Measuring the effectiveness of DNS software fingerprinting tools

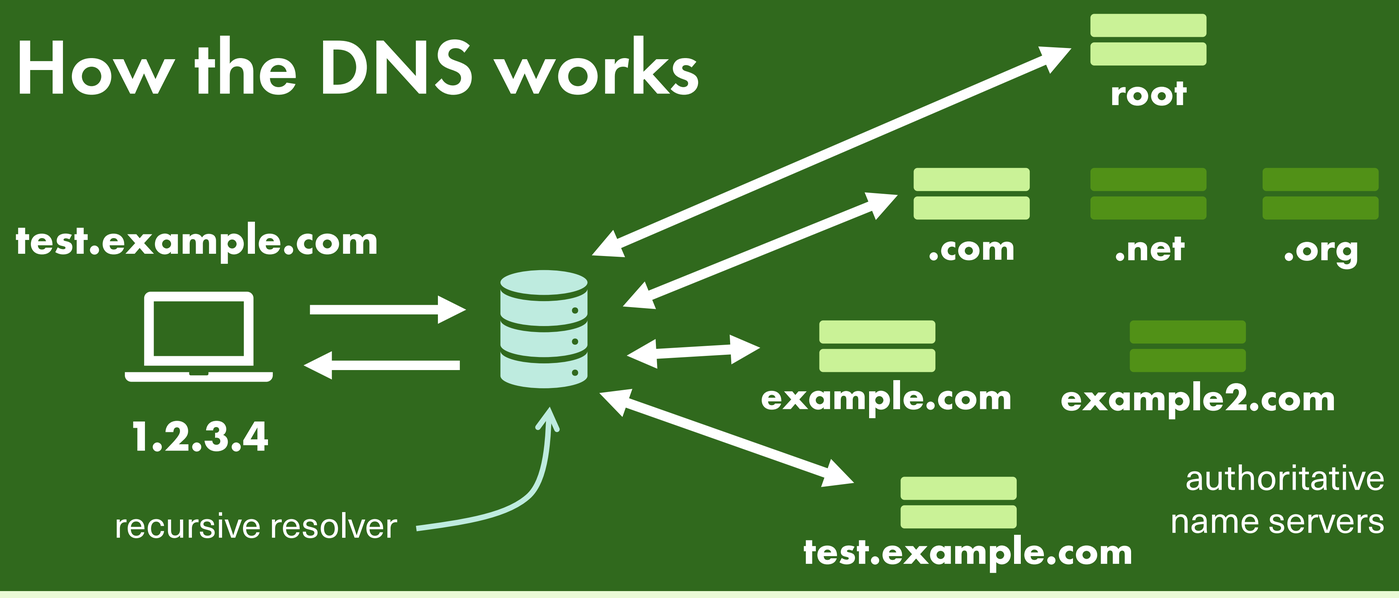
Results suggest that existing tools are unreliable

Rebecca Kempe*, AbdelRahman Abdou*
*School of Computer Science, Carleton University, Ottawa, ON

rebeccakempe@cmail.carleton.ca
https://cs.rkempe.ca

The Domain Name System (DNS) is the backbone of the Internet; it translates human-memorisable domain names into machine-readable IP addresses. DNS software fingerprinting tools remotely identify the specific software each server is using, which allows researchers to pinpoint potential security and privacy concerns in the DNS. We present the first systematic evaluation of two open-source DNS software fingerprinting tools: `fpdns` and `dnssoftver`. We empirically assess the accuracy of both tools and evaluate their strengths and limitations.

How the DNS works



Background & Objectives

DNS software implementations may be partial, flawed, or insecure. Fingerprinting tools allow researchers to identify vulnerabilities likely to affect DNS servers (e.g., memory exhaustion attacks [1]).

We found only two existing DNS software fingerprinting tools:

- `fpdns` [2], which compares DNS responses to a set of signatures to determine whether a product and version match can be found.
- `dnssoftver` [3, 4], which uses a decision tree–based ML classifier to determine the software running on resolvers at the product, major, minor, or patch version granularities.

Our goals were to measure the accuracy of these tools on software they claimed to support and to see whether product identification capabilities extended to newer or older versions.

Methodology

We set up 196 resolvers as our ground truth data set. We chose to test popular software that were supported by `dnssoftver`.

For each minor version of software, the earliest, the latest, and an intermediate patch version were chosen for testing. We used default settings for our configurations.

We additionally tested each tool on a set of 116 open resolvers identified through Censys [5, 6]. We had two objectives:

- Coverage of software we were unable to install locally.
- To see whether exposure to non-default configurations found in the wild would degrade results.

Resolvers were manually selected for the sample based on their self-reported software versions.

Results

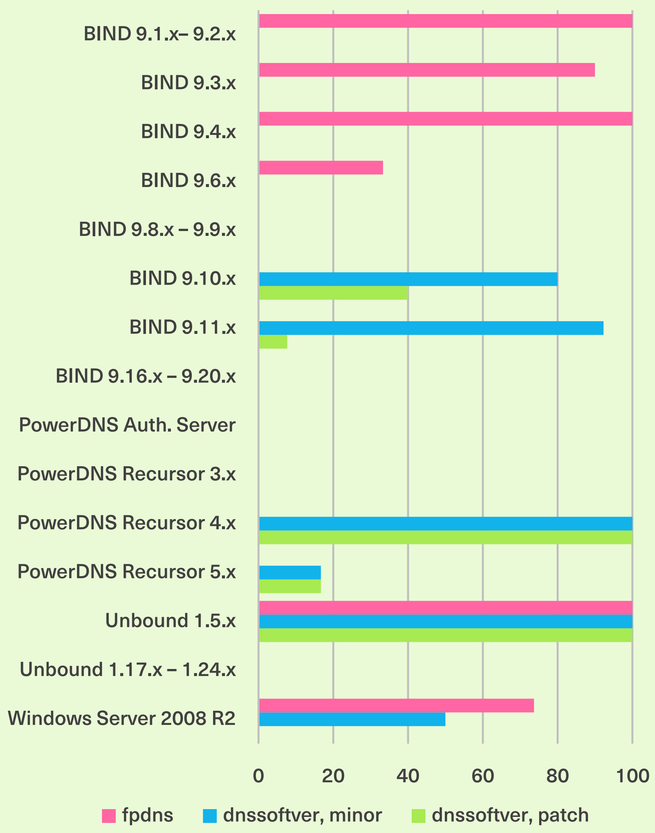


Figure 1: Percent accuracy of fingerprinting tools at the minor/patch version granularity when tested on open resolvers. While `fpdns` is accurate for some older software versions (mainly pre-2008 releases), `dnssoftver` is inaccurate for the majority of software versions tested.

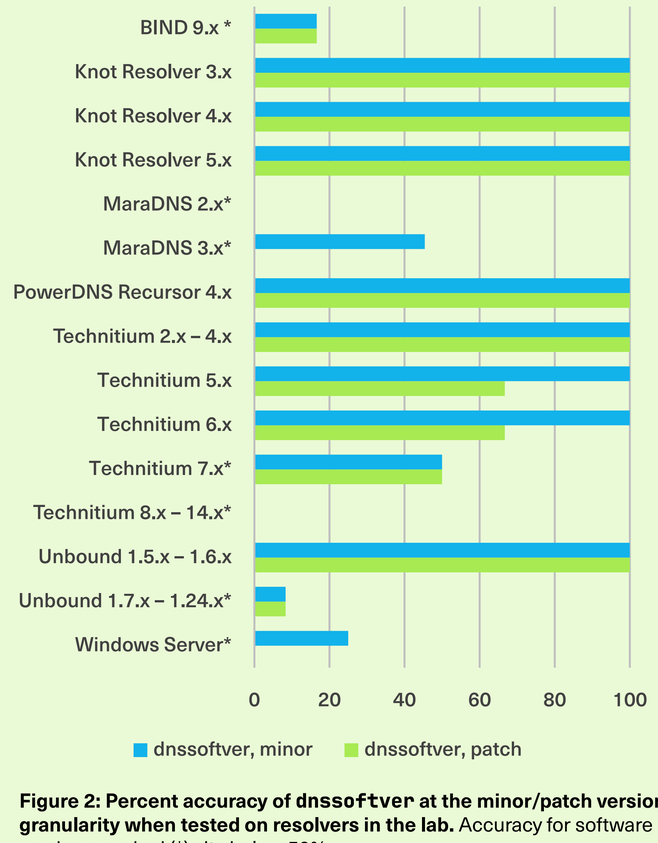


Figure 2: Percent accuracy of `dnssoftver` at the minor/patch version granularity when tested on resolvers in the lab. Accuracy for software versions marked (*) sits below 50%.

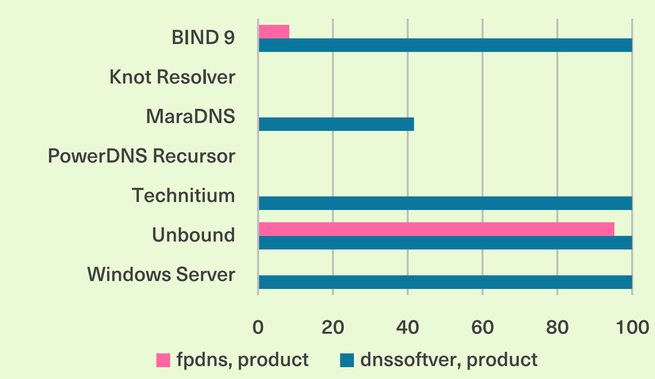


Figure 3: Percent accuracy of fingerprinting tools at the product granularity when tested on resolvers in the lab. fpdns can only reliably identify Unbound software, and `dnssoftver` consistently fails to identify Knot Resolver, PowerDNS Recursor, and MaraDNS.

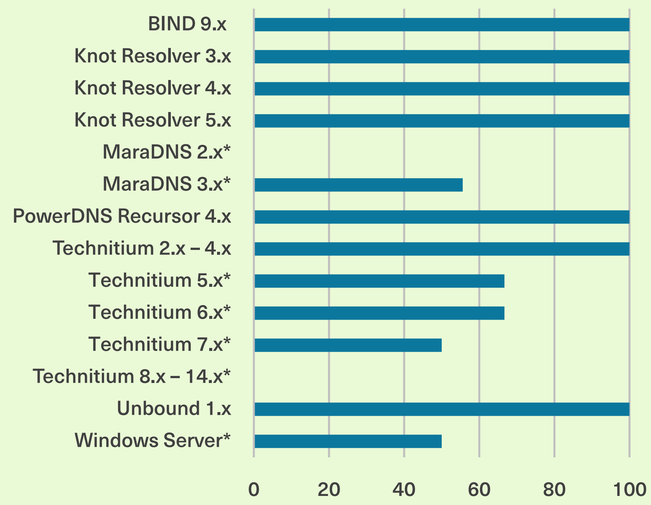


Figure 4: Percent accuracy of `dnssoftver` at the major version granularity when tested on resolvers in the lab. Accuracy for software versions marked (*) sits below 70%.

Conclusion

Our results suggest that `fpdns` reliably identifies pre-2008 software and consistently fails to identify newer software, whereas `dnssoftver` is unreliable across the board. The software `dnssoftver` was able to identify depended on the level of fingerprinting granularity chosen, and accuracy of `dnssoftver` dropped significantly when tested on open resolvers.

We posit that `dnssoftver`'s unreliability could be caused by insufficient training data and poor model training practices. Since `dnssoftver` is only trained on default configurations, it likely cannot adapt to the wide range of alternative configurations found in the wild.

References

[1] M. Kührer, T. Hupperich, J. Bushart, C. Rossow, and T. Holz, "Going Wild: Large-Scale Classification of Open DNS Resolvers", in *ACM IMC 2015*.
[2] R. Arends and J. Schlyter, *fpdns*. [Online]. Available: https://github.com/kirei/fpdns
[3] Y. Nosyk, *dnssoftver*. [Online]. Available: https://github.com/yevheniya-nosyk/dnssoftver
[4] Y. Nosyk, J. Bayer, A. Duda, and M. Korczyński, "dnssoftver: a tool to fingerprint DNS resolver software versions", *DNS-OARC 42*, Feb. 2024. [Online]. Available: https://www.youtube.com/watch?v=dyg8jcGoz-I
[5] Z. Durumeric, D. Adrian, A. Mirian, M. Bailey, and J. A. Halderman, "A Search Engine Backed by Internet-Wide Scanning", in *ACM CCS 2015*.
[6] Z. Durumeric et al., "Censys: A Map of Internet Hosts and Services", in *ACM SIGCOMM 2025*.
[7] Internet Systems Consortium (ISC), *BIND 9*. [Online]. Available: https://www.isc.org/bind/
[8] CZ.NIC, *Knot Resolver.* [Online]. Available: https://www.knot-resolver.cz/
[9] S. Trenholme, *MaraDNS.* [Online]. Available: https://maradns.samiam.org/
[10] PowerDNS, *PowerDNS Recursor.* [Online]. Available: https://www.powerdns.com/powerdns-recursor
[11] Technitium, *Technitium DNS Server.* [Online]. Available: https://technitium.com/dns/
[12] NLnet Labs, *Unbound.* [Online]. Available: https://nlnetlabs.nl/projects/unbound/about/
[13] Microsoft, What is Domain Name System (DNS)? [Online]. Available: https://learn.microsoft.com/en-us/windows-server/networking/dns/dns-overview