

Lab 01 Template – Ethan Roepke

1. WHOIS query Screenshot (15 points)

The screenshot shows a WHOIS query for the domain **figopetinsurance.com**. The interface includes a search bar at the top with the domain name entered. Below the search bar, there are two main sections: **Domain Information** and **Registrant Contact**. The **Domain Information** section lists details such as the domain name, registrar (Network Solutions, LLC), registration and expiration dates, and name servers. The **Registrant Contact** section lists the registrant's name (PERFECT PRIVACY, LLC), address, city, state, postal code, country, phone number, and email address. A red vertical bar is visible on the right side of the screenshot.

Domain Information	
Domain:	figopetinsurance.com
Registrar:	Network Solutions, LLC
Registered On:	2012-11-02
Expires On:	2024-11-02
Updated On:	2023-09-03
Status:	clientTransferProhibited
Name Servers:	ns89.worldnic.com ns90.worldnic.com

Registrant Contact	
Name:	PERFECT PRIVACY, LLC
Street:	5335 Gate Parkway care of Network Solutions PO Box 459
City:	Jacksonville
State:	FL
Postal Code:	32256
Country:	US
Phone:	+1.5707088622
Email:	ha83u2nd6zz@networksolutionsprivateregistration.com

- Domain owner and contact info
 - No given info on Domain information but the registrar is Network Solutions, LLC
 - Perfect Privacy, LLC
 - Phone - +1.5707088622
 - Email - **ha83u2nd6zz**@networksolutionsprivateregistration.com
- Domain administrator and contact info
 - Perfect Privacy, LLC
 - Phone - +1.5707088622
 - Email - **ha83u2nd6zz**@networksolutionsprivateregistration.com
- The IP ranges that the domain has registered to it (include the CIDR)
 - IP - 13.89.172.22
 - IP range – 13.64.0.0 - 13.95.255.255
 - CIDR – 13.64.0.0/11

2. DNS Interrogation screenshot (15 points)

- Mail server

```
[ethanroepke@ethroepke ~ % nslookup
> set type=mx
> figopetinsurance.com
Server:      129.186.140.200
Address:     129.186.140.200#53
```

```
Non-authoritative answer:
figopetinsurance.com      mail exchanger = 0 figopetinsurance-com.mail.protection.outlook.com.
```

The mail server is shown in above image -> figopetinsurance-com.mail.protection.outlook.com
This lets us know that they work through Microsoft

b. DNS server

```
[ethanroepke@ethroepke ~ % nslookup
> set type=ns
> figopetinsurance.com
Server:      129.186.140.200
Address:     129.186.140.200#53

Non-authoritative answer:
figopetinsurance.com      nameserver = ns90.worldnic.com.
figopetinsurance.com      nameserver = ns89.worldnic.com.

Authoritative answers can be found from:
> █
```

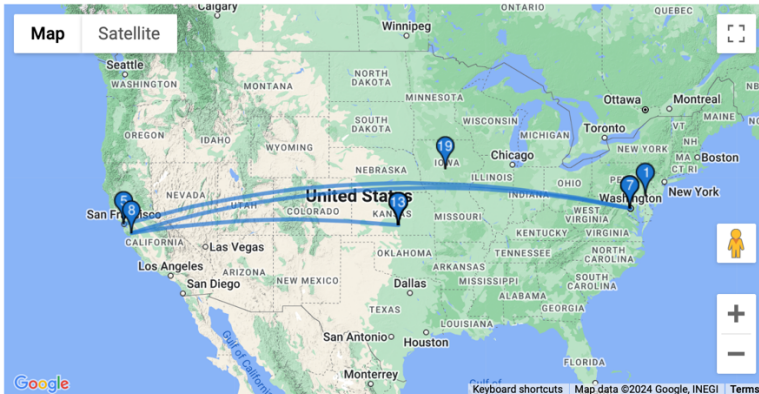
Figopet Insurance uses worldnic for their domain name host

c. Find one other server

```
[> set type=SOA
> figopetinsurance.com
Server:      129.186.140.200
Address:     129.186.140.200#53

Non-authoritative answer:
figopetinsurance.com
    origin = NS89.WORLDDNIC.com
    mail addr = namehost.WORLDDNIC.com
    serial = 123071416
    refresh = 10800
    retry = 3600
    expire = 604800
    minimum = 3600
```

3. Screenshot of traceroutes - include both a visual and textual (10 points)

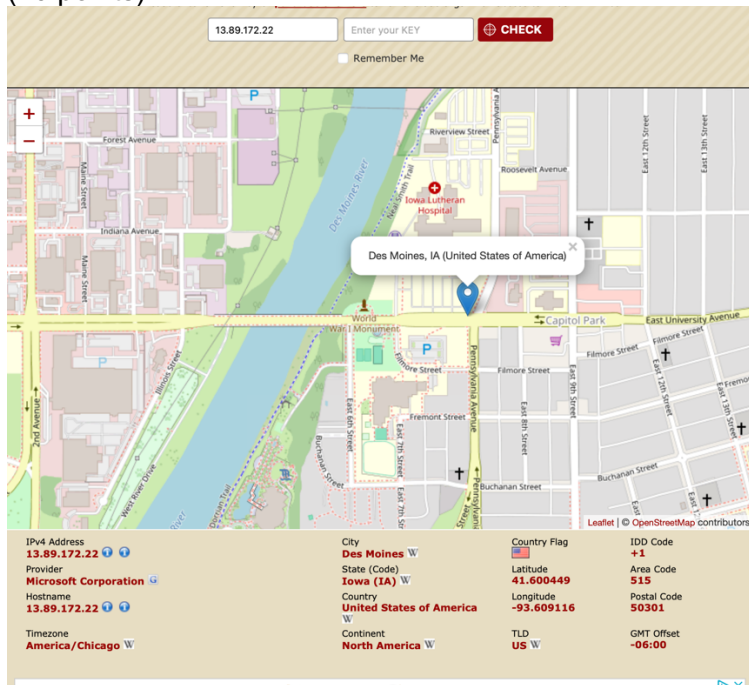


traceroute to figopetinsurance.com (13.89.172.22), 30 hops max

Hop	Host	IP	Time (ms)
1	_gateway	209.151.144.1	0.130ms
2	100.70.166.129	100.70.166.129	0.195ms
3	172.23.255.93	172.23.255.93	0.214ms
4	172.23.255.238	172.23.255.238	0.255ms
5	te0-3-1-3.rcr51.b034314-0.sjc01.atlas.cogentco.com	38.104.135.225	1.496ms
6	be2298.ccr22.sjc01.atlas.cogentco.com	154.54.90.185	0.918ms
7	be3144.ccr41.sjc03.atlas.cogentco.com	154.54.5.102	1.369ms
8	38.142.245.114	38.142.245.114	1.412ms
9	ae32-0.icr01.by21.ntwk.msn.net	104.44.238.244	13.287ms
10	be-120-0.ibr03.by21.ntwk.msn.net	104.44.22.167	48.110ms
11	be-10-0.ibr03.cys04.ntwk.msn.net	104.44.28.148	48.298ms
12	be-4-0.ibr03.dsm05.ntwk.msn.net	104.44.28.248	47.318ms
13	ae214-0.icr08.dsm05.ntwk.msn.net	104.44.32.77	46.049ms
14	*	*	*
15	*	*	*
16	*	*	*
17	*	*	*
18	*	*	*
19	13.89.172.22	13.89.172.22	46.252ms

```
ethanroepke@ethroepke ~ % traceroute figopetinsurance.com
traceroute to figopetinsurance.com (103.224.182.189), 64 hops max, 52 byte packets
 1  routera-10-48-214-0.tele.iastate.edu (10.48.215.252)  44.180 ms  3.589 ms  3.622 ms
 2  b31-mpls-p-hu0-2-0-4--to--b31-mpls-pe-wifi2-1-0-51.tele.iastate.edu (129.186.0.150)  9.086 ms  4.784 ms  3.732 ms
 3  b31-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135)  9.069 ms
   e63-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-3-0-1.tele.iastate.edu (129.186.0.137)  196.482 ms
   b31-mpls-fpe-eth1-10--to--b31-mpls-p-hu0-2-0-1.tele.iastate.edu (129.186.0.135)  4.296 ms
 4  b31fr--e63fpe-vrf-data.tele.iastate.edu (129.186.254.247)  25.722 ms
   e63fr--b31fpe-vrf-data.tele.iastate.edu (129.186.254.245)  25.194 ms
   b31fr--e63fpe-vrf-data.tele.iastate.edu (129.186.254.247)  5.160 ms
 5  b31be-eth2-2.fusion.tele.iastate.edu (192.188.159.233)  10.559 ms
   e63be-eth2-2.fusion.tele.iastate.edu (192.188.159.231)  8.025 ms  3.772 ms
 6  routerb-192-188-159-96.tele.iastate.edu (192.188.159.101)  10.039 ms  3.934 ms  3.833 ms
 7  rtr-e63be-vlan933.tele.iastate.edu (192.188.159.106)  10.859 ms  4.406 ms  4.694 ms
 8  rtr-b31isp1-be158.tele.iastate.edu (192.188.159.159)  13.927 ms  5.003 ms  4.591 ms
 9  bundle-ether100.1421.core2.kans.net.internet2.edu (198.71.47.103)  34.555 ms  12.240 ms  11.556 ms
10  fourhundredge-0-0-0-4079.core1.chic.net.internet2.edu (163.253.2.28)  74.056 ms  21.983 ms  109.355 ms
11  fourhundredge-0-0-0-4079.core1.eqch.net.internet2.edu (163.253.1.207)  48.002 ms  21.090 ms  21.278 ms
12  fourhundredge-0-0-0-48.4079.aggr2.eqch.net.internet2.edu (163.253.1.217)  49.178 ms  19.977 ms  20.631 ms
13  * * *
14  * * ae8.cs4.ord2.us.zip.zayo.com (64.125.25.74)  89.308 ms
15  * * *
16  * * *
17  * * *
18  ae1.mcs2.lax112.us.eth.zayo.com (64.125.28.237)  90.978 ms  76.041 ms  189.299 ms
19  128.177.170.94.ipyx-099220-zyo.zip.zayo.com (128.177.170.94)  85.185 ms  78.036 ms  55.610 ms
20  * sw01-te01-san.trellian.com (103.224.213.212)  236.351 ms  127.578 ms
21  1b-182-189.above.com (103.224.182.189)  65.132 ms  55.578 ms  57.327 ms
```

4. **Geolocation of host(s) screenshot**
(10 points)



- a. What country
 - 1. United States
- b. Which ISP
 - 1. Microsoft Corporation
- c. Who is providing the hosting of the website?
 - 1. worldNic is the hosting of website
- d. Who is providing the target's DNS?
 - 1. Microsoft Azure

5. **Sensitive information on public website - screenshots/description of why useful**
(10 points)

- a. Employee rosters and email addresses



After scrolling through the source code and website for quite some time, I have been unsuccessful in gathering employee roster and contacts. All that I could find in support phone numbers and email. Given that this is mostly a remote job, there personal information is hidden. All that I was able to find was images with some of the workers

and their pets as well as their first name. Using that we could possibly use keywords in google and find personal information about them online.

Unlike some competitors, every member of our US-based customer experience team is P&C licensed, so they are qualified to give expert advice on which policy is right for you and your pet.


And as you may have guessed, we are all obsessed with our pets.

Join the Figo Team


We work hard so pets can play harder.

[View Open Positions](#)


Lizz & Greta



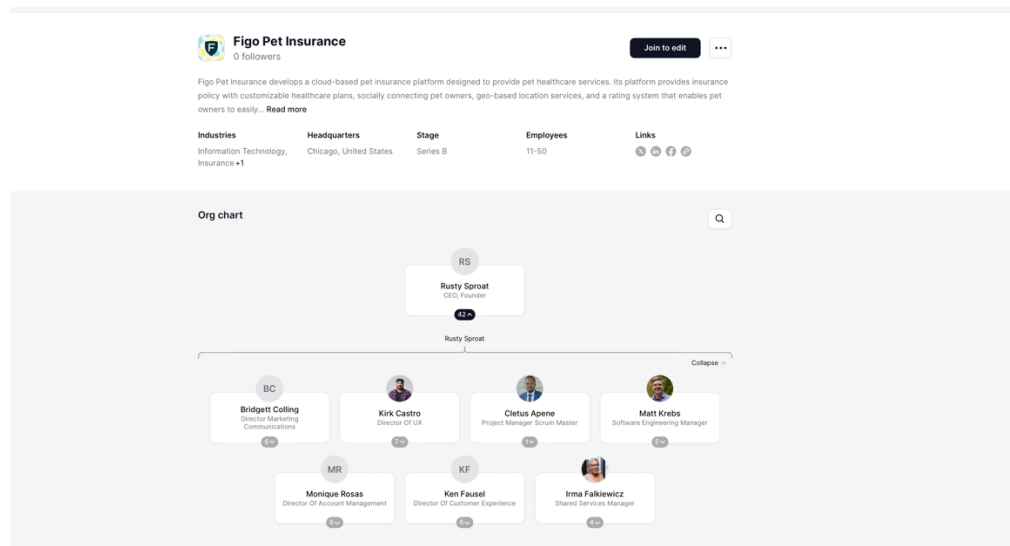
Vanessa & Richard Parker



Javier



After doing this process of looking up a name and working at figo, it brought me to another website called “The org” which gives a branch of employers starting from CEO and all the subdivisions. This is a big progress to now finding contact information next.



b. Technical documents (how to use services/login/etc)

5. you're done!

Phone/Fax Claims Submission

You can also call Claims Support at (888) 223-0596 and they can assist you with your claim.

If you love paper, you can always **download the claims form** and it to us via email at claims@figopetinsurance.com. For those of you who love paper and faxes we have that covered too. You can fax the form to (773) 966-0769.

Documents Required

- List of All Vets Seen
- Medical Records
- Paid Invoice

Medical Records: In order to process your (initial) claim, we need a confirmed list of all vets seen (including emergency and specialty hospitals) either since adoption or within 2 years prior to policy inception. You can email this list to records@ifigo.com.

For an even speedier turnaround, please include the last 2 years of medical records (prior to policy inception) including notes and DOB/adoption date. Your veterinarian can fax the records to (773) 796-4907 or email them to records@ifigo.com. Your veterinarian can also email the records to your Pet Cloud directly using your Personal Pet Cloud Email Address. The email address is located at the top of the page after you log into your account on desktop or mobile. If you are unsure what medical records to **send, click here** for more information.

Claims Reimbursement

After your completed claims form, along with all necessary invoices and medical records are submitted, we will work diligently to expedite your claim. We will process your claim within 30 days of our receipt of all required information, but our goal is 7-10 business days. Note: Some claims can take longer to process if required documentation is not submitted in a timely fashion.

6. Recent happenings in the news - screenshots/description of why useful (10 points)

a. Mergers

The screenshot shows the Costco Wholesale website. At the top, there's a navigation bar with links like Shop, Grocery, Same-Day, Deals, Business Delivery, Optical, Pharmacy, Services, Photo, Travel, Membership, and Locations. Below this, there's a section for "My Warehouse" and "Delivery Location" with a dropdown menu set to "Omaha". The main content area features a banner for "REMEMBER PET INSURANCE" with a photo of a man smiling next to a small dog. To the right of the photo, the text reads "FIGO" and "Costco Members Could Save Through Figo Pet Insurance¹". Below this, a small disclaimer states: "Quality, affordable pet insurance can help pay for unexpected veterinary bills. As a Costco member, you may be eligible to receive an exclusive discount¹ on plans through Figo Pet Insurance."

b. Acquisitions

About FIGO Pet Insurance

On October 19th, 2021, FIGO Pet Insurance was acquired by JAB Holding Company.

 CB Insights
<https://www.cbinsights.com/company/figo-pet-insura...>

FIGO Pet Insurance - CB Insights

c. Where do you believe vulnerabilities may lie?

1. I believe vulnerabilities may lie in between the JAB servers and Figo servers. If JAB has a flaw in their server that an attacker could gain access to, theoretically they would be able to get access to the Figo servers since they need some sort of connections between them.
2. Costco partners with figo pet insurance so members at Costco can get a discount through figo and be able to get pet prescriptions as well at Costco for free. Between these two companies, a vulnerability is if an attacker wants to attack Costco and finds a hole in Figo's server and gains access, then they are able to find a way to get inside Costco's server since they need to have some connection to be able to know Costco memberships and information.

7. **Vulnerable web apps**
(15 points)

a. Can you find any vulnerable web apps using Google Dorks against your target?

1. When using google dork against Figopetinsurance.com, for filetypes, I chose these options because maybe I would be able to find a file with usernames/passwords or possibly files claimed but, I mostly got in return "brochures" and "claim a file".
2. I next did a "intitle:login" that would give specific text in html titles and hoping would give me webs for login pages. All I got in return was a website that had multiple figo web pages directing you to a login page.
3. Next I did a "inurl:admin" hoping to get something in return with "admin" or "login.php" in the URL, however after searching it pops up with nothing.
4. Lastly I tried a "cache" which I am not familiar with so I did not know what I was completely looking for but when I entered it in, it sent me to their website. I do not know if I did something wrong or found nothing important.

b. Provide list of google queries you tried

1. Filetype:pdf
2. Filetype:doc
3. Filetype:xls
4. Filetype:log
5. Intitle:login
6. Inurl:admin
7. Inurl:login.php
8. Cache:figopetinsurance.com/login.php

8. **Similar Domains**
(15 points)

- a. Can you find any domains similar to the target for sale?
 - 1. It looks like they only own figopetinsurance.com, however figopetinsurance.org(.net, and more that could be used) that were available. As well as this being a long domain name, an attacker could change a letter in the domain name (i -> l or a-> o) and most independent people would not recognize the difference and could be looking at a fake website. As well they could change the domain name to "figo-petinsurance.com" and would be very believable that it's the real website.
- b. Are there domains that might benefit an attacker, should they be purchased?
 - 1. There are many domain names available that would benefit attackers, especially in an insurance world if paying a monthly subscription, an attacker could set up the exact website and set up and gain valuable money with not many people realizing a difference between the fake and real domain.
 - 2. I do believe Figo should purchase these domain names so they are protected from attackers making copies of their website with a very familiar domain name. This would help customers to reach the correct website and not a fake website where Figo could be losing money from.