

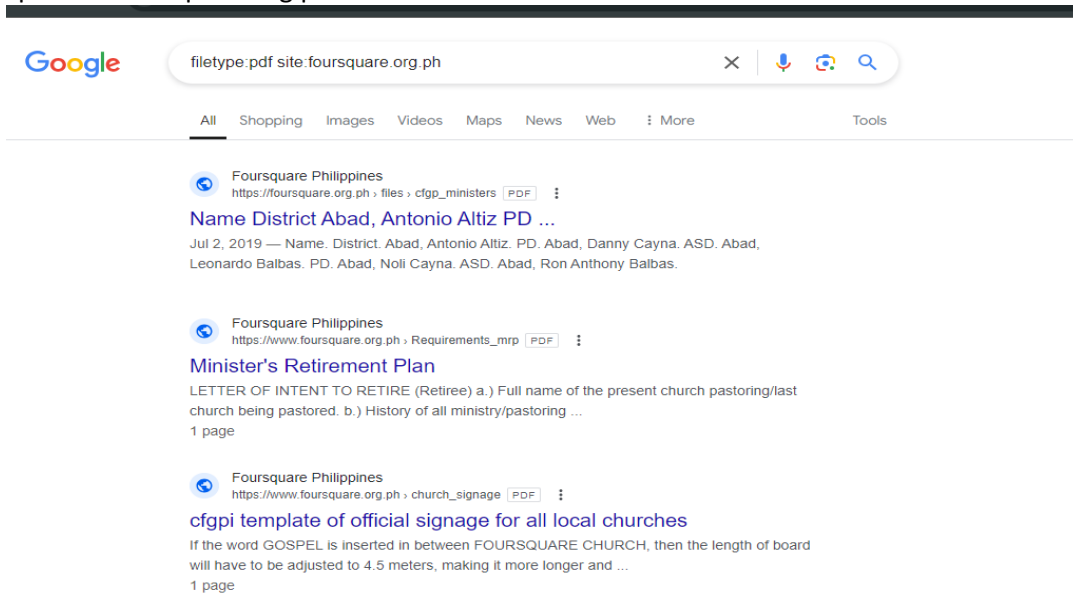
ICT 139 – Information, Assurance and Security 2

Laboratory Practice Exercises: Google Dork

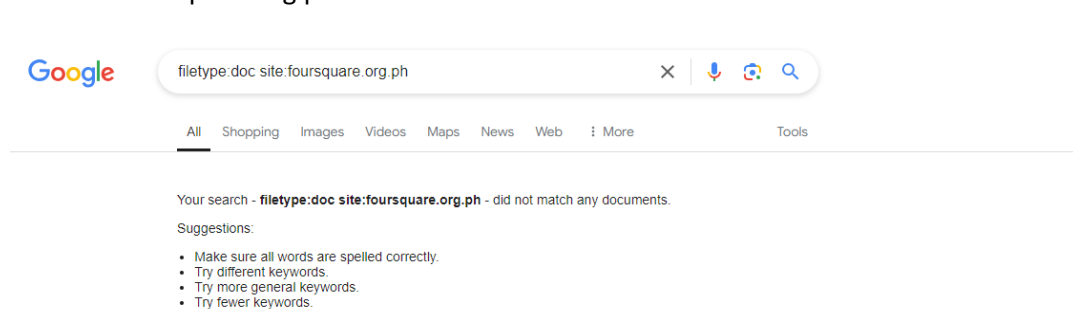
Exercise 1: Finding Exposed Files

- **foursquare.org.ph**

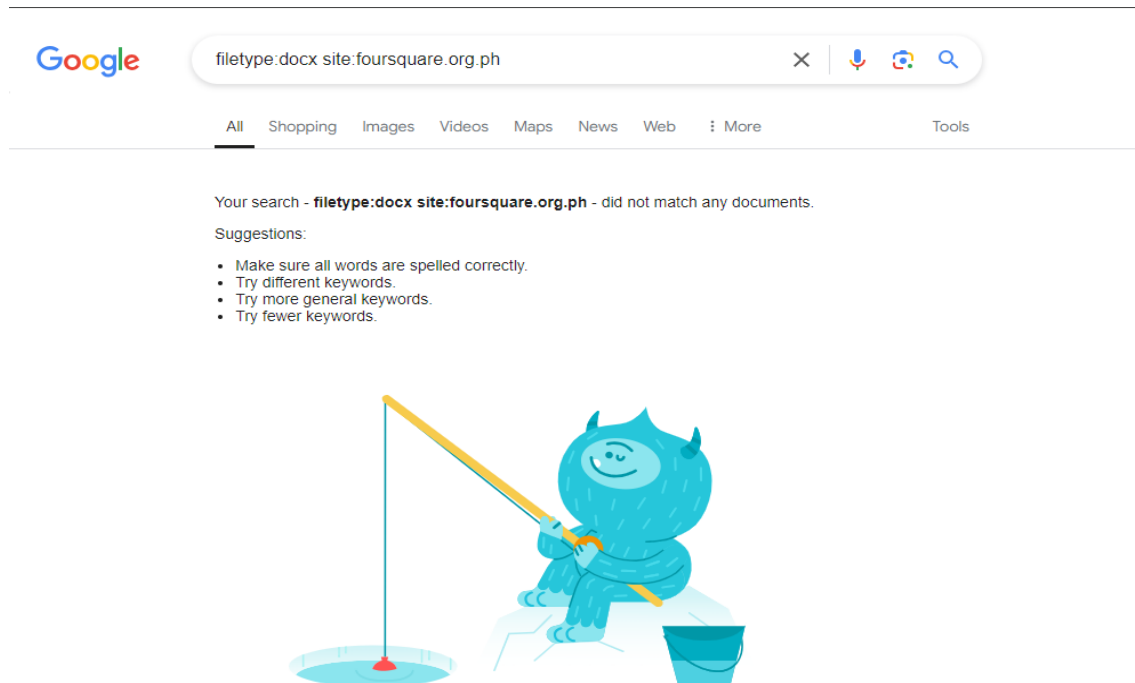
filetype:pdf site:foursquare.org.ph



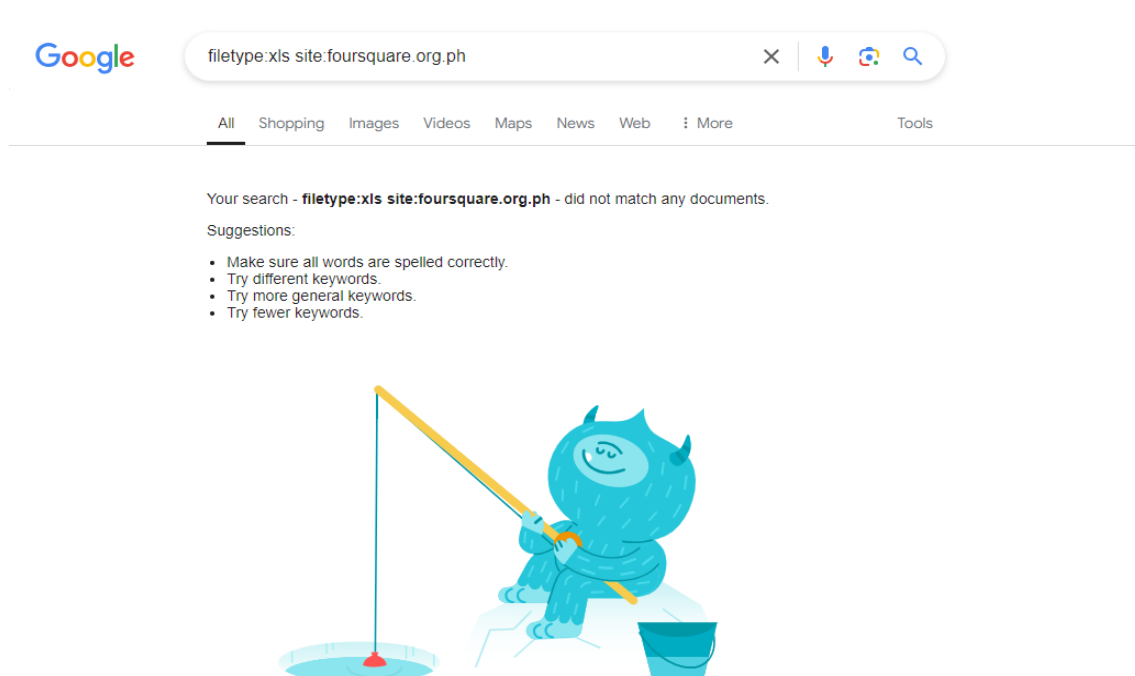
filetype:doc site:foursquare.org.ph



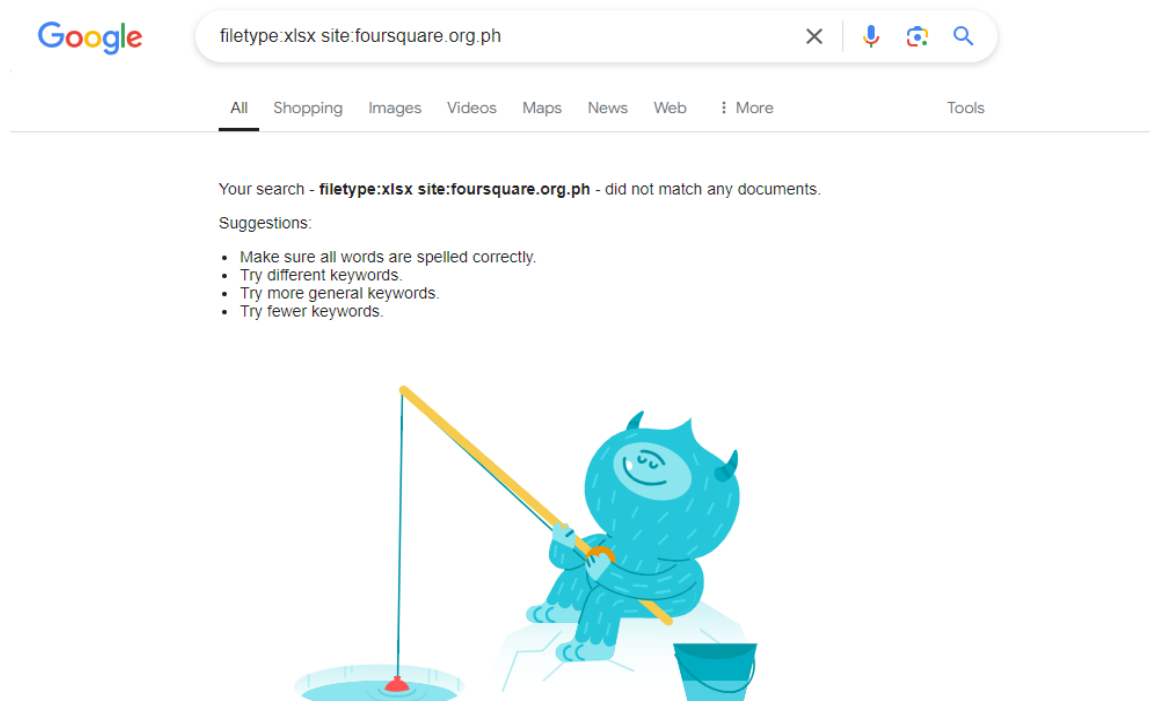
filetype:docx site:foursquare.org.ph



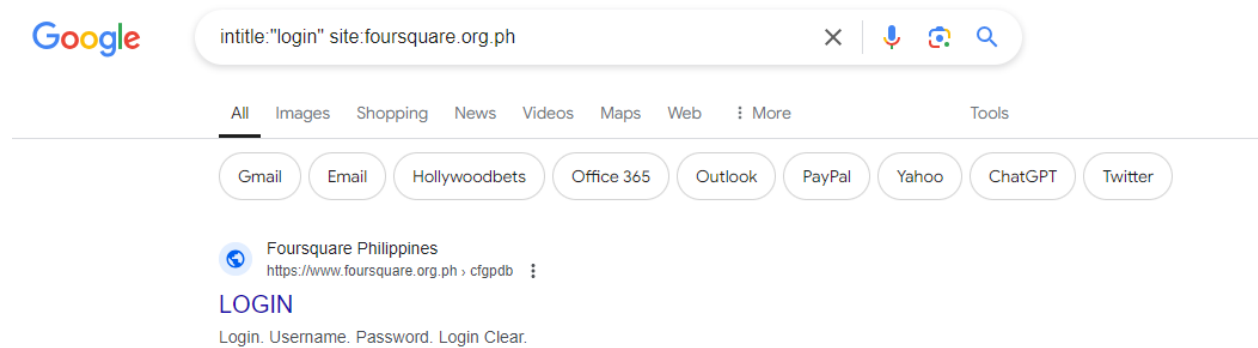
filetype:xls site:foursquare.org.ph



filetype:xlsx site:foursquare.org.ph



intitle:"login" site:foursquare.org.ph



Exercise 2: Discovering Sensitive Information

Google filetype:pdf site:foursquare.org.ph

All Shopping Images Videos Maps News Web More Tools

Foursquare Philippines
https://foursquare.org.ph › files › cfgp_ministers PDF

Name District Abad, Antonio Altiz PD ...
Jul 2, 2019 — Name. District. Abad, Antonio Altiz. PD. Abad, Danny Cayna. ASD. Abad, Leonardo Balbas. PD. Abad, Noli Cayna. ASD. Abad, Ron Anthony Balbas.

Foursquare Philippines
https://www.foursquare.org.ph › Requirements_mrp PDF

Minister's Retirement Plan
LETTER OF INTENT TO RETIRE (Retiree a.) Full name of the present church pastoring/last church being pastored. b.) History of all ministry/pastoring ...
1 page

Foursquare Philippines
https://www.foursquare.org.ph › church_signage PDF

cfgpi template of official signage for all local churches
If the word GOSPEL is inserted in between FOURSQUARE CHURCH, then the length of board will have to be adjusted to 4.5 meters, making it more longer and ...
1 page

https://foursquare.org.ph/files/ministers/cfgp_ministers.pdf

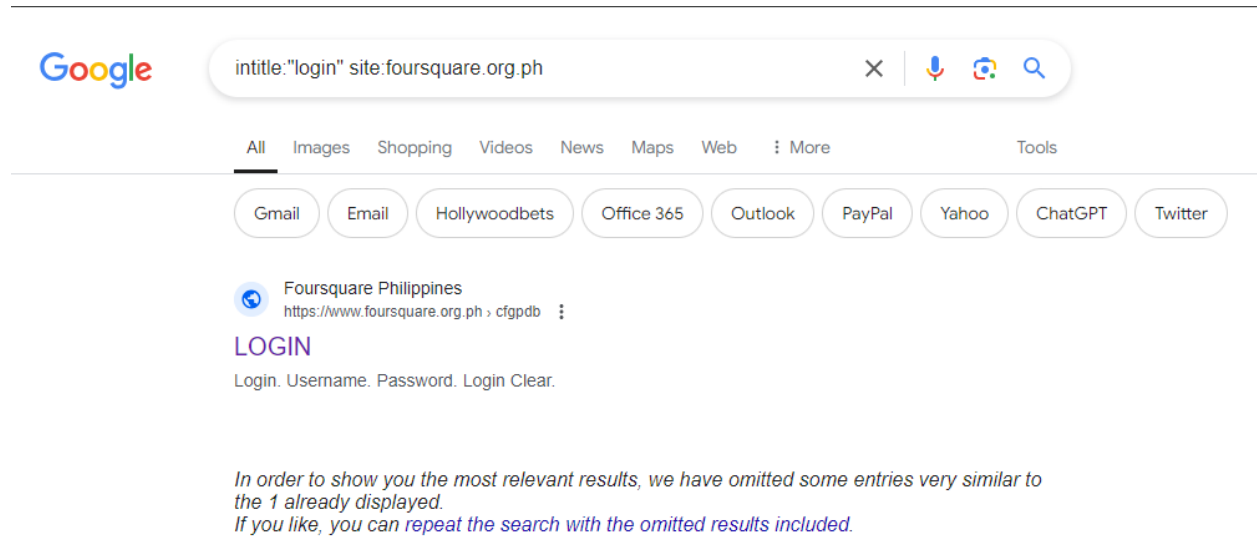
foursquare.org.ph/files/ministers/cfgp_ministers.pdf

cfgp_ministers.pdf 1 / 71 100%

7/2/2019 https://www.foursquare.org.ph/cfgpdb/summary.php?col=min_fullname&tbl=tbl_minister&status=min_status&statusVal=%27Active%27&dt...

Name	District
Abad, Antonio Altiz	PD
Abad, Danny Cayna	ASD
Abad, Leonardo Balbas	PD
Abad, Noli Cayna	ASD
Abad, Ron Anthony Balbas	PD
Abagon, Jireh Mae Testimio	CLD
Abagon, Samel Mora	CLD
Abaigar, Jimmy Munar	NWLD
Aban, Letecia Sinadjan	NMD
Abanilla, Margarita Pazon	EVD
Abante, Domingo Alcaraz	SLD
Abel, Chester Lee Digay	CD
Abella, Anita Misana	MMND
Abiera, Samuel	NEMD
Abines, Grace Botigan	NMD
Abines, Rolando Mendoza	NMD
Abing, Ferdinand Suerte	CMD
Abobo, Zenaida Batalla	CLD
Aboloc, Esther Orque	ZBSD
Aboloc, Roland Alazar Belmes	ZBSD
Aboloc, Rosalina Belmes	ZBSD

Exercise 3: Identifying Vulnerable Systems



A screenshot of a Google search results page. The search bar contains the query "intitle:login site:foursquare.org.ph". Below the search bar, there are tabs for "All", "Images", "Shopping", "Videos", "News", "Maps", "Web", and "More". Below these tabs, there are buttons for "Gmail", "Email", "Hollywoodbets", "Office 365", "Outlook", "PayPal", "Yahoo", "ChatGPT", and "Twitter". The search results show a single result for "Foursquare Philippines" with the URL "https://www.foursquare.org.ph/cfgpdb". Below the result, there is a "LOGIN" link and a text input field for "Login. Username. Password. Login Clear.".

Google

intitle:"login" site:foursquare.org.ph

All Images Shopping Videos News Maps Web More Tools

Gmail Email Hollywoodbets Office 365 Outlook PayPal Yahoo ChatGPT Twitter

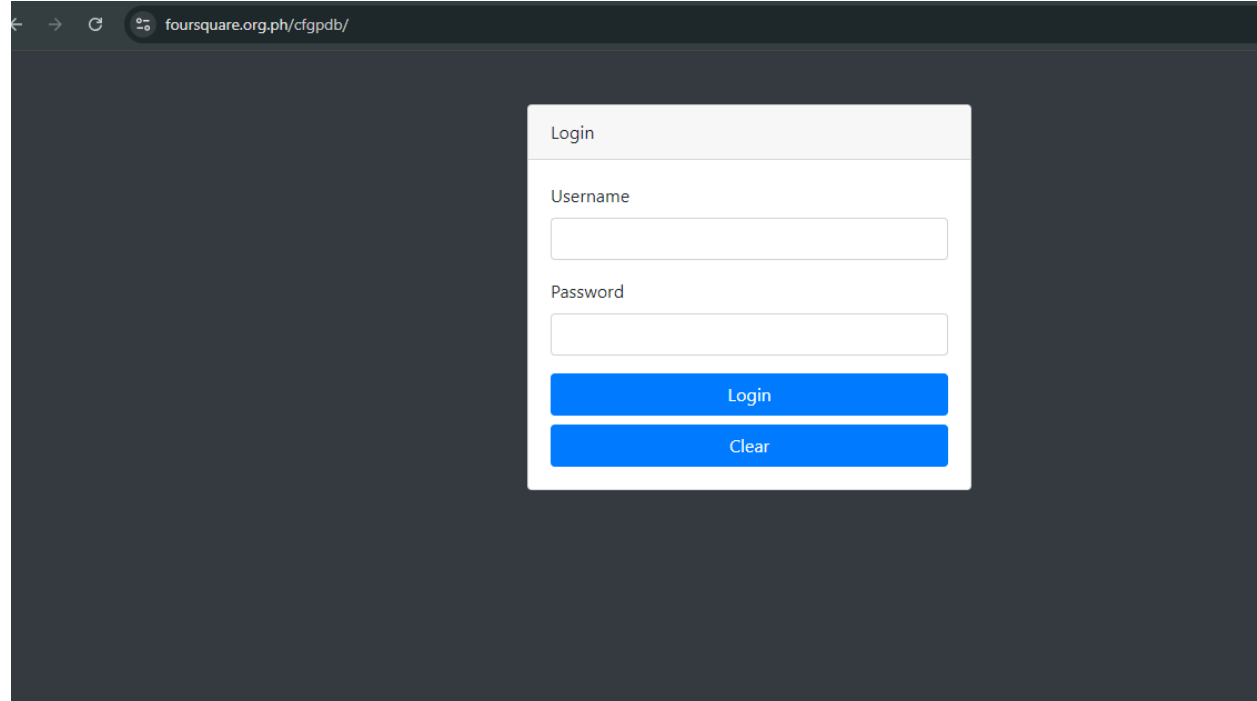
Foursquare Philippines
https://www.foursquare.org.ph/cfgpdb

LOGIN

Login. Username. Password. Login Clear.

*In order to show you the most relevant results, we have omitted some entries very similar to the 1 already displayed.
If you like, you can [repeat the search with the omitted results included](#).*

https://www.foursquare.org.ph/cfgpdb/



A screenshot of a web browser showing the login page for "foursquare.org.ph/cfgpdb/". The page has a dark background. In the center, there is a white login form with a title "Login". Below the title, there are two input fields: "Username" and "Password". Below the "Password" field, there are two blue buttons: "Login" and "Clear".

foursquare.org.ph/cfgpdb/

Login

Username

Password

Login

Clear

Exercise 4: Gathering Intelligence on Organizations


Google

"staff" site:foursquare.org.ph

All Images Shopping Videos News Maps Web More Tools

Synonym Members Meaning Portal Music Schedule Emirates Bow Travel

Images :



Foursquare Philippines
Foursquare Philippines

Foursquare Philippines
Foursquare Philippines


Foursquare Philippines
Foursquare Philippines

Feedback

6 more images

Foursquare Philippines

foursquare.org.ph/aboutus_leadership.html



CHURCH OF THE FOURSQUARE GOSPEL IN THE PHILIPPINES, INC.

HOME ABOUT US LOCATOR CORE PROGRAMS DEPARTMENTS MINISTRIES CONTACT US

/ About Us / Philippine Foursquare Leaders

National Leaders

Board of Directors District Supervisors Bible College Directors Service Org. Heads CFGP Staff



What We Are All About

The Foursquare Church in the Philippines meets in church buildings, sanctuaries, living rooms, garage, and everywhere in between. We spread God's love from Aparri to Sulu, introducing the world to Jesus Christ: the Savior, Baptizer, Healer and Soon Coming King.

Click on the links below to learn more about us.

Laboratory Practice Exercise: Whois & Reverse DNS

Exercise 1: Basic Whois Lookup

- **foursquare.org.ph**

.COM @ \$8.98

Register a .COM domain for only **\$8.98!** While stocks last!

BUY NOW

Whois
identity for everyone

Domains Hosting Servers Email Security Whois Deals

Enter Domain or IP

WHOIS

0

Invalid domain name

We are unable to perform a lookup for **foursquare.org.ph**. It appears to be an invalid or unsupported domain.

Sale

.space

~~\$29.88~~ **\$1.88**

BUY NOW

*while stocks last

On Sale!

.biz

Exercise 2: Advanced Whois Queries

intoDNS
before

foursquare.org.ph

Report

Work in progress!
Follow IntoDNS on [Twitter](#)

Category	Status	Test name	Information	send feedback
Parent		Domain NS records	Nameserver records returned by the parent servers are: ns15.domaincontrol.com. [97.74.107.8] (NO GLUE) [TTL=86400] ns16.domaincontrol.com. [173.201.75.8] (NO GLUE) [TTL=86400] ns4.apnic.net was kind enough to give us that information.	send feedback
		TLD Parent Check	WARNING: Looks like the parent servers do not have information for your TLD when asked. This is ok but can be confusing.	
		Your nameservers are listed	Good. The parent server ns4.apnic.net has your nameservers listed. This is a must if you want to be found as anyone that does not know your DNS servers will first ask the parent nameservers.	
		DNS Parent sent Glue	The parent nameserver ns4.apnic.net is not sending out GLUE for every nameservers listed, meaning he is sending out your nameservers host names without sending the A records of those nameservers. It's ok but you have to know that this will require an extra A lookup that can delay a little the connections to your site. This happens a lot if you have nameservers on different TLD (domain.com for example with nameserver ns.domain.org.)	
		Nameservers A records	Good. Every nameserver listed has A records. This is a must if you want to be found.	
NS		NS records from your nameservers	NS records got from your nameservers listed at the parent NS are: ns15.domaincontrol.com [97.74.107.8] [TTL=3600] ns16.domaincontrol.com [173.201.75.8] [TTL=3600]	

	records	
✓	Reverse MX A records (PTR)	Your reverse (PTR) record: 3.80.204.92.in-addr.arpa -> sxb1plibsmtp01-v02.prod.sxb1.secureserver.net 0.80.204.92.in-addr.arpa -> sxb1plibsmtp01-v01.prod.sxb1.secureserver.net You have reverse (PTR) records for all your IPs, that is a good thing.
i	WWW A Record	Your www.foursquare.org.ph A record is: www.foursquare.org.ph -> foursquare.org.ph -> [107.180.46.243] [Looks like you have CNAME's]
✓	IPs are public	OK. All of your WWW IPs appear to be public IPs.
✓	WWW CNAME	OK. You do have a CNAME record for www.foursquare.org.ph. Your CNAME entry also returns the A record for the CNAME entry, which is good.

Processed in 0.649 seconds.

.COM @ \$8.98
Register a .COM domain for only \$8.98! While stocks last!
BUY NOW


Whois Domains Hosting Servers Email Security Whois Deals
WHOIS



Whois IP 107.180.46.243

Updated 31 seconds ago

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2024, American Registry for Internet Numbers, Ltd.
#
```

```
NetRange: 107.180.0.0 - 107.180.127.255
CIDR: 107.180.0.0/17
NetName: GO-DADDY-COM-LLC
NetHandle: NET-107-180-0-0-1
Parent: NET107 (NET-107-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS26496
Organization: GoDaddy.com, LLC (GODAD)
RegDate: 2014-02-11
```

//shop.whois.com/domain-registration/index.php?tid=shop

Sale
.space
\$29.88 \$1.88
BUY NOW
*while stocks last

On Sale!
.shop
.SHOP @ \$1.88 \$37.88

Exercise 3: Gathering Intelligence on Organizations

```
NetRange:      107.180.0.0 - 107.180.127.255
CIDR:          107.180.0.0/17
NetName:       GO-DADDY-COM-LLC
NetHandle:     NET-107-180-0-0-1
Parent:        NET107 (NET-107-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS26496
Organization:  GoDaddy.com, LLC (GODAD)
RegDate:       2014-02-11
Updated:       2014-02-25
Comment:       Please send abuse complaints to abuse@godaddy.com
Ref:           https://rdap.arin.net/registry/ip/107.180.0.0
```

related domain names

godaddy.com icann.org dnsmadeeasy.com

```
OrgTechHandle: NOC124-ARIN
OrgTechName:   Network Operations Center
OrgTechPhone:  +1-480-505-8809
OrgTechEmail:  noc@godaddy.com
OrgTechRef:    https://rdap.arin.net/registry/entity/NOC124-ARIN

OrgAbuseHandle: ABUSE51-ARIN
OrgAbuseName:   Abuse Department
OrgAbusePhone:  +1-480-624-2505
OrgAbuseEmail:  abuse@godaddy.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE51-ARIN

OrgNOCHandle:  NOC124-ARIN
OrgNOCName:    Network Operations Center
OrgNOCPhone:   +1-480-505-8809
OrgNOCEmail:   noc@godaddy.com
OrgNOCRef:     https://rdap.arin.net/registry/entity/NOC124-ARIN

RNOCHandle:    NOC124-ARIN
RNOCName:      Network Operations Center
RNOCPhone:     +1-480-505-8809
RNOCEmail:     noc@godaddy.com
RNOCRef:       https://rdap.arin.net/registry/entity/NOC124-ARIN
```