Browser Artifacts of Google Drive and Gmail

Elizabeth Schweinsberg

Why are we here?

- Uploading information to a personal drive account is a great way to steal insider information
- HTTPS makes it hard to see what “pages” on google.com someone visits
- This is not the easiest way to get this info for enterprise accounts
- I’ve not see this information published, and had to figure out a lot of it on my own

Gen Beringer is at it again

Our favorite BBQ sauce recipe stealing suspect is back at it.

This time, he’s sharing even more recipes and logos with the competitors.

We have a copy of his Chrome Browser History, so let’s see what he’s been up to...

GMail

Open the Inbox @ 0404

```
2017-07-10T04:04:12.079842+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#inbox
(Inbox (15) - genberinger@gmail.com - Gmail) [count: 0]
Host: mail.google.com
Type: [AUTO_BOOKMARK - Got through a suggestion in the UI]
(URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

GMail

Read the Promos tab @ 0405

```
2017-07-10T04:05:12.136710+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#inbox
(Inbox (15) - genberinger@gmail.com - Gmail) [count: 0]
Host: mail.google.com
Type: [LINK - User clicked a link]
(URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

GMail

Read an Email @ 0404

```
2017-07-10T04:04:53.731192+00:00
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#inbox/15d29ce53ec0c642
(New sign-in from Chrome on Mac - genberinger@gmail.com - Gmail) [count: 0]
Host: mail.google.com
Type: [LINK - User clicked a link]
(URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

GMail

Search for “bbq” @ 0408

```
2017-07-10T04:08:06.555745+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#search/bbq
(Search results - genberinger@gmail.com - Gmail) [count: 0]
Host: mail.google.com
Type: [LINK - User clicked a link]
(URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,browser_search
```

GMail

Page through the search results @ 0408

```
2017-07-10T04:08:50.745471+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#search/bbq/p2 [count: 0]
Host: mail.google.com
Type: [LINK - User clicked a link]
(URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,browser_search
```

GMail

View one of the search results @ 0408

```
2017-07-10T04:09:26.788149+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#search/bbq/13fd0c17af27c338
(Conference tomorrow - genberinger@gmail.com - Gmail) [count: 0]
Host: mail.google.com
Type: [LINK - User clicked a link]
(URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,browser_search
```

GMail

Compose a new email from the Inbox @ 0413

```
2017-07-10T04:13:22.273499+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#inbox?compose=new [count: 0]
Host: mail.google.com
Visit from: https://mail.google.com/mail/u/0/#inbox
(Inbox (15) - genberinger@gmail.com - Gmail)
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-

2017-07-10T04:13:46.509807+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#inbox?compose=15d2ab4015080221 [count: 0]
Host: mail.google.com
Visit from: https://mail.google.com/mail/u/0/#inbox?compose=new ()
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

GMail

Send the email @ 0415

```
2017-07-10T04:14:02.683510+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#inbox?compose=15d2ab4409dd446c [count: 0]
Host: mail.google.com
Visit from: https://mail.google.com/mail/u/0/#inbox?compose=15d2ab4015080221 ()
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-

2017-07-10T04:15:49.979495+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#inbox
(Inbox (15) - genberinger@gmail.com - Gmail) [count: 0]
Host: mail.google.com
Visit from: https://mail.google.com/mail/u/0/#inbox?compose=15d2ab47e490aefa
(Inbox (15) - genberinger@gmail.com - Gmail)
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

GMail

Reply to an email @ 0411

```
2017-07-10T04:11:17.069331+00:00,
Page Visited,WEBHIST,Chrome History,
https://mail.google.com/mail/u/0/#inbox/14888a7464012031?compose=new [count: 0]
Host: mail.google.com
Visit from: https://mail.google.com/mail/u/0/#inbox/14888a7464012031
(Join The Party with Camfrog EXTREME! - genberinger@gmail.com - Gmail)
Type: [LINK - User clicked a link]
(URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

GMail

So, you can get some information from GMail browser history, but it doesn’t tell you anything about who they are talking to.

Inbox

From 0417 to 0423, did a lot of the same actions -- read emails, search, mark as done, reply, compose, and create a reminder. This is what you get:

```
2017-07-10T04:17:19.679538+00:00,Page Visited,WEBHIST,Chrome History,https://inbox.google.com/?pli=1 (Inbox - genberin
ger@gmail.com) [count: 0] Host: inbox.google.com Type: [LINK - User clicked a link] (URL not typed directly - no typed
 count),sqlite/chrome_history,OS:History,-
2017-07-10T04:17:21.857847+00:00,Page Visited,WEBHIST,Chrome History,https://inbox.google.com/?pli=1 (Inbox - genberin
ger@gmail.com) [count: 0] Host: inbox.google.com Type: [LINK - User clicked a link] (URL not typed directly - no typed
 count),sqlite/chrome_history,OS:History,-
2017-07-10T04:19:35.619023+00:00,Page Visited,WEBHIST,Chrome History,https://inbox.google.com/search/?pli=1 [count: 0]
 Host: inbox.google.com Type: [LINK - User clicked a link] (URL not typed directly - no typed count),sqlite/chrome_his
tory,OS:History,-
2017-07-10T04:19:37.379752+00:00,Page Visited,WEBHIST,Chrome History,https://inbox.google.com/search/cam?pli=1 [count:
 0] Host: inbox.google.com Type: [LINK - User clicked a link] (URL not typed directly - no typed count),sqlite/chrome_
history,OS:History,-
2017-07-10T04:19:39.324606+00:00,Page Visited,WEBHIST,Chrome History,https://inbox.google.com/search/camfrog?pli=1 [co
unt: 0] Host: inbox.google.com Type: [LINK - User clicked a link] (URL not typed directly - no typed count),sqlite/chr
ome_history,OS:History,-
2017-07-10T04:20:44.191511+00:00,Page Visited,WEBHIST,Chrome History,https://inbox.google.com/?pli=1 (Inbox - genberin
ger@gmail.com) [count: 0] Host: inbox.google.com Type: [LINK - User clicked a link] (URL not typed directly - no typed
 count),sqlite/chrome_history,OS:History,-
```

Inbox

Well, that’s not very helpful...

Drive

Log into Google Drive @ 0426

```
2017-07-10T04:26:28.555646+00:00,
Page Visited,WEBHIST,Chrome History,
https://drive.google.com/drive/ (Google Drive) [count: 0]
Host: drive.google.com
Visit from: https://drive.google.com/?authuser=0 (Google Drive)
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

View a Folder @ 0437

```
2017-07-10T04:37:06.134906+00:00,
Page Visited,WEBHIST,Chrome History,
https://drive.google.com/drive/folders/0B135PS1X10DmYXJrN2sxdEtMdjQ
(Google Drive) [count: 0]
Host: drive.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

View a Google Doc @ 0431

```
2017-07-10T04:31:17.420697+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/document/d/14BQNFhoA3oACwY1kddnng5HvYoAyUbt7fwiwsvSsqYc/edit
[count: 0]
Host: docs.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

If you leave Docs open in Chrome, you get **a lot** of entries in your browser history.

```
$ grep "1GN" genb-drive.csv | wc
      91    2672   29991
$ grep "1Ml" genb-drive.csv | wc
      80    1739   23721
```

Drive

Download Doc as PDF @ 0432

```
2017-07-10T04:32:08.010571+00:00,
File Downloaded,WEBHIST,Chrome History,
https://docs.google.com/document/export?format=pdf&id=14BQNFhoA3oACwY1kddnng5HvY
oAyUbt7fwiwsvSsqYc&token=AC4w5Vg9oRjxr1dvfaGXcS4Ex4HvE-q-iA%3A1499661076826
(/BBQSecretSauce.pdf).
Received: 53611 bytes out of: 53611 bytes.,
sqlite/chrome_history,OS:History,-
```

Drive

Create a new Google Doc @ 0432

```
2017-07-10T04:32:34.742811+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/document/u/0/create?zx=ft8we5242can&usp=docs_web
(Untitled document - Google Docs) [count: 0]
Host: docs.google.com
Visit from: https://docs.google.com/document/create?zx=ft8we5242can&usp=docs_web
(Untitled document - Google Docs)
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

```
2017-07-10T04:32:34.742811+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/document/u/0/d/1GN31PQuUceDRwjWbOAdUXQ1oYKoZnGXpgAW7IaA-M2M/edit
(Untitled document - Google Docs) [count: 0]
Host: docs.google.com
Visit from: https://docs.google.com/document/u/0/create?zx=ft8we5242can&usp=docs_web
(Untitled document - Google Docs)
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

Copy a Doc from the Docs interface @ 0451 (and another day)

```
2017-07-25T04:51:08.726349+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/document/d/1epf2wn4BtSDKYEPn7oqlzLJp4kpgP3iirXhYxHOtPM0/edit
(Copy of BBQ Secret Sauce - Google Docs) [count: 0]
Host: docs.google.com
Visit from: https://docs.google.com/document/d/14BQNFhoA3oACwY1kddnng5HvYoAyUbt7fwiwsvSsqYc/
copy?id=14BQNFhoA3oACwY1kddnng5HvYoAyUbt7fwiwsvSsqYc&copyCollaborators=false&copyComments=fa
lse&title=Copy%20of%20BBQ%20Secret%20Sauce&token=AC4w5ViaKKYMbaTsuYd7qENEBKnVlMo8nA%3A150095
8239265&usp=docs_web (Copy of BBQ Secret Sauce - Google Docs)
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:/History,-
```

Drive

Copy a Doc from the Drive interface @ 0437

```
2017-07-10T04:37:14.599472+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/document/d/1MlrafNBA9pzvnvtocT3aHM5Q384wqzewNRNJHcZm9Aw/edit?usp=drive_web
(Copy of I am a new document - Google Docs) [count: 0]
Host: docs.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

Viewing the First Sheet in a Spreadsheet @ 0439

```
2017-07-10T04:39:25.126861+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/spreadsheets/d/1jOUWDFc39zFbJXneCFJUQNzMWAtWWP2m6uWnEmUnK2I/edit#gid=0
(spreadsheets are the best!!! - Google Sheets) [count: 0]
Host: docs.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

Viewing Other Sheets in a Spreadsheet @ 0439

```
2017-07-10T04:39:28.200170+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/spreadsheets/d/1jOUWDFc39zFbJXneCFJUQNzMWAtWWP2m6uWnEmUnK2I/edit#gid=200246688
[count: 0]
Host: docs.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-

2017-07-10T04:39:34.992330+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/spreadsheets/d/1jOUWDFc39zFbJXneCFJUQNzMWAtWWP2m6uWnEmUnK2I/edit#gid=1272553202
[count: 0]
Host: docs.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

Viewing Presentation @ 0439

```
2017-07-10T04:39:46.680822+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/presentation/d/1y_AIDbHb6LJTLmNZqWqAd49TbGckAjXj3ypiY-Ct_oU/
edit#slide=id.p
(I like to make presentations - Google Slides)
[count: 0]
Host: docs.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

Viewing Presentation @ 0440 -- Next Slide

```
2017-07-10T04:40:54.518961+00:00,
Page Visited,WEBHIST,Chrome History,
https://docs.google.com/presentation/d/1y_AIDbHb6LJTLmNZqWqAd49TbGckAjXj3ypiY-Ct_oU/
edit#slide=id.g1e9502d382_0_0
[count: 0]
Host: docs.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

Viewing an Image @ 0444

```
2017-07-10T04:44:22.908684+00:00,
Page Visited,WEBHIST,Chrome History,
https://drive.google.com/open?id=1-dB2VHhBJswgNHciMGuQJZm7FT10r_UxDw&authuser=0
(bbq-dragon-xl.jpg - Google Drive) [count: 0]
Host: drive.google.com
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

Open a PDF in its own tab @ 0438

```
2017-07-10T04:38:50.398036+00:00,
Page Visited,WEBHIST,Chrome History,
https://drive.google.com/file/d/1dUdb6FYKr7BlXgwiKUjWzrQBJG5j6kPmVDZylznWuGEONDe
4CzFBLSzy2OxgxqbinkDb_tC6yhRIdqSP/view?usp=drive_web
(BBQ Secret Sauce - Google Docs.pdf - Google Drive) [count: 0]
Host: drive.google.com
Visit from: https://drive.google.com/open?id=1dUdb6FYKr7BlXgwiKUjWzrQBJG5j6kPmVD
ZylznWuGEONDe4CzFBLSzy2OxgxqbinkDb_tC6yhRIdqSP
(BBQ Secret Sauce - Google Docs.pdf - Google Drive)
Type: [LINK - User clicked a link] (URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,-
```

Drive

Searching in Drive @ 0441

```
2017-07-10T04:41:52.182584+00:00,
Page Visited,WEBHIST,Chrome History,
https://drive.google.com/drive/search?q=bbq
(Search results - Google Drive) [count: 0]
Host: drive.google.com
Type: [LINK - User clicked a link]
(URL not typed directly - no typed count),
sqlite/chrome_history,OS:History,browser_search
```

Drive

Things that didn’t end up in Browser history:

- Sharing files
- Printing files
- Uploading files

Next Steps

- Someday I will write a plaso analysis plugin to find things like copying and downloading files.
- In the meantime, the History file, a timeline of the actions take on the account, and these slides will be on my github page:

https://github.com/bethlogic/drivetesting

bethlogic@

In Summary

- You can see some information on reading and writing emails, but not the recipient
- But only on GMail -- you are out of luck if they are using Inbox
- Searches in GMail, Inbox, and Drive are easy to see!
- In Drive, you can get an idea what they were looking at, if they give their files useful titles
    - There are some patterns to the DocIDs, but it’s easier to find out what kind of file it is from the URL
- And get some hints if they were trying to take it (downloads, copies), but not printing or sharing