

Forensik sozialer Medien und Netzwerke

Yves Nießen

Lehrgebiet Datennetze



- Problemstellung
- Vorgehensweise
- Erste Ergebnisse

- **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

- 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

- 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

1A	1B	1C	1D	1E	1F	20	21
75	73	65	73	22	3A	5B	7B
5F	73	74	72	22	3A	22	36
5F	61	74	22	3A	22	53	61
31	31	22	2C	22	69	6E	5F
76	6F	72	69	74	65	64	22
72	65	74	77	65	65	74	5F
6E	5F	72	65	70	6C	79	5F
65	70	6C	79	5F	74	6F	5F
70	6C	79	5F	74	6F	5F	73
7B	22	68	61	73	68	74	61
22	75	72	6C	73	22	3A	5B
6F	22	3A	6E	75	6C	6C	2C
79	5F	74	6F	5F	75	73	65
6F	75	6E	74	72	79	5F	63
69	22	2C	22	63	6F	75	6E
6E	67	5F	62	6F	78	22	3A
61	74	65	73	22	3A	5B	5B
36	35	36	38	2C	35	30	2E
32	5D	2C	5B	36	2E	31	30
75	74	65	73	22	3A	7B	22
72	63	6B	73	74	72	61	5C
22	2C	22	66	75	6C	6C	5F
22	69	64	22	3A	22	37	65
70	3A	5C	2F	5C	2F	61	70
2F	37	65	33	38	65	31	66
74	65	73	22	3A	6E	75	6C
37	38	37	22	2C	22	66	6F
66	61	6C	73	65	2C	22	63
32	39	3A	32	33	20	2B	30
6C	6F	72	22	3A	22	33	33
64	65	66	61	75	6C	74	5F
6C	65	5F	73	69	64	65	62
6F	6C	6C	6F	77	65	72	73
75	6E	64	5F	74	69	6C	65
22	70	72	6F	66	69	6C	65
77	69	6D	67	2E	63	6F	6D
69	6D	61	67	65	73	5C	2F
6E	67	22	2C	22	64	65	66
5F	72	65	71	75	65	73	74
75	6C	6C	2C	22	70	72	6F
22	73	63	72	65	65	6E	5F
73	5F	74	72	61	6E	73	6C
61	72	5F	62	6F	72	64	65
6C	5F	69	6E	6C	69	6E	65
22	67	65	6F	5F	65	6E	61

```
[unregistriert]
Physischer Arbeitssp...
Dateisystem: (RAM)
[Schreibschutz-Modus]

Gesamtkapazität: 511 MB
536.330.240 Bytes

Bytes pro Sektor: 0
Sektoren insges.: 130.940

Physischer Datenträger: 0

Modus: Text
Zeichensatz: ANSI ASCII
Offsetdarstellung: virtuell
Bytes pro Seite: 46x34=1564

Fenster-Nr.: 1
Geöffnete Fenster: 3
Fall-Verknüpfung: Nein
```

```
{
  "text": "dasisteintest",
  "id_str": "66892177501995009",
  "created_at": "Sat May 07 15:48:32 +0000 2011",
  "in_reply_to_user_id": null,
  "favorited": false,
  "truncated": false,
  "retweet_count": 0,
  "source": "web",
  "in_reply_to_screen_name": null,
  "in_reply_to_status_id_str": null,
  "in_reply_to_status_id": null,
  "entities": {
    "hashtags": [],
    "user_mentions": [],
    "urls": [],
    "contributors": null,
    "geo": null,
    "retweeted": false,
    "in_reply_to_user_id_str": null,
    "place": {
      "country_code": "DE",
      "place_type": "poi",
      "country": "Deutschland",
      "bounding_box": {
        "type": "Polygon",
        "coordinates": [[
          [6.106568, 50.769032],
          [6.106568, 50.769032],
          [6.106568, 50.769032],
          [6.106568, 50.769032]
        ]
      ],
      "attributes": {
        "street_address": "113 Bismarckstra\u00dfe",
        "name": "Insulaner",
        "full_name": "Insulaner, Aachen",
        "id": "7e38e1f9ef9e6411",
        "url": "http://api.twitter.com/1/geo/id/7e38e1f9ef9e6411.json",
        "coordinates": null,
        "user": {
          "id_str": "289449787",
          "following": false,
          "verified": false,
          "created_at": "Thu Apr 28 17:29:23 +0000 2011",
          "profile_text_color": "333333",
          "description": null,
          "default_profile_image": true,
          "profile_sidebar_fill_color": "DDEEF6",
          "followers_count": 0,
          "profile_background_tile": false,
          "friends_count": 0,
          "profile_image_url": "http://a1.twimg.com/sticky/default_profile_images/default_profile_4_normal.png",
          "default_profile": true,
          "follow_request_sent": false,
          "time_zone": null,
          "profile_link_color": "0084B4",
          "screen_name": "BAsozialemedien",
          "is_translator": false,
          "profile_sidebar_border_color": "CODEED",
          "show_all_inline_media": false,
          "lang": "de",
          "geo_ena"
        }
      }
    }
  }
}
```

@BAsozialemedien
Bachelorarbeit Sozia

dasisteintest



von Insulaner
113 Bismarckstraße
Aachen, Aachen
+(49)-(241)-501416
Siehe Tweets zu diesem Ort

- 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-Filterung)
- Angenommene Cookies (laut Schnittstelle)
- Angenommene Cookies (laut Rohdaten)

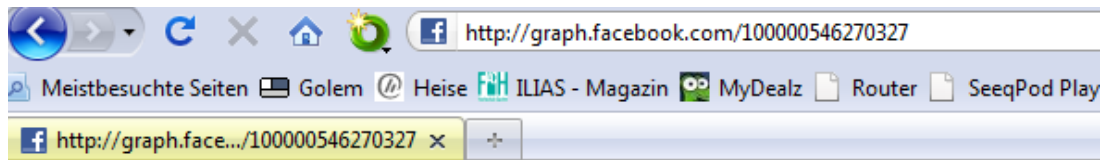
```

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=c8551fddc4ee9d82d5278b720464fa5f&bid=dDLJervurgDgVg&bn=Thumb&url=
http://ts1.mm.bing.net/videos/thumbnail.aspx?q=924555280500&id=11946eae99197ee0dfa9a14f856c419f&bid=%2bny0CNegY9AHEA&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/
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=66891311126548480&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

```

■ Beispiel Facebook

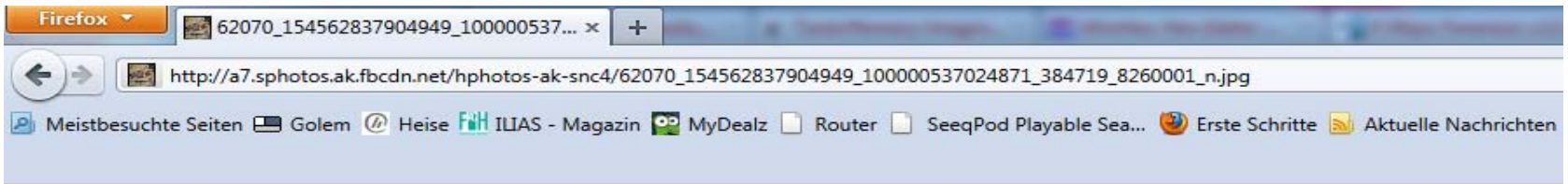
- Private Bilder anderer User für jeden zugänglich
 - Voraussetzung: User an PC ist befreundet und hat Fotos angeschaut
- Cookie -> UserID -> Fotos des Users
- UserID lässt sich durch <http://graph.facebook.com/UserID> jedem User zuordnen



```
{
  "id": "100000546270327",
  "name": "Yves Niessen",
  "first_name": "Yves",
  "last_name": "Niessen",
  "link": "http://www.facebook.com/people/Yves-Niessen/100000546270327",
  "gender": "male",
  "locale": "en_US"
}
```

- Postings und Kommentare im RAM

Bisheriger Ergebnisse



TESTBI Bachelorarbeit Soziale Medien



kartoffelsalat

vor 9 Minuten · Gefällt mir · Kommentieren



Yves Niessen Nudelsalat?

vor einigen Sekunden · Gefällt mir

Schreibe einen Kommentar ...

```

0 65 73 73 61 67 65 pc fbx=&xhpc timeline=&xhpc_message
1 73 61 67 65 3D 6B _text=kartoffelsalat&xhpc_message=k
2 5B 30 5D 3D 38 30 artoffelsalat&UIPrivacyWidget[0]=80
3 63 79 5F 64 61 74 &privacy_data[value]=80&privacy_dat
4 74 5F 61 6E 6F 6E a[friends]=0&privacy_data[list_anon
5 3D 30 26 6E 63 74 ]=0&privacy_data[list_x_anon]=0&nct
6 70 6F 73 74 5F 66 r[_mod]=pagelet_composer&lsd&post_f
7 6E 2E 6E 65 74 25 orm_id_source=AsyncRequestbcdn.net%
8 39 71 63 5F 41 74 2Frsrc.php%2Fv1%2Fy2%2Fr%2F_u9qc_At
9 61 6B 2E 66 62 63 DSM.js&r=http%3A%2F%2Fstatic.ak.fb
0 46 72 25 32 46 54 dn.net%2Frsrc.php%2Fv1%2FyI%2Fr%2FT
1 67 3A 20 67 7A 69 F8WVXsmqcX.js Accept-Encoding: gzi
2 6C 61 2F 34 2E 30 p, deflate User-Agent: Mozilla/4.0
3 77 73 20 4E 54 20 (compatible; MSIE 8.0; Windows NT
4 2E 63 68 61 6E 6E 5.1; Trident/4.0) Host: 0.21.chann
5 4B 65 65 70 2D 41 el.facebook.com Connection: Keep-A
6 68 74 74 70 25 33 live Cookie: L=2; x-referer=http%3
7 72 65 66 25 33 44 A%2F%2Fwww.facebook.com%2F%3Fref%3D
8 31 33 30 34 37 38 home%23%2F%3Fref%3Dhome; act=130478
9 38 35 38 38 34 31 2843051%2F2; c_user=100002340858841
0 34 36 63 61 30 39 ; sct=1304693488; xs=62%3A92c46ca09
1 05 72 9B 06 CA F1 +J'U0|ii|>Y%>+{|15aaæC·üt{B%| r| Eñ
2 1A A2 CF 7E 8C B3 'q !÷|T²|PkÜ×N³cB6mÜ6PPDÑÑg|T cİ~|³
3 DB D7 ED 1B A7 63 | % b %Å Å #)^d İii{?ª_ēNifÜxi Sc
4 51 46 39 BC 9E D0 ·||&K|K1|ä|6D È|-ē|Dí·|W '|QF9%|D
5 89 10 C0 B1 52 B9 ø2~çGÈ 'WÓ|HI2d | @|ì| Máb <| À±R¹
6 DA CD F6 CD AD 7F èY|| N FL%6i F|| áVq|nàuCfaÜ³Úíöf-|
7 11 92 68 5E 43 AA i w$ioÍ4_ ý|d |t P:æz$* '|m|r 'h^Cª
8 9D 0F 1A 1F 36 AD )|ð pe ú:À ||k|I|È&8GnV0|9R| 6-
9 2D E1 FC 34 7F 79 =|\ Î|Pi^B|+ `·!ãdîql4^ èy7|-áü4|y
0 EF 79 05 A6 54 58 Ká\ i||:è ø '¼|tü|V9Ö|úGTä|||äiy |TX
1 26 70 81 62 35 D3 %áE` `f ç|pkzÖtçYÁ³%PQ<²xw| &p|b5Ó
2 87 8B 74 3E ED D7 B b|B)ù|Öè4xab|òj|bÈè{8X| 3ú0 ||t>ix
3 93 46 67 B0 0C C3 U|ÿi .ù||iâq%MYCÖuÖvpÅAX* pÖ|Fg` Å
4 30 39 31 38 34 37 Y@p>| ÿÿ 0871,|oid": "1091847
5 35 38 38 34 31 22 49169553", "owner": "100002340858841"
6 5F 69 64 22 3A 22 "text": "Nudelsalat?", "object_id":
7 73 22 3A 30 7D 2C ", "story_type": 22, "num_credits": 0},
8 6D 49 64 22 3A 6E "userId": 100002340858841, "fromId": "n
9 3D 5C 22 62 6C 75 ull, "title": "\u003cspan class=\
0 70 61 6E 3E 20 68 eName">Yves Niessen\u003c\/span> h
1 22 2C 22 62 6F 64 at deinen Status kommentiert.", "bod
2 63 65 62 6F 6F 6B y": "", "link": "http://www.facebook
3 64 3D 31 30 39 31 .com/permalink.php?story_fbid=1091
4 31 22 2C 22 75 73 84749169553&id=100002340858841", "us
5 00 00 00 00 00 00 %253
  
```

■ 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?

