

WHAT AN XKEYSCORE FINGERPRINT LOOKS LIKE

As part of its cooperation with New Zealand's best journalist on that country's SIGINT activities, Nicky Hager, the Intercept has published a story on the targets of a particular XKeyscore query (note: these stories say the outlets obtained this document; they don't actually say they obtained it from Edward Snowden): top officials in the Solomon Islands and an anti-corruption activist there.

Aside from the targets, which I'll get to, the story is interesting because it shows in greater detail than we've seen what an XKS query looks like. It's a fairly standard computer query, though initiated by the word "fingerprint." Some of it is consistent with what Snowden has described fingerprints to include: all the correlated identities that might be associated with a search. The query searches on jremobatu – presumably an email unique name – and James Remobatu, for example. As I have noted, if they wanted to target all the online activities of one particularly person – say, me! – they would add on all the known identifiers, so emptywheel, @emptywheel, Marcy Wheeler, and all the cookies they knew to be associated with me.

What's interesting, though, is this query is not seeking email or other Internet communication per se. It appears to be seeking documents, right out of a file labeled Solomon government documents. Those may have been pulled and stored as attachments on emails. But the query highlights the degree to which XKS sucks up everything, including documents.

Finally, consider the target of the query. As both articles admit, the reason behind some of the surveillance is understandable, if sustained. Australia and New Zealand had peacekeepers in the Solomons to deal with ethnic

tensions there, though were withdrawing by January 2013 when the query was done. The query included related keywords.

In the late 1990s and early 2000s the islands suffered from ethnic violence known as "The Tensions." This led to the 2003 deployment to the Solomons of New Zealand, Australian and Pacific Island police and military peacekeepers. By January 2013, the date of the target list, both New Zealand and Australia were focused on withdrawing their forces from the island country and by the end of that year they were gone.

The XKEYSCORE list shows New Zealand was carrying out surveillance of several terms associated with militant groups on the island, such as "former tension militants," and "malaita eagle force." But with the security situation stabilized by 2013, it is unclear why New Zealand spies appear to have continued an expansive surveillance operation across the government, even tailoring XKEYSCORE to intercept information about an anti-corruption campaigner.

More specifically, however, the query was targeting not the militants, but the Truth and Reconciliation process in the wake of the violence.

I would go further than these articles, however, and say I'm not surprised the Five Eyes spied on a Truth and Reconciliation process. I would fully expect NSA's "customer" CIA to ask it to track the South African and Colombian Truth and Reconciliation processes, because the CIA collaborated in the suppression of the opposition in both cases (going so far as providing the intelligence behind Nelson Mandela's arrest in the former case). While I have no reason to expect CIA was involved in the Solomons, I would expect one or more of the

myriad intelligence agencies in the Five Eyes country was, particularly given the presence of Aussie and Kiwi peacekeepers there. And they would want to know how their role were being exposed as part of the Truth and Reconciliation process. This query would likely show that.

Which brings me to the point the activist in question, Benjamin Afuga (who sometimes publishes leaked documents) made: this spying, which would definitely detail all cooperation between him and the government, might also reveal his sources.

Benjamin Afuga, the anti-corruption campaigner, said he was concerned the surveillance may have exposed some of the sources of the leaks he publishes online.

"I'm an open person – just like an open book," Afuga said. "I don't have anything else other than what I'm doing as a whistleblower and someone who exposes corruption. I don't really understand what they are looking for. I have nothing to hide."

Ah, but Afuga does have things to hide: his sources. And again, if one or another Five Eyes country had intelligence operatives involved both during the tensions and in the peace keeping process, they would definitely want to know them.

Again, this is all standard spying stuff. I expect CIA (or any other HUMINT agency) would want to know if they're being talked about and if so by whom – I even expect CIA does a more crude version of this within the US about some of its most sensitive topics, not least because of the way they went after the SSCI Torture investigators.

But this query does provide a sense of just how powerful this spying is in a world when our communications aren't encrypted.