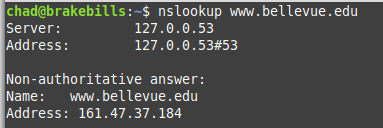
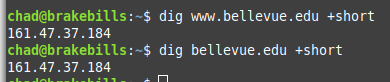
**James Chad Ballay**

**Bellevue Nslookup**

The nslookup tool will resolve the .edu tld and query it for the dns record. In that record we are looking for the IP address associated with that name. (Analogy would be a phone book lookup.)



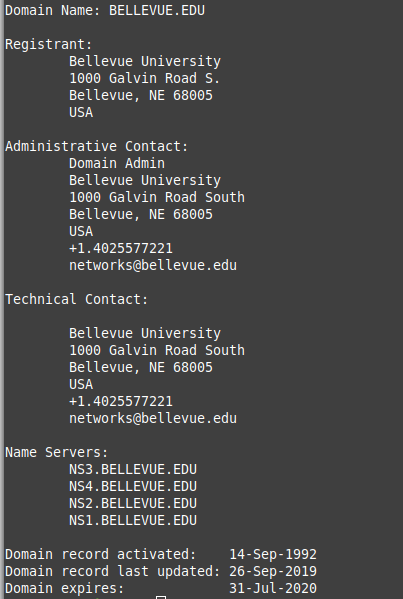
Another interesting bit is that both [www.bellevue.edu](http://www.bellevue.edu) and bellevue.edu both resolve to the same IP address. This article gives a brief overview of the why.



<https://computer.howstuffworks.com/internet/basics/question180.htm>

**Bellevue Whois**

Similarly when using the whois command, the request hits the Registar for that TLD. From right to left the domain name is processed until the lookups are narrowed down enough to identify the single record that is being queried for.



For the points of contact all three list the same entity, Bellevue University.

Bellevue University

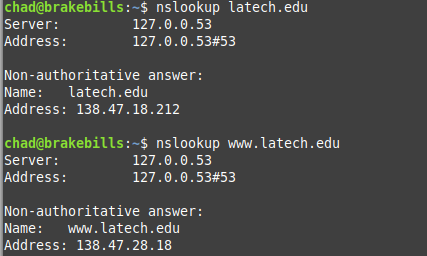
1000 Galvin Road South

Bellevue, NE 68005

(402) 557-7221

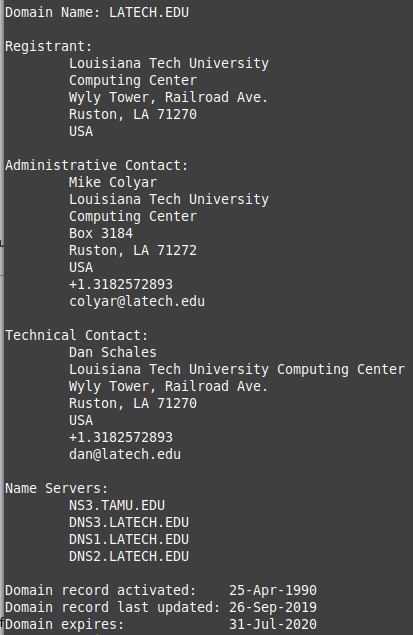
**Latech.edu Nslookup**

Conversely from Bellevue, Louisiana Tech has [www.latech.edu](http://www.latech.edu) and latech.edu resolve to different IP’s. This isn’t enough to give much insight but it is still a data point to note.



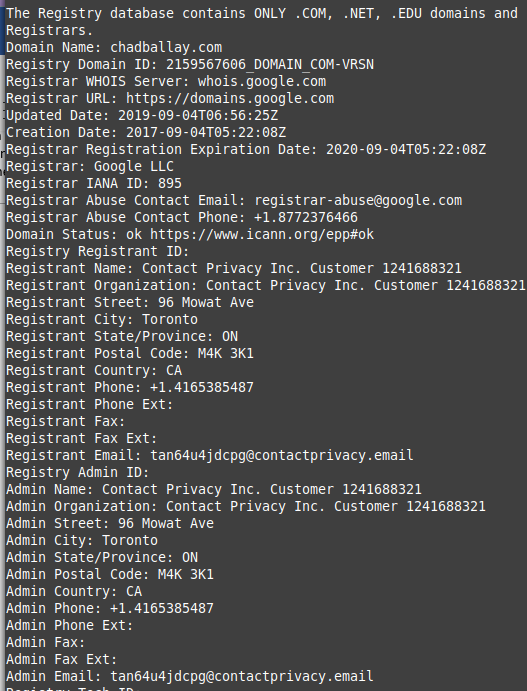
**Latech.edu Whois**

In contrast to Belleuve’s record Lousiana Tech lists named people as points of contact for Administration and Technical contacts. They also have chosen two different people for both of those roles. I’m not sure which approach is better but it certainly compares and contrasts different approaches. On one hand it makes it simplerer to not have to update this with HR changes. On the other hand, when you don’t have a single entity responsible then things fall between the cracks.



**Publice vs Private**

I specifically chose EDU records because of the transparency involved. In the COM side of things it is defacto practice to obfuscate the contact information. My own vanity domain has no info directly about myself. At first this seemed like a good idea but with the leakage of people’s PII data the point seems moot. Massive databases of public records are already around. A cursory google search for [“Chad Ballay”](https://www.google.com/search?q=%22chad+Ballay%22) reveals more info about myself than I realized. (Most of it data that I shared willingly.....)



I think that this data should be public but just because the current posture is to have so much PII data already public. The benefit puts people doing cursory research on the same field as people able to understand all the nooks and cranies PII data lives at on the internet. For right now there is no clear standard on how to reach out to an entity if you find an issue. Last year Chic-Fil-A had a bug with how their recipt survey process worked. The github repo has since been removed but the gist was that it used proxies/selenium/bruteforce to submit survey attempts until you earned a free sandwich.

<https://news.ycombinator.com/item?id=20083070>

<https://hackerfall.com/story/using-python-to-get-free-chicken-sandwiches>

<https://github.com/BinaryWasp/CFA-2019-1337>

With a clear and accurate whois record you have at least one inside point of contact to reach out to. In this specific case, front line tech support had no idea and weren’t interested. I lucked out that I had met one of their engineers at Kubecon and was able to give them a head’s up. But that was pure happenstance and luck. A better solution would be to have a standard for how to engage for technical problems but I’m sure spammers and other bad actors would ruin that too.