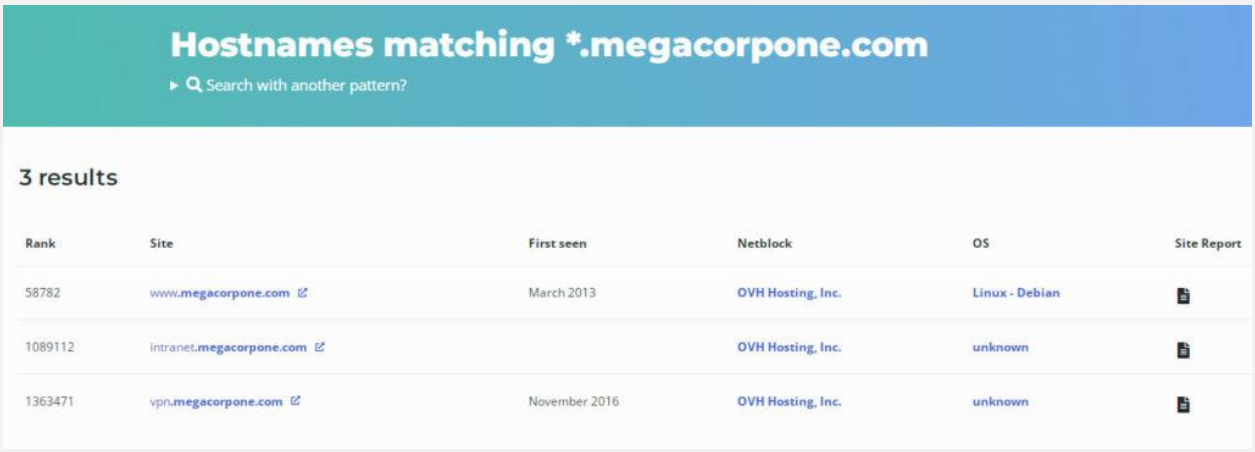
АКАДЕМИЯ
КОДЕБАЙ

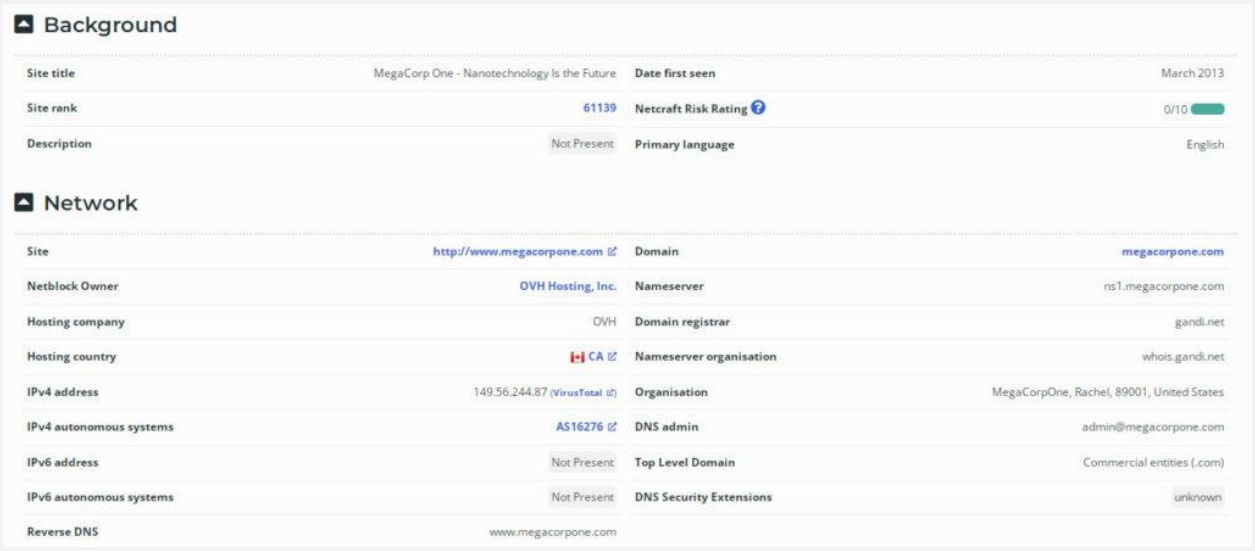
ПРОФЕССИЯ ПЕНТЕСТЕР

Netcraft — это компания по предоставлению интернет-услуг, базирующаяся в Англии, предлагающая бесплатный веб-портал, который выполняет различные функции по сбору информации. Использование услуг, подобных тем, которые предлагает Netcraft, считается пассивной техникой, поскольку мы никогда не взаимодействуем с целью напрямую.

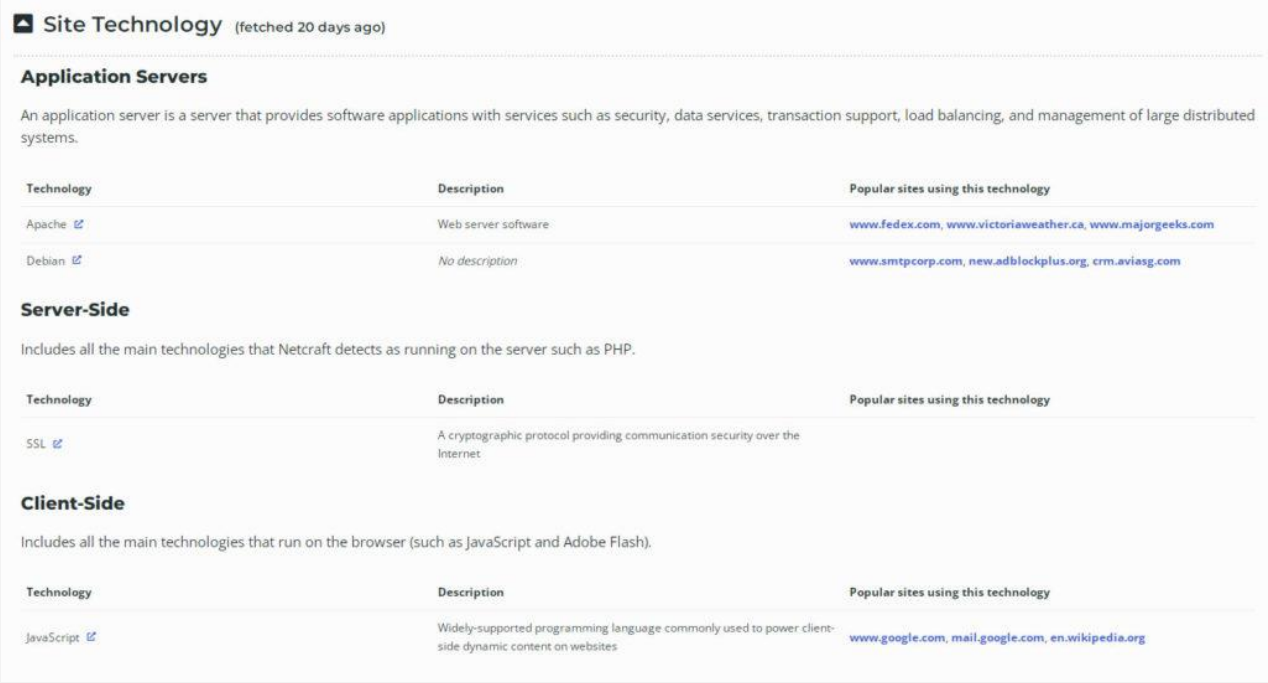
Давайте рассмотрим некоторые возможности Netcraft. Например, мы можем использовать страницу DNS-поиска Netcraft (https://searchdns.netcraft.com) для сбора информации о домене megacorpone.com:



Для каждого найденного сервера мы можем просмотреть отчет, который предоставляет дополнительную информацию о сервере, нажав на значок файла рядом с URL каждого сайта:



В начале отчета представлена информация о регистрации. Однако, если мы прокрутим вниз, то обнаружим различные записи "Site Technology":



Site Technology (fetched 20 days ago)

Application Servers

An application server is a server that provides software applications with services such as security, data services, transaction support, load balancing, and management of large distributed systems.

Technology	Description	Popular sites using this technology
Apache	Web server software	www.fedex.com, www.victoriaweather.ca, www.majorgeeks.com
Debian	*No description*	www.smtpcorp.com, new.adblockplus.org, crm.aviasg.com

Server-Side

Includes all the main technologies that Netcraft detects as running on the server such as PHP.

Technology	Description	Popular sites using this technology
SSL	A cryptographic protocol providing communication security over the Internet	

Client-Side

Includes all the main technologies that run on the browser (such as JavaScript and Adobe Flash).

Technology	Description	Popular sites using this technology
JavaScript	Widely-supported programming language commonly used to power client-side dynamic content on websites	www.google.com, mail.google.com, en.wikipedia.org

Список полученных поддоменов и технологий, используемых на сайте, окажется полезным, когда мы перейдем к эксплуатации информации. Пока же мы добавим его в наши заметки.