



INTERNATIONAL CYBERSECURITY AND DIGITAL FORENSICS ACADEMY

Assignment Title: Cryptocurrency, Chrome history investigations and understand user web activity

Course Code: CI901 Cybercrime Investigations Case Studies

Student Name: Ahtisham Tanveer

Student ID: 2025/ACI/9979

Programme: Advance Cybercrime Investigations

Instructor Name: Aminu Idris

Date of Submission: 01/11/2026

Contents

Course Code: CI901 Cybercrime Investigations Case Studies	1
1. Introduction.....	3
2. Investigation Objectives	3
3. Understanding URLs in Digital Investigations	3
4. URL Structure and Resource Identification.....	3
5. User-Agent Interaction with Web Resources	3
6. Creation and Hosting of Web Resources.....	3
7. URL Redirection and Its Forensic Significance	4
8. Differentiating URL Rewriting and Redirecting.....	4
9. User Web Activity and Browser Interaction Types	4
10. How User Actions Modify URLs	4
11. Browser History as a Forensic Artifact.....	4
12. Location of Browser History Files	4
13. Identification and Verification of the History Database	4
14. Examination of Browser History Database Structure	5
15. Analysis of the URLs Table	5
16. Analysis of the Visits Table	5
17. Interpretation of Visit Transition Types.....	5
18. Timestamp Normalization and Conversion	5
19. Identification of Online Marketplace Activity.....	5
20. Email-Based Communication Analysis.....	5
21. Cryptocurrency Transaction Verification Activity	5
22. Analysis of Downloaded Evidence	6
23. Correlation of Web Activity Across Platforms	6
24. Timeline Reconstruction of Illegal Activities.....	6
25. Findings and Interpretation	6
26. Conclusion and Summary	6
Practical: Cryptocurrency investigations	6
Practical: User_web_activity	17

1. Introduction

This investigation analyzes user web activity and browser history artifacts to reconstruct suspected illegal online behavior. By examining URL structures, browser interactions, and stored history records, the investigation aims to interpret user intent and establish a reliable activity timeline.

2. Investigation Objectives

The objective of this investigation was to understand how user actions are reflected in browser history and to reconstruct illegal activities by correlating URLs, visit records, user interactions, and timestamps.

3. Understanding URLs in Digital Investigations

This step explains how URLs function as identifiers for web resources and how they act as forensic artifacts representing communication between a browser and a web server.

4. URL Structure and Resource Identification

The structure of URLs was examined to understand how domains, paths, parameters, and queries reveal user intent and accessed resources during browsing sessions.

5. User-Agent Interaction with Web Resources

This step focuses on how browsers act as user agents, sending requests to servers and receiving responses that are reflected in browser history records.

6. Creation and Hosting of Web Resources

This phase demonstrates how web resources are created, stored on a server, and accessed via URLs, establishing foundational knowledge for interpreting server-side and client-side artifacts.

[7. URL Redirection and Its Forensic Significance](#)

URL redirection behavior was analyzed to understand how browsers automatically navigate users between resources and how redirects are recorded in browser history databases.

[8. Differentiating URL Rewriting and Redirecting](#)

This step distinguishes between URL rewriting and URL redirecting, explaining how both mechanisms can affect visible URLs and recorded browser history.

[9. User Web Activity and Browser Interaction Types](#)

Different types of user interactions were examined, including typing URLs, clicking links, submitting forms, and interacting with web elements, all of which influence recorded browsing behavior.

[10. How User Actions Modify URLs](#)

This step explains how form submissions, searches, selections, and uploads dynamically change URLs, providing insight into user intent and behavior.

[11. Browser History as a Forensic Artifact](#)

Browser history was identified as a comprehensive record of user web activity, containing direct requests, redirects, and navigation sequences useful in forensic analysis.

[12. Location of Browser History Files](#)

This phase identifies standard storage locations of browser history files across operating systems, ensuring proper acquisition of relevant forensic artifacts.

[13. Identification and Verification of the History Database](#)

The Chrome History database was identified and verified as a valid SQLite file, confirming its suitability for forensic examination.

[14. Examination of Browser History Database Structure](#)

The internal structure of the History database was examined to identify key tables that record URLs, visits, downloads, and search activity.

[15. Analysis of the URLs Table](#)

The URLs table was analyzed to identify visited websites, page titles, visit counts, and timestamps, providing a high-level overview of browsing behavior.

[16. Analysis of the Visits Table](#)

The visits table was examined to reconstruct navigation paths, visit sequences, visit duration, and how web pages were accessed.

[17. Interpretation of Visit Transition Types](#)

Transition values were interpreted to determine whether pages were accessed via direct typing, link clicking, redirects, or form submissions.

[18. Timestamp Normalization and Conversion](#)

Browser timestamps stored in WebKit format were converted into human-readable date and time values to accurately reconstruct the browsing timeline.

[19. Identification of Online Marketplace Activity](#)

Browser history revealed user interaction with an online classified platform, indicating advertisement creation, navigation, and post management activities.

[20. Email-Based Communication Analysis](#)

Webmail access patterns were analyzed to identify communication between the suspect and a buyer, including opened messages and replies.

[21. Cryptocurrency Transaction Verification Activity](#)

Web activity related to blockchain explorers and cryptocurrency platforms was analyzed to identify payment verification behavior.

22. Analysis of Downloaded Evidence

Downloaded files recorded in browser history were examined to identify artifacts related to transaction confirmation and record keeping.

23. Correlation of Web Activity Across Platforms

Activities from classified advertisements, email communication, cryptocurrency verification, and downloads were correlated to establish a consistent sequence of events.

24. Timeline Reconstruction of Illegal Activities

A structured timeline was reconstructed to show the progression from advertisement posting to communication, payment verification, and transaction confirmation.

25. Findings and Interpretation

The combined analysis of URLs, user actions, timestamps, and navigation behavior provided strong evidence supporting the investigation hypothesis.

26. Conclusion and Summary

This investigation demonstrates how user web activity and browser history artifacts can be effectively used to reconstruct illegal online behavior. The findings highlight the forensic value of URLs, browser interactions, and history databases in establishing timelines and supporting digital evidence.

Practical: Cryptocurrency investigations

Download History:

```
root@kali:~/home/kali# wget https://raw.githubusercontent.com/frankwxu/digital-forensics-lab/main/Digital_Currency/LabFiles/History
--2026-01-11 05:33:13-- https://raw.githubusercontent.com/frankwxu/digital-forensics-lab/main/Digital_Currency/LabFiles/History
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 196608 (192K) [application/octet-stream]
Saving to: 'History'

History                                     100%[=====] 192.00K   706KB/s   in 0.3s

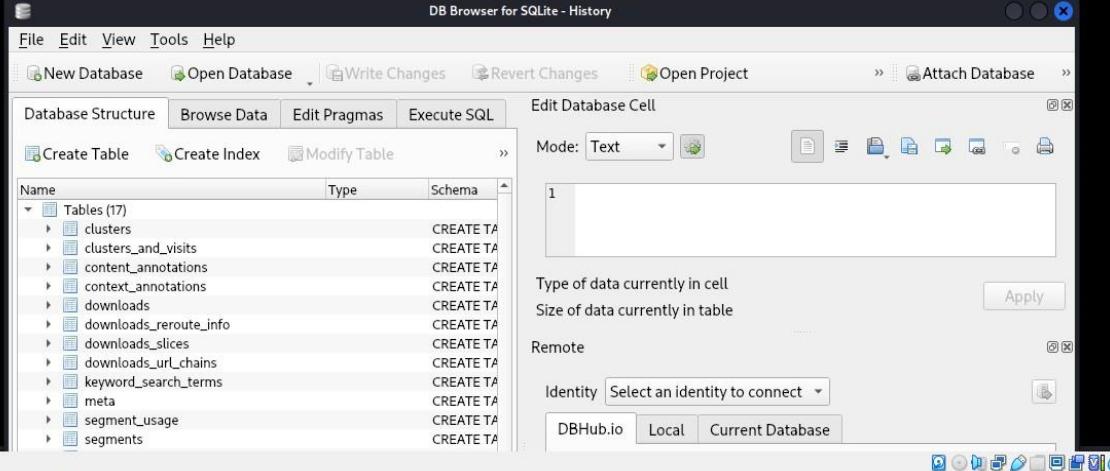
2026-01-11 05:33:13 (706 KB/s) - 'History' saved [196608/196608]
```

Examine main tables of History:

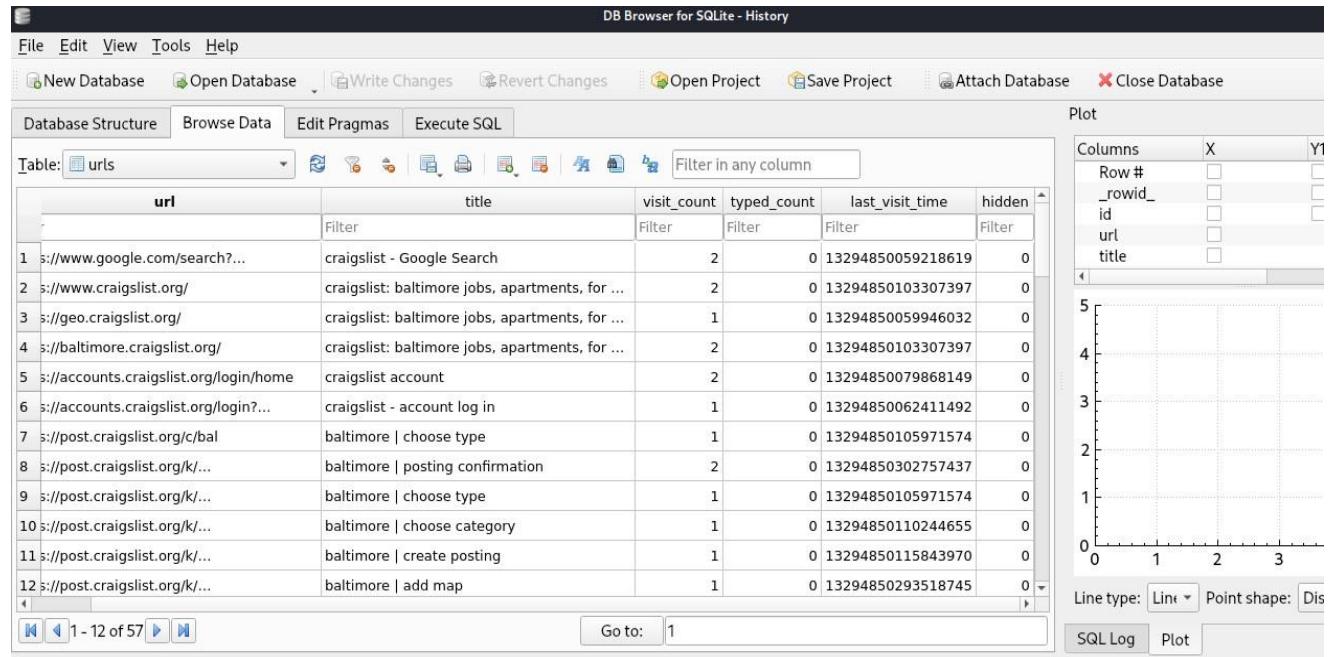
```
root@kali:~/home/kali]
# file History
History: SQLite 3.x database, last written using SQLite version 3036000, file counter 33, database pages 41, cookie 0xa7, schema 4, UTF-8, version-valid-for 33

root@kali:~/home/kali]
# sqlitebrowser History
StandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'

[...]
```



Tables View:



	url	title	visit_count	typed_count	last_visit_time	hidden
1	s://www.google.com/search?...	craigslist - Google Search	2	0	13294850059218619	0
2	s://www.craigslist.org/	craigslist: baltimore jobs, apartments, for ...	2	0	13294850103307397	0
3	s://geo.craigslist.org/	craigslist: baltimore jobs, apartments, for ...	1	0	13294850059946032	0
4	s://baltimore.craigslist.org/	craigslist: baltimore jobs, apartments, for ...	2	0	13294850103307397	0
5	s://accounts.craigslist.org/login/home	craigslist account	2	0	1329485007986149	0
6	s://accounts.craigslist.org/login?...	craigslist - account log in	1	0	13294850062411492	0
7	s://post.craigslist.org/c/bal	baltimore choose type	1	0	13294850105971574	0
8	s://post.craigslist.org/k/...	baltimore posting confirmation	2	0	13294850302757437	0
9	s://post.craigslist.org/k/...	baltimore choose type	1	0	13294850105971574	0
10	s://post.craigslist.org/k/...	baltimore choose category	1	0	13294850110244655	0
11	s://post.craigslist.org/k/...	baltimore create posting	1	0	13294850115843970	0
12	s://post.craigslist.org/k/...	baltimore add map	1	0	13294850293518745	0

Plot

Columns X Y1

Row #	
rowid	
id	
url	
title	

5
4
3
2
1
0

Line type: Line Point shape: Disp

SQL Log Plot

Show example records of urls:

```
root@kali:~/home/kali]
# sqlite3 History

SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> select id, title, datetime(last_visit_time/1000000+strftime('%s','1601-01-01'), 'unixepoch', 'localtime') from urls;
|craigslist - Google Search|2022-04-19 09:54:19
|craigslist: baltimore jobs, apartments, for sale, services, community, and events|2022-04-19 09:55:03
|craigslist: baltimore jobs, apartments, for sale, services, community, and events|2022-04-19 09:54:19
|craigslist: baltimore jobs, apartments, for sale, services, community, and events|2022-04-19 09:55:03
|craigslist account|2022-04-19 09:54:39
|craigslist - account log in|2022-04-19 09:54:22
|baltimore | choose type|2022-04-19 09:55:05
|baltimore | posting confirmation|2022-04-19 09:58:22
|baltimore | choose type|2022-04-19 09:55:05
0|baltimore | choose category|2022-04-19 09:55:10
1|baltimore | create posting|2022-04-19 09:55:15
2|baltimore | add map|2022-04-19 09:58:13
3|baltimore | create posting|2022-04-19 09:58:17
4|baltimore | create posting|2022-04-19 09:58:19
5|baltimore | manage posting|2022-04-19 09:58:27
6|cheaper than Rx supplements - health and beauty - by owner - ... |2022-04-19 09:58:31
7|gmail - Google Search|2022-04-19 09:58:39
8|Gmail: Free, Private & Secure Email | Google Workspace|2022-04-19 09:58:40
9|Inbox (12) - unsub.fscs@gmail.com - Gmail|2022-04-19 09:59:29
0|Inbox (12) - unsub.fscs@gmail.com - Gmail|2022-04-19 09:59:29
1|Gmail: Free, Private & Secure Email | Google Workspace|2022-04-19 09:58:40
2|Gmail: Free, Private & Secure Email | Google Workspace|2022-04-19 09:58:40
```

Convert timestamps in visits table to a readable format using sql statement

```
root@kali:~/home/kali]
# sqlitebrowser History
QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-root'

root@kali:~/home/kali]
# sqlite3 History

SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> select url, datetime(last_visit_time/1000000+strftime('%s','1601-01-01'), 'unixepoch', 'localtime'), from_visit, transition, visit_duration/1000 from visits order by visit_time;
1|2022-04-19 09:54:18|0|1805306373|0
1|2022-04-19 09:54:19|0|1805306368|727
2|2022-04-19 09:54:19|2|268435456|0
3|2022-04-19 09:54:19|3|-2147483648|0
4|2022-04-19 09:54:19|4|-1610612736|2465
5|2022-04-19 09:54:22|5|268435456|0
6|2022-04-19 09:54:22|6|-1610612736|17456
5|2022-04-19 09:54:39|7|1805306375|23439
2|2022-04-19 09:55:03|8|268435456|0
4|2022-04-19 09:55:03|9|-1610612736|2664
7|2022-04-19 09:55:05|10|268435456|0
8|2022-04-19 09:55:05|11|-2147483648|0
9|2022-04-19 09:55:05|12|-1610612736|14273
10|2022-04-19 09:55:10|13|1805306375|5599
11|2022-04-19 09:55:15|14|1805306375|177674
12|2022-04-19 09:58:13|15|1805306375|4389
13|2022-04-19 09:58:17|16|1805306375|1649
14|2022-04-19 09:58:19|17|1805306375|3199
8|2022-04-19 09:58:22|18|1805306375|4989
15|2022-04-19 09:58:27|19|1805306368|5597
16|2022-04-19 09:58:31|0|1805306368|0
17|2022-04-19 09:58:38|0|1838860805|0
17|2022-04-19 09:58:39|0|1805306368|842
18|2022-04-19 09:58:40|23|268435456|0
```

Segment visit records:

```
[root@kali]~[~/home/kali]
# sqlite3 History

SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> select id, "url_ref_ID: " || url, datetime(visit_time/1000000+strftime('%s','1601-01-01'), 'unixepoch', 'localtime'), "From_visit: " || from_visit, 'Tran:' || transition , "Duration: " || (visit_duration/1000) from visits order by visit_time;
1|url_ref_ID: 1|2022-04-19 09:54:18|From_visit: 0|Tran:805306373|Duration: 0
2|url_ref_ID: 1|2022-04-19 09:54:19|From_visit: 0|Tran:805306368|Duration: 727
3|url_ref_ID: 2|2022-04-19 09:54:19|From_visit: 2|Tran:268435456|Duration: 0
4|url_ref_ID: 3|2022-04-19 09:54:19|From_visit: 3|Tran:-2147483648|Duration: 0
5|url_ref_ID: 4|2022-04-19 09:54:19|From_visit: 4|Tran:-1610612736|Duration: 2465
6|url_ref_ID: 5|2022-04-19 09:54:22|From_visit: 5|Tran:268435456|Duration: 0
7|url_ref_ID: 6|2022-04-19 09:54:22|From_visit: 6|Tran:-1610612736|Duration: 17456
8|url_ref_ID: 5|2022-04-19 09:54:39|From_visit: 7|Tran:805306375|Duration: 23439
9|url_ref_ID: 2|2022-04-19 09:55:03|From_visit: 8|Tran:268435456|Duration: 0
10|url_ref_ID: 4|2022-04-19 09:55:03|From_visit: 9|Tran:-1610612736|Duration: 2664
11|url_ref_ID: 7|2022-04-19 09:55:05|From_visit: 10|Tran:268435456|Duration: 0
12|url_ref_ID: 8|2022-04-19 09:55:05|From_visit: 11|Tran:-2147483648|Duration: 0
13|url_ref_ID: 9|2022-04-19 09:55:05|From_visit: 12|Tran:-1610612736|Duration: 4273
14|url_ref_ID: 10|2022-04-19 09:55:10|From_visit: 13|Tran:805306375|Duration: 5599
15|url_ref_ID: 11|2022-04-19 09:55:15|From_visit: 14|Tran:805306375|Duration: 177674
16|url_ref_ID: 12|2022-04-19 09:58:13|From_visit: 15|Tran:805306375|Duration: 4389
17|url_ref_ID: 13|2022-04-19 09:58:17|From_visit: 16|Tran:805306375|Duration: 1649
18|url_ref_ID: 14|2022-04-19 09:58:19|From_visit: 17|Tran:805306375|Duration: 3199
19|url_ref_ID: 8|2022-04-19 09:58:22|From_visit: 18|Tran:805306375|Duration: 4989
20|url_ref_ID: 15|2022-04-19 09:58:27|From_visit: 19|Tran:805306368|Duration: 5597
21|url_ref_ID: 16|2022-04-19 09:58:31|From_visit: 0|Tran:805306368|Duration: 0
22|url_ref_ID: 17|2022-04-19 09:58:38|From_visit: 0|Tran:838860805|Duration: 0
23|url_ref_ID: 17|2022-04-19 09:58:39|From_visit: 0|Tran:805306368|Duration: 842
24|url_ref_ID: 18|2022-04-19 09:58:40|From_visit: 23|Tran:268435456|Duration: 0
25|url_ref_ID: 19|2022-04-19 09:58:40|From_visit: 24|Tran:-2147483648|Duration: 0
26|url_ref_ID: 20|2022-04-19 09:58:40|From_visit: 25|Tran:-2147483648|Duration: 0
27|url_ref_ID: 21|2022-04-19 09:58:40|From_visit: 26|Tran:-2147483648|Duration: 0
28|url_ref_ID: 22|2022-04-19 09:58:40|From_visit: 27|Tran:-2147483648|Duration: 0
```

Seg1: Search “craiglist” (visit id=1-2):

```
sqlite> select "url_id: " || id, url, title from urls where id=1;
url_id: 1|https://www.google.com/search?q=craiglist&lz=LCl0NGR_enUS989U989&oq=craiglist&qs=chrome..69i57j46i131i199i433i465i512j0i40l2j0i512l3j0i131i433l2j0i512..2595j0j15&sourceid=chrome&ie=UTF-8|craiglist - Google Search
sqlite> |
```

Seg2: Jump to https://www.craigslist.org/ (visits id=3-5)

```
[root@kali]~[~/home/kali]
# sqlite3 History

SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> select "url_id: " || id, url, title from urls where id=2 or id=3 or id=4;
url_id: 2|https://www.craigslist.org/craigslist: baltimore jobs, apartments, for sale, services, community, and events
url_id: 3|https://geo.craigslist.org/craigslist: baltimore jobs, apartments, for sale, services, community, and events
url_id: 4|https://baltimore.craigslist.org/craigslist: baltimore jobs, apartments, for sale, services, community, and events
sqlite> |
```

Analyze segment 3 (visits id=6-7):

```
sqlite> select "url_id: " || id, url, title from urls where id=5 or id=6;
url_id: 5|https://accounts.craigslist.org/login/home|craigslist account
url_id: 6|https://accounts.craigslist.org/login?rp=%2Flogin%2Fhome&rt=L|craigslist - account log in
sqlite> |
```

Analyze segment 4 (visits id=8), Analyze segment 5 (visits id=9-10), Analyze segment 6 (visits id=11-13), Analyze segment 7 (visits id=14), Analyze segment 8 (visits id=15), Analyze segment 9 (visits id=16), Analyze segment 10 (visits id=17), Analyze segment 11 (visits id=18), Analyze segment 12 (visits id=19), Analyze segment 13 (visits id=20), Analyze segment 14 (visits id=21-23)

```
sqlite> select "url_id: " || id, url, title from urls where id=5;
url_id: 5|https://accounts.craigslist.org/Login/home|craigslist account
sqlite> select "url_id: " || id, url, title from urls where id=2 or id=4;
url_id: 2|https://www.craigslist.org/craigslist: baltimore jobs, apartments, for sale, services, community, and events
url_id: 4|https://baltimore.craigslist.org/craigslist: baltimore jobs, apartments, for sale, services, community, and events
sqlite> select "url_id: " || id, url, title from urls where id between 7 and 9;
url_id: 7|https://post.craigslist.org/c/baltimore | choose type
url_id: 8|https://post.craigslist.org/k/shb0U0i_7BG68quUDIbeTbQ/bQTi5|baltimore | posting confirmation
url_id: 9|https://post.craigslist.org/k/shb0U0i_7BG68quUDIbeTbQ/bQTi5?s=type|baltimore | choose type
sqlite> select "url_id: " || id, url, title from urls where id=10;
url_id: 10|https://post.craigslist.org/k/shb0U0i_7BG68quUDIbeTbQ/bQTi5?s=cat|baltimore | choose category
sqlite> select "url_id: " || id, url, title from urls where id=11;
url_id: 11|https://post.craigslist.org/k/shb0U0i_7BG68quUDIbeTbQ/bQTi5?s=edit|baltimore | create posting
sqlite> select "url_id: " || id, url, title from urls where id=12;
url_id: 12|https://post.craigslist.org/k/shb0U0i_7BG68quUDIbeTbQ/bQTi5?s=geoverify|baltimore | add map
sqlite> select "url_id: " || id, url, title from urls where id=13;
url_id: 13|https://post.craigslist.org/k/shb0U0i_7BG68quUDIbeTbQ/bQTi5?s=editimage|baltimore | create posting
sqlite> select "url_id: " || id, url, title from urls where id=14;
url_id: 14|https://post.craigslist.org/k/shb0U0i_7BG68quUDIbeTbQ/bQTi5?s=preview|baltimore | create posting
sqlite> select "url_id: " || id, url, title from urls where id=8;
url_id: 8|https://post.craigslist.org/k/shb0U0i_7BG68quUDIbeTbQ/bQTi5|baltimore | posting confirmation
sqlite> select "url_id: " || id, url, title from urls where id=15;
url_id: 15|https://post.craigslist.org/manage/7473121658|baltimore | manage posting
sqlite> select "url_id: " || id, url, title from urls where id between 16 and 17;
url_id: 16|https://baltimore.craigslist.org/hab/d/baltimore-cheaper-than-rx-supplements/7473121658.html|cheaper than Rx supplements - health and beauty - by owner - ...
url_id: 17|https://www.google.com/search?q=gmail&rll=1C10NGR_enUS989US9896qq=gmail&aqs=chrome..69i57j0i433i512l6j0i131i433i512j0i433i512.1553j0j4&sourceid=chrome&ie=UTF-8|gmail - Google Search
sqlite> 
```

[Navigation icons] Right Ctrl

Analyze segment 15 (visits id=24-26), Analyze segment 15 part 2 (visits id=27-29), Analyze segment 15 part 3 (visits id=30-32), Analyze segment 15 part 4 (visits id=33-36), Analyze segment 16 (visits id=37-39), Analyze segment 17 part 1(visits id=40-41), Analyze segment 17 part 2 (visits id=42-43)

```
sqlite> select "url_id: " || id, url, title from urls where id between 18 and 20;
url_id: 18|https://www.google.com/gmail/Gmail: Free, Private & Secure Email | Google Workspace
url_id: 19|https://mail.google.com/mail/|Inbox (12) - unsub.fscs@gmail.com - Gmail
url_id: 20|https://mail.google.com/mail/u/0/|Inbox (12) - unsub.fscs@gmail.com - Gmail
sqlite> select "url_id: " || id, url, title from urls where id between 27 and 29;
url_id: 27|https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1|Gmail
url_id: 28|https://accounts.google.com/signin/v2/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1&flowName=GifWebSignIn&flowEntry=ServiceLogin|Gmail
url_id: 29|https://accounts.google.com/signin/v2/challenge/pwd?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1&flowName=GifWebSignIn&flowEntry=ServiceLogin&cid=1&navigationDirection=forward&TL=AM3QAYa1BR72H1BnwAVfbyUL6WFCiaAco03Di5PiNPclfyKBQPh15Z9040uek44c3|Gmail
sqlite> select "url_id: " || id, url, title from urls where id between 24 and 26;
url_id: 24|https://www.google.com/gmail/about/Gmail: Free, Private & Secure Email | Google Workspace
url_id: 25|https://accounts.google.com/AccountChooser/signinchooser?service=mail&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&flowName=GifWebSignIn&flowEntry=AccountChooser|Gmail
url_id: 26|https://accounts.google.com/AccountChooser?service=mail&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&flowName=GifWebSignIn&flowEntry=AccountChooser|Gmail
sqlite> select "url_id: " || id, url, title from urls where id between 27 and 29;
url_id: 27|https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1|Gmail
url_id: 28|https://accounts.google.com/signin/v2/identifier?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1&flowName=GifWebSignIn&flowEntry=ServiceLogin|Gmail
url_id: 29|https://accounts.google.com/signin/v2/challenge/pwd?continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&service=mail&sacu=1&rip=1&flowName=GifWebSignIn&flowEntry=ServiceLogin&cid=1&navigationDirection=forward&TL=AM3QAYa1BR72H1BnwAVfbyUL6WFCiaAco03Di5PiNPclfyKBQPh15Z9040uek44c3|Gmail
sqlite> select "url_id: " || id, url, title from urls where id between 24 and 26;
url_id: 24|https://www.google.com/gmail/about/Gmail: Free, Private & Secure Email | Google Workspace
url_id: 25|https://accounts.google.com/AccountChooser/signinchooser?service=mail&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&flowName=GifWebSignIn&flowEntry=AccountChooser|Gmail
url_id: 26|https://accounts.google.com/AccountChooser?service=mail&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F&flowName=GifWebSignIn&flowEntry=AccountChooser|Gmail
sqlite> select "url_id: " || id, url, title from urls where id between 19 and 20;
url_id: 19|https://mail.google.com/mail/|Inbox (12) - unsub.fscs@gmail.com - Gmail
url_id: 20|https://mail.google.com/mail/u/0/|Inbox (12) - unsub.fscs@gmail.com - Gmail
sqlite> select "url_id: " || id, url, title from urls where id between 33 and 34;
url_id: 33|https://mail.google.com/mail/u/0/#inbox/Inbox (12) - unsub.fscs@gmail.com - Gmail
url_id: 34|https://mail.google.com/mail/u/0/#inbox/WhctKKXXDrFcqXBGCnHkHGzNzbkXkdXnjTmxwZwPtjVmVHmrPPRthPXJgXngHcFLmggwv|cheaper than Rx supplements - order - unsub.fscs@gmail.com - Gmail
sqlite> 
```

Analyze segment 19 (visits id=44-45), Analyze segment 20 (visits id=46-48), Analyze segment 21 (visits id=49-50)

```
sqlite>
sqlite> select "url_id: " || id, url, title from urls where id between 35 and 36;
url_id: 35|https://mail.google.com/mail/u/0/#inbox/WhtCKXXDrfcqXBGcnHKhGxZnZbkXXdXnJtmxwZwPtjVmVHmrFPPRthPXJgXngHcFLmggWv?compose=JHrtffdgkFidrvzMfJPRMHgQmSZbjzPlcxTW
PRLXfsGwhzrQgsKTQWxQLFWsMhvscKrDpXcPbhKpCDnqPgtmpWSJWbLLCJcpRbwKDFNrmPLzKkvKl|cheaper than Rx supplements - order - unsub.fscs@gmail.com - Gmail
url_id: 36|https://mail.google.com/mail/u/0/#inbox/WhtCKXXDrfcqXBGcnHKhGxZnZbkXXdXnJtmxwZwPtjVmVHmrFPPRthPXJgXngHcFLmggWv?compose=DXDwSwxqg2WzDRtRJhRTXQgRWQdLXLDsZN
CgswmtqsxJBwbSdXxSkvPCxdcbxBxggBdwWDSvwScdmrjtqTpcdbWhdHQqGstTBblLnfbhchZLqdPKdpwL|cheaper than Rx supplements - order - unsub.fscs@gmail.com - Gmail
sqlite>
select "url_id: " || id, url, title from urls where id between 33 and 34;
select "url_id: " || id, url, title from urls where id=37;
url_id: 33|https://mail.google.com/mail/u/0/#inbox|inbox (12) - unsub.fscs@gmail.com - Gmail
url_id: 34|https://mail.google.com/mail/u/0/#inbox/WhtCKXXDrfcqXBGcnHKhGxZnZbkXXdXnJtmxwZwPtjVmVHmrFPPRthPXJgXngHcFLmggWv|cheaper than Rx supplements - order - unsub.
fscs@gmail.com - Gmail
url_id: 37|https://mail.google.com/mail/u/0/#inbox/WhtCKXXDrfcqXBGcnHKhGxZnZbkXXdXnJtmxwZwPtjVmVHmrFPPRthPXJgXngHcFLmggWv|cheaper than Rx supplements -- txid: 517b215
6914944339a96137ad8978408ea52b2fc144c98d3b0b16b21888afdc5 - unsub.fscs@gmail.com - Gmail
sqlite> select "url_id: " || id, url, title from urls where id between 38 and 39;
url_id: 38|https://www.google.com/url?q=https://imgur.com/dTgrkP7&source=gmail&ust=1650466604648000&usg=A0Vvaw0058wuJx6Jub4I72ZRaQpM|Imgur: The magic of the Internet
url_id: 39|https://imgur.com/dTgrkP7|Imgur: The magic of the Internet
sqlite> ■
```

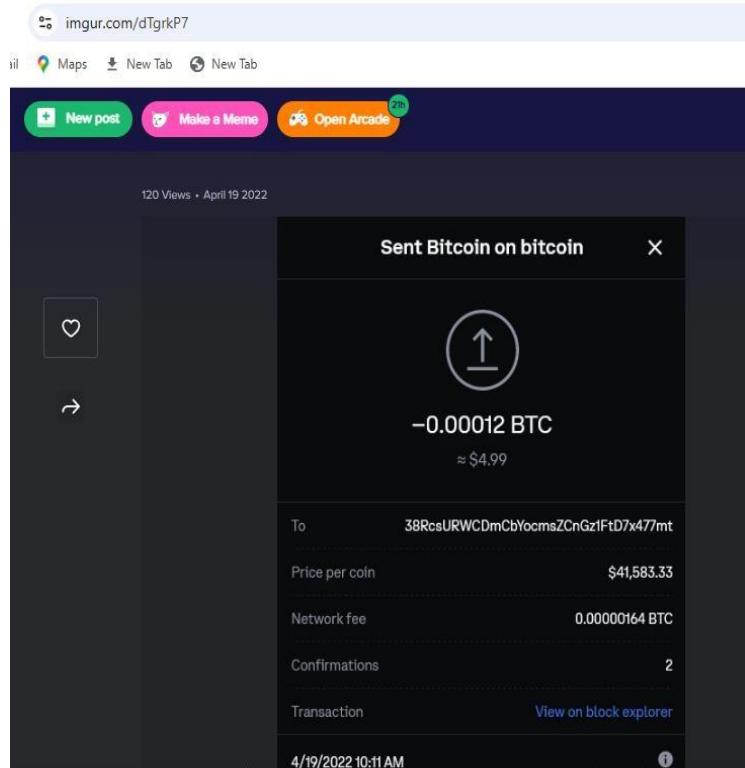
Imgur:

Imgur is an online image sharing and hosting service. Images can be uploaded anonymously and shared.

Imgur link received in Gmail and opened in above screenshot at url_id=39.

In database, you can see the imgur link from message has parameter source=gmail

Look at the imgur post – URL does not have enough information about the image post.



Block chain Explorer:

Block chain Explorer is a block and crypto transaction search engine – queries can include wallet addresses and transaction IDs.

visits id=50 Using the TXID from the Gmail message we can search it on a Blockchain Explorer to verify authenticity.

The screenshot shows a web browser displaying the Blockchain.com transaction explorer. The URL in the address bar is blockchain.com/explorer/transactions/btc/517b2156914944339a96137ad8978408ea52b2fc144c98d3b0b16b21888afdc5. The page title is "Blockchain.com". The main content area is titled "Bitcoin Transaction" and shows the following details:

- Broadcasted on 19 Apr 2022 07:12:09 GMT+5
- Hash ID: 517b2156914944339a96137ad8978408ea52b2fc144c98d3b0b16b21888afdc5
- Amount: 5.55267291 BTC • \$503,011
- Fee: 12,692 SATS • \$11.50
- From: bc1qm-p72ka
- To: 76 Outputs
- Status: Confirmed
- Fee/VB: 4.987 sat/vByte
- Weight: 10,177
- Coinbase: No
- RBF: No
- Version: 1
- Block ID: 732,558
- Time: 19 Apr 2022 07:12:09
- Inputs: 1
- Outputs: 76
- Output Value: 5.55267291 BTC
- Fee/B: 4.833 sat/B
- Size: 2,626 Bytes
- Weight Unit: 1.247 sat/WU
- Witness: Yes
- Locktime: 0
- BTC Price: \$90,589.07

The page also includes a summary stating: "This transaction was first broadcasted on the Bitcoin network on April 19, 2022 at 07:12 AM GMT+5. The transaction currently has 199,285 confirmations on the network. The current value of this transaction is now \$503,011."

This segment is a transition from the transaction to a wallet address:

Analyze segment 25 (visits id=58), Analyze segment 26 (visits id=59-60)

```
(root㉿kali)-[~/home/kali]
# sqlite3 History

SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> select "url_id" || id, url, title from urls where id=44;
url_id: 44|https://www.blockchain.com/btc/address/38RcsURWCDmCbYocmsZCnGz1FtD7x477mt|Address: 38RcsURWCDmCbYocmsZCnGz1FtD7x477mt | Blockchain Explorer
sqlite> select "url_id" || id, url, title from urls where id=45;
url_id: 45|https://www.google.com/search?q=kraken&rllz=1C10NGR_enUS989US989&oq=kraken&aqs=chrome..69i57j46i67i433j0i67j0i67i433j0i67j0i131i433i512j0i512l2
.2504j0j7ssourceid=chrome&ie=UTF-8|kraken - Google Search
sqlite> select "url_id" || id, url, title from urls where id=46;
url_id: 46|https://www.kraken.com/en-us/sign-in|Sign in to Kraken - Kraken | Buy, Sell and Margin Trade Bitcoin (BTC) and Ethereum (ETH)
sqlite> select "url_id" || id, url, title from urls where id=47-49;
```

Kraken:

Kraken is a cryptocurrency exchange and banking platform.

This segment is a transition from Google search results to www.kraken.com.

Analyze segment 27 (visits id=61-62)

This segment is the transition from the mempool.space page to Kraken History Ledger page. Analyze segment 31 (visits id=71).

This segment are the transitions back to suspect's Gmail inbox and another two replies being composed to one message. Analyze segment 32 (visits id=72-73).

```
(root@kali)-[~/home/kali]
# sqlite3 History

SQLite version 3.46.1 2024-08-13 09:16:08
Enter ".help" for usage hints.
sqlite> select "url_id: " || id, url, title from urls where id=55;
url_id: 55|https://www.kraken.com/u/history/ledger|41,563.70 USD - Kraken - History - Ledger
sqlite> select "url_id: " || id, url, title from urls where id=55;
url_id: 55|https://www.kraken.com/u/history/ledger|41,563.70 USD - Kraken - History - Ledger
sqlite> select "url_id: " || id, url, title from urls where id=56;
url_id: 56|https://mail.google.com/mail/u/0/#inbox/WhctKXXDrfCqvtRjhGdkMBqVNFnwtCnJjRvqlXsZNkFbrkGDZwdVPkdDvjBPxRxDLqKDSv?compose=JHrtffdgkFjdsFdVFrNvsxdZrPvcWRNCNxk
cfgKzhGsgLbhJdvrmbxZmtmQDrNtCmsDQGGwsbKqsWgvflHKLJRfkQxxzGKQpdVVBLCgMpnk|cheaper than Rx supplements - order - unsub.fscs@gmail.com - Gmail
sqlite> select "url_id: " || id, url, title from urls where id=57;
url_id: 57|https://mail.google.com/mail/u/0/#inbox/WhctKXXDrfCqvtRjhGdkMBqVNFnwtCnJjRvqlXsZNkFbrkGDZwdVPkdDvjBPxRxDLqKDSv?compose=xQTrpQHKFJPcWTcvdCmpkQMlJJjqLLXrvVm
rRlfJzMfBKjnCHwKnnVqVKNLwLLQrtxpznXkFwdTSMpnQJfQhFggKjBjXlgJFGBxgfTTBSfTzxLhpGtTp|cheaper than Rx supplements - order - unsub.fscs@gmail.com - Gmail
sqlite> 
```

Materials of Interest:

Material	Description/Value	Value
Possible Suspect Location	Baltimore Region	Narrows search area
Suspect/Dealer-Buyer TXID	517b2156914944339a96137ad8978408ea52b2fc144c98d3b0b 16b21888afdc5	Allows us to create a paper trail for transaction
Suspect BTC Wallet Address	38RcsURWCDmCbYocmsZCnGz1FtD7x477mt	Can monitor BTC address
Suspect Email Address	unsub.fscs@gmail.com	Can monitor email address
Downloaded File	proof_of_payment.png	Connects receipt of transaction to suspect
Downloads File Location	C:\Users\FSCS_User\Desktop\	Gives us an idea of suspect's device file structure
Chrome History File Location	C:\Users\FSCS_User\Local\Google\Chrome\User Data\Default\	

Confirming Hypothesis with Timeline

1. Suspected drug dealer posted ad on a website listing sale of illegal drugs

Visit ID	Date	Description	Duration (in second)
1	Tue Apr 19 09:54:18 AM EDT 2022	User typed "craiglist" into Chrome address bar and generate a URL	0 (indicate a redirect)
2	Tue Apr 19 09:54:19 AM EDT 2022	Without any delay (duration =0), Chrome sends the URL to Google and google returns results in web page with the title "craiglist - Google Search"	User stayed in the page for 0.727 second
3-5	Tue Apr 19 09:54:19 AM EDT 2022	User clicked a link (from visits.id=2) and visited https://www.craigslist.org/ . However, it was redirected to https://geo.craigslist.org/ and https://baltimore.craigslist.org/	User stayed in the page https://baltimore.craigslist.org/ for 2.465 second
6-7	Tue Apr 19 09:54:22 AM EDT 2022	User click an account link https://accounts.craigslist.org/login/home in order to log in. User was redirected to another link https://accounts.craigslist.org/login?rp=%2Flogin%2Fhome&rt=L	User stayed in the page https://post.craigslist.org/c/bal for 17 second
8	Tue Apr 19 09:54:39 AM EDT 2022	User filled out the form and submit	User stayed in the page for 29 second

1. Suspected drug dealer posted ad on a website listing sale of illegal drugs

Visit ID	Date	Description	Duration (in second)
9-10	Tue Apr 19 09:55:03 AM EDT 2022	User clicked a link https://www.craigslist.org/ and was redirected to https://baltimore.craigslist.org/	User stayed in the page for 24 second
11-13	Tue Apr 19 09:55:05 AM EDT 2022	User clicked a link (create a posting) https://post.craigslist.org/c/bal User was redirect to url id 8 and then url id 9	User stayed in the page url id 9 for 4 second
14	Tue Apr 19 09:55:10 AM EDT 2022	User filled out the form (chosen types) and submit it User needs to choose category	User stayed in the page for 5 second
15	Tue Apr 19 09:55:15 AM EDT 2022	User filled out the form (select category) and submit it User needs to add information (description, title, price, delivery, etc.)	User stayed in the page for 17 second
16	Tue Apr 19 09:58:13 AM EDT 2022	User filled out the form (description title, price, delivery, etc.) User needs to choose their location	User stayed in the page for 4 second
17	Tue Apr 19 09:58:17 AM EDT 2022	User filled out the form (choose location) User needs to choose to upload image or not	User stayed in the page for 1 second
18	Tue Apr 19 09:58:19 AM EDT 2022	User filled the form (choose image option), URL doesn't show if they uploaded an image or not but we can always check the post itself User can edit post, edit location, edit images or publish post	User stayed in the page for 3 second
19	Tue Apr 19 09:58:22AM EDT 2022	User filled the form (selected publish) User can share, view, or manage post or return to account page	User stayed in the page for 4 second

1. Suspected drug dealer posted ad on a website listing sale of illegal drugs

Visit ID	Date	Description	Duration (in second)
20	Tue Apr 19 09:58:27 AM EDT 2022	User clicked a link (https://post.craigslist.org/manage/7473121658 baltimore) to manage the post User can edit post, update images, edit location, delete post or visit post	User stayed in the page for 5 second
21-23	Tue Apr 19 09:58:31 AM to 09:58:39 AM EDT 2022	User clicked a link (https://baltimore.craigslist.org/hab/d/baltimore-cheaper-than-rx-supplements/7473121658.html) to view post Then user typed "gmail" in Chrome address bar and URL was generated to Google Search results	User stayed in the page 17 for .8 second

2. Interested buyer messaged dealer

Visit ID	Date	Description	Duration (in second)
24-26	Tue Apr 19 09:58:40 AM AM EDT 2022	User clicked a link (https://www.google.com/gmail) to Gmail Then user was redirected to unsub.fscs@gmail.com inbox Then user was redirected to URL containing path /u/0/ indicating user is logged into account 0	User stayed in the page for 0 second
27-29	Tue Apr 19 09:58:40 AM AM EDT 2022	User was redirected to accounts.google.com with the URL to their inbox as a parameter to ServiceLogin?service=mail.google.com User was then directed to about page /help/about.html on mail.google.com User was then redirected again to another about page /help.about.html on google.com	User stayed in the page for 0 second
30-32	Tue Apr 19 09:58:40 AM AM to 09:58:43 AM EDT 2022	User clicked a link (https://www.google.com/gmail/About/) to Google Workspace Then user clicked a link (https://accounts.google.com/AccountChooser/) with query /signinchooser?service=mail to a login page Then user was redirected to accounts.google.com with query AccountChooser?service=mail to choose an account	User stayed in the page for 0 second

2. Interested buyer messaged dealer

Visit ID	Date	Description	Duration (in second)
33-36	Tue Apr 19 09:58:43 AM AM to 09:58:44 AM EDT 2022	User clicked a link (https://accounts.google.com/) to Gmail with query ServiceLogin?continue= to a login page Then user clicked a link (https://accounts.google.com/) to Gmail with same query (https://accounts.google.com/) to Gmail with path /signin/ with query Identifier?continue to a login page prompting identifier email address/username Then user clicked a link (https://accounts.google.com/) with path /signin/challenge/ and query pwd?continue= to a login page prompting challenge password	User stayed in the page 29 for 2 second
37-39	Tue Apr 19 09:59:29 AM EDT 2022	User clicked a link (https://accounts.google.com/) with query CheckCookie?continue= and parameter value loginDoneHtml to unsub.fscs@gmail.com 's inbox Then user was redirected (https://mail.google.com/) with path /accounts/ and query SetOSID?authuser to unsub.fscs@gmail.com 's inbox Then user was redirected (https://accounts.youtube.com/) with path /accounts/ and query SetSID? To unsub.fscs@gmail.com 's inbox	User stayed in the page for 0 second

2. Interested buyer messaged dealer

Visit ID	Date	Description	Duration (in second)
40-41	Tue Apr 19 09:59:29 AM EDT 2022	User clicked a link (https://mail.google.com/) with path /mail/ to unsub.fscs@gmail.com 's inbox User clicked a link (https://mail.google.com/) with path /u/0/ to unsub.fscs@gmail.com 's inbox	User stayed in the page for 0 second
42-43	Tue Apr 19 09:59:31 AM AM to 10:04:12 EDT 2022	User clicked a link (https://mail.google.com/) with path /mail/u/0/#inbox to unsub.fscs@gmail.com 's inbox User clicked a link (https://mail.google.com/) with string WhctKIXXDrfCq... indicating ID for opened email with subject header cheaper than Rx supplements - order	User stayed in the page for 0 second

3. Dealer replied with transaction details (Bitcoin wallet)

Visit ID	Date	Description	Duration (in second)
44-45	Tue Apr 19 10:04:35 AM AM to 10:04:46 EDT 2022	User clicked a link (https://mail.google.com/) with query ?compose=JHrtff referring to open message WhctKKXX with subject header " order " User then clicked a link (https://mail.google.com/) with query ?compose=DxDWs referring to same message WhctKKXX indicating two replies were made for the same message	User stayed in the page for 0 second

4. Buyer sent payment

Visit ID	Date	Description	Duration (in second)
46-48	Tue Apr 19 10:04:52 AM AM to 10:04:59 EDT 2022	User clicked a link (https://mail.google.com/mail/u/0/#inbox) to unsub.fscs@gmail.com's inbox User clicked a link (https://mail.google.com/mail/u/0/#inbox) with string WhctKKXXDrFCqXBGC "order" message open User clicked a link (https://mail.google.com/mail/u/0/#inbox) with string WhctKKXXDrfCqtRj , another new message with subject header " txid: 517b2159... "	User stayed in the page for 0 second

5. Dealer confirmed payment

Visit ID	Date	Description	Duration (in second)
49-50	Tue Apr 19 10:56:52 AM EDT 2022	User clicked a link (https://www.google.com/) with query url=https://imgur.com/dTgrkp7 and parameter source=gmail indicating the imgur link originated from a Gmail message User clicked a link (https://imgur.com/dTgrkp7) to imgur post	User stayed in the page 39 for 18 second
51-52	Tue Apr 19 10:58:59 AM to 10:59:00 EDT 2022	User typed " blockchain explorer " into Chrome address bar and generated a URL to Google Search results	User stayed in the page for 1 second
53-54	Tue Apr 19 10:59:01 AM to 10:59:02 EDT 2022	User clicked a link (https://www.blockchain.com/explorer) to Blockchain Explorer	User stayed in the page for 18 second

5. Dealer confirmed payment

Visit ID	Date	Description	Duration (in second)
55-57	Tue Apr 19 10:59:06 AM EDT 2022	User clicked a link (https://www.blockchain.com/) with query ?search= value 517b215... then a URL was generated User then clicked a link (https://blockchain.com/) with path /btc/tx and string matching 517b215 transaction to view the transaction	User stayed in the page for 0 second
58	Tue Apr 19 10:59:21 AM EDT 2022	User clicked a link (https://www.blockchain.com) with path /btc/address/ and string 38RcsURW... to the suspect's address	User stayed in the page for 0 second
59-60	Tue Apr 19 10:59:38 AM to 10:59:39 AM EDT 2022	User typed " kraken " into Chrome address bar and generated a URL to Google Search results	User stayed in the page for 7 second
61-62	Tue Apr 19 10:59:47 AM EDT 2022	User clicked link (https://kraken.com/) with path /en-us/sign in to Kraken Sign in page	User stayed in the page for 0 second
63-65	Tue Apr 19 11:00:21 AM to 11:01:12 AM EDT 2022	User clicked a link (https://www.kraken.com) with path /en-us/device-approval to approve signing in from new device User then clicked a link (https://www.kraken.com) with path /u/ and query trade?=true after successfully signing-in User then clicked a link (https://www.kraken.com) with path /u/instant	User stayed in the page for 104 seconds or 1.7 minutes

5. Dealer confirmed payment

Visit ID	Date	Description	Duration (in second)
66	Tue Apr 19 11:00:21 AM EDT 2022	User clicked a link (https://www.kraken.com) with path /u/funding to Funding page	User stayed in the page for 0 seconds
67-70	Tue Apr 19 11:01:31 AM to 11:01:33 AM EDT 2022	User clicked a link (https://www.kraken.com) with query redirect?url= pointing to https://mempool.space/tx/517b21... Then page is refreshed by server Then refresh page is redirected to link (https://www.kraken.com) with query redirect? and title Transaction: 517b21.. Then redirected to link (https://mempool.space) with path /tx/517b21...	User stayed in the page for 0 seconds
71	Tue Apr 19 11:02:05 AM EDT 2022	User clicked a link (https://www.kraken.com) with path /u/history/ledger to Kraken History Ledger page	User stayed in the page for 0 seconds

6-7. Dealer shipped drugs and buyer received drugs

Visit ID	Date	Description	Duration (in second)
72-73	Tue Apr 19 11:02:05 AM to 11:02:44 AM EDT 2022	User clicked a link (https://mail.google.com) with path /u/0/#inbox with string pointing to WhctKXXdRfC... message with subject " order " and query ?compose=JhrtffdgkF... as one reply to the message User then clicked a link (https://mail.google.com) with same path pointing to same WhctKXXdRfC... message but with another reply xQTrpQHKf...	User stayed in the page for 0 seconds
74	Tue Apr 19 11:02:05 AM EDT 2022	User clicked a link (https://mail.google.com) with path /mail/u/0/#inbox/ with string WhctKXXDRf message with subject header txid from earlier visit id=48	User stayed in the page for 0 seconds

Practical: User_web_activity

Define recourse on a web server

HTML files and images

Save resource to a specific location on web server

/var/www/html/

Find the domain name/IP

URL in a browser

- Download an image building.jpg
- Save it to /var/www/html
- Add building.jpg in a webpage image.html
- Show the webpage with the image

```
[root@kali]~[/home/kali]
# cd /var/www/html/
[root@kali]~[/var/www/html]
# ls
dvwa

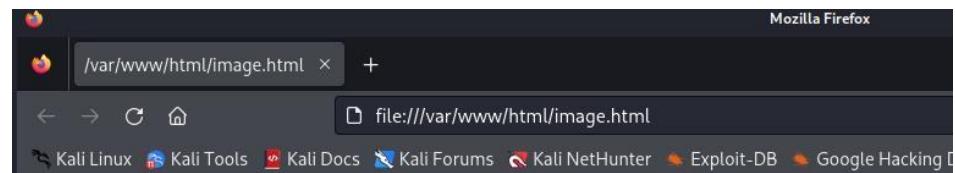
[root@kali]~[/var/www/html]
# ls -l /var/www/html
total 4
drwxr-xr-x 12 www-data www-data 4096 Jul 13 14:58 dvwa

[root@kali]~[/var/www/html]
# chmod 777 /var/www/html
[root@kali]~[/var/www/html]
# ls -l /var/www/html
total 4
drwxr-xr-x 12 www-data www-data 4096 Jul 13 14:58 dvwa

[root@kali]~[/var/www/html]
# wget -q https://www.dropbox.com/s/jiq17tgi8u1xls3/building.jpg
[root@kali]~[/var/www/html]
# ls
building.jpg dvwa

[root@kali]~[/var/www/html]
# ls -l /var/www/html
total 72
-rw-r--r-- 1 root      root      68661 Jan 11 10:54 building.jpg
drwxr-xr-x 12 www-data www-data 4096 Jul 13 14:58 dvwa

[root@kali]~[/var/www/html]
#
```



My First Heading

My first paragraph.



How an agent requests resource using a URL?

```
[root@kali]~| /var/www/html]
# curl -v 127.0.0.1/image.html
* Trying 127.0.0.1:80 ...
* Connected to 127.0.0.1 (127.0.0.1) port 80
> GET /image.html HTTP/1.1
> Host: 127.0.0.1
> User-Agent: curl/8.9.1
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Sun, 11 Jan 2026 16:07:42 GMT
< Server: Apache/2.4.58 (Debian)
< Last-Modified: Sun, 11 Jan 2026 16:05:48 GMT
< ETag: "88-6481eee87ea98"
< Accept-Ranges: bytes
< Content-Length: 136
< Vary: Accept-Encoding
< Content-Type: text/html
<
<!DOCTYPE html>
<html>
<body>

<h1>My First Heading</h1>

<p>My first paragraph.</p>


</body>
</html>
* Connection #0 to host 127.0.0.1 left intact

[root@kali]~| /var/www/html]
#
```

Curl a live page of University of Baltimore at /var/www/html/about/ub-strategic-plan.cfm

```
[root@kali]~| /var/www/html]
# curl -v http://www.ubalt.edu/about-ub/ub-strategic-plan.cfm | more
% Total    % Received % Xferd  Average Speed   Time     Time      Time  Current
          Dload  Upload   Total   Spent    Left  Speed
0       0     0     0       0      0  --:--:-- --:--:-- --:--:-- 0* Host www.ubalt.edu:80 was resolved.
IPv6: (none)
IPv4: 204.52.129.211
Trying 204.52.129.211:80 ...
0       0     0     0       0      0  --:--:-- --:--:-- --:--:-- 0* Connected to www.ubalt.edu (204.52.129.211) port 80
GET /about-ub/ub-strategic-plan.cfm HTTP/1.1
Host: www.ubalt.edu
User-Agent: curl/8.9.1
Accept: */*

Request completely sent off
HTTP/1.1 404 Not Found
Content-Length: 50385
Content-Type: text/html; charset=UTF-8
Server: Microsoft-IIS/10.0
Set-Cookie: CFID=194238653; Expires=Mon, 12-Jan-2026 16:09:28 GMT; Path=/; HttpOnly
Set-Cookie: CFTOKEN=30b4b701938989c6-CA2C9266-0CBB-C127-39AB34AE2F812326; Expires=Mon, 12-Jan-2026 16:09:28 GMT; Path=/; HttpOnly
X-Powered-By: ASP.NET
Access-Control-Allow-Origin: *
Date: Sun, 11 Jan 2026 16:09:27 GMT
X-Connection: close
Set-Cookie: BIGipServer611/wppqZLyANkvhXT2uPA=!hZnh0bTMZWadGie5haiV6TQall8yW5eeGAwciUKx3xM1aW6XFqplTBhRC56JUkV115I4VbWe3bjrj4=; path=/; HttpOnly
Set-Cookie: f5avraaaaaaaaaaaa_session_=NEJ0DMBCHNBKFNLLGNPGDFLBFGIHOOJBPKDPOIOLGKDAFGOEMNLDMNKHNCPHHKAJDEDIELPCKDFHDLBACNAJGGKKMFFCNLJNCCLMAELLKFOLKEHPOL
PLHKPJ; HttpOnly;
```

What is URL redirecting?

- “This thing is no longer here. Go over here.”
- Browser may redirect URLs for various reasons:
 - Site moved to new domain
 - Several different URLs for one site
 - Merging sites together
 - Page removed
- Redirect reasons are not recorded by browsers
 - Must guess what reason for redirect might be

```
└─(root㉿kali)-[~/var/www/html]
  └─# curl -v google.com
* Host google.com:80 was resolved.
* IPv6: 2a00:1450:4018:80d::200e
* IPv4: 142.250.202.238
* Trying 142.250.202.238:80 ...
* Connected to google.com (142.250.202.238) port 80
> GET / HTTP/1.1
> Host: google.com
> User-Agent: curl/8.9.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 301 Moved Permanently
< Location: http://www.google.com/
< Content-Type: text/html; charset=UTF-8
< Content-Security-Policy-Report-Only: object-src 'none'
< Content-Security-Policy: default-src 'none'; script-src 'self' https:; report-uri https://csp.withgoogle.com/report-uri
< Date: Sun, 11 Jan 2026 16:18:40 GMT
< Expires: Tue, 10 Feb 2026 16:18:40 GMT
< Cache-Control: public, max-age=2592000
< Server: gws
< Content-Length: 219
< X-XSS-Protection: 0
< X-Frame-Options: SAMEORIGIN
<
<HTML><HEAD><meta http-equiv="content-type" content="text/html; charset=UTF-8">
<TITLE>301 Moved</TITLE></HEAD><BODY>
<H1>301 Moved</H1>
The document has moved
<A HREF="http://www.google.com/">here</A>.
</BODY></HTML>
* Connection #0 to host google.com left intact
```

```

[+] Root@Kali : /var/www/html/
# curl -v http://www.google.com
* Host www.google.com:80 was resolved.
* IPv6: 2a00:1450:4018:812 :: 2004
* IPv4: 142.250.202.36
* Trying 142.250.202.36:80 ...
* Connected to www.google.com (142.250.202.36) port 80
> GET / HTTP/1.1
> Host: www.google.com
> User-Agent: curl/8.9.1
> Accept: */*
>
* Request completely sent off
< HTTP/1.1 200 OK
< Date: Sun, 11 Jan 2026 16:18:55 GMT
< Expires: -1
< Cache-Control: private, max-age=0
< Content-Type: text/html; charset=ISO-8859-1
< Content-Security-Policy-Report-Only: object-src 'none';base-uri 'self';script-src 'nonce-ACg-H7MAoPg0wr2P49wzaw' 'strict-dynamic' 'report-afe-inline' https: http://report-uri https://csp.withgoogle.com/csp/gws/other-hp
< P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info."
< Server: gws
< X-XSS-Protection: 0
< X-Frame-Options: SAMEORIGIN
< Set-Cookie: __Secure-STRP=AD6Dogur_AsUXUVSMGNicORK6MzFD7ndd7MMSuRkHcInYsjooylMZYeTsKs8ISyWkRlykMzF__g3MDeP0R24sXrrUkBhN1fiMoQi; expires=Sun, 11-Jan-2026 16:18:55 GMT; path=/; domain=.google.com; Secure; SameSite=strict
< Set-Cookie: AEC=AaJma5uDbZTtkP3IsafroUwZwfvpBSzm0QGXG8CbqeSqbRHvNu6Q0q2ng; expires=Fri, 10-Jul-2026 16:18:55 GMT; path=/; domain=.google.com; eSite=lax
< Set-Cookie: NID=528=IJJzsvUctVMk_ofqFHN_lK0qzqbSaE1YouM5CFiueB1FB_9zDtQMVSbE9ww07H5zcapQuZBIS4qJ09AmUqaKu6-zC2hVGwu7uPwaFeBLbyL4yw-FGRTYSFG_C9IqNLGmrCx6J3nxWUKUHajrlespIh6RPNMmkYt_GZwt-vFDAzuklzlne0dBkS8ypHcqVYrmlP; expires=Mon, 13-Jul-2026 16:18:55 GMT; path=/; domain=.google.com
< Accept-Ranges: none
< Vary: Accept-Encoding
< Transfer-Encoding: chunked

```

Location of Google Chrome history

- Windows XP
 - **C:\Documents and Settings\<username>\Local Settings\Application Data\Google\Chrome\User Data\Default**
 - **C:\Documents and Settings\<username>\Local Settings\Application Data\Google\Chrome\User Data\Default\Cache**
- Windows Vista, 7, 8, 10
 - **C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default**
 - **C:\Users\<username>\AppData\Local\Google\Chrome\User Data\Default\Cache**
- Mac OS X
 - **/Users/<username>/Library/Application Support/Google/Chrome/Default**
 - **/Users/<username>/Library/Caches/Google/Chrome/Default/Cache**
- Linux/Unix
 - **/home/<username>/.config/google-chrome/Default**
 - **/home/<username>/.cache/google-chrome/Default/Cache**