Московский институт электроники и математики им. А.Н. Тихонова

Департамент компьютерной инженерии

Москва **2024**

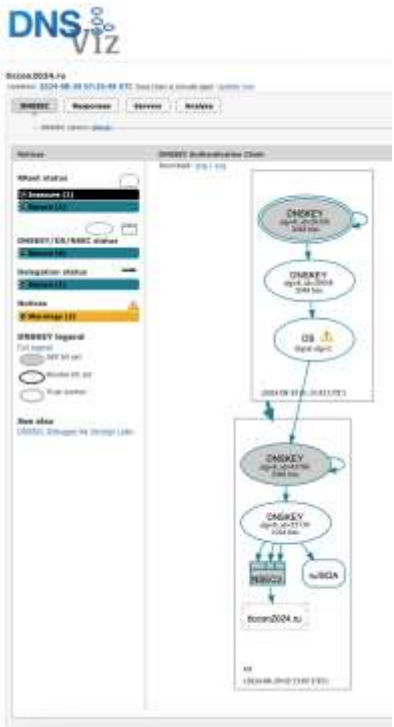
Логические схемы интернет-сервисов: взгляд от DNS

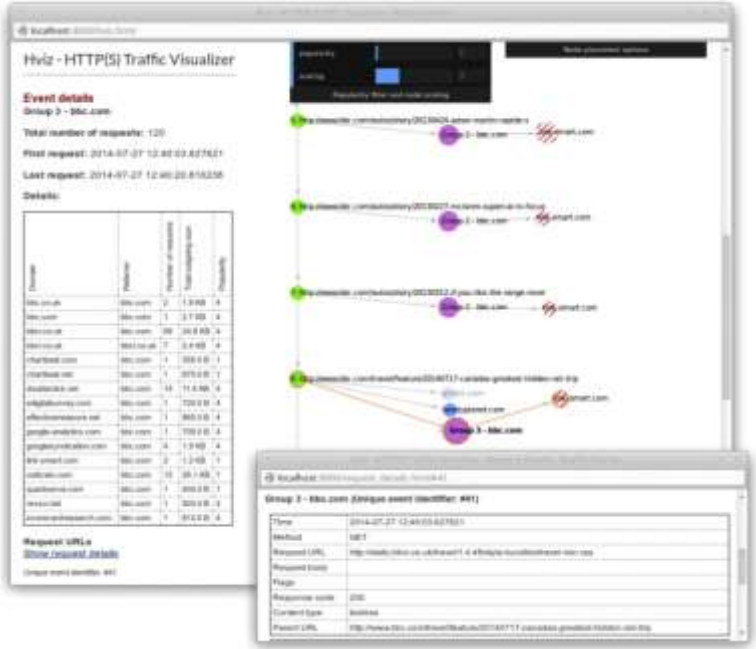
Александр Венедюхин, Артём Ождихин

"Сложность инфраструктуры, стоящей за современными интернет-сервисами, возникает как результат сопряжения различных сетевых протоколов, работающих на разных уровнях, но влияющих друг на друга. Например, использование HTTPS для доступа к DNS. При этом многие "технологические феномены" становятся хорошо видны только через достаточно общие методы визуализации, отталкивающиеся от "протокол-независимой" логики. DNS, являясь элементом фундамента Интернета, как раз предоставляет отличную точку старта для визуализации устройства прочих интернет-сервисов."

Цель работы: исследование вариантов визуализации для «протокол-независимой» логики

Аналоги





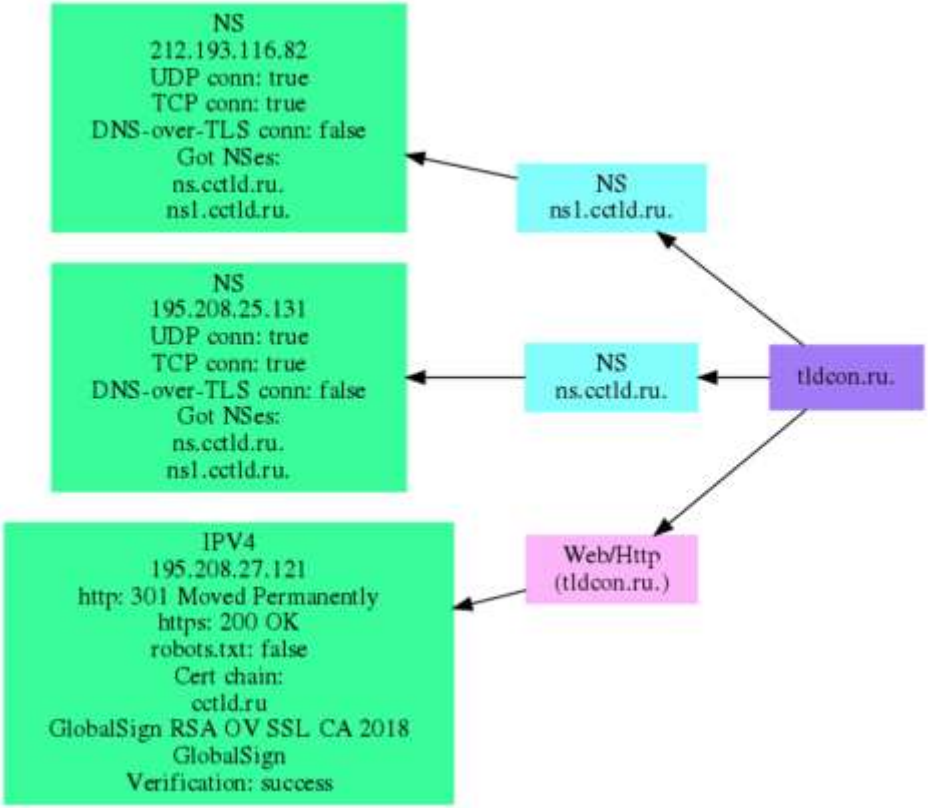
indata

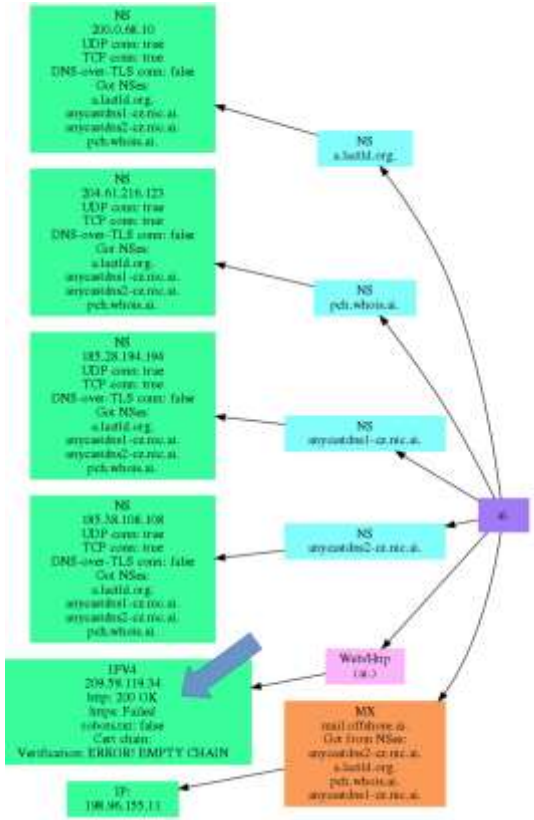
Данные:

1) DNS - NS-серверы, запросы по UDP/TCP, проверка запросом SOA, сбор списков NS-ов непосредственно с авторитативных NSов;
2) DoT на NS-ах;
3) A-записи, AAAA-записи;
4) TLS по A-записям (HTTP, 80/tcp);
5) HTTP - GET-, HEAD-запросы, GET /robots.txt;
6) MX - получение имён и A-записей для имён;
7) сравнение списков NS;
8) валидация TLS-сертификатов - для HTTPS, для DoT;
9) различные методы валидации сертификатов: с проверкой имени хоста, без проверки имени хоста, по системному списку доверенных сертификатов УЦ, по заданному списку сертификатов УЦ).

Инструменты: Golang, библиотека meikg/dns, остальное - типовые библиотеки.

Реализовано в рамках совместного проекта ФРСТ "ИнДата" и МИЭМ, 2024.

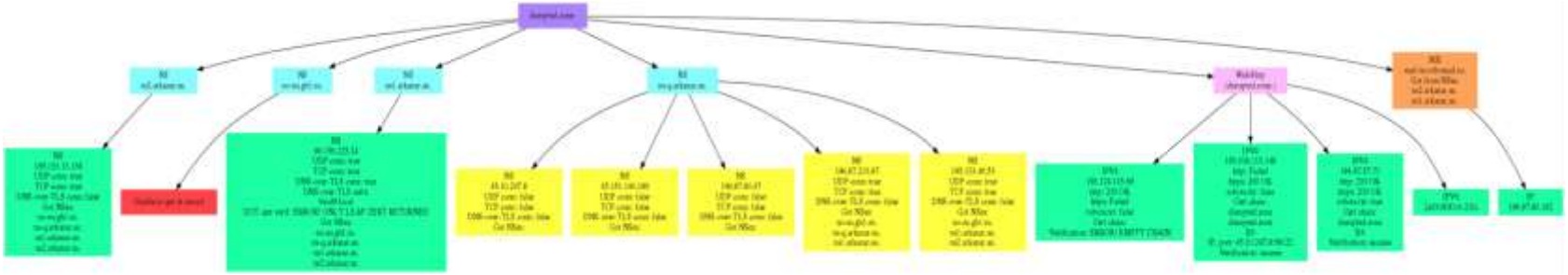

NS
212.193.116.82
UDP conn: true
TCP conn: true
DNS-over-TLS conn: false
Got NSes:
ns.cctld.ru.
ns1.cctld.ru.
NS
ns1.cctld.ru.
NS
195.208.25.131
UDP conn: true
TCP conn: true
DNS-over-TLS conn: false
Got NSes:
ns.cctld.ru.
ns1.cctld.ru.
NS
ns.cctld.ru.
tldcon.ru.
IPV4
195.208.27.121
http: 301 Moved Permanently
https: 200 OK
robots.txt: false
Cert chain:
cctld.ru
GlobalSign RSA OV SSL CA 2018
GlobalSign
Verification: success
Web/Http
(tldcon.ru.)



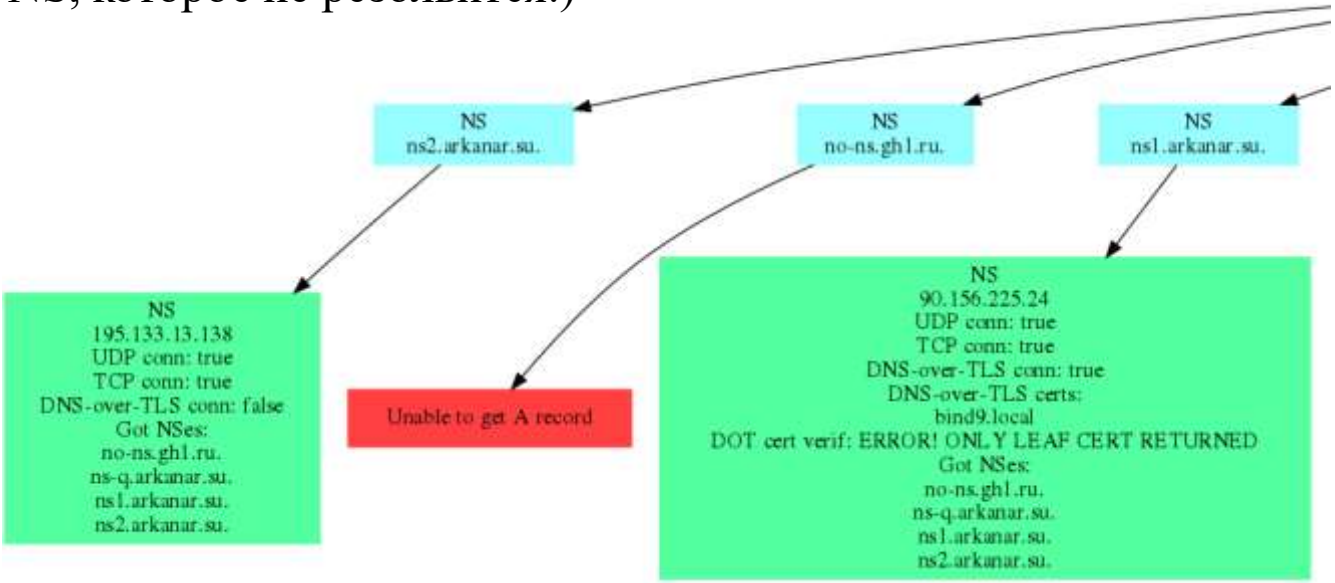
AI. (TLD)

В зоне есть A-запись: на графе видно, что под соответствующим адресом отвечает веб-сервер по HTTP, но не по HTTPS (видимо, не удалось сертификат выпустить через хорошо известный УЦ для зоны первого уровня).

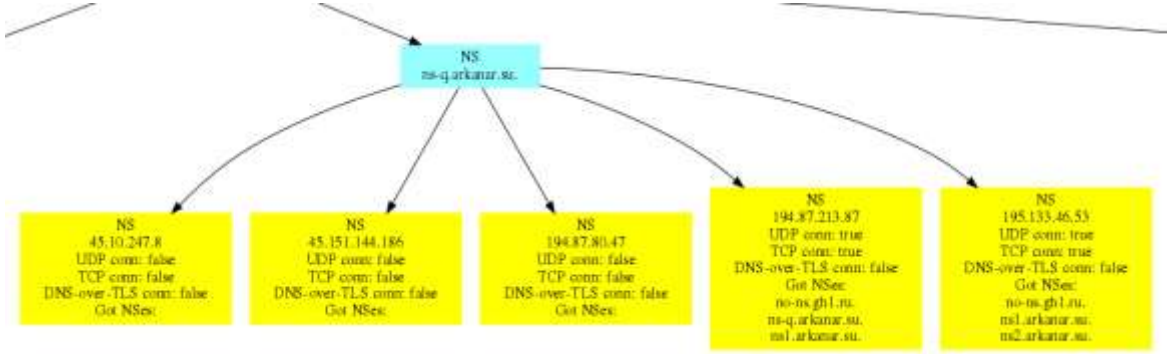
disrupted.zone -- специальная тестовая зона, используемая в ходе разработки сервисов;
показывает, как отображаются неверные настройки и дефекты.



disrupted.zone -- специальная тестовая зона.
(Имя NS, которое не резолвится.)

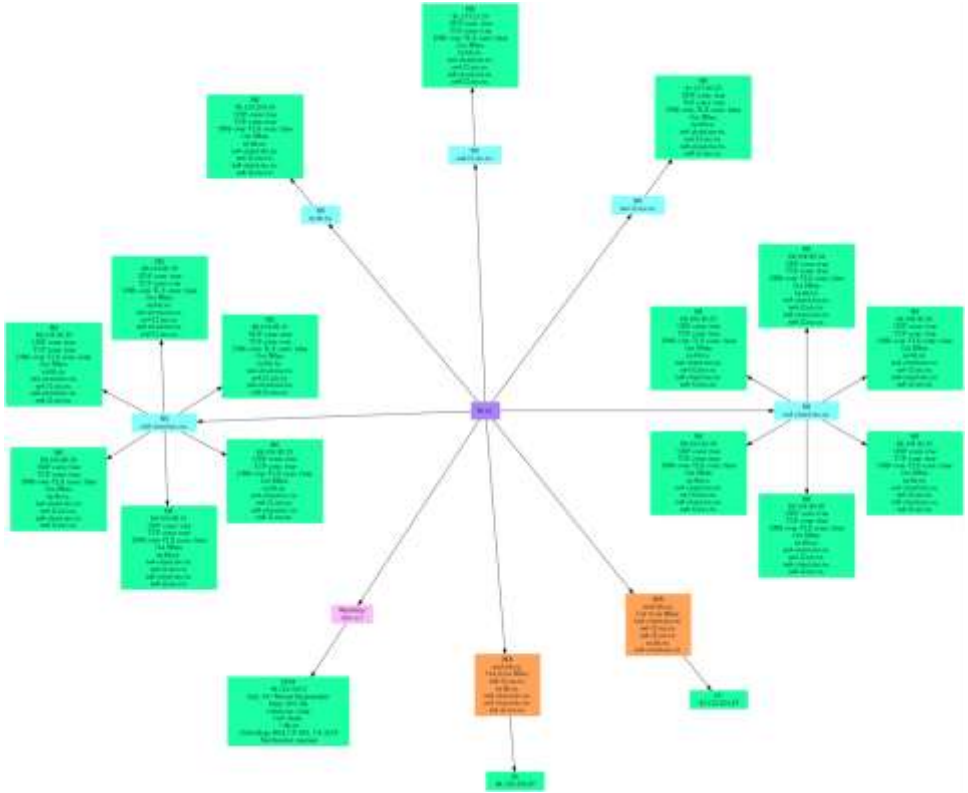


disrupted.zone -- специальная тестовая зона. (Одно имя NS-а, много IP, узлы под которыми возвращают разные списки NS-ов (некоторые – недоступны); на графе выделяется цветом.)



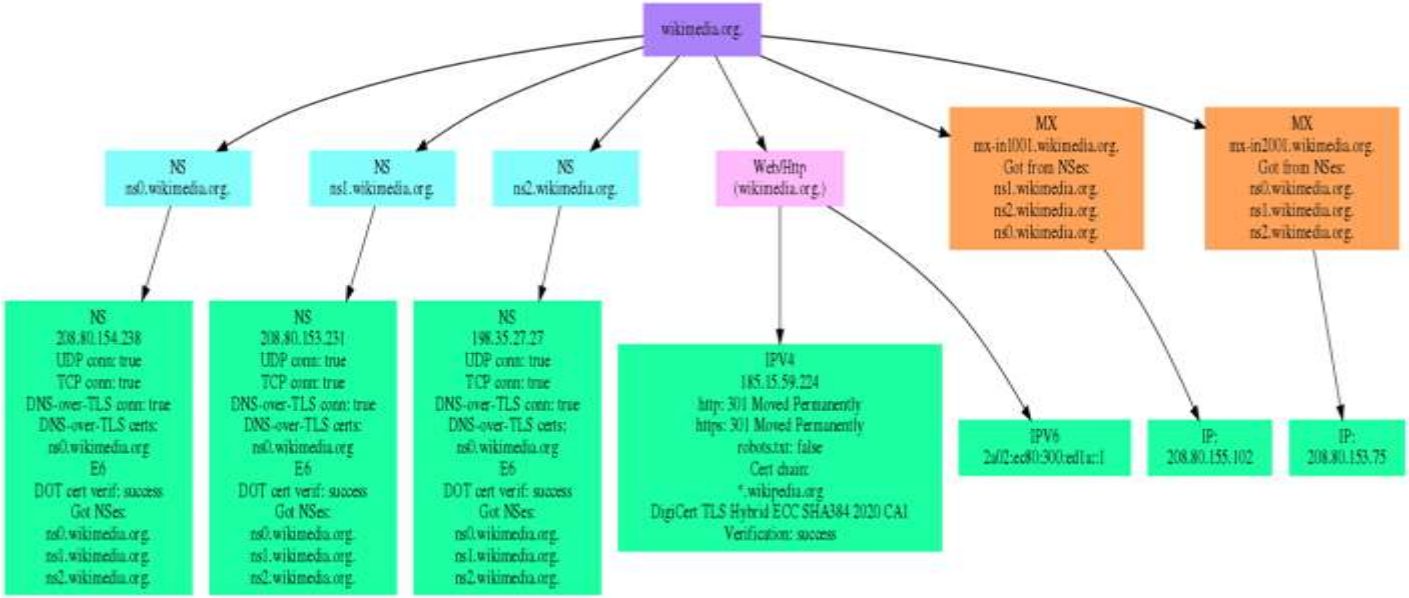
Недоступные узлы

Разные списки ns-ов



hh.ru
-- разнообразные схемы адресации NS-ов nic.ru (удобно использовать для иллюстрации того, что граф можно нарисовать "окружностями"; занятный IP-адрес в A-записи.)

wikimedia.org -- **есть поддержка DoT** на авторитативных NS-ах.



Результаты:

Ограничения (некоторые):

1) пока нет поддержки IPv6-соединений (только извлечение AAAA-записей, без подключения);
2) нет проверки HTTP-заголовков (только код статуса ответа);
3) (реализация пока не использует параллельный опрос узлов.)

Отображение:

Выводится описание графа (вершины-рёбра) на формальном языке, то есть, граф в машинно-читаемом виде, а это позволяет преобразовать результат к любому варианту отображения.
Описание графа на входном языке GraphViz - можно непосредственно использовать разные визуализаторы из пакета GraphViz.
Вывод двнных по узлам в формате JSON - годится для обработки другими инструментами, для записи в БД и пр.

Вопросы?