To get a better view and more transparency on keweon for us (and others), we would like to ask a few questions to keweon.

We ask for honest and detailed answers.

---

1. **How many average DNS queries does keweon receive daily?**

   There is no statistic because there are no logs implemented within any Service. Even on OS level I have no logs activated because I need every CPU and RAM power for DNS Service. I invented a system against data collection. Why I should do it when I'm so hard against this? Keweon is a PoC (that means a Proof of Concept) that things are working even without logging.

2. **How much bandwidth do keweon servers use and how much traffic is generated in one day?**

   The average traffic by day is at round about 4 to 9 GB traffic per Server. I don't really care about this because actually it's only important to see if I still within my monthly traffic range. This info is based on the Web interface from vultr.com

3. **How much CPU and GPU load does a keweon server utilize and on which system?**

   The CPU load is at round about 8 to 15%. This info is based on the Web interface from vultr.com

4. **On which software is keweon based? Which (programming) languages are used for development?**

   I will give no details about OS and other related things because of security risk. The service is based on my own DNS Server. As Programming languages I'm using C, C++ and Assembler.

5. **Why is DNSSEC not used, although this could create a higher level of user trust in keweon through increased security?**

   Keweon is a so named URL and Domain blocking system for Security and System Protection. DNSSEC has nothing to do with security because DNSSEC means "DOMAIN NAME SERVICE SECURITY EXTENSION". DNSSEC confirmations are useful to use it within a DNS Blocking System but DNSSEC also has a lot of disadvantages.

   https://ianix.com/pub/dnssec-outages.html
   https://ititch.com/dnssec-what-you-need-to-know

   In addition the DNSSEC validation cause too much traffic it also causes too much latency because of the verification procedure. keweon is still within a PoC status and everyone knows why he is using this DNS server when he is using it. If I ever have the money for a real infrastructure I'm fine to enable DNSSEC. But it will not change my opinion to DNSSEC. It's a nice Idea but its crap. If you take a look at the "DNSSEC" enabled domains then you will see a

few Domains has this feature not implemented on TLD Level. If DNSSEC is indeed a so good "feature" – which has nothing to do with security – then explain to me please why so many Top Level Domains has this feature not enabled.

6. **Does keweon use proxy servers? With those it could on one hand remove ads cosmetically like other ad-blockers, on the other hand it could, in combination with the root cert, read all kinds of data from the user (including banking passwords, emails, documents, pictures and also cookies which could be used to steal sessions from users accounts). On top of that, code could be injected like for example cryptominers or key-loggers.**

Keweon is NOT USING ANY (!) kind of proxy Server. That's exactly the reason why I'm doing it via DNS because I don't want to have the same crap solution as almost other have. We have had already a discussion about this during almost two or three weeks (!) – and there is still this question about it? There are enough possibilities to check and confirm this from your side. Feel so free and do it.

7. **Why are queries not redirected to 0.0.0.0 instead of a Web server, which could easily track or monitor users behavior, visited pages not only by their domain but also by their URL and could also collect cookies from users?**

The reason of this Service is just to prevent errors. When you point to a non-valid IP Address (0.0.0.0 is a Network address) this will cause a lot of troubles within routing and routing protocols. The reason of the "keweon ZSB Server" (Zero Session Broker) is to prevent errors caused by Ad-blocking.

This specific server and in addition with the HTTPS Certificate will prevent errors which are caused by Ad-blocking. Every request will cause a HTTP(S)/200 confirmations from your browser or App. By blocking with 127.0.0.1 this would be never possible. Also with 0.0.0.0 – but I don't want to argument about this because the usage of the IP Address is technical nonsense.

The use of the IP address 0.0.0.0 to block domain or host data in the HOSTS files is technically wrong, since the "IP address" 0.0.0.0 is a network address and not a valid host address. This can also be calculated in a simple way:

```
Address:   0.0.0.0                00000000 .00000000.00000000.00000000

Netmask:   255.0.0.0 = 8          11111111 .00000000.00000000.00000000
Wildcard:  0.255.255.255          00000000 .11111111.11111111.11111111
Network:   0.0.0.0/8              00000000 .00000000.00000000.00000000
Broadcast: 0.255.255.255          00000000 .11111111.11111111.11111111
HostMin:   0.0.0.1                00000000 .00000000.00000000.00000001
HostMax:   0.255.255.254          00000000 .11111111.11111111.11111110
Hosts/Net: 16777214
```

IP addresses are not decimal but binary. The routing algebra framework, so the basics for the e.g. routing on the internet works based on math and not on guess numbers.

The address 0.0.0.0 is a so-called "Route Aggregation (RA)". It's the method for replacing a set of routes on a single more general route, which is a fundamental mechanism for the scalability of the Internet.

Of course you can ignore that the address 0.0.0.0 is not an IP address. Likewise, if you suddenly decide, the term "1 + 1 = 3" would be the same and validated. Since the number 1 is not a number, but only a successor of the axiom 0, one can do that. Or take the Roman number 12 (XII), then half of it would be 7 (VII). That too is mathematical. On the other hand, it may also be possible that all online IP addresses have a computer error and that are too stupid to calculate correctly.

Or to put it another way, if you throw yourself on the floor and pedal like a little kid, somebody will come over and say that's right because it's just too annoying to discuss about this.

The address 0.0.0.0 can have very different meanings depending on the purpose.

- *There is definitely no valid address given on an actual (or fictitious) network interface together with another address in subnet 0.0.0.0/8.*
- *When used in a routing table, this is identified as the default gateway. A route to 0.0.0.0 is the default route, ie. H. the route used when no more specific route is available for a destination address.*
- *When used in a firewall, the address is 0.0.0.0 for "All valid networks"*

Moreover, using this address in HOSTS files from Windows will result in a system error "ERROR_INVALID_NETNAME 1214". The definition for this can be found in the Windows SDK in WinError.h. Any errors within Windows cause delays as well as additional system resources. These include logging, analyzing and writing events. Thus, it is not just a myth that blocking domains and HOST entries at the 0.0.0.0 address should be faster, about which there is not a single record to date, but it is also mathematically, logically and technically wrong. Because writing and issuing errors in the system always causes delays.

This Wiki entry:

https://en.wikipedia.org/wiki/Null_route

is totally and complete (!) wrong. Although a lot of HOSTS files are pre-defined in the Internet with the "IP Address" 0.0.0.0 will make this entry not better.
Its 1500 yrs ago and the whole world knew that the earth was the center of the universe. Although the entire world knew this it was wrong. It is 500 yrs ago and the entire world knew that the earth was a plate. Although the entire world knew this it was also wrong.

8. **How much do the keweon servers currently cost and how much would they cost if keweon plans to expand? Transparency is important in this point, because money could easily be used elsewhere.**

I was thinking about to answer this question because I only hear complains and "don't use keweon" from your side. Why this would be important for being transparent to you?

The current system will cost exactly 720 Euro per Month. The average cost when keweon expands varies.

When we talk about the "XXL Premium Ultra Gold Platinum TJ Special Infrastructure" then its round about 150.000 EUR per month. This includes 2 global load balancer as like as 1.1.1.1 or 8.8.8.8 DNS Server address with same performance as like as Google and it's a little bit more than DNS. But this is not the right point to talk about keweon and the future.

If you think that's too expensive then you should ask Google why they spend a 3 digit million Dollar budget only for their DNS infrastructure which includes round about 400 people as DNS Team.

9. **Why does keweon only take money donations? It would be more convenient to use free resources which are already available anyways.**

   I don't take money donations but if someone will do it it's OK for me. They are actually 2 monthly donations and I'm happy about every single Euro.

   Because of DNS it's not possible to use "free resources". I would wonder if this would be possible and I'm always open for doing it better. I appreciate your support if you can provide me some links but you can be sure that this will not work.

   At the moment only CloudDNS would be the only one option to use as partner with keweonDNS. The monthly costs would be at round about 25.000 EUR.

   I was asking many times to show me this "free resources" but there was no answer until today. I haven't had found any useable free resources which I can use for making keweon running as it is because it's technically not possible.

10. **Why a root certificate is advertised, which keweon could use to steal user data?**

    If you can provide a better way to prevent HTTPS errors which will be caused by ad-blocking and you are also able to do it with 0 Data send then I'm open for everything.

    A lot of websites are using HTTPS errors for Adblock detection because Webdevelopers don't sleep and they know about Hosts based adblocking.

    If you're doing normal adblocking then you're always in trouble if you have an HTTPS call. So, let's say the address is called werbung.com and it's in a javascript.

    So if you block the address via the HOSTS file and you call that with HTTPS on you get an error message. Quite logical and also clear.

    Exactly the same if you do this over Javascript. Meanwhile, these programmers are also up to date and know, aha, bug in HTTPS is adblocking. This is also easy to determine.

    Since more and more HTTPSs connection are in use and due to more and more errors, blocking becomes either ineffective or simply reduced.

    Now the certificate is there. Regardless of whether the address comes via HTTP or HTTPS, your browser or the app always gets an HTTP / 200 status despite the blocking because no errors occur. In addition, it has the advantage that your download will come faster and your Internet will speed up just because no errors come and therefore the server does not have to ask 20 times or senselessly process errors.

    My friend from the company told to me that the HTTPS "confirmation bug" is annoying. And he said to me, not bad, but as long as that is not gone automatically the use within a company environment makes no sense. It took me almost 2 years to find out how to do that best. And that's exactly what the certificate is for.

I hear so many times that it is not technically possible to make the internet faster or to make a faster download. DNS has more or less nothing to do with it. But with a bit of logic, that makes sense in the case of being knowledgeable about programming. Errors in the program, no matter in which are always speed brakes. And only for that thing is responsible. No mistakes. Everything else is just logical and with pleasant side effects.

Why is this faster?

Windows and Linux are not just a multitasking Operation System as like as a real time processing OS. They are working as "Preemptive Multitasking" (German: Präemtives Multitasking). Because of this the "Error Management and Handling" is essential and if you know how "time slice" is working within OS, Windows kernel and Browser then you will understand why it is important to prevent errors within Browser (HTTPS) and Windows (0.0.0.0 HOSTS).

> ***Technical explanation:***
>
> *A multitasking operating system divides the available processor time among the processes or threads that need it. The system is designed for preemptive multitasking; it allocates a processor time slice to each thread it executes. The currently executing thread is suspended when its time slice elapses, allowing another thread to run. When the system switches from one thread to another, it saves the context of the preempted thread and restores the saved context of the next thread in the queue.*
>
> *The length of the time slice depends on the operating system and the processor. Because each time slice is small (approximately 20 milliseconds), multiple threads appear to be executing at the same time. This is actually the case on multiprocessor systems, where the executable threads are distributed among the available processors. However, you must use caution when using multiple threads in an application, because system performance can decrease if there are too many threads.*

More details will lead into OS development and teaching but this is seriously not my Job. Because of this error management and the reduction of errors at all within this way it is simple logic that keweon make a faster download possible.

And finally - stealing data with just a certificate is technically not possible!!!!!
For this you need an App or an Application which transmit the Data. That's the reason why you will never see an App or Application by keweon.

If you still say its possible then proof and confirm this please. Tell me a Server, give me a Root Certificate and try to steal my data. As I already said I'm always open for better solutions.

Stealing data with just using or installing a "Root Certificate" is in simple word a big bullshit and technically not possible. Here is my offer:

1. *Provide me a DNS Server of your choice*
2. *Hand me over a Self-Created Root Certificate*
3. *I will do my Paypal payment via your DNS Server*
4. *Enable FULL LOGING of whatever you want or need*
5. *Grab my login Data – I will even let you know when I do a Paypal Payment*
6. *If you can get the Data you can use it and send yourself 500 EUR from my Paypal Account to you.*
7. *You have my official allowance for doing this*

This questionary stays online and you can even get a confirmation by letter or by email for doing this if you have legal concerns. If you can get the Data then do it. Have fun!

11. Are there any emergency plans for keweon if Torsten should be prevented, and what do they look like?

Why should this be required at the moment? keweon is a PoC, it's a hobby, no one pay's for this and it's my private fun which I share at the moment. And if there would be ever an emergency plan I would never make them public because of security concerns.

12. What happens if the private key of the keweon CA is compromised (i.e. leaked / cracked)? Since the users themselves have imported the certificate on their own, it will probably be difficult to revoke it. User data could be intercepted not only by keweon as a third party but even by a fourth party.

The same thing happens as with any other CA within your Windows or Linux System when they become compromised. The Certificate will be revoked immediately and if you take a look into the Root Certificate you will see the Root CA CRL is already prepared. In addition are all "ZSB Servers" located only in Germany within BSI recommended and certified Datacenters.

13. How is keweon currently financed? This is important for users, so they know that the future of keweon is assured and that there is no company behind it, which would censor the Internet or track their behavior.

It's financed by me because it's my baby, my hobby and as long as I have not a Crowdfunding or a usable Investor for this there will be no change. I also explained this so many times.

14. **Is keweon GDPR compliant? Is there a data privacy declaration / privacy policy? This is also important, because Users should know where their data is sent and what is done with it.**

   Keweon is GDPR compliant and there is actually no privacy declaration or privacy policy because keweon is still a hobby or a PoC.

   In Germany it's damn expensive when you even have a typo within the privacy declaration or policy. If you get a "warning letter" (Abmahnung) because of this it might cost up to 25.000 EUR.

   Help from a German lawyer to make this 100% proof will cost round about 2.000 to 2.500 EUR. I neither have the money for it nor do I see the need to spend the money.

   According to EuGH Judgment by 27.03.2014 (C-314/12) are all requirements about Privacy and Data Privacy fulfilled. Keweon is also working in compliance with German, EU and US law.

15. **How does keweon determine the average number of requests per user without writing logs?**

   I'm doing this with Microsoft Excel because I'm too lazy to calculate this manually.

   If you want to know how many queries a user will create then install a DNS Server and run this over a few months. The other option is to use INTRA. In the meantime you can see the daily DNS request at Intra very easy. Collect this number, add it to Excel and you can easily get a valid average number.

   In 2010 or 2011 I have had a DNS Server with full logging and on this I was collecting information because I have had not numbers for a base to start. This Server was restricted to a few users only (round about 200) and to 3 companies. Today it's just estimated. No idea and data about the real numbers of queries and there is also no reason to get this number.

16. **How would keweon like to improve the Internet with a centralized solution? One big problem with centralized solutions is: If there is one fault, like false positives / negatives for white- / blacklist, then this affects every user. Users have to rely on one person to manage everything. Users also have to rely on the uptime from their specific DNS servers in their country. There are no alternatives to the selection of DNS servers provided by keweon.**

   There are different DNS Services outside and it's up to everyone to decide. Why you don't ask Symantec or CISCO or OpenDNS for this de-centralized solution? Advertising lists are dynamic. They will change daily and if I have a perfect whitelist today this might change tomorrow. If you have concerns about white or blacklisting then run your own server. If you will do this you can also point this to your "blackhole" Address or point it to 127.0.0.1. Be surprised about the result.

When I release everything as open source – which we have discussed so many times and you didn't accept the answer – the ads industries know in detail how keweon will work. When they knows how it's working then the might have a chance to prevent adblocking by keweon and this would be the death of this solution.

We have had discussed also round about 2 weeks and you was also only complaining about this and keweon at all. For security reasons keweon will NEVER become a OpenSource solution. I would rather delete everything than doing this.

Since 2003, where I have had started this Idea I have spent round about 200.000 Euro into this Project by Hardware, Server, Software, Data Center tests and a lot of other things. In addition, I don't talk about time and work which I have spent into this Project.

17. **Why are whole gTLDs blocked by keweon (e.g. in the case of .xyz)? Blocking entire networks or gTLDs is bad. Anyone can buy these domains, they don't necessarily mean, that they only contain malware, advertising or scam pages. An example for this is available in your browsers address bar right now.**

Also this question you was asking round about 10 times. As long as almost all hosts are poison or dangerous threats for users I will block the entire domain and unlock requested domains. XYZ, TOP and WIN domains are entirely blocked by default at keweon and they stay closed. If you know a website which is safe then send this to unlock. Malwarebytes and Symantec reported that more than 97% of all registered domains are dangerous, poison or a threat.

https://www.symantec.com/connect/blogs/exploring-xyz-another-shady-tld-report

It's the same as ad-blocking but just the other way around.

After showing this report your answer was "It is questionable if one can trust the reports." I already told you if you have a better idea then this is welcome. Your answer was: "Not to use keweon". OK, I'm fine with this.

18. **According to the German Patent and Trademark Office the word mark keweon is not owned by the keweon owner Torsten but by a woman named Tanja Wild. It is also registered under the keyword online advertisement. We would ask for an explanation of that. (source)**

The option „Internetwerbung VERHINDERN" (prevent online advertising) was unfortunately not available. The Name registration itself was a big "thank you" and a gift from a good friend. The actual registration owner is my girlfriend and fiancée because she is the best whatever happens within my live. In honor to her the name is registered to her and I trust no one more than her.

19. **Torsten keeps saying that he does not like Let's Encrypt, but keweon is still using certificates from Let's Encrypt on multiple keweon.center domains. Why is that?**

If you take a look at so many ransomware, cryptoware, malware, spyware and other poison things you will see they are almost certified by Let's Encrypt. That's a good reason not to like this PKI because everyone can easily get a certificate from them without any validation. That's not my understanding of HTTPS or security.

20. **We found in the source of Q18 the subdomain youtube.keweon.center. Is there a plan to set up a youtube proxy for blocking youtube ads, or what is the purpose?**

This is for me, my daughter and for development ONLY. Its just to get YouTube free of ads, free of data collection and to get YouTube free of Porns. To prevent things I need to understand them first. That's the reason for this.

As she was 4 yrs old she was watching a "kids Video" on YouTube because she is a little researcher. Dealing with mucus and other chemical experiments for kids is her hobby. During watching one of these videos she gets Ads with "Bloody Headshot shooter advertising" and of cause a warning only for "18+".

She was crying about this and she has had 3 days nightmares. At this point I have sworn to fight against ANY advertising and they should find a better solution then this. I don't care about ads anyway. When I see it then I remove it.

So many people are claiming about these things since years. Politicians and so named technical experts are always telling us it is not possible to do something against this, privacy violation and data stealing. We have to live with this. Unfortunately I'm not someone who wants to accept things and that's also the reason why I'm thinking sometimes some kind of strange. Ask my Girlfriend. She is NLP Coach and Trainer and sometimes it's really hard for her with me ;)

But this is the only reason for keweon. I don't say it's the "golden solution" or the "holy grail" against any threats within the Internet. I only have problems with the sentence "We have to accept these things". I must accept things which I don't want? I give a fucking shit on this.