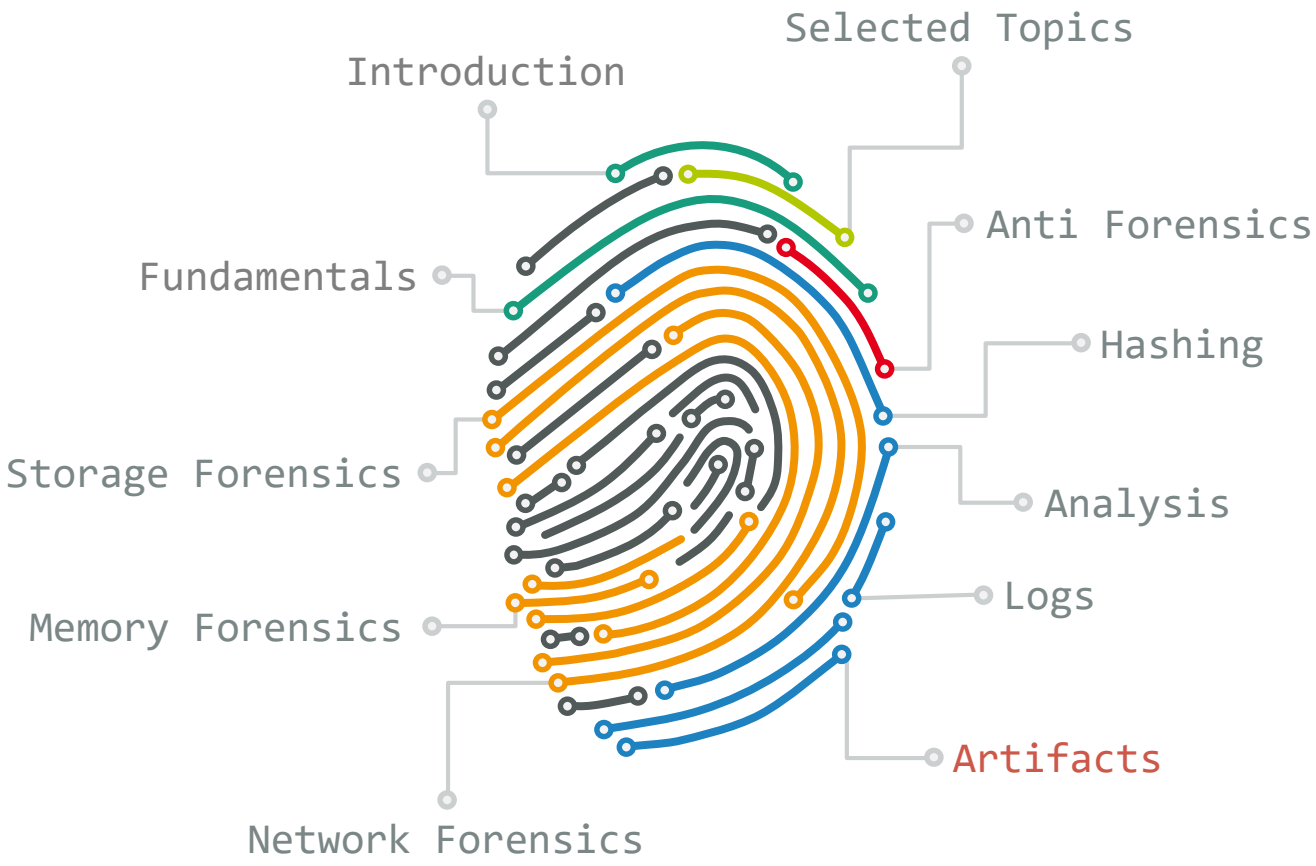
Hochschule Bonn-Rhein-Sieg

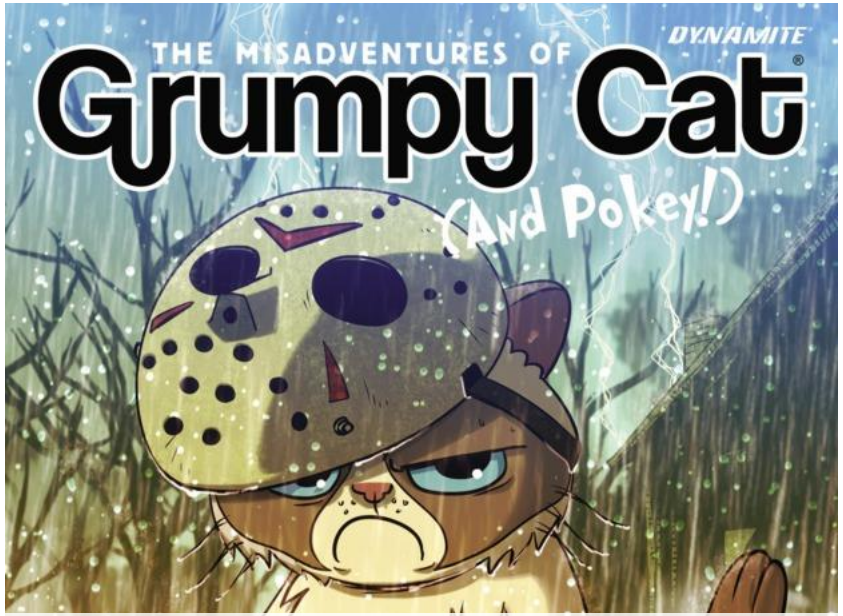
Fraunhofer FKIE

Prof. Dr. Elmar Padilla et al.

Digitale Forensik

06 - Artifacts



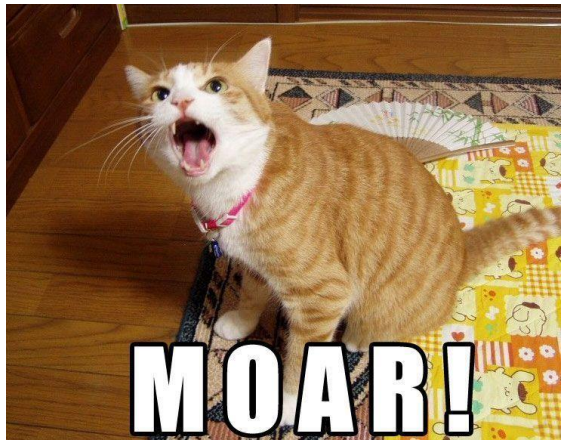


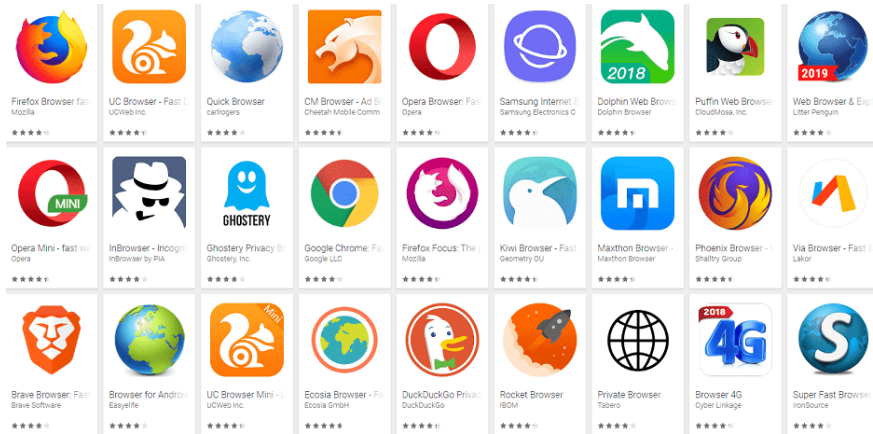
„Internet“ applications artifacts: browsers & email clients

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Web Browsers





Web Browsers






visited URLs


search history


bookmarks


browser cache


logins


download history


thumbnails


sync history

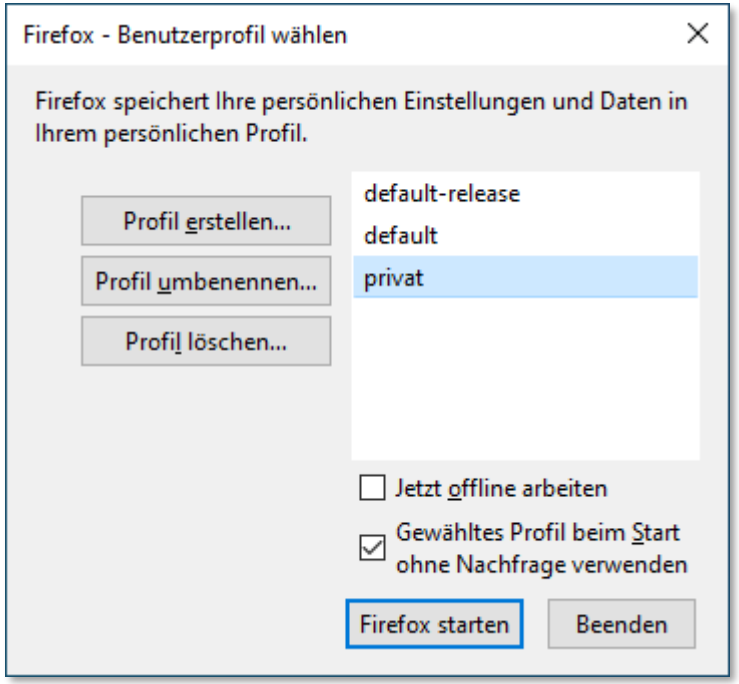

account infos


session info

Hochschule Bonn-Rhein-Sieg

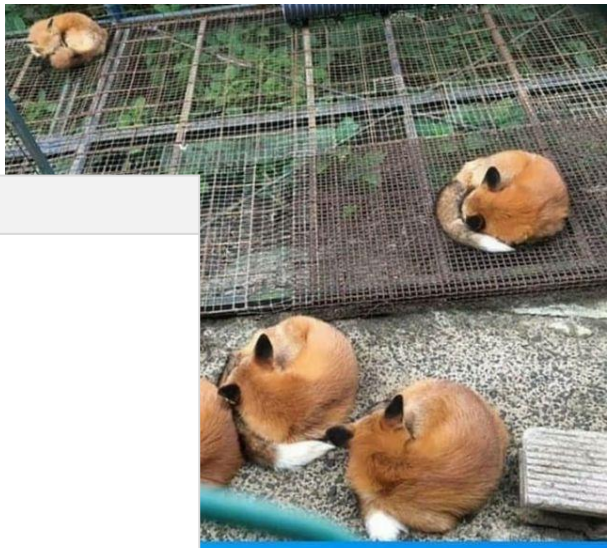
Fraunhofer FKIE

Firefox



Inspect all profiles found!

```
PS C:\Users\blau\AppData\Roaming\Mozilla\Firefox\> tree /F
C:.
│   installs.ini
│   profiles.ini
└───Profiles
    ├───02g9obmq.privat
    ├───y1il2nh4.default-release
    └───y5i5mm3b.default
…
```



Linux:

`$user/.mozilla/firefox/`

Windows 10:

`%UserProfile%\AppData\Roaming\Mozilla\Firefox\`

Hochschule Bonn-Rhein-Sieg

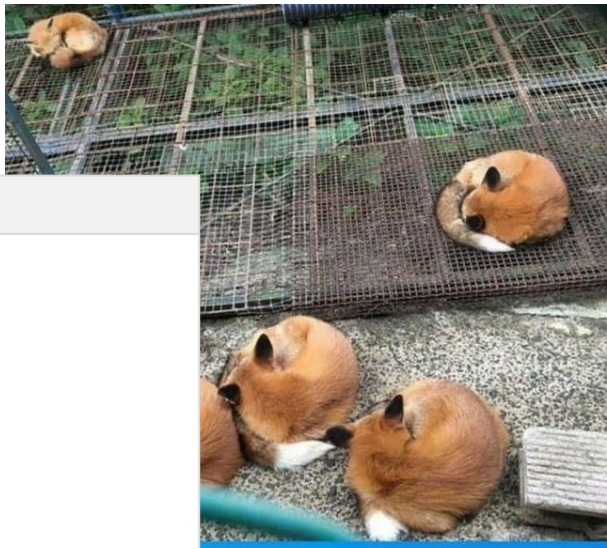
Fraunhofer FKIE

Firefox

profiles.ini

```
[Install308046B0AF4A39CB]
Default=Profiles/02g9obmq.privat
Locked=1

[Profile2]
Name=privat
IsRelative=1
Path=Profiles/02g9obmq.privat

[Profile1]
Name=default
IsRelative=1
Path=Profiles/y5i5mm3b.default
Default=1

[Profile0]
Name=default-release
IsRelative=1
Path=Profiles/y1il2nh4.default-release

[General]
StartWithLastProfile=1
Version=2
```

Inspect all profiles found!



PS C:\Users\blau\AppData\Roaming\Mozilla\Firefox\> tree /F

```
C:.
│   installs.ini
│   profiles.ini
└───Profiles
    ├───02g9obmq.privat
    ├───y1il2nh4.default-release
    └───y5i5mm3b.default
…
```

installs.ini

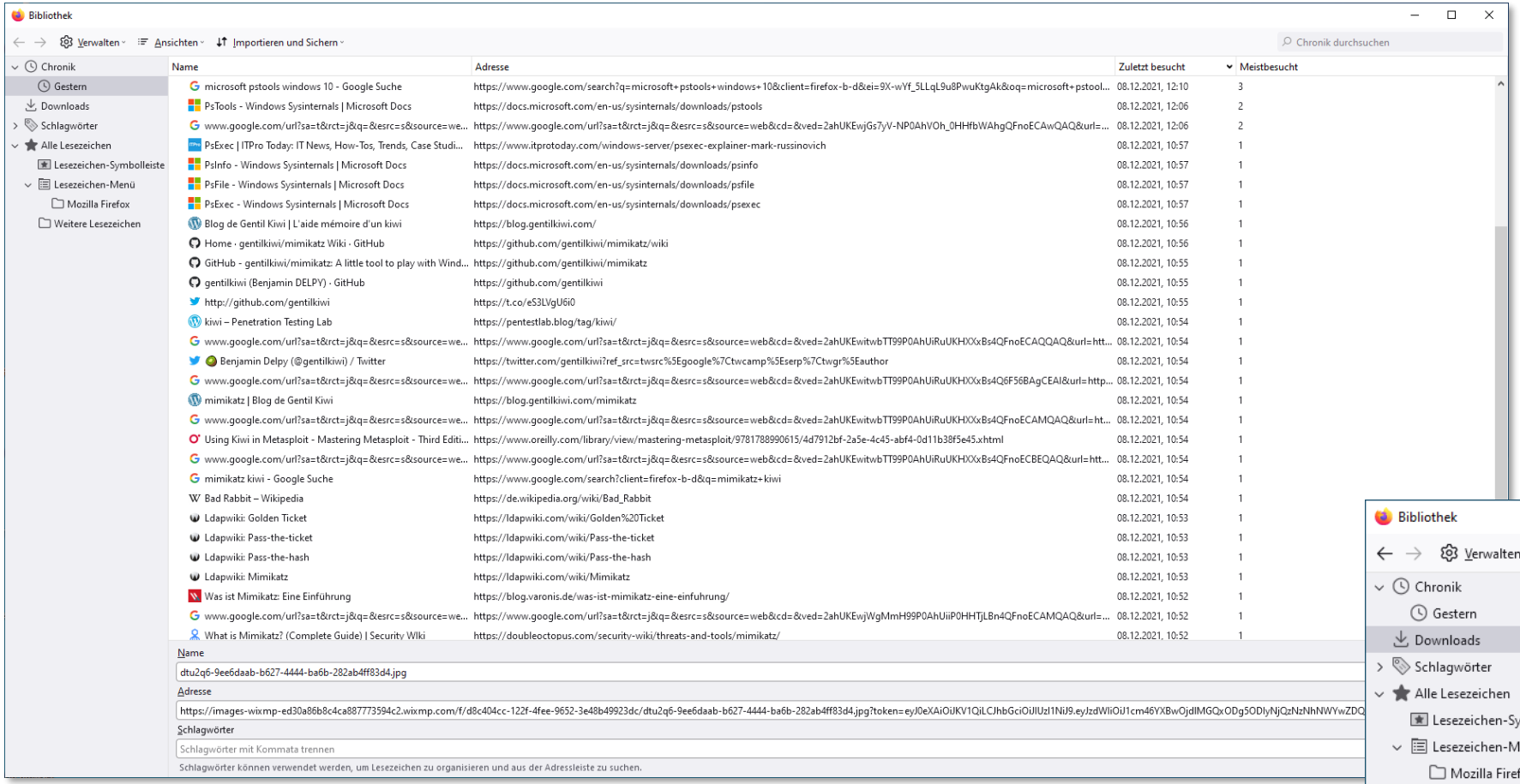
```
[308046B0AF4A39CB]
Default=Profiles/02g9obmq.privat
Locked=1
```

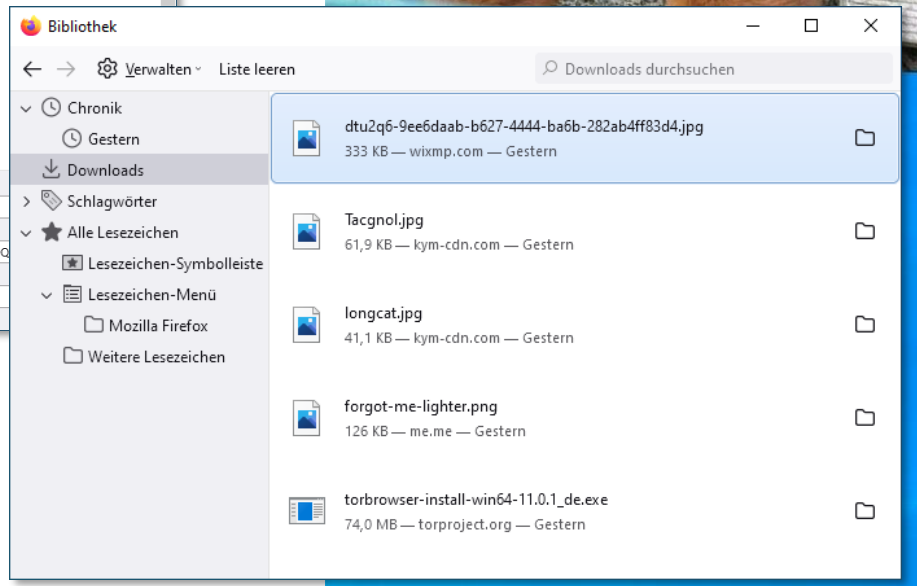
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Firefox

Setup firefox instance, copy corresponding profile folder to …\Profiles\ and adjust profiles.ini





…or simply adjust profiles.ini to point to the profile…

Firefox


```
PS %UserProfile%\AppData\Mozilla\firefox\Profiles\02g9obmq.privat> ls -Name
bookmarkbackups
crashes
datareporting
minidumps
saved-telemetry-pings
security_state
sessionstore-backups
storage
weave
addons.json
addonStartup.json.lz4
AlternateServices.txt
cert9.db
compatibility.ini
containers.json
content-prefs.sqlite
cookies.sqlite
extension-preferences.json
extensions.json
favicons.sqlite
formhistory.sqlite
handlers.json
key4.db
parent.lock
permissions.sqlite
pkcs11.txt
places.sqlite
prefs.js
protections.sqlite
search.json.mozlz4
serviceworker.txt
sessionCheckpoints.json
sessionstore.jsonlz4
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Firefox

visited URLs

moz_places

moz_places

search history

bookmarks

moz_bookmarks

browser cache

logins

download history

moz_annos

thumbnails

sync history

account infos

session info

places.sqlite

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

What websites did the user visit recently?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Visited URLs

moz_places

places.sqlite

id	url	title	rev_host	visit_count	hidden	typed	frecency	ast_visit_date	guid	foreign_count	url_hash	description	preview_image_url	origin_id
58	https://www.google.com/search?…	7-Zip 21.06 hash - Google Suche	moc.elgoog.www.	1	0	1	2000	1638957765956000	xZatxEFvs6ZO	0	47358310394880	NULL	NULL	3
57	https://7-zip.org/download.html	Download	gro.piz-7.	1	0	0	100	1638957708349000	8-76VCVS7cuQ	0	47357913388463	NULL	NULL	20
56	https://d2.7-zip.org/a/7z2106-…	7z2106-x64.exe	gro.piz-7.2d.	0	0	0	0	1638957680765000	HUnwhl1rf9Qu	0	47359201609499	NULL	NULL	21
55	https://7-zip.org/a/7z2106-…	NULL	gro.piz-7.	1	1	0	25	1638957677769000	DjZJRiRbx29h	0	47360232745625	NULL	NULL	20
54	https://7-zip.org/	7-Zip	gro.piz-7.	1	0	0	100	1638957658178000	KZx_OIo5j_9a	0	47360578613219	NULL	NULL	20
53	https://de.wikipedia.org/wiki/7z	7z – Wikipedia	gro.aidepikiw.ed.	1	0	0	100	1638957641332000	cOncWmsqu_LZ	0	47356843135918	NULL	NULL	7
52	https://www.google.com/search?…	wiki 7z - Google Suche	moc.elgoog.www.	1	0	1	2000	1638957639081000	JcwKPXuiz6s7	0	47360458447290	NULL	NULL	3
51	https://www.itprotoday.com/…	PsExec | ITPro Today: IT News, …	moc.yadotorpti.www.	1	0	0	100	1638957453588000	0wfXHtNyWa8F	0	47357703940954	Find out how PsExec works and …	https://www.itprotoday.com/…	19
50	https://www.itprotoday.com/…	NULL	moc.yadotorpti.www.	1	1	0	25	1638957453535000	OdaSGrnjsCtC	0	47357090903590	NULL	NULL	19
49	https://docs.microsoft.com/en-…	PsInfo - Windows Sysinternals |…	moc.tfosorcim.scod.	1	0	0	100	1638957433047000	kiTBCnWqhfm_	0	47358714575418	Obtain information about a …	https://docs.microsoft.com/en-…	18
48	https://docs.microsoft.com/en-…	PsFile - Windows Sysinternals |…	moc.tfosorcim.scod.	1	0	0	100	1638957430510000	iRbFSoIHLrAH	0	47359261142229	See what files are opened …	https://docs.microsoft.com/en-…	18
47	https://docs.microsoft.com/en-…	PsExec - Windows Sysinternals |…	moc.tfosorcim.scod.	1	0	0	100	1638957427978000	uNeTlq	0	47357916955044	Execute processes on remote …	https://docs.microsoft.com/en-…	18
46	https://docs.microsoft.com/en-…	PsTools - Windows Sysinternals …	moc.tfosorcim.scod.	1	0	0	100	1638957425446000	aW74RA	0	47357542041397	Command-line utilities for …	https://docs.microsoft.com/en-…	18
45	https://www.google.com/url?…	NULL	moc.elgoog.www.	1	0	0	100	1638957420891000	DIlNGnEAL4ui	0	47356816361521	NULL	NULL	3
44	https://www.google.com/search?…	microsoft pstools windows 10 - …	moc.elgoog.www.	1	0	0	100	1638957417724000	FqJfI8REpxIV	0	47359077501890	NULL	NULL	3
43	https://blog.gentilkiwi.com/	Blog de Gentil Kiwi | L'aide …	moc.iwiklitneg.golb.	1	0	0	100	1638957367403000	yDBV9YvcfoLJ	0	47357711255860	NULL	NULL	12
42	https://github.com/gentilkiwi/…	Home · gentilkiwi/mimikatz Wiki…	moc.buhtig.	1	0	0	100	1638957366168000	ATNFtg9IRgxG	0				
41	https://github.com/gentilkiwi/…	GitHub - gentilkiwi/mimikatz: A…	moc.buhtig.	1	0	0	100	1638957342874000	G1CqZHI7QZD3	0				
40	https://github.com/gentilkiwi	gentilkiwi (Benjamin DELPY) · …	moc.buhtig.	1	0	0	100	1638957334222000	RSWmDVWXzj3V	0				
39	http://github.com/gentilkiwi	NULL	moc.buhtig.	1	0	0	100	1638957333350000	HjcxdWJAx2-P	0	125508387850164			
38	https://t.co/eS3LVgU6i0	http://github.com/gentilkiwi	oc.t.	1	0	0	100	1638957333205000	kDY_ygjxPpwC	0	47357137429832			
37	https://pentestlab.blog/tag/…	kiwi – Penetration Testing Lab	golb.baltsetnep.	1	0	0	100	1638957294916000	GwUfEoco8Bp9	0	47359321475006			
36	https://www.google.com/url?…	NULL	moc.elgoog.www.	1	0	0	100	1638957293931000	Dy_hmIQeDaAu	0	47360503905496			
35	https://twitter.com/gentilkiwi?…	Benjamin Delpy (@gentilkiwi…	moc.rettiwt.	1	0	0	100	1638957291015000	SSY2iPNBHCN_	0	47357281384579			
34	https://www.google.com/url?…	NULL	moc.elgoog.www.	1	0	0	100	1638957290688000	qdUUcTgg8OyR	0	47356888607823			
33	https://blog.gentilkiwi.com/…	mimikatz | Blog de Gentil Kiwi	moc.iwiklitneg.golb.	1	0	0	100	1638957289111000	GQyyj_ruHQYl	0	47357765226590			
32	https://www.google.com/url?…	NULL	moc.elgoog.www.	1	0	0	100	1638957287809000	Mm1NuMye0jus	0	47358340057118			
31	https://www.oreilly.com/library…	Using Kiwi in Metasploit - …	moc.ylliero.www.	1	0	0	100	1638957287638000	KsIO-WacVvlY	0	47357274647639			
30	https://www.oreilly.com/library…	NULL	moc.ylliero.www.	1	1	0	25	1638957286923000	ihk-Ck4pRReV	0	47357781835605			
29	https://www.google.com/url?…	NULL	moc.elgoog.www.	1	0	0	100	1638957286427000	3w3I9i2QgQB8	0	47360105549848			
28	https://www.google.com/search?…	mimikatz kiwi - Google Suche	moc.elgoog.www.	1	0	1	2000	1638957279193000	HZDBXvrZ4p_h	0	47356473054489			
27	https://de.wikipedia.org/wiki/…	Bad Rabbit – Wikipedia	gro.aidepikiw.ed.	1	0	0	100	1638957253180000	gNvbM2amEYFj	0	47358476800881			
26	https://ldapwiki.com/wiki/…	Ldapwiki: Golden Ticket	moc.ikiwpadl.	1	0	0	100	1638957212883000	zcchb9Y2_-mK	0	47357326027091			
25	https://ldapwiki.com/wiki/Pass-…	Ldapwiki: Pass-the-ticket	moc.ikiwpadl.	1	0	0	100	1638957208164000	0hzaS8uNdb3O	0	47360403737720			
24	https://ldapwiki.com/wiki/Pass-…	Ldapwiki: Pass-the-hash	moc.ikiwpadl.	1	0	0	100	1638957205684000	NTiVuDbVkZBK	0	47357763086185			

weird timestamps…

don't care about most of the columns

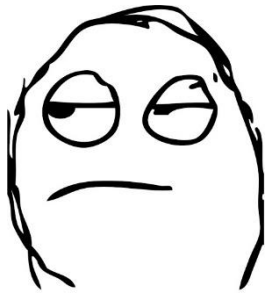
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Speakin‘ about timestamps

`1638962082` Unix Time: seconds elapsed since January 1, 1970 UTC (Unix Epoch)

`1638962082957000` microseconds elapsed since January 1, 1970 UTC (Unix Epoch)



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Speakin‘ about timestamps

`1638962082` Unix Time: seconds elapsed since January 1, 1970 UTC (Unix Epoch)

`1638962082957000` microseconds elapsed since January 1, 1970 UTC (Unix Epoch)

converts Unix timestamps

```
datetime(VALUE/1000000, 'unixepoch', 'localtime')
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Speakin‘ about timestamps

`1638962082` Unix Time: seconds elapsed since January 1, 1970 UTC (Unix Epoch)

`1638962082957000` microseconds elapsed since January 1, 1970 UTC (Unix Epoch)

```
datetime(VALUE/1000000, 'unixepoch', 'localtime')
```

converts microseconds to seconds

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Speakin‘ about timestamps

`1638962082` Unix Time: seconds elapsed since January 1, 1970 UTC (Unix Epoch)

`1638962082957000` microseconds elapsed since January 1, 1970 UTC (Unix Epoch)

```
datetime(VALUE/1000000, 'unixepoch', 'localtime')
```

display in system timezone instead of UTC

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Visited URLs

```
select id, datetime(moz_places.last_visit_date/1000000, 'unixepoch', 'localtime') as last_visit_date,
       visit_count, title, url,
       last_visit_date as unix_timestamp
from moz_places order by unix_timestamp desc;
```

moz_places

unambiguously identifies visited URL

time of last URL visit

How often URL was visited

title of the website (if any)

„unique“ visited URLs

id	last_visit_date	visit_count	title	url	unix_timestamp
58	2021-12-08 11:02:45	1	7-Zip 21.06 hash - Google Suche	https://www.google.com/search?…	1638957765956000
57	2021-12-08 11:01:48	1	Download	https://7-zip.org/download.html	1638957708349000
56	2021-12-08 11:01:20	0	7z2106-x64.exe	https://d2.7-zip.org/a/7z2106-…	1638957680765000
55	2021-12-08 11:01:17	1	NULL	https://7-zip.org/a/7z2106-…	1638957677769000
54	2021-12-08 11:00:58	1	7-Zip	https://7-zip.org/	1638957658178000
53	2021-12-08 11:00:41	1	7z – Wikipedia	https://de.wikipedia.org/wiki/7z	1638957641332000
52	2021-12-08 11:00:39	1	wiki 7z - Google Suche	https://www.google.com/search?…	1638957639081000
	8 10:57:33	1	PsExec | ITPro Today: IT News, …	https://www.itprotoday.com/	1638957453588000
	8 10:57:33	1	NULL	https://www.…	5000
	8 10:57:13	1	PsInfo - Windows Sysinternals |…	https://docs.microsoft.com/en-…	1638957433047000
48	2021-12-08 10:57:10	1	PsFile - Windows Sysinternals |…	https://docs.microsoft.com/en-…	1638957430510000
47	2021-12-08 10:57:07	1	PsExec - W…	https://docs.microsoft.com/en-…	1638957427206000
46	2021-12-08 10:57:01	1	PsTools -	https://docs.microsoft.com/en-…	1638957421184000
45	20	1	NULL	https://www.google.com/url?…	1638957420891000
44	20	1	microsoft pstools windows 10 - …	https://www.google.com/search?…	1638957417724000
43	2021-12-08 10:56:07	1	Blog de Gentil Kiwi | L'aide …	https://blog.gentilkiwi.com/	1638957367403000
42	2021-12-08 10:56:06	1	Home · gentilkiwi/mimikatz Wiki…	https://github.com/gentilkiwi/…	1638957366168000
41	2021-12-08 10:55:42	1	GitHub - gentilkiwi/mimikatz: A…	https://github.com/gentilkiwi/…	1638957342874000
40	2021-12-08 10:55:34	1	gentilkiwi (Benjamin DELPY) · …	https://github.com/gentilkiwi	1638957334222000
39	2021-12-08 10:55:33	1	NULL	http://githu	
38	2021-12-08 10:55:33	1	http://github.com/gentilkiwi	https://t.co	
37	2021-12-08 10:54:54	1	kiwi – Penetration Testing Lab	https://pent	
36	2021-12-08 10:54:53	1	NULL	https://www.	
35	2021-12-08 10:54:51	1	Benjamin Delpy (@gentilkiwi…	https://twit	
34	2021-12-08 10:54:50	1	NULL	https://www.google.com/url?…	1638957290688000

Is NOT browsing history, just a list of visited URLs.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Things the user typed

```
select datetime(moz_places.last_visit_date/1000000, 'unixepoch', 'localtime') as last_visit_date,
       title, url, typed, last_visit_date as timestamp
from moz_places
where typed == 1
order by timestamp desc;
```

last_visit_date	title	url	typed	timestamp
2021-12-13 12:00:40	MITRE ATT&CK®	https://attack.mitre.org/	1	1639393240511000
2021-12-13 11:59:12	*NULL*	http://amazon.com/	1	1639393152967000
2021-12-13 11:59:03	amazon - Google Suche	https://www.google.com/search?…	1	1639393143747000
2021-12-08 12:13:26	forgot me lighter - Google Suche	https://www.google.com/search?…	1	1638962006415000
2021-12-08 12:10:41	microsoft pstools windows 10 - …	https://www.google.com/search?…	1	1638961841034000
2021-12-08 12:06:58	*NULL*	https://www.google.com/url?…	1	1638961618179000
2021-12-08 10:54:39	mimikatz kiwi - Google Suche	https://www.google.com/search?…	1	1638957279193000
2021-12-08 10:52:00	mimikatz wiki - Google Suche	https://www.google.com/search?…	1	1638957120162000
2021-12-08 10:50:45	tor browser how to - Google …	https://www.google.com/search?…	1	1638957045776000
2021-12-08 10:50:19	tor browser - Google Suche	https://www.google.com/search?…	1	1638957019756000

URL or search query explicitly typed into address bar by the user

`moz_places` tells us only the most recent visit times…

Can we get complete history aka. timeline of websites visits?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Browsing history

moz_historyvisits places.sqlite

id	from_visit	place_id	visit_date ▴1	visit_type
F…	Filtern	Filtern	Filtern	Filtern
76	0	74	1639393240511000	2
75	74	73	1639393154085000	5
74	73	72	1639393153615000	5
73	0	71	1639393152967000	2
72	0	70	1639393143747000	2
71	70	69	1638962106265000	7
70	69	68	1638962099060000	1
69	67	67	1638962091245000	1
68	67	66	1638962082957000	7
67	66	65	1638962075475000	1
66	65	64	[illegible]	1
65	63	[illegible]	[illegible]	1
64	63	62	1638962065950000	7
63	62	61	[illegible]	1
62	60	60	[illegible]	[illegible]
61	60	59	1638962028181000	7
60	59	58	1638962017505000	1
59	58	57	1638962013018000	1
58	0	56	1638962006415000	2
57	0	44	1638961841034000	3
56	0	44	1638961651839000	2
55	54	46	1638961618882000	1

URL visit time

the way the URL was accessed

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Browsing history

id	from_visit	place_id	visit_date	visit_type
F…	Filtern	Filtern	Filtern	Filtern
76	0	74	1639393240511000	2
75	74	73	1639393154085000	5
74	73	72	1639393153615000	5
73	0	71	1639393152967000	2
72	0	70	1639393143747000	2
71	70	69	1638962106265000	7
70	69	68	1638962099060000	1
69	67	67	1638962091245000	1
68	67	66	1638962082957000	7
67	66	65	1638962075475000	1
66	65	64	1638962073685000	1
65	63	63	1638962067292000	1
64	63	62	1638962065950000	7
63	62	61	1638962047887000	1
62	60	60	1638962030181000	7
61	60	59	1638962028181000	7
60	59	58	1638962017505000	1
59	58	57	1638962013018000	1
58	0	56	1638962006415000	2
57	0	44	1638961841034000	3
56	0	44	1638961651839000	2
55	54	46	1638961618882000	1

URL visit time

the way the URL was accessed

moz_historyvisits

places.sqlite

1	TRANSITION_LINK	This transition type means the user followed a link and got a new toplevel window.
2	TRANSITION_TYPED	This transition type means that the user typed the page's URL in the URL bar or selected it from URL bar autocomplete results, clicked on it from a history query (from the History sidebar, History menu, or history query in the personal toolbar or Places organizer.
3	TRANSITION_BOOKMARK	This transition is set when the user followed a bookmark to get to the page.
4	TRANSITION_EMBED	This transition type is set when some inner content is loaded. This is true of all images on a page, and the contents of the iframe. It is also true of any content in a frame, regardless of whether or not the user clicked something to get there.
5	TRANSITION_REDIRECT_PERMANENT	Set when the transition was a permanent redirect.
6	TRANSITION_REDIRECT_TEMPORARY	Set when the transition was a temporary redirect.
7	TRANSITION_DOWNLOAD	Set when the transition is a download.

[https://forensicswiki.xyz/wiki/index.php?title=Mozilla_Firefox_3_History_File_Format]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Browsing history

id	from_visit	place_id	visit_date ▲1	visit_type
F…	Filtern	Filtern	Filtern	Filtern
76	0	74	1639393240511000	2
75	74	73	1639393154085000	5
74	73	72	1639393153615000	5
73	0	71	1639393152967000	2
72	0	70	1639393143747000	2
71	70	69	1638962106265000	7
70	69	68	1638962099060000	1
69	67	67	1638962091245000	1
68	67	66	1638962082957000	7
67	66	65	1638962075475000	1
66	65	64	1638962073685000	1
65	63	63	1638962067692000	1
64	63	62	1638962065950000	7
63	62	61	1638962047887000	1
62	60	60	1638962043783000	1
61	60	59	1638962028181000	7
60	59	58	1638962017505000	1
59	58	57	1638962013018000	1
58	0	56	1638962006415000	2
57	0	44	1638961841034000	3
56	0	44	1638961651839000	2
55	54	46	1638961618882000	1

Visit time is great to have, but wait a minute… Where are the actual website URLs?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Browsing history

id	from_visit	place_id	visit_date ▲1	visit_type
F…	Filtern	Filtern	Filtern	Filtern
76	0	74	1639393240511000	2
75	74	73	1639393154085000	5
74	73	72	1639393153615000	5
73	0	71	1639393152967000	2
72	0	70	1639393143747000	2
71	70	69	1638962106265000	7
70	69	68	1638962099060000	1
69	67	67	1638962091245000	1
68	67	66	1638962082957000	7
67	66	65	1638962075475000	1
66	65	64	1638962073685000	1
65	63	63	1638962067692000	1
64	63	62	1638962065950000	7
63	62	61	1638962047887000	1
62	60	60	1638962043783000	1
61	60	59	1638962028181000	7
60	59	58	1638962017505000	1
59	58	57	1638962013018000	1
58	0	56	1638962006415000	2
57	0	44	1638961841034000	3
56	0	44	1638961651839000	2
55	54	46	1638961618882000	1

link to `moz_places` table

Visit time is great to have, but wait a minute… Where are the actual website URLs?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Browsing history: putting all together

visit_date	url_id	title	url	visit_type	timestamp
2021-12-13 12:00:40	74	MITRE ATT&CK®	https://attack.mitre.org/	2	1639393240511000
2021-12-13 11:59:14	73	Amazon.com. Spend less. Smile …	https://www.amazon.com/	5	1639393154085000
2021-12-13 11:59:13	72	NULL	https://amazon.com/	5	1639393153615000
2021-12-13 11:59:12	71	NULL	http://amazon.com/	2	1639393152967000
2021-12-13 11:59:03	70	amazon - Google Suche	https://www.google.com/search?…	2	1639393143747000
2021-12-08 12:15:06	69	dtu2q6-9ee6daab-b627-4444-…	https://images-wixmp-…	7	1638962106265000
2021-12-08 12:14:59	68	longcat - Google Suche	https://www.google.com/search?…	1	1638962099060000
2021-12-08 12:14:51	67	longcat - Google Suche	https://www.google.com/search?…	1	1638962091250000
2021-12-08 12:14:43	66	Tacgnol.jpg	https://i.kym-cdn.com/entries/…	7	1638962082957000
2021-12-08 12:14:35	65	longcat - Google Suche	https://www.google.com/search?…	1	1638962075475000
2021-12-08 12:14:33	64	longcat - Google Suche	https://www.google.com/search?…	1	1638962073685000
2021-12-08 12:14:27	63	longcat - Google Suche	https://www.google.com/search?…	1	1638962067692000
2021-12-08 12:14:25	62	longcat.jpg	https://i.kym-cdn.com/photos/…	7	1638962065950000
2021-12-08 12:14:07	61	longcat - Google Suche	https://www.google.com/search?…	1	1638962047887000
2021-12-08 12:14:03	60	longcat - Google Suche	https://www.google.com/search?…	1	1638962043783000
2021-12-08 12:13:48	59	forgot-me-lighter.png	https://pics.me.me/forgot-me-…	7	1638962028181000
2021-12-08 12:13:37	58	forgot me lighter - Google Suche	https://www.google.com/search?…	1	1638962017505000
2021-12-08 12:13:33	57	forgot me lighter - Google Suche	https://www.google.com/search?…	1	1638962013018000
2021-12-08 12:13:26	56	forgot me lighter - Google Suche	https://www.google.com/search?…		
2021-12-08 10:56:57	44	microsoft pstools windows 10 - …	https://www.google.com/search?…		
2021-12-08 12:07:31	44	microsoft pstools windows 10 - …	https://www.google.com/search?…		
2021-12-08 12:10:41	44	microsoft pstools windows 10 - …	https://www.google.com/search?…		
2021-12-08 10:57:01	46	PsTools - Windows Sysinternals …	https://docs.microsoft.com/en-…		
2021		Sysinternals …	https://docs.microsoft.com/en-…		
2021			https://www.google.com/url?…		

URL visit time

website title

URL

type of access

e.g. pstools website visited on 3 different times

places.sqlite

moz_historyvisits

moz_places

```
select datetime(moz_historyvisits.visit_date/1000000, 'unixepoch', 'localtime')
       as visit_date,
       moz_places.id as url_id,
       title, url, typed,
       last_visit_date as timestamp
from moz_places
inner join moz_historyvisits on moz_places.id = moz_historyvisits.place_id
order by timestamp desc;
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

What about downloaded files?

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Downloads

moz_annos

date_added	id	place_id	anno_attribute_id	content	timestamp
2021-12-08 12:15:06	10	69	2	{"state":1,"endTime":1638962106278,"fileSize":340773}	1638962106339000
2021-12-08 12:15:06	9	69	1	file:///C:/Users/blau/Pictures/dtu2q6-9ee6daab-b627-4444-ba6b-282ab4ff83d4.jpg	1638962106338000
2021-12-08 12:14:42	8	66	2	{"state":1,"endTime":1638962082971,"fileSize":63431}	1638962082998000
2021-12-08 12:14:42	7	66	1	file:///C:/Users/blau/Pictures/Tacgnol.jpg	1638962082977000
2021-12-08 12:14:26	6	62	1	file:///C:/Users/blau/Pictures/longcat.jpg	1638962066056000
2021-12-08 12:14:26	5	62	2	{"state":1,"endTime":1638962065980,"fileSize":42128}	1638962066050000
2021-12-08 12:13:48	4	59	1	file:///C:/Users/blau/Downloads/forgot-me-lighter.png	1638962028370000
2021-12-08 12:13:48	3	59	2	{"state":1,"endTime":1638962028345,"fileSize":129046}	1638962028369000
2021-12-08 10:51:21	2	15	2	{"state":1,"endTime":1638957081604,"fileSize":77563504}	1638957081642000
2021-12-08 10:51:15	1	15	1	file:///C:/Users/blau/Downloads/torbrowser-install-win64-11.0.1_de.exe	1638957075842000

2 records per download

```
select datetime(moz_annos.dateAdded/1000000, 'unixepoch', 'localtime') as date_added,
       id, place_id, anno_attribute_id, content,
       dateAdded as timestamp
from moz_annos
order by timestamp desc;
```

Tacgnol.jpg

longcat.jpg

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Downloads

moz_annos

Meta record (attribute id 2):
download size in bytes,
download status (1 – success), …

date_added	id	place_id	anno_attribute_id	content	timestamp
2021-12-08 12:15:06	10	69	2	{"state":1,"endTime":1638962106278,"fileSize":340773}	1638962106339000
2021-12-08 12:15:06	9	69	1	file:///C:/Users/blau/Pictures/dtu2q6-9ee6daab-b627-4444-ba6b-282ab4ff83d4.jpg	1638962106338000
2021-12-08 12:14:42	8	66	2	{"state":1,"endTime":1638962082971,"fileSize":63431}	1638962082998000
2021-12-08 12:14:42	7	66	1	file:///C:/Users/blau/Pictures/Tacgnol.jpg	1638962082977000
2021-12-08 12:14:26	6	62	1	file:///C:/Users/blau/Pictures/longcat.jpg	1638962066056000
2021-12-08 12:14:26	5	62	2	{"state":1,"endTime":1638962065980,"fileSize":42128}	1638962066050000
2021-12-08 12:13:48	4	59	1	file:///C:/Users/blau/Downloads/forgot-me-lighter.png	1638962028370000
2021-12-08 12:13:48	3	59	2	{"state":1,"endTime":1638962028345,"fileSize":129046}	1638962028369000
2021-12-08 10:51:21	2	15	2	{"state":1,"endTime":1638957081604,"fileSize":77563504}	1638957081642000
2021-12-08 10:51:15	1	15	1	file:///C:/Users/blau/Downloads/torbrowser-install-win64-11.0.1_de.exe	1638957075842000

link to URL

File record (attribute id 1):
path to downloaded file

```
select datetime(moz_annos.dateAdded/1000000, 'unixepoch', 'localtime') as date_added,
       id, place_id, anno_attribute_id, content,
       dateAdded as timestamp
from moz_annos
order by timestamp desc;
```

Tacgnol.jpg

longcat.jpg

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Downloads: putting all together

url_last_visit	date_added	title	url	content
2021-12-08 12:15:06	2021-12-08 12:15:06	dtu2q6-9ee6daab-b627-4444-…	https://images-wixmp-ed30a86b8c4ca887773594c2.wixmp.com/f/…	file:///C:/Users/blau/Pictures/dtu2q6-9ee6daab-b627-4444-…
2021-12-08 12:15:06	2021-12-08 12:15:06	dtu2q6-9ee6daab-b627-4444-…	https://images-wixmp-ed30a86b8c4ca887773594c2.wixmp.com/f/…	{"state":1,"endTime":1638962106278,"fileSize":340773}
2021-12-08 12:14:42	2021-12-08 12:14:42	Tacgnol.jpg	https://i.kym-cdn.com/entries/icons/facebook/000/001/643/Tacgnol.jpg	file:///C:/Users/blau/Pictures/Tacgnol.jpg
2021-12-08 12:14:42	2021-12-08 12:14:42	Tacgnol.jpg	https://i.kym-cdn.com/entries/icons/facebook/000/001/643/Tacgnol.jpg	{"state":1,"endTime":1638962082971,"fileSize":63431}
2021-12-08 12:14:25	2021-12-08 12:14:26	longcat.jpg	https://i.kym-cdn.com/photos/images/newsfeed/000/002/110/longcat.jpg?…	{"state":1,"endTime":1638962065980,"fileSize":42128}
2021-12-08 12:14:25	2021-12-08 12:14:26	longcat.jpg	https://i.kym-cdn.com/photos/images/newsfeed/000/002/110/longcat.jpg?…	file:///C:/Users/blau/Pictures/longcat.jpg
2021-12-08 12:13:48	2021-12-08 12:13:48	forgot-me-lighter.png	https://pics.me.me/forgot-me-lighter-42727738.png	{"state":1,"endTime":1638962028345,"fileSize":129046}
2021-12-08 12:13:48	2021-12-08 12:13:48	forgot-me-lighter.png	https://pics.me.me/forgot-me-lighter-42727738.png	file:///C:/Users/blau/Downloads/forgot-me-lighter.png
2021-12-08 10:51:15	2021-12-08 10:51:15	torbrowser-install-…	https://dist.torproject.org/torbrowser/11.0.1/torbrowser-install-…	file:///C:/Users/blau/Downloads/torbrowser-install-…
2021-12-08 10:51:15	2021-12-08 10:51:21	torbrowser-install-…	https://dist.torproject.org/torbrowser/11.0.1/torbrowser-install-…	{"state":1,"endTime":1638957081604,"fileSize":77563504}

actual URLs of the downloads

```
select
    datetime(moz_places.last_visit_date/1000000, 'unixepoch', 'localtime') as url_last_visit,
    datetime(moz_annos.dateAdded/1000000, 'unixepoch', 'localtime') as date_added,
    moz_places.title as title , moz_places.url as url, moz_annos.content
from moz_places inner join moz_annos on moz_places.id = moz_annos.place_id
order by moz_places.last_visit_date desc;
```

Tacgnol.jpg

longcat.jpg

Firefox

visited URLs

bookmarks

search history

browser cache

logins

download history

thumbnails

sync history

account infos

session info

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Saved logins

Firefox [Mozilla] generally stores *sensitive infos* encrypted on disc.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Saved logins

Firefox [Mozilla] generally stores *sensitive infos* encrypted on disc.

`…/profile-name/logins.json` ← For example, saved logins

`…/profile-name/key4*.db` ← Data needed for decryption (password, salt, etc.)

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

logins.json


```
{
   "nextId":4,
   "logins":[
      {
         "id":1,
         "hostname":"https://github.com",
         "httpRealm":null,
         "formSubmitURL":"https://github.com",
         "usernameField":"login",
         "passwordField":"password",
         "encryptedUsername":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECPzmIBvJ4vJGBBCiBdAi/hJNFUx5yDylhb3h",
         "encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECEDW6jABqKJaBBD2fDb0kUYEEMRRqXDFFw2s",
         "guid":"{6e4ab777-02ee-4dbf-8ebd-7499a8178aa1}",
         "encType":1,
         "timeCreated":1639059789340,
         "timeLastUsed":1639059789340,
         "timePasswordChanged":1639059789340,
         "timesUsed":1
      },
      {
         "id":2,
         "hostname":"https://www.pcloud.com",
         …
         "usernameField":"email",
         "passwordField":"password",
         "encryptedUsername":"MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECKpUEqMrHT/bBBicZypyx/o+KMBV7VXQ35x5b54ehB7P+cw=",
         "encryptedPassword":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECDnQhjQRN69LBBDpQH0j47T+Q5L7kpuyOisO",
         …
      },
      {
         "id":3,
         "hostname":"https://kunde.comdirect.de",
         "formSubmitURL":"https://kunde.comdirect.de",
         "usernameField":"param1",
         "passwordField":"param3",
         "encryptedUsername":"MDoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECL5DfCblWYzeBBDuab5Kyok1IjYkElBqcmQM",
         "encryptedPassword":"MDIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECPL7mCCcdiXvBAiOJWtcG2NKXg==",
      }
   ],
   "potentiallyVulnerablePasswords":[
```

Saved logins

key4*.db content is protected by master password.

…/profile-name/logins.json

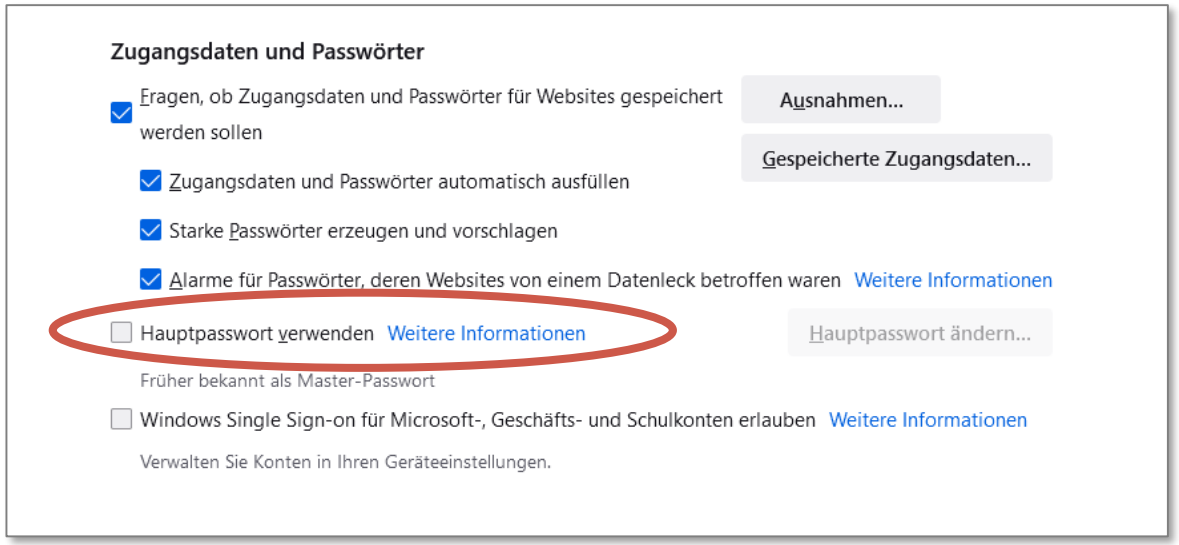
…/profile-name/key4*.db

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Saved logins

key4*.db content is protected by master password.



…which is not set by default…

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Saved logins

[https://www.nirsoft.net/utils/passwordfox.html]

[https://www.nirsoft.net/utils/web_browser_password.html]

PasswordFox: C:\Users\lynx\AppData\Roaming\Mozilla\Firefox\Profiles\n3wx7jkv.privat

File Edit View Options Help

Recor...	Web Site	User Name	Password	User Name Field	Password Field	Signons File	HTTP Realm	Password Strength	Firefox Ver...	Created Time	Last Time Used	Password Change ...	Password Use ...
1	https://github.com	herrx1982	qwertyZxcvb6	login	password	logins.json		Very Strong	32+	09/12/2021 15:23:09	09/12/2021 15:23:09	09/12/2021 15:23:09	1
2	https://www.pcloud.com	herrx1982@web.de	1982catsXXX	email	password	logins.json		Strong	32+	09/12/2021 15:24:20	09/12/2021 15:24:20	09/12/2021 15:28:34	1
3	https://kunde.comdirect.de	herrx1982	789345	param1	param3	logins.json		Very Weak	32+	09/12/2021 15:27:32	09/12/2021 15:27:32	09/12/2021 15:27:32	1

3 item(s), 1 Selected NirSoft Freeware. http://www.nirsoft.net

WebBrowserPassView

File Edit View Options Help

URL	Web Browser	User Name	Password	Password Stre...	User Name Field	Password Field	Created Time	Modified Time	Filename
https://github.com	Firefox 32+	herrx1982	qwertyZxcvb6	Very Strong	login	password	09/12/2021 15:23:09	09/12/2021 15:23:09	C:\Users\lynx\AppData\Roaming...
https://kunde.comdirect.de	Firefox 32+	herrx1982	789345	Very Weak	param1	param3	09/12/2021 15:27:32	09/12/2021 15:27:32	C:\Users\lynx\AppData\Roaming...
https://www.pcloud.com	Firefox 32+	herrx1982@web.de	1982catsXXX	Strong	email	password	09/12/2021 15:24:20	09/12/2021 15:28:34	C:\Users\lynx\AppData\Roaming...

3 Passwords NirSoft Freeware. http://www.nirsoft.net

```
$ python firepwd.py -d PATH-TO-PROFILE
```

```
…
decrypting login/password pairs
https://github.com:b'herrx1982',b'qwertyZxcvb6'
https://www.pcloud.com:b'herrx1982@web.de',b'1982catsXX'
https://kunde.comdirect.de:b'herrx1982',b'789345'
```

"Firepwd.py, an open source tool to decrypt Mozilla protected passwords"

[https://github.com/lclevy/firepwd]

```
$ firefed -p PATH-TO-PROFILE logins
```

Host	Username	Password
https://github.com	herrx1982	qwertyZxcvb6
https://www.pcloud.com	herrx1982@web.de	1982catsXXX
https://kunde.comdirect.de	herrx1982	789345

[https://github.com/numirias/firefed]

Firefox

visited URLs

bookmarks

search history

browser cache

logins

download history

thumbnails

sync history

account infos

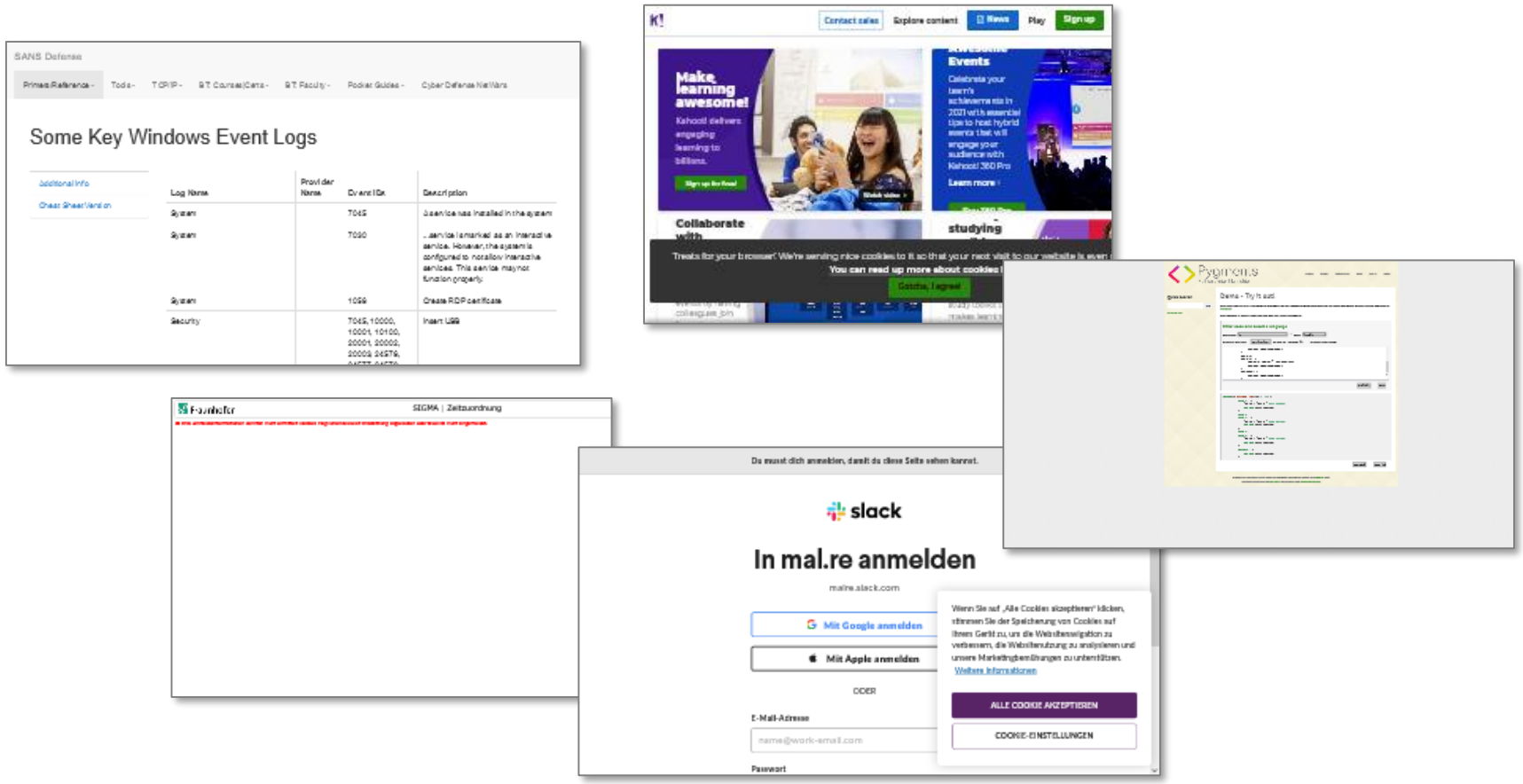
session info

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thumbnails

…/profile-name/thumbnails/



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Cache

…/profile-name/cache2/entries/

001AB6688D085441DAEDDE36C38715343CF15E2B
001BAA9A757219DA028FCC0D5EF3717CB1462765
001F048248CA332263CFFC08FC20F7FF1B020E79
00205C21355A82BA22FD4483A4DDB37B416C71D
003523D29CBE832D5E9068F0906B47E59B18FDE0
003BA59919273EF3EFAB199C3056C04518D77DE8
007D3C8164FE3C239CCCB55B8B9A7EEBE958E15A
007FAD3BBE5D2B0879B934FB8CF212233F60EA91
0098505569D0D80CCD509596F68762DCC759608A
00B14AB055CD89C1A798B15AB0F8574CB4ADC9BA
00B47F94C42281463DA232400DFA6AA47C0907CF
00B6B72CD4DCB8220FE8014C57647A239009F0CD
00BB77BC7A20E6BC735D09FE5E8D99560575A406
00DE55DEF4975BFC593F373A5BB92545BDBD6C8F
00F4F9E30A2798CC9CCB265C1B1D3E6585843E19
00F6F401F2F6DADDF82FD3B9C3F9FD3C29F4539E
0108C21A2099A86DA163FF344FA8810D033BFAE6
01285DE21CCBB6F37DB2A5346A4D82C8C73B0E94
0131498090BDB0D58D2F06B488ECE125490611A4
013B0DB7750286A737CFC5CA9BFA8A1438080961
01488A25431BA7080F5E0C131E8B1DAD41A9A5B4
014C98341EB1374763C7D4C2BC02A7FA5C93DF6A
014DC570C22F02983D2CCB61E2F42182DE5D1257
0153E3E27E215288DF11D4EE5D44B0025D38DCCE
01778417E37021841850FD860615259F3522F1CC
017BE3C98BFDA6DF51F0991F9D11ADAA2672ADEF
0189707F802DD70972A53F575893F44CDF1851CB
018BE5BB5BA4AD3787BB302900A108602A6C90B1
01AA86ED8B832A15B8F1E8C0897A0E5DA9BCB209
01AD2BC9BB3557BF1C4D6FAFA122857873998380
01B788380BD3A5C1BB721EEE3FAF826B08AD2560
01[illegible]
01D42CEE01E31D8CED60177B4C4353C358444A363
01D9313F921D77BE912F77D8343D357E0CC1233C
01F13588A2D55E4BDC0BF5D2C45456DA96E635A9
0220EAD1EAC0702E401C49CF96642F99A5A68FCA
0228458D907D96F69BC8827A75F1D175F6ACD64A
023EBEDA14D2CE9C98C60E57D5B87F01826B171C
024DC5C272CEB53D5F595470830922F306F50487
025FC38805DDB825DD6D282EC2C1825B181C130D
0265364BD7D7D9065D09C6C6A40ED0FDA799FCB2
026E65E4ED1B9A8D88C948A5E4B6AE6963B9DC6A
026FD955A241188CDD7C8FF5BE44320798B02481
028CD54DEF48F10419FF3732FCA664493FB423CB
02AE5A2F991C4E56D6871C0FFC0415F879766602
02BB572AD624DB4BE1A4E19706FB320479BB7AA4
02D10321E75C6DF79020E7388A1940A854FC284C
02F507023B1BE362FB768E4A504860C3DB49D371
0304F0A8DACE79C535013F0F72D69EF0C0794598
0305336B20162807CDDCBFC42246EEC5083A60BF
0309D82AD38C32E5C32AB79EB437BDDBA71E39E9
0316831DBFA75FB201942AD385CB80DF9B46A8A9
0317977F00892575682C1E37FE71B3822DB69FB5
032D2C55585B1ACE5869652AD03F2EDEB83F9674
0343220A44D4AEF1E0F1A182DAE7ACD159BFCAB5
034480248336559736679306626 1EABB1C5B8B13
034B0199ECC38559AC8D1FA48DB478E2C99DFA7C
034C3B23BA0431A8AF29F0766B5E6E333F83BD7D
035CC5DE58485883E6D31298A473E3B32170D49E
0360093680EAB31DFEA809E400039550 71698BA2
0376C1266B58A8BA454DD9A44B4F7AC5BD32AB7B
037778A55E1B7E9BED3390289866D09402D6C913
03810A5ED60465641FDA9A93D7BECE9DB9C7218D
038AF74DFA379A26D41C078652150B1B8EFD5DE2
039090029E64BC91E87E77199A6A6BE11FC39B6F
0398E864D5E966EC211356E0976F9D4FBB230E6C
03B14A148ED93C29F77DCFB5A6DD5C0715FC1AAE
03B37411C87798A6664A4DA2DB3EDD7A2403E88F
03B4CCDF926D38F3C25DE2E396660ADE72AA752A
03BFBD029EF5462FE31E5F833D234B3BF8AB56C6
03C0A29B11089246C2E32A41A571CFB57B834E3C
03C33BFC64C2DD4B99ACC31146CDA50D8D531F88

001AB6688D085441DAEDDE36C38715343CF15E2B: image/jpeg;
003BA59919273EF3EFAB199C3056C04518D77DE8: image/jpeg;
007FAD3BBE5D2B0879B934FB8CF212233F60EA91: image/gif;
00F6F401F2F6DADDF82FD3B9C3F9FD3C29F4539E: image/jpeg;
01285DE21CCBB6F37DB2A5346A4D82C8C73B0E94: image/jpeg;
01778417E37021841850FD860615259F3522F1CC: image/jpeg;
0376C1266B58A8BA454DD9A44B4F7AC5BD32AB7B: image/jpeg;
03B4CCDF926D38F3C25DE2E396660ADE72AA752A: image/jpeg;
0488C86548166E494FC3AFDBC07E822E87F003A5: image/jpeg;
0530B409BEB0B5E096027DFE443D54CBA3433CCB: image/jpeg;
054C6B4FE41C9FD3B5D00658D27411BA7D72DC61: image/gif;
0565A7BFFDDF9713BC8E8AC9E30292E39DB7978D: image/png;
057CFD3C074253C365BEADD2A393D4ED34CAEB47: image/jpeg;
05B64CFF940B5C2D5170AF785316D95B8E157B86: image/gif;
05D9F599317A1A1BEAB9E2A5DFF34A30DA85435A: image/webp;
0634DD354ECE1BB89CC384F7773A0350DA3EC0A3: image/jpeg;
064433C4CAC32F95942AEDB0F5931531933E7E22: image/gif;
064FE71B9F3DF67C1A0F8DD7773FBBF39424E4B0: image/jpeg;
065A69D7B299DF8DACCC027C7235ACA75E4409A2: image/gif;
066C5C183514CB6D6F55FF32D6B57477381ED520: image/png;
06D853953A259D2DD4C45C81748D22B09294A1E5: image/png;
0786A19C2A7B9F633FC5D75B87036774B5451DDC: image/gif;
078F62CA494C1B3A81512CE5DCC08110045B149D: image/jpeg;
07BC41DD6519639444C51F92E8C6D2A215A31E53: image/jpeg;
0807D6F11361D28E8237CD4F6FF9E912D1860CCF: image/webp;
08254EC6D1ADE0E81CFBF072939E9A10FEB715F8: image/gif;
083183AF2E2165106A15ECE5DF9CBEB8B80A7275: image/jpeg;
083D103F0AF99DF0CA89284120CD8B86362A9280: image/gif;
085B762362028D15C42A6956A8AE5E1028162B8C: image/jpeg;
087AA301278A30FFD938CC3A23493B1DA99C0CB5: image/jpeg;
08[illegible]9879E3650DC1FB27D00E82ADCB9F5A51052D68: image/jpeg;
08[illegible]EEC647[illegible]96[illegible]: image/jpeg;
08[illegible]FAE843[illegible]: image/gif;
09[illegible]9174EC[illegible]: image/png;
09[illegible]C7E21836759111F5C3931094CE0C390523F6528: image/gif;
0A2CBCEA4AC274CACA9695D915137015FDD5B922: image/gif;
0A36B6F09731E843F6F8D5BD71EF3A83103C2B88: image/gif;
0A80D436F310476A74AA4B889414978E9CE3333A: image/jpeg;
0A8295E234CD9D19C64CB547A427B5EA61B99737: image/jpeg;
0ADBA117B94FAEF9D2C9DD57226F108B77CD39D0: image/jpeg;
0B259305C63492C3B5624C4CEDD7D67CFBB049FA: image/png;
0B39513238A4469BADBF90CF41B670946FAC742D: image/gif;
0B51AC4C0D3FFAB1200BA5B8A777C9347B73E967: image/png;
0B6313D2624F6F099D59A617CEA905B29414A6CB: image/jpeg;
0B7AB60AD08E934C351CB3A685C045D335BA4B85: image/jpeg;
0BABF52A64DC7B1FCCDD563D131A086B80FE77E0: image/webp;
0BAE8F9C82BC090FBE01FE1C5E1F0B4160444CA4: image/gif;
0BC01BD5310FE2A3FB68E2587AF03110D86AD14D: image/png;
0BE92CFAA15E9C0C5DE903F9A779D03A557B53BF: image/gif;
0C4468AAAD0CCCF6FAB391DE9B1FA35269B410B2: image/gif;
0C8509A22F3C71F894EA6F6192D97F66A80FF32C: image/vnd.microsoft.icon;
0D87AF5D6E8844D7C5DE3F5871F232CD231D5D26: image/webp;
0DCF0B376A9DEB5E345CFEF474834A4186AB4F06: image/png;
0E4FCF8935808508778F1E4D99EC898E5203047A: image/jpeg;
0E6EE942C1AD73DF82EF64877ABB0CDE2B8AC2BD: image/png;
0EAE293CD176877E17A5CB2188F64A0CEB588A86: image/jpeg;
0EE42C9E23C9292E413CCC58E276802E4631AFBC: image/jpeg;
0F25160E4A13DA2FB87CEAF35436CB2905AD31F5: image/png;
0F30B37890A9B103B511C6351629F991C4A1A95B: image/svg+xml;
0F4067CEAEE4D96F61943EA539283784E2B65CF1: image/jpeg;
1058A76A59F3BDEFF0AA5A51017CBC015C0B09CB: image/jpeg;
109D080055C1548CE320A422FD98DA1D5E1A5BC8: image/svg+xml;
10DF6F1CDA45E89BC8836121515008CDD1323059: image/webp;
11184869B68F2E2C647F0D5121DC64616272E5B0: image/jpeg;
11DAD4BE1B17C9F993164FC979CFADB730D1F3C6: image/jpeg;
11F689421B9ABAE42E6B2427BA529C22777C9DF5: image/png;
121272309A6B40A93B13A70E22DA313318E461A0: image/png;
124DC53BA63E318C50FC3D7AF8C8503A55E0BE9D: image/jpeg;
1251164777CE76130F11BDC982415F17371A841B: image/jpeg;
12C6AD6D0CE3E11889A06DA9F2A1AEBD4F5A57FB: image/jpeg;
136DF037EDBE6EA4B9FC3F59630BF7670AA761ED: image/png;
145B6F3187B72769F3496596C84BFBE138A3A9DC: image/png;
147C964944D096CA92C7B78FAD55D5095A8232F1: image/jpeg;
14A19501A612AD09247B440403CA88A72D5D67C5: image/jpeg;

5729 entries

901 images

At least the user was searching for longcats…

FEC2182831E63B874C710F90D7B198C49F25B7D2

What the hell is this one???

FDD61BB9EA7B3527CB1FB571D5360DA9547263A1

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Cache

MZCacheView: [redacted]02g9obmq.privat\cache2

File Edit View Options Help

Filename	Content Type	URL	File Size	Cache Name	Fetch Count	Last Modified	Last Fetched	Expiration Time	Server Name	Server Response	Server Time	Server Last Modi...	Conte
727fc609.png	image/png	https://www.torproject.org/static/images/t...	85.818	8004933330D2E2A41CA7...	1	09.12.2021 14:12:38	09.12.2021 14:12:38	09.12.2021 10:50:24	Apache	HTTP/1.1 200 OK	08.12.2021 10:50:24	07.12.2021 03:27:...	
out.png	image/png	https://ldapwiki.com/images/out.png	927	32F0CDD248D2D51C207...	6	09.12.2021 14:12:38	09.12.2021 14:12:38	15.12.2021 10:53:15	nginx	HTTP/1.1 200 OK	08.12.2021 10:53:15	19.11.2018 11:20:...	
arrow-down.p...	image/png	https://www.torproject.org/static/fonts/fo...	3.381	D6438B68137344953B7A...	2	09.12.2021 14:12:38	09.12.2021 14:12:38	09.12.2021 10:51:11	Apache	HTTP/1.1 200 OK	08.12.2021 10:51:11	07.12.2021 03:28:...	
arrow-down.p...	image/png	https://www.torproject.org/static/fonts/fo...	3.202	5E31AA0819DAFD6C071...	2	09.12.2021 14:12:38	09.12.2021 14:12:38	09.12.2021 10:51:11	Apache	HTTP/1.1 200 OK	08.12.2021 10:51:11	07.12.2021 03:28:...	
arrow_down.p...	image/png	https://ssl.gstatic.com/ui/v1/zippy/arrow_...	94	A024E835137DF86EBE4E...	1	09.12.2021 14:12:38	09.12.2021 14:12:38	06.12.2022 19:00:42	sffe	HTTP/3 200 OK	06.12.2021 19:00:42	03.03.2020 21:15:...	
7ziplogo.png	image/png	https://7-zip.org/7ziplogo.png	1.417	E0547F4C6212418E70DA...	5	09.12.2021 14:12:38	09.12.2021 14:12:38	15.12.2021 11:00:58	nginx/1.14.1	HTTP/1.1 200 OK	08.12.2021 11:00:58	10.03.2018 10:07:...	
825f9a2c.png	image/png	https://www.torproject.org/static/css/imag...	195.473	E73ADCCAC797EE3B5F6...	2	09.12.2021 14:12:38	09.12.2021 14:12:38	09.12.2021 10:51:11	Apache	HTTP/1.1 200 OK	08.12.2021 10:51:11	07.12.2021 03:49:...	
915929603405...	image/png	https://tpc.googlesyndication.com/daca_i...	107.717	9AF48047F1914C7B29F9...	1	09.12.2021 14:12:38	09.12.2021 14:12:38	05.12.2022 11:59:09	sffe	HTTP/2 200 OK	05.12.2021 11:59:09	03.11.2021 08:52:...	
f539211219b79...	image/png	https://cdn.taboola.com/libtrc/static/thum...	254	145B6F3187B72769F3496...	1	09.12.2021 14:12:38	09.12.2021 14:12:38	08.12.2022 08:13:32	AmazonS3	HTTP/2 200 OK	08.12.2021 10:51:11	24.06.2015 09:14:...	
search.png	image/png	https://blog.gentilkiwi.com/wp-content/th...	440	0565A7BFFDDF9713BC8...	3	09.12.2021 14:12:38	09.12.2021 14:12:38	15.12.2021 10:54:49	Apache	HTTP/2 200 OK	08.12.2021 10:54:49	26.07.2021 08:12:...	
sea.mashable....	image/png	https://encrypted-tbn2.gstatic.com/favico...	287	BF313B447EA517CC984...	1	09.12.2021 14:12:38	09.12.2021 14:12:38	14.12.2021 21:14:20	sffe	HTTP/3 200 OK	07.12.2021 21:14:20	03.08.2020 00:54:...	
ac-topright-sp...	image/png	https://images-eu.ssl-images-amazon.com...	1.873	FD84ACE70C009CE7C31...	1	09.12.2021 14:12:38	09.12.2021 14:12:38	09.12.2021 08:27:58	Server	HTTP/2 200 OK	08.12.2021 08:27:58	17.04.2014 00:13:...	

Cache files:

- Original and cache names
- Metadata
- Origin
- Preview
- …

5226 item(s), 1 Selected (190.89 KB) NirSoft Freeware. http://www.nirsoft.net

[https://www.nirsoft.net/utils/mozilla_cache_viewer.html]

Firefox

bookmarks

visited URL

Think twice before using such infos as the only evidence!

browser cache

logins

download history

thumbnails

sync history

account infos

session info

Email clients





message contents


attachments


email headers


communications


address book


account passwords &
private keys

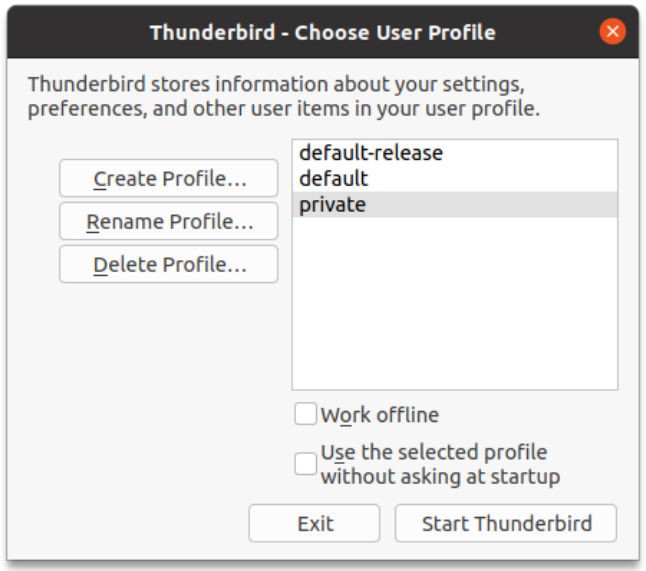

calender

Before we continue

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thunderbird



Linux:

`$user/.thunderbird/`

Windows 10:

`%UserProfile%\AppData\Roaming\Thunderbird\Profiles\`

[https://cheezburger.com/7829473792/blue-fairy-wern-is-a-beauty]

Thunderbird

```
$ ls .thunderbird
sj9a0u0t.default-release
0mc56zjt.default
installs.ini
profiles.ini
…
```

Inspect all profiles found!

```
installs.ini
[FDC34C9F024745EB]
Default=/home/sf/.important
Locked=1
```

```
profiles.ini
[Profile2]
Name=private
IsRelative=0
Path=/home/sf/.important

[Profile1]
Name=default
IsRelative=1
Path=0mc56zjt.default
Default=1

[Profile0]
Name=default-release
IsRelative=1
Path=sj9a0u0t.default-release

[General]
StartWithLastProfile=0
Version=2

[InstallFDC34C9F024745EB]
Default=/home/sf/.important
Locked=1
```

lies not in default profile folder

[https://cheezburger.com/7829473792/blue-fairy-wern-is-a-beauty]

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Thunderbird

message contents

attachments

email headers

communications

address book

account passwords & private keys

calender

```
$ tree .important #path to profile
.
├── 0x8B9C85B271943CFC_rev.asc
├── abook
├── abook.sqlite
├── addons.json
├── addonStartup.json.lz4
…
├── ImapMail          Name depends on protocol used
│   ├── imap.gmx.net  Name depends on mail provider
│   │   ├── Archives.msf
│   │   ├── Drafts.msf
│   │   ├── Entw&APw-rfe.msf
│   │   ├── filterlog.html
│   │   ├── Gel&APY-scht.msf
│   │   ├── Gesendet
│   │   ├── Gesendet.msf
│   │   ├── INBOX      <-- actual contents
│   │   ├── INBOX.msf  <-- mail summary
│   │   ├── msgFilterRules.dat
│   │   ├── OUTBOX.msf
│   │   ├── Sent.msf
│   │   ├── Spamverdacht.msf
│   │   └── Templates.msf
│   └── imap.gmx.net.msf
├── key4.db
├── logins.json
├── Mail
│   └── Local Folders
│       ├── filterlog.html
│       ├── msgFilterRules.dat
│       ├── Trash
│       ├── Trash.msf
│       ├── Unsent Messages
│       └── Unsent Messages.msf
├── mailViews.dat
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

[http://kb.mozillazine.org/Files_and_folders_in_the_profile_-_Thunderbird]

[https://cheezburger.com/7829473792/blue-fairy-wern-is-a-beauty]

MSF files

"Index files for mail messages. They contain a cache of the folder listing plus a few folder specific settings."

[http://kb.mozillazine.org/Files_and_folders_in_the_profile_-_Thunderbird]

$ cat Sent.msf

```
// <!-- <mdb:mork:z v="1.4"/> -->
< <(a=c)> // (f=iso-8859-1)
  (80=ns:msg:db:row:scope:msgs:all)(81=subject)(82=sender)(83=message-id)
  (84=references)(85=recipients)(86=date)(87=size)(88=flags)(89=priority)
  (8A=label)(8B=statusOfset)(8C=numLines)(8D=ccList)(8E=bccList)
  (8F=msgThreadId)(90=threadId)(91=threadFlags)(92=threadNewestMsgDate)
  (93=children)(94=unreadChildren)(95=threadSubject)(96=msgCharSet)
  (97=ns:msg:db:table:kind:msgs)(98=ns:msg:db:table:kind:thread)
  (99=ns:msg:db:table:kind:allthreads)
  (9A=ns:msg:db:row:scope:threads:all)(9B=threadParent)(9C=threadRoot)
  (9D=msgOffset)(9E=offlineMsgSize)
  (9F=ns:msg:db:row:scope:dbfolderinfo:all)
  (A0=ns:msg:db:table:kind:dbfolderinfo)(A1=numMsgs)(A2=numNewMsgs)
  (A3=folderSize)(A4=expungedBytes)(A5=folderDate)(A6=highWaterKey)
  (A7=mailboxName)(A8=UIDValidity)(A9=totPendingMsgs)
  (AA=unreadPendingMsgs)(AB=expiredMark)(AC=version)(AD=forceReparse)
  (AE=fixedBadRefThreading)(AF=onlineName)(B0=folderName)>
{1:^80 {(k^97:c)(s=9)} }
{FFFFFFFD:^9A {(k^99:c)(s=9)} }

<(80=1)(81=0)(82=Sent)(83=200)>
{1:^9F {(k^A0:c)(s=9u)}
  [1(^AC=1)(^AD=0)(^AE=1)(^AF^82)(^88^83)]}

@$${1{@
@$$}1}@
```

„empty" msf
(mailbox summary files?)

$ cat Gesendet.msf

```
// <!-- <mdb:mork:z v="1.4"/> -->
< <(a=c)> // (f=iso-8859-1)
  (B8=dateReceived)(B9=ProtoThreadFlags)(BA=folderName)(BB=storeToken)
  (BC=gloda-id)(BD=gloda-dirty)(BE=junkscore)(BF=keywords)(C0=retainBy)
  (C1=daysToKeepHdrs)(C2=numHdrsToKeep)(C3=daysToKeepBodies)
  (C4=useServerDefaults)(C5=cleanupBodies)(C6=applyToFlaggedMessages)
  (C7=useServerRetention)(C8=pseudoHdr)(C9=ns:msg:db:row:scope:ops:all)
  (CA=ns:msg:db:table:kind:ops)(CB=op)(CC=msgKey)(CD=opFlags)
  (CE=newFlags)(CF=moveDest)(D0=sortType)(D1=sortOrder)(D2=viewFlags)
  (D3=viewType)(D4=columnStates)(D5=MRUTime)(D6=sortColumns)
  (D7=customSortCol)(D8=imageSize)(D9=recipient_names)
  (DA=notAPhishMessage)(80=ns:msg:db:row:scope:msgs:all)(81=subject)
  (82=sender)(83=message-id)(84=references)(85=recipients)(86=date)
  (87=size)(88=flags)(89=priority)(8A=label)(8B=statusOfset)(8C=numLines)
  (8D=ccList)(8E=bccList)(8F=msgThreadId)(90=threadId)(91=threadFlags)
  (92=threadNewestMsgDate)(93=children)(94=unreadChildren)
  (95=threadSubject)(96=msgCharSet)(97=ns:msg:db:table:kind:msgs)
  (98=ns:msg:db:table:kind:thread)(99=ns:msg:db:table:kind:allthreads)
  (9A=ns:msg:db:row:scope:threads:all)(9B=threadParent)(9C=threadRoot)
  (9D=msgOffset)(9E=offlineMsgSize)
  (9F=ns:msg:db:row:scope:dbfolderinfo:all)
  (A0=ns:msg:db:table:kind:dbfolderinfo)(A1=numMsgs)(A2=numNewMsgs)
  (A3=folderSize)(A4=expungedBytes)(A5=folderDate)(A6=highWaterKey)
  (A7=mailboxName)(A8=UIDValidity)(A9=totPendingMsgs)
  (AA=unreadPendingMsgs)(AB=expiredMark)(AC=version)(AD=forceReparse)
  (AE=fixedBadRefThreading)(AF=onlineName)(B0=indexingPriority)
  (B1=highestModSeq)(B2=imapFlags)(B3=charSetOverride)(B4=charSet)
  (B5=highestRecordedUID)(B6=ns:msg:db:row:scope:pending:all)
  (B7=ns:msg:db:table:kind:pending)>
<(80=1)(93=fffffffe)(8E=61b34113)(81=0)>
[1:m(^9C=1)(^90^93)(^92^8E)(^91=0)(^93=1)]
<(9A=2)(98=61b34196)>[2:m(^9C=2)(^90=2)(^92^98)(^91=0)(^93=1)]
<(A4=3)(AC=61b4a6fd)>[3:m(^9C=3)(^90=3)(^92^AC)(^91=0)(^93=1)]

<(9B=91)(88=American Lynx <american.lynx@gmx.de>)(89
  ="Rybalka, Mariia" <mariia.rybalka@fkie.fraunhofer.de>)(8B=Paper stuff)
  (8C=72095a19-ffc6-f0c4-2323-c582b514c1f7@gmx.de)(8D
    =<5ea51904-8e52-c614-0d26-85b6512d2bda@fkie.fraunhofer.de>)(8F=UTF-8)
  (90=3aa)(92=ffffffff)(9C=3fd)(9D=1a)(A1=28)(87=)(B9=0|Rybalka, Mariia)
  (94=Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>)(95
    =Timelining stuff)(96=d05604e7-b8fe-d7a9-c8f2-a591f0bb6e3d@gmx.de)
  (97=<edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>)(99=37f)
  (9E=1021)(9F=3d2)(A0=21)(BA=0|Martin Lambertz)(B0=10000081)(A8
    =Scottish Fold <american.lynx@gmx.de>)(A9=scottish.fold@protonmail.de)
  (AA=key)(AB=ae47551c-4c8d-5274-f155-9bcba93df846@gmx.de)(B1=d29)(A2=7cf)
  (A3=1999)(AE=d22)(B3=29)(BB=0|scottish.fold@protonmail.de)>
{1:^80 {(k^97:c)(s=9)}
  [1(^88=91)(^82^88)(^85^89)(^81^8B)(^83^8C)(^84^8D)(^B8^8E)(^86^8E)
    (^89=1)(^96^8F)(^87^90)(^9B^92)(^8F^93)(^B9=0)(^9D=0)(^BB=0)(^9E^9C)
    (^8C=1a)(^BC=28)(^BF=)(^8A=0)(^D9^B9)]
  [2(^88=91)(^82^88)(^85^94)(^81^95)(^83^96)(^84^97)(^B8^98)(^86^98)
   …
```

email addresses

subjects

message IDs

„non-empty" msf

MBOX files

Hochschule Bonn-Rhein-Sieg

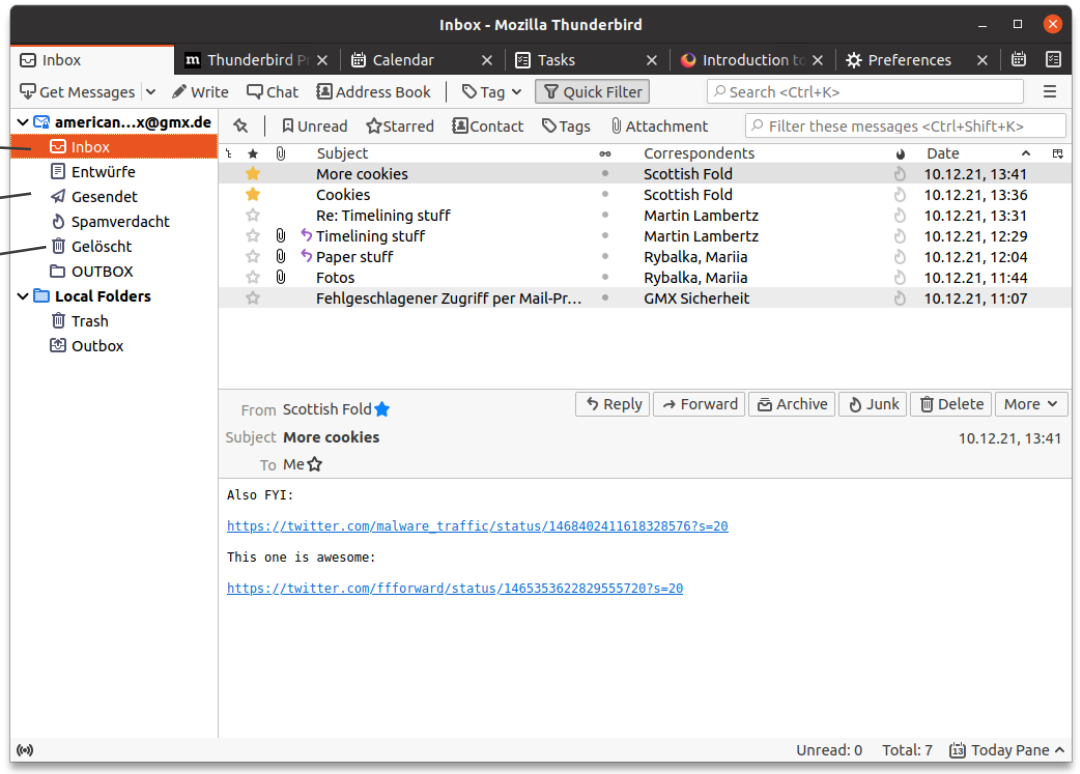
Fraunhofer FKIE

Single MBOX file contain all emails of certain non-empty folder: *inbox*, *sent*, *trash*, *spam*, etc… as a plain text.

INBOX mbox

Gesendet mbox

Gelöscht mbox



Hochschule Bonn-Rhein-Sieg

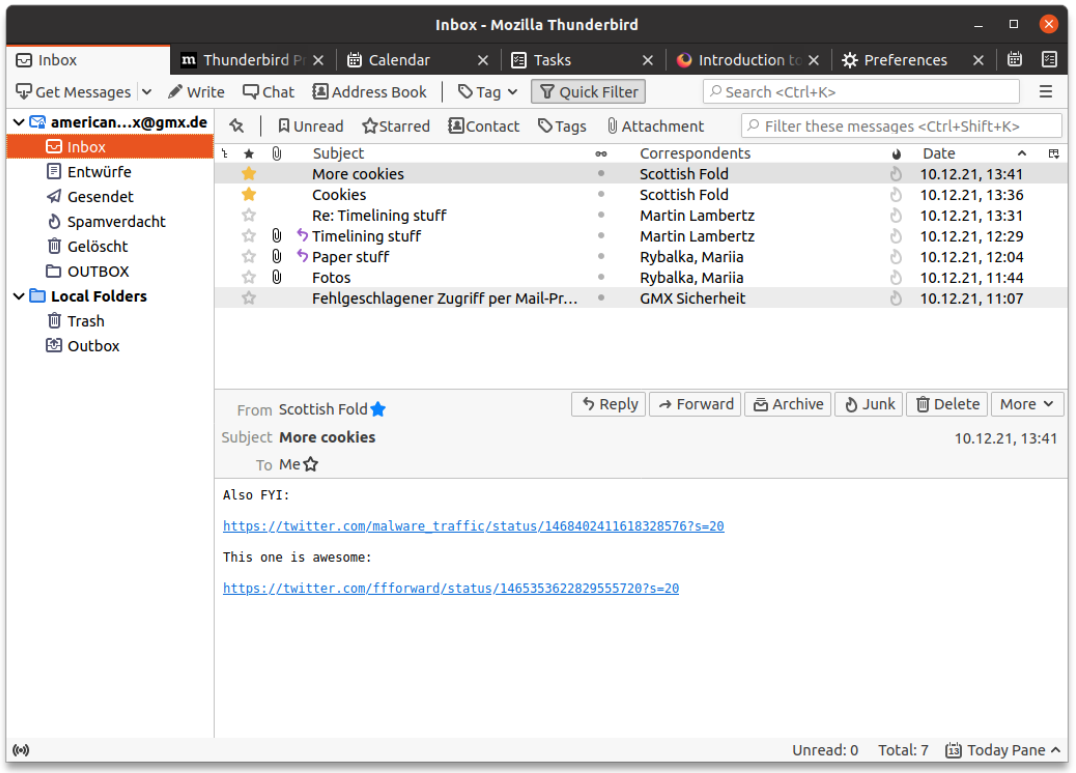
Fraunhofer FKIE

MBOX files

Single MBOX file contain all emails of certain non-empty folder: *inbox*, *sent*, *trash*, *spam*, etc… as a plain text.

E.g. INBOX mbox file contains pro email:

- Complete email headers (each SMTP server contributes :D)
- To and From email addresses
- Subjects
- Actual text/html messages
- Attachments



Hochschule Bonn-Rhein-Sieg

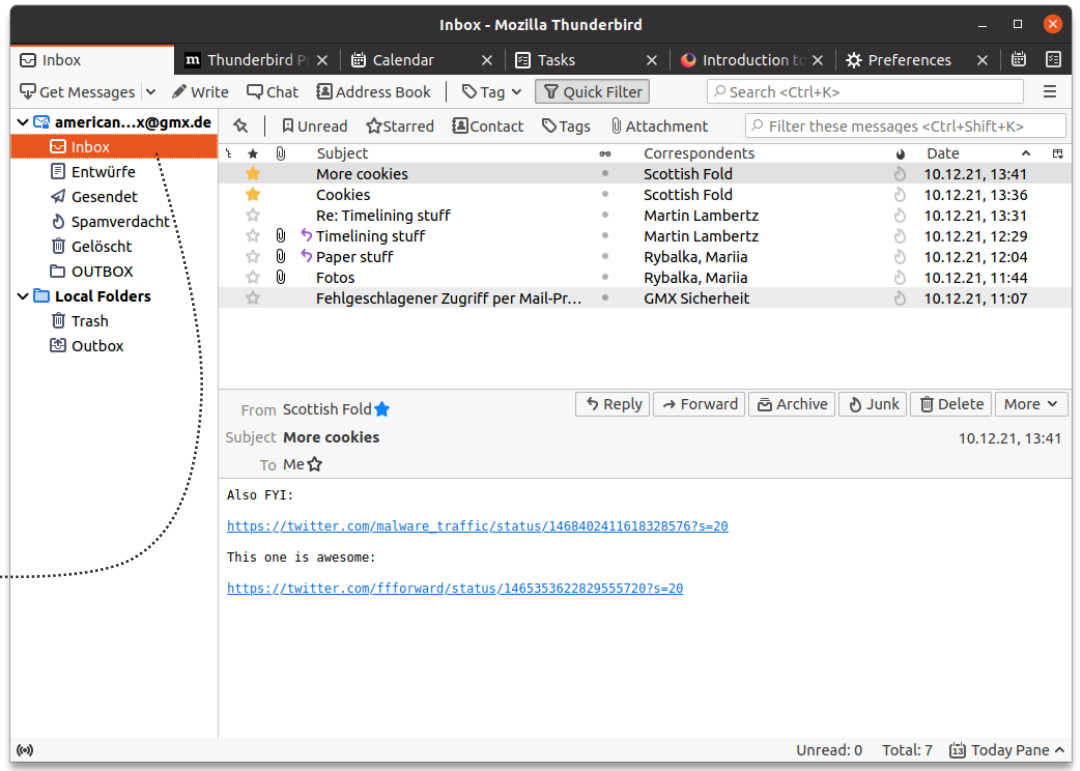
Fraunhofer FKIE

MBOX files

Single MBOX file contain **all** emails of certain **non-empty** folder: *inbox, sent, trash, spam,* etc… as a plain text.

E.g. INBOX mbox file contains pro email:

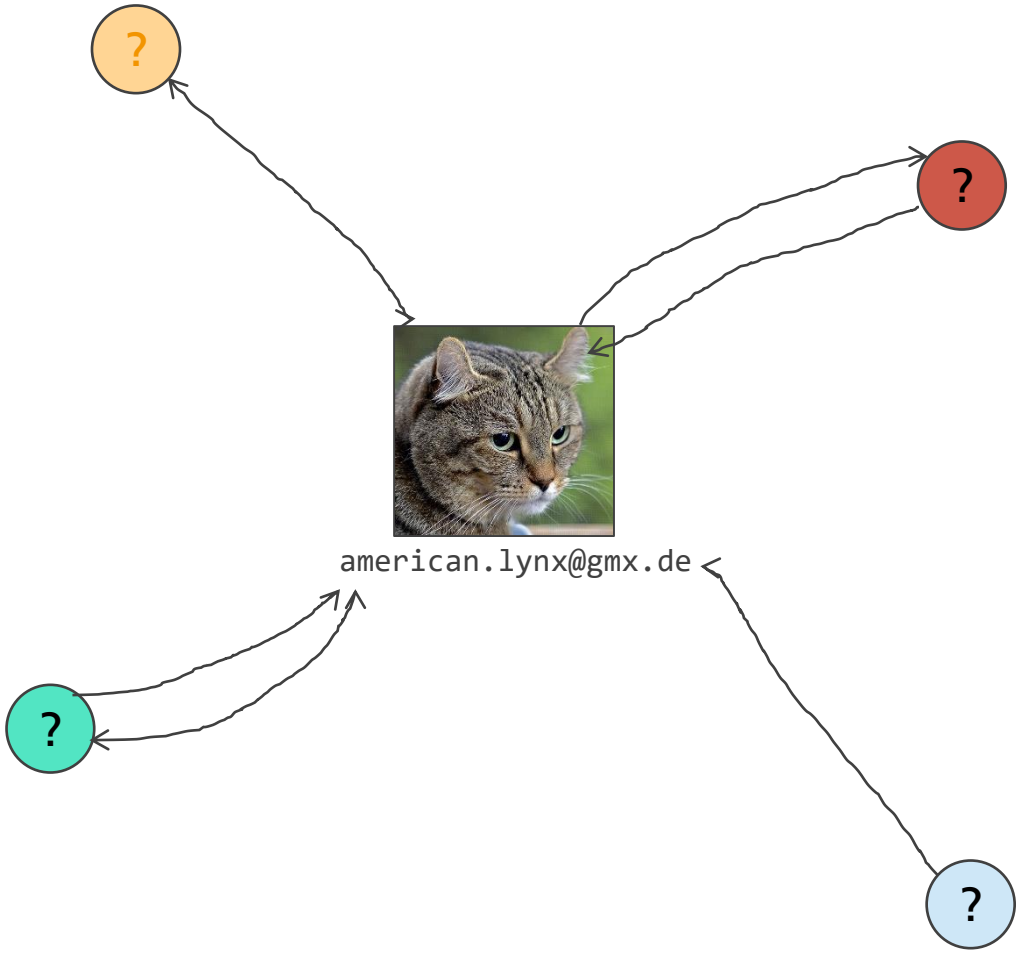
- Complete email headers (each SMTP server contributes :D)
- To and From email addresses
- Subjects
- Actual text/html messages
- Attachments



108733 lines

mbox files can reach Gbs-sizes on „real“ system

Who is sending mails?



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Small header sample

```
$ cat INBOX
```

```
Return-Path: <scottish.fold.42@protonmail.com>
Authentication-Results:  mqgmx120.server.lan; dkim=pass header.i=@protonmail.com
Received: from mail-4325.protonmail.ch ([185.70.43.25]) by mx-ha.gmx.net           # Received: chain of mailservers delivering the message
 (mxgmx114 [212.227.17.5]) with ESMTPS (Nemesis) id 1Mdtz4-1mN9rc3xZu-00b36B       # received by mailserver-X from mailserver-Y
Date: Fri, 10 Dec 2021 12:36:28 +0000                                             # date, set by sender
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=protonmail.com;
            s=protonmail2; t=1639139790;
            bh=CVDwi3csKytDLOEwHXadk0NhM0ihB4+i1VKEDkZBsqY=;
            h=Date:To:From:Reply-To:Subject:Message-ID:From:To:Cc;
            b=AEc1LTgaOWfCKzfT8AJk0X/y30g3dvV6kkYKwtv95Ni9/9cIe94mRX/OISYNaiELS
             vLYKGuZqqzNa8/rb3owntWAy0mhFCYI6+c3PqZNMd9p+A/GjLSfOcgk8l0jJtKujvR
…
To: "american.lynx@gmx.de" <american.lynx@gmx.de>                                  # recipient
From: Scottish Fold <scottish.fold.42@protonmail.com>                             # sender
Reply-To: Scottish Fold <scottish.fold.42@protonmail.com>
Subject: Cookies                                                                  # subject of the message; unique message id
Message-ID: <xb8Q7sVM_AVat62xXVMXlsnt7C8VWxESjdSQNCHqkhBgZ_2KHmRlc9bQcEJbHO4hpnQfdRz11q1_RpJlQboHYLL08J0YKCDlMyb04wsjPNQ=@protonmail.com>
MIME-Version: 1.0
Content-Type: text/plain; charset=utf-8
Content-Transfer-Encoding: quoted-printable
X-Spam-Status: No, score=-0.7 required=10.0 tests=ALL_TRUSTED,DKIM_SIGNED,       # extention or exprimental; store extra infos, non-manadatory
            DKIM_VALID,DKIM_VALID_AU,DKIM_VALID_EF,FREEMAIL_ENVFROM_END_DIGIT,
            FREEMAIL_FROM,FREEMAIL_REPLYTO_END_DIGIT shortcircuit=no
            autolearn=disabled version=3.4.4
X-Spam-Checker-Version: SpamAssassin 3.4.4 (2020-01-24) on                        # extention or expreimental; store extra infos, non-manadatory
            mailout.protonmail.ch
…
Hey!                                                                              # actual message

Have you already noticed this one:
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Who is sending mails?

martin.lambertz@fkie.fraunhofer.de

scottish.fold@protonmail.de

american.lynx@gmx.de

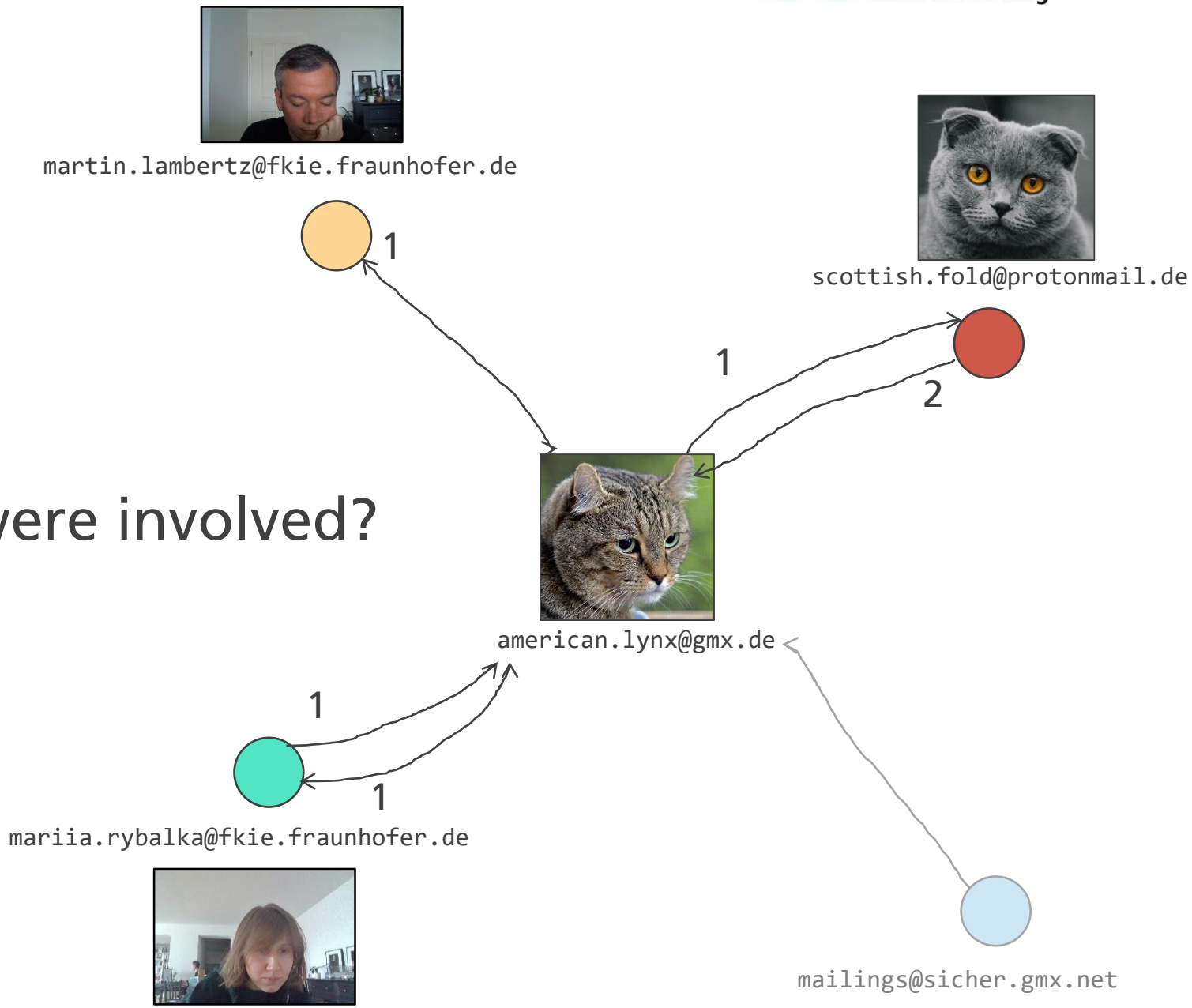
mariia.rybalka@fkie.fraunhofer.de

mailings@sicher.gmx.net

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Which mail servers were involved?



Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Not so-small header sample

```
$ cat INBOX
```

```
Return-Path: <martin.lambertz@fkie.fraunhofer.de>
Authentication-Results:  mqgmx130.server.lan; dkim=pass header.i=@fkie.fraunhofer.de
Received: from mail-edgeKA27.fraunhofer.de ([153.96.1.27]) by mx-ha.gmx.net
 (mxgmx114 [212.227.17.5]) with ESMTPS (Nemesis) id 1Mf22s-1mJoAo3QcM-00gWRh
…
Received: from mail-mtaka28.fraunhofer.de ([153.96.1.28])
  by mail-edgeKA27.fraunhofer.de with ESMTP/TLS/ECDHE-RSA-AES256-GCM-SHA384; 10 Dec 2021 12:29:55 +0100
…
Received: from mailguard.fkie.fraunhofer.de (HELO a.mx.fkie.fraunhofer.de) ([128.7.3.5])
  by mail-mtaKA28.fraunhofer.de with ESMTP/TLS/ECDHE-RSA-AES256-GCM-SHA384; 10 Dec 2021 12:29:49 +0100
…
Received: from srv-mailhost-b.fkie.fraunhofer.de ([128.7.10.131])
          by a.mx.fkie.fraunhofer.de with esmtps (TLS1.2:ECDHE_RSA_AES_256_GCM_SHA384:256)
…
Received: from srv-mail-03.fkie.fraunhofer.de ([128.7.11.18] helo=srv-mail-03.gaia.fkie.fraunhofer.de)
          by srv-mailhost-b.fkie.fraunhofer.de with esmtps (TLS1.2:ECDHE_RSA_AES_256_CBC_SHA1:256)
…
Received: from [10.69.133.172] (128.7.89.212) by
 srv-mail-03.gaia.fkie.fraunhofer.de (128.7.11.18) with Microsoft SMTP Server
 (TLS) id 15.0.1497.26; Fri, 10 Dec 2021 12:29:46 +0100
Content-Type: multipart/mixed;
          boundary="------------0vuRhiwvAwvcvyAnLVOD0qA4"
Message-ID: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
Date: Fri, 10 Dec 2021 12:29:45 +0100
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Thunderbird/91.3.2
Content-Language: de-DE
To: <american.lynx@gmx.de>
From: Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>
Subject: Timelining stuff
Organization: Fraunhofer FKIE
X-Originating-IP: [128.7.89.212]
X-ClientProxiedBy: srv-mail-01.gaia.fkie.fraunhofer.de (128.7.11.16) To
 srv-mail-03.gaia.fkie.fraunhofer.de (128.7.11.18)
```

added by server F

added by server E

added by server D

added by server C

added by server B

added by server A

original header

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Not-so-small header sample


```
$ cat INBOX
```

```
Return-Path: <martin.lambertz@fkie.fraunhofer.de>
Authentication-Results:  mqgmx130.server.lan; dkim=pass header.i=@fkie.fraunhofer.de
Received: from mail-edgeKA27.fraunhofer.de ([153.96.1.27]) by mx-ha.gmx.net
 (mxgmx114 [212.227.17.5]) with ESMTPS (Nemesis) id 1Mf22s-1mJoAo3QcM-00gWRh
…
Received: from mail-mtaka28.fraunhofer.de ([153.96.1.28])
  by mail-edgeKA27.fraunhofer.de with ESMTP/TLS/ECDHE-RSA-AES256-GCM-SHA384; 10 Dec 2021 12:29:55 +0100
…
Received: from mailguard.fkie.fraunhofer.de (HELO a.mx.fkie.fraunhofer.de) ([128.7.3.5])
  by mail-mtaKA28.fraunhofer.de with ESMTP/TLS/ECDHE-RSA-AES256-GCM-SHA384; 10 Dec 2021 12:29:49 +0100
…
Received: from srv-mailhost-b.fkie.fraunhofer.de ([128.7.10.131])
            by a.mx.fkie.fraunhofer.de with esmtps (TLS1.2:ECDHE_RSA_AES_256_GCM_SHA384:256)
…
Received: from srv-mail-03.fkie.fraunhofer.de ([128.7.11.18] helo=srv-mail-03.gaia.fkie.fraunhofer.de)
            by srv-mailhost-b.fkie.fraunhofer.de with esmtps (TLS1.2:ECDHE_RSA_AES_256_CBC_SHA1:256)
…
Received: from [10.69.133.172] (128.7.89.212) by
 srv-mail-03.gaia.fkie.fraunhofer.de (128.7.11.18) with Microsoft SMTP Server
 (TLS) id 15.0.1497.26; Fri, 10 Dec 2021 12:29:46 +0100
Content-Type: multipart/mixed;
            boundary="------------0vuRhiwvAwvcvyAnLVOD0qA4"
Message-ID: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
Date: Fri, 10 Dec 2021 12:29:45 +0100
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Thunderbird/91.3.2
Content-Language: de-DE
To: <american.lynx@gmx.de>
From: Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>
Subject: Timelining stuff
Organization: Fraunhofer FKIE
X-Originating-IP: [128.7.89.212]
X-ClientProxiedBy: srv-mail-01.gaia.fkie.fraunhofer.de (128.7.11.16) To
 srv-mail-03.gaia.fkie.fraunhofer.de (128.7.11.18)
```

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Not so-small header sample

```
$ cat INBOX
```

```
Return-Path: <martin.lambertz@fkie.fraunhofer.de>
Authentication-Results:  mqgmx130.server.lan; dkim=pass header.i=@fkie.fraunhofer.de
Received: from mail-edgeKA27.fraunhofer.de ([153.96.1.27]) by mx-ha.gmx.net
 (mxgmx114 [212.227.17.5]) with ESMTPS (Nemesis) id 1Mf22s-1mJoAo3QcM-00gWRh
…
Received: from mail-mtaka28.fraunhofer.de ([153.96.1.28])
  by mail-edgeKA27.fraunhofer.de with ESMTP/TLS/ECDHE-RSA-AES256-GCM-SHA384; 10 Dec 2021 12:29:55 +0100
…
Received: from mailguard.fkie.fraunhofer.de (HELO a.mx.fkie.fraunhofer.de) ([128.7.3.5])
  by mail-mtaKA28.fraunhofer.de with ESMTP/TLS/ECDHE-RSA-AES256-GCM-SHA384; 10 Dec 2021 12:29:49 +0100
…
Received: from srv-mailhost-b.fkie.fraunhofer.de ([128.7.10.131])
          by a.mx.fkie.fraunhofer.de with esmtps (TLS1.2:ECDHE_RSA_AES_256_GCM_SHA384:256)
…
Received: from srv-mail-03.fkie.fraunhofer.de ([128.7.11.18] helo=srv-mail-03.gaia.fkie.fraunhofer.de)
          by srv-mailhost-b.fkie.fraunhofer.de with esmtps (TLS1.2:ECDHE_RSA_AES_256_CBC_SHA1:256)
…
Received: from [10.69.133.172] (128.7.89.212) by
 srv-mail-03.gaia.fkie.fraunhofer.de (128.7.11.18) with Microsoft SMTP Server
 (TLS) id 15.0.1497.26; Fri, 10 Dec 2021 12:29:46 +0100
Content-Type: multipart/mixed;
          boundary="------------0vuRhiwvAwvcvyAnLVOD0qA4"
Message-ID: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
Date: Fri, 10 Dec 2021 12:29:45 +0100
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101 Thunderbird/91.3.2
Content-Language: de-DE
To: <american.lynx@gmx.de>
From: Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>
Subject: Timelining stuff
Organization: Fraunhofer FKIE
X-Originating-IP: [128.7.89.212]
X-ClientProxiedBy: srv-mail-01.gaia.fkie.fraunhofer.de (128.7.11.16) To
 srv-mail-03.gaia.fkie.fraunhofer.de (128.7.11.18)
```

originating IP

mail client that sent the message.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Content

message contains contents of different type (probably with attachment)

separates blocks of content

body-block, text

attachment-block, pdf

```
$ cat INBOX
Content-Type: multipart/mixed;
boundary="------------0vuRhiwvAwvcvyAnLVOD0qA4"
Message-ID: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
Date: Fri, 10 Dec 2021 12:29:45 +0100
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Thunderbird/91.3.2
Content-Language: de-DE
To: <american.lynx@gmx.de>
From: Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>
Subject: Timelining stuff
Organization: Fraunhofer FKIE
X-Originating-IP: [128.7.89.212]
…
--------------0vuRhiwvAwvcvyAnLVOD0qA4
Content-Type: text/plain; charset="UTF-8"; format=flowed
Content-Transfer-Encoding: 7bit

Here is the timlining material you asked for.

https://www.sans.org/blog/digital-forensic-sifting-super-timeline-creation-using-log2timeline/

Best,
Martin
--------------0vuRhiwvAwvcvyAnLVOD0qA4
Content-Type: application/pdf;
             name="Mastering the Super Timeline With log2timeline.pdf"
Content-Disposition: attachment;
             filename="Mastering the Super Timeline With log2timeline.pdf"
Content-Transfer-Encoding: base64

JVBERi0xLjMKMSAwIG9iago8PAovVHlwZSAvUGFnZXMKL0NvdW50IDgzCi9LaWRzIFsgMyAw
IFIgNCAwIFIgNSAwIFIgNiAwIFIgNyAwIFIgOCAwIFIgOSAwIFIgMTAgMCBSIDExIDAgUiAx
MiAwIFIgMTMgMCBSIDE0IDAgUiAxNSAwIFIgMTYgMCBSIDE3IDAgUiAxOCAwIFIgMTkgMCBS
…
YWlsZXIKPDwKL1NpemUgMzEyCi9Sb290IDg2IDAgUgovSW5mbyAyIDAgUgo+PgpzdGFydHhy
ZWYKNDI1MjQ1NwolJUVPRgo=
--------------0vuRhiwvAwvcvyAnLVOD0qA4--
```

Attachments

```
$ cat INBOX
Content-Type: multipart/mixed;
boundary="------------0vuRhiwvAwvcvyAnLVOD0qA4"
Message-ID: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
Date: Fri, 10 Dec 2021 12:29:45 +0100
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Thunderbird/91.3.2
Content-Language: de-DE
To: <american.lynx@gmx.de>
From: Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>
Subject: Timelining stuff
Organization: Fraunhofer FKIE
X-Originating-IP: [128.7.89.212]
…
--------------0vuRhiwvAwvcvyAnLVOD0qA4
Content-Type: text/plain; charset="UTF-8"; format=flowed
Content-Transfer-Encoding: 7bit

Here is the timlining material you asked for.

https://www.sans.org/blog/digital-forensic-sifting-super-timeline-creation-using-log2timeline/

Best,
Martin
--------------0vuRhiwvAwvcvyAnLVOD0qA4
Content-Type: application/pdf;
            name="Mastering the Super Timeline With log2timeline.pdf"
Content-Disposition: attachment;
            filename="Mastering the Super Timeline With log2timeline.pdf"
Content-Transfer-Encoding: base64

JVBERi0xLjMKMSAwIG9iago8PAovVHlwZSAvUGFnZXMKL0NvdW50IDgzCi9LaWRzIFsgMyAw
IFIgNCAwIFIgNSAwIFIgNiAwIFIgNyAwIFIgOCAwIFIgOSAwIFIgMTAgMCBSIDExIDAgUiAx
MiAwIFIgMTMgMCBSIDE0IDAgUiAxNSAwIFIgMTYgMCBSIDE3IDAgUiAxOCAwIFIgMTkgMCBS
…
YWlsZXIKPDwKL1NpemUgMzEyCi9Sb290IDg2IDAgUgovSW5mbyAyIDAgUgo+PgpzdGFydHhy
ZWYKNDI1MjQ1NwolJUVPRgo=
--------------0vuRhiwvAwvcvyAnLVOD0qA4--
```

Type of attachment (image, application, etc.)

attachment filename

binary data ist (base64,…) encoded

Content of the pdf file (base64 encoded)

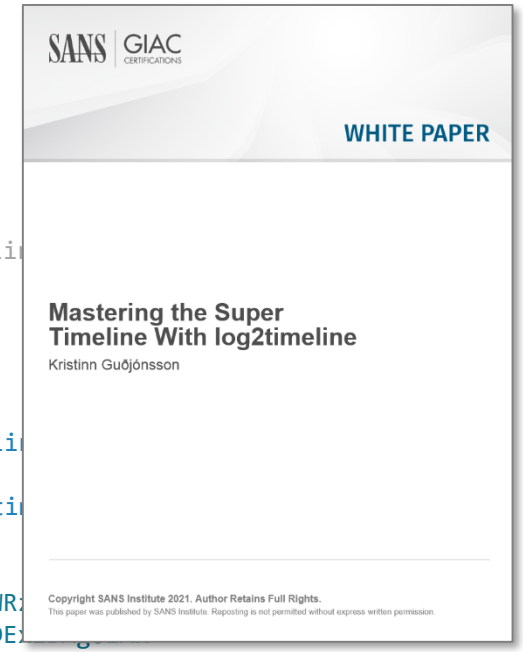
78867 lines total

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Attachments

```
$ cat INBOX
Content-Type: multipart/mixed;
boundary="------------0vuRhiwvAwvcvyAnLVOD0qA4"
Message-ID: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
Date: Fri, 10 Dec 2021 12:29:45 +0100
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Thunderbird/91.3.2
Content-Language: de-DE
To: <american.lynx@gmx.de>
From: Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>
Subject: Timelining stuff
Organization: Fraunhofer FKIE
X-Originating-IP: [128.7.89.212]
…
--------------0vuRhiwvAwvcvyAnLVOD0qA4
Content-Type: text/plain; charset="UTF-8"; format=flowed
Content-Transfer-Encoding: 7bit

Here is the timlining material you asked for.

https://www.sans.org/blog/digital-forensic-sifting-super-timeli

Best,
Martin
--------------0vuRhiwvAwvcvyAnLVOD0qA4
Content-Type: application/pdf;
             name="Mastering the Super Timeline With log2timeli
Content-Disposition: attachment;
             filename="Mastering the Super Timeline With log2ti
Content-Transfer-Encoding: base64

JVBERi0xLjMKMSAwIG9iago8PAovVHlwZSAvUGFnZXMKL0NvdW50IDgzCi9LaWR
IFIgNCAwIFIgNSAwIFIgNiAwIFIgNyAwIFIgOCAwIFIgOSAwIFIgMTAgMCBSIDE
MiAwIFIgMTMgMCBSIDE0IDAgUiAxNSAwIFIgMTYgMCBSIDE3IDAgUiAxOCAwIFIgMTkgMCBS
…
YWlsZXIKPDwKL1NpemUgMzEyCi9Sb290IDg2IDAgUgovSW5mbyAyIDAgUgo+PgpzdGFydHhy
ZWYKNDI1MjQ1NwolJUVPRgo=
--------------0vuRhiwvAwvcvyAnLVOD0qA4--
```



78867 lines total

Type of attachment (image, application, etc.)

attachment filename

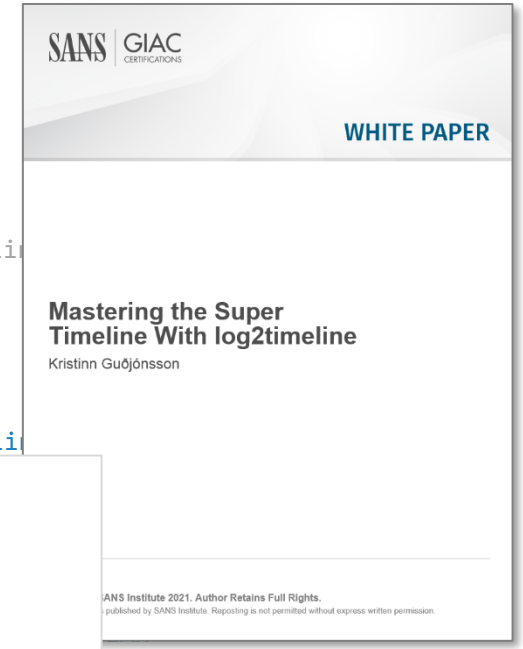
binary data ist (base64,…) encoded

Content of the pdf file (base64 encoded)

Attachments

```
$ cat INBOX
```

```
Content-Type: multipart/mixed;
boundary="------------0vuRhiwvAwvcvyAnLVOD0qA4"
Message-ID: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
Date: Fri, 10 Dec 2021 12:29:45 +0100
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Thunderbird/91.3.2
Content-Language: de-DE
To: <american.lynx@gmx.de>
From: Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>
Subject: Timelining stuff
Organization: Fraunhofer FKIE
X-Originating-IP: [128.7.89.212]
…
--------------0vuRhiwvAwvcvyAnLVOD0qA4
Content-Type: text/plain; charset="UTF-8"; format=flowed
Content-Transfer-Encoding: 7bit

Here is the timlining material you asked for.

https://www.sans.org/blog/digital-forensic-sifting-super-timeli

Best,
Martin
--------------0vuRhiwvAwvcvyAnLVOD0qA4
Content-Type: application/pdf;
              name="Mastering the Super Timeline With log2timeli
```




```
--------------WLIKraU5i4xNPiSeC4B55Jku
Content-Type: image/jpeg; name="lynx1.jpg"
Content-Disposition: attachment; filename="lynx1.jpg"
Content-Transfer-Encoding: base64

/9j/4AAQSkZJRgABAQAAAQABAAD/2wBDAAgFBQUGBQgGBggLBwYHCw0KCAgKDQ8MDA0MDA8R
DA0NDQ0MEQ8REhMSEQ8XFxkZFxciISEhIiYmJiYmJiYmJib/2wBDAQgJCRAOEB0UFB0gGhUa
ICYmJiYmJiYmJiYmJiYmJiYmJiYmJiYmJiYmJiYmJiYmJiYmJiYmJiYmJib/wgAR
CAKKBLADABEAAREBAhEB/8QAGwAAAgMBAQEAAAAAAAAAAAAAAQIAAwQFBgf/xAAYAQEBAQEB
AAAAAAAAAAAAAAAAAQIDBP/aAAwDAAABEAIQAAAB8/yzKASEWBgktEhCNDQ6GICoCgKq6oEo
…
```

78867 lines total

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Sent: reply

```
$ cat Gesendet
```

```
Message-ID: <d05604e7-b8fe-d7a9-c8f2-a591f0bb6e3d@gmx.de>
Date: Fri, 10 Dec 2021 13:01:26 +0100
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:91.0) Gecko/20100101
 Thunderbird/91.4.0
Subject: Re: Timelining stuff
To: Martin Lambertz <martin.lambertz@fkie.fraunhofer.de>
References: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
From: American Lynx <american.lynx@gmx.de>
In-Reply-To: <edfc9ed9-9290-b1f9-dcae-3754dfdb4af7@fkie.fraunhofer.de>
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit

Hi Martin,

Am 10/12/2021 um 12:29 schrieb Martin Lambertz:
> Here is the timlining material you asked for.
>
> https://www.sans.org/blog/digital-forensic-sifting-super-timeline-creation-using-log2timeline/

thanks a lot for the link!

Best regards,
Lynx

P.S. You made a typo in "timlining'. XD
```

ID of message on which this message replies

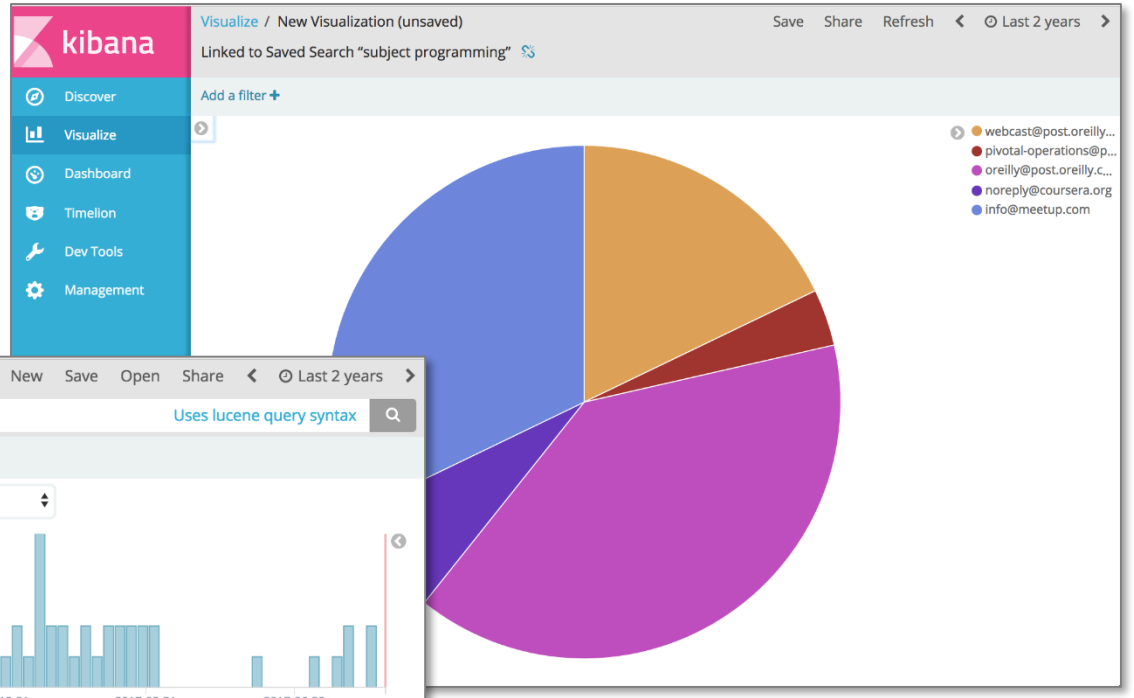
original message (chain) parts if not deleted by sender

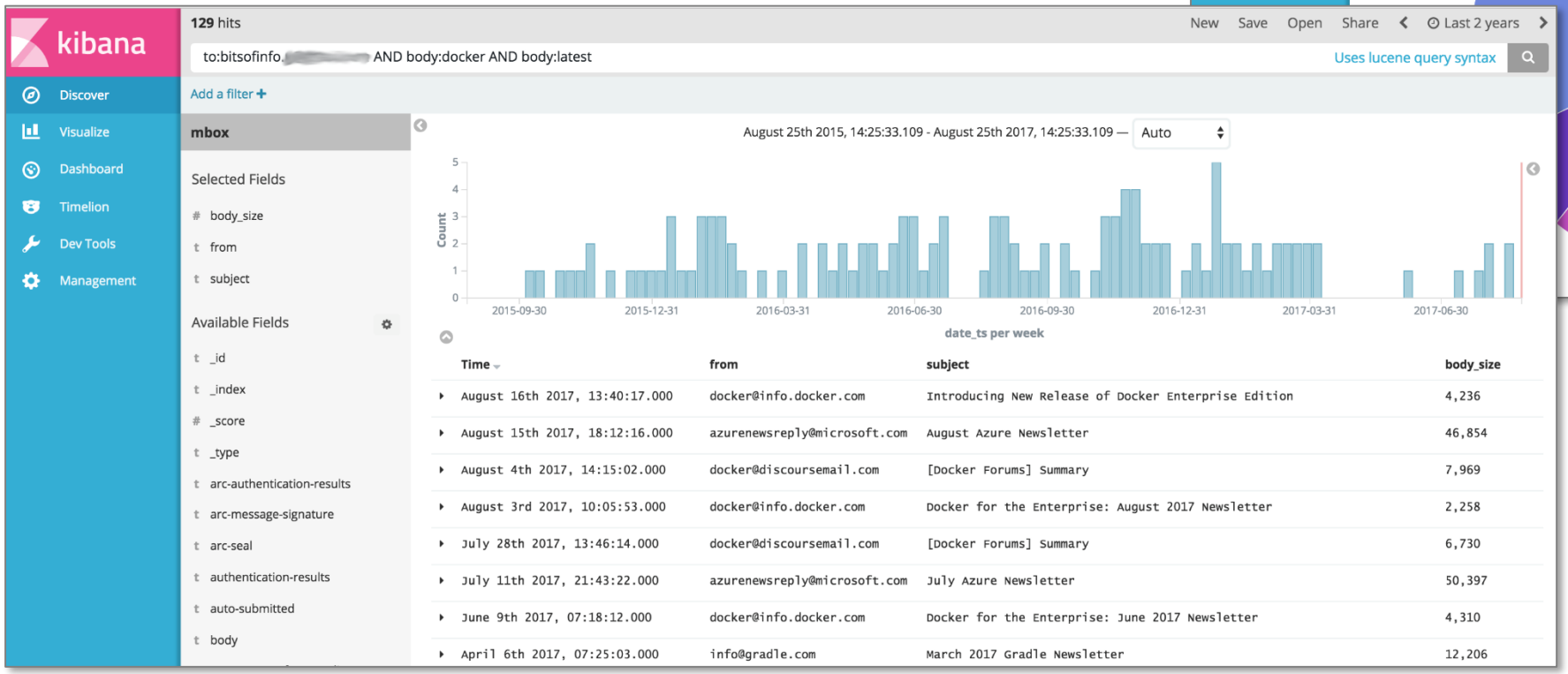
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Content

Fulltext search on mail content



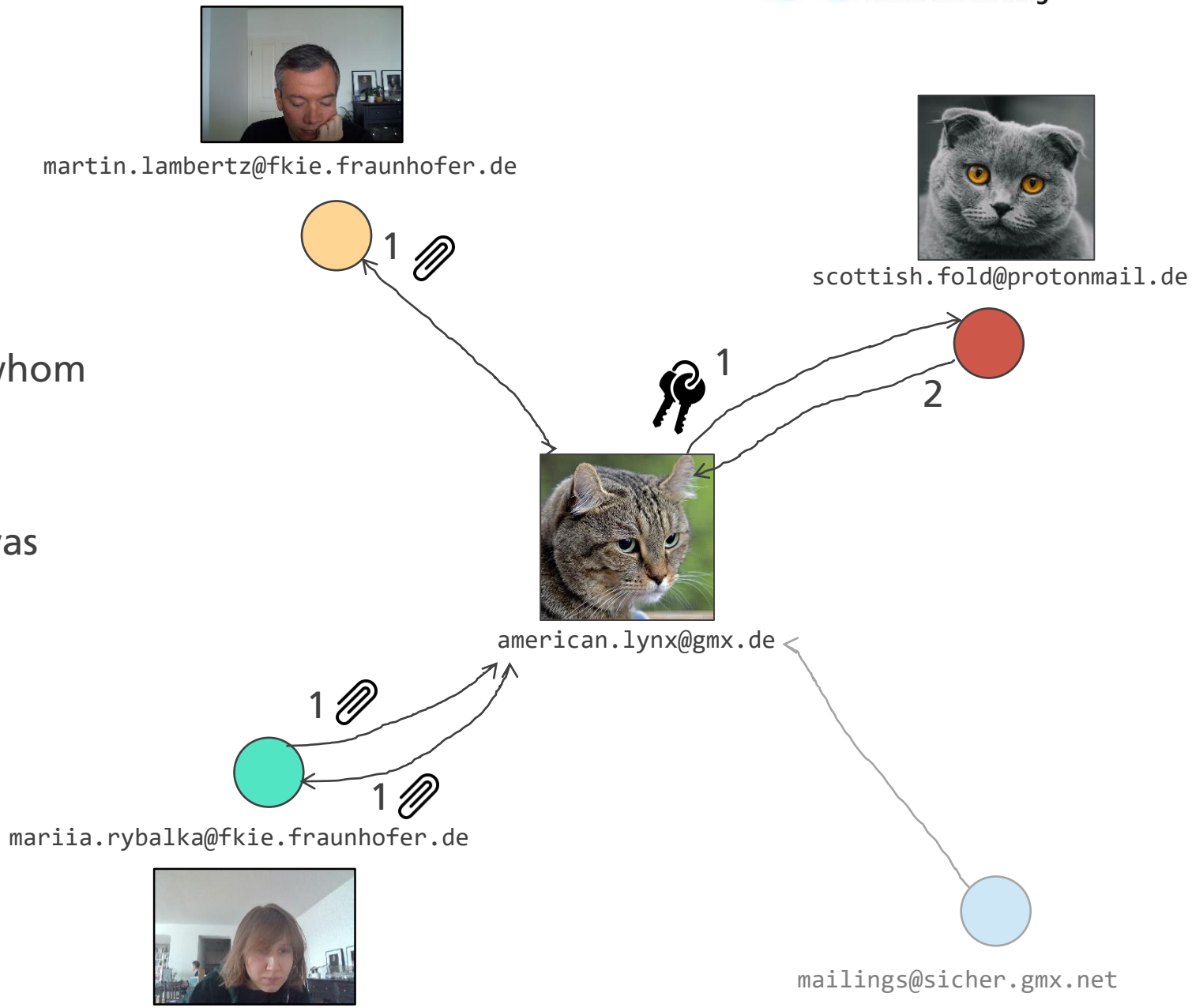


comms-analyzer-toolbox

[https://github.com/bitsofinfo/comms-analyzer-toolbox]

Can we find out more about whom a user is communicating with?

Or about what the user is or was doing?



Thunderbird

message contents

attachments

email headers

communications

address book

SQLite

account passwords & private keys

calender

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Address Book

…/profile-name/abook.sqlite

uid	localId
Filtern	Filtern
e98f7e5c-ce32-493b-88d3-…	1
0e0ef53d-1ade-4ff2-9ab9-1c4bff5…	2
ca0c8562-d920-42e1-…	3

cards

contact's card

name

email address

card	name	value
Filtern	Filtern	Filtern
e98f7e5c-ce32-493b-88d3-…	PreferMailFormat	0
e98f7e5c-ce32-493b-88d3-…	PopularityIndex	0
e98f7e5c-ce32-493b-88d3-…	DisplayName	Scottish Fold
e98f7e5c-ce32-493b-88d3-…	PrimaryEmail	scottish.fold.42@protonmail.com
e98f7e5c-ce32-493b-88d3-…	LastModifiedDate	1639255191
0e0ef53d-1ade-4ff2-9ab9-1c4bff5…	PreferMailFormat	0
0e0ef53d-1ade-4ff2-9ab9-1c4bff5…	PopularityIndex	0
0e0ef53d-1ade-4ff2-9ab9-1c4bff5…	DisplayName	Martin Lambertz
0e0ef53d-1ade-4ff2-9ab9-1c4bff5…	PrimaryEmail	martin.lambertz@fkie.fraunhofer…
0e0ef53d-1ade-4ff2-9ab9-1c4bff5…	LastModifiedDate	1639255427
ca0c8562-d920-42e1-…	PreferMailFormat	0
ca0c8562-d920-42e1-…	PopularityIndex	0
ca0c8562-d920-42e1-…	DisplayName	Rybalka, Mariia
ca0c8562-d920-42e1-…	PrimaryEmail	mariia.rybalka@fkie.fraunhofer.…
ca0c8562-d920-42e1-…	LastModifiedDate	1639255431

properties

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Calender

```
PS …> tree
├── calendar-data
│   ├── cache.sqlite
│   ├── deleted.sqlite
│   └── local.sqlite
…
```

calender synchronized with server

local, profile-only calender

```
select title,
       datetime(event_start/1000000, 'unixepoch') as start,
       datetime(event_end/1000000, 'unixepoch') as end,
       event_start_tz as timezone,
       datetime(time_created/1000000, 'unixepoch') as created,
       datetime(last_modified/1000000, 'unixepoch') as modified
from cal_events;
```

cal_events table

title	start	end	timezone	created	modified
Student Meeting (Max)	2021-12-09 14:00:00	2021-12-09 15:00:00	Europe/Brussels	NULL	NULL
Team Meeting	2021-12-06 08:00:00	2021-12-06 09:00:00	Europe/Brussels	NULL	NULL
Forensics Lecture	2021-12-07 12:30:00	2021-12-07 14:00:00	Europe/Brussels	NULL	NULL
Team Meeting	2021-12-13 08:00:00	2021-12-13 09:00:00	Europe/Berlin	2021-12-11 18:28:10	2021-12-11 18:28:28

cal_events table

title	start	end	timezone	created	modified
Important	2021-12-16 10:15:00	2021-12-16 11:15:00	Europe/Berlin	2021-12-11 18:29:12	2021-12-11 18:29:36
Very important	2021-12-21 00:00:00	2021-12-22 00:00:00	floating	2021-12-11 20:44:29	2021-12-11 20:44:55

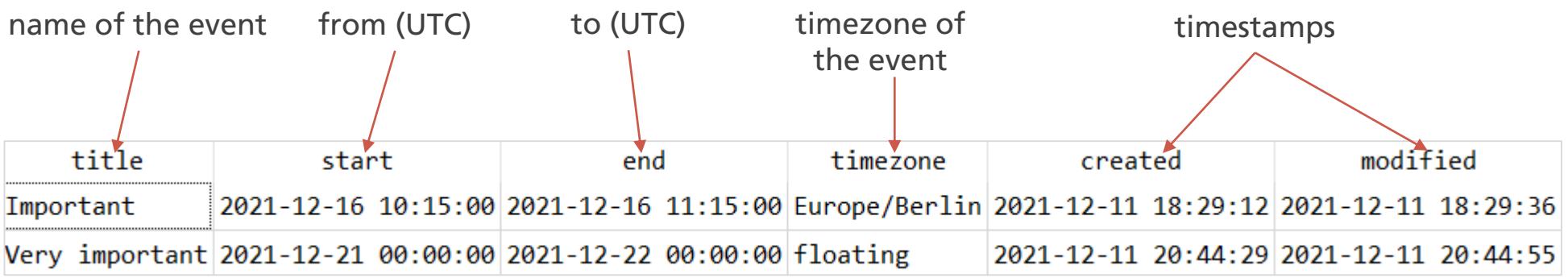
Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Calender

```
PS …> tree
├── calendar-data
│   ├── cache.sqlite
│   ├── deleted.sqlite
│   └── local.sqlite
…
```

```
select title,
       datetime(event_start/1000000, 'unixepoch') as start,
       datetime(event_end/1000000, 'unixepoch') as end,
       event_start_tz as timezone,
       datetime(time_created/1000000, 'unixepoch') as created,
       datetime(last_modified/1000000, 'unixepoch') as modified
from cal_events;
```



title	start	end	timezone	created	modified
Important	2021-12-16 10:15:00	2021-12-16 11:15:00	Europe/Berlin	2021-12-11 18:29:12	2021-12-11 18:29:36
Very important	2021-12-21 00:00:00	2021-12-22 00:00:00	floating	2021-12-11 20:44:29	2021-12-11 20:44:55

Email clients

message contents

attachments

email headers

communications

address book

account passwords &
private keys

calender

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Account passwords

Account passwords

Thunderbird [Mozilla] generally stores *sensitive infos* encrypted on disc.

`…/profile-name/logins.json` ← For example, saved email account logins

`…/profile-name/key4*.db` ← Data needed for decryption (password, salt, etc.)

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

logins.json


```
{
   "nextId":4,
   "logins":[
      {
         "id":1,
         "hostname":"imap://imap.gmx.net",
         "httpRealm":"imap://imap.gmx.net",
         "formSubmitURL":null,
         "usernameField":"",
         "passwordField":"",
         "encryptedUsername":"MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECEjxZDJlbVFoBBh8w1hzfwKIOyCnqrdWo82uBrhtCcUqGqA=",
         "encryptedPassword":"MEoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECHwEGf1xbZTPBCAu7cnFCg1qdQ7j++fvOTNG4L/vp8Ohiy6ndEc8ES3w7A==",
         "guid":"{80fb1e33-8921-4ede-b369-288d10d58ba8}",
         "encType":1,
         "timeCreated":1639228265021,
         "timeLastUsed":1639228265021,
         "timePasswordChanged":1639228265021,
         "timesUsed":1
      },
      {
         "id":2,
         "hostname":"smtp://mail.gmx.net",
         "httpRealm":"smtp://mail.gmx.net",
         …
         "encryptedUsername":"MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECC5fQ3Pwh27FBBhG8/UTlZ2C5wdfBjOFSHSmVlw7PrpohDE=",
         "encryptedPassword":"MEoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECEhCkYU04jmwBCD198BeDqNPIKScsSllVqfJih0gvSUAsPZ9YxqipM5NIw==",
         …
      },
      {
         "id":3,
         "hostname":"https://caldav.gmx.net",
         "httpRealm":"Service",
         …
         "encryptedUsername":"MEIEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECD2/NwHlEphbBBhxoyl/Y4C3CBRQnt0/4DpGgEEY6OCrVPk=",
         "encryptedPassword":"MEoEEPgAAAAAAAAAAAAAAAAAAAEwFAYIKoZIhvcNAwcECICbN4hn7jgsBCCIpHLDB4FPrwUnPBq7ZoRZUiaNMsx/PNz/u0pqJsIbhw==",
         …
      }
   ],
   "potentiallyVulnerablePasswords":[
```


destination mail server

encrypted email account name

encrypted email account password

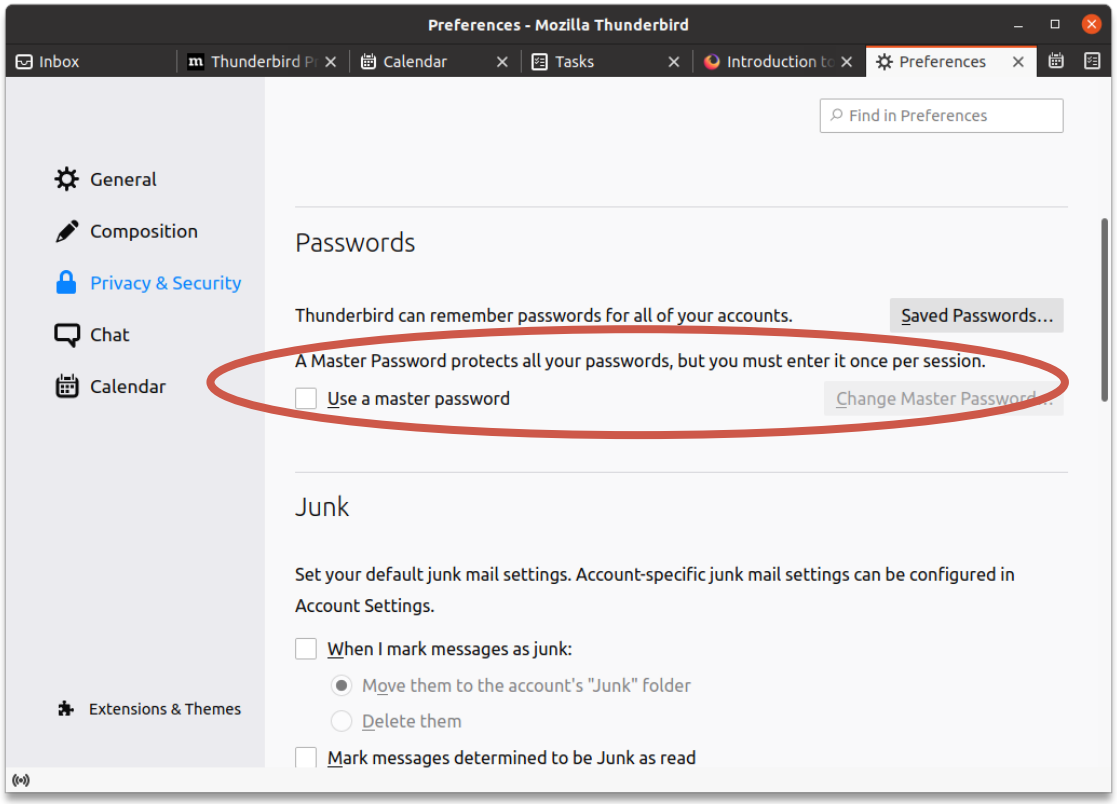
source mail server

mail provider [calender] service

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Sensitive data



…which is not set by default…

key4*.db content is protected by master password.

…/profile-name/logins.json

…/profile-name/key4*.db

…which is also used to protect your private keys – of course, if you set it…

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

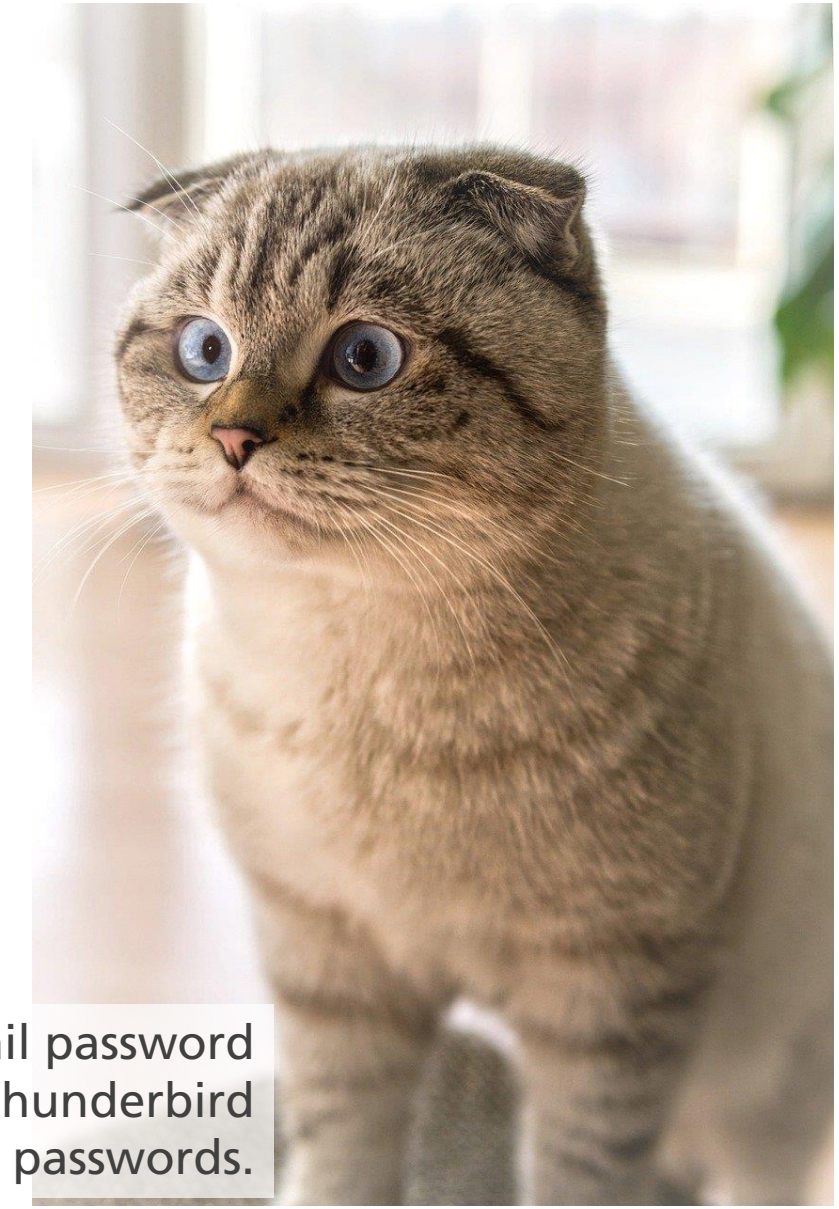
Account passwords

```
$ python firepwd.py -d PATH-TO-PROFILE
```

```
…
decrypting login/password pairs  decrypting login/password pairs
imap://imap.gmx.net:b'american.lynx@gmx.de',b'vZ2gAa9g@T9bPJ7aQswMRG5c'
smtp://mail.gmx.net:b'american.lynx@gmx.de',b'vZ2gAa9g@T9bPJ7aQswMRG5c'
https://caldav.gmx.net:b'american.lynx@gmx.de',b'vZ2gAa9g@T9bPJ7aQswMRG5c'
```

"Firepwd.py, an open source tool to decrypt Mozilla protected passwords"

[https://github.com/lclevy/firepwd]



When you have strong email password but have no idea about thunderbird master passwords.

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Artifacts


OneDrive


VeraCrypt


zoom


STEAM®


KeePass


ownCloud


MySQL™

Hochschule Bonn-Rhein-Sieg

Fraunhofer FKIE

Any Questions?