

УО «Гомельский государственный университет им. Ф. Скорины»
Физический факультет
Кафедра общей физики

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 1

Сбор предварительной информации

Проверил:
Грищенко В.В.

Выполнили:
студент группы МС-42
Гончаров Владислав

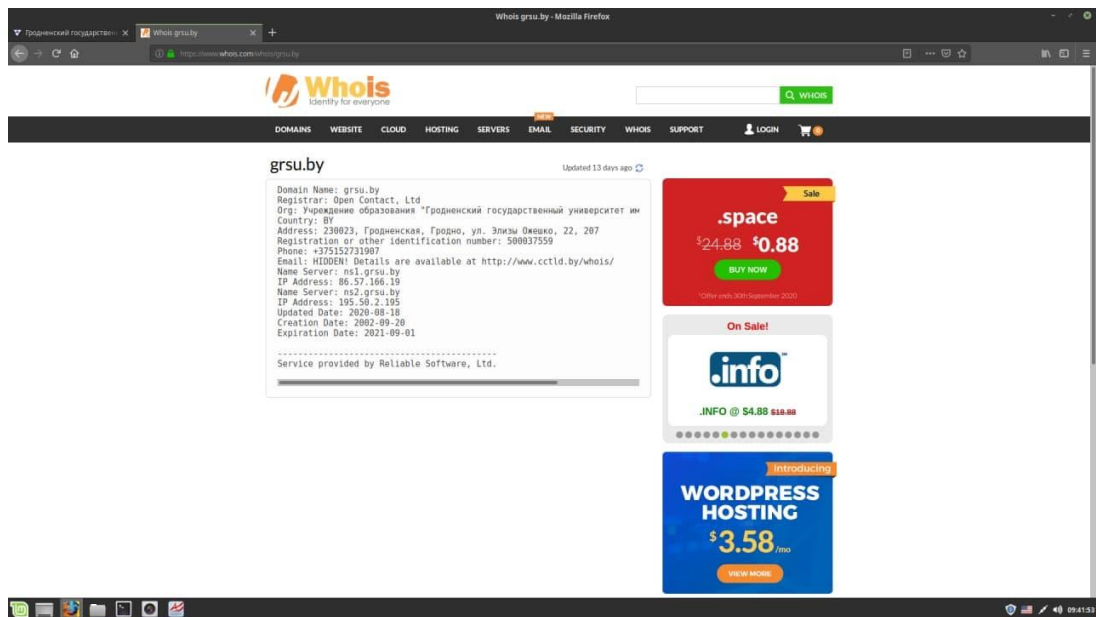
Гомель 2020

Лабораторная работа №1

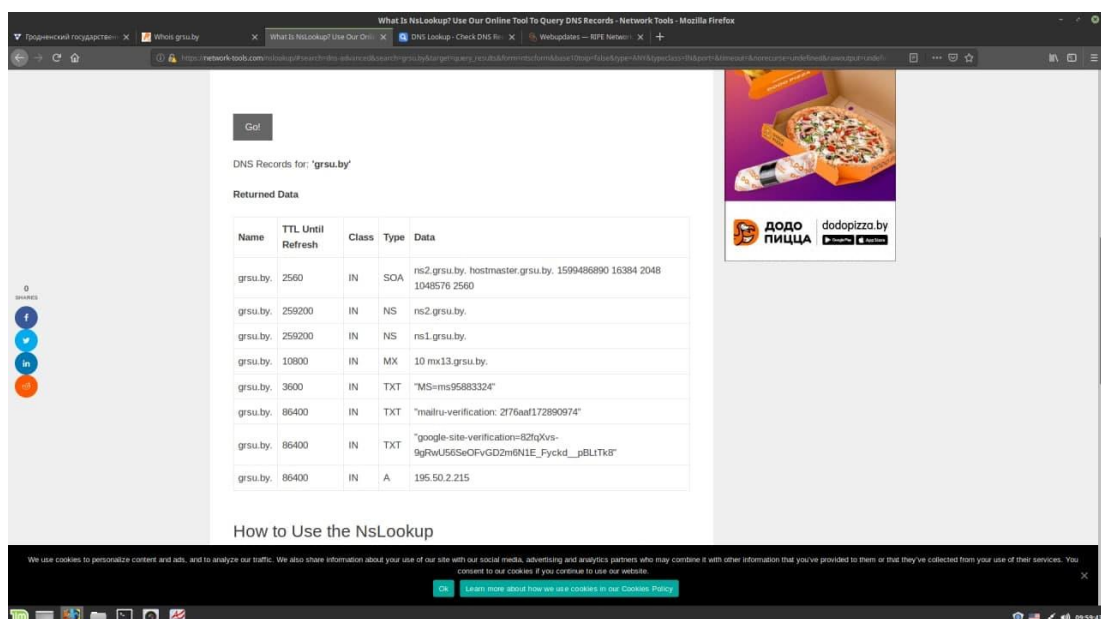
Цель работы: обучение методам и средствам сбора предварительной информации в Интернет об анализируемой КС.

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

Шаг 1. Перейти по адресу <https://www.whois.com> Проанализировать полученные данные. Найти DNS-имена и IP-адреса серверов имен.



Шаг 2. Перейти по адресу <http://network-tools.com/nslookup>. Определить почтовый сервер организации.



Webupdates — RIPE Network Coordination Centre - Mozilla Firefox

By submitting this form you explicitly express your agreement with the RIPE Database Terms and Conditions

Search results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

Responsible organisation: Republican Unitary Telecommunication Enterprise Beltelecom
Abuse contact info: abuse@rodna.by

inetnum: 88.57.166.0 - 88.57.166.255
netname: BYELY-GRODNO-ETHERNET
descr: BELTELECOM
descr: GRODNO branch
descr: BYELY(tn) static assignments
descr: Ethernet subscriber network
descr: Republic of Belarus
country: BY
admin-c: BYEG-RIPE
tech-c: BYEG-RIPE
abuse-c: BYEG-RIPE
status: LIR-PARTITIONED PA
mnt-by: ASS607-MNT
mnt-routes: ASS607-MNT
mnt-lower: GRODNOBELTELECOM-MNT
mnt-domains: GRODNOBELTELECOM-MNT
created: 2020-02-25T13:02:53Z
last-modified: 2020-02-25T13:02:53Z
source: RIPE

route: 88.57.166.0/24
origin: ASS607
mnt-by: ASS607-MNT
created: 2017-12-04T15:57:26Z
last-modified: 2017-12-04T15:57:26Z
source: RIPE

RIPE Database Software Version 1.97.2

The RIPE NCC uses cookies. Some of these cookies may have been set already. More information about our cookies can be found in our [privacy policy](#). You can accept our cookies either by [clicking here](#) or by continuing to use the site.

Webupdates — RIPE Network Coordination Centre - Mozilla Firefox

Search results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

Responsible organisation: Institution Central Information and Analytical Center at the Ministry of Education of Belarus
Abuse contact info: admin@unibel.by

inetnum: 195.50.0.0 - 195.50.3.255
netname: UNIBEL
descr: Education and Science Computer
descr: Network of the Republic of Belarus
country: BY
org: ORG-UA2-RIPE
admin-c: UNBK
tech-c: UNBK
tech-c: UNBK
status: ASSIGNED PA
mnt-by: ASS498-MNT
mnt-domains: ASS498-MNT
mnt-routes: ASS498-MNT
created: 2016-06-20T16:35:44Z
last-modified: 2016-10-12T15:06:59Z
source: RIPE-Filtered

route: 195.50.2.0/24
descr: UNIBEL
origin: ASS498
mnt-by: ASS498-MNT
created: 2011-09-04T14:10:11Z
last-modified: 2011-09-04T14:10:11Z
source: RIPE

RIPE Database Software Version 1.97.2

Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Terms of Service

The RIPE NCC uses cookies. Some of these cookies may have been set already. More information about our cookies can be found in our [privacy policy](#). You can accept our cookies either by [clicking here](#) or by continuing to use the site.

Webupdates — RIPE Network Coordination Centre - Mozilla Firefox

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database (WebUI) | Website

Search IP Address or ASN

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

You are here: Home > Manage IPs and ASNs > RIPE Database > Webupdates

Resources >

RIPE Database

Query the RIPE Database

Full Text Search

Synopses

Create an Object

Lookup results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

person: Kate Plinukovich
address: Belarus
address: 220088 Minsk
address: 59, Zaharova str.
address: UNIBEL
phone: +375 17 2100250
fax-no: +375 17 2100099
e-mail: katec.ripe@unibel.by
nic-hdl: UNBK
remarks: -----
notify: ripe@unibel.by
mnt-by: ASS498-MNT
created: 2016-10-12T15:08:14Z
last-modified: 2017-10-30T23:26:26Z
source: RIPE

RIPE Database Software Version 1.97.2

Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Terms of Service

The RIPE NCC uses cookies. Some of these cookies may have been set already. More information about our cookies can be found in our [privacy policy](#). You can accept our cookies either by [clicking here](#) or by continuing to use the site.

Webupdates — RIPE Network Coordination Centre - Mozilla Firefox

Prodamenskiy gosudarstvennyy... Reseller Windows Hosting... DNG Lookup - Check DNG Ri... Webupdates — RIPE Network... Webupdates — RIPE Network... +

https://apps.db.ripe.net/db-web-ui/lookup/lookup.html?ip=217.18.38723.26

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website

Search IP Address or ASN

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

You are here: Home > Manage IPs and ASNs > RIPE Database > Webupdates

Resources >

RIPE Database >

Query the RIPE Database

Full Text Search

Synupdates

Create an Object

Lookup results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

person: Vitaliy Gerl
address: Belarus
address: 220088 Minsk
address: 59, Zaharova str.
address: UNIBEL
phone: +375 17 2100250
fax-no: +375 17 2100899
e-mail: grr@unibel.by
nic-hdl: UBWZ
remarks: -----
mnt-by: ripe@unibel.by
mnt-by: ASS498-MNT
created: 2010-10-12T15:04:03Z
last-modified: 2017-10-30T23:26:21Z
source: RIPE

Login to update

RIPE Database Software Version 1.97.2

f t in

Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Terms of Service

The RIPE NCC uses cookies. Some of these cookies may have been set already. More information about our cookies can be found in our [privacy policy](#). You can accept our cookies either by [clicking here](#) or by continuing to use the site.

09:54:48

Webupdates — RIPE Network Coordination Centre - Mozilla Firefox

Prodamenskiy gosudarstvennyy... Reseller Windows Hosting... DNG Lookup - Check DNG Ri... Webupdates — RIPE Network... Webupdates — RIPE Network... +

https://apps.db.ripe.net/db-web-ui/lookup/lookup.html?ip=217.18.38723.26

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website

Search IP Address or ASN

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

You are here: Home > Manage IPs and ASNs > RIPE Database > Webupdates

Resources >

RIPE Database >

Query the RIPE Database

Full Text Search

Synupdates

Create an Object

Lookup results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

person: Vitalii Zhdanovich
address: Belarus
address: 220088 Minsk
address: 59, Zaharova str.
address: UNIBEL
phone: +375 17 2100250
fax-no: +375 17 2100899
e-mail: zhdanovich@unibel.by
nic-hdl: UBWZ
remarks: -----
mnt-by: ripe@unibel.by
mnt-by: ASS498-MNT
created: 2010-09-02T14:46:47Z
last-modified: 2017-10-30T22:09:34Z
source: RIPE

Login to update

RIPE Database Software Version 1.97.2

f t in

Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Terms of Service

The RIPE NCC uses cookies. Some of these cookies may have been set already. More information about our cookies can be found in our [privacy policy](#). You can accept our cookies either by [clicking here](#) or by continuing to use the site.

09:55:16

Webupdates — RIPE Network Coordination Centre - Mozilla Firefox

Prodamenskiy gosudarstvennyy... Whois.groby... DNG Lookup - Check DNG Ri... Webupdates — RIPE Network... Webupdates — RIPE Network... Webupdates — RIPE Network... +

https://apps.db.ripe.net/db-web-ui/lookup/lookup.html?ip=217.18.38723.26

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

RIPE Database (Whois) Website

Search IP Address or ASN

Manage IPs and ASNs > Analyse > Participate > Get Support > Publications > About Us >

You are here: Home > Manage IPs and ASNs > RIPE Database > Webupdates

Resources >

RIPE Database >

Query the RIPE Database

Full Text Search

Synupdates

Create an Object

Lookup results

This is the RIPE Database search service. The objects are in RPSL format. The RIPE Database is subject to Terms and Conditions.

role: Beltelecom Grodno Admins
admin-c: AB3939-RIPE
tech-c: SMI2727-RIPE
address: Grodno Branch
address: 29, K. Marks str.
address: Republic of Belarus
e-mail: abuse@grodno.by
abuse-mailbox: abuse@grodno.by
nic-hdl: BYG-RIPE
mnt-by: ASS687-MNT
created: 2018-10-08T12:02:43Z
last-modified: 2020-02-25T07:14:00Z
source: RIPE

Login to update

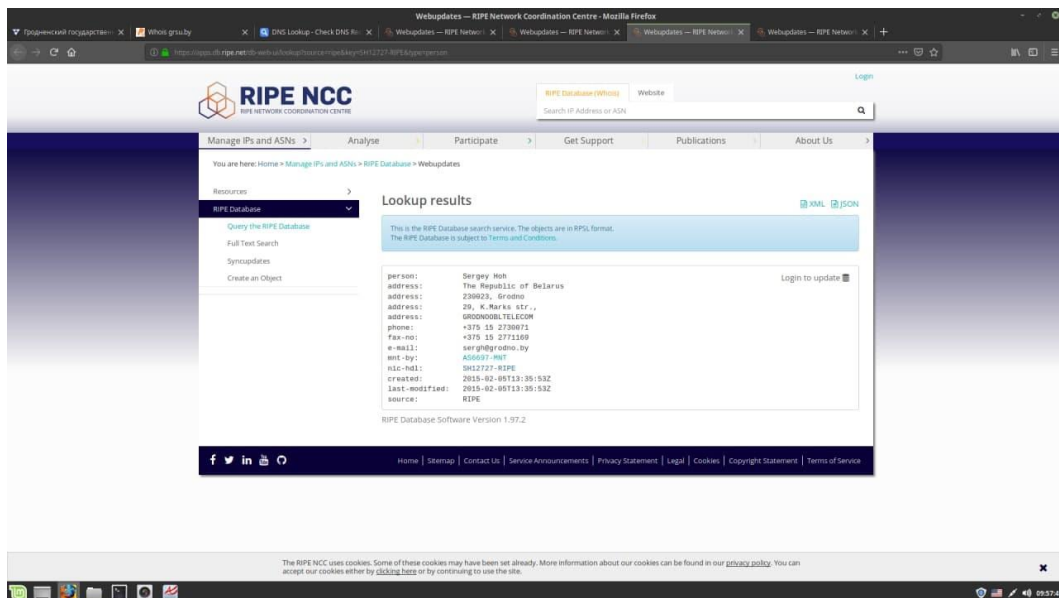
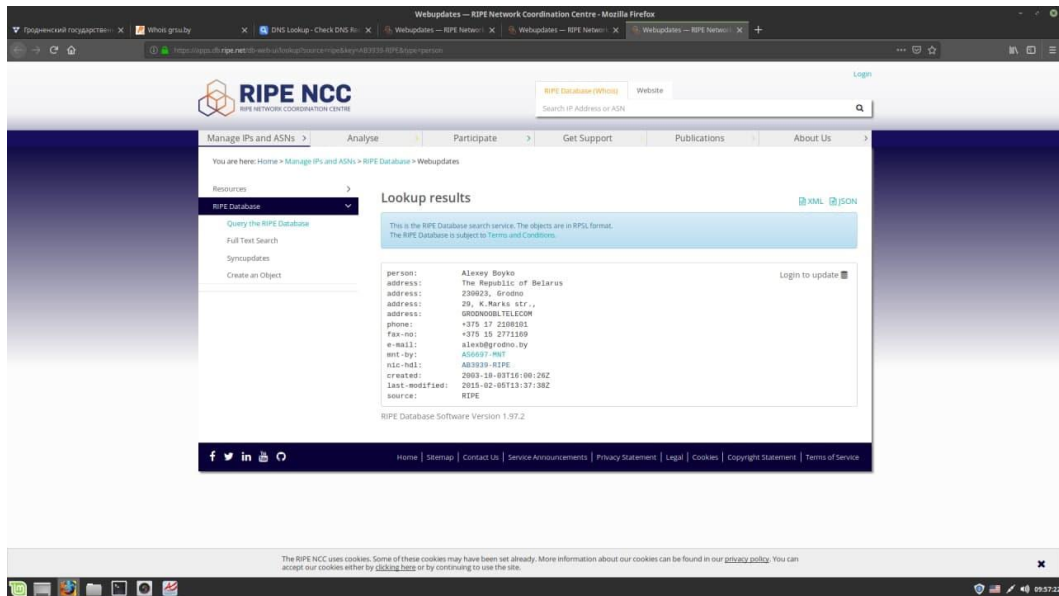
RIPE Database Software Version 1.97.2

f t in

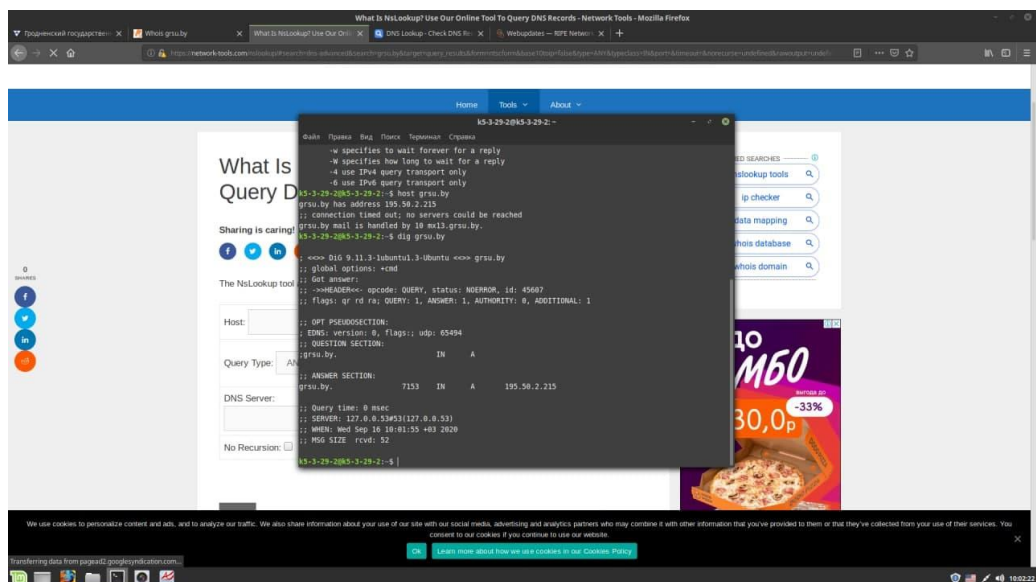
Home | Sitemap | Contact Us | Service Announcements | Privacy Statement | Legal | Cookies | Copyright Statement | Terms of Service

The RIPE NCC uses cookies. Some of these cookies may have been set already. More information about our cookies can be found in our [privacy policy](#). You can accept our cookies either by [clicking here](#) or by continuing to use the site.

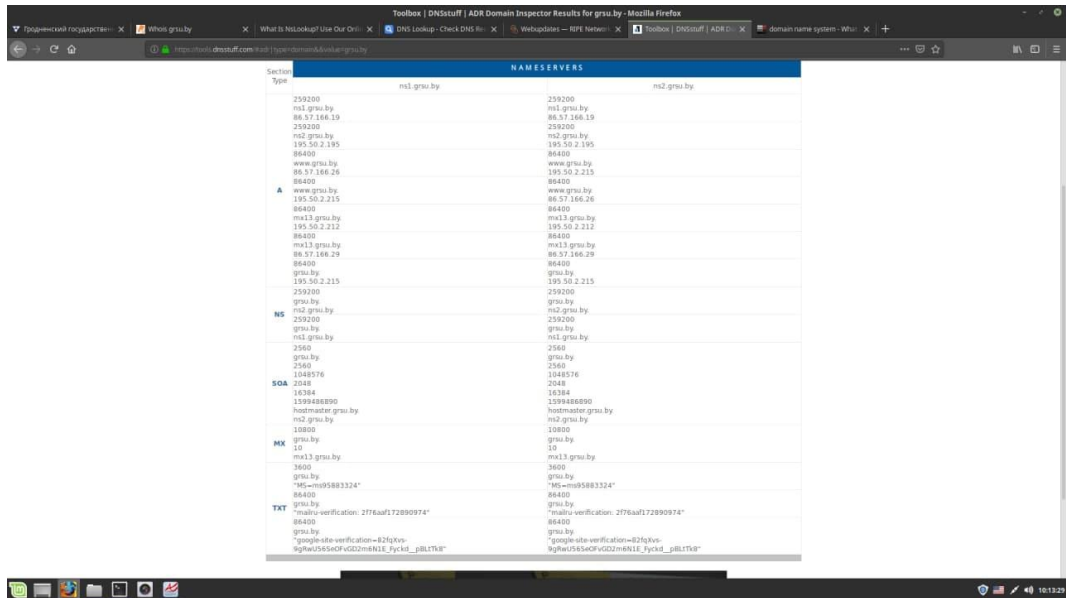
09:57:04



Шаг 3. Выполнить предыдущие проверки, используя средства host и dig.



Шаг 4. Определить DNS-имена и роли узлов из выделенных диапазонов IP-адресов. Использовать веб-средства <http://dnsstuff.com> и <http://dnsreport.com>.

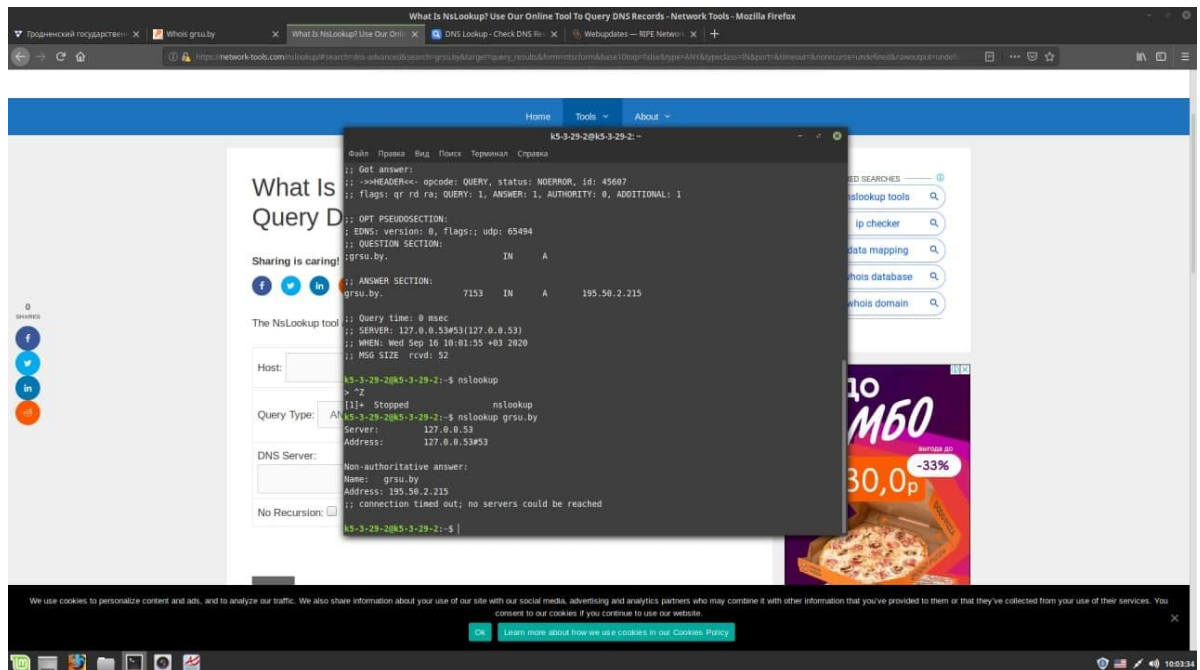


Section	Type	Value
NAMESERVERS	ns1.grsu.by	195.50.2.195
	ns2.grsu.by	195.50.2.195
A	grsu.by	195.50.2.195
	www.grsu.by	195.50.2.195
NS	ns1.grsu.by	195.50.2.195
	ns2.grsu.by	195.50.2.195
SOA	grsu.by	195.50.2.195
	www.grsu.by	195.50.2.195
MX	grsu.by	195.50.2.195
	www.grsu.by	195.50.2.195
TXT	grsu.by	195.50.2.195
	www.grsu.by	195.50.2.195

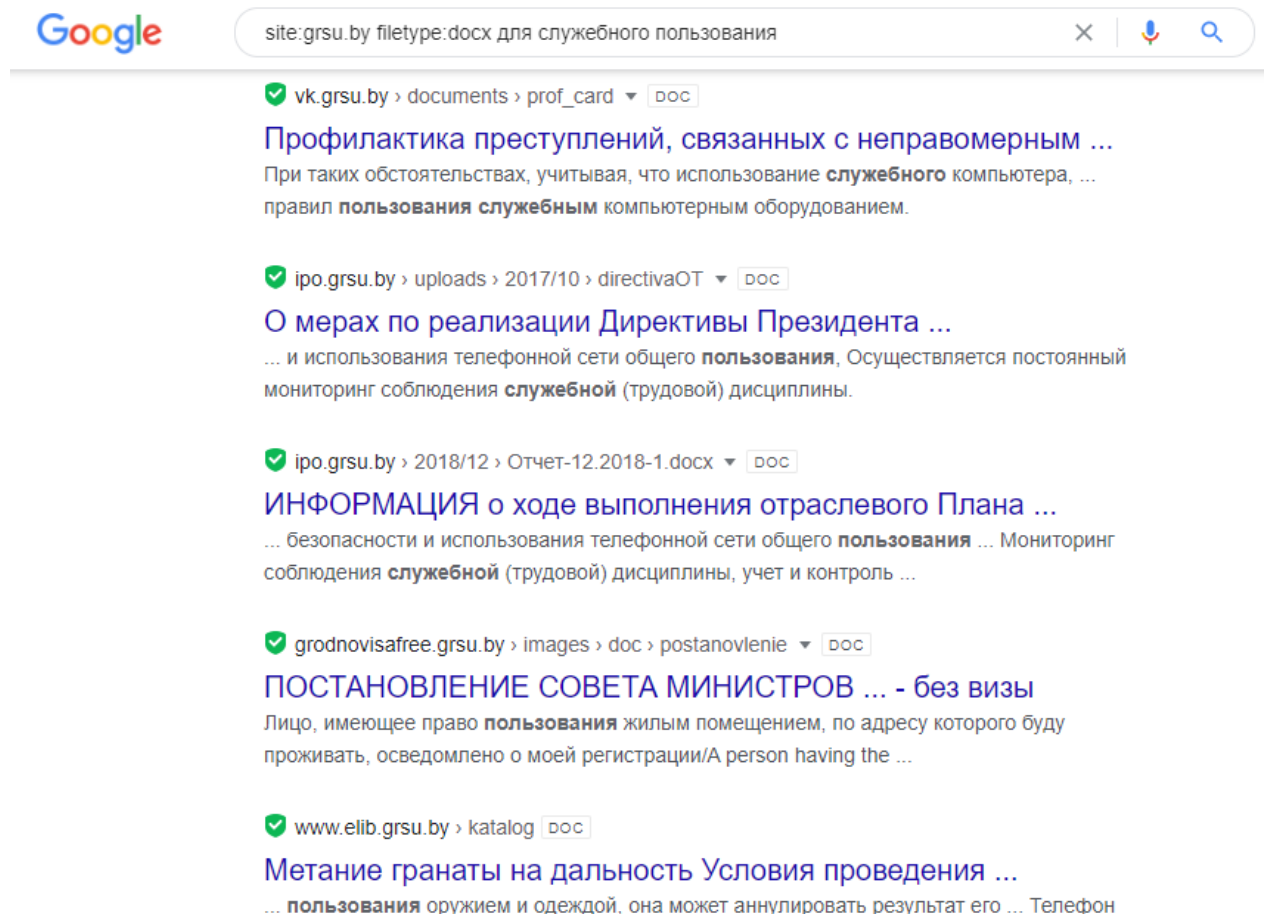
Шаг 5. Проверить наличие узлов найденных сетей в базах данных спам-отправителей и бот-сетях.

grsu.by	
updated:	
DNSBL stands for DNS block list, previously more commonly called RBL as in Realtime Block List	
bogusmx.rfc-clueless.org	127.0.0.8
fulldom.rfc-clueless.org	127.0.0.1
contacts.abuse.net	
ex.dnsbl.org	
in.dnsbl.org	
whois.rfc-clueless.org	
ospamurl.fusionzero.com	
_vouch.dwl.spamhaus.org	
abuse.rfc-clueless.org	
abuse.rfc-ignorant.org	
bl.deadbeef.com	
blacklist.netcore.co.in	
bogusmx.rfc-ignorant.org	
bsb.empty.us	
bsb.spamlookup.net	
db.l.spamhaus.org	
db.l.suomispam.net	
dnsbl.othello.ch	
dnsrbl.swinog.ch	
dob.sibl.support-intelligence.net	
dsn.rfc-clueless.org	
dsn.rfc-ignorant.org	
dyndns.rbl.jp	
elitist.rfc-clueless.org	
fresh.spameatingmonkey.net	
fresh10.spameatingmonkey.net	
fresh15.spameatingmonkey.net	
jwrh.dnsbl.net.au	
mailsl.dnsbl.rjek.com	
multi.surbl.org	
nobl.junkemailfilter.com	
postmaster.rfc-clueless.org	
postmaster.rfc-ignorant.org	
rrdn.dnsbl.net.au	
reputation-domain.rbl.scrolloutf1.com	
reputation-ns.rbl.scrolloutf1.com	
rhsbl.rymsho.ru	
rhsbl.scientificspam.net	
rhsbl.sorbs.net	
rhsbl.zapbl.net	

Шаг 6. Проверить возможность выполнения переноса зоны на первичном и вторичном DNS-серверах:



Шаг 7. Перейти по адресу <http://google.ru>. Задать следующие поисковые запросы и проанализировать результаты.





site:grsu.by filetype:docx секретно



[All](#) [Images](#) [News](#) [Maps](#) [Videos](#) [More](#)

[Settings](#) [Tools](#)

1 result (0.28 seconds)

It looks like there aren't many great matches for your search

Tip: Try using words that might appear on the page you're looking for. For example, "cake recipes" instead of "how to make a cake."

Need help? Take a look at other [tips](#) for searching on Google.

✓ elib.grsu.by > katalog ▾ [doc](#)

УГОЛОВНОЕ ПРЕСЛЕДОВАНИЕ НАЦИСТСКИХ ...

21 ноября 1945 года было принято Постановление Политбюро ЦК ВКП(б) (строго **секретно**) «О проведении судебных процессов над бывшими ...



site:grsu.by filetype:doc ФИО



[All](#) [Images](#) [Maps](#) [News](#) [Videos](#) [More](#)

[Settings](#) [Tools](#)

About 966 results (0.42 seconds)

✓ www.grsu.by > images > Documents > Praktika > Obrazec ▾ [doc](#)

Ф 06-002 - Гродненский государственный университет ...

(название факультета) (ФИО декана). 4. Контроль за исполнением приказа возложить на декана факультета экономики и управления Фатеева В.С.

✓ www.grsu.by > images > Documents ▾ [doc](#)

министерство образования республики беларусь

Проректор, отвечающий за идеологическую работу (ФИО, точное название должности, дата назначения на данную должность, ученая степень, ученое ...

✓ www.grsu.by > images > Documents > Praktika [doc](#)

Ф 30 - Гродненский государственный университет имени ...

(название факультета и фамилия, имя, отчество декана). действующего на основании доверенности и _____. .. (наименование юридического лица).



site:grsu.by filetype:doc для служебного использования



[All](#) [Images](#) [News](#) [Videos](#) [Maps](#) [More](#)

[Settings](#) [Tools](#)

About 53 results (0.37 seconds)

It looks like there aren't many great matches for your search

Tip: Try using words that might appear on the page you're looking for. For example, "cake recipes" instead of "how to make a cake."

Need help? Take a look at other [tips](#) for searching on Google.

✓ www.grsu.by > images > Documents > odnookno ▾ [doc](#)

Об основах административных процедур

о месте нахождения, номере **служебного** телефона, фамилии, ... без **использования** средств идентификации, указанных в абзацах третьем и ...

✓ www.xtt.grsu.by > download > TDP10 > Korruptcij ▾ [doc](#)

Коррупция и её общественная опасность

... заключающуюся в **использовании** должностными лицами доверенных им прав и ... **использования** возможностей занимаемого **служебного** положения.

Шаг 8. Используя веб-инструмент traceroute, расположенный на вебресурсе <http://network-tools.com>, определить маршруты прохождения IP-дейтаграмм до исследуемой сети.

<input type="text" value="grsu.by"/>	<input type="text" value="64"/>	<input type="button" value="Go »"/>
--------------------------------------	---------------------------------	-------------------------------------

Related Tools: [Looking Glass](#) [Ping](#) [Ping-IPv6](#) [Traceroute-IPv6](#) [DNS Traversal](#)

Hop number: 1 Connected to: assc-ultrafw-vlan2598.dc10.neustar.com (10.176.98.1) Roundtrip times: 1,748 ms 3,266 ms 1,492 ms
Hop number: 2 Connected to: ashlfns02-vlan102.dc10.neustar.com (10.176.2.3) Roundtrip times: 3,08 ms 1,7 ms 3,3 ms
Hop number: 3 Roundtrip times: Timed out.
Hop number: 4 Connected to: et-0-0-43-3.cr2-was1.ip4.gtt.net (173.205.39.229) Roundtrip times: 13,926 ms 13,884 ms 13,886 ms Country: germany
Hop number: 5 Connected to: ae12.cr1-was1.ip4.gtt.net (213.200.120.54) Roundtrip times: 3,125 ms 8,734 ms 4,121 ms Country: united states
Hop number: 6 Connected to: as3356.cr1-was1.ip4.gtt.net (199.229.230.98) Roundtrip times: 2,884 ms 2,976 ms 1,873 ms Country: united states
Hop number: 7 Connected to: ae-2-3602.edge3.Berlin1.Level3.net (4.69.159.5) Roundtrip times: 98,424 ms 98,923 ms 98,762 ms Country: united states
Hop number: 8 Connected to: 212.162.10.82 (212.162.10.82) Roundtrip times: 104,171 ms 103,391 ms 103,411 ms Country: germany
Hop number: 9 Connected to: z-poznan-gw3.basnet.rtr.pionier.gov.pl (212.191.224.14) Roundtrip times: 121,86 ms 121,44 ms 121,811 ms Country: poland
Hop number: 10 Connected to: r1u-s16.basnet.by (80.94.160.110) Roundtrip times: 124,221 ms 138,546 ms 138,603 ms Country: belarus
Hop number: 11 Connected to: r1c-zah-te3-1-813.basnet.by (80.94.160.109) Roundtrip times: 120,909 ms 119,893 ms 119,767 ms Country: belarus
Hop number: 12 Connected to: r1c-ac1-te4-2.basnet.by (80.94.160.84) Roundtrip times: 124,819 ms 122,762 ms 122,699 ms Country: belarus

Hop number: 13 Connected to: <code>icc-3560.unibel.by</code> (195.50.3.249) Roundtrip times: 122,504 ms 121,127 ms 120,172 ms Country: <code>belarus</code>
Hop number: 14 Connected to: <code>195.50.3.2</code> (195.50.3.2) Roundtrip times: 122,686 ms 120,163 ms 120,97 ms Country: <code>belarus</code>
Hop number: 15 Connected to: <code>195.50.3.201</code> (195.50.3.201) Roundtrip times: 127,361 ms 127,298 ms 126,162 ms Country: <code>belarus</code>