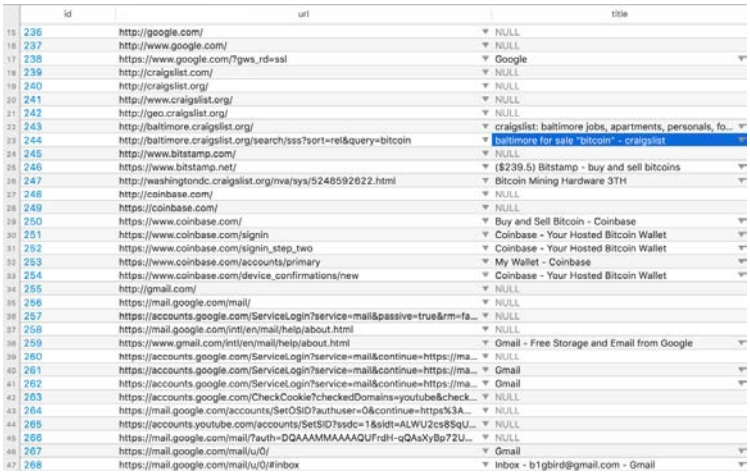
Log Analysis

History (Medium)

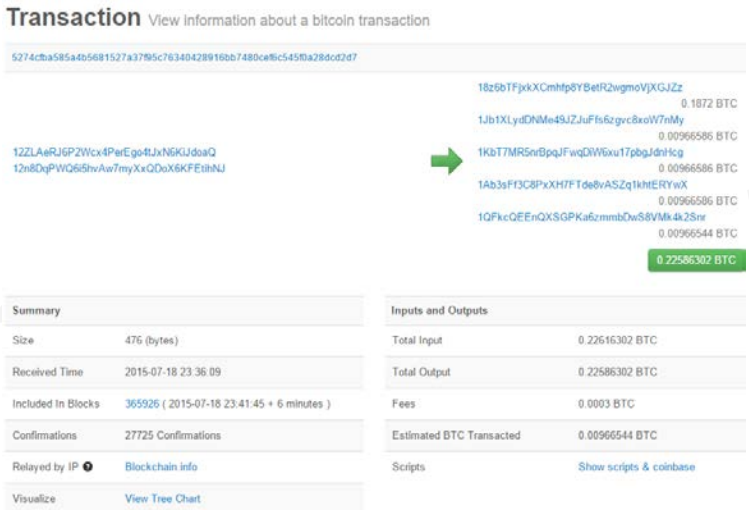
This challenge evaluates the contestant's ability to analyze a SQLite database. The answers can be obtained by using the "sqlite3" Linux program or a GUI-based viewer. The examples below use the SQLPro viewer for OSX.

Questions 1 – 4 can be answered by simply looking at the url and title columns.



	id	url	title
15	236	http://google.com/	NULL
16	237	http://www.google.com/	NULL
17	238	https://www.google.com/?gws_rd=ssl	Google
18	239	http://craigslist.com/	NULL
19	240	http://craigslist.org/	NULL
20	241	http://www.craigslist.org/	NULL
21	242	http://geo.craigslist.org/	NULL
22	243	http://baltimore.craigslist.org/	craigslist: baltimore jobs, apartments, personals, fo...
23	244	http://baltimore.craigslist.org/search/sss?sort=rel&query=bitcoin	baltimore for sale "bitcoin" - craigslist
24	245	http://www.bitstamp.com/	NULL
25	246	https://www.bitstamp.net/	($239.5) Bitstamp - buy and sell bitcoins
26	247	http://washingtondc.craigslist.org/nva/sys/5248592622.html	Bitcoin Mining Hardware 3TH
27	248	http://coinbase.com/	NULL
28	249	https://coinbase.com/	NULL
29	250	https://www.coinbase.com/	Buy and Sell Bitcoin - Coinbase
30	251	https://www.coinbase.com/signin	Coinbase - Your Hosted Bitcoin Wallet
31	252	https://www.coinbase.com/signin_step_two	Coinbase - Your Hosted Bitcoin Wallet
32	253	https://www.coinbase.com/accounts/primary	My Wallet - Coinbase
33	254	https://www.coinbase.com/device_confirmations/new	Coinbase - Your Hosted Bitcoin Wallet
34	255	http://gmail.com/	NULL
35	256	https://mail.google.com/mail/	NULL
36	257	https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=fa...	NULL
37	258	https://mail.google.com/intl/en/mail/help/about.html	NULL
38	259	https://www.gmail.com/intl/en/mail/help/about.html	Gmail - Free Storage and Email from Google
39	260	https://accounts.google.com/ServiceLogin?service=mail&continue=https://ma...	NULL
40	261	https://accounts.google.com/ServiceLogin?service=mail&continue=https://ma...	Gmail
41	262	https://accounts.google.com/ServiceLogin?service=mail&continue=https://ma...	Gmail
42	263	https://accounts.google.com/CheckCookie?checkedDomains=youtube&check...	NULL
43	264	https://mail.google.com/accounts/SetOSID?authuser=0&continue=https%3A...	NULL
44	265	https://accounts.youtube.com/accounts/SetSID?ssdc=1&sidt=ALWU2cs8SqU...	NULL
45	266	https://mail.google.com/mail/?auth=DQAAAMMAAAAQUFrdH-qQAaXyBp72U...	NULL
46	267	https://mail.google.com/mail/u/0/	Gmail
47	268	https://mail.google.com/mail/u/0/#inbox	Inbox - b1gbird@gmail.com - Gmail

Questions 5 – 7 can be answered by visiting the URLs listed in the database. The URL with id 290 is for a bitcoin transaction listed on blockchain.info. The main page displays the ID as well as the total value of the inputs.



Transaction View information about a bitcoin transaction

5274cfba585a4b5681527a37f95c76340428916bb7480ce8c545f0a28dcd2d7

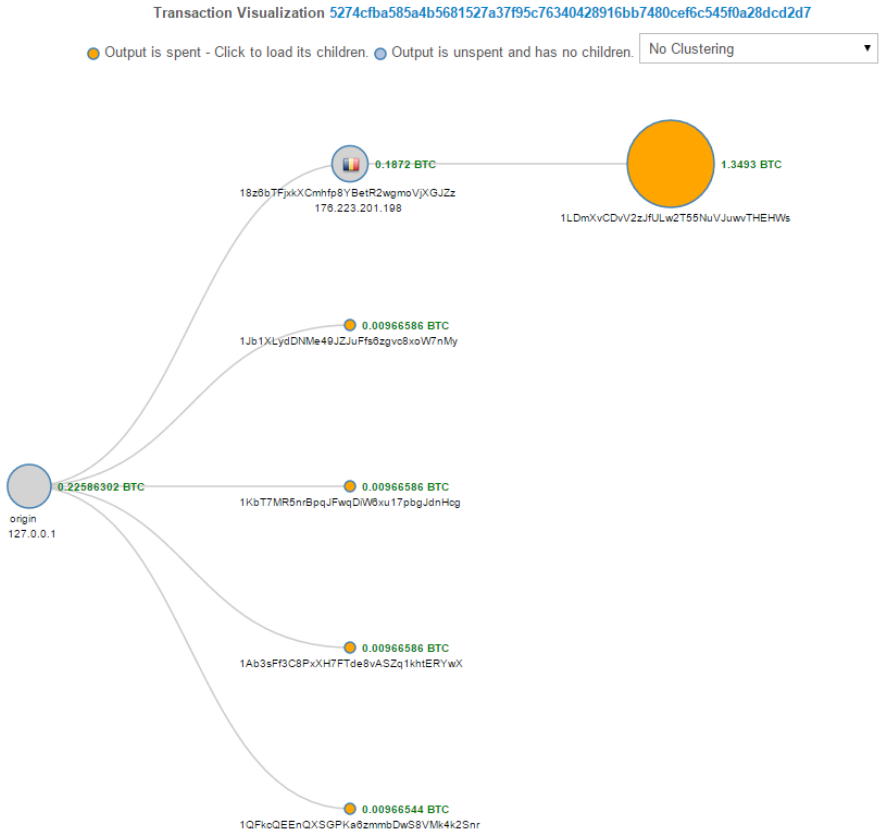
12ZLAeRJ6P2Wcx4PerEgo4tJxN6KiJdoaQ
12n8DqPWQ6i5hvAw7myXxQDoX6KFEthNJ

18z6bTFjxkXCmhfp8YBetR2wgmoVjXGJZz 0.1872 BTC
1Jb1XLydDNMe49JZJuFfs6zgvc8xoW7nMy 0.00966586 BTC
1KbT7MR5nrBpqJFwqDiW6xu17pbgJdnHcg 0.00966586 BTC
1Ab3sFf3C8PxXH7FTde8vASZq1khtERYwX 0.00966586 BTC
1QFkcQEEnQXSGPKa6zmmbDwS8VMk4k2Snr 0.00966544 BTC

0.22586302 BTC

Summary		Inputs and Outputs	
Size	476 (bytes)	Total Input	0.22616302 BTC
Received Time	2015-07-18 23:36:09	Total Output	0.22586302 BTC
Included In Blocks	365926 (2015-07-18 23:41:45 + 6 minutes)	Fees	0.0003 BTC
Confirmations	27725 Confirmations	Estimated BTC Transacted	0.00966544 BTC
Relayed by IP	Blockchain.info	Scripts	Show scripts & coinbase
Visualize	View Tree Chart		

The “View Tree Chart” link provides a visualization of outputs along with the IP addresses of the Bitcoin wallets.



Question	Answer
What did the user search for on Craigslist?	`bitcoin`
What was the current price of bitcoin when the user was browsing?	`$239.50`
What Bitcoin exchange did the user log in to?	`Coinbase`
What is the email that was used to log into the bitcoin exchange?	`b1gbird@gmail.com`
What was the ID of the Bitcoin transaction that the user looked at?	`5274cfba585a4b5681527a37f95c76340428916bb7480cef6c545f0a28dcd2d7`
What was the total value of all the inputs of the Bitcoin transaction?	`0.22616302`
To which IP address did the majority of the Bitcoin in the transaction go?	`176.223.201.198`