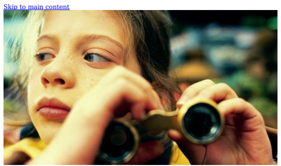
Skip to main content



How pre-teens using metadata found a whistleblower in two hours

Posted Mon 12 Dec 2016, 6:58pm
Updated Mon 12 Dec 2016, 10:34pm

By James Purtill

Team Sherlock began the scenario with one clue: the leaked documents about fracking chemicals had been sent to anna@minewatch.org.au.

With access to the kind of metadata that has been retained and made available to Australian government agencies for the past year, the team of three primary school students were then able to track down the mock corporate whistleblower in two hours.

They were part of a 'cyber fox hunt' co-hosted by University of Melbourne to explore how Australia's 2015 metadata laws affect our privacy. In the scenario, twelve teams used software to filter through a database of mobile, internet and location metadata. All but one team tracked down the home address of the whistleblower, and the winning team took just one hour.

Hunting the snitch.

Supplied

Since October 2015, potentially every phone call you make, text message you send and email you write has been tracked by the government. Only authorised agencies can access metadata, though many unauthorised government organisations have been getting around this by asking the AFP to do metadata searches for them. They don't need a warrant, and they don't need to warn you. It's just possible that sometime in 2016 unauthorised agencies such as Racing NSW and the Taxi Services Commission (Victoria) have asked the AFP to search your metadata.

Your metadata includes the addresses of people you have emailed, the numbers of people you have called, the time, date and duration of the communication, the location of your phone, and the postal and billing addresses of your mobile plan. Because this is intangible and abstract, it can be hard to grasp what this means for your privacy, which is why Melbourne University co-organised the 'snitch hunt'. Gen, a 12-year-old from Team Sherlock, told *Hack* how her team used the metadata.

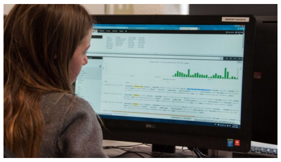
"It was a lot easier than I expected," she said.

"Basically what happened was we found the data that had the Google searches and the ones that corresponded with searches the whistleblower would use. We then found the IP address they used with the Google searches and we linked the IP address to their email. We used the email to find their phone number and their address."

Dr Suelette Dreyfus, a Melbourne Uni technology researcher and privacy expert who helped organise the 'snitch hunt' at the weekend, said she was "shocked, surprised and slightly horrified" by how quickly the teams found the whistleblower.

"It illustrates this data is easy to get - agencies don't need to have a warrant," she said.

You can have a go at the scenario here, using the analysis tools to try and find the whistleblower. Or read below for a step-by-step guide. (The screenshots aren't of what people would have searched for in the scenario, but they are of the same kinds of searches).



Searching the metadata database.

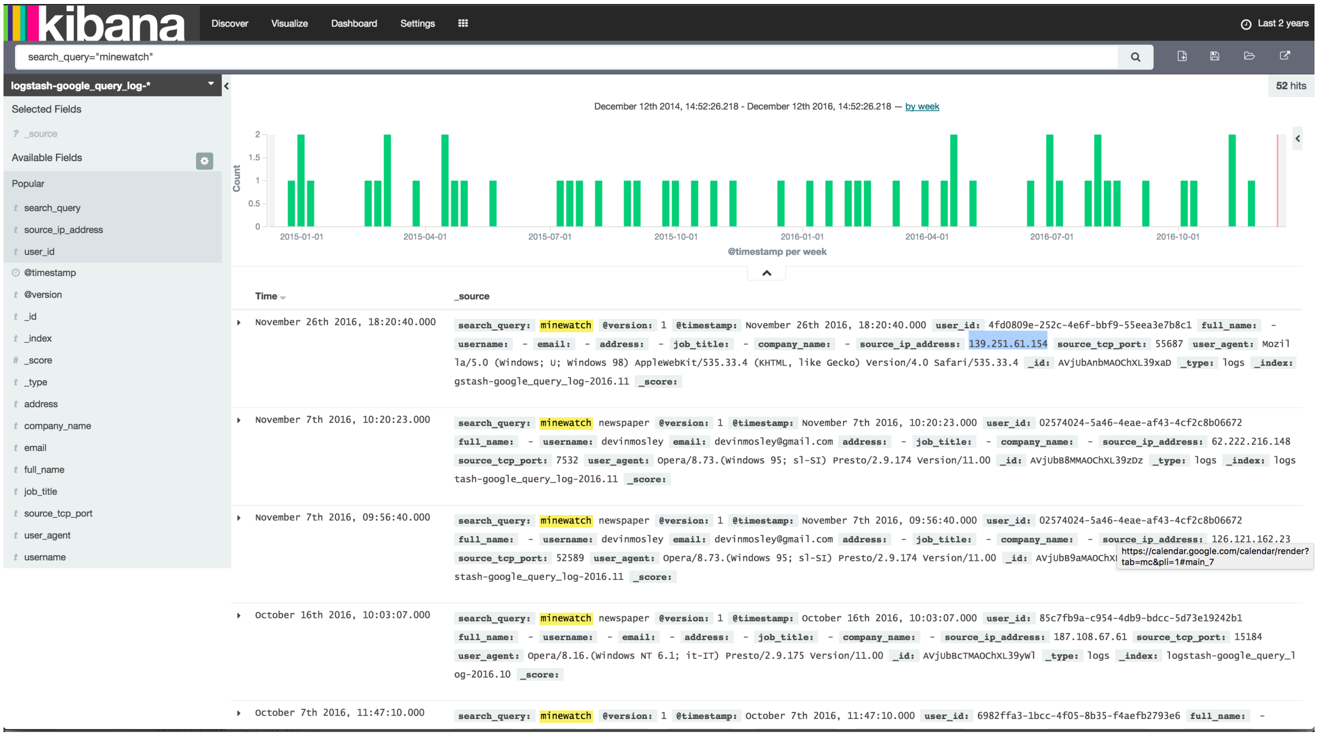
Supplied: Snitch Hunt

Step One: Search Google for suspicious searches

The scenario is about an employee at 'Minecorp' emailing confidential information to an investigative journalist at 'MineWatch'. You are a police data analyst who is told to identify and arrest the employee. "May I remind you the mines in Australia are all critical infrastructure, and those leaked docs cannot get into the wrong hands," your boss tells you.

You can sift through four sets of information.

One set is a search query log that represents information that would be held by Google and other search engines about what their users have searched for.



search_query="minewatch"

```
Time                               _source

November 26th 2016, 18:20:40.000   search_query: minewatch @version: 1 @timestamp: November 26th 2016, 18:20:40.000 user_id: 4fd0809e-252c-4e6f-bbf9-55eea3e7b8c1 full_name: -
                                   username: - email: - address: - job_title: - company_name: - source_ip_address: 139.251.61.154 source_tcp_port: 55687 user_agent: Mozil
                                   la/5.0 (Windows; U; Windows 98) AppleWebKit/535.33.4 (KHTML, like Gecko) Version/4.0 Safari/535.33.4 _id: AVjUbAnbMAOChXL39xaD _type: logs _index:
                                   gstash-google_query_log-2016.11 _score:

November 7th 2016, 10:20:23.000    search_query: minewatch newspaper @version: 1 @timestamp: November 7th 2016, 10:20:23.000 user_id: 02574024-5a46-4eae-af43-4cf2c8b06672
                                   full_name: - username: devinmosley email: devinmosley@gmail.com address: - job_title: - company_name: - source_ip_address: 62.222.216.148
                                   source_tcp_port: 7532 user_agent: Opera/8.73.(Windows 95; sl-SI) Presto/2.9.174 Version/11.00 _id: AVjUbB8MMAOChXL39zDz _type: logs _index: logs
                                   tash-google_query_log-2016.11 _score:

November 7th 2016, 09:56:40.000    search_query: minewatch newspaper @version: 1 @timestamp: November 7th 2016, 09:56:40.000 user_id: 02574024-5a46-4eae-af43-4cf2c8b06672
                                   full_name: - username: devinmosley email: devinmosley@gmail.com address: - job_title: - company_name: - source_ip_address: 126.121.162.23
                                   source_tcp_port: 52589 user_agent: Opera/8.73.(Windows 95; sl-SI) Presto/2.9.174 Version/11.00 _id: AVjUbB9aMAOChX
                                   stash-google_query_log-2016.11 _score:

October 16th 2016, 10:03:07.000    search_query: minewatch newspaper @version: 1 @timestamp: October 16th 2016, 10:03:07.000 user_id: 85c7fb9a-c954-4db9-bdcc-5d73e19242b1
                                   full_name: - username: - email: - address: - job_title: - company_name: - source_ip_address: 187.108.67.61 source_tcp_port: 15184
                                   user_agent: Opera/8.16.(Windows NT 6.1; it-IT) Presto/2.9.175 Version/11.00 _id: AVjUbBcTMAOChXL39yWl _type: logs _index: logstash-google_query_l
                                   og-2016.10 _score:

October 7th 2016, 11:47:10.000     search_query: minewatch @version: 1 @timestamp: October 7th 2016, 11:47:10.000 user_id: 6982ffa3-1bcc-4f05-8b35-f4aefb2793e6 full_name: -
```

Search query metadata.

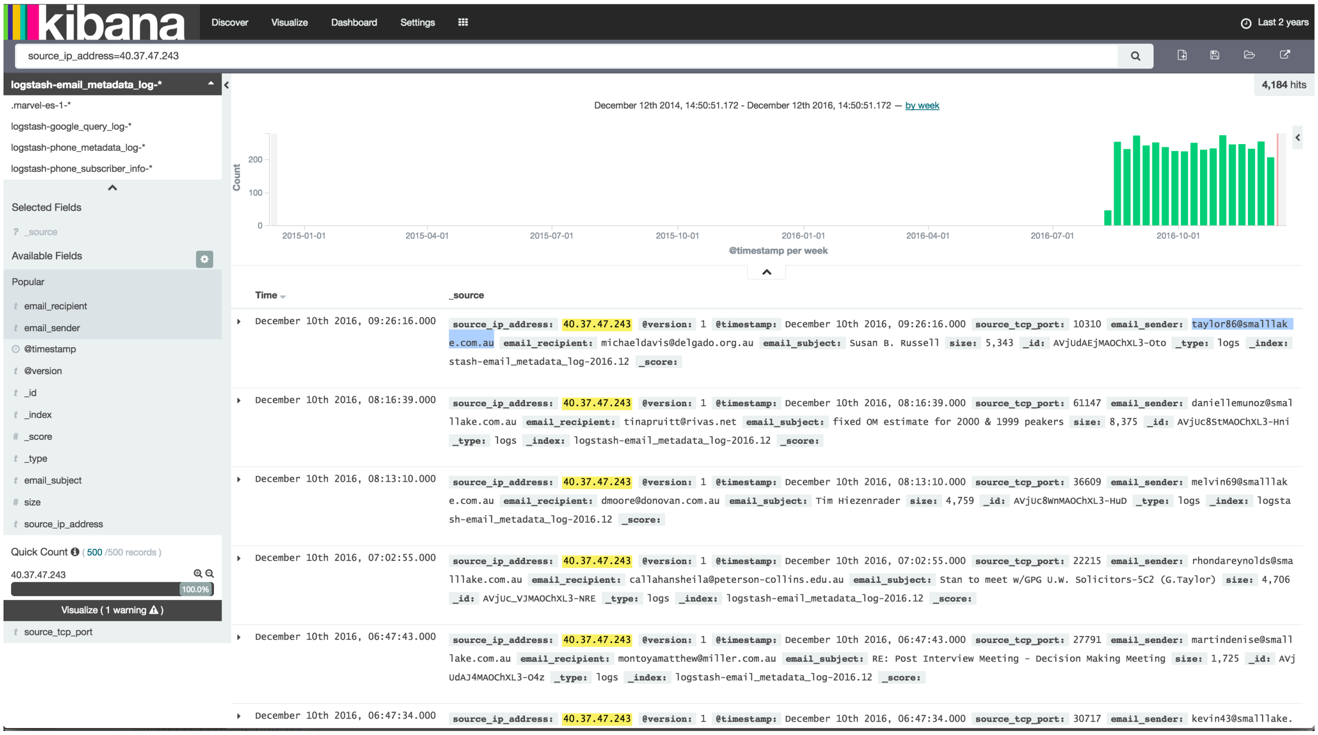
HackforPrivacy: Robin Doherty

You can find the IP address of anyone who has searched for log for "MineWatch" (the news website) or "Anna Dupont" (the name of the journalist who wrote the story).

Through a combination of searches you can narrow it down to a few likely IP addresses.

Step Two: Link the IP address with an email address

Once you have the IP, you can also search the database for what email address has been using that IP.



```
Time                            _source

December 10th 2016, 09:26:16.000   source_ip_address: 40.37.47.243 @version: 1 @timestamp: December 10th 2016, 09:26:16.000 source_tcp_port: 10310 email_sender: taylor86@smalllak
                                   e.com.au email_recipient: michaeldavis@delgado.org.au email_subject: Susan B. Russell size: 5,343 _id: AVjUdAEjMAOChXL3-Oto _type: logs _index:
                                   stash-email_metadata_log-2016.12 _score:

December 10th 2016, 08:16:39.000   source_ip_address: 40.37.47.243 @version: 1 @timestamp: December 10th 2016, 08:16:39.000 source_tcp_port: 61147 email_sender: daniellemunoz@smal
                                   llake.com.au email_recipient: tinapruitt@rivas.net email_subject: fixed OM estimate for 2000 & 1999 peakers size: 8,375 _id: AVjUc8StMAOChXL3-Hni
                                   _type: logs _index: logstash-email_metadata_log-2016.12 _score:

December 10th 2016, 08:13:10.000   source_ip_address: 40.37.47.243 @version: 1 @timestamp: December 10th 2016, 08:13:10.000 source_tcp_port: 36609 email_sender: melvin69@smalllak
                                   e.com.au email_recipient: dmoore@donovan.com.au email_subject: Tim Hiezenrader size: 4,759 _id: AVjUc8WnMAOChXL3-HuD _type: logs _index: logsta
                                   sh-email_metadata_log-2016.12 _score:

December 10th 2016, 07:02:55.000   source_ip_address: 40.37.47.243 @version: 1 @timestamp: December 10th 2016, 07:02:55.000 source_tcp_port: 22215 email_sender: rhondareynolds@sma
                                   lllake.com.au email_recipient: callahansheila@peterson-collins.edu.au email_subject: Stan to meet w/GPG U.W. Solicitors-5C2 (G.Taylor) size: 4,706
                                   _id: AVjUc_VJMAOChXL3-NRE _type: logs _index: logstash-email_metadata_log-2016.12 _score:

December 10th 2016, 06:47:43.000   source_ip_address: 40.37.47.243 @version: 1 @timestamp: December 10th 2016, 06:47:43.000 source_tcp_port: 27791 email_sender: martindenise@small
                                   lake.com.au email_recipient: montoyamatthew@miller.com.au email_subject: RE: Post Interview Meeting - Decision Making Meeting size: 1,725 _id: AVj
                                   UdAJ4MAOChXL3-O4z _type: logs _index: logstash-email_metadata_log-2016.12 _score:

December 10th 2016, 06:47:34.000   source_ip_address: 40.37.47.243 @version: 1 @timestamp: December 10th 2016, 06:47:34.000 source_tcp_port: 30717 email_sender: kevin43@smalllake.
```

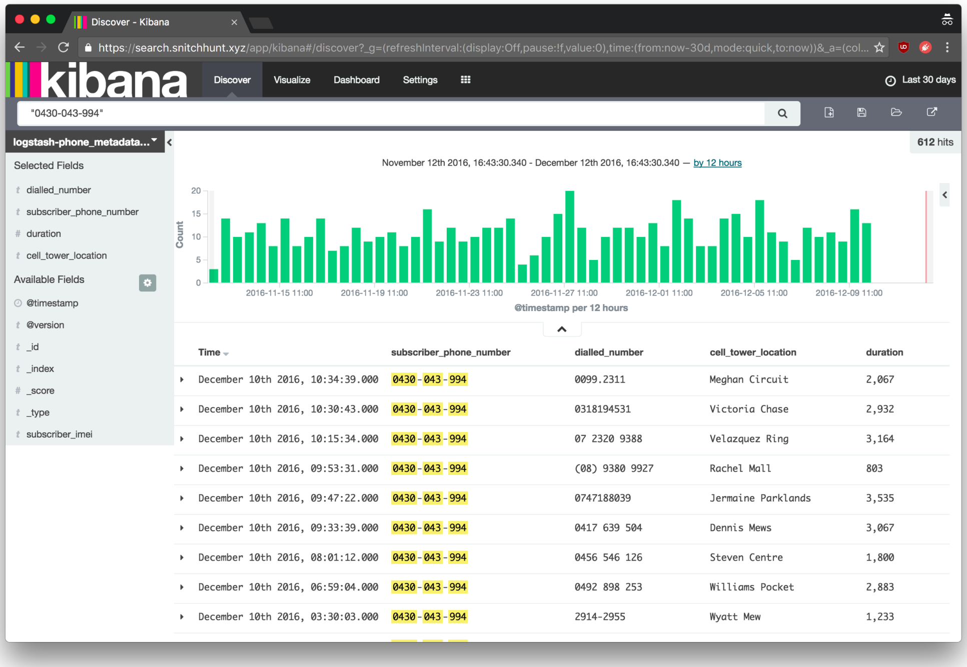
Email metadata.

HackforPrivacy: Robin Doherty

Step Three: Use email address to access address and phone number

Once you know the email, you can search the telcos' customer list for a phone number and the billing and postal address. (When you activate a SIM card you have to provide photo ID with an address).

The email and phone metadata logs also contain information about who has emailed who, and who has phoned who, and when. These are kept by telcos and made available without a warrant to 22 agencies. You can now confirm an email was sent from the address to 'anna@minewatch.org.au'.



Time	subscriber_phone_number	dialled_number	cell_tower_location	duration
December 10th 2016, 10:34:39.000	0430-043-994	0099.2311	Meghan Circuit	2,067
December 10th 2016, 10:30:43.000	0430-043-994	0318194531	Victoria Chase	2,932
December 10th 2016, 10:15:34.000	0430-043-994	07 2320 9388	Velazquez Ring	3,164
December 10th 2016, 09:53:31.000	0430-043-994	(08) 9380 9927	Rachel Mall	803
December 10th 2016, 09:47:22.000	0430-043-994	0747188039	Jermaine Parklands	3,535
December 10th 2016, 09:33:39.000	0430-043-994	0417 639 504	Dennis Mews	3,067
December 10th 2016, 08:01:12.000	0430-043-994	0456 546 126	Steven Centre	1,800
December 10th 2016, 06:59:04.000	0430-043-994	0492 898 253	Williams Pocket	2,883
December 10th 2016, 03:30:03.000	0430-043-994	2914-2955	Wyatt Mew	1,233

Phone metadata.

HackforPrivacy: Robin Doherty

Step Four: Use phone number to get a recent location

The phone metadata also gives a record of where the suspected whistleblower has travelled. This is based on cell tower records.

You can use this to predict where they will be, and then intercept them to make an arrest.

Metadata isn't only about knowing a person's past movements, it also about predicting their future activities. That's because most of us live according to routine. Once you know the pattern, it's easy to work out where a person will be on a given day.

"There's been research that's shown nearly half of most people's everyday activities follow a pretty regular pattern," Dr Dreyfus said.

"You go to your university class every Tuesday or you go to your job every Monday morning or Mum's house for dinner every Saturday night. Those patterns become a way of identifying people. One study that was done looked at the geolocation data points of more than a million people. It found that four space and time location points were all you needed to uniquely identify 95 per cent of people."

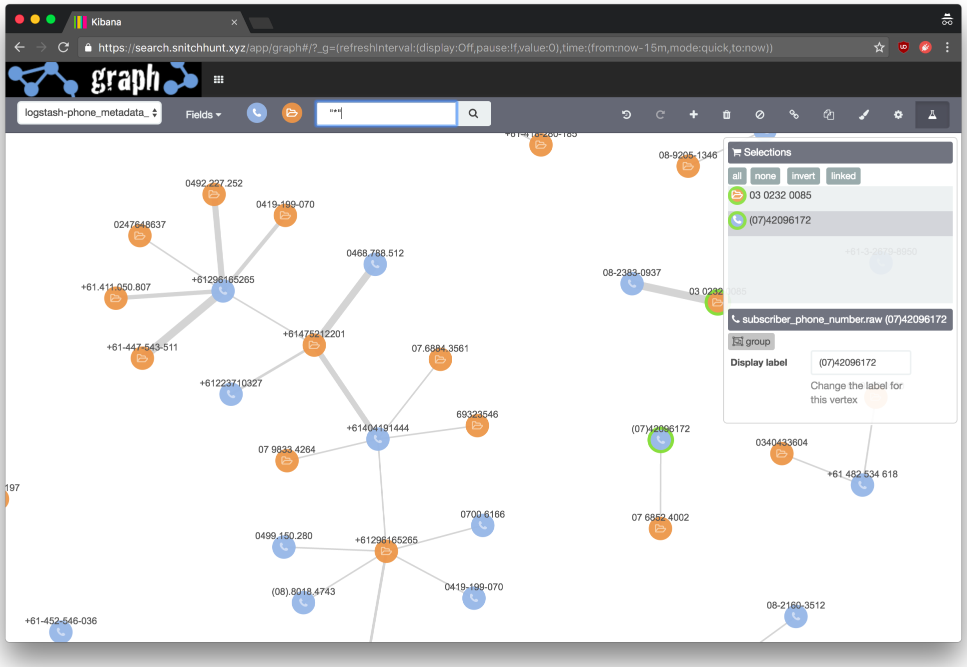
In a graphic illustration of how this works, the US's armed drone program identifies targets through their metadata. People are killed on the basis their metadata fits pattern of a terrorist. "We know former head of the National Security Agency said 'We kill people based on metadata'," Dr Dreyfus said.

Step Five: Find out who else has contacted the journalist

Using a graphing tool, you can interpret the metadata to understand relationships and social connections - you can use this to identify the journalist's other sources.

In April, the AFP admitted it had sought access to a Guardian reporter's metadata without a warrant in an attempt to hunt down his sources.

The Snitch Hunt used data analysis software that might be similar to that used by the AFP, Dr Dreyfus said.



Graphing phone calls.

Supplied

Gen, the 12-year-old from Team Sherlock, said she had expected it would be harder to find the whistleblower.

"It's interesting how easy it is to find small pieces of data, and then linking them you can find out so much about a person."

Her brother, Miles, 10, said that it was fun and his team beat half the adults.

The Snitch Hunt is co-sponsored by partners ThoughtWorks, CryptoParty Sydney, the Platypus Initiative, Hack for Privacy, Blueprint for Free Speech, Digital Rights Watch and Electronic Frontiers Australia.

Credits

- **Author James Purtill**

Facebook Comments

Ghostery blocked comments powered by Facebook Connect.

More Stories

The rise of Live Nation and the fear of an emerging music monopoly

5 DEC 2016

DIY Ayahuasca: Meet the Aussie dudes brewing hallucinogenic tea at home

7 DEC 2016

'I want my fkn ATAR': SMS technical glitch, all hell breaks loose

8 DEC 2016

#CUB55: Unions declare victory in 180-day Melbourne brewery strike

7 DEC 2016

More Stories

What do you care about this election?

9 May 2016

If you don't enrol soon you can't vote

8 May 2016

Could your parents afford to help you buy a house?

5 May 2016

Budget 2016: Making some uni degrees much more expensive

4 May 2016

Most Popular

- How pre-teens using metadata found a whistleblower in two hours
- The rise of Live Nation and the fear of an emerging music monopoly
- DIY Ayahuasca: Meet the Aussie dudes brewing hallucinogenic tea at home
- What happens to the family left behind in a missing person case
- 'I want my fkn ATAR': SMS technical glitch, all hell breaks loose

About Hack

Hack talks about the stuff that matters to young Australians. In your feed 24/7, on your radio 5:30pm weekdays.

- triple j
- Facebook
- Twitter
- Instagram
- YouTube
- Soundcloud

Listen Back

Listen to Hack

Hack on iTunes

Contact Form

To contact us during the show -

Call 1300 0555 36
(Local and mobile call costs)

SMS 0439 75 7555
(Usual SMS costs apply)

If you've got a tip off, a lead for a good story or a crackin' idea -

Email Hack

- Your Name
- Email
- Subject
- Your Message
- Send Email

Footer brand link

Topics

- All
- Listen
- World
- Tech
- Sport
- Sex
- Relationships
- Identity
- Environment
- Education
- Culture
- Politics
- Your Body
- Listen
- Drugs

triple J Logo

triple j unearthed Logo

double j Logo
Topics *icon-chevron-right*