Министерство образования Республики Беларусь
Учреждение образования
“Гомельский государственный университет им. Франциска Скорины”

Отчёт по лабораторной работе №1

«Сбор предварительной информации»

Выполнил студент группы МС-42: Баль П. М.
Проверил: Грищенко В. В.

2022

Отчёт по лабораторной работе №1
«Сбор предварительной информации»

Цель работы: целью лабораторной работы является обучение методам и средствам сбора предварительной информации в Интернет об анализируемой КС.

Постановка задачи: выполнить предварительный сбор информации о домене gsmu.by. Работа выполняется на АРМ, имеющем доступ в сеть Интернет.

Последовательность действий

Шаг 1. Использование сервиса whois и RIPE Database

Полученная информация:

```
Регистратор:
ООО "Надежные программы"
Reliable Software, Ltd
Владелец домена:
Учреждение образования "Гомельский государственный медицинский
  университет"
BY, г. Гомель, -, 246000, ул. Ланге, д. 5, оф. 706
Регистрационный или иной идентификационный номер: 400022681
Телефон: +375232359766
E-mail: it.dep@gsmu.by
DNS-серверы:
Responsible organisation: Reliable Software, Ltd.
  Abuse contact info: abuse@hoster.by
u1.hoster.by       2a0a:7d80:1:1::4:0      93.125.30.201
inetnum:         93.125.30.0 - 93.125.30.255
netname:         HOSTERBY-6
org:             ORG-RSL39-RIPE
country:         BY
admin-c:         SP17043-RIPE
tech-c:          DO616-RIPE
status:          ASSIGNED PA
mnt-by:          BYGIS-MNT
mnt-by:          by-hosterby-1-mnt
mnt-routes:      AS6697-MNT
created:         2010-04-19T15:41:37Z
last-modified:   2022-04-06T12:13:08Z
route:           93.125.30.0/24
descr:           DELEGATED FROM BELPAK
origin:          AS6697
mnt-by:          AS6697-MNT
created:         2010-04-19T14:50:21Z
last-modified:   2010-04-19T20:34:37Z
source:          RIPE

u2.hoster.by       2a0a:7d80:3:2::b        178.172.137.158
```

```
inetnum:          178.172.136.0 - 178.172.139.255
netname:          HOSTERBY
country:          BY
admin-c:          SP17043-RIPE
tech-c:           DO616-RIPE
status:           ASSIGNED PA
mnt-routes:       AS12406-MNT
mnt-by:           AS35594-MNT
mnt-by:           by-hosterby-1-mnt
created:          2019-03-28T07:28:42Z
last-modified:    2019-03-28T07:28:42Z
route:            178.172.136.0/22
descr:            BN for HOSTERBY
origin:           AS12406
mnt-by:           AS12406-MNT
created:          2019-03-28T07:43:57Z
last-modified:    2021-11-16T07:14:55Z
source:           RIPE
Состояние:
Дата создания: 2012-05-14
Дата последнего обновления: 2022-03-15
Дата окончания: 2023-05-14
```

Шаг 2. Использование инструмента nslookup на веб-ресурсе network-tools.com

Name	TTL Until Refresh	Class	Type	Data
gsmu.by.	300	IN	SOA	u1.hoster.by. support.hoster.by. 2022091601 43200 7200 604800 600
gsmu.by.	300	IN	MX	10 mx3.dc.beltelecom.by. 178.124.138.141
gsmu.by.	300	IN	A	195.50.7.160
gsmu.by.	300	IN	TXT	"google-site-verification=25jR3c3eJsK_1Mawt3rg_u3pTdJjqwwF4cxvZNmjIMA"

Name	TTL Until Refresh	Class	Type	Data
gsmu.by.	300	IN	TXT	"v=spf1 +a +mx include:_spf.hoster.by include:_spf.yandex.ru ~all"
gsmu.by.	300	IN	NS	u1.hoster.by. 93.125.30.201
gsmu.by.	300	IN	NS	u2.hoster.by. 178.172.137.158

A: the IPv4 address of the domain.
AAAA: the domain's IPv6 address.
CNAME: the canonical name — allowing one domain name to map on to another. This allows more than one website to refer to a single web server.
MX: the server that handles email for the domain.
NS: one or more authoritative name server records for the domain.
TXT: a record containing information for use outside the DNS server. The content takes the form name=value. This information is used for many things including authentication schemes such as SPF and DKIM.

Шаг 3. Проверить полученные данные вручную, использую инструменты host, dig и nslookup

Google Admin Toolbox Dig:

```
gsmu.by. 600 IN NS u1.hoster.by.
gsmu.by. 600 IN NS u2.hoster.by.
gsmu.by. 21600 IN TXT "google-site-
  verification=25jR3c3eJsK_1Mawt3rg_u3pTdJjqwwF4cxvZNmjIMA"
gsmu.by. 21600 IN TXT "v=spf1 +a +mx include:_spf.hoster.by
  include:_spf.yandex.ru ~all"
gsmu.by. 600 IN A 195.50.7.160
gsmu.by. 600 IN MX 10 mx3.dc.beltelecom.by.
gsmu.by. 600 IN SOA u1.hoster.by. support.hoster.by. 2022101902
  43200 7200 604800 600
```

Check-host.net:

IP: 151.249.161.143 **Country:** Belarus (Homyel' Voblasc', Homyel)

lgsmu.by

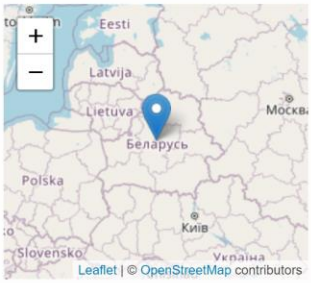
Info | Ping | HTTP | TCP port | UDP port | DNS

IP and website location: gsmu.by

DB-IP (03.10.2022)

IP address	**195.50.7.160**
Host name	195.50.7.160
IP range	195.50.4.0-195.50.7.255 CIDR
ISP	BeCloud 2
Organization	
Country	**Belarus** (BY)
Region	Minsk City
City	Minsk (Lieninski rajon)
Time zone	Europe/Minsk, GMT+0300
Local time	19:59:37 (+03) / 2022.10.19
Postal Code	220030

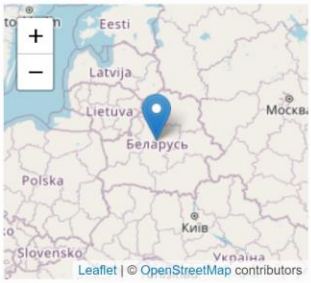
Powered by DB-IP



IPGeolocation.io (13.10.2022)

IP address	**195.50.7.160**
Host name	195.50.7.160
IP range	195.50.7.0-195.50.7.255 CIDR
ISP	Belarusian Cloud Technologies LLC
Organization	Belarusian Cloud Technologies LLC
Country	**Belarus** (BY)
Region	Minsk
City	Minsk
Time zone	Europe/Minsk, GMT+0300
Local time	19:59:37 (+03) / 2022.10.19
Postal Code	220036

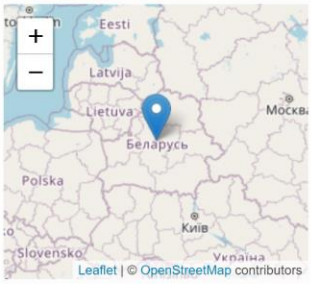
Powered by IPGeolocation.io



IP2Location (03.10.2022)

IP address	**195.50.7.160**
Host name	195.50.7.160
IP range	195.50.0.0-195.50.31.255 CIDR
ISP	
Organization	
Country	**Belarus** (BY)
Region	Minskaya voblasts'
City	Minsk
Time zone	+03:00
Local time	19:59:37 (+0300) / 2022.10.19
Postal Code	220088

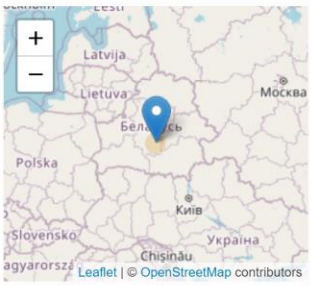
Powered by IP2Location



MaxMind GeoIP (06.10.2022)

IP address	**195.50.7.160**
Host name	195.50.7.160
IP range	
ISP	
Organization	
Country	**Belarus** (BY)
Region	
City	
Time zone	Europe/Minsk, GMT+0300
Local time	19:59:37 (+03) / 2022.10.19
Postal Code	

Powered by MaxMind GeoIP



Nslookup:

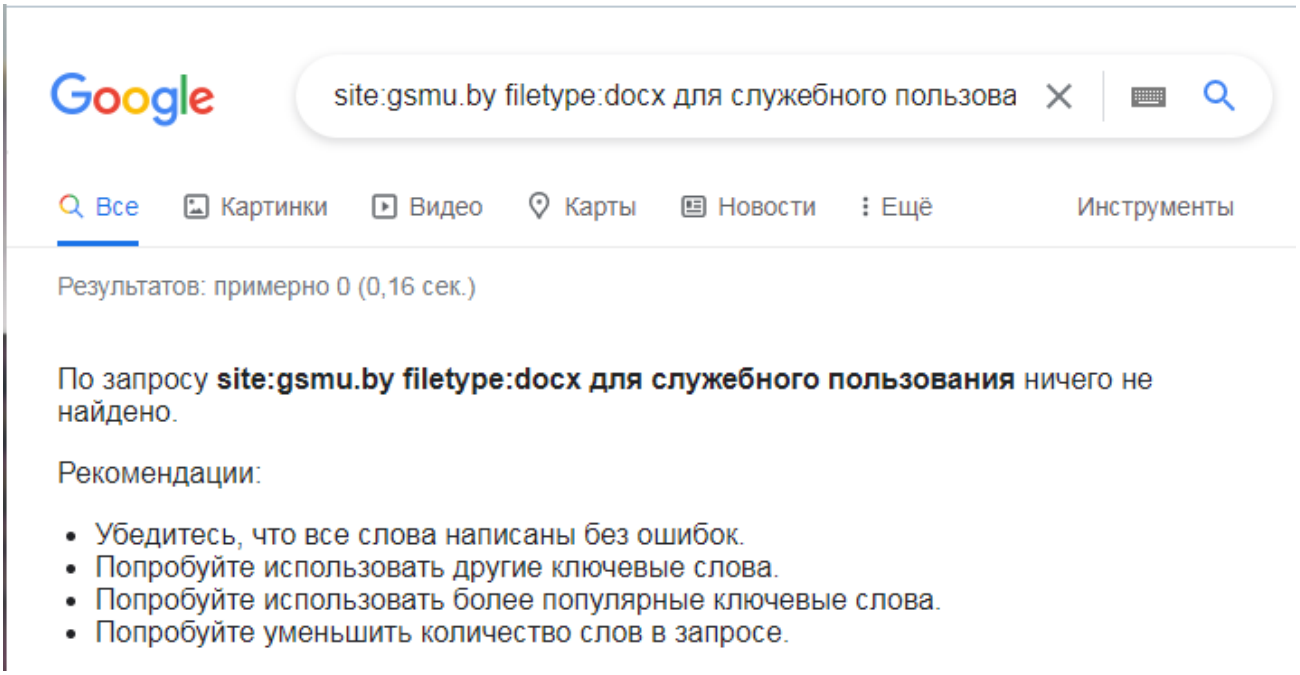
```
λ nslookup gsmu.by
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    gsmu.by
Address:  195.50.7.160
```

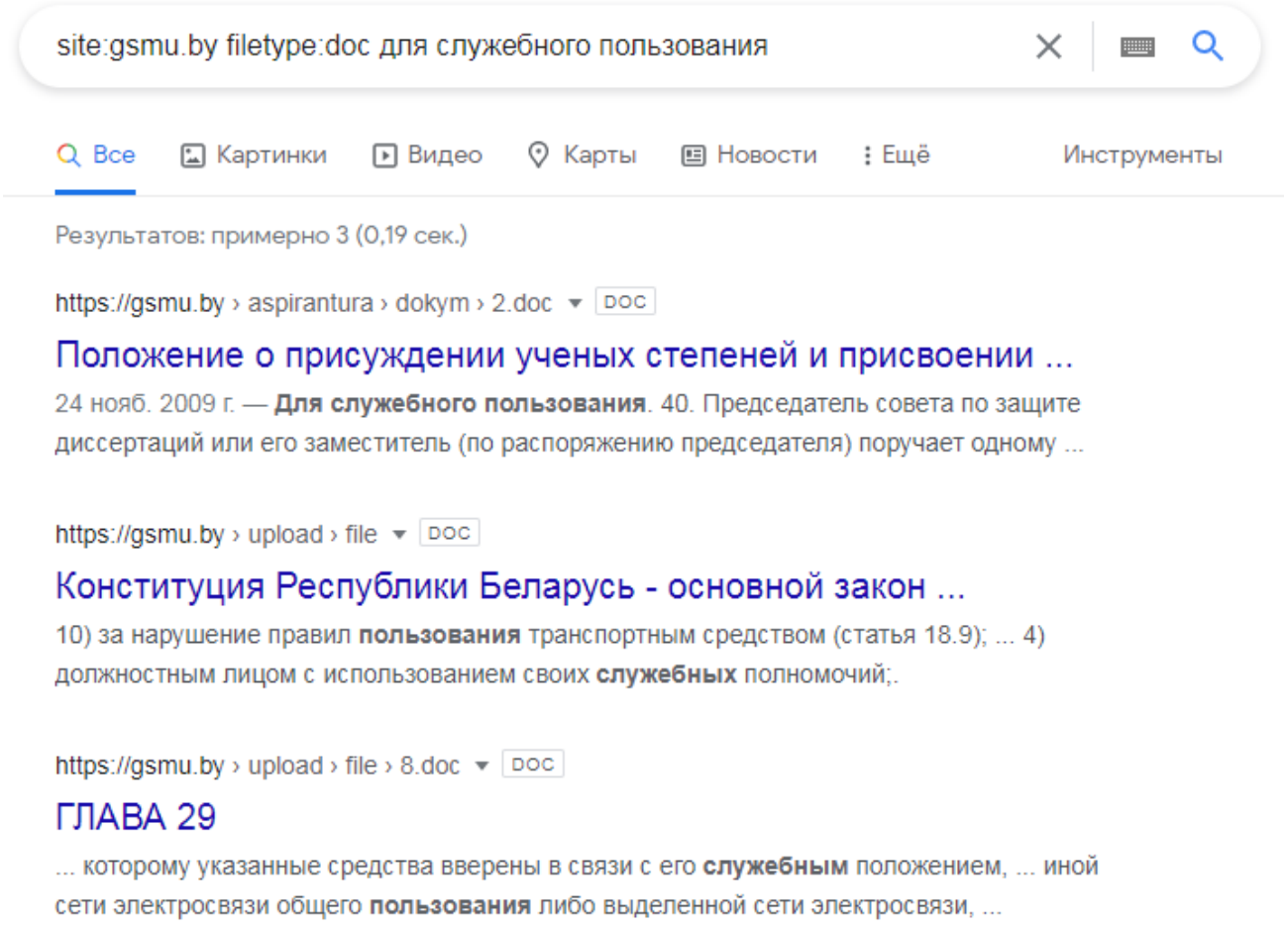
Шаг 4. Проверим наличие узлов найденных сетей в базах данных спам-отправителей

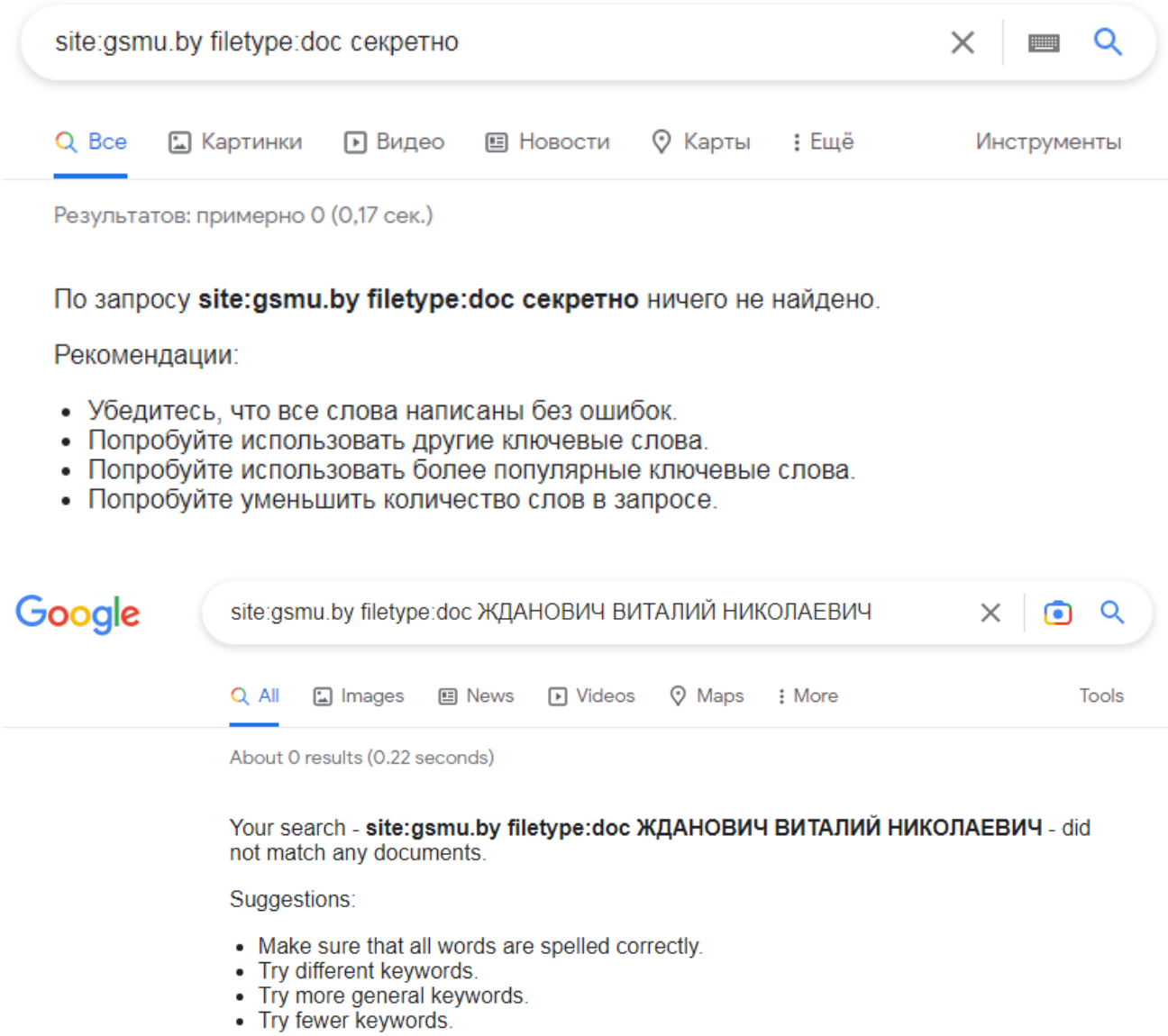
Шаг 5. Проверим возможность выполнения переноса зоны на первичном и вторичном DNS-серверах:

```
λ nslookup
Default Server:  UnKnown
Address:  192.168.0.1

> server mx3.dc.beltelecom.by
Default Server:  mx3.dc.beltelecom.by
Address:  178.124.138.141

> set type=any
> ls -d gsmu.by
*** Can't list domain gsmu.by: No response from server
The DNS server refused to transfer the zone gsmu.by to your
  computer. If this is incorrect, check the zone transfer security
  settings for gsmu.by on the DNS server at IP address
  178.124.138.141.
```

Шаг 6. Попытаемся найти потенциально интересующую нас информацию в google.ru:


Google
site:gsmu.by filetype:docx для служебного пользова
Все
Картинки
Видео
Карты
Новости
Ещё
Инструменты
Результатов: примерно 0 (0,16 сек.)
По запросу site:gsmu.by filetype:docx для служебного пользования ничего не найдено.
Рекомендации:
Убедитесь, что все слова написаны без ошибок.
Попробуйте использовать другие ключевые слова.
Попробуйте использовать более популярные ключевые слова.
Попробуйте уменьшить количество слов в запросе.


site:gsmu.by filetype:doc для служебного пользования
Все
Картинки
Видео
Карты
Новости
Ещё
Инструменты
Результатов: примерно 3 (0,19 сек.)
https://gsmu.by › aspirantura › dokym › 2.doc
DOC
Положение о присуждении ученых степеней и присвоении ...
24 нояб. 2009 г. — Для служебного пользования. 40. Председатель совета по защите диссертаций или его заместитель (по распоряжению председателя) поручает одному ...
https://gsmu.by › upload › file
DOC
Конституция Республики Беларусь - основной закон ...
10) за нарушение правил пользования транспортным средством (статья 18.9); ... 4) должностным лицом с использованием своих служебных полномочий;.
https://gsmu.by › upload › file › 8.doc
DOC
ГЛАВА 29
... которому указанные средства вверены в связи с его служебным положением, ... иной сети электросвязи общего пользования либо выделенной сети электросвязи, ...



Шаг 7. Используя веб-инструмент traceroute, расположенный на веб-ресурсе http://network-tools.com, определим маршруты прохождения IP-дейтаграмм до исследуемой сети.

Traceroute Check for: **195.50.7.160**

traceroute to 195.50.7.160 (195.50.7.160), 10 hops max, 60 byte packets
1 216.182.237.223 (216.182.237.223) 3.653 ms 216.182.237.209 (216.182.237.209) 53.566 ms 216.182.237.223 (216.182.237.223) 3.585 ms
2 100.65.16.128 (100.65.16.128) 19.998 ms 100.65.19.0 (100.65.19.0) 17.537 ms 100.65.16.128 (100.65.16.128) 19.916 ms
3 100.66.8.48 (100.66.8.48) 21.253 ms 100.66.8.140 (100.66.8.140) 19.599 ms 100.66.8.54 (100.66.8.54) 11.816 ms
4 100.66.11.68 (100.66.11.68) 11.950 ms 100.66.11.66 (100.66.11.66) 16.140 ms 100.66.11.96 (100.66.11.96) 16.851 ms
5 241.0.6.131 (241.0.6.131) 0.500 ms 241.0.6.132 (241.0.6.132) 0.499 ms 241.0.6.140 (241.0.6.140) 0.495 ms
6 240.0.176.20 (240.0.176.20) 0.527 ms 240.0.176.17 (240.0.176.17) 0.327 ms 240.0.176.27 (240.0.176.27) 0.327 ms
7 242.2.44.129 (242.2.44.129) 0.394 ms 242.2.45.1 (242.2.45.1) 1.400 ms 242.2.45.129 (242.2.45.129) 0.427 ms
8 52.93.237.213 (52.93.237.213) 1.780 ms 15.230.36.85 (15.230.36.85) 1.988 ms 52.93.47.83 (52.93.47.83) 2.340 ms
9 150.222.30.198 (150.222.30.198) 5.960 ms 52.93.237.240 (52.93.237.240) 1.643 ms 150.222.31.42 (150.222.31.42) 2.286 ms
10 150.222.30.47 (150.222.30.47) 6.536 ms 150.222.97.49 (150.222.97.49) 1.727 ms 54.240.242.99 (54.240.242.99) 1.555 ms

Вывод: изучили методы и средства сбора предварительной информации в Интернет.