FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

# Forensik sozialer Medien und Netzwerke

Yves Nießen
Lehrgebiet Datennetze

IT Forensik
FH Aachen

# Struktur



- Problemstellung
- Vorgehensweise
- Erste Ergebnisse

# Problemstellung

- WARUM soziale Netzwerke und Medien?
  - Werden immer beliebter
  - Viele persönliche Informationen
  - Oft für jeden zugänglich
- WELCHE Informationen sind Interessant?
  - Bilder (eigene, angesehene)
  - Postings (eigene, angesehene)
  - Beziehungen (eigene)
  - Standorte (eigene)
- WO könnte man diese Informationen finden?
  - Rechner des Verdächtigen (RAM, Chronik, Cookies, ...)
  - Öffentliches Profil

# Vorgehensweise



- Testdaten erzeugen (innerhalb einer VM)
  - Bei sozialen Netzwerken registrieren
    - Momentan Facebook & Twitter
  - Bilder von anderen Usern anschauen
  - Postings erstellen
  - An Aufenthaltsorten „einchecken“ (Facebook)
- Analyse der Daten
  - Öffentliches Profil
    - Welche Informationen sind sichtbar*
  - Rechner des Verdächtigen (VM)
    - Nicht flüchtige Daten: Cookies, Chronik,…
    - Flüchtige Daten: RAM

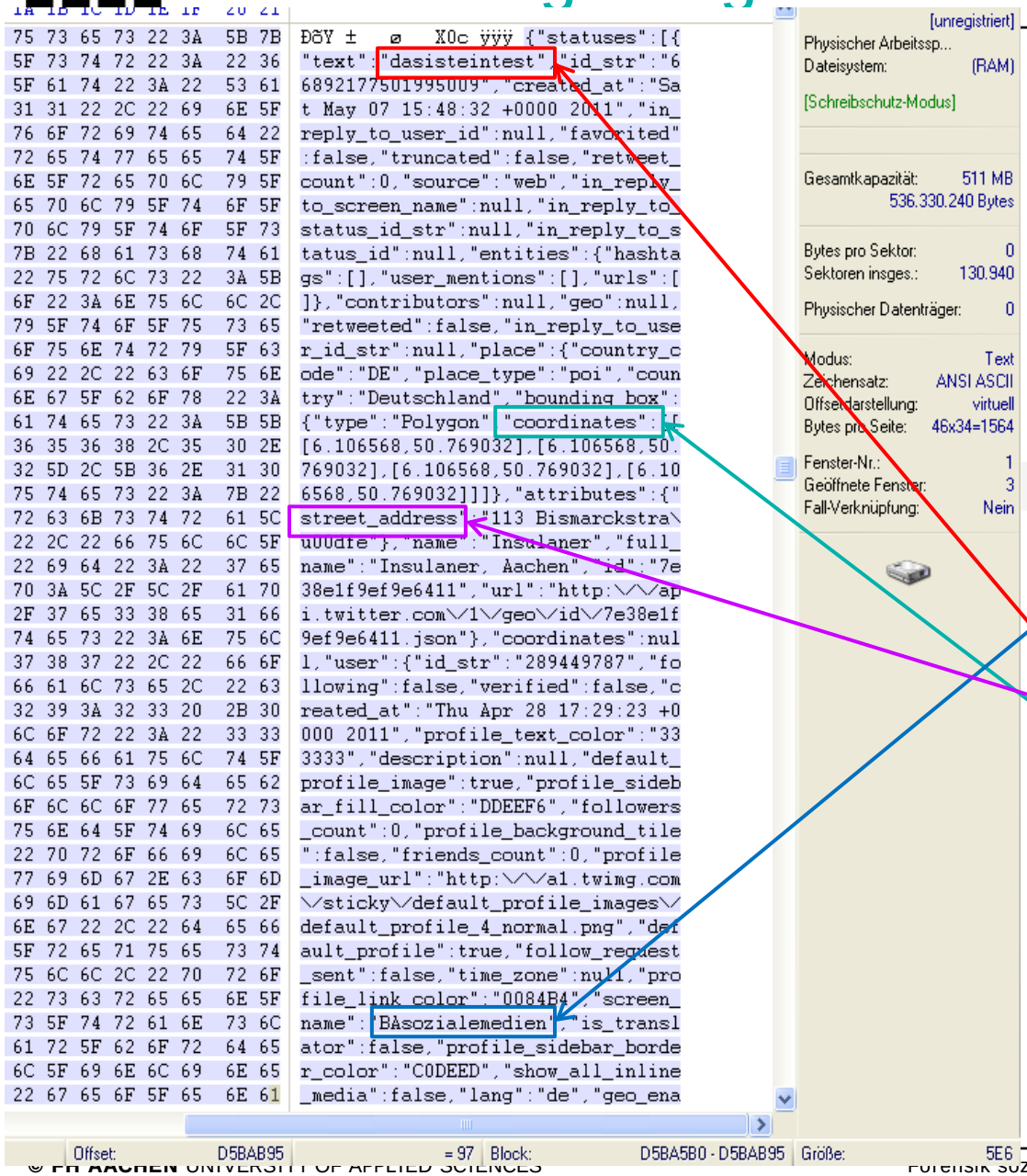
* Standard Privatsphären Einstellungen

# Bisherige Ergebnisse



- Beispiel Twitter Post
  - generell alles öffentlich zugänglich
  - Im RAM alle Informationen auffindbar
  - Ebenfalls in der Chronik des Browsers
  - Probleme bei Zuordnung des Users am Rechner

# Bisherige Ergebnisse




# Bisherige Ergebnisse

- Zuletzt eingegebene URLs
- Zuletzt besuchte Seiten (Verlauf)
- Zuletzt besuchte Seiten (laut Schnittstelle)
- Zuletzt besuchte Seiten (laut Rohdaten)
- Geladene Dateien (laut Schnittstelle)
- Geladene Dateien (laut Rohdaten)
- Geladene Dateien (für die InPrivate-Filterun
- Angenommene Cookies (laut Schnittstelle)
- Angenommene Cookies (laut Rohdaten)

http://ts1.mm.bing.net/videos/thumbnail.aspx?q=891028178340&id=409ba7f714943ab678cb4ffb6d0886db&bid=hb9%2blpoUanPSow&bn=Thumb
http://ts1.mm.bing.net/videos/thumbnail.aspx?q=896980354028&id=c8551ffdc4ee9d82d5278b720464fa5f&bid=dDLJervurgDgVg&bn=Thumb&url=
http://ts1.mm.bing.net/videos/thumbnail.aspx?q=924555280500&id=11946eae99197ee0dfa9a14f856c419f&bid=%2bny0CNeoy9AHEA&bn=Thumb
http://ts1.mm.bing.net/videos/thumbnail.aspx?q=950643327276&id=3db156eca723ee53db52197608f2a868&bid=evPG1LP8EyUm2Q&bn=Thumb
http://twitter.com/
http://twitter.com/
http://twitter.com/
http://twitter.com/
http://twitter.com/
http://twitter.com/
http://twitter.com/
http://twitter.com/
http://twitter.com/#!/BAsozialemedien
http://twitter.com/account/available_features
http://twitter.com/account/available_features
http://twitter.com/account/available_features
http://twitter.com/account/bootstrap_data?r=0.051653735600455664
http://twitter.com/account/bootstrap_data?r=0.1449984365978515
http://twitter.com/account/bootstrap_data?r=0.26071147647282705
http://twitter.com/account/bootstrap_data?r=0.2963492735553036
http://twitter.com/account/bootstrap_data?r=0.3439265554728943
http://twitter.com/account/bootstrap_data?r=0.39935102552303014
http://twitter.com/account/bootstrap_data?r=0.4306695840161516
http://twitter.com/account/bootstrap_data?r=0.43818840190651875
http://twitter.com/account/bootstrap_data?r=0.8059243702870811
http://twitter.com/account/bootstrap_data?r=0.9660072866724807
http://twitter.com/account/password_reset_sent
http://twitter.com/account/resend_password
http://twitter.com/account/resend_password06995a65
http://twitter.com/accouURL
http://twitter.com/BAsozialemedien
http://twitter.com/find_sources/contacts/services.json
http://twitter.com/images/reset_pw/bird_key.png
http://twitter.com/images/reset_pw/confirm.png
http://twitter.com/images/spinner.gif
http://twitter.com/images/spinner.gif
http://twitter.com/images/tiny-map.gif
http://twitter.com/login
http://twitter.com/messages
http://twitter.com/messages
http://twitter.com/messages
http://twitter.com/messages
http://twitter.com/phoenix/favicon.ico
http://twitter.com/phoenix/img/loader.gif
http://twitter.com/phoenix/img/poi-pin.png
http://twitter.com/phoenix/img/tiny-timeline-bird.png
http://twitter.com/phoenix_search.phoenix?q=6689131112654848O&include_entities=1&include_available_features=1&contributor_details=true
http://twitter.com/phoenix_search.phoenix?q=basoziale&include_entities=1&include_available_features=1&contributor_details=true
http://twitter.com/phoenix_search.phoenix?q=basozialemedien&include_entities=1&include_available_features=1&contributor_details=true
http://twitter.com/phoenix_search.phoenix?q=BASozialemedien&include_entities=1&include_available_features=1&contributor_details=true
http://twitter.com/phoenix_search.phoenix?q=sozialemedien&include_entities=1&include_available_features=1&contributor_details=true
http://twitter.com/promos/random_json_promo.json?promo_type=&limit=1
http://twitter.com/promos/random_json_promo.json?promo_type=related_service&limit=2
http://twitter.com/promos/random_json_promo?promo_type=&limit=1
http://twitter.com/search?q=_mad
http://twitter.com/search?q=_mad
http://twitter.com/users/show_for_profile.json?screen_name=BAsozialemedien

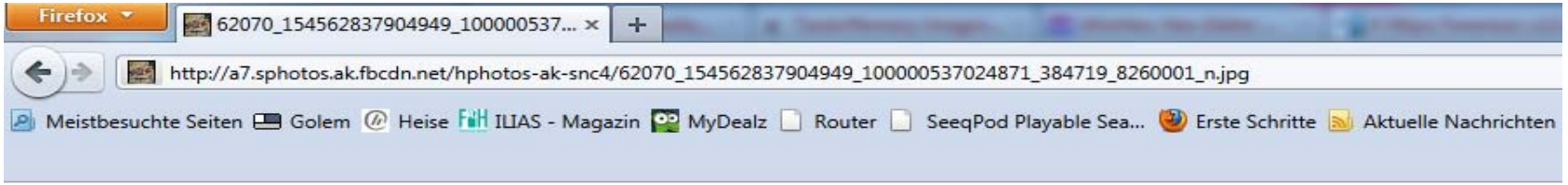
# Bisherige Ergebnisse



- Beispiel Facebook
  - Private Bilder anderer User für jeden zugänglich
    - Voraussetzung: User an PC ist befreundet und hat Fotos angeschaut
  - Cookie -> UserID -> Fotos des Users
  - UserID lässt sich durch http://graph.facebook.com/UserID jedem User zuordnen


  - Postings und Kommentare im RAM

# Bisheriger Ergebnisse




# Bisherige Ergebnisse


```
) 65 73 73   61 67 65   pc_fbx=&xhpc_timeline=&xhpc_message
3 73 61 67   65 3D 6B   _text=kartoffelsalat&xhpc_message=k
4 5B 30 5D   3D 38 30   artoffelsalat&UIPrivacyWidget[0]=80
. 63 79 5F   64 61 74   &privacy_data[value]=80&privacy_dat
3 74 5F 61   6E 6F 6E   a[friends]=0&privacy_data[list_anon
) 3D 30 26   6E 63 74   ]=0&privacy_data[list_x_anon]=0&nct
5 70 6F 73   74 5F 66   r[_mod]=pagelet_composer&lsd&post_f
4 6E 2E 6E   65 74 25   orm_id_source=AsyncRequestbcdn.net%
5 39 71 63   5F 41 74   2Frsrc.php%2Fv1%2Fy2%2Fr%2F_u9qc_At
: 61 6B 2E   66 62 63   DSM.js&r=http%3A%2F%2Fstatic.ak.fbc
2 46 72 25   32 46 54   dn.net%2Frsrc.php%2Fv1%2FyI%2Fr%2FT
: 67 3A 20   67 7A 69   F8WVXsmqcX.js  Accept-Encoding: gzi
: 6C 61 2F   34 2E 30   p, deflate  User-Agent: Mozilla/4.0
' 77 73 20   4E 54 20    (compatible; MSIE 8.0; Windows NT
. 2E 63 68   61 6E 6E   5.1; Trident/4.0)  Host: 0.21.chann
) 4B 65 65   70 2D 41   el.facebook.com  Connection: Keep-A
) 68 74 74   70 25 33   live  Cookie: L=2; x-referer=http%3
5 72 65 66   25 33 44   A%2F%2Fwww.facebook.com%2F%3Fref%3D
) 31 33 30   34 37 38   home%23%2F%3Fref%3Dhome; act=130478
) 38 35 38   38 34 31   2843051%2F2; c_user=100002340858841
3 34 36 63   61 30 39   ; sct=1304693488; xs=62%3A92c46ca09
```

```
U5 72 9B   U6 CA F1   ÷]'U¦ıı'>Y¾>÷{ıbääëC·ü±{B¾ r Eñ
1A A2 CF   7E 8C B3   ´q !÷T²!PkÛ×N³cß6mÜ6PPDÑÑg T ¢Ï~³
DB D7 ED   1B A7 63    % b ¼Ã Ã #}^d  Î ï{(?ª_êNÍfÛ×í $c
51 46 39   BC 9E D0   ·&K K1 ä|6Ð Ë -£ Dî·  W  ´ QF9¼ Ð
89 10 C0   B1 52 B9   ø2¬çGË ´WÓ HI2d  © ¿  ¤åb <  À±R¹
DA CD F6   CD AD 7F   ëY  N FL¼6i F  åYq]nàuCfaÜ³ÚÍöÍ-
11 92 68   5E 43 AA   ¡ w$íoÍ4_ ý d t P:æz$* ¨!m r ´h^Cª
9D 0F 1A   1F 36 AD    )õ pe ú:À I kÏÍ|È&8GnV0¦9R   6-
2D E1 FC   34 7F 79   =\ Î Þ¡^B +  ` ·!ãd£q14^  ëy7 -áü4 y
EF 79 05   A6 54 58   Ká\ î :è ø ´¼ ±ü V9ÕÎúGTã  äïy ¦TX
26 70 81   62 35 D3   %áE`  `f ç µkzÖ±çYÅ³¾ÞQ<²×w   &p b5Ó
87 8B 74   3E ED D7   ß þ ß)ùïÓë4xab ôj þÊë{8X  3ú0  t>íx
93 46 67   B0 0C C3    U ÿï .ù  íâq¾MYCÕüÕvÞÃAX* ÞÖ Fg° Ã
30 39 31   38 34 37   Y©p>     ÿÿ       0871,"oid":"1091847
35 38 38   34 31 22   49169553","owner":"100002340858841"
5F 69 64   22 3A 22   ,"text":"Nudelsalat?","object_id":"
73 22 3A   30 7D 2C   ","story_type":22,"num_credits":0},
6D 49 64   22 3A 6E   "userId":100002340858841,"fromId":n
3D 5C 22   62 6C 75   ull,"title":"\u003cspan class=\"blu
70 61 6E   3E 20 68   eName\">Yves Niessen\u003c\/span> h
22 2C 22   62 6F 64   at deinen Status kommentiert.","bod
63 65 62   6F 6F 6B   y":"","link":"http:\/\/www.facebook
64 3D 31   30 39 31   .com\/permalink.php?story_fbid=1091
31 22 2C   22 75 73   84749169553&id=100002340858841","us
00 00 00   00 00 00       %253
```

# Zusammenfassung

- Twitter
  - Postings
  - Angeschaute User
  - Koordinaten (Adressen)
  - Timestamps
  - Verbindungen
- Facebook
  - Postings
  - Angeschaute User / Fotos
  - Koordinaten
  - Timestamps
  - Verbindungen
  - Kommentare
  - UserID
  - Profilfoto

# Vielen Dank für Ihre Aufmerksamkeit!

Fragen oder Anregungen?