

# MARYMOUNT UNIVERSITY

**Assignment:** IT557; Monitoring, Auditing, and Penetration Testing

**Assigned:** Sep. 23, 2018

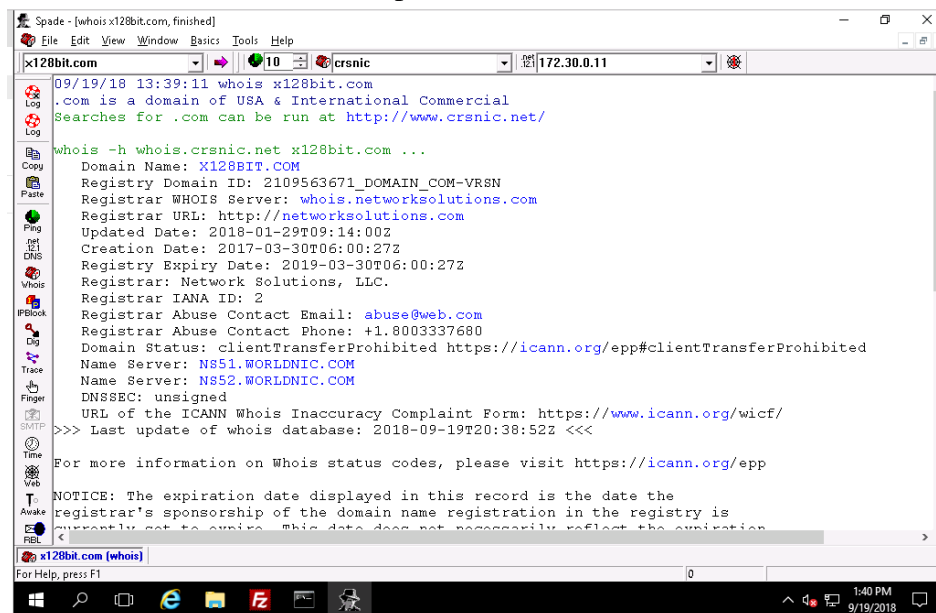
**Instructor:** Professor Ali Bicak

**Student Name:** George Boakye

## LAB REPORT FILE (LAB3)

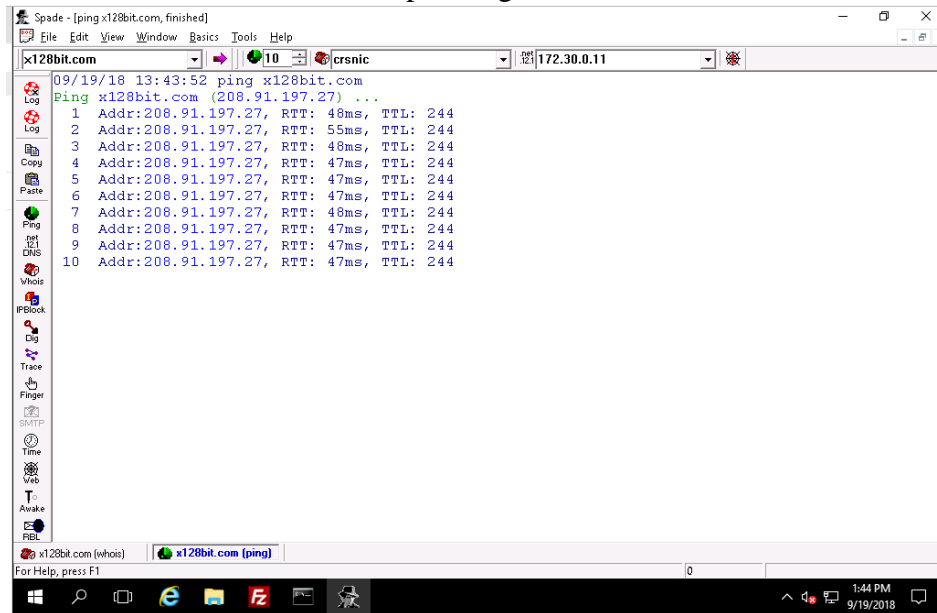
### SECTION 1

Part 1: Step4: Whois x128bit.com

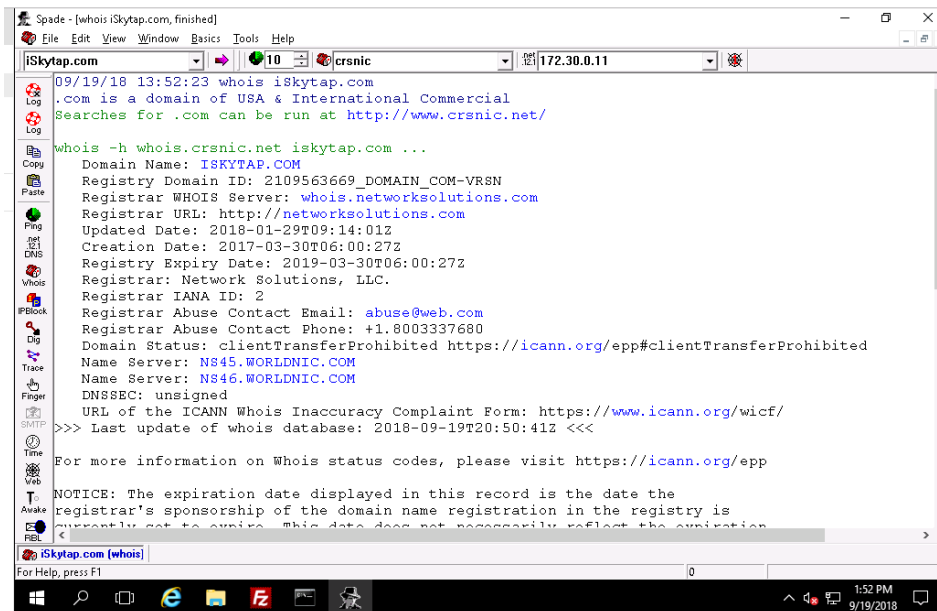


```
Spade - [whois x128bit.com, finished]
File Edit View Window Basics Tools Help
x128bit.com crsnic 172.30.0.11
09/19/18 13:39:11 whois x128bit.com
.com is a domain of USA & International Commercial
Searches for .com can be run at http://www.crsnic.net/
whois -h whois.crsnic.net x128bit.com ...
Domain Name: X128BIT.COM
Registry Domain ID: 2109563671_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.networksolutions.com
Registrar URL: http://networksolutions.com
Updated Date: 2018-01-29T09:14:00Z
Creation Date: 2017-03-30T06:00:27Z
Registry Expiry Date: 2019-03-30T06:00:27Z
Registrar: Network Solutions, LLC.
Registrar IANA ID: 2
Registrar Abuse Contact Email: abuse@web.com
Registrar Abuse Contact Phone: +1.8003337680
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: NS51.WORLDDNIC.COM
Name Server: NS52.WORLDDNIC.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-09-19T20:38:52Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
```

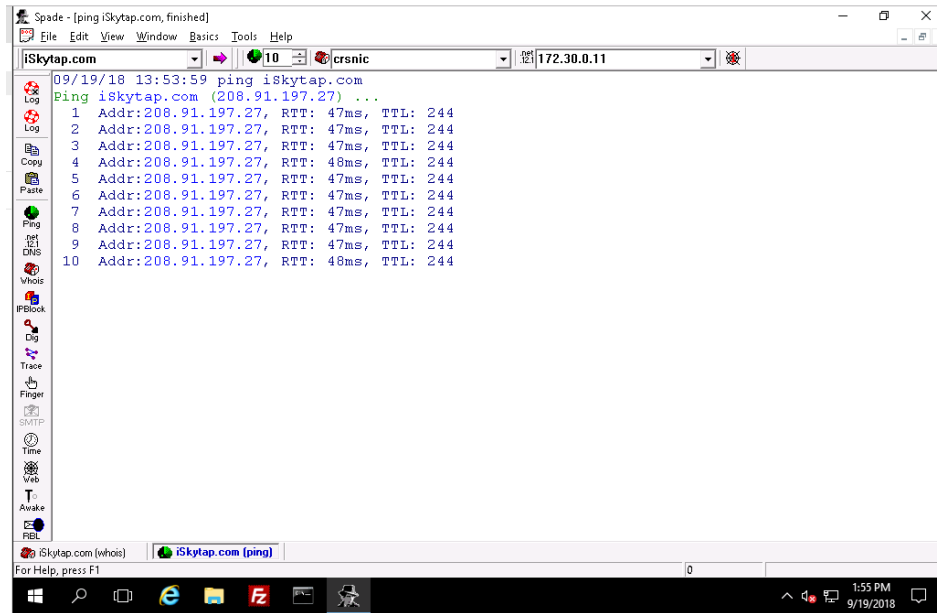
## Part 1: Step8: Ping x128bit.com



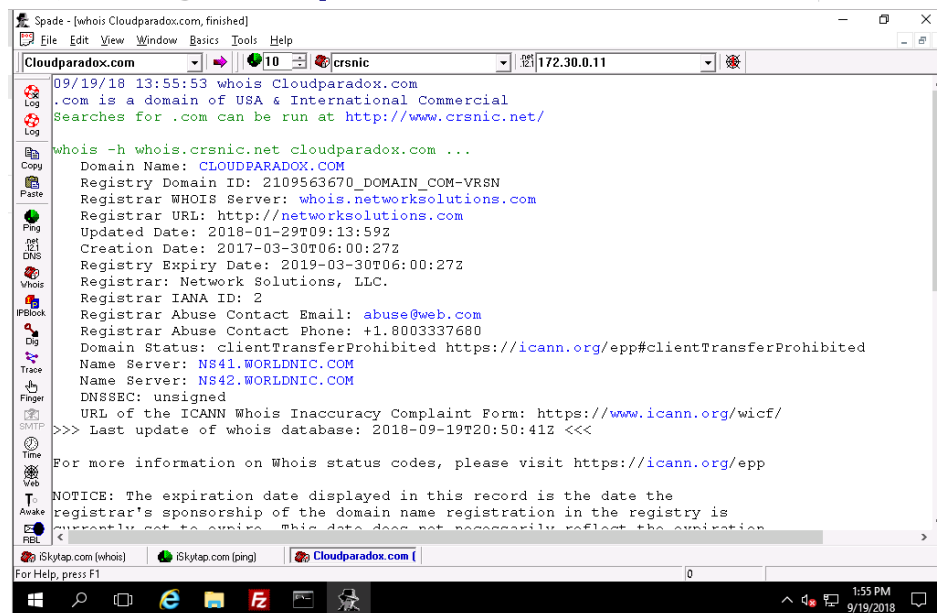
## Part 1: Step13: Whois iSkytap.com



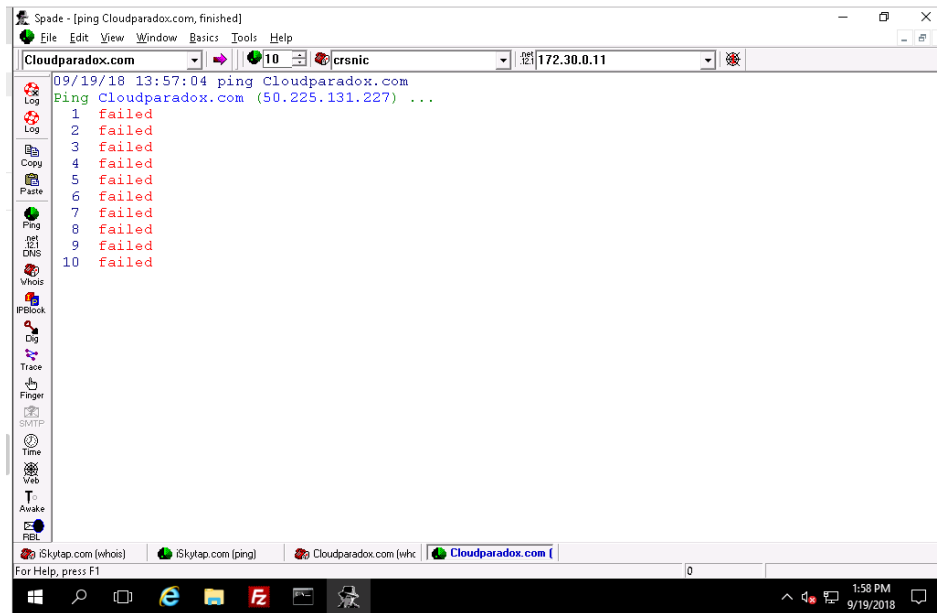
## Part 1: Step13: Ping iSkytap.com



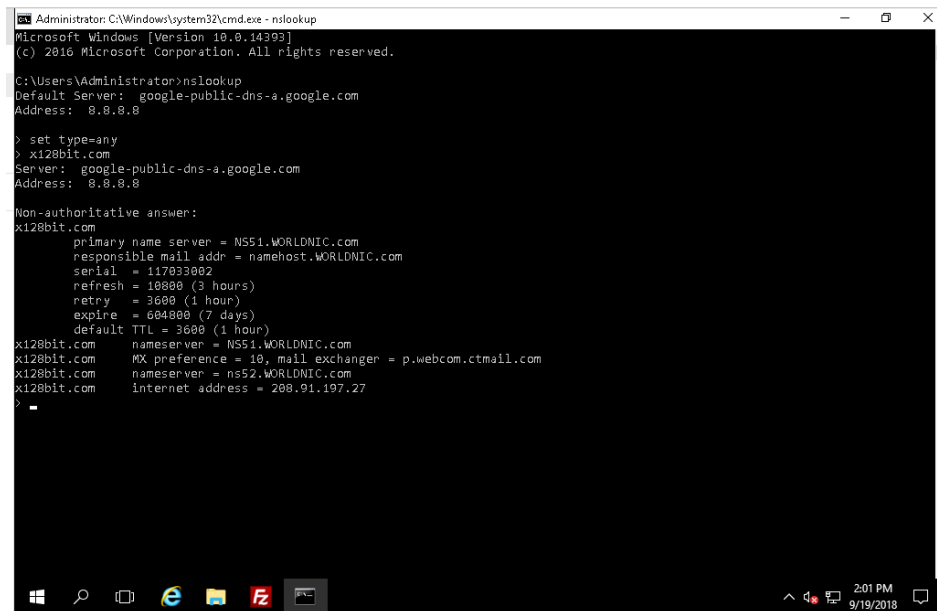
## Part 1: Step13: Whois Cloudparadox.com



## Part 1: Step13: Ping cloudparadox.com



## Part 1: Step20: Nslookup result for x128bit.com



## Part 1: Step21: Nslookup result for iSkytap.com

```
Administrator: C:\Windows\system32\cmd.exe - nslookup
C:\Users\Administrator>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> set type=any
> iskytap.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
iskytap.com
      primary name server = NS45.WORLDNIC.com
      responsible mail addr = namehost.WORLDNIC.com
      serial = 117033002
      refresh = 10000 (3 hours)
      retry = 3600 (1 hour)
      expire = 604800 (7 days)
      default TTL = 3600 (1 hour)
iskytap.com      nameserver = NS45.WORLDNIC.com
iskytap.com      internet address = 208.01.197.27
iskytap.com      nameserver = ns46.WORLDNIC.com
iskytap.com      MX preference = 10, mail exchanger = p.webcom.ctmail.com
>
```

## Part 1: Step21: Nslookup result for cloudparadox.com

```
Administrator: C:\Windows\system32\cmd.exe - nslookup
C:\Users\Administrator>nslookup
Default Server:  google-public-dns-a.google.com
Address:  8.8.8.8

> set type=any
> Cloudparadox.com
Server:  google-public-dns-a.google.com
Address:  8.8.8.8

Non-authoritative answer:
Cloudparadox.com      nameserver = ns42.worldnic.com
Cloudparadox.com      MX preference = 10, mail exchanger = p.webcom.ctmail.com
Cloudparadox.com
      primary name server = NS41.worldnic.com
      responsible mail addr = namehost.worldnic.com
      serial = 117002200
      refresh = 10000 (3 hours)
      retry = 3600 (1 hour)
      expire = 604800 (7 days)
      default TTL = 3600 (1 hour)
Cloudparadox.com      nameserver = NS41.worldnic.com
Cloudparadox.com      internet address = 50.225.131.227
>
```

## Part 1: Step24: traceroute result for x128bit.com

```
Administrator: C:\Windows\system32\cmd.exe
Non-authoritative answer:
x128bit.com MX preference = 10, mail exchanger = p.webcom.ctmail.com
x128bit.com
    primary name server = NS51.WORLONIC.com
    responsible mail addr = namehost.WORLONIC.com
    serial = 117033002
    refresh = 10000 (3 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 3600 (1 hour)
x128bit.com nameserver = NS51.WORLONIC.com
x128bit.com nameserver = ns52.WORLONIC.com
x128bit.com internet address = 208.91.197.27
> exit

C:\Users\Administrator>tracert x128bit.com

Tracing route to x128bit.com [208.91.197.27]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  192.168.151.254
  2  <1 ms  <1 ms  <1 ms  172.18.249.252
  3  <1 ms  <1 ms  <1 ms  172.18.0.2
  4  2 ms  2 ms  9 ms  76.75.74.129
  5  1 ms  1 ms  2 ms  216.168.115.173
  6  34 ms  1 ms  2 ms  xe2-2-0-1.core1.toronto1.nexicom.net [98.124.49.233]
  7  9 ms  8 ms  9 ms  xe2-0-0.core1.montreal1.nexicom.net [76.75.120.2]
  8  15 ms  15 ms  15 ms  xe2-0-3.core1.newyork1.nexicom.net [76.75.120.6]
  9  15 ms  15 ms  15 ms  tge8-3.fr3.lga.llnwd.net [198.32.118.26]
 10  15 ms  17 ms  15 ms  siteprotect.security.neustar [68.142.82.65]
 11  16 ms  16 ms  15 ms  10.14.221.226
 12  *  *  *  Request timed out.
 13  47 ms  47 ms  47 ms  208.91.197.27

Trace complete.

C:\Users\Administrator>
```

## Part 1: Step25: traceroute result for iSkytap.com

```
Administrator: C:\Windows\system32\cmd.exe
Non-authoritative answer:
iSkytap.com
    primary name server = NS45.WORLONIC.com
    responsible mail addr = namehost.WORLONIC.com
    serial = 117033002
    refresh = 10000 (3 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 3600 (1 hour)
iSkytap.com internet address = 208.91.197.27
iSkytap.com nameserver = NS45.WORLONIC.com
iSkytap.com nameserver = ns46.WORLONIC.com
iSkytap.com MX preference = 10, mail exchanger = p.webcom.ctmail.com
> exit

C:\Users\Administrator>tracert iSkytap.com

Tracing route to iSkytap.com [208.91.197.27]
over a maximum of 30 hops:

  1  <1 ms  <1 ms  <1 ms  192.168.151.254
  2  <1 ms  <1 ms  <1 ms  172.18.249.252
  3  1 ms  <1 ms  <1 ms  172.18.0.2
  4  1 ms  1 ms  2 ms  76.75.74.129
  5  1 ms  1 ms  1 ms  216.168.115.173
  6  2 ms  1 ms  1 ms  xe2-2-0-1.core1.toronto1.nexicom.net [98.124.49.233]
  7  9 ms  7 ms  8 ms  xe2-0-0.core1.montreal1.nexicom.net [76.75.120.2]
  8  15 ms  15 ms  15 ms  xe2-0-3.core1.newyork1.nexicom.net [76.75.120.6]
  9  15 ms  15 ms  23 ms  tge8-3.fr3.lga.llnwd.net [198.32.118.26]
 10  16 ms  16 ms  15 ms  siteprotect.security.neustar [68.142.82.65]
 11  15 ms  15 ms  15 ms  10.14.221.226
 12  *  *  *  Request timed out.
 13  48 ms  48 ms  47 ms  208.91.197.27

Trace complete.

C:\Users\Administrator>
```

## Part 1: Step25: tracer result for cloudparadox.com

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>tracert cloudparadox.com

Tracing route to cloudparadox.com [50.225.131.227]
over a maximum of 30 hops:


  0  <1 ms <1 ms <1 ms 192.168.151.254
  1  <1 ms <1 ms <1 ms 172.18.249.252
  2  <1 ms <1 ms <1 ms 172.18.0.2
  3  2 ms 1 ms 1 ms 76.75.74.120
  4  1 ms 1 ms 1 ms 216.160.115.173
  5  1 ms 1 ms 1 ms xe2-2-0-1.core1.toronto1.nexicom.net [98.124.49.233]
  6  1 ms 1 ms 1 ms xe-2-2-1-101.cr0-tor1.ip4.gtt.net [77.67.71.81]
  7  15 ms 16 ms 15 ms et-0-0-05.cr6-chi1.ip4.gtt.net [89.149.140.205]
  8  15 ms 14 ms 17 ms as7922.chi111.ip4.gtt.net [199.229.229.250]
  9  15 ms 15 ms 15 ms be-10563-cr02.350ecermak.il.ibone.comcast.net [68.86.82.157]
 10  38 ms 39 ms 39 ms be-10521-cr02.1601milehigh.co.ibone.comcast.net [68.86.85.170]
 11  39 ms 39 ms 38 ms be-12021-cr01.champa.co.ibone.comcast.net [68.86.84.225]
 12  63 ms 62 ms 62 ms be-11020-cr02.sunnyvale.ca.ibone.comcast.net [68.86.84.9]
 13  62 ms 62 ms 62 ms be-7922-ar01.santaclara.ca.sfb.comcast.net [68.86.90.94]
 14  64 ms 64 ms 64 ms 162.151.86.58
 15  65 ms 65 ms 65 ms po-1-nur01.pleasanton.ca.sfb.comcast.net [162.151.78.210]
 16  65 ms 65 ms 65 ms be-11-sur03.pleasanton.ca.sfb.comcast.net [162.151.79.166]
 17  * * * Request timed out.
 18  * * * Request timed out.
 19  * * * Request timed out.
 20  * * * Request timed out.
 21  * * * Request timed out.
 22  * * * Request timed out.
 23  * * * Request timed out.
 24  * * * Request timed out.
 25  * * * Request timed out.
 26  * * * Request timed out.
 27  * * * Request timed out.
 28  * * * Request timed out.
 29  * * * Request timed out.
 30  * * * Request timed out.


Trace complete.
```

## Part 2: Step4: Name of Target Organization: eBay

eBay

E-commerce company



 [ebay.com](https://www.ebay.com)

eBay Inc. is an American multinational e-commerce corporation based in San Jose, California that facilitates consumer-to-consumer and business-to-consumer sales through its website. eBay was founded by Pierre Omidyar in 1995, and became a notable success story of the dot-com bubble. [Wikipedia](#)

**Customer service:** 1 (866) 540-3229

**Technical support:** 1 (866) 961-9253

**Stock price:** EBAY (NASDAQ) \$34.22 +0.10 (+0.29%)  
Sep 19, 4:00 PM EDT - Disclaimer


**Founder:** [Pierre Omidyar](#)


**Founded:** September 3, 1995, San Jose, CA


**Subsidiaries:** [mobile.de](#), [StubHub](#), [Tradera](#), [Shutl](#), [Auction Co.](#), [MORE](#)


**Did you know:** eBay is the world's ninth-largest internet company by revenue. [wikipedia.org](#)


Profiles

 Facebook

 Twitter

 YouTube

 Instagram

 LinkedIn

## Part 2: Step4: Domain Name & Extension

[ebay.com](https://www.ebay.com)

## Part 2: Step4: eBay URL & Social Networking Sites

<https://www.ebay.com/>

<https://twitter.com/eBayIncCareers>

<https://www.facebook.com/ebaycareers>

<https://www.instagram.com/lifeatebay/>



<https://www.linkedin.com/company/ebay/>

<https://www.glassdoor.com/Overview/Working-at-eBay-EI-IE7853.11,15.htm>

## Part 2: Step4: Physical Address of eBay Headquarters

eBay Headquarters  
2025 Hamilton Avenue  
San Jose, California 95125  
USA


### *Web view of eBay HQ*


[Our Company](#)[Stories](#)[Impact](#)[Investors](#)[Join Our Team](#)[Press Room](#)[Follow Us](#)[Contact Us](#)

[Overview](#)[Who We Are](#)[Partner to Sellers](#)[Our Leaders](#)[Our History](#)[Our Businesses](#)[Diversity & Inclusion](#)[Responsible Business](#)[Government Relations](#)[Privacy Center](#)[Follow Us](#)[Contact Us](#)

## Contact Us

**eBay Headquarters**  
2025 Hamilton Avenue  
San Jose, California 95125  
USA

[Get Directions](#) 



### Customer Service Contacts

Need help? Contact our Customer Service team.

### Media & Press Contacts

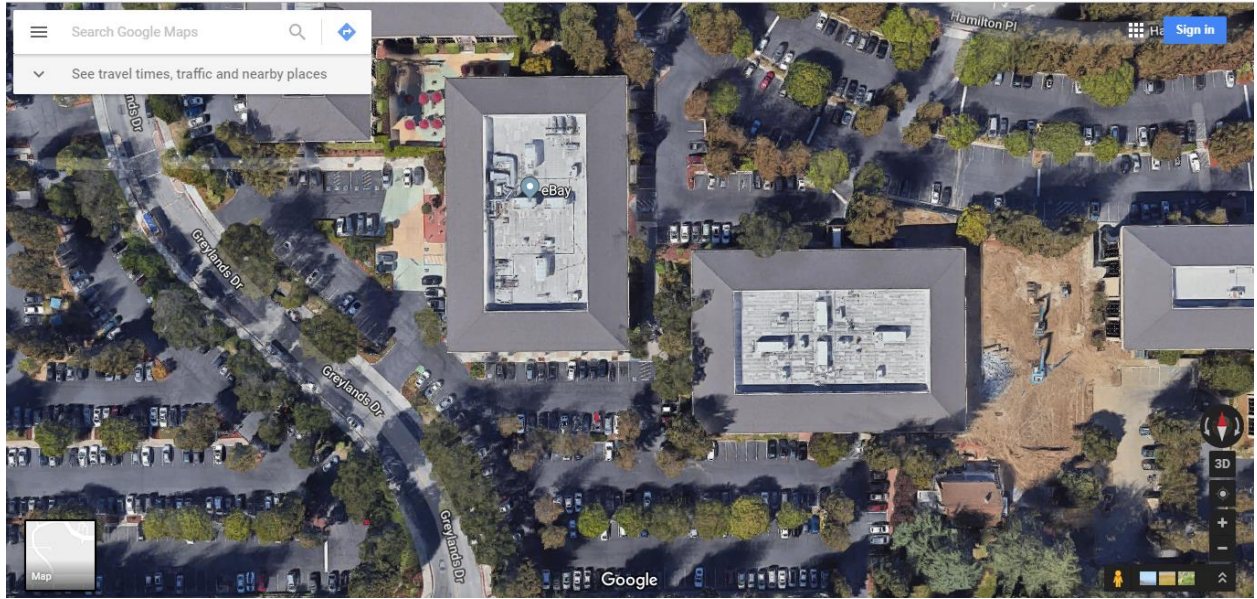
If you're a member of the press with editorial inquiries, please contact our Media and Press Team.

### Careers Contacts

Interested in joining us? Get in touch with our Careers Team.



*Google Map view of eBay HQ*



## Part 2: Step4: Information about Officers

### EXECUTIVE LEADERS



**Devin Wenig**  
President & CEO



**Alessandro Coppo**  
SVP, General Manager, eBay Classifieds Group



**Scott Cutler**  
SVP, Americas



**Steve Fisher**  
SVP, Payments



**Marie Oh Huber**  
SVP Legal Affairs, General Counsel & Secretary



**Wendy Jones**  
SVP, Global Operations



**Jay Lee**  
SVP, EMEA



**Kris Miller**  
SVP, Chief Strategy Officer



**Jooman Park**  
SVP, APAC



**Mohan Patt**  
VP, Core Product Experience



**Mazen Rawashdeh**  
VP, Platform Engineering



**Scott Schenkel**  
SVP, Chief Financial Officer



**Sukhinder Singh Cassidy**  
SVP & President, StubHub



**Dan Tarman**  
SVP, Chief Communications Officer



**Kristin Yetto**  
SVP, Chief People Officer

## Part 2: Step4: Number of employees and each physical location

### Fast Facts

#### eBay Inc. | By The Numbers

Collectively, we connect millions of buyers and sellers around the world

eBay Inc. is a global commerce leader, which includes our Marketplace, StubHub and Classifieds platforms. Collectively, we connect millions of buyers and sellers around the world. The technologies and services that power our platforms are designed to enable sellers worldwide to organize and offer their inventory for sales, and buyers to find and purchase it, virtually anytime and anywhere. eBay Inc. employs approximately 14,100 people globally<sup>1</sup>.

#### FEATURED OFFICES



**Dublin**  
Ireland



**Salt Lake City, UT**  
United States



**San Jose, CA**  
United States

Click the links to learn more about each individual location and their respective unique office cultures.

##### North America

###### United States

Austin, TX [Location Info](#) >  
New York, NY [Location Info](#) >  
Portland, OR [Location Info](#) >  
Salt Lake City, UT [Location Info](#) >  
San Francisco, CA [Location Info](#) >  
San Jose, CA [Location Info](#) >  
Seattle, WA [Location Info](#) >

##### Europe, Middle East & Africa

###### Ireland [Location Info](#)

Dublin

###### Netherlands [Location Info](#)

Amsterdam

###### Turkey [Location Info](#)

Istanbul

###### United Kingdom [Location Info](#)

London

##### Asia Pacific

###### China [Location Info](#)

Hong Kong  
Shanghai  
Shenzhen

###### India [Location Info](#)

Bangalore  
Mumbai

###### Singapore [Location Info](#)

Singapore

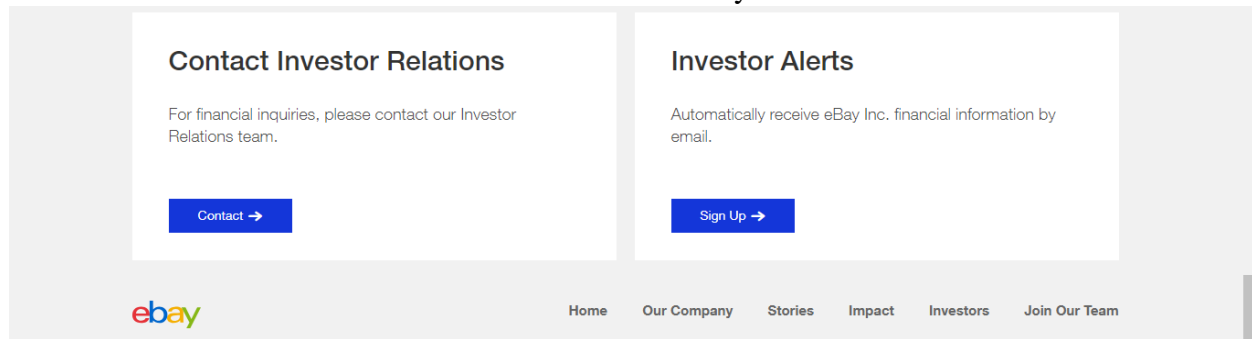
## Part 2: Step4: eBay Investors

Top 4 eBay shareholders. This information is restricted on ebay.com domain

Names	# of Shares
Pierre Omidyar	58.5m as of April 4, 2018
John Donahoe	823,896 as of July 17, 2015
Devin N. Wenig	702,053 as of June 15, 2018
Michael Jacobson	518,559 as of July 15, 2017

Pines (2018)

## Investor search from eBay domain



### Part 2: Step4:

## HACKING RESEARCH REPORT

### A. Executive Summary

Data gathering and footprinting on x128bit.com, iSkytap.com, cloudparadox.com, ebay.com, and issaseries.com domains proved to be legitimate and responded to some queries. Queries such as ping, traceroute, nslookup, Whois, and public domain search (Google) provided some valuable information. Common among the gathered and footprints are the specific locations of the IP addresses, owners of the domains, shareholders and number of shares held, and the regional registrars.

While some of the domains could suffer vishing attack, eBay could be highly prone to whaling attack. The fact that eBay has thrown almost every information about top management out there and is freely available, makes it easy for targeted senior level attack. Iskytap.com does similar by publishing its most sensitive routes and SOA information. It's also worth noting that except cloudparadox.com which denied ping query, almost all the other domains could be subjected to ping flood attack which can lead to a DOS attack

It can also be noted that of all the listed domains, issaseries.com and cloudparadox.com seem to have instituted some form of security measures by way of limiting the amount of information published and the ping domain query respectively.

### B. Methodology

Ping command sent series of packet to the target hosts to verify if they were available for connection. Cloudparadox.com ping returned failed because the host (50.225.131.227) was configured to drop ICMP packets.

Traceroute was used in the footprinting processes of the three fictitious companies to identify the network path which must be followed to get to a system, provided the names and IP addresses of all intermediate systems and helped identify potential attack points. Whois command has offered



very vital information about the companies such as the domain owner, either real or disguised and included contact names; addresses; numbers as well as names of associated servers (e.g. Part1 Step13: Cloudparadox.com which even included how to report abuse). The Nslookup command helped to obtain information about the internet servers (Owners of systems). It found name server information for all domains by querying their respective DNS which revealed that some domains were registered to one primary server name (i.e. worldnic.com).

Google Hacking was used to gather as many information about eBay as possible and yielded enough information to lead an attacker plan and execute attack. Google provided an aerial view of the eBay Headquarters, Social Media Sites, information about Management and they were all confirmed at eBay through the path Google provided.

### **C. Technical Research Results**

The technical research conducted on the company domains provided great leads that when tactically followed, could lead a successful attack. Information such as when domain names were registered, server names and locations, whether there's MX, contacts persons and numbers as well as the paths leading to the destination of these domains were all successfully footprinted except cloudparadox.com that somehow had instituted security measure to block connectivity when pinged. The issaseries.com domain according to Whois was registered in 2010, updated and expiring on 2018 and 2019 respectively. It's an IANA regional registered IP owned by namecheap.com and runs a primary server named dns01.ascendlearning.com.

### **D. Public Domain Results**

eBay has put out a lot of information in the public domain. Information such as names of management, global locations, addresses to specific and strategic buildings, financial gains over the years, subsidiaries and even the history of the company. A hacker, learning these valuable information might be able to launch a successful phishing/social engineering attack at eBay. For instance, a malicious intent insider attacker (e.g. a terminated employee from say Europe) can successfully engineer his way into the U.S.A HQ and cause massive havoc.

### **E. Findings and Conclusions**

Techniques employed in determining the routes and prints of the companies as stated earlier provided great leads that can lead to a successful attack. Reasons backing a successful attack are that, it can be concluded and verified that all domains are registered and run on the internet.

Ping, Whois, and Traceroute on x128bit.com provided registrar name and identification (Network Solutions, LLC) which is IANA registered, dates (creation, updated, and expiration), and contacts; 10 responses to ping command; and running a mail exchanger server (i.e. p.webcom.ctmail.com) It must be emphasized that iSkytap.com and x128bit share common characteristics in terms of IP address (208.91.197.27), same creation, updated and expiration dates, same contact numbers, same MX, and registrars but different registrar IDs. Again, Nslookup sections values including serial, refresh, retry, expire, and default are just exact.

Cloudparadox.com also share similar properties as shown in the Whois capture but certain unique Nslookup output and ping page showing different IP address (50.225.131.227) on a different subnet.

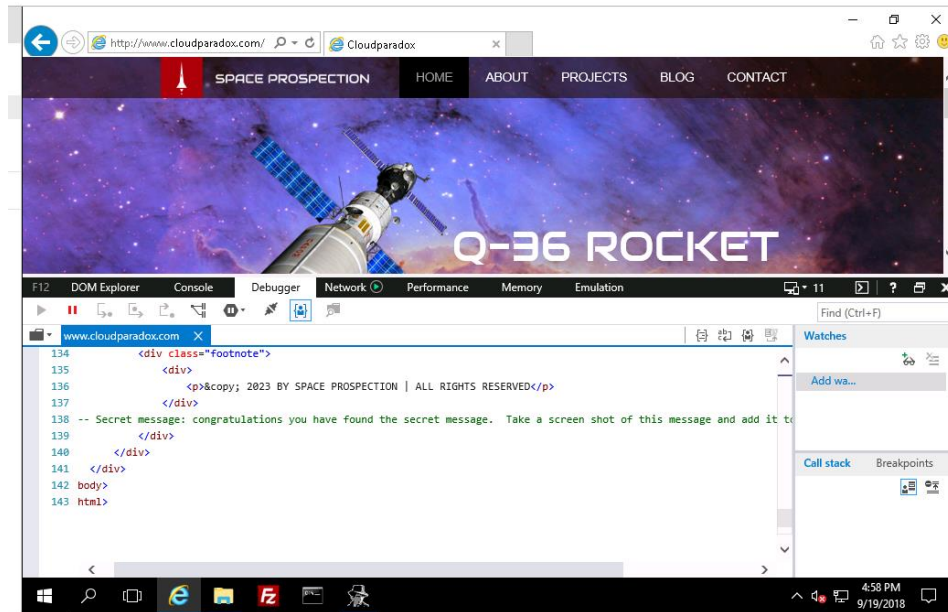
Traceroute to issaseries.com showed from the route as going through Toronto in Canada and routing through Cincinnati on Level3 network. This is then connected and associated with informedpublishing.com with IP address 198.187.138.94 (Registered to issaseries.com) in Massachusetts

#### **F. Avenue for Further Research**

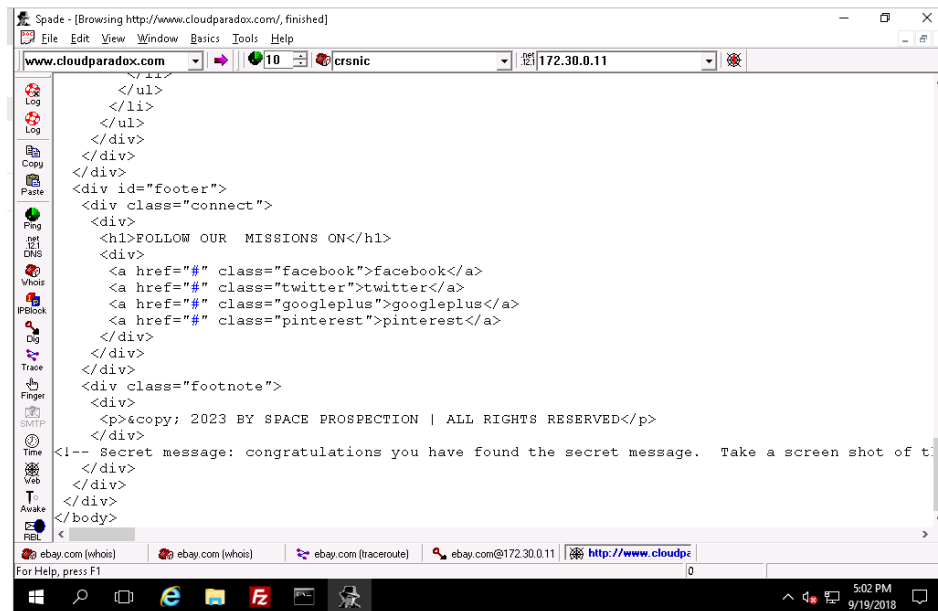
Additional information that may be needed to plan a successful attack can include mapping the IP addresses to a physical geographic location. These could be achieved by doing a public domain research to know what exact businesses do the companies undertake, how large in order to strategize the attack and also to know their security measures in place. Cloudparadox.com is a typical example of the need to know security measures since a ping command failed as well as issaseries.com. This should indicate to an attacker that there are some measures in place to protect the domains, thus its separate subnet and limited public domain information.

## SECTION 2

Part 1: Step25: Secret message in [www.cloudparadox.com](http://www.cloudparadox.com) source code from explorer



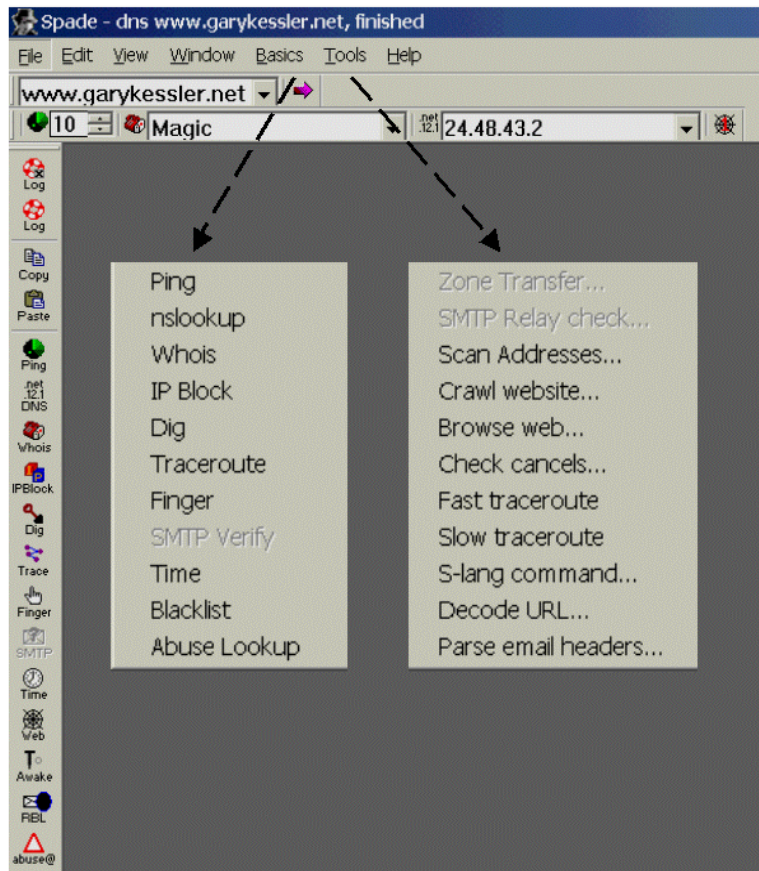
Part 1: Step28: Secret message in [www.cloudparadox.com](http://www.cloudparadox.com) source code from Sam Spade



## SECTION 3

### Part 1

#### Basics and Tools menus in Sam Spade



*Adopted from (Kessler, 2001)*

#### **Tools for Address, Domain and Host Information (Kessler, 2001)**

**Ping:** Sends packets to host to determine if it's reachable via the network and provides TTL.

**Traceroute:** Traces the route that packets take from the user's system to the specified target host address, listing all intermediate routers and showing a graph of the hop-by-hop delay times.

**DIG (Domain Internet Groper):** Looks up DNS information.

**Whois:** Provides ownership and contact information for the specified host's domain.

**Nslookup & Decode URL:** display the IP address and name of a specified host.

**IP Block:** Indicates the owner of the IP address block to which the specified host belongs.

**Zone Transfer:** Used to request that a DNS server send all of the information that it has about a given domain.

**Finger:** obtains host/user information from a system running the finger daemon (TCP port 79).

**SMTP Verify:** Used to send a Simple Mail Transfer Protocol (SMTP) VRFY command to a suspect mail server to confirm the validity of an e-mail address, such as that of the sender of a spam message.

**Time:** Sets the user's host system time from a network time server.



**Blacklist:** Checks to see if the specified host name/address is listed with the Mail Abuse Prevention System (MAPS) Realtime Blackhole List (RBL), Dial-up Users List (DUL) or Relay Spam Stopper (RSS).

**SMTP Relay Check:** Determines if a specified e-mail server will allow SMTP relaying.

**Abuse Lookup:** Finds the e-mail address to where notifications of possible spam coming from the specified domain should be sent.

**Check Cancels:** Searches for USENET canceled messages.

**Fast & Slow traceroute:** Differ only in the number of attempts made to learn the route.

**Scan Addresses:** A minimal port-scanning utility that allows a user to scan a specified set of IP address to detect open ports.

**Browse Web:** A bare-bones Web browser.

**Crawl Web site:** Allows you to specify a URL and download all accessible pages from a Web site.

**S-Lang:** An embedded S-Lang interpreter.

**Parse e-mail headers:** Allows the user to verify a set of headers from an e-mail message.

## Part 2: Step 1

iskytap.com domain has put so much information out for attackers to utilize

**IP-ADDRESS.COM**

HomeMy IPSpeedtestSitemapSearch Website, Domain, Host, or IP address

Proxy CheckerProxy ListVerify Email AddressTrace Email AddressIP to Zip CodeIP Address Distance

### iskytap.com

The domain registration date is March 30, 2017.

#### IP Addresses

IP Address	Autonomous System Number (ASN)	Internet Service Provider (ISP) / Organization	Location
208.91.197.27	AS40034 Confluence Networks Inc	Confluence Networks / Network Solutions, LLC	United States of America

#### Server Locations

208.91.197.27

Location	United States of America (US)
Latitude	37.7510° (37° 45' 3" N)
Longitude	-97.8220° (97° 49' 19" W)

#### IANA IPv4 Address Space Allocation

208.91.197.27

Prefix	208/8
Designation	ARIN
Allocation Date	April 1996
Status	ALLOCATED - delegated entirely to specific RIR (Regional Internet Registry) as indicated.

#### DNS Resource Records

In this section you will find important DNS resource records for *iskytap.com*. SOA records, Name Server records, and MX records are included when available. Additional supporting data includes serial numbers, refresh rates, retry times, TTL, priority, and length to expire will be shown.

Node Name	Class	Type	Data	TTL
iskytap.com	IN	SOA	ns45.worldnic.com. namehost.worldnic.com. ( 117033002 ; serial 10800 ; refresh 3600 ; retry 604800 ; expire 3600 ) ; minttl	7200
iskytap.com	IN	NS	ns45.worldnic.com	7200
iskytap.com	IN	NS	ns46.worldnic.com	7200
iskytap.com	IN	MX	10 p.webcom.ctmail.com	3600
iskytap.com	IN	A	208.91.197.27	7200


x128bit.com domain is dead as shown in the upper right corner




## Part 2: Step 2

Physical IP address locations (x128bit.com, iSkytap.com, and cloudparadox.com)


*Physical Location of x128bit.com*

IP Address	Country	Region	City
208.91.197.27	United States 	Texas	Austin
ISP	Organization	Latitude	Longitude
Network Solutions LLC	Not Available	30.2672	-97.7431

*Physical Location of iSkytap.com*

IP Address	Country	Region	City
208.91.197.27	United States 	Texas	Austin
ISP	Organization	Latitude	Longitude
Network Solutions LLC	Not Available	30.2672	-97.7431

*Physical Location of cloudparadox.com*

IP Address	Country	Region	City
50.225.131.227	United States 	Texas	Houston
ISP	Organization	Latitude	Longitude
Comcast Cable Communications LLC	Not Available	29.7633	-95.3633

Physical Location Source: (IP Location, 2006-2008)

Part 3  
Data gathering and footprinting on [www.issaseries.com](http://www.issaseries.com)

This OSNIT <https://www.owler.com/company/issaseries> provides some more information about issaseries.com

Social Networking Sites  
<https://www.facebook.com/JBLCyber>  
<https://twitter.com/JBLearning>

Information available about issaseries.com Facebook page

The screenshot displays the Facebook profile of Jones & Bartlett Learning - Computer Science and Cybersecurity (@JBLCyber). The profile picture is a yellow square with a white lighthouse icon. The cover photo shows a world map with a blue overlay containing the text "JONES & BARTLETT LEARNING Computer Science and Cybersecurity @JBLcyber". Below the cover photo are buttons for "Like", "Share", "Suggest Edits", "Contact Us", and "Send Message". The "About" section is visible, showing contact information: "Call (800) 832-0034", "info@jblearning.com", and "http://www.issaseries.com". The "About" section also includes a description of the ISSA Series curriculum, which is a full curriculum solution for cyber security and cyber defense, comprising of texts, first-of-its-kind Virtual Security Cloud Labs, game-enhanced learning environments, with full instructor support.

## Whois issaseries.com

Data Gathering and Footprinting on a Targeted Web Site  
George Boakye  
2 hours remaining

Spade - [whois issaseries.com, finished]

issaseries.com | crsnic | 172.30.0.11

09/20/18 13:55:15 whois issaseries.com  
.com is a domain of USA & International Commercial  
Searches for .com can be run at <http://www.crsnic.net/>

whois -h whois.crsnic.net issaseries.com ...  
Domain Name: ISSASERIES.COM  
Registry Domain ID: 1601069669\_DOMAIN\_COM-VRSN  
Registrar WHOIS Server: whois.namecheap.com  
Registrar URL: <http://www.namecheap.com>  
Updated Date: 2018-05-08T07:32:12Z  
Creation Date: 2010-06-07T20:59:12Z  
Registry Expiry Date: 2019-06-07T20:59:12Z  
Registrar: NameCheap Inc.  
Registrar IANA ID: 1068  
Registrar Abuse Contact Email: [abuse@namecheap.com](mailto:abuse@namecheap.com)  
Registrar Abuse Contact Phone: +1.6613102107  
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Name Server: DNS01.ASCENDLEARNING.COM  
Name Server: DNS02.ASCENDLEARNING.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: <http://www.icann.org/wicf/>

issaseries.com [whois] | issaseries.com [ping]

For Help, press F1

powered by  
**Hatsize** Copyright 2018 Hatsize Corporation. All Rights Reserved.

## Ping issaseries.com

Data Gathering and Footprinting on a Targeted Web Site  
George Boakye  
2 hours remaining

Spade - [ping issaseries.com, finished]

issaseries.com | crsnic | 172.30.0.11

09/20/18 13:55:26 ping issaseries.com  
Ping issaseries.com (198.187.138.94) ...  
1 Addr: 198.187.138.94, RTT: 29ms, TTL: 242  
2 Addr: 198.187.138.94, RTT: 24ms, TTL: 242  
3 Addr: 198.187.138.94, RTT: 24ms, TTL: 242  
4 Addr: 198.187.138.94, RTT: 24ms, TTL: 242  
5 Addr: 198.187.138.94, RTT: 24ms, TTL: 242  
6 Addr: 198.187.138.94, RTT: 23ms, TTL: 242  
7 Addr: 198.187.138.94, RTT: 23ms, TTL: 242  
8 Addr: 198.187.138.94, RTT: 24ms, TTL: 242  
9 Addr: 198.187.138.94, RTT: 24ms, TTL: 242  
10 Addr: 198.187.138.94, RTT: 23ms, TTL: 242

issaseries.com [whois] | issaseries.com [ping]

For Help, press F1

powered by  
**Hatsize** Copyright 2018 Hatsize Corporation. All Rights Reserved.

## Nslookup issaseries.com

Data Gathering and Footprinting on a Targeted Web Site  
George Boakye  
2 hours remaining

Spade - [ping issaseries.com, finished]

Administrator: C:\Windows\system32\cmd.exe - nslookup

Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup

Default Server: google-public-dns-a.google.com  
Address: 8.8.8.8

> set type=any

> issaseries.com

Server: google-public-dns-a.google.com  
Address: 8.8.8.8

Non-authoritative answer:  
issaseries.com internet address = 198.187.138.94  
issaseries.com nameserver = dns01.ascendlearning.com  
issaseries.com nameserver = dns02.ascendlearning.com  
issaseries.com  
primary name server = dns01.ascendlearning.com  
responsible mail addr = admin.jbpub.com  
serial = 2014013026  
refresh = 1200 (20 mins)  
retry = 600 (10 mins)  
expire = 1209600 (14 days)  
default TTL = 300 (5 mins)

powered by  
**Hatsize** Copyright 2018 Hatsize Corporation. All Rights Reserved.

## Tracert issaseries.com

Data Gathering and Footprinting on a Targeted Web Site  
George Boakye  
2 hours remaining

Spade - [ping issaseries.com, finished]

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>tracert issaseries.com

Tracing route to issaseries.com [198.187.138.94]  
over a maximum of 30 hops:


Hop	Source	Destination	Source IP	Destination IP	Source Port	Destination Port	Source MAC	Destination MAC	Source ASN	Destination ASN	Source Org	Destination Org
1	<1 ms	<1 ms	<1 ms	192.168.230.254								
2	<1 ms	<1 ms	<1 ms	172.18.249.252								
3	<1 ms	<1 ms	<1 ms	172.18.0.2								
4	1 ms	1 ms	1 ms	76.75.74.129								
5	<1 ms	1 ms	<1 ms	216.168.115.173								
6	1 ms	1 ms	1 ms	xe2-0-0.core1.toronto3.nexicom.net	[66.79.244.146]							
7	1 ms	<1 ms	<1 ms	xe-8-1-3.edge1.Toronto2.Level3.net	[4.59.183.165]							
8	*	22 ms	22 ms	ae-2-7.bear1.Cincinnati1.Level3.net	[4.69.210.229]							
9	22 ms	22 ms	22 ms	CYRUSONE-IL.bear1.Cincinnati1.Level3.net	[4.15.99.234]							
10	21 ms	22 ms	22 ms	209.172.217.201								
11	24 ms	23 ms	23 ms	teng-1-1.core0-ev.cncndc.net	[67.208.157.6]							
12	24 ms	24 ms	23 ms	216-195-64-78.cncndc.net	[216.195.64.78]							
13	24 ms	24 ms	24 ms	www.informedpublishing.com	[198.187.138.94]							
14	24 ms	23 ms	23 ms	www.informedpublishing.com	[198.187.138.94]							

Trace complete.

C:\Users\Administrator>

powered by  
**Hatsize** Copyright 2018 Hatsize Corporation. All Rights Reserved.

*Physical Location of issaseries.com*

Domain Name	Country	Region	City
issaseries.com	United States 	Massachusetts	Boston
ISP	Organization	Latitude	Longitude
Ascend Learning LLC	Not Available	42.3584	-71.0598

*issaseries.com Canada location as shown in Traceroute and contact person*

Questions?

United States:

[Contact Your Account Specialist](#)

Canada:

**Nelson Education, Ltd**

1120 Birchmount Road  
Toronto, Ontario M1K5G4  
Canada

Phone [\(416\) 752-9448](tel:(416)752-9448) | [\(800\) 268-2222](tel:(800)268-2222)

Fax [\(416\) 752-8101](tel:(416)752-8101) | [\(800\) 430-4445](tel:(800)430-4445)

For orders:

[nelson.orderdesk@nelson.com](mailto:nelson.orderdesk@nelson.com)

For all other inquiries:

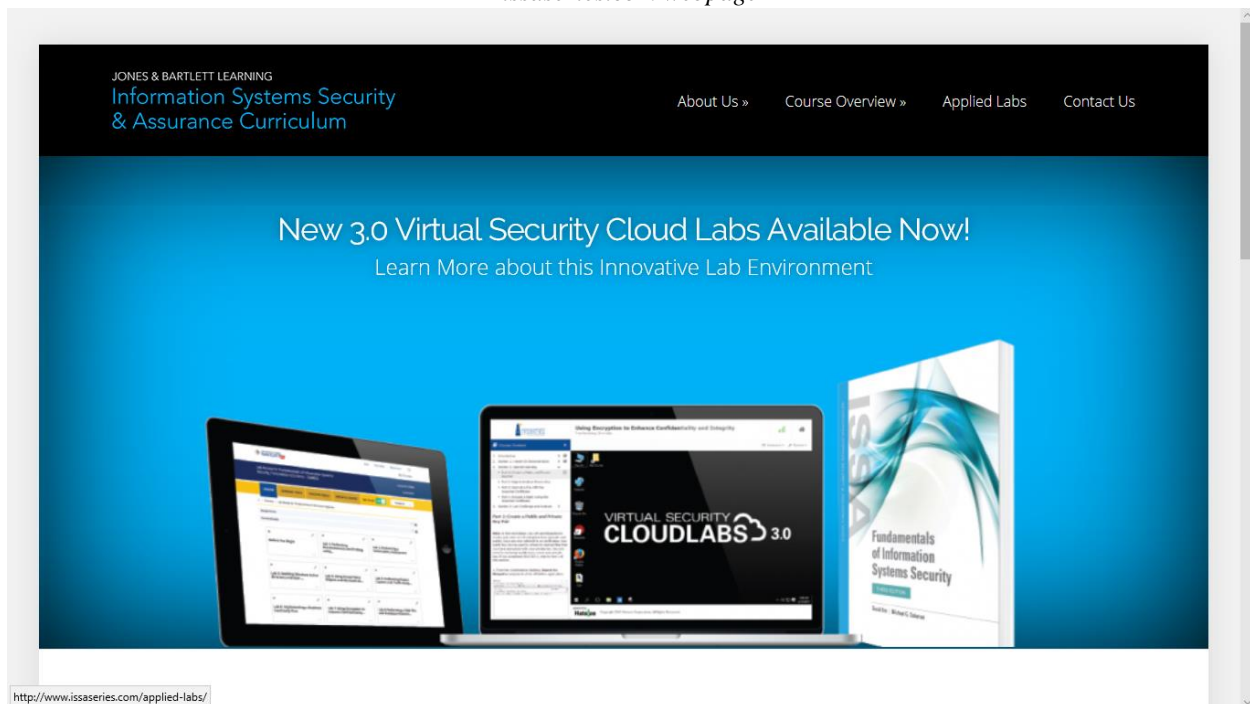
[nelson.her@nelson.com](mailto:nelson.her@nelson.com)

*issaseries.com Canada location street view (Google map)*

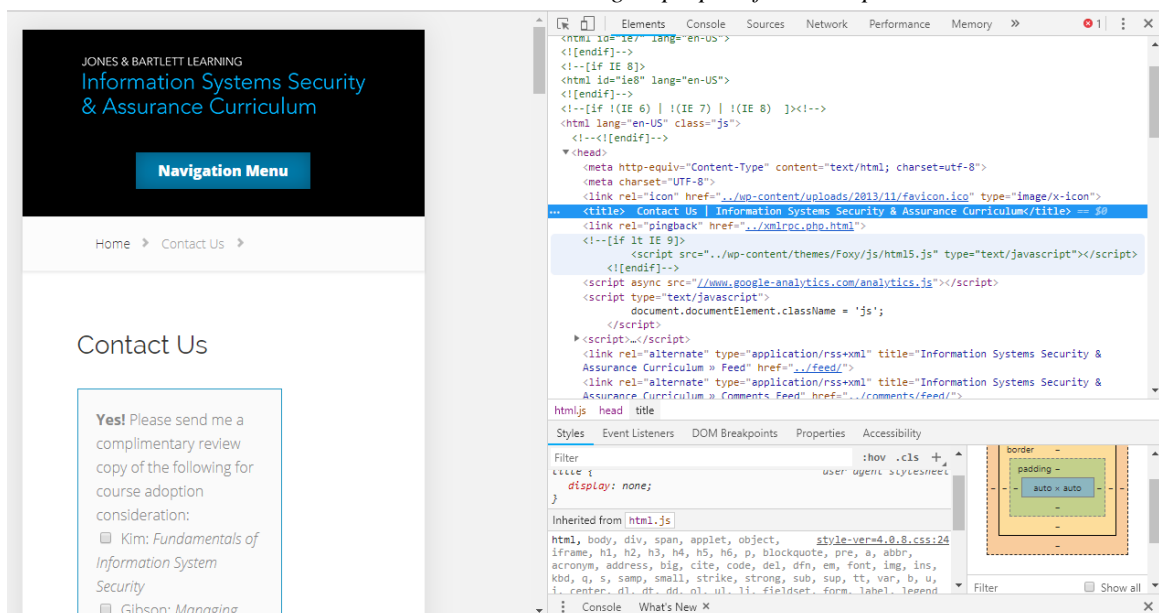




## issaseries.com webpage



## issaseries.com source code showing its purpose for development



## References

*eBay*. (1995-12018). Retrieved from ebay: <https://www.ebayinc.com/our-company/>

*IP Location*. (2006-2008). Retrieved from <https://www.iplocation.net/>

Kessler, G. C. (2001, May). *Sam Spade: A Multifunction Information Toolkit*. Retrieved from [https://www.garykessler.net/library/is\\_tools\\_sam\\_spade.html](https://www.garykessler.net/library/is_tools_sam_spade.html)

Pines, L. (2018, July 18). Retrieved from Investopedia:  
<https://www.investopedia.com/articles/insights/052716/top-4-ebay-shareholders-ebay.asp>