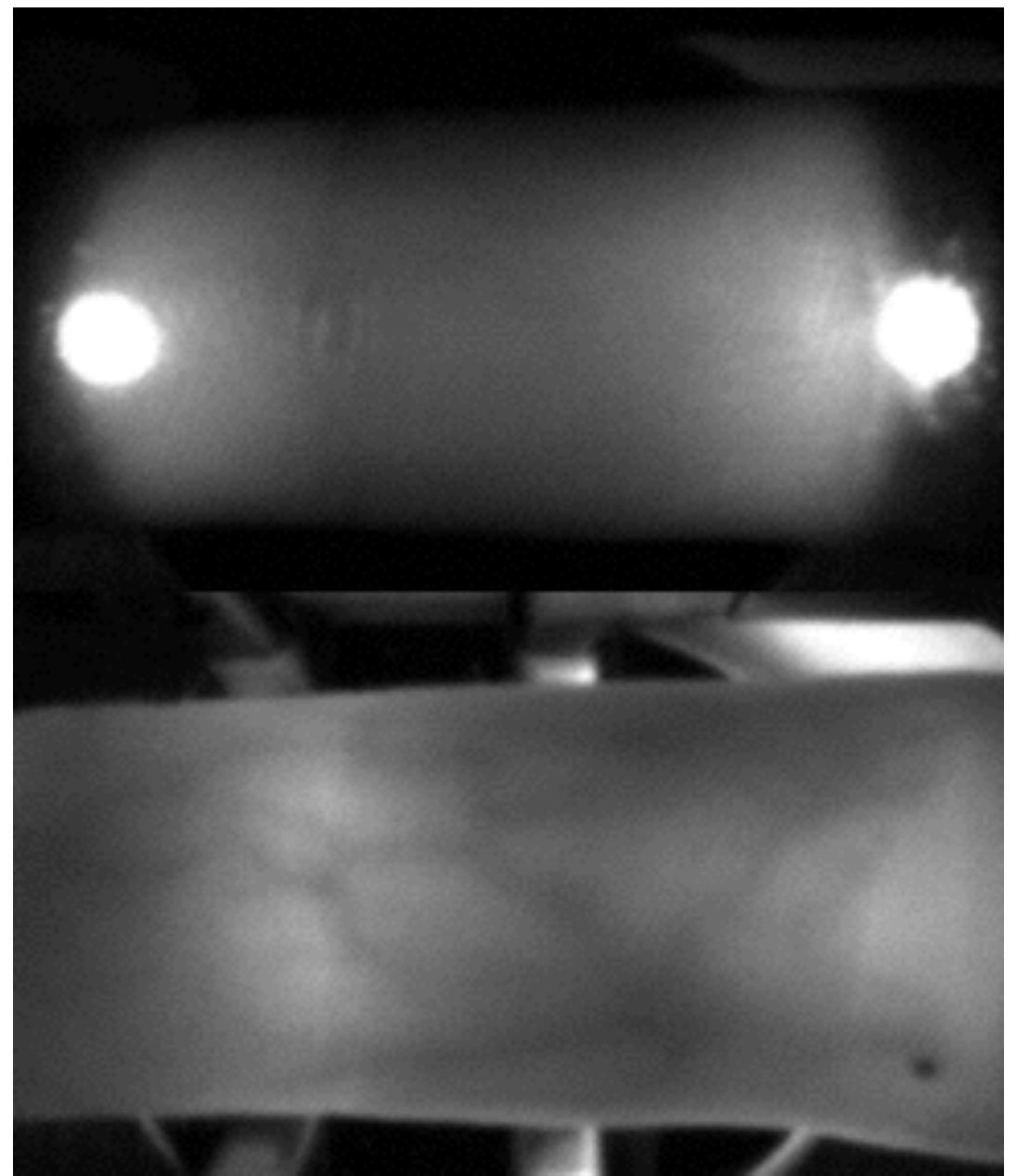
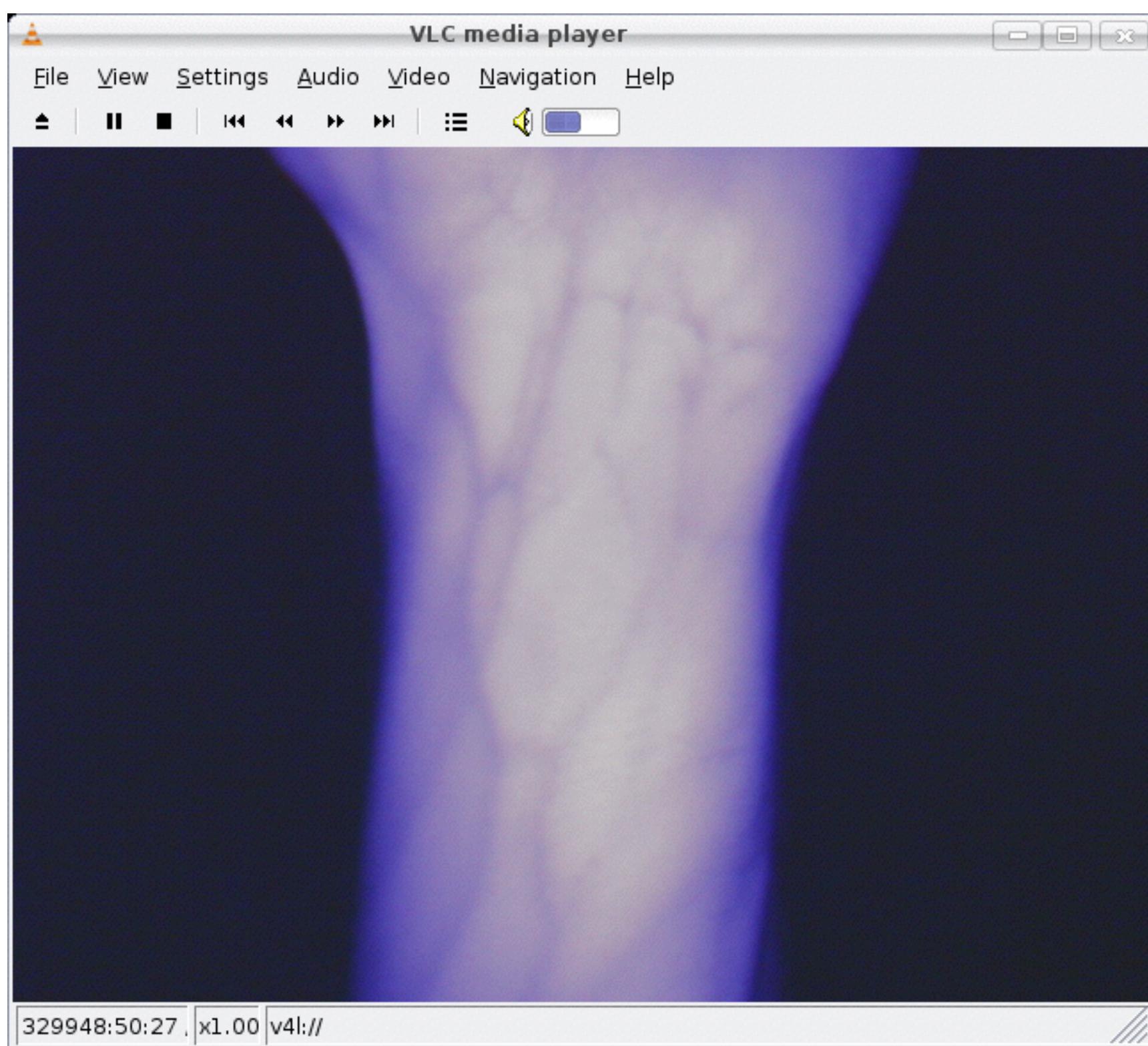
Venenerkennung



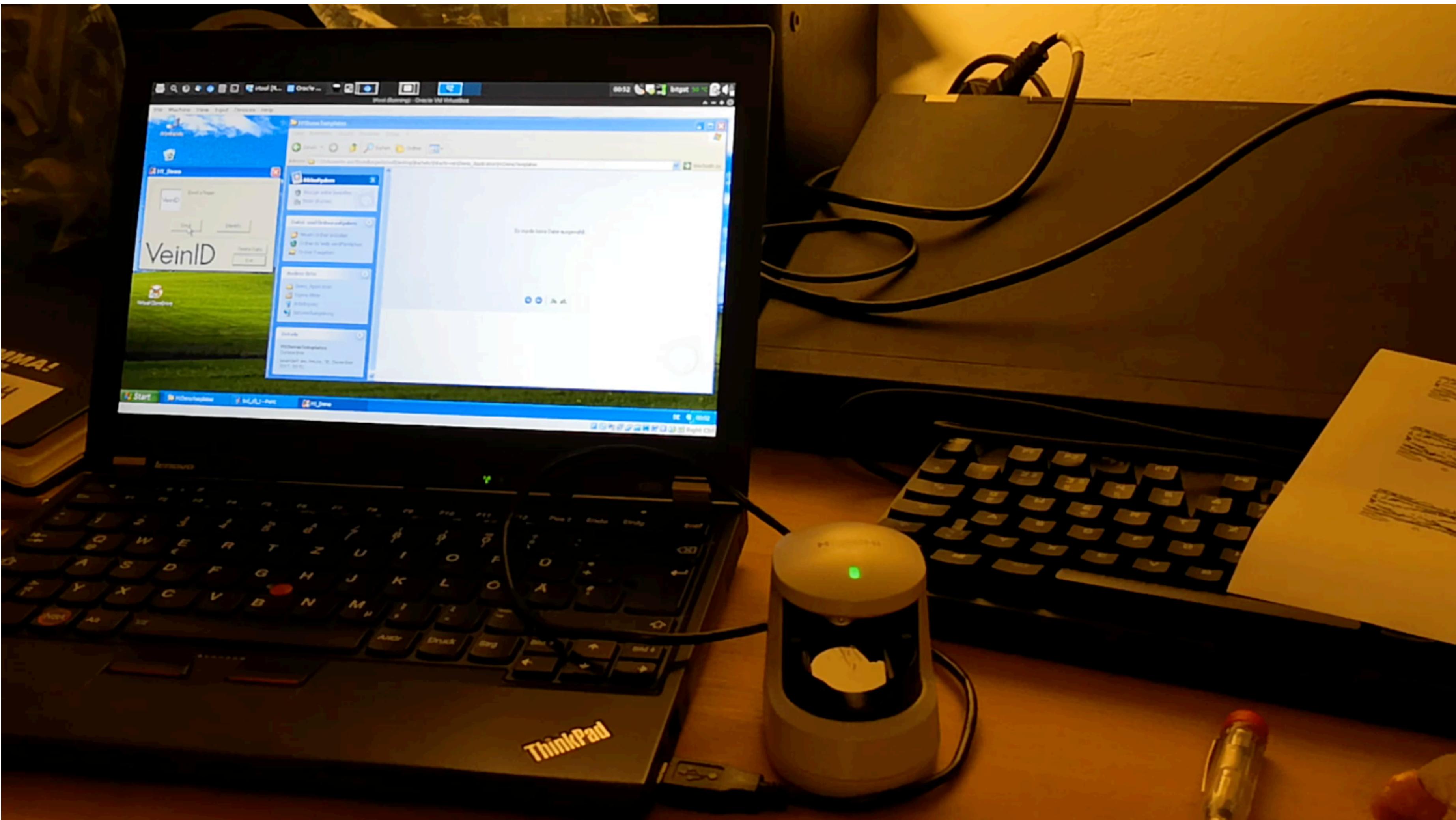
6. In Fujitsu's Palm Secure technology for biometrics, contact-less palm-vein sensing can be used to project a vein and hand contour image.



Junkie?



finally



conclusion

Passwort:

- neben der Länge zählt auch die Eingabeumgebung

Token:

- RFID ist convienient, birgt aber Risiken
- proprietäre Kryptoalgorithmen sind böse

Biometrie:

- man hinterlässt Spuren von fast allen biom. Merkmalen
- Lebenderkennung prüft nicht unbedingt Leben

vielen Dank



Fragen?

starbug@ccc.de