DNS Nameserver Spoofability Test

Should you trust the Domain Name Servers you are using?

(If this page doesn't work for you, please see our DNS FAQ page.)

What's going on?

The display of this page initiates a comprehensive search for all Internet DNS nameservers that respond to your system's requests for domain name lookups. **As this process can take up to several minutes, some patience will be required.** Once no additional nameservers are being found, the search terminates and a comprehensive security and spoofability analysis of the data obtained from the DNS nameserver(s) currently being used by your PC and web browser will be displayed.

Searching for all DNS nameservers used by your system:

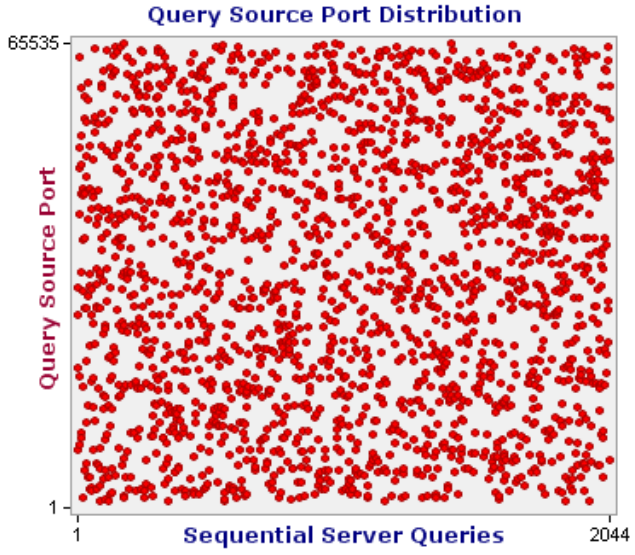
Query Round	Receiving Nameserver Queries...(per round results)	Servers Found	Queries Received
1	••	7	1,292
2	••	1	1,384
3	••	1	1,559
4	••	0	2,553
5	••	0	2,067
6	••	0	1,783
7	••••••••••••••••••••••••	0	475
	Totals for all rounds:	**9**	**11,113**

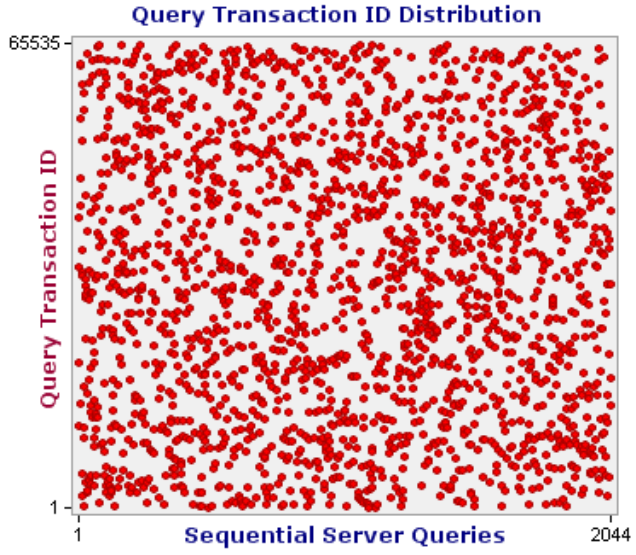
Please see the guide at the bottom of this page
for help interpreting the following analysis results:

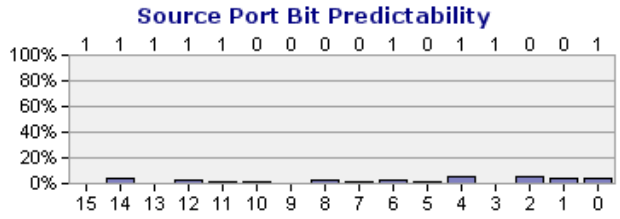
Analysis of **2,041** queries from nameserver at [**41.128.82.2**]

Anti-Spoofing Safety: **Moderate** (See Spoofability Mitigation Note below)

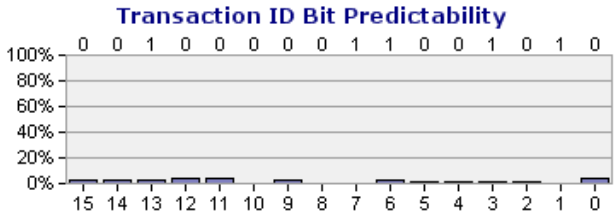
(This nameserver has no associated domain name)







Query Source Port Analysis (worst case)



Query Transaction ID Analysis (worst case)

Max Entropy:	15.98 **Excellent**	Dir Bias:	0.59% **Excellent**		
Lost Entropy:	0.66 **Moderate**	Stuck Bits:	0 **Excellent**		

Max Entropy:	16 **Excellent**	Dir Bias:	1.57% **Excellent**
Lost Entropy:	0.02 **Excellent**	Stuck Bits:	0 **Excellent**

DNS Nameserver Access Details

External Ping:	**ignored**	(Nice, as it's preferable for it to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**absent**	(This nameserver might need to be updated.)
Alphabetic Case:	**mixed**	(Extra bits of entropy are present in these queries!)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

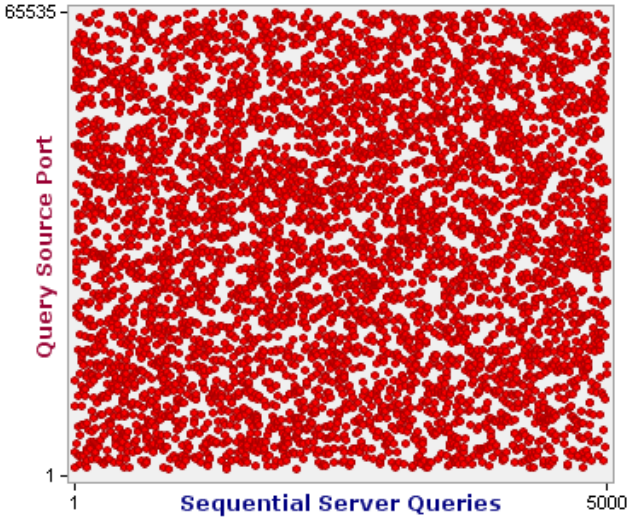
Spoofability Mitigation Note: Even though one or more of the individual "spoofability" parameters shown above does indicate a worrying spoofability grade of "**Moderate**", our attempt to directly query this server from the Internet failed. Therefore, "Kaminsky-style" cache poisoning attacks will be either more difficult or impossible to conduct. As long as this nameserver remains inaccessible to Internet queries, there is little danger of it becoming a victim of Kaminsky-style cache poisoning attacks.

Analysis of **4,977** queries from **10** IP addresses in [**146.112.136.***]

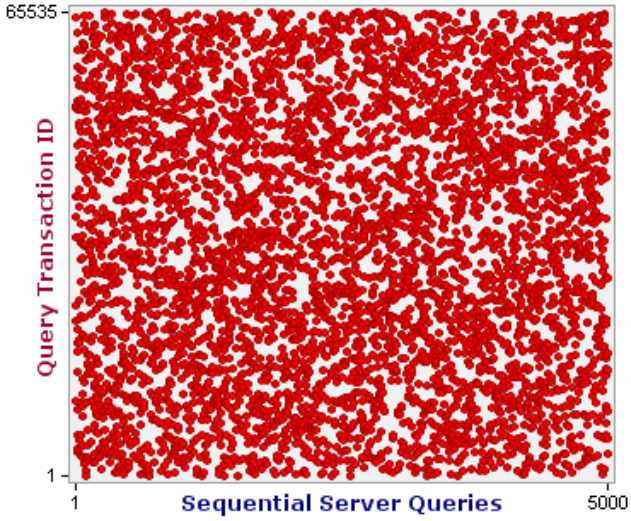
Anti-Spoofing Safety: **Excellent**

Network Name: ***.compute.mil1.edc.strln.net**

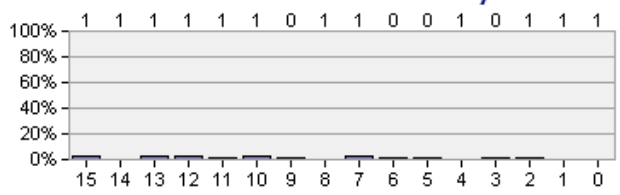
Query Source Port Distribution



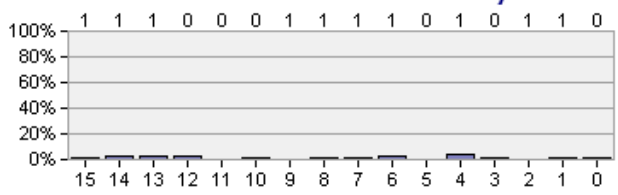
Query Transaction ID Distribution



Source Port Bit Predictability



Transaction ID Bit Predictability



Query Source Port Analysis (worst case)

Max Entropy:	15.98 **Excellent**	Dir Bias:	0.64% **Excellent**
Lost Entropy:	0.05 **Excellent**	Stuck Bits:	0 **Excellent**

Query Transaction ID Analysis (worst case)

Max Entropy:	16 **Excellent**	Dir Bias:	0.6% **Excellent**
Lost Entropy:	0.05 **Excellent**	Stuck Bits:	0 **Excellent**

DNS Nameserver Access Details

External Ping:	**replied**	(It might be better for the server to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**supported**	(This server supports improved security standards.)
Alphabetic Case:	**all lower**	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

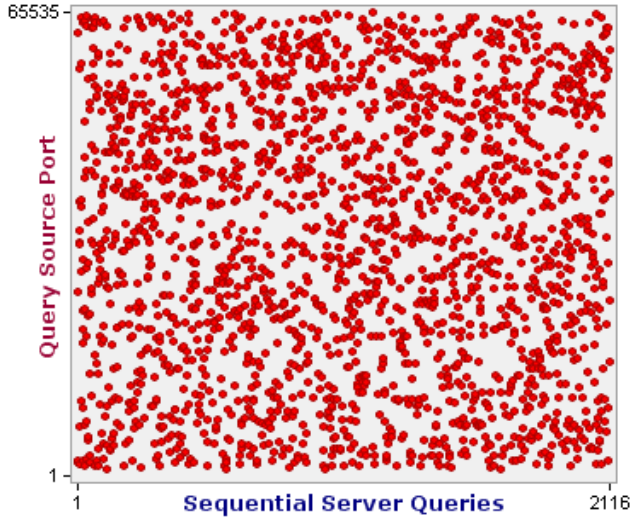
10 "Pseudo-Resolvers" in a Class-C Network: As you can see from the details provided in the blue bar above, **4,977** queries were received from **10** unique IP addresses closely grouped within a single class-C network.
In other words, only the *last byte* of the IP addresses of those **4,977** queries differed from each other. This indicates
that rather than there being **10** actual nameservers at those individual IP addresses, only a **single** nameserver
is located behind a "reverse NAT", causing it to emit queries from up to 256 randomly-chosen IP addresses. This
introduces an additional eight (8) bits of uncertainty into this nameserver's queries, since the querying IP might
have any least significant byte. Therefore, even if the nameserver's query source port range, or its transaction
IDs, are limited, significant additional randomness has been introduced into this nameserver's queries.

Analysis of **2,112** queries from nameserver at [**45.240.0.2**]

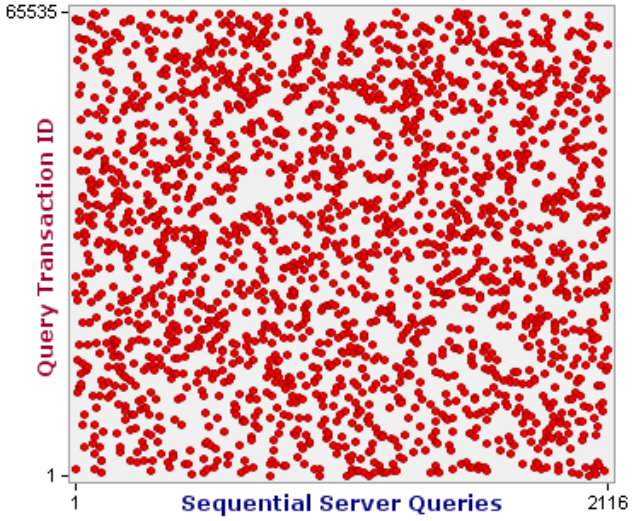
Anti-Spoofing Safety: **Moderate** (See Spoofability Mitigation Note below)

(This nameserver has no associated domain name)

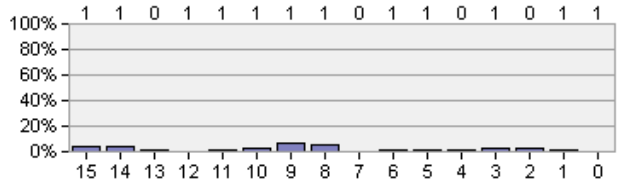
Query Source Port Distribution



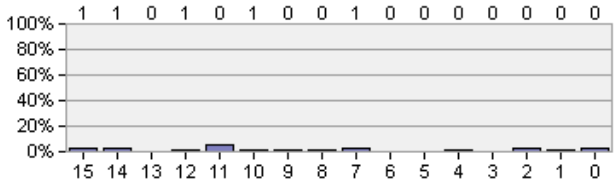
Query Transaction ID Distribution



Source Port Bit Predictability



Transaction ID Bit Predictability



Query Source Port Analysis (worst case)

Max Entropy:	15.98	**Excellent**	Dir Bias:	0.43%	**Excellent**
Lost Entropy:	0.67	**Moderate**	Stuck Bits:	0	**Excellent**

Query Transaction ID Analysis (worst case)

Max Entropy:	16	**Excellent**	Dir Bias:	0.9%	**Excellent**
Lost Entropy:	0.03	**Excellent**	Stuck Bits:	0	**Excellent**

DNS Nameserver Access Details

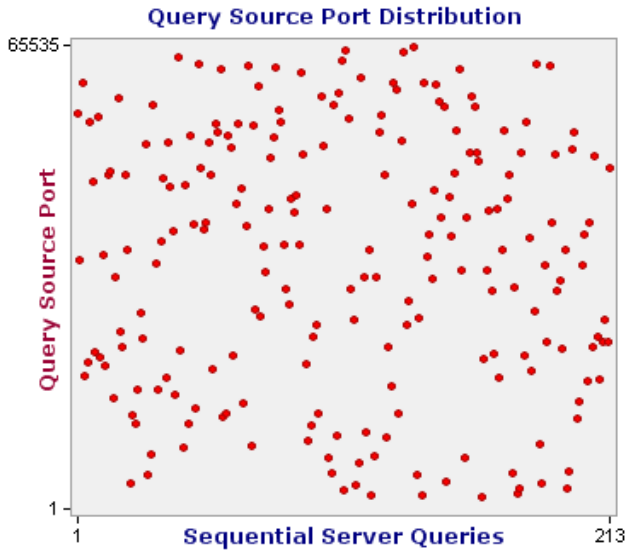
External Ping:	**ignored**	(Nice, as it's preferable for it to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**absent**	(This nameserver might need to be updated.)
Alphabetic Case:	**mixed**	(Extra bits of entropy are present in these queries!)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

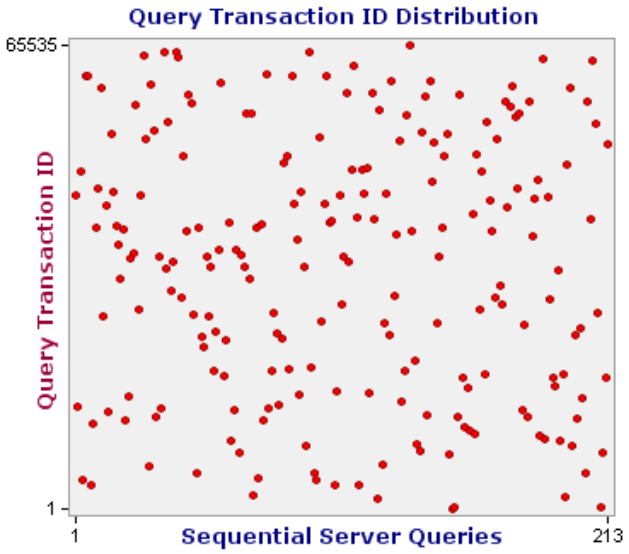
Spoofability Mitigation Note: Even though one or more of the individual "spoofability" parameters shown above does indicate a worrying spoofability grade of "**Moderate**", our attempt to directly query this server from the Internet failed. Therefore, "Kaminsky-style" cache poisoning attacks will be either more difficult or impossible to conduct. As long as this nameserver remains inaccessible to Internet queries, there is little danger of it becoming a victim of Kaminsky-style cache poisoning attacks.

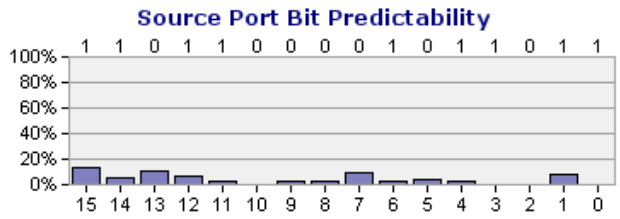
Analysis of **213** queries from nameserver at [**146.112.128.76**]

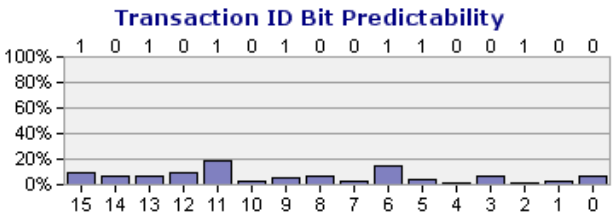
Anti-Spoofing Safety: **Excellent**

Server Name: **r3003.compute.cdg1.edc.strln.net**









Query Source Port Analysis (worst case)

Max Entropy:	15.96	**Excellent**	Dir Bias:	0.94%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

Query Transaction ID Analysis (worst case)

Max Entropy:	16	**Excellent**	Dir Bias:	0.94%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

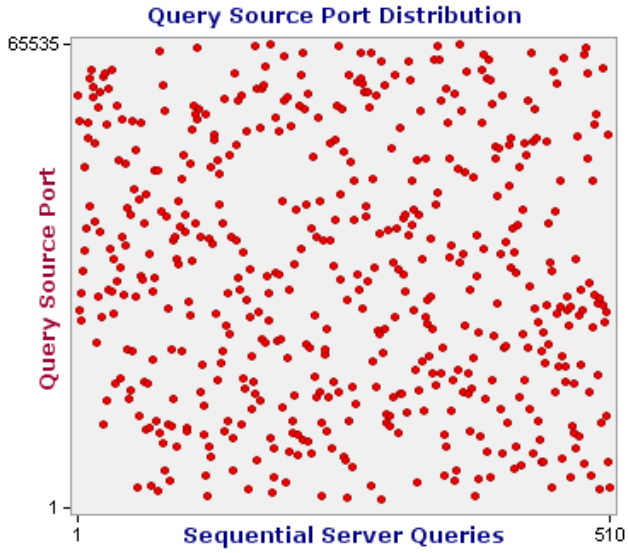
DNS Nameserver Access Details

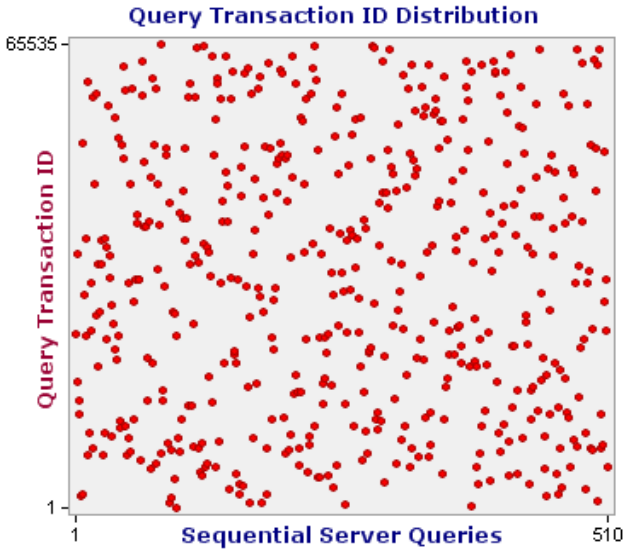
External Ping:	**replied**	(It might be better for the server to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**supported**	(This server supports improved security standards.)
Alphabetic Case:	**all lower**	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

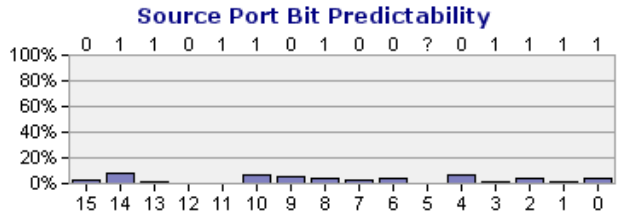
Analysis of **461** queries from nameserver at [**146.112.128.75**]

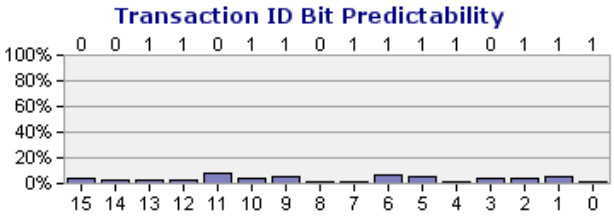
Anti-Spoofing Safety: **Excellent**

Server Name: **r3002.compute.cdg1.edc.strln.net**









Query Source Port Analysis (worst case)

Max Entropy:	15.97	**Excellent**	Dir Bias:	1.74%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

Query Transaction ID Analysis (worst case)

Max Entropy:	16	**Excellent**	Dir Bias:	1.3%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

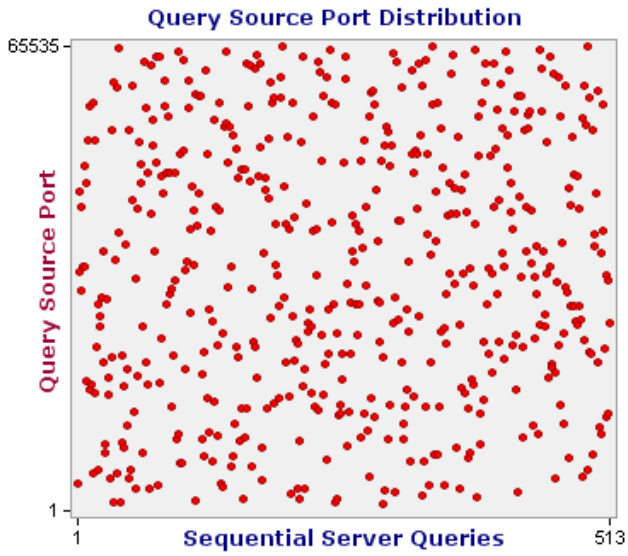
DNS Nameserver Access Details

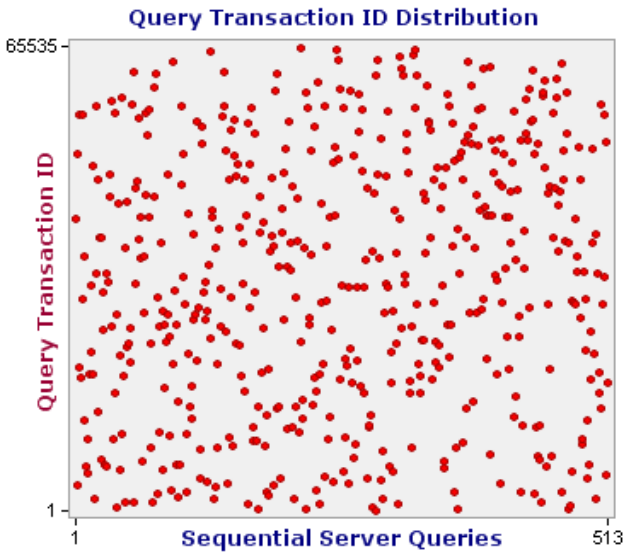
External Ping:	**replied**	(It might be better for the server to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**supported**	(This server supports improved security standards.)
Alphabetic Case:	**all lower**	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

Analysis of **466** queries from nameserver at [**146.112.128.70**]

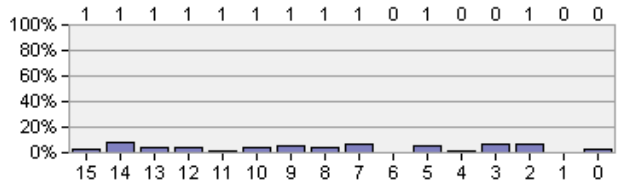
Anti-Spoofing Safety: **Excellent**

Server Name: **r7.compute.cdg1.edc.strln.net**

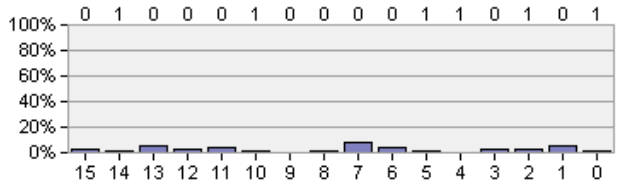




Source Port Bit Predictability



Transaction ID Bit Predictability



Query Source Port Analysis (worst case)

Max Entropy:	15.98	**Excellent**	Dir Bias:	0.65%	**Excellent**
Lost Entropy:	0.01	**Excellent**	Stuck Bits:	0	**Excellent**

Query Transaction ID Analysis (worst case)

Max Entropy:	15.99	**Excellent**	Dir Bias:	2.8%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

DNS Nameserver Access Details

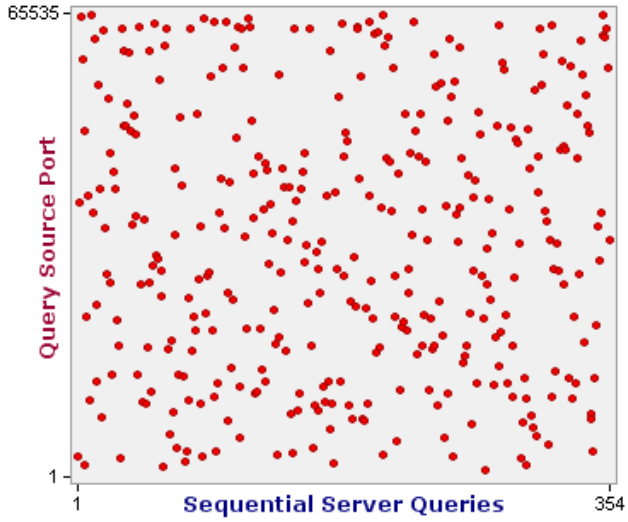
External Ping:	**replied**	(It might be better for the server to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**supported**	(This server supports improved security standards.)
Alphabetic Case:	**all lower**	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

Analysis of **306** queries from nameserver at [**146.112.128.77**]

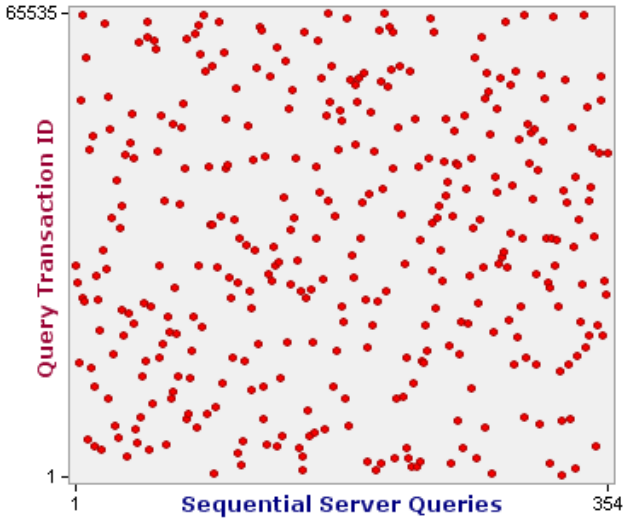
Anti-Spoofing Safety: **Excellent**

Server Name: **r3004.compute.cdg1.edc.strln.net**

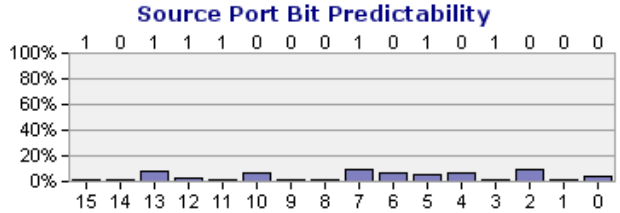
Query Source Port Distribution



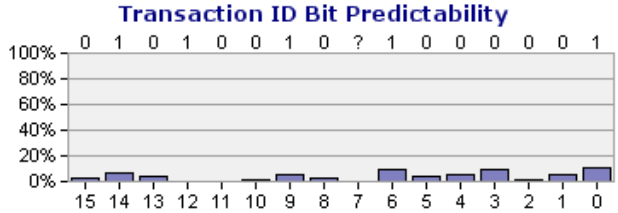
Query Transaction ID Distribution



Source Port Bit Predictability



Transaction ID Bit Predictability



Query Source Port Analysis (worst case)

Max Entropy:	15.97	**Excellent**	Dir Bias:	2.95%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

Query Transaction ID Analysis (worst case)

Max Entropy:	15.99	**Excellent**	Dir Bias:	0.33%	**Excellent**
Lost Entropy:	0.01	**Excellent**	Stuck Bits:	0	**Excellent**

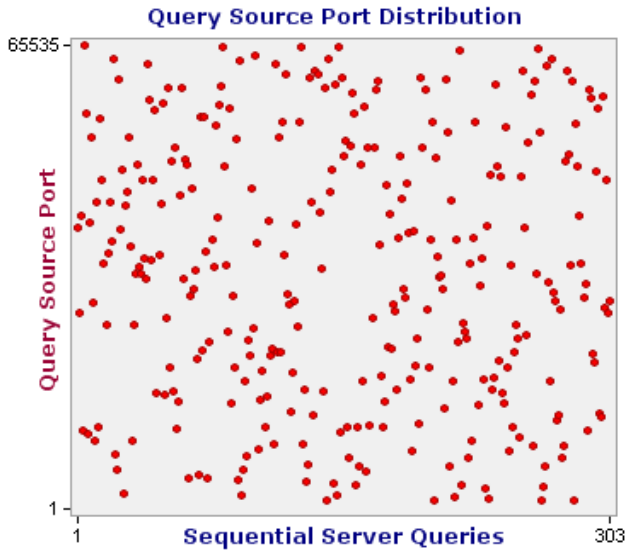
DNS Nameserver Access Details

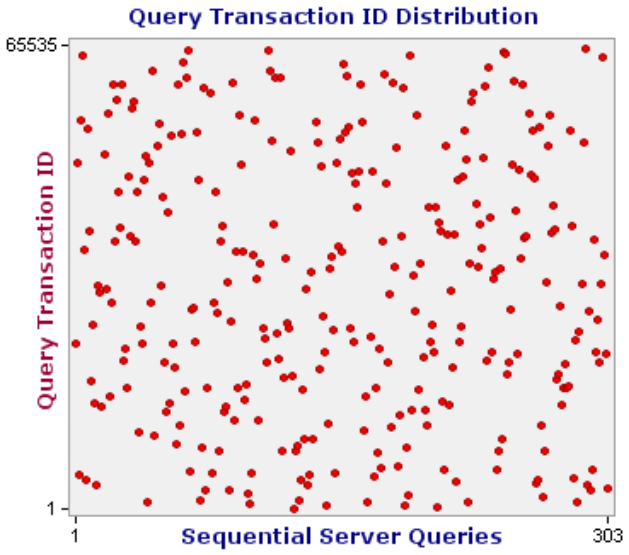
External Ping:	**replied**	(It might be better for the server to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**supported**	(This server supports improved security standards.)
Alphabetic Case:	**all lower**	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

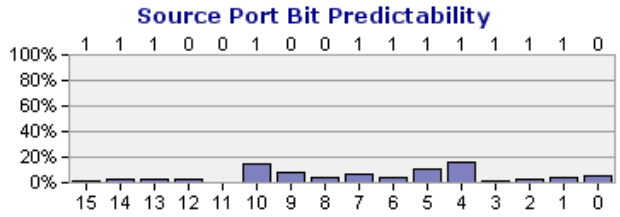
Analysis of **303** queries from nameserver at [**146.112.128.74**]

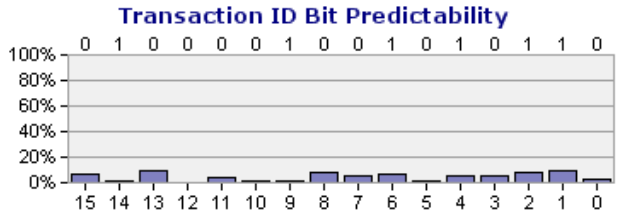
Anti-Spoofing Safety: **Excellent**

Server Name: **r3001.compute.cdg1.edc.strln.net**









Query Source Port Analysis (worst case)

Max Entropy:	15.97	**Excellent**	Dir Bias:	3.97%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

Query Transaction ID Analysis (worst case)

Max Entropy:	15.99	**Excellent**	Dir Bias:	1.99%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

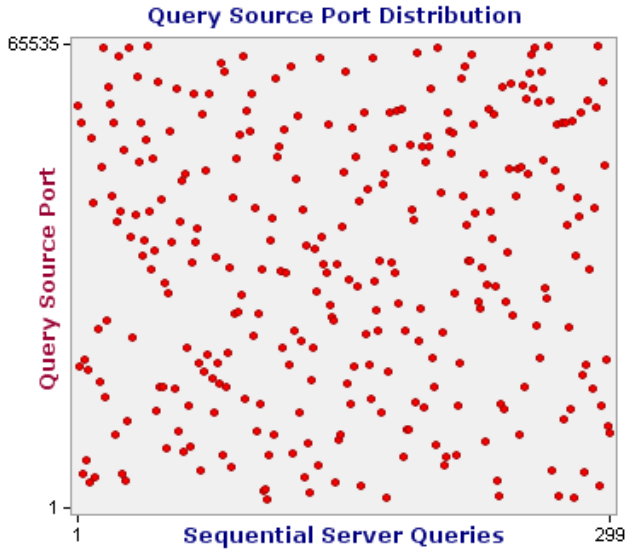
DNS Nameserver Access Details

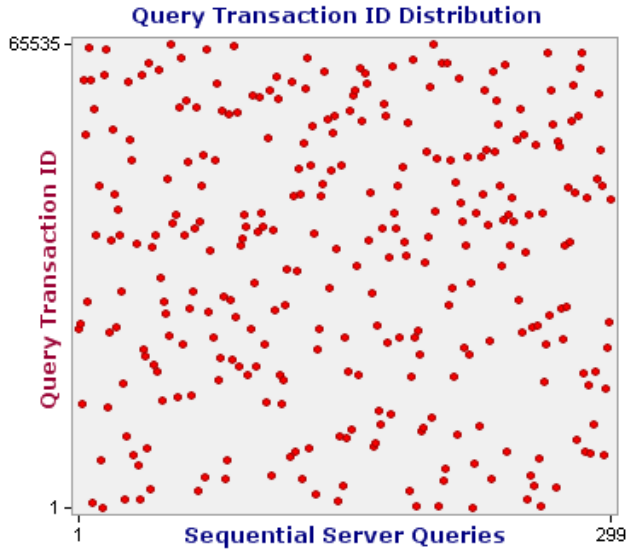
External Ping:	**replied**	(It might be better for the server to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**supported**	(This server supports improved security standards.)
Alphabetic Case:	**all lower**	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

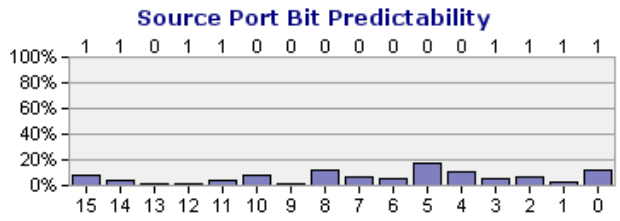
Analysis of **299** queries from nameserver at [**146.112.128.72**]

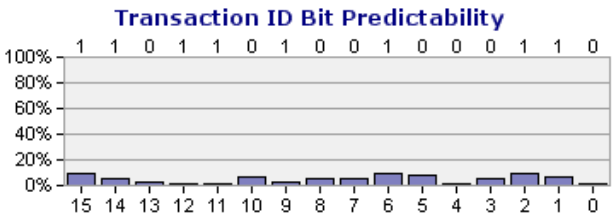
Anti-Spoofing Safety: **Excellent**

Server Name: **r9.compute.cdg1.edc.strln.net**









Query Source Port Analysis (worst case)

Max Entropy:	15.97	**Excellent**	Dir Bias:	2.01%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

Query Transaction ID Analysis (worst case)

Max Entropy:	16	**Excellent**	Dir Bias:	1.34%	**Excellent**
Lost Entropy:	0	**Excellent**	Stuck Bits:	0	**Excellent**

DNS Nameserver Access Details

External Ping:	**replied**	(It might be better for the server to be less visible.)
External Query:	**ignored**	(This means the nameserver is more spoof resistant.)
DNSSEC Security:	**supported**	(This server supports improved security standards.)
Alphabetic Case:	**all lower**	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	**unknown**	(Unable to obtain server fingerprint.)

- **DNS Spoofability:** If you are not familiar with the purpose and intention of this nameserver spoofability analysis, please refer to the introductory page of this site's DNS section. The detailed test results above and notes below assume a familiarity with the problem and terminology of "DNS spoofability."

And . . . would you like improved Internet performance?

- **DNS Benchmarking:** In addition to determining the spoofability of your DNS nameservers, GRC's free "DNS Benchmark" utility can test, compare and rank the name resolution performance of any DNS nameservers accessible to you. If the DNS nameservers provided by your ISP are overloaded, slow, or poorly connected (as too many are) you might find that your Internet experience can be dramatically improved by switching to faster, publicly available DNS nameservers. (We'll show you how.) Check it out!

Analysis Interpretation Guide

- **Excellent**
  Good
  Moderate
  Bad
  Very Bad

On the page above, several nameserver "spoofability" characteristics are ranked as shown to the left. These are intended to be rough but useful "rule of thumb" appraisals based upon our evolving experience with the Internet's nameservers as well as upon what's possible, reasonable and expected. Today, about 75% of the Internet's DNS nameservers rank "**Excellent.**" So if one or more of your DNS nameservers do not, understanding and exploring the reason for their sub-standard security may be worthwhile.

Scatter Charts:

Since your results may be totally perfect, we have assembled a gallery of decidedly less than perfect scatter charts, generated by real nameservers and submitted by this system's early testers, to give you a clear idea of some of the ways the charts might not be perfect.

Gallery of Sample DNS Nameserver Scatter Charts

- **The first question is: Is there a visible pattern to the dots?**
  The most prominent and important features of the nameserver spoofability analysis above are the two "scatter charts" that plot the values, over time, of the query source ports and transaction IDs contained within each resolving nameserver's query packets.

  So the question is: Are both charts filled with an **entirely random looking scattering** of red dots?

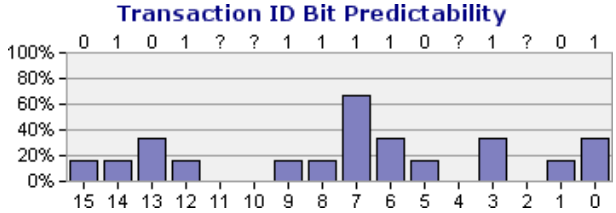
  Although we provide additional mathematical analysis underneath each chart, the human visual system and brain is extremely adept at discerning patterns. Any attacker who can successfully guess the location of the next dot within each of the charts will be able to successfully poison a nameserver's cache by creating a spoofed but apparently valid reply. And since any attacker can probe a nameserver just as we have, any pattern that **you** can detect can similarly be detected by an attacker. So the question is: Do **you** see any pattern that might allow the prediction of the next dot position?

- **The second question is: Is the entire chart space filled?**
  To minimize the predictability in a nameserver's queries, the values used for source port and transaction ID should use all of their available range. A restricted range means that attackers, who would also restrict the range of their guesses, have an increased chance of guessing correctly. So it's not good if there are large unoccupied regions in the charts above.

- **Scatter chart samples from real nameservers:**
  As we mentioned above, to give you a complete sense for how good and bad scatter charts would appear, we have assembled a gallery of scatter charts, many which did not fill us with confidence, that the testers of this system actually encountered. This link will open a second tab or window so that your results (above) will not be lost:

Gallery of Sample DNS Nameserver Scatter Charts

Bit Predictability Charts:



As good as the human eye is at detecting overall patterns, there are digital subtleties that humans would miss. For example, looking at a scatter chart, we would not notice if every random seeming value happened to be evenly divisible by four. If this were the case, an attacker could avoid guessing any port numbers that were not divisible by four to improve, by a factor of four, their chance of guessing the number. However, if those port numbers were represented as binary bits, the least significant two bits would always be zero (for any ports divisible by four.) In other words, those two bits out of sixteen would be completely predictable. To aid in helping to spot important digital subtleties that might otherwise be missed, the Bit Predictability chart analyzes and displays the predictability of each of the sixteen individual bits used to represent the query ports and transaction IDs.

Analysis Tables:

Query Source Port Analysis (worst case)

Max Entropy: 3.46 **Very Bad**	Dir Bias: 66.67% **Very Bad**
Lost Entropy: 0.22 **Good**	Stuck Bits: 11 **Very Bad**

The Query Port Analysis and Transaction ID Analysis tables each calculate four measures of randomness (or entropy) from their respective query sample sets. The table presents the "worst case" evaluation because that's the best that can be determined from sample sets that are small relative to the possible range of samples. These measurements are designed to quantify useful measures of nameserver query randomness:

- **Max Entropy** — from 0.00 (worst) to 16.00 (best) bits:
  This is the number of binary bits required to represent all of the possible values between the lowest and highest observed sample values. In effect, this provides a logarithmically

shaped indication of the observed span of sample values where 16 (bits) is the maximum possible and the larger the number is, the better.

- **Lost Entropy** — from 0.00 (best) to 16.00 (worst) bits:
  Even though there might be a high maximum potential entropy as measured by the lowest and highest value range above, a large number of duplicate sample values has the effect of wasting that potential entropy and making spoofed reply guessing more successful. Therefore, "Lost Entropy" measures the number of effective bits of entropy lost due to observed duplicate values.

- **Dir Bias** — from 0% (best) to 100% (worst) **dir**ection **bias**:
  A linearly increasing sample value would have a good, large "Max Entropy" (using the whole port range) and good, zero "Lost Entropy" (due to no repeats) which would, by those measures, appear to be terrific. But a simple linearly increasing value would obviously be very non-random and readily guessable. So the "Direction Bias" measurement examines every pair of adjacent values to detect any overall bias in the trend of the samples.

- **Stuck Bits:** — from 0 (best) to 16 (worst):
  Nothing reduces the effective randomness of sample values more than value bits that are "stuck" and never change. Every such stuck bit cuts the number of possible values in half, doubling the possible effectiveness of spoof reply guessing. But stuck bits, especially the lower numbered bits, are not visually obvious in a scatter chart. So this measure makes stuck bits very clear.

Access Details Table:

DNS Nameserver Access Details

External Ping:	**replied**	(It might be better for the server to be less visible.)
External Query:	**replied**	(It would be better for it to ignore external queries.)
DNSSEC Security:	**supported**	(This server supports improved security standards.)
Alphabetic Case:	**all lower**	(An improvement could be created by mixing case.)
Extra Anti-Spoofing:	**not present**	(No additional anti-spoofing technology.)

This table lists a number of features that have a bearing on a DNS nameserver's overall spoofability and security. The most important characteristic is whether the nameserver responds to external queries, since a nameserver that does not will be significantly more difficult, or perhaps impossible, to spoof because an attacker may be unable to induce such a nameserver to expect, and therefore accept, their spoofed replies. Additionally, some brands of nameserver — notably "Nominum" servers — may be equipped with advanced and proprietary anti-spoofing technology.

- **External Ping:**
  This is the classic "ping" (ICMP Echo) test to which most Internet appliances of any type will reply. Ignoring external pings (pings originating from outside the ISP's own local network) renders devices somewhat less visible, especially if the server also ignores external DNS queries.

- **External Query:**
  Any DNS resolver that only resolves DNS queries on behalf of its own ISP's network clients, while ignoring resolution queries originating from the Internet outside of the ISP's network, will be significantly more difficult, if not impossible, to spoof. If your ISP's resolvers ignore external queries you may have nothing to worry about — period.

- **DNSSEC Security:**
  Modern DNS servers support an advanced, next-generation technology known as "DNS Security" (DNSSEC). This system is not yet widely deployed on the Internet, so support for DNSSEC doesn't mean that a nameserver is spoof resistant. But if it is supported, it's a good sign that your ISP is keeping their nameservers up to date.

- **Alphabetic Case:**
  The DNS system is not sensitive to alphabetic case, so the domain "WWW.GRC.COM" is identical to "www.grc.com". DNS is designed to ignore but preserve the alphabetic case used in queries and replies. This creates an opportunity for a DNS resolver to add additional unknown bits of "entropy" to its queries by randomly changing the case of any alphabetic characters in the queried domain name. When replies are received, only the valid replying nameserver that received the mixed-case query could know the proper case for its reply. No spoofing server would know. This would give a clever resolver another way to reject spoofed replies. We know of no nameservers that are deliberately mixing case in this way, but through this test we are helping you to keep your eye out for any.

- **Extra Anti-Spoofing:**
  Since some nameservers, notably those by "Nominum", are claimed to incorporate advanced and proprietary anti-spoofing measures, this test attempts to determine the make, model and version of each querying resolver to detect whether they might be spoof-immune even though some of their other characteristics might be cause for alarm. In such

a case, we will display an explicit "Spoofability Mitigation Notice" to bring this to your attention so that you are not unduly alarmed.

Optional Spoofability Mitigation Notes:

> **Spoofability Mitigation Note:** Even though one or more of the individual "spoofability" parameters shown above indicates a worrying spoofability grade of "**Very Bad**", our fingerprinting of this server (see: Extra Anti-Spoofing) determined that it is enhanced with anti-spoofing technology rendering it immune to "Kaminsky-style" cache poisoning attacks.

> **Spoofability Mitigation Note:** Even though one or more of the individual "spoofability" parameters shown above does indicate a worrying spoofability grade of "**Bad**", our attempt to directly query this server from the Internet failed. Therefore, "Kaminsky-style" cache poisoning attacks will be either more difficult or impossible to conduct. As long as this nameserver remains inaccessible to Internet queries, there is little danger of it becoming a victim of Kaminsky-style cache poisoning attacks.

> **166 "Pseudo-Resolvers" in a Class-C Network:** As you can see from the details provided in the blue bar above, **474** queries were received from **166** unique IP addresses closely grouped within a single class-C network. In other words, only the *last byte* of the IP addresses of those **474** queries differed from each other. This indicates that rather than there being **166** actual nameservers at those individual IP addresses, only a **single** nameserver is located behind a "reverse NAT", causing it to emit queries from up to 256 randomly-chosen IP addresses. This introduces an additional eight (8) bits of uncertainty into this nameserver's queries, since the querying IP might have any least significant byte. Therefore, even if the nameserver's query source port range, or its transaction IDs, are limited, significant additional randomness has been introduced into this nameserver's queries.

A notice such as one of those above might be appended to a nameserver's report if we want to bring something to your attention. Typically this would be in response to an alarming report which should be of less concern due to some other factor, such as a resolver that ignores external queries or one whose make, model, and version are known to possess explicit anti-spoofing technology.

GRC's DNS Nameserver Spoofability Testing Pages:

1	DNS Introduction	5	DNS Benchmark
2	Router Crash Test	6	DNS Alternatives
3	Customizable Test	7	Frequent Questions
4	How This Works	8	Send Us Feedback

DNS Tests Usage Statistics:

	Standard	Custom	CrashTest
Daily Usage:	169	2	13
Total Usage:	1,904	18	135

Jump To Top