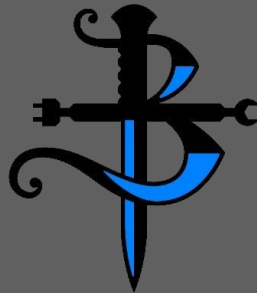


Introduction to Browser Forensics

Sileniia - Blue Team Village - July 8th, 2021



Who Am I?

- Beginning InfoSec practitioner with 3 years of experience
 - Software Development, Security Operations, Incident Response
 - Daily use of browser forensics
- Let's Connect!
 - [Blue Team Village Discord](#)
 - Discord: Sileniiia#5737
 - LinkedIn: [/in/jacksonparsons/](#)

Roadmap

1. Why browser forensics?
2. Privacy, ethics
3. Chrome directory structure
4. History, Cache, Login Data
5. Resources
6. Q&A

Why?

- Browsers are a cornucopia of value for...
- Attackers
 - Persistence (AutoRefresh extension)
 - Pivot (internal sites via bookmarks, history)
 - Post-exploitation (data exfiltration, account enumeration)
 - Scrape login data
 - Steal PII
- Security operations and incident response
 - Investigate
 - Attackers
 - Suspicious DNS requests
 - Malicious browser extensions
 - Corroborate / disprove testimony
 - Unmask HTTPS
 - Review form data
 - Recover deleted files
 - Not typically logged or reported

Ethics

- Browser artifacts can be *highly* sensitive
 - PII - financial, education, health information
 - Encrypted connections
 - Persistence, Post-Exploitation
- Ensure that you have just cause
 - Set expectations up front about use of browser forensics techniques
- Ensure proper handling
 - Be *very* cautious of public-facing sandbox, detonation services (ANY.RUN, URLScan)
 - Delete unnecessary information / artifacts afterwards (and document deletion)
 - Report / auditing mechanism?

Chrome Directory Structure

Top-level directory depends on OS

- **Windows:**

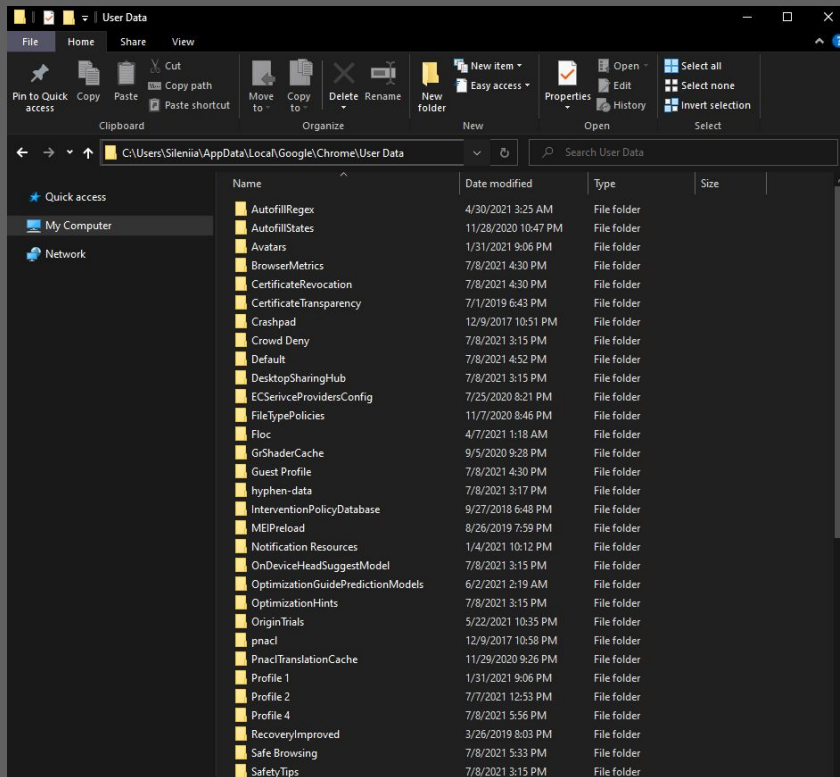
- C:\Users\<user>\AppData\Local\Google\Chrome (7+)
- C:\Documents and Settings\<user>\Local Settings\Application Data\Google\Chrome\ (XP)

- **Linux:**

- /home/<user>/.config/google-chrome (Google distribution)
- /home/<user>/.config/chromium/ (Linux distribution)

- **Mac:**

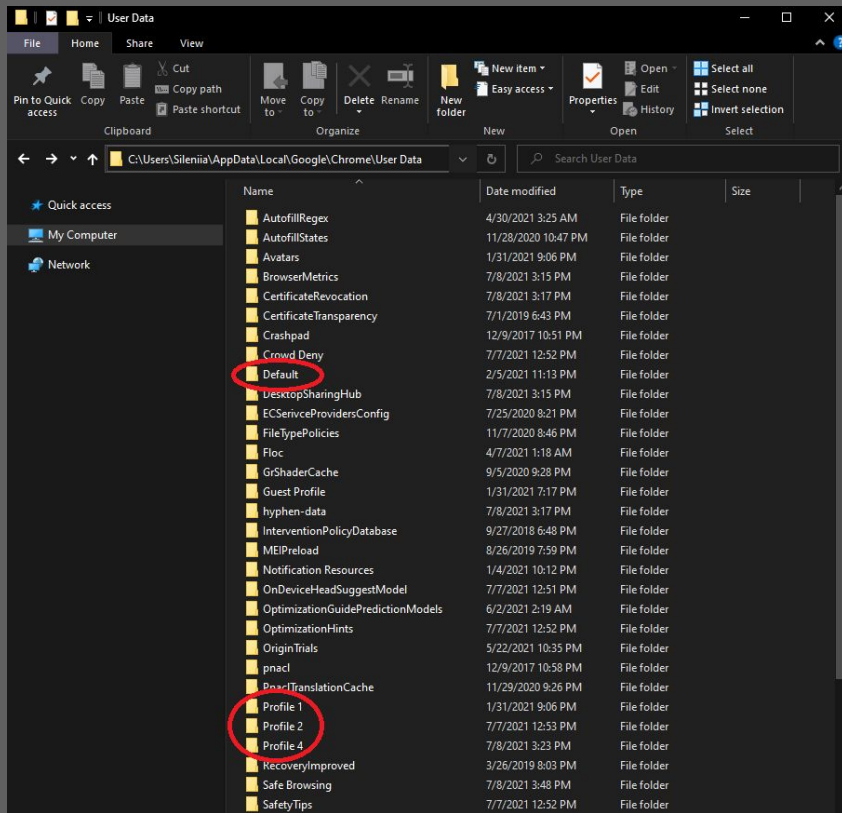
- /Users/<user>/Library/Application Support/ Google/Chrome



Chrome Directory Structure

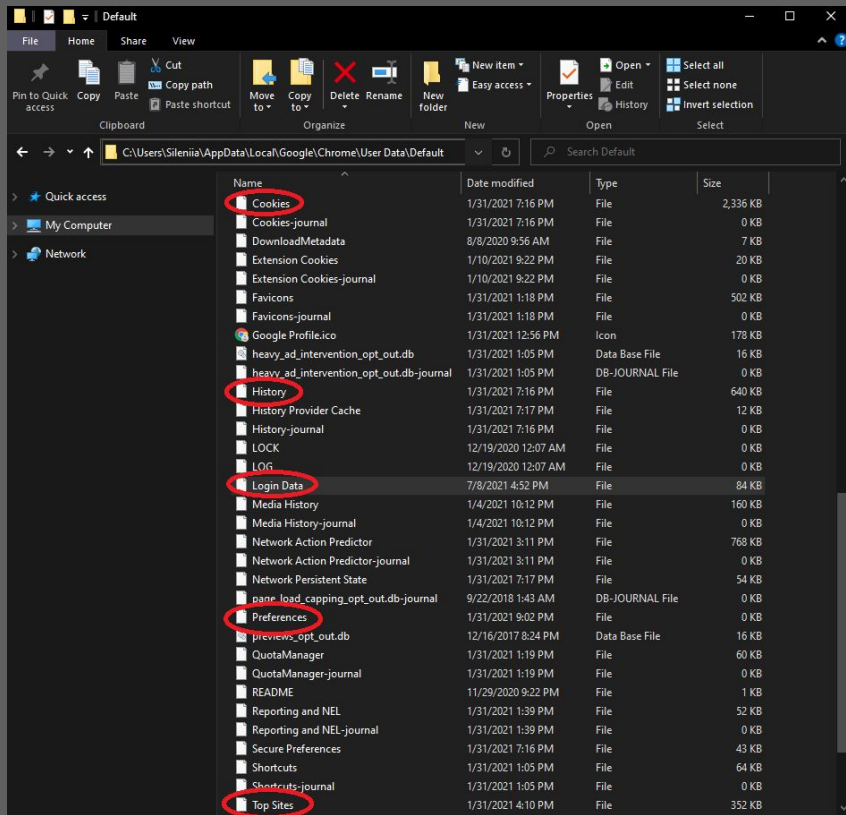
“Profiles” for multiple users or sessions

- *Default* (“Profile 0”)
 - What we’re after ~95% of the time
- *Profile #*
 - Created in order after Default
 - Don’t necessarily stay that way



Chrome Directory Structure

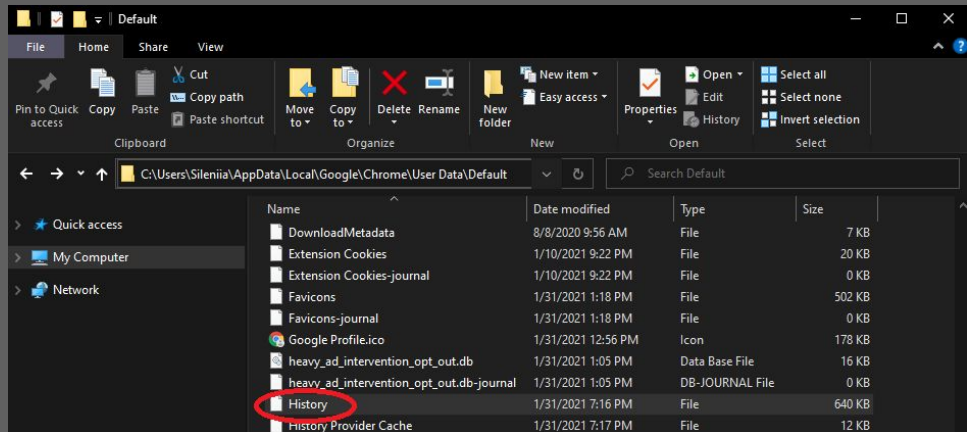
- Profiles contain *tons* of interesting and valuable information
 - Bookmarks
 - Cache
 - Cookies
 - Extensions
 - Form Data
 - History
 - Login Data
 - Preferences
 - Top Sites
 - Sessions (Past + Current)
 - ...



History

C:\Users\<user>\AppData\Local\Google\Chrome
\User Data\<profile>\History

- Silver bullet for unusual DNS traffic
 - Often ad- or resource-related
 - “Replay” their traffic in a sandbox to test your hypotheses
 - Be **very** careful of public-only sandboxes like ANY.RUN
- Corroborate proxy logs and behavior
 - “It doesn’t *look* like their attempt to visit `http[:]//evil[.]com` was blocked...”
 - Discover broken proxy agents
- SQLite format
 - View with [NirSoft](#)
- Scale with SOAR, URLScan, sandbox



Exploring History

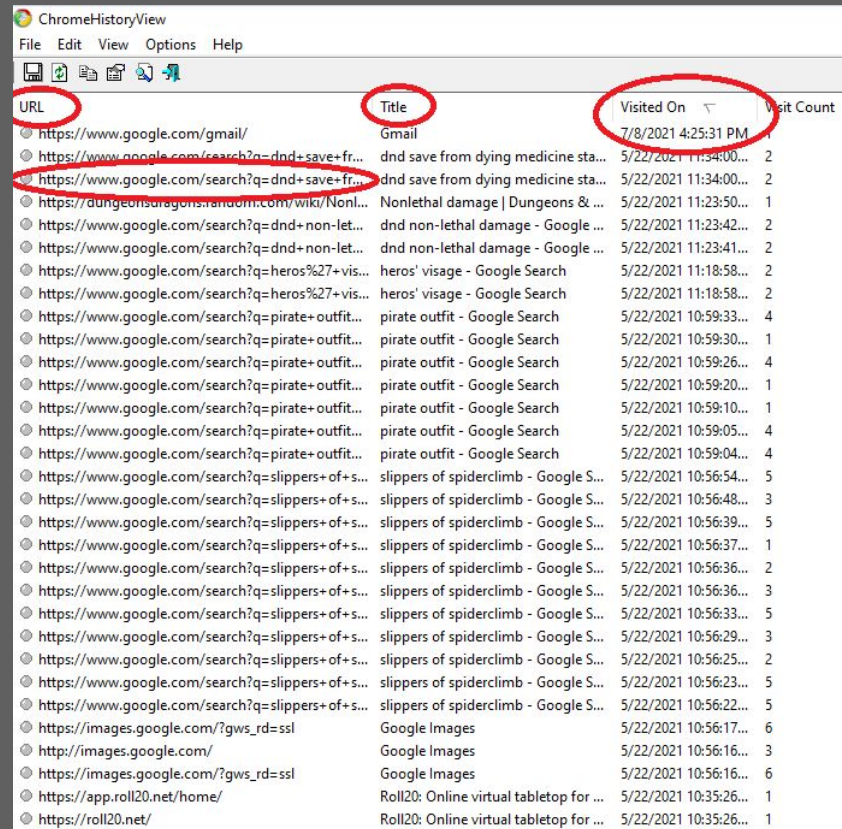
ChromeHistoryView											
File Edit View Options Help											
URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit ID	Profile	URL Length	Transition Type	Transition Qualifiers	History File
https://www.google.com/gmail/	Gmail	7/8/2021 4:25:31 PM	1	0	https://gmail.com/	3	Profile 4	29	Typed	Server Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=dnd+save+fr...	dnd save from dying medicine sta...	5/22/2021 11:34:00...	2	0		914	Profile 2	164	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=dnd+save+fr...	dnd save from dying medicine sta...	5/22/2021 11:34:00...	2	0		913	Profile 2	164	Generated	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://dungeonsdragons.fandom.com/wiki/Nonle...	Nonlethal damage Dungeons & ...	5/22/2021 11:23:50...	1	0		912	Profile 2	56	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=dnd+non-let...	dnd non-lethal damage - Google ...	5/22/2021 11:23:42...	2	0		911	Profile 2	140	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=dnd+non-let...	dnd non-lethal damage - Google ...	5/22/2021 11:23:41...	2	0		910	Profile 2	140	Generated	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=heros%27+vis...	heros' visage - Google Search	5/22/2021 11:18:58...	2	0		909	Profile 2	138	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=heros%27+vis...	heros' visage - Google Search	5/22/2021 11:18:58...	2	0		908	Profile 2	138	Generated	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:33...	4	0	https://www.google.com/search?q=pirate...	907	Profile 2	360	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:30...	1	0	https://www.google.com/search?q=pirate...	906	Profile 2	381	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:26...	4	0	https://www.google.com/search?q=pirate...	905	Profile 2	360	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:20...	1	0	https://www.google.com/search?q=pirate...	904	Profile 2	381	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:10...	1	0	https://www.google.com/search?q=pirate...	903	Profile 2	381	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:05...	4	0	https://www.google.com/search?q=pirate...	902	Profile 2	360	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:04...	4	0	https://www.google.com/search?q=slipper...	901	Profile 2	360	Link	Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:54...	5	0		900	Profile 2	355	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:48...	3	0		899	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:39...	5	0		898	Profile 2	355	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:37...	1	0		897	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:36...	2	0		896	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:36...	3	0		895	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:33...	5	0		894	Profile 2	355	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:29...	3	0		893	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:25...	2	0		892	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:23...	5	0		891	Profile 2	355	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:22...	5	0		890	Profile 2	355	Form Submit	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://images.google.com/?gws_rd=ssl	Google Images	5/22/2021 10:56:17...	6	0		889	Profile 2	37	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://images.google.com/	Google Images	5/22/2021 10:56:16...	3	3		887	Profile 2	25	Typed	Chain Start	C:\Users\Silenia\AppData\Local\Google\Ch...
https://images.google.com/?gws_rd=ssl	Google Images	5/22/2021 10:56:16...	6	0	http://images.google.com/	888	Profile 2	37	Typed	Chain End,Server Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://app.roll20.net/home/	Roll20: Online virtual tabletop for ...	5/22/2021 10:35:26...	1	0		878	Profile 2	28	Form Submit	Chain Start	C:\Users\Silenia\AppData\Local\Google\Ch...
https://roll20.net/	Roll20: Online virtual tabletop for ...	5/22/2021 10:35:26...	1	0	https://app.roll20.net/home/	879	Profile 2	19	Form Submit	Server Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...

Exploring History

ChromeHistoryView											
File Edit View Options Help											
URL	Title	Visited On	Visit Count	Typed Count	Referrer	Visit ID	Profile	URL Length	Transition Type	Transition Qualifiers	History File
https://www.google.com/gmail/	Gmail	7/8/2021 4:25:31 PM	2	0	https://gmail.com/	3	Profile 4	29	Typed	Server Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=dnd+save+fr...	dnd save from dying medicine sta...	5/22/2021 11:54:00...	2	0		914	Profile 2	164	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=dnd+save+fr...	dnd save from dying medicine sta...	5/22/2021 11:34:00...	1	0		913	Profile 2	164	Generated	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://dungeonsanddragons.fandom.com/wiki/Nonle...	Nonlethal damage Dungeons & ...	5/22/2021 11:23:50...	1	0		912	Profile 2	56	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=dnd+non-let...	dnd non-lethal damage - Google ...	5/22/2021 11:23:42...	2	0		911	Profile 2	140	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=dnd+non-let...	dnd non-lethal damage - Google ...	5/22/2021 11:23:41...	2	0		910	Profile 2	140	Generated	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=heros%27+vis...	heros' visage - Google Search	5/22/2021 11:18:58...	2	0		909	Profile 2	138	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=heros%27+vis...	heros' visage - Google Search	5/22/2021 11:18:58...	2	0		908	Profile 2	138	Generated	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:33...	4	0	https://www.google.com/search?q=pirate...	907	Profile 2	360	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:30...	1	0	https://www.google.com/search?q=pirate...	906	Profile 2	381	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:26...	4	0	https://www.google.com/search?q=pirate...	905	Profile 2	360	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:20...	1	0	https://www.google.com/search?q=pirate...	904	Profile 2	381	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:10...	1	0	https://www.google.com/search?q=pirate...	903	Profile 2	381	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:05...	4	0	https://www.google.com/search?q=pirate...	902	Profile 2	360	Link	Chain End,Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:04...	4	0	https://www.google.com/search?q=slipper...	901	Profile 2	360	Link	Client Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:54...	5	0		900	Profile 2	355	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:48...	3	0		899	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:39...	5	0		898	Profile 2	355	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:37...	1	0		897	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:36...	2	0		896	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:36...	3	0		895	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:33...	5	0		894	Profile 2	355	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:29...	3	0		893	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:25...	2	0		892	Profile 2	376	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:23...	5	0		891	Profile 2	355	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:22...	5	0		890	Profile 2	355	Form Submit	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://images.google.com/?gws_rd=ssl	Google Images	5/22/2021 10:56:17...	6	0		889	Profile 2	37	Link	Chain Start,Chain End	C:\Users\Silenia\AppData\Local\Google\Ch...
https://images.google.com/	Google Images	5/22/2021 10:56:16...	3	3		887	Profile 2	25	Typed	Chain Start	C:\Users\Silenia\AppData\Local\Google\Ch...
https://images.google.com/?gws_rd=ssl	Google Images	5/22/2021 10:56:16...	6	0	http://images.google.com/	888	Profile 2	37	Typed	Chain End,Server Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...
https://app.roll20.net/home/	Roll20: Online virtual tabletop for ...	5/22/2021 10:35:26...	1	0		878	Profile 2	28	Form Submit	Chain Start	C:\Users\Silenia\AppData\Local\Google\Ch...
https://roll20.net/	Roll20: Online virtual tabletop for ...	5/22/2021 10:35:26...	1	0	https://app.roll20.net/home/	879	Profile 2	19	Form Submit	Server Redirect	C:\Users\Silenia\AppData\Local\Google\Ch...

Exploring History

- URL
 - If not decrypting HTTPS, URI path is normally unavailable in proxy logs
 - Allows us to replay traffic for investigations
- Title
 - Takes on value of search engine queries
 - Shows visits to proxy block / redirects
- Visited On



URL	Title	Visited On	Visit Count
https://www.google.com/gmail/	Gmail	7/8/2021 4:25:31 PM	1
https://www.google.com/search?q=dnd+save+fr...	dnd save from dying medicine sta...	5/22/2021 11:34:00...	2
https://www.google.com/search?q=dnd+save+fr...	dnd save from dying medicine sta...	5/22/2021 11:34:00...	1
https://dungeonsanddragons.random.com/wiki/Nonl...	Nonlethal damage Dungeons & ...	5/22/2021 11:23:50...	2
https://www.google.com/search?q=dnd+non-let...	dnd non-lethal damage - Google ...	5/22/2021 11:23:42...	2
https://www.google.com/search?q=dnd+non-let...	dnd non-lethal damage - Google ...	5/22/2021 11:23:41...	2
https://www.google.com/search?q=heros%27+vis...	heros' visage - Google Search	5/22/2021 11:18:58...	2
https://www.google.com/search?q=heros%27+vis...	heros' visage - Google Search	5/22/2021 11:18:58...	2
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:33...	4
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:30...	1
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:26...	4
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:20...	1
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:10...	1
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:05...	4
https://www.google.com/search?q=pirate+outfit...	pirate outfit - Google Search	5/22/2021 10:59:04...	4
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:54...	5
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:48...	3
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:39...	5
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:37...	1
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:36...	2
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:36...	3
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:33...	5
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:29...	3
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:25...	2
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:23...	5
https://www.google.com/search?q=slippers+of+s...	slippers of spiderclimb - Google S...	5/22/2021 10:56:22...	5
https://images.google.com/?gws_rd=ssl	Google Images	5/22/2021 10:56:17...	6
http://images.google.com/	Google Images	5/22/2021 10:56:16...	3
https://images.google.com/?gws_rd=ssl	Google Images	5/22/2021 10:56:16...	6
https://app.roll20.net/home/	Roll20: Online virtual tabletop for ...	5/22/2021 10:35:26...	1
https://roll20.net/	Roll20: Online virtual tabletop for ...	5/22/2021 10:35:26...	1

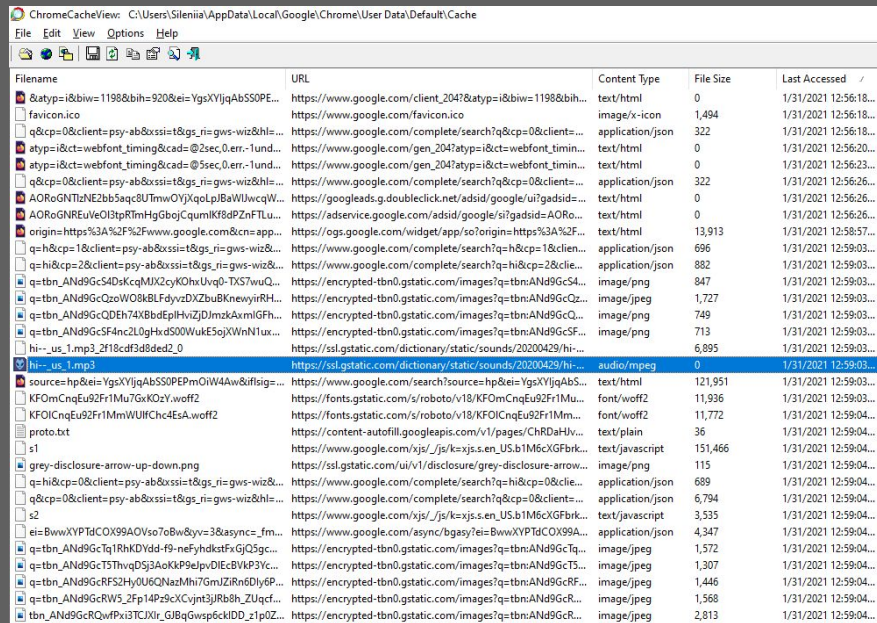
Exploring History

- Referrer
 - Source / where the user came from
- Profile
 - Which profile generated the traffic
- Transition Type
 - **Link**: user clicked a link
 - **Typed**: user typed the URL into the address bar
 - **Auto_Bookmark**: user visited the site through a bookmark
 - **Form_Submit**: user filled out a form and submitted
 - **Reload**: user reloaded the page

Referrer	Visit ID	Profile	URL Length	Transition Type
https://gmail.com/	3	Profile 4	29	Typed
	914	Profile 2	164	Link
	913	Profile 2	164	Generated
	912	Profile 2	56	Link
	911	Profile 2	140	Link
	910	Profile 2	140	Generated
	909	Profile 2	138	Link
	908	Profile 2	138	Generated
	907	Profile 2	360	Link
	906	Profile 2	381	Link
https://www.google.com/search?q=pirate...	905	Profile 2	360	Link
https://www.google.com/search?q=pirate...	904	Profile 2	381	Link
https://www.google.com/search?q=pirate...	903	Profile 2	381	Link
https://www.google.com/search?q=pirate...	902	Profile 2	360	Link
https://www.google.com/search?q=slipper...	901	Profile 2	360	Link
	900	Profile 2	355	Link
	899	Profile 2	376	Link
	898	Profile 2	355	Link
	897	Profile 2	376	Link
	896	Profile 2	376	Link
	895	Profile 2	376	Link
	894	Profile 2	355	Link
	893	Profile 2	376	Link
	892	Profile 2	376	Link
	891	Profile 2	355	Link
	890	Profile 2	355	Form Submit
	889	Profile 2	37	Link
	887	Profile 2	25	Typed
http://images.google.com/	888	Profile 2	37	Typed
	878	Profile 2	28	Form Submit
https://app.roll20.net/home/	879	Profile 2	19	Form Submit

Cache

- Chrome caches various resources to help speed up browsing experience
 - HTML, CSS, JavaScript
 - Audio
 - Images
 - Executables
 - ...
- Cached files can act as backups in case originals are deleted



Filename	URL	Content Type	File Size	Last Accessed
&atyp=i&biw=1198&bih=920&ei=YgsYVjgAbSSOPE...	https://www.google.com/client_204?atyp=i&biw=1198&bih=...	text/html	0	1/31/2021 12:56:18...
favicon.ico	https://www.google.com/favicon.ico	image/x-icon	1,494	1/31/2021 12:56:18...
q&cp=0&client=psy-ab&sssi=t&gs_r=gs-wiz&hl=...	https://www.google.com/complete/search?q&cp=0&client=...	application/json	322	1/31/2021 12:56:18...
atyp=i&ct=webfont_timing&cad=@2sec,0,err-1und...	https://www.google.com/gen_204?atyp=i&ct=webfont_timin...	text/html	0	1/31/2021 12:56:20...
atyp=i&ct=webfont_timing&cad=@5sec,0,err-1und...	https://www.google.com/gen_204?atyp=i&ct=webfont_timin...	text/html	0	1/31/2021 12:56:23...
q&cp=0&client=psy-ab&sssi=t&gs_r=gs-wiz&hl=...	https://www.google.com/complete/search?q&cp=0&client=...	application/json	322	1/31/2021 12:56:26...
AORoGNtLzE2b5aqc8UTmwOYjXqoLpBaWUwqW...	https://googleads.g.doubleclick.net/adsid/google/ui7gadsid=...	text/html	0	1/31/2021 12:56:26...
AORoGNtLzE2b5aqc8UTmwOYjXqoLpBaWUwqW...	https://adservice.google.com/adsid/google/si7gadsid=AORo...	text/html	0	1/31/2021 12:56:26...
origin=https%3A%2F%2Fwww.google.com&cn=app...	https://ogs.google.com/widget/app/so?origin=https%3A%2F...	text/html	13,913	1/31/2021 12:56:57...
q=h&cp=1&client=psy-ab&sssi=t&gs_r=gs-wiz&...	https://www.google.com/complete/search?q=h&cp=1&clien...	application/json	696	1/31/2021 12:59:03...
q=hi&cp=2&client=psy-ab&sssi=t&gs_r=gs-wiz&...	https://www.google.com/complete/search?q=hi&cp=2&clie...	application/json	882	1/31/2021 12:59:03...
q=tbm_ANd9GcS4DskcMjX2cyK0hUvq0-TX57wuQ...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcS4...	image/png	847	1/31/2021 12:59:03...
q=tbm_ANd9GcQz0W08KBLFdyvZDXbu8KnewyirRH...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcQz...	image/jpeg	1,727	1/31/2021 12:59:03...
q=tbm_ANd9GcQDEh74XBbdEplHvZjDImzkAxmGFh...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcQ...	image/png	749	1/31/2021 12:59:03...
q=tbm_ANd9GcSF4nc2L0gHxd500WukE5ojXWnN1u...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcSF...	image/png	713	1/31/2021 12:59:03...
hi--us_1.mp3_2f18cdf3d8ded2_0	https://ssl.gstatic.com/dictionary/static/sounds/20200429/hi...	audio/mpeg	6,895	1/31/2021 12:59:03...
hi--us_1.mp3	https://ssl.gstatic.com/dictionary/static/sounds/20200429/hi...	audio/mpeg	0	1/31/2021 12:59:03...
sources=hp&ei=YgsYVjgAbSSOPEmOiw4Aw&fifs=...	https://www.google.com/search/sources=hp&ei=YgsYVjgAbS...	text/html	121,951	1/31/2021 12:59:03...
KFOmCngEu2FrlMu7GXoKvY.woff2	https://fonts.gstatic.com/s/roboto/v18/KFOmCngEu2FrlMu...	font/woff2	11,936	1/31/2021 12:59:04...
KFOlCngEu2FrlMmVUIFChc4EsA.woff2	https://fonts.gstatic.com/s/roboto/v18/KFOlCngEu2FrlMm...	font/woff2	11,772	1/31/2021 12:59:04...
proto.txt	https://content-autofill.googleapis.com/v1/pages/ChRD4hV...	text/plain	36	1/31/2021 12:59:04...
s1	https://www.google.com/xjs/_/js/k=xjs.en_US.b1M6cXGfBrk...	text/javascript	151,466	1/31/2021 12:59:04...
grey-disclosure-arrow-up-down.png	https://ssl.gstatic.com/ui/v1/disclosure/grey-disclosure-arrow...	image/png	115	1/31/2021 12:59:04...
q=h&cp=0&client=psy-ab&sssi=t&gs_r=gs-wiz&...	https://www.google.com/complete/search?q=h&cp=0&clie...	application/json	689	1/31/2021 12:59:04...
q&cp=0&client=psy-ab&sssi=t&gs_r=gs-wiz&hl=...	https://www.google.com/complete/search?q&cp=0&client=...	application/json	6,794	1/31/2021 12:59:04...
s2	https://www.google.com/xjs/_/js/k=xjs.en_US.b1M6cXGfBrk...	text/javascript	3,535	1/31/2021 12:59:04...
ei=BwwXYPTdCOX99AOvso7Bw&y3s=3&asyncc=fm...	https://www.google.com/asyncc/gasy/ei=BwwXYPTdCOX99A...	application/json	4,347	1/31/2021 12:59:04...
q=tbm_ANd9GcTq1RhKDvdd-f9-nefyhdkfFrGjQ5gc...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcTq...	image/jpeg	1,572	1/31/2021 12:59:04...
q=tbm_ANd9GcT3ThvqD53AoKkP9elpDIcBVKP3Yc...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcT3...	image/jpeg	1,307	1/31/2021 12:59:04...
q=tbm_ANd9GcRF52Hy0U6QNaZm7GmZIRn6Dly6P...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcRF...	image/jpeg	1,446	1/31/2021 12:59:04...
q=tbm_ANd9GcRW5_2Fp14Pz9cXCvjnt3jRbBh_ZUqcf...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcR...	image/jpeg	1,568	1/31/2021 12:59:04...
tbm_ANd9GcRQwFPxi3TCJXlr_GJBqGwsp6ckIDD_1p0Z...	https://encrypted-tbn0.gstatic.com/images?q=tbm:ANd9GcR...	image/jpeg	2,813	1/31/2021 12:59:04...

Login Data

- Saving logins necessitates:
 - Origin domain
 - Plaintext usernames
 - Encrypted usernames
- Data can be used by attackers for enumeration and further compromise

DB Browser for SQLite - C:\Users\Silenia\AppData\Local\Google\Chrome\User Data\Default>Login Data

File Edit View Tools Help

New Database Open Database Write Changes Revert Changes Open Project Save Project Attach Database Close Database

Database Structure Browse Data Edit Pragma Execute SQL

Table: logins

	action_url	username_value	password_value	submit_element	signon_realm	date_created	acklisted_by_user	scheme	password_type	times_used	for
1					https://discord.com/	13235370420...	1	0	0	0	
2					https://www.netflix.com/	13235271196...	1	0	0	0	
3					https://turbotax.intuit.com/	13226552198...	1	0	0	0	
					https://www.twitch.tv/	13222070402...	1	0	0	0	
					https://www.hackthebox.eu/	13198789483...	1	0	0	0	
						13198744759...	1	0	0	0	
						13198734387...	1	0	0	0	
						13198729293...	1	0	0	0	
						13198708815...	1	0	0	0	
						13198125876...	1	0	0	0	
						13191201930...	1	0	0	0	
					https://www.humblebundle.com/	13188779680...	1	0	0	0	
						13188170102...	1	0	0	0	
					https://accounts.nintendo.com/	13187479254...	1	0	0	0	
					https://www.reddit.com/	13182075822...	1	0	0	0	

Edit Database Cell

Mode: Binary

Import Export Set as NULL

0000 01 00 00 00 ...

Type of data currently in cell: Binary
230 byte(s)

Apply

Database Structure Browse Data Edit Pragma Execute SQL

Table: stats

	origin_domain	username_value	dismissal_count	update_time
1			1	13160374393...
2			1	13179174110...
3			1	13179174741...
4	https://notarealwebsite.com	Silenia	1	13186477193...
5			1	13191288087...
6			1	13191395949...
7			1	13195002595...
8			1	13197574019...
9			2	13197576670...
10			1	13198734491...
11			1	13220328002...

Resources

- Kevin Hendricks
- Foxton Forensics: [Browser History Examiner — User Guide](#)
- Foxton Forensics: [Analysing Chrome Login Data](#)
- SANS: [Google Chrome Forensics](#) (Kristinn Guðjónsson)
- [NirSoft](#)
 - BrowsingHistoryView
 - ChromeHistoryView
 - ChromeCacheView
 - ...
- [Hindsight](#)

Questions?